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

6 The Real Numbers **1**

6.1 Field Axioms 1

6.2 Order Axioms 5

6.3 Completeness of the Reals 8

6.3.1 Upper and lower bounds 8

7 Introduction to Cardinality **13**

7.1 The Cardinality of a Set 13

7.2 Finite Sets 16

7.3 Denumerable Sets 19

7.3.1 The Rationals 23

7.3.2 The Reals 24

8 The Cantor-Bernstein Theorem **25**

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. We prove parts *(Item ii)*, *(Item iii)*, and *(Item vi)*. The remaining proofs are exercises.

We first show that *(Item ii)* is true. To see this, note that $-(-a)$ is the additive inverse of $-a$. The reader should justify each of the following steps:

$$\begin{aligned} a + (-a) &= 0 \\ &= -a + (-(-a)) \\ &= -(-a) + (-a) \end{aligned}$$

so $a + (-a) = -(-a) + (-a)$. We apply part *(Item i)* to see that $a = -(-a)$ as desired.

To prove *(item iii)*, suppose that $a \neq 0$ and $ab = ac$. Since $a \neq 0$, a has a multiplicative inverse a^{-1}. The reader should give a justification for each step of the following:

$$\begin{aligned} b &= 1 \cdot b \\ &= (a^{-1}a)b \\ &= a^{-1}(ab) \\ &= a^{-1}(ac) \\ &= (a^{-1}a)c \\ &= 1 \cdot c \\ &= c \end{aligned}$$

To prove *(Item vi)*, let a be any real number. Then:

$$\begin{aligned} a + (-1)a &= 1 \cdot a + (-1)a \\ &= a(1 + (-1)) \\ &= a \cdot 0 \\ &= 0 \end{aligned}$$

Hence $a + (-1)a = 0 = a + (-a)$ and we may apply part *(Item i)* to see that $(-1)a = -a$.

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. To prove part *(Item i)*, assume first that $a > 0$. We have:

$$\begin{aligned} a &> 0 \\ a + (-a) &> 0 + (-a) && \text{using Order Axiom 3)} \\ 0 &> -a \end{aligned}$$

The converse is similar and left as an exercise.

We next prove part *(Item ii)*. The reader should determine which axiom or theorem justifies each step of the following:

$$a < b$$

$$a + (-b) < b + (-b)$$

$$a + (-b) < 0$$

$$((-a) + a) + (-b) < (-a) + 0$$

$$-b < -a$$

The proofs of the remaining parts of the theorem are left to the reader.

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. To prove part *(Item i)* we assume $a > 0$ and apply Trichotomy. If $a^{-1} < 0$, then $1 = aa^{-1} < 0$ by Theorem 6.4, but this contradicts Theorem 6.3*(Item iv)*. If $a^{-1} = 0$, then we have $1 = aa^{-1} = a \cdot 0 = 0$, which again contradicts Theorem 6.3*(Item iv)*. The only remaining possibility is that $a^{-1} > 0$ as desired.

The proof of *(Item ii)* is similar and is left for the reader.

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

Proof. We assume throughout that $a \geq 0$ and $b \geq 0$. By Trichotomy we have exactly one of $a < b$, $a = b$, or $a > b$; we also have exactly one of $a^2 < b^2$, $a^2 = b^2$, or $a^2 > b^2$.

If $a < b$, then $a^2 < b^2$ by an application of Problem 6.8 from the homework (where you prove that if $a > b \geq 0$ and $c > d \geq 0$, then $ac > bd$).

If $a = b$, then $a^2 = b^2$.

If $a > b$, then $a^2 > b^2$ by another application of Problem 6.8 from the homework.

It now follows that $a < b$ if and only if $a^2 < b^2$.

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. *Let* A *and* B *be the following sets:*

$$A = \{q \in \mathbb{Q} \mid q > 0 \text{ and } q^2 \leq 2\}$$

$$B = \{x \in \mathbb{R} \mid x > 0 \text{ and } x^2 \leq 2\}$$

As we will show in Theorem 6.14, there is a real number $\sqrt{2}$ *whose square is 2. The number* $\sqrt{2}$ *is in* B *and* $\sqrt{2}$ *is larger than every other number in* B.

