Group Structure on arbitrary sets: An algebraic application of the Axiom of Choice

by Oskar Emmerich

14th May 2025

LUND
UNIVERSITY
Faculty of Science
Department of Mathematics

Bachelor's Thesis in Mathematics

Thesis advisor: Anitha Thillaisundaram

Abstract

The thesis should include an abstract that summarizes its contents; mathematical jargon can be utilized here. The typical length of an abstract is between 100 and 300 words.

Contents

Introduction v

1 Preliminaries 1
- 1.1 First-Order Logic and Classes . . . 1
- 1.2 Zermelo-Fraenkel Axioms of Set Theory . . . 3
- 1.3 The Axiom of Choice . . . 6

2 Orderings and Well-Orderings 9
- 2.1 Linear, Partial and Well-Orderings . . . 9
- 2.2 Properties of Linear Orderings . . . 13
- 2.3 Ordinals . . . 14
- 2.4 The Well-Ordering Theorem . . . 17
- 2.5 Hartogs' Lemma . . . 19

3 Model Theory 21
- 3.1 Models of Formal Languages . . . 21
- 3.2 The Löwenheim-Skolem Theorem . . . 21

4 Hajnal's and Kertész's Theorem 23

Bibliography 25

Introduction

Historical Background

In 1902 Bertrand Russell showed with what is now known as *Russell's Paradox* that the previously used approach to set theory was inconsistent. Ernst Zermelo then created an axiomatic framework for set theory in 1905, motivated both by attempting to preserve results such as the theory of infinities by Georg Cantor, as well as avoiding paradoxes. These axioms, later modified by Abraham Fraenkel, became known as the nine *Zermelo-Fraenkel Axioms* (ZF) as well as the *Axiom of Choice* (AC)[Gol98, pp.66-70, 75].

The axiom of choice in particular is of special interest in many areas of mathematics, especially in algebra and topology, often in the form of the equivalent statement of *Zorn's Lemma*, which says that every non-empty partially ordered set with an upper bound has a maximal element [Jec78].

Finally in 1971 András Hajnal and Andor Kertész published a paper [HK72] which provided another equivalence to AC, namely that there exists a cancellative groupoid structure on every (uncountably infinite) set. This paper makes use of first-order model theory, an area of logic developed during the first half of the 20th century, which utilizes models of formal languages to obtain results. Kertész later expanded on this, providing an alternative algebraic partial proof in a lecture series given at the University of Jyväskylä [Ker75].

Thesis Structure

The aim of this thesis is to provide context to the paper [HK72] and to derive the theory needed for the proof of its main theorem:

Theorem 0.0.1. *The following sentences are equivalent in ZF:*

1. *Axiom of Choice*

2. *Every non-empty set admits a cancellative groupoid structure*

We start in the first chapter by briefly giving an overview of some of the necessary background knowledge needed for the rest of the text. This includes stating the ZF axioms as well as the Axiom of Choice itself.

Then, in the second chapter, we will explore orderings and well-orderings in the context of axiomatic set theory. Of special importance here will be Zorn's Lemma, a well-known equivalence of AC. We will finish this chapter by giving a proof for a lemma by Hartogs [Har15], which is also found in [HK72]. This lemma states that for any arbitrary set, there always exists an ordinal which no subset of that set can be injectively mapped to.

In the third chapter we will move on to an introduction to model theory. This is done with the aim of proving the upwards Löwenheim-Skolem Theorem, which states that a language with a countable model also has a uncountable model. Model theory is a very useful tool for applying results from logic to non-logic areas of mathematics, especially abstract algebra as we will see later. As Chang and Heisler put it in [CK90] (a very good historical introduction to model theory and the first comprehensive textbook for the subject),

Model Theory = Universal Algebra + Logic.

Finally, in the fourth and final chapter, we will give a detailed proof of the aforementioned theorem by Hajnal and Kertész, In this, we will apply the previous results by Hartogs and Löwenheim and Skolem from chapters two and three.

Chapter 1

Preliminaries

The convention in this thesis will be to say **ZF** when talking about Zermelo-Fraenkel set theory *without* the axiom of choice. When talking about the axiom of choice on its own we will say **AC**, and when talking about Zermelo-Fraenkel set theory together with the axiom of choice we use **ZFC**.

We will use the convention of including 0 at the beginning of the natural numbers $\mathbb{N}$, i.e. $\mathbb{N} = \{0, 1, 2 \ldots\}$. This is a *natural* choice, since we then can use $\mathbb{N}$ to mean the set described by the Axiom of Infinity. If we want to talk about strictly positive integers we use the notation $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$.

Lastly, whenever we deal with the negation of some symbol, we cross it out to mean this, for example $a \neq b$ means $\neg (a = b)$.

1.1 First-Order Logic and Classes

When talking about first order logic we mean the symbol

$$= \text{ (equals)}$$

in conjunction with the logical connectives

$$\neg \text{ (not)}, \ \wedge \text{ (and)}, \ \vee \text{ (or)}, \ \rightarrow \text{ (implies) and } \ \leftrightarrow \text{ (if and only if)}$$

as well as the quantifiers

$$\forall \text{ (for all) and } \exists \text{ (exists).}$$

Additionally, as we are talking about sets, we use the symbol $\in$ to denote set inclusion. [Jec78, pp.2-3]

In order to effectively talk about properties of set and set-like structures we need to somehow properly define formulas. We will go more into depth about formulas in Chapter 3, where we will introduce the notion of a formal language.

For now we are only concerned with the language of sets defined above.

Definition 1.1.1 (Formula of a Set)**.** An *atomic formula* in set theory is either

1. $x = y$, or
2. $x \in y$

A *formula* ϕ is an any combination of atomic formulas with logical connectives and quantifiers.

The symbols x and y above are called variables and for any two variables an atomic formula is either true or false for each x and y. A variable *occurs freely* inside of a formula if it does not appear inside of a $\exists$ or $\forall$ quantifier, otherwise the variable is *bound*. We write $\phi(x_1, \ldots, x_n)$ for a formula with $n \in \mathbb{Z}^+$ free variables. A formula where every variable is bound is called a *sentence*. [Mar02, pp.10-11]

A sentence is either true are false and a formula with free variables is true or false for each choice of the free variables. Each of the **ZF** axioms below are examples of sentences and as axioms we assume them to be inherently true (within the framework of our theory). An example of a formula with a free variable would be

$$\phi(x) = \exists y \ (y \in x).$$

This formula is only false for the empty set, since it is the unique set which does not contain any elements. In that sense we think of formulas with free variables describing a *property*, something we make use of in *classes*.

