Ordinals and Cardinals

Exavery Philemon ENOCK (exavery@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by: Dr Gareth Boxall
Stellenbosch University, South Africa
Co-supervised by: Georg Anegg
AIMS, South Africa

18 May 2017

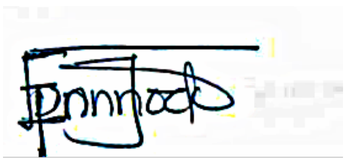
Submitted in partial fulfillment of a structured masters degree at AIMS South Africa

Abstract

In this project, we introduce the notions of ordinals and cardinals rigorously. We define ordinals as a special class of well-orderings and use them to define cardinals. Properties of ordinals and cardinals are stated and proved. We use cardinals to study the size of infinite sets. Finally, we discuss Goodstein sequences as an application in finite arithmetic. These sequences seem to increase spectacularly in the beginning, however, we will show that they terminate to zero in a finite number of steps.

Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.



Exavery Philemon ENOCK, 18 May 2017

Contents

1. Introduction

In normal language, ordinal numbers (commonly ordinals) are words indicating the position of things in a certain arrangement e.g. first, second, third, fourth, fifth and so on. Whereas cardinal numbers (commonly cardinals) are words indicating the size of a given collection of things e.g. one, two, three, four, five and so on.

"A natural number (which, in this context, includes the number 0) can be used for two purposes: to describe the size of a set, or to describe the position of an element in a sequence. When restricted to finite sets these two concepts coincide, there is only one way to put a finite set into a linear sequence, up to isomorphism. When dealing with infinite sets one has to distinguish between the notion of size, which leads to cardinal numbers, and the notion of position, which is generalized by the ordinal numbers" (Wikipedia, b).

"Whereas the notion of cardinal number is associated with a set with no particular structure on it, the ordinals are intimately linked with the special kind of sets that are called well-ordered (so intimately linked, in fact, that some mathematicians make no distinction between the two concepts)" (Wikipedia, b).

Below are ideas of set theorists about ordinal numbers and cardinal numbers.

John Von Neumann ideas of ordinal numbers.

The Hungarian-American mathematician John Von Neumann thought of the natural numbers and he suggested we could formalize them by setting $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, $\ldots$, $n = \{0, 1, 2, \ldots, (n-1)\}$. Due to above formalization of the natural numbers, then he formally defined ordinal number as follows: Any set S is said to be an ordinal if and only if it is strictly well-ordered by set membership and every element of S is a subset of S. And so he concluded that the natural numbers are also ordinals.

Georg Cantor ideas of cardinal numbers.

We have seen above that we can use natural numbers to describe the size of a finite set, which is its cardinality. The idea of cardinality was formulated by German mathematician Georg Ferdinand Ludwig Philipp Cantor, the originator of set theory, in 1874-1884. He compared the cardinalities of two sets by considering the existence of a one-to-one correspondence (bijection) between the two sets.

"Cantor applied his concept of bijection to infinite sets; e.g. the set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, ...\}$. Thus, all sets having a bijection with $\mathbb{N}$ he called denumerable (countably infinite) sets and they all have the same cardinal number. This cardinal number is called $\aleph_0$, aleph-null. He called the cardinal numbers of infinite sets transfinite cardinal numbers" (Wikipedia, c).

This project is focusing on discussing the ordinals and cardinals. We will pay attention to their properties by stating and proving them, do some arithmetic operations on each and look at applications. We start our discussion with ordinals, then we will move on to cardinals and conclude our project by considering the applications.

2. Ordinals

Before we introduce what ordinals are, first we consider the intuition of what they look like. Think of the natural numbers we know. Then we can construct some special sets which correspond nicely to the natural numbers as follows:

$$\begin{aligned}
0 &\leftrightarrow \emptyset \\
1 &\leftrightarrow \{\emptyset\} \\
2 &\leftrightarrow \{\emptyset, \{\emptyset\}\} \\
3 &\leftrightarrow \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 &\leftrightarrow \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
&\vdots
\end{aligned}$$

As you can see at each stage we form the set of all the previous sets in the sequence. We can extend this construction up to ω which we imagine to be the first number greater than all natural numbers. And so we will have:

$$0, 1, 2, \ldots, \omega.$$

But we can extend the construction by finding a successor of ω, that is $\omega^+ = \omega \cup \{\omega\}$. Then we can construct another sequence of numbers greater than ω which are of the form $\omega + n$ for $n \in \mathbb{N}$ and $n > 0$. We will have $\omega + \omega$ as the first ordinal greater than all ordinals of the form $\omega + n$. And so our construction now looks like:

$$0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega + \omega.$$

But $\omega + \omega = \omega.2$. Now we can extend the construction by constructing another sequence of numbers greater than $\omega \cdot 2$ which are of the form $\omega \cdot k + n$ for $n, k \in \mathbb{N}$ where $k > 1$ and $n > 0$. We will have $\omega \cdot \omega$ as the first ordinal greater than all ordinals of the form $\omega \cdot k + n$. And so our construction now looks like:

$$0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \omega \cdot 2 + 2, \ldots, \omega \cdot 3, \omega \cdot 3 + 1, \omega \cdot 3 + 2, \ldots, \omega \cdot \omega.$$

But $\omega \cdot \omega = \omega^2$. Now we can extend the construction by constructing another sequence of numbers greater than ω^2 which are of the form $\omega^k + n$ for $n, k \in \mathbb{N}$ where $k > 1$ and $n > 0$. We will have ω^ω as the first ordinal greater than all ordinals of the form $\omega^k + n$. And so our construction now looks like:

$$0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \omega \cdot 2 + 2, \ldots, \omega \cdot 3, \omega \cdot 3 + 1, \omega \cdot 3 + 2, \ldots, \omega^2, \omega^2 + 1, \omega^2 + 2, \\ \ldots, \omega^3, \omega^3 + 1, \omega^3 + 2, \ldots, \omega^\omega.$$

We can continue by taking another sequence of the form $\omega^\omega + n$ for $n \in \mathbb{N}$ and $n > 0$. By following the same procedures we obtain the following sequence

$$0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \omega \cdot 2 + 2, \ldots, \omega \cdot 3, \omega \cdot 3 + 1, \omega \cdot 3 + 2, \ldots, \omega^2, \omega^2 + 1, \omega^2 + 2, \\ \ldots, \omega^3, \omega^3 + 1, \omega^3 + 2, \ldots, \omega^\omega, \omega^\omega + 1, \omega^\omega + 2, \ldots, \omega^{\omega \cdot 2}, \omega^{\omega \cdot 2} + 1, \omega^{\omega \cdot 2} + 2, \ldots, \omega^{\omega \cdot 3}, \omega^{\omega \cdot 3} + 1, \omega^{\omega \cdot 3} + 2, \\ \ldots, \omega^{\omega^2}, \omega^{\omega^2} + 1, \omega^{\omega^2} + 2, \ldots, \omega^{\omega^3}, \omega^{\omega^3} + 1, \omega^{\omega^3} + 2, \ldots, \omega^{\omega^\omega}, \omega^{\omega^\omega} + 1, \omega^{\omega^\omega} + 2, \ldots, \omega^{\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}} = \epsilon_0.$$

We can continue with this construction indefinitely as follows:

$$\ldots, \epsilon_0, \epsilon_0 + 1, \ldots, \epsilon_0 + \omega, \epsilon_0 + \omega + 1, \ldots, \epsilon_0.2, \epsilon_0.2 + 1, \ldots, \epsilon_0.3, \epsilon_0.3 + 1, \ldots, \epsilon_0.\omega, \epsilon_0.\omega + 1, \ldots,$$

$$\epsilon_0^2, \epsilon_0^2 + 1, \ldots, \epsilon_0^3, \ldots, \epsilon_0^{\omega}, \ldots, \epsilon_0^{\omega^2}, \ldots, \epsilon_0^{\omega^3}, \ldots, \epsilon_0^{\omega^{\omega}}, \ldots, \epsilon_0^{\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}} = \epsilon_0^{\epsilon_0}, \ldots, \epsilon_0^{\epsilon_0^{\epsilon_0}}, \ldots, \epsilon_0^{\epsilon_0^{\epsilon_0^{\epsilon_0^{\cdot^{\cdot^{\cdot}}}}}} = \epsilon_1, \ldots$$

and so on.

After being familiar with the intuition of ordinals now we can move on to discuss about their properties and define them properly. Now we are going to state and prove some properties of ordinals.

2.1 Concepts, definitions and properties of ordinals

In this section we will build up useful concepts and then we will move on to state and prove some theorems about the properties of ordinals.

2.1.1 Definition (Totally ordered set)**.** (I. B. Leader) Let S be a set. Let $<$ be a binary relation on S. We say (S,$<$) is a totally ordered set if the following conditions are satisfied.

1. Irreflexive: $\forall a \in S$, $a \not< a$
2. Trichotomous: $\forall a, b \in S$, exactly one of the following is true: $a = b$, $a < b$ or $b < a$.
3. Transitive: $\forall a, b, c \in S$, if $a < b$ and $b < c$ then $a < c$

2.1.2 Definition (Well-ordered set)**.** (Boxall, 2017) Let $(S, <)$ be a totally ordered set. We say that $(S, <)$ is well-ordered if every non-empty subset of S has a least element with respect to $<$.

For example $\mathbb{N}$ is well-ordered but $\mathbb{Z}$ is not.

2.1.3 Remark. Where appropriate, $\in$ actually means the restriction of $\in$ to a certain set. And sometimes the symbol $<$ has the same meaning as $\in$, from now onwards whenever there is no confusion we will be using them interchangeably.

2.1.4 Definition (Transitive)**.** (Murphy, James) A set z is transitive if whenever x and y are sets such that $x \in y$ and $y \in z$, we have $x \in z$.

2.1.5 Definition (Ordinal)**.** (Gabriel Lehéricy) A set α is called an ordinal if

1. α is transitive.
2. $(\alpha, \in)$ is a well-ordered set.

2.1.6 Example. $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$ are ordinals.

2.1.7 Theorem. *(Murphy, James) If α is an ordinal and $\beta \in \alpha$ then β is an ordinal.*

Proof. To prove that β is an ordinal we need to show that β is transitive and well-ordered.

First we show that β is transitive.

Let a and b be sets with $a \in b$ and $b \in \beta$. Then to prove that β is transitive we need to show that $a \in \beta$. We have $b \in \beta$ and $\beta \in \alpha$. Since α is transitive it implies that $b \in \alpha$. We have $a \in b$ and $b \in \alpha$. It implies that $a \in \alpha$ by transitivity of α. Now we have $a, b, \beta \in \alpha$, $a \in b$ and $b \in \beta$. Since α is totally ordered then we have $a \in \beta$. Hence β is transitive.

Now we show that $(\beta, \in)$ is well-ordered.

Since $\beta \in \alpha$ and α is transitive, it implies that $\beta \subseteq \alpha$. But $\in$ is a well-ordering on α, it follows that $\in$ is a well-ordering on β. Hence $(\beta, \in)$ is well-ordered. □

2.1.8 Theorem. *(Don Monk, c) If α and β are ordinals and $\alpha \neq \beta$ such that $\beta \subseteq \alpha$ then $\beta \in \alpha$*

Proof. Since $\alpha \neq \beta$ and $\beta \subseteq \alpha$, it implies that $\alpha \setminus \beta$ is a non-empty subset of α. Let y be the least element of $\alpha \setminus \beta$ and suppose $x \in \beta$. Since $\in$ is a well-ordering on α, either $y \in x$ or $x \in y$. If $y \in x$ we have $y \in x$ and $x \in \beta$. This implies that $y \in \beta$ since β is transitive. This is a contradiction since $y \in \alpha \setminus \beta$. So $x \in y$. Therefore $\beta \subseteq y$. For all $\gamma \in y$, $\gamma \notin \alpha \setminus \beta$ since y is the least element of $\alpha \setminus \beta$. Hence $\gamma \in \beta$ and so $y \subseteq \beta$. Now we have $y \subseteq \beta$ and $\beta \subseteq y$ implies that $y = \beta$. Since $y \in \alpha$ and $y = \beta$ $\implies \beta \in \alpha$. □

2.1.9 Lemma. (Murphy, James) If α is an ordinal then $\alpha \notin \alpha$.

Proof. Suppose that α is an ordinal and $\alpha \in \alpha$. Since $\alpha \in \alpha$, $\in$ is not irreflexive on α and so $\in$ is not a well-ordering on α. This is a contradiction since α is an ordinal. □

2.1.10 Theorem. *(Murphy, James) Suppose that α and β are ordinals. Then exactly one of the following is true: $\alpha \in \beta$, $\alpha = \beta$ or $\beta \in \alpha$.*

Proof. We first prove that either one of $\alpha \in \beta$, $\alpha = \beta$ or $\beta \in \alpha$ is true.

Claim: We claim that $\alpha \cap \beta$ is an ordinal.

Proof of the claim.

We need to prove that $\alpha \cap \beta$ is transitive and well-ordered.

First we show the transitivity of $\alpha \cap \beta$.

Let x and y be sets. Suppose that $x \in y$ and $y \in \alpha \cap \beta$. We need to show that $x \in \alpha \cap \beta$. Since $y \in \alpha \cap \beta$, implies that $y \in \alpha$ and $y \in \beta$. We have $x \in y$ and $y \in \alpha$ implies $x \in \alpha$ since α is transitive. Also we have $x \in y$ and $y \in \beta$ implies $x \in \beta$ since β is transitive. Now we have $x \in \alpha$ and $x \in \beta$ implies $x \in \alpha \cap \beta$ and so $\alpha \cap \beta$ is transitive.

