Set Theory

Patrick Oare

1 Introduction

Set theory provides the foundations for essentially all of modern mathematics. It is used in every mathematical field, often implicitly. In these notes, we will study how to make this foundation rigorous. We will study the axiomatization of set theory in such a way that properties of sets can be deduced from **only** the axioms which we decide upon. We will build upon these axioms and study how to construct different mathematical objects, including many objects that you may have studied before. Various number systems will also be constructed, so you can be at ease the next time you want to verify *why* $2 + 3 = 5$.

2 First Order Logic

Many of the axioms of set theory will be written down precisely in **first order logic**. This is a system which makes precise notions like "membership in" a set, as well as rules of logic like the symbols $\implies$, $\wedge$, $\vee$, and more. It is the *language* in which we make statements in set theory. We will treat first order logic briefly, as it is only needed in certain statements we will make later. A statement in first order logic contains the following **symbols**[1]:

- **Variables**: Letters like $x, y, z, a, b, ...$
- The symbols $\in$ and $=$.
- **Logical connectors**: $\wedge$ or & ("and"), $\vee$ ("or"), $\neg$ ("not"), $\implies$ ("implies"), $\iff$ ("equivalent").
- **Quantifiers**: $\exists$ ("exists"), $\forall$ ("for all").

Using symbols, we can write formulas, which are essentially just statements of truth. Formulas can have different types of variables, which may give different conditions of truth depending on context. As an example, consider the formula:

$$\phi(x) = \exists y \exists z((y \in z) \wedge (z \in x))$$

This is a first order formula because it only makes use of the symbols presented above. The variables y and z are called **bound variables**; they are bound by quantifiers to make it clear what context they are being used in for the formula. The variable x is a **free variable**; you are allowed to input a value for x yourself, and the formula will be either true or false. For example, $\phi(\emptyset)$ is true, yet $\phi(\{\{\emptyset\}\})$ is false. First order logic can be used to generate more complicated formulas or symbols to use, which can then be used to simplify different formulas. For example, we may write the symbol $a \subseteq b$ as shorthand for the formula $\forall t(t \in a \implies t \in b)$. Note that to specify exactly the elements of a set a, we will often write $\forall x(x \in a \iff ...)$.

[1] When asked to provide a first order formula, you must **only** use these symbols.

3 Axiomatization of Set Theory

When we study the properties of sets, we need to decide upon a common language: what exactly do we mean by a set? One will have an intuitive understanding of this question, but a rigorous set of axioms must be decided on before propositions may be proved. We will state the axioms of set theory here, and develop them further as we use them more. The first 9 axioms are the **Zermelo-Fraenkel (ZF) Axioms** of set theory, and they are widely accepted to be the foundations most of mathematics is built off of. The tenth axiom listed is the axiom of choice, and its acceptance is more controversial than the other 9. The system of all ten axioms is denoted **ZFC**, standing for ZF with Choice.

1. **Extensionality axiom**: If two sets have the same members, then they are equal.
$$\forall a \forall b (\forall x (x \in a \iff x \in b) \implies a = b) \tag{1}$$

2. **Empty set axiom**: There is a set $\emptyset$ which has no members.
$$\exists a \forall x \neg (x \in a) \tag{2}$$

3. **Pairing axiom**: For any sets u and v, there is a set $\{u, v\}$ whose members are exactly u and v.
$$\forall u \forall v \exists x (\forall z (z \in x \implies z = u \vee z = v)) \tag{3}$$

4. **Union axiom**: For any set a, there is a set b (denoted $\bigcup a$) whose members are precisely the members of members of a.
$$\forall a \exists b (\forall x (x \in b) \iff \exists c (c \in a \wedge x \in c)) \tag{4}$$

5. **Subset axiom**: For any set c and any first order formula $\Phi(x, t_1, ..., t_k)$, there is a set b whose elements are precisely the elements of c that satisfy $\Phi(x, t_1, ..., t_k)$.
$$\forall c \forall t_1, ..., t_k \exists b (\forall x (x \in b) \iff x \in c \wedge \Phi(b, t_1, ..., t_k)) \tag{5}$$

6. **Power set axiom**: For any set a, there is a set b (denoted $\mathcal{P}a$) whose elements are precisely the subsets of a.
$$\forall a \exists b (\forall x (x \in b) \iff \forall y (y \in x \implies y \in a)) \tag{6}$$

7. **Infinity axiom**: There exists an inductive set.
$$\exists a (\emptyset \in a \wedge \forall b \in a (b^+ \in a)) \tag{7}$$

8. **Replacement axiom**:

9. **Regularity axiom**:

10. **Axiom of choice**: For any relation R, there is a function $G \subseteq R$ such that $dom(G) = dom(R)$.
$$\forall a \forall R ((R \subset a \times a) \iff (\exists G \subseteq R)(dom(G) = dom(R))) \tag{8}$$

We will now discuss the importance of the first six axioms listed here. We will eventually have the tools needed to discuss Axioms 7 - 10 in depth, but at the moment these axioms are best studied after some additional knowledge is built up.

