To Infinity and Beyond

Some Notes on Set Theory and Transfinite Numbers

Prerna Nadathur

August 15, 2008

Contents

1 Introduction

Perhaps the first problem we encounter in set theory is that of the definition of a *set*. It is a remarkable (although not altogether curious) fact that most books on set theory either actively decline to define a set, or else neglect to mention the problem of definition altogether. Intuitively, we know that sets contain things–elements, or objects, and so in some sense, we

can define a set as a collection of objects. Yet this can lead us into trouble: we shall see that there are collections of objects that are *not* sets, that are "too big" to be sets, that create paradoxes if we regard them as sets.

For example, although Cantor's original development of set theory was not axiomatic, it is clear that he relied implicitly on three assumptions: the *axiom of extension* (more later), the *axiom of abstraction*, and the *axiom of choice*. The axiom of abstraction in particular causes problems: for any given property, it postulates the existence of a set containing all elements for which the property holds. Bertrand Russell pointed out the problem with this in 1901: consider the set of all sets which are not members of themselves. This may be more familiar as the "barber" paradox. If Fred the barber shaves all men who do not shave themselves, then who shaves Fred the barber? At any rate, this results in a paradox, and will not do as it stands.

The lesson to be learned from this is as follows. While we have some strong intuitive ideas about sets and set theory, it will not do to work from those alone; we must formulate a set of axioms from which to develop our theory. Moreover, these axioms must be carefully examined in order to avoid paradoxes such as the one above. A desire to clear up confusion is, hopefully, is enough to motivate the following standard axioms. We will use the quantifiers $\forall, \exists, \exists!$ freely, as well as the symbols $\implies$ and $\iff$.

2 The Axioms

2.1 The Axioms

We begin, perhaps obviously, by postulating that we are not, in fact, wasting our time.

Axiom 2.1. Axiom of Existence. $\exists A$ such that A is a set.

Our intuition has given us one binary relation at the moment: given a set A, either an elements a is contained in A, or it is not contained in A. We represents this as follows: $a \in A$ or $a \notin A$. This seems reasonable, and is moreover compatible with the intuitive notion that sets are somehow uniquely defined by their membership. This gives us a way of comparing sets. We would like to consider two sets as equal if they have the same elements: that is, given two set A and B, we want $a \in B$ for all $a \in A$ and $b \in A$ for all $b \in B$ to be the necessary and sufficient condition that $A = B$. We formalize this as follows:

Axiom 2.2. Axiom of Extension. Given any two sets A and B, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

The symbol $\subseteq$ represents the *subset* relation. $A \subseteq B$ means that A is a subset of B: alternatively, that every element in A is also in B. A might constitute all of B, or it might not. We use $A \subset B$ to indicate that A is a *proper* subset of B; that is, that all of A is contained in B, but that A does not constitute all of B.

We next move to a modification of the aforementioned axiom of abstraction.

Axiom 2.3. Axiom of Separation. For every set A and every condition $S(a)$, there exists a set B whose elements are those elements $a \in A$ for which $S(a)$ holds. That is, $B = \{a \in A : S(a)\}$.

What do we mean by a condition? Informally, just a sentence involving the element a, usually referring to some property of the element. For example, consider the following "condition":

$$S(a) : a \notin a \tag{1}$$

Now consider two sets A and B, where $B = \{a \in A : S(a)\}$. We can rewrite this as follows:

$$B = \{a \in A : a \notin a\} \tag{2}$$

What is an element of B, in this case? An element b is in B if and only if $b \in A$ and $b \notin b$. Is $B \in A$? Is $B \in B$? If $B \in A$, then either $B \in B$, or $B \notin B$. But $B \in B$ is only true if $B \notin B$; hence $B \notin B$. But then, by definition of B, $B \in B$. Thus B cannot be in A. (This should seem familiar; it's the barber paradox reformulated.) A was an arbitrary set; hence our conclusion generalizes to this: A cannot contain everything. That is, *there is no set which contains everything.* And we somehow appear to have learned something more about what constitutes a set.

The axiom of specification does something else for us as well: it gives us a way of building new sets from old. Given any set, however, we can only create a new set that is "smaller." As we've just shown that there is no set that contains everything, this appears to be a problem. It is a straightforward thing to postulate the existence of an "empty set." Using the axiom of specification, we consider an arbitrary set A and consider:

$$B = \{a \in A : a \notin A\} \tag{3}$$

But there is nothing in A that is also *not* in A, hence B is empty. We can write this either as $B = \{\}$ or as $B = \emptyset$.

Knowing nothing about the elements in A, however, this is about all we can do. We need a way to construct sets "up;" that is, we need a way of making larger sets from smaller.

Axiom 2.4. Axiom of Pairing. Given any two sets, there is a set to which they both belong. That is, for any two sets A and B, there exists a set C such that $A \in C$ and $B \in C$.

Using the Axiom of Separation, we can in fact make this more particular: given A and B, we can specify a set D which contains A, B and nothing else. We do this by setting:

$$D = \{c \in C : c = A \text{ or } c = B\} \tag{4}$$

We now have a way of creating sets from other sets. But something doesn't seem quite satisfying yet; we want a way of building sets out of the *elements* of other sets, just as we did in the axiom of separation. That is, we want the concept of unions.

Axiom 2.5. Axiom of Unions. For any collection of sets, there exists a set which contains all elements which are contained in at least one set of the collection. Formally, if $\mathcal{F}$ is a collection (usually called a *family*) of sets, there exists a set U such that $a \in U$ if and only if $a \in A$ for some set $A \in \mathcal{F}$.

U is referred to as the *union* of the family $\mathcal{F}$; by the axiom of extension, there is only one such U. We write U as follows:

$$U = \bigcup_{A \in \mathcal{F}} A \tag{5}$$

So far, we have postulated the existence of some set. From this, using the axiom of separation, we can get the empty set. Using the axiom of pairing, we can create the set: $\{\emptyset, \emptyset\}$. However, something weird happens here. The axiom of extension tells us that two sets are empty if they have the same elements. Does this mean that $\{\emptyset, \emptyset\} = \{\emptyset\}$? As it happens, it doesn't matter, since we don't have a way of creating $\{\emptyset\}$ yet. The next axiom allows us to do that, as well as create a number of other sets.

Axiom 2.6. Axiom of Powers. For any set A, there is a set $\mathcal{P}(A)$ such if $B \subseteq A$, then $B \in \mathcal{P}(A)$.

That is, $\mathcal{P}(A)$ is the set which consists of all subsets of A. Hence $\{\emptyset\} = \mathcal{P}(\emptyset)$. $\mathcal{P}(A)$ is called the *power set* of A. It is unique by the axiom of extension (and hence, the answer to the question above is yes, apparently $\{\emptyset, \emptyset\} = \{\emptyset\}$).

Example 2.7. Let us use the axiom of pairing to create the following set:

$$A = \{\{\emptyset\}, \emptyset\} \tag{6}$$

What is $\mathcal{P}(A)$? Certainly it contains $\emptyset$.

$$\mathcal{P}(A) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\emptyset\}, \emptyset\}\} \tag{7}$$

There are two more axioms which must be listed before continuing with our development: these two are listed last because they are the least intuitive, and, particularly in the case of the first one, lead to some rather peculiar results. We will not discuss these in detail here, but save such a discussion for later.

Axiom 2.8. Axiom of Choice. Let $\mathcal{U}$ be a set such that every $A \in \mathcal{U}$ is nonempty and such that any two sets A and B which share an element a are in fact equal. Then there exists a set C such that for every set A in $\mathcal{U}$, there is exactly one $a \in C$ with $a \in A$.

We finish with an axiom that reminds us of where we started: its goal is to eliminate circular sets (such as the one giving rise to Russell's paradox. This makes it unique among the axioms–it is the only one that asserts the *nonexistence* of certain sets.

Axiom 2.9. Axiom of Foundation. Given a set $A \neq \emptyset$, there exists $a \in A$ such that there is no set b with the property that $b \in A$ and $b \in a$.

2.2 Some Consequences

2.2.1 Intersections, Unions and Complements

We are still missing some things that seem standard; the Axiom of Unions above provides us (indirectly) with the union operator, but we do not seem to have yet discovered the intersection operator which is in some sense its complement. Why do we have an axiom for unions but not for intersections? It turns out that the intersection operator can be developed as a consequence of the Axioms of Extension and Separation.

Theorem 2.10. *Given two sets A and B, $\exists! C$ such that $x \in C$ if and only if $x \in A$ and $x \in B$.*

Proof. Letting $x \in A$ and $x \in B$ be our condition, the Axiom of Separation gives us:

$$\exists C \text{ such that } x \in C \iff x \in A \text{ and } x \in B \tag{8}$$

In order to show that C is unique, we assume there exists a set D with the same properties. That is,

$$x \in D \iff x \in A \text{ and } x \in B \tag{9}$$

Then we have

$$\begin{aligned} x \in D &\implies x \in A \text{ and } x \in B && (10)\\ &\implies x \in C && (11)\\ &\implies D \subseteq C && (12) \end{aligned}$$

and similarly,

$$\begin{aligned} x \in C &\implies x \in A \text{ and } x \in B && (13)\\ &\implies x \in D && (14)\\ &\implies C \subseteq D && (15) \end{aligned}$$

and by the Axiom of Extension, we have

$$C = D \tag{16}$$

Thus C is unique. □

We notice that C is in fact what we think of as the *intersection* of A and B, and formalize this with the following definition:

Definition 2.11. The *intersection* of two sets A and B is the set $A \cap B$ comprising all elements common to A and B. That is, $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

We can now prove some facts about the $\cap$ operator:

Proposition 2.12. *Let A, B, C be sets.*

1. *$\cap$ is commutative. That is, $A \cap B = B \cap A$.*
2. *$\cap$ is associative. That is, $(A \cap B) \cap C = A \cap (B \cap B)$.*
3. *$\cap$ is* idempotent*: $A \cap A = A$.*
4. *$A \cap \emptyset = \emptyset$*
5. *$A \cap B \subseteq A$*

Proof. 1. $A \cap B = \{x : x \in A \text{ and } x \in B\} = \{x : x \in B \text{ and } x \in A\} = B \cap A$.

2. $(A \cap B) \cap C = \{x : x \in A \cap B \text{ and } x \in C\} = \{x : x \in A \text{ and } x \in B \text{ and } x \in C\} = \{x : x \in A \text{ and } x \in B \cap C\} = A \cap (B \cap C)$.
3. $A \cap A = \{x : x \in A \text{ and } x \in A\} = \{x : x \in A\} = A$
4. $A \cap \emptyset = \{x : x \in A \text{ and } x \in \emptyset\}$. But there is no x such that $x \in \emptyset$; hence there is no x such that $x \in A$ and $x \in \emptyset$. Thus $A \cap \emptyset = \emptyset$.
5. $x \in A \cap B \implies x \in A$ and $x \in B \implies x \in A \implies A \cap B \subseteq A$.

