Elementary Set Theory

Xianghui Shi

School of Mathematical Sciences
Beijing Normal University

Fall 2024

Overview

- Orderings: partial, total
- Well-Ordering: order-type
- Ordinal numbers, natural numbers

Overview

- Orderings: partial, total
- Well-Ordering: order-type
- Ordinal numbers, natural numbers

Overview

- Orderings: partial, total
- Well-Ordering: order-type
- Ordinal numbers, natural numbers

Overview

- Orderings: partial, total
- Well-Ordering: order-type
- Ordinal numbers, natural numbers

  Theorem. *Every well-ordered set is uniquely isomorphic to an ordinal number.*

Overview

- Orderings: partial, total
- Well-Ordering: order-type
- Ordinal numbers, natural numbers

  Theorem. *Every well-ordered set is uniquely isomorphic to an ordinal number.*
- **Transfinite induction and transfinite recursion**

Overview

- Orderings: partial, total
- Well-Ordering: order-type
- Ordinal numbers, natural numbers

  Theorem. *Every well-ordered set is uniquely isomorphic to an ordinal number.*
- **Transfinite induction and transfinite recursion**
- **Ordinal arithmetic: Cantor's Normal Form**

Coming up next

Orderings

Definition 1

A binary relation $<$ on a set P is a **partial ordering** (or **partially ordered set**, poset) of P if for any $p, q, r \in P$,

1. (irreflexive) $\quad p \not< p$;
2. (transitive) $\quad p < q \wedge q < r \rightarrow p < r$.

$(P, <)$ is called a **partial order**. Define $\leq$ as

$$p \leq q \quad \iff \quad p < q \vee p = q$$

$(P, \leq)$ is reflexive and transitive. It is called a **preorder**. Partial orders are **strict** preorders.

Orderings

Definition 1

A binary relation $<$ on a set P is a **partial ordering** (or **partially ordered set**, poset) of P if for any $p, q, r \in P$,

1. (irreflexive) $p \not< p$;
2. (transitive) $p < q \wedge q < r \to p < r$.

$(P, <)$ is called a **partial order**. Define $\leq$ as

$$p \leq q \iff p < q \vee p = q$$

$(P, \leq)$ is reflexive and transitive. It is called a **preorder**. Partial orders are **strict** preorders.

A partial ordering $<$ of P is a **linear ordering** (or **total ordering** if moreover for any $p, q \in P$,

3. (trichotomous) $p < q \vee p = q \vee q < p$.

Max-N-Mins

Definition 2

If $(P, <)$ is a poset, $\varnothing \neq X \subseteq P$ and $a \in P$, then:

- a is a **maximal** element of X if $a \in X$ and
$$\forall x \in X\,(a \not< x)$$
- a is a **minimal** element of X if $a \in X$ and
$$\forall x \in X\,(x \not< a)$$
- a is a **greatest** element of X if $a \in X$ and
$$\forall x \in X\,(x \leq a)$$
- a is a **least** element of X if $a \in X$ and
$$\forall x \in X\,(a \leq x)$$

Max-N-Mins

Definition 2 (Cont'd)

- a is a **upper bound** of X if $\forall x \in X\ (x \leq a)$.
- a is a **lower bound** of X if $\forall x \in X\ (a \leq x)$.
- a is a **supremum** of X, $\sup(X)$, if a is the least upper bound of X.
- a is a **infimum** of X, $\inf(X)$, if a is the greatest lower bound of X.

Max-N-Mins

The following remarks apply to their counterparts as well.

- "Greatest" $\implies$ "Maximal".
- "Greatest" is unique, if exists.
- "Maximal" is not necessary unique, unless $(X, <)$ is linear.
- "Upper bound" and "Supremum" refer to elements outside X.

Max-N-Mins

- "Upper bound" may not exists. If not, X is **unbounded** in P.
- $\sup(X)$ may not exists, even when upper bounds exist. If exists, it must be unique.
- When "Greatest" exists,

$$\text{"Greatest"} = \text{"Supremum".}$$

- If X is linear and "Maximal" exists,

$$\text{"Greatest"} = \text{"Maximal"} = \text{"Supremum".}$$

Order-Preserving Function

Definition 3

If $(P, <_P)$ and $(Q, <_Q)$ are posets and $f : P \to Q$, then f is **order-preserving** if $\forall x, y \in P\,(x <_P y \to f(x) <_Q f(y))$.

- An order-preserving function is a **monomorphism**.

Order-Preserving Function

Definition 3

If $(P, <_P)$ and $(Q, <_Q)$ are posets and $f : P \to Q$, then f is **order-preserving** if $\forall x, y \in P\, (x <_P y \to f(x) <_Q f(y))$.

- An order-preserving function is a **monomorphism**.
- If P and Q are linear, then an order-preserving function is also called **increasing**.

Order-Preserving Function

Definition 4

- A bijection $f : P \to Q$ is an **isomorphism** of P and Q if
$$\forall x, y \in P\, (x <_P y \longleftrightarrow f(x) <_Q f(y)).$$
- An isomorphism of P onto itself is an **automorphism** of $(P, <)$.

Order-Preserving Function

Definition 4

- A bijection $f : P \to Q$ is an **isomorphism** of P and Q if
$$\forall x, y \in P\, (x <_P y \longleftrightarrow f(x) <_Q f(y)).$$
- An isomorphism of P onto itself is an **automorphism** of $(P, <)$.

If two orderings are isomorphic, we say they have the same **order-type**.

Coming up next

Well-Ordering

Definition 5

We say $(P, <)$ is a **well-ordering**, or $<$ **well-orders** P, if $(P, <)$ is a linear ordering and every nonempty subset of P has a least element.

Well-Ordering

Definition 5

We say $(P, <)$ is a **well-ordering**, or $<$ **well-orders** P, if $(P, <)$ is a linear ordering and every nonempty subset of P has a least element.

The notion of well-orderings gives us a convenient way of stating an equivalent version of the Axiom of Choice (AC).

Axiom 9 (Choice)

$$\forall X \exists R\, (R \text{ well-orders } X).$$

Properties of Well-Orderings

Proposition 6

- *If* $(W, <)$ *is a well ordering and* $U \subset W$*, then* $(U, < \cap (U \times U))$ *is a well ordering.*
- *If* $(W_1, <_1)$ *and* $(W_2, <_2)$ *are two well orderings and* $W_1 \cap W_2 = \varnothing$*, then* $W_1 \oplus W_2 = (W_1 \cup W_2, \prec)$ *is a well ordering, where*

$$\prec \; = \; <_1 \cup <_2 \cup \{(a, b) \mid a \in W_1 \wedge b \in W_2\}$$

- *If* $(W_1, <_1)$ *and* $(W_2, <_2)$ *are two well orderings, then* $W_1 \otimes W_2 = (W_1 \times W_2, \prec)$ *is a well ordering, where*

$$(a_1, b_1) \prec (a_2, b_2) \leftrightarrow b_1 <_2 b_2 \vee (b_1 = b_2 \wedge a_1 <_1 a_2).$$

Plan

Things to do:

- Well-ordered sets can be compared by their lengths.
- In fact, the class of all well-orderings can be (non-strictly) well-ordered.
- Ordinal numbers will be introduced as order-types of well-ordered sets.

A Lemma

Lemma 7

If $(W, <)$ *is a well-ordered set and* $f : W \to W$ *is an increasing function, then* $f(x) \geq x$ *for each* $x \in W$*.*

A Lemma

Lemma 7

If $(W, <)$ is a well-ordered set and $f : W \to W$ is an increasing function, then $f(x) \geq x$ for each $x \in W$.

PROOF.

Suppose NOT. Consider z, the least element of

$$S_f = \{x \in W \mid f(x) < x\}.$$

$f(z) < z \implies f(z) \notin S_f \implies f^2(z) \geq f(z)$. But f is increasing, $f(z) < z \implies f^2(z) < f(z)$, Contradiction! □

The converse to this lemma holds for countable linear ordering.

Theorem

Let W be a countable linear ordering and suppose that for every function $f : W \to W$,

if f is order-preserving, then $f(x) \geq x$ for every $x \in W$.

Then W is a well ordering.[1]

[1] Reference: Rosenstein, Joseph G. *Linear orderings*. Pure and Applied Mathematics, 98. Academic Press, Inc. New York-London, 1982. xvii+487 pp.

The converse to this lemma holds for countable linear ordering.

Theorem

Let W be a countable linear ordering and suppose that for every function $f : W \to W$,

if f is order-preserving, then $f(x) \geq x$ for every $x \in W$.