3.1 Extensionality and empty set axioms

These are the most basic axioms of set theory, yet give us a surprising amount of power. Extensionality allows us to know when two sets are equal; this is if they have exactly the same members, which is quite an obvious statement. However, using this axiom allows us to make well-defined definitions of types of sets; in other words, we can[2] specify a set using **set builder** notation. This is a completely unambiguous notation which allows one to specify a set's elements exactly. However, we will see later that we need the subset axiom to do this correctly, as simply defining the elements of a set does not prove that such a set **exists**.

The **empty set** axiom gives us our first element to work with in set theory. At the time this axiom is introduced, no sets actually exist; it is the first of its kind, which gives the empty set a special role in set theory. Without other axioms, the only set which exists is the empty set.

Theorem 3.1. There is a unique set which has no members

This follows immediately from its definition and the extensionality axiom.

3.2 Pairing and union axioms

The pairing axiom can be used in conjunction with the empty set axiom to start constructing sets, although these sets are rather limited. First, we can use the pairing axiom with $u = v = \emptyset$ to create the set $\{\emptyset\}$. We can then join together copies of these sets to create 2-element sets. However, it is severely limited; pairing can only be used to produce sets with two elements, and we should be able to produce sets with arbitrary amounts of elements. This is done precisely by the union axiom. The union of a set is unique, because as with all other sets, specifying exactly the elements as we have done means we may use the extensionality axiom. We denote the union of the set $\{c, d\}$ (which we note exists by pairing) by $c \cup d$. Given n sets $\{c_j\}_{j=1}^{n}$, we can inductively construct the union of this set by:

$$\bigcup_{j=1}^{n} c_j := \left(\bigcup_{j=1}^{n-1} c_j \right) \cup c_n \tag{9}$$

We can now build sets which have more than 2 elements. Suppose we wish to construct $\{a, b, c\}$. Then we can use the pairing axiom to build $\{a, b\}$ and the set $\{c\}$, then union these to form $\{a, b, c\}$, i.e. $\{a, b, c\} = \{a, b\} \cup \{c\}$.

As one final note on this subject, in proofs it is often easiest to use the following fact: we have $x \in \bigcup a$ if there is $b \in a$ such that $x \in b$.

3.3 Subset axiom

The subset axiom is necessary to prevent paradoxes which may be encountered when studying certain types of sets. The most famous example of this is **Russel's paradox**, which states that if the set $a = \{x : x \notin x\}$ exists, we have a contradiction. This leads to the following theorem.

Theorem 3.2. There is no set of all sets, i.e. there is no set which contains all other sets as elements.

Proof. Suppose that M was such a set. Then we can construct the set $\{x \in M : x \notin x\}$ and obtain Russell's paradox, a contradiction. □

[2] Almost; we must also prove the existence of the set which has been defined.

The easiest way to show a set exists is to exhibit that it is a subset of an existing set. This will be our method of proof when trying to construct sets. In other words, if you can use the set builder notation:

$$\{x \in a : \Phi(x, t_1, ..., t_k)\} \tag{10}$$

where a is a set which we have previously shown exists, then **this set exists**.

We can use the subset axiom to define the intersection of sets, which we will do in the following way.

Proposition 3.3. Let a and b be two sets. Then there is a unique set c whose elements are precisely the members of a and b, and c is unique.

Proof. Apply the subset axiom with the formula $\Phi(x, a, b) = x \in a \wedge x \in b$ to the set a, i.e. the set c is the following:

$$c = \{x \in a : x \in b\}$$

That c is unique follows from extensionality. □

Definition 3.1 (Intersection)**.** The set c is denoted $a \cap b$, and called the **intersection** of a and b.

Proposition 3.4. Let $A \neq \emptyset$. Then there is a set B, denoted $\bigcap A$ whose elements are precisely the sets which are members of **all** members of A.

Proof. $A \neq \emptyset$, so pick $c \in A$. Then we can construct the following set:

$$B = \{x \in c : \forall C(C \in A \iff x \in C)\}$$

□

3.4 Power set axiom and set algebra

The power set axiom is only needed for infinite sets; it would be possible to construct the power set of a finite set with the union and subset axioms we have already seen. Now that we can construct all subsets of any set, we can worry about how to deal with subsets and what operations we can use on them. Namely, we will discuss **set algebra** and how different operations relate to one another.

