Lect. #13A

Ch. 4 - Cardinal Numbers

In the last chapter we studied well-ordered sets. With each well-ordering we associated an ordinal & called it the <u>length</u> of the well-ordering. In this chapter we will study the sizes of sets. With each set we will associate ~~an ordinal~~ a special kind of ordinal and call it the <u>cardinality</u> of the set

<u>Def.</u> Let A and B be sets. We say that A <u>has the same size</u> as B if we can find a bijective function $f: A \to B$.

We say that A <u>is smaller than or equal to</u> B if we can find an injective function $f: A \to B$.

We write $A \approx B$ if A has the same size as B

$A \preccurlyeq B$ if A is smaller than or equal to B.

We say that A is <u>finite</u> if for some $n \in \mathbb{N}$, $A \approx \{0, 1, 2, \ldots, n-1\}$.

We say that A is <u>denumerable</u> if $A \approx \mathbb{N}$.

Proposition 1

(a) $A \approx A$ for any set A

(b) If $A \approx B$, then $B \approx A$

(c) If $A \approx B$ & $B \approx C$, then $A \approx C$.

Proof: (Easy) Complete for H.W.

(a) Hint: $id : A \to A$ is a bijective function

(b) Hint: If $f : A \to B$ is bijective, then $f^{-1} : B \to A$ will also be bijective

(c) Hint: If $f : A \to B$ & $g : B \to C$ are bijective then $g \circ f : A \to C$ will be bijective.

Proposition 2

(a) $A \preccurlyeq A$ for any set A

(b) If $A \preccurlyeq B$ & $B \preccurlyeq C$, then $A \preccurlyeq C$.

Proof: (Trivial)

(a) $id : A \to A$ is injective

(b) If $f : A \to B$ & $g : B \to C$ are injective then $g \circ f : A \to C$ will also be injective.

Prop. 1 says that "$\approx$" behaves like an equiv. rel.
Prop. 2 says that "$\preccurlyeq$" behaves like a reflexive and transitive relation.

Qu: If $A \preccurlyeq B$ & $B \preccurlyeq$ does it follow that $A = B$?

Ans: NO. However we have the following resul

Def: We will write "$A \prec B$" to mean $A \preccurlyeq B$ and $A \not\approx B$.

Theorem 3: (Cantor's diagonal theorem)
For any set A, we have $A \prec \mathcal{P}(A)$.

Proof: Let $j : A \to \mathcal{P}(A)$ be defined by $j(x) = \{x\}$. Then j is clearly an injective function. So $A \preccurlyeq \mathcal{P}(A)$.

Now suppose that $A \approx \mathcal{P}(A)$. Then we can find a bijective function $f: A \to \mathcal{P}(A)$. Let

$$D = \{x \in A : x \notin f(x)\}.$$

Then $D \subseteq A$, so $D \in \mathcal{P}(A)$. Since f is bijective we can find an $x_0 \in A$ such that

$$f(x_0) = D.$$

Now either $x_0 \in D$ or $x_0 \notin D$.
But if $x_0 \in D$, then $x_0 \notin f(x_0)$ by def. of D and since $D = f(x_0)$ we get $x_0 \notin D$.
And if $x_0 \notin D$, then $x_0 \notin f(x_0)$ bec. $f(x_0) = D$ and so by the def. of D, $x_0 \in D$.

So in either case we get a contradiction.
Hence $A \not\approx \mathcal{P}(A)$ and we are done.

Lecture 13B **Def.** Let $\Omega =$ class of all ordinals and $f : \Omega \to \Omega$ be a class-function.

We say that f is <u>increasing</u> if
$$\alpha < \beta \Rightarrow f(\alpha) < f(\beta).$$

We say that f is <u>continuous</u> if for limit ordinal λ
$$f(\lambda) = \sup\{f(\alpha) : \alpha < \lambda\}$$

If f is both increasing and continuous we say that it is <u>normal</u>.