Definition 1.1.2 (Class)**.** Let $\phi(x, p_1, \ldots, p_n)$ be a formula in first order logic. Then a *class* $\mathbf{C}$ is defined as

$$\mathbf{C} = \{x \mid \phi(x, p_1, \ldots, p_n)\}.$$

The class $\mathbf{C}$ is called *definable from* $p_1, \ldots, p_n$. Furthermore, if x is the only free variable of ϕ, the class $\mathbf{C}$ is simply called *definable*. [Jec78, p.3]

In practice, we use classes as a tool to help us construct useful sets in **ZFC**, as elements of classes are always sets in the stricter sense. All sets are classes, but not all classes are sets, since if we have a fixed set s we can always construct the corresponding class would be $\mathbf{S} = \{x \mid x = s\}$. A class which is not a set is called a *proper class*.

We consider to two classes to be the same if they have the same elements. The familiar operations of *inclusion*, *union*, *intersection*, and *difference* are definable using formulas. As such for classes $\mathbf{C}$, $\mathbf{D}$,

$$\begin{aligned}
\mathbf{C} \subseteq \mathbf{D} &\iff \forall x \, (x \in \mathbf{C} \implies x \in \mathbf{D}) \\
\mathbf{C} \cup \mathbf{D} &= \{x \mid x \in \mathbf{C} \vee x \in \mathbf{D}\} \\
\mathbf{C} \cap \mathbf{D} &= \{x \mid x \in \mathbf{C} \wedge x \in \mathbf{D}\} \\
\mathbf{C} \setminus \mathbf{D} &= \{x \mid x \in \mathbf{C} \wedge x \notin \mathbf{D}\} \\
\bigcup \mathbf{C} &= \{x \mid x \in S \text{ for some } S \in \mathbf{C}\}
\end{aligned}$$

[Jec78, pp.3-4]

For the use in this text, classes are in a sense "naive sets-like object"; they to help us describe collections of sets without worrying about paradoxes. Consider for example the class $\mathbf{V} = \{x \mid x = x\}$, which is the universe of all sets and does not exist in pure set theory. Another important class which we will make use of later is the *empty class* $\varnothing = \{x \mid x \neq x\}$ (although this is also a set as we will see).

1.2 Zermelo-Fraenkel Axioms of Set Theory

We assume that the reader has some familiarity with axiomatic set theory, but for convenience and consistency we restate some of the necessary basics here. For a more thorough introduction of the topic, see [Gol98, §§4.3-4.5], alternatively [Jec78, §1.1] gives a more technical overview. The formulation of the axioms below is based on both textbooks.

1.2.1 Axiom of Extensionality

$$\forall x \, \forall y \, \big(x = y \iff \forall z \, (z \in x \iff z \in y)\big)$$

Two sets are equal if and only if they contain the same elements.[Gol98, §4.3, p.76]

1.2.2 Axiom of Pairs

$$\forall x \, \forall y \, \exists z \, \forall w \, \big(w \in z \iff (w = x \vee w = y)\big)$$

For any two sets, there is a set whose elements are precisely these sets.

We define an ordered pair $\langle x, y \rangle$ to be the set $\big\{\{x\}, \{x, y\}\big\}$. Further, ordered n-tuples are defined recursively as $\langle x_1, x_2, x_3, \ldots, x_n \rangle = \langle x_1, \langle x_2, x_3, \ldots, x_n \rangle\rangle$.[Gol98, §4.3, pp.76, 79-80]

Ordered pairs satisfy the property that for any sets x, y, u, v, if $\langle x, y \rangle = \langle u, v \rangle$, then $x = u$ and $y = v$.[Gol98, Theorem 4.2]

1.2.3 Axiom Schema of Separation

Let $\phi(z, p)$ be a formula in first order logic with free variables z and x. Then

$$\forall x \, \forall p \, \exists y \, \forall z \, \big(z \in y \iff (z \in x \wedge \phi(z, p))\big). \tag{1.2.1}$$

For any sets x and p there exists a unique set consisting of all elements z in x for which $\phi(z, p)$ holds. This is an axiom schema, meaning an infinite collection of axioms, since (1.2.1) is a separate axiom for every formula $\phi(z, p)$.

Assume $\psi(z, p_1, \ldots, p_n)$ is a more general formula for which we want to utilize the axiom schema for. We can then let $\phi(z, p)$ be the formula

$$\phi(z, p) = \exists p_1 \cdots \exists p_n \left(\left(p = \langle p_1, \ldots, p_n \rangle \right) \text{ and } \psi(z, p_1, \ldots, p_n) \right),$$

where we have that $\phi(z, \langle p_1, \ldots, p_n \rangle)$ is true if and only if $\psi(z, p_1, \ldots, p_n)$ is true. Hence we can generalize the axiom schema to

$$\forall x \, \forall p_1 \cdots \forall p_n \, \exists y \, \forall z \left(z \in y \iff \left(z \in x \wedge \psi(z, p_1, \ldots, p_n) \right) \right). \tag{1.2.2}$$

Let $\mathbf{C} = \{ z \mid \psi(z, p_1, \ldots, p_n) \}$ be the class containing all sets z which satisfy the formula ψ for any free variables $p_1, \ldots, p_n$. We can then utilize 1.2.2 and have that

$$\forall x \, \exists y \, \left(\mathbf{C} \cap x = y \right),$$

describes the same set. This means that any subclass of a set is also a set, and naturally a subclass of a set is called a subset.

As a consequence the set theoretic operations *difference* $(x \setminus y) \subseteq x$ and *intersection* $(x \cap y) \subseteq x$ are also defined for any two sets x and y, since all sets also are classes. Further the intersection

$$\bigcap \mathbf{C} = \{ z \mid z \in x \text{ for every } x \in \mathbf{C} \}$$

of a class $\mathbf{C}$ is a set, since it is a subset of all of its elements, which are strictly sets. [Jec78, pp.5-6]

1.2.4 The Empty Set

$$\exists x \forall y \; y \notin x$$

There is a set with no elements. We call this set $\varnothing = \{\}$. [Gol98]

This statement stands out, as it is not an axiom, the existence of the empty set also arises from the Axiom Schema of Seperation. We include it here for the sake of completeness.