Now we show that $(\alpha \cap \beta, \in)$ is well-ordered.

But $\in$ is a well-ordering on β implies that $\in$ is a well-ordering on $\alpha \cap \beta$. Hence $(\alpha \cap \beta, \in)$ is well-ordered.

Hence $\alpha \cap \beta$ is an ordinal.

Now we have $\alpha \cap \beta \subseteq \alpha$ and $\alpha \cap \beta \subseteq \beta$. If $\alpha \cap \beta \neq \alpha$ and $\alpha \cap \beta \neq \beta$, then $\alpha \cap \beta \in \alpha$ and $\alpha \cap \beta \in \beta$ by Theorem 2.1.8. This implies that $\alpha \cap \beta \in \alpha \cap \beta$ which is a contradiction by Lemma 2.1.9. So $\alpha \cap \beta = \alpha$ or $\alpha \cap \beta = \beta$. If $\alpha \cap \beta = \alpha$, then $\alpha \subseteq \beta$. Since $\alpha \subseteq \beta$, if $\alpha \neq \beta$ then $\alpha \in \beta$ by Theorem 2.1.8. If $\alpha \cap \beta = \beta$, then $\beta \subseteq \alpha$. Since $\beta \subseteq \alpha$, if $\beta \neq \alpha$ then $\beta \in \alpha$ by Theorem 2.1.8. And so at least one of $\alpha \in \beta$, $\alpha = \beta$ or $\beta \in \alpha$ holds.

Now we show that exactly one of $\alpha \in \beta$, $\alpha = \beta$ or $\beta \in \alpha$ holds.

If $\alpha \in \beta$ and $\alpha = \beta$, then $\alpha \in \alpha$ which is a contradiction by Lemma 2.1.9. Similarly, if $\beta \in \alpha$ and $\beta = \alpha$, then $\beta \in \beta$ which is a contradiction by Lemma 2.1.9. And if $\alpha \in \beta$ and $\beta \in \alpha$, then $\alpha \in \alpha$ and $\beta \in \beta$ which is a contradiction by Lemma 2.1.9. So exactly one of $\alpha \in \beta$, $\alpha = \beta$ or $\beta \in \alpha$ holds. □

After this discussion on some set-theoretic properties of ordinals now we can take a look at the class of all ordinals which we denote as **Ord**. This is just a collection of all the ordinals and so it is too big for it to be a set as the **Burali-Forti paradox** shows. This will be proved in the next Theorem.

2.1.11 Definition (Class of Ordinals)**.** The class **Ord** of all ordinals is defined as the collection of all ordinals i.e.

$$\textbf{Ord} = \{\alpha : \ \alpha \text{ is an ordinal}\} .$$

2.1.12 Theorem (Burali-Forti paradox)**.** *(Don Monk, c)* ***Ord*** *is not a set.*

Proof. Suppose that **Ord** is a set.

We claim that **Ord** is an ordinal.

Proof of the claim.

First we show that **Ord** is totally ordered.

Irreflexive: Since **Ord** contains ordinals, for any $\alpha \in \textbf{Ord}$, $\alpha \notin \alpha$ by Lemma 2.1.9. Irreflexive holds.

Trichotomous: Take $\alpha, \beta \in \textbf{Ord}$. Since α and β are ordinals, by Theorem 2.1.10 either $\alpha \in \beta$, $\alpha = \beta$ or $\beta \in \alpha$. Trichotomous holds.

Transitive: Take $\alpha, \beta, \gamma \in \textbf{Ord}$ such that $\alpha \in \beta$ and $\beta \in \gamma$. Since γ ordinal and we have $\alpha \in \beta$ and $\beta \in \gamma$, by transitivity of γ we have $\alpha \in \gamma$. Transitive holds.

Since the three conditions hold, **Ord** is totally ordered.

Now we show that **Ord** is transitive.

Let $\alpha \in \textbf{Ord}$. Then α is an ordinal. If $\beta \in \alpha$, then by Theorem 2.1.7 we have that β is an ordinal and so $\beta \in \textbf{Ord}$. Thus **Ord** is transitive.

Finally we show that **Ord** is well-ordered.

Let S be a non-empty subset of **Ord**. We need to show that S has a least element.

Let $\alpha \in S$. If $\alpha \cap S = \emptyset$, then α is a least element of S. Otherwise, if $\alpha \cap S \neq \emptyset$, then since α is well-ordered, its non-empty subset $\alpha \cap S$ must have a least element β. Then we have $\beta \in S$ and $\beta \in \alpha$. We claim that $\beta \cap S = \emptyset$. Otherwise, if $\beta \cap S \neq \emptyset$, then there is some $\gamma \in \beta \cap S$. Now we have $\gamma \in \beta$ and $\beta \in \alpha$, it follows that $\gamma \in \alpha$ by transitivity of α. Since $\gamma \in \alpha$ it follows that $\gamma \in \alpha \cap S$. Now we have $\gamma \in \alpha \cap S$ and $\gamma \in \beta$. This is a contradiction since β is the least element of $\alpha \cap S$. Thus we have $\beta \cap S = \emptyset$, and so β is the least element of S. Hence **Ord** is well-ordered.

Thus **Ord** is an ordinal. Since **Ord** contains all ordinals we have $\textbf{Ord} \in \textbf{Ord}$ which is a contradiction by Lemma 2.1.9. And so we have **Ord** is not a set. □

2.1.13 Theorem. *(Murphy, James) If A is a set of ordinals, then $\bigcup A$ is an ordinal.*

Proof. Let $\alpha = \bigcup A$. We need to show that α is an ordinal, i.e α is transitive and well-ordered.

First we show that α is transitive.

Let x and y be sets such that $x \in y$ and $y \in \alpha$. Required to show that $x \in \alpha$. By the definition of union, we have $y \in z$ for some $z \in A$. Since A is a set of ordinals, z is transitive. Since $y \in z$ and $x \in y$, we have $x \in z$ by transitivity of z. Now we have $x \in z$ and $z \in A$, implies $x \in \bigcup A$ and so $x \in \alpha$. Thus α is transitive.

Now we show that $(\alpha, \in)$ is well-ordered.

Since α is a subset of the class of ordinals, it follows that α is well-ordered by $\in$. Thus $(\alpha, \in)$ is well-ordered. □

Now we need to introduce an important idea of limit and successor ordinals. In this idea we consider the ordinals with an immediate predecessor which we call **successor ordinals** and those without an immediate predecessor which we call **limit ordinals**. In the following section below we are going to define them formally and the idea will be useful in proving some properties.

2.2 Successor and limit ordinals

2.2.1 Definition (Successor ordinals)**.** (Boxall, 2017) Let α be an ordinal. If α has a maximum element with respect to $\in$, then we say that α is a successor ordinal.

2.2.2 Definition. (Boxall, 2017) If α is an ordinal, then the successor of α is $\alpha + 1 = \alpha^+ = \alpha \cup \{\alpha\}$.

2.2.3 Example. 1 is successor of 0, 2 is successor of 1, and $\omega + 1$ is successor of ω.

2.2.4 Definition (Limit ordinals)**.** (Boxall, 2017) Let α be an ordinal. If α does not have a maximum element with respect to $\in$, then we say that α is a limit ordinal. Alternatively, we say that α is limit ordinal if α does not have an immediate predecessor.

2.2.5 Example. 0 is a limit ordinal, and ω is a limit ordinal.

2.2.6 Definition. (Boxall, 2017) Let $(A, <)$ and $(B, <')$ be totally ordered sets. An isomorphism $f : (A, <) \longrightarrow (B, <')$ is a bijection such that $\forall a, b \in A,\ a < b$ iff $f(a) <' f(b)$, i.e. This isomorphism preserves order.

The totally ordered sets $(A, <)$ and $(B, <')$ are said to be isomorphic if such isomorphism f exists.

Note that:

1. $id_A : (A, <) \longrightarrow (A, <)$ is an isomorphism.
2. If $f : (A, <) \longrightarrow (B, <')$ is an isomorphism then $f^{-1} : (B, <') \longrightarrow (A, <)$ is an isomorphism.
3. If $f : (A, <) \longrightarrow (B, <')$ and $g : (B, <') \longrightarrow (C, <'')$ are both isomorphisms then

   $g \circ f : (A, <) \longrightarrow (C, <'')$ is an isomorphism. In other words, the composition of isomorphisms is an isomorphism.

Thus being isomorphic is an equivalence relation.

2.2.7 Definition (Order-type)**.** (Wikipedia, a) Let X and Y be ordered sets. Then we say that X and Y have the same order-type if they are isomorphic.

2.2.8 Remark. Georg Cantor defined the order type as that property of totally ordered sets that remains when the set is considered, not with respect to the properties of its elements, but with respect to their order (Encyclopedia of Mathematics, a).

2.2.9 Theorem. *(Edward) Let $(A, <)$ be a well-ordered set. Then there exists a unique ordinal that is isomorphic to $(A, <)$.*

Proof. We use transfinite induction to prove this theorem.

Consider the following construction of sequences of subsets of $(A, <)$ by using transfinite induction.

Base case:

When $\alpha = 0$ we have $A_\alpha = A_0 = \emptyset$.

Successor case:

For all successor ordinals $\alpha + 1$, we define x_α to be the least element of $A \setminus A_\alpha$, provided that $A \setminus A_\alpha \neq \emptyset$. Then $A_{\alpha+1} = A_\alpha \cup \{x_\alpha\}$.

Limit case:

For all non-zero limit ordinals α, we define $A_\alpha = \bigcup_{\lambda<\alpha} A_\lambda$.

Notice that in this construction, the ordinal numbers can be embedded into A, which makes A, contradicting Theorem 2.1.12. To avoid this contradiction, this construction must terminate for some ordinal β, where $A \setminus A_\beta = \emptyset$, i.e. $A_\beta = A$.

We can write $A_\alpha = \{x_\sigma : \sigma < \alpha\}$ for all $\alpha < \beta$.

Now we prove that A_α is uniquely order isomorphic to α for all $\alpha \leq \beta$ by induction on α.

Base case:

When $\alpha = 0$ we have $A_0 = \emptyset$ which is order isomorphic to $0 = \emptyset$ by the unique empty function.

Successor case:

Suppose that it holds for some $\alpha < \beta$. Therefore A_α is uniquely order isomorphic to α. Let $f_\alpha : A_\alpha \to \alpha$ be the unique order isomorphism. By definition we know that $A_{\alpha+1} = A_\alpha \cup \{x_\alpha\}$ where x_α is the least element of $A \setminus A_\alpha$. We define a function $f_{\alpha+1} : A_{\alpha+1} \to \alpha + 1$ by $f_{\alpha+1}(x) = f_\alpha(x)$ for all $x \in A_\alpha$ and $f_{\alpha+1}(x_\alpha) = \alpha$. Since f_α is a unique order isomorphism, we have $f_{\alpha+1}$ is an order isomorphism and it is unique since it has to send the maximal element to the maximal element.

Limit case:

Let $\alpha < \beta$ be a limit ordinal and suppose our result holds for all $\lambda < \alpha$. Let $f_\lambda : A_\lambda \to \lambda$ be the unique order isomorphism for all $\lambda < \alpha$. Since $A_\gamma \subset A_\sigma$ for any $\gamma < \sigma$, it follows that these order isomorphisms must agree, that is $\forall\ \gamma < \sigma$, $f_{\gamma+1}(x_\gamma) = f_\sigma(x_\gamma)$. We define $f_\alpha : A_\alpha \to \alpha$ by $f_\alpha(x_\lambda) = f_{\lambda+1}(x_\lambda) = \lambda$ for all $x_\lambda \in A_\alpha$ where $\lambda < \alpha$. We need to prove that f_α is a bijection, an order preserving isomorphism and unique.

To prove that f_α is bijective we need to show that f_α is injective and surjective.

Injectivity:

For $\gamma \leq \sigma < \alpha$, suppose that $f_\alpha(x_\gamma) = f_\alpha(x_\sigma)$. We need to show that $x_\gamma = x_\sigma$.

But $f_\alpha(x_\gamma) = f_{\gamma+1}(x_\gamma)$ and $f_\alpha(x_\sigma) = f_{\sigma+1}(x_\sigma)$ by the definition of f_α. Then from $f_\alpha(x_\gamma) = f_\alpha(x_\sigma)$ we have $f_{\gamma+1}(x_\gamma) = f_{\sigma+1}(x_\sigma)$. Since the order isomorphisms agree on the subsets we have $f_{\gamma+1}(x_\gamma) = f_{\sigma+1}(x_\gamma)$. This implies that $f_{\sigma+1}(x_\gamma) = f_{\sigma+1}(x_\sigma)$. And so we have $x_\gamma = x_\sigma$. Thus, f_α is injective.

Surjectivity:

Required to prove that for any $\lambda \in \alpha$, we have $f_\alpha(x_\lambda) = \lambda$.

Let $\lambda \in \alpha$. Since order isomorphisms must agree, for $\lambda < \alpha$ we have $f_{\lambda+1}(x_\lambda) = f_\alpha(x_\lambda)$ for all $x_\lambda \in A_\alpha$. But by the definition of f_α we know that $f_\alpha(x_\lambda) = f_{\lambda+1}(x_\lambda) = \lambda$. Thus we have $f_\alpha(x_\lambda) = \lambda$ as required. Hence f_α is surjective.

