Introduction to the Theory of Sets

Mathematics 135
Spring 2017

Professor Thomas Scanlon
Scribe: Sinho Chewi

Contents

Lecture 1

January 18

1.1 Axiom of Extensionality

Here are examples of sets.

Example 1.1. $\mathbb{R}$: the set of real numbers.

Example 1.2. $F = \{x : x \text{ is one of my favorite things}\}$.

We will require all of the elements of our sets to be sets. (Alternative: start with a collection U of basic things, "ur elements".)

$A = B$ means $A \subseteq B$ and $B \subseteq A$, which means $\forall x\, [x \in A \implies x \in B]$ and $\forall z\, [z \in B \implies z \in A]$.

Remark: $A = B \implies \forall x\, [x \in A \iff x \in B]$ is a validity of first-order logic. The reverse implication is called extensionality and needs to be taken as an axiom.

Take $V = \{A, B\}$, with $A \notin^V A$, $B \notin^V B$, $A \notin^V B$, and $B \notin^V A$. Then, V entails $A \neq B$ and $\forall x\, [x \in A \iff x \in B]$. Here, extensionality does not hold.

Let $A = \{n : n > 2, \exists \text{ integers } x, y, z > 0, x^n + y^n = z^n\}$ and $B \neq \varnothing$. Let $C = \varnothing$ and $D = \varnothing$. Saying that $A = B$ and $C = D$ uses the axiom of extensionality.

Axiom of Extensionality: $A = B \iff \forall x\, [x \in A \iff x \in B]$.

Collection: Given any "property" (a first-order formula $\varphi(x)$), $\Phi = \{x \mid \varphi \text{ is true of } x\}$, i.e.

$$x \in \Phi \iff \varphi \text{ is true of } x.$$

Proposition 1.3. *Given φ, there exists at most one set Φ such that $x \in \Phi \iff \varphi$ is true of x.*

Proof. Suppose Ψ is a set and $x \in \Psi$ iff φ is true of x.

$$x \in \Psi \iff \varphi \text{ is true of } x \iff x \in \Phi$$

By extensionality, $\Psi = \Phi$. $\square$

If $\varphi := x \neq x$, then $\varnothing = \Phi = \{x \mid x \neq x\}$.

Let $R = \{x \mid x \notin x\}$.

Proposition 1.4. *$R \in R \iff R \notin R$.*

Lecture 2

January 20

2.1 Signatures

Definition 2.1. A **signature** σ consists of sets $\mathcal{C}_\sigma$ (constant symbols), $\mathcal{R}_\sigma$ (relation symbols), $\mathcal{F}_\sigma$ (function symbols), and functions

$$\begin{aligned} \text{arity} &: \mathcal{F}_\sigma \to \mathbb{Z}_+, \\ \text{arity} &: \mathcal{R}_\sigma \to \mathbb{Z}_+. \end{aligned}$$

Example 2.2. The empty signature has $\mathcal{C}_\sigma = \mathcal{R}_\sigma = \mathcal{F}_\sigma = \varnothing$.

Example 2.3. The signature for set theory has $\mathcal{C}_\sigma = \varnothing = \mathcal{F}_\sigma$, $\mathcal{R}_\sigma = \{\in\}$, $\text{arity}(\in) = 2$.

Example 2.4. The signature of ordered rings is $\mathcal{C}_\sigma = \{0, 1\}$, $\mathcal{F}_\sigma = \{+, \cdot, -\}$, $\mathcal{R}_\sigma = \{\leq\}$. We have

$$\begin{aligned} \text{arity}(+) &= 2, \\ \text{arity}(\cdot) &= 2, \\ \text{arity}(-) &= 1, \\ \text{arity}(\leq) &= 2. \end{aligned}$$

Example 2.5. $\mathcal{C}_\sigma = \{\text{Sven}\}$, $\mathcal{F}_\sigma = \{\text{Matthew}\}$, $\mathcal{R}_\sigma = \{\text{Spencer}\}$, $\text{arity}(\text{Matthew}) = 5000000000$, $\text{arity}(\text{Spencer}) = 1$.

2.2 Interpretations

Definition 2.6. Given a signature σ, a **σ-structure** $\mathfrak{A}$ consists of:

- a set A, the universe of $\mathfrak{A}$ (we require $A \neq \varnothing$),
- for each $c \in \mathcal{C}_\sigma$, $c^{\mathfrak{A}} \in A$,
- for each $f \in \mathcal{F}_\sigma$, $\text{arity}(f) = n$, $f^{\mathfrak{A}} : A^n \to A$,
- for each $R \in \mathcal{R}_\sigma$, $\text{arity}(R) = n$, $R^{\mathfrak{A}} \subseteq A^n$.

By way of notation: if $\text{arity}(R) = 2$, we often write $a\ R\ b$ for $(a, b) \in R^a$; for a binary operation, i.e. $\text{arity}(f) = 2$, $a\ f\ b := f^a(a, b)$.

Notation: $(\mathbb{R}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, -^{\mathbb{R}}, \leq^{\mathbb{R}})$ is a σ-structure for the signature of ordered rings. $\mathbb{T} = (\mathbb{R}, \wedge, +, x \mapsto 0, \leq)$, where $\wedge$ is min:

$$+^{\mathbb{T}}(x,y) := \min\{x,y\},$$
$$\cdot^{\mathbb{T}}(x,y) := x +^{\mathbb{R}} y.$$

2.3 Terms

Definition 2.7. Given a signature σ and a set $\mathcal{V}$ of variables, we define the set of **σ-terms** $\mathcal{T}(\sigma, \mathcal{V})$ with variables in $\mathcal{V}$ by recursion.

- If $c \in \mathcal{C}_\sigma$, then c is a term.
- If $x \in \mathcal{V}$, then x is a term.
- If $f \in \mathcal{F}_\sigma$, arity$(f) = n$, $t_1, \ldots, t_n \in \mathcal{T}(\sigma, \mathcal{V})$, then $f(t_1, \ldots, t_n) \in \mathcal{V}$.

If $\mathfrak{A}$ is a σ-structure, $t \in \mathcal{T}(\sigma, \mathcal{V})$, and $\iota : \mathcal{V} \to A$ is an assignment of the variables, then $t^{(\mathfrak{A},\iota)} \in A$.

- If $t = c \in \mathcal{C}_\sigma$, $t^{(\mathfrak{A},\iota)} = c^{(\mathfrak{A},\iota)} := c^{\mathfrak{A}}$.
- If $t = x \in \mathcal{V}$, $t^{(\mathfrak{A},\iota)} := \iota(x)$.
- If $t = f(t_1, \ldots, t_n)$, $t^{(\mathfrak{A},\iota)} := f^{\mathfrak{A}}(t_1^{(\mathfrak{A},\iota)}, \ldots, t_n^{(\mathfrak{A},\iota)})$.

Lecture 3

January 23

3.1 Example Proof

Problem: $B \subseteq C \to \mathcal{P}(B) \subseteq \mathcal{P}(C)$.

Proof. By definition of $\subseteq$, we must show that if $x \in \mathcal{P}(B)$, then $x \in \mathcal{P}(C)$.

If $x \in \mathcal{P}(B)$, then by the definition of $\mathcal{P}(B)$, $x \subseteq B$, i.e.

$$(\forall y)\ y \in x \to y \in B. \tag{3.1}$$

By hypothesis, $B \subseteq C$, i.e.

$$(\forall y)\ y \in B \to y \in C. \tag{3.2}$$

Combining (3.1) and (3.2),

$$(\forall y)\ y \in x \to y \in C, \tag{3.3}$$

and by definition, $x \subseteq C$. By the definition of $\mathcal{P}(C)$, $x \in \mathcal{P}(C)$. Therefore, $\mathcal{P}(B) \subseteq \mathcal{P}(C)$. □

3.2 Formulae

Definition 3.1. Given a signature σ and a set of variables $\mathcal{V}$ (usually: $\mathcal{V} := \{x_n : n \in \mathbb{N}\}$; in this case, we drop $\mathcal{V}$ from the notation), we define the set of **σ-formulae** with variables from $\mathcal{V}$, $\mathcal{L}(\sigma, \mathcal{V})$, or just $\mathcal{L}(\sigma)$ if $\mathcal{V}$ is understood, also called the (first-order) **language** associated to σ and $\mathcal{V}$, by recursion:

- Given terms $s, t \in \mathcal{T}(\sigma, \mathcal{V})$, the expression $(s = t)$ is an atomic formula.
- If $R \in \mathcal{R}_\sigma$ and $\text{arity}(R) = n$, and $t_1, \ldots, t_n \in \mathcal{T}(\sigma, \mathcal{V})$, then the expression $R(t_1, \ldots, t_n) \in \mathcal{L}(\sigma, \mathcal{V})$ (atomic).
- If $\varphi, \psi \in \mathcal{L}(\sigma, \mathcal{V})$, then so are:

$$\begin{aligned} \neg\varphi \quad & \text{“not } \varphi\text{”} \\ (\varphi \mathbin{\&} \psi) \quad & \text{“}\varphi \text{ and } \psi\text{” (sometimes } (\varphi \wedge \psi)) \\ (\varphi \vee \psi) \quad & \text{“}\varphi \text{ or } \psi\text{”} \\ (\varphi \to \psi) \text{ (or } \implies) \quad & \text{“}\varphi \text{ implies } \psi\text{”} \end{aligned}$$

- If $\varphi \in \mathcal{L}(\sigma, \mathcal{V})$ and $x \in \mathcal{V}$, then

$$(\exists x)\ \varphi \in \mathcal{L}(\sigma, \mathcal{V}),$$

$$(\forall x)\ \varphi \in \mathcal{L}(\sigma, \mathcal{V}).$$

Example 3.2. In the signature of ordered rings, $\mathcal{C}_\sigma = \{0,1\}$, $\mathcal{F}_\sigma = \{+, \cdot, -\}$, $\mathcal{R}_\sigma = \{\leq\}$, with arity$(+)$ = arity$(\cdot)$ = 2, arity$(-)$ = 1, arity$(\leq)$ = 2, $\mathcal{V} = \{x, y, z\}$, $+(x, 0) = \cdot(y, +(0, z))$ is an atomic formula.

$\leq (+(x, z), y)$ is a formula. Typically we write $(x + z) \leq y$.

Interlude on expansions and reducts: If $\sigma \subseteq \tau$ are signatures (example: $\mathcal{C}_\sigma = \{0\}$, $\mathcal{F}_\sigma = \{+, -\}$, $\mathcal{R}_\sigma = \varnothing$, arity$(+) = 2$, arity$(-) = 1$, $\mathcal{C}_\tau = \{0, 1\}$, $\mathcal{F}_\tau = \{+, \cdot, -\}$, $\mathcal{R}_\tau = \varnothing$, arity$(\cdot) = 2$, and $\mathfrak{A}$ is a τ-structure, then $\mathfrak{A} \restriction \sigma$ ("$\mathfrak{A}$ restricted to σ") is the σ-structure with the same universe and for $S \in \mathcal{C}_\sigma \cup \mathcal{F}_\sigma \cup \mathcal{R}_\sigma$, $S^{(\mathfrak{A} \restriction \sigma)} := S^{\mathfrak{A}}$. $\mathfrak{A} \restriction \sigma$ is also called the reduct of $\mathfrak{A}$ to σ, or simply "a reduct". We call $\mathfrak{A}$ an expansion of $\mathfrak{A} \restriction \sigma$ to τ.

If σ is any signature and $\mathfrak{A}$ is a σ-structure of $B \subseteq A$, then σ_B is the signature with

$$\begin{aligned} \mathcal{C}_{\sigma_B} &:= \mathcal{C}_\sigma \cup B, \\ \mathcal{F}_{\sigma_B} &:= \mathcal{F}_\sigma, \\ \mathcal{R}_{\sigma_B} &:= \mathcal{R}_\sigma. \end{aligned}$$

$\mathfrak{A}_B$ is the σ_B expansion of $\mathfrak{A}$ defined by $b^{\mathfrak{A}_B} := b$. The universe of $\mathfrak{A}$ is A (sometimes written $|\mathfrak{A}|$).

Example 3.3. Take σ: $\mathcal{C}_\sigma = \mathcal{R}_\sigma = \mathcal{F}_\sigma = \varnothing$. $\mathbb{Q}$ is an example of a σ-structure. Take $B := \{2/3\}$. Then $\mathbb{Q}_{\{2/3\}}$ is the underlying universe $\mathbb{Q}$ with $(2/3)^{\mathbb{Q}_{\{2,3\}}} = 2/3$.

Example 3.4. Let $\mathcal{V} = \{x, y\}$, $\mathcal{F}_\sigma = \{+\}$, $\mathcal{R}_\sigma = \{\leq\}$, $\mathcal{C}_\sigma = \{0\}$, arity$(+)$ = arity$(\leq)$ = 2. Consider the formula $(x = y)$. The truth value depends on whether the variables are bound or not.

Consider

$$\varphi : (\exists x)\ (+(x, y) \leq y) \wedge (\forall y)\ \neg(x \leq y).$$

Both variables are both free and bound.

Lecture 4

January 25

4.1 Bound & Free Variables

Let $\mathcal{V} = \{x, y\}$, and consider

$$((\exists x)(x = y) \,\&\, ((y = y) \vee \neg(x = y))).$$

The first x is bound and the second x is free. The first y is free, and the other y variables are bound.

- In an atomic formula, each instance of a variable is **free**.
- In a boolean combination, "each instance of a variable which was free (respectively, bound) in a constituent formula is free (respectively, bound)", i.e.: if $\varphi \in \mathcal{L}(\sigma, \mathcal{V})$,

  $$\varphi = s_0 s_1 s_2 \cdots s_n,$$

  and $\psi = \neg\varphi$,

  $$\psi = \neg s_0 s_1 \cdots s_n,$$

  and $s_j \in \mathcal{V}$, and $x = s_j \in \mathcal{V}$ was free in φ, then the $(j+1)$st position of $\psi = \neg\varphi$ is x and is a free instance of x. If $\theta \in \mathcal{L}(\sigma, \mathcal{V})$ and $\psi = (\varphi \vee \theta)$, write $\theta = r_0 r_1 \cdots r_m$,

  $$\psi = (s_0 \cdots s_n \vee r_0 \cdots r_m),$$

  if $r_j = y \in \mathcal{V}$ is bound in θ, then the $(n+2+j)$th symbol in ψ is y and is bound.
- If $\varphi \in \mathcal{L}(\sigma, \mathcal{V})$ and $x \in \mathcal{V}$, and $\psi = (\exists x)\,\varphi$, then every instance of x is bound in ψ, and if $y \in \mathcal{V}$ and $y \neq x$, then each instance of y in ψ is free (respectively bound) if the corresponding instance of y in φ is free (respectively bound). Likewise for $(\forall x)\,\varphi$.

In $(x = y)$, both variables are free.

In $(y = y)$, both instances of y are free.

In $\neg(x = y)$, both variables are free.

In $(\exists x)(x = y)$, x is bound and y is free.

In $(\forall y)((y = y) \vee \neg(x \neq y))$, the x is free and each y is bound.

In the whole statement

$$((\exists x)(x = y) \,\&\, ((y = y) \vee \neg(x = y))),$$

each variable is free or bound as described above.

4.2 Sentences

Definition 4.1. $\varphi \in \mathcal{L}(\sigma, \mathcal{V})$ is a **sentence** if φ has no free variables. Let σ be a signature and $\mathfrak{A}$ a σ-structure.

- For an atomic sentence φ, $(s = t)$, where s and t are termathfrak, we say $\mathfrak{A} \models \varphi$ ("φ is true in $\mathfrak{A}$" or "$\mathfrak{A}$ satisfies φ" or "$\mathfrak{A}$ models φ") iff $s^a = t^a$. If $\varphi = R(t_1, \ldots, t_n)$, $R \in \mathcal{R}_\sigma$, $t_1, \ldots, t_n \in \mathcal{T}(\sigma, \varnothing)$, arity$(R) = n$, $\mathfrak{A} \models R(t_1, \ldots, t_n)$ iff $(t_1^a, \ldots, t_n^a) \in \mathcal{R}^{\mathfrak{A}} \subseteq A^n$. If $\varphi = \neg\psi$, then $\mathfrak{A} \models \neg\psi$ iff $\mathfrak{A} \models \psi$ is false. $\mathfrak{A} \models (\varphi \vee \psi)$ iff $\mathfrak{A} \models \varphi$ or $\mathfrak{A} \models \psi$. $\mathfrak{A} \models (\varphi \to \psi)$ iff if $\mathfrak{A} \models \varphi$, then $\mathfrak{A} \models \psi$, i.e. either $\mathfrak{A} \not\models \varphi$ or $\mathfrak{A} \models \psi$.

- If $x \in \mathcal{V}$, $\varphi \in \mathcal{L}(\sigma, \mathcal{V})$, $(\exists x)\, \varphi$ is a sentence, $\mathfrak{A} \models (\exists x)\, \varphi$ iff there is some assignment of an element a to x making φ true, iff there is some $a \in A$ such that $\mathfrak{A}_{\{a\}} \models \tilde{\varphi}$, where $\tilde{\varphi}$ is the formula in $\mathcal{L}(\sigma_{\{a\}}, \mathcal{V})$ obtained by replacing each *free* instance of x by a.

4.3 Set Theory

The signature of set theory has

$$\begin{aligned} \mathcal{C}_\sigma &= \varnothing, \\ \mathcal{F}_\sigma &= \varnothing, \\ \mathcal{R}_\sigma &= \{\in\}, \\ \text{arity}(\in) &= 2. \end{aligned}$$

Extensionality Axiom:

$$\varphi = (\forall A)(\forall B)((A = B) \leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B))$$

Last week: we found $\mathfrak{A}$, a σ-structure, such that $\mathfrak{A} \not\models \varphi$, e.g. $A = \{1, 2\}$, $\in^{\mathfrak{A}} = \varnothing$, $\mathfrak{A} \models \neg\varphi$. $\mathfrak{A} \models \varphi$ iff for every choice of $a, b \in A$,

$$\mathfrak{A} \models a = b \leftrightarrow \forall x\, (x \in a \leftrightarrow x \in B).$$

Consider $a = 1$ and $b = 2$. $\mathfrak{A} \not\models a = b$. Hence,

$$\mathfrak{A} \models (\forall x)(x \in a \leftrightarrow x \in b).$$

Lecture 5

January 27

5.1 Empty Set Axiom

ZF (Zermelo-Frenkel Set Theory) is a certain set of sentences in $\mathcal{L}(\in)$.

The theory we will develop is often called ZFC, which is Zermelo-Frenkel set theory with choice.

So far, we have the Extensionality Axiom:

$$(\forall A)(\forall B)[A = B \leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)]$$

The **Empty Set Axiom** says

$$(\exists A)(\forall x)\ \neg(x \in A).$$

We would like to define $x \notin y$ to be $\neg(x \in y)$. To do this formally, the signature of set theory, $\sigma_{\text{Set Theory}}$ has

$$\begin{aligned} \mathcal{C}_{\sigma_{\text{Set Theory}}} &= \varnothing, \\ \mathcal{F}_{\sigma_{\text{Set Theory}}} &= \varnothing, \\ \mathcal{R}_{\sigma_{\text{Set Theory}}} &= \{\in\}, \qquad \text{with arity} = 2. \end{aligned}$$

We extend to σ', with

$$\begin{aligned} \mathcal{C}_{\sigma'} &= \varnothing, \\ \mathcal{F}_{\sigma'} &= \varnothing, \\ \mathcal{R}_{\sigma'} &= \{\in, \notin\}, \qquad \text{arity}(\in) = 2 = \text{arity}(\notin). \end{aligned}$$

Then, $\sigma' \supseteq \sigma_{\text{Set Theory}}$. If $\mathcal{V} = (V, \in^V)$ is a $\sigma_{\text{Set Theory}}$-structure, we can expand $\mathcal{V}$ to a σ'-structure $\mathcal{V}'$ in exactly one way so that

$$\mathcal{V}' \models (\forall x)(\forall y)(x \notin y \leftrightarrow \neg(x \in y)).$$

$\mathcal{V}'$ is a definitional expansion of $\mathcal{V}$.

Δ will contain all of the definitions.

$$(\forall x)(\forall y)(x \notin y \leftrightarrow \neg(x \in y)) \in \Delta$$

Then, the Empty Set Axiom can be written as

$$(\exists A)(\forall x)\ x \notin A.$$

Expand to $\sigma'' \supseteq \sigma'$, with

$$\begin{aligned}\mathcal{C}_{\sigma''} &= \{\varnothing\},\\ \mathcal{F}_{\sigma''} &= \varnothing,\\ \mathcal{R}_{\sigma''} &= \{\in, \notin\}.\end{aligned}$$

We include in Δ

$$(\forall x)[x = \varnothing \leftrightarrow (\forall y)(y \notin x)].$$

Proposition 5.1. *If $(V, \in^V) \models \mathrm{ZF}$, then there is a unique extension $\mathcal{V}'$ to $\mathcal{L}(\sigma'')$ such that $\mathcal{V}' \models \Delta$.*

Proof. We define

$$\begin{aligned}\notin^{\mathcal{V}'} &:= V^2 \setminus \in^{\mathcal{V}}\\ &= \{(a,b) : a, b \in V\} \setminus \in^{\mathcal{V}}\\ &= \{(a,b) : a, b \in V \mathbin{\&} (a,b) \notin \in^{\mathcal{V}}\}.\end{aligned}$$

$\mathcal{V} \models \mathrm{ZF}$, so $\mathcal{V} \models (\exists A)(\forall x)\ x \notin A$. Let $a \in V$ such that $(\mathcal{V}, a) \models \forall x\ x \notin a$. Set $\varnothing^{\mathcal{V}'} := a$. Then $\mathcal{V}' \models \mathrm{ZF} \cup \Delta$.

Why is this the only such expansion? Suppose $\mathcal{V}'' = (V, \in^{\mathcal{V}}, \notin'', \varnothing'')$ and $\mathcal{V}'' \models \mathrm{ZF} \cup \Delta$. Since $\mathcal{V}'' \models \Delta$, $(c,d) \in \mathcal{V}''$ has

$$\begin{aligned}(c,d) \in \notin'' &\iff (c,d) \notin \in^{\mathcal{V}}\\ &\iff (c,d) \in \notin^{\mathcal{V}'}.\end{aligned}$$

$\mathcal{V}'' \models (\forall x)\ x \notin \varnothing$, i.e. for every $c \in V$, $(\mathcal{V}'', c) \models c \notin \varnothing$, i.e. for every $c \in V$, $(c, \varnothing^{\mathcal{V}''}) \in \notin^{\mathcal{V}''}$, i.e. for every $c \in V$, $(c, \varnothing^{\mathcal{V}''} = d) \notin \in^{\mathcal{V}}$, i.e. for every $c \in V$, $(c,d) \notin \in^{\mathcal{V}}$, so that $(\mathcal{V}, d) \models (\forall x)\ \neg(x \in d)$. However, $(\mathcal{V}, a) \models (\forall x)\ \neg(x \in a)$. Hence, $(\mathcal{V}, a, d) \models \forall x\ (x \in d \leftrightarrow x \in a)$, which implies by Extensionality, $(\mathcal{V}, a, d) \models a = d$. □

5.2 Pair Set Axiom

Pair Set Axiom:

$$(\forall x)(\forall y)(\exists z)(\forall w)[w \in z \leftrightarrow (w = x \vee w = y)]$$

Extensionality and the Pair Set Axiom imply that z is unique.