Since we can define the empty class $\varnothing = \{ u \mid u \neq u \}$, the empty set is also a set. However this follows from $\varnothing$ being a subset of all sets and hence only under the assumption that at least one other set exists. The existence of that set, in turn, follows from the Axiom of Infinity.[Jec78, p.6]

1.2.5 Axiom of Unions

$$\forall x \exists y \forall z \left(z \in y \iff \exists w \left(z \in w \wedge w \in x \right) \right)$$

For any set x there is a set, denoted by $\bigcup x$, which is the union of all the elements of x. meaning it contains all elements of the members of x.

For any sets, we recursively define their union as

$$x \cup y = \bigcup \{x, y\}$$
$$x \cup y \cup z = (x \cup y) \cup z$$
$$\dots$$

as well as a set with more then two members as,

$$\{x_1, \dots, x_n\} = \{x_1\} \cup \dots \cup \{x_n\}$$

where the existence of $\{x, y\}$ and $\{x\} = \{x, x\}$ is justified by the Axiom of Pairs. [Jec78, p.6]

1.2.6 Axiom of Power Sets

$$\forall x \, \exists y \, \forall z \, (z \in y \iff z \subseteq x)$$

For any set x there is a set, denoted by $\mathcal{P}(x)$ and called the power set of x, consisting of all subsets $s \subseteq x$.

Using the axioms of Separation, Union and Power Set we can define the *cartesian product* of the sets X and X as

$$x \times y = \{(u, v) \mid u \in x \vee v \in y\} \subseteq \mathcal{P}(\mathcal{P}(x \cup y)),$$

and for multiple sets $x_1, \dots, x_n$ as

$$x^n = \underbrace{x_1 \times \dots x_{n-1} \times x_n}_{n \text{ times}} = (x_1 \times \dots \times x_{n-1}) \times x_n.$$

We call a set $R \subseteq X^n$ a *n-ary* relation over X. In general R is a set of tuples and if R is a binary relation, we write $x \, R \, y$ for $(x, y) \in R$.

A binary relation $f \subseteq X \times Y$ is called a *function* (or *map*), if

$$((x, y) \in f \wedge (x, z) \in f) \implies y = z$$

holds for all $x \in X$ and $y, z \in Y$, and if for all $u \in X$ there exists some $v \in Y$, such that $(u, v) \in f$.

In the definition above, we call X the *domain* and Y the *codomain* of f. The set

$$\mathbf{Im}(f) = \{y \mid \exists x \in X \ ((x, y) \in f)\}$$

is called the *image* of f. In general we write $f : X \to Y$ for $f \subseteq X \times Y$ and $f(x) = y$ whenever $(x, y) \in f$, in the latter case saying that x *maps to* y in f.

A function $f : X \to Y$ is called a *surjection* if $\mathbf{Im}(f) = Y$ and an *injection*, if

$$(f(x_1) = y \wedge f(x_2) = y) \implies x_1 = x_2.$$

A function is *bijection*, if it is both a surjection and an injection. [Jec78, pp.7-10]

1.2.7 Axiom of Infinity

$$\exists x \left(\varnothing \in x \wedge \forall y \left(y \in x \implies y \cup \{y\} \in x\right)\right)$$

There is an inductive set. An inductive set contains both the empty set $\varnothing$ as well as the successor x^+ of every x in the set. In this context the successor of a set x is defined as $x^+ = x \cup \{x\}$. We will go into more detail on this in Section 2.3.

1.2.8 Axiom Schema of Replacement

Let $\phi(x,\ y,\ p)$ a formula in first-order logic with free variables x, y and p.

$$\begin{aligned} &\forall x\, \forall y\, \forall z\ \left(\phi(x,\ y,\ p) \wedge \phi(x,\ z,\ p) \implies y = z\right) \\ &\implies \forall x'\, \exists y'\, \forall y\ \left(y \in y' \iff (\exists x \in x')\, \phi(x,\ y,\ p)\right) \end{aligned} \tag{1.2.3}$$

Similar to the Axiom Schema of Seperation, this is an axiom schema, meaning that (1.2.3) is a separate axiom for each formula $\phi(x,\ y,\ p)$. We can also generalize the Axiom of replacement in a similar way, by replacing $\phi(x,\ y,\ p)$ with $\phi(x,\ y,\ p_1, \ldots,\ p_n)$.

The axiom schema states that if $\mathbf{F} = \left\{(x\, y) \mid \phi(x,\ y,\ p)\right\}$ is a class function, then the image $\mathbf{Im}(\mathbf{F})$ is a set whenever we restrict the domain of $\mathbf{F}$ to a set. Consequently this restriction of $\mathbf{F}$ is also a function of sets. [Jec78, p.11]

1.2.9 Axiom of Foundation

$$\forall x \exists y \left(y \in x \wedge x \cap y = \varnothing\right)$$

Every set contains an $\in$-minimal element, we call this being *well-founded*.[Gol98, p.92] This also means there exist no infinitely descending chains of sets, such as $x_0 \ni x_1 \ni x_2 \ni \cdots$.[Gol98, Theorem 4.3, p.95]

1.3 The Axiom of Choice

To talk about the axiom of choice we need to first define what a choice function is, the concept which the axiom is centered around.

Definition 1.3.1 (Choice Function)**.** [Jec78, p.38] Let S be a family of nonempty sets. A function $f : S \to \bigcup S$ is called a *choice function* of S if

$$f(X) \in X$$

holds for all sets $X \in S$.

The Axiom of Choice is then defined as follows:

Definition 1.3.2 (Axiom of Choice)**.** [Jec78, p.38] There exists a choice function for every family of nonempty sets.

The Axiom of Choice is not always needed for showing that a choice function exist. Take for example $S = \mathcal{P}(\mathbb{N})$, under the usual order $<$ every subset of $\mathbb{N}$ has a least element. We can therefore construct a choice function $f : S \to \mathbb{N}$ by letting $f(N)$ be the unique least element of N for $N \in S$. This is however not possible for a family of possibly infinite subsets of $\mathbb{R}$; for example the open interval $(0,\ 1)$ does not contain a least element.