As we showed in Theorem 2.18, there is no rational number whose square is 2. It can be shown that for every number in A*, there are larger numbers that are also in* A.

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. *Let* $A = \{a \mid a^2 < 5\}$, $B = [0, 7)$, $C = \mathbb{N}$, *and* $D = \mathbb{Z}$.

The number 5 *is an upper bound for* A *and* -3 *is a lower bound for* A.

The set B *has an upper bound at* 7 *and a lower bound at* 0.

The set C *has a lower bound at* 1, *but no upper bound.*

The set D *has no upper or lower bounds.*

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. Suppose that u is the least upper bound for A and that $x < u$. Assume that there is no $a \in A$ such that $x < a$, then $a \leq x$ for every $a \in A$ by Trichotomy. It follows by definition that x is an upper bound for A, but this contradicts the fact that u is the least upper bound for A since $x < u$.

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. Assume to the contrary that there is a real number x so that $n < x$ for every natural number n. In this case x is an upper bound for the set $\mathbb{N}$. Applying the Completeness Axiom, $\mathbb{N}$ must have a least upper bound m in $\mathbb{R}$. Since $m - 1 < m$, Theorem 6.12 implies that there is a natural number n such that $m - 1 < n$. Now $n + 1$ is also a natural number and $m < n + 1$, which contradicts the fact that m is an upper bound for $\mathbb{N}$.

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. Let $A = \{a \in \mathbb{R} \mid a^2 \leq 2\}$. Note that A is not empty since $1 \in A$. We claim that 2 is an upper bound for A. To see this note that if $t > 2$, then $t^2 > 2 \cdot 2 = 4 > 2$ (see problem 6.18 in the homework), so $t \notin A$. Since A is a nonempty subset of $\mathbb{R}$ that is bounded above, A must have a least upper bound x. We will use Trichotomy to show that $x^2 = 2$.

Assume first that $x^2 < 2$. Note that $\dfrac{2x+1}{2-x^2}$ is a positive real number. By the Archimedian Property there must be a natural number n such that $n > \dfrac{2x+1}{2-x^2}$. Since $n > \dfrac{2x+1}{2-x^2} > 0$, it follows that $\dfrac{1}{n} < \dfrac{2-x^2}{2x+1}$. We will show that $x + \dfrac{1}{n} \in A$, which will

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

contradict the fact that x is an upper bound for A. To see that $x + \frac{1}{n} \in$ A, we compute:

$$\begin{aligned}\left(x + \frac{1}{n}\right)^2 &= x^2 + \frac{2x}{n} + \frac{1}{n^2} \\ &= x^2 + \frac{1}{n}\left(2x + \frac{1}{n}\right) \\ &\leq x^2 + \frac{1}{n}(2x + 1) \\ &< x^2 + (2 - x^2) \\ &= 2\end{aligned}$$

Now $x + \frac{1}{n} \in$ A, which leads to the desired contradiction. It follows that $c^2 < 2$ cannot hold.

Next suppose that $x^2 > 2$. In this case $\frac{2x}{x^2 - 2}$ is a positive number and we may find $m \in \mathbb{N}$ such that $m > \frac{2x}{x^2 - 2}$. This in turn implies that $\frac{1}{m} < \frac{x^2 - 2}{2x}$. We show that $(x - \frac{1}{m})^2 > 2$:

$$\begin{aligned}\left(x - \frac{1}{m}\right)^2 &= x^2 - \frac{2x}{m} + \frac{1}{m^2} \\ &> x^2 - \frac{2x}{m} \\ &> x^2 - (2x)\frac{x^2 - 2}{2x} \\ &= 2\end{aligned}$$

Now Theorem 6.6 implies that if $s > x - \frac{1}{m}$, then $s^2 > (x - \frac{1}{m})^2 > 2$, so $x - \frac{1}{m}$ is an upper bound for A. This would contradict the fact that x is the least upper bound for A, so $x^2 > 2$ cannot hold.

