MATH 412 - Set Theory 7.10.21 Th

2 midterms + 1 final (%30 & %40)

Set: A collection of things

Russel's Paradox: C: Catalog of catalogs that does not contain itself. (Red books)

Does C list itself as a catalogue?

If $C \in C$, then $C \notin C$

If $C \notin C$, then $C \in C$. ※

Class Theory

autological - pentasyllabic, short

heterological - trisyllabic, long

Question: Is heterological heterological?

Theorem: There is no set S such that $x \in S \leftrightarrow x \notin x$.

Proof: If such a set exists, by taking $x = S$,

$$S \in S \leftrightarrow S \notin S$$

$$P \leftrightarrow \neg P \quad ※$$

Defn: (Empty set) is a set with no elts. ($\emptyset$)

Axiom of Extension $X = Y \leftrightarrow \forall x,\ x \in X \leftrightarrow x \in Y$

Thm: $\emptyset$ is unique.

12.10.21 T

Remark: Everything is a set.

- $X \subseteq Y$ means every elt. of X is an elt. of Y.
- $\mathcal{P}(X)$: power set of X.

  $\mathcal{P}(X) = \{y : y \subseteq X\}$
- Union set $\bigcup X = \{y : y \in z \text{ for some } z \in X\}$

  $X = \{x_1, x_2, x_3\}$ $\quad \bigcup X = x_1 \cup x_2 \cup x_3$

- $\cap \mathcal{X} = \{y : y \in z \text{ for all } z \in \mathcal{X}\}$
  $= \{y : z \in \mathcal{X} \to y \in z\}$
- $\cap \emptyset = \{y : \underbrace{\underbrace{z \in \emptyset}_{F} \to y \in z}_{T}\}$ → a bit problematic. If it is a set, then it is the self of all the sets.
- $X_1 \cup X_2 = \cup \{X_1, X_2\}$
- $X_1 \cap X_2 = \cap \{X_1, X_2\}$
- $\cap \mathcal{X}$ makes sense if $\mathcal{X} \neq \emptyset$.
- $\cup \emptyset = \emptyset$
- $X \setminus Y = \{x \in X : x \notin Y\}$
- $X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$
  ↳ sym. difference
  $(X \Delta Y) = (X \cup Y) \setminus (X \cap Y)$

- $X \Delta X = \emptyset$
- $X \Delta \emptyset = X$
- $X \Delta Y = Y \Delta X$ (com.)
- $(X \Delta Y) \Delta Z = X \Delta (Y \Delta Z)$
- identity of Δ: $\emptyset$
- Δ: every elt. is the inverse of itself. (idempotent)

Cartesian Products Relations & Functions

$X \times Y = \{(x, y) : x \in X, y \in Y\}$

If $(x, y) = \{x, y\}$, then $(y, x) = \{y, x\} = \{x, y\}$. We don't want that.

- $\{x, \{y\}\} = \{z, \{t\}\}$, then $x = z$ & $\{y\} = \{t\}$. But, what about if $x = \{t\}$ & $\{y\} = z$?
- $(x, y) = \{\{x\}, \{x, y\}\}$. We need to check: If $(x, y) = (z, t)$, is it true that $x = z$ & $y = t$?

  $\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, t\}\}$, then either:
  - $\{x\} = \{z\} \to x = z$
    $\{x, y\} = \{z, t\} \to y = t$ (since $x = z$), or:
  - $\{x\} = \{z, t\}$ possible only when $x = z = t$
    $\{z\} = \{x, y\}$ " " " $z = x = y$
    } $x = y = z = t$, no problem.

HW: which of the following would be suitable for defining ordered tripple?

a) $(x,y,z) = \{(x,y),(y,z)\}$

b) $(x,y,z) = ((x,y),(y,z))$

c) $(x,y,z) = \{\{x\},\{x,y\},\{x,y,z\}\}$

$(x_1,x_2) = \{\{x_1\},\{x_1,x_2\}\}$

$(x_1,x_2,\ldots,x_n) = ((x_1,x_2,\ldots,x_{n-1}),x_n)$. By induction we define it this way.

$(x_1,\ldots,x_n) = (y_1,\ldots,y_n)$. Does it imply that $x_1=y_1, x_2=y_2, \ldots, x_n=y_n$?

$$((x_1,x_2,\ldots,x_{n-1}),x_n) = ((y_1,y_2,\ldots,y_{n-1}),y_n).$$

By induction hypothesis $\Rightarrow x_1=y_1, x_2=y_2, \ldots, x_n=y_n$

If X and Y are sets, $X\times Y = \{(x,y) : x\in X \ \& \ y\in Y\}$

Remark: $\prod_{i\in I} X_i$ not defined yet. → if I is infinite

Relation on a set X: is a subset R of $X\times X$.

- reflexive: $\forall x\in X \quad (x,x)\in R$
- transitive: $(x,y)\in R, (y,z)\in R \to (x,z)\in R$
- sym. : $(x,y)\in R \to (y,x)\in R$
- antisym. : $(x,y)\in R \to (y,x)\notin R$

A function from a set X to a set Y is a subset F of $X\times Y$. satisfying

$$\forall x\in X, \exists! y \text{ s.t. } (x,y)\in F$$

If $(x,y_1)\in F \ \& \ (x,y_2)\in F \to y_1=y_2$

- 1-1 function: $\forall x_1,x_2,y$ if $(x_1,y),(x_2,y)\in F \to x_1=x_2$
- onto function: $\forall y \ \exists x : (x,y)\in F$

$f: X \to Y$, $f^{-1}: Y \to X$ exists if f is 1-1 and onto.

- identity function : $\{(x,x) : x \in X\}$
- $f^{-1} = \{(y,x) : (x,y) \in f\}$
- $f \circ g(x) = \{(x,z) : \exists y : (y,z) \in f \ \& \ (x,y) \in g\}$
- $Y^X = \{$all functions from X to $Y\}$
- $2 = \{0,1\} = \{\emptyset, \{\emptyset\}\}$

  $\emptyset = 0$ $= \{0\} = \{\{\emptyset\}\}$

  $3 = \{0,1,2\}$
- $\{0,1\}^X = \{f : f: X \to \{0,1\}\}$
- $|2^X| = |\mathcal{P}(X)|$
- $\{a,b,c,d,e\} \to \{0,1\}$

$$\left.\begin{array}{l} a \longmapsto 0 \\ b \longmapsto 1 \\ c \longmapsto 1 \\ d \longmapsto 1 \\ e \longmapsto 1 \end{array}\right\} \begin{array}{l} \text{32 possibilities} \\ \& \ |\mathcal{P}(X)| = 32 \end{array}$$

- $f^{-1}(\{1\})$ is a subset of X.

<u>A family of sets</u>

I : index set

$F : I \to W$ for some W.

$X_i = F(i)$

$\{X_i : i \in I\}$ is called a family of sets indexed by the set I.

$\bigcup_{i \in I} X_i = \bigcup \{X_i : i \in I\}$ $\qquad$ $\bigcap_{i \in I} X_i = \bigcap \{X_i : i \in I\}$

$\mathcal{F}: I \to W$

$i \mapsto \mathcal{F}(i) = X_i \in W$

$\{X_i : i \in I\}$ is a famiy of sets. $\} \subseteq W$

Given a famiy of sets. A <u>choice function</u> $f: I \to \bigcup W$

s.t. $f(i) \in \mathcal{F}(i) = X_i$ for every $i \in I$.

$I = \{1, 2\}$.

The set of all choice functions on $X_1 \times X_2$ is the set of all ordered <u>pairs</u>.

<u>Note</u>: If one of the X_i's is empty, then $\prod_{i \in I} X_i = \emptyset$

$\prod X_i =$ choice functions on I. (?)

14.10.21 Th

<u>A famiy of sets</u> (indexed by the set I)

$\mathcal{F}: I \to W$ (for some W)

$i \mapsto \mathcal{F}(i) = X_i$

<u>remark</u>

$(x, y) = \{\{x\}, \{x, y\}\}$

$(x, x) = \{\{x\}\}$

$\{X_i : i \in I\}$ is a famiy of set.

$\bigcup_{i \in I} X_i = \bigcup \{X_i : i \in I\}$

A famiy of sets $\{X_i : i \in I\}$ given by $\mathcal{F}: I \to W$.

A choice function for this famiy $f: I \to \bigcup W$

$f(i) = x_i \in X_i = \mathcal{F}(i)$

$\prod_{i \in I} X_i = \{f : f$ is a choice funct. of the famiy $\{X_i : i \in I\}\}$

$\mathbb{Q}^{[2]} = I =$ set of 2 element-subsets of $\mathbb{Q}$

$F: \mathbb{Q}^{[2]} \to P(\mathbb{R})$ famiy of rational intervals of $\mathbb{R}$

$\{r, s\} \mapsto (r, s)$ if $r < s$

$f: \mathbb{Q}^{[2]} \to \bigcup \mathcal{P}(\mathbb{R}) = \mathbb{R}$

$\{r,s\} \longmapsto f(\{r,s\}) = \frac{r+s}{2} \in (r,s)$

$I = \mathcal{P}(\mathbb{N})$

$F: \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\} \to \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$

$x \longmapsto x$

$\{X_x : x \text{ is a subset of } \mathbb{N}\}$

Is there a choice function for this family? YES.
Pick the minimal elt. of every set.

$I = \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\}$ & $W = \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\}$

$F: \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\} \to \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\}$

$x \longmapsto x$

can you think of a choice function for F? (HW)

Axiom of Choice : Every family of sets has a choice function.

Equivalence Relation on a set X.

$R \subseteq X \times X$ satisfying

- $(x,x) \in R \quad \forall x \in X$ (ref.)
- $(x,y) \in R \to (y,x) \in R$ (sym.)
- $(x,y) \in R$ & $(y,z) \in R \to (x,z) \in R$ (tran.)

Equivalence Classes

$x \in X$, $\bar{x} = \{y : (y,x) \in R\}$ where R is an equivalence relation and $\bar{x}$ is an equivalence class of x.

Equivalence relation on $X \leftrightarrow$ Partition of X.

19.10.21 T

$I = \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\}$

$$F : \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\} \to \mathcal{P}(\mathbb{R})$$
$$X \longmapsto X$$

(HW1)

$$f : \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\} \to \mathbb{R}$$
$$X \longmapsto f(X) \in X$$

What if you pick $\mathbb{N}$ or $\mathbb{Q}$ instead of $\mathbb{R}$? Is this possible?

$I = \mathcal{P}(\mathbb{Q}) \setminus \{\emptyset\}$

$$F : I \to \mathcal{P}(\mathbb{Q})$$
$$X \longmapsto X$$

(HW2)

Is there a choice function for this family of sets?