In general there does not always exist an external structure for sets which we can utilize to construct a choice function. The Axiom of Choice ensures that we can, but not how that choice function might look like. In fact **AC** is the only axiom of **ZFC** which states the existence of a mathematical object without explicitly defining it. This is a powerful tool, but can lead lead to fairly unintuitive results. As such, with **AC** there exists a way to order the real numbers where every subset has a least element (including open intervals like $(0,\ 1)$)!

Chapter 2

Orderings and Well-Orderings

2.1 Linear, Partial and Well-Orderings

We start by defining the two types of partial orderings, *strict* and *weak* ones. To give a more intuitive understanding of how these differ we use the notation $<$ and $\leq$ respectively, but R is also commonly used to denote a relation.

Definition 2.1.1 (Strict Partial Order)**.** [Gol98, p.165] Let X be a set and $< \subseteq X \times X$ a binary relation on X. Then $<$ is called a *(strict) partial order of* X, and $(X, <)$ called a *(strictly) partially ordered set*, if it is

(i) **irreflexive**: $\forall x \in X \, (x \not< x)$

(ii) **transitive**: $\forall x, y, z \in X \, \big((x < y \wedge y < z) \implies x < z\big)$

It is called *linear* if for all x, y in X, $x < y$ or $y < x$ or $x = y$.

Definition 2.1.2 (Weak Partial Order)**.** [Gol98, p.164] Let X be a set and $\leq \subseteq X \times X$ a binary relation on X. Then $\leq$ is called a *weak partial order* of X, and $(X, \leq)$ called a *weakly partially ordered set*, if it is

(i) **reflexive**: $\forall x \in X \, (x \leq x)$

(ii) **transitive**: $\forall x, y, z \in X \, \big((x \leq y \wedge y \leq z) \implies x \leq z\big)$

(iii) **anti-symmetric**: $\forall x, y \in X \, \big((x \leq y) \wedge (y \leq x) \implies x = y\big)$

It is called *linear* if for all x, y in X, $x \leq y$ or $y \leq x$.

Definition 2.1.3. [Jec78, p.13] If $(X, <_X)$ and $(Y, <_Y)$ are two partially ordered sets, we call a function $f : X \to Y$ *order-preserving* if

$$x_1 <_X x_2 \iff f(x_1) <_Y f(x_2).$$

If X and Y are both linearly ordered, an order-preserving function is also said to be *increasing*.

The function f is called an *order-isomorphism* if f is both order-preserving and a bijective. Whenever it is clear from context that we are talking about ordered sets we simply call f an *isomorphism* and write $X \simeq Y$. If f is order-preserving and injective, it is called an *order-embedding*. [Gol98, p.167]

A partially ordered set $(X, <)$ is sometimes also referred to simply as X by some abuse of notation when the relation $<$ is known. Additionally, whenever we talk about partially or linearly ordered sets without specifying which type, and where the type of partial order matters, we are referring to strict ones. [Jec78, p.12] Out of convenience, when talking about a strict partial order $<$, we sometimes refer to the term $(a < b \vee a = b)$ as $a \leq b$.

Clearly it is straightforward to define a weak partial order R' from a strict partial order R, letting $\langle x, y \rangle \in R'$ whenever $\langle x, y \rangle \in R$ or $x = y$.

Example 2.1.4. Let $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$ be the rational and real numbers with their respective usual order. Then, both $\mathbb{Q}$ and $\mathbb{R}$ are strictly partially and linearly ordered with respect to $<$. Additionally the function $f : \mathbb{Q} \to \mathbb{R}$ defined as $f(x) = x$ is an order-embedding, however due to the differences in cardinality the inverse f^{-1} is not a proper function.

Example 2.1.5. Consider the complex numbers $\mathbb{C}$ with $<_{\mathbb{R}}$ the usual order as defined on $\mathbb{R}$. Then $(\mathbb{C}, <_{\mathbb{R}})$ is a strict partial order, but not linear since $<_{\mathbb{R}}$ is only defined for strictly real numbers. Let us denote a complex number as an element of $\mathbb{R}^2$, so we express $z = a + bi$ as $\langle a, b \rangle$. We can then define a linear order on $\mathbb{R}^2$, by letting

$$\langle a_1, b_1 \rangle < \langle a_2, b_2 \rangle \text{ if } a_1 < a_2 \\ \text{or } a_1 = a_2 \wedge b_1 < b_2.$$

This is called the *lexicographical order* of $\mathbb{R}^2$ with respect to the order $<$ on $\mathbb{R}$ and is perhaps the most natural way to a cartesian product. [Gol98, p.182] The *anti-lexicographical order* order of $\mathbb{R}^2$ would be

$$\langle a_1, b_1 \rangle < \langle a_2, b_2 \rangle \text{ if } b_1 < b_2 \\ \text{or } b_1 = b_2 \wedge a_1 < a_2.$$

If we express a complex number as $z = re^{\varphi i}$, we can define a linear order a different way:

$$z_1 = r_1 e^{\varphi_1 i} < z_2 = r_2 e^{\varphi_2 i} \text{ if } r_1 < r_2 \\ \text{or } r_1 = r_2 \wedge (\varphi_1 < \varphi_2 \bmod 2\pi).$$

If we view the number $z = re^{\varphi i}$ as the ordered pair $\langle r, \varphi \rangle$, this is then the lexicographical ordering of $\mathbb{R} \times [0, 2\pi)$.

Definition 2.1.6. [Jec78, p.12] An element a of an ordered set $(X, <)$ is the *least element* of X with respect to $<$, if $\forall x \in X\ (a < x \vee x = a)$. Similarly, an element z is called the *greatest element* of X if $\forall x \in X\ (x < a \vee x = a)$.

This notion of a least element lets us define a special kind of linearly ordered set:

Definition 2.1.7 (Well-Order)**.** [Jec78, p.13] A strict linear order $<$ of a set X is called a *well-ordering* if every subset of X has a least element.

Example 2.1.8. The natural numbers $\mathbb{N}$ are a well-ordered set with respect to their usual order. The least element of $\mathbb{N}$ is 0.

Example 2.1.9. The integers $\mathbb{Z}$ are not well-ordered under their usual order. They have no least element, and while of course every finite subset has a least element, this does not hold for all subsets of $\mathbb{Z}$ (for example the set of even integers).