The only possibility left is that $x^2 = 2$ as desired.

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. Let A, B, and C be arbitrary sets.

Since the identity function on any set is a bijection, $A \equiv A$ and $\equiv$ is reflexive.

If $A \equiv B$, then there is a bijection $f : A \to B$. Applying Theorem 5.15, the function

f is invertible. By Problem 5.15 in the homework, the inverse function $f^{-1} : Y \to X$ is a bijection. Hence $B \equiv A$ and $\equiv$ is symmetric.

To see that $\equiv$ is transitive, suppose that $A \equiv B$ and $B \equiv C$. By definition there are bijective functions $f : A \to B$ and $g : B \to C$. Now apply Corollary 5.14 to see that $g \circ f : A \to C$ is a bijective function. Hence $A \equiv C$ and $\equiv$ is transitive. Therefore, $\equiv$ is an equivalence relation as desired.

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. Let A, B, and C be any sets. Since the identity function on any set is injective, $A \preceq A$ and $\preceq$ is reflexive. To see that $\preceq$ is transitive, suppose that $A \preceq B$ and $B \preceq C$. By definition there are injections $f : A \to B$ and $g : B \to C$. We apply Theorem 5.13 to see that the composition $g \circ f : A \to C$ is also injective, hence $A \preceq C$ as desired.

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. *Define the functions $f : (-1,1) \to [-1,1]$ and $g : [-1,1] \to (-1,1)$ by $f(x) = x$ and $g(x) = x/2$, respectively. It is easy to show that both of these functions are injective, so $(-1,1) \preceq [-1,1]$ and $[-1,1] \preceq (-1,1)$. The Canter-Bernstein Theorem implies that there must be a bijection between the open interval $(-1,1)$ and the closed interval $[-1,1]$, but the theorem itself doesn't tell us how to find such a bijection. We construct such a bijection here.*

We wish to find a bijective function $h : (-1,1) \to [-1,1]$. For most elements $x \in (-1,1)$ we want $h(x) = f(x) = x$. Unfortunately, if we let $h(x) = f(x)$ for all x, then the function is not bijective because $-1 \neq f(x)$ and $1 \neq f(x)$ for all $x \in (-1,1)$. We use the function g to help us fix this problem. Consider first the element $1 \in [-1,1]$. While $1 \neq f(x)$ for any x, there is an element of the open interval associated with 1 by g. In particular $g(1) = 1/2$. We could define h so that $h(1/2) = 1$ and $h(x) = f(x)$ for other $x \in (-1,1)$, but that creates a new problem. Now 1 is in the image of the function, but $1/2$ is not. To fix this we let $h(1/4) = 1/2$, because $g(1/2) = 1/4$. Of course, now $1/4$ is not in the image of h. We continue fixing one problem at a time using g, each time creating a new problem. Naturally, we will need to do the same with -1.

These particular functions are simple enough that we can write down a formula for the function h that we end up with. We end up defining $h : (-1,1) \to [-1,1]$ by

$$h(x) = \begin{cases} 2^{-(n-1)} & \text{if } x = 2^{-n} \text{ for some } n \in \mathbb{N} \\ -2^{-(n-1)} & \text{if } x = -2^{-n} \text{ for some } n \in \mathbb{N} \\ x & \text{otherwise} \end{cases}$$

We claim that this function is the desired bijection.

We first show that h is surjective. To see this, let $t \in [-1,1]$. If $t = 2^{-(n-1)}$ for some

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 $\mathbb{N}_n \equiv A$.

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 $A = \emptyset$, we say that A has 0 elements. If $A \equiv \mathbb{N}_n$ 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* $A \preceq \mathbb{N}$.