Since f_α is injective and surjective, it follows that f_α is bijective.

Order preserving:

Let $x_\gamma < x_\sigma \in A_\alpha$. We need to show that $f_\alpha(x_\gamma) < f_\alpha(x_\sigma)$.

Since $x_\gamma < x_\sigma$, this implies that $f_{\sigma+1}(x_\gamma) < f_{\sigma+1}(x_\sigma)$. But $f_{\sigma+1}(x_\gamma) = f_{\gamma+1}(x_\gamma) = f_\alpha(x_\gamma)$ and $f_{\sigma+1}(x_\sigma) = f_\alpha(x_\sigma)$. Then from $f_{\sigma+1}(x_\gamma) < f_{\sigma+1}(x_\sigma)$ we have $f_\alpha(x_\gamma) < f_\alpha(x_\sigma)$. Therefore, f_α preserves order.

Uniqueness:

We know that f_α is an order isomorphism, so f_α is unique since its restriction to A_λ must be an order isomorphism with λ.

Now we have a unique order isomorphism from A_α to α for all $\alpha \leq \beta$ and so, in particular, for β. So we have $(A, <)$ is uniquely isomorphic to $(\beta, \in)$ as required. □

2.2.10 Remark. From now onward the order type of $(A, <)$ is the unique ordinal α such that $(A, <)$ is isomorphic to $(\alpha, \in)$.

As in natural numbers, it is also possible to perform arithmetic in the ordinal numbers. In the following section we are going to introduce three important operations of ordinal arithmetic: ordinal addition, ordinal multiplication and ordinal exponentiation. We will do some examples and then try to compare some properties of each operation in the natural numbers and see if they hold for the ordinal numbers. These properties include associativity, commutativity, left distribution, right distribution e.t.c.

2.3 Ordinal arithmetic

Let us start by building up some useful concepts and then we will define the three ordinal arithmetic operations and consider examples for each.

2.3.1 Definition (Normal function)**.** (Don Monk, b) A normal function is a function f : **Ord** → **Ord** that is strictly increasing and continuous i.e. for all $\alpha, \beta, \gamma \in$ **Ord**

1. If $\alpha < \beta$, then $f(\alpha) < f(\beta)$.
2. If α is a non-zero limit ordinal, then $f(\alpha) = \bigcup_{\gamma<\alpha} f(\gamma)$.

2.3.2 Addition of Ordinals. (Murphy, James) We define ordinal addition by transfinite recursion as follows:

1. $\alpha + 0 = \alpha$.
2. $\alpha + \beta^+ = (\alpha + \beta)^+$.
3. $\alpha + \beta = \bigcup \{\alpha + \gamma | \gamma < \beta\}$ if β is a non-zero limit ordinal.

2.3.3 Proposition. For all $\alpha \in$ **Ord** we have $0 + \alpha = \alpha$.

Proof. We prove by induction on α.

Base case:

When $\alpha = 0$ we have $0 + 0 = 0$. It holds for $\alpha = 0$.

Successor case:

Assume that $0 + \alpha = \alpha$. We need to show that $0 + \alpha^+ = \alpha^+$.

But $0 + \alpha^+ = (0 + \alpha)^+ = \alpha^+$ as required.

Limit case:

Assume that α is a limit and suppose that $0 + \beta = \beta$ for all $\beta < \alpha$. We need to show that $0 + \alpha = \alpha$.

Since α is a limit, $0 + \alpha = \bigcup\{0 + \beta | \beta < \alpha\} = \bigcup\{\beta | \beta < \alpha\} = \alpha$ as required. □

2.3.4 Example. Let us consider the following:

i) $\omega + 1 = \omega + 0^+ = (\omega + 0)^+ = \omega^+$.

ii) $1 + \omega = \bigcup \{1 + \gamma | \gamma < \omega\} = \bigcup \{1 + \gamma_1, 1 + \gamma_2, 1 + \gamma_3, \ldots\} = \omega$.

iii) $\omega + 2 = \omega + 1^+ = (\omega + 1)^+ = (\omega + 0^+)^+ = ((\omega + 0)^+)^+ = (\omega^+)^+ = \omega^{++}$.

iv)

$$\begin{aligned} \omega + 3 &= \omega + 2^+ = (\omega + 2)^+ = (\omega + 1^+)^+ = ((\omega + 1)^+)^+ = ((\omega + 0^+)^+)^+ \\ &= (((\omega + 0)^+)^+)^+ = (\omega^+)^{++} = \omega^{+++}. \end{aligned}$$

v) $5 + \omega = \bigcup \{5 + \gamma | \gamma < \omega\} = \omega$.

vi) $\omega + \omega = \bigcup \{\omega + \gamma | \gamma < \omega\}$.

2.3.5 Theorem. *(Don Monk, b) If α, β and γ are ordinals, then $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.*

Proof. By induction on γ.

Base case:

When $\gamma = 0$ we have

L.H.S: $(\alpha + \beta) + 0 = \alpha + \beta$.

R.H.S: $\alpha + (\beta + 0) = \alpha + \beta$.

It holds for $\gamma = 0$.

Successor case:

Assume $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$. We need to show that $(\alpha+\beta)+\gamma^{+}=\alpha+(\beta+\gamma^{+})$.

Consider R.H.S

$$\begin{aligned}\alpha+(\beta+\gamma^{+}) &= \alpha+(\beta+\gamma)^{+}\\ &= (\alpha+(\beta+\gamma))^{+}\\ &= ((\alpha+\beta)+\gamma)^{+}\\ &= (\alpha+\beta)+\gamma^{+} \quad \text{which is the L.H.S.}\end{aligned}$$

Limit case:

Assume $(\alpha+\beta)+\lambda=\alpha+(\beta+\lambda)$ for all $\lambda<\gamma$. We need to show that $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$.

For all $\lambda<\gamma$ we define the normal functions f, g and h as follows:

$$\begin{aligned}f(\lambda) &= \alpha+\lambda\\ g(\lambda) &= (\alpha+\beta)+\lambda\\ h(\lambda) &= \beta+\lambda\end{aligned}$$

All the three functions i.e. f, g and h are normal functions also the composite of two normal functions is normal (see Don Monk (b)).

Then from $\alpha+(\beta+\gamma)$ we have $\alpha+(\beta+\gamma)=\alpha+h(\gamma)$ since $\beta+\gamma=h(\gamma)$ by definition of h. But $\alpha+h(\gamma)=f(h(\gamma))$ by definition of f. Thus $\alpha+(\beta+\gamma)=f(h(\gamma))$. Since γ is a limit ordinal we have $f(h(\gamma))=\bigcup\limits_{\lambda<\gamma} f(h(\lambda))$. But $h(\lambda)=\beta+\lambda$. Then we have $f(h(\gamma))=\bigcup\limits_{\lambda<\gamma} f(\beta+\lambda)$. But $f(\beta+\lambda)=\alpha+(\beta+\lambda)$. Then we have $f(h(\gamma))=\bigcup\limits_{\lambda<\gamma}(\alpha+(\beta+\lambda))=\bigcup\limits_{\lambda<\gamma}((\alpha+\beta)+\lambda)$. But $(\alpha+\beta)+\lambda=g(\lambda)$ by definition of g. Then we have $f(h(\gamma))=\bigcup\limits_{\lambda<\gamma} g(\lambda)$. But $\bigcup\limits_{\lambda<\gamma} g(\lambda)=g(\gamma)$ since g is normal. Then we have $f(h(\gamma))=g(\gamma)=(\alpha+\beta)+\gamma$. Hence we have $\alpha+(\beta+\gamma)=f(h(\gamma))=(\alpha+\beta)+\gamma$.

Thus, we have $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$ when γ is a limit.

Therefore, $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$. □

2.3.6 Remark. The commutative property for ordinal addition is not true: $\omega+1=\omega^{+}\neq\omega=1+\omega$, since ω^{+} has a maximum element while ω does not. But the associativity property holds for ordinal addition as we have shown in Theorem 2.3.5.

2.3.7 Ordinal multiplication. (Murphy, James) We define ordinal multiplication by transfinite recursion as follows:

1. $\alpha\cdot 0=0$.
2. $\alpha\cdot\beta^{+}=(\alpha\cdot\beta)+\alpha$.
3. $\alpha\cdot\beta=\bigcup\{\alpha\cdot\gamma|\gamma<\beta\}$ if β is a non-zero limit ordinal.

2.3.8 Example. 1) $1\cdot\omega=\bigcup\{1\cdot\gamma|\gamma<\omega\}=\bigcup\{1\cdot\gamma_1, 1\cdot\gamma_2, 1\cdot\gamma_3,\ldots\}=\bigcup\{\gamma_1,\gamma_2,\gamma_3,\ldots\}=\omega$.

ii) $\omega\cdot 2=\omega\cdot 1^{+}=(\omega\cdot 1)+\omega=(\omega\cdot 0^{+})+\omega=((\omega\cdot 0)+\omega)+\omega=(0+\omega)+\omega=\omega+\omega$.

iii) $2\cdot\omega=\bigcup\{2\cdot\gamma|\gamma<\omega\}=\omega$

iv) $3\cdot\omega=\bigcup\{3\cdot\gamma|\gamma<\omega\}=\omega$.

v) $\omega \cdot \omega = \bigcup\{\omega \cdot \gamma | \gamma < \omega\}$.

2.3.9 Example. Consider the following $(1+1)\cdot\omega \neq 1\cdot\omega + 1\cdot\omega$.

L.H.S: $(1+1)\cdot\omega = 2\cdot\omega = \omega$.

R.H.S: $1\cdot\omega + 1\cdot\omega = \omega + \omega$.

Now we have $(1+1)\cdot\omega = \omega$ and $1\cdot\omega+1\cdot\omega = \omega+\omega$ implies that $(1+1)\cdot\omega \neq 1\cdot\omega+1\cdot\omega$, because, for example, the element $\omega \in \omega\cdot 2$ has infinitely many elements below it, whereas no element of ω has this property.

2.3.10 Remark. The commutative property we know is not always true for ordinal multiplication as we have shown in Example 2.3.8 that $\omega\cdot 2 = \omega+\omega$ while $2\cdot\omega = \omega$. Also Example 2.3.9 shows that the right distribution law is not always true for ordinal multiplication. But the left distribution law holds for ordinal multiplication as proved in the following Theorem.

2.3.11 Theorem. *(Don Monk, b) If α, β and γ are ordinals, then $\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$.*

Proof. By induction on γ.

Base case:

When $\gamma = 0$ we have

L.H.S: $\alpha\cdot(\beta+0) = \alpha\cdot\beta$.

R.H.S: $\alpha\cdot\beta+\alpha\cdot 0 = \alpha\cdot\beta$.

It holds for $\gamma = 0$.

Successor case:

Assume $\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$. We need to show that $\alpha\cdot(\beta+\gamma^+) = \alpha\cdot\beta+\alpha\cdot\gamma^+$.

Consider L.H.S

$$\begin{aligned}
\alpha\cdot(\beta+\gamma^+) &= \alpha\cdot(\beta+\gamma)^+ \\
&= \alpha\cdot(\beta+\gamma)+\alpha \\
&= \alpha\cdot\beta+\alpha\cdot\gamma+\alpha \\
&= \alpha\cdot\beta+\alpha\cdot(\gamma+1) \\
&= \alpha\cdot\beta+\alpha\cdot\gamma^+ \quad \text{which is the R.H.S.}
\end{aligned}$$

Limit case:

Assume $\alpha\cdot(\beta+\lambda) = \alpha\cdot\beta+\alpha\cdot\lambda$ for all $\lambda<\gamma$. We need to show that $\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$.

For all $\lambda<\gamma$ we define the normal functions f, g and h as follows:

$$\begin{aligned}
f(\lambda) &= \alpha\cdot\lambda \\
g(\lambda) &= \alpha\cdot\beta+\alpha\cdot\lambda \\
h(\lambda) &= \beta+\lambda
\end{aligned}$$

All the three functions i.e. f, g and h are normal functions also the composite of two normal functions is normal (see Don Monk (b)).

Then we have $\alpha \cdot (\beta + \gamma) = \alpha \cdot h(\gamma)$, since $\beta + \gamma = h(\gamma)$ by definition of h. But $\alpha \cdot h(\gamma) = f(h(\gamma))$ by definition of f. Thus $\alpha \cdot (\beta + \gamma) = f(h(\gamma))$. Since γ is a limit ordinal we have $f(h(\gamma)) = \bigcup_{\lambda<\gamma} f(h(\lambda))$. But $h(\lambda) = \beta + \lambda$. Then we have $f(h(\gamma)) = \bigcup_{\lambda<\gamma} f(\beta + \lambda)$. But $f(\beta + \lambda) = \alpha \cdot (\beta + \lambda)$. Then we have $f(h(\gamma)) = \bigcup_{\lambda<\gamma} (\alpha \cdot (\beta + \lambda)) = \bigcup_{\lambda<\gamma} (\alpha \cdot \beta + \alpha \cdot \lambda)$. But $\alpha \cdot \beta + \alpha \cdot \lambda = g(\lambda)$ by definition of g. Then we have $f(h(\gamma)) = \bigcup_{\lambda<\gamma} g(\lambda)$. But $\bigcup_{\lambda<\gamma} g(\lambda) = g(\gamma)$ since g is normal. Then we have $f(h(\gamma)) = g(\gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$. Hence we have $\alpha \cdot (\beta + \gamma) = f(h(\gamma)) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Thus, we have $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ when γ is a limit.