Then W is a well ordering.[1]

NOTATION: Fix a well-ordered set $(W, <)$. For $x \in W$, let

$$W_x = \{y \in W \mid y < x\}.$$

It can be well-ordered by $<_x \equiv < \cap (W_x \times W_x)$.

[1] Reference: Rosenstein, Joseph G. *Linear orderings*. Pure and Applied Mathematics, 98. Academic Press, Inc. New York-London, 1982. xvii+487 pp.

Corollaries

Corollary 8

If $(W, <)$ *is a well-ordering, then for all* $x \in W$*,*

$$(W, <) \not\cong (W_x, <_x).$$

Corollaries

Corollary 8

If $(W, <)$ *is a well-ordering, then for all* $x \in W$*,*

$$(W, <) \not\cong (W_x, <_x).$$

PROOF.

Suppose NOT. Let $f : W \to W_x$ be an isomorphism. Then $f(x) < x$, contradicting Lemma 7. □

Corollaries

Corollary 9

If $f : W \to W$ *is an automorphism, then* $f = \mathrm{id}$.

Corollaries

Corollary 9

If $f : W \to W$ *is an automorphism, then* $f = \mathrm{id}$.

Corollary 10

If W_1 *and* W_2 *are isomorphic well-orderings and* $f, g : W_1 \to W_2$ *are two isomorphisms, then*

$$f \circ g^{-1} = \mathrm{id}_{W_2} \text{ and } g^{-1} \circ f = \mathrm{id}_{W_1}.$$

Thus $f = g$.

Corollaries

Corollary 9

If $f : W \to W$ is an automorphism, then $f = \mathrm{id}$.

The point is that f^{-1} is order-preserving as well.

Corollary 10

If W_1 and W_2 are isomorphic well-orderings and $f, g : W_1 \to W_2$ are two isomorphisms, then

$$f \circ g^{-1} = \mathrm{id}_{W_2} \text{ and } g^{-1} \circ f = \mathrm{id}_{W_1}.$$

Thus $f = g$.

Theorem 11

We have shown that

- No well-ordered set is isomorphic to an initial segment of itself.
- If W_1 and W_2 are isomorphic well-orderings, then the isomorphism between them is unique.

Theorem 11

These lead to

Theorem 11

Let $(U, <_U)$ and $(V, <_V)$ be two well-orderings. Then exactly one of the following holds:

1. $(U, <_U) \cong (V, <_V)$;
2. $(U, <_U) \cong (V_y, (<_V)_y)$, *for some* $y \in V$;
3. $(U_x, (<_U)_x) \cong (V, <_V)$, *for some* $x \in U$.

PROOF.

Let $$f = \{(x, y) \mid x \in U \land y \in V \land (U_x, (<_U)_x) \cong (V_y, (<_V)_y)\}$$

PROOF.

Let $$f = \{(x, y) \mid x \in U \wedge y \in V \\ \wedge (U_x, (<_U)_x) \cong (V_y, (<_V)_y)\}$$

Note that

CLAIM. f *is an isomorphism from some initial segment of* U *onto some initial segment of* V.

Proof.

Let $$f = \{(x, y) \mid x \in U \wedge y \in V \wedge (U_x, (<_U)_x) \cong (V_y, (<_V)_y)\}$$

Note that

Claim. *f is an isomorphism from some initial segment of U onto some initial segment of V.*

Claim. *These initial segments cannot both be proper.*

PROOF.

Let $$f = \{(x,y) \mid x \in U \wedge y \in V \wedge (U_x, (<_U)_x) \cong (V_y, (<_V)_y)\}$$

Note that

CLAIM. *f is an isomorphism from some initial segment of U onto some initial segment of V.*

CLAIM. *These initial segments cannot both be proper.*

Otherwise, let

$$x_f = \min(U - \mathrm{dom}(f)), \quad y_f = \min(V - \mathrm{ran}(f)).$$

Then $(x_f, y_f) \in f$. Contradiction! □

Homework

1. Show that the function f given in the proof of Theorem 11 is an isomorphism.
2. The relation "$(P, <) \cong (Q, <)$" is an equivalence relation (on the class of all partially ordered sets).
3. Let $\mathcal{A}$ denote the class of all well orderings. For any $a, b \in \mathcal{A}$,
$$[a]_{\cong} \prec [b]_{\cong} \quad \text{iff} \quad a \cong b_x \text{ for some } x \in b.$$
Show that $\prec$ is (well defined and) a well ordering on $\mathcal{A}/_{\cong}$, where $\cong$ is the equivalence relation given as above.
4. Prove Proposition 6.

Coming up next

Ordinal

Motivation

- The class of well-ordered sets is partitioned into equivalence classes.

Ordinal

Motivation

- The class of well-ordered sets is partitioned into equivalence classes.
- A typical well-ordered set, an **ordinal**, is selected from each equivalence class to represent the corresponding order-type.

Ordinal

Motivation

- The class of well-ordered sets is partitioned into equivalence classes.
- A typical well-ordered set, an **ordinal**, is selected from each equivalence class to represent the corresponding order-type.
- Some criteria for defining ordinals:

Ordinal

Motivation

- The class of well-ordered sets is partitioned into equivalence classes.
- A typical well-ordered set, an **ordinal**, is selected from each equivalence class to represent the corresponding order-type.
- Some criteria for defining ordinals:
    1. $\alpha < \beta$ iff $(\beta, <_\beta)$ is longer than $(\alpha, <_\alpha)$.

Ordinal

Motivation

- The class of well-ordered sets is partitioned into equivalence classes.
- A typical well-ordered set, an **ordinal**, is selected from each equivalence class to represent the corresponding order-type.
- Some criteria for defining ordinals:
  1. $\alpha < \beta$ iff $(\beta, <_\beta)$ is longer than $(\alpha, <_\alpha)$.
  2. The class of all ordinals, Ord, is well-ordered by $<$.

Ordinal

Motivation

- The class of well-ordered sets is partitioned into equivalence classes.
- A typical well-ordered set, an **ordinal**, is selected from each equivalence class to represent the corresponding order-type.
- Some criteria for defining ordinals:
  1. $\alpha < \beta$ iff $(\beta, <_\beta)$ is longer than $(\alpha, <_\alpha)$.
  2. The class of all ordinals, Ord, is well-ordered by $<$.
  3. The definition of $<$ and $<_\alpha$ should be as simple as possible.

Ordinal

Motivation

Von Neumman's Solution.

$$\alpha < \beta \quad \text{iff} \quad \alpha \in \beta.$$

Ordinal

Motivation

Von Neumman's Solution.

$$\alpha < \beta \quad \text{iff} \quad \alpha \in \beta.$$

First, $0 = \varnothing$.

Ordinal

Motivation

Von Neumman's Solution.

$$\alpha < \beta \quad \text{iff} \quad \alpha \in \beta.$$

First, $0 = \varnothing$. By criteria-2.,

$$1 = \{\varnothing\},$$

Ordinal

Motivation

Von Neumman's Solution.

$$\alpha < \beta \quad \text{iff} \quad \alpha \in \beta.$$

First, $0 = \varnothing$. By criteria-2.,

$$\begin{aligned} 1 &= \{\varnothing\}, \\ 2 &= \{\varnothing, \{\varnothing\}\} = 1 \cup \{1\}, \end{aligned}$$

Ordinal

Motivation

VON NEUMMAN'S SOLUTION.

$$\alpha < \beta \quad \text{iff} \quad \alpha \in \beta.$$

First, $0 = \varnothing$. By criteria-2.,

$$\begin{aligned} 1 &= \{\varnothing\}, \\ 2 &= \{\varnothing, \{\varnothing\}\} = 1 \cup \{1\}, \\ 3 &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = 2 \cup \{2\}, \end{aligned}$$

Ordinal

Motivation

Von Neumman's Solution.

$$\alpha < \beta \quad \text{iff} \quad \alpha \in \beta.$$

First, $0 = \varnothing$. By criteria-2.,

$$\begin{aligned} 1 &= \{\varnothing\}, \\ 2 &= \{\varnothing, \{\varnothing\}\} = 1 \cup \{1\}, \\ 3 &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = 2 \cup \{2\}, \\ \cdots & \quad \cdots \quad \cdots \quad \cdots \end{aligned}$$

Ordinal

Definition

Definition 12

A set T is **transitive** if $\forall x(x \in T \to x \subseteq T)$.

EXAMPLES. $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$ and $\{\{\{\varnothing\}\}, \{\varnothing\}, \varnothing\}$ are transitive.