<u>Relations, Functions</u>

Partition of a set X : family of non-empty subsets of X s.t.

i) $\bigcup \{X_i : i \in I\} = X$

ii) $X_i \cap X_j = \emptyset$ if $i \neq j$

<u>Thm</u>: If R is an equivalence relation on X then

i) $P = \{\bar{x} : x \in X\}$ is a partition of X.

ii) If P is a partition on X, then $R = \{(x,y) : x, y \in p$ for some $p \in P\}$ is an equivalence relation.

iii) $X/R = P$ (HW3 : Prove!)

$(X/R = \{\bar{x} : x \in X\}$

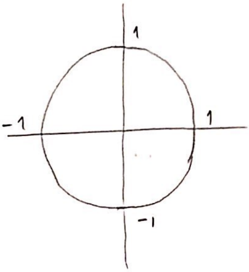
- $X = \mathbb{R}$, $(x,y) \in R \leftrightarrow x^2 = y^2$

$\bar{x} = \{y : (x,y) \in R\} = \{y : x^2 = y^2\} = \{x, -x\}$

$|y \cap \bar{x}| = 1$ for every $x \in X$.

- $X = \mathbb{R}\times\mathbb{R}$, $((x,y),(z,t)) \in R$ if $x^2+y^2 = z^2+t^2$

$(1,0) \sim (0,1) \sim \left(\frac{3}{5}, \frac{4}{5}\right) \sim \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$

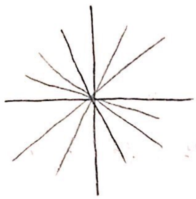


$\overline{(1,1)} = \{(x,y) : x^2+y^2 = 1^2+1^2 = 2\}$

$= \{(x,y) : x^2+y^2 = 2\}$

- $X = \mathbb{R}\times\mathbb{R} \setminus \{(0,0)\}$

$((x,y),(z,t)) \in R \longleftrightarrow z = \alpha x,\ t = \alpha y,\ \alpha \neq 0$



projector line

$\overline{(x,y)} = \{$ pts. on the line passing through the origin & (x,y), except $\{(0,0)\}\ \}$

A Few Axioms of Set Theory

1) Axiom of Extensionality

$x = y$ iff $\forall z \quad z \in x \longleftrightarrow z \in y$

2) Empty set Axiom : $\emptyset$ exists.

3) Axiom of Pairs (Pair set axiom) : If x and y sets then $\{x,y\}$ is a set.

$x = \emptyset \quad y = \emptyset^0 \qquad \{\emptyset,\emptyset\} = \{\emptyset\}^{\to 1}$ is a set.

$x = \emptyset \quad y = \{\emptyset\} \qquad$ then $\{\emptyset, \{\emptyset\}\}^{\to 2}$ is a set.

$\{\{\emptyset\}, \{\{\emptyset\}\}\}$ be careful with parenthesis.

$n = \{0, 1, \dots, n-1\}$

4) Axiom of Unions : If X is a set then $\bigcup X$ is a set.

Thm: If a & b sets then $a \cup b$ is also a set.

Proof: By pair set axiom $\{a, b\}$ is a set by union axiom $\bigcup\{a, b\} = a \cup b$ is a set.

5) Subset Axiom: Suppose A is a set and $\phi(x)$ is a statement in the language of set theory.

$\{x \in A : \phi(x)\}$ is a set.

Prop.: If a & b are sets, so is $a \setminus b$.

$a \setminus b = \{x \in a : x \notin b\}$

Prop.: If X is a set then $\bigcap X$ is also a set.

Proof: $\bigcup X$ is a set. $\bigcap X = \{a \in \bigcup X : a \in y \text{ for } \forall y \in X\}$

There is no set of all sets.

$V = \{\text{set of all sets}\}$

$D = \{x \in V : x \notin x\}$, $D \in D \leftrightarrow D \notin D$, $P \leftrightarrow \neg P$ ※ $\}$ V does not exist.

6) Axiom of Foundation: If X is a non-empty set then X has an $\in$-minimal elt. If X is a non-empty set then $\exists y \in X$ s.t. $y \cap X = \emptyset$

Order Relation

irreflexive, transitive $\}$ Strict order

anti-sym: $a \leq b \land b \leq a \Rightarrow a = b$

transitive: $a \leq b \land b \leq c \Rightarrow a \leq c$

$\Big] \leqslant$

$x = \{x\}$: nothing like this happens under the rule of axiom of foundation.

$X = \{x, y, z\}$

$X = \{\{x, y, z\}, y, z\}$

$X = \{\{\{x, y, z\}, y, z\}, y, z\}$

7) Power Set Axiom: If X is a set, then $\mathcal{P}(X)$ is also a set.

21.10.21 Th

ORDER: A strict partial order on a set X is a binary relation which is irreflexive, anti-symmetric & transitive.

- $(a, a) \notin R \quad \forall a \in X$
- $(a, b) \in R$ & $(b, a) \in R \rightarrow a = b \quad \forall a, b \in X$
- $(a, b), (b, c) \in R \rightarrow (a, c) \in R$

A non-strict partial order on X is a subset $R \subseteq X \times X$

- $(a, a) \in R \quad \forall a \in X$
- $(a, b) \in R$ & $(b, a) \in R \rightarrow a = b \quad \forall a, b \in X$
- $(a, b), (b, c) \in R \rightarrow (a, c) \in R$

Total Order is a partial order which satisfies the tricothomy: $\forall x, y$, either $(x, y) \in R$ or $(y, x) \in R$ or $x = y$.

Ex: 1) Take any set A. $\mathcal{P}(A)$ we define a partial order by $x, y \in \mathcal{P}(A)$, $(x, y) \in R \Leftrightarrow x \subseteq y$.

$x = \{1, 2\} \quad y = \{2, 3\} \quad x \nsubseteq y, y \nsubseteq x$ & $y \neq x$

NOT a TOTAL ORDER.

2) $X = \mathbb{N} \setminus \{0\}$, $x < y \Leftrightarrow x | y$. Take $x = 2$ & $y = 3$

NOT a TOTAL ORDER.

Remark: If R is a strict order on X then $S = R \cup \{(x,x) : x \in X\}$ then S is a non-strict order.

If S is a non-strict order on X then $R = \{(xy) \in S \mid x \neq y\}$ is a strict order.

Least elt. of X : $\forall x \in X$, $y \leq x$, then y is a least elt. of X.

Minimal elt. of X : $\forall x \in X$, if y is a minimal elt, then $x \leq y \rightarrow x = y$.

Ex: an ordered set having a minimal elt. but no least elt.

Let X : $\mathcal{P}(\{1,2,3\}) \setminus \{\emptyset\}$, order: subset relation ($\subseteq$)

Then $\{1\}$, $\{2\}$ & $\{3\}$ are minimal elts.

This set has no least elt. If X is total ordered, then the minimal & least elts coincide if they exist.

$\mathbb{N} \setminus \{0,1\}$ with division order.

↳ least elt : DNE

↳ minimals : prime #s.

Note: The least elt is unique. If x_1 & x_2 are least elts, by def, $x_1 \leq x_2$ & $x_2 \leq x_1$ $\Rightarrow$ $x_1 = x_2$

Lexicographical Order If $(X,<)$ & $(Y,<)$ are ordered sets then one can define an order on $X \times Y$ as

$(x_1, y_1) < (x_2, y_2)$ if; either $x_1 < x_2$

or $x_1 = x_2$ & $y_1 < y_2$

$\mathbb{N} \times \mathbb{N}$ can be ordered lexicographically.

maximal: if y is maximal $\rightarrow$ $\forall x$ $x \geq y \rightarrow x = y$

maximum: if y is maximum $\rightarrow$ $\forall x$ $y \geq x$

$(X, <_X)$ & $(Y, <_Y)$, there is an order isomorphism between these orders if

$f: X \to Y$ is a bijection 1-1 & onto.

$a <_X b \longleftrightarrow f(a) <_Y f(b)$

Exercise: Try to find an isomorphism b/w $\mathbb{Q}$ & $\mathbb{N}$.

(2 orders & 1 bijection) ?

26.10.21 T

The Natural Numbers

$0 = \emptyset$

$1 = \{0\} = \{\emptyset\}$

$2 = \{0,1\} = \{\emptyset, \{\emptyset\}\}$

$\vdots$

$n+1 = n \cup \{n\} = \{0, 1, \dots, n-1, n\}$

$S: x \longmapsto x \cup \{x\}$ (successor operation)

Notation: If X is a set, then $x^+ = x \cup \{x\}$.

Definition: A successor set is a set Ω such that
(i) $\emptyset \in \Omega$
(ii) If $x \in \Omega$ then $x^+ \in \Omega$.

Axiom of Infinity: There exist a successor set

Went: $w = \{0, 1, 2, 3, \dots, \}$

Theorem: w exists (is a set) and it is the smaller successor set.

Proof:
By axiom of infinity, there exists a successor set, say Ω.

$A = \{Y \subseteq \Omega : Y \text{ is a successor set}\} \subseteq \mathcal{P}(\Omega)$, so

A is a set (by power set axiom & subset axiom).

$A \neq \emptyset$, $\cap A$ is a set. Is $\emptyset \in \cap A$? YES.

If $x \in \cap A$, is $x^+ \in \cap A$? YES.

1) Claim that $\cap A = w$ is in every successor set.

Let S be a successor set. WTS: $w \subseteq S$.

Claim: $S \cap \Omega$ is a successor set.

YES. $\emptyset \in S$ $\emptyset \in \Omega$ $\rightarrow$ $\emptyset \in S \cap \Omega$

$$\left.\begin{array}{l} \text{If } x \in S \quad x^+ = x \cup \{x\} \in S. \\ x \in \Omega \quad x^+ = x \cup \{x\} \in \Omega \end{array}\right\} x^+ \in S \cap \Omega$$

$x^+ = x \rightarrow x^+ = x \cup \{x\} = x \rightarrow x \in x$ ※

w is the only successor set which is included in every successor set. *

Proof: If there is w' with property * then $w \subseteq w'$, $w' \subseteq w$ so $w = w'$.

Theorem: (Proof by induction) Suppose $P(x)$ is a property of natural numbers. s.t. $P(0)$ holds and for all n if $P(n)$ holds then $P(n+1)$ holds. Then P holds for every natural number n.

Natural numbers $= w = \{0, 1, 2, 3, \ldots\}$

$0 = \emptyset$ $\quad n+1 = \{0, 1, \ldots, n\}$

$1 = \{\emptyset\}$

$A = \{x : P(x)$ does not hold$\}$ if $A = \emptyset$

Suppose $A \neq \emptyset$ by well-ordering of $w = \mathbb{N}$. A has a least element m, $m \neq 0$.

$m = n+1$ for some $n \in \mathbb{N}$

Is $n \in A$? No. Otherwise n would have been minimal.