Therefore, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$. □

2.3.12 Ordinal Exponentiation. We define ordinal exponentiation by transfinite recursion as follows. Let $\alpha > 0$.

1. $\alpha^0 = 1$.
2. $\alpha^{\beta^+} = \alpha^\beta \cdot \alpha$.
3. $\alpha^\beta = \bigcup\{\alpha^\gamma | \gamma < \beta\}$ if β is a non-zero limit ordinal.

2.3.13 Example. Let us consider the following:

i) $\omega^2 = \omega^{1^+} = \omega^1 \cdot \omega = \omega^{0^+} \cdot \omega = (\omega^0 \cdot \omega) \cdot \omega = (1 \cdot \omega) \cdot \omega = \omega \cdot \omega$.

ii) $8^\omega = \bigcup\{8^\gamma | \gamma < \omega\} = \omega$.

iii) $\omega^\omega = \bigcup\{\omega^\gamma | \gamma < \omega\}$.

2.3.14 Lemma. (Don Monk, b) Let α, β, γ be ordinals and $\alpha > 0$. Then $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$.

Proof. By induction on γ.

Base case:

When $\gamma = 0$ we have

L.H.S: $\alpha^{\beta+0} = \alpha^\beta$.

R.H.S: $\alpha^\beta \cdot \alpha^0 = \alpha^\beta \cdot 1 = \alpha^\beta \cdot 0^+ = (\alpha^\beta \cdot 0) + \alpha^\beta = \alpha^\beta$.

It holds for $\gamma = 0$.

Successor case:

Assume $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$. We need to show that $\alpha^{\beta+\gamma^+} = \alpha^\beta \cdot \alpha^{\gamma^+}$.

Consider L.H.S

$$\begin{aligned}
\alpha^{\beta+\gamma^+} &= \alpha^{(\beta+\gamma)^+} \\
&= \alpha^{\beta+\gamma} \cdot \alpha \\
&= \alpha^\beta \cdot \alpha^\gamma \cdot \alpha \\
&= \alpha^\beta \cdot (\alpha^\gamma \cdot \alpha) \\
&= \alpha^\beta \cdot \alpha^{\gamma^+} \quad \text{which is the R.H.S.}
\end{aligned}$$

Limit case:

Assume $\alpha^{\beta+\lambda} = \alpha^{\beta} \cdot \alpha^{\lambda}$ for all $\lambda < \gamma$. We need to show that $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$.

For all $\lambda < \gamma$ we define the normal functions f, g and h as follows:

$$f(\lambda) = \alpha^{\lambda}$$
$$g(\lambda) = \alpha^{\beta} \cdot \alpha^{\lambda}$$
$$h(\lambda) = \beta + \lambda$$

All the three functions i.e. f, g and h are normal functions also the composite of two normal functions is normal (see Don Monk (b)).

Then we have $\alpha^{\beta+\gamma} = \alpha^{h(\gamma)}$, since $\beta + \gamma = h(\gamma)$ by definition of h. But $\alpha^{h(\gamma)} = f(h(\gamma))$ by definition of f. Thus $\alpha^{\beta+\gamma} = f(h(\gamma))$. Since γ is a limit ordinal we have $f(h(\gamma)) = \bigcup_{\lambda<\gamma} f(h(\lambda))$. But $h(\lambda) = \beta + \lambda$. Then we have $f(h(\gamma)) = \bigcup_{\lambda<\gamma} f(\beta + \lambda)$. But $f(\beta + \lambda) = \alpha^{\beta+\lambda}$. Then we have $f(h(\gamma)) = \bigcup_{\lambda<\gamma} \left(\alpha^{\beta+\lambda}\right) = \bigcup_{\lambda<\gamma} (\alpha^{\beta} \cdot \alpha^{\lambda})$. But $\alpha^{\beta} \cdot \alpha^{\lambda} = g(\lambda)$ by definition of g. Then we have $f(h(\gamma)) = \bigcup_{\lambda<\gamma} g(\lambda)$. But $\bigcup_{\lambda<\gamma} g(\lambda) = g(\gamma)$ since g is normal. Then we have $f(h(\gamma)) = g(\gamma) = \alpha^{\beta} \cdot \alpha^{\gamma}$. Hence we have $\alpha^{\beta+\gamma} = f(h(\gamma)) = \alpha^{\beta} \cdot \alpha^{\gamma}$.

Thus, we have $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$ when γ is a limit.

Therefore, $\alpha^{\beta+\gamma} = \alpha^{\beta} \cdot \alpha^{\gamma}$. □

2.3.15 Lemma. If α is an ordinal, then $\alpha \leq \omega^{\alpha}$.

Proof. **Base case:**

When $\alpha = 0$ we have $0 \leq \omega^{0}$ because $0 \leq 1$. It holds for $\alpha = 0$.

Successor case:

Assume it holds for α. Now we need to show that $\alpha^{+} \leq \omega^{\alpha^{+}}$. Since $\alpha \leq \omega^{\alpha}$ it follows that $\alpha \leq \omega^{\alpha} < \omega^{\alpha} + 1 \leq \omega^{\alpha} + \omega^{\alpha} = \omega^{\alpha} \cdot 2 \leq \omega^{\alpha} \cdot \omega = \omega^{\alpha^{+}}$. Thus we have $\alpha < \omega^{\alpha^{+}}$. This implies that $\alpha + 1 \leq \omega^{\alpha+1}$. Thus $\alpha^{+} \leq \omega^{\alpha^{+}}$. So it is true when α is a successor ordinal.

Limit case:

Assume it holds for all $\beta < \alpha$. Then we have $\beta \leq \omega^{\beta}$ for all $\beta < \alpha$. Now we need to show that $\alpha \leq \omega^{\alpha}$. Since α is a limit ordinal, $\omega^{\alpha} = \sup_{\beta<\alpha}(\omega^{\beta})$. But $\sup_{\beta<\alpha} \omega^{\beta} \geq \omega^{\beta} \geq \beta$ for all $\beta < \alpha$. This implies that $\omega^{\alpha} \geq \beta$ for all $\beta < \alpha$. This implies that $\omega^{\alpha} \geq \sup_{\beta<\alpha}(\beta) = \alpha$. Therefore we have $\alpha \leq \omega^{\alpha}$ as required. □

2.3.16 Lemma. If $\alpha, \beta \in$ **Ord**, then $\alpha \geq \beta$ iff there exists $\delta \in$ **Ord** such that $\beta + \delta = \alpha$.

Proof. $(\Leftarrow)$ If $\delta = 0$, then $\beta = \alpha$. If $\delta > 0$, then $\beta < \beta + \delta = \alpha$.

$(\Rightarrow)$ We use induction on α.

Base case:

For $\alpha = \beta$, $\delta = 0$.

Successor case:

Assume $\alpha > \beta$ and α is a successor. Then let $\alpha = \alpha_1^+$ and $\beta + \delta_1 = \alpha_1$. Then $\beta + \delta_1^+ = (\beta + \delta_1)^+ = \alpha_1^+ = \alpha$.

Limit case:

Assume $\alpha > \beta$ and α is a limit. Then $\alpha = \sup_{\beta \leq \lambda < \alpha} \lambda$. Each $\lambda < \alpha$ such that $\lambda \geq \beta$, let δ_λ be such that $\beta + \delta_\lambda = \lambda$. Consider $\delta = \sup_{\lambda < \alpha} \delta_\lambda$. If δ is a successor, then $\delta = \delta_{\lambda_0}$ for some $\lambda_0 < \alpha$. Choose λ_0' such that $\lambda_0 < \lambda_0' < \alpha$. Then $\lambda_0' = \beta + \delta_{\lambda_0'} \leq \beta + \delta_{\lambda_0} = \lambda_0$ which is a contradiction. Hence δ is a limit and δ_λ is such that for each $\varepsilon < \delta$ there is $\lambda_\varepsilon < \alpha$ such that $\varepsilon < \delta_{\lambda_\varepsilon} < \delta$. Then $\beta + \delta = \sup_{\gamma < \delta}(\beta + \gamma) = \sup_{\beta \leq \lambda < \alpha} (\beta + \delta_\lambda) = \sup_{\lambda < \alpha} \lambda = \alpha$. □

2.3.17 Lemma. If χ is an ordinal such that $\chi \geq \omega$, then $n + \chi = \chi$ for any $n < \omega$.

Proof. Notice that we consider $n+\chi$ as a well-ordered set with elements labelled $0, 1, \ldots, n-1, \alpha_0, \alpha_1, \ldots \alpha_i, \ldots$ for $i \in \chi$. We define $f : n + \chi \longrightarrow \chi$ as $f(i) = i$ for all $0 \leq i \leq n-1$, $f(\alpha_j) = j + n$ for all $j \in \omega$, and $f(\alpha_l) = l$ for all $\omega \leq l < \chi$. Then f is an isomorphism. □

2.3.18 Lemma. If $0 < n, m < \omega$, then

$$\omega^\beta \cdot n + \omega^\gamma \cdot m = \begin{cases} \omega^\beta \cdot n + \omega^\gamma \cdot m & \text{if} \quad \beta > \gamma \\ \omega^\beta \cdot (n + m) & \text{if} \quad \beta = \gamma \\ \omega^\gamma \cdot m & \text{if} \quad \beta < \gamma \end{cases}$$

Proof. **Case 1:** If $\beta > \gamma$ there is nothing to prove.

Case 2: If $\beta = \gamma$, then it follows from left distributive law (Theorem 2.3.11).

Case 3: If $\beta < \gamma$, then by Lemma 2.3.16 there exist $\delta > 0$ such that $\beta + \delta = \gamma$. Hence $\omega^\beta \cdot n + \omega^\gamma \cdot m = \omega^\beta \cdot n + \omega^{(\beta+\delta)} \cdot m = \omega^\beta \cdot n + \omega^\beta \cdot \omega^\delta \cdot m = \omega^\beta \cdot (n + \omega^\delta \cdot m)$ by Lemma 2.3.14. But $n + \omega^\delta \cdot m = \omega^\delta \cdot m$ by Lemma 2.3.17. Then $\omega^\beta \cdot n + \omega^\gamma \cdot m = \omega^\beta \cdot (\omega^\delta \cdot m) = \omega^{\beta+\delta} \cdot m = \omega^\gamma \cdot m$ □

2.3.19 Theorem (Cantor Normal Form (CNF))**.** *Any ordinal $\alpha > 0$ can be uniquely expressed as $\alpha = \omega^{\beta_1} \cdot n_1 + \omega^{\beta_2} \cdot n_2 + \cdots + \omega^{\beta_k} \cdot n_k$ for some k. Where $\beta_1 > \beta_2 > \ldots > \beta_k$ and $0 < n_i < \omega$ for $i = 1, 2, \ldots, k$.*

Proof. **Existence:**

Suppose CNF exists for all $\delta < \alpha$. Consider $\{\beta \leq \alpha + 1 : \alpha < \omega^\beta\}$. It is non-empty because $\alpha < \omega^{\alpha^+}$. Let β_1' be its least element. If β_1' is a limit, then $\omega^\lambda \leq \alpha < \omega^{\beta_1'}$ for all $\lambda < \beta_1'$ and $\omega^{\beta_1'} = \sup_{\lambda < \beta_1'} (\omega^\lambda) \leq \alpha < \omega^{\beta_1'}$, which is a contradiction. So let $\beta_1' = \beta_1^+$. Then $\omega^{\beta_1} \leq \alpha < \omega^{\beta_1^+} = \omega^{\beta_1} \cdot \omega$. Take biggest n_1 such that $\omega^{\beta_1} \cdot n_1 \leq \alpha$. Then $\omega^{\beta_1} \cdot (n_1 + 1) > \alpha$. By Lemma 2.3.16, $\alpha = \omega^{\beta_1} \cdot n_1 + \delta$ for some δ. Since $\alpha < \omega^{\beta_1} \cdot (n_1 + 1) = \omega^{\beta_1} \cdot n_1 + \omega^{\beta_1}$, we have $\delta < \omega^{\beta_1}$. Since $\delta < \omega^{\beta_1} \leq \alpha$, δ has a CNF. Let $\delta = \omega^{\beta_2} \cdot n_2 + \cdots \omega^{\beta_k} \cdot n_k$ be the CNF of δ. Then $\alpha = \omega^{\beta_1} \cdot n_1 + \omega^{\beta_2} \cdot n_2 + \cdots \omega^{\beta_k} \cdot n_k$ is a CNF of α.

Uniqueness:

Let $\alpha = a = b$ where $a = \omega^{\alpha_1} \cdot n_1 + \omega^{\alpha_2} \cdot n_2 + \cdots + \omega^{\alpha_k} \cdot n_k$ and $b = \omega^{\beta_1} \cdot m_1 + \omega^{\beta_2} \cdot m_2 + \cdots + \omega^{\beta_l} \cdot m_l$ are in CNF.