Well-ordered sets are central to the axiomatic set theory at hand. In fact, one of the most important results we will treat here, is that every set can we well-ordered (with the Axiom of Choice).

Further, we will introduce the concept of ordinals as a way effectively classify all well-ordered sets. The next two lemmata are needed for the proof of Theorem 2.3.5, an important result with regards to ordinals. For this we need to define the initial section of an ordered set first:

Definition 2.1.10. If X is a well-ordered set and $s \in X$, we call the set $\{x \in X \mid x < s\}$ an *initial segment* of X.

Lemma 2.1.11. *[Jec78, Lemma 2.1, p.13] If $(W, <)$ is a well-ordered set and $f : W \to W$ is an increasing function, then $f(x) \geq x$ for each $x \in W$.*

Proof. [Jec78, Lemma 2.1, p.13] In order to contrive a contradiction, we assume that $X = \{x \in W \mid f(x) < x\}$, the collection of elements of W not satisfying the lemma, is a non-empty set. We then let z be the least element of X and $w = f(z)$ its preimage in f. By the definition of X we this means that $f(w) < w$, contradicting the initial assumption that f is an increasing function. □

Lemma 2.1.12. *[Jec78, Lemma 2.2, p.13] No well-ordered set is isomorphic to an initial segment of itself.*

Proof. [Jec78, Lemma 2.2, p.13] Assume for a contradiction that f is an order-isomorphism from an ordered set $(X, <)$ to an initial segment $(S, <) = \{x \in X \mid x < s\}$, for some $s \in X$ of itself. The image of f is then $\mathbf{Im}(f) = \{x \in X \mid x < s\} = S$, but we know this is not possible by Lemma 2.1.11. □

Theorem 2.1.13. *[Jec78, Theorem 1] Let $(W_1, <_1)$ and $(W_1, <_2)$ be well-ordered sets. Then one of the following holds:*

1. *W_1 is isomorphic to W_2,*
2. *W_1 is isomorphic to an initial segment of W_2,*
3. *W_2 is isomorphic to an initial segment of W_1.*

Proof. [Jec78, Theorem 1] Let W_1 and W_2 be as in the statement of the theorem and let $W_i(u)$ be the initial segment $\{u \in W_i \mid u < v\}$ of W_i for $i \in \{1, 2\}$. We can then define the following set of ordered pairs:

$$f = \left\{\langle x, y\rangle \in W_1 \times W_2 \mid W_1(x) \simeq W_2(y)\right\}.$$

By Lemma 2.1.12 no element of either W_1 or W_2 can be a member of more than one ordered pair in f, since

$$\langle x, y_1\rangle, \langle x, y_1\rangle \in f \implies y_1 \simeq x \simeq y_2.$$

Hence f is a bijective function, however not necessarily one of which the domain and image are W_1 and W_2.

Let $h : W_1(u) \to W_2(v)$ be an isomorphism between two initial segments of W_1 and W_2. Then if we have $u' < u$ in W_1, it follows that $W_1(u') \simeq W_2(h(u'))$ and hence $\langle u', h(u')\rangle$ must be in f.

Based on these properties we can explore the following cases:

1. If $\mathbf{Dom}(f) = W_1$ is the domain of f and $\mathbf{Im}(f) = W_2$, we have that W_1 and W_2 must be isomorphic. Hence case 1 of the the theorem holds.

2. If $\mathbf{Im}(f) \neq W_2$, we have that $W_2 \setminus \mathbf{Im}(f)$ is non-empty and denote the least element of $W_2 \setminus \mathbf{Im}(f)$ by y_0. Then $\mathbf{Im}(f) = W_2(y_0)$, since for $y_1 < y_2$ in W_2, having $y_2 \in \mathbf{Im}(W_2)$ means that $y_1 \in \mathbf{Im}(W_2)$.

   Further $\mathbf{Dom}(f) = W_1$, because otherwise $\mathbf{Dom}(f) = W_1(w_0)$ for the least element x_0 of $W_1 \setminus \mathbf{Dom}(f)$. This in turn results in a contradiction as $W_1(x_0)$ is necessarily isomorphic to $W_2(y_0)$, meaning that $\langle x_0, y_0\rangle \in f$ and $x_0 \in \mathbf{Dom}(f)$.

   As such we have that $f : W_1 \to W_2(y_0)$ is an order-isomorphism and case 2 of the theorem holds.

3. If $\mathbf{Dom}(f) \neq W_1$, we have that $\mathbf{Dom}(f) = W_1(w_0)$ for the least element x_0 of the set $W_1 \setminus \mathbf{Dom}(f)$. Proceeding analogously to case before we have that $\mathbf{Im}(f) = W_2$. Hence W_2 is order-isomorphic to an initial segment of W_1 and case 3 of the theorem holds.

By case 2 it is clear that these are the only possibilities for $\mathbf{Dom}(f)$ and $\mathbf{Im}(f)$ and by Lemma 2.1.12 the cases must be mutually exclusive. □

2.2 Properties of Linear Orderings

There are some more important concepts to define when discussing linear orderings, namely how we describe their properties. The sets $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ are all countable, but their usual orderings clearly all differ. On the other hand, $\mathbb{Q}$ and $\mathbb{R}$ have different cardinalities, however the way both are ordered seems very similar.[1]

Definition 2.2.1. [Ros82, Definition 1.20] Let $(X, <)$ be a strictly linearly ordered set and $b \in X$ an element of X. Then an element $c \in X$ is called the (unique and immediate) *successor* of b, if

$$\forall x \in X \ (x < c \implies x < b \vee x = b) .$$

Similarly an element $a \in X$ is called the (unique and immediate) *predecessor* of b, if

$$\forall x \in X \ (a < x \implies x = b \vee b < x) .$$

Every element in $\mathbb{N}$ and $\mathbb{Z}$ has an immediate successor and every element in $\mathbb{Z}$ has an immediate predecessor. This is however not the case for elements of $\mathbb{Q}$, as the natural order of the rationals is *dense*.