$n \notin A$ so $P(n)$ holds so $P(n+1) = P(m)$ holds ※

So $A=\emptyset$, $P(x)$ holds for every $x \in \mathbb{N}$.

Proof: $A = \{n \in \omega : P(n) \text{ holds}\}$ $\quad 0 \in A$

$x \in A \to x^+ \in A$.

A is a successor set.

$\omega \subseteq A$ and $A \subseteq \omega \Rightarrow \omega = A$

Defn: If $m, n \in \omega$, then we say that $m \leq n$ if $m \in n$ or $m = n$.

Claim 1 $\leq$ is transitive. If $m, n, k \in \omega$ $m \leq n$ and $n \leq k$ $\to m \leq k$. By induction on k. If $k = 0 = \emptyset$ then the statement is vacious.

Suppose the statement holds for k: show for $k+1 = k \cup \{k\}$.

$n \leq k$ and $m \leq n \to m \leq k$ } we know

$n \leq k+1$ and $m \leq k+1 \to m \leq k+1$ } WTS.

If $n = k+1$ $\quad m \leq k+1 \Rightarrow m \leq k+1$

If $n \in k+1 = k \cup \{k\}$

$n \in k$ and $m = n$ or $m \in n \to m \in k$

$n \in \{k\}$ then $n = k$ and $m \in n \to m \leq k$

Try to show $(\leq, \omega)$ is a total order.

2.11.21 T

Remember

A successor set S

- $\emptyset \in S$
- if $x \in S \to x \cup \{x\} = x^+ \in S$

Axiom of Infinity

A successor set exists:

$$\omega = \bigcap_{S \text{ successor}} S$$

$\phi = 0, \quad \phi \cup \{\phi\} = 0^+ = 1$

$m, n \in \omega$, $m \leq n \Leftrightarrow m \in n$ or $m = n$.

HW Problems for all $m, n, k \in \mathbb{N}$

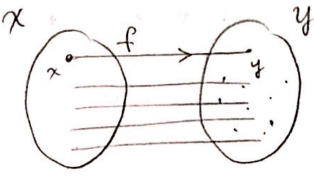
1. Show that $\leq$ a partial order on ω. (transitivity by induction.
2. $m < n^+ \rightarrow m \leq n$
3. $m \leq n$ iff $m \subseteq n$
4. $\leq$ is a total order on ω. (For all $m, n \in \omega$, $m \leq n$ or $n \leq m$.
5. Every element of ω is either 0 or the successor of a unique elt of ω.
6. Principle of strong induction: If $P(0)$ holds and $[P(n)$ holds for every $n \in m$ then $P(m)$ holds$]$ then $P(k)$ holds for every k in ω.
7. ω is well-ordered.

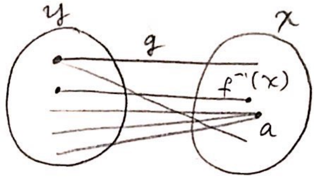
Defn: X and Y are sets. ① $|X| = |Y|$ means there is a bijection from the set X to the set Y.
② $|X| \leq |Y|$ means there is an injection from X to Y.
③ $|X| < |Y|$ means $|X| \leq |Y|$ and $|X| \neq |Y|$ → no bijection b/w X & Y

- Any two elts are comparable. [we need AC to prove]
- There exists an injection from X to Y iff there exists a surjection from Y to X. (Need a.c)

Theorem: If there is an injection from X to Y then there is a surjection from Y to X.

Proof: Let $f: X \rightarrow Y$ be an injection, we want to find $g: Y \rightarrow X$ which is a surjection.





Let $a \in \mathcal{X}$

$$g(y) = \begin{cases} x & \text{if } f(x) = y \text{, such an } x \text{ exists} \\ a & \text{if such an } x \text{ does not exists} \end{cases}$$

Show that g is a function if

$g(y_1) \neq g(y_2) \Rightarrow y_1 \neq y_2$

$x_1 \neq x_2$

If $\exists\, x_1, x_2$ s.t. $f(x_1) = y_1$ & $f(x_2) = y_2$, then since f is an injection, $y_1 = y_2 \Rightarrow g(y_1) = g(y_2)$

$$\underset{x_1}{\overset{\shortparallel}{g(y_1)}} = \underset{x_2}{\overset{\shortparallel}{g(y_2)}}$$

Schröder – Bernstein Theorem

If $|\mathcal{X}| \leq |\mathcal{Y}|$ and $|\mathcal{Y}| \leq |\mathcal{X}|$ then $|\mathcal{X}| = |\mathcal{Y}|$.

Ex: $\mathbb{N} \to \mathbb{Q}^{\geq 0}$ & $\mathbb{Q}^{\geq 0} \to \mathbb{N}$

$n \longmapsto n$ $\qquad$ $a/b \longmapsto 2^a 3^b$

Proof: Let $f: \mathcal{X} \to \mathcal{Y}$ and $g: \mathcal{Y} \to \mathcal{X}$ be injections.

(inj : $f(x_1) = f(x_2) \to x_1 = x_2$ OR $x_1 \neq x_2 \to f(x_1) \neq f(x_2)$)

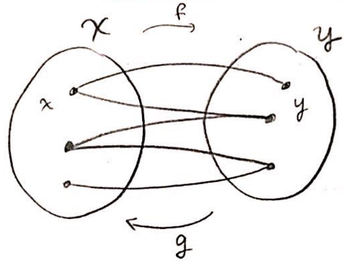
WLOG assume $\mathcal{X} \cap \mathcal{Y} = \emptyset$.

Set $\mathcal{X}' = \mathcal{X} \times \{0\}$ $\to$ $\mathcal{X}' \cap \mathcal{Y}' = \emptyset$

$\mathcal{Y}' = \mathcal{Y} \times \{1\}$

$y \in \mathcal{Y}$ is called the parent of x if $g(y) = x$.

$x \in \mathcal{X}$ " " " " y " $f(x) = y$.



Since both f and g are injective each element has at most 1 parent.

An ancestral chain for $z \in X \cup Y$ is a tuple $(z_0, z_1, z_2, \ldots)$ where $z_0 = z$ & z_{i+1} is the parent of z_i. If length of such chain is n then $d(z) = n$. There are two possibilities for $z \in X \cup Y$: either there exists arbitrarily long ancestral chains, or not. (There is a unique largest ancestral chain.)

$X_e = \{ x \in X : d(x) \text{ is even} \}$

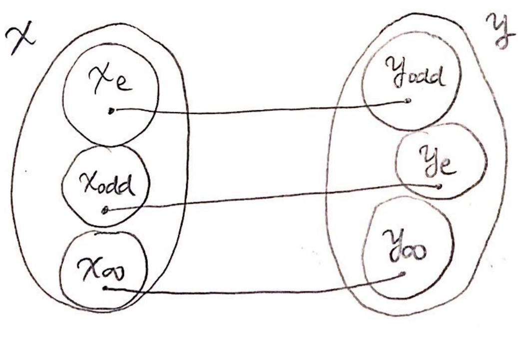
X_{odd}: $\{ x \in X : d(x) \text{ is odd} \}$

$X_\infty = \{ x \in X : d(x) \text{ is unbounded} \}$

$Y_e = \{ y \in Y : d(y) \text{ is even} \}$

$Y_{odd} = \{ y \in Y : d(y) \text{ is odd} \}$

$Y_\infty = \{ y \in Y : d(y) \text{ is unbounded} \}$



- Every element of $\mathcal{Y}_{odd}$ has a parent.
- If $x \in \mathcal{X}_e \to f(x) \in \mathcal{Y}_{odd}$
- If x has infinite depth, then $f(x)$ has infinite depth (d).
- f maps $\mathcal{X}_e \to \mathcal{Y}_{odd}$ bijectively.

  $\mathcal{X}_\infty \to \mathcal{Y}_\infty$

  $\mathcal{X}_{odd} \to \mathcal{Y}_e$ – not necessarily a surjection since $\mathcal{Y}_e$ contains elts with no parents.

$$h(x) = \begin{cases} f(x) & \text{if } x \in \mathcal{X}_e \cup \mathcal{X}_\infty \\ g^{-1}(x) & \text{if } x \in \mathcal{X}_{odd} \end{cases}$$

↳ exists since g is a bijection b/w $\mathcal{Y}_{even}$ & $\mathcal{X}_{odd}$ (injectivity given, surjective since $\forall x \in \mathcal{X}_{odd}$ there exists an ancestor of x.)

$h(x)$ is a bijection. □

Cantor's Theorem: There is no bijection b/w a set and its powerset.

Remark: Clearly there is an injection from X to $\mathcal{P}(X)$.

$$X \to \mathcal{P}(X)$$
$$x \mapsto \{x\}$$

This implies;
$|X| \leq |\mathcal{P}(X)|$.

Proof: Assume for contradiction, that there is a bijection $f: X \to \mathcal{P}(X)$.

$\mathbb{N} \to \mathcal{P}(\mathbb{N})$. set $A = \{x \in X : x \notin f(x)\}$

$$1 \longmapsto \{1,2,3\} \qquad 2 \in A$$
$$2 \longmapsto \{3,4\} \qquad 1 \notin A$$

$A \subseteq X$, $A \in \mathcal{P}(X)$.

f is onto by assumption. So $\exists z \in X$ s.t. $f(z) = A$.

Now, where is z?

If $z \in A$, then $z \notin A = f(z)$ ※

If $z \notin A$, then $z \in A$.

$|X| < |\mathcal{P}(X)|$. □

4.11.21 Th

<u>Defn</u>: A set is called finite if it has a bijection with an element of ω. $n = \{0, 1, \dots, n-1\}$

<u>Theorem</u>: If there is a bijection between n & m then $n = m$.

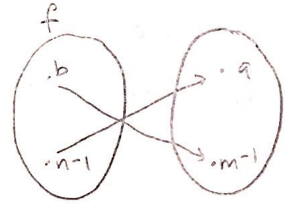
<u>Proof</u>: By induction $n = 0 = \emptyset$ then we are done. Assume true for $n-1$, show for n.

Assume $n = \{0, 1, 2, \dots, n-1\} \longleftrightarrow \{0, 1, 2, \dots, m-1\}$ there is a bijection between n & m.

* If $f(n-1) = m-1$ then $f|_{\{0,1,\dots,n-2\}}$ is a bijection b/w $\{0, 1, 2, \dots, n-1\}$ and $\{0, 1, 2, \dots, m-1\}$. Then by induction hypothesis $n-1 = m-1 \Rightarrow n = m$.

* If $f(n-1) \neq m-1$, $f(n-1) = a$, $f(b) = m-1$.

$$f'(x) = \begin{cases} f(x) & \text{if } x \neq b,\ x \neq n-1 \\ a & \text{if } x = b \\ m-1 & \text{if } x = n-1 \end{cases}$$



$f'(m-1) = n-1$. So by above, $n = m$.

