# Lecture Notes

for

# Elementary Set Theory

## Part III

Textbook By
Richard P. Millspaugh
University of North Dakota

Lecture Notes Prepared By
Bryce A. Christopherson
University of North Dakota

# Lecture Notes for Elementary Set Theory

# Chapter 6

# The Real Numbers

## Introduction

We now turn our attention to developing a mathematical description of the real numbers. All of the results of calculus can be derived from these basic properties of the real number system, which is usually done in a first course in real analysis. Our basic assumptions about the real numbers are called axioms, and they are divided into several groups. Many of these axioms will be familiar to you from previous courses in algebra.

## 6.1

## Field Axioms

Taken as a group, the field axioms tell us that the real numbers together with the operations of addition and multiplication form what is known as a *field*. Very informally, you might think of a field as something that satisfies the usual rules you encountered in high school algebra. Fields and related objects are studied in more depth in a course in abstract algebra.

**Definition 6.1.** The set of real numbers $\mathbb{R}$ is a collection of objects together with the two binary operations addition and multiplication that satisfy the following properties (known as the field axioms):

(i) Commutative Laws: For every $a, b \in \mathbb{R}$, $a + b = b + a$ and $ab = ba$.

(ii) Associative Laws: For every $a, b, c \in \mathbb{R}$, $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

(iii) Distributive Law: For every $a, b, c \in \mathbb{R}$, $a(b + c) = ab + ac$.

(iv) Identities: There are distinct elements 0 and 1 in $\mathbb{R}$ such that $a \cdot 1 = a$ and $a + 0 = a$ for every $a \in \mathbb{R}$.

(v) Additive Inverses: For every $a \in \mathbb{R}$, there is an element $-a \in \mathbb{R}$ such that $a + (-a) = 0$.

(vi) Multiplicative Inverses: For every $a \in \mathbb{R}$ with $a \neq 0$, there is an element $a^{-1} \in \mathbb{R}$ such that $aa^{-1} = 1$.

Any set of objects satisfying all of these properties is a *field*.

Other examples of fields include the fields of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$. As we develop further axioms for the real numbers, we will also narrow the list of fields that satisfy all of the axioms.

A number of the familiar algebraic properties of the real numbers are immediate consequences of the field axioms. A few of them are collected in the following theorem, though there are certainly many others.

**Theorem 6.2.** *For any real numbers $a, b, c$, the following are true:*

*(i) If $a + b = a + c$, then $b = c$.*

*(ii) $-(-a) = a$.*

*(iii) If $a \neq 0$ and $ab = ac$, then $b = c$.*

*(iv) If $a \neq 0$, then $(a^{-1})^{-1} = a$.*

*(v) $a \cdot 0 = 0$.*

*(vi) $-a = (-1)a$.*

*(vii) If $ab = 0$, then $a = 0$ or $b = 0$.*

*Proof.*

# 6.2

## Order Axioms

As noted previously, there are a number of common fields. One of the differences between $\mathbb{R}$ and $\mathbb{C}$ is that we think of the real numbers as lying in order along a line. There is no natural way to organize the complex numbers in this fashion. The next group of axioms make precise what we mean when we say that the real numbers form an *ordered field*.

**Order Axioms.** There is an order $<$ defined on the real numbers $\mathbb{R}$ satisfying:

(i) Transitivity: If $a < b$ and $b < c$, then $a < c$.

(ii) Trichotomy: For every two real numbers $a$ and $b$, exactly one of the following holds:

$$a < b \quad \text{or} \quad a = b \quad \text{or} \quad b < a$$

(iii) If $a < b$, then $a + c < b + c$ for every $c \in \mathbb{R}$.

(iv) If $a < b$ and $c > 0$, then $ac < bc$.

We derive several consequences of the fact that $\mathbb{R}$ is an ordered field.

**Theorem 6.3.** *The following statements are true in* $\mathbb{R}$*:*

*(i)* $a > 0$ *iff* $-a < 0$.

*(ii) If* $a < b$*, then* $-a > -b$.

*(iii) If* $a \neq 0$*, then* $a^2 > 0$.

*(iv)* $1 > 0$.