We expand the signature further:

$$\Delta : (\forall x)(\forall y)(\forall z)[z = \{x, y\} \leftrightarrow \forall w\ (w \in z \leftrightarrow (w = x \vee w = y))]$$

Also,

$$(\forall x)(\forall z)(z = \{x\} \leftrightarrow z = \{x, x\}).$$

We can now construct $\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\{\{\varnothing\}\}\}, \ldots$.

Lecture 6

January 30

6.1 Union Axiom

Axioms we have so far:

- Extensionality
- Empty Set
- Pair Set

The next axiom (temporary) is the **Union Axiom**: "$\forall x\, \forall y\, x \cup y$ is a set". Formally,

$$(\forall x)(\forall y)(\exists z)(\forall t)[t \in z \leftrightarrow (t \in x \vee t \in y)].$$

We include in our definitions:

$$\Delta \ni \forall x\, \forall y\, \forall z\, [z = x \cup y \leftrightarrow (\forall t)(t \in z \leftrightarrow (t \in x \vee t \in y))]$$

Proposition 6.1. *For each $n \in \mathbb{Z}_+$,*

$$\forall x_1\, \cdots\, \forall x_n\, \exists z\, \forall t\, [t \in z \leftrightarrow (t = x_1 \vee t = x_2 \vee \cdots \vee t = x_n)].$$

We define

$$z = \{x_1, \ldots, x_n\} \leftrightarrow (\forall t)[t \in z \leftrightarrow (t = x_1 \vee \cdots \vee t = x_n)].$$

Proof. By induction on n.

$n = 1$: For all x_i, by the Pair Set Axiom, $\exists!\, z\, \forall t\, [t \in z \leftrightarrow t = x]$, i.e. $z = \{x_1\}$.

$n + 1$: By the IH, $\forall x_1\, \forall x_2\, \cdots\, \forall x_n\, \exists z\, \forall t\, [t \in z \leftrightarrow \bigvee_{i=1}^{n} t = x_i]$. $z = \{x_1, \ldots, x_n\}$ is a set. By case 1, $\{x_{n+1}\}$ is set. By the Union Axiom, $w := \{x_1, \ldots, x_n\} \cup \{x_{n+1}\}$ is a set.

$$\begin{aligned}(\forall t)\ t \in w &\leftrightarrow t \in \{x_1, \ldots, x_n\} \vee t \in \{x_{n+1}\} \\ &\leftrightarrow \bigvee_{i=1}^{n} t = x_i \vee t = x_{n+1} \\ &\leftrightarrow \bigvee_{i=1}^{n+1} t = x_i \end{aligned}$$ □

6.2 Power Set Axiom

We introduce the subset symbol:

$$\forall x\ \forall y\ (x \subseteq y \leftrightarrow (\forall t)(t \in x \to t \in y)) \in \Delta$$

Power Set Axiom: $(\forall x)(\exists y)(\forall t)[t \in y \leftrightarrow t \subseteq x]$.

$$\forall x\ \forall y\ [y = \mathcal{P}(x) \leftrightarrow (\forall t)[t \in y \leftrightarrow t \subseteq x]] \in \Delta$$

Remark: The Power Set Axiom does not follow from the other axioms.

6.3 Subset Axiom

Given $\varphi \in \mathcal{L}(\in)$ with free variables amongst $t, x_1, \ldots, x_n$ not containing A or B, the **Subset Axiom** for φ says:

$$(\forall A)(\forall x_1) \cdots (\forall x_n)(\exists B)(\forall t)[t \in B \leftrightarrow \varphi \,\&\, t \in A]$$

We write the set as $B = \{t \in A : \varphi(t, x_1, \ldots, x_n)\}$.

Lecture 7

February 1

7.1 Subset Axiom Example

Subset Axiom (Scheme), also called **(Restricted) Comprehension**: For each φ with free variables amongst $t, x_1, \ldots, x_n$ (such that the variables A and B do not appear) we have the axiom

$$(\forall A)(\forall x_1)\cdots(\forall x_n)(\exists B)(\forall t)[t \in B \leftrightarrow (t \in A \,\&\, \varphi)].$$

We write:

$$B = \{t \in A : \varphi(t, x_1, \ldots, t_n)\} \leftrightarrow (\forall t)(t \in B \leftrightarrow (t \in A \,\&\, \varphi(t, x_1, \ldots, x_n))) \in \Delta.$$

Proposition 7.1. *If X and Y are sets, then $X \cap Y$ is also a set.*

Proof. Consider the formula

$$\theta : (t \in x_3 \leftrightarrow (t \in x_1 \,\&\, t \in x_2)).$$

$(\forall t)\, \theta(X/x_1, Y/x_2, Z/x_3)$ is true iff $Z = X \cap Y$. Take

$$\varphi := t \in x_1.$$

Apply the Subset Axiom for φ for $A = X$, $x_1 = Y$. We have

$$(\forall A)(\forall x_1)(\exists B)(\forall t)[t \in B \leftrightarrow (t \in A \,\&\, \varphi)],$$

which is

$$(\forall A)(\forall x_1)(\exists B)(\forall t)[t \in B \leftrightarrow (t \in A \,\&\, t \in x_1)].$$

Substitute X for A and Y for x_1, so

$$(\exists B)(\forall t)[t \in B \leftrightarrow (t \in X \,\&\, t \in Y)],$$

i.e. $X \cap Y$ exists. □

7.2 Union Axiom

Given sets $X_0, X_1, X_2, \ldots,$ we would like to form the union

$$\bigcup_{i=0}^{\infty} X_i = \{t : \exists i \in \mathbb{N}\ t \in X_i\}.$$

There are many problems with this approach. Instead, we will write

$$(\forall y)(\forall x)\ y = \bigcup x \leftrightarrow (\forall t)[t \in y \leftrightarrow (\exists z)[t \in z \;\&\; z \in x]]$$

Then, if $x = \{X_i : i \in \mathbb{N}\}$, we have "$\bigcup x = \bigcup_{i=0}^{\infty} X_i$".

Union Axiom:

$$(\forall x)(\exists y)(\forall t)[t \in y \leftrightarrow (\exists z)[z \in x \;\&\; t \in z]].$$

Proposition 7.2. *The provisional Union Axiom follows from the Pair Set Axiom and the Union Axiom.*

Proof. Given sets a, b, by the Pair Set Axiom, $x := \{a, b\}$ is a set. By the Union Axiom,

$$y := \bigcup x = \bigcup \{a, b\}$$

is a set. For any t,

$$\begin{aligned} t \in y &\leftrightarrow t \in \bigcup x \\ &\leftrightarrow t \in \bigcup \{a, b\} \\ &\leftrightarrow (\exists z)[t \in z \;\&\; z \in \{a, b\}] \\ &\leftrightarrow (\exists z)[t \in z \;\&\; (z = a \vee z = b)] \\ &\leftrightarrow (\exists z)[(t \in z \;\&\; z = a) \vee (t = z \;\&\; z = b)] \\ &\leftrightarrow (t \in a \vee t \in b) \\ &\leftrightarrow t \in a \cup b. \end{aligned}$$

□

7.3 Ordered Pairs

Write $\mathbb{V}$ for the class of all sets. $\mathbb{V} = \{t : t = t\}$ is *not* a set. Apply the Subset Axiom to $A = \mathbb{V}$, $\varphi : \neg(t \in t)$, and $R = \{t \in \mathbb{V} : \neg(t \in t)\}$ would be a set, and $R = \{t : t \notin t\}$. Then $R \in R \leftrightarrow R \notin R$, which is a contradiction.

We want to define an operation $\langle \cdot, \cdot \rangle : \mathbb{V}^2 \to \mathbb{V}$ which maps $a, b \mapsto \langle a, b \rangle$. Then, we want $\pi_1 : \mathbb{V} \to \mathbb{V}$ with $\pi_1(\langle a, b \rangle) = a$ and $\pi_2 : \mathbb{V} \to \mathbb{V}$ with $\pi_2(\langle a, b \rangle) = b$.

We will take $\langle a, b \rangle = \{\{a\}, \{a, b\}\}$.

Lecture 8

February 3

8.1 Ordered Pairs

Definition 8.1. For sets x, y, the **ordered pair** $\langle x, y\rangle := \{\{x\}, \{x, y\}\}$. That is,

$$\forall x\, \forall y\, \forall z\, [z = \langle x, y\rangle \leftrightarrow z = \{\{x\}, \{x, y\}\}] \in \Delta.$$

Proposition 8.2. *For sets a, b, c, d,*

$$\langle a, b\rangle = \langle c, d\rangle \iff a = c \,\&\, b = d.$$

Proof. $\Longleftarrow$: Obvious.

$\Longrightarrow$: Suppose $\langle a, b\rangle = \langle c, d\rangle$, i.e. $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Since $\{a\} \in \langle a, b\rangle = \langle c, d\rangle$, then $\{a\} \in \langle c, d\rangle = \{\{c\}, \{c, d\}\}$, so $\{a\} = \{c\}$ $(a = c)$ or $\{a\} = \{c, d\}$. In the second case, a is the unique member of $\{a\}$, and $c \in \{c, d\} = \{a\}$ which implies that $c = a$. Either way, $a = c$.

By the first case, $\{c, b\} = \{a, b\} \in \langle a, b\rangle = \langle c, d\rangle = \{\{c\}, \{c, d\}\}$. Therefore, we have $\{c, b\} = \{c\}$ or $\{c, b\} = \{c, d\}$. In the first case, $b = c$. $\{b, d\} = \{c, d\} \in \langle a, b\rangle = \{\{a\}, \{a, b\}\}$, so $\{b, d\} = \{a\}$ or $\{b, d\} = \{a, b\}$. If $\{b, d\} = \{a\}$, then $c = a = b = d$. If $\{b, d\} = \{a, b\}$, then $d = a = c = b$, or $d = b$. Otherwise, if $\{c, b\} = \{c, d\}$, then $b = d$ or $b = c$. If $b = c$, then $\{c, b\} = \{c\}$, which implies that $d = c = b$. ☐

Try: $\langle a, b\rangle^* := \{a, \{b\}\}$.

Try "**Proposition**": $\langle a, b\rangle^* = \langle c, d\rangle^* \to a = c \,\&\, b = d$. Can we distinguish $\langle a, b\rangle^*$ and $\langle \{b\}, a\rangle^*$? If $\{a, \{b\}\} = \{\{b\}, \{a\}\}$ so $a = \{a\}$. This does not provide a contradiction unless we introduce another axiom. Also, $\langle \{a\}, b\rangle^* = \langle \{b\}, a\rangle^*$ but the coordinates are not necessarily equal.

Want: $\langle x_1, x_2, x_3\rangle^* =$? We could try $\{\{x_1\}, \{x_1, x_2\}, \{x_1, x_2, x_3\}\}$, but we would have $\langle a, a, b\rangle^* = \langle a, b, a\rangle^*$. We could also try

$$\langle x_1, x_2, x_3\rangle^{**} := \{\underbrace{\{\{\{x_1\}, \{x_1, x_2\}\}\}}_{\{\langle x_1, x_2\rangle\}}, \underbrace{\{\{\{x_1\}, \{x_1, x_2\}\}, x_3\}}_{\{\langle x_1, x_2\rangle, x_2\}}\} = \langle\langle x_1, x_2\rangle, x_3\rangle.$$

This works.

Definition 8.3.

$$\langle x_1, \ldots, x_n \rangle = y \leftrightarrow \begin{cases} y = \{x_1\}, & \text{if } n = 1, \\ y = \{\{x_1\}, \{x_1, x_2\}\}, & \text{if } n = 2, \\ y = \langle \langle x_1, \ldots, x_{n-1} \rangle, x_n \rangle, & \text{if } n > 2. \end{cases}$$

8.2 Cartesian Product

Definition 8.4. If A and B are sets, $A \times B$ is the set of ordered pairs

$$\{\langle a, b \rangle : a \in A \,\&\, b \in B\}.$$

Proposition 8.5. *For any sets A, B, there exists a set C such that*

$$(\forall t)[t \in C \leftrightarrow (\exists a)(\exists b)(t = \langle a, b \rangle \,\&\, a \in A \,\&\, b \in B)],$$

i.e. $C = A \times B$ exists.

Proof.

$$A \times B = \{t \in \mathcal{P}(\mathcal{P}(A \cup B)) : (\exists a)(\exists b)[t \in \langle a, b \rangle \,\&\, a \in A \,\&\, b \in B]\}$$

Why? We need only check that if $t \in A \times B$, then $t \in \mathcal{P}(\mathcal{P}(A \cup B))$. So,

$$(\exists a)(\exists b)\; a \in A \,\&\, b \in B \,\&\, t = \langle a, b \rangle = \{\{a\}, \{a, b\}\}.$$

$a \in A$, so $\{a\} \subseteq A$, so $\{a\} \in \mathcal{P}(A) \subseteq \mathcal{P}(A \cup B)$. Also, $a \in A$ and $b \in B$, so $a, b \in A \cup B$, so $\{a, b\} \in \mathcal{P}(A \cup B)$, so $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. $\square$

Lecture 9

February 6

9.1 Relations

Definition 9.1. A **relation** R is a set of ordered pairs.

$$(\forall R)[\mathsf{Relation}(R) \leftrightarrow (\forall t)[t \in R \to (\exists x)(\exists y)(t = \langle x, y\rangle)]]$$

We write $x\,R\,y$ for $\langle x, y\rangle \in R$.

Definition 9.2.

$$C = \mathrm{dom}(R) \leftrightarrow (\forall t)[t \in C \leftrightarrow (\exists y)(\langle x, y\rangle \in R)]$$

Remark: If R is any set, then $\mathrm{dom}(R)$ makes sense as a set. (We apply the Subset Axiom to the formula

$$\varphi := (\exists y)[\langle t, y\rangle \in x_1]$$

to $x_1 = R$.) We want $A =$ "projection of R to the first coordinate". Let's take $A = \bigcup\bigcup R$. By the Union Axiom, A is a set. If t satisfies $\varphi(R/x_1)$, then $\exists y$ such that

$$\{\{t\}, \{t, y\}\} = \langle t, y\rangle \in R.$$

Then, $\{t\}, \{t, y\} \in \bigcup R$, so $t, y \in \bigcup\bigcup R$, so $\mathrm{dom}(R) \subseteq \bigcup\bigcup R$.

Definition 9.3.

$$C = \mathrm{ran}(R) \leftrightarrow (\forall t)[t \in C \leftrightarrow (\exists x)(\langle x, t\rangle \in R)]$$

Remark: For any R, $\mathrm{ran}(R)$ is a set.

Definition 9.4. The **field** of R is

$$\mathrm{fld}(R) := \mathrm{dom}(R) \cup \mathrm{ran}(R).$$

Proposition 9.5. *For a set R, the following are equivalent:*

1. $\mathsf{Relation}(R)$.
2. $R \subseteq \mathrm{dom}(R) \times \mathrm{ran}(R)$.

3. $(\exists A)(\exists B)\ R \subseteq A \times B$.

Proof. 1 $\to$ 2: Let $t \in R$. As R is a relation,

$$(\exists x)(\exists y)\ t = \langle x, y \rangle.$$

Let x, y witness this existential condition. By the definition of $\mathrm{dom}(R)$, $x \in \mathrm{dom}(R)$ and by the definition of $\mathrm{ran}(R)$, $y \in \mathrm{ran}(R)$. By the definition of the Cartesian product,

$$t = \langle x, y \rangle \in \mathrm{dom}(R) \times \mathrm{ran}(R).$$

By the definition of $\subseteq$,

$$R \subseteq \mathrm{dom}(R) \times \mathrm{ran}(R).$$

2 $\to$ 3: Let $A := \mathrm{dom}(R)$, $B := \mathrm{ran}(R)$.

3 $\to$ 1: If $t \in R$, then as $R \subseteq A \times B$, $t \in A \times B$. So, $(\exists a \in A)(\exists b \in B)(t = \langle a, b \rangle)$, so t is an ordered pair. By definition, $\mathsf{Relation}(R)$. $\square$

Example 9.6. $\varnothing$ is a relation.

Example 9.7. $R = \{\langle \varnothing, \varnothing \rangle\}$ is a relation.

$$\begin{aligned}\mathrm{dom}(R) &= \{\varnothing\},\\ \mathrm{ran}(R) &= \{\varnothing\},\\ \mathrm{fld}(R) &= \{\varnothing\}.\end{aligned}$$

Example 9.8. $N := \{\varnothing\}$. N is *not* a relation.

Proof. Consider $t = \varnothing \in N$. $\varnothing$ is *not* an ordered pair as if $\varnothing = \langle x, y \rangle$ for some x, y. Then,

$$\varnothing = \{\{x\}, \{x, y\}\},$$

which would give $\{x\} \in \varnothing$, but $(\forall t)\ t \notin \varnothing$. Therefore, $\varnothing$ is not an ordered pair and N is *not* a relation. $\square$

9.2 Functions

Definition 9.9. f is a **function** if f is a relation and

$$(\forall x)(\forall y)(\forall z)[(\langle x, y \rangle \in f \ \&\ \langle x, z \rangle \in f) \to y = z].$$

Then,

$$\mathsf{Function}(f) \leftrightarrow [\mathsf{Relation}(f) \ \&\ (\forall x)(\forall y)(\forall z)[(\langle x, y \rangle \in f \ \&\ \langle x, z \rangle \in f) \to y = z]].$$

Definition 9.10. For sets f, A, and B,

$$f : A \to B \iff \mathsf{Function}(f) \ \&\ \mathrm{dom}(f) = A \ \&\ \mathrm{ran}(f) \subseteq B.$$

Definition 9.11. Given $f : A \to B$,

- f is **one-to-one (injective)** if $(\forall x)(\forall y)(\forall z)[(\langle y, x\rangle \in f \;\&\; \langle z, x\rangle \in f) \to y = z]$,
- f is **onto (surjective)** B if $\mathrm{ran}(f) = B$,
- f is **one-to-one and onto (bijective)** if f is one-to-one and f is onto.

Example 9.12. For any set A,

$$I_A : A \to A,$$

defined by

$$(\forall t)[t \in I_A \leftrightarrow (\exists a)[t = \langle a, a\rangle \;\&\; a \in A]]$$

is one-to-one and onto.

Example 9.13. Let $A = \varnothing$, $f : A \to \varnothing$. Such a function does not exist!

Proposition 9.14. *If $f : A \to \varnothing$ is a function, then $A = \varnothing$.*

Proof. If $A \neq \varnothing$, then $\exists x \in A = \mathrm{dom}(f)$. So, $\exists y\ \langle x, y\rangle \in f$, so $\exists y \in \mathrm{ran}(f) \subseteq \varnothing$, which is a contradiction. $\square$

Lecture 10

February 8

10.1 Functions

Definition 10.1.

$$f(x) = y \iff \mathsf{Function}(f) \;\&\; \langle x, y\rangle \in f.$$

Remark: This expression "$f(x) = y$" is technically the interpretation of a ternary relation symbol.

10.1.1 Function Restriction

Last time, we introduced the notation $f : A \to B$.

Definition 10.2. For sets f, A,

$$f \restriction A := f \cap (A \times \operatorname{ran}(f)).$$

Proposition 10.3. *Given f, A,*

1. $\operatorname{dom}(f \restriction A) = \operatorname{dom}(f) \cap A$.
2. *If f is a function, then $f \restriction A$ is a function.*

Proof.

1. If $x \in \operatorname{dom}(f \restriction A)$, then $\exists y\ \langle x, y\rangle \in f \restriction A$, i.e. we have $\langle x, y\rangle \in f$ (so $x \in \operatorname{dom}(f)$) and $\langle x, y\rangle \in A \times \operatorname{ran}(f)$, so $x \in A$, which implies that $x \in \operatorname{dom}(f) \cap A$, i.e. $\operatorname{dom}(f \restriction A) \subseteq (\operatorname{dom} f) \cap A$.

   If $x \in (\operatorname{dom} f) \cap A$, then $\exists y \in \operatorname{ran}(f)\ \langle x, y\rangle \in f$. $x \in A$ implies $\langle x, y\rangle \in A \times \operatorname{ran}(f)$, so we have shown $\operatorname{dom}(f \restriction A) \supseteq (\operatorname{dom} f) \cap A$.

2. f is a function. Take x, y, z such that $\langle x, y\rangle \in f \restriction A = f \cap (A \times \operatorname{ran} f) \subseteq f$ and $\langle x, z\rangle \in f \restriction A \subseteq f$. f is a function, so $y = z$.

$\square$

10.1.2 Composition

Suppose S, R are functions. We want

$$R \circ S = \{\langle x, R(S(x))\rangle : x \in \operatorname{dom} S\}.$$

Definition 10.4. Given R, S,

$$R \circ S := \{t \in \mathrm{dom}(S) \times \mathrm{ran}(R) : (\exists x)(\exists y)(\exists z)[t = \langle x, z\rangle \;\&\; \langle x, y\rangle \in S \;\&\; \langle y, z\rangle \in R]\}.$$

Recall. For any set X,

$$\mathrm{dom}(X) = \left\{x \in \bigcup\bigcup X : (\exists y)(\langle x, y\rangle \in X)\right\}.$$

Proposition 10.5. *If R, S are functions, then $R \circ S$ is a function.*

Proof. Suppose x, u, v are sets such that $\langle x, u\rangle \in R \circ S$ and $\langle x, v\rangle \in R \circ S$. By the definition of $R \circ S$,

$$(\exists y)\langle x, y\rangle \in S \;\&\; \langle y, u\rangle \in R,$$
$$(\exists z)\langle x, z\rangle \in S \;\&\; \langle z, v\rangle \in R.$$

Then, $y = z$ and $u = v$. $\square$

$$\mathrm{dom}(R \circ S) = \{x \in \mathrm{dom}\, S : (\exists y)[y \in \mathrm{dom}\, R \;\&\; \langle x, y\rangle \in S]\}.$$

Corollary 10.6. *If $S : A \to B$ and $R : B \to C$, then $R \circ S : A \to C$.*

10.1.3 Inverse

Definition 10.7. Given R,

$$R^{-1} := \{t \in \mathrm{ran}(R) \times \mathrm{dom}(R) : (\exists x)(\exists y)\; t = \langle y, x\rangle \;\&\; \langle x, y\rangle \in R\}.$$

What is $R \circ R^{-1}$? What is $R^{-1} \circ R$?

Proposition 10.8. *If R is a function, i.e. $R : A \to B$, is onto, then $R \circ R^{-1} = I_B$.*

Proof. Let $x \in B = \mathrm{ran}\, R$. Then, $(\exists y)\; \langle y, x\rangle \in R$, so $\langle x, y\rangle \in R^{-1}$. Therefore, $\langle x, x\rangle \in R \circ R^{-1}$ and $I_{\mathrm{ran}(R)} \subseteq R \circ R^{-1}$.