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 $C \equiv \mathbb{N}_n$? 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* $A \preceq \mathbb{N}_n$ *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. Since $f : A \to \mathbb{N}_n$ is not surjective, the set $B = \mathbb{N}_n \setminus f(A)$ is nonempty. Choose $b \in B$. If $b = n$, then $f(a) \neq n$ for any element $a \in A$ and we may define $g : A \to \mathbb{N}_{n-1}$ by $g(a) = f(a)$ for each $a \in A$. If $b \neq n$, we define g by:

$$g(a) = \begin{cases} f(a) & \text{if } f(a) \neq n \\ b & \text{if } f(a) = n \end{cases}$$

In either case $g : A \to \mathbb{N}_{n-1}$ is as desired since for all $a \in A$, $g(a) \neq n$.

It remains to be shown that g is injective. Suppose that $a_1, a_2 \in A$ and that $g(a_1) = g(a_2) = m$. If $m = b$, then by definition of g we have $f(a_1) = n = f(a_2)$. If $m \neq b$, then our definition of g implies that $f(a_1) = m = f(a_2)$. In either case we have $f(a_1) = f(a_2)$, so $a_1 = a_2$ because the function f is injective. Therefore g is injective as desired.

We will now prove the theorem.

Proof of Theorem 7.8. First note that if $A = \varnothing$, then A is finite by definition. We assume for the remainder of the proof that $A \neq \varnothing$. By hypothesis, there is an injective function $f_0 : A \to \mathbb{N}_n$ for some natural number n. If f_0 is also surjective, then we have the desired

bijection. If f_0 is not surjective, then we may apply Lemma 7.9 to find an injection $f_1 : A \to \mathbb{N}_{n-1}$. We now consider the function f_1.

If $f_1 : A \to \mathbb{N}_{n-1}$ is surjective, then f_1 is a bijection. If f_1 is not surjective, then we again apply Lemma 7.9 to find an injective function $f_2 : A \to \mathbb{N}_{n-2}$.

We continue this process recursively. If any of the injective functions $f_i : A \to \mathbb{N}_{n-i}$ are surjective, then we have the desired bijection and the proof is complete. We claim that this must occur for some $0 \leq i \leq n-1$. To see this, suppose that $f_{n-2} : A \to \mathbb{N}_2$ is not surjective. Applying Lemma 7.9 we find an injection $f_{n-1} : A \to \mathbb{N}_1$. Since $A \neq \emptyset$, we may choose $a \in A$. Now $f_{n-1}(a)$ must be an element of $\mathbb{N}_1 = \{1\}$, so $f_{n-1}(a) = 1$. It follows that f_{n-1} is surjective as desired.

We have shown that there is a bijective function $f_i : A \to \mathbb{N}_{n-1}$ for some $0 \leq i \leq n-1$, so $A \equiv \mathbb{N}_{n-i}$ and A is finite.

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 $\mathbb{N}_m \not\equiv \mathbb{N}_n$?

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. Suppose to the contrary that $A \setminus B$ is finite. It is easy to show that for any subset $B \subset A$, $A = B \cup (A \setminus B)$. Since both B and $A \setminus B$ are finite, it follows from Problem 7.4 in the homework that A is finite. This contradicts our hypothesis that A is infinite, so it must true that $A \setminus B$ is infinite.

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 set* $A = \{2k \mid k \in \mathbb{N}\}$ *of even natural numbers is denumerable. To see this, define the function* $f : \mathbb{N} \to A$ *by* $f(n) = 2n$*. It is routine to check that* f *is a bijection, so* $\mathbb{N} \equiv A$ *as desired.*

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 ≡ A, *then* B *is denumerable.*

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

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

Proof. If A is finite, then A is countable by definition.

