0.1 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 0.1.1 (Strict Partial Order)**.** [1, 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**: $\forall x \in X\ (x \nless x)$

(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 0.1.2 (Weak Partial Order)**.** [1, 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 $(X, \leq)$ is 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 0.1.3. [2, 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 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* [1, 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 [2, 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 0.1.4. 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 0.1.5. 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

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

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 [1, p.182]. The *anti-lexicographical order* order of $\mathbb{R}^2$ would be

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

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

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

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 0.1.6. [2, 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 0.1.7 (Well-Order)**.** [2, 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 0.1.8. 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 0.1.9. 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 to properly classify all well-ordered sets. The next two lemmata are needed for the proof of Theorem 0.3.5, an important result with regards to ordinals. For this we need to define the initial section of an ordered set first:

Definition 0.1.10. 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 0.1.11. *[2, 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. 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 this means that $f(w) < w$, contradicting the initial assumption that f is an increasing function. □

Lemma 0.1.12. *[2, Lemma 2.2, p.13] No well-ordered set is isomorphic to an initial segment of itself.*

Proof. 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 0.1.11. □

Theorem 0.1.13. *[2, 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. 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:

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

By Lemma 0.1.12 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 the 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 0.1.12 the cases must be mutually exclusive. □

0.2 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]

[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.

Definition 0.2.1. [3, 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 0.2.2 (Dense orderings)**.** [3, 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 too 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 [3, §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 0.1.13.

Definition 0.2.3 (Order Type)**.** [3, Definitions 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.

Example 0.2.4. 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 0.2.5. [3, 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.

Oskar:

This is still left to do, I have focussed on writing Chapter 3 for now. There is a similar theorem in the Jech Set Theory book [2] though, which might be helpful.

0.3 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 [1, p.39].

Definition 0.3.1. [1, 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 0.3.2. [2, p.14] A set T is called *transitive* if

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

Definition 0.3.3. [2, 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 0.3.4. *[2, 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. We prove each statement of the lemma separately.

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 0.3.5. *[2, Theorem 2, p.15] Every well-ordered set is order-isomorphic to a unique ordinal.*

Proof. 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 0.1.12.

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 0.5.2 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 0.3.6 (Successor Ordinal)**.** [2, 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 0.3.7 (Limit Ordinal)**.** [2, 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 $\{\beta \,|\, \beta < \alpha\}$ 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 0.3.8 (Transfinite Induction)**.** *[2, Theorem 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. 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 $Ord = \mathbf{C}$. □

0.4 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 0.4.1 (Zermelo's Well-Ordering Theorem)**.** [2, Theorem 15, p.39]
Every set can be well ordered.

We do not provide a proof for Definition 0.4.1 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 **??**, 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 0.4.2. *[2, Theorem 15, p.39] The Well-Ordering Theorem is equivalent to the Axiom of Choice.*

Proof. 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 $S = \mathcal{P}(A) \setminus \emptyset$ 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. □

0.5 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 0.4.1, this is used in the proof of our final result, Theorem **??**. Since our goal is to prove an equivalence with the Axiom of Choice, we will work completely in **ZF** without **AC** in this section.

Lemma 0.5.1. *[4, Appendix] Let M be an arbitrary set. Then there exists a set M_Ω consisting of all well-ordered subsets of M.*

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

Proof. We follow the proof from [4] and adjust it to fit our own set-theoretic definition of orderings.

Recall that an ordering of M is defined as a subset $R \subseteq M \times M$. We first construct the set M_ω of all possible well-orderings of the set M itself. Note that since we cannot assume the Well-Ordering Theorem, the set M_ω might also be the empty set.

We can define formulas $\phi_1, \dots, \phi_4$ with free variables M and R, such that these hold true only for well-order relations R of a given set M (in the right context). Then

$$
\begin{aligned}
\phi_1(R, M) &= && \forall x \in M \ \langle x, x\rangle \notin R \\
\phi_2(R, M) &= && \forall x, y, z \in M \ \left(\left\langle x, y\right\rangle \in R \land \left\langle y, z\right\rangle \in R\right) \to \langle x, z\rangle \in R \\
\phi_3(R, M) &= && \forall x, y \in M \ \left(\left\langle x, y\right\rangle \in R \lor x = y \lor \left\langle y, x\right\rangle \in R\right) \\
\phi_4(R, M) &= && \forall S \in \mathcal{P}(M)\, \exists m \in S \ (\forall x \in S \ (\langle m, x\rangle \in R \lor m = x))
\end{aligned}
$$

are all valid formulas in **ZF**, with ϕ_1, ϕ_2, ϕ_3 utilizing only the Axiom of Pairs and ϕ_4 using the Axiom of Pairs and the Axiom of Power Sets.