For the other direction, we use the fact that R is a function. Suppose $\langle x, z\rangle \in R \circ R^{-1}$. So,

$$\exists y\; \langle x, y\rangle \in R^{-1} \;\&\; \langle y, z\rangle \in R.$$

Then, $\langle y, x\rangle \in R$. Hence, $x = z$. $\square$

Definition 10.9.

$$z = x \setminus y = \{t \in x : t \notin y\}.$$

Proposition 10.10. *The following are equivalent for $f : A \to B$ (with $A \neq \varnothing$).*

1. *f is one-to-one.*
2. *f^{-1} is a function.*

3. $(\exists g)$ $g : B \to A$ *and* $g \circ f = I_A$.

We could also add:

(2.5) $f^{-1} \circ f = I_A$.

Proof. 1 $\implies$ 2: Take x, y, z, sets. Suppose $\langle x, y\rangle \in f^{-1}$ (so $\langle y, x\rangle \in f$) and $\langle x, z\rangle \in f^{-1}$ (so $\langle z, x\rangle \in f$). Then, $y = z$.

2 $\implies$ 3: Let $a \in A$. Let $g := f^{-1} \cup (B \setminus \operatorname{ran}(f)) \times \{a\}$. f^{-1} is a function by 2. Suppose $\langle x, y\rangle \in g$, $\langle x, z\rangle \in g$. Either $x \in \operatorname{ran}(f)$ or $x \notin \operatorname{ran}(f)$. In the first case, $\langle x, y\rangle \in f^{-1}$ & $\langle x, z\rangle \in f^{-1}$, so $y = z$. In the second case, $\langle x, y\rangle = \langle x, a\rangle$ and $\langle x, z\rangle = \langle x, a\rangle$, so $y = z$. Take $x \in A$.

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) = f^{-1}(f(x)) \\ &= x\end{aligned}$$

3 $\implies$ 1: Suppose $\langle y, x\rangle \in f$, $\langle z, x\rangle \in f$.

$$y = g(f(y)) = g(x) = g(f(z)) = (g \circ f)(z) = z,$$

so f is one-to-one. □

Question. If $f : A \to B$ is a function, under what condition is f onto?

Lecture 11

February 10

11.1 Axiom of Choice

Proposition 11.1. *$f : A \to B$ is onto if $\exists g : B \to A$ $f \circ g = I_B$.*

Proof. Let $b \in B$. Then

$$\begin{aligned} b &= I_B(b) \\ &= (f \circ g)(b) \\ &= f(g(b)). \end{aligned}$$

Thus, $b \in \operatorname{ran}(f)$, so f is onto. □

Proposition 11.2. *If $f : A \to B$ is onto, then $\exists g : B \to A$ $f \circ g = I_B$.*

Proof. We know that $f \circ f^{-1} = I_B$.

We want $g : B \to A$ such that for each $b \in B$, $f(g(b)) = b$. We want to define $g(b)$ to be *some* a with $f(a) = b$. Just do that! Set $g(b)$ to be some choice of a with $f(a) = b$. □

If we have a statement $(\exists a)(a \in A)$, then we can find a witness. However, from the statement $(\forall b)(\exists a)\ \varphi$, if B is infinite, then we cannot form the association $b \mapsto a$ without the Axiom of Choice.

Axiom of Choice [I, Official]:

$$(\forall R)[\mathsf{Relation}(R) \to (\exists g)(g \subseteq R \,\&\, \mathsf{Function}(g) \,\&\, \operatorname{dom}(g) = \operatorname{dom}(R))].$$

Proof (Continued). To finish the proof, apply the Axiom of Choice to $R = f^{-1}$ to get $g \subseteq R = f^{-1}$, a function with $\operatorname{dom}(g) = \operatorname{dom}(R) = \operatorname{dom}(f^{-1})$. Let $b \in B$. Then, $\langle b, g(b)\rangle \in g \subseteq R = f^{-1}$, i.e. $\langle g(b), f(g(b))\rangle = \langle g(b), b\rangle \in f$. Therefore, $b = f(g(b)) = (f \circ g)(b)$, so g is a right inverse of f. □

AC 0:

$$(\forall f)(\forall A)(\forall B)[f : A \to B \,\&\, \operatorname{ran} f = B \leftrightarrow (\exists g)[g : B \to A \,\&\, f \circ g = I_B]].$$

Proposition 11.3. *Relative to the other axioms of set theory, AC I $\leftrightarrow$ AC 0.*

Proof. $\Longleftarrow$: We just did this part.

$\Longrightarrow$: Given a relation R, we need to find $g \subseteq R$, a function, with $\mathrm{dom}(g) = \mathrm{dom}(R)$. Let $B = \mathrm{dom}(R)$ and

$$\begin{aligned} f &: R \to \mathrm{dom}(R) = B, \\ &\langle x, y\rangle \mapsto x, \end{aligned}$$

that is,

$$f = \{t \in R \times \mathrm{dom}\, R : \exists x\ \exists y\ t = \langle\langle x, y\rangle, x\rangle \;\&\; \langle x, y\rangle \in R\}.$$

Then, $f : R \to \mathrm{dom}\, R$ and f is *onto* $\mathrm{dom}(R)$. (Why? Take $x \in \mathrm{dom}(R)$. By definition, $\exists y\ \langle x, y\rangle \in R$. Then, $x = f(\langle x, y\rangle)$.) Apply AC 0 to obtain $g : \mathrm{dom}(R) \to R$ such that $f \circ g = I_{\mathrm{dom}(R)}$. Define $\tilde{g} := \{\langle x, y\rangle : \langle x, y\rangle = g(x)\}$. $\tilde{g} \subseteq R$, $\tilde{g}$ is a function, and $\mathrm{dom}(\tilde{g}) = \mathrm{dom}(R)$. □

11.2 Cardinality

Proposition 11.4. *Consider $f : A \to B$ and $g : B \to C$.*

1. *If f and g are one-to-one, then $g \circ f$ is one-to-one.*
2. *If f and g are onto, then $g \circ f : A \to C$ is onto.*

Proof.

1. Exercise.
2. Let $c \in C$. By hypothesis, $\exists b \in B\ g(b) = c$. f is onto B, so $\exists a \in A\ f(a) = g(b)$.

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) \\ &= g(b) \\ &= c \end{aligned}$$

□

Corollary 11.5. *If $f : A \to B$, $g : B \to C$ are bijective, then so is $g \circ f : A \to C$.*

Definition 11.6. $A \approx B$ ("A and B have the same cardinality") iff

$$(\exists f)[f : A \to B \text{ is one-to-one and onto}].$$

Lecture 12

February 13

12.1 Power Set Cardinality

Recall: $A \approx B$ means $(\exists f)(f : A \to B$ a bijection).

- $A \approx A$ (take $f = I_A$).
- $A \approx B \to B \approx A$ (if $f : A \to B$ is a bijection, then f^{-1} is a function, $\mathrm{dom}(f^{-1}) = \mathrm{ran}(f) = B$, $\mathrm{ran}(f^{-1}) = \mathrm{dom}(f) = A$, $f \circ f^{-1} = I_B$, and $f^{-1} \circ f = I_A$).
- $(A \approx B \,\&\, B \approx C) \to A \approx C$ (if $f : A \to B$ is bijective and $g : B \to C$ is bijective, $g \circ f : A \to C$ is also bijective).

Definition 12.1. For X, Y sets,

$$^{Y}X := \{f \in \mathcal{P}(Y \times X) : f : Y \to X\}.$$

Example 12.2. Take $X = \{0, 1\}$, $Y = \{0, 1, 2\}$. Then

$$^{Y}X = \{f : f : Y \to X\}$$

is the set of "triples" of 0s and 1s. There are 8 elements in ^{Y}X.

If we take "X^Y" to be ^{X}Y, the set of "pairs" of elements of $\{0, 1, 2\}$, there are 9 such elements.

We will define

$$\begin{aligned}
&0 := \varnothing, \\
&1 := \{\varnothing\} = \{0\}, \\
&2 := \{\varnothing, \{\varnothing\}\} = \{0, 1\}, \\
&3 := \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \\
&\;\vdots
\end{aligned}$$

Definition 12.3. Given R and Y,

$$R[\![Y]\!] := \{x \in \mathrm{ran}\, R : (\exists y)(y \in X \,\&\, \langle y, x\rangle \in R)\}.$$

Often, if $R = f^{-1}$, we write $f^{-1}Y$ for $R[\![Y]\!]$.

Proposition 12.4.

$$(\forall X)\ \mathcal{P}(X) \approx {}^X 2.$$

Proof. Define $\chi : \mathcal{P}(X) \to {}^X 2$ by

$$X \subseteq Y \mapsto \left[x \mapsto \begin{cases} 1, & \text{if } x \in Y \\ 0, & \text{if } x \in X \setminus Y \end{cases} \right],$$

i.e. $\chi = \{\langle Y, f\rangle \in \mathcal{P}(X) \times {}^X 2 : f = (Y \times \{1\}) \cup (X \setminus Y) \times \{0\}\}$. [*Recall*: $X \setminus Y := \{t \in X : t \notin Y\}$.] Define

$$\begin{aligned} Z &: {}^X 2 \to \mathcal{P}(X), \\ &f \mapsto f^{-1}\{1\} := \{x \in X : f(x) = 1\}. \end{aligned}$$

Then,

$$\begin{aligned} Z \circ \chi &= I_{\mathcal{P}(X)}, \\ \chi \circ Z &= I_{{}^X 2}, \end{aligned}$$

so χ is one-to-one and onto. □

Preview:

$$\begin{aligned} \mathbb{R} &\approx \{t \in \mathbb{C} : t \text{ is irrational}\} = \mathbb{C} \setminus \mathbb{Q} \\ &\approx \{t \in \mathbb{C} : t \text{ is transcendental}\} \end{aligned}$$

12.2 Equivalence Relations & Partial Orders

Definition 12.5. E is an **equivalence relation** on A:

$$\begin{aligned} \mathsf{EqRel}(E, A) \leftrightarrow (&\mathsf{Relation}(E) \\ &\&\ \text{fld}(E) = A \\ &\&\ (\forall a)[a \in A \to \langle a, a\rangle \in E] \end{aligned}$$

(E is reflexive on A, or $E \supseteq I_A$, where $A = \text{fld}(E)$)

$$\&\ (\forall a)(\forall b)[\langle a, b\rangle \in E \to \langle b, a\rangle \in E]$$

(E is symmetric, $E^{-1} \subseteq E$)

$$\&\ (\forall a)(\forall b)(\forall c)[(\langle a, b\rangle \in E\ \&\ \langle b, c\rangle \in E) \to \langle a, c\rangle \in E])$$

(E is a transitive relation, $E \circ E \subseteq E$)

Definition 12.6. R is a **(non-strict) partial order** if R is reflexive and transitive.

Example 12.7. If X is any set,

$$\{\langle A, B\rangle \in \mathcal{P}(X) \times \mathcal{P}(X) : A \subseteq B\}$$

is a partial order.

Definition 12.8. If E is an equivalence relation on A and $a \in A$, then $[a]_E := \{b \in A : a \mathrel{E} b\}$ is the **E-equivalence class of** a.

Proposition 12.9. *If E is an equivalence relation on A and $a, b \in A$, then either $[a]_E \cap [b]_E = \varnothing$ or $[a]_E = [b]_E$.*

Proof. Suppose $[a]_E \cap [b]_E \neq \varnothing$. Let $c \in [a]_E \cap [b]_E$, i.e. $a \mathrel{E} c$ & $b \mathrel{E} c$. By reflexivity, $c \mathrel{E} b$, and by transitivity, $a \mathrel{E} b$. If $x \in [b]_E$, i.e. $b \mathrel{E} x$, by transitivity $a \mathrel{E} x$, i.e. $x \in [a]_E$, so $[b]_E \subseteq [a]_E$. Reversing roles, $[a]_E \subseteq [b]_E$, which implies $[a]_E = [b]_E$. □

Lecture 13

February 15

13.1 Equivalence Relations and Partitions

Proposition: If E is an equivalence relation on X and $a, b \in X$, then $[a]_E = [b]_E$ or $[a]_E \cap [b]_E = \varnothing$.

Definition 13.1. If E is an equivalence relation on X,

$$X/E := \{t \in \mathcal{P}(X) : (\exists a)[a \in X \;\&\; t = [a]_E]\}.$$

Also, we define

$$\begin{aligned} \pi_E : X &\to X/E, \\ a &\mapsto [a]_E. \end{aligned}$$

Proposition 13.2. *If E is an equivalence relation on X, then X/E is a set of disjoint sets.*

Proposition 13.3. *If E is an equivalence relation on X, then*

$$X = \bigcup X/E.$$

Proof. If $x \in \bigcup X/E$, then $\exists a \in X \; x \in [a]_E = \{t \in X : a \; E \; t\} \subseteq X$, so $x \in X$. Therefore, $X/E \subseteq X$.

For the other inclusion: if $x \in X$, then $x \in [x]_E$. Therefore, $x \in \bigcup X/E$, and $X/E \subseteq X$.

Hence, $X = \bigcup X/E$. □

Definition 13.4. Π is a partition of X if and only if

1. $X = \bigcup \Pi$,
2. $\forall \pi, \rho \in \Pi \; \pi = \rho$ or $\pi \cap \rho = \varnothing$,
3. $\varnothing \notin \Pi$.

Proposition 13.5. *If E is an equivalence relation on X, then X/E is a partition of X.*

Proof.

1. 13.3.
2. 13.2.
3. If $\pi \in X/E$, then $(\exists a)(a \in X \,\&\, \pi = [a]_E)$ and $a \in [a]_E$ because $a \, E \, a$. Hence, $\pi \neq \varnothing$.

$\square$

Proposition 13.6. *If Π is a partition of X, then there exist E, an equivalence relation on X, such that $\Pi = X/E$.*

Proof. Let

$$E := \{t \in X \times X : (\exists a)(\exists b)(\exists \pi)[t = \langle a, b\rangle \,\&\, \pi \in \Pi \,\&\, a \in \pi \,\&\, b \in \pi]\}.$$

E is a relation with $\operatorname{fld}(E) \subseteq X$.

- Let $a \in X = \bigcup \Pi$. This implies that $\exists \pi \in \Pi \; a \in \pi$. By the definition of E, $\langle a, a\rangle \in E$. Therefore, E is reflexive with $\operatorname{dom}(E) = \operatorname{ran}(E) = X$.
- Suppose $\langle a, b\rangle \in E$. Then, by the definition of E,

  $$(\exists \pi)[a \in \pi \,\&\, b \in \pi \,\&\, \pi \in \Pi].$$

  Then,

  $$(\exists \pi)[b \in \pi \,\&\, a \in \pi \,\&\, \pi \in \Pi],$$

  so $\langle b.a\rangle \in E$.
- Suppose $\langle a, b\rangle \in E$ and $\langle b, c\rangle \in E$. Then,

  $$(\exists \pi)(\exists \rho)[(a \in \pi \,\&\, b \in \pi \,\&\, \pi \in \Pi) \,\&\, (b \in \rho \,\&\, c \in \rho \,\&\, \rho \in \Pi)].$$

  $b \in \pi \cap \rho$, so $\pi = \rho$. $a \in \pi = \rho$ and $c \in \rho$, so $a \, E \, c$.

Therefore, E is an equivalence relation.

Suppose $t \in X/E$. $t = [a]_E$ for some $a \in X$. Let $\pi \in \Pi$ such that $a \in \pi$. If $b \in \pi$, then $a, b \in \pi$, which implies that $a \, E \, b$, so $b \in [a]_E = t$. Therefore, $\pi \subseteq [a]_E$. If $c \in [a]_E$, i.e. $a \, E \, c$, then

$$(\exists \rho)[\rho \in \Pi \,\&\, a \in \rho \,\&\, c \in \rho].$$

Then, $a \in \rho \cap \pi$ implies $\pi = \rho$, so $c \in \pi$. We have shown $t = [a]_E \subseteq \pi$, so $t = \pi$, and $X/E \subseteq \Pi$.

If $\pi \in \Pi$, Π is a partition, so $\pi \neq \varnothing$. Therefore, $(\exists a)\; a \in \pi \subseteq X$.

Claim: $\pi = [a]_E$.

Therefore, $\Pi = X/E$. $\square$

Proposition 13.7. *If $f : X \to Y$ is given, then*

$$E_f := \{t \in X \times X : (\exists x)(\exists y)[x \in X \,\&\, y \in X \,\&\, f(x) = f(y) \,\&\, t = \langle x, y\rangle]\},$$

*the **fiber equivalence relation**, is an equivalence relation on X.*

Proposition 13.8. *If E is an equivalence relation on X, then $\exists f : X \to Y$ such that $E = E_f$.*

Proof. Let $f := \pi_E : X \to X/E$.

$$\pi_E(a) = [a]_E.$$

If $\langle a, b\rangle \in E_f$, then $[a]_E = [b]_E$, which implies that $a \, E \, b$. Therefore, $E_f \subseteq E$. If $\langle a, b\rangle \in E$, i.e. $a \, E \, b$, then $f(a) = [a]_E = [b]_E = f(b)$. $a \, E_f \, b$, so $E = E_f$. □

Theorem 13.9. *If E is an equivalence relation on X and $f : X \to Y$ is a function which respects E, i.e. $x \, E \, y \implies f(x) = f(y)$, then $\exists! \, \bar{f} : X/E \to Y$ such that $f = \bar{f} \circ \pi_E$.*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi_E"] & Y \\ X/E \arrow[ur, dashed, "\exists! \bar{f}"'] & \end{tikzcd}$$

Proof. Let $\bar{f} : \{t \in (X/E) \times Y : (\exists x) \; t = \langle [x]_E, f(x)\rangle\}$. $\bar{f} \subseteq (X/E) \times Y$. If $\langle a, b\rangle \in \bar{f}$ and $\langle a, c\rangle \in \bar{f}$, then $\exists x \in X \; \langle a, b\rangle = \langle [x]_E, f(x)\rangle$ and $\exists y \; \langle a, c\rangle = \langle [y]_E, f(y)\rangle$. Then, $[x]_E = [y]_E$ implies that $f(x) = f(y)$.

$\mathrm{dom}(\bar{f}) \subseteq X/E$. If $a \in X/E$, let $x \in X$ such that $a = [x]_E$. Then, $\langle a, f(x)\rangle \in \bar{f}$, so $a \in \mathrm{dom}(\bar{f})$.

If $x \in X$,

$$(\bar{f} \circ \pi_E)(x) = \bar{f}([x]_E)$$

(because $\langle [x]_E, f(x)\rangle \in \bar{f}$)

$$= f(x).$$ □

Lecture 14

February 17

14.1 Review Lecture

14.1.1 Definitions

As an example, here is the formal definition of the union:

$$(\forall y)(\forall x)\left[y = \bigcup X \leftrightarrow (\forall t)[t \in y \leftrightarrow (\exists z)[z \in x \,\&\, t \in z]]\right]$$

As another example, Π is a partition of A iff

- $(\forall x)(x \in A \to \exists!\, \pi \in \Pi\ x \in \pi)$,
- $(\forall \pi)[\pi \in \Pi \leftrightarrow \pi \subseteq A]$,
- $(\forall \pi)[\pi \in \Pi \to \pi \neq \varnothing]$.

We could break up the uniqueness condition into the two statements

$$(\forall x)[x \in A \to (\exists \pi)[x \in \pi \,\&\, \pi \in \Pi]]$$

and

$$(\forall \pi)(\forall \rho)[\pi \in \Pi \,\&\, \rho \in \Pi \to (\pi = \rho \vee \pi \cap \rho = \varnothing)].$$

The first of these could equivalently be written as $A = \bigcup \Pi$. If we are not allowed to use the empty set symbol, we could write

$$(\forall x)[x = \varnothing \leftrightarrow (\forall t)[t \in x \leftrightarrow \neg(t = t)]]$$

or

$$(\forall x)(x = \varnothing \leftrightarrow (\forall t)[\neg(t \in x)]).$$

We must also define the subset and intersection:

- $(\forall x)(\forall y)[x \subseteq y \leftrightarrow \forall t\ (t \in x \to t \in y)]$,
- $(\forall x)(\forall y)(\forall z)[z = x \cap y \leftrightarrow (\forall t)[t \in z \leftrightarrow (t \in x \,\&\, t \in y)]]$.

(We could have formally added a symbol $\mathsf{IsPartitionOf}(X, A)$.)

Additionally, $(\exists a \in A) \cdots$ means $(\exists a)[a \in A \,\&\, \cdots]$.

14.1.2 Axiom of Choice

Proposition 14.1.

$$AC\ I \leftrightarrow (\forall \Pi)\left[\Pi \textit{ a partition} \rightarrow (\exists y)\left[y \subseteq \bigcup \Pi \,\&\, (\forall \pi)[\pi \in \Pi \rightarrow (\exists x)(\pi \cap y = \{x\})]\right]\right].$$

Proof. AC I:

$$(\forall R)[\mathsf{Relation}(R) \rightarrow (\exists f)[\mathsf{Function}(f) \,\&\, f \subseteq R \,\&\, \operatorname{dom} f = \operatorname{dom} R]].$$

$\Longrightarrow$: Let $A = \bigcup \Pi$. Let $R \subseteq \Pi \times A$ be defined by

$$R = \{\langle \pi, a\rangle \in \Pi \times A : a \in \pi\}.$$

Claim: $\operatorname{dom} R = \Pi$.

- Clearly $\operatorname{dom} R \subseteq \Pi$.
- If $\pi \in \Pi$, then $\pi \neq \varnothing$ and $\pi \subseteq A$, so $(\exists a)[a \in A \,\&\, a \in \pi]$, so $\langle \pi, a\rangle \in R$.

Therefore, $\operatorname{dom} R = \Pi$.

By AC I, $\exists f : \Pi \rightarrow A$ such that $f \subseteq R$. Set $y := \operatorname{ran} f \subseteq A$. Let $\pi \in \Pi$. Then, $\langle \pi, f(\pi)\rangle \in R$, so

$$y = \operatorname{ran} f \ni f(\pi) \in \pi.$$

This gives $f(\pi) \in \pi \cap y$. If $t \in \pi \cap y$, then $(\exists x)[x \in \Pi = \operatorname{dom} f\ \ t = f(x)]$. Then $\langle x, f(x)\rangle \in R$, so $x \in \Pi$ and $f(x) \in x$, and $f(x) \in \pi$. Hence, $f(x) \in x \cap \pi$, so $x = \pi$, so $t = f(x) = f(\pi)$. Therefore, $y \cap \pi = \{f(\pi)\}$.

$\Longleftarrow$: Given a relation R, we need to find $f \subseteq R$, a function with $\operatorname{dom} f = \operatorname{dom} R$. Let π be the partition of R associated to the equivalence relation,

$$\langle a, b\rangle \sim \langle c, d\rangle \iff a = c.$$

By the assertion on partitions, $\exists y \subseteq R$ such that $\forall \pi \in \Pi\ \exists x\ y \cap \pi = \{x\}$.

Claim: y is a function and $\operatorname{dom} y = \operatorname{dom} R$.