Definition 2.2.2 (Dense orderings)**.** [Ros82, Definition 2.1] Let $(Y, <)$ be a strictly linearly ordered set. Then Y is called *dense*, if

$$\forall a_1, a_2 \in Y \ (a_1 < a_2 \implies \exists a \in Y \ (a_1 < a \wedge a < a_2)) .$$

We will not dwell on the concept of density to long. Especially the distinction between the two dense orderings of $\mathbb{Q}$ and $\mathbb{R}$ goes more into the direction of point-set topology and is beyond the scope of this text. For a treatment of this topic from the perspective of linear orderings we refer the curious reader to [Ros82, §2].

The broader discussion of the properties of linear orderings is important however, as we need a way to classify and compare ordered sets. For the classification we utilize order preserving functions; this is especially useful for the use-case of well-ordered sets all they always relate to each other in this way by Theorem (2.1.13).

Definition 2.2.3 (Order Type)**.** [Ros82, Definition 1.12, 1.13] Let $(X, <_X)$ and $(Y, <_Y)$ be linear orderings. We say that X and Y have the same *order type*, if there exists an order-isomorphism $f : X \to Y$.

Assume that α is some linear ordering that we choose as a representative. If X and α are order-isomorphic we also say that X has *order type* α.

[1] The sets $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are used without formally defining them or their orders here. It is assumed the reader is familiar.

Example 2.2.4. Consider the positive integers $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$. We can define the function $s : \mathbb{N} \to \mathbb{Z}^+$ by $s(n) = n + 1$ and have that s is an order-isomorphism:

$$n < m \iff n + 1 < m + 1.$$

Hence $\mathbb{Z}^+$ has the same order-type as $\mathbb{N}$.

Example 2.2.5. [Ros82, Exercise 2.3] We denote the order type of the rational numbers $\mathbb{Q}$ under the usual order by η. Then the punctured rationals $\mathbb{Q} \setminus \{0\}$ with the usual ordering also have order type η.

2.3 Ordinals

There are several ways to define the natural numbers $\mathbb{N}$, the way we do it here, and the way generally used in set theory, is to use the Axiom of Infinity, motivated by the Peano Axioms. This states that $\mathbb{N}$ is an *inductive set*, meaning that it contains 0, defined as $\varnothing = \{\}$, as well as the successor of every element in it, including of course 0 itself. [Gol98, p.39]

Definition 2.3.1. [Gol98, p.38] The successor of a set α is $\alpha^+ = \alpha \cup \{\alpha\}$. The successor of $0 = \varnothing$ is called 1 and the successor of 1 is called 2, etc.

The consequence of this is that $\mathbb{N}$ is the set we are familiar with: $\{0, 1, 2, 3, \ldots\}$. It also means that any natural number is defined as the set of all of its predecessors. For example $3 = \{0, 1, 2\} = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}$ and $5 = \{0, 1, 2, 3, 4\}$.

Perhaps slightly more subtle then is that, under the usual ordering, $n < m \implies n \in m \wedge n \subset m$. This is an important property and the natural numbers, as well as the set $\mathbb{N}$ at large, are called *transitive* sets. The notion of a *transitive set* is not to be confused with that of a *transitive (binary) relation*, which is an unfortunate overlap in terminology.

Definition 2.3.2. [Jec78, p.14] A set T is called *transitive* if

$$\forall x \, (x \in T \implies x \subseteq T).$$

Definition 2.3.3. [Jec78, p.14] A set is called an *ordinal number* or *ordinal* if it is transitive and well-ordered by $\in$. We say $\alpha < \beta$ if and only if $\alpha \in \beta$.

Ordinals are denoted by lowercase Greek letters: $\alpha, \beta, \gamma, \ldots$. The ordinal associated with $(\mathbb{N}, \in)$ specifically is denoted by ω. We know that ω is indeed an ordinal by construction. It follows from the following lemma that every natural number also is an ordinal with respect to set inclusion.

Lemma 2.3.4. *[Jec78, Lemma 2.3, p.15]*

1. *The empty set $\varnothing$ is an ordinal.*
2. *If α is an ordinal and $\beta \in \alpha$, then β is an ordinal.*
3. *If α, β are ordinals and $\alpha \subset \beta$, then $\alpha \in \beta$.*
4. *If α, β are ordinals, then either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.*

Proof. [Jec78, Lemma 2.3, p.15]

1. The empty set has no non-empty subsets, hence it is transitive and well-ordered by $\in$.
2. If $\beta \in \alpha$, then $\beta \subseteq \alpha$ by definition. Since α is well-ordered and transitive, so is β.
3. Let γ be the least element of the set $\beta \setminus \alpha$. We show that $\alpha = \gamma$.

   The ordinal α is transitive by definition and from this it follows that there are no "gaps" in the order. Indeed α must be an initial segment of β. As an initial segment, we can describe α as the set $\{\xi \in \beta \mid \xi < \gamma\}$. Again by the definition of ordinals, this is the set γ itself and $\alpha = \beta$.
4. We know that the intersection $\alpha \cap \beta = \gamma$ must be an ordinal, since not least the empty set also is an ordinal. However anything other than $\alpha = \gamma$ or $\beta = \gamma$ results in a contradiction:

   Assume for this contradiction that $\gamma \in \alpha$. Then $\gamma \in \beta$ by the second point of the lemma. Because γ is defined as the intersection of α and β, this means that $\gamma \in \gamma$. Since γ is an ordinal, strictly linearly ordered, this is not possible. □

Theorem 2.3.5. *[Jec78, Theorem 2, p.15] Every well-ordered set is order-isomorphic to a unique ordinal.*

Proof. [Jec78, Theorem 2] Let W be a well ordered set. We will show that W is order-isomorphic to an ordinal α, the uniqueness of α follows from Lemma 2.1.12.

Let $\mathbf{F}$ be the class function

$$\mathbf{F} = \{\langle x, \alpha\rangle \mid W(x) \simeq \alpha\},$$

which maps an element x to the ordinal α, only if the initial segment $\{u \in W \mid u < x\}$ given by x is order-isomorphic to α. Then, by the Axiom Schema of Replacement, the restriction $\mathbf{F}|_W$ is a function of sets, since $\mathbf{Dom}(\mathbf{F}|_W) \subseteq W$. As such $\mathbf{Im}(\mathbf{F}|_\mathbf{W})$ is also a set.

Additionally, we have that $\mathbf{F}(w)$ is defined for each $w \in W$: Consider for a contradiction the least element w_0 of W not isomorphic to an ordinal. Then $W(w_0) \simeq \beta$

for some ordinal β and consequently the least ordinal α_0 for which $\beta < \alpha_0$ holds must be isomorphic to w_0.