$(\mathbb{N}, +) \rightsquigarrow (\mathbb{Z}, +)$

$\mathbb{N} \times \mathbb{N} = \{(a,b) : a,b \in \mathbb{N}\}$

$(a,b) \simeq (c,d)$ iff $a+d = b+c$

① reflexive : $(a,b) \simeq (a,b)$

② symmetric : If $(a,b) \sim (c,d)$ then $(c,d) \sim (a,b)$

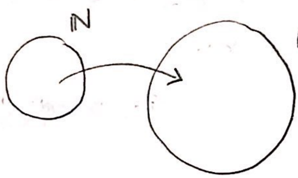
③ transitive : If $(a,b) \sim (c,d)$ & $(c,d) \sim (e,f)$ then $(a,b) \sim (e,f)$

Define $(a,b) + (c,d) = (a+c, b+d)$

$\mathbb{N} \times \mathbb{N} / \sim \; = \{\overline{(a,b)} : a,b \in \mathbb{N}\}$

$(a,b) \sim (a',b')$ & $(c,d) \sim (c',d')$

$(a,b) + (c,d) \sim (a',b') + (c',d')$ ✓ well-defined



$\mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N} / \sim$

$n \longmapsto (n,0)$

$(a,b) \sim (c,0) \rightarrow a-b = c$ if $a-b \geq 0$

$b-a$ if $a-b < 0$

On $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ define an eq. rel. as follows.

$(a,b) \sim (c,d) \Leftrightarrow ad = bc$

$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$ This is well-defined.

$\overline{(1,1)}$ is the identity. $(a,a) \sim (1,1)$ $\forall a \neq 0$

$\overline{(a,b)}^{-1} = \overline{(b,a)}$

$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$ This is well-defined.

$(\mathbb{R} \to \mathbb{N} \to \mathbb{Z} \to \mathbb{Q})$

$\mathbb{Z} \to \mathbb{Q}$

$z \longmapsto (z,1)$

9.11.21 T

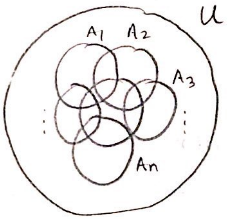
Principle of Inclusion Exclusion

Let A_i be a family of subsets of a finite set $\mathcal{U}$. $(A_i : i \in I)$ with $|I| = n$. for any nonempty set $J \subseteq I$.

Let $A_J = \bigcap_{i \in I} A_i$ and let $A_\emptyset = \mathcal{U}$.

Then the number of elts of $\mathcal{U}$ which lie in none of the A_i's is equal to

$$\sum_{J \subseteq I} (-1)^J \cdot |A_j| \qquad |A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n| = \sum_{J \subseteq I} (-1)^J |A_j|$$



$\{1,2,3\} = I$

$A_\emptyset = \mathcal{U}$

$A_{\{1\}} = (-1)^1 \cdot |A_1|$ $\qquad$ $A_{\{1,2\}} = (-1)^2 \cdot |A_1 \cap A_2|$

$A_{\{2\}} = (-1)^1 \cdot |A_2|$ $\qquad$ $A_{\{1,3\}} = (-1)^2 \cdot |A_1 \cap A_3|$

$A_{\{3\}} = (-1)^1 \cdot |A_3|$ $\qquad$ $A_{\{2,3\}} = (-1)^2 \cdot |A_2 \cap A_3|$

$A_{\{1,2,3\}} = (-1)^3 \cdot |A_1 \cap A_2 \cap A_3|$

$\star\ |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$

Let $x \in$ some of the A_i's.

$K = \{i : x \in A_i\} \neq \emptyset$.

$$\sum_{J \subseteq K} (-1)^{|J|} = \sum_{|J|=0}^{|K|} (-1)^{|J|} \binom{|K|}{|J|} = (1-1)^{|K|} = 0$$

X is finite if X has a bijection with $n \in \omega$ for some n.

X, Y finite sets. $|X| = m$ & $|Y| = n$. # of functions from X to Y is n^m. # of 1-1 fncts. from X to Y $n \cdot (n-1) \dots (n-m+1)$.
(If $m > n$, $\exists$ no 1-1 fnct.)

# of onto fncts. from X to Y. ! later !

$|A_i|$ = # of fnc. which do not hit $a_i = (n-1)^m$

# of surjective functions from $\mathcal{X}$ to $\mathcal{Y}$. is

$$\sum_{j=0}^{n} (-1)^j \cdot \binom{n}{j} \cdot (n-j)^m$$

Countable Sets

A set is countable if it has a bijection with $\mathbb{N}$. A set is at most countable if it is countable or finite.

Thm: A set $\mathcal{X}$ is at most countable if there is an injection from $\mathcal{X}$ to $\mathbb{N}$, $f: \mathcal{X} \to \mathbb{N}$.

Proof: Let $A = f(\mathcal{X}) = \{n \in \mathbb{N} : n = f(x) \text{ for some } x \in \mathcal{X}\}$

Since $A \subseteq \mathbb{N}$ A has a least elt, say $f(x_0)$. Define g as follows:

$$g(x_0) = 0$$

$$\underbrace{f(\mathcal{X} \setminus \{x_0\})} \subseteq \mathbb{N}$$

has a least elt $g(x_1)$, $g(x_1) = 1$.

Define $g(x)$ to be n, if $f(x)$ is the n^{th} elt. in the image of f. If this procedure stop at a finite step, there is a bijection of $\mathcal{X}$ with $\{0, 1, 2, \dots, n-1\} = n$. Otherwise, it does not stop. So our every $n \in \mathbb{N}$ there is $x \in \mathcal{X}$ s.t. $g(n) = x$.

$$|\mathbb{N}| \leq |\mathcal{X}| \ \& \ |\mathcal{X}| \leq |\mathbb{N}| \Rightarrow |\mathcal{X}| = |\mathbb{N}|.$$

Thm: a) At most countable union of at most countable sets is at most countable.

b) Cartesion product of two at most countable sets is at most countable.

$f_0 : A_{i_0} \to \mathbb{N}$

$f_1 : A_{i_1} \to \mathbb{N}$

$f_2 : A_{i_2} \to \mathbb{N}$

$\vdots$

$|I|$ = index set, suppose $|I|$ is at most countable, then $|I| = n$. or

$$g : \mathbb{N} \to I$$
$$n \mapsto i_n$$

Is $\mathbb{N} \times \mathbb{N}$ countable?

$$\left.\begin{array}{l} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ (i,j) \longmapsto [(2i+1).2^j] - 1. \end{array}\right\} \text{bijection.}$$

$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ & $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$

$(i,j) \longmapsto 2^i.3^j$ $\quad$ $n \longmapsto (n,0)$

injection $\quad$ injection

$\Downarrow \longrightarrow$ Schröder - Bernstein !

$\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$

$\cup A_i \to \mathbb{N} \times \mathbb{N}$ find an injection !

16.11.21 T

$\mathbb{Q} \times \mathbb{Q}$ is countable.

$\mathbb{Q} \to \mathbb{N}$ $\quad$ one-to-one

$(-1)^i . \frac{a}{b} \longmapsto 2^i.3^a.5^b$

$\mathbb{N} \to \mathbb{Q}$ $\quad$ one-to-one

$a \longmapsto a$

Schröder - Bernstein thm. says there is a bijection b/w $\mathbb{N}$ & $\mathbb{Q}$

$\mathbb{Q} \times \mathbb{Q} \longleftrightarrow \mathbb{N} \times \mathbb{N} \longleftrightarrow \mathbb{N}$ $\quad$ if f is a bijection b/w $\mathbb{N}$ & $\mathbb{Q}$.

$(a,b) \longmapsto (f(a), f(b))$

I: index set

for each $i \in I$ let X_i be a set.

$\{X_i : i \in I\}$ is a family of sets indexed by the set I.

$\cup \{X_i : i \in I\} = \{x : x \in X_i \text{ for some } i \in I\}$

$F : I \to \bigcup \{X_i : i \in I\}$

$i \longmapsto x_i \quad : x_i \in X_i$

$\left[\begin{matrix} AC \\ WOP \\ ZL \end{matrix}\right]$ equiv.

Axiom of Choice : Every family of sets has a choice function.

well ordered Principle : Totally ordered & every nonempty subset has a least elt.

Zorn's Lemma:

ORDINALS

✓ partially ordered reflexive, transitive & anti-symmetric
✓ totally ordered - any two element can be compared
✓ well ordered - any nonempty subset has a least elt.

$\mathbb{Z}$ is not well ordered! (least elt?)

if $(X, \leq)$ is a well order then any subset of X is also well ordered by $\leq$.

$\mathcal{P}(\mathbb{N})$ not well orderd since it is not totally ordered.

Theorem: Let $(X, \leq)$ be a well ordered set. Suppose that Y is a subset of X such that for all $x \in X$, if (it holds that) $y \in Y$ for all $y < x$, then $x \in Y$.

I claim that $X = Y$.

Proof: Suppose $X \setminus Y \neq \emptyset$. Since X is well-ordered $X \setminus Y$ has a least elt. x; then for every y if $y < x$ then $y \in X$ then by hypothesis $x \in Y$ $\times$. so $X = Y$.

& let a be the least elt. of X. I claim that $a \in Y$.

The Principle of Induction

Let $(X,<)$ be a well-ordered set. Let P be a property which may hold for elements of X. Suppose that for every $x \in X$ "if every $y<x$ has the property P then x has the property P." then every elt of X has the property P.

"Every well ordered set is $\left\{\begin{matrix}\text{order}\\ \text{isomorphic}\end{matrix}\right\}$ to a unique ordinal"

<u>Defn</u>: An ordinal is a well ordered set. $(X,<)$ with the property that $X_a = \{y \in X : y<a\} = a$ for all $a \in X$. In other words each ordinal consists of ordinals preceeding itself.

<u>Ex</u>: $\emptyset$ is an ordinal.

$\{\emptyset\}$ " "

$\{\emptyset, \{\emptyset\}\}$ " " ".

<u>theorem</u>: If X is an ordinal then $X \cup \{X\}$ is an ordinal.

<u>Theorem</u>: If A is a set of ordinals then $\cup A$ is ordinal.

18.11.21 Th

<u>Defn</u>: An ordinal is a well-ordered set $(X,<)$ such that $X_a = a$ for every $a \in X$.

$X_a = \{y \in X : y<a\}$

$\emptyset$ is an ordinal.

$X = \{\emptyset\}$ is an ordinal. $X_\emptyset = \{y \in \{\emptyset\} : y < \emptyset\}$

Theorem:

a) If X is an ordinal then $X \cup \{X\}$ is also an ordinal.

b) The union of a set of ordinals is an ordinal.

Proof: $a = X \cup \{X\}$

$a_y = X_y = y$ if $y \in X$

If $y \in X$ then $y = X_y = a_y$

All the elements of X are smaller then X

$a_X = X$ this means every elt. of a satisfies this property $a_y = y$ so $X \cup \{X\}$ is an ordinal.