Assume that A is infinite. We define a function $f : \mathbb{N} \to A$ as follows. Recall that every nonempty subset of $\mathbb{N}$ has a smallest element. Let $f(1)$ be the smallest element of $A_0 = A$. Since A is an infinite the set $A_1 = A \setminus \{f(1)\}$ is nonempty, so we may define $f(2)$ to be the smallest element of A_1. Continuing recursively, suppose that we have defined $f(1), \dots, f(n)$ for some $n \in \mathbb{N}$. Let $A_n = A \setminus \{f(1), \dots, f(n)\}$. Since $\{f(1), \dots, f(n)\}$ is finite, A_n is infinite by Theorem 7.11. In particular, A_n is nonempty and we may define $f(n+1)$ to be the smallest element of this set. Before showing that f is bijective we note the following facts that follow immediately from our construction:

(i) For every natural number n, $A \setminus A_n = \{f(1), \dots, f(n)\}$.

(ii) For every natural number n, $f(n) \geq n$.

(iii) For all natural numbers m, n, if $f(n) \in A_m$ then $m < n$.

(iv) For all natural numbers $m < n$, $f(n) \in A_m$.

(v) For all natural numbers $m \leq n$, $f(m) \notin A_n$.

For any two natural numbers $m < n$ we have shown that $f(n) \in A_m$ and $f(m) \notin A_m$, so $f(n) \neq f(m)$ and f is injective.

To see that f is surjective, let $k \in A$. We must show that $k = f(m)$ for some $m \in \mathbb{N}$. If $k = f(k)$, we are done. Otherwise we have $f(k) > k$. Now $f(k)$ is the smallest element of A_{k-1} and $k < f(k)$, so $k \notin A_{k-1}$. We also know that $k \in A$, so it follows that $k \in A \setminus A_{k-1} = \{f(1), \ldots, f(k-1)\}$. Therefore $k = f(n)$ for some $1 \leq n < k$ and f is surjective as desired.

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. Suppose that we are given any two denumerable sets A and B. By definition there are bijective functions $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$. We define a function $h : A \cup B \to \mathbb{N}$ by the following rule:

$$h(x) = \begin{cases} 2f(x) & \text{if } x \in A \\ 2g(x) + 1 & \text{if } x \notin A \end{cases}$$

We claim that h is an injection. To see this, let $x \neq y$ be two elements of $A \cup B$. If $x \in A$ and $y \notin A$, then $h(x) \neq h(y)$ since $h(x)$ is even and $h(y)$ is odd. Similarly if $x \notin A$ and $y \in A$, then $h(x) \neq h(y)$. If x and y are both in A, then $h(x) = 2f(x)$ and $h(y) = 2f(y)$, so $h(x) \neq h(y)$ because f is injective. Finally, if neither x nor y are in A, then $h(x) = 2g(x) + 1$ and $h(y) = 2g(y) + 1$, so $h(x) \neq h(y)$ because g is injective. In any case, we have shown that $h(x) \neq h(y)$ so $h : A \cup B \to \mathbb{N}$ is injective.

We have shown that $A \cup B \preceq \mathbb{N}$, so $A \cup B$ must be countable. Note however that the function h constructed above is not necessarily a bijection. (Do you see why?) To see that $A \cup B$ is actually denumerable, note that $A \subset A \cup B$. Applying Problem 7.1 from the homework, it follows that $A \preceq A \cup B$. Since $\mathbb{N} \preceq A$ we may apply Theorem 7.2 to obtain $\mathbb{N} \preceq A \cup B$. It now follows from the Cantor-Bernstein Theorem that $A \cup B \equiv \mathbb{N}$ as desired.

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. Since $\mathbb{N} \times \mathbb{N}$ is infinite, we need only show that it is countable. Define the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(a, b) = 2^{a-1}(2b - 1)$. We will show that f is injective, then apply Corollary 7.18 to obtain the desired result.

