

# Cardinals for the working mathematician

Zigheem Abdelrahman

August 2024

I have a few maths friends, already well-versed in mathematics, that do not know much about set theory. In particular, they blackbox the very little amount of (non-foundational) set theory they should, and actually, care about in their daily life as mathematicians. This set theory may be described as "Theorems that depend on the axiom of choice but are not immediate corollaries of Zorn's lemma" and my experience is that in practice, those questions are questions related to cardinals.

This note is an answer to that situation. I try to keep everything as minimal and efficient as it is possible without obscuring the ideas. Some standard definitions about ordered sets are not recalled but may be found in any standard references. This text is heavily based on the exposition given in these [notes](#) by Kenneth Kunen.

## Contents

<b>1 Preliminaries</b>	<b>2</b>
<b>2 Ordinal numbers</b>	<b>2</b>
2.1 The structure of the class $\mathcal{O}$ . . . . .	2
2.2 Ordinals and well-ordered sets . . . . .	3
<b>3 Cardinals</b>	<b>4</b>
3.1 Using the axiom of choice . . . . .	4
3.2 Discussing the axiom of choice . . . . .	5

# 1 Preliminaries

We begin by recalling that

**Definition 1.0.1.** A set  $E$  is strictly ordered by a binary relation  $R \subset E \times E$  if it satisfies:

- Irreflexivity:  $\forall x \in E, \neg(xRx)$
- Transitivity:  $\forall x, y, z \in E, (xRy \wedge yRz) \implies (xRz)$

We say that  $E$  is strictly ordered by  $R$  and that  $(E, R)$  is a strictly ordered set.

Notice that it implies  $\forall x, y \in E, xRy \implies \neg(yRx)$ , which is a fact we will use quite a few times. We will interchangeably use ordered and strictly ordered sets. Indeed, we may pass from one to the other by either adding or removing the relations  $xRx$ . We also define:

**Definition 1.0.2.** A (strictly) ordered set  $(E, \leq)$  is (strictly) well-ordered if any nonempty subset  $A \subset E$  has a minimum.

Another fact we will implicitly use a few times is

**Proposition 1.0.1.** A well-ordered set  $(E, \leq)$  is totally ordered.

*Proof.* Let  $x, y \in E$ . The set  $\{x, y\}$  has a minimum, which must be comparable to both elements.

## 2 Ordinal numbers

Von Neumann ordinals are defined to be "concrete" representation of well-ordered sets. It will be a theorem that any well-ordered set is isomorphic to exactly one Von Neumann ordinal (where the morphisms are the strictly increasing maps).

**Definition 2.0.1.** A set  $\alpha$  is said to be transitive if it satisfies  $\forall \beta \in \alpha, \beta \subset \alpha$ . Moreover,  $\alpha$  is said to be a Von Neumann ordinal if it is strictly well-ordered by the relation  $\in$ . We denote by  $\mathcal{O}$  the class<sup>a</sup> of all ordinals.

---

<sup>a</sup>Collection of sets that may be too large to be a set. We will not delve into these subtleties as they do not matter to us. See also [Russell's paradox](#)

The definition may seem convoluted but it turns out this is actually an easy to work with class of representatives modulo isomorphism of well-ordered sets. The empty set  $\emptyset$  is an ordinal. We will show that  $S(\alpha) = \alpha \cup \{\alpha\}$  is an ordinal whenever  $\alpha$  is, and we may build the natural numbers using that: We set 0 to be  $\emptyset$  and  $n+1$  is  $S(n)$ . The set of all natural numbers is also an ordinal, the smallest (in a sense to be defined) infinite one. In the context of ordinal theory, we denote it by  $\omega$  instead of  $\mathbb{N}$ .

The roadmap is as follows:

- The class  $\mathcal{O}$  behaves like an ordinal, in the sense that it is well-ordered by  $\in$  and transitive.
- Any well-ordered set is order-isomorphic to exactly one ordinal.
- How does transfinite induction on ordinals work ?
- Any set can be well-ordered.
- The relation  $A \prec B$  iff there exists an injection  $A \hookrightarrow B$  is a total order.
- The equivalences  $AC \iff \text{Zorn} \iff \text{Zermelo}$  in ZF.