Definition 3.2 (Relative Complement)**.** For sets A, B, the **relative complement** of B in A is the set:

$$A \setminus B = \{x \in A : x \notin B\} \tag{11}$$

Now that we have all the major set operations, we can enumerate some important laws when dealing with set algebra. The first are the **distributive laws**:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (\bigcap B) = \bigcap\{A \cup b : b \in B\} \qquad A \cap (\bigcup B) = \bigcup\{A \cap b : b \in B\}$$

As important as these are **DeMorgan's laws**:

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B) \qquad C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$$

$$C \setminus (\bigcup A) = \bigcap\{C \setminus a : a \in A\} \qquad C \setminus (\bigcap A) = \bigcup\{C \setminus a : a \in A\}$$

3.5 Axiom of Choice

The axiom of choice is perhaps the most controversial axiom in set theory. Although it is quite intuitive, assuming this axiom often leads to many non-intuitive results, while at the same time gives one a very useful tool for proofs dealing with infinite sets.

TODO

4 Ordered Pairs, Relations, and Functions

We now turn to the discussion of ordered pairs, and how these will give us a way to define relations and functions. We will formalize the notion of an ordered pair and discuss how to write one explicitly as a set, then develop relations and functions as specific types of sets of ordered pairs.

4.1 Ordered Pairs

As you have most likely seen before, an ordered pair is an object of the form (a, b). We will seek to encode this pair specifically as a set. Note that (a, b) is a different object than $\{a, b\}$; to see this, $(a, b) \neq (b, a)$ unless $a = b$, while the sets $\{a, b\}$ and $\{b, a\}$ are equal. Ordered pairs also do not collapse under repeated elements, i.e. the ordered pair (a, a) does not equal the tuple (a). We will use the notation $\langle a, b\rangle$ interchangeably with (a, b).

Definition 4.1 (Ordered Pair)**.** Let x and y be sets. Then the **ordered pair** (x, y) is defined to be:

$$(x, y) := \{\{x\}, \{x, y\}\} \tag{12}$$

Proposition 4.1. If $(a, b) = (c, d)$, then $a = c$ and $b = d$.

Proof. Suppose that $(a, b) = (c, d)$. If $a = b$, then $(a, b) = \{\{a\}\}$ contains 1 element, so $\{c\} = \{c, d\} \implies c = d$, and so $\{\{a\}\} = \{\{c\}\}$, hence $a = b = c = d$. Suppose $a \neq b$. Then $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, hence $\{a\} = \{c\}$ and $\{a, b\} = \{c, d\}$ because the number of the elements in each of these sets are the same. Thus $a = c$ and $b = d$, so we are done. □

We see that this definition of an ordered pair indeed has the properties that we want; namely, that the order in the pair matters. We will now define the product of sets and prove that it exists.

Definition 4.2 (Cartesian Product)**.** If A and B are sets, the **Cartesian product** of A and B, denoted $A \times B$, is the set of pairs of the form (a, b) for $a \in A$ and $b \in B$.

To show that $A \times B$ exists for sets A and B, the easiest way to approach this is to use the subset axiom. Namely, we want to find a set which contains $A \times B$ as a subset.

Lemma 4.2. If $x \in A$ and $y \in B$, then $(x, y) \in \mathcal{P}\mathcal{P}(A \cup B)$.

The proof of this lemma is immediate from the definition of (x, y). It also proves the existence of $A \times B$ for given sets A and B, because we can see that:

$$A \times B = \{(a, b) \in \mathcal{P}\mathcal{P}(A \cup B) : a \in A, b \in B\}$$

For notation's sake, we will denote $A \times A$ by A^2. As another quick lemma, we have the following statement which is often useful to remember when we deal with relations in the next subsection.

Lemma 4.3. If $(x, y) \in A$, then x and y are in $\bigcup\bigcup A$.

Finally, note that now we have defined pairs, we can define n-tuples for $n \geq 1$. We will give an inductive definition as to not clutter the definitions.

Definition 4.3 (n-tuple)**.** For sets $x_1, ..., x_n$, we define the **n-tuple** to be:

$$(x_1, ..., x_n) := ((x_1, ..., x_{n-1}), x_n) \tag{13}$$

4.2 Relations and Functions

We begin with the definition of a relation, as well as some basic terminology we will need.

Definition 4.4 (Relation)**.** A **relation** is a set of ordered pairs. If R is a relation, we use the notation xRy to denote $(x, y) \in R$.