Definition 12

A set T is **transitive** if $\forall x(x \in T \to x \subseteq T)$.

Examples. $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$ and $\{\{\{\varnothing\}\}, \{\varnothing\}, \varnothing\}$ are transitive.

Homework

Show that the following are equivalent:

a. T is transitive;

b. $\bigcup T \subseteq T$;

c. $T \subseteq \mathscr{P}(T)$.

Definition 12

A set T is **transitive** if $\forall x(x \in T \to x \subseteq T)$.

Examples. $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$ and $\{\{\{\varnothing\}\}, \{\varnothing\}, \varnothing\}$ are transitive. $\{\{\varnothing\}\}$ is not.

Homework

Show that the following are equivalent:

a. T is transitive;

b. $\bigcup T \subseteq T$;

c. $T \subseteq \mathscr{P}(T)$.

Ordinal

Definition 13

A set is an **ordinal (number)** if it is transitive and well-ordered by $\in$.

Ordinal

Definition 13

A set is an **ordinal (number)** if it is transitive and well-ordered by $\in$.

More formally, the assertion that x is well-ordered by $\in$ means that $(x, \in_x)$ is a well-ordering, where $\in_x \equiv \in \cap (x \times x)$. We often drop the subscript in $\in_x$.

Ordinal

Definition 13

A set is an **ordinal (number)** if it is transitive and well-ordered by $\in$.

More formally, the assertion that x is well-ordered by $\in$ means that $(x, \in_x)$ is a well-ordering, where $\in_x \equiv \in \cap (x \times x)$. We often drop the subscript in $\in_x$.

EXAMPLE. $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$ are ordinals, whereas $\{\{\{\varnothing\}\}, \{\varnothing\}, \varnothing\}$ (not $\in$-well-ordered) and $\{\{\varnothing\}\}$ (not transitive) are not.

Ordinal

Definition 13

A set is an **ordinal (number)** if it is transitive and well-ordered by $\in$.

More formally, the assertion that x is well-ordered by $\in$ means that $(x, \in_x)$ is a well-ordering, where $\in_x \equiv \in \cap (x \times x)$. We often drop the subscript in $\in_x$.

EXAMPLE. $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$ are ordinals, whereas $\{\{\{\varnothing\}\}, \{\varnothing\}, \varnothing\}$ (not $\in$-well-ordered) and $\{\{\varnothing\}\}$ (not transitive) are not. If $x = \{x\}$, then x is transitive, but $x \notin \mathrm{Ord}$.

Ordinals

NOTATION. Ordinals are denoted by lower case Greek letters $\alpha, \beta, \gamma, \ldots$. The class of all ordinals is denoted as Ord.

$$\alpha < \beta \quad \text{IFF} \quad \alpha \in \beta.$$

Ordinals

NOTATION. Ordinals are denoted by lower case Greek letters $\alpha, \beta, \gamma, \ldots$. The class of all ordinals is denoted as Ord.

COMPARE ORDINALS.

$$\alpha < \beta \quad \text{IFF} \quad \alpha \in \beta.$$

Properties

When $\alpha < \beta$, let $\beta_\alpha = \{\gamma \in \beta \mid \gamma < \alpha\}$.

Properties

When $\alpha < \beta$, let $\beta_\alpha = \{\gamma \in \beta \mid \gamma < \alpha\}$.

First, we show that Ord and "$\in$" reflect order-types of well-orderings faithfully.

Properties

When $\alpha < \beta$, let $\beta_\alpha = \{\gamma \in \beta \mid \gamma < \alpha\}$.

First, we show that Ord and "$\in$" reflect order-types of well-orderings faithfully.

Theorem 14

1. *If* $\beta \in \mathrm{Ord}$ *and* $\alpha < \beta$, *then* $\alpha \in \mathrm{Ord}$ *and* $\alpha = \beta_\alpha$.
2. *If* $\alpha, \beta \in \mathrm{Ord}$ *and* $\alpha \cong \beta$, *then* $\alpha = \beta$.

Properties

When $\alpha < \beta$, let $\beta_\alpha = \{\gamma \in \beta \mid \gamma < \alpha\}$.

First, we show that Ord and "$\in$" reflect order-types of well-orderings faithfully.

Theorem 14

1. *If* $\beta \in \mathrm{Ord}$ *and* $\alpha < \beta$*, then* $\alpha \in \mathrm{Ord}$ *and* $\alpha = \beta_\alpha$*.*
2. *If* $\alpha, \beta \in \mathrm{Ord}$ *and* $\alpha \cong \beta$*, then* $\alpha = \beta$*.*

PROOF.

Key for (2): show that $f : \alpha \xrightarrow{\cong} \beta$ equals to id. Let $\alpha_0 =$ least γ s.t. $f(\gamma) \neq \gamma$. Show that $\alpha_0 = f''\alpha_0 = \beta_{f(\alpha_0)} = f(\alpha_0)$. □

Properties

Theorem 14-1 says that every ordinal forms an initial segment of Ord. Conversely, any **proper** initial segment of Ord is an ordinal.

Lemma 15

Suppose that X is a subset of Ord such that

$$\forall x \in X \forall y < x \, (y \in X),$$

then $X \in \mathrm{Ord}$.

Properties

As corollary, we have

Theorem 16

If $(W, \prec)$ *is a well-ordering, then there is a unique* $\alpha \in \mathrm{Ord}$ *such that* $(W, \prec) \cong (\alpha, \in)$.

Properties

As corollary, we have

Theorem 16

If $(W, \prec)$ *is a well-ordering, then there is a unique* $\alpha \in \mathrm{Ord}$ *such that* $(W, \prec) \cong (\alpha, \in)$*.*

Given a well-ordering $(W, \prec)$, let $\mathrm{ordertype}((W, \prec))$ denote the unique $\alpha \in \mathrm{Ord}$ such that $(W, \prec) \cong (\alpha, \in)$.

PROOF.

Uniqueness follows from Theorem 14-2.

PROOF.

Uniqueness follows from Theorem 14-2.
For the existence, let

$$U = \{x \in W \mid \exists \alpha \in \mathrm{Ord}\,(W_x \cong \alpha)\}$$

and let f be the function with $\mathrm{dom}(f) = U$ such that for every $x \in U$,

$$f(x) = \text{the (unique) } \alpha \in \mathrm{Ord} \text{ s.t. } W_x \cong \alpha.$$

PROOF.

Uniqueness follows from Theorem 14-2.
For the existence, let

$$U = \{x \in W \mid \exists \alpha \in \mathrm{Ord}\,(W_x \cong \alpha)\}$$

and let f be the function with $\mathrm{dom}(f) = U$ such that for every $x \in U$,

$$f(x) = \text{the (unique) } \alpha \in \mathrm{Ord} \text{ s.t. } W_x \cong \alpha.$$

Check that

- $\mathrm{ran}(f)$ is an ordinal.

PROOF.

Uniqueness follows from Theorem 14-2.
For the existence, let

$$U = \{x \in W \mid \exists \alpha \in \mathrm{Ord}\,(W_x \cong \alpha)\}$$

and let f be the function with $\mathrm{dom}(f) = U$ such that for every $x \in U$,

$$f(x) = \text{the (unique) } \alpha \in \mathrm{Ord} \text{ s.t. } W_x \cong \alpha.$$

Check that

- $\mathrm{ran}(f)$ is an ordinal.
- f is an isomorphism between U and $\mathrm{ran}(f)$.

PROOF.

Uniqueness follows from Theorem 14-2.
For the existence, let

$$U = \{x \in W \mid \exists \alpha \in \mathrm{Ord}\,(W_x \cong \alpha)\}$$

and let f be the function with $\mathrm{dom}(f) = U$ such that for every $x \in U$,

$$f(x) = \text{the (unique) } \alpha \in \mathrm{Ord} \text{ s.t. } W_x \cong \alpha.$$

Check that

- $\mathrm{ran}(f)$ is an ordinal.
- f is an isomorphism between U and $\mathrm{ran}(f)$.
- either $U = W$

  or $U = W_x$ for some $x \in W$

□

Proof.

Uniqueness follows from Theorem 14-2.
For the existence, let

$$U = \{x \in W \mid \exists \alpha \in \mathrm{Ord}\,(W_x \cong \alpha)\}$$

and let f be the function with $\mathrm{dom}(f) = U$ such that for every $x \in U$,

$$f(x) = \text{the (unique) } \alpha \in \mathrm{Ord} \text{ s.t. } W_x \cong \alpha.$$

Check that

- $\mathrm{ran}(f)$ is an ordinal. — need Replacement.
- f is an isomorphism between U and $\mathrm{ran}(f)$.
- either $U = W$

  or $U = W_x$ for some $x \in W$

□

PROOF.