□

Proposition 2.13. $A \subseteq B \iff A \cap B = A$

Proof. Let $A \subseteq B$. Then, $\forall x \in A$, we have $x \in B$. $A \cap B \iff x \in A$ and $x \in B$. But since $x \in A \implies x \in B$, we have $A \cap B \iff x \in A$. Thus, $A \cap B = A$.

For the reverse direction, assume $A \cap B = A$. By the Axiom of Extension, $A \cap B \subseteq A$ and $A \subseteq A \cap B$. $A \subseteq A \cap B$ implies that, $\forall x \in A$, we have $x \in A \cap B$. That is, $x \in A \implies x \in A$ and $x \in B$. That is, $x \in A \implies x \in B$, and so $A \subseteq B$. □

It is clear that $A \cap B = \emptyset$ iff A and B have no elements in common. In this case, we refer to A and B as *pairwise disjoint*.

We proceed to establish the union operator:

Theorem 2.14. *Given two sets A and B, $\exists! C$ such that $x \in C$ if and only if $x \in A$ or $x \in B$.*

Proof. Using the axiom of unions, we have

$$\exists C \text{ such that } x \in C \iff x \in A \text{ or } x \in B \tag{17}$$

To prove uniqueness, we assume there exists a set D with the same properties:

$$x \in D \iff x \in A \text{ or } x \in B \tag{18}$$

Then we have

$$x \in D \implies x \in A \text{ or } x \in B \tag{19}$$
$$\implies x \in C \tag{20}$$
$$\implies D \subseteq C \tag{21}$$

and similarly,

$$x \in C \implies x \in A \text{ or } x \in B \tag{22}$$
$$\implies x \in D \tag{23}$$
$$\implies C \subseteq D \tag{24}$$

and by the Axiom of Extension, we have

$$C = D \tag{25}$$

Thus C is unique. □

C, as above, is clearly the set that we think of as the *union* of A and B. We formally define the union operator:

Definition 2.15. The *union* of two sets A and B is the set $A \cup B$ comprising all elements contained in at least one of A and B. That is, $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

In particular, $A \cup B$ is the smallest set containing all the elements in at least one of A and B. We prove some facts about the $\cup$ operator:

Proposition 2.16. *Let A, B, C be sets.*

1. *$\cup$ is commutative. That is, $A \cup B = B \cup A$.*
2. *$\cup$ is associative. That is, $(A \cup B) \cup C = A \cup (B \cup B)$.*
3. *$\cup$ is* idempotent*: $A \cup A = A$.*
4. *$A \cup \emptyset = A$*
5. *$A \subseteq A \cup B$*

Proof. 1. $A \cup B = \{x : x \in A \text{ or } x \in B\} = \{x : x \in B \text{ or } x \in A\} = B \cup A$.

2. $(A \cup B) \cup C = \{x : x \in A \cup B \text{ or } x \in C\} = \{x : x \in A \text{ or } x \in B \text{ or } x \in C\} = \{x : x \in A \text{ or } x \in B \cup C\} = A \cup (B \cup C)$.

3. $A \cup A = \{x : x \in A \text{ or } x \in A\} = \{x : x \in A\} = A$

4. $A \cup \emptyset = \{x : x \in A \text{ or } x \in \emptyset\}$. But there is no x such that $x \in \emptyset$; hence $A \cap \emptyset = \{x : x \in A\} = A$

5. $x \in A \implies x \in A$ or $x \in B \implies x \in A \cup B \implies A \subseteq A \cup B$.

□

Proposition 2.17. $A \subseteq B \iff A \cup B = B$

Proof. Let $A \subseteq B$. Then, $\forall x \in A$, we have $x \in B$. $A \cup B \iff x \in A$ or $x \in B$. But since $x \in A \implies x \in B$, ($x \in A$ or $x \in B$) is equivalent to $x \in B$. Thus, $A \cup B = \{x : x \in B\} = B$.

For the reverse direction, assume $A \cup B = B$. By the Axiom of Extension, $A \cup B \subseteq B$ and $B \subseteq A \cup B$. We have from above that $A \subseteq A \cup B$, and therefore, by transitivity, $A \subseteq B$. □

It turns out, in addition, that the intersection and union operations are *distributive*:

Proposition 2.18. *Let A, B and C be sets.*

1. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

2. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Proof. The proofs are somewhat syntactic in nature.

1. $(A \cup B) \cap C = \{x : x \in A \cup B \text{ and } x \in C\} = \{x : x \in A \text{ or } B \text{ and } x \in C\} = \{x : x \in A \text{ and} C \text{ or } x \in B \text{ and } C\} = \{x : x \in A \cap C \text{ and } x \in B \cap C\} = (A \cap C) \cup (B \cap C)\}$

2. $(A \cap B) \cup C = \{x : x \in A \text{ and } B \text{ or } x \in C\} = \{x : x \in A \text{ or } C \text{ and } x \in B \text{ or } C\} = (A \cup C) \cap (B \cup C)$

□

Finally, we justify the operation of *complementation*:

Theorem 2.19. *Given two sets A and B, $\exists! C$ such that $x \in C \iff x \in A$ and $x \notin B$.*

Proof. We use the Axiom of Separation to postulate the existence of such a C, and then the Axiom of Extension to prove its uniqueness. □

Definition 2.20. For two sets A and B, the *complement* of B in A is the set $A - B$ comprising all elements contained in A and not B. That is, $A - B = \{x : x \in A \text{ and } x \notin B\}$.

We also talk about the *complement* of a set without referring to the set from which to "subtract" it; in these circumstances, we are considering a set as part of a larger "universe," the nature of which should be apparent from the context. For example, we might refer to the complement of the even numbers: the natural name for this set is the odd numbers, and we have assumed that we are in the "universe" of natural numbers. We will refer to the universe as E (for "everything"). In these cases, we write the complement of A as A'. This allows us to state some facts:

Proposition 2.21. *Let A and B be sets.*

1. $(A')' = A$
2. $\emptyset' = E$
3. $E' = \emptyset$
4. $A \cap A' = \emptyset$
5. $A \cup A' = E$.

Proof. 1. $x \in (A')' \iff x \notin A' \iff x \in A$. Therefore, $(A')' = A$.

2. $\emptyset' = \{x : x \in Eandx \notin \emptyset\}$. But there is no x such that $x \in \emptyset$, so $\emptyset' = \{x : x \in E\} = E$.

3. This follows from 2.

4. $A \cap A' = \{x : x \in A \text{ and } x \in A'\} = \{x : x \in A \text{ and } x \in E \text{ and } x \notin A\}$. But there is no x such that $x \in A$ and $x \notin A$, hence $A \cap A' = \emptyset$.

5. $A \cup A' = \{x : x \in A \text{ or } x \in A'\} = \{x : x \in A \text{ or } x \in E \text{ and } \notin A\} = \{x : x \in A \text{ or } \notin A \text{ and } x \in A \text{ or } x \in E\} = \{x : x \in E\} = E$.

□

Proposition 2.22. $A \subset B \iff B' \subset A'$.

Proof. Assume $A \subset B$. Then $x \in A \implies x \in B$. Thus $x \notin B \implies x \notin A$. $\forall x, x \in E$, so we can write $x \in E$ and $x \notin B \implies x \in E$ and $x \notin A$. Therefore, $B' \subset A'$.

The reverse follows by remembering that $(A')' = A$.

□

The most important laws about complements are the *De Morgan laws*, which are generalizable to infinite collections of sets:

Proposition 2.23. (De Morgan Laws) *Let A, B be sets.*

1. $(A \cup B)' = A' \cap B'$
2. $(A \cap B)' = A' \cup B'$

Proof. 1. $(A \cup B)' = \{x : x \in E \text{ and } x \notin A \cup B\} = \{x : x \in E \text{ and } x \notin A \text{ and } x \notin B\} = \{x : x \in A' \text{ and } x \in B'\} = A' \cap B'$.

2. $(A \cap B)' = \{x : x \in E \text{ and } x \notin A \cap B\} = \{x : x \in E \text{ and } x \notin A \text{ or } x \notin B\} = \{x : x \in A' \text{ or } x \in B'\} = A' \cup B'$.

□

2.2.2 Ordered Pairs and Cartesian Products

We noticed one of the unexpected consequences of the Axiom of Extension when we examined the natural numbers in the previous section: namely, that a set $\{a, a\}$ is the same as the set $\{a\}$. Another consequence is that the set $\{a, b\}$ is equivalent to the set $\{b, a\}$. This satisfies our ideas about sets as collections of objects, but does not give us a way of representing *ordered pairs*. In particular, then, we want a way of ordering a set so that the order we intend is obvious from the set itself.

Suppose we want to consider

$$a \; b$$

in that order. We can, for each spot in the order, consider the set of elements that occur in or before that spot:

Definition 2.24. The *ordered pair* (a, b) is represented by the set $\{\{a\}, \{a, b\}\}$. That is, $(a, b) = \{\{a\}, \{a, b\}\}$.

This seems satisfactory, but we need to check that it does not lead to contradictions. In particular, we need to be sure that if $(a, b) = (c, d)$, then $a = c$ and $b = d$:

Proof. If $a = b$, then $(a, b) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$, and if (a, b) is represented by a singleton set $\{\{a\}\}$, then $\{\{a\}\} = \{\{a\}, \{a\}\} = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a, b\}\}$, so in particular, $\{a\} = \{a, b\}$ and $a = b$.

Assume $(a, b) = (c, d)$. If $a = b$, then for $(a, b) = (c, d)$, we must have both (a, b) and (c, d) represented by singletons. In particular, $(a, b) = \{\{a\}\}$ and $(c, d) = \{\{c\}\}$, so $(a, b) = (c, d) \implies a = c$ and since $a = b$ and $c = d$, reflexivity and transitivity of equality gives $b = d$.

If $a \neq b$, then the sets (a, b) and (c, d) each contain one singleton set: $\{a\}$ and $\{c\}$, respectively, so $(a, b) = (c, d)$ requires that the singletons be equal. That is, $a = c$. Each of (a, b) and (c, d) contain exactly one pair: $\{a, b\}$ and $\{c, d\}$, respectively. $(a, b) = (c, d)$ gives us that $\{a, b\} = \{c, d\}$, and since $a = c$, b and d must be equal (by the Axiom of Extension).