Lemma: If X is well-ordered $Y \subseteq X$ and $f: X \to Y$ is an isomorphism

$$a < b \Rightarrow f(a) < f(b)$$

then $f(x) \geq x$ for all $x \in X$.

Proof: $E = \{x \in X : f(x) < x\}$

If E is nonempty, then E has a least elt. say x_0.

$$f(x_0) < x_0$$

$$f(\underbrace{f(x_0)}_{y}) < \underbrace{f(x_0)}_{y} \quad (\text{i.e } f(y) \in E)$$

But $f(y) < y = f(x_0) < x_0$ i.e $f(y) < x_0$

$\times$ since x_0 was a least elt.

Lemma: There is at most one isomorphism b/w two well-ordered sets. $(X, <)$, $(Y, <)$

$f: X \to Y$, $g: X \to Y$ are two isomorphisms b/w X & Y. (assumption.)

$g^{-1} \circ f(X) = X$ $\qquad\qquad$ $f^{-1} \circ g(x) = X$

$x \leq g^{-1}(f(x))$ $\qquad\qquad$ $x \leq f^{-1}(g(x))$

$g(x) \leq f(x)$ $\qquad\qquad$ $f(x) \leq g(x)$

$\therefore f(x) = g(x)$

Lemma: There is no isomorphism from a well-ordered set $(X, <)$ to an initial segment of it.

$a \in X \Rightarrow X_a = \{y \in X : y < a\}$

Proof: if $f: X \to X_a$ is an isomorphism

$f(a) \in X_a \Rightarrow f(a) < a$ $\times$ contradiction to lemma 1

Lemma 4: Let $(X, <)$ be a well-ordered set

$A = \{X_a : a \in X\}$ be the set of sections of X. $\subseteq \mathcal{P}(X)$

$(A, \subset) \simeq (X, <)$

$X \to A$

$a \mapsto X_a$

Proof: onto ✓ (By defn.)

1-1 if $a \neq b$ then $X_a \neq X_b$

Then wlog, $a < b$ then $a \in X_b$ but $a \notin X_a$, so $X_a \neq X_b$.

Suppose $a < b$ then WTS. $X_a \subseteq X_b$.

Let $y \in X_a \Rightarrow y \in X_b$. So f is an order preserving isomorphism.

23.11.21 T

Lemma 1: If X is well-ordered $Y \subseteq X$ and $f: X \to Y$ is an isomorphism, $(a<b \Rightarrow f(a)<f(b))$ then $f(x) \geq x$ for all $x \in X$.

Lemma 2: There is at most one isomorphism b/w two well-ordered sets. $(X,<)$, $(Y,<)$

Lemma 3: There is no isomorphism from a well-ordered set $(X,<)$ to an initial segment of it.

$$a \in X \Rightarrow X_a = \{y \in X : y<a\}$$

Lemma 4: Let $(X,<)$ be a well-ordered set.
(?)
$A = \{X_a : a \in X\}$ be the set of sections of $X \subseteq \mathcal{P}(X)$.

$$(A, \subset) \cong (X,<) \qquad \begin{aligned} X &\to A \\ a &\mapsto X_a \end{aligned}$$

Ordinal : A well ordered set $(X,<)$ s.t each elt. $a \in X$ is of the form $X_a = \{y \in X : y<a\}$

$\emptyset < \{\emptyset\}$

$X = \{\emptyset, \{\emptyset\}\}$ $\qquad \{\emptyset\} = \{y \in X : y < \{\emptyset\}\} = \{\emptyset\}$

$\emptyset = \{y \in X : y < \emptyset\} = \emptyset$

? Smallest elt. of every ordinal ist $\emptyset$.

Lemma 4: There is no isomorphism from an ordinal to an elt. of an ordinal.

Lemma 5: An element of an ordinal is an ordinal.

Proof of 5: Let X be an ordinal, X_a be an initial segment of X.

$(X_a)_b = \{y \in X_a : y < b\}$
$\|$
X_b
$\|$
b

Observe: $(X_a)_b \subseteq X_b$ ✓

! Check : $X_b \subseteq (X_a)_b$.

! $y \in X_b$, wts : $y \in (X_a)_b$

$y \in \{y \in X : y < b\}$; enough to show $y < a$ ie $y \in X_a$

$y < b$, $b < a$ so $y < a$

Hence, $y \in X_a \to y \in (X_a)_b$.

Lemma 6: If X and Y are ordinals & $Y \subseteq X$ then Y is an initial segment of X.

Proof: Let a = min. elt. of $X \setminus Y \neq \emptyset$

Claim : $X_a = Y$; (i) $X_a \subseteq Y$ & (ii) $Y \subseteq X_a$

$X_a \subseteq Y$: because if any element in X which is less than a is not in Y then it is in $X \setminus Y$ and contradicts with the minimality of a, hence it must be in Y.

$Y \subseteq X_a$: Let $y \in Y \subseteq X$, clearly $y \in X$. We need to show that $y < a$. Since X and Y well ordered, $y = a$ or $y > a$ or $y < a$. We show $y = a$ & $y > a$ are not possible.

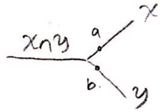
$y = a$ ⨳.

$y > a$ then $a \gg y$ ⨳. Since $a \in X$.

Thm: If X and Y are distinct ordinals, then one is an initial segment of the other.

Proof: $X \cap Y$ is an ordinal which is contained in both X and Y. Assume for a contradiction that

$x \setminus y \neq \emptyset$ & $y \setminus x \neq \emptyset$



If $a = \min x \setminus x \cap y$

$x_a = x \cap y$

$y_b = x \cap y$

$b = y_b = x_a = a \iff a = b$ ※

with both $x \setminus y \neq \emptyset$

& $y \setminus x \neq \emptyset$

So at least one of $x \setminus y$ or $y \setminus x$ is empty.

i.e $x \subseteq y$ or $y \subseteq x$.

! The union of a set of ordinals is an ordinal.

1. Any member of an ordinal is an ordinal.

Since any $a \in x$ $x_a = a$ initial segment which is ord.

2. If X is a set of ordinals then $\bigcup X$ is also a set of ordinals.

! x, y $x < y$ or $x = y$ or $x > y$

25.11.21 Th

If x, y are two ordinals then $x \subset y$ and in particular x is initial segment of y ($x = y_a$ for some $a \in y$, $x \in y$.

$\subset$ Transitive

$\subset$ Irreflexive

$\subset$ On the "class of ordinals" it satisfies the tricothomy.

x, y ordinals $\Rightarrow x = y$ or $x \subset y$ or $y \subset x$

$\Rightarrow$ Total order.

Is this a well-order?

Theorem: If $\mathcal{X}$ is a set of ordinals then $\cup \mathcal{X}$ is also an ordinal.

Proof: $A = \cup \mathcal{X}$ elements of ordinals are ordinals themselves so A is a set of ordinals.

Claim: $\subset$ defines a total order on A.

It is also a well order.

Let $B \neq \emptyset \subseteq A$. Let $b \in B$. If b is the least element of B then we are done. If not, then since b is itself an ordinal, it is well ordered. Then $\{c \in B : c < b\} \subseteq b$. has a least elt which is the least elt. of B.

$$z < x < b \qquad z \in B, x \in b, x \subseteq b$$

Finally we need to show that if $a \in A = \cup \mathcal{X}$ then

WTS:

$a = A_a \qquad a = x_a$ for some $x \in \mathcal{X}$.

$x_a \subseteq A_a$ obvious.

$z \in A_a \subseteq x_a$, z is an ordinal which is less then a. a is less then x. so z is in x (ordinal), so z is in $x_a \Rightarrow A_a \subseteq x_a$

$\Rightarrow x_a = A_a$ we are done.

Theorem: Any well ordered set is isomorphic to a unique ordinal.

Proof: By transfinite induction.

Claim: $(\mathcal{X}, <)$ well ordered set for all $a \in \mathcal{X}$ wherever x_a is isomorphic to an ordinal then a is isomorphic to an ordinal.

Proving the claim shows that X is isomorphic to an ordinal.

30.11.21 T

<u>Ordinal</u>: $(X,<)$ well ordered, $X_a = a$ for every $a \in X$.

<u>Remarks</u>

1) $\emptyset$ is an ordinal.

2) If x is an ordinal then $x \cup \{x\} = x^+$ is an ordinal.

$$\underbrace{\cdots\cdots\cdots}_{x}\ \overset{x}{\bullet}$$

3) For all $x \in \omega$, x is an ordinal.

$\left.\begin{array}{l} \emptyset \text{ is an ordinal,} \\ x \text{ is an ordinal} \rightarrow x+1 \text{ is an ordinal} \end{array}\right\}$ induction

4) If x, y are ordinals and $x \subseteq y$, then x is an initial segment of y. $x = y_a$ for some $a \in y$.

– 5) For x, y ordinals, either $x \subseteq y$ or $y \subseteq x$.

– 6) If x, y ordinals, then exactly one of the following holds.

$x = y$, $x \subset y$ or $y \subset x$.

7) There is at most one isomorphism between well-ordered sets.

8) If X is a set of ordinals then $\bigcup X$ is also a set of ordinals.

! 9) If x and y are isomorphic ordinals, then $x = y$.

<u>Theorem</u>: If $(X,<)$ is a well-ordered set, then it is isomorphic to a unique ordinal.

<u>Proof</u>: <u>Claim</u>: If $(X,<)$ is a well ordered set such that for each $a \in X$ X_a is isom. to an ordinal then X is isomorphic

to an ordinal, then X is isomorphic to an ordinal."

$P(a) = X_a$ is isomorphic to an ordinal.

(show $P(a)$ holds for all $a \in X$)

<u>Proof of the Claim:</u>

[! If $P(x)$ holds for all $x < y$, then $P(y)$ holds !]

Let $g_a : X_a \to Z(a)$ (ordinal) be an isomorphism. Note that $Z(a)$ and g_a are unique, since X_a and $Z(a)$ well ordered and isomorphism must be unique.

$* \; W = \{Z(a) : a \in X\}$

<u>Claim</u>: W is well-ordered. One can order it by inclusion

$x, y \qquad Z(a) < Z(b)$

$$Z : X \to W \quad \text{is 1-1.}$$
$$a \mapsto Z(a)$$

If X_a and X_b match to the same ordinal, what happens?
Let's say $X_a \subset X_b$.

$$\begin{tikzcd} X_a \arrow[r, bend right, "id"'] \arrow[rr, bend right=60] & \subset X_b \arrow[r, "g_b"] & Z(b) (= Z(a)) \end{tikzcd}$$

Then Z is an order isomorphism between X and W.

$$\begin{tikzcd} X_a \arrow[d, shift left, "g_a"] & \supseteq & X_b \arrow[d, shift right, "g_b"'] \\ Z(a) \arrow[u, shift left] \arrow[rr] & & Z(b) \arrow[u, shift right] \end{tikzcd}$$

W is a set whose members are ordinals and satisfies for every $a \in W$, $Z(a) \in W$

$W_a = a$ for all $a \in W$, since a is an ordinal.