Uniqueness follows from Theorem 14-2.
For the existence, let

$$U = \{x \in W \mid \exists \alpha \in \mathrm{Ord}\,(W_x \cong \alpha)\}$$

and let f be the function with $\mathrm{dom}(f) = U$ such that for every $x \in U$,

$$f(x) = \text{the (unique) } \alpha \in \mathrm{Ord} \text{ s.t. } W_x \cong \alpha.$$

Check that

- $\mathrm{ran}(f)$ is an ordinal. — need Replacement.
- f is an isomorphism between U and $\mathrm{ran}(f)$.
- either $U = W$ — in this case we are done.
  or $U = W_x$ for some $x \in W$

□

PROOF.

Uniqueness follows from Theorem 14-2.
For the existence, let

$$U = \{x \in W \mid \exists\alpha \in \mathrm{Ord}\,(W_x \cong \alpha)\}$$

and let f be the function with $\mathrm{dom}(f) = U$ such that for every $x \in U$,

$$f(x) = \text{the (unique) } \alpha \in \mathrm{Ord} \text{ s.t. } W_x \cong \alpha.$$

Check that

- $\mathrm{ran}(f)$ is an ordinal. — need Replacement.
- f is an isomorphism between U and $\mathrm{ran}(f)$.
- either $U = W$ — in this case we are done.
  or $U = W_x$ for some $x \in W$ — if so, $x \in U$, contradiction!

□

Properties (about $<$)

Theorem 17

1. *If* $\alpha \in \mathrm{Ord}$, *then* $\alpha \not< \alpha$.
2. *If* $x, y, z \in \mathrm{Ord}$, $x < y$ *and* $y < z$, *then* $x < z$.
3. *If* $\alpha, \beta \in \mathrm{Ord}$, *then exactly one of the following is true:*
$$\alpha < \beta, \quad \alpha = \beta, \quad \beta < \alpha.$$
4. *If* C *is a nonempty* **subclass** *of* Ord, *then*
$$\bigcap C = \inf(C) \in \mathrm{Ord}.$$

Properties (about $<$)

Theorem 17

1. *If* $\alpha \in \mathrm{Ord}$*, then* $\alpha \not< \alpha$*.*
2. *If* $x, y, z \in \mathrm{Ord}$*,* $x < y$ *and* $y < z$*, then* $x < z$*.*
3. *If* $\alpha, \beta \in \mathrm{Ord}$*, then exactly one of the following is true:*
$$\alpha < \beta, \quad \alpha = \beta, \quad \beta < \alpha.$$
4. *If* C *is a nonempty* **subclass** *of* Ord*, then*
$$\bigcap C = \inf(C) \in \mathrm{Ord}.$$

This theorem implies that the set of all ordinals, if it existed, would be an ordinal, and thus Ord is not a set.

Properties (about $<$)

Theorem 17

1. *If* $\alpha \in \mathrm{Ord}$*, then* $\alpha \not< \alpha$*.*
2. *If* $x, y, z \in \mathrm{Ord}$*,* $x < y$ *and* $y < z$*, then* $x < z$*.*
3. *If* $\alpha, \beta \in \mathrm{Ord}$*, then exactly one of the following is true:*
$$\alpha < \beta, \quad \alpha = \beta, \quad \beta < \alpha.$$
4. *If* C *is a nonempty* **subclass** *of* Ord*, then*
$$\bigcap C = \inf(C) \in \mathrm{Ord}.$$

This theorem implies that the set of all ordinals, if it existed, would be an ordinal, and thus Ord is not a set. More precisely,

$$\neg \exists z \forall x \in \mathrm{Ord}\,(x \in z).$$

This is so-called **Burali-Forti** paradox.

Properties (about $\subseteq$)

Proposition 18

1. $\varnothing \in \mathrm{Ord}$.
2. *If* $\alpha, \beta \in \mathrm{Ord}$, $\alpha \neq \beta$ *and* $\alpha \subset \beta$, *then* $\alpha \in \beta$.
3. *For any* $\alpha, \beta \in \mathrm{Ord}$, $\alpha \leq \beta \leftrightarrow \alpha \subseteq \beta$.
4. *If* $\alpha, \beta \in \mathrm{Ord}$, *then* $\alpha \subsetneq \beta \vee \alpha = \beta \vee \beta \subsetneq \alpha$.
5. *If* D *is a nonempty* **subset** *of* Ord, *then*
$$\bigcup D = \sup(D) \in \mathrm{Ord}.$$

Successor Ordinal and Limit Ordinal

Definition 19

$$S(\alpha) = \alpha \cup \{\alpha\}.$$

Successor Ordinal and Limit Ordinal

Definition 19

$$S(\alpha) = \alpha \cup \{\alpha\}.$$

Lemma 20

For any $\alpha \in \mathrm{Ord}$,

1. $\alpha < S(\alpha)$,
2. $S(\alpha) = \inf\{\beta \mid \beta > \alpha\} \in \mathrm{Ord}$, *and*
3. *for every* $\beta \in \mathrm{Ord}$, $\beta < S(\alpha) \leftrightarrow \beta \leq \alpha$.

Successor Ordinal and Limit Ordinal

Definition 21

α is a **successor** ordinal iff $\exists\beta\,(\alpha = S(\beta))$.
α is a **limit** ordinal iff $\alpha \neq \varnothing$ and α is not a successor ordinal.

Lemma 22

If α is not a successor ordinal, then $\alpha = \sup(\alpha) = \bigcup \alpha$.

Successor Ordinal and Limit Ordinal

Definition 21

α is a **successor** ordinal iff $\exists\beta\,(\alpha = S(\beta))$.
α is a **limit** ordinal iff $\alpha \neq \varnothing$ and α is not a successor ordinal.

Lemma 22

If α is not a successor ordinal, then $\alpha = \sup(\alpha) = \bigcup \alpha$.

This includes $\varnothing$ and all limit ordinals. The existence of limit ordinals follows from the **Axiom of Infinity**.

Natural Numbers

Definition 23

$0 = \varnothing$, $1 = S(0)$, $2 = S(1)$, $3 = S(2)$, ..., etc.

Natural Numbers

Definition 23

$0 = \varnothing$, $1 = S(0)$, $2 = S(1)$, $3 = S(2)$, ..., etc.

So $1 = 0$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, ..., etc.

Natural Numbers

Definition 23

$0 = \varnothing$, $1 = S(0)$, $2 = S(1)$, $3 = S(2)$, ..., etc.

So $1 = 0$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, ..., etc.

Definition 24

Suppose $\alpha \in \mathrm{Ord}$. α is a **natural number** iff

$$\forall \beta \leq \alpha \, (\beta = 0 \vee \beta \text{ is a successor ordinal}).$$

Letters n, m, l, k, j, i are often used to denote natural numbers.

Natural Numbers

It is immediate from the definition that the natural numbers form an initial segment of the ordinals.

Natural Numbers

It is immediate from the definition that the natural numbers form an initial segment of the ordinals.

Proof: By definition $\mathbb{N} \subseteq \mathrm{Ord}$. Suppose $\beta \in \mathbb{N}$ and $\gamma < \beta$. Then γ is either 0 or a successor ordinal. Any $\eta < \gamma$ is also $< \beta$, thus is either 0 or a successor ordinal. Hence $\gamma \in \mathbb{N}$.

Natural Numbers

It is immediate from the definition that the natural numbers form an initial segment of the ordinals.

Proof: By definition $\mathbb{N} \subseteq \mathrm{Ord}$. Suppose $\beta \in \mathbb{N}$ and $\gamma < \beta$. Then γ is either 0 or a successor ordinal. Any $\eta < \gamma$ is also $< \beta$, thus is either 0 or a successor ordinal. Hence $\gamma \in \mathbb{N}$.

With the concept of "natural number", one can define the notion of "finite/infinite". However, it uses the idea of bijection from Chapter 3.

Natural Numbers

It is immediate from the definition that the natural numbers form an initial segment of the ordinals.

<u>Proof</u>: By definition $\mathbb{N} \subseteq \mathrm{Ord}$. Suppose $\beta \in \mathbb{N}$ and $\gamma < \beta$. Then γ is either 0 or a successor ordinal. Any $\eta < \gamma$ is also $< \beta$, thus is either 0 or a successor ordinal. Hence $\gamma \in \mathbb{N}$.