Finally we let γ be the least ordinal such that $\gamma \notin \mathbf{Im}(\mathbf{F}|_W)$ and have that γ is order-isomorphic to W as every $\alpha \in \gamma$ is isomorphic to an initial segment of W. □

This theorem makes it possible for us to associate the order type of a well-ordered sets with precisely the ordinal it is order-isomorphic to. In that sense we use the terms order type and ordinal interchangeably when talking about well-ordered sets.

The idea of ordinals was introduced using the natural numbers and while that is a useful comparison, we want to think about ordinals more as a generalization of $\mathbb{N}$, rather that a direct analog. As the name implies, ordinals describe magnitudes of *order* rather than *size*.

Consider for example the ordinal $\omega + 1 = \omega \cup \{\omega\}$, which describes the element coming after the "number" which is larger that every natural number. We can still define a bijective function from $\omega + 1$ to the natural numbers, so $\omega + 1$ is not larger in a *cardinal* sense, but rather relates to order. We will not deal with the proper notion of cardinality, the size of sets, in this text, however we will see in Theorem 2.5 that the distinction between cardinality and ordinals is not always clear cut.

In $\omega + 1$ and ω we can also recognize the two important types of ordinals, *successor ordinals* and *limit ordinals*.

Definition 2.3.6 (Successor Ordinal)**.** [Jec78, p.13] We call an ordinal α a *successor ordinal*, if it is the direct successor

$$\alpha = \beta^+ = \beta + 1$$

for some other ordinal β.

Definition 2.3.7 (Limit Ordinal)**.** [Jec78, Exercise 2.3] We call an ordinal α a *limit ordinal* if it is not a successor ordinal. Then $\alpha = \bigcup \alpha$ is the least upper bound of the set $\{\beta \mid \beta < \alpha\}$ and

$$\beta < \alpha \implies \beta + 1 < \alpha.$$

The latter follows since $\beta + 1 \not< \alpha$ would imply that both $\beta \in \alpha$ and $\beta \in \beta + 1$ hold. But since α is not a successor ordinal by definition we also have $\alpha \neq \beta + 1$. This means $\beta + 1 \in \alpha$ must be true by contradiction, because ordinals are well-ordered by set inclusion.

We also say consider 0 a limit ordinal and say that the least upper bound of 0 is itself.

We now introduce the final concept important for ordinals, that of *transfinite induction*. When we do a proof by (regular) induction, we show that some property holds for every natural number. Transfinite is the same concept extended to the ordinal numbers; loosely speaking we show not only that a property holds for a base case

and every successive number, but also that if it holds for all ordinals smaller than some limit ordinal, that it holds for the limit ordinal as well. This concept is generalized in the following theorem:

Theorem 2.3.8 (Transfinite Induction)**.** *[Jec78, Theroem 3] Let* $\mathbf{C}$ *be a class containing only ordinals and let the following hold for* $\mathbf{C}$*:*

(i) $0 \in \mathbf{C}$*,*

(ii) If $\alpha \in \mathbf{C}$ *is an ordinal, then* $\alpha + 1 \in \mathbf{C}$*,*

(iii) If α *is a non-zero ordinal and* $\beta \in \mathbf{C}$ *holds for all* $\beta < \alpha$*, then* $\alpha \in \mathbf{C}$*.*

Then $\mathbf{C}$ *is the class of all ordinals.*

Proof. [Jec78, Theroem 3] Let *Ord* be the class of all ordinals. Assume for a contradiction that the theorem does not hold and assume that α is the least ordinal contained in the class $Ord \setminus \mathbf{C}$.

If $\alpha = 0$ we immediately arrive at a contradiction, hence assume that α is some non-zero ordinal. If α is a successor ordinal we have that its direct predecessor must be a member of $\mathbf{C}$ and by the second criteria of the theorem we have that $\alpha \in \mathbf{C}$.

Similarly, if α is a limit ordinal we have that $\beta \in \mathbf{C}$ for all $\beta < \alpha$. Therefore, by the third criteria of the theorem, we must also have that $\alpha \in \mathbf{C}$, a contradiction. Hence $Ord = \mathbf{C}$. □

2.4 The Well-Ordering Theorem

The following, along with *Zorn's Lemma*, is one of the most fundamental results in set theory. There is a (bad) joke that goes:

> The *Axiom of Choice* is obviously true, the *Well-Ordering Theorem* obviously false, and who knows with *Zorn's Lemma*.

Definition 2.4.1 (Zermelo's Well-Ordering Theorem)**.** [Jec78, Theorem 15, p.39] Every set can be well ordered.

We could provide a proof for Definition 2.4.1 in **ZFC** here directly. This theorem, as it turn out, is not just another regular theorem, and we will therefore also not treat it as one.

Indeed, the Well-Ordering Theorem is actually equivalent to the Axiom of Choice. This means that if either statement is assumed to be true (and it has to be assumed since we are talking about *axioms*), the other one can be proved from it. This is the same methodology we will use for proving our main result, Theorem 4.0.1, as well.

There we will show equivalence of our main statement, that a group structure exists on all arbitrary sets, with the Well-Ordering Theorem. As such by transitivity, this main statement is also equivalent to the Axiom of Choice.

Theorem 2.4.2. *The Well-ordering Theorem is equivalent to the Axiom of Choice.*

Proof. [Jec78, Theorem 15, p.39] We provide a proof in two parts; first showing that the Well-Ordering Theorem is true in **ZFC**. Then, conversely, we prove **AC** in **ZF**, assuming that the Well-Ordering Theorem holds true.

1. **Axiom of Choice $\implies$ Well-Ordering Theorem**

   We proceed by transfinite induction.

   Let A be an arbitrary set and let $S = \mathcal{P}(A) \setminus \varnothing$ be the collection of all non-empty subsets of A. Let $f : S \to A$ be a choice function (as specified by the Axiom of Choice). We then define an ordinal sequence $(a_\alpha \mid \alpha < \theta)$ the following way:

   $$\begin{aligned} a_0 &= f(A) \\ a_\alpha &= f\left(A \setminus \left\{a_\xi \mid \xi < \alpha\right\}\right) \qquad \text{if } A \setminus \left\{a_\xi \mid \xi < \alpha\right\} \text{ is non-empty.} \end{aligned}$$

   Now let θ be the smallest ordinal such that $A = \left\{a_\xi \mid \xi < \theta\right\}$.