*Proof.*

**Theorem 6.4.** *Let $a, b \in \mathbb{R}$.*

*(i) If $a > 0$ and $b > 0$, then $ab > 0$.*

*(ii) If $a < 0$ and $b < 0$, then $ab > 0$.*

*(iii) If $a > 0$ and $b < 0$, then $ab < 0$.*

**Theorem 6.5.** *Let $a \in \mathbb{R}$.*

*(i) If $a > 0$, then $a^{-1} > 0$.*

*(ii) If $a < 0$, then $a^{-1} < 0$.*

*Proof.*

**THEOREM 6.6.** *Let $a \geq 0$ and $b \geq 0$. Then $a < b$ iff $a^2 < b^2$.*

*Proof.*

## 6.3 Completeness of the Reals

Our axioms so far insure that $\mathbb{R}$ is an ordered field. The field $\mathbb{Q}$ of rational numbers is also an ordered field, so we need something further to distinguish between $\mathbb{R}$ and $\mathbb{Q}$. Our last axiom is based on the observation that the field $\mathbb{Q}$ has *holes*, whereas $\mathbb{R}$ does not. Let's first consider an example to clarify what we mean by this.

**Example 6.7.**

### 6.3.1 Upper and lower bounds

**Definition 6.8.** Let $A$ be a nonempty set of real numbers. We say that a number $u$ is an *upper bound* for $A$ if $x \leq u$ for every $x \in A$. We say that a number $m$ is a *lower bound* for $A$ if $x \geq m$ for every $x \in A$. We say that $A$ is *bounded above* if $A$ has an upper bound, that $A$ is *bounded below* if $A$ has a lower bound, and that $A$ is *bounded* if $A$ is bounded above and below.

**Example 6.9.**

The previous example illustrates several things. It is possible for a nonempty set to have both upper and lower bounds, just one bound, or no bounds at all. Upper and lower bounds may or may not be elements of the set. Finally, upper and lower bounds are not unique. Transitivity implies that if M is an upper bound for a set A, then every number larger than M is also an upper bound for A. Similarly, if $m$ is a lower bound for A then every number smaller than $m$ is a lower bound for A.

Consider the set $A = \{a \mid a^2 \leq 5\}$ from the previous example again. We claimed that 5 is an upper bound, and that is certainly true, but note that 3 is also an upper bound. In some sense this smaller upper bound is a "better" bound for A because it puts a tighter restriction on the size of the elements of A. This is approximately like saying that Grand Forks is a better way to describe the location of UND than North Dakota. In this sense the best possible upper bound would be the smallest one, if there is one. In this particular case, A has a smallest upper bound in $\mathbb{R}$ ($\sqrt{5}$) but not in $\mathbb{Q}$. This is the basic difference between $\mathbb{Q}$ and $\mathbb{R}$ that we wish to capture in an axiom. First, we need another couple of definitions.

**Definition 6.10.** Let A be a nonempty subset of $\mathbb{R}$. We say that a number $u$ is a *least upper bound* (LUB) for A if both of the following are true:

(i) For every $a \in A$, $a \leq u$.

(ii) For every upper bound $b$ of A, $u \leq b$.

We say that a number $m$ is a *greatest lower bound* (GLB) for A if both of the following are true:

(i) For every $a \in A$, $a \geq m$.

(ii) If $b$ is a lower bound for A, then $m \geq b$.

Note that a LUB is sometimes called a *supremum* and a GLB is sometimes called an *infimum*.

It is not hard to prove that, unlike upper bounds, a set can have only one least upper bound. This fact is made explicit in the following theorem, whose proof is left as a homework exercise.

**Theorem 6.11.** *Let* A *be a nonempty subset of* $\mathbb{R}$. *If $u$ and $v$ are least upper bounds for* A, *then $u = v$.*

The following theorem says that the least upper bound of a set must in some sense be "close to" the set.

**Theorem 6.12.** *Let* A *be a nonempty subset of* $\mathbb{R}$ *and let $u$ be the least upper bound for* A. *If $x < u$, then there is an element $a \in A$ such that $x < a$.*

*Proof.*

We are now ready to state our final axiom, which says that $\mathbb{R}$ is *complete*.

**The Completeness Axiom.** Let A be a nonempty subset of $\mathbb{R}$. If A has an upper bound, then A has a least upper bound.