Actually, we won't discuss the third point in details, but all the core ideas will appear in the proof of the second statement. See Kunen's text for a more thorough development of that part of the theory. One must also know that there is two entirely distinct notions of ordinal arithmetic and cardinal arithmetic, that are completely incompatible, even though cardinals will turn out to be defined as a particular kind of ordinals. This notion of ordinal arithmetic can be safely ignored as it is of no use and completely absent in non set-theory related mathematics.

### 2.1 The structure of the class $\mathcal{O}$

**Lemma 2.1.1.** For any ordinals  $\alpha, \beta$

1. The set  $S(\alpha) = \alpha \cup \{\alpha\}$  is an ordinal, called the successor of  $\alpha$ .
2. The sets  $\alpha \cap \beta, \alpha \cup \beta$  are ordinals.
3. If  $z \in \alpha$ , then  $z$  is an ordinal.
4. We have the equivalence  $\alpha \subset \beta \iff (\alpha = \beta \vee \alpha \in \beta)$

*Proof.* We only prove 3. and 4.

Let  $\alpha$  be an ordinal and  $z \in \alpha$ . It is clear that  $z$  is still well-ordered by  $\in$ , and we only need to check it is transitive, that is  $x \in y \in z \implies x \in z$ . It is enough to show that  $x, y \in \alpha$ , because the statement  $x \leq y \leq z \implies x \leq z$  is definitionally part of being ordered by  $\in$ . As  $\alpha$  is transitive, we have  $y \in z \subset \alpha$ , that is  $y \in \alpha$ . It follows that  $y \subset \alpha$  and  $x \in \alpha$ . As  $\alpha$  is ordered by  $\in$  and  $x \in y \in z$ , we must have  $x \in z$ .

The reverse implication part of 4. is transitivity. Assuming  $\alpha \subset \beta$  and  $\alpha \neq \beta$  gives that  $X = \beta \setminus \alpha$  is nonempty, so let  $\gamma$  be its minimum. Showing  $\gamma = \alpha$  is enough as  $\gamma \in \beta$ . For any  $z \in \gamma$  we have  $z \in \beta$  as  $\beta$  is transitive and  $z \notin X$  as  $\gamma$  is a minimum, so  $\gamma \subset \alpha$ .

If  $\gamma \subsetneq \alpha$ , let once again  $\mu$  be the minimum of  $Y = \alpha \setminus \gamma$ , assuming  $Y$  is nonempty. As  $\mu \notin \gamma$ ,  $\gamma = \mu$  or  $\gamma \in \mu$ . The first is contradictory as  $\mu = \gamma \in X$  but  $\mu \in \alpha$ , while the second is because  $\gamma \in \mu \in \alpha$  gives  $\gamma \in \alpha$ . It must mean  $Y$  was empty and we are done.

**Theorem 2.1.2 (Structure theorem for  $\mathcal{O}$ ).** The class  $\mathcal{O}$  behaves like an ordinal, in the sense that it is well-ordered by  $\in$  and transitive.

*Proof.* Let  $\alpha, \beta$  be ordinals

- Irreflexivity:  $\alpha \in \alpha$  contradicts the [axiom of foundation](#)<sup>1</sup>
- Transitivity: If  $\alpha \in \beta, \beta \in \gamma$ , then by the 3th lemma  $\beta \subset \gamma$  and  $\alpha \in \gamma$ .
- Well-order: Let  $X$  be any nonempty *class* (in particular, set) of ordinals and set  $\alpha \in X$ . If  $\alpha$  is a minimum, we are done. Otherwise, the class  $\alpha \cap X = \{\beta \in \alpha \mid \beta \in X\}$  is a nonempty set (as it is a subset of  $\alpha$ ), and its minimum is a minimum of  $X$ .

The main takeaway is that any set of ordinals is well-ordered.

## 2.2 Ordinals and well-ordered sets

We now describe some of the categorical structure of  $\mathcal{O}$ . In less pedantic word, what are the increasing maps between ordinals? The answer turns out to be very simple for isomorphisms

**Proposition 2.2.1.** For any ordinals  $\alpha, \beta$ , let  $f : \alpha \rightarrow \beta$  be a strictly increasing bijection, i.e an isomorphism. We must have  $\alpha = \beta$  and  $f = \text{id}_\alpha$ .