With the concept of "natural number", one can define the notion of "finite/infinite". However, it uses the idea of bijection from Chapter 3.

Definition 25

A set X is **finite** if there is a bijection from X to some natural number. X is **infinite** if X is not finite.

Infinity

Intuitively, natural numbers are obtained by applying S to 0 a finite number of times. Let β be the least ordinal not so obtained, β could not be a successor ordinal, and hence all large α would not satisfy Definition 24.

Infinity

Intuitively, natural numbers are obtained by applying S to 0 a finite number of times. Let β be the least ordinal not so obtained, β could not be a successor ordinal, and hence all large α would not satisfy Definition 24. This is where the AXIOM OF INFINITY comes in.

AXIOM 6 (Infinity)

$$\exists x\,(0 \in x \wedge \forall y\,(y \in x \to S(y) \in x).$$

Infinity

If x satisfies the Axiom of Infinity, then x contains all natural numbers.

Infinity

If x satisfies the Axiom of Infinity, then x contains all natural numbers.

Idea: Suppose NOT. Let n be least such that $n \in \mathbb{N} - x$. $\varnothing \in x$, so $n \neq 0$, and it must be that $n = S(m)$, some m. Then $m \in \mathbb{N} \cap x$. But it follows that $S(m) \in x$. Contradiction!

ω

By Comprehension, there is a set of natural numbers.

Definition 26

ω is the set of natural numbers.

ω

By Comprehension, there is a set of natural numbers.

Definition 26

ω is the set of natural numbers.

- $\omega \in \mathrm{Ord}$, by Lemma 15.
- ω is a limit ordinal (otherwise, it would be a natural number).
- ω is the least limit ordinal.
- ω satisfies the **Peano Postulates**.

Peano Postulates

Theorem 27 (Peano Posulates)

1. $0 \in \omega$.
2. $\forall n \in \omega \, (S(n) \in \omega)$.
3. $\forall n, m \in \omega \, (n \neq m \rightarrow S(n) \neq S(m))$.
4. (*Induction*)

$$\forall X \subseteq \omega \, [(0 \in X \wedge \forall n \in X \, (S(n) \in X)) \rightarrow X = \omega].$$

Peano Postulates

Theorem 27 (Peano Posulates)

1. $0 \in \omega$.
2. $\forall n \in \omega \, (S(n) \in \omega)$.
3. $\forall n, m \in \omega \, (n \neq m \rightarrow S(n) \neq S(m))$.
4. (*Induction*)

$$\forall X \subseteq \omega \, [(0 \in X \wedge \forall n \in X \, (S(n) \in X)) \rightarrow X = \omega].$$

PROOF.

For 4., if $X \neq \omega$, let $\gamma = \min(\omega - X)$, and show that γ is a limit ordinal $< \omega$. □

Developing Mathematics (early attempt)

Given the natural numbers with the Peano Postulates, one may temporarily forget about ordinals and proceed to develop elementary mathematics directly: constructing the integers and the rationals, and then introducing the Power Set Axiom and constructing the set of real numbers.

Developing Mathematics (early attempt)

Given the natural numbers with the Peano Postulates, one may temporarily forget about ordinals and proceed to develop elementary mathematics directly: constructing the integers and the rationals, and then introducing the Power Set Axiom and constructing the set of real numbers.

The first step would be to define $+$ and $\cdot$ on ω. However, we take an alternative approach via which we can discuss $+$ and $\cdot$ on all ordinals. Our approach doesn't need the Axiom of Infinity.

Addition and Multiplication

Definition 28

- $\alpha + \beta = \mathrm{ordertype}((\alpha \times \{0\}) \oplus (\beta \times \{1\}))$.

Addition and Multiplication

Definition 28

- $\alpha + \beta = \text{ordertype}((\alpha \times \{0\}) \oplus (\beta \times \{1\}))$.
- $\alpha \cdot \beta = \text{ordertype}(\alpha \otimes \beta)$.

Addition and Multiplication

Definition 28

- $\alpha + \beta = \text{ordertype}((\alpha \times \{0\}) \oplus (\beta \times \{1\}))$.
- $\alpha \cdot \beta = \text{ordertype}(\alpha \otimes \beta)$.

More general version will be discussed later.

Addition and Multiplication

Proposition 29

For any α, β, γ,

1. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

Addition and Multiplication

Proposition 29

For any α, β, γ,

1. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
2. $\alpha + 0 = \alpha$.

Addition and Multiplication

Proposition 29

For any α, β, γ,

1. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
2. $\alpha + 0 = \alpha$.
3. $\alpha + 1 = S(\alpha)$.

Addition and Multiplication

Proposition 29

For any α, β, γ,

1. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
2. $\alpha + 0 = \alpha$.
3. $\alpha + 1 = S(\alpha)$.
4. $\alpha + S(\beta) = S(\alpha + \beta)$.

Addition and Multiplication

Proposition 29

For any α, β, γ,

1. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
2. $\alpha + 0 = \alpha$.
3. $\alpha + 1 = S(\alpha)$.
4. $\alpha + S(\beta) = S(\alpha + \beta)$.
5. *If* β *is a limit ordinal,* $\alpha + \beta = \sup\{\alpha + \xi \mid \xi < \beta\}$.

Addition and Multiplication

Proposition 30

For any α, β, γ,

1. $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

Addition and Multiplication

Proposition 30

For any α, β, γ*,*

1. $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$
2. $\alpha \cdot 0 = 0$

Addition and Multiplication

Proposition 30

For any α, β, γ*,*

1. $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$
2. $\alpha \cdot 0 = 0$
3. $\alpha \cdot 1 = \alpha$

Addition and Multiplication

Proposition 30

For any α, β, γ,

1. $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$
2. $\alpha \cdot 0 = 0$
3. $\alpha \cdot 1 = \alpha$
4. $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha$

Addition and Multiplication

Proposition 30

For any α, β, γ,

1. $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$
2. $\alpha \cdot 0 = 0$
3. $\alpha \cdot 1 = \alpha$
4. $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha$
5. *If* β *is a limit ordinal,* $\alpha \cdot \beta = \sup\{\alpha \cdot \xi \mid \xi < \beta\}$.

Addition and Multiplication

Proposition 30

For any α, β, γ,

1. $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$
2. $\alpha \cdot 0 = 0$
3. $\alpha \cdot 1 = \alpha$
4. $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha$
5. *If* β *is a limit ordinal,* $\alpha \cdot \beta = \sup\{\alpha \cdot \xi \mid \xi < \beta\}$.
6. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Addition and Multiplication

Unlike the case with natural numbers,

- $+$ is not commutative.

Addition and Multiplication

Unlike the case with natural numbers,

- $+$ is not commutative.
- $\cdot$ is not commutative.

Addition and Multiplication

Unlike the case with natural numbers,

- $+$ is not commutative. (e.g. $1 + \omega \neq \omega + 1$.)
- $\cdot$ is not commutative.

Addition and Multiplication

Unlike the case with natural numbers,

- $+$ is not commutative. (e.g. $1 + \omega \neq \omega + 1$.)
- $\cdot$ is not commutative. (e.g. $2 \cdot \omega \neq \omega \cdot 2$.)

Finite Sequences

Natural numbers give us a way of handling finite sequences.

Definition 31

1. ${}^{n}X$ is the set of functions from n into X.
2. ${}^{<\omega}X = \bigcup\{{}^{n}X \mid n \in \omega\}$. ▸ ConCat

Finite Sequences

In the literature, X^n and $X^{<\omega}$ are often used. The intention here is to emphasize the difference between ${}^2X$ and $X \times X$, although there is an obvious bijection between them. We shall not make distinction when it causes no confusion.

Finite Sequences

In the literature, X^n and $X^{<\omega}$ are often used. The intention here is to emphasize the difference between ${}^2X$ and $X \times X$, although there is an obvious bijection between them. We shall not make distinction when it causes no confusion.

REMARK: It is not completely trivial to see that this definition makes sense without using the Power Set Axiom.

Finite Sequences

We often think that of the elements of ${}^{n}X$ as the sequences from X of length n.

Definition 32

For each n, $\langle x_0, \ldots, x_{n-1} \rangle$ is the function s with domain n such that $s(0) = x_0$, $s(1) = x_1$, ..., $s(n-1) = x_{n-1}$.