Thus, ordered pairs are well-defined. □

This begs the question: Given two sets A and B, can we construct a set containing all the ordered pairs (a, b) where $a \in A$ and $b \in B$? Certainly: if $a \in A$ and $b \in B$, then $\{a\} \subseteq A$ and $\{b\} \subseteq B$, and clearly $\{a, b\} \subseteq A \cup B$. But then both $\{a\}$ and $\{a, b\}$ are subsets of $A \cup B$, so by the Axiom of Powers, $\{a\}$ and $\{a, b\}$ are in $\mathcal{P}(A \cup B)$, so $\{\{a\}, \{a, b\}\} \subset \mathcal{P}(A \cup B)$ and $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$.

This a bit complicated, and really, we'd like a set that consists of the aforementioned ordered pairs and nothing. We can apply the Axiom of Separation to $\mathcal{P}(\mathcal{P}(A \cup B))$ to achieve the desired result:

Definition 2.25. The *Cartesian product* of two sets A and B is the set consisting of ordered pairs (a, b) where $a \in A$ and $b \in B$. We write this set as $A \times B$. That is, $A \times B = \{x : x = (a, b) \text{ with } a \in A \text{ and } b \in B\}$.

This leads us to a "converse" proposition:

Proposition 2.26. *If C is a set such that every element of C is an ordered pair, then $\exists A, B$ sets such that $C \subseteq A \times B$.*

Proof. Let $c \in C$. Then $c = (a, b) = \{\{a\}, \{a, b\}\}$ for some a, b. Thus, the elements of C are sets. Consider $D = \bigcup_{c \in C} c$. For any $c = (a, b) \in C$ as above, $\{a\} \in D$ and $\{a, b\} \in D$. We notice that the elements of D are again sets, so we take $F = \bigcup_{d \in D} d$. For any $c = (a, b) \in C$, $a \in F$ and $b \in F$. Set $A = F = B$. Then $C \subseteq A \times B$. □

We can, in fact, be more specific: using the Axiom of Separation, we can set $A = \{a : \exists b \text{ with } (a, b) \in C\}$ and $B = \{b : \exists a \text{ with } (a, b) \in C\}$. If we define A and B this way, it becomes clear that $C = A \times B$. This seems somewhat redundant, but will be useful later.

We prove a few standard results about Cartesian products:

Proposition 2.27. *Let A, B, C, D be sets.*

1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
2. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$
3. $(A - B) \times C = (A \times C) - (B \times C)$.

Proof.

1. $(A \cup B) \times C = \{x : x = (y, z) \text{ with } y \in A \cup B \text{ and } z \in C\} = \{x : x = (y, z) \text{ with } y \in A \text{ or } B \text{ and } z \in C\} = \{x : x = (y, z) \text{ with } y \in A \text{ and } z \in C \text{ or} y \in B \text{ and } z \in C\} = \{x : x \in A \times C \text{ or } x \in B \times C\} = (A \times C) \cup (C \times C)$.
2. $(A \cap B) \times (C \cap D) = \{x : x = (y, z) \text{ with } y \in A \cap B \text{ and } z \in C \cap D\} = \{x : x = (y, z) \text{ with } y \in A \text{ and } B \text{ and } z \in C \text{ and } D\} = \{x : x = (y, z) \text{ with } y \in A \text{ and } z \in C \text{ and } y \in B \text{ and } z \in D\} = \{x : x \in A \times C \text{ and } x \in B \times D\} = (A \times C) \cap (B \times D)$.
3. $(A - B) \times C = \{x : x = (y, z) \text{ with } y \in A - B \text{ and } z \in C\} = \{x : x = (y, z) \text{ with } y \in A \text{ and } y \notin B \text{ and } z \in C\} = \{x : x = (y, z) \text{ with } y \in A \text{ and } z \in C \text{ and } y \notin B \text{ and } z \in C\} = \{x : x \in A \times C \text{ and } x \notin B \times C\} = (A \times C) - (B \times C)$.

□

2.2.3 Relations and Functions

Armed with ordered pairs, we can now define a *relation*

Definition 2.28. A set R is a *relation* if every element of R is an ordered pair.

Example 2.29. The Cartesian product $A \times B$ of two sets A and B is a relation. This should be obvious.

If R is a relation, we often represent $(a, b) \in R$ by aRb.

We recall from Proposition 2.26 that, given a set R consisting of ordered pairs, we can define sets A and B such that $R = A \times B$. In this case, we say that R is a relation *from* A *to* B. We let A and B be defined as above; they are referred to, respectively, as the *domain* and *range* of the relation R:

$$domR = \{a : \exists b \text{ with } aRb\} \tag{26}$$

$$ranR = \{b : \exists a \text{ with } aRb\} \tag{27}$$

Consider for a moment a relation R for which $domR = ranR$. There are some properties that such relations commonly have:

Definition 2.30. Let A be a set and let R be a relation from A to A. That is, $domR = A = ranR$.

1. R is *reflexive* if $\forall a \in A, aRa$.
2. R is *symmetric* if $\forall a, b \in A, aRb \implies bRa$.
3. R is *transitive* if $\forall a, b, c \in A, aRb$ and $bRc \implies aRc$.
4. If R is reflexive, symmetric and transitive, we call R an *equivalence relation*

An equivalence relation on a set A divides up A in a very particular fashion: into a pairwise disjoint collection of subsets $\mathcal{C}$ such that $\bigcup C = A$. (This is called a *partition.*) If R is an equivalence relation on A, then for each $a \in A$, we refer to the set of all elements $b \in A$ for which aRb as the *equivalence class* of a with respect to the relation R. The equivalence classes are the pairwise disjoint subsets. To prove this, we need the following proposition:

Proposition 2.31. *Let A be a set and let R be an equivalence relation on A. For any $a \in A$, we represent the equivalence class of a by $\pi(a)$. If $a, b \in A, \pi(a) \cap \pi(b) \neq \emptyset \implies \pi(a) = \pi(b)$.*

Proof. If $\pi(a) \cap \pi(b) \neq \emptyset$, then $\exists c$ such that $c \in \pi(a)$ and $c \in \pi(b)$. Then we have aRc and bRc. R is an equivalence relation, so $aRc \implies cRa$ and thus bRa by transitivity. But then, by transitivity, $bRd \forall d \in \pi(a)$ and $\pi(a) \subseteq \pi(b)$.

To get the reverse inclusion, we note that, by symmetry, $bRa \implies aRb$. Thus $aRf \forall f \in \pi(b)$, so $\pi(a) \subseteq \pi(b)$.

Thus, by the Axiom of Extension, $\pi(a) \cap \pi(b) \neq \emptyset \implies \pi(a) = \pi(b)$. □

We can also define a more specific kind of a relation:

Definition 2.32. A *function* from A to B (abbreviated $f : A \to B$) is a relation f such that $domf = A$ and for each $a \in A, \exists! b \in B$ with $(a, b) \in f$. If $(a, b) \in f$, we write $f(a) = b$.

Note that $ranf$ is not specified to be B: we refer to the subset of B comprised of $b \in B$ such that $\exists a \in A$ with $f(a) = b$ as the *image* of f (denoted $im(f)$).

Definition 2.33. Let A, B be sets. Let $f : A \to B$.

1. f is *injective* if $f(a_1) = f(a_2) \implies a_1 = a_2 \forall a_1, a_2 \in A$.
2. f is *surjective* if $\forall b \in B, \exists a \in A$ such that $f(a) = b$.
3. f is *bijective* if it is injective and surjective.

It is easy enough (if perhaps circular) to note that $f : A \to im(f)$ is surjective.
We can now reformulate the Axiom of Choice in terms of functions:

Axiom 2.34. Axiom of Choice. For every set A, there exists a *choice* function $f : (\mathcal{P}(A) - \{0\} \to A$ such that $\forall B \subset A, f(B) \in A$.

Writing $f(B)$ is a slight abuse of notation: it represents the image of the subset B. Formulating the Axiom of Choice in this manner will allows us to work more comfortably with it later.

2.3 An Axiom for the Natural Numbers

Building from sets, we seem to have captured a number of standard mathematical concepts. We still seem to be missing numbers, however. How are we to capture numbers from sets? The most logical connection seems to be to equate a number with the number of elements contained in a given set. (We can say, without confusion that two sets have the same "number" of elements if we can put a *bijection* between them. This would give us some concept of the natural numbers. But then are we to consider $\{a, b\}$ equal to $\{c, d\}$ merely because we can put a bijection between them? This doesn't seem right. Moreover, what is the relationship to be between one number and the next? Intuitively, we think that 2 contains 1, and 3 contains 1 and 2, etc. This idea motivates the following definition:

Definition 2.35. For any set n, we call n^+ the *successor* of n if $n^+ = n \cup \{n\}$.

Now we can try assigning numbers to sets. The first is easy:

$$0 = \emptyset \tag{28}$$

From here, we simply use the definition of *successor*. Thus we set

$$1 = 0^+ = \{\emptyset\} = \{0\} \tag{29}$$

$$2 = 1^+ = \{\emptyset, \{\emptyset\}\} = \{0, 1\} \tag{30}$$

$$3 = 2^+ = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\} = \{0, 1, 2\} \tag{31}$$

and so on. It is part of our intuition about the natural numbers that they form a set. Nothing said so far appears to justify this; in fact, we need a new axiom:

Axiom 2.36. Axiom of Infinity. There exists a set $\mathbb{N}$ such that $\emptyset \in \mathbb{N}$ and for all $n \in \mathbb{N}$, n^+ is in $\mathbb{N}$.

Here we have used the standard notation for the natural numbers. We shall return to examine this axiom in greater detail later.

We notice that the set corresponding to each natural number seems, intuitively, to have the correct number of elements in it. While our definition of $\mathbb{N}$ prevents such things as $\{a, b\} = \{c, d\} \forall a, b, c, d$ (which is a good thing!), we want to have some idea of similarity between two sets with the same number of elements. This follows from before.

Definition 2.37. Two set A and B are *similar* if $\exists f : A \to B$ such that f is a bijection. In this case, we write: $A \sim B$.

Thus, $\{a, b\} \sim \{c, d\} \sim 2$. In fact, we refer to an arbitrary set A as *finite* if it is equivalent to a natural number; else A is *infinite*. It is clear that $\mathbb{N}$ is infinite.

3 Order

We now have a concept of the natural numbers and of the equivalence of sets. It would be nice to have a way of comparing sets that tells us more about them than simply whether or not they are equivalent. To this end, we provide the following definitions.

Definition 3.1. A relation R on a set A is *antisymmetric* if, $\forall a, b \in A aRb$ and $bRa \implies a = b$.

We can now define the concept of *order*.

Definition 3.2. A relation R on a set A is a *partial order* if it is reflexive, antisymmetric, and transitive.

Example 3.3. Consider $\mathbb{N}$. The inclusion ($\subseteq$) relation is a partial order on this set:

Proof. Let $n, m, k \in \mathbb{N}$.