Definition 4.5. Let R be a relation. Then the **domain** of R is:

$$dom(R) := \{x : \exists y (x, y) \in R\} \tag{14}$$

The **range** of R is:

$$ran(R) := \{y : \exists x (x, y) \in R\} \tag{15}$$

The **field** of R is:

$$fld(R) := dom(R) \cup ran(R) \tag{16}$$

To prove that these sets exists, it suffices to show they are a subset of an already constructed set. Note that by Lemma 4.3, we know that $dom(R)$ and $ran(R)$ are subsets of $\bigcup\bigcup R$. Thus these sets do in fact exist. We now define the notion of a function.

Definition 4.6 (Function)**.** A **function** F is a relation such that for each $x \in dom(F)$, there is exactly one y with $(x, y) \in F$. This y is called the **image** of x under F, and denoted $y = F(x)$.

Definition 4.7. We say F is a function from A to B if $A = dom(F)$ and $ran(F) \subseteq B$. If $ran(F) = B$, we say that F is **surjective**. If for each $y \in ran(F)$ we have a unique x with $y = F(x)$, then we say F is **injective**.

This definition of a function is probably very different than what one would typically think of as a function; usually a function is thought of as an abstract rule which associates an output with any input, yet we just defined it as what is usually considered to be the **graph** of a function. However, this definition allows us to encode all the information from a function into a single set F, and so we now can use all of the axioms we have stated to deal with functions.

We now turn our attention to creating new relations from existing ones. We will apply these ideas to functions as well, as we will be able to specify things more precisely with functions.

Definition 4.8. Let R, S be relations.

1. The **inverse** of R is the relation:

$$R^{-1} := \{(v, u) : (u, v) \in R\} \tag{17}$$

2. The **composition** of R and S is the set:

$$R \circ S := \{(u, v) : \exists t (uSt \wedge tRv)\} \tag{18}$$

3. The **restriction** of R to a set A is the set:

$$R|_A := \{(u, v) : u \in A \wedge uRv\} \tag{19}$$

4. The **image** of a set A under R is:

$$R[A] := ran(R|_A) \tag{20}$$

To remember the definition $R \circ S$, think of these as functions $F \circ G$ acting on x. If $(x, z) \in F \circ G$, then $z = F(G(x))$, i.e. we can find y with $y = G(x)$ and $z = F(y)$, equivalently xGy and yFz. We will study composition in the specific case of functions.

Proposition 4.4. If F and G are functions, then $F \circ G$ is a function whose domain is:

$$dom(F \circ G) := \{x \in dom(G) : G(x) \in dom(F)\} \tag{21}$$

Proof. TODO. □

Definition 4.9 (Identity)**.** Let A be a set. Then we define the **identity function** of A to be:

$$I_A := \{(a, a) : a \in A\} \tag{22}$$

If $F : A \to B$ is a bijection, then F^{-1} is a function and $F \circ F^{-1} = I_B$, $F^{-1} \circ F = I_A$.

Theorem 4.5. Assume $F : A \to B$ and $A \neq \emptyset$.

1. There is a function $G : B \to A$ such that $G \circ F = I_A$ (a **left inverse**) iff F is injective.
2. There is a function $G : B \to A$ such that $F \circ G = I_B$ (a **right inverse**) iff F is onto B.

Proof. TODO. □

Note that to prove one direction of the surjective part of the theorem, we need to use the axiom of choice. Our original formulation of this axiom states that we can choose one element of the range of each element of a relation to turn it into a function.

Definition 4.10 (Single-rooted)**.** A relation R is **single-rooted** if for each $y \in ran(R)$, there is a unique $x \in dom(R)$ such that xRy.

Single rooted relations are the analogs of injective functions, and they are useful because they preserve certain equalities among the set algebra.

Theorem 4.6. Let R be a relation. Then for any set $\mathcal{A}$, we have the following.

1. $$R\left[\bigcup \mathcal{A}\right] = \bigcup_{A \in \mathcal{A}} R[A] \tag{23}$$

2. $$R\left[\bigcap \mathcal{A}\right] \subseteq \bigcap_{A \in \mathcal{A}} R\left[A\right] \tag{24}$$

   with equality iff R is single-rooted.

3. $$R\left[A \setminus B\right] \supseteq R\left[A\right] \setminus R\left[B\right] \tag{25}$$

   with equality iff R is single-rooted.

Proof. TODO □

These theorems give rise to immediate corollaries about the inverse relations of functions. These are extremely useful in areas of math like topology, where the preimage of open sets is used to determined if a function is continuous or not.