$\to W$ is well ordered.

Thm: Ordinal numbers do not form a set! It is called the class of ordinals. ($\mho$)

WHY?

Remark / Theorem:

For ordinals x, y the following are equivalent:

$$\left.\begin{array}{l} x<y \\ x\subset y \\ x\in y \end{array}\right]$$

write the proofs of some of the implications. (?)

For two ordinals x and y, wlog assume $x \subset y$. But this means $x = y_a$ for some $a \in y$. But all the elements less than a is a. So $x = y_a = a (\in y)$. So $x \in y$. ✓

$x<y$ since y is an ordinal and it consists of elements which are less than itself.

? Try to prove remark 6).

Definition (Types of ordinals)

- smallest ordinal $\emptyset = 0$
- successor ordinal $\lambda = \alpha \cup \{\alpha\} = \alpha^+$
- limit ordinal $\lambda = \bigcup_{\alpha<\lambda} \alpha$

Thm: Any nonzero ordinal is either a successor ordinal or a limit ordinal.

Proof: Take $\lambda \neq 0$ s.t λ is not a successor ordinal.

Claim: λ is a limit ordinal.

$M := \bigcup_{\alpha<\lambda} \alpha$, by prev. thm, M is an ordinal.

Then either $\underset{\subseteq M}{\lambda \leq M}$ or $\underset{\subseteq \lambda.}{M \leq \lambda}$

Suppose $\mu \underset{\in}{<} \lambda$, then μ is the greatest ordinal less than λ. (why?)

(**) "$\mu < \dots < \lambda$" is impossible since μ consists of every elt. less than λ.

Now, $\mu + 1 \neq \lambda$ since λ is not <u>successor</u> ordinal. But it can not be strictly less than λ too (**).

So, $\mu = \lambda$, i.e; λ is a limit ordinal.

! If P is a property of ordinals then to prove that P holds for all ordinals.

1) check $P(\emptyset)$

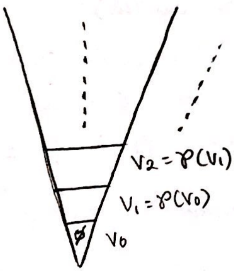
2) Suppose $P(\alpha)$; show $P(\alpha^+)$.

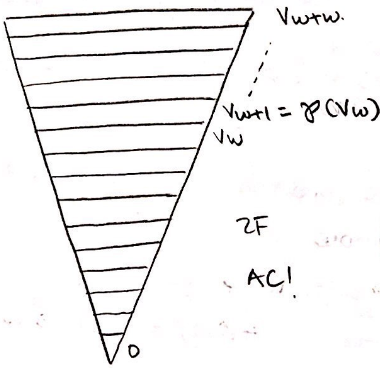
3) If λ is a limit ordinal and [$P(\beta)$ holds for all $\beta < \lambda$, then $P(\lambda)$ holds], then <u>P holds for every ordinal</u>!

• Find a property of ordinals that can be proven this way.

- $V_{\omega+1} = \mathcal{P}(\omega)$

- $V_\omega = \bigcup_{\alpha \in \omega} V_\alpha$ (?)





ZF

AC!

(?)

ORDINAL ARITHMETIC

Defn: Let α, β be ordinals.

Define $+$ on $O \times O$ (?) recursively

- $\alpha + 0 = \alpha$
- $\alpha + S(\beta) = S(\alpha + \beta)$
- $\alpha + \lambda = \bigcup_{\beta < \lambda} \alpha + \beta$ (if λ is a limit ordinal.)

- For all α ordinals; prove:

$0 + \alpha = \alpha$

If $\alpha = 0$, then $0 + 0 = 0$

If $\alpha = S(\beta)$ for some β

If $0 + S(\beta) = S(0+\beta) = S(\beta)$

If true for all $\beta < \lambda$ then true for λ.

$$0 + \lambda = \bigcup_{\beta < \lambda} 0 + \beta = \bigcup_{\beta < \lambda} \beta = \lambda.$$

$1 + \omega = \omega$? (note that ω is a limit ordinal)

$$\bigcup_{\beta \in \omega} (1+\beta) = \omega$$

$\to$ all elements of ω, except 0.

$$\lambda = \overset{=1}{\{\emptyset\}} \cup \underset{2}{\{\emptyset, \{\emptyset\}\}} \cup 3 \cup \dots = \omega$$

Question: Is addition commutative? Either prove or find a counter example.

$$1 + \omega = \omega \not\ni \omega$$
$$\neq$$
$$\omega + 1 = \omega + S(0) = S(\omega) \ni \omega, \text{ where } S(\omega) = \omega \cup \{\omega\}$$

NOT COMMUTATIVE.

Defn: Let α, β be ordinals.

- $\alpha . 0 = 0$
- $\alpha . S(\beta) = \alpha . \beta + \alpha$
- $\alpha . \lambda = \bigcup_{\beta < \alpha} \alpha . \beta$ (if λ is a limit ordinal.)

- For all α ordinals; prove;

- $\alpha . 1 = \alpha$

$\alpha . S(0) = \alpha . 0 + \alpha = 0 + \alpha = \alpha$

- $\alpha . 2 = \alpha . S(1) = \alpha . 1 + \alpha = \alpha + \alpha$.

Question: Is multiplication commutative? YES.

2.12.21 Th

Types of Ordinals

1) $\alpha = 0$ zero ordinal
2) $\alpha = S(\beta)$ successor ordinal.
3) $\alpha = \bigcup_{\beta < \alpha} \beta$ limit ordinal.

- If "$P(0)$ holds" and "$P(\beta)$ holds then $P(\beta^+)$ holds for every β"; and
- If "$P(\beta)$ holds for all $\beta < \lambda$ then $P(\lambda)$ holds";

then P holds for every ordinal. (λ: limit ordinal.)

Two defn's for ordinal arithmetic

Recursively for $\alpha, \beta, \lambda \in$ class of ordinals

- $\alpha + 0 = \alpha$
- $\alpha + \beta^+ = (\alpha + \beta)^+$
- if λ is a limit ordinal, $\alpha + \lambda = \bigcup_{\beta < \lambda} \alpha + \beta$.

Thm: $0+\alpha = \alpha$ for every ordinal α.

Proof: • If $\alpha = 0$ $\quad 0+0=0$

• Assume $P(\beta)$, show: $P(\beta^+)$. $\quad 0+\alpha = 0+\beta^+ = (0+\beta)^+ \xrightarrow{\text{by ind. hyp.}} = \beta^+ = \alpha$ $\quad$ ($P(\beta)$ holds)

• Assume $(0+\beta)=\beta$ for all $\beta<\lambda$, then $0+\lambda = \bigcup_{\beta<\lambda}(0+\beta)$

$$= \bigcup_{\beta<\lambda}\beta = \lambda.$$

• $\alpha.0 = 0$

• $\alpha.\beta^+ = \alpha\beta + \alpha$

• $\alpha.\lambda = \bigcup_{\beta<\lambda}\alpha\beta$ $\quad$ (λ limit ordinal)

Defn: Let $(X, <_X)$ $(Y, <_Y)$ be two well ordered sets, we define the ordered sum of these sets to be $(Z, <_Z)$, where

$$Z = (X \times \{0\}) \cup (Y \times \{1\}) \text{ and}$$

• $(x_1, 0) <_Z (x_2, 0)$ iff $x_1 <_X x_2$

• $(y_1, 1) <_Z (y_2, 1)$ iff $y_1 <_Y y_2$

• $(x, 0) <_Z (y, 1)$ for all $x \in X$ & $y \in Y$.

Show: Z is a well order.

[$\alpha+\beta = \gamma$ if γ is the ordinal isomorphic to the ordered sum of α and β. (?)]

• irreflexive

• transitive

• we can compare any two elts.

} total order

Let S be a subset of Z.

If $S \cap X \times \{0\} = \emptyset$, then $S \subseteq Y \times \{1\}$.

$\{y : y \in S\} \subseteq Y$ (?)

$Z = X \times \{0\} \cup Y \times \{1\}$. is well ordered by the order defined above.

Let $S \subseteq Z$. Two cases:

(1) $S \cap X \times \{0\} = \emptyset \rightarrow S \subseteq Y \times \{1\}$

$S_1 = \{y \in Y : (y, 1) \in S\} \subseteq Y$. (or $Y \times \{1\}$?)

Since Y is well ordered, S_1 has a minimal elt. y_1, then $(y_1, 1)$ is the min. elt. of S_1.

(2) $S \cap X \times \{0\} \neq \emptyset \rightarrow X_1 = \{x \in X : (x, 0) \in S\} \subseteq X$.

X_1 has a minimal elt. say x_1, then $(x_1, 0) \in S$ and it is the minimal elt. of S.

<u>Lexicographic Product</u> $(X, <)$ and $(Y, <)$.

$W = X \times Y$.

$(x_1, y_1) < (x_2, y_2)$ if $y_1 < y_2$

$(x_1, y) < (x_2, y)$ if $x_1 < x_2$

Show that W is well-ordered by this ordering. (case analysis)

$$W \times 2 = W \times \{0, 1\} = W \times \{0\} \cup W \times \{1\}$$

$$= W + W$$

$\female$ $\alpha \times \beta$ is the unique ordinal which is isom. to the lexic. product of α and β.

α, β, γ ordinals.

If α^β is known, $\alpha^{\beta^+} = \alpha^\beta . \alpha$

If λ is limit ordinal, then $\alpha^\lambda = \bigcup_{\beta<\lambda} \alpha^\beta$.

- $\alpha^0 = 1$
- $\alpha^1 = \alpha^{S(0)} = \alpha^0 . \alpha = 1.\alpha = S(0).\alpha = 1.\alpha = \alpha.$
- $\alpha . 0 = 0$
- $\alpha . S(\beta) = \alpha.\beta + \alpha$
- $\alpha.\lambda = \bigcup_{\beta<\lambda} \alpha\beta$ $(\lambda : \text{limit})$
- $\alpha.1 = \alpha.S(0) = \alpha.0 + \alpha = 0 + \alpha = \alpha.$
- $S(\beta) = \beta^+$ = successor of β = $\beta \cup \{\beta\}$.
- $\alpha + 0 = \alpha$
- $\alpha + S(\beta) = \alpha.\beta + \alpha$ $[= S(\alpha+\beta)]$
- $\alpha + \lambda = \bigcup_{\beta<\lambda} \alpha+\beta$ $(\lambda : \text{limit})$

Thm: $0 + \alpha = \alpha$ for every ordinal α.