<u>Examples</u>

1. Let $f(\alpha) = \alpha + 2$. Then
   f is increasing but
   f is not continuous
   $f(\omega) = \omega + 2 \neq \omega = \sup\{n+2 : n < \omega\}$

2. Let $g(\alpha) = \alpha \cdot \omega$ Then
   g is not increasing bec. $1 < 2$ but $1 \cdot \omega = 2 \cdot \omega$
   Also g is not cont. bec: $\underset{\uparrow \atop \lambda}{\omega} \cdot \omega = \sup\{\underset{\uparrow}{n \cdot \omega} : n < \underset{\uparrow \atop \lambda}{\omega}\}$

3. Let $h(\alpha) = 2^\alpha$. Then
   h is both continuous & increasing.
   So it is normal.

Def. An ordinal γ is said to be a *fixed-point* of the function f if $f(\gamma)=\gamma$.

Theorem 12 (Fixed-point Theorem)
Let $f:\Omega\to\Omega$ be a *normal* class-function. Then for any ordinal α_0, we can find a fixed point γ of f such that $\gamma \geq \alpha_0$.

Proof: Since f is increasing we know from Prop. 2 Ch. 2 that $f(\alpha)\geq\alpha$. Now if $f(\alpha_0)=\alpha_0$, then take $\gamma=\alpha_0$ and we are done.

So suppose $f(\alpha_0)>\alpha_0$. Let
$$f^{(n)} = f\circ f\circ f\ldots\circ f \quad (n \text{ times composition})$$
Since f is increasing we have
$$\alpha_0 < f(\alpha_0) < f(f(\alpha_0)) < \ldots < f^{(n)}(\alpha_0) < \ldots$$

Let $\gamma = \sup\{f^{(n)}(\alpha_0) : n<\omega\}$. Then γ is an ordinal and clearly $\gamma>\alpha_0$.

Now suppose $\gamma=\beta+1$. Then $f^{(n)}(\alpha_0)\geq\beta$ for some $n_0\in\omega$ (otherwise $f^{(n)}(\alpha_0)$ would be $\leq\beta$ for all $n\in\omega$ and we would get $\gamma=\sup\{f^{(n)}(\alpha_0): n<\omega\}\leq\beta$ - contradiction). But then $f^{(n_0+1)}(\alpha_0)\geq\beta+1$ and $f^{(n_0+2)}(\alpha_0)\geq\beta+2$ contradicting the fact that $\beta+1=\gamma=\sup\{f^{(n)}(\alpha_0): n<$
So γ must be a limit ordinal. Since f is a normal function
$$f(\gamma)=\sup\{f(\alpha):\alpha<\gamma\}=\sup\{f^{(n)}(\alpha_0): n<\omega\}=\gamma.$$
So γ is a fixed-point of f and we are done.

$\varepsilon_0 = \sup\{ \underbrace{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}_{n \text{ times}} : n < \omega \}$

$\omega^{\varepsilon_0} = \varepsilon_0$.

ε_0 is the smallest fixed point of, $\omega^\alpha = f(\alpha)$

$f(0) = \omega^0 = 1$

$f^2(0) = \omega^{f(0)} = \omega^1 = \omega$

$f^3(0) = \omega^{f^2(0)} = \omega^\omega$

$f^4(0) = \omega^{f^3(0)} = \omega^{\omega^\omega}$

$\vdots$

$f^n(0) = \underbrace{\omega^{\omega^{\cdot^{\cdot^{\omega}}}}}_{\cancel{n-1} \text{ times}}$

$f^\omega(0) = \sup\{f^n(0) : n<\omega\} = \sup\{ \underbrace{\omega^{\omega^{\cdot^{\cdot^{\omega}}}}}_{(n-1)\text{ times}} : n< \} = \varepsilon$

$f(\varepsilon_0+1) = \omega^{\varepsilon_0+1} = \omega^{\varepsilon_0} \cdot \omega^1 = \varepsilon_0 \cdot \omega$

$f^2(\varepsilon_0+1) = f(\varepsilon_0 \cdot \omega) = \omega^{\varepsilon_0 \cdot \omega} =$

$f^3(\varepsilon_0+1) = f(\omega^{\varepsilon_0 \cdot \omega}) = \omega^{\omega^{\varepsilon_0 \cdot \omega}}$

$f^4(\varepsilon_0+1) = f(\omega^{\omega^{\varepsilon_0 \cdot \omega}}) = \omega^{\omega^{\omega^{\varepsilon_0 \cdot \omega}}} = \omega^{\omega^{\omega^{\omega^{\varepsilon_0+1}}}}$

$f^\omega(\varepsilon_0+1) = \sup\{ \underbrace{\omega^{\omega^{\omega^{\cdot^{\cdot^{\omega^{\varepsilon_0 \cdot \omega}}}}}}}_{n-1 \text{ times}} : n<\omega \} = \varepsilon_1$

ε_n = n-th fixed point of f.