Proof: $y \subseteq R$ implies that y is also a relation. Suppose $\langle a, b\rangle \in y$ and $\langle a, c\rangle \in y$. Then, $\langle a, b\rangle \sim \langle a, c\rangle$, hence $\exists \pi \in \Pi\ \langle a, b\rangle \in \pi \,\&\, \langle a, c\rangle \in \pi$. Since $\langle a, b\rangle \in \pi \cap y$ and $\langle a, c\rangle \in \pi \in y$, and $\pi \cap y$ is a singleton, $\langle a, b\rangle = \langle a, c\rangle$, which implies that $b = c$. If $a \in \operatorname{dom} R$, $\exists b\ \langle a, b\rangle \in R$. Let $\pi \in \Pi$ such that $\langle a, b\rangle \in \pi$. Then, $\langle a, y(a)\rangle \in y \cap \pi$. Therefore, $a \in \operatorname{dom} y$. Hence, $\operatorname{dom} y = \operatorname{dom} R$. $\square$

Lecture 15

February 24

15.1 Natural Numbers

Definition 15.1. $0 := \varnothing$.

The **successor of** x is $x^+ := x \cup \{x\}$.

From the definition,

$$\begin{aligned} 1 &:= 0^+ = \varnothing \cup \{\varnothing\} \\ &= \{\varnothing\}, \\ 2 &:= 1^+ \\ &= \{\varnothing\} \cup \{\{\varnothing\}\} \\ &= \{\varnothing, \{\varnothing\}\} \\ &= \{0, 1\}, \\ 3 &:= 2^+ = \{0, 1, 2\}. \end{aligned}$$

"**Definition**": The set of natural numbers is $\omega := \{0, 1, 2, 3, \dots\}$. We would like to say

$$(\forall t)[t \in \omega \leftrightarrow \text{formula of set theory}],$$

but we need another approach.

15.1.1 Inductive Sets

Definition 15.2. A set I is **inductive** iff

$$0 \in I \mathbin{\&} (\forall x)(x \in I \to x^+ \in I).$$

Question: Is it possible for $x = x^+$?

Definition 15.3. t is a **natural number** if for every inductive set I, $t \in I$. In other words, t is a natural number iff

$$(\forall I)[I \text{ inductive} \to t \in I].$$

We could have written the "intersection of inductive sets",

$$t \in \bigcap X \iff (\forall Y)(Y \in X \to t \in Y),$$

but the problem is that if $X = \varnothing$, then $(\forall t)\ t \in \bigcap X$, which is not a set.

$\{1\}$ is *not* a natural number. How do we prove this? $\{1\} \notin \{\varnothing, \{\varnothing\}\}$, but $\{\varnothing, \{\varnothing\}\}$ is not inductive. On the other hand, $\{1\} \notin \omega$, but we don't know that ω exists.

Axiom of Infinity:

$$(\exists I)(I \text{ is inductive}).$$

Proposition 15.4.

$$(\exists \omega)\ t \in \omega \leftrightarrow t \textit{ is a natural number.}$$

Proof. Let I be an inductive set. Let $\omega := \{t \in I : (\forall J)[J \text{ inductive} \to t \in J]\}$. This is a set by the Subset Axiom.

If t is a natural number, then $t \in I$ and

$$(\forall J)[J \text{ inductive} \to t \in J],$$

so $t \in \omega$. Conversely, if $t \in \omega$, then t is a natural number. □

Proposition 15.5. *ω is inductive.*

Proof. For any inductive J, $0 \in J$. Therefore, $0 \in \omega$. If $x \in \omega$, then

$$(\forall J)\ J \text{ inductive} \to x \in J \to x^+ \in J,$$

so $x^+ \in \omega$. □

Proposition 15.6. *If A is an inductive set, then $A \supseteq \omega$.*

Proof. If A is inductive, then

$$(\forall t)(\underbrace{t \text{ is a natural number}}_{t \in \omega} \to t \in A),$$

so $\omega \subseteq A$. □

Proposition 15.7. *If $A \subseteq \omega$ and $0 \in A$ and $(\forall n)(n \in A \to n^+ \in A)$, then $A = \omega$.*

Proof. A is inductive, so by 15.6, $\omega \subseteq A$. Since $A \subseteq \omega$, we have $A = \omega$. □

Are there other inductive sets? Consider:

$$\begin{aligned} \omega &= \{0, 1, 2, 3, \dots\}, \\ \omega^+ &= \{0, 1, 2, 3, \dots, \omega\}, \\ \omega^{++} &= \{0, 1, 2, 3, \dots, \omega, \omega^+\}, \\ &\vdots \end{aligned}$$

$$\omega^{\overbrace{+\cdots+}^{n \text{ times}}} = \{0, 1, 2, 3, \ldots, \omega, \omega^+, \ldots, \omega^{\overbrace{+\cdots+}^{n-1 \text{ times}}}\},$$
$$\vdots$$
$$\omega \cdot 2 = \{0, 1, 2, \ldots, \omega, \omega^+, \omega^{++}, \ldots\}.$$

$\omega \cdot 2$ is inductive, but we need another axiom to show that it exists.

15.1.2 Transitive Sets

Plan: We will order ω by saying

$$\begin{aligned} n < m &\iff n \in m \\ &\iff n \subsetneq m. \end{aligned}$$

Definition 15.8. x is a **transitive set** if $(\forall y)(\forall z)[z \in y \;\&\; y \in x \to z \in x]$.

Proposition 15.9.

$$(\forall k)[k \in \omega \to k \text{ is transitive}].$$

Lecture 16

February 27

16.1 Transitive Sets

We would like to define ω as $\{0, 1, 2, 3, \dots\}$, but this never correctly defines a set. This is a result from first-order logic.

Definition: x is a **transitive set** if and only if $(\forall y)(\forall z)[(z \in y \,\&\, y \in x) \to z \in x]$.

Proposition 16.1. *The following are equivalent.*

1. *x is transitive.*
2. *$\bigcup x \subseteq x$.*
3. *$x \subseteq \mathcal{P}x$.*

Proof. 1 $\implies$ 3: Let $y \in x$. Then, by transitivity of x,

$$(\forall z)[z \in y \to z \in x],$$

so $y \subseteq x$, which says $y \in \mathcal{P}(x)$. Therefore, $x \subseteq \mathcal{P}(x)$.

3 $\implies$ 2: Let $z \in \bigcup x$, i.e. $(\exists y)(y \in x \subseteq \mathcal{P}x \,\&\, z \in y)$. Then, $y \subseteq x$, so $z \in y \to z \in x$, which implies $\bigcup x \subseteq x$.

2 $\implies$ 1. Let $y \in x$ and $z \in y$. Then, by 2, $z \in \bigcup x \subseteq x$, so $z \in x$. Therefore, x is transitive. □

Lemma 16.2. *If x is transitive, then so is x^+.*

Proof.

$$\begin{aligned}
\bigcup(x^+) &= \bigcup(x \cup \{x\}) \\
&= \bigcup x \cup \bigcup\{x\} \\
&= \bigcup x \cup x \\
&\subseteq x \cup x = x \subseteq x \cup \{x\} = x^+.
\end{aligned}$$

□

Lemma 16.3. *If $k \in \omega$, then $k^+ \in \omega$.*

Proof. If $k \in \omega$, then for every inductive set I, $k \in I$. $k \in I$, which is inductive, so $k^+ \in I$, so $k^+ \in \omega$. □

Proposition 16.4.

$$(\forall k)[k \in \omega \to k \textit{ is transitive}]$$

Proof. Let $A := \{k \in \omega : k \text{ is transitive}\}$.

Goal: To show $A = \omega$, it suffices to show that A is inductive.

$0 = \varnothing$ is transitive as

$$\bigcup \varnothing = \varnothing \subseteq \varnothing.$$

By 16.2, if $k \in A$, then k^+ is transitive, so $k^+ \in A$. Hence, A is inductive, which gives

$$\omega \subseteq A \subseteq \omega,$$

so $A = \omega$. Therefore, $(\forall k)\ k \in \omega \to k$ is transitive. □

Proposition 16.5. *ω is transitive.*

Proof. Let

$$A := \{k \in \omega : k \subseteq \omega\}.$$

We will show A is inductive.

$$0 = \varnothing \subseteq \omega,$$

so $0 \in A$. Suppose $k \in A$. Then,

$$k^+ = \underbrace{k}_{\subseteq \omega} \cup \underbrace{\{k\}}_{\subseteq \omega} \subseteq \omega,$$

so A is inductive, which implies $A = \omega$.

Therefore, $(\forall k)[k \in \omega \to k \subseteq \omega]$, so $\omega \subseteq \mathcal{P}(\omega)$, so ω is transitive. □

Corollary 16.6.

$$(\forall k)(k \in \omega \to k \textit{ is a set of transitive sets}).$$

ω is a set of transitive sets.

16.2 Recursion

Theorem 16.7 (Construction by Recursion)**.** *Given a function $g : A \to A$ and $a \in A$, there is a unique function $f : \omega \to A$ such that $f(0) = a$ and $(\forall n)(n \in \omega \to f(n^+) = g(f(n)))$.*

"Morally":

$$n \mapsto \overbrace{g \circ \cdots \circ g}^{n \text{ times}}(a) = f(n).$$

Proof. First, we show that if f_1 and f_2 are two functions with $f_1 : \omega \to A$, $f_2 : \omega \to A$, such that $f_1(0) = a = f_2(0)$, and for all $n \in \omega$, $f_1(n^+) = g(f_1(n))$ and $f_2(n^+) = g(f_2(n))$, then $f_1 = f_2$. Since $\mathrm{dom}(f_1) = \omega = \mathrm{dom}(f_2)$, it suffices to show that

$$\begin{aligned} G &:= \{n \in \omega : f_1(n) = f_2(n)\} \\ &= \omega. \end{aligned}$$

Since $f_1(0) = a = f_2(0)$, $0 \in G$. Suppose $n \in G$.

$$\begin{aligned} f_1(n^+) &= g(f_1(n)) \\ &= g(f_2(n)) \\ &= f_2(n^+), \end{aligned}$$

so $n^+ \in G$. So, G is inductive, and we have $(\forall n \in \omega)\ f_1(n) = f_2(n)$, so $f_1 = f_2$.

We know that:

$$\begin{aligned} f(0) &= a, \\ f(1) &= g(a), \\ f(2) &= g(g(a)), \\ f(3) &= g(g(g(a))). \end{aligned}$$

Let

$$\begin{aligned} \mathcal{F} := \{h \in \mathcal{P}(\omega \times A) :& \\ & h \text{ is a function}, \\ & \mathrm{dom}(h) \subseteq \omega, \\ & \mathrm{ran}(h) \subseteq A, \\ & 0 \in \mathrm{dom}\, h, \\ & h(0) = a, \\ & \text{if } n \in \omega \,\&\, n^+ \in \mathrm{dom}(h), \text{then } n \in \mathrm{dom}(h) \,\&\, h(n^+) = g(h(n))\} \end{aligned}$$

Plan:

1. We'll show that if $h_1, h_2 \in \mathcal{F}$ and $n \in \mathrm{dom}(h_1) \cap \mathrm{dom}(h_2)$, then $h_1(n) = h_2(n)$.
2. If $h \in \mathcal{F}$ and $n \in \mathrm{dom}(h)$, then $\exists \tilde{h} \in \mathcal{F}$ with $n^+ \in \mathrm{dom}\, \tilde{h}$.
3. $\forall n \in \omega\ \exists h \in \mathcal{F}\ n \in \mathrm{dom}\, h$.
4. Set $f := \bigcup \mathcal{F}$. This f solves the problem.

□

Lecture 17

March 1

Lecturer: Professor Slaman

17.1 Recursion Theorem

Theorem 17.1. *Let A be a set, $a \in A$, $F : A \to A$. There is a unique $h : \omega \to A$ such that $h(0) = a$ and for all $n \in \omega$, $h(n^+) = F(h(n))$.*

Use: $(\mathbb{N}, \text{successor}, 0)$ is a **Peano system**:

1. 0 is not in the range of the successor function.
2. The successor function is injective.
3. Any subset of $\mathbb{N}$ containing 0 and closed under the successor function is equal to $\mathbb{N}$.

Proof. **Define**: A function v with domain contained in $\mathbb{N}$, range contained in A is **acceptable** iff:

1. if $0 \in \text{dom}(v)$, then $v(0) = a$,
2. if $n^+ \in \text{dom}(v)$, then $n \in \text{dom}(v)$ and $v(n^+) = F(v(n))$.

For example, $\varnothing$ and $\{\langle 0, a\rangle\}$ are both acceptable.

Let

$$\begin{aligned} \mathcal{H} &= \{v : v \text{ is acceptable}\}, \\ h &= \bigcup \mathcal{H} \\ &= \{\langle x, y\rangle : \text{there is an acceptable } v \in \mathcal{H}, v(x) = y\}. \end{aligned}$$

Need:

- h is single-valued.
- $\text{dom}(h) = \mathbb{N}$.
- h satisfies the recursion conditions.

Claim 1: h is a function, i.e. h is single-valued on its domain.

Consider $V = \{n : \text{there is at most one } y \text{ such that } \langle n, y\rangle \in h\}$. To show that $V = \mathbb{N}$,

(a) 0: Observe that $\{\langle 0, a\rangle\} \in \mathcal{H}$, so $\langle 0, a\rangle \in h$. For all y, if $\langle 0, y\rangle \in h$, then there is a $v \in \mathcal{H}$ such that $v(0) = y$, but $v \in \mathcal{H} \;\&\; v(0) = y \to y = a$, so $y = a$.

(b) *Next*: Suppose that $n \in V$. We need to show: $n^+ \in V$. If $n^+ \notin \mathrm{dom}(h)$, then we are done, so assume $n^+ \in \mathrm{dom}(h)$. This happens by some $v \in \mathcal{H}$, such that $n^+ \in \mathrm{dom}(v)$. We have $v(n^+) = y$, so $n \in \mathrm{dom}(v)$, $v(n^+) = F(v(n))$. If also $\langle n^+, z\rangle \in h$, there would be a $u \in \mathcal{H}$ with $u(n^+) = z$, $n \in \mathrm{dom}(h)$, $u(n^+) = F(u(n))$. Using the assumption that $n \in V$: since $n \in V$, $u(n) = v(n)$. But then, $y = v(n^+) = F(v(n)) = F(u(n)) = u(n^+) = z$, i.e. $n^+ \in V$.

$\square$

Lecture 18

March 3

Lecturer: Professor Slaman

18.1 Recursion Theorem

Peano System: $(\mathbb{N}, S, 0)$

1. $0 \notin \operatorname{ran}(S)$.
2. S is injective.
3. For any subset $A \subseteq \mathbb{N}$, if $0 \in A$ and for all $a \in A$, $S(a) \in A$, then $A = \mathbb{N}$.

Theorem (Recursion Theorem): For A a set, $F : A \to A$, and $a \in A$, there is a unique h, $h : \mathbb{N} \to A$, which satisfies

$$h(0) = a,$$
$$h(n^+) = F(h(n)).$$

Recall. v is acceptable if $\operatorname{dom}(v) \subseteq \mathbb{N}$ and:

1. If $0 \in \operatorname{dom}(v)$, then $v(0) = a$.
2. If $n^+ \in \operatorname{dom}(v)$, then $n \in \operatorname{dom}(v)$ and $v(n^+) = f(v(n))$.

$$\mathcal{H} = \{v : v \text{ is acceptable}\},$$
$$h = \bigcup \mathcal{H}.$$

Showed: h is a function, i.e. h is single-valued.

Proof, Continued. **Fact 2**: h is acceptable.

Check:

1. Suppose $0 \in \operatorname{dom}(h)$. Then $\exists v$ acceptable, $0 \in \operatorname{dom}(v)$, and 1 for v implies $v(0) = a$. So, $h(0) = a$.
2. Similar argument: use 2 for the v that puts n^+ in $\operatorname{dom}(h)$.

Fact 3: $\operatorname{dom}(h) = \mathbb{N}$.

Proof by induction on $\operatorname{dom}(h)$.

Check: $0 \in \operatorname{dom}(h)$. $\{\langle 0, a\rangle\}$ is acceptable, so $h(0) = a$. Suppose that $n \in \operatorname{dom}(h)$. To show:

$n^+ \in \text{dom}(h)$. Let v be acceptable and $n \in \text{dom}(v)$. If $n^+ \in \text{dom}(v)$, we are done. Otherwise, let $v^* = \{\langle n^+, F(v(n))\rangle\} \cup v$. To show that v^* is acceptable:

1. Suppose that $0 \in \text{dom}(v^*)$. 0 is not in the range of successor: $0 \neq n^+$. Then, $0 \in \text{dom}(v)$, so $v(0) = a$ by acceptability of v, so $v^*(0) = a$.

2. Suppose $m^+ \in \text{dom}(v^*)$.

   Case 1: $m^+ \in \text{dom}(v)$. Then, $m^+ \neq n^+$ and $v(m^+) = F(v(m))$ and $m \in \text{dom}(v)$. Since v^* extends v, $v^* = v$ on m, m^+, so

   $$v^*(m^+) = F(v^*(m)).$$

   Case 2: $m^+ \notin \text{dom}(v)$, hence $m^+ = n^+$ is a new point in $\text{dom}(v^*) \setminus \text{dom}(v)$. Since the successor is injective, $m = n$ and

   $$\begin{aligned} v^*(m^+) = v^*(n^+) &= F(v(n)) \\ &= F(v^*(n)) \\ &= F(v^*(m)). \end{aligned}$$

So, there is an acceptable v^* with $n^+ \in \text{dom}(v^*)$, which implies that $n^+ \in \text{dom}(h)$. By induction 3, $\text{dom}(h) = \mathbb{N}$.

The facts together imply the Recursion Theorem. $\square$

18.2 Characterization of Peano Systems

Theorem 18.1. *Suppose (N, S, e) is a Peano system. Then, $(\mathbb{N}, \text{successor}, 0)$ (or any other Peano system) and $(\mathbb{N}, S, e)$ are isomorphic. $\exists \pi : \mathbb{N} \to N$ such that π is a bijection and $\pi(0) = e$, and for all x, $\pi(x^+) = S(\pi(x))$.*

Lecture 19

March 6

Lecturer: Professor Slaman

19.1 Characterization of Peano Systems

Theorem: Suppose that (N, S, e) is a Peano system. Then, $(\mathbb{N}, \text{successor}, 0)$ is isomorphic to (N, S, e).

Proof. Define $h : \mathbb{N} \to N$ to be the unique function satisfying

$$h(0) = e,$$
$$h(n^+) = S(h(n)).$$

Show:

1. h is surjective, i.e. $\text{ran}(h) = N$. Induction: show $e \in \text{ran}(h)$ and if $x \in \text{ran}(h)$, then $S(x) \in \text{ran}(h)$. $h(0) = e$. Suppose $x \in \text{ran}(h)$, i.e. $x = h(n)$. By definition, $h(n^+) = S(h(n)) = S(x)$. Hence, $\text{ran}(h) = N$ by 3, since N is a Peano system.

2. h is injective, i.e. for all $x_1, x_2 \in \mathbb{N}$, $h(x_1) = h(x_2) \to x_1 = x_2$. Let

$$\begin{aligned} I &= \{x : h^{-1}(h(x)) = \{x\}\} \\ &= \{x : h(x') = h(x) \leftrightarrow x' = x\} = \text{domain on which } h \text{ is injective.} \end{aligned}$$

   To show: $0 \in I$ & $(x \in I \to x^+ \in I)$.

   $0 \in I$: By definition, $h(0) = e$. If $h(x) = e$ and $x \neq 0$, then let $x = n^+$ (since $x \neq 0$), and then $h(x) = h(n^+) = S(h(n))$ and e is not in the range of S, so $h(x) \neq e$.

   Suppose $n \in I$:

$$h(n^+) = S(h(n)).$$

   If $h(m) = h(n^+) = S(h(n))$, then $m \neq 0$ since $e \notin \text{ran}(S)$. Suppose that $m = k^+$.

$$h(m) = h(k^+) = S(h(k)),$$

   i.e. $S(h(n)) = S(h(k))$. By 2 of tbe Peano system axioms, S is injective, so $h(n) = h(k)$. Since $n \in I$, $k = n$ and $m = k^+ = n^+$, so $n^+ \in I$.

So, h is a bijection, as required. $\square$

19.2 Arithmetic

We can define addition $a + b$ by

$$a + 0 = a,$$
$$a + (b^+) = (a + b)^+.$$

Then, $a < b \iff \exists t\, (t \neq 0 \,\&\, a + t = b)$.

How should we define a finite set? We could say F finite iff $\exists (N, S, e)\ \exists A \subseteq N$ such that if $m \in A$, then $m = 0$ or $m = n^+$ and $n \in A$, and $A \neq N$, and A is bijective with F.

Lecture 20

March 8

Lecturer: Professor Slaman

20.1 Arithmetic on a Peano System (N, S, e)

Addition is a binary function $N \times N \to N$ (subset of $(N \times N) \times N$):

$$\underbrace{n + m}_{\text{arguments}} = \overbrace{k}^{\text{value}}.$$

Definition 20.1. For $n \in N$, define $A_m : N \to N$ by:

$$A_m(0) = m, \qquad \underbrace{A_m(S(n))}_{m+S(n)} = \underbrace{S(A_m(n))}_{S(m+n)}. \tag{20.1}$$

Define $m + n = A_m(n)$.

$$m + n = k \iff \exists f : N \to N \; f \text{ satisfies (20.1) and } f(n) = k.$$

Proposition 20.2. *1. + is associative, i.e. for all m, n, k,*

$$(m + n) + k = m + (n + k).$$

2. Addition is commutative: $m + n = n + m$.

Proof. 1. Prove it by induction on k (for all m, n simultaneously).

Case 1: $k = 0$. We have to show $(m + n) + 0 = m + (n + 0)$ (for all m, n).

$$\begin{aligned}(m + n) + 0 &= A_{m+n}(0)\\ &= m + n\\ &= m + \overbrace{A_n(0)}^{n}\\ &= m + (n + 0).\end{aligned}$$

Case 2 (Inductive Case): Assume that the statement holds for k, show that the statement holds for $S(k)$.

$$
\begin{aligned}
(m+n)+S(k) &= S((m+n)+k) \\
&= S(m+(n+k)) && \text{induction assumption} \\
&= m+S(n+k) \\
&= m+(n+S(k)).
\end{aligned}
$$

2. Proof by induction on n.

   Initial Case: Show that

$$
\underbrace{m+0}_{m} = 0+m.
$$

The definition of addition is $k+0=k$, $k+S(m)=S(k+n)$. To show $0+m=m$, we use induction on m.

$$
\begin{aligned}
0+0 &= 0, \\
0+S(n) &= S(0+n) && \text{definition of } + \\
&= S(n) && \text{induction}
\end{aligned}
$$

Inductive Case: Assume $m+n=n+m$ for all m. Show that $m+S(n)=S(n)+m$ for all m.

$$
\begin{aligned}
m+S(n) &= S(m+n) \\
&= S(n+m) && \text{by induction} \\
&= n+S(m)
\end{aligned}
$$

To show: $n+S(m)=S(n)+m$ for all n, m. Show it by induction on m. If $m=0$:

$$
\begin{aligned}
S(n)+0 &= S(n) \\
&= S(n+0) \\
&= n+S(0).
\end{aligned}
$$

Given that $n+S(p)=S(n)+p$, show that $n+S(S(p))=S(n)+S(p)$.

$$
\begin{aligned}
n+S(S(p)) &= S(n+S(p)) && \text{definition of } + \\
&= S(S(n)+p) && \text{induction} \\
&= S(n)+S(p) && \text{definition of } +
\end{aligned}
$$

Hence, $m+S(n)=S(n)+m$ as required. Then, addition commutes.