Proof: • For $\alpha = 0$, $0+0=0$ ✓

• Assuming $0+\beta=\beta$, show $0+S(\beta) = S(\beta)$.

$$0 + S(\beta) = S(0+\beta) = S(\beta) \quad \text{(by ind. hyp.)}$$

• Assuming $0+\beta=\beta$ for all $\beta<\lambda$, show $0+\lambda=\lambda$. $(\lambda : \text{limit})$

$$0+\lambda = \bigcup_{\beta<\lambda} 0+\beta \overset{\text{ind. hyp.}}{=} \bigcup_{\beta<\lambda} \beta \overset{\text{just defn.}}{=} \lambda$$

What we did?

- Prove it for zero.
- Assume $P(\beta)$, show $P(\beta^+)$
- Assume $P(\beta)$ for all $\beta<\lambda$, show $P(\lambda)$.

Note: $\omega + 1 \neq 1 + \omega$.

α, β ordinals. Ordered sum of α and β is

$$\alpha \times \{0\} \cup \beta \times \{1\}.$$

- $(\alpha_i, 0) < (\beta_j, 1)$
- $(\alpha_i, 0) < (\alpha_j, 0)$ if $\alpha_i < \alpha_j$.
- $(\beta_i, 1) < (\beta_j, 1)$ if $\beta_i < \beta_j$.

? Show that this is a well ordering! (Case by case).

$\alpha \oplus \beta = \gamma$: unique ordinal that this well ordered set is isomorphic to, with the given order.

Thm: Two defn's of addition are equivalent.

Proof: Show $\alpha + \beta$ and $\alpha \times \{0\} \cup \beta \times \{1\}$ are isomorphic as ordered sets. Induction on β.

- If $\beta = 0$

$- \ \alpha + \beta = \alpha + 0 = \alpha$ //

$- \ \alpha \oplus \beta = \alpha \times \{0\} \cup \underbrace{\emptyset \times \{1\}}_{\emptyset}$ (since $\beta = 0 = \emptyset$)

$\alpha \oplus \beta^+ = \alpha \oplus \beta \cup \{(\alpha+\beta, 1)\}$

$= \alpha \times \{0\}$ //

α and $\alpha \times \{0\}$ are isomorphic.

$\therefore$ For $\beta = 0$, we are done.

- Assuming the theorem holds for β. Show that it holds for β^+.

$$\alpha + \beta \cong \alpha \oplus \beta \rightarrow \alpha + \beta^+ \cong \alpha \oplus \beta^+$$

$$\alpha + \beta \cup \{\alpha + \beta\} \qquad \alpha \oplus \beta \cup \{(\alpha + \beta), 1\}$$

$\alpha + \beta \cong \alpha \oplus \beta$ (ind. hyp.)

$\{\alpha + \beta\} \cong \{(\alpha + \beta), 1\}$

$\therefore$ $P(\beta) \to P(\beta^+)$, we are done.

- Now assume $\alpha+\beta \cong \alpha \oplus \beta$ for all $\beta < \lambda$ and show $\alpha+\lambda \cong \alpha \oplus \lambda$ (λ: limit)

$$\alpha+\beta \cong \alpha\oplus\beta \quad \text{for all } \beta<\lambda.$$

$$\bigcup_{\beta<\lambda} \alpha+\beta = \alpha+\lambda \cong \bigcup_{\beta<\lambda} \alpha\oplus\beta = \alpha\oplus\lambda$$

Taking the union of all isomorphisms b/w $\alpha+\beta$ and $\alpha\oplus\beta$'s for all $\beta<\lambda$, we get an isomorphism b/w $\alpha+\lambda$ and $\alpha\oplus\lambda$.

? $3+\omega = \bigcup_{n<\omega} 3+n = 3 \cup 4 \cup 5 \cup \dots$ (where $3 = \{0,1,2\}$)

$= \omega$

? $\omega+1 = \omega + S(0) = S(\omega+0) = \omega^+ = \omega \cup \{\omega\}$

? $\omega+3 = \omega + S(2) = S(\omega+2)$

$= \omega+2 \cup \{\omega+2\}$

$= \omega + S(1) \cup \{\omega+2\}$

$= S(\omega+1) \cup \{\omega+2\}$

$= \omega+1 \cup \{\omega+1\} \cup \{\omega+2\}$

$= \omega \cup \{\omega\} \cup \{\omega+1\} \cup \{\omega+2\}$

$= \omega \cup \{\omega, \omega+1, \omega+2\}$

$= \omega \cup \omega+3 \neq \omega = 3+\omega$?

$\alpha . \beta$ recursive defn.

$\alpha \times \beta = \alpha \times \beta$ (?)

order; $(\alpha_1, \beta_1) < (\alpha_2, \beta_2)$ if $\beta_1 < \beta_2$

$(\alpha_1, \beta) < (\alpha_2, \beta)$ if $\alpha_1 < \alpha_2$

- For $\beta = 0$ ✓
- Assume $P(\beta)$, show $P(\beta^+)$.
- Assume $P(\beta)$ for all $\beta < \lambda$, show $P(\lambda)$. (λ: limit).

<u>Thm</u> 1) Any infinite ordinal can be written in the form $\lambda + n$ where λ is a limit ordinal and $n \in \omega$.

2) Any limit ordinal can be written in the form $\omega . \alpha$ for some ordinal α.

<u>Proof</u>: • If $\alpha = 0$ ✓ Does not apply.

• If α is a successor ordinal,

$\alpha = S(\beta)$ (note that β can not be zero(?))

- if β is a limit ordinal,

$\alpha = S(\beta) = \beta + 1$, where β: limit, $1 \in \omega$.

$\beta = S(\gamma)$

- if β is a successor ordinal, then by ind. hyp. $\boxed{\gamma = \lambda + n}$ for some ordinal λ and $n \in \omega$.

$$\begin{aligned} \alpha = S(\beta) &= S(S(\gamma)) \\ &= S(\gamma + 1) = \gamma + 2 \\ &= (\lambda + n) + 2 \\ &= \lambda + (n+2) \end{aligned}$$

, where λ: limit, $n+2 \in \omega$

• If α is a limit ordinal,

$\alpha = \alpha + 0$, where α: limit, $0 \in \omega$.

Thm: α, β, γ ordinals.

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

Proof: By induction on γ.

- If $\gamma = 0$, $\alpha + (\beta + 0) = (\alpha+\beta) + 0$

  $\alpha + \beta = \alpha + \beta + 0$ ✓

- Assume true for γ, show for γ^+.

$$\begin{aligned} \alpha + (\beta + S(\gamma)) &= \alpha + S(\beta+\gamma) \\ &= S(\alpha + (\beta + \gamma)) \\ \text{ind. hyp.} &= S((\alpha+\beta) + \gamma) \\ &= (\alpha+\beta) + S(\gamma). \checkmark \end{aligned}$$

- If γ is a limit ordinal, assume for all $\delta < \gamma$, show for γ.

$$\begin{aligned} \alpha + (\beta + \gamma) &= \alpha + \left(\bigcup_{\delta < \gamma} \beta + \delta \right) \\ &= \bigcup_{\delta < \gamma} \alpha + (\beta + \delta) \\ &= \bigcup_{\delta < \gamma} (\alpha + \beta) + \delta \\ &= (\alpha+\beta) + \bigcup_{\delta<\gamma} \delta \\ &= (\alpha + \beta) + \gamma. \checkmark \end{aligned}$$

∇_0 $\{ m - \frac{1}{n} : m \geq 1, n \geq 2 \} \cong \omega^2$

EXERCISE (Easy!) $0^+ = 1$.

$0 = \emptyset \quad (1 = 2^1 - 1)$ $\quad\quad \emptyset \quad \{ \quad \} \quad ,$

$1 = \{\emptyset\} \quad (3 = 2^2 - 1) \rightarrow a_1 = 1, \ b_1 = 1, \ c_1 = 1, \ d_1 = 0$

$2 = \{\emptyset, \{\emptyset\}\} \quad (7 = 2^3 - 1) \Rightarrow a_2 = 2, \ b_2 = 2, \ c_2 = 2, \ d_2 =$

$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \quad (15 = 2^4 - 1) \rightarrow a_3 = 4, \ b_3 = 4, c_3 = 4, \ d_3 =$

$4 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \quad (31 = 2^5 - 1)$

$a_4 = 8, \ b_4 = 8, \ c_4 = 8, \ d_4 =$

How many symbols do we use for representating n?

9.12.21 Th

Axioms of set Theory

1) Extension Axiom: If two sets have the same elements then they are equal.

2) Empty set Axiom: There exists a set with no elements.

3) Pair set Axiom: If x and y are sets, there exists a set whose elts are only x and y. : $\{x, y\}$.

4) Union Axiom: If X is a set then $\cup X = \{z : z \in y$ for some $y \in X\}$

5) Power set Axiom: If X is a set, $\mathcal{P}(X) = \{y : y \subseteq X\}$ is a set.

6) Axiom of Infinity: There is an infinite set. There exists a set θ, $\emptyset \in \theta$ and if $x \in \theta$ then $x \cup \{x\} \in \theta$

7) Selection (Subset) Axiom: Let φ be a "first order formula" in language of set theory. If a is a set, then $b = \{x \in a : \varphi(x)\}$ is a set.

Ex: $P(\{1,2,3\}) \supseteq b = \{x \in P(\{1,2,3\}) : 1 \notin x\}$

8) Replacement Axiom : Let φ be a first order formula with two free variables. ($\varphi(x,y)$) which defines a partial function, that is for all x, there is at most one y s.t. $\varphi(x,y)$ holds. Let a be any set. Then there is a b consisting of all y s.t $\varphi(x,y)$ holds for some $x \in a$.

$b = \{f(x) : x \in a\}$ where f is the function defined by φ.

- $\varphi(x,y) =$ y is the smallest elt. of x.

$x = 3 = \{0,1,2\}$

$f(x) = \{0\}$.

∇ ZFC axioms ∇

- $\varphi(x,y)$ holds $\Leftrightarrow$ $y = x \cup \{x\} = f(x)$

$f(x) = y$ if $\varphi(x,y)$ holds

If $\varphi(x,y_1)$ & $\varphi(x,y_2)$ holds, then $y_1 = y_2$.

Take $a = w$.

Then $f(w) = \{1, 2, 3, 4, \dots\}$

$\uparrow\uparrow\uparrow\uparrow$ $x \cup \{x\}$

$w = \{0, 1, 2, 3, \dots\}$

9) Foundation Axiom : For any nonempty set x, there is $y \in x$ s.t. $y \cap x = \emptyset$.

- If not, then $\dots \in x \in x \in x \in x \in x \in x \in \dots$.