$\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots$

ζ_0 = smallest α such that $\varepsilon_\alpha = \alpha$

$g(\alpha) = \varepsilon_\alpha$

$g(0) = \varepsilon_0$

$g^2(0) = \varepsilon_{\varepsilon_0}$ $\qquad g^\omega(0) = \zeta_0 = \sup\{ \underbrace{\varepsilon_{\varepsilon_{\varepsilon_{\cdot_{\cdot_{\varepsilon_0}}}}}}_{n \text{ times}} : n<\omega \}$

$g^3(0) = \varepsilon_{\varepsilon_{\varepsilon_0}}$

$\vdots$

Lect #14

Theorem 5 (Cantor-Bernstein Equivalence Theorem)
If $A \preceq B$ and $B \preceq A$, then $A \approx B$, (i.e., if there exist an injection $f: A \to B$ and an injection $g: B \to A$, then there is a bijection $f: A \to B$.)

Proof: Let $f: A \to B$ and $g: B \to A$ be bijections. Define the sets $\langle A_n \rangle_{n \in \omega}$ and $\langle B_n \rangle_{n \in \omega}$ recursively as follows:

$A_0 = A$ & $A_{n+1} = g[f[A_n]]$ for $n \geq 0$,

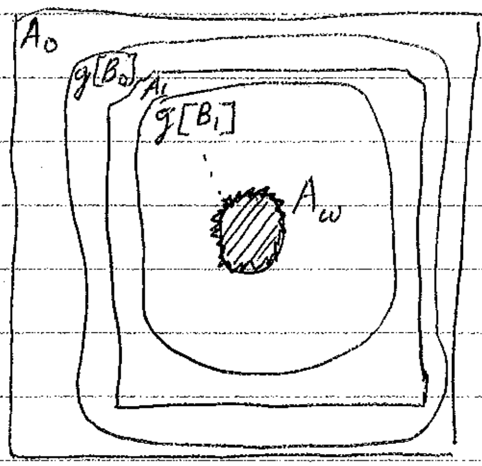
$B_0 = B$ & $B_{n+1} = f[g[B_n]]$ for $n \geq 0$.

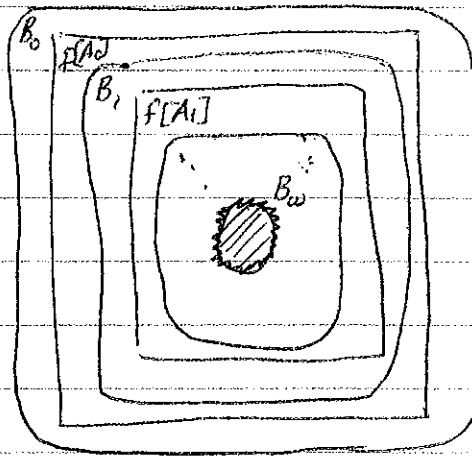
Then it is easy to see that for each $n \geq 0$

$A_n \supseteq g[B_n] \supseteq A_{n+1}$ & $B_n \supseteq f[A_n] \supseteq B_{n+1}$

So $A_0 \supseteq g[B_0] \supseteq A_1 \supseteq g[B_1] \supseteq A_2 \supseteq \cdots$ and

$B_0 \supseteq f[A_0] \supseteq B_1 \supseteq f[A_1] \supseteq B_2 \supseteq \cdots$





Now let $A_\omega = \bigcap_{n \in \omega} A_n$ & $B_\omega = \bigcap_{n \in \omega} B_n$. Then

$B_\omega = \bigcap_{n \in \omega} B_n \supseteq \bigcap_{n \in \omega} f[A_n] \supseteq \bigcap_{n \in \omega} B_{n+1} = B_\omega$.