1. $x \in n \implies x \in n$. Therefore, $n \subseteq n$.
2. Suppose $n \subseteq m$ and $m \subseteq n$. By the Axiom of Extension, $n = m$.
3. Suppose $n \subseteq m$ and $m \subseteq k$. $x \in n \implies x \in m$ and $x \in m \implies x \in k$, hence $x \in n \implies x \in k$ and $n \subseteq k$.

□

In fact, for $\mathbb{N}$, the partial order $\subseteq$ is the familiar inequality: $\leq$. On $\mathbb{N}$ this order has an additional property: given any $n, m \in \mathbb{N}$, either $n \leq m$ or $m \leq n$.

Definition 3.4. A partial order $\leq$ on a set A is called a *total order* if, $\forall a, b \in A$, either $a \leq b$ or $b \leq a$.

So $\leq$ on $\mathbb{N}$ is a total order. Essentially, a total order allows us to compare any two elements in a set. We refer to a set A as partially ordered or totally ordered if it has a partial order or total order (respectively) on it.

Definition 3.5. If A is a partially ordered set, and if $a \in A$, the set $\{x \in A | x < a\}$ is the *initial segment* or *prefix* determined by a; we denote it by $s(a)$.

For $n \in \mathbb{N}$ with the $\leq$ ordering, we notice that $s(n) = n$.

$\mathbb{N}$ has another nice property: every subset of $\mathbb{N}$ contains a smallest element. This allows us to use *induction*.

Theorem 3.6. ***Induction.*** *Let $A \subseteq \mathbb{N}$. If $\forall n \in \mathbb{N}$, we have the property that $s(n) \subseteq A \implies n \in A$, then $A = \mathbb{N}$.*

Proof. Suppose not. Then $\mathbb{N} - A \neq \emptyset$, and since $\mathbb{N} - A \subseteq \mathbb{N}$, $\mathbb{N} - A$ contains a smallest element n. But then $s(n) \subseteq A$, and so, by hypothesis, $n \in A$. But n cannot belong to both $mathbbN - A$ and A; hence our assumption is false, and $\mathbb{N} - A = \emptyset$. □

A set in which we can use the inductive principle is called *well-ordered*.

Definition 3.7. A set W is *well-ordered* if, for any $A \subseteq W$ such that $A \neq \emptyset$, A contains a smallest element.

This allows us to state a generalized version of the inductive principle:

Theorem 3.8. ***Principle of Transfinite Induction.*** *Let $A \subseteq B$, where B is well-ordered. If $\forall b \in B$, we have the property that $s(b) \subseteq A \implies b \in A$, then $A = B$.*

The proof follows from above.

Proposition 3.9. *A totally ordered set is well-ordered if and only if the initial segment of each element is well-ordered.*

Proof. Let A be a totally ordered set which is well-ordered. Consider an arbitrary element $a \in A$. The set $s(a)$ is a subset of A; hence, by transitivity of the $\subseteq$ relation, $B \subseteq s(a) \implies B \subseteq A$. A is a well-ordering; hence any subset has a smallest element. Thus any subset of $s(a)$ has a smallest element, and $s(a)$ is well-ordered. The choice of a was arbitrary, so the initial segment of every element of A is well-ordered.

For the reverse, assume that the initial segment of every element of A is well-ordered. Consider a nonempty subset B of A. Let $b \in B$, and assume that B has no smallest element. Then $s(b) \cap B \neq \emptyset$ (else b would be the smallest element in B). In particular, $s(b) \cap B \subseteq s(b)$, and since $s(b)$ is well-ordered, $s(b) \cap B$ has a smallest element, c. But $c \leq b$ (since $c \in s(b)$), so if c is the smallest element in $s(b) \cap B$, $s(c) \cap B = \emptyset$. But then c is the smallest element in B, and A is well-ordered. □

Proposition 3.10. *Given two well-ordered sets A and B, either $A \sim B$ or one of A and B is isomorphic to a prefix of the other.*

Proof. Let A_0 be the set of elements of A for which there exists $b \in B$ with $s(a) \sim s(b)$. A_0 is nonempty; A, B well-ordered implies that $\exists a_0 \in A, b_0 \in B$ such that if $a \in A, b \in B$, then $a_0 < a$ and $b_0 < b$; i.e., there exist smallest elements a_0 and b_0 in A and B, respectively. Consider their initial segments: $s(a_0) = \emptyset, s(b_0) = \emptyset$, hence $s(a_0) \sim s(b_0)$. Thus $a_0 \in A_0$.

For each $a \in A_0$, write $f(a)$ for the corresponding b in B, and let B_0 be the range of f. This is well-defined: if $\exists b, d \in B$ such that $s(b) \sim s(a)$ f and $s(d) \sim s(a)$ or some particular $a \in A_0$, then $s(b) \sim s(d)$. But B is well-ordered, so $s(b) \sim s(d)$ for $b, d \in B \implies b = d$.

We claim that both A_0 and B_0 are closed downwards. That is, if $a \in A_0$, then $s(a) \subseteq A_0$ and $b \in B_0 \implies s(b) \subseteq B_0$.

Assume $a \in A_0$ such that $\exists z \in A - A_0$ with $z < a$. $a \in A_0 \implies \exists b \in B$ with $s(a) \sim s(b)$. Let ϕ be the isomorphism between the initial segments: $\phi : s(a) \to s(b)$. Then $s(z) \sim s(\phi(z))$, and $z \in A_0$.

Similarly, let $b \in B_0$ such that $\exists y \in B - B_0$ with $y < b$. Then $\exists a \in A_0$ s.t. $s(a) \sim s(b)$. Let ψ be the isomorphism: $\psi : s(b) \to s(a)$. Then $s(y) \sim s(\psi(y))$, and $y \in B_0$.

If $A_0 = A$, or $B = B_0$ then we are done, so assume both $A - A_0$ and $B - B_0$ are nonempty. Let x, w be the smallest elements in $A - A_0$ and $B - B_0$, respectively. It is clear from above that $s(x) = A_0$ and $s(w) = B_0$. But by construction, it is clear that $A_0 \sim B_0$. Hence $s(x) \sim s(w)$, and $x \in A_0, w \in B_0$. Thus we cannot have both $A - A_0$ and $B - B_0$ nonempty; either one or both is empty. Thus, either $A \sim B$ or one of A and B is isomorphic to a prefix of the other.

□

We now state a particularly useful theorem, although one with some peculiar baggage.

Theorem 3.11. ***Well-Ordering Theorem*** *Every set can be well-ordered.*

The proof relies (indirectly) on the Axiom of Choice, and we will return to it in the final section.

4 Ordinals and Cardinals

4.1 Ordinals

We defined the *successor* of a set n as $n \cup \{n\}$, and then constructed the natural numbers to contain $0 = \emptyset$ and to containn^+ whenever it contains n. This property allowed us to use the inductive principle, which we saw above generalized to well-ordered sets.

We have been thinking of $\mathbb{N}$ as a set containing numbers; yet from our construction, $n \in \mathbb{N}$ is a set containing all predecessors of n. We rename the set $\mathbb{N}$ as ω: this set contains the natural numbers, so we may think of ω as the set containing all the predecessor of ω. It seems only logical, then, that we may form $\omega^+ = \omega \cup \{\omega\}$. We appear to be able to count, then, beyond the natural numbers.

For each natural number, we note that $m < n$ is the same statement as $m \in n$ and $m \subset n$. Since ω is well-ordered by $\in$, Proposition 3.9 give us that, for any $n \in \omega$, $s(n)$ is

well-ordered by $\in$. Moreover, $s(n) = n$ by construction. These are the properties we want to extend.

4.1.1 Ordinal Numbers

Definition 4.1. An *ordinal* number is a well-ordered set α such that $s(\beta) = \beta \; \forall \beta \in \alpha$.

Proposition 4.2. *$\forall n \in \omega$, n is an ordinal. ω is an ordinal.*

Proof. ω is a well-ordered set; hence the prefix of any element $n \in \omega$ is well-ordered. For any $m \in \omega$, $s(m) = m$; hence, for all $m \in \omega$ such that $m \in n (m < n)$, $s(m) = m$. It follows that ω is an ordinal. □

Proposition 4.3. *If α is an ordinal, α^+ is an ordinal.*

Proof. If $\alpha^+ = \alpha \cup \{\alpha\}$. Then $\alpha \cap \alpha^+ = \alpha$, so every element in α^+ except for α is contained in α, and α is the largest element in α^+ under the $\in$ ordering. Consider a subset A of α^+. If $A \cap \alpha \subseteq \alpha$, so if $A \cap \alpha$ nonempty, the smallest element of A is the smallest element of $A \cap \alpha$. If $A \cap \alpha = \emptyset$, then, since $A \subseteq \alpha^+$, $A = \{\alpha\}$ and hence α is the smallest element of A. Thus, every subset of α^+ has a smallest element, and so α^+ is well-ordered under the $\in$ ordering.

For all $\beta \in \alpha$, $s(\beta) = \beta$, so we only need to verify this property for $\alpha \in \alpha^+$. From above, we have that α is the largest element in α^+, so $s(\alpha)$ in α^+ is precisely everything in α^+ that is not α. But $\alpha^+ = \alpha \cup \{\alpha\}$, hence $s(\alpha) = \alpha$, and α^+ is an ordinal. □

Thus, ω^+ is an ordinal. All ordinals greater than or equal to ω are called *transfinite*. Unlike the finite ordinals (every element of ω), not all transfinite ordinals have an immediate predecessors. For example, ω^+ has predecessor ω, but ω has no largest element and hence no immediate predecessor. An ordinal with an immediate predecessor is called a *successor* ordinal; the others (such as ω) are called *limit* ordinals. It is clear that the ordinals are well-ordered; that is, that any set of ordinals has a smallest element by extension of the $\in$ ordering.

Just as we found ω to be the set of all natural numbers, is there a set containing all of the ordinals? As it turns out, it doesn't make any sense to talk about such a set.

Proposition 4.4. *There is no set comprised precisely of all the ordinal numbers.*

Lemma 4.5. *If α is an ordinal, $\alpha \notin \alpha$.*

Proof. If α is an ordinal, then α^+ is also an ordinal, so $s(\alpha) = \alpha$. Then $\alpha \in \alpha \implies \alpha \in s(\alpha)$, which contradicts the definition of $s(\alpha)$. □

Proof. Suppose there does exist such a set Ω. Then Ω itself is an ordinal: it is well-ordered, and $\forall \beta \in \Omega$, $s(\beta) = \beta$. Then $\Omega \in \Omega$, and so by the previous lemma, Ω cannot be an ordinal. Hence there cannot be such a set Ω. □

In fact, the collection of all ordinals is called a *class*. We will refer to this class when necessary, but otherwise we are not concerned with the notion of a class.