Lemma 4.7. For any function G and sets A, B, and $\mathcal{A}$, we have:

1. $$G^{-1}\left[\bigcup \mathcal{A}\right] = \bigcup\{G^{-1}[A] : A \in \mathcal{A}\} \tag{26}$$

2. If $\mathcal{A} \neq \emptyset$, we have: $$G^{-1}\left[\bigcap \mathcal{A}\right] = \bigcap\{G^{-1}[A] : A \in \mathcal{A}\} \tag{27}$$

3. $$G^{-1}[A \setminus B] = G^{-1}[A] \setminus G^{-1}[B] \tag{28}$$

4.3 Equivalence Relations

Definition 4.11. Let R be a relation on a set A. Then:

- R is **reflexive** if for each $x \in A$, xRx.
- R is **symmetric** if for all x, y, xRy implies yRx.
- R is **transitive** if for all x, y, z, xRy and yRz implies that xRz.

Definition 4.12 (Equivalence Relation)**.** R is an **equivalence relation** on A if R is a relation on A and R is reflexive, symmetric, and transitive. If R is an equivalence relation on A and $x \in A$, the set:

$$[x]_R := \{t : xRt\} \tag{29}$$

is called the **equivalence class** of x modulo R. We denote the set of equivalence classes on A modulo R by A/R, called the **quotient** of A mod R.

We will show that the equivalence classes of an equivalence relation form a partition of a set, and that one can equally well describe such a relation with the relation itself, the equivalence classes, or the canonical projection map it induces.

Definition 4.13 (Partition)**.** A partition Π of a non-empty set A is a set of subsets of A such that:

- $\emptyset \in \Pi$.
- $\forall B, C \in \Pi, B \neq C \implies B \cap C = \emptyset$.
- $A = \bigcup \Pi$.

Lemma 4.8. Let R be an equivalence relation on A. Let $x, y \in A$. Then:

- $x \in [x]_R$.
- If xRy, then $[x]_R = [y]_R$.
- If $(x, y) \notin R$, then $[x]_R \cap [y]_R = \emptyset$.

In other words, the equivalence classes of R form a **partition** of A.

Suppose that $f : A \to B$ is a function. We may define a relation E_f by xE_fy iff $f(x) = f(y)$. This is in fact an equivalence relation. Given a set of equivalence classes $\{[x]_R : x \in A\}$ on a set A, we can construct a function $f : A \to A/R, x \mapsto [x]_R$. Then the equivalence clases $[x]_R$ will be exactly the equivalence classes of the relation E_f.

As in algebra, every equivalence relation induces a canonical map into the quotient, $\pi_R : A \to A/R, x \mapsto [x]_R$. Given the projection π_R, we have $R = E_{\pi_R}$. This is because $\pi_R(x) = \pi_R(y)$ iff xRy, so $xE_{\pi_R}y$ iff xRy.

Finally, given a partition Π, we can construct an equivalence relation R_Π by $xR_\Pi z$ iff $\exists z \in Pi$ such that $x \in z$ and $y \in z$. This relation satisfies $\Pi = A/R_\Pi$. We see that given one of the following:

- A relation on A.
- The partition A/R.
- The canonical projection $\pi : A \to A/R$.

we can construct the other two descriptions of a corresponding equivalence relation without any ambiguity. Thus, any of these descriptions equivalently identifies an equivalence relation on A.

As one last topic in this section, we will discuss maps between quotients. Let R be an equivalence relation and $G : A/R \to B$ a function. Then we can lift G to A by defining $\hat{G} = G \circ \pi_R$, i.e. the following diagram commutes.

$$\begin{tikzcd}
A \arrow[r, "\hat{G}"] \arrow[d, "\pi_R"] & B \\
A/R \arrow[ur, "G"] &
\end{tikzcd}$$

However, the interesting question is to consider the other direction: when can we factor a map through the quotient?

Lemma 4.9. Let R be an equivalence relation on A and $F : A \to B$ a function. Then we can factor F through A/R iff $\forall x, y \in A, xRy \implies F(x) = F(y)$ (i.e. F sends each member of each equivalence class to the same image, F is **constant** on each equivalence class). In other words, we can find $\tilde{F} : A/R \to B$ such that the diagram commutes.

$$\begin{tikzcd}
A \arrow[d, "\pi"] \arrow[dr, "F"] & \\
A/R \arrow[r, "\tilde{F}"] & B
\end{tikzcd}$$

There is one more notion of a function respecting an equivalence relation. Let $F : A \to A$ be a function, R an equivalence relation on A. We say that F is **compatible with** R if $xRy \implies F(x)RF(y)$. If this is the case, then we can find $\tilde{F} : A/R \to A/R$ such that $[F(x)]_R = \tilde{F}([x]_R)$, i.e. we can factor F through the following commutative square.

$$\begin{tikzcd}
A \arrow[r, "F"] \arrow[d, "\pi"] & A \arrow[d, "\pi"] \\
A/R \arrow[r, "\tilde{F}"] & A/R
\end{tikzcd}$$

5 Number Systems

In this section, we will explicitly construct the most common number systems used in mathematics: the naturals, the integers, the rationals, and the reals. Although you have most likely already seen each of these number systems used in different areas in math, this section will show that these numbers *actually exist* as concrete mathematical entities. We will build them up from scratch using the set theory that we have already established (introducing one new axiom on the way), and exhibit that the structures we construct share the important properties of each of these number systems.