□

20.1.1 Multiplication

Similarly, we could define multiplication

$$
m \cdot n = B_m(n) \qquad \begin{cases} B_m(0) &= 0 \\ B_m(S(n)) &= B_m(n)+m \end{cases}
$$

and show:

$$
\begin{aligned}
(m\cdot n)\cdot k &= m\cdot(n\cdot k) && \text{associativity} \\
(m\cdot n) &= (n\cdot m) && \text{commutativity} \\
m\cdot(n+k) &= m\cdot n + m\cdot k && \text{distributivity}
\end{aligned}
$$

It's worth checking your ability by doing at least one yourself.

20.2 The Special Rule of ω

Recall: $(\omega, {}^+, \varnothing)$, where ω is the collection of x such that x belongs to any inductive set.

$$A \text{ is inductive} \iff \varnothing \in A \,\&\, n \in A \to \underbrace{n \cup \{n\}}_{n^+} \in A.$$

1. $(\omega, {}^+, \varnothing)$ is a Peano system.
2. Elements of ω are transitive.
3. ω is inductive.

Lecture 21

March 10

Lecturer: Professor Slaman

21.1 Ordering of the Natural Numbers

ω is a stand-in for the natural numbers.

Today: ω is linearly ordered by $\in$. The proof is "fiddly".

Lemma 21.1. *(a) For all natural numbers n, m,*

$$m \in n \leftrightarrow m^+ \in n^+.$$

(b) If $n \in \omega$, $n \notin n$.

Proof. (a) $\implies$: By induction. Let $S = \{n : \text{for all } m, m \in n \to m^+ \in n^+\}$.

Initial Case: $\varnothing \in S$ (vacuously).

Successor Case: Suppose $n \in S$. To show: $n^+ \in S$, i.e. show that for all m, if $m \in n^+$, then $m^+ \in (n^+)^+$. Let $m \in n^+ = n \cup \{n\}$. Case 1: $m = n$. Then, $m^+ = n^+ \in \{n^+\} \cup n^+$. Otherwise, $m \in n$. Since $n \in S$, $m^+ \in n^+ \subseteq (n^+)^+$, so $m^+ \in (n^+)^+$.

So, $S = \omega$ as required.

$\impliedby$: Suppose that $m^+ \in n^+$. To show: $m \in n$.

$$m^+ = m \cup \{m\}, \qquad n^+ = n \cup \{n\}.$$

Case 1: $m^+ = n$. Then, $m \in n$ since $m \in m^+$.

Case 2: $m^+ \in n$. Then, $m \in n$ by transitivity of n.

$$m \in m^+ \in n.$$

(b) Show $n \in \omega \to n \notin n$. Let $T = \{n : n \in \omega \,\&\, n \notin n\}$. Induction: $T = \omega$.

Initial Case: $\varnothing \in T$ since $\varnothing \notin \varnothing$.

Successor Case: Assume $n \in T$. Then, $n^+ = n \cup \{n\}$. If $n^+ \in n^+$, then either: $n^+ = n$ and $n \in n^+ = n$, or $n^+ \in n$, and by transitivity, $n \in n$. This is impossible since $n \in T$.

$\square$

Proposition 21.2 (Trichotomy)**.** *For all $m, n \in \omega$, exactly one of $m \in n$, $m = n$, or $n \in m$ holds.*

Proof. First, show that the cases are mutually exclusive. If $m = n$, then neither $m \in n$ nor $n \in m$ by (b). If $m \in n$, if $n \in m$, we would have $m \in n \in m$, and by transitivity, $m \in m$, which is a contradiction. Then, $n \notin m$.

Consider

$$T = \{n : \forall m \in \omega \ (m \in n \text{ or } m = n \text{ or } n \in m)\}$$

and show by induction that $T = \omega$.

Initial: To show $\varnothing \in T$, we need $\forall m \in \omega \ (m = \varnothing \text{ or } \varnothing \in m)$. Proof by induction on m.

Successor Step: Assume $n \in T$. Need to show $n^+ \in T$, i.e. $\forall m \in \omega \ (m \in n^+ \text{ or } m = n^+ \text{ or } n^+ \in m)$. Let $m \in \omega$. Since $n \in T$, either $m \in n$, $m = n$, or $n \in m$. If $m \in n$, then $m \in n^+ = n \cup \{n\}$. If $m = n$, then $m \in n^+ = n \cup \{n\}$. Otherwise, $n \in m$. By 21.1, $n^+ \in m^+ = m \cup \{m\}$. Possibilities: (1) $n^+ = m$. (2) $n^+ \in m$. QED. $\square$

Observations. For all $m, n \in \omega$,

- $m \in n$ iff $m \subsetneq n$. ($\Longleftarrow$ uses Trichotomy, 21.2.)
- $m \underline{\in} n$ iff $m \subseteq n$.

21.2 Well-Ordering

Well-Ordering Property of ω. For any non-empty $A \subseteq \omega$, there is $a \in A$ such that for all $n \in A$, $a \underline{\in} n$. (Any non-empty subset of ω has a least element.)

Well-ordering is a linear ordering for which every non-empty subset has a least element.

Observation. Given the WO property, we can conclude that there is no $f : \omega \to \omega$ such that for all n, $f(n^+) < f(n)$.

Question: Is "L is a WO" equivalent to "there is no $f : \omega \to L$ such that $\forall n \ (f(n^+) < f(n))$"?

Lecture 22

March 13

Lecturer: Professor Slaman

22.1 Ordering on the Natural Numbers

Last Time: **Trichotomy Theorem**. For all $m, n \in \omega$, exactly one of the following holds: $m \in n$, $m = n$, $n \in m$.

Application.

Theorem 22.1. *For all m, n, p,*

$$m \in n \leftrightarrow m + p \in n + p.$$

Proof. $\implies$: Assume $m \in n$. To show: $m + p \in n + p$. By induction on p.

Initial Case: $p = 0$. We need

$$\underbrace{m + 0}_{m} \in \underbrace{n + 0}_{n}.$$

Successor Case: Assume $m + k \in n + k$. Need to show: $m + (k^+) \in n + (k^+)$.

$$m + (k^+) = (m + k)^+; \qquad n + (k^+) = (n + k)^+.$$

Last time: $a \in b \leftrightarrow a^+ \in b^+$. Then,

$$(m + k)^+ \in (n + k)^+$$
$$m + k^+ \in n + k^+.$$

$\impliedby$: Assume $m + p \in n + p$. To show: $m \in n$. Use trichotomy: could we have $n = m$? This would give $n + p \in n + p$, which is impossible. Could we have $n \in m$? Then, $n + p \in m + p$ (by $\implies$), so $n + p \in m + p \in n + p$ and $\in$ is transitive on elements of ω, so $n + p \in n + p$ is impossible. Thus, the only remaining possibility, $m \in n$, must hold. $\square$

22.2 Comments about Induction

Theorem 22.2 (Well-Ordering Property for ω)**.** *For any $A \subseteq \omega$, if $A \neq \varnothing$, then there is an $a \in A$ such that for all $n \in A$, $a \subseteq n$ (i.e. $\forall n \in \omega\ (a > n \to n \notin A)$). a is the least element of A.*

Proof. Let $M = \{x : x \in \omega \,\&\, \forall y \leq x\ y \notin A\}$. Assume A is a counterexample to W-O for ω. Show M satisfies the inductive hypothesis.

$\varnothing \in M$ follows from the fact that $\varnothing$ is the least element of ω.

Suppose $k \in M$. Then, consider k^+. We know $\forall y \leq k\ y \notin A$, so $\forall y < k^+\ y \notin A$.

$$\begin{aligned} n < k^+ &\iff n \in \overbrace{k \cup \{k\}}^{k^+} \\ &\iff n = k \text{ or } n \in k \\ &\iff n = k \text{ or } n < k. \end{aligned}$$

Then, $\forall y\ (y \in A \to y \geq k^+)$. If $k^+ \in A$, then $k^+ = a$ shows that A is not a counterexample to the claim, so $k^+ \notin A$. □

Corollary 22.3. *There is no $f : \omega \to \omega$ such that for all n, $f(n) > f(n^+)$.*

Proof. Consider the range of f. It would have to have a least element a. Then, $\exists n\ (f(n) = a)$ and then $a = f(n) > f(n^+)$, which is a contradiction. □

Challenge: Suppose that we are given $<$ on a set L and there is a non-empty subset of L with no $<$ least element. Does there exist a $f : \omega \to L$ as in 22.3, i.e. $\forall n\ (f(n) > f(n^+))$?

Try to define it by recursion. For $f(1)$, pick some value $< f(0)$. Pick some $f(2) < f(1)$. In order to run the recursion, we would need a function "pick" such that $\text{dom(pick)} = \{x : x \neq \varnothing, x \subseteq A\}$ and for all $x \in \text{dom(pick)}$, $\text{pick}(x) \in x$. This is an instance of the Axiom of Choice.

Recall. We were experimenting with ways to identify finite sets.

$$F \text{ is finite} \iff \exists n\ (n \in \omega \,\&\, \exists \text{ bijection } g : n \to F). \tag{22.1}$$

g is one-to-one and onto.

$$F \text{ is finite} \iff \text{every injection } F \to F \text{ is also a surjection.} \tag{22.2}$$

AC: For every set A, there is a function $g : A \to \bigcup A$ such that for all $a \in A$, $a \neq \varnothing \to g(a) \in a$.

Lecture 23

March 15

Lecturer: Professor Slaman

23.1 Cardinality & the Axiom of Choice

Definition 23.1. A set A is **equinumerous** to another set B iff there is a bijection between A and B.

Example 23.2. $\mathbb{N}$ and $\{2n : n \in \mathbb{N}\}$ are equinumerous: $n \mapsto 2n$ is a bijection between the two sets.

Example 23.3. ω and $\omega \times \omega$ are equinumerous. We will give two different proofs.

I. (i) Define $f_1 : \omega \xrightarrow{\text{onto}} \omega \times \omega$. $f_1 : k \mapsto (n_1, n_2)$ if k's prime factorization has $2^{n_1} \cdot 3^{n_2} \cdots$ or $(0, 0)$ if $k = 0$.

(ii) Make our map injective. Define $f_2 : \omega \xrightarrow[\text{onto}]{\text{one-to-one}} \omega \times \omega$ by recursion.

$$\begin{aligned} f_2(0) &= f_1(0), \\ f_2(n+1) &= f_1(x), \quad \text{where } x \text{ is the least number such that } f_1(x) \notin \{f_2(0), \ldots, f_2(n)\}. \end{aligned}$$

f_2 is injective. Let $M = \{x : \exists x_1 < x \ f_2(x_1) = f_2(x)\}$. If f_2 is not injective, then M has a least element. Suppose m is the least element of M. Then, $\exists x_1 < m$ such that $f_2(x_1) = f_2(m)$, so $f_2(m) \in \{f_2(0), \ldots, f_2(m-1)\}$ contradicts the fact that f_2 satisfies the recursion property.

II. View the elements of $\omega \times \omega$ as lattice points on a two-dimensional grid. An injection from ω is given by walking along the diagonal lines of the lattice.

Example 23.4. ω and $\mathbb{Q}$ are equinumerous. We have a map

$$(p, q) \mapsto \begin{cases} \dfrac{p}{q}, & q \neq 0, \\ 1, & q = 1, \end{cases}$$

which is a map $\omega \xrightarrow{\text{onto}} \mathbb{Q} \geq 0$. We can change the map to

$$(p, q) \mapsto \begin{cases} \dfrac{p}{q}, & \text{if } p, q \neq 0 \text{ are relatively prime or } p = 0, \\ -\dfrac{p}{q}, & \text{if } p, q \neq 0 \text{ are not relatively prime,} \\ 0, & \text{if } p = 0, \\ 1, & \text{otherwise,} \end{cases}$$

which gives a map $\omega \xrightarrow[\text{onto}]{\text{one-to-one}} \omega^2 \xrightarrow{\text{onto}} \mathbb{Q}$. We can convert the map as earlier into a bijection.

Example 23.5. ω and the set of polynomials in one variable with integer coefficients are equinumerous.

First, consider $\omega^* = \bigcup_{k \geq 1} \omega^k$, the k-fold Cartesian product.

$$\begin{aligned} &\omega \xrightarrow{\text{onto}} \omega^*, \\ &k \mapsto (n_1, \ldots, n_i), \quad \text{where the prime factorization of } k \text{ is } 2^{n_1} \cdot 3^{n_2} \cdots p_i^{n_i}, \\ &\qquad p_{i+1} \text{ is the largest prime that divides } k, \\ &1 \mapsto (1), \\ &0 \mapsto (0). \end{aligned}$$

For any $(n_1, \ldots, n_i)$, let $k = 2^{n_1} \cdots p_i^{n_i} p_{i+1}$. Then, $k \mapsto (n_1, \ldots, n_i)$.

Second, we need $\omega \xrightarrow{\text{onto}} \mathbb{Z}^* = \bigcup_k \mathbb{Z}^k$. Consider $\omega \xrightarrow{\text{onto}} \mathbb{Z}$ by

$$n \mapsto \begin{cases} 0, & \text{if } n = 0, \\ k, & \text{if } n = 2k \neq 0, \\ -k, & \text{if } n = 2k + 1 \neq 0. \end{cases}$$

This yields $\omega \xrightarrow{\text{onto}} \mathbb{Z}^*$ by $k \mapsto (n_1, \ldots, n_i) \mapsto (g(n_1), \ldots, g(n_i))$.

Define $\mathbb{Z}^* \to$ set of $\mathbb{Z}$ polynomials by $(a_1, a_2, \ldots, a_k) \mapsto a_1 + a_2 x + a_3 x^2 + \cdots + a_k x^{k-1}$. This yields $\omega \xrightarrow{\text{onto}} \mathbb{Z}$-polynomials. Make the map injective by discarding repeated values.

Example 23.6. Finally, we have a map $\omega \xrightarrow[\text{onto}]{\text{one-to-one}} \{\xi \in \mathbb{R} : \xi \text{ is algebraic}\}$.

Lecture 24

March 17

Lecturer: Professor Slaman

24.1 Liouville Number

Last Time: We showed that a variety of sets are countable.

In particular, $\{\xi : \xi \in \mathbb{R} \text{ and } \xi \text{ is algebraic}\}$ is countable.

Q: Is every element of $\mathbb{R}$ algebraic?

Liouville 1855: There is a transcendental number.

Lemma 24.1. *Suppose a is algebraic and not in $\mathbb{Q}$. Then, there is a*

1. *$k \in \mathbb{N}$, $k \geq 1$, and*
2. *$D > 0$,*

such that for all p/q,

$$\left| a - \frac{p}{q} \right| > D \cdot \frac{1}{q^k}.$$

Proof. Fix an $f \in \mathbb{Z}[x]$ of degree ≥ 1, $f(a) = 0$, which is of minimal degree with respect to having a as a root. Choose an interval $I \ni a$ such that a is the only solution to $f(x) = 0$ in I. Let M be the maximum of $|f'(x)|$ for $x \in I$. Let p/q be given with $p/q \in I$. Invoke the Mean Value Theorem.

$$\exists x \in I \quad f'(x) = \frac{f(a) - f(p/q)}{a - p/q}, \qquad q > 0.$$

Hence,

$$\left| a - \frac{p}{q} \right| = \frac{|\cancel{f(a)} - f(p/q)|}{|f'(x)|},$$
$$\left| a - \frac{p}{q} \right| \geq \frac{1}{M} \cdot \left| \frac{1}{q^k} \right|, \qquad q > 0,$$

where k is the degree of f. ∎

The **Liouville Number**

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}.$$

yields $\forall k\ \exists p/q\ |\alpha - p/q| < 1/q^k$, where q will be a power of 10. Also, the decimal expansion does not repeat, so it is not in $\mathbb{Q}$ either.

24.2 Cantor's Diagonalization

Theorem 24.2 (Cantor 1873). *$\mathbb{R}$ is not countable.*

Proof. Suppose not. Then, consider the counting of $\mathbb{R}$ $n \mapsto a_n$. Fix the decimal expansion of a_i so that we don't use any such with all but finitely many 9s. Define

$$\alpha = \sum_{i=0}^{\infty} \frac{d_i}{10^i},$$

where we set

$$d_i = \begin{cases} 1, & \text{if the } i\text{th place digit in } a_i \neq 1, \\ 2, & \text{otherwise.} \end{cases}$$

Then, $\alpha \neq a_i$ for all i. *Reason*: α has a unique decimal expansion and it is different from any of the expansions for $\{a_i : i \in \mathbb{N}\}$. $\square$

Exercise: Suppose that $\{A_i : i \in \mathbb{N}\}$ is a collection of subsets of $\mathbb{R}$ such that for all i, A_i is not equinumerous with $\mathbb{R}$. Show: $\bigcup_i A_i \neq \mathbb{R}$.

Question: Is every $A \subseteq \mathbb{R}$ either equinumerous or countable? (Not decided by the usual axioms of set theory.)

Exercise: $\mathbb{R} \setminus \mathbb{Q}$ is equinumerous with $\mathbb{R}$.

Lecture 25

March 20

25.1 Finite Sets

Definition 25.1. A set X is **finite** if $\exists n \in \omega\ X \approx n$ [X has the same cardinality as n].

Provisionally: $\mathrm{card}(X) = n$.

Theorem 25.2. *If X is finite and $f : X \to X$ is one-to-one, then f is into.*

Remark: $(\exists X)\ f : X \to X$ is one-to-one but not onto, e.g. $X = \omega$, $f : \omega \to \omega$ given by $n \mapsto 2n$.

Definition 25.3. X is **Dedekind-finite** if whenever $f : X \to X$ is one-to-one, f must be onto.

Proposition 25.4. $(\forall n \in \omega)$ *If $f : n \to n$ is one-to-one, then f is onto.*

Proof. By induction on n.

$n = 0$: The only function with domain $0 = \varnothing$ is $\varnothing$, and $\varnothing : \varnothing \to \varnothing$ is a bijection.

Suppose that the proposition is true of n. Consider $f : n^+ \to n^+$.

Case 1: $f[\![n]\!] \subseteq n$. Define $g := f$, $h := I_{n^+}$.

Case 2: $f[\![n]\!] \not\subseteq n$. Then, $\exists!\, a \in n\ f(a) = n$. Define $g : n^+ \to n^+$ by

$$m \mapsto \begin{cases} f(n), & \text{if } m = a, \\ n, & \text{if } m = n, \\ f(m), & \text{otherwise.} \end{cases}$$

So, $g = (f \upharpoonright n \setminus \{a\}) \cup \{\langle a, f(n)\rangle\} \cup \{\langle n, n\rangle\}$. Then, define $h : n^+ \to n^+$ by

$$m \mapsto \begin{cases} n, & \text{if } m = a, \\ a, & \text{if } m = n, \\ m, & \text{otherwise.} \end{cases}$$

Hence, $f = g \circ h$, since:

$$\begin{tikzcd} a \arrow[r, mapsto, "h"] \arrow[rr, bend left, "f"] & n \arrow[r, mapsto, "g"] & n \end{tikzcd}$$

$$\begin{tikzcd} n \arrow[r, mapsto, "h"] \arrow[rr, bend left, "f"] & a \arrow[r, mapsto, "g"] & f(n) \end{tikzcd}$$

g is one-to-one and $g \restriction n : n \to n$ because g is one-to-one and $g(n) = n$. $g \restriction n$ is one-to-one. By the IH, $g \restriction n$ is onto. $g(n) = n$, so $n^+ = \operatorname{ran}(g)$. Therefore, g is onto. $h : n^+ \to n^+$ is bijective, so $f = g \circ h$ is onto. □

Proof of 25.2. Let X be finite and $f : X \to X$ be one-to-one. Since X is finite, $\exists n \in \omega\ \exists g : X \to n$ which is one-to-one and onto. $g \circ f \circ g^{-1} : n \to n$ is one-to-one. By 25.4, $g \circ f \circ g^{-1}$ is onto. Hence, $f = g^{-1} \circ (g \circ f \circ g^{-1}) \circ g$ is onto. □

Corollary 25.5 (Pigeon Hole Principle)**.** *If X is finite and $f : X \to X$ is not onto,*

$$\exists a, b \in X\ a \neq b\ f(a) = f(b).$$

Corollary 25.6. *If X is finite, then $\exists!\, n \in \omega\ X \approx n$.*

Proof. X is finite implies $\exists n \in \omega\ X \approx n$. Suppose $m \in \omega\ \&\ X \approx m$. If $m \neq n$, then WLOG by the trichotomy, we may assume $m \in n$, so $m \subsetneq n$. However, $X \approx m$ via h and $X \approx n$ via g, so $h \circ g^{-1} : n \xrightarrow{\approx} m \subsetneq n$. Therefore, $h \circ g^{-1} : n \to n$ would be one-to-one but not onto. □

Theorem 25.7. *If X is finite and $Y \subseteq X$, then Y is also finite.*

Proposition 25.8. $(\forall n \in \omega)$ *If $Y \subseteq n$, then Y is finite.*

Proof. By induction on n.

$n = 0$: $Y \subseteq 0 \implies Y = \varnothing \approx 0$.

n^+: $n^+ = n \cup \{n\}$, so we can write $Y = (Y \cap n) \cup (Y \cap \{n\})$. $Y \cap n \subseteq n$, so by induction, we know that $\exists m \in \omega\ \exists f : (Y \cap n) \to m$ which is a bijection. *Case 1*: $Y \cap \{n\} = \varnothing$. Here, $Y = Y \cap n$ and $Y \cap n$ is finite. *Case 2*: $Y \cap \{n\} = \varnothing$, so $Y \cap \{n\} = \{n\}$. Define $h := f \cup \{\langle n, m \rangle\}$ (functions with disjoint domains), so h is a function. The ranges are disjoint and each is one-to-one, so h is a one-to-one function.

$$\operatorname{ran}(h) = \operatorname{ran}(f) \cup \operatorname{ran}(\{\langle n, m \rangle\}) = m \cup \{m\} = m^+.$$

Therefore, $Y \approx m^+$ is finite. □

25.7 follows from 25.8 by conjugating with a bijection $X \approx n$.

25.2 Cardinality Arithmetic

Suppose

$$\kappa := \operatorname{card}(K),$$

$$\lambda := \operatorname{card}(L).$$

We will define

$$\begin{aligned}
\kappa \cdot \lambda &:= \operatorname{card}(K \times L), \\
\kappa + \lambda &:= \operatorname{card}(K \mathbin{\dot\cup} L), \\
\kappa^{\lambda} &:= \operatorname{card}({}^{L}K).
\end{aligned}$$

The disjoint union is $K \times \{0\} \cup L \times \{1\}$.