Finite Sequences

The case $n = 2$ gives us another way to define ordered pairs. In the literature, the ordered pair (a, b) is often written as $\langle a, b\rangle$. Here different notations are used to differentiate two ways of defining ordered pairs.

Finite Sequences

The case $n = 2$ gives us another way to define ordered pairs. In the literature, the ordered pair (a, b) is often written as $\langle a, b \rangle$. Here different notations are used to differentiate two ways of defining ordered pairs.

(a, b) is convenient for developing basic notions of functions and relations, while $\langle a, b \rangle$ is more useful in handling sequences of various lengths. We shall make no distinction from now on.

General Sequences

In general, we think of $I = \mathrm{dom}(s)$ as an index set and s as a sequence indexed by I. So $s(i)$ is often written as s_i. More generally, $\langle s_i : i \in I \rangle$ is used to denote general sequences.

General Sequences

In general, we think of $I = \mathrm{dom}(s)$ as an index set and s as a sequence indexed by I. So $s(i)$ is often written as s_i. More generally, $\langle s_i : i \in I \rangle$ is used to denote general sequences.

When $\mathrm{dom}(s) = \alpha$, we may view s as a sequence of length α. Thus we can generalize Definition 31 to ${}^{\alpha}X$ and ${}^{<\alpha}X$.

Definition 33

If s, t are two functions with $\mathrm{dom}(s) = \alpha$ and $\mathrm{dom}(t) = \beta$, $s^\frown t$ is the function with $\mathrm{dom}(s^\frown t) = \alpha + \beta$ such that

$$(s^\frown t) \restriction \alpha = s, \quad \text{and}$$
$$(s^\frown t)(\alpha + \xi) = t(\xi), \text{ for all } \xi < \beta.$$

Coming up next

Transfinite Induction

The Induction Principle and the Recursion Theorem are the main tools for proving theorems about natural numbers. In this section, we show how these results generalize to ordinal numbers.

Transfinite Induction

The Induction Principle and the Recursion Theorem are the main tools for proving theorems about natural numbers. In this section, we show how these results generalize to ordinal numbers.

Theorem 34 (The Induction Principle)

Let $\varphi(x)$ be a property (possibly with parameters). Assume that,

1. $\varphi(0)$ *holds.*
2. *For all $n \in \omega$, $\varphi(n)$ implies $\varphi(n+1)$.*

Then $\varphi(n)$ holds for all $n \in \omega$.

Transfinite Induction

Theorem 35 (Transfinite Induction, Version I)

Let $\varphi(x)$ *be a property (possibly with parameters). Assume that, for all* $\alpha \in \mathrm{Ord}$*,*

$$\text{If } \varphi(\beta) \text{ holds for all } \beta < \alpha, \text{ then } \varphi(\alpha). \qquad (*)$$

Then $\varphi(\alpha)$ *holds for all* $\alpha \in \mathrm{Ord}$*.*

Transfinite Induction

<u>PROOF</u>.

Suppose NOT.

Transfinite Induction

PROOF.

Suppose NOT. Consider the class

$$E = \{\gamma \in \mathrm{Ord} \mid \neg\varphi(\gamma)\}$$

Transfinite Induction

PROOF.

Suppose NOT. Consider the class

$$E = \{\gamma \in \mathrm{Ord} \mid \neg\varphi(\gamma)\}$$

By the assumption $E \neq \varnothing$.

Transfinite Induction

PROOF.

Suppose NOT. Consider the class

$$E = \{\gamma \in \mathrm{Ord} \mid \neg\varphi(\gamma)\}$$

By the assumption $E \neq \varnothing$. As a subclass of Ord, E has a least element α.

Transfinite Induction

PROOF.

Suppose NOT. Consider the class

$$E = \{\gamma \in \mathrm{Ord} \mid \neg\varphi(\gamma)\}$$

By the assumption $E \neq \varnothing$. As a subclass of Ord, E has a least element α. Since $\varphi(\beta)$ holds for every $\beta < \alpha$, it follows from $(*)$ that $\varphi(\alpha)$ holds. Contradiction! □

Transfinite Induction

Theorem 36 (Transfinite Induction, Version II)

Let $\varphi(x)$ be a property. Assume that

1. $\varphi(0)$ *holds.*
2. $\varphi(\alpha) \to \varphi(\alpha + 1)$, *for all* $\alpha \in \mathrm{Ord}$.
3. *For all limit ordinals* α, *if* $\varphi(\beta)$ *holds for all* $\beta < \alpha$, *then* $\varphi(\alpha)$ *holds.*

Then $\varphi(\alpha)$ *holds for all* $\alpha \in \mathrm{Ord}$.

Transfinite Induction

Theorem 36 (Transfinite Induction, Version II)

Let $\varphi(x)$ be a property. Assume that

1. $\varphi(0)$ *holds.*
2. $\varphi(\alpha) \to \varphi(\alpha + 1)$, *for all* $\alpha \in \mathrm{Ord}$.
3. *For all limit ordinals* α, *if* $\varphi(\beta)$ *holds for all* $\beta < \alpha$, *then* $\varphi(\alpha)$ *holds.*

Then $\varphi(\alpha)$ *holds for all* $\alpha \in \mathrm{Ord}$.

It suffices to show that 1-3 implies $(*)$.

The Recursion Theorem

Theorem 37 (The Recursion Theorem)

For any set X *and any function* $g : {}^{<\omega}X \to X$*, there exists a unique infinite sequence* $f : \omega \to X$ *such that*

$$f_n = g(f \restriction n) = g(\langle f_0, \dots, f_{n-1} \rangle), \quad \textit{for all } n \in \omega.$$

Theorem 38 (The Transfinite Recursion Theorem)

Let $\Omega \in \mathrm{Ord}$*,* X *a set, and* $S = {}^{<\Omega}X$*. Let* $g : S \to X$ *be a function. Then there exists a unique function* $f : \Omega \to X$ *such that*

$$f(\alpha) = g(f \restriction \alpha), \quad \textit{for all } \alpha < \Omega.$$

Coming up next

Recursive Definitions

Definition 39

Let $\alpha > 0$ be a limit ordinal and let $\langle \gamma_\xi : \xi < \alpha \rangle$ be a nondecreasing sequence of ordinals (i.e. $\xi < \eta \implies \gamma_\xi \leq \gamma_\eta$). The **limit** of the sequence is $\lim_{\xi \to \alpha} \gamma_\xi = \sup\{\gamma_\xi \mid \xi < \alpha\}$.

Recursive Definitions

Addition and Multiplication of ordinal numbers can be defined recursively.

Recursive Definitions

Addition and Multiplication of ordinal numbers can be defined recursively.

Definition 40 (Addition)

For all ordinal numbers α,

1. $\alpha + 0 = \alpha$.
2. $\alpha + (\beta + 1) = (\alpha + \beta) + 1$, for all β.
3. $\alpha + \beta = \lim_{\xi \to \beta} (\alpha + \xi)$, for limit $\beta > 0$.

Recursive Definitions

Definition 41 (Multiplication)

For all ordinal numbers α,

1. $\alpha \cdot 0 = 0$.
2. $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$, for all β.
3. $\alpha \cdot \beta = \lim_{\xi \to \beta}(\alpha \cdot \xi)$, for limit $\beta > 0$.

Recursive Definitions

We've shown that the geometrical definitions given in the early section satisfy these properties. By induction, one can show that

Lemma 42

For all ordinals α *and* β, $\alpha + \beta$ *and* $\alpha \cdot \beta$ *are, respectively, isomorphic to* $\alpha \oplus \beta$ *and* $\alpha \otimes \beta$.

Recursive Definitions

We've shown that the geometrical definitions given in the early section satisfy these properties. By induction, one can show that

Lemma 42

For all ordinals α and β, $\alpha + \beta$ and $\alpha \cdot \beta$ are, respectively, isomorphic to $\alpha \oplus \beta$ and $\alpha \otimes \beta$.

Next is the recursive definition of the exponentiation of ordinals, which is much easier to grasp than it's geometrical version.

Exponentiation

Definition 43 (Exponentiation)

For all ordinal numbers α,

1. $\alpha^0 = 1$.
2. $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$, for all β.
3. $\alpha^\beta = \lim_{\xi \to \beta} \alpha^\xi$, for all limit $\beta > 0$.

Proposition 44

For all $\alpha, \beta, \gamma \in \mathrm{Ord}$*,*

1. $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$*.*
2. $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$*.*

Exponentiation

Geometrical Definition

Here, for those who are curious, is the geometrical definition of exponentiation of ordinal numbers.