By Lemma 2.3.16 we have $a \geq \omega^{\alpha_1} \cdot n_1$. If $\alpha_1 > \beta_1$, then Lemma 2.3.18 implies $a \geq \omega^{\alpha_1} \cdot n_1 > \omega^{\beta_1} \cdot (m_1 + 1)$. Then Lemma 2.3.16 and 2.3.18 implies $a \geq \omega^{\alpha_1} \cdot n_1 > \omega^{\beta_1} \cdot (m_1 + 1) \geq b$ which is a contradiction.

If $\alpha_1 = \beta_1$ and $n_1 > m_1$, then by Lemma 2.3.18 we have $a = b + (n_1 - m_1)\omega^{\alpha_1} + \omega^{\alpha_2} \cdot n_2 + \cdots + \omega^{\alpha_k} \cdot n_k$, Lemma 2.3.16 implies $a = b + (n_1 - m_1)\omega^{\alpha_1} + \omega^{\alpha_2} \cdot n_2 + \cdots + \omega^{\alpha_k} \cdot n_k > b$. Hence $\alpha_1 = \beta_1$ and $n_1 = m_1$. Using similar reasoning we can then show $\alpha_2 = \beta_2$ and $n_2 = m_2, \ldots, \alpha_k = \beta_l$ and $n_k = m_l$. In particular, $k = l$. □

2.3.20 Corollary. If $\alpha = \omega^{\alpha_1} \cdot n_1 + \omega^{\alpha_2} \cdot n_2 + \cdots + \omega^{\alpha_k} \cdot n_k$ and $\beta = \omega^{\beta_1} \cdot m_1 + \omega^{\beta_2} \cdot m_2 + \cdots + \omega^{\beta_k} \cdot m_k$ are in CNF, then

$$\alpha > \beta \quad \text{if and only if} \quad \begin{array}{l} (\alpha_1 > \beta_1) \quad \text{or} \\ (\alpha_1 = \beta_1) \wedge (n_1 > m_1) \quad \text{or} \\ (\alpha_1 = \beta_1) \wedge (n_1 = m_1) \wedge (\alpha_2 > \beta_2) \quad \text{or} \\ \qquad\qquad \vdots \\ \ldots \wedge (n_{k-1} = m_{k-1}) \wedge (\alpha_k > \beta_k) \quad \text{or} \\ \ldots \wedge (\alpha_k = \beta_k) \wedge (n_k > m_k). \end{array}$$

Proof. This follows from the proof of the uniqueness part of 2.3.19. □

3. Cardinals

In this section we are going to discuss some properties of cardinals by stating and proving them where necessary. We start by building up concepts that will be useful in our discussions.

3.1 Concepts, definitions and properties of cardinals

3.1.1 Definition (Cardinal)**.** A cardinal is an ordinal α such that α is not in bijection with any ordinal $\beta < \alpha$.

3.1.2 Theorem. *(Murphy, James) Every natural number is a cardinal and ω is a cardinal.*

Proof. Let $p, q \in \mathbb{N}$ such that $p < q$. Since p and q are both finite sets with different numbers of elements, so we cannot have a bijection between p and q. Therefore, p is in not in bijection with q. Thus, every natural number is a cardinal.

Now let α be an ordinal less than ω. Clearly α is a finite natural number by the definition of ω. But finite sets cannot be in bijection with infinite sets. So we have α is not in bijection with ω. Thus, ω is a cardinal. □

3.1.3 Theorem. *(Don Monk, a) Every infinite cardinal is a limit ordinal.*

Proof. Suppose that is not true. Then there exists an infinite successor ordinal say β such that β is a cardinal. Since β is a successor ordinal, $\beta = \alpha^+$ for some α with both β and α infinite. Similarly to 2.3.17, we can define a bijection $f : \alpha \to \beta$ as follows: $f(0) = \alpha$, $f(\nu + 1) = \nu$ for all $\nu \in \omega$, and $f(\gamma) = \gamma$ for $\gamma \in \alpha \setminus \omega$. This implies that α is in bijection with β. This is a contradiction by definition of cardinals. Therefore, every infinite cardinal is a limit ordinal. □

3.1.4 Definition. (Boxall, 2017) Let A and B be sets. We write $|A| \leq |B|$ if there is an injection $f : A \to B$ and we say A injects into B. We write $|A| = |B|$ if there is a bijection $f : A \to B$ and we say A bijects with B.

3.1.5 Theorem (Cantor-Schröder-Bernstein)**.** *(Anon) If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$. In other words, if there is an injection from A into B and an injection from B into A, then there is a bijection from A to B.*

We direct the reader to look at the proof of the above theorem which can be found in Anon.

3.1.6 Theorem. *[Hartog's Lemma](Murphy, James) Let A be a set. Then there exists an ordinal α such that α does not inject into A.*

Proof. Let A be a set.

Consider $F = \{(B, R) : B \subseteq A, R \text{ is a well-ordering on } B\} \subseteq \mathcal{P}(A) \times \mathcal{P}(A \times A)$. Each (B, R) is a well-ordered set, so it is isomorphic to a unique ordinal by Theorem 2.2.9. Let $X = \{\text{order type of } (B, R) \in F\}$. Note that X is a set of ordinals injecting into A. So $\bigcup X$ is an ordinal by Theorem 2.1.13. Let α be an ordinal such that $\alpha > \bigcup X$. Now we need to show that α does not inject into A. Suppose that α injects into A. Then there exists an injection $f : \alpha \to A$. Then we can let $B = ran(f)$. Then we could transfer the order of α to obtain a well-ordering on B call it R. Now we have (B, R) is of order-type α

and $(B, R) \in F$. This implies that $\alpha \in X$, which is a contradiction by our supposition that $\alpha > \bigcup X$. And so we have that α does not inject into A. □

3.1.7 Definition. (Murphy, James) Let A be a set. The least ordinal α such that α does not inject A is called the Hartog's number of A, and is denoted by $H(A)$.

3.1.8 Theorem. *(Murphy, James) If A is a set, then $H(A)$ is a cardinal.*

Proof. Let A be a set. Let $\alpha = H(A)$. Suppose that $\beta < \alpha$ and β is in bijection with α. Let $f : \alpha \to \beta$ be such a bijection. Since $\beta < \alpha$ and $\alpha = H(A)$ it implies that $\beta < H(A)$. Since $\beta < H(A)$, there exists an injection $g : \beta \to A$. Then the composite $g \circ f : \alpha \to A$ is an injection which contradicts the fact that α does not inject into A. Therefore, α is not in bijection with β for any $\beta < \alpha$ and so $\alpha = H(A)$ is a cardinal. □

3.1.9 Theorem. *(Murphy, James) There is no largest cardinal number.*

Proof. Suppose that there is largest cardinal number, and let $\aleph$ be the largest cardinal number. But we know that $H(\aleph)$ is a successor of $\aleph$, which implies that $\aleph < H(\aleph)$ which is a contradiction since $\aleph$ is the largest cardinal number by our supposition. Hence our supposition was false and so there is no largest cardinal number. □

3.1.10 Theorem. *(Murphy, James) Let A be a set. There exists an ordinal α such that A is in bijection with α.*

Proof. Let $<$ be a binary relation on A such that $(A, <)$ is well-ordered. Since $(A, <)$ is well-ordered, there exists a unique ordinal α that is isomorphic to A by Theorem 2.2.9. Hence α is in bijection with A. □

3.1.11 Definition. (Murphy, James) Let A be a set. We define $|A|$ to be the least ordinal α such that A is in bijection with α.

3.1.12 Remark. By 3.1.10, there is an ordinal α in bijection with A. Hence we can consider the set $\{\beta : \beta \text{ in bijection with } A, \beta \leq \alpha\} \subseteq \alpha^+$, which has a least element by the proof of 2.1.12

3.1.13 Remark. The expressions $|A| = |B|$, $|A| \leq |B|$, according to Definition 3.1.4, are equivalent to the interpretation of those expressions according to Definition 3.1.11.

3.1.14 Lemma. (Murphy, James) Let A be a set. Then $|A|$ is a cardinal.

Proof. There exists an ordinal α such that A is in bijection with α by Theorem 3.1.10. Since we can have more than one ordinal which are in bijection with A, we take the least ordinal $|A|$ of this set which is in bijection with A. Then for every $\sigma < |A|$, σ is not in bijection with $|A|$ because if σ is in bijection with $|A|$, then we have σ is in bijection with A since $|A|$ is in bijection with A, which is a contradiction by minimality of $|A|$. Therefore, $|A|$ is a cardinal. □

3.1.15 Remark. Notice that all sets are well-orderable by the well-ordering principle (see Appendix A).

3.2 Cardinal Arithmetic.

In this section we will discuss cardinal arithmetic: cardinal addition, cardinal multiplication and cardinal exponentiation.

3.2.1 Cardinal Addition. We define cardinal addition as follows:

3.2.2 Definition. (Murphy, James) Let I be a set. For $i \in I$, let κ_i be a cardinal. Let $\{A_i : i \in I\}$ be a family of disjoint sets such that, for each i, $|A_i| = \kappa_i$. Then we define addition of cardinals as follows:

$$\sum_{i \in I} \kappa_i = |\bigcup_{i \in I} A_i|.$$

3.2.3 Cardinal Multiplication. We define cardinal multiplication as follows:

3.2.4 Definition. (Boxall, 2017) Let κ and λ be cardinals. Let A and B be sets such that $|A| = \kappa$ and $|B| = \lambda$. Then $\kappa \cdot \lambda = |A \times B|$.

3.2.5 Cardinal Exponentiation. We define cardinal exponentiation as follows:

3.2.6 Definition. (Boxall, 2017) Let κ and λ be cardinals. Then κ^λ is defined to be the cardinality of the set of all functions $f : \lambda \longrightarrow \kappa$.

3.2.7 Definition. (Murphy, James) If κ is a cardinal, we define κ^+ to be $H(\kappa)$. In other words the successor of a cardinal is its Hartog's number.

3.2.8 Definition. (Don Monk, a) We define the cardinal $\aleph_\alpha$ for $\alpha \in$ **Ord** as:

1. $\aleph_0 = \omega$.
2. $\aleph_{\alpha+1} = \aleph_\alpha^+$.
3. $\aleph_\alpha = \bigcup_{\beta<\alpha} \aleph_\beta$: if α is a limit ordinal greater than 0.

3.2.9 Lemma. $\aleph_\alpha$ is a cardinal for all $\alpha \in$ **Ord**.

Proof. To prove that $\aleph_\alpha$ is a cardinal we use induction on α.

Base case:

If $\alpha = 0$ we need to prove that $\aleph_0$ is a cardinal. But we know that $\aleph_0 = \omega$. But ω is cardinal by Theorem 3.1.2. So we have $\aleph_0$ is a cardinal.

Successor case:

Suppose the theorem holds for α and so we have $\aleph_\alpha$ is a cardinal. Required to prove that $\aleph_{\alpha+1}$ is also a cardinal.

Since $\aleph_{\alpha+1} = H(\aleph_\alpha)$ and $H(\aleph_\alpha)$ is a cardinal by Theorem 3.1.8, it follows that $\aleph_{\alpha+1}$ is a cardinal.

Limit case:

When α is a limit ordinal, let $\gamma < \aleph_\alpha$. There exists $\beta < \alpha$ such that $\gamma < \aleph_\beta$. If not, $\gamma \geq \aleph_\beta$ for all $\beta < \alpha$. Hence $\aleph_\alpha = \bigcup_{\beta<\alpha} \aleph_\beta \leq \gamma < \aleph_\alpha$, which is a contradiction. So we have some β such that $\aleph_\beta > \gamma$ and $\aleph_\beta$ is a cardinal by induction hypothesis. Hence $\aleph_\beta$ does not inject into γ and so $\aleph_\alpha$ does not inject into γ. Thus, $\aleph_\alpha$ is not in bijection with γ. This implies $\aleph_\alpha$ is a cardinal by definition of cardinals. □

Notice that, if κ is a ordinal, then it is an infinite cardinal iff there exists an ordinal α with $\kappa = \aleph_\alpha$. To prove this we need the following lemmas.

3.2.10 Lemma. (Rahim Moosa) For ordinals α and β, if $\alpha < \beta$, then $\aleph_\alpha < \aleph_\beta$.

This Lemma can be proved by transfinite induction on β see Rahim Moosa for the proof of this Lemma.

3.2.11 Lemma. (Don Monk, a) If α is an ordinal, then $\alpha \leq \aleph_\alpha$.

Proof. We prove this Theorem by transfinite induction on α.

Base case:

If $\alpha = 0$, we have $\aleph_\alpha = \aleph_0$. But by the definition of $\aleph_\alpha$ we know that $\aleph_0 = \omega$. But we know that $0 \leq \omega$, this implies that $0 \leq \aleph_0$. So the Theorem holds for $\alpha = 0$.

Successor case:

Assume that the Theorem holds for α, and the assumption gives $\alpha \leq \aleph_\alpha$. Now we need to show that $\alpha + 1 \leq \aleph_{\alpha+1}$. Since $\alpha \leq \aleph_\alpha$ it follows that $\alpha \leq \aleph_\alpha < \aleph_{\alpha^+}$ since $\alpha < \alpha^+$. This implies that $\alpha + 1 \leq \aleph_{\alpha+1}$. So the Theorem holds when α is a successor ordinal.