Lecture 26

March 22

26.1 Cardinal Arithmetic

Let

$$\kappa = \operatorname{card}(K),$$
$$\lambda = \operatorname{card}(L).$$

We define the operation

$$\kappa + \lambda := \operatorname{card}(K \amalg L),$$

where

$$K \amalg L := (K \times \{0\}) \cup (L \times \{1\}).$$

Also, $K \approx K \times \{0\}$ by taking the map $k \mapsto \langle k, 0 \rangle$. Likewise, $L \approx L \times \{1\}$.

Aside. Suppose we have an indexed set $(\kappa_i)_{i \in I}$. Later, we will discuss

$$\sum_{i \in I} \kappa_i := \operatorname{card}\left(\bigcup_{i \in I} \kappa_i \times \{i\} \right).$$

As an example,

$$1 + 1 = \operatorname{card}(\overbrace{1}^{\{0\}} \times \{0\} \cup \overbrace{1}^{\{0\}} \times \{1\}) = \operatorname{card}(\underbrace{\{\langle 0, 0 \rangle, \langle 0, 1 \rangle\}}_{\approx \{0,1\}}) = 2.$$

We also define

$$\kappa \cdot \lambda = \operatorname{card}(K \times L).$$

For example, you can check that

$$5 \cdot 7 = 35.$$

Similarly,

$$\kappa^\lambda := \operatorname{card}({}^L K).$$

For example,

$$0^0 := \operatorname{card}({}^{\varnothing}\varnothing) = \operatorname{card}(\{\varnothing\}) = 1.$$

Previously, for $n, m \in \omega$, we defined

$$
\begin{aligned}
n +^\omega 0 &:= n, \\
n +^\omega m^+ &:= (n +^\omega m)^+, \\
n \cdot^\omega 0 &:= 0, \\
n \cdot^\omega m^+ &:= n \cdot^\omega m +^\omega n, \\
n^0 &:= 1, \\
n^{m^+} &= n^m \cdot^\omega n.
\end{aligned}
$$

Fact. If $K \approx K'$, $L \approx L'$, and then $K \amalg L \approx K' \amalg L'$, $K \times L \approx K' \times L'$, and ${}^L K \approx {}^{L'} K'$.

Theorem 26.1. $\forall n, m \in \omega$,

$$
\begin{aligned}
n +^\omega m &= n + m, \\
n \cdot^\omega m &= n \cdot m, \\
\underbrace{n^m}_{\textit{recursive form}} &= \underbrace{n^m}_{\textit{cardinal form}}.
\end{aligned}
$$

Proof (for addition). Fix $n \in \omega$. We argue by induction on m.

$$
\begin{aligned}
n + 0 &\approx n \times \{0\} \cup 0 \times \{1\} \\
&= n \times \{0\} \\
&\approx n \\
&= n +^\omega 0. \\
n + m^+ &\approx (n \times \{0\}) \cup (m^+ \times \{1\}) \\
&= (n \times \{0\}) \cup ((m \cup \{m\}) \times \{1\}) \\
&= (n \times \{0\}) \cup (m \times \{1\} \cup \{m\} \times \{1\}) \\
&= (n \times \{0\} \cup m \times \{1\}) \cup \{m\} \times \{1\} \\
&\approx (n +^\omega m) \cup \{\langle m, 1 \rangle\}
\end{aligned}
$$

(by the IH, and $\langle m, 1 \rangle \notin n +^\omega m$)

$$
\begin{aligned}
&\approx (n +^\omega m) \cup \{n +^\omega m\} \\
&= (n +^\omega m)^+ \\
&= n +^\omega m^+.
\end{aligned}
$$

□

Definition 26.2.

$$\aleph_0 := \omega.$$

Definition 26.3. If $X \approx \omega$,

$$\operatorname{card}(X) = \aleph_0.$$

$$
\begin{aligned}
\aleph_0 + 1 &= \aleph_0, \\
(\omega \times \{1\}) \cup (1 \times \{1\}) &\approx \omega.
\end{aligned}
$$

To see this, define the map

$$\begin{aligned} f : (\omega \times \{0\}) \cup \{0\} \times \{1\} &\to \omega, \\ \langle 0, 1\rangle &\mapsto 0, \\ \langle n, 0\rangle &\mapsto n^+. \end{aligned}$$

$$\begin{aligned} \aleph_0 + \aleph_0 &= \aleph_0, \\ (\omega \times \{0\}) \cup (\omega \times \{1\}) &\approx \omega. \end{aligned}$$

Take the map

$$\begin{aligned} \langle n, 0\rangle &\mapsto 2n, \\ \langle n, 1\rangle &\mapsto 2n + 1. \end{aligned}$$

In general, we have

$$\begin{aligned} \kappa \cdot \lambda &= \lambda \cdot \kappa, \\ \kappa + \lambda &= \lambda + \kappa, \\ \kappa \cdot (\lambda + \mu) &= \kappa \cdot \lambda + \kappa \cdot \mu, \\ (\kappa^\lambda)^\mu &= \kappa^{\lambda \cdot \mu}. \end{aligned}$$

We want to prove

$${}^M({}^L K) \approx {}^{L \times M} K.$$

Consider $f : {}^{L \times M} K$. We will map

$$f : L \times M \to K \mapsto [\underbrace{m}_{\in M} \mapsto [\underbrace{\ell}_{\in L} \mapsto f(\langle l, m\rangle)]].$$

In other words, $f(m)(\ell) = f(\langle l, m\rangle)$.

Think about the following:

$$\aleph_0^{\aleph_0} \neq \aleph_0.$$

Lecture 27

March 24

27.1 Larger Cardinals

Last time, we considered $\aleph_0^{\aleph_0}$.

Theorem 27.1. *If K is any set with $K \neq \varnothing$ and $K \not\approx 1$, and L is any set, then $L \not\approx {}^L K$.*

Observation. If we let $a, b \in K$, $a \neq b$, then $\exists \iota : L \to {}^L K$ which is one-to-one.

$$x \in L \mapsto \left[y \mapsto \begin{cases} a, & \text{if } y = x \\ b, & \text{if } y \neq x \end{cases} \right].$$

Proof. We show that for any function $f : L \to {}^L K$, f is *not* onto. We need to find $g : L \to K$ such that $g \notin \operatorname{ran}(f)$. Let $a, b \in K$ with $a \neq b$. Define $g : L \to K$, i.e. $g \in {}^L K$, by

$$x \mapsto \begin{cases} b, & \text{if } f(x)(x) = a, \\ a, & \text{otherwise.} \end{cases}$$

Claim. $g \notin \operatorname{ran}(f)$.

If $g \in \operatorname{ran}(f)$, then $\exists x \in L$ such that $g = f(x)$.

$$g(x) = f(x)(x).$$

If $f(x)(x) = a$, then $g(x) = b \neq a = f(x)(x)$. So, $f(x)(x) \neq a$. Then, $g(x) = a \neq f(x)(x)$. This is a contradiction. □

Corollary 27.2. *For cardinals κ, λ, if $\kappa \neq 0$ and $\kappa \neq 1$, then $\lambda \neq \kappa^\lambda$.*

Corollary 27.3.

$$\begin{aligned} \aleph_0^{\aleph_0} &\neq \aleph_0, \\ \beth_1 = 2^{\aleph_0} &\neq \aleph_0, \\ 2^\kappa &\neq \kappa. \end{aligned}$$

Now, we define

$$\beth_0 := \aleph_0 = \omega,$$

$$\beth_{n^+} := 2^{\beth_n}.$$

Question: If $A \subseteq {}^\omega\omega$ and A is infinite, must we have $A \approx \omega$ or $A \approx {}^\omega\omega$? Note that

$${}^\omega\omega \approx \mathbb{R}.$$

Question: For a set X, define $\mathrm{Sym}(X) := \{f : f : X \to X \text{ is one-to-one and onto}\}$. For $\kappa = \mathrm{card}(K)$, define $\kappa! = \mathrm{card}(\mathrm{Sym}(K))$. Is $\aleph_0! = 2^{\aleph_0}$?

27.2 Ordering of Cardinals

Definition 27.4. $X \preceq Y$: "X has cardinality less than or rqual to that of Y", if $\exists f : X \to Y$ which is one-to-one. ($\iff \exists Z \subseteq Y$ such that $X \approx Z$).

If $\kappa = \mathrm{card}(K)$, $\lambda = \mathrm{card}(L)$, then

$$\kappa \leq \lambda \iff K \preceq L.$$

Write $X \prec Y$ if $X \preceq Y$ and $X \not\approx Y$.

$$\kappa < \lambda \iff K \prec L.$$

Example 27.5. For $n, m \in \omega$,

$$\begin{aligned} n \leq m &\iff n \in m \text{ or } n = m \\ &\iff n \subseteq m. \end{aligned}$$

Example 27.6. For $n \in \omega$, $n < \aleph_0$.

Example 27.7. For any κ, $2^\kappa > \kappa$.

Properties we would like our ordering on cardinals to have:

1. $X \preceq X$. [Use $f = I_X$.]
2. $(X \preceq Y \,\&\, Y \preceq Z) \to X \preceq Z$. [Composition of one-to-one functions is one-to-one.]
3. $(X \preceq Y \,\&\, Y \preceq Z) \to Y \approx Z$.
4. $(\forall X)(\forall Y)\ X \preceq Y \vee Y \preceq X$. [**CC: Cardinal Comparability**]

To prove ${}^\omega\omega \approx \mathbb{R}$, the easiest way is to use 3. Similarly, one can prove $(0,1) \approx [0,1]$ with the injection

$$x \mapsto \frac{1}{4} + \frac{1}{2}x$$

(the injection in the other direction is the identity).

Theorem 27.8. *If $X \preceq Y$ and $Y \preceq X$, then $X \approx Y$.*

Proof. Given $f : X \to Y$, one-to-one, and $g : Y \to X$, one-to-one, we construct $h : Y \to X$, one-to-one and onto. Define

$$\begin{aligned} C(0) &:= Y \setminus \mathrm{ran}(f), \\ C(n^+) &:= (f \circ g)[\![C(n)]\!]. \end{aligned}$$

Formally, let $Z = \mathcal{P}(Y)$ and $a = Y \setminus \operatorname{ran}(f) \in a$. Then, $\Phi : Z \to Z$ maps $U \subseteq Y \mapsto (f \circ g)[\![U]\!]$. $\square$

Lecture 28

April 3

28.1 Schröder-Bernstein Theorem

Theorem: If $X \preceq Y$ and $Y \preceq X$, then $X \approx Y$.

Proof. If $f : X \hookrightarrow Y$ is one-to-one and $g : Y \hookrightarrow X$, define $C : \omega \to \mathcal{P}(Y)$ by

$$C(0) := Y \setminus \operatorname{ran}(f),$$
$$C(n^+) := (f \circ g)[\![C(n)]\!].$$

The function to which we apply the Recursion Theorem is $Z \mapsto (f \circ g)[\![Z]\!]$. Define $h : Y \to X$ by

$$y \mapsto \begin{cases} g(y), & \text{if } y \in \bigcup \operatorname{ran}(C), \\ f^{-1}(y), & \text{if } y \in Y \setminus \bigcup \operatorname{ran}(C). \end{cases}$$

Note that $\operatorname{ran}(C) = \{C(n) : n \in \omega\}$, so $\bigcup \operatorname{ran}(C) = \{y \in Y : \exists n \in \omega \; y \in C(n)\}$.

Claim 1: h is a well-defined function with $\operatorname{dom}(h) = Y$.

Proof of Claim: $\bigcup \operatorname{ran}(C) \supseteq C(0) = Y \setminus \operatorname{ran}(f)$, so $Y \setminus \bigcup \operatorname{ran}(f) \subseteq Y \setminus (Y \setminus \operatorname{ran}(f)) = \operatorname{ran}(f)$. So, $Y \setminus \bigcup \operatorname{ran}(C) \subseteq \operatorname{dom}(f^{-1})$. As f is one-to-one, f^{-1} is a function. So, $f^{-1} \restriction (Y \setminus \bigcup \operatorname{ran} C)$ is a function and so is $g \restriction \bigcup \operatorname{ran}(C)$, and therefore $h = g \restriction \bigcup \operatorname{ran}(C) \cup f^{-1} \restriction (Y \setminus \bigcup \operatorname{ran}(C))$ is a function with $\operatorname{dom}(h) = \bigcup \operatorname{ran}(C) \cup (Y \setminus \bigcup \operatorname{ran} C) = Y$.

Claim 2: h is one-to-one.

Proof: Let $y, z \in Y$. Suppose $h(y) = h(z)$. Because g is one-to-one and f^{-1} is one-to-one, we may assume $y \in \bigcup \operatorname{ran}(C)$ and $z \in Y \setminus \bigcup \operatorname{ran}(C)$. Then, $\exists n \; y \in C(n)$, and

$$g(y) = h(y) = h(z) = f^{-1}(z).$$

We know that $\forall m \; z \notin C(m)$. Then,

$$(f \circ g)(y) = f(g(y)) = f(f^{-1}(z)) = z,$$

but $(f \circ g)(y) \in C(n^+)$, which is a contradiction. The case of $y \in \bigcup \operatorname{ran}(C)$, $z \notin \bigcup \operatorname{ran}(C)$, $h(y) = h(z)$ is impossible.

Claim 3: h is onto.

Let $x \in X$. Consider $f(x) \in Y$.

Case A: $f(x) \notin \bigcup \operatorname{ran}(C)$. Then, $h(f(x)) = f^{-1}(f(x)) = x$, so $x \in \operatorname{ran}(h)$.

Case B: $f(x) \in \bigcup \operatorname{ran}(C)$. Then, $\exists n\ f(x) \in C(n)$. We know that $f(x) \in \operatorname{ran}(f)$, which is disjoint from $Y \setminus \operatorname{ran}(f) = C(0)$, so $n \neq 0$. So, $\exists m\ n = m^+$, i.e. $f(x) = C(m^+) = (f \circ g)[\![C(m)]\!]$, i.e. $\exists y \in C(m)\ f(x) = (f \circ g)(y) = f(g(y))$. f is one-to-one, so $x = g(y) = h(y)$, as $y \in C(m) \subseteq \bigcup \operatorname{ran}(C)$. So, $x \in \operatorname{ran}(h)$. $\square$

Corollary 28.1. $(0,1) \approx [0,1]$. *($\aleph_0 + 1 = \aleph_0$, or $\aleph_0 + 2 = \aleph_0$.)*

($\{f : f : (0,1) \to [0,1] \text{ is a bijection}\} \approx \mathcal{P}(\mathcal{P}(\omega)) \approx \mathcal{P}(\mathbb{R})$, which has cardinality $\beth_2$.)

Corollary 28.2.

$$\aleph_0 2^{\aleph_0} = 2^{\aleph_0}.$$

Proof. We give a map $\omega \times \mathbb{R} \approx \omega \times (0,1) \hookrightarrow \mathbb{R}$ given by $\langle n, x\rangle \mapsto n + x$.

We have a map $\mathbb{R} \hookrightarrow \omega \times \mathbb{R}$ given by $r \mapsto \langle 0, r\rangle$.

Alternatively,

$$\begin{aligned} 2^{\aleph_0} &= 1 \cdot 2^{\aleph_0} \\ &\leq \aleph_0 \cdot 2^{\aleph_0} \\ &\leq 2^{\aleph_0} \cdot 2^{\aleph_0} \\ &= 2^{\aleph_0 + \aleph_0} \\ &= 2^{\aleph_0}. \end{aligned}$$

$\square$

Fact:

$$\bigcup \operatorname{ran}(C) \approx \begin{cases} \varnothing \\ \omega \\ Y \setminus \operatorname{ran}(f) \end{cases}$$

Lecture 29

April 5

29.1 Review

1. If A is infinite, must there exist $B, C \subseteq A$, $B \approx C \approx A$, $B \cap C = \varnothing$, $A = B \cup C$?
2. For $\kappa \geq \aleph_0$, is it true that $\kappa! > 2^\kappa$?
3. Given A with $|A| > 1$, does there exist $\sigma : A \to A$ such that $\forall x\, \sigma(x) \neq x$?

Topics:

- natural numbers
  - induction
  - recursion
  - ordering on ω
  - arithmetic of ω
- cardinality
  - finite sets
  - some cardinal arithmetic
  - $\aleph_0, \beth_1, \ldots$
  - Schröder-Bernstein

State the Axiom of Infinity with the language $\mathcal{L}(\in, \varnothing, (\cdot)^+)$.

Axiom of Infinity:

$$(\exists A)[(\forall x)[x \in A \to x^+ \in A] \,\&\, \varnothing \in A].$$

29.1.1 Defining Cardinals

$$\aleph_0 := \omega,$$

where

$$(\forall x)[x \in \omega \leftrightarrow (\forall I)[I \text{ inductive} \to x \in I]]$$

and

$$I \text{ is inductive} \iff \varnothing \in I \,\&\, (\forall a)[a \in I \to a^+ \in I].$$

Fix I, inductive.

$$\omega = \{n \in I : (\forall J)[J \text{ inductive} \to n \in J]\}.$$

Also,

$$\beth_0 := \aleph_0,$$
$$\beth_{n^+} := 2^{\beth_n}.$$

29.1.2 Peano Systems

A Peano system is (N, e, S), such that $e \in N$, $S : N \to N$ is one-to-one and $e \notin \operatorname{ran}(S)$, S has no cycles, and $(X \subseteq N \,\&\, e \in X \,\&\, [x \in X \to Sx \in X]) \implies X = N$.

29.1.3 Recursion

Given $g : A \to A$, $a \in A$, $\exists!\, f : \omega \to A$ such that $f(0) = a$ and $(\forall n)(f(n^+) = g(f(n)))$. Morally, $f(n) = g \overbrace{\circ \cdots \circ}^{n \text{ times}} g(a)$.

29.1.4 Cardinality

$$X \approx Y \iff \exists f : X \to Y \text{ bijection}$$
$$X \preceq Y \iff \exists f : X \hookrightarrow Y \text{ one-to-one}$$

We discussed $\kappa + \lambda$, $\kappa \cdot \lambda$, κ^λ, $\kappa!$. $\kappa \leq \lambda \,\&\, \lambda \leq \kappa \implies \kappa = \lambda$. Use basic properties such as $\aleph_0 + \aleph_0 = \aleph_0$ and $\kappa^{\lambda+\mu} = \kappa^\lambda + \kappa^\mu$. For the cardinals we have defined, $\kappa = \operatorname{card}(\kappa)$ by definition.

Lecture 30

April 10

30.1 Zorn's Lemma

Cardinal Comparability:

$$(\forall X)(\forall Y)[X \preceq Y \text{ or } Y \preceq X].$$

Lemma 30.1 (Zorn's Lemma)**.**

$$(\forall \mathcal{A})\left[(\forall \mathcal{C})\left[\mathcal{C} \subseteq \mathcal{A} \textit{ a chain} \implies \bigcup \mathcal{C} \in \mathcal{A}\right] \,\&\, \mathcal{A} \neq \varnothing \implies (\exists m)[m \in \mathcal{A} \textit{ maximal}]\right].$$

Definition 30.2. $\mathcal{C}$ is a **chain** if

$$(\forall x)(\forall y)[(x \in \mathcal{C} \,\&\, y \in \mathcal{C}) \to (x \subseteq y \vee y \subseteq x)].$$

Observation: There are sets A which are not chains, e.g. $A = \mathcal{P}(\omega)$, $x = \{1\}$, $y = \{2\}$.

Definition 30.3. $m \in A$ is **maximal (in** A**)** if $(\forall a \in A)[m \subseteq a \to m = a]$.

For example, let $A = \{\varnothing, \{1\}, \{2\}\}$. Then, $\varnothing \subseteq \{1\}$ and $\varnothing \subseteq \{2\}$, so there are two maximal elements.

Observation: If $\mathcal{B}$ is any set, $\bigcup \mathcal{B}$ is an upper bound for B, i.e. $\forall b \in \mathcal{B}$, $b \subseteq \bigcup \mathcal{B}$, and $\bigcup \mathcal{B}$ is the *least* upper bound. If c satisfies $(\forall b \in \mathcal{B})$ $b \subseteq c$, then $\bigcup \mathcal{B} \subseteq c$.

Theorem 30.4.

$$\text{ZL} \implies \text{AC1}.$$

Proof. Given R a relation, we must find $f \subseteq R$ a function with $\operatorname{dom}(f) = \operatorname{dom}(R)$. Let

$$\mathcal{A} := \{f \in \mathcal{P}(R) : f \text{ is a function}\}.$$

We check that if $\mathcal{C} \subseteq \mathcal{A}$ is a chain, then $\bigcup \mathcal{C} \in \mathcal{A}$. By 30.5, $\bigcup \mathcal{C}$ is a function and $\bigcup \mathcal{C} \subseteq R$ $[\forall f \in \mathcal{C} \subseteq \mathcal{A}\ f \in \mathcal{A}$, so $f \subseteq R]$, so $\bigcup \mathcal{C} \in \mathcal{A}$. ZL 30.1 implies $\exists f \in \mathcal{A}$ maximal. $f \subseteq R$, f is a function, and if $g \subseteq R$ is a function with $f \subseteq g$, then $f = g$.

$\operatorname{dom}(f) \subseteq \operatorname{dom}(R)$. Let $x \in \operatorname{dom}(R)$ and suppose $x \notin \operatorname{dom}(f)$. $\exists y\ \langle x, y\rangle \in R$. Pick some witness. Set $g := f \cup \{\langle x, y\rangle\}$, which is the union of two functions with disjoint domains. Hence, g is a function.

$f \subsetneq g \subseteq R$. This would contradict the maximality of f, so $\operatorname{dom}(f) = \operatorname{dom}(R)$. □

Lemma 30.5. *If $\mathcal{C}$ is a chain of functions, then $\bigcup \mathcal{C}$ is a function and*

$$\operatorname{dom} \bigcup \mathcal{C} = \bigcup \{\operatorname{dom}(f) : f \in \mathcal{C}\},$$
$$\operatorname{ran} \bigcup \mathcal{C} = \bigcup \{\operatorname{ran}(f) : f \in \mathcal{C}\}.$$

Proof. If $t \in \bigcup \mathcal{C}$, then $\exists f \in \mathcal{C}\ t \in f$. f is a function, hence a relation, so t is an ordered pair. So, $\bigcup \mathcal{C}$ is a relation. If $\langle x, y\rangle \in \bigcup \mathcal{C}$, $\langle x, z\rangle \in \mathcal{C}$, then $\exists f, g \in \mathcal{C}$ such that $\langle x, y\rangle \in f$, $\langle x, z\rangle \in g$. $\mathcal{C}$ is a chain, so $f \subseteq g$ or $g \subseteq f$. WLOG take $f \subseteq g$. So, $\langle x, y\rangle \in g$ & $\langle x, z\rangle \in g$, and g is a function, which implies that $y = z$. Therefore, $\bigcup \mathcal{C}$ is a function.