Lemma 4.6. *If α is an ordinal, $s(\alpha)$ is an ordinal.*

Proof. α well-ordered implies that every subset of α is well-ordered. Thus $s(\alpha)$ is well-ordered. As above, α an ordinal implies that α^+ is an ordinal, hence $s(\alpha) = \alpha$. Hence, $\forall \beta \in s(\alpha), \beta \in \alpha$. But α an ordinal implies that $\forall \beta \in \alpha, s(\beta) = \beta$, hence for all $\beta \in s(\alpha), s(\beta) = \beta$, and $s(\alpha)$ is an ordinal. □

Theorem 4.7. ***Counting Theorem*** *Each well-ordered set is isomorphic to a unique ordinal number.*

Proof. Let A be a well-ordered set. Assuming it is isomorphic to some ordinal, uniqueness is easy: $A \sim \alpha$ and $A \sim \beta$ for α, β ordinals implies that $\alpha \sim \beta$ by transitivity, and since the ordinals are well-ordered, $\alpha \sim \beta \implies \alpha = \beta$.

We recall Proposition 3.10. We let A be our well-ordered set, and construct a subset A_0 as before, where A_0 is the set of $a \in A$ such that $s(a) \sim s(\alpha)$ for α an ordinal. We define a function $f : A_0 \to$ ordinals where, for each $a \in A_0, f(a) = \alpha$ such that $s(a) \sim s(\alpha)$. By the above uniqueness argument, f is well-defined. Let Ω_0 be the image of A_0 under f.

By the argument in Proposition 3.10, both A_0 and Ω_0 are closed downwards. If $A = A_0$, then we are done, so assume not. Then let x be the smallest element in $A - A_0$. Ω_0 is an ordinal, by construction, so Ω_0^+ is the smallest ordinal not in Ω_0. Then, using the argument in Proposition 3.10, $s(x) \sim s(\Omega_0)$, so $x \in A_0$. Hence $A - A_0$ cannot contain a smallest element, and is therefore empty. Then $A = A_0$, and A is isomorphic to a unique ordinal (Ω_0 by construction). □

4.1.2 Ordinal Arithmetic

When we are talking about natural numbers, we generally represent the successor of $n \in \omega$ as $n + 1$, not n^+. The problem with this is that we have not made sense of the $+$ operator. Our intuition tells us that $n+1$ should just mean to adjoin 1 to the set n. But $1 \in n$ already, so doing this would mean that $n + 1 = n$. What we need $n + 1$ to mean is to add one *new* element to the set n. Thus, using n^- to represent the *predecessor* of n (which existd because n is finite, if $n = \{0, 1, 2, \ldots, n^-\}$, then we could write $n + 1 = \{0, 1, 2, \ldots, n^-, a\}$ where $a \notin n$. Ideally, we would like $a = n$, but by demanding that a be the largest element in the set $n+1$, we do not upset the well-ordering, and hence, by Theorem 4.7. $n+1$ is isomorphic to a unique ordinal; namely, n^+. Note that we are regarding $\sim$ as equivalent to $=$.

This idea can be generalized.

Definition 4.8. For two ordinals α and β, $\alpha + \beta := \alpha \sqcup \beta$.

$\sqcup$ represents the *disjoint* union of the sets α and β; since for any two ordinals, either $\alpha \in \beta, \alpha = \beta$, or $\beta \in \alpha$, α and β are not *a priori* disjoint: we can achieve this very easily by replacing β with $\beta \times \{1\}$. The two are isomorphic, so this is not a problem.

Ideally, we would hope that the class of ordinals is closed under this addition operation:

Proposition 4.9. *If α and β are ordinals, $\alpha + \beta$ is an ordinal.*

Proof. We retain the well-ordering on α and on β, respectively. Replacing β with $\beta \times \{1\}$ does not disrupt this at all: we simply order $\beta \times \{1\}$ by the first coordinate of every ordered pair. Then we require that, for $b \in \beta$ the smallest element, $a < (b, 1)$ for all $a \in \alpha$. Consider a subset A of $\alpha + \beta$. If $A \cap \alpha$ is nonempty, then the smallest element of A is the smallest element of $A \cap \alpha$. If $A \cap \alpha$ is empty, then $A \subseteq \beta \times \{1\}$, and since $\beta \times \{1\}$ is well-ordered, A has a smallest element. Hence $\alpha + \beta$ is well-ordered.

Next, consider $s(\gamma)$ for some γ in $\alpha + \beta$. If $\gamma \in \alpha$, then we already have $s(\gamma) = \gamma$. Now suppose $\gamma = (b, 1)$ where b is as defined above. Then $s(\gamma) = \alpha$, and by Theorem 4.7, $\gamma \sim \alpha$, so $s(\gamma) = \gamma$. This argument extends by induction, and hence $\forall \gamma \in \alpha + \beta$, $s(\gamma) = \gamma$. □

Consider, then, ω and $1 + \omega$, and consider the inclusion mapping between them. Since neither has a last element, and neither contains any limit ordinals, this mapping is a bijection, and hence $\omega = 1 + \omega$. Clearly, however $\omega + 1$ is the successor of ω: ω has no last element, but $\omega + 1$ does. Addition, therefore, is not commutative.

We now write α^+ as $\alpha + 1$. This allows us to write $\omega + 1, \omega + 2 (= (\omega + 1)^+), \omega + 3, \ldots$. It is easy to see in this way that we will come eventually to $\omega + \omega$, usually written as $\omega * 2$, and gives us some idea of what it means to multiply ordinals.

Definition 4.10. For α and β ordinals, $\alpha * \beta := \alpha + \alpha + \cdots + \alpha$, where there are β additions of α.

Thus $\omega * 2 = \omega + \omega$, but $2 * \omega = 2 + 2 + \cdots + 2$ ω times. It is clear from this that multiplication is *not* commutative: adding two together ω times will never allow us to get beyond the natural numbers; hence $2 * \omega = \omega$, while $w * 2$ does not.

We have one more arithmetic definition:

Definition 4.11. For α, β ordinals, $\alpha^\beta := \alpha * \alpha * \cdots * \alpha$, where the multiplication is performed β times.

Again, just as addition and multiplication do not quite work in the familiar way, not all of the usual properties of exponentiation hold: for example, $(\alpha * \beta)^\gamma \neq \alpha^\gamma * \beta^\gamma$ in general.

The above definitions can all also be formulated recursively, which will make them easier to work with:

Definition 4.12. Let α, β be ordinals

1. If β is a successor ordinal (i.e. $\beta = \gamma + 1$), then $\alpha + \beta = (\alpha + \gamma) + 1$. If β is a limit ordinal, then $\alpha + \beta = \sup_{\gamma < \beta} \alpha + \gamma$.
2. If $\beta = \gamma + 1$, then $\alpha * \beta = (\alpha * \gamma) + \alpha$. Else, $\alpha * \beta = \sup_{\gamma < \beta} \alpha * \gamma$.
3. If $\beta = \gamma + 1$, then $\alpha^\beta = \alpha^\gamma * \alpha$. Else, $\alpha^\beta = \sup_{\gamma < \beta} \alpha^\gamma$.

4.1.3 Countability

Definition 4.13. Let α be an ordinal, and A be a set.

1. We call α *countably infinite* if there exist injections from ω to α and α to ω.
2. We call α *countable* if α is either finite or countably infinite.
3. We call α *uncountable* if it is not countable. We define ω_1 as the smallest uncountable ordinal (the set of all countable ordinals); thus, $\omega_1 = \sup \alpha$, where α are countable ordinals.

Lemma 4.14. *There is no countable sequence of countable ordinals such that their* sup *is* ω_1.

Proof. Assume so. Then we have a monotone increasing function $f : \omega \to \omega_1$ such that $\sup_{\alpha \in \omega} f(\alpha) = \omega_1$. Consider $\mathcal{U} = \bigcup_{\alpha < \omega} s(f(\alpha))$. Note that $\forall \alpha < \omega, f(\alpha) \in \omega_1$, so $f(\alpha)$ is countable, and hence $s(f(\alpha))$ is a countable set. Thus $\mathcal{U}$ is a countable union of countable sets, and is hence countable by the following "diagonalization" argument:

Send 1 to the smallest element in $s(f(1))$, 2 to the smallest element in $s(f(2))$, 3 to the smallest remaining element in $s(f(1))$, 4 to the smallest element in $s(f(3))$, 5 to the smallest remaining element in $s(f(2))$, and so on. If there is no smallest remaining element in some set, then it is empty since it is an ordinal by Lemma **??** and hence well-ordered. If this happens, then send $n \in \omega$ to the next item on the list as ordered above. This gives a bijection between ω and $\mathcal{U}$.

Now, $\forall \alpha < \omega_1, \exists \beta$ such that $\alpha < f(\beta)$ by definition of our function f. Thus, $\forall \alpha < \omega_1, \exists \beta < \omega$ such that $\alpha \in s(f(\beta))$. Thus, $\forall \alpha < \omega_1, \alpha \in \mathcal{U}$, and $\omega_1 \subseteq \mathcal{U}$. But then $\mathcal{U}$ is uncountable.

Hence there can exist no function f with the properties we assumed, and there is no countable sequence of countable ordinals with supremum ω_1. In general, the supremum of a countable sequence of countable things is countable. □

Lemma 4.15. *If* α *is an ordinal,* $\omega^\alpha \geq \alpha$

Proof. We use induction. Let α be such that for all ordinals $\beta < \alpha, \omega^\beta \geq \beta$.

$\omega^\alpha = \sup_{\beta < \alpha} \omega^\beta$, and $\alpha = \sup_{\beta < \alpha} \beta$. By the induction hypothesis, $\omega^\beta \geq \beta$ for each $\beta < \alpha$, so $\sup_{\beta < \alpha} \omega^\beta \geq \sup_{\beta < \alpha} \beta$. But then $\omega^\alpha \geq \alpha$. □

Proposition 4.16. *If* α *and* β *are both countable ordinals, then* α^β *is countable.*

Proof. In order to use induction, assume α^γ is countable $\forall \gamma < \beta$.

Suppose β is a successor ordinal, $\beta = \gamma + 1$. Then $\alpha^\beta = \alpha^\gamma * \alpha$, and α^γ is countable by the induction hypothesis. But then $\alpha^\gamma * \alpha$ is countable by a diagonalization argument similar to the one from Lemma 4.14: send 1 to the smallest element in the "first" α^γ, 2 to the smallest element in the "second" α^γ, 3 to the smallest remaining element in the first α^γ, 4 to the smallest element in the "third" α_γ, and so on. Since α is countable, this gives a bijection between ω and α.