To see that f is injective, suppose that

$$2^{a-1}(2b - 1) = 2^{c-1}(2d - 1) \tag{7.1}$$

for $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. We show first that $a = c$. If not, then we may assume without loss of generality that $a < c$. Dividing both sides of Equation (7.1) by 2^{a-1} yields $(2b - 1) = 2^{c-a}(2d - 1)$. But this is a contradiction since the quantity on the left side of the

equation is odd and the quantity on the right is even. Since $a = c$, we may reduce Equation (7.1) to $(2b-1) = (2d-1)$, from which it follows that $b = d$. Now $(a,b) = (c,d)$ and f is injective as desired.[1]

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. Let $\mathbb{F} = \{\frac{a}{b} \mid a, b \in \mathbb{N}\}$ be the set of fractions whose numerators and denominators are natural numbers. We claim that $\mathbb{F} \equiv \mathbb{N} \times \mathbb{N}$. To see this, define $f : \mathbb{F} \to \mathbb{N} \times \mathbb{N}$ by $f\left(\frac{a}{b}\right) = (a,b)$. We leave it to you to show that f is a bijection (see Problem 7.7 in the homework), so $\mathbb{F} \equiv \mathbb{N} \times \mathbb{N}$. We may now apply Theorem 7.21 and Theorem 7.14 to see that $\mathbb{F}$ is denumerable. Since the positive rationals are exactly those numbers that can be expressed as fractions of natural numbers, the function taking each fraction in $\mathbb{F}$ to the corresponding rational number is a surjection from $\mathbb{F}$ onto $\mathbb{Q}^+$. We now apply Corollary 7.18 to see that $\mathbb{Q}^+$ is countable.

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. Suppose to the contrary that the set $\mathbb{R}$ is countable, then there is a surjection $f : \mathbb{N} \to \mathbb{R}$. For convenience we use the notation x_n to denote the n th digit to the right of the decimal place in the unique infinite decimal expansion of x. In particular, the n th digit to the right of the decimal place in the expansion of $f(m)$ will be denoted $f(m)_n$. For example if $f(2) = \pi = 3.141592\ldots$, then $f(2)_4 = 5$. We will construct a real number y such that $y \neq f(n)$ for any $n \in \mathbb{N}$, which contradicts the fact that f is surjective.

For each $n \in \mathbb{N}$, define:

$$y_n = \begin{cases} 1 & \text{if } f(n)_n = 9 \\ 9 & \text{if } f(n)_n \neq 9 \end{cases}$$

Next we define

$$y = \sum_{i=1}^{\infty} \frac{y_i}{10^i}$$

so $y = 0.y_1y_2y_3\ldots$. In other words, y is the unique real number in $(0, 1]$ such that the n th term to the right of the decimal place in the infinite decimal expansion of y is y_n. By definition, $y_n \neq f(n)_n$ for every $n \in \mathbb{N}$, so $y \neq f(n)$ for any $n \in \mathbb{N}$ as desired.

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. By hypothesis there exist injections $f : X \to Y$ and $g : Y \to X$. We will find a bijective function $h : X \to Y$ with the property that $h(x) = f(x)$ for most $x \in X$ and $h(x) = g^{-1}(x)$ (since g is injective, $g^{-1}(x)$ is always a single point) for the remaining $x \in X$. As in Example 7.4, we use $g^{-1}(x)$ only as necessary to insure that the final function is bijective.

For every point $y \in Y \setminus f(X)$, we define a sequence of points in X as follows: $x_1 = g(y)$, $x_2 = g(f(x_1)) = g \circ f(g(y))$, $x_3 = g(f(x_2)) = (g \circ f)^2(g(y))$, and in general $x_{n+1} = g(f(x_n)) = (g \circ f)^{n-1}(g(y))$ for each $n \in \mathbb{N}$. Note that since g is injective $g^{-1}(x_1)$ contains only the point y and that for $k \geq 2$, $g^{-1}(x_k)$ contains only the point x_{k-1}. Define the set

$$S = \{x \mid x = (g \circ f)^n(g(y)) \text{ for some } y \in Y \setminus f(X) \text{ and for some } n \in \mathbb{N} \cup \{0\}\}.$$

In other words, the set S contains every point of each of the sequences we created above. This set will be the set of points on which h is not the same as f.

Step 1: We prove the following facts about the set S.