*Proof.* For any  $\gamma \in \alpha$ , we have the equality  $f([\emptyset; \gamma]) = [\emptyset; f(\gamma)]$ . The transitivity of  $\alpha$  gives  $f([\emptyset; \gamma]) = \{f(x) \mid \mu \in \gamma \wedge \mu \in \alpha\} = \{f(\mu) \mid \mu \in \gamma\}$ . On the other hand, as  $\beta$  is transitive,  $[\emptyset; f(\gamma)] = f(\gamma)$ . To sum up, we have  $f(\gamma) = \{f(\mu) \mid \mu \in \gamma\}$ . Now assume  $f$  is not the identity and let  $\gamma$  be the least element not satisfying  $f(\gamma) = \gamma$ . We would have  $f(\gamma) = \{f(\mu) \mid \mu \in \gamma\} = \{\mu \mid \mu \in \gamma\} = \gamma$ , absurd.

**Theorem 2.2.2.** Any well-ordered set  $(E, \leq)$  is isomorphic to an ordinal.

<sup>1</sup>We may avoid it in the case of ordinals as it is actually part of the definition: as  $\in$  strictly order  $\alpha$ , it is irreflexive, and  $\alpha \in \alpha$  would imply  $\alpha \notin \alpha$ .

*Proof.* The idea is to do some kind of induction, i.e to show there is no smallest element that can satisfy the negation of the theorem.

Assume for the time being that for any  $y \in E$ , we have isomorphisms  $f_y : [0, y] \rightarrow \alpha_y$  where  $\alpha_y$  is an ordinal depending on  $y$ . We may actually check those maps must be compatible, in the sense that the images agree whenever they are simultaneously defined:

Indeed, if  $x, y \in E$  and say  $x \leq y$ , then  $\beta := f_y([0; x])$  is an ordinal isomorphic to  $[0; x]$  through  $f_{y,|[0;x]}$ . It follows that  $f_{y,|[0;x]} \circ f_x^{-1} : \alpha_x \rightarrow \beta$  is an isomorphism of ordinals, so we must have  $\alpha_x = \beta$  and the maps coincide on  $[0; x]$ .

Now, define a map

$$g : E \rightarrow \bigcup_{x \in E} \alpha_x, y \mapsto f_y(y)$$

we can check  $g$  is an isomorphism: we already showed that  $\alpha_x \in \alpha_y$  whenever  $x < y$ , which gives both injectivity and that  $g$  is strictly increasing. Moreover, we know that for any  $y \in E$ ,  $g([0, y]) = \{f_x(x) \mid x \leq y\} = \{f_y(x) \mid x \leq y\} = \alpha_y$  by the compatibility property, giving surjectivity.

Let  $y$  be the smallest element such that  $[0; y]$  is not isomorphic to some ordinal. By setting  $E = [0; y[$  in the above construction, we have a contradiction.

The proposition ensures uniqueness and the theorem existence, so we may define unambiguously

**Definition 2.2.1.** The order type of a well-ordered set  $(E, \leq)$  is the unique ordinal it is isomorphic to it. We denote it by  $\text{type}(E, \leq)$  or  $\text{type}(E)$  when there's no ambiguity.

## 3 Cardinals

### 3.1 Using the axiom of choice

Our next goal is now to enable all of the usages of the theory of well-ordered sets for regular sets. This is the following result:

**Theorem 3.1.1 (Zermelo, ZFC).** Any set can be well-ordered

We won't discuss the proof in this section and only explore its consequences. First, we have

**Corollary 3.1.2.** For any two sets  $E, F$ , there is either an injection from  $E$  to  $F$  or an injection from  $F$  to  $E$ .

*Proof.* Indeed, let  $\leq_E, \leq_F$  be well-orders on  $E$  and  $F$  respectively. We must have either  $\text{type}(E, \leq_E) \subset \text{type}(F, \leq_F)$  or  $\text{type}(F, \leq_F) \subset \text{type}(E, \leq_E)$  as ordinals are totally ordered by inclusion. Assume the first wlog, then have a composition of maps

$$(E, \leq_E) \simeq \text{type}(E, \leq_E) \subset \text{type}(F, \leq_F) \simeq (F, \leq_F)$$

where  $\simeq$  denote the canonical bijections.