5.1 The Natural Numbers $\mathbb{N}$

The natural numbers are the building blocks of all mathematics; they give us a way to quantify objects by counting, and from this number system we can construct many other more intricate systems. *In these notes, we will denote the set of natural numbers by the symbol ω.* This notation will be useful later as we study ordinals later.As you are probably well aware, the set $\omega = \{0, 1, 2, 3, ...\}$[3] and is equipped with two canonical operations addition $+_\omega : \omega \times \omega \to \omega$ and multiplication $\cdot_\omega : \omega \times \omega \to \omega$. We also require a relation $<_\omega \subset \omega \times \omega$ which describes exactly how the natural numbers are ordered, and satisfies some intuitive properties. We will soon see precisely how to define the system $(\omega, +_\omega, \cdot_\omega, <_\omega)$, and then state and prove some statements that may be familiar to you from your discrete math class. Note that I will often drop the subscripts on the $+, \cdot$, and $<$ symbols.

In constructing ω, we are looking to associate each number with a set that we will specify, similar to how we encoded the definition of a tuple into a set definition. We will define the $+$ and $\cdot$ operations on these sets, and we will show that this association of sets with the number system forms a Peano system[4]. The easiest way to do this is to first make the assignment $0 := \emptyset$ and count up from this definition. The most obvious choice for 1 is to let it be the set containing 0 and so on, i.e. we let $1 := \{0\}$, $2 := \{1\}$, $3 = \{2\}$, continuing forever. However, this assignment makes it difficult to order the natural numbers. We must have $0 < 1 < 2 < 3 < ...$, but there is no clear definition of $<_\omega$ in this case. Instead, we make the following definition.

Definition 5.1 (Successor)**.** Let a be a set. The **successor** of a, denoted a^+, is the set:

$$a^+ := a \cup \{a\} \tag{30}$$

We will represent each natural number as the successor of the preceding number, with 0 being defined as the empty set. This is known as the **von-Neumann representation** of the natural numbers. For the first few numbers, this looks like the following:

$$\begin{cases} 0 := \emptyset \\ 1 := 0^+ = \{\emptyset\} = \{0\} \\ 2 := 1^+ = \{\emptyset, \{\emptyset\}\} = \{0, 1\} \\ 3 := 2^+ = \{0, 1, 2\} \\ \cdots \end{cases} \tag{31}$$

Note that for each of these small numbers, we may write $n = \{0, 1, 2, ..., n-1\}$. This is no accident, and in fact will hold for a general $n \in \omega$, once we complete the definition of ω.

[3] Although in many areas of math ω starts at 1, when constructing the number system we generally take it to start at 0 and associate this with the empty set. For the positive natural numbers, we will use the symbol ω^+.

[4] The Peano axioms are the basic properties that the set ω must satisfy.

Definition 5.2 (Inductive set)**.** A set a is **inductive** if $\emptyset \in a$ and if $b \in a$ implies $b^+ \in a$.

In other words, an inductive set contains 0 and contains the successor of every element in it. Notice that the natural numbers will end up being the smallest possible inductive set, as they contain $0, 1, 2, 3$, and so on. However, under the axioms of set theory we have currently discussed (axioms 1 - 6) we cannot prove the existence of or construct an inductive set. Hence we require axiom 7 to postulate the existence of the natural numbers, which we will restate here for convenience.

Axiom 5.1 (Infinity axiom)**.** There exists an inductive set.

Definition 5.3 (Natural number)**.** A **natural number** is a set which belongs to all inductive sets. We let ω denote the set of natural numbers.

Note that we can define ω now by the subset axiom. Pick an inductive set a by the infinity axiom, then define ω to be:

$$\omega := \{n \in a : \forall b(b \text{ inductive } \implies n \in b)\} \tag{32}$$

By examining this construction of ω, it is clear that ω is an inductive set. Indeed, $\emptyset$ is contained in every inductive set, and if $n \in \omega$, then n is in every inductive set, hence n^+ is contained in every set, and hence $n^+ \in \omega$. We state this as a proposition.

Proposition 5.2. ω is inductive.

This proposition, although obvious, will now allow us to state the induction principle, which is a key property of the natural numbers.

Theorem 5.3 (Induction Principle)**.** Any inductive subset of ω is ω.