Limit case:

If α is a limit ordinal, first we assume the Theorem holds for all $\beta < \alpha$ and the assumption gives $\beta \leq \aleph_\beta$. Now we need to show that $\alpha \leq \aleph_\alpha$. By Lemma 3.2.10 we have $\aleph_\beta < \aleph_\alpha$, which implies that $\beta \leq \aleph_\beta < \aleph_\alpha$. Then we have $\beta < \aleph_\alpha$. Since α is a limit ordinal, we have $\alpha = \sup_{\beta<\alpha} \beta \leq \aleph_\alpha$. And so we have $\alpha \leq \aleph_\alpha$ as required. So the Theorem holds when α is a limit ordinal. ☐

3.2.12 Theorem. *(Murphy, James) Let κ be an ordinal. Then κ is an infinite cardinal iff there exists $\alpha \in$ **Ord** with $\kappa = \aleph_\alpha$.*

Proof. We only need to prove the forward direction. The other direction follows from Lemma 3.2.9.

Suppose κ is an infinite cardinal. Required to prove that, there exists $\alpha \in$ **Ord** with $\kappa = \aleph_\alpha$.

Since κ is an infinite cardinal, κ is a limit ordinal by Lemma 3.1.3. Since κ is an ordinal, $\kappa \leq \aleph_\kappa$ by Theorem 3.2.11. Suppose $\kappa < \aleph_\kappa$. Then consider $\{\alpha \leq \kappa : \aleph_\alpha > \kappa\}$. This set is non-empty and so it has a least element say α_1. Since κ is a limit ordinal, α_1 cannot be a limit ordinal because if α_1 is a limit ordinal, then $\kappa < \aleph_\beta$ for some $\beta < \alpha_1$ which is a contradiction since α_1 is the least element. If α_1 is a successor ordinal, let α_0 be an immediate predecessor of α_1 such that $\alpha_1 = \alpha_0^+$. Then $\aleph_{\alpha_1} > \kappa \geq \aleph_{\alpha_0}$. But $\aleph_{\alpha_1} = H(\aleph_{\alpha_0})$, so it is the smallest cardinal that does not inject into $\aleph_{\alpha_0}$, hence $\kappa = \aleph_{\alpha_0}$. ☐

3.2.13 Theorem. *(Don Monk, a) For all infinite cardinals κ we have $\kappa \cdot \kappa = \kappa$.*

Proof. Suppose that is not true. Let κ be the least infinite cardinal such that $\kappa \cdot \kappa \neq \kappa$. Then we have $\kappa \cdot \kappa \geq \kappa \cdot 1$. Since $\kappa \cdot 1 = \kappa$ so we have $\kappa \cdot \kappa > \kappa$. We define a relation $\prec$ on $\kappa \times \kappa$ as follows. $\forall \alpha, \beta, \gamma, \sigma \in \kappa$, the pair $(\alpha, \beta) \prec (\gamma, \sigma)$ iff $\max(\alpha, \beta) < \max(\gamma, \sigma)$ or $\max(\alpha, \beta) = \max(\gamma, \sigma)$ and $\alpha < \gamma$ or $\max(\alpha, \beta) = \max(\gamma, \sigma)$ and $\alpha = \gamma$ and $\beta < \sigma$. By definition of $\prec$, clearly $(\kappa \times \kappa, \prec)$ is a well-ordering. Suppose $\kappa \times \kappa$ is isomorphic to δ with an isomorphism $f : \kappa \times \kappa \longrightarrow \delta$. It follows that $|\delta| = |\kappa \times \kappa| > \kappa$. Then $\delta > \kappa$ as ordinals. So there is $(\beta, \gamma) \in \kappa \times \kappa$ such that $f(\beta, \gamma) = \kappa$. By the choice of κ (minimality), we have $\lambda^2 = \lambda$ for all infinite cardinals $\lambda < \kappa$. Let $S = \{(\varphi, \nu) \in \kappa \times \kappa : (\varphi, \nu) \prec (\beta, \gamma)\}$. Now $f(S) = \kappa$, thus with $\psi = \max(\beta, \gamma) + 1 < \kappa$, $\kappa = |S| \leq |\psi \times \psi|$. But $|\psi \times \psi| = |\psi| \cdot |\psi|$. Then we have $\kappa \leq |\psi| \cdot |\psi|$. But $\psi < \kappa$ as ordinals, means $|\psi| < \kappa$ as cardinals. Also $|\psi| \cdot |\psi| = |\psi|$ by minimality of κ. Thus, we have $|\psi| \cdot |\psi| < \kappa$. Now we have $|\psi| \cdot |\psi| < \kappa$ and $\kappa \leq |\psi| \cdot |\psi|$ which is a contradiction. Therefore we have $\kappa \cdot \kappa = \kappa$. ☐

3.2.14 Theorem. *(Boxall, 2017) Let κ and λ be cardinals and suppose that at least one of them is infinite. Then $\kappa + \lambda = \max\{\kappa, \lambda\}$. If it is the case that neither of them is 0, then $\kappa \cdot \lambda = \max\{\kappa, \lambda\}$.*

Proof. Let $m = \max(\kappa, \lambda)$. Let A and B be disjoint sets such that $|A| = \kappa$ and $|B| = \lambda$. Suppose that κ is infinite. Then we have $\kappa \leq m$ and $\lambda \leq m$. It follows that $\kappa + \lambda \leq m + m = 2 \cdot m$ as cardinal arithmetic. But $2 \cdot m \leq m \cdot m$. Since m is infinite by Theorem 3.2.13 we have $m \cdot m = m$ and so we have $2 \cdot m \leq m$. It follows that $\kappa + \lambda \leq m$. But $m \leq |A \cup B|$, implies $m \leq \kappa + \lambda$. Now we have $\kappa + \lambda \leq m$ and $m \leq \kappa + \lambda$. By antisymmetric property we have $\kappa + \lambda = m$. Thus, $\kappa + \lambda = \max(\kappa, \lambda)$. Also notice that $\kappa \cdot \lambda \leq m \cdot m$. Since m is infinite so by Theorem 3.2.13 we have $\kappa \cdot \lambda \leq m$. But $m \leq |A \times B|$ where A and B be disjoint sets with $|A| = \kappa$ and $|B| = \lambda$, implies $m \leq \kappa \cdot \lambda$. Now we have $\kappa \cdot \lambda \leq m$ and $m \leq \kappa \cdot \lambda$. Again by antisymmetric property we have $\kappa \cdot \lambda = m$. Thus, $\kappa \cdot \lambda = \max(\kappa, \lambda)$. Therefore we have $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$. □

3.2.15 Theorem. *(Hammack, 2013) For every set A, A has smaller cardinality than its power set. That is $|A| < |\mathcal{P}(A)|$.*

Proof. To prove that $|A| < |\mathcal{P}(A)|$, we need to show that there exists an injection from A into $\mathcal{P}(A)$ but no surjection from A into $\mathcal{P}(A)$.

First we show the existence of an injection from A into $\mathcal{P}(A)$.

Let $f : A \longrightarrow \mathcal{P}(A)$ such that for every $x \in A$, $f(x) = \{x\} \in \mathcal{P}(A)$. That is f sends every element x of A to the singleton set $\{x\} \in \mathcal{P}(A)$. Then f is injective because, if $f(x) = f(y)$, then $\{x\} = \{y\}$. But the two singletons $\{x\}$ and $\{y\}$ can be equal only if $x = y$, and so we have $x = y$. Thus f is injective.

Now we want to show that there exists no surjection from A into $\mathcal{P}(A)$.

Suppose that there exists surjection $f : A \longrightarrow \mathcal{P}(A)$. By definition of surjection, for every element $y \in \mathcal{P}(A)$ we have $x \in A$ so that $f(x) = y$. This means that f sends elements of A to subsets of A. Thus for any $x \in A$, either $x \in f(x)$ or $x \notin f(x)$. Let $X = \{x \in A : x \notin f(x)\}$. Notice that $X \in \mathcal{P}(A)$ since $X \subseteq A$. Since f is surjective, there exists $a \in A$ for which $f(a) = X$. Now either $a \in X$ or $a \notin X$. If $a \in X$, then by definition of X this implies that $a \notin f(a)$. But $f(a) = X$ then implies that $a \notin X$, which is a contradiction. If $a \notin X$, then by definition of X this implies that $a \in f(a)$. But $f(a) = X$ then implies that $a \in X$, which is a contradiction. Thus, f is not surjective and hence $|A| < |\mathcal{P}(A)|$. □

3.2.16 Remark. Notice that $|\mathcal{P}(A)| = |2^A|$ and from now onward we will be using them interchangeably.

Now we are familiar with the concept of cardinality of sets. We are going to use this concept to deduce the countability of a given set.

3.3 Cardinality of sets

In this section we will discuss the countability of different sets by considering their cardinality. First let us consider some useful definitions in understanding countability of sets.

3.3.1 Definition. We say that a set is countable if it is in bijection with a subset of the set of natural numbers.

3.3.2 Definition. We say that a set is uncountable if it is not countable, i.e. if it is not in bijection with any subset of the set of natural numbers.

3.3.3 Definition. A set is said to be countably infinite if it can be put in bijection with the set of natural numbers.

3.3.4 Remark. (Hammack, 2013) The cardinality of the natural numbers is $|\mathbb{N}| = \aleph_0$. Any countably infinite set has cardinality $\aleph_0$ and any uncountable set has cardinality greater than $\aleph_0$.

Now we move on with our discussion by proving that the sets of integers and rational numbers are countable. Although they seem to be uncountable but we are going to prove that those sets are countable.

3.3.5 Theorem. *(Hammack, 2013) The set of integers is countably infinite i.e.* $|\mathbb{Z}| = \aleph_0$.

Proof. To prove that the set of integers is countable we need to prove that $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$. To prove that $|\mathbb{Z}| = |\mathbb{N}|$ we need to prove that $|\mathbb{N}| \leq |\mathbb{Z}|$ and $|\mathbb{Z}| \leq |\mathbb{N}|$ by Cantor-Schröder-Bernstein Theorem.

First we prove that $|\mathbb{N}| \leq |\mathbb{Z}|$ by showing that there exists an injection from $\mathbb{N}$ to $\mathbb{Z}$. Let $f : \mathbb{N} \longrightarrow \mathbb{Z}$ be defined by $f(n) = n$, $\forall n \in \mathbb{N}$. Now we need to prove that f is an injection.

Take $n, m \in \mathbb{N}$ such that $f(m) = f(n)$. We need to prove that $m = n$.

By definition of f we have $f(m) = m$ and $f(n) = n$. Then from $f(m) = f(n)$ we have $m = n$ as required. Hence f is an injection and so we have $|\mathbb{N}| \leq |\mathbb{Z}|$.

Lastly we prove that $|\mathbb{Z}| \leq |\mathbb{N}|$ by showing that there exists an injection from $\mathbb{Z}$ to $\mathbb{N}$. Let $g : \mathbb{Z} \longrightarrow \mathbb{N}$ be defined by:

$$g(n) = \begin{cases} 2|n| + 1 & \text{if} \quad n < 0 \\ 2n & \text{if} \quad n > 0 \\ 0 & \text{if} \quad n = 0 \end{cases}$$

Now we are required to show that g is injective.

Take $m, n \in \mathbb{Z}$ such that $g(n) = g(m)$ then we need to show that $n = m$.

Case 1: When both m and n are negative integers i.e $m, n < 0$, we have

$g(n) = 2|n| + 1$ and $g(m) = 2|m| + 1$. But $g(n) = g(m)$. Then we have $2|n| + 1 = 2|m| + 1 \implies |n| = |m| \implies n = m$ as required.

Case 2: When both m and n are positive integers i.e. $m, n > 0$, we have

$g(n) = 2n$ and $g(m) = 2m$. But $g(n) = g(m)$. Then we have $2n = 2m \implies n = m$ as required.

Case 3: When $m = 0$ and $n = 0$ it is trivial that $m = n = 0$ and so we have $m = n$ as required.

Case 4: When $m > 0$ and $n < 0$: For this case we have $m \neq n$ since m is a positive integer and n is a negative integer, so we need to show that $g(m) \neq g(n)$. From the definition of g we have

$g(n) = 2|n| + 1$ and $g(m) = 2m$. Clearly $g(m) \neq g(n)$ as required.

Case 5: When $m > 0$ and $n = 0$: For this case we have $m \neq n$ since m is a positive integer and n is zero, so we need to show that $g(m) \neq g(n)$. From the definition of g we have

$g(n) = 0$ and $g(m) = 2m$. Clearly $g(m) \neq g(n)$ as required.

Case 6: When $m = 0$ and $n < 0$: For this case we have $m \neq n$ since m is zero and n is a negative integer, so we need to show that $g(m) \neq g(n)$. From the definition of g we have

$g(n) = 2|n| + 1$ and $g(m) = 0$. Clearly $g(m) \neq g(n)$ as required.

So g is injective and hence $|\mathbb{Z}| \leq |\mathbb{N}|$.

Since we have shown that $|\mathbb{N}| \leq |\mathbb{Z}|$ and $|\mathbb{Z}| \leq |\mathbb{N}|$ then it follows that, $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$. Therefore, the set of integers is countably infinite. □

3.3.6 Theorem. *(Hammack, 2013) The set of rational numbers is countably infinite i.e. $|\mathbb{Q}| = \aleph_0$.*

Proof. To prove that the set of rational numbers is countably infinite we need to prove that $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$. To prove that $|\mathbb{Q}| = |\mathbb{N}|$ we need to prove that $|\mathbb{N}| \leq |\mathbb{Q}|$ and $|\mathbb{Q}| \leq |\mathbb{N}|$ by Cantor-Schröder-Bernstein Theorem.

