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

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

The *identity relation on A* is defined by

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

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

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

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

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

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 $h(x) = x \quad \forall x \in P$.
(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. □

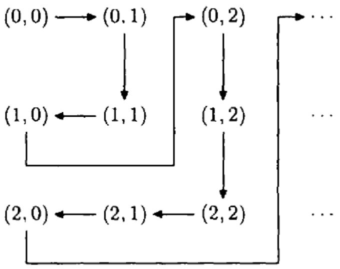
Corollary 8.9. *The union of a finite system of countable sets is countable.*

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 $S = \{n \in N \,|\, n \notin f(n)\}$. 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.