There are a number of consequences of the Completeness Axiom, most of which are beyond the scope of this text. We will look at only a couple of them. We begin with the fairly intuitive seeming fact that for any real number $x$, there is a natural number larger than $x$.

**Theorem 6.13.** *(Archimedian Property) If $x \in \mathbb{R}$, then there is a number $n_x \in \mathbb{N}$ such that $x \leq n_x$.*

*Proof.*

We previously commented, without proof, that the Completeness Axiom would allow us to distinguish $\mathbb{R}$ from $\mathbb{Q}$. We will now make this explicit by proving that there is at least one real number that is not rational.[1] We proved previously (Theorem 2.18) that there is no rational number whose square is 2. We now show that the Completeness Axiom implies that there must be a real number $x$ with $x^2 = 2$.

**Theorem 6.14.** *There is a number $x \in \mathbb{R}$ such that $x^2 = 2$.*

*Proof.*

[1]In fact there are more irrational numbers than there are rational numbers, as we shall see in the final chapter.

# Chapter 7

# Introduction to Cardinality

## Introduction

What do we mean when we say that there are *four* suits in a standard deck of cards? More generally, what does it mean to count any collection of objects? Since you may no longer actually think about counting, it may help to watch a child who is just learning to count. Given four objects to count, the child is likely to point to each object in turn and count "one, two, three, four." In other words, the child is explicitly constructing a bijective function between the objects she is counting and the elements of the set $\{1, 2, 3, 4\}$. Our goal in this chapter is to extend this idea to infinite sets.

## 7.1 The Cardinality of a Set

Let $A$ and $B$ be two sets. We define the relation $\equiv$ by $A \equiv B$ if there is a bijective function $f : A \to B$. In this case we say that $A$ and $B$ are *equinumerous* or that they have the same *cardinality*. We define $A \preceq B$ to mean that there is an injective function $f : A \to B$. We may also write this as $B \succeq A$. We write $A \prec B$ to indicate that $A \preceq B$ and $A \not\equiv B$. Note: it is fairly common to use the notation $|A| = |B|$ rather than $A \equiv B$.

**Theorem 7.1.** *The relation $\equiv$ defined above is an equivalence relation.*

*Proof.*

Note that Theorem 7.1 allows us to say that two sets $A$ and $B$ have the same cardinality if we are able to find a bijection from $A$ to $B$ or a bijection from $B$ to $A$.

**Theorem 7.2.** *The relation $\preceq$ is reflexive and transitive.*

*Proof.*

While we would probably not expect $\preceq$ to be symmetric, it wouldn't be too surprising if it was antisymmetric. If $A \preceq B$ and $B \preceq A$, does it follow that $A \equiv B$? George Cantor (1845-1918) was interested in just this question. One of his doctoral students, Felix Bernstein (1878-1956) was able to prove that the answer is yes. The resulting theorem is usually known as the Cantor-Bernstein Theorem.

**Theorem 7.3** (Cantor-Bernstein). *If $A \preceq B$ and $B \preceq A$, then $A \equiv B$.*

We defer the proof of this theorem to the Appendix. The following example uses the same ideas as the proof in order to construct a bijection between the open interval $(-1, 1)$ and the closed interval $[-1, 1]$.

**Example 7.4.**

# 7.2

## Finite Sets

**Question 7.5.** What does it mean to say that a set A is finite?

At first glance, this may seem like something you've known for a long time. Don't we just mean that we can count the elements of A? If so, is the number of cells in your body finite? Can you count them? Maybe the answer to our question isn't quite so obvious after all.

Let's try to make our answer a bit more precise. First, for any natural number $n$ we define the set $\mathbb{N}_n = \{k \in \mathbb{N} \mid k \leq n\}$. So $\mathbb{N}_4 = \{1, 2, 3, 4\}$, for example.

Next, we use the sets $\mathbb{N}_n$ to formalize the idea of counting introduced in the introduction to this chapter. We say that a set A has $n$ elements if $\mathbb{N}_n \equiv \mathrm{A}$.

Now it seems that we can say the set A is finite if A has $n$ elements for some $n \in \mathbb{N}$. Almost, but we're still forgetting something. Is the empty set finite? Clearly we would like to say that the empty set has zero elements, making it finite. This doesn't quite fit our scheme, so we must treat the empty set as a special case. In keeping our previous idea, here is one way to do so.