Proof. If $a \subseteq \omega$ is inductive, then $\omega \subseteq a$ by its definition as the smallest inductive set, hence $a = \omega$. □

The inductive principle is the induction that you know and love, just wrapped in layers of abstraction. To use it like induction, we must prove that a subset $a \subseteq \omega$ is inductive. We do this by showing:

1. $0 \in a$. This is equivalent to showing a base case for the induction.
2. $n \in a$ implies $n^+ \in a$. This is equivalent to the inductive step; If you assume something holds for case n (i.e. $n \in a$), then you must show that it holds for n^+ (i.e. $n^+ \in a$).

Many of the following proofs about the set ω will use induction as a tool. Upon studying them carefully, it will become intuitive that the induction principle is the same as the induction you are used to.

Proposition 5.4. Every nonzero natural number n is the successor of another natural number.

Proof. Let $P = \{n \in \omega : n = 0 \vee \exists m \in \omega(n = m^+)\}$. We show that P is inductive. Clearly $0 \in P$, so assume that $n \in P$. Then $n \in \omega$, so $n^+ \in P$ by definition. Hence P is inductive, so $P = \omega$. □

Along with a set being inductive, there is another important quality a set may have that will be of use to us as we continue to study ω; it is called transitivity, not to be confused with transitivity of a relation.

Definition 5.4 (Transitive)**.** A set a is transitive if:

$$\forall x \in a \forall y \in x (y \in a) \tag{33}$$

An easy way to remember this (and why it is called a transitive set) is that a is transitive if $y \in x \in a$ implies that $y \in a$, i.e. if the symbol $\in$ is "transitive". Note that there are three equivalent definitions of a set being transitive. a is transitive if and only if:

- $y \in x \in a \implies y \in a$
- $a \subseteq Pa$
- $\forall b \in a, b \subseteq a$

Lemma 5.5. If a is transitive, then $a = \bigcup a^+$.

Proof. $\bigcup a^+ = \bigcup a \cup \{a\} = (\bigcup a) \cup a = a$ since $\bigcup a \subseteq a$ because a is transitive. □

Proposition 5.6. Every natural number n is a transitive set.

Proof. Let $P = \{n \in \omega : n \text{ is transitive}\}$. Then $\emptyset \in P$ as it has no members. Suppose that $n \in P$. Then $\bigcup n^+ = n \subseteq n$, so n^+ is transitive, hence $n^+ \in P$, which shows that $P = \omega$. □

Proposition 5.7. ω is a transitive set.

Proof. Again by induction. Let $P = \{n \in \omega : n \subseteq \omega\}$. Then $\emptyset \in P$ and if $n \in P$, $n^+ = n \cup \{n\} \subseteq \omega$ because $n \subseteq \omega$ and $\{n\} \subseteq \omega$, so P is inductive. □

Notice that although we do not define the "predecessor" operation, for nonzero n the previous natural number is $\bigcup n$, as $n = \bigcup n^+$. This proves the following claim.

Proposition 5.8. The function $\omega \to \omega, n \mapsto n^+$ is injective.

Our next goal is to build up the operations of addition and multiplication on ω. We will do this by recursively defining these operations, but first we need to define what we mean by recursion. We will use the following theorem.

Theorem 5.9 (Recursion)**.** Let A be a set, $a \in A$ and $F : A \to A$. Then there exists a unique function $h : \omega \to A$ such that:

1. $h(0) = a$
2. $\forall n \in \omega, h(n^+) = F(h(n))$

For notation which may be a little more intuitive, notice that this theorem allows us to define a sequence by defining a_0 and $a_{n^+} = F(a_n)$, i.e. the function h represents a sequence of elements of A, and F tells us how to get from one element in the sequence to the next. The proof of this is involved, but can be found in any textbook on the subject or the internet. Using recursion, we may now define addition and multiplication.

Definition 5.5 (Addition)**.** For $m \in \omega$, use recursion to define a function $A_m : \omega \to \omega$ with $A_m(0) := m$ and $A_m(n^+) := A_m(n)^+$ (here $F : \omega \to \omega$ with $F(k) = k$). We define:

$$m + n := A_m(n) \tag{34}$$

Definition 5.6 (Multiplication)**.** For $m \in \omega$, define $M_n : \omega \to \omega$ with $M_m(0) := 0$ and $M_m(n^+) := M_m(n) + m$. Define:

$$m \cdot n := M_m(n) \tag{35}$$

Without the clutter of A_m and M_m, note that these definitions are equivalent to letting $m+0 = m$, $m + n^+ = (m+n)^+$, $m \cdot 0 = 0$, and $m \cdot n^+ = m \cdot n + m$, so these operations do exactly what we expect. We must now prove that they have additional properties that we expect, so that we do not have to wonder whether an expression like $1 + 2$ is the same as $2 + 1$.