Suppose β is a limit ordinal. Then $\alpha^\beta = \sup_{\gamma<\beta} \alpha^\gamma$. But by the induction hypothesis, and β countable, this is the supremum of a countable sequence of countable ordinals; hence, by Lemma 4.14, α^β is countable. □

Definition 4.17. ϵ_0 is defined as the smallest ordinal such that $\omega^\alpha = \alpha$.

Lemma 4.18. $\omega^{\omega_1} = \omega_1$

Proof. $\omega^{\omega_1} = \sup_{\alpha<\omega_1} \omega^\alpha$. Every element in this sequence is countable, so $\omega^{\omega_1} \leq \omega_1$. But we have an uncountably long sequence, which cannot be indexed by any countable ordinal, hence $\omega^{\omega_1} \geq \omega_1$, and so $\omega^{\omega_1} = \omega_1$. □

Lemma 4.19. *Let $\beta = \sup\{\alpha_0, \alpha_1, \alpha_2, \dots\}$ where the αs are not necessarily* all *the ordinals less than β.. Then $\omega^\beta = \sup\{\omega^{\alpha_0}, \omega^{\alpha_1}, \omega^{\alpha_2}, \dots\}$.*

Proof. It is clear that $\omega^\beta \geq \sup\{\omega^{\alpha_0}, \omega^{\alpha_1}, \omega^{\alpha_2}, \dots\}$.

Now assume that $\omega^\beta > \sup\{\omega^{\alpha_0}, \omega^{\alpha_1}, \omega^{\alpha_2}, \dots\}$. We will refer to the set $\{\alpha_0, \alpha_1, \alpha_2, \dots\}$ as A. By definition, $\omega^\beta = \sup_{\gamma<\beta} \omega^\gamma$. But $\beta = \sup A$, so $\omega^\beta = \sup_{\gamma<\sup A} \omega^\gamma$, and our assumption becomes: $\sup_{\gamma<\sup A} \omega^\gamma > \sup_{\alpha\in A} \omega^\alpha$.

$$\sup_{\gamma<\sup A} \omega^\gamma > \sup_{\alpha\in A} \omega^\alpha$$
$$\implies \exists \gamma < \sup A \text{ such that } \omega^\gamma > \sup_{\alpha\in A} \omega^\alpha$$

and

$$\gamma < \sup A \implies \exists \alpha \in A \text{ such that } \alpha > \gamma$$

But then $\omega^\gamma < \omega^\alpha$ for some $\alpha \in A$, so $\omega^\gamma > \sup_{\alpha\in A} \omega^\alpha$ cannot hold, and our assumption is false. Hence $\omega^\beta \leq \sup\{\omega^{\alpha_0}, \omega^{\alpha_1}, \omega^{\alpha_2}, \dots\}$.

Then we have $\omega^\beta \geq \sup\{\omega^{\alpha_0}, \omega^{\alpha_1}, \omega^{\alpha_2}, \dots\}$ and $\omega^\beta \leq \sup\{\omega^{\alpha_0}, \omega^{\alpha_1}, \omega^{\alpha_2}, \dots\}$, so $\omega^\beta = \sup\{\omega^{\alpha_0}, \omega^{\alpha_1}, \omega^{\alpha_2}, \dots\}$. □

Proposition 4.20. *ϵ_0 is countable.*

Proof. Consider $\gamma = \sup\{1, \omega, \omega^\omega, \omega^{\omega^\omega}, \dots\}$. Then, by Lemma 4.19, $\omega^\gamma = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \dots\}$. It is clear that $\sup\{1, \omega, \omega^\omega, \omega^{\omega^\omega}, \dots\} = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \dots\}$, so $\omega^\gamma = \gamma$. Thus $\epsilon_0 \leq \gamma$.

For efficiency's sake, we will write ω^ω as ${}^2\omega$, ω^{ω^ω} as ${}^3\omega$, and so on. By repeated application of Proposition 4.16, ${}^n\omega$ is countable for any finite ordinal n.

γ is countable: it is the supremum of a countable (the bijection sends 0 to 1, 1 to ω, 2 to ${}^2\omega$, etc) sequence of countable ordinals. By definition, $\epsilon_0 \leq \gamma$, so γ countable $\implies$ ϵ_0 countable. □

Proposition 4.21. *$\epsilon_0 = \gamma$, where γ is defined as in the proof of Proposition 4.20.*

Proof. We know that $\epsilon_0 \leq \gamma$ since $\omega^\gamma = \gamma$ and ϵ_0 is defined as the smallest ordinal α for which $\omega^\alpha = \alpha$. From Lemma 4.15, we know that $\omega^\alpha \geq \alpha$ in general. Thus, to show that $\epsilon_0 = \gamma$, we need to show that, $\forall \alpha < \gamma, \omega^\alpha > \alpha$.

Let $\alpha < \gamma$. If $\alpha = {}^k\omega$ for some finite k, then $\omega^\alpha = {}^{k+1}\omega$, and $\omega^\alpha > \alpha$.

Assume that $\alpha \neq {}^k\omega$. Then, $\exists n$ finite such that ${}^n\omega > \alpha > {}^{n-1}\omega$. But then $\omega^{{}^n\omega} > \omega^\alpha > \omega^{{}^{n-1}\omega}$; that is, ${}^{n+1}\omega > \omega^\alpha > {}^n\omega$, and since ${}^n\omega > \alpha$, $\omega^\alpha > \alpha$.

Thus, $\forall \alpha < \gamma$, $\omega^\alpha > \alpha$, and $\epsilon_0 = \gamma$. □

Theorem 4.22. ***Cantor's Theorem.*** *$\forall A$ sets, $A < \mathcal{P}(A)$.*

Proof. It is clear that $A \leq \mathcal{P}(A)$, since we have the injective function $f : A \to \mathcal{P}(A)$ with $f(a) = \{a\}$ for all $a \in A$.

Now assume there exists a surjective map g from A to $\mathcal{P}(A)$. $B = \{a \in A : a \notin g(a)\}$.$B \in \mathcal{P}(A)$, and g onto, so $\exists b \in A$ such that $f(b) = B$. If $b \in B$, then by definition of B, $b \notin g(b)$, and since $g(b) = B$ this cannot happen. If $b \notin B$, then $b \in g(b)$, which is also impossible. Hence, there exists no such g, and $A \nsim \mathcal{P}(A)$.

Hence $A < \mathcal{P}(A)$. □

This leads us into the next concept.

4.2 Cardinals

Ideas about countability lead us to questions about the relative sizes of sets. We understand the set $\{a, b\}$ as different from the set $\{c, d, e\}$ not merely because they have different elements (we do not know if any of a, b, c, d, or e are equal), but because we can see that they contain different numbers of elements.

Definition 4.23. We write $|A| \leq |B|$ for two sets A and B if there is an injection from A to B. We write $|A| = |B|$ if there is a bijection between A and B.

Proposition 4.24. *$|A| \leq |B|$ and $|B| \leq |A|$ if and only if $|A| = |B|$.*

Proof. For the forward direction, if $|A| \leq |B|$ then we have $f : A \to B$ an injection. Similarly, if $|B| \leq |A|$, we have $g : B \to A$ an injection. If either f or g is surjective, we are done, so assume not. Assume A and B are disjoint; if not, replace A with $A \times \{1\}$.

Call $a \in A$ the *parent* of $f(a) \in B$, and similarly, $b \in B$ the parent of $g(b) \in A$. Each $a \in A$ has an infinite sequence of *descendants*, in particular, $f(a), g(f(a)), f(g(f(a)))$, etc. Each term in the sequence is a descendant of all preceding terms and an *ancestor* of all following terms.

For each element in A or B, one of three things must happen. If we trace it back as far as possible, then we either come to an element of A which has no parent, or an element of B that has no parent, or the sequence regresses infinitely. Let A_A be the set of elements of A which originate in A; that is, A_A is the union of $A - g(B)$ (nonempty by assumption) and its descendants in A. Let A_B be the set of elements of A which originate in B; A_B comprises the descendants in A of the elements of $B - f(A)$ (nonempty by assumption), and

let A_∞ be the set of elements in A with no parentless ancestor. We partition B similarly into $B_A, B_B, and B_\infty$.

If $a \in A_A$, it is clear that $f(a) \in B_A$. In particular, elements of B_A are, by definition, of the form $f(a)$ for some $a \in A_A$. This gives us injectivity and surjectivity, and thus, $f|_{A_A}$ (f restricted to A_A) is a bijection between A_A and B_A. If $b \in B_B$, then $g(b) \in A_B$. Elements of A_B are of the form $g(b)$ for some $b \in B_B$, so we have $g|_{B_B}$ a bijection between B_B and A_B. Thus, $g^{-1}|_{A_B}$ is a bijection between A_B and B_B. If $a \in A_\infty$, then $f(a) \in B_\infty$ and vice versa, and $f|_{A_\infty}$ is a bijection between A_∞ and B_∞. Combining these three bijections, we get a bijection between A and B. Thus, by Definition 4.23, we have $|A| = |B|$.

The reverse direction is obvious: $|A| = |B|$ implies there is a bijection $f : A \to B$, hence f is an injection from A into B, and f^{-1} is an injection from B into A. □

We have used the notation $|A|$ for a set A without explaining what it means. From Definition 4.23 and Proposition 4.24, it should seem apparent that $|A|$ relates to the *size* of A as a set. We formalize this below:

Definition 4.25. The *cardinality* of a set A, written $|A|$, is the smallest ordinal α such that there is a bijection between α and A.

In particular, then, two ordinals α and β have the same cardinality if we can find an injection from α into β and vice versa. It is apparent, then, that no two distinct finite ordinals can have the same cardinality. This requires a simple application of the finite *pigeonhole principle*: consider the two finite cardinals $m > n$ as natural numbers, and it is clear that we cannot map the larger into the smaller without sending at least two elements from m to the same element in n (if we have m pigeons and n pigeonholes, then at least two of them must share.) Similarly, no finite ordinal has the same cardinality as a transfinite ordinal.

Can we have transfinite ordinals with the same cardinality? The answer is yes: in fact, from our definition of countably infinite, it is apparent that any two countably infinite ordinals have the same cardinality.

Example 4.26. Consider ω and $\omega + 1$.

The inclusion map $f : \omega \hookrightarrow \omega + 1$ is clearly an injection. Consider the map $g : \omega + 1 \to \omega$ which sends ω (the largest element in $\omega + 1$) to $0 \in \omega$, and then $\forall n \in \omega + 1$ such that $n < \omega$, $g(n) = n + 1$. Is this an injection?

It is clear that only ω maps to 0 since 0 has no predecessor in ω. Now suppose $f(n) = f(m)$ for $n, m \neq 0$. Then $n + 1 = m + 1$, and $n = m$. Hence g is injective, and we have an injection from $\omega + 1$ to ω.