So $\bigcap_{n \in \omega} f[A_n] = B_\omega$

$\therefore f[A_\omega] = f[\bigcap_{n \in \omega} A_n]$

$= \bigcap_{n \in \omega} f[A_n]$ because f is injective

$= B_\omega$.

Now A can be partitioned into disjoint sets as follows:

$$A = A_\omega \cup (A_0 - g[B_0]) \cup (g[B_0] - A_1) \cup (A_1 - g[B_1]) \cup \cdots$$
$$= A_\omega \cup \bigcup_{n\in\omega} (A_n - g[B_n]) \cup \bigcup_{n\in\omega} (g[B_n] - A_{n+1})$$

Similarly B can be partitioned into disjoints sets as follows:

$$B = B_\omega \cup (B_0 - f[A_0]) \cup (f[A_0] - B_1) \cup (B_1 - f[A_1]) \cup \cdots$$
$$= B_\omega \cup \bigcup_{n\in\omega} (B_n - f[A_n]) \cup \bigcup_{n\in\omega} (f[A_n] - B_{n+1})$$

Since f is injective and $f[A_\omega] = B_\omega$,
$f: A_\omega \to B_\omega$ will be a bijection

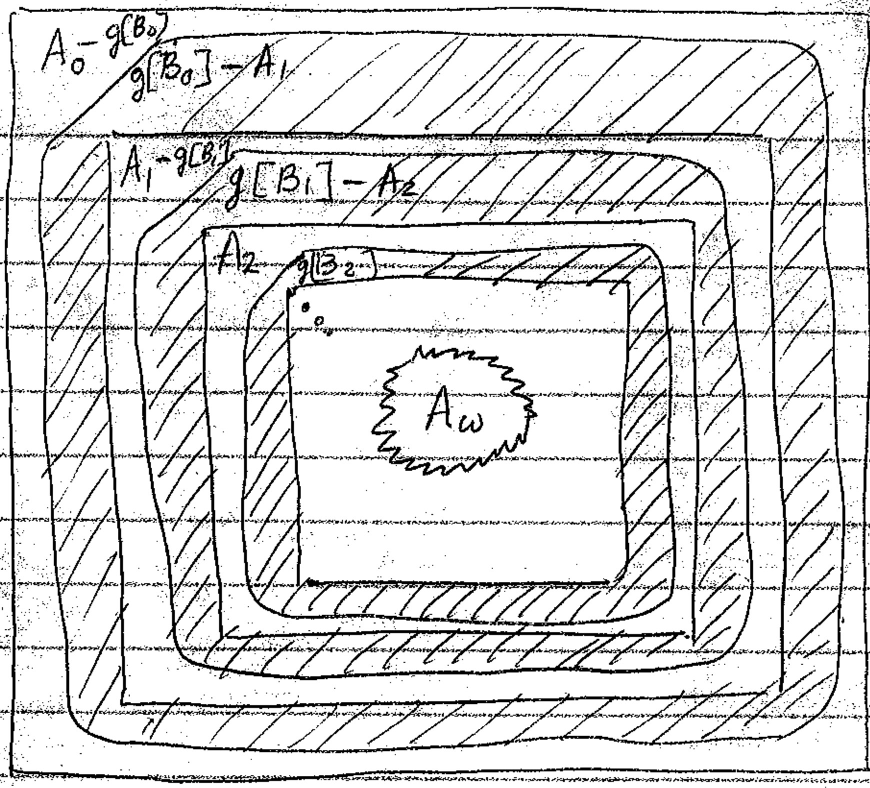
Also $f[A_n - g[B_n]] = f[A_n] - f[g[B_n]]$ bec. f is inj
$= f[A_n] - B_{n+1}$.
So $f: A_n - g[B_n] \to f[A_n] - B_{n+1}$ will be a bijection

Finally $g[B_n - f[A_n]] = g[B_n] - g[f[A_n]]$ bec. g is inj
$= g[B_n] - A_{n+1}$
So $g: B_n - f[A_n] \to g[B_n] - A_{n+1}$ will be a bijection
$\therefore$ $g^{-1}: g[B_n] - A_{n+1} \to B_n - f[A_n]$ will be a bijection.