$\exists y \in x$ $y \cap x \neq \emptyset \to z \in y \cap x \to z \in y \in x \to t \in z \in y \in x$.

10) Axiom of Choice : Every non empty family of sets has a choice function. which goes from the index set to the union of the main set.

14.12.21 T

- Axiom of Extension

$$\forall x \forall y \, [x = y \leftrightarrow \forall z \, (z \in x \leftrightarrow z \in y)$$

- Foundation Axiom

$$\forall x \mid x \neq \emptyset \rightarrow \exists z \quad z \in x \wedge z \cap x = \emptyset$$

Question: which axioms do you use to show that (a,b) is a set?

$(a,b) = \{\{a\}, \{a,b\}\}$: pair set axiom

How about $X \times Y$?

$X \times Y = \{(x,y) : x \in X, y \in Y\}$

$X \times Y = \{(x,y) \in \mathcal{P}(\mathcal{P}(X \cup Y)) : x \in X, y \in Y\}$.

$\subseteq \mathcal{P}(\mathcal{P}(X \cup Y))$. : power set axiom + selection axiom

The Axiom of Choice

- Every nonempty family of sets has a choice function.

I: index set $\quad X = \{X_i : i \in I\}$

$f : I \to \bigcup X$

$i \longmapsto f(i) \in X_i$

Ex: $I : \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$

$f : I \longrightarrow \bigcup \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\} = \mathbb{N}$

$A \subseteq \mathbb{N} \longmapsto \min(A)$ exists since $\mathbb{N}$ is well-ordered & $A \neq \emptyset$.

Ex: $\quad I : P(\mathbb{R}) \setminus \{\emptyset\} \to \bigcup P(\mathbb{R}) \setminus \{\emptyset\}$

we can't find a function like that. We need axiom of choice.

Well Ordering Principle: Every set can be well ordered.

Try to well order $\mathbb{Z}$.

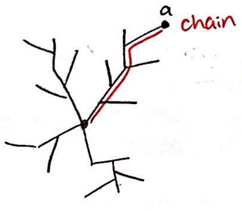
instead of $\quad \cdots -3, -2, -1, 0, 1, 2, 3, \cdots$

write $\quad 0, -1, 1, -2, 2, -3, 3, -4, 4, \cdots$

Put $-a$ between $a-1$ and a.

Zorn's Lemma: If Z is a partially ordered non-empty set such that every chain in Z has an upper bound in Z; Then Z has a maximal element.

(chain: totally ordered subset of Z)



lattice

Theorem: The following are equivalent;

1) Axiom of Choice (AC)
2) Well ordering Principle (WO)
3) Zorn's Lemma (ZL)

Proof: (WOP $\to$ AC)

Let $\{X_i : i \in I\}$ be a family of sets.

Let $X = \bigcup \{X_i : i \in I\}$, then by WOP let $(X, <)$ be a well-ordered of X. Define $f: I \to X = \bigcup_{i\in I} X_i$

$$i \longmapsto f(i) \in X_i$$

$f(i)$ be the minimum element of X.

$\forall x \in X_i,\ f(i) \leq x$.

Then every family of sets has a choice function. AC ✓

(AC → ZL)

Let $(X, <)$ be a partially ordered set for which every chain in X has an upper bound in X. We need to find a maximal element using (AC). Assume for a contradiction that there is no maximal element in X.

Let f be a choice function for the nonempty subsets of X.

$$f: \mathcal{P}(X) \setminus \{\emptyset\} \to X$$
$$A \longmapsto a \in A$$

We will "try" to define a map from ordinals to X.

$H(0) = f(X)$

$H(S(\alpha)) = f(\{x \in X : x > H(\alpha)\})$

$H(\lambda) = f(Y)$ where Y = all upper bounds for $\{H(\alpha) : \alpha < \lambda\}$

$$\underset{\in X}{H(0)} < \underset{\in X}{H(1)} < \underset{\in X}{H(2)} < \cdots$$

This defines an order preserving map from ordinals to X. Using this function one can define ordinals as a subset of X. X. since θ is not a set, contradicts with Axiom of Foundation.

(ZL → WOP)

Let X be a nonempty set, we want to insert a well order on X.

$Z = \{$ all well orders on subsets of $X \}$

$(X_1, <_{X_1}) < (X_2, <_{X_2})$ where X_1, X_2 subsets of X.

- $X_1 \subseteq X_2$
- $(X_1, <_{X_1}) = (X_1, <_{X_2}|_{X_1})$

Note that $Z \neq \emptyset$ since $X \neq \emptyset$ $\exists a \in X$ $(\{a\}, <)$ is a total order.

Every chain has an upper bound?

$(X_1, <_{X_1}) < (X_2, <_{X_2}) < \dots < \dots < (\bigcup X_i, \underset{\substack{\downarrow \\ \text{union of orders.}}}{<})$

So by ZL, Z has a maximal elt.

$(Y, <)$. <u>Claim</u>: $Y = X$

21.12.21 T

If this set has a maximal elt. say $(Y, <)$ then $Y = X$, if not, if $X \setminus Y \neq \emptyset$, $x \in X \setminus Y$;

$(Y \cup \{x\}) < \bigcup \{(a, x) : a \in Y\}$ which contradicts with maximality of $(Y, <)$, so $X = Y$.

▽ Think of $\bigcup((-n, n), <)$

$\underset{Y_1}{((-1,1), <)}, \overset{Y_2}{((-2,2), <)}, \dots$ are well orders but

$\bigcup((-n,n), <) = (\mathbb{Z}, <)$ is not!

(Y, f) $f : Y \to \theta$ (ordinals)

$(Y_1, f_1) < (Y_2, f_2)$ if;

- $Y_1 \subseteq Y_2$
- $f_1 \subseteq f_2$

1) <u>Theorem</u>: Let R be a commutative ring with <u>unity</u>. Then every ideal of R is contained in a maximal ideal.

[R: ring, I: ideal : subgroup with $\forall r \in R$, $\forall a \in I$, $ra \in I$;
maximal ideal: M is an ideal of R s.t. if $M \subseteq M' \subseteq R$ (M': ideal of R) then either $M = M'$ or $M' = R$]

<u>Proof</u>: (AC) $Z = \{J : J \text{ is a proper ideal of } R \text{ and } J \supseteq I\} \ni I$, so nonempty. Z is partially ordered with inclusion $\subseteq$.

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be a chain of ideals in Z.

I claim that $\bigcup_{i \in \mathbb{N}} I$ is a proper ideal containing I.

$\bigcup I$ is an ideal (OBVIOUS!). Since neither of the elements in this chain contain the unity 1; union does not contain the unit element so union is a proper ideal of R.

<u>By Zorn's Lemma</u>, Z has a maximal elt. which is a maximal ideal containing I. $\square$

2) <u>Theorem</u>: Every vector space has a basis.

<u>Proof</u>: A basis is a maximal linearly independent set.

$Z = \{\text{linearly independent subsets of } V\}$

- Z is partially ordered with inclusion.
- If $v_1 \neq 0$, $\{v_1\} \in Z$, $Z \neq \emptyset$.
- Does every chain has an upper bound?
  - Let $B_1 \subseteq B_2 \subseteq B_3 \subseteq \dots$ be a chain of elements of Z.

<u>Claim</u>: $\bigcup_{i \in \mathbb{N}} B_i$ is also in Z.

<u>Proof of the claim</u>: Let $v_1, v_2, \dots, v_n \in B_i$.

$v_1 \in B_{i_1}$, $v_2 \in B_{i_2}$, ..., $v_n \in B_{i_n}$

if $i = \max\{i_1, i_2, i_3, \dots, i_n\}$ then $v_1, \dots, v_n \in B_i$, so lin. ind.

By Zorn's Lemma Z has a maximal elt.

I claim that B is a basis for V. B is clearly lin. independent. WTS: B spans V.

Let $v \in V$, if $v \in span(B)$ ✓, if not, then $B \cup \{v\}$ is a linearly independent set contradicting the maximality of B. ※ so $span(B) = V$.

<u>Lebesque Measure</u> (μ): measures the size of the sets of real numbers.

- $\mu : \mathcal{P}(\mathbb{R}) \to \mathbb{R}$
  - $A \subseteq B$ then $\mu(A) < \mu(B)$
  - $\mu([a,b]) = b-a$
  - countably additive; $\mu(\bigcup_{n \in \mathbb{N}} X_n) = \sum_{n \in \mathbb{N}} \mu(X_n)$ pairwise disjoint sets
  - $\mu(\{a\}) = 0$

    $\mu(S) = 0$ if S is countable.

P Cantor set is an uncountable subset of $\mathbb{R}$, which has 0 measure.

  - translating a set should not change its measure.

    $\mu([0,1]) = 1$ & $\mu([a, a+1]) = 1$.

? Does every bounded set have a Lebesque measure?

<u>Theorem</u>: (AC) There exists a non-measurable bounded subsets of real numbers.

<u>Proof</u>: in $[0,1]$

$x \sim y$ if $x-y$ is a rational number (EQ. REL.)

$$\overline{\frac{1}{e}} = \left\{ \frac{1}{e} + \frac{1}{-2}, \dots, \frac{1}{e} - \frac{1}{2}, \dots \right\}$$

S = { a representative from each equivalence class }

S exists by AC.

$\mu(S) = ?$ if $\mu(S) = 0 \to \bigcup_{q \in [-1,1]} S+q = \underset{1}{\underset{\shortparallel}{[0,1]}} \neq 0$

$\mu(\bigcup S+q \cap [0,1]) = \sum \qquad = 0 \supseteq [0,1]$

if $\mu(S) = c$ $\quad \mu(\bigcup S+q) = \sum_{q \in \mathbb{Q}} c = \infty \subseteq [0,1]$

23.12.21 Th

<u>Proof:</u> Step 1: On $[0,1]$ define an eq. relation as follows.

$x \sim y$ iff $x - y \in \mathbb{Q}$ (uncountable many equivalence classes.)

Let S be a set of representatives for this equivalence rel.

If $q \in \mathbb{Q} \cap [-1,1]$ then $S_q = \{q+s : s \in S\} \subseteq [-1,2]$

$[0,1] \subseteq \bigcup_{q \in \mathbb{Q} \cap [-1,1]} S_q \subseteq [-1,2]$

what is $\mu(S)$?

- if $\mu(S) = 0 \quad = \mu(\bigcup S_q) = \sum \mu(S_q) = 0$

but it contains a subset of measure 1. ⁘

$\forall A \subseteq B \Rightarrow \mu(A) \leq \mu(B)$.

- if $\mu(S) = c$ for some $c < 1$, then $\mu(\bigcup S_q) = \sum_{q \in \mathbb{Q}} \underbrace{\mu(S_q)}_{c} \subseteq [-1,2]$

So S is a non measurable bounded subset of $\mathbb{R}$. □

uncountably many c = infinite < 3 ⁘