Motivated by this, we define for any two sets  $A, B$  the relation  $A \prec B$  to mean that there exists an injection  $A \hookrightarrow B$ . It is natural to ask if  $\prec$  is an ordering on the class **Set** of all sets? If it were, the corollary would give us that it is even a total order. Obviously  $A \prec A$  and if we have both  $A \prec B$  and  $B \prec C$  then we have  $A \prec C$  through composition. But  $A \prec B \wedge B \prec A$  does not imply  $A = B$ : take for instance  $A = \{\emptyset\}, B = \{A\}$ . Luckily, the next best thing is true

**Theorem 3.1.3 (Cantor-Bernstein, ZF).** Let  $A, B$  be sets and  $f : A \hookrightarrow B, g : B \hookrightarrow A$  be injections. Then  $A$  and  $B$  are in bijection.

One must know<sup>2</sup> that this theorem holds without assuming the axiom of choice, but the proofs without are tedious and not particularly enlightening. I therefore chose to prove it using the theory we already developed (well, we have yet to prove Zermelo theorem...). We still need to do a little work:

---

<sup>2</sup>Nerds are everywhere...

**Definition 3.1.1.** An ordinal is a cardinal if it does not inject in any strictly smaller ordinal.

A cardinal is the smallest ordinal representative of its class, modulo the equivalence relation on **Set** given by  $A \sim B \iff A$  and  $B$  are in bijection. Standard examples are given by finite ordinals or  $\omega$ , as its elements are exactly finite ordinals. A simple non-example is  $S(\omega)$ . It is an easy exercise to check  $S(\omega) \sim \omega$ . A more complex example is the cardinality of  $\mathbb{R}$ . It may be shown, using Cantor-Bernstein for instance, that  $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$ , i.e that their cardinals are equal. For a long-time, mathematicians wondered whether there was a cardinal between  $\omega$  and  $|\mathbb{R}|$ , and the question was called the Continuum Hypothesis (CH). It is now known that there is no satisfying answer to that question<sup>3</sup>. Our needs are simpler, we only want

**Theorem 3.1.4 (ZFC).** Any set  $E$  is in bijection with exactly one cardinal, called the cardinal of  $E$  and denoted  $|E|$

*Proof.* By Zermelo the set<sup>4</sup> of ordinals in bijection with  $E$  is non-empty, so let  $\kappa$  be its minimum. Then minimality ensures that any  $\mu \in \kappa$  is not in bijection with  $E$ , and thus not in bijection with  $\kappa$ , that is  $\kappa$  is a cardinal. Uniqueness is obvious.

We may now prove the Cantor-Bernstein theorem:

*Proof.* For any well-ordering  $(A, \leq_A)$ , we have an injection  $|A| \sim A \hookrightarrow B \sim |B|$ . In particular,  $|A|$  injects in  $|B|$  and thus  $|A| \subset |B|$ . Symmetrically we get  $|B| \subset |A|$ , and since cardinals are ordered by inclusion (as ordinals are), we get  $|A| = |B|$ , which is equivalent to  $A \sim B$ .

## 3.2 Discussing the axiom of choice

This is a good spot to stop reading. We defined cardinals and discussed elementary facts about them. But we still ignored the proof of Zermelo's theorem. To discuss it, we must discuss the axiom of choice. It has a lot of equivalent forms and the purpose of this subsection is to describe its most common forms and the equivalences.

**Axiom 3.2.1 (Axiom<sup>a</sup> of choice).** For any set  $X$ , we can find a map  $f : \mathcal{P}(X) \setminus \{\emptyset\} \rightarrow X$  such that for any  $Y \subset X$  we have  $f(Y) \in Y$

<sup>a</sup>See [here](#) for a short explanation on why it is an axiom and not a theorem

The map  $f$  is a way to *choose* an element in each of the subsets  $Y \subset X$ . We now state Zorn lemma. Recall that

**Definition 3.2.1.** Let  $(E, \leq)$  be an ordered set:

- A subset  $A \subset E$  is called a chain if it is totally ordered.
- An upper bound of a subset  $A$  is an element  $x \in E$  such that  $a \leq x$  for any  $a \in A$ .
- An element  $m \in E$  is said to be maximal<sup>a</sup> if for any  $x \in E$  such that  $m \leq x$ , we have  $x = m$ .