**Definition 7.6.** Let A be a set. If $\mathrm{A} = \emptyset$, we say that A has 0 elements. If $\mathrm{A} \equiv \mathbb{N}_n$ for some $n \in \mathbb{N}$, we say that A has $n$ elements. Finally, we say that A is *finite* if it has $n$ elements for some $n \in \mathbb{N} \cup \{0\}$. We say that A is *infinite* if it is not finite.

Applying Theorem 5.13 and Problem 7.1 from the homework, we obtain the following:

**Theorem 7.7.** *If* A *is finite, then* $\mathrm{A} \preceq \mathbb{N}$.

Now that we have a definition of finite, let's reconsider the set C of cells in your body. Is C finite? If so, for which $n$ is $\mathrm{C} \equiv \mathbb{N}_n$? We still can't really count them, so perhaps we've just obscured the question rather than answering it. Scientists estimate that there are about 10,000,000,000,000 cells in the average adult human body. That's not an actual count of the number of cells in any individual human body, though. These kinds of estimates are based on the sizes of various kinds of cells and the approximate proportion of each kind of cell in the body. In fact, we could determine the maximum number of cells that might be in a person's body by figuring out how many of the smallest kinds of cells would be required to build a body of a particular volume, or weight, etc. It seems reasonable to think that we could say a set was finite if we were sure it had at most $n$ elements for some natural number $n$. That is the intent of the next result.

**Theorem 7.8.** *If* $\mathrm{A} \preceq \mathbb{N}_n$ *for some natural number* $n$*, then* A *is finite.*

Before attempting to prove this result, let's make sure we understand what we are trying to prove. We are assuming that there is an injective function $f : A \to \mathbb{N}_n$. Unfortunately, our definition of finite requires us to produce a bijective function to some $\mathbb{N}_k$ and the function $f$ is probably not bijective. Since $f$ is injective, the potential difficulty is that there are extra elements of $\mathbb{N}_n$ (i.e. $f$ is not surjective). This seems like something we should be able to overcome without much difficulty since a set with fewer elements than some finite set should certainly be finite. How do we construct the required bijection though? Let's first consider a simpler result which will prove useful.

**Lemma 7.9.** *Let $f : A \to \mathbb{N}_n$ be an injective function that is not surjective. Then there is an injective function $g : A \to \mathbb{N}_{n-1}$.*

*Proof.*

We will now prove the theorem.

*Proof of Theorem 7.8.*

We conclude this section with a question, the answer to which may seem obvious to you.

**Question 7.10.** If $m, n \in \mathbb{N}$ and $m \neq n$, can you prove that $\mathbb{N}_m \not\approx \mathbb{N}_n$?

# 7.3

## Denumerable Sets

George Cantor was able to define a complete system of infinite numbers and of arithmetic on those numbers. We will not discuss his system here, but we will look at one particular kind of infinite number that is important in many areas of mathematics.

**Theorem 7.11.** *If $A$ is an infinite set and $B$ is a finite subset of $A$, then the set $A \setminus B$ is infinite.*

*Proof.*

**Definition 7.12.** Let $A$ be a set. We say that $A$ is:

- *denumerable* if $A \equiv \mathbb{N}$.
- *countable* if $A$ is either finite or denumerable.
- *uncountable* if $A$ is infinite and not denumerable.

**Example 7.13.**

The preceding example points out a very important difference between finite and infinite sets. The set $A$ is a proper subset of $\mathbb{N}$, but has the same cardinality as $\mathbb{N}$. All infinite sets have proper subsets of the same cardinality. In fact, this property is sometimes used to define what it means for a set to be infinite.

We would like to determine which of our results about finite sets are also true for denumerable sets. If $A$ and $B$ are denumerable, must $A \cup B$ also be denumerable? Are subsets of denumerable sets denumerable? Is there an analog of Theorem 7.8? Are there other ways to tell that a set is denumerable?

**Theorem 7.14.** *If* $A$ *is a denumerable set and* $B \equiv A$*, then* $B$ *is denumerable.*

*Proof.* By definition we have $A \equiv \mathbb{N}$. Since $\equiv$ is an equivalence relation, it follows that $B \equiv \mathbb{N}$ as desired.

