

## o.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 o.1.1** (Strict Partial Order). [?, 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:**  $\forall x, y, z \in X ((x < y \wedge y < z) \implies x < z)$

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

**Definition o.1.2** (Weak Partial Order). [?, 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:**  $\forall x, y, z \in X ((x \leq y \wedge y \leq z) \implies x \leq z)$
- (iii) **anti-symmetric:**  $\forall x, y \in X ((x \leq y) \wedge (y \leq x) \implies x = y)$

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

**Definition o.1.3.** [?, p.13] If  $(X, <_X)$  and  $(Y, <_Y)$  are two partially ordered sets, we call a function  $f : X \rightarrow Y$  *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*. [?, 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. [?, 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  $f : \mathbb{Q} \rightarrow \mathbb{R}$  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. [?, p.182] The *anti-lexicographical 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.** [?, 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).** [?, 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 o.i.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 o.i.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 be 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 o.3.5, an important result with regards to ordinals. For this we need to define the initial section of an ordered set first:

**Definition o.i.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 o.i.11.** [?, Lemma 2.1, p.13] If  $(W, <)$  is a well-ordered set and  $f : W \rightarrow W$  is an increasing function, then  $f(x) \geq x$  for each  $x \in W$ .

*Proof.* [?, 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.  $\square$

**Lemma o.i.12.** [?, Lemma 2.2, p.13] No well-ordered set is isomorphic to an initial segment of itself.

*Proof.* [?, 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  $\text{Im}(f) = \{x \in X \mid x < s\} = S$ , but we know this is not possible by Lemma o.i.11.  $\square$

**Theorem o.i.13.** [?, Theorem 1] Let  $(W_1, <_1)$  and  $(W_2, <_2)$  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.* [?, 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:

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

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

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

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

Let  $h : W_1(u) \rightarrow W_2(v)$  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  $W_1$  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 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  $\text{dom}(f) = W_1$ , because otherwise  $\text{dom}(f) = W_1(w_0)$  for the least element  $w_0$  of  $W_1 \setminus \text{dom}(f)$ . This in turn results in a contradiction as  $W_1(w_0)$  is necessarily isomorphic to  $W_2(y_0)$ , meaning that  $\langle w_0, y_0 \rangle \in f$  and  $w_0 \in \text{dom}(f)$ .

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

3. If  $\text{dom}(f) \neq W_1$ , we have that  $\text{dom}(f) = W_1(w_0)$  for the least element  $w_0$  of the set  $W_1 \setminus \text{dom}(f)$ . 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  $\text{dom}(f)$  and  $\mathbf{Im}(f)$  and by Lemma 0.1.12 the cases must be mutually exclusive.  $\square$

## 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.<sup>1</sup>

**Definition 0.2.1.** [?, 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). [?, 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 [?, §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). [?, 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  $f : X \rightarrow Y$ .

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

*Example 0.2.4.* Consider the positive integers  $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$ . We can define the function  $s : \mathbb{N} \rightarrow \mathbb{Z}^+$  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  $\mathbb{N}$ .

<sup>1</sup>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.

---

## 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. This states that  $\mathbb{N}$  is an *inductive set*, meaning that it contains 0, defined as  $\emptyset = \{\}$ , as well as the successor of every element in it, including of course 0 itself. [?, p.39]

**Definition 0.3.1.** [?, p.38] The successor of a set  $\alpha$  is  $\alpha^+ = \alpha \cup \{\alpha\}$ . The successor of  $0 = \emptyset$  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:  $\{0, 1, 2, 3, \dots\}$ . 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 than 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.** [?, p.14] A set  $T$  is called *transitive* if

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

**Definition 0.3.3.** [?, 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:  $\alpha, \beta, \gamma, \dots$ . The ordinal associated with  $(\mathbb{N}, \in)$  specifically is denoted by  $\omega$ . We know that  $\omega$  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.** [?, Lemma 2.3, p.15]

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

*Proof.* [?, 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  $\alpha$  is well-ordered and transitive, so is  $\beta$ .

3. Let  $\gamma$  be the least element of the set  $\beta \setminus \alpha$ . We show that  $\alpha = \gamma$ .

The ordinal  $\alpha$  is transitive by definition and from this it follows that there are no “gaps” in the order. Indeed  $\alpha$  must be an initial segment of  $\beta$ . As an initial segment, we can describe  $\alpha$  as the set  $\{\xi \in \beta \mid \xi < \gamma\}$ . Again by the definition of ordinals, this is the set  $\gamma$  itself and  $\alpha = \gamma$ .

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  $\gamma$  is defined as the intersection of  $\alpha$  and  $\beta$ , this means that  $\gamma \in \gamma$ . Since  $\gamma$  is an ordinal, strictly linearly ordered, this is not possible.  $\square$

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

## o.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). [?, Theorem 15, p.39]  
Every set can be well ordered.

We could provide a proof for Definition 0.4.1 in **ZFC** here directly. This theorem, as it turns 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.** *The Well-ordering Theorem is equivalent to the Axiom of Choice.*

---

*Proof.* [?, 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  $S = \mathcal{P}(A) \setminus \{\emptyset\}$  be the collection of all non-empty subsets of  $A$ . Let  $f : S \rightarrow A$  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:

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

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

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  $a_\gamma$  in the sequence, does not contain any elements  $a_\alpha$  for  $\alpha < \gamma$ , and by definition  $f$  cannot map to any of these members.

As such  $\text{Im}((a_\alpha \mid \alpha < \theta)) = A$  and  $(a_\alpha \mid \alpha < \theta)$  enumerates  $A$ , meaning the sequence is a bijection.<sup>2</sup> 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  $f : S \rightarrow \bigcup S$  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.  $\square$

## 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

---

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



final result, Theorem (??). Before we can state and prove this however, we need the following lemma:

**Lemma o.5.1.** *[?, 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 o.5.2.** *[?] Let  $A$  be an arbitrary set and let  $S = \mathcal{P}(A)$  be the collection of subsets of  $A$ . Then there exists an ordinal  $\alpha$ , such that no mapping  $f_s : s \rightarrow \alpha$  from any subset  $s \in S$  of  $A$  to the ordinal  $\alpha$  is a bijection.*

*Proof.* [?, Lemma] We let the ordinal  $\alpha$  take the following value:

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

We will show that  $\alpha$  is such that it satisfies the lemma's statement.

□