Then, fixing the set M, we have that

$$M_\omega = \left\{R \in \mathcal{P}(M \times M) \mid \phi_1(R, M) \land \phi_2(R, M) \land \phi_3(R, M) \land \phi_4(R, M)\right\}$$

is the initially desired set of all well-orders of M and a valid construction following from the Axiom Schema of Replacement and Axiom of Power Sets.

We can also see that we are able to construct such a set X_ω for any arbitrary set X. Hence, finally, given a set M, the set of all possible well-orderings of any subsets m of M is given by the union

$$M_\Omega = \bigcup_{m \in \mathcal{P}(M)} m_\omega.$$

Note that M_Ω is non-empty, since we are always able to define a well-order for finite subsets of M[3]. □

With this lemma in mind, we now continue to the desired statement. We follow the outline given in [5] for the proof of this lemma, the more detailed steps are taken from [4].

Lemma 0.5.2. *[4][5, Lemma] Let A be an arbitrary set. Then there exists an ordinal α, such that no mapping from a subset $S \subseteq A$ to the ordinal α is a bijection.*

Proof. We let the ordinal α take the following value:

$$\alpha = \bigcup \left\{\text{type}\,(X, R) + 1 \mid X \subseteq A, R \subseteq A \times A \land R \text{ well-orders } A\right\}. \tag{0.5.3}$$

[3]Compare with the proof of Theorem 0.4.2, however we do not need **AC** for a choice function on finite sets.

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

We can see that the right hand side of the set is precisely the set described in Lemma 0.5.1. As such we can express the ordinal in (0.5.3) as

$$\alpha = \bigcup \left\{ \text{type}(R) + 1 \mid R \in A_\Omega \right\},$$

where type (R) is the order type of each well-order R[4] in the set A_Ω of all well-orderings of subsets of A.

Recall that we associate the order type of a well-ordered set with the unique ordinal it is isomorphic to, motivated by Theorem 0.3.5. Hence α describes the smallest ordinal which is larger (in an ordinal sense) than all well-orderable subsets of A. The latter property follows from the fact that such an ordinal is either an successor ordinal or a limit ordinal, the term "+1" and the union symbol in the definition of α make sure that both these cases are accounted for.

By construction we now have that every subset associated with an order R in A_Ω is isomorphic to an initial segment of α, but not to α itself. Further, there can not exist a bijective map from an arbitrary subset $S \subseteq A$ to α.

If such a map were to exist, we could define a well-ordering of S according to α; however we have already established that S either has no well-order or that there exists a bijection to an initial segment of α. This is a contradiction and we must have that no injective function from α to A exists, satisfying the requirements of the lemma. $\square$

Remark 0.5.4. We say that two sets X and Y have the same *cardinality* and write

$$|X| = |Y| \tag{0.5.5}$$

if there exists a bijective map between X and Y. Further we say that X has cardinality greater or equal to Y and write $|X| \geq |Y|$, if there exists a injective function from Y to X [2, p.22].

We call an ordinal κ a *cardinal* if $|\kappa| \neq |\alpha|$ for all $\alpha < \kappa$ [2, p.24]. The ordinal ω representing the natural numbers is the smallest infinite cardinal.

It seems tempting to use the definition of cardinality in the statement of Lemma 0.5.2, saying that "for all sets A there exists an ordinal α with cardinality greater than A". However, the relation (0.5.5) is only an equivalence relation over the universe of sets if we assume **AC**. As such the comparability of sets, meaning that for any sets $|X|$ and $|Y|$ we either have $|X| \leq |Y|$ or $|X| \geq |Y|$, does in general *not* hold in **ZF** [2, p.38]. We therefore refrained from talking about cardinals here, instead opting for a more general formulation.

[4] This is an abuse of notation, since we usually refer to the ordering R of a set X using (X, R). Here the underlying set was left out in order to more clearly convey what ordinal we are talking about.

However, if we only view the set structure of an ordering and how we defined ordered pairs, we have that $\bigcup \langle x, y \rangle = \bigcup \left\{ \{x\}, \{x, y\} \right\} = \{x, y\}$. In a linear ordering every element relates to every other element in some way, therefore we have that $\bigcup \bigcup R = X$.

For this reason it is justified to leave out the underlying set of the well-order R.