(i) If $y \in Y \setminus f(X)$, then $g(y) \in S$.

(ii) If $x \in S$, then $g \circ f(x) \in S$.

(iii) If $g(f(x)) \in S$, then $x \in S$.

For $y \in Y \setminus f(X)$ we have $g(y) = (g \circ f)^0(g(y))$, so (i) is true.

If $x \in S$, then $x = (g \circ f)^n(g(y))$ for some $n \in \mathbb{N} \cup \{0\}$ and some $y \in Y \setminus f(X)$. Now $g \circ f(x) = (g \circ f)^{n+1}(g(y))$, so $g \circ f(x) \in S$ and (ii) holds.

To see that (iii) is true, suppose that $g(f(x)) = (g \circ f)^n(g(y))$ for some $y \in Y \setminus f(X)$ and some $n \in \mathbb{N} \cup \{0\}$. If $n = 0$ then we have $g(f(x)) = g(y)$. Since g is injective this would imply $y = f(x)$, which contradicts our choice of y. Hence $n \geq 1$ and the point $w = (g \circ f)^{n-1}(g(y))$ is an element of S by definition. Now $g \circ f(w) = (g \circ f)^n(g(y)) = g \circ f(x)$. But $g \circ f$ is injective by Theorem 5.13, so we have $w = x$ and $x \in S$ as desired.

Step 2: We now define the function $h : X \to Y$.

For $x \in X$ we define:

$$h(x) = \begin{cases} g^{-1}(x) & \text{if } x \in S \\ f(x) & \text{otherwise.} \end{cases}$$

Clearly $h(x)$ is defined for every $x \in X \setminus S$. If $x \in S$ then by definition $x = (g \circ f)^n(g(y))$ for some n and y, but this implies that $x \in g(Y)$ and $g^{-1}(x)$ is nonempty. We must also be sure that we have actually defined a function, i.e. that there is only one point in $g^{-1}(x)$ for each $x \in S$. To this end, suppose that y_1 and y_2 are each in $g^{-1}(x)$ for some $x \in S$. By definition we have $g(y_1) = g(y_2)$. Since g is injective this implies that $y_1 = y_2$ as desired. It remains to be shown that h is bijective.

Step 3: We show that h is surjective.

Let $z \in Y$. Either $g(z) \in S$ or not.

Case 1: If $g(z) \in S$, then $h(z) = g^{-1}(g(z)) = z$.

Case 2: Suppose $g(z) \notin S$. By (i) $z \notin Y \setminus f(X)$, so there is an $x \in X$ such that $f(x) = z$. Since $g(f(x)) = g(z) \notin S$, $x \notin S$ by (ii). Therefore $h(x) = f(x) = z$.

In either case we have shown that $z \in h(X)$, so h is surjective as desired.

Step 4: We show that h is injective, which will complete the proof of the theorem.

Suppose that $h(x_1) = h(x_2)$ for some $x_1, x_2 \in X$. We consider several cases.

Case 1: Suppose that neither of x_1 or x_2 are in S. Then $f(x_1) = h(x_1) = h(x_2) = f(x_2)$ and $x_1 = x_2$ because f is injective.

Case 2: Suppose both x_1 and x_2 are in S. Then $g^{-1}(x_1) = h(x_1) = h(x_2) = g^{-1}(x_2)$, so there is an element $y \in S$ so that $g(y) = x_1$ and $g(y) = x_2$. This implies that $x_1 = x_2$ because g is a function.

Case 3: Finally, suppose that $x_1 \in S$ and $x_2 \notin S$. In this case we have $g^{-1}(x_1) = h(x_1) = h(x_2) = f(x_2)$, so $x_1 = g(g^{-1}(x_1) = g(f(x_2))$ and $g(f(x_2)) \in S$. Applying (iii) it follows that $x_2 \in S$, which is a contradiction. Therefore this case is impossible. Clearly it is also impossible to have $x_1 \notin S$ and $x_2 \in S$.