First we prove that $|\mathbb{N}| \leq |\mathbb{Q}|$ by showing that there exists an injection from $\mathbb{N}$ to $\mathbb{Q}$. Let $f : \mathbb{N} \longrightarrow \mathbb{Q}$ be defined by $f(n) = n$, $\forall n \in \mathbb{N}$. Now we need to prove that f is an injection.

Take $n, m \in \mathbb{N}$ such that $f(m) = f(n)$ we need to prove that $m = n$.

By definition of f we have $f(m) = m$ and $f(n) = n$. Then from $f(m) = f(n)$ we have $m = n$ as required. Hence f is an injection and so we have $|\mathbb{N}| \leq |\mathbb{Q}|$.

Lastly we prove that $|\mathbb{Q}| \leq |\mathbb{N}|$ by showing that there exists an injection from $\mathbb{Q}$ to $\mathbb{N}$. We know that elements of $\mathbb{Q}$ are of the form $\frac{a}{b}$ with $b \neq 0$. Then for each $q \in \mathbb{Q}$, let $q = \frac{a}{b}$ such that $b > 0$ and $\gcd(a, b) = 1$ where $a, b \in \mathbb{Z}$. Then we define g as follows:

$$g(q) = 2^r 3^s 5^t \quad \forall q \in \mathbb{Q}$$

Where $r = |a|$, $s = b$ and

$$t = \begin{cases} 1 & \text{if} \quad q \geq 0 \\ 0 & \text{if} \quad q < 0 \end{cases}$$

Now we need to prove that g is injective.

Take $p, q \in \mathbb{Q}$ such that $g(p) = g(q)$ where $p = \frac{c}{d}$ such that $d > 0$ and $\gcd(c, d) = 1$ where $c, d \in \mathbb{Z}$ and q as is above. We are required to prove that $p = q$.

Since we know that the factorisation of a natural number into powers of prime numbers is unique, then for $g(p) = g(q)$ we must have $g(p) = 2^r 3^s 5^t$ and $g(q) = 2^r 3^s 5^t$ where $r = |a| = |c|$, $s = b = d$ and

$$t = \begin{cases} 1 & \text{if} \quad q \geq 0 \text{ and } p \geq 0 \\ 0 & \text{if} \quad q < 0 \text{ and } p < 0 \end{cases}$$

Now we have $b = d$ and $|a| = |c|$. When $t = 1$ we have $q \geq 0$ and $p \geq 0$. But $p = \frac{c}{d}$ such that $d > 0$ and $q = \frac{a}{b}$ such that $b > 0$. Thus for $p \geq 0$ we must have $c \geq 0$ and for $q \geq 0$ we must have $a \geq 0$. Since $a \geq 0$, $c \geq 0$ and $|a| = |c|$, then $a = c$. When $t = 0$ we have $q < 0$ and $p < 0$. But $p = \frac{c}{d}$ such that $d > 0$ and $q = \frac{a}{b}$ such that $b > 0$. Thus for $p < 0$ we must have $c < 0$ and for $q < 0$ we must have $a < 0$. Since $a < 0$, $c < 0$ and $|a| = |c|$, then $a = c$. And so we have $a = c$ in both cases. Then we have $\frac{a}{b} = \frac{c}{d}$ implies $q = p$ as required. Therefore g is injective and so we have $|\mathbb{Q}| \leq |\mathbb{N}|$.

Since we have shown that $|\mathbb{N}| \leq |\mathbb{Q}|$ and $|\mathbb{Q}| \leq |\mathbb{N}|$ then it follows that $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$ by Cantor-Schröder-Bernstein Theorem. Therefore, the set of rational numbers is countably infinite. □

Now we know that the set of integer numbers and the set of rational numbers are all countable, as we proved above. In the following discussion we are going to show that there exist sets which are uncountable.

3.3.7 Theorem. *there is a bijection between the closed interval* $[0,1] \subset \mathbb{R}$ *and* $|\mathcal{P}(\mathbb{N})|$.

Proof. To prove that $|[0,1]| = |\mathcal{P}(\mathbb{N})|$ we need to show that $|[0,1]| \leq |\mathcal{P}(\mathbb{N})|$ and $|\mathcal{P}(\mathbb{N})| \leq |[0,1]|$ by Cantor-Schröder-Bernstein Theorem.

First we prove that $|[0,1]| \leq |\mathcal{P}(\mathbb{N})|$ by showing that there exists an injection $f : [0,1] \to \mathcal{P}(\mathbb{N})$. For each $X \in [0,1]$ let $(X_n)_{n\in\mathbb{N}}$ be its binary expansion where we pick the one which ends in $0's$ if applicable. Let $f(X)$ be the set $\{n \in \mathbb{N} : X_n = 1\}$.

Given $X, Y \in [0,1]$ such that $f(X) = f(Y)$. Required to prove that $X = Y$. But $f(X) = \{n \in \mathbb{N} : X_n = 1\}$ and $f(Y) = \{n \in \mathbb{N} : Y_n = 1\}$ by definition of f. Since $f(X) = f(Y)$, this implies that $\{n \in \mathbb{N} : X_n = 1\} = \{n \in \mathbb{N} : Y_n = 1\}$. But $\{n \in \mathbb{N} : X_n = 1\} = \{n \in \mathbb{N} : Y_n = 1\}$ only if $\sum\limits_{n\geq 0} X_n 2^{-(n+1)} = \sum\limits_{n\geq 0} Y_n 2^{-(n+1)}$. This implies that $X = Y$ as required. Therefore we have $|[0,1]| \leq |\mathcal{P}(\mathbb{N})|$.

Now we prove that $|\mathcal{P}(\mathbb{N})| \leq |[0,1]|$ by showing that there exists an injection from $\mathcal{P}(\mathbb{N})$ to $[0,1]$. Mapping a set to its binary expansion gives rise to non-uniqueness if the binary expansion ends in 1's. Hence we separate these cases.

Let $X \subseteq \mathcal{P}(\mathbb{N})$ be the set of subsets that contain a set of the form $\{n : \ n \geq N\}$ for some $N \in \mathbb{N}$.

Now given $A \subseteq \mathbb{N}$, let $(A_n)_{n\in\mathbb{N}}$ be its binary sequence where $A_n = 1$ if $n \in A$ and $A_n = 0$ if $n \notin A$. Then we define $g : \mathcal{P}(\mathbb{N}) \to [0,1]$ as follows:

$$g(A) = \begin{cases} \dfrac{1}{2}\left(\sum\limits_{n\geq 0} A_n 2^{-(n+1)}\right) & \text{if} \quad A \in X \\ \\ \dfrac{3}{4} + \dfrac{1}{4}\left(\sum\limits_{n\geq 0} A_n 2^{-(n+1)}\right) & \text{if} \quad A \notin X \end{cases}$$

Thus, if $A \in X$ then $g(A) \in \left[0, \frac{1}{2}\right]$ which is unique and if $A \notin X$ then $g(A) \in \left[\frac{3}{4}, 1\right]$ which is also unique. Then g is injective. Therefore we have $|\mathcal{P}(\mathbb{N})| \leq |[0,1]|$.

Since we have shown that $|[0,1]| \leq |\mathcal{P}(\mathbb{N})|$ and $|\mathcal{P}(\mathbb{N})| \leq |[0,1]|$ it follows that $|[0,1]| = |\mathcal{P}(\mathbb{N})|$. □

3.3.8 Corollary. (Murphy, James) The set $[0,1] \subset \mathbb{R}$ is uncountable.

Proof. This follows from Theorem 3.3.7 which gives us that $|[0,1]| = |\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| = 2^{\aleph_0}$ by definition and by Theorem 3.2.15 we know that $\mathcal{P}(\mathbb{N}) > |\mathbb{N}|$. It follows that $|[0,1]| > |\mathbb{N}| = \aleph_0$. Thus we have $|[0,1]| > \aleph_0$ and so the set $[0,1] \subset \mathbb{R}$ is uncountable. □

3.3.9 Corollary. The set of real numbers is uncountable.

Proof. This follows from the fact that $[0,1] \subset \mathbb{R}$ and $[0,1]$ is uncountable. Thus $\mathbb{R}$ is uncountable. □

3.3.10 Theorem. $|\mathbb{R}| = 2^{\aleph_0}$.

Proof. Theorem 3.3.7 tells us that $|[0,1]| = |\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| = 2^{\aleph_0}$. Then to prove that $|\mathbb{R}| = 2^{\aleph_0}$ we need to prove that $|\mathbb{R}| = |[0,1]|$. Thus we need to show that $|[0,1]| \leq |\mathbb{R}|$ and $|\mathbb{R}| \leq |[0,1]|$ by Cantor-Schröder-Bernstein Theorem.

First we prove that $|[0,1]| \leq |\mathbb{R}|$. Since we know that $|[0,1]| \subset |\mathbb{R}|$ it follows that $|[0,1]| \leq |\mathbb{R}|$.

Now we prove that $|\mathbb{R}| \leq |[0,1]|$ by showing that there exists an injection $f : \mathbb{R} \to [0,1]$. For all $x \in \mathbb{R}$ let $f(x)$ be defined as follows:

$$f(x) = \frac{1}{\pi}\cot^{-1}(x).$$

Now we need to prove that f injective.

Let $a, b \in \mathbb{R}$ such that $f(a) = f(b)$. We are required to prove that $a = b$.

Since $f(a) = f(b)$ we have $\frac{1}{\pi}\cot^{-1}(a) = \frac{1}{\pi}\cot^{-1}(b)$, implies $\cot^{-1}(a) = \cot^{-1}(b)$, which in turn, implies $a = b$ as required.Thus f is injective.

Therefore we have $|\mathbb{R}| \leq |[0,1]|$.

Thus $|\mathbb{R}| = 2^{\aleph_0}$. □

3.3.11 Remark. The Continuum Hypothesis (CH) states that there is no set that has cardinality which is strictly between the cardinalities of the set of natural numbers and the set of real numbers i.e. there is no κ such that $\aleph_0 < \kappa < 2^{\aleph_0}$, which implies $2^{\aleph_0} = \aleph_1$. The Generalised Continuum Hypothesis (GCH) states that $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$ for all ordinals α. Using this, we get that $\aleph_1 = 2^{\aleph_0}$ for $\alpha = 0$ which is the CH. Then from Theorem 3.3.10 we have $|\mathbb{R}| = \aleph_1$. The CH cannot be proved in ZFC but CH (and in fact GCH) is consistent with ZFC (provided that ZFC is consistent), but not CH is also consistent.

4. Application.

In this section we are going to use ordinals to prove that Goodstein sequences terminate to zero. "Goodstein sequences were introduced by the British logician R. L. Goodstein in 1944" (Klein). These sequences initially increase so rapidly that it can lead someone to believe that they tend to infinity, but in this section we will use ideas of ordinals to prove that they terminate to zero in a finite number of steps.

Before we prove this fact, first we introduce the weak Goodstein sequences.

4.1 Weak Goodstein sequences.

These are sequences where we choose an arbitrary natural number u_0 as a starting value and we express it in base 2 e.g. $u_0 = 2^6 + 2^5 + 2^4 + 2^3 + 2^1 = 122$. Then to obtain the next term of the sequence we use the same representation as u_0 but we change the base of the powers from 2 to 3 and then we subtract 1 e.g. $u_1 = 3^6 + 3^5 + 3^4 + 3^2 + 3^1 - 1 = 3^6 + 3^5 + 3^4 + 3^2 + 2 = 1082$. Continuing with this process of changing the base of the powers of the previous representation from the previous integer to the next large integer and subtracting 1 we obtain the following.

$u_0 = 2^6 + 2^5 + 2^4 + 2^3 + 2^1 = 122.$

$u_1 = 3^6 + 3^5 + 3^4 + 3^3 + 3^1 - 1 = 3^6 + 3^5 + 3^4 + 3^3 + 2 = 1082.$

$u_2 = 4^6 + 4^5 + 4^4 + 4^3 + 2 - 1 = 4^6 + 4^5 + 4^4 + 4^3 + 1 = 5441.$

$u_3 = 5^6 + 5^5 + 5^4 + 5^3 + 1 - 1 = 5^6 + 5^5 + 5^4 + 5^3 = 19500.$

$u_4 = 6^6+6^5+6^4+6^3-1 = 6^6+6^5+6^4+6^2\cdot5+6^1\cdot5+6-1 = 6^6+6^5+6^4+6^2\cdot5+6^1\cdot5+5 = 55943.$

$\vdots$

It appears terms grow quickly and indefinitely. In fact it is not so but rather they converge to zero.

For example consider $u_0 = 1$, then $u_1 = 1 - 1 = 0$, so in this case we see that the sequence converges to zero in 1 step.

If $u_0 = 2 = 2^1$, then $u_1 = 3^1 - 1 = 2$, $u_2 = 2 - 1 = 1$, $u_3 = 1 - 1 = 0$. Also for this case we observe that the sequence terminates to zero in 3 steps.

For $u_0 = 3$ the sequence terminates in 5 steps, for $u_0 = 4$ the sequence terminates in 21 steps.

As we increase the value of u_0 the number of steps in which the sequence terminates seems to increase rapidly.

Now we associate each weak Goodstein sequence to a sequence of ordinals by replacing each base of each term by ω and we obtain the following sequence of ordinals, for $u_0 = 122$.