<sup>a</sup>Which is not the same thing as being a maximum !

**Theorem 3.2.1 (Zorn's lemma).** Let  $(E, \leq)$  be an ordered set such that any chain has an upper bound. Then  $E$  has a maximal element.

We will prove that AC, Zorn and Zermelo are equivalent. Some implications are easy, some are notably harder. Let us start with the easiest ones

Zermelo  $\implies$  AC: Let  $X$  be a set. Pick a well-order  $\leq_X$ , and define  $f : Y \mapsto \min Y$ , which is a well-defined choice function.

Zorn  $\implies$  Zermelo: Let  $X$  be a set and let  $M$  be the set of all tuples  $(Y, \leq)$  where  $Y \subset X$  and  $\leq$  is a well-ordering of  $Y$ . We define an order relation on  $M$  as  $(Y, \leq_Y) \prec (Z, \leq_Z) \iff Y \subset Z \wedge \leq_Y$  extends  $\leq_Z$ . If  $C$  is a chain of  $(M, \prec)$ , then an upper-bound is given by the union (in the appropriate and obvious sense) of the elements in  $C$ . Zorn lemma applies, and let  $(Y, \leq_Y)$  be a maximal element of  $M$ . We must have  $Y = X$ , as otherwise by picking  $z \in X \setminus Y$  and extending  $\leq_Y$

<sup>3</sup>More precisely, CH is independent from ZF(C). Concretely it means that ZF(C) is unable to prove CH nor its negation.

<sup>4</sup>Actually, it is not entirely obvious it is a set. But even if it was a proper class, it would not matter for our use.

so that  $y \leq_Y z$  for any  $y \in Y$  contradicts maximality, and  $\leq_Y$  is a well-ordering of  $X$ .

$AC \implies Zorn$ : This is by far the hardest implication. We will need the ordinal theory we already built and a little more. Let  $(X, \leq)$  be an ordered set satisfying the assumptions of Zorn lemma, and let  $f : \mathcal{P}(X) \setminus \{\emptyset\} \rightarrow X$  be a choice map. We argue by contradiction and assume  $X$  has no maximal element. In particular, any chain  $C \subset X$  has a strict upper-bound. For any chain, let  $M(C)$  denote the set of all strict upper bounds of  $C$ .

We begin by assuming we have some ordinal  $\gamma$  that can't be injected in  $X$ <sup>5</sup>. Let  $g : \gamma \rightarrow X$  be the uniquely defined map<sup>6</sup> such that  $g(\alpha) = f(M(\{g(\beta) \in \alpha\}))$ . As  $M(C)$  is never empty, this map is well-defined and is strictly increasing. In particular, it is an injection, which contradicts the hypothesis as desired.

Now, we need to show  $\gamma$  exists without assuming Zermelo. Actually, this part does not depend on the axiom of choice at all. There are two roads:

- Either we let  $\gamma$  be the whole class  $\mathcal{O}$ . We just defined an injective map from  $\mathcal{O}$  to  $X$ . But  $\mathcal{O}$  cannot be a set, as otherwise by the structure theorem it would be itself an ordinal, and  $\mathcal{O} \in \mathcal{O}$  is absurd for one of the two reasons already discussed. An injective map from a proper class to a set contradicts the [replacement scheme](#). This is the standard proof.
- The other option is to pick  $\gamma$  as given by Hartog's theorem below. That is, if the idea of working with something that may not be a set to do set theory bothers you.

**Theorem 3.2.2 (Hartog, ZF).** *For any set  $X$ , there is a cardinal  $\kappa$  that does not inject in  $X$ .*

*Proof.* TODO. See Kunen's notes on p.53 for the time being.

<sup>5</sup>Assuming Zermelo's theorem, the smallest cardinal that's strictly greater than  $|X|$  works, as for any cardinal, there is always a larger cardinal, see for instance [Cantor's theorem](#)

<sup>6</sup>This is the good old definition by induction. But, I'll admit it, I am sweeping the dust under the carpet here. It is not as obvious as I make it seem like that  $g$  actually exists. The details are kinda annoying and obscure the idea, so just trust me bro. Or read Kunen's text, the details are page 45.