Theorem 5.10. Addition and multiplication are associative and commutative. Addition distributes over multiplication, i.e. $m \cdot (n + p) = m \cdot n + m \cdot p$.

Proof. Fix a number in the equation you are trying to prove and induct on the other number. You will need to prove the following lemma as well:

Lemma 5.11. $\forall m \in \omega, 0 + m = m$

□

The last piece of the puzzle for ω is to define the ordering $<_\omega$. As each natural number has the form $n = \{0, 1, 2, ..., n-1\}$, we see that each $n \in \omega$ contains all smaller natural numbers. Indeed, we make the definition of $<_\omega$ to be the membership operation.

Definition 5.7 ($<_\omega$)**.** For $m, n \in \omega$, define $m <_\omega n$ if $m \in n$. We write $m \leq_\omega n$ if $m <_\omega n$ or $m = n$.

Lemma 5.12. For $m, n \in \omega$, the following hold.

1. $m \in n$ iff $m^+ \in n^+$.

2. $m \notin m$.

Definition 5.8 (Linear ordering)**.** Let $<$ be a relation on a set a. We say that $<$ is a **linear ordering** on a if:

1. $<$ is transitive.

2. The relation $<$ is a **trichotomy**, i.e. for any $x, y \in a$, *precisely one of the following holds.*

    - $x < y$
    - $y < x$
    - $x = y$

Theorem 5.13. The relation $<_\omega$ is a linear ordering on ω.

Proof. We have already shown that $<_\omega$ is a transitive relation by showing that each $n \in \omega$ is a transitive set. To show $<_\omega$ is a trichotomy, let $T = \{n \in \omega : \forall m \in \omega (n <_\omega m \land n = m \land m <_\omega n)\}$, and we show T is inductive. Clearly $\emptyset \in T$, so let $n \in T$. We show that $n^+ \in T$ as well. Let $m \in \omega$. Then either we have $m <_\omega n$, $m = n$, or $n <_\omega m$. Suppose that $m <_\omega n$. Then we have $m <_\omega n <_\omega n^+$, since $n \in n^+$. If $m = n$, then again $m <_\omega n^+$. Finally, suppose that $m >_\omega n$. If $m = n^+$, we are done. If not, then $n^+ \in m$, hence $n^+ <_\omega m$. In any case, we see that $n^+ \in T$¡ so T is a transitive set and we are done. □

Linear orderings will come up later in the course when we discuss another type of ordering called a well-ordering, so keep the intuition in mind from the linearly ordered system $(\omega, <_\omega)$. To end this section, we will state a few simple propositions and theorems about $(\omega, <_\omega)$.

Corollary 5.13.1. For all $m, n, p \in \omega$, we have:

1. $m <_\omega n \iff m \subset n$ (strictly).
2. $m \leq_\omega n \iff m \subseteq n$.
3. $m < n \iff m + p <_\omega n + p$
4. If $p \neq 0$, then $m < n \iff m \cdot p <_\omega n \cdot p$.

Theorem 5.14 (Well-ordering property for ω)**.** Let $A \subseteq \omega$ be nonempty. Then A has a least element, that is, $\exists a \in A$ such that $a \leq b \forall b \in A$.

Proof. Assume that A does not have a least element. Let $B = \{n \in \omega : \forall m <_\omega n, m \notin A\}$ and show that B is inductive. □

Theorem 5.15 (Strong induction principle)**.** Let $A \subseteq \omega$ and assume that $\forall a \in \omega$, if $\forall b < a, b \in A$, then $a \in A$. Then $A = \omega$.

Proof. Suppose that $\omega \neq A$, so $\omega \setminus A$ is nonempty. Then the set $\omega \setminus A$ has a least element, and show that this leads towards a contradiction. □

5.2 The Integers $\mathbb{Z}$ and the Rational Numbers $\mathbb{Q}$.

We will now construct the integers and the rational numbers. The construction of both of these systems is quite similar; we will take an existing structure (ω for the case of the integers, and $\mathbb{Z}$ for the case of the rationals) and manipulate it via set products and quotients until we have an object that behaves as we wish it to.

We begin with the integers. As we have already constructed ω, we have the numbers $0, 1, 2, 3, ...$ equipped with a canonical addition and multiplication. We wish to include additive inverses in addition to the numbers in ω in the form of $-1, -2, -3, ...$, such that the entire set forms a commutative ring under $+$ and $\cdot$.

5.3 The Real Numbers $\mathbb{R}$

6 Acknowledgements

These notes are primarily based on two sources. First, Pierre Simon's Math 135 lectures at the *University of California, Berkeley.* Second, the text *Elements of Set Theory* by Herbert Enderton.