$\alpha_0 = \omega^6 + \omega^5 + \omega^4 + \omega^3 + \omega^1.$

$\alpha_1 = \omega^6 + \omega^5 + \omega^4 + \omega^3 + 2.$

$\alpha_2 = \omega^6 + \omega^5 + \omega^4 + \omega^3 + 1.$

$\alpha_3 = \omega^6 + \omega^5 + \omega^4 + \omega^3.$

$\alpha_4 = \omega^6 + \omega^5 + \omega^4 + \omega^2 \cdot 5 + \omega^1 \cdot 5 + 5.$

$\vdots$

We claim that the ordinals sequence we constructed above is a strictly decreasing sequence i.e for each n, $\alpha_{n+1} < \alpha_n$.

Proof. Notice that α_n and α_{n+1} are in CNF because u_n and u_{n+1} are in 'normal form' with base $n+2$ and $n+3$ respectively. Then by Corollary 2.3.20 (padding with 0's if necessary) we have $\alpha_{n+1} < \alpha_n$ for each n.Therefore the ordinals sequence is a strictly decreasing sequence. □

Now since we have a strictly decreasing sequence of ordinals we use the following Theorem to prove that our weak Goodstein sequence converges to zero.

4.1.1 Theorem. *There cannot be an infinitely long strictly decreasing sequence of ordinals.*

Proof. Suppose that there is an infinitely long strictly decreasing sequence of ordinals. Let $S = \{\alpha_0, \alpha_1, \alpha_2, \alpha_3, \ldots\}$ be the set of all terms of the sequence. Since the class of ordinals is well-ordered by the proof of Theorem 2.1.12, this non-empty subset has a least element α_n for some $n \in \mathbb{N}$. But since the sequence is strictly decreasing, we have $\alpha_{n+1} < \alpha_n$. This contradicts the minimality of α_n. Therefore there cannot be an infinitely long strictly decreasing sequence of ordinals. □

Theorem 4.1.1 tells us that sequence of ordinals must terminate at a finite term α_k for some $k \in \mathbb{N}$. This means that the weak Goodstein sequence has to stop. It won't stop unless $u_k = 0$ for some $k \in \mathbb{N}$. Since k is finite it means that weak Goodstein sequences converge to zero at a finite number of steps.

4.1.2 Remark. Although for some value of u_0 this number of steps can be a very large number but still the sequence converges to zero at a finite number of steps.

After understanding the weak Goodstein sequences we move on and discuss about the Goodstein sequences.

4.2 Goodstein sequences.

Goodstein sequences are slightly different from the weak Goodstein sequences but the terms in the Goodstein sequences increase quickly because of the way they are defined. For weak Goodstein sequences in which we considered our staring value to be 122 we have $u_0 = 2^6 + 2^5 + 2^4 + 2^3 + 2^1 = 122$. To obtain the Goodstein sequence for this particular example of weak Goodstein sequence we use hereditary base q notation where by we change each exponent of each power to be a power of base not exceeding 2 and rewrite the result i.e $6 = 2^2 + 2$, $5 = 2^2 + 1$, $4 = 2^2$ and $3 = 2 + 1$. Then we have $m_0 = 2^{2^2+2} + 2^{2^2+1} + 2^{2^2} + 2^{2+1} + 2^1 = 122$. To obtain the next term we use the same technique as in the weak Goodstein sequence. We replace each base 2 by 3, then we subtract 1. Continuing the same way by replacing each base by the next large number and subtracting 1 we obtain the following.

$m_0 = 2^{2^2+2} + 2^{2^2+1} + 2^{2^2} + 2^{2+1} + 2^1 = 122.$

$m_1 = 3^{3^3+3} + 3^{3^3+1} + 3^{3^3} + 3^{3+1} + 3^1 - 1 = 3^{3^3+3} + 3^{3^3+1} + 3^{3^3} + 3^{3+1} + 2 = 236393522034680.$

$m_2 = 4^{4^4+4} + 4^{4^4+1} + 4^{4^4} + 4^{4+1} + 1 \approx 10^{157}.$

$m_3 = 5^{5^5+5} + 5^{5^5+1} + 5^{5^5} + 5^{5+1} \approx 10^{2188}.$

$m_4 = 6^{6^6+6} + 6^{6^6+1} + 6^{6^6} + 6^5 \cdot 5 + 6^4 \cdot 5 + 6^3 \cdot 5 + 6^2 \cdot 5 + 6^1 \cdot 5 + 5 \approx 10^{36311}$.

$\vdots$

Again here the terms increase quickly as we increase the number of steps and we even got a very big number at the first step. One can believe that in this case we must diverge to infinity, but still we can convince you that this sequence converges to zero at a finite number of steps. As in weak Goodstein sequences we associate each term of the Goodstein sequence to an ordinal by replacing each base by ω. We obtain the following sequence.

$\beta_0 = \omega^{\omega^\omega+\omega} + \omega^{\omega^\omega+1} + \omega^{\omega^\omega} + \omega^{\omega+1} + \omega^1$.

$\beta_1 = \omega^{\omega^\omega+\omega} + \omega^{\omega^\omega+1} + \omega^{\omega^\omega} + \omega^{\omega+1} + 2$.

$\beta_2 = \omega^{\omega^\omega+\omega} + \omega^{\omega^\omega+1} + \omega^{\omega^\omega} + \omega^{\omega+1} + 1$.

$\beta_3 = \omega^{\omega^\omega+\omega} + \omega^{\omega^\omega+1} + \omega^{\omega^\omega} + \omega^{\omega+1}$.

$\beta_4 = \omega^{\omega^\omega+\omega} + \omega^{\omega^\omega+1} + \omega^{\omega^\omega} + \omega^5 \cdot 5 + \omega^4 \cdot 5 + \omega^3 \cdot 5 + \omega^2 \cdot 5 + \omega^1 \cdot 5 + 5$.

$\vdots$

Here again we claim that the ordinals sequence obtained above is a strictly decreasing sequence i.e for each β_n, $\beta_{n+1} < \beta_n$. And to prove the claim we use the similar argument that we have used to prove the claim for α_n.

Now since we have a strictly decreasing sequence of ordinals, using the same argument as in weak Goostein sequences and Theorem 4.1.1 we conclude that Goodstein sequences converge to zero at a finite number of steps. But unlike weak Goodstein sequences, Goodstein sequences can have much more large number of steps but it still will be finite.

Therefore we use the same argument to conclude that any Goodstein sequence converges to zero at a finite number of steps.

4.2.1 Remark. The fact that weak Goodstein sequences converge to zero can be proved by Peano arithmetic. But the fact that Goodstein sequences converge to zero cannot be proved by Peano arithmetic as in the year 1982 "Laurie Kirby and Jeff Paris showed that if convergence could be proved using only the well-ordering principle for the integers (i.e. within Peano arithmetic), then the theorem about Goodstein sequences could be reduced to a theorem of Gentzen (1936), from which the consistency of Peano arithmetic could be deduced. But we know from the Gödel incompleteness theorem (1931) that the consistency of Peano arithmetic cannot be proved using only Peano arithmetic" (Klein). Therefore it is difficult to prove that Goodstein sequences converge to zero without using transfinite ordinals.

Appendix A. ZFC Axioms

"ZFC is the acronym for Zermelo-Fraenkel set theory with the axiom of choice, formulated in first-order logic. ZFC is the basic axiom system for modern set theory, regarded both as a field of mathematical research and as a foundation for ongoing mathematics" (Encyclopedia of Mathematics, b). These axioms give rules of construction for sets.

The ZFC axioms are as follows and are taken from Encyclopedia of Mathematics (b).

1. Axiom of empty set:
$$\exists x(\forall y(y \notin x)).$$

2. Axiom of power set:
$$\forall x \exists y \forall z(z \in y \leftrightarrow \forall t(t \in z \to t \in x)).$$

3. Axiom of union:
$$\forall x \exists y \forall z(z \in y \leftrightarrow \exists t(t \in x \wedge z \in t)).$$

4. Axiom of pairs:
$$\forall x \forall y \exists z \forall t(t \in z \leftrightarrow (t = x \vee t = y)).$$

5. Axiom of extensionality:
$$\forall x \forall y(\forall z(z \in x \leftrightarrow z \in y) \to x = y).$$

6. Axiom of separation:

   For any first-order formula $p(t, t_1, \ldots, t_n)$, in the language of set theory, with free variables among $t_1, \ldots, t_n$ and t,
$$\forall t_1 \ldots t_n \forall x \exists y \forall t(t \in y \leftrightarrow (t \in x \wedge p(t, t_1, \ldots, t_n))).$$

7. Axiom of foundation:
$$\forall x((x \neq \emptyset) \to \exists y(y \in x \wedge \forall z(z \in x \to z \notin y))).$$

8. Axiom of infinity:
$$\exists y(\emptyset \in y \wedge \forall x(x \in y \to x \cup \{x\} \in y)).$$

9. Axiom of replacement:

   For any first-order formula $p(x_1, x_2, t_1, \ldots, t_n)$, in the language of set theory, in free variables among $t_1, \ldots, t_n$ and x,
$$\forall t_1, \ldots, \forall t_n \exists y(\forall r \forall s \forall s'(p(r, s, t_1, \ldots, t_n) = p(r, s', t_1, \ldots, t_n) \to s = s'))$$
$$\to (w \in y \leftrightarrow \exists z(z \in x : p(z, w, t_1, \ldots, t_n))).$$

10. Axiom of choice:
$$\forall x \forall v \forall w(((v \in x \wedge w \in x) \wedge \exists t(t \in v \wedge t \in w)) \to v = w)$$
$$\to \exists y \exists v((v \in x \wedge (v \neq \emptyset)) \to \exists s \forall t((t \in v \wedge t \in y) \leftrightarrow s = t)).$$

It is well-known that the axiom of choice is equivalent to the well-ordering principle.

A.1.2 Theorem (Well-ordering principle)**.** *Every set can be well-ordered.*

Acknowledgements

First of all I would like to thank God almighty for helping me to reach this far in my studies, it is not by my abilities and powers but it is by His grace and mercy. I would like to thank my supervisor: **Dr Gareth Boxall** and my co-supervisor: **Georg Anegg** for their strong support and help towards the completion of this project. Also I would like to thank my family members for their prayers to me in my studies. Finally I would like to thank the staff at AIMS and everyone at AIMS for their cooperation and support during my stay here in AIMS.

References

Anon. Lecture 4 supplement: detailed proof. CS2008, http://www.cs.cornell.edu/courses/cs2800/2017sp/lectures/lec05-cantor.html, Accessed April 2017.

G. Boxall. Model Theory Notes, 2016. Unpublished manuscript.

G. Boxall. Ordinal and Cardinal, 2017. Unpublished manuscript.

Don Monk. 6. cardinals. Chapter 6. Cardinals, http://euclid.colorado.edu/~monkd/m6730/gradsets06.pdf, Accessed February 2017a.

Don Monk. 4. ordinals. Chapter 4. Ordinals, http://euclid.colorado.edu/~monkd/m6730/gradsets04.pdf, Accessed February 2017b.

Don Monk. Properties of ordinals. Properties of ordinals-PlanetMath, http://euclid.colorado.edu/~monkd/m6730/gradsets06.pdf, Accessed January 2017c.

Edward. Ordinal numbers. The Ordinal Numbers and Transfinite Induction, http://www.math.purdue.edu/~price79/OrdinalNumbers.pdf, Accessed April 2017.

Encyclopedia of Mathematics. Order type. Encyclopedia of Mathematics, https://www.encyclopediaofmath.org/index.php/Order_type, Accessed May 2017a.

Encyclopedia of Mathematics. ZFC. Encyclopedia of Mathematics, https://www.encyclopediaofmath.org/index.php/ZFC, Accessed May 2017b.

Gabriel Lehéricy. Ordinal numbers. Ordinal numbers, http://www.math.uni-konstanz.de/~lehericy/Ordinals.pdf, Accessed February 2017.

R. H. Hammack. Cardinality of Sets. In L. Mitchell, editor, *Book of proof*, pages 202–214,267. Richard Hammack, Richmond, Virginia, 23284, 2013.

I. B. Leader. Logic and set theory. Logic and Set Theory, https://tartarus.org/gareth/maths/notes/ii/Logic_and_Set_Theory.pdf, Accessed January 2017.

Klein. Goodstein Sequences: The Power of a Detour via Infinity. Wikipedia, the Free Encyclopedia, http://blog.kleinproject.org/?p=674, Accessed April 2017.

Murphy, James. CARDINAL AND ORDINAL NUMBERS. Cardinal and ordinal numbers-University of Chicago Math, http://www.math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Murphy.pdf, Accessed January 2017.

Rahim Moosa. Set Theory and Model Theory VERSION 2. Set theory and model theory lecture notes, http://www.math.uwaterloo.ca/~rmoosa/modeltheory-notes.pdf, Accessed May 2017.

Wikipedia. Order type. Wikipedia, the Free Encyclopedia, https://en.wikipedia.org/wiki/Order_type, Accessed April 2017a.

Wikipedia. Ordinal number. Wikipedia, the Free Encyclopedia, https://en.wikipedia.org/wiki/Ordinal_number, Accessed April 2017b.

Wikipedia. Cardinal number. Wikipedia, the Free Encyclopedia, https://en.wikipedia.org/wiki/Cardinal_number, Accessed April 2017c.