We can now piece this all together and get a bijection $h: A \to B$ as follows. Let

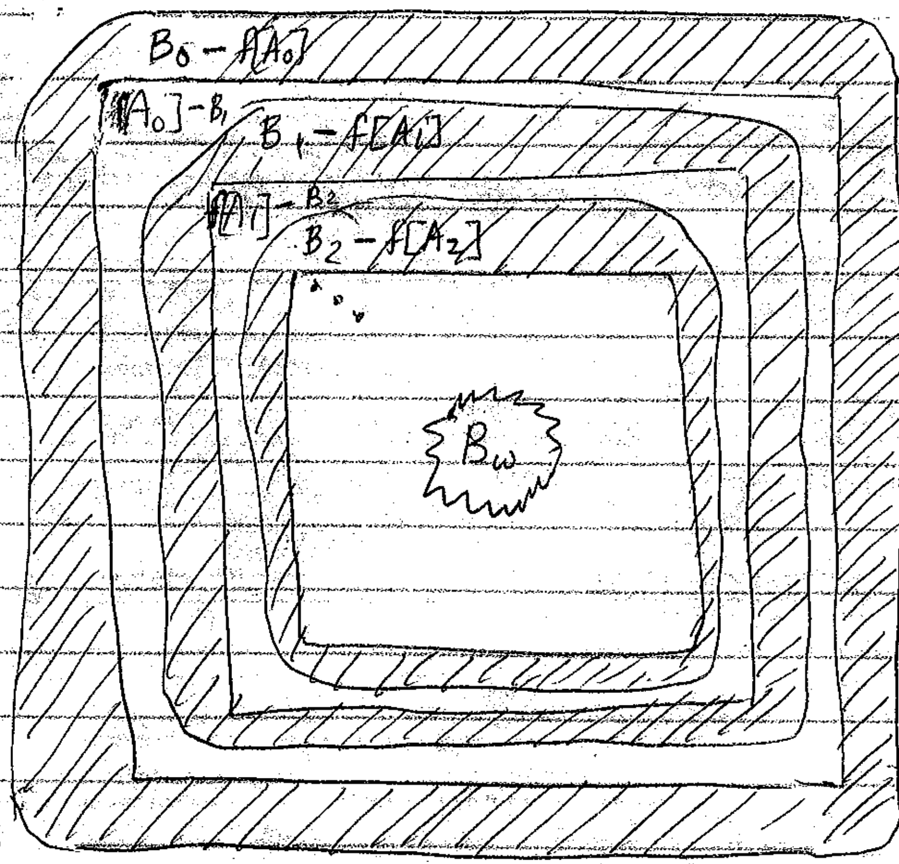
$$h(x) = \begin{cases} f(x) & \text{if } x \in A_\omega \\ f(x) & \text{if } x \in (A_n - g[B_n]) \text{ for some } n \in \omega \\ g^{-1}(x) & \text{if } x \in (g[B_n] - A_{n+1}) \text{ for some } n \in \omega. \end{cases}$$

Then h will be a bijection from A to B.



A_0 - g[B_0]
g[B_0] - A_1
A_1 - g[B_1]
g[B_1] - A_2
A_2
g[B_2]
A_ω

$g : B \to A$



B_0 - f[A_0]
f[A_0] - B_1
B_1 - f[A_1]
f[A_1] - B_2
B_2 - f[A_2]
B_ω

Lect. #15 Recall that we defined the following notions in our attempt to measure the sizes of sets.

$A \approx B$ — A is equipotent to B
$A \preccurlyeq B$ — A is smaller than or equal to B
$A \prec B$ — A is smaller than B.

We also proved the following theorem

1. $A \prec \mathcal{P}(A)$ (Cantor's diagonal theorem)
2. If $A \preccurlyeq B$ & $B \preccurlyeq A$ then $A \approx B$ (Cantor-Bernstein theorem)

<u>Fact 1</u>: $\mathbb{Z} \approx \mathbb{N}$

<u>Proof</u>: Let $f(z) = \begin{cases} 2z & \text{if } z \geq 0 \\ -2z-1 & \text{if } z < 0 \end{cases}$.
Then f is a bijection from $\mathbb{Z}$ to $\mathbb{N}$
So $\mathbb{Z} \approx \mathbb{N}$.