   We know that such an ordinal must exist, since the sequence $(a_\alpha \mid \alpha < \theta)$ is entirely defined by the choice function f. The function f maps every non-empty subset of A, i.e. members of S, to an element of that subset (in A).

   By defining the ordinal sequence the way we did, it is not possible for any element of A to occur in the sequence twice. Any subset of A, which is the input of the choice function for some element a_γ in the sequence, does not contain any elements a_α for $\alpha < \gamma$, and by definition f cannot map to any of these members.

   As such $\mathbf{Im}\left((a_\alpha \mid \alpha < \theta)\right) = A$ and $(a_\alpha \mid \alpha < \theta)$ enumerates A, meaning the sequence is a bijection.[2] Hence A can be well-ordered, the least element of any subset being the one which corresponds to the smallest ordinal in the sequence.

2. **Well-Ordering Theorem $\implies$ Axiom of Choice**

   Let S be a set of non-empty sets.

   The union $\bigcup S$ can be well-ordered by assumption and clearly $s \in S$ implies $s \subseteq \bigcup S$. We can then define the function $f : S \to \bigcup S$ to map any elements of S to its least element, according to the well-order of $\bigcup S$.

   Evidently f is a choice function and since the set S was arbitrary the Axiom of Choice holds. □

[2] Recall that a sequence is just a function from $\mathbb{N}$, respectively an ordinal, to the set of its elements

2.5 Hartogs' Lemma

We continue with the conclusion of this chapter, a lemma originally stated by Hartogs in a paper from 1915. Just as with Theorem (2.4.1), this is used in the proof of our final result, Theorem (4.0.1). Before we can state and prove this however, we need the following lemma:

Lemma 2.5.1. *[Har15, Annex] Let M be an arbitrary set. Then there exists a set M_0 consisting only of elements which are well-ordered set, whose elements are also elements of M.*

Lemma 2.5.2. *[Har15] Let A be an arbitrary set and let $S = \mathcal{P}(A)$ be the collection of subsets of A. Then there exists an ordinal α, such that no mapping $f_s : s \longrightarrow \alpha$ from any subset $s \in S$ of A to the ordinal α is a bijection.*

Proof. [HK72, Lemma] We let the ordinal α take the following value:

$$\alpha = \cup \left\{ \text{type}\,(X, R) + 1 \,|\, X \subseteq A, R \subseteq A \times A \wedge R \text{ well-orders } A \right\}.$$

We will show that α is such that it satisfies the lemma's statement.

□

Chapter 3

Model Theory

3.1 Models of Formal Languages

Definition 3.1.1. [Mar02, Definition 1.1.1] A *formal language* $\mathcal{L}$ in first order logic is given by the following:

1. A set $\mathcal{F}$ of functions f of n_f variables, with $n_f \in \mathbb{Z}^+$ a positive integer,
2. A set $\mathcal{R}$, of n_r-ary relations r, with $n_r \in \mathbb{Z}^+$ a positive integer,
3. A set $\mathcal{C}$ of constants.

3.2 The Löwenheim-Skolem Theorem

Lemma 3.2.1. *[CK90, Lemma 2.1.1] Let T be a consistent set of sentences of $\mathcal{L}$. Let C be a set of new constant symbols of power $|C| = \|\mathcal{L}\|$ and let $\bar{\mathcal{L}} = \mathcal{L} \cup C$ be the simple expansion of $\mathcal{L}$ formed by adding C.*

Then T can be expanded to a consistent set of sentences $\bar{T}$ in $\bar{\mathcal{L}}$, which has C as a set of witnesses in $\bar{\mathcal{L}}$.

Lemma 3.2.2. *[CK90, Lemma 2.1.2] Let T be a set of sentences and let C be a set of witnesses of T in $\mathcal{L}$. Then T has a model $\mathfrak{U}$, such that every element of $\mathfrak{U}$ is an interpretation of a constant $c \in C$.*

Theorem 3.2.3 (Extended Completeness Theorem)**.** *[CK90, Theorem 1.3.21] Let Σ be a set of sentences in $\mathcal{L}$. Then Σ is consistent if and only if Σ has a model.*

Theorem 3.2.4 (Downward Löwenheim-Skolem Theorem)**.** *[CK90, Corollary 2.1.4] Every consistent theory T in $\mathcal{L}$ has a model of power at most $\|\mathcal{L}\|$.*

Theorem 3.2.5 (Compactness Theorem)**.** *[CK90, Theorem 1.3.22] A set of sentences* Σ *has a model if and only if every finite subset of* Σ *has a model.*

Theorem 3.2.6 (Upward Löwenheim-Skolem Theorem)**.** *[CK90, Corollary 2.1.6] If* T *has infinite models, then it has infinite models of any given power* $\alpha \geq \|\mathcal{L}\|$.

Chapter 4

Hajnal's and Kertész's Theorem

Theorem 4.0.1. *[HK72] The following are equivalent in ZF:*

1. *Axiom of Choice*
2. *Every non-empty set admits a cancellative groupoid structure*

Bibliography

[CK90] Chen Chung Chang and H. Jerome Keisler. *Model Theory*. North-Holland Publishing Co., Amsterdam, 3. edition, 1990.

[Gol98] D.C. Goldrei. *Classic set theory*. CRC Press, Boca Raton, 1998.

[Har15] F. Hartogs. Über das Problem der Wohlordnung. *Math. Ann.*, 76(4):438–443, 1915.

[HK72] A. Hajnal and A. Kertész. Some new algebraic equivalents of the axiom of choice. *Publ. Math. Debrecen*, 19:339–340, 1972.

[Jec78] Thomas Jech. *Set Theory*. Pure and applied Mathematics. Academic Press, New York, 1978.

[Ker75] Andor Kertész. *Einführung in die transfinite Algebra*. Birkhäuser, Basel, cop. 1975.

[Mar02] David Marker. *Model theory*. Graduate texts in mathematics. Springer, New York, cop. 2002.

[Ros82] Joseph G. Rosenstein. *Linear Orderings*. Pure and applied Mathematics. Academic Press, New York, 1982.