But then ω and $\omega + 1$ have the same cardinality, and since ω is the smallest transfinite cardinal, that cardinality is ω. We refer to ω as a *cardinal number.*

Definition 4.27. A *cardinal number* is an ordinal α such that if β is an ordinal number of the same cardinality as α, then $\beta \geq \alpha$.

It is clear that the ordinals can be partitioned by cardinality, and thus that the definition of cardinal from above simply selects the smallest representative of each equivalence class. The equivalence classes are also called *cardinals*, but we use the ordinal notation when we are speaking of their standard representative, and a different notation when we are speaking of the equivalence class. Thus, the cardinal equivalence class of ω is written $\aleph_0$ (aleph nought). The finite cardinals are singleton classes and are thus written as ordinals.

The smallest uncountable number, ω_1 is by definition *not* in bijection with any countable ordinal; hence it must be in a different equivalence class. We call this class $\aleph_1$. By the same argument as above, $\omega_1 + 1$ has the same cardinality as ω_1, as do $\omega_1 + \omega$, and, in fact, $\omega_1 + \alpha$, where α is any countable ordinal.

We regard $\aleph_1$ as the *successor cardinal* of $\aleph_0$; in general, $\aleph_{\beta+1}$ is the successor of $\aleph_\beta$, where β is an ordinal. If β is a limit ordinal, then $\aleph_\beta$ is a *limit cardinal* and $\aleph_\beta = \sup_{\gamma<\beta} \aleph_\gamma$.

For our purposes, when we refer to a cardinal, we will be referring to the standard representative and not the equivalence class unless specified.

Proposition 4.28. *If α is a cardinal, then α is a limit ordinal.*

Proof. Suppose α is a successor ordinal. Then $\alpha = \beta+1$, where β is an ordinal. The inclusion map $f : \beta \hookrightarrow \alpha$ is clearly an injection from β to α. To find an injection from α to β, send the largest element (β) of α to $0 \in \beta$. Then for each $\gamma \in \alpha$, send γ to $\gamma + 1 \in \beta$. The function g so defined is injective, as per the argument in Example 4.26. Then, by Proposition 4.24, α has the same cardinality as β, and since $\beta < \alpha$, α is not the smallest ordinal with this cardinality and is hence not a cardinal. Thus, no successor ordinals can be cardinals, and all cardinals are limit ordinals. (Note: the converse is not true). □

Claim 4.29. *The cardinals are well-ordered.*

Proof. This is apparent: all cardinals are ordinals and hence the cardinals form a subcollection of a well-ordered collection. Thus any subset of cardinals has a least element, since it is a subset of ordinals, and the cardinals are well-ordered. □

The relationship between cardinals and cardinality is very close: in fact, for any cardinal a, we can write a as the cardinality of some set A. This allows us to define arithmetic operations on cardinals in terms of set operations.

Definition 4.30. Let A and B be sets:

1. $|A| + |B| = |A \sqcup B|$.
2. $|A| * |B| = |A \times B|$
3. $|A|^{|B|} = |A^B|$, where A^B represents the set of all functions from B to A.

The first two of these are generalizable to families of sets:

Definition 4.31. For all $i \in I$ some indexing set, let A_i be a set.

1. $\sum_{i\in I} |A_i| = |\bigsqcup_{i\in I} A_i|$
2. $\prod_{i\in I} |A_i| = |\prod_{i\in I} A_i|$, where the product on the right hand side represents a cartesian product.

These definitions hold for infinite sets, but we must be a little careful, as some things work counterintuitively.

Example 4.32. Let $I = \omega$ and $|B_i| = 1$, $|A_i| = 2$ for all i. Then, $\forall i, |B_i| < |A_i|$, which would suggest that $\sum_{i\in\omega} |B_i| < \sum_{i\in\omega} |A_i|$.

But $\sum_{i\in\omega} |B_i| = 1 + 1 + \ldots$ ω times and $\sum_{i\in\omega} |A_i| = 2 + 2 + \ldots$ ω times; that is, $|B_i| = \omega, |A_i| = 2 * \omega = \omega$, so $|B_i| = |A_i|$.

Thus we cannot, in general, make the claim that if $\forall i \in I, |B_i| < |A_i|$, $\sum_{i\in I} |B_i| < \sum_{i\in I} |A_i|$

Claim 4.33. ***Gyula Konig.*** *For two families of sets A_i and B_i, $i \in I$ well-ordered, $|B_i| < |A_i|, \forall i \implies \sum_{i\in I} |B_i| < \prod_{i\in I} |A_i|$.*

Proof. We use transfinite induction. Let

$$K = \{n \in I| \text{ if } i \leq n, \sum_{i\in I}^{n} |B_i| < \prod_{i\in I}^{n} |A_i| \text{ when } |B_i| < |A_i|, \forall i\} \tag{32}$$

$K \subseteq I$, so let $j \in I$ be such that $\forall i < j, i \in K$. Then we have $\sum_{i<j} |B_i| < \prod_{i<j} |A_i|$. $\sum_{i<j} |B_i| = |\sqcup_{i<j} B_i|$, so let $\mathcal{B}_1 = \sqcup_{i<j} B_i$. Similarly, $\prod_{i<j} |A_i| = |A_1 \times A_2 \times \cdots \times A_i \times \ldots| = |\prod_{i<j} A_i|$, so let $\mathcal{A}_1 = \prod_{i<j} A_i$. By hypothesis, $|\mathcal{B}_1| < |\mathcal{A}_1|$. We let $\mathcal{B}_2 = B_j$, and $\mathcal{A}_2 = A_j$. Again by hypothesis, $|\mathcal{B}_2| < |\mathcal{A}_2|$. Thus, by the induction hypothesis, $|\mathcal{B}_1| + |\mathcal{B}_2| < |\mathcal{A}_1||\mathcal{A}_2|$. But

$$\begin{aligned}
& |\mathcal{B}_1| + |\mathcal{B}_2| < |\mathcal{A}_1||\mathcal{A}_2| \\
\implies & |\mathcal{B}_1 \sqcup \mathcal{B}_2| < |\mathcal{A}_1 \times \mathcal{A}_2| \\
\implies & |\bigsqcup_{i\in I}^{j} B_i| < |\prod_{i\in I}^{j} A_i| \\
\implies & \sum_{i\in I}^{j} |B_i| < \prod_{i\in I}^{j} |A_i| \\
& \implies j \in K
\end{aligned}$$

But then $\forall i < j, i \in K \implies j \in K$, so by the principle of transfinite induction, $K = I$. □

Theorem 4.34. *If a is an infinite cardinal, $a * a = a$. If at least one of a, b is infinite, $a * b = \max\{a, b\}$.*

Proof. If a is a cardinal, then $a = |A|$ for some set A. $a * a = |A| * |A| = |A \times A|$. Thus we need to show that for $|A|$ infinite, $|A \times A| = |A|$. A is well-orderable by Theorem 3.11, and we can say $|A| = \aleph_\alpha$ for some ordinal α. To use induction, we assume that, for all infinite $\beta < \alpha$, $\aleph_\beta * \aleph_\beta = \aleph_\beta$.

If A is well-ordered, we can induce a well-ordering on $A \times A$:
For $a, b, c, d \in A, (a, b) < (c, d)$ if

1. $\max(a, b) < \max(c, d)$
2. $\max(a, b) = \max(c, d)$ and $a < c$
3. $\max(a, b) = \max(c, d)$ and $a = c$ and $b < d$

This is clearly a well-ordering, since it relies only on the comparison of elements of A.

For $(a, b) \in A \times A$, let $\epsilon = \max(a, b) + 1$. Then $|\epsilon| < \aleph_\alpha$, and so we can say $|\epsilon| = \aleph_\beta$ for some $\beta < \alpha$. Consider the initial segment $s((a, b))$:

$$s((a, b)) = \{(c, d) \in A \times A : (c, d) < (a, b)\} \tag{33}$$

$$s((a, b)) \leq |\epsilon| * |\epsilon| = \aleph_\beta * \aleph_\beta = \aleph_\beta \tag{34}$$

by the induction hypothesis.

By Theorem 4.7, $|A \times A| \sim \gamma$, where γ is an ordinal. Thus we have an isomorphism $\phi : A \times A \to \gamma$. It is clear that $\aleph_\alpha \leq \gamma$ (we can inject A into $A \times A$ by simply mapping a to (a, a)), so we want to show that $\aleph_\alpha \geq \gamma$.

Assume $\aleph_\alpha < \gamma$. Then $\exists (a, b) \in A \times A$ such that $\phi(a, b) = \aleph_\alpha$. But since ϕ is an isomorphism, $s(\phi(a, b)) = s((a, b))$ and so $|s(\phi(a, b))| = |s((a, b))| = \aleph_\alpha$ contradicts Equation 34 above. Hence $\aleph_\alpha \geq \gamma$, and since $\aleph_\alpha \leq \gamma$, we have $\aleph_\alpha = \gamma$, and $|A \times A| = |A|$. Thus, for a an infinite ordinal, $a * a = a$.

The second part of the theorem follows. □

4.3 Cofinality

Definition 4.35. Let B be a subset of an ordered set A. A is *cofinal* with B if $\forall a \in A, \exists b \in B$ such that $b \geq a$.

Proposition 4.36. *Every ordered set A is cofinal with a well-ordered subset.*

Proof. Let the cardinality of A be $\aleph_\alpha$, and let B be a well-ordered set such that $|B| > \aleph_\alpha$. We can regard B as an ordinal. Define a function as follows:

$f : B \to A \cup \{\infty\}$. Let f be monotone increasing except on "∞". We regard ∞ as greater than all elements of A. If β is a limit ordinal in B such that $\exists a \in A$ with the property that $\forall \gamma < \beta, a > f(\gamma)$, then let $f(\beta) = a$. If there does not exist such an a, then let $f(\beta) = \infty$.

A is cofinal with $f(B) \cap A$ by construction, and since $f(B)$ is the image of a well-ordered set under an order-preserving map, $f(B)$ is well-ordered. Hence A is cofinal with a well-ordered subset. □

Proposition 4.37. *ω is cofinal with every countable limit ordinal.*

Proof. Let α be a countable ordinal. Then there is a bijection $f : \omega \to \alpha$. We want to construct $A \subseteq \omega$ such that $f|_A$ is monotone increasing and $f(A)$ is cofinal in α. We can construct a set A_k as follows:

Let $0 \in A_k$. Then, for each $\beta \in \alpha$, $\beta \in A_k$ if $f(\beta) > f(\gamma)$ for all $\gamma \in A_k$ with $\gamma < \beta$. Clearly, $f|_{A_k}$ is monotone.