If $x \in \operatorname{dom} \bigcup \mathcal{C}$, then $\exists y\ \langle x, y\rangle \in \bigcup \mathcal{C}$, so $\exists f \in \mathcal{C}\ \langle x, y\rangle \in f$. Then, $x \in \operatorname{dom} f \subseteq \bigcup \{\operatorname{dom}(g) : g \in \mathcal{C}\}$ and likewise for $\operatorname{ran} \bigcup \mathcal{C}$. □

30.2 Cardinal Comparability

Theorem 30.6.

$$\text{ZL} \implies \text{CC}.$$

Proof. We are given X and Y. Let $\mathcal{A} := \{f \in \mathcal{P}(X \times Y) : f \text{ is a one-to-one function}\}$. Let $\mathcal{C} \subseteq \mathcal{A}$ be a chain. By 30.5, $\bigcup \mathcal{C}$ is a function, $\operatorname{dom}(\bigcup \mathcal{C}) \subseteq X$, $\operatorname{ran}(\bigcup \mathcal{C}) \subseteq Y$, and $\bigcup \mathcal{C}$ is one-to-one. If $\langle x, z\rangle \in \bigcup \mathcal{C}$, $\langle y, z\rangle \in \bigcup \mathcal{C}$, then $\exists f, g \in \mathcal{C}\ \langle x, z\rangle \in f$ & $\langle y, z\rangle \in g$. As $\mathcal{C}$ is a chain, WLOG $f \subseteq g$, so $\langle x, z\rangle \in g$ & $\langle y, z\rangle \in g$, so $x = y$ as g is one-to-one. Therefore, $\bigcup \mathcal{C} \in \mathcal{A}$. By ZL 30.1, $\exists f \in \mathcal{A}$ maximal.

Claim: $\operatorname{dom} f = X$ or $\operatorname{ran} f = Y$.

Proof of Claim: If not, $\exists x \in X \setminus \operatorname{dom} f$, $\exists y \in Y \setminus \operatorname{ran} f$. Set $g := f \cup \{\langle x, y\rangle\}$. g is a function and so is $g^{-1} = f^{-1} \cup \{\langle y, x\rangle\}$. $X \times Y \supseteq g \supsetneq f$, which violates the maximality of f.

If $\operatorname{dom} f = X$, then $X \preceq Y$. If $\operatorname{ran} f = Y$, then $Y \preceq X$ (witnessed by f^{-1}). □

Corollary 30.7.

$$(\text{ZL} \implies)\ \text{CC} \implies (\forall X)(X \textit{ infinite} \iff \omega \preceq X).$$

Proof. Suppose X is infinite. By CC, $\omega \preceq X$ or $X \preceq \omega$. If $X \preceq \omega$, $\exists A \subseteq \omega$ and $g : X \to A$ one-to-one and onto. If A is finite, we have $n \approx \omega$. □

Lecture 31

April 12

31.1 Subsets of ω Are Countable

Theorem 31.1. *If $A \subseteq \omega$, then either A is finite or $A \approx \omega$.*

Proof. WLOG A is infinite. Define $F : \mathcal{P}(\omega) \setminus \{\varnothing\} \to \omega$ by the rule $B \mapsto$ the least element of B. F is a choice function for ω and we do not need AC to prove its existence! (Given a set X, a **choice function** for X is a function $g : \mathcal{P}(X) \setminus \{\varnothing\} \to X$ such that $\forall a \in \operatorname{dom}(g)\ g(a) \in a$.) Set $G : \mathcal{P}(\omega) \setminus \{\varnothing\} \to \mathcal{P}(\omega)$ which maps $C \mapsto C \setminus \{F(C)\}$.

Fact: If C is infinite, then so is $G(C)$. ($C = G(C) \cup \{F(C)\}$. If $G(C)$ were finite, so would be C.)

Define $h : \omega \to \mathcal{P}(\omega)$ by

$$\begin{aligned} h(0) &:= A, \\ \forall n \quad h(n^+) &:= G(h(n)). \end{aligned}$$

Note that $G \restriction \mathcal{P}^{(\infty)}(\omega) : \mathcal{P}^{(\omega)}(\omega) \circlearrowleft$, where $\mathcal{P}^{(\infty)}(\omega) := \{C \subseteq \omega : C \text{ infinite}\}$. Define $f : \omega \to A$ by $f(n) := F(h(n))$.

Claim 1: $\forall n\ h(n) \subseteq A$.

By induction on n: For $n = 0$, $h(0) = A \subseteq A$. For n^+:

$$\begin{aligned} h(n^+) &= G(h(n)) \\ &= h(n) \setminus \{F(h(n))\} \\ &\subseteq A. \end{aligned}$$

Claim 2: $n < m \implies f(n) \neq f(m)$.

Proof: By induction on m. Really, write $m = n + k^+$ and proceed by induction on k. We will show that $f(n) \notin h(m)$. $h = 0$:

$$\begin{aligned} h(n + 0^+) &= h(n^+) \\ &= h(n) \setminus \{F(h(n))\} \\ &= h(n) \setminus \{f(n)\} \\ f(n) \notin h(n^+) &= h(n + 0^+) = h(m). \end{aligned}$$

$h(n) \supsetneq h(n^+)$, so $h(n) \supsetneq h(n+k^+)$.

$$\begin{aligned} h(n+k^{++}) &= h(n+k^+) \setminus \{F(h(n+k^+))\} \\ &\subsetneq h(n+k^+) \subsetneq h(n), \\ f(n) \notin h(n^+) &\supseteq h(n+k^{++}). \end{aligned}$$

So, $\forall m > n\ f(n) \notin h(m)$, and $f(m) = F(h(m)) \in h(m)$. Therefore, $f(n) \neq f(m)$, so $f : \omega \hookrightarrow A$ is one-to-one. Therefore, $\omega \preceq A \,\&\, A \preceq \omega \implies \omega \approx A$. ☐

31.2 Idempotent Cardinals

Lemma 31.2. *Let $\lambda \geq \aleph_0$ and $1 \leq \mu \leq \lambda$.*

1. *If $\lambda^2 = \lambda$, then $\lambda\mu = \lambda$.*
2. *If $\lambda \geq \aleph_0$ and $\nu \leq \lambda$ and $\lambda^2 = \lambda$, then $\lambda + \nu = \lambda$.*

Proof. 1.

$$\lambda \leq \lambda \cdot 1 \leq \lambda \cdot \mu \leq \lambda \cdot \lambda = \lambda^2 = \lambda.$$

2.

$$\lambda \leq \lambda + \nu \leq \lambda + \lambda = \lambda \cdot 2 = \lambda.$$

☐

Theorem 31.3. *(ZL $\implies$) If K is infinite, $K \times K \approx K$.*

Proof. Let $\mathcal{A} = \{f \in \mathcal{P}(K \times (K \times K)) : \exists B \subseteq K\ f : B \to (B \times B)$ is a bijection$\}$.

Note: $\varnothing \in \mathcal{A}$. If $x \in K$, $\{\langle x, \langle x, x\rangle\rangle\} \in \mathcal{A}$. ZL 30.1 implies $\omega \preceq K$, so $\exists A \subseteq K$, $A \approx \omega$, $A \approx A \times A$. Moreover, for any $x \in K$, $\exists A' \subseteq K\ x \in A' \,\&\, A' \approx \omega$. ($A' = A \cup \{x\}$.) ☐

Lecture 32

April 14

32.1 Idempotent Cardinals

Theorem: (ZL) If K is infinite, then $K \approx K \times K$.

Proof.

$$\mathcal{A} := \{f \in \mathcal{P}(K \times (K \times K)) : \exists A \subseteq K \; f : A \to A \times A \text{ a bijection}\}.$$

Let $\mathcal{C} \subseteq \mathcal{A}$ be a chain. $\bigcup \mathcal{C} \in \mathcal{A}$. (Lemma: If $\mathcal{C}$ is a chain of (one-to-one) functions, then $\bigcup \mathcal{C}$ is a (one-to-one) function.) Let

$$\begin{aligned} A &:= \operatorname{dom}\left(\bigcup \mathcal{C}\right) \\ &= \bigcup_{f \in \mathcal{C}} \operatorname{dom}(f) \\ &\subseteq K. \end{aligned}$$

Let $t \in \operatorname{ran}(\bigcup \mathcal{C})$. So, $\exists x \; \langle x, t \rangle \in \bigcup \mathcal{C}$, which implies $\exists f \in \mathcal{C} \; \langle x, t \rangle \in f$. Since

$$f : \operatorname{dom}(f) \to \operatorname{dom}(f) \times \operatorname{dom}(f),$$

$t \in \operatorname{dom}(f) \times \operatorname{dom}(f)$, so $A = \operatorname{dom}(\bigcup \mathcal{C}) \supseteq \operatorname{dom}(f)$, so $t \in A \times A$.

Let $s \in A \times A$. Write $s = \langle a, b \rangle$, $a, b \in A$. Since $A = \operatorname{dom}(\bigcup \mathcal{C}) = \bigcup_{f \in \mathcal{C}} \operatorname{dom}(f)$, then we see that $\exists f, g \in \mathcal{C}$ such that $a \in \operatorname{dom}(f), b \in \operatorname{dom}(g)$. $\mathcal{C}$ is a chain, so $f \subseteq g$ or $g \subseteq f$. WLOG $f \subseteq g$, $a, b \in \operatorname{dom}(g)$. $g : \operatorname{dom}(g) \to \operatorname{dom}(g) \times \operatorname{dom}(g)$ is onto, so $\exists x \in \operatorname{dom}(g) \subseteq \operatorname{dom}(\bigcup \mathcal{C})$ such that $g(x) = \langle a, b \rangle = \bigcup \mathcal{C}(x)$. Hence, $\bigcup \mathcal{C} \in \mathcal{A}$.

By ZL, $\exists f \in \mathcal{A}$ maximal. Let $A := \operatorname{dom}(f)$, $\alpha = \operatorname{card}(A)$, $\kappa = \operatorname{card}(K)$. If $\alpha = \kappa$, then we are done since $f : A \to A \times A$ is a bijection, so $\alpha^2 = \alpha$.

If $\alpha \neq \kappa$, then $\alpha < \kappa$, so $(K \setminus A) \succeq A$. To see this, note that $K = (K \setminus A) \,\dot{\cup}\, A$, so $\kappa = \operatorname{card}(K \setminus A) + \alpha$. By CC, either $K \setminus A \succeq A$ or $A \succeq K \setminus A$. If $A \succ K \setminus A$, then

$$\begin{aligned} \kappa &= \operatorname{card}(K) \\ &= \operatorname{card}(K \setminus A) + \alpha \\ &\leq \alpha + \alpha \end{aligned}$$

$$
\begin{aligned}
&= 2 \cdot \alpha \\
&\leq \alpha \cdot \alpha \\
&= \alpha.
\end{aligned}
$$

(*Remark*: We noted before on Wednesday that necessarily A is infinite.)

Let $B \subseteq K \setminus A$ with $\text{card}(B) = \alpha$. Note that

$$
\begin{aligned}
A \times A &\approx A, \\
A \times B &\approx A, \\
B \times A &\approx A, \\
B \times B &\approx A.
\end{aligned}
$$

Observe that $\text{card}((A \times B) \dot\cup (B \times A) \dot\cup (B \times B)) = 3 \cdot \text{card}(A \times B) = 3 \cdot \alpha^2 = 3\alpha = \alpha = \text{card}(B)$. So, $\exists g : B \to [(A \times B) \cup (B \times A) \cup (B \times B)]$ a bijection. Let $h := f \cup g$, $h : (A \cup B) \to (A \cup B) \times (A \cup B)$ is a bijection. Then, $\mathcal{A} \ni h \supsetneq f$, which contradicts maximality of $\mathcal{A}$. Therefore, $\alpha = \kappa$, and we know $\alpha^2 = \alpha$, so $\kappa^2 = \kappa$. $\square$

Corollary 32.1. *If κ is infinite, λ is any cardinal, then*

$$\kappa + \lambda = \max(\kappa, \lambda).$$

If $\lambda \neq 0$, then

$$\kappa \cdot \lambda = \max(\kappa, \lambda).$$

We know that $\kappa < 2^\kappa$. If $2 \leq \kappa$, then $\kappa! > \kappa$.

Lecture 33

April 17

33.1 Well-Ordered Sets

Definition 33.1. A **well-ordering** is a relation $\leq$ with $\text{fld}(\leq) = X$ such that

1. $\leq$ is a transitive relation,
2. $(\forall x)[x \in X \to \langle x, x\rangle \in \leq]$,
3. $(\forall x)(\forall y)[((x \in X \;\&\; y \in X) \;\&\; (x \leq y \;\&\; y \leq x)) \to x = y]$,
4. $(\forall x)(\forall y)[(x \in X \;\&\; y \in X) \to (x \leq y \vee y \leq x)]$,
5. $(\forall Y)[(Y \subseteq X \;\&\; Y \neq \varnothing) \to (\exists y)[y \in Y \;\&\; (\forall z)(z \in Y \to y \leq z)]]$.

Example 33.2. For $X = \omega$, $\leq\, = \,\subseteq\, = \,\underline{\in}$ is a well-ordering.

Example 33.3. $X = \mathbb{R}$, where $\leq$ is the usual order, is a totally ordered set, *but* it is not well-ordered. $Y = (-\infty, 0)$ has no least element! Also, $Z := \{x \in \mathbb{Q} : x > 0\}$ has no least element.

Question: For which sets Y does there exist some relation $\leq$ with $\text{fld}(\leq) = X$ such that $\leq$ is a well-ordering?

Answer: Every set admits a well-ordering.

Example 33.4. If X is finite and $\leq$ is a total order on X, then $\leq$ is a well-ordering.

Example 33.5. Let $X = \omega$ with

$$\leq := \left\{ \langle a, b\rangle \in \omega \times \omega : \begin{cases} a, b \text{ are both even } \& \; a \leq b \text{ or} \\ a, b \text{ are both odd } \& \; a \leq b \text{ or} \\ a \text{ is even } \& \; b \text{ is odd} \end{cases} \right\}.$$

Let $Y \subseteq X = \omega$, $Y \neq \varnothing$. If $Y \cap 2 \cdot \omega \neq \varnothing$, then let $y \in Y \cap 2 \cdot \omega$ be the least element relative to $\leq$. Otherwise, $\varnothing \neq Y \subseteq 1 + 2 \cdot \omega$. Let y be the $\leq$-least element of Y. If $z \in Y$ and z is even, then y is even and $y \leq z$, so $y \leq' z$. If z is odd and y is even, then $y \leq' z$. If y is odd, then y is the $\leq$-least element of Y, so $y \leq' z$.

(*Remark*: If $y, z \in Y$ are least elements of Y, $(Y, \leq)$ is linearly ordered, so $y = z$.)

Example 33.6. If $X = \omega \times \omega$, we can take $\leq$ to be the lexicographic order. Then, one has

$$\langle 0,0\rangle, \langle 0,1\rangle, \ldots, \langle 1,0\rangle, \ldots, \langle 2,0\rangle, \ldots .$$

Similarly, one can take $\langle 0,0,0\rangle, \ldots, \langle 1,0,0\rangle, \ldots$.

33.2 Ordinals & Cardinals

Definition 33.7. A transitive set α is an **ordinal** if $\underline{\in}_\alpha := \{\langle \beta,\gamma\rangle \in \alpha \times \alpha : \beta \underline{\in} \gamma\}$ is a well-ordering.

Example 33.8. 5 is an ordinal.

Example 33.9. ω is an ordinal.

Example 33.10. $\omega^+ = \omega \cup \{\omega\}$ is an ordinal.

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

Definition 33.11. κ is a **cardinal** if κ is an ordinal and $\forall \alpha \in \kappa\ \alpha \prec \kappa$.

33.3 Transfinite Recursion

Definition 33.12. A **class function** $\mathbb{G} : \mathbb{V} \to \mathbb{V}$ is a formula $\gamma(x, y)$ of set theory (possibly with parameters) such that $\forall x\ \exists! y\ \gamma(x, y)$.

$$\mathbb{G}(x) = y \iff \gamma(x, y).$$

Theorem 33.13. *Given a class function* $\mathbb{G}$ *and a well-ordered set* $(X, \leq)$*, there exists a unique function* f *with* $\mathrm{dom}(f) = X$ *such that* $\forall x \in X\ f(x) = \mathbb{G}(f \restriction \{y \in X : y < x\})$.

Lecture 34

April 19

34.1 Axiom of Replacement

Axiom (Schema) of Replacement: Given a formula $\varphi(x, y, t_1, \ldots, t_n)$ of set theory with free variables amongst $\{x, y, t_1, \ldots, t_n\}$, we have

$$\text{Replacement}_\varphi : (\forall t_1) \cdots (\forall t_n)(\forall A)[(\forall x)(\forall y)(\forall z)((x \in A \,\&\, \varphi(x, y, t_1, \ldots, t_n) \,\&\, \varphi(x, z, t_1, \ldots, t_n) \to y = z) \\ \to (\exists B)(\forall u)(u \in B \leftrightarrow (\exists a)(a \in A \,\&\, \varphi(a, u, t_1, \ldots, t_n))))].$$

Informal: φ defines a "class relation". Let $\mathbb{F} := \{\langle x, y\rangle : \varphi(x, y)\}$. Replacement says that if $\mathbb{F} \restriction A$ is a class function, then $\mathbb{F} \restriction A$ is actually a function.

34.2 Transfinite Recursion

Theorem (Transfinite Recursion): Given a formula $\gamma(x, y)$ such that $\forall x\ \exists! y\ \gamma(x, y)$ (i.e. γ is a "class function", $\mathbb{G}(x) = y \iff \gamma(x, y)$) and a well-ordered set $(X, \leq)$, then $\exists! F : X \to Y$ with the property $\forall x \in X\ F(x) = \mathbb{G}(F \restriction \operatorname{seg}(x))$, where $\operatorname{seg}(x) = \{t \in X : t < x\}$.

Proof. Let $\mathcal{F}$ be the set of f such that

- f is a function,
- $\operatorname{dom} f \subseteq X$,
- $\operatorname{dom} f$ is an initial segment of X (i.e. if $x \in \operatorname{dom} f$ and $y < x$, then $y \in \operatorname{dom} f$),
- $(\forall x \in \operatorname{dom} f)\ f(x) = \mathbb{G}(f \restriction \operatorname{seg}(x))$, or $\gamma(f \restriction \operatorname{seg}(x), f(x))$.

Let

$$\varphi(x, y) := x \in X \,\&\, y \text{ is a function} \,\&\, \operatorname{dom}(y) = \operatorname{seg}(x) \cup \{x\} \,\&\, (\forall t \in \operatorname{dom} y)\ y(t) = \mathbb{G}(y \restriction \operatorname{seg}(t)).$$

Claim 1: $\forall x \in X\ \exists! y\ \varphi(x, y)$.

Proof of Claim: First, we show $\forall x\ \forall y\ \forall z\ (\varphi(x, y) \,\&\, \varphi(x, z) \to y = z)$. If this were false, then

$$\{x \in X : \exists y\ \exists z\ y \neq z \,\&\, \varphi(x, y) \,\&\, \varphi(x, z)\} \neq \varnothing.$$

So, $\exists x \in X$, least, with $\exists y\ \exists z\ \varphi(x, y) \,\&\, \varphi(x, z) \,\&\, y \neq z$. Fix y, z witnessing this. Then,

$$\operatorname{dom}(y) = \operatorname{dom}(z) = \operatorname{seg}(x) \cup \{x\},$$

so

$$y(x) = \mathbb{G}(y \upharpoonright \operatorname{seg}(x)),$$
$$z(x) = \mathbb{G}(z \upharpoonright \operatorname{seg}(x)).$$

Take $t < x$. Then $\varphi(t, y \upharpoonright \operatorname{seg}(t) \cup \{t\})$ & $\varphi(t, z \upharpoonright \operatorname{seg}(t) \cup \{t\})$. So, $\mathbb{G}(y \upharpoonright \operatorname{seg}(x)) = \mathbb{G}(z \upharpoonright \operatorname{seg}(x))$, and therefore $y = z$, which is a contradiction.

By Replacement, $\exists B\, \forall u\, u \in B \leftrightarrow \exists x \in X\, \varphi(x, u)$. So, $\mathcal{F}$ is B.

Claim 2: $\mathcal{F}$ is a chain. Take $f, g \in \mathcal{F}$.

Sub-Claim 1: $\operatorname{dom} f \subseteq \operatorname{dom} g$ or $\operatorname{dom} g \subseteq \operatorname{dom} f$.

Proof of Sub-Claim 2: If not, take x, least, such that

$$x \in \operatorname{dom} f \triangle \operatorname{dom} g = (\operatorname{dom} f \setminus \operatorname{dom} g) \cup (\operatorname{dom} g \setminus \operatorname{dom} f).$$

WLOG, $x \in \operatorname{dom} f \setminus \operatorname{dom} g$. Then $\forall y < x\ y \in \operatorname{dom} f \cap \operatorname{dom} g$. Suppose $z \in \operatorname{dom} g$. $\operatorname{dom} g$ is an initial segment of X, so either $x < z$ or $z < x$. If $x < z$, then $x \in \operatorname{dom} g$ which is a contradiction. So, $z < x$, and $\operatorname{dom} g \subseteq \operatorname{dom} f$.

Sub-Claim 2: If $x \in \operatorname{dom} f \cap \operatorname{dom} g$, $f(x) = g(x)$. If not, there would be a least x with $f(x) \neq g(x)$. Then, $f \upharpoonright \operatorname{seg}(x) = g \upharpoonright \operatorname{seg}(x)$. So, $f(x) = \mathbb{G}(f \upharpoonright \operatorname{seg}(x)) = \mathbb{G}(g \upharpoonright \operatorname{seg}(x)) = g(x)$.

Sub-Claim 3: $\forall x \in X\ \exists f \in \mathcal{F}\ x \in \operatorname{dom} f$.

Proof of Sub-Claim 3: If not, there would be a least counterexample x. Let $h := \bigcup \mathcal{F}$. h is a function. $\operatorname{dom} g$ is an initial segment of X. h satisfies the recursion condition. If $t \in \operatorname{dom} h$, then $\exists f \in \mathcal{F}\ t \in \operatorname{dom} f$. Then, $h(t) = f(t) = \mathbb{G}(f \upharpoonright \operatorname{seg}(t)) = \mathbb{G}(h \upharpoonright \operatorname{seg}(t))$. So, $\operatorname{dom} h = \operatorname{seg}(x)$. Set $H := h \cup \{\langle x, \mathbb{G}(h)\rangle\}$ and $H \in \mathcal{F}$, so x is not a counterexample.

Therefore, $h : X \to \operatorname{ran} h$ solves the problem. $\square$

Lecture 35

April 21

35.1 Applications of Transfinite Recursion

Definition 35.1. If $(Z, \leq)$ is a totally ordered set, $I \leq Z$ is an **initial segment** if

$$\forall i \in I\ \forall z \in Z\ (z < i \to z \in I).$$

Theorem 35.2. *Given a set X with a choice function $F : \mathcal{P}(X) \setminus \{\varnothing\} \to X$ (i.e. $\forall A \in \mathcal{P}(X)\ F(A) \in A$) and a well-ordered set $(Y, \leq)$, there exists an initial segment $Y' \subseteq Y$ and a function $g : Y' \to X$ which is one-to-one such that either $Y' = Y$ or g is onto.*

Proof. Fix $\star$ a set which is *not* an element of X.

$$\gamma(x, y) := (X \setminus \operatorname{ran}(x) = \varnothing \ \&\ y = \star) \vee (X \setminus \operatorname{ran}(x) \neq \varnothing \ \&\ y = F(X \setminus \operatorname{ran}(x))).$$

The corresponding class function is

$$\mathbb{G}(f) = \begin{cases} \star & \text{if } X \subseteq \operatorname{ran} f, \\ F(X \setminus \operatorname{ran}(f)) & \text{if } X \setminus \operatorname{ran}(f) \neq \varnothing. \end{cases}$$

By transfinite recursion, there exists a function h with $\operatorname{dom}(h) = Y$ such that

$$\forall y \in Y\ h(y) = \mathbb{G}(h \restriction \operatorname{seg}(y))$$

Let $Y' := \{y \in Y : h(y) \in X\}$ and let $g := h \restriction Y'$.