**Theorem 7.15.** *If* $A \subset \mathbb{N}$*, then* $A$ *is countable.*

*Proof.*

Applying Theorem 7.15, Theorem 5.13, and Corollary 5.14 we have:

**Corollary 7.16.** *A subset of a countable set is countable.*

**Corollary 7.17.** *A set* $A$ *is countable if and only if* $A \preceq \mathbb{N}$.

Note that this Corollary allows us to say that a set $A$ is countable if we can find an injection from $A$ to $\mathbb{N}$. This is equivalent to finding a surjection from $\mathbb{N}$ to $A$, as you will show in Problem 7.8 in the homework. This allows us to conclude the following:

**Corollary 7.18.** *A set* $A$ *is countable if either of the following is true:*

*(i) There is an injection* $f : A \to \mathbb{N}$.

*(ii) There is a surjection* $f : \mathbb{N} \to A$.

**Theorem 7.19.** *The union of two denumerable sets is denumerable.*

*Proof.*

Using Mathematical Induction on the number of sets, we obtain:

**Corollary 7.20.** *The union of finitely many denumerable sets is denumerable.*

**Theorem 7.21.** *The set* $\mathbb{N} \times \mathbb{N}$ *is denumerable.*

*Proof.*

### 7.3.1 The Rationals

At first glance it may seem that there are more rational numbers than there are natural numbers. After all, there are infinitely many rational numbers between any two natural numbers. One of Cantor's accomplishments was to show that the set of rational numbers is actually denumerable. Our intuition developed from years of working with finite sets just doesn't serve us very well when working with infinite sets.

**Lemma 7.22.** *The set $\mathbb{Q}^+$ of positive rational numbers is countable.*

*Proof.*

Since the function taking every positive rational to it's additive inverse is bijective, the following Corollary follows immediately from our Lemma.

**Corollary 7.23.** *The set $\mathbb{Q}^-$ of negative rational numbers is countable.*

We know that $\mathbb{Q}^+$, $\mathbb{Q}^-$, and $\{0\}$ are all countable sets. Applying Problem 7.10 from the homework, we may conclude that:

**Theorem 7.24.** *The set of $\mathbb{Q}$ of rational numbers is countable.*

[1]While it is not necessary for the purposes of this example, it is not to difficult to show that the function $f$ defined here is actually bijective.

### 7.3.2 The Reals

By this point it may seem possible that all sets are countable, making denumerability a useless distinction. We will show that this is not true by demonstrating that the set of real numbers is uncountable. First recall that every real number can be written as an infinite decimal. There is one danger in using such representations, it is possible to have different decimal representations that represent the same real number: e.g. $1.0\overline{0} = 0.9\overline{9}$. There is only one way that this can happen, though. A real number with a decimal expansion ending in an infinite string of 0's also has an expansion ending in an infinite string of 9's. If we disallow expansions ending in a string of 0's (the decimal expansions we normally think of as terminating), the infinite decimal representation of each real number is unique. This is important in the following proof since we will want to know that real numbers with different infinite decimal expansions are distinct.

**Theorem 7.25.** *The set $\mathbb{R}$ of real numbers is uncountable.*

*Proof.*

# Chapter 8

# The Cantor-Bernstein Theorem

In this chapter we present a proof of the Cantor-Bernstein Theorem. The proof uses the same idea we used to construct the bijection between an open interval and a closed interval in Example 7.4. First we introduce some convenient notation.

Let $f : X \to Y$ be any function. For $A \subset X$, the *image* of A is the set $f(A) = \{f(x) \mid x \in A\}$. For $B \subset Y$ we use $f^{-1}(B)$ to denote the set $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$. The set $f^{-1}(B)$ is called the *preimage* of B. We also use the notation $f^{-1}(x)$ to denote $f^{-1}(\{x\})$. You should not assume from our use of this notation that the function $f$ is invertible! If $f : X \to X$ we use the notation $f^2$ to denote the function $f \circ f : X \to X$. Recursively, for a natural number $n \geq 2$, $f^{n+1}$ is used to denote the function $f \circ f^n : X \to X$. Finally, we define $f^0$ to be the identity function on X.

**Conjecture 8.1** (Cantor-Bernstein). *If* $X \preceq Y$ *and* $Y \preceq X$*, then* $X \equiv Y$.

*Proof.*