Suppose $A_k = \{a_1 < a_2, \ldots, a_k\}$. If $f(A_k)$ is cofinal in α, then let $A = A_k$ and we are done. If not, then choose $a_{k+1} \in \omega$ such that $f(a_{k+1}) > f(a_k)$ and $f(a_{k+1}) > f(k)$. Adjoin a_{k+1} to A_k and call the new set A_{k+1}. If $f(A_{k+1})$ is cofinal then $A_{k+1} = A$. If not, then choose a_{k+2} in a similar fashion. The limit of this process yields a cofinal set A.

□

Definition 4.38. The *cofinality* of a set A (written $\mathrm{cf}(A)$) is the smallest ordinal with which A is cofinal.

Proposition 4.39. *The cofinality of any successor ordinal is* 1.

Proof. Let α be a successor ordinal. Then $\alpha = \beta + 1$ for some ordinal β, and the largest element in α is β. Consider the $\{\beta\} \subset \alpha$. For all $\gamma \in \alpha$, $\beta \geq \gamma$, and hence α is cofinal with $\{\gamma\}$. But $\{\gamma\} \sim 1$, so $\mathrm{cf}(\alpha) = 1$. □

Proposition 4.40. *For any set A, cf(A) is a cardinal.*

Proof. $\mathrm{cf}(A)$ is an ordinal, by definition. If $\mathrm{cf}(A)$ is finite, then it is of course a cardinal. Hence we are only concerned with sets A such that $\mathrm{cf}(A)$ is transfinite. Let $\mathrm{cf}(A) = \alpha$ where α is transfinite. If α is not a cardinal, it has the same cardinality as β for some ordinal β. By a construction similar to the one in Proposition 4.37, α and β are cofinal, and since cofinality is transitive, β is cofinal to A. Then $\alpha \leq \beta$ by definition of cofinality, and hence $\alpha \leq \gamma$ if γ has the same cardinality as α, and hence α is a cardinal. □

5 The Axiom of Choice, Zorn's Lemma, and the Well-Ordering Theorem

Axiom 5.1. Axiom of Choice. For every set A, there exists a *choice* function $f : (\mathcal{P}(A) - \{\emptyset\} \to A$ such that $\forall B \subset A, f(B) \in A$.

In several of these proofs, we have used Theorem 3.11, namely, that every set can be well-ordered. As mentioned earlier, we need the axiom of choice to prove this, but it may be noticed that, while we have used the other axioms set out in Section 2.1, we have not used the Axiom of Choice in order to prove anything else. As it turns out, there are two models of set theory which use the axioms stated: one includes the axiom of choice, and the other does not. The Axiom of Choice is commonly accepted; indeed, any results which have used the Well-Ordering Theorem cannot be shown without it.

We first state a well-known lemma which is equivalent to the Axiom of Choice and which we will use to prove the Well-Ordering Theorem.

Theorem 5.2. ***Zorn's Lemma*** *If A is a partially ordered set such that every totally ordered subset has an upper bound, then A contains a maximal element.*

Proof. In this proof, we will refer to a totally ordered subset of a set A as a *chain* in A.

For each element in A consider the *weak* initial segment $\overline{s}(a)$ consisting of a as well as its predecessors. We can regard $\overline{s}$ as a function from A to $\mathcal{P}(A)$. Let $\mathcal{S}$ be the image of $\overline{s}$. $\overline{s}$ is clearly injective; moreover, $\overline{s}(a) \subseteq \overline{s}(b) \iff a \leq b$. Thus we have translated the partial order on A into the subset relation, and our problem is now one of maximal sets rather than maximal elements.

Let $\mathcal{B}$ be the collection of all subsets $\mathcal{A}$ of A such that $\mathcal{A} \subseteq \overline{s}(a)$ for some $a \in A$. $\emptyset \in \mathcal{B}$, so $\mathcal{B}$ is clearly nonempty, and is partially ordered by inclusion.

If $\mathcal{C}$ is a chain in B, then $\bigcup \mathcal{C} = \bigcup_{C \in \mathcal{C}} C \subseteq \mathcal{B}$. It is clear that, $\forall \mathcal{A} \in \mathcal{B}, \mathcal{S} \geq \mathcal{A}$. Moreover, $\bigcup \mathcal{C}$ is an upper bound for $\mathcal{C}$.

We now generalize the problem: Let B be a collection of subsets of $\mathcal{A}$ with the properties above: namely, that if $X \in B$, then every subset of X is in B, and the union of any chain of sets in B is also in B. Clearly, $\emptyset \in B$. We have thus reduced the problem to this: we need to show that B has a maximal element.

Let f be a *choice* function (see Axiom 5.1 above) for A. For each $D \in B$, let $\hat{D} = \{a \in A : D \cup \{a\} \in B\}$. We define a function $g : B \to B$ as follows: if $\hat{D} - D \neq \emptyset$, then $g(D) = D \cup \{f(\hat{D} - D\}$ and if $\hat{D} - D = \emptyset, g(D) = D$. Two things are clear: $g(D) - D$ is at most a singleton, and $\hat{D} - D = \emptyset \iff D$ is maximal. Thus we need to show that there exists a $D \in B$ sucht that $g(D) = D$.

We must introduce one more definition here before continuing:

Definition 5.3. $\mathcal{T} \in B$ is a *tower* if

1. $\emptyset \in \mathcal{T}$
2. $g(D) \in \mathcal{T}$ for all $D \in \mathcal{T}$
3. if $\mathcal{F}$ is a chain in $\mathcal{T}$, then $\bigcup_{F \in \mathcal{F}} F \in \mathcal{T}$.

We note that B itself is a tower.

Now let $\mathcal{T}_0$ be the intersection of all towers in B and hence the smallest. We want to show that $\mathcal{T}_0$ is a chain.

Call $X \in \mathcal{T}_0$ *comparable* if we can compare it with every set in $\mathcal{T}_0$ by the subset ordering. Then $\mathcal{T}_0$ is a chain if and only if every $X \in \mathcal{T}_0$ is comparable.

We let X be comparable. Suppose $D \in \mathcal{T}_0$ such that $D \subseteq X$. Since X is comparable, either $g(D) \subseteq X$ or $X \subseteq g(D)$. The latter requires that D be a proper subset of a proper subset of $g(D)$, but since $g(D) - D$ is at most a singleton, this cannot hold. Hence $g(D) \subseteq X$.

Now consider $\mathcal{U} = \{X \in \mathcal{T}_0 : D \subset X \text{ or } g(X) \subset D\}$. If $D \in \mathcal{U}$ then either $D \subset X$ or $g(X) \subset D$.

$\mathcal{U}$ is a tower:

1. It is clear that $\emptyset \subset X$.

2. If $D \subseteq X$, then $g(D) \subseteq X$, so $g(D) \in \mathcal{U}$. If $D = X$, then $g(D) = g(X)$, so $g(X) \subseteq g(D)$, and $g(D) \in \mathcal{U}$ If $g(X) \subseteq D$, then $g(X) \subseteq g(D)$ and $g(D) \in \mathcal{U}$.

3. That the union of a chain in $\mathcal{U}$ is in $\mathcal{U}$ follows from construction of $\mathcal{U}$.

Thus $\mathcal{U} \subseteq \mathcal{T}_0$ is a tower and since $\mathcal{T}_0$ is the smallest tower in B, $\mathcal{U} = \mathcal{T}_0$.

For each comparable $X, g(X)$ is also comparable. Given X, we form $\mathcal{U}$ as above, and since $\mathcal{U} = \mathcal{T}_0$, we have that for each $D \in \mathcal{T}_0$ either $D \subseteq X$ (so $D \subseteq g(X)$) or $g(X) \subseteq D$.

From this, we have that $\emptyset$ is comparable, and that g sends comparable sets to comparable sets. The union of a chain of comparable sets is comparable, so the comparable sets in $\mathcal{T}_0$ form a tower, and hence $\mathcal{T}_0$ is comparable.

$\mathcal{T}_0$ is a chain, so the union U of everything in $\mathcal{T}_0$ is also in $\mathcal{T}_0$. Thus $g(U) \subseteq U$, and since $U \subseteq g(U)$ for all U, $U = g(U)$ and we are done. □

We will use this to prove the well-ordering theorem.

Definition 5.4. Let A, B be well-ordered. A is a *continuation* of B if

1. $B \subseteq A$

2. B is a prefix of A.

3. $B \cap A \subseteq B$ is ordered identically to $B \cap A \subseteq A$.

It is clear that if we take a set $\mathcal{C}$ of initial segments of a set A, then $\mathcal{C}$ is a chain under continuation.

Lemma 5.5. *If $\mathcal{C}$ is a collection of initial segments of a well-ordered set X then the union U of $\mathcal{C}$ is well-ordered.*

Proof. Let $a, b \in U$. Then $\exists A, B \in \mathcal{C}$ with $a \in A, b \in B$. By definition of $\mathcal{C}$, either $A = B$ or one is a prefix of the other. Then there is a set in $\mathcal{C}$ which contains both a and b, and we order these two elements the way they are ordered in any set in $\mathcal{C}$ which contains both. This is unambiguous since $\mathcal{C}$ is a chain under continuation.

This gives an order: consider a nonempty subset S of U. It has nonempty intersection with some $C \in \mathcal{C}$, hence there is a smallest element in $S \cap C$. Since $\mathcal{C}$ is a continuation chain, this smallest element is the smallest element in S. Thus every subset has a smallest element, and U is well-ordered. □

Theorem 5.6. *Every set can be well-ordered.*

Proof. Given a set A, consider the set $\mathcal{W}$ consisting of all well-ordered subsets of A. $\emptyset$ can be regarded as well-ordered, so $\emptyset \in \mathcal{W}$ so $\mathcal{W}$ is nonempty, and can be partially ordered by continuation.

Let $\mathcal{C}$ be a chain in $\mathcal{W}$. $U = \bigcup \mathcal{C}$ has a unique well-ordering that makes $U \geq C$ for all $C \in \mathcal{C}$. Then U is an upper bound for $\mathcal{C}$, so by Zorn's Lemma, $\exists M \in \mathcal{W}$ so that M is maximal.

If $M = A$, we are done, since M is well-ordered. Assume $M \neq A$. Then, since $M \subseteq A, \exists a \in A$ so that $a \notin M$. But then U can be enlarged by placing a after all the elements of M, and we can reconstruct M to contain a. □

References

[1] Laszlo Babai. Lecture Notes: Transfinite Combinatorics. University of Chicago. 2007.

[2] Paul Halmos. Naive Set Theory. University Series in Undergraduate Mathematics. 1960.

[3] Joseph R. Mileti. Lecture Notes: An Introduction to Axiomatic Set Theory. Dartmouth University. 2007.

[4] Patrick Suppes. Axiomatic Set Theory. University Series in Undergraduate Mathematics 1960.