Claim 1: Y' is an initial segment.

Proof: Let $y \in Y'$ and $z \in Y$ with $z < y$. Then, $h(y) \in X$, i.e. $h(y) \neq \star$, i.e.

$$h(y) = F(X \setminus \operatorname{ran}(h \restriction \operatorname{seg}(y))),$$

so

$$X \supsetneq \operatorname{ran}(h) \restriction \operatorname{seg}(y). \tag{35.1}$$

$\operatorname{seg}(z) \subsetneq \operatorname{seg}(y)$, which implies

$$\operatorname{ran}(h \restriction \operatorname{seg}(z)) \subseteq \operatorname{ran}(h \restriction \operatorname{seg}(y)). \tag{35.2}$$

(35.1) and (35.2) imply $X \setminus \operatorname{ran}(h \restriction \operatorname{seg}(z)) \neq \varnothing$, so $h(z) = F(X \setminus \operatorname{ran}(h \restriction \operatorname{seg}(z))) \in X$, so $z \in Y'$.

Claim 2: g is one-to-one.

Proof: Suppose $y, z \in Y'$ and $y \neq z$. WLOG $y < z$.

$$\begin{aligned} g(z) = h(z) &= \mathbb{G}(h \restriction \operatorname{seg}(z)) \\ &= F(X \setminus \operatorname{ran}(h \restriction \operatorname{seg}(z))). \end{aligned}$$

$y < z \to y \in y \in \operatorname{seg}(z)$, so

$$g(z) = F(X \setminus \operatorname{ran}(h \restriction \operatorname{seg}(z))) \neq g(y) = h(y) \in \operatorname{ran}(h \restriction \operatorname{seg}(z)).$$

Claim 3: Either g is onto or $Y' = Y$.

Proof: If $Y' \neq Y$, then $\exists y \in Y$ such that $h(y) = \star$, so $X \setminus \operatorname{ran}(h \restriction \operatorname{seg}(y)) = \varnothing$. Therefore,

$$X \subseteq \operatorname{ran}(h \restriction \operatorname{seg}(y)) \implies X \subseteq \operatorname{ran}(g).$$ □

Definition 35.3. If (X, R) and (Y, S) are pairs of a set X, a set Y, $R \subseteq X \times X$, and $S \subseteq Y \times Y$, a **homomorphism** $f : (X, R) \to (Y, S)$ is a function $f : X \to Y$ such that $\forall a, b \in X\ a\, R\, b \to f(a)\, S\, f(b)$. f is an **isomorphism** if f^{-1} is also a homomorphism.

Theorem 35.4. *For any well-ordered set $(X, \leq)$, there is an ordinal α and an isomorphism*

$$E : (X, \leq) \to (\alpha, \underline{\in}_\alpha).$$

$$\langle \beta, \gamma \rangle \in \underline{\in}_\alpha \iff (\beta \in \gamma \vee \beta = \gamma)\ \&\ \beta, \gamma \in \alpha.$$

Proof. Let $\gamma(x, y) := y = \operatorname{ran}(x)$. Alternatively, $\mathbb{G}(x) = \operatorname{ran}(x)$. By transfinite recursion, there exists a unique function $E : X \to \alpha$, $\alpha = \operatorname{ran}(X)$, such that $\forall x \in X\ E(x) = \operatorname{ran}(E \restriction \operatorname{seg}(x))$.

Note: E is onto α by the definition of α.

Claim 1: If $y < z$, $y, z \in X$, then $E(y) \in E(z)$. ($E(z) = \operatorname{ran}(E \restriction \operatorname{seg}(z))$, $y \in \operatorname{seg}(z)$, so we can conclude $E(y) \in \operatorname{ran}(E \restriction \operatorname{seg}(z)) = E(z)$.)

Claim 2: $\forall x \in X\ E(x) \notin E(x)$.

Proof: If this were false, there would be a least $x \in X$ with $E(x) \in E(x) = \operatorname{ran}(E \restriction \operatorname{seg}(x))$, so

$$\exists y < x\ E(y) \in \operatorname{ran}(E \restriction \operatorname{seg}(x)) = E(x) = E(y),$$

i.e. $E(y) \in E(y)$, which contradicts the minimality of x.

Claim 3: $\forall x \in X$, $E(x)$ is transitive.

Proof: Suppose $t \in E(x)$ and $s \in t$. Then, $t \in E(x) = \operatorname{ran}(E \restriction \operatorname{seg}(x))$, so

$$\exists y < x\ t = E(y) = \operatorname{ran}(E \restriction \operatorname{seg}(y)).$$

so $\exists z < y$ such that $s = E(z) \in E(x)$.

Claim 4: If $x < y$, then $E(y) \notin E(x)$. $\square$

Lecture 36

April 24

36.1 The Class of Ordinals

Definition 36.1.

$$\alpha \in \mathbb{ON} \iff \alpha \text{ is an ordinal.}$$

Proposition 36.2. *$\mathbb{ON}$ is a transitive class, i.e. if $\alpha \in \mathbb{ON}$ and $\beta \in \alpha$, then $\beta \in \mathbb{ON}$.*

Recall that

$$\underline{\in}_\alpha := \{t \in \alpha \times \alpha : \exists \beta, \gamma \in \alpha\ \beta \in \gamma \text{ or } \beta = \gamma \;\&\; t = \langle \beta, \gamma \rangle\}.$$

Lemma 36.3. *If $\alpha \in \mathbb{ON}$, then the ε-image function E, i.e. the function satisfying*

$$\forall x \in \alpha\ E(x) = \operatorname{ran}(E \restriction \operatorname{seg}(x)),$$

for $(\alpha, \underline{\in}_\alpha)$ is I_α.

Proof. If not, then the set $\{\beta \in \alpha : E(\beta) \neq \beta\}$ is non-empty and hence has a least element β.

$$\begin{aligned} E(\beta) &= \operatorname{ran}(E \restriction \operatorname{seg}(\beta)) \\ &= \operatorname{ran}(E \restriction \{\gamma \in \alpha : \gamma \in \beta\}) \\ &= \operatorname{ran}(E \restriction \beta) \end{aligned}$$

(since α is *transitive*)

$$= \operatorname{ran}(I_\beta) = \beta.$$

□

Consider $(X, \leq) = (\mathbb{N}, \leq')$, where the ordering is

$$0 < 2 < 4 < 6 < 8 < \cdots < 1 < 3 < 5 < 7 < \cdots.$$

We have

$$\begin{aligned} E(0) &= \operatorname{ran}(E \restriction \operatorname{seg}(0)) \\ &= \operatorname{ran}(\varnothing) \\ &= \varnothing. \\ E(2) &= \operatorname{ran}(E \restriction \operatorname{seg}(2)) \end{aligned}$$

$$\begin{aligned}
&= \operatorname{ran}(E \restriction \{0\}) \\
&= \{E(0)\} = \{\varnothing\} = 1. \\
E(4) &= \operatorname{ran}(E \restriction \operatorname{seg}(4)) \\
&= \operatorname{ran}(E \restriction \{0, 2\}) \\
&= \{E(0), E(2)\} \\
&= \{0, 1\} = 2. \\
E(2n) &= n. \\
E(1) &= \operatorname{ran}(E \restriction \operatorname{seg}(1)) \\
&= \operatorname{ran}(E \restriction \{2n : n \in \omega\}) \\
&= \{E(2n) : n \in \omega\} \\
&= \{n : n \in \omega\} \\
&= \omega. \\
E(3) &= \operatorname{ran}(E \restriction \operatorname{seg}(3)) \\
&= \operatorname{ran}(E \restriction \operatorname{seg}(1) \cup E \restriction \{1\}) \\
&= \omega \cup \{E(1)\} \\
&= \omega \cup \{\omega\} \\
&= \omega^+. \\
E(5) &= \omega^{++} = \omega + 2. \\
E(2n+1) &= \omega + n \\
&= \omega^{\overbrace{+\cdots+}^{n \text{ times}}}. \\
E[\![X]\!] &= \omega + \omega = \omega \cdot 2.
\end{aligned}$$

Theorem 36.4. *For α a set, the following are equivalent:*

1. $\alpha \in \mathbb{ON}$.
2. $\exists (X, \leq)$*, well-ordered, such that* $\alpha = E[\![X]\!]$.
3. $\exists (Y, \leq)$*, well-ordered, and* $y \in Y$, $\alpha = E(y)$.

Proof. 1 $\implies$ 2: Sri-obvious. This is a corollary of 36.3.

$$\alpha = I_\alpha[\![\alpha]\!] = E[\![\alpha]\!].$$

2 $\implies$ 3: We have $\alpha = E[\![X]\!]$. Pick $\star \notin X$. Set $Y := X \cup \{\star\}$. Define $\star > X$.

$$\begin{aligned}
E(\star) &= \operatorname{ran}(E \restriction \operatorname{seg}(\star)) \\
&= \operatorname{ran}(E \restriction X) \\
&= \alpha.
\end{aligned}$$

3 $\implies$ 1:

$$\begin{aligned}
\alpha = E(y) &= \operatorname{ran}(E \restriction \operatorname{seg}(y)) \\
&= \varepsilon\text{-image of } (\operatorname{seg}(y), \leq \restriction \operatorname{seg}(y)),
\end{aligned}$$

and hence $\alpha \in \mathbb{ON}$. $\square$

Proposition 36.5.

$$\alpha \in \mathbb{ON} \implies \alpha \notin \alpha.$$

Proof. By 3 in 36.4, $\alpha = E(y)$ for some $y \in Y$, $(Y, \leq)$ well-ordered. We showed $E(y) \notin E(y)$. □

Proof of 36.2. Realize $\alpha = E[\![X]\!]$, $(X, \leq)$ well-ordered. $\beta \in \alpha \implies \exists x \in X \ \beta = E(x)$. By 3, $\beta \in \mathbb{ON}$. □

Proposition 36.6.

$$\alpha, \beta \in \mathbb{ON} \implies \alpha \subseteq \beta \text{ or } \beta \subseteq \alpha.$$

Proof. If not, there exists a least $\gamma \in \alpha \setminus \beta$ and a least $\delta \in \beta \setminus \alpha$. $\forall \rho \ \rho \in \gamma \implies \rho \in \alpha$ (because α is transitive) and $\rho \in \beta$ (because γ is the least element in α with $\gamma \notin \beta$). So, $\gamma \subseteq \alpha \cap \beta$. Likewise, $\delta \subseteq \alpha \cap \beta$.

Claim: If $\nu \in \gamma$, then $\nu \in \delta$.

Proof of Claim: $(\beta, \underline{\in}_\beta)$ is totally ordered so if the Claim fails, then $\delta \,\underline{\in}\, \nu \in \gamma \in \alpha$. By transitivity, $\delta \in \alpha$, which is a contradiction.

$\gamma \subseteq \delta$ and dually, $\delta \subseteq \gamma$, which implies $\delta = \gamma$. This is a contradiction. □

36.2 Ordinal Arithmetic

Ordinal arithmetic is defined as follows:

$$\begin{aligned} \alpha + 0 &:= \alpha, \\ \alpha + \beta &:= (\alpha + \beta)^+, \\ \alpha + \lambda &:= \bigcup_{\beta \in \lambda} (\alpha + \beta), \end{aligned}$$

for λ a limit. Note that

$$\omega + 1 = \omega^+ \neq \omega,$$

but

$$1 + \omega = \bigcup_{n \in \omega} (1 + n) = \omega.$$

Lecture 37

April 26

37.1 Ordering on Ordinals

Proposition 37.1. *If $\alpha, \beta \in \mathbb{ON}$, then $\alpha \in \beta$ or $\alpha = \beta$ or $\beta \in \alpha$.*

Lemma 37.2. *For $\alpha, \beta \in \mathbb{ON}$,*

$$\alpha \in \beta \leftrightarrow \alpha \subsetneq \beta.$$

Proof. $\implies$ $\alpha \in \beta$, then because β is transitive, $\alpha \subseteq \beta$. We know $\beta \notin \beta$, then because $\alpha \in \beta$ & $\alpha \subseteq \beta$, so $\alpha \subsetneq \beta$.

[*Recall*: We showed if $(X, \leq)$ is well-ordered and $E : X \to \gamma$ is the ε-image function, i.e.

$$\forall x \in X \quad E(x) = \operatorname{ran}(E \restriction \operatorname{seg}(x)),$$

then $\forall x \in X$ $E(x) \notin E(x)$. $\alpha \in \mathbb{ON} \iff \exists (X, \leq)$, well-ordered, and $y \in X$ such that $\alpha = E(y)$.]

$\impliedby$ Suppose $\alpha \subsetneq \beta$.

$$\begin{aligned} I_\beta = E_\beta &:= \varepsilon\text{-image function on } \beta, \\ I_\alpha = E_\alpha &:= \varepsilon\text{-image function on } \alpha. \end{aligned}$$

So,

$$\begin{aligned} \alpha &= \operatorname{ran}(E_\alpha) \\ &= \operatorname{ran}(E_\beta \restriction \alpha) \\ &= E_\beta(\alpha) \\ &\in \operatorname{ran}(E_\beta) = \beta. \end{aligned}$$

since $E_\alpha = I_\alpha = I_\beta \restriction \alpha = E_\beta \restriction \alpha$. So, $\alpha \in \beta$. $\square$

Now, we have

$$\alpha < \beta \iff \alpha \in \beta \iff \alpha \subsetneq \beta.$$

Proposition 37.3. *Let $\alpha, \beta, \gamma \in \mathbb{ON}$.*

- $\alpha \notin \alpha$.
- $(\alpha \in \beta \,\&\, \beta \in \gamma) \to \alpha \in \gamma$.
- $\alpha \in \beta \vee \beta \in \alpha \vee \alpha = \beta$.

Proposition 37.4. *If X is a non-empty set of ordinals, then $\exists \alpha \in X$ least.*

Proof. Let $\alpha \in X$. If $\alpha \cap X = \varnothing$, then α is the least element of X. Otherwise, $X \cap \alpha \subseteq \alpha$ is non-empty. Let $\beta \in X \cap \alpha$ be least. Then $\forall \gamma \in X$, either $\gamma \in X \cap \alpha$ (so $\beta \underline{\in} \gamma$) or $\gamma \notin \alpha$ so $\alpha \underline{\in} \gamma$ which implies $\beta \in \gamma$. □

Proposition 37.5. *If X is a transitive set of ordinals, then $X \in \mathbb{ON}$.*

Proof. The restriction of the $\in$ relation of $\mathbb{ON}$ to X gives a total well-ordering of X. By hypothesis, X is transitive, so $X \in \mathbb{ON}$. □

Corollary 37.6. *If X is a set of ordinals, then $\bigcup X \in \mathbb{ON}$.*

Proof. X is a set of transitive sets, so $\bigcup X$ is transitive.

$$\beta \in \alpha \in X \to \beta \in \mathbb{ON},$$

so therefore $\bigcup X \subseteq \mathbb{ON}$. Hence, $\bigcup X \in \mathbb{ON}$. □

$\bigcup X$ is the least upper bound of X.

The following does not use AC.

Theorem 37.7.

$$\forall X \quad \exists \alpha \in \mathbb{ON} \quad \alpha \not\preceq X.$$

Proof. Let $Y := \{R \in \mathcal{P}(X \times X) : R \text{ is a well-ordering of } \mathrm{fld}(R)\}$. Let $\alpha := \{E(R) : R \in Y\} \subseteq \mathbb{ON}$. α is transitive: if $u \in \alpha$, then $\exists R \in Y \ u = E(R)$ and if $t \in u$, $\exists x \in \mathrm{fld}(R) \ t = E(x) = \mathrm{ran}(E \restriction \mathrm{seg}(x))$. Then, $R \cap (\mathrm{seg}(x) \times \mathrm{seg}(x)) \in Y$, so $t \in \alpha$. Therefore, $\alpha \in \mathbb{ON}$.

If $\alpha \preceq X$, then $\exists f : \alpha \hookrightarrow X$, one-to-one. Set $R := \{\langle f(\beta), f(\gamma)\rangle : \beta \underline{\in} \gamma \in \alpha\}$. Then,

$$f : (\alpha, \underline{\in}_\alpha) \xrightarrow{\sim} (\mathrm{fld}(R), R)$$

is an isomorphism of structures, so $R \in Y$. Then, $\alpha = E(R) \in \alpha$, because R and $\underline{\in}_\alpha$ are isomorphic well-orderings. But, $\alpha \notin \alpha$, so this is a contradiction. □

Theorem 37.8. *AC $\implies$ the well-ordering principle (WOP): $\forall X \ \exists \leq \ (X, \leq)$ is well-ordered.*

Proof. Let $\alpha \in \mathbb{ON}$ such that $\alpha \not\precsim X$. By AC, $\exists F : \mathcal{P}(X) \setminus \{\varnothing\} \to X$ a choice function, i.e.

$$\forall A \subseteq X \ A \neq \varnothing, F(A) \in A.$$

Let $\star \notin X$ and define $g : \alpha \to X \cup \{\star\}$ by transfinite recursion:

$$g(\beta) := \begin{cases} \star & \text{if } X \subseteq \operatorname{ran}(g \restriction \beta) \\ F(X \setminus \operatorname{ran}(g \restriction \beta)) & \text{otherwise} \end{cases}$$

Either: $\exists Y' \subseteq \alpha$ such that $g \restriction Y' : Y' \to X$ is onto or g is one-to-one and $g : \alpha \hookrightarrow X$. Since $\alpha \not\precsim X$, the latter cannot happen. $\square$

Lecture 38

April 28

38.1 Proof of Zorn's Lemma

Theorem 38.1.

$$\text{WO} \implies \text{ZL},$$

that is, the Well-Ordering Principle implies Zorn's Lemma.

Proof. Given $\mathcal{A}$ a set such that $\forall \mathcal{C} \subseteq \mathcal{A}$, a chain, $\bigcup \mathcal{C} \in \mathcal{A}$. We must find $M \in \mathcal{A}$ maximal.

By WO, $\exists \leq$, a well-ordering of $\mathcal{A}$. Define a function $\chi : \mathcal{A} \to \{0, 1\} = 2$ by transfinite recursion:

$$\chi(a) = \begin{cases} 1 & \text{if } \forall b < a \ (\chi(b) = 1 \to b \subseteq a) \\ 0 & \text{otherwise} \end{cases}$$

If c is the least element of $\mathcal{A} \setminus \operatorname{dom} f$, then

$$\gamma(f, y) \iff y = 1 \ \& \ (\forall b \in \operatorname{dom} f) \ [f(b) = 1 \to b \subseteq c] \text{ or } y = 0 \ \& \ \neg(\forall b \in \operatorname{dom} f) \ [f(b) = 1 \to b \subseteq c].$$

Let $\mathcal{C} = \{a \in \mathcal{A} : \chi(a) = 1\}$.

Claim 1: $\mathcal{C}$ is a chain.

Let $a, b \in \mathcal{C}$. WLOG $a > b$. Then, $\chi(a) = 1 \implies \forall c < a \ (\chi(c) = 1 \to c \subseteq a)$. In particular, $\chi(b) = 1 \ \& \ b < a$, so $b \subseteq a$.

By hypothesis, $\bigcup \mathcal{C} =: c \in \mathcal{A}$.

Claim 2: c is maximal.

$\chi(c) = 1$ since if $\chi(b) = 1$ and $b < c$, then $b \in \mathcal{C}$, so $b \subseteq \mathcal{C} = c$. Therefore, $c \in \mathcal{C}$. Suppose $b \in \mathcal{A}$, $c \subseteq b$. $\chi(b) = 1$ since $\forall a \ \chi(a) = 1 \to a \subseteq c \subseteq b$, so in particular, if $a < b \ \& \ \chi(a) = 1$, then $a \subseteq b$. So, $b \in \mathcal{C}$, which implies $b \subseteq c$, so $b = c$. So, c is maximal. $\square$

Corollary 38.2. *All of our forms of AC are equivalent relative to ZF.*

- *AC0: Onto functions have right inverses.*

- *AC1: R a relation $\implies \exists f \subseteq R$ a function,* $\operatorname{dom} f = \operatorname{dom} R$.
- *AC2: The Cartesian product of non-empty sets is non-empty.*
- *AC3: $\forall A\ \exists F : \mathcal{P}(A) \setminus \{\varnothing\} \to A\ \forall a\ F(a) \subseteq a$.*
- *ZL (with respect to $\subseteq$).*
- *ZL' (arbitrary partial order).*
- *CC: $\forall X\ \forall Y\ X \preceq Y \vee Y \preceq X$.*
- *WO: $\forall X\ \exists \leq\ (X, \leq)$ is well-ordered.*

$$\begin{tikzcd}
AC0 \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & AC1 \arrow[d, leftrightarrow] & ZL \arrow[l] \arrow[d] \\
AC3 \arrow[r, leftrightarrow] \arrow[drr] & AC2 & CC \arrow[d] \\
 & & WO \arrow[u, bend right, to=1-3]
\end{tikzcd}$$

Reminder: CC $\to$ WO: $\exists \alpha \in \mathbb{ON}\ \alpha \not\preceq X$. By CC, $X \preceq \alpha$.

38.2 Axiom of Regularity

Axiom of Regularity:

$$\forall x\ [x \neq \varnothing \to (\exists m)[m \in x \,\&\, m \cap x = \varnothing]].$$

Proposition 38.3.

$$\forall x \quad x \notin x.$$

Define

$$\begin{aligned} V_0 &:= \varnothing \\ V_{\alpha^+} &:= V_\alpha \cup \mathcal{P}(V_\alpha) \\ V_\lambda &:= \bigcup_{\beta < \lambda} V_\beta, \end{aligned}$$

for λ a limit. Then, $\operatorname{rank}(x)$ is the least α such that $x \subseteq V_\alpha$ (∞ if $\forall \alpha\ x \not\subseteq V_\alpha$).

- $x \in y \iff \operatorname{rank}(x) \in \operatorname{rank}(y)$.
- $\alpha \in \mathbb{ON} \to \operatorname{rank}(\alpha) = \alpha$.
- $\implies$ If x is ranked, then $x \notin x$.

Proposition 38.4.

$$\textit{Axiom of Regularity} \iff \forall x\ \operatorname{rank}(x) \in \mathbb{ON}.$$

Proof. $\impliedby$: Given $x \neq \varnothing$, let $m \in x$ have minimal rank.

$\implies$: Uses transitive closures. □