Definition 45 (Exponentiation)

Let

$$F(\alpha, \beta) = \{f \in {}^{\beta}\alpha \mid \{\xi \mid f(\xi) \neq 0\} \text{ is finite.}\}$$

If $f, g \in F(\alpha, \beta)$ and $f \neq g$, then

$$f \prec g \leftrightarrow f(\xi) < g(\xi),$$

where ξ is the largest ordinal such that $f(\xi) \neq g(\xi)$. Then

$$\alpha^{\beta} = \mathrm{ordertype}((F(\alpha, \beta), \prec)).$$

Properties

Here are some additional properties of the three ordinal operations.

Lemma 46

1. *If* $\beta < \gamma$ *then* $\alpha + \beta < \alpha + \gamma$*.*
2. *If* $\alpha \leq \beta$ *then there exists a unique* δ *such that* $\alpha + \delta = \beta$*.*
3. *Suppose* $\alpha > 0$*. If* $\beta < \gamma$ *then* $\alpha \cdot \beta < \alpha \cdot \gamma$*.*
4. *If* $\alpha > 0$ *and* γ *is arbitrary, then there exist a unique* β *and a unique* $\rho < \alpha$ *such that* $\gamma = \alpha \cdot \beta + \rho$*.*
5. *Suppose* $\alpha > 1$*. If* $\beta < \gamma$ *then* $\alpha^\beta < \alpha^\gamma$*.*

Properties

Here are some additional properties of the three ordinal operations.

Lemma 46

1. *If* $\beta < \gamma$ *then* $\alpha + \beta < \alpha + \gamma$.
2. *If* $\alpha \leq \beta$ *then there exists a unique* δ *such that* $\alpha + \delta = \beta$.
3. *Suppose* $\alpha > 0$. *If* $\beta < \gamma$ *then* $\alpha \cdot \beta < \alpha \cdot \gamma$.
4. *If* $\alpha > 0$ *and* γ *is arbitrary, then there exist a unique* β *and a unique* $\rho < \alpha$ *such that* $\gamma = \alpha \cdot \beta + \rho$.
5. *Suppose* $\alpha > 1$. *If* $\beta < \gamma$ *then* $\alpha^\beta < \alpha^\gamma$.

(1), (3), (5) are in fact "if and only if".

Cantor's Normal Form

Theorem 47 (Cantor's Normal Form Theorem)

Every nonzero ordinal α can be represented uniquely in the form

$$\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n,$$

where $n \geq 1$, $\alpha \geq \beta_1 > \cdots > \beta_n$, and $k_1, \ldots, k_n$ are nonzero natural numbers.

Cantor's Normal Form

Theorem 47 (Cantor's Normal Form Theorem)

Every nonzero ordinal α *can be represented uniquely in the form*

$$\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n,$$

where $n \geq 1$, $\alpha \geq \beta_1 > \cdots > \beta_n$, *and* $k_1, \ldots, k_n$ *are nonzero natural numbers.*

PROOF.

By induction on α. Use Lemma 46-4. □

Factorization of ordinals

An application of CNF

Definition 48

A ordinal $\alpha > 1$ is *prime* if there are no ordinals $\beta, \gamma < \alpha$ such that $\alpha = \beta \cdot \gamma$.

Factorization of ordinals

An application of CNF

Definition 48

A ordinal $\alpha > 1$ is *prime* if there are no ordinals $\beta, \gamma < \alpha$ such that $\alpha = \beta \cdot \gamma$.

There are three sorts of prime ordinals:

- $2, 3, 5, \ldots$ (finite primes)
- ω^{ω^α}, for any $\alpha \in \mathrm{Ord}$. (limit primes)
- $\omega^\alpha + 1$, for any $\alpha \in \mathrm{Ord} \setminus \{0\}$. (infinite successor primes)

Factorization of ordinals

An application of CNF

Theorem 49 (Siepínski, 1958[2])

The Cantor normal form ordinal

$$\omega^{\alpha_1} n_1 + \cdots + \omega^{\alpha_k} n_k \ (\text{with } \alpha_1 > \cdots > \alpha_k)$$

is uniquely factored into a minimal product of infinite primes and integers of the following form

$$\omega^{\omega^{\beta_1}} \cdots \omega^{\omega^{\beta_m}} n_k (\omega^{\alpha_{k-1}-\alpha_k} + 1) n_{k-1} \cdots n_2 (\omega^{\alpha_1 - \alpha_2} + 1) n_1$$

where

- *each* n_i *should be replaced by its unique factorization of finite primes, and*
- $\alpha_k = \omega^{\beta_1} + \cdots + \omega^{\beta_m}$ *with* $\beta_1 > \cdots > \beta_m$.

[2] This was rediscovered by a BNU undergrad, YOU Hangyu.

About ε_0

Note that it is possible that $\alpha = \beta_1$, i.e. $\alpha = \omega^\alpha$. The least such ordinal is called ε_0.

- (Gentzen) Transfinite induction on ε_0 proves $\mathrm{Con}(\mathsf{PA})$, the consistency of the first-order Peano axioms (PA).
- By Gödel's 2^{nd} Incompleteness, PA can not prove transfinite induction for (or beyond) ε_0
- PA are not strong enough to show that ε_0 is an ordinal
- while ε_0 can easily be arithmetically described

[3] See https://en.wikipedia.org/wiki/Veblen_function.

About ε_0

Note that it is possible that $\alpha = \beta_1$, i.e. $\alpha = \omega^\alpha$. The least such ordinal is called ε_0.

- (Gentzen) Transfinite induction on ε_0 proves $\mathrm{Con}(\mathsf{PA})$, the consistency of the first-order Peano axioms (PA).
- By Gödel's 2^{nd} Incompleteness, PA can not prove transfinite induction for (or beyond) ε_0
- PA are not strong enough to show that ε_0 is an ordinal
- while ε_0 can easily be arithmetically described

Define $\varphi_0(\beta) = \omega^\beta$, $\varphi_{\gamma+1}(\beta) = \beta$-th fixed point of φ_γ, and $\varphi_\delta(\beta) =$ the β-th common fixed point of φ_γ, $\gamma < \delta$. Then $\varphi_1(0) = \varepsilon_0$. φ_γ is called the γ-th Veblen function.[3]

[3] See `https://en.wikipedia.org/wiki/Veblen_function`.

Goodstein Sequence

Another application of CNF

- Recall that for every natural number $a \geq 2$, every natrual number m can be written in **base** a, i.e., as a sum of powers of a:

  $$m = a^{b_1} \cdot k_1 + \cdots + a^{b_n} \cdot k_n,$$

  with $b_1 > \cdots > b_n$ and $0 < k_i < a$, $i = 1, \ldots, n$.

Goodstein Sequence

Another application of CNF

- Recall that for every natural number $a \geq 2$, every natrual number m can be written in **base** a, i.e., as a sum of powers of a:

$$m = a^{b_1} \cdot k_1 + \cdots + a^{b_n} \cdot k_n,$$

  with $b_1 > \cdots > b_n$ and $0 < k_i < a$, $i = 1, \ldots, n$.

- A number m is written in **pure base** $a \geq 2$ if it is first written in base a, then so are the exponents and the exponents of exponents, etc. For instance, 324 in pure base 3:

$$(324)_3 = 3^{3+2} + 3^{3+1}.$$

Goodstein Sequence

Definition 50

The **Goodstein sequence** starting at $m > 0$ is a sequence $m_0, m_1, m_2, \ldots$ obtained as follows: Let $m_0 = m$ and write m_0 in pure base 2. By induction, to get m_{k+1}, write m_k in pure base $k+2$, replace each $k+2$ by $k+3$, and subtract 1.

Goodstein Sequence

The Goodstein sequence starting at $m = 21$:

$$
\begin{aligned}
m_0 = (21)_2 &= 2^{2^2} + 2^2 + 1 \\
m_1 &= 3^{3^3} + 3^3 && \sim 7.6 \times 10^{12} \\
m_2 &= 4^{4^4} + 4^4 - 1 \\
&= 4^{4^4} + 4^3 \cdot 3 + 4^2 \cdot 3 + 4 \cdot 3 + 3 && \sim 1.3 \times 10^{154} \\
m_3 &= 5^{5^5} + 5^3 \cdot 3 + 5^2 \cdot 3 + 5 \cdot 3 + 2 && \sim 1.9 \times 10^{2184} \\
m_4 &= 6^{6^6} + 6^3 \cdot 3 + 6^2 \cdot 3 + 6 \cdot 3 + 1 && \sim 2.6 \times 10^{36305} \\
& \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots
\end{aligned}
$$

Goodstein Sequence

Theorem 51 (Goodstein, 1944)

For each $m > 0$, the Goodstein sequence starting at m eventually terminates with $m_n = 0$ for some n.

Goodstein Sequence

Theorem 51 (Goodstein, 1944)

For each $m > 0$, the Goodstein sequence starting at m eventually terminates with $m_n = 0$ for some n.

<u>Proof</u>.

We define a (finite) sequence of ordinals $\beta_0 > \cdots > \beta_n > \cdots$ as follows. When m_n is written in pure base $n + 2$, we get β_n by replacing each $n + 2$ by ω. The ordinals β_n are in normal form, and they form a (finite) decreasing sequence. Therefore $\beta_n = 0$ for some n, and since $m_n < \beta_n$ for all n, we have $m_n = 0$. □

Goodstein Sequence

Take the Goodstein sequence starting at $m = 21$ as an example:

$$m_0 < \beta_0 = \omega^{\omega^\omega} + \omega^\omega + 1$$
$$m_1 < \beta_1 = \omega^{\omega^\omega} + \omega^\omega$$
$$m_2 < \beta_2 = \omega^{\omega^\omega} + \omega^3 \cdot 3 + \omega^2 \cdot 3 + \omega \cdot 3 + 3$$
$$m_3 < \beta_3 = \omega^{\omega^\omega} + \omega^3 \cdot 3 + \omega^2 \cdot 3 + \omega \cdot 3 + 2$$
$$m_4 < \beta_4 = \omega^{\omega^\omega} + \omega^3 \cdot 3 + \omega^2 \cdot 3 + \omega \cdot 3 + 1$$
$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

Goodstein Sequence

Take the Goodstein sequence starting at $m = 21$ as an example:

$$
\begin{aligned}
m_0 &< \beta_0 = \omega^{\omega^{\omega}} + \omega^{\omega} + 1 \\
m_1 &< \beta_1 = \omega^{\omega^{\omega}} + \omega^{\omega} \\
m_2 &< \beta_2 = \omega^{\omega^{\omega}} + \omega^{3} \cdot 3 + \omega^{2} \cdot 3 + \omega \cdot 3 + 3 \\
m_3 &< \beta_3 = \omega^{\omega^{\omega}} + \omega^{3} \cdot 3 + \omega^{2} \cdot 3 + \omega \cdot 3 + 2 \\
m_4 &< \beta_4 = \omega^{\omega^{\omega}} + \omega^{3} \cdot 3 + \omega^{2} \cdot 3 + \omega \cdot 3 + 1 \\
&\qquad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots
\end{aligned}
$$

$$\beta_n \to 0 \quad \Longrightarrow \quad m_n \to 0.$$

Hydra Problem

Figure: Hercules slaying the Hydra

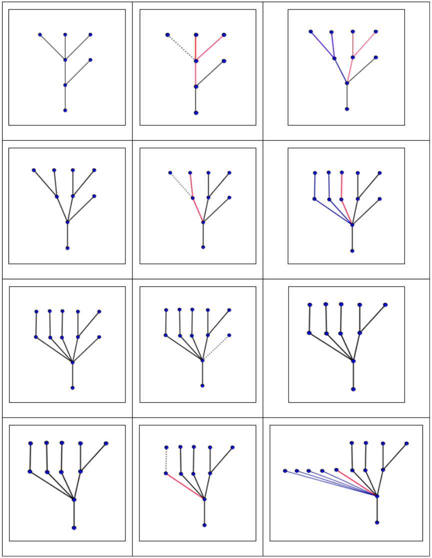
Hydra Problem

Step 1

Step 2

Step 3

Step 4



Arithmetic statements not provable in PA

Goodstein's Theorem was the third example of a true statement that is unprovable in Peano arithmetic.

1. (1931) Gödel's incompleteness theorem
2. (1943) Gerhard Gentzen's direct proof of the unprovability of ε_0-induction in Peano arithmetic
3. (1944) Goodstein's Theorem
   [Its unprovability was proved by Kirby and Paris, 1982]
4. (1977) Paris–Harrington theorem
5. (1987) Kanamori–McAloon theorem
6. ...

Kirby-Paris Theorem

Theorem 52 (Kirby-Paris, 1982[4])

Let $I\Sigma_k$ *denote Peano's axioms with induction restricted to* Σ_k *formulae. Then for* $k \in \mathbb{N}$ *and* $k \geq 1$, *for each fixed* $p \in \mathbb{N}$,

1. $I\Sigma_k \vdash \forall m, n > 1$ (*if* $m < n^{n^{\cdot^{\cdot^{\cdot^{p}}}}}$, *where* n *occurs* k *times, then the Goodstein sequence for* m *starting at* n *eventually hits zero*).
2. $I\Sigma_k \nvdash \forall m, n > 1$ (*if* $m < n^{n^{\cdot^{\cdot^{\cdot^{p}}}}}$, *where* n *occurs* $k + l$ *times, then the Goodstein sequence for* m *starting at n eventually hits zero*).

[4] Kirby, L.; Paris, J. *Accessible Independence Results for Peano Arithmetic*. Bulletin of the London Mathematical Society. 1982 14(4):285.

Homework

1. Let $\alpha, \beta, \gamma \in \mathrm{Ord}$ and let $\alpha < \beta$. Then
   a. $\alpha + \gamma \leq \beta + \gamma$.
   b. $\alpha \cdot \gamma \leq \beta \cdot \gamma$.
   c. $\alpha^\gamma \leq \beta^\gamma$.

   Given examples to show that $\leq$ cannot be replaced by $<$ in either inequality.

2. Show that the following rules do not hold for all $\alpha, \beta, \gamma \in \mathrm{Ord}$:
   a. If $\alpha + \gamma = \beta + \gamma$ then $\alpha = \beta$.
   b. If $\gamma > 0$ and $\alpha \cdot \gamma = \beta \cdot \gamma$ then $\alpha = \beta$.
   c. $(\beta + \gamma) \cdot \alpha = \beta \cdot \alpha + \gamma \cdot \alpha$.

Homework

3. Find a set $A \subset \mathbb{Q}$ such that $(A, <_{\mathbb{Q}}) \cong (\alpha, \in)$, where
   - $a.$ $\alpha = \omega + 1$,
   - $b.$ $\alpha = \omega \cdot 2$,
   - $c.$ $\alpha = \omega \cdot \omega$,
   - $d.$ $\alpha = \omega^{\omega}$,
   - $e.$* $\alpha = \varepsilon_0$.
   - $f.$* α is any ordinal $< \omega_1$.

Problems with stars are not assigned as homework, however, good students are encouraged to try.

Homework

4. An ordinal α is a limit ordinal iff $\alpha = \omega \cdot \beta$ for some $\beta \in \mathrm{Ord}$.
5. Find the first three $\alpha > 0$ s.t. $\xi + \alpha = \alpha$ for all $\xi < \alpha$.
6. Find the least ξ such that
   a. $\omega + \xi = \xi$.
   b. $\omega \cdot \xi = \xi$, $\xi \neq 0$.
   c. $\omega^\xi = \xi$.

(Hint for (1): Consider a sequence $\langle \xi_n \rangle$ s.t. $\xi_{n+1} = \omega + \xi_n$.)

About V

By transfinite recursion, define

$$V_0 = \varnothing,$$
$$V_{n+1} = \mathscr{P}(V_n).$$

Exercise

1. Every $x \in V_\omega$ is finite.
2. V_ω is transitive.
3. V_ω is an inductive set.

The elements of V_ω are called **hereditarily finite sets**.

About V

Exercise

1. If $x, y \in V_\omega$ then $\{x, y\} \in V_\omega$.
2. If $x \in V_\omega$ then $\bigcup x \in V_\omega$ and $\mathscr{P}(x) \in V_\omega$.
3. If $A \in V_\omega$ and f is a function on A such that $f(x) \in V_\omega$ for each $x \in A$, then $f[A] \in V_\omega$.
4. If x is a finite subset of V_ω, then $x \in V_\omega$.

About V

In fact, one can check that V_ω satisfies ZFC − **Infinity**. This hierarchical structure can be extended all the way up along Ord.

$$\begin{aligned} V_0 &= \varnothing, \\ V_{\alpha+1} &= \mathscr{P}(V_\alpha), \\ V_\alpha &= \textstyle\bigcup_{\beta<\alpha} V_\beta,\ \beta \text{ is a limit ordinal.} \end{aligned}$$