<u>Fact 2</u>: $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$

<u>Proof</u>: Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by
$$f(m,n) = 2^m(2n+1) - 1$$
Then f is a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.
So $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

<u>Fact 3</u>: Let $SEQ(\mathbb{N})$ be set of all <u>finite</u> sequences of natural numbers. Then $SEQ(\mathbb{N}) \approx \mathbb{N}$.

<u>Proof</u>: Let $p_0, p_1, p_2, p_3 \ldots$ be the sequence of all prime numbers. Define $f : SEQ(\mathbb{N}) \to \mathbb{N}$ by

$$f(\langle a_0, a_1, a_2, \ldots, a_{n-1} \rangle) = \langle TZ(\underset{\sim}{s}), (p_0^{a_0} p_1^{a_1} \cdots p_n^{a_{n-1}}) - 1 \rangle$$

where $TZ(\underset{\sim}{s})$ = the sequence of 0s with which $\langle a_0, \ldots, a_{n-1} \rangle = \underset{\sim}{s}$ ends
Then f is a bijection from $SEQ(\mathbb{N})$ to $\mathbb{N}$.

<u>Fact 4</u>: $\mathbb{Q} \approx \mathbb{N}$.

<u>Proof</u>: We do not have any simple bijection from $\mathbb{Q}$ to $\mathbb{N}$. We will show that $\mathbb{N} \preccurlyeq \mathbb{Q}$ and $\mathbb{Q} \preccurlyeq \mathbb{N} \times \mathbb{N}$. Since $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$, it will follow that $\mathbb{Q} \preccurlyeq \mathbb{N}$ & $\mathbb{N} \preccurlyeq \mathbb{Q}$. So from the Cantor-Bernstein theorem we will get $\mathbb{Q} \approx \mathbb{N}$.

Let $i : \mathbb{N} \to \mathbb{Q}$ be defined by $i(n) = n/1$
Then i is clearly an injection from $\mathbb{N}$ to $\mathbb{Q}$. So $\mathbb{N} \preccurlyeq \mathbb{Q}$.

Now let $j : \mathbb{Q} \to \mathbb{N} \times \mathbb{N}$ be defined as follows:
First we express each element $q \in \mathbb{Q}$ in lowest terms, ($q = m/n$ with $n \geq 1$ and m having no common divisor with n).
Define

$$j(m/n) = \begin{cases} \langle m, 2n \rangle & \text{if } m \geq 0 \\ \langle -m, 2 & \text{if } m < 0 \end{cases}$$

Then j is an injection. So $\mathbb{Q} \preccurlyeq \mathbb{N} \times \mathbb{N}$.

Def. An <u>algebraic number</u> is any number that is the root of a polynomial with integer coefficients

<u>Ex.</u> $\sqrt{2}$ is an alg. no. bec. $\sqrt{2}$ is a root of the eq. $x^2-2=0$

$i\sqrt{3}$ is an alg. no. bec. $i\sqrt{3}$ is a root of $x^2+3=0$.

<u>Fact 5</u>: Let $\mathbb{A}$ = set of all algebraic nos. Then $\mathbb{A} \approx \mathbb{N}$.

There are three ways to define the real numbers rigorously.

(i) Dedekind cuts
(ii) Cauchy sequences of rational nos.
(iii) Nested rational intervals

In what follows we shall assume that the real nos. are defined by using Dedekind cuts (but any of the other two definitions will be equally fine).

<u>Fact 6</u>: $\mathbb{N} \prec \mathbb{R}$ (i.e. $\mathbb{N} \preccurlyeq \mathbb{R}$ & $\mathbb{N} \not\approx \mathbb{R}$)

Proved by the usual Cantor's diagonal argument from Discrete Math.

From fact 5 and fact 6 we can see that

$$\mathbb{R} - (\mathbb{R} \cap \mathbb{A}) \neq \emptyset$$

So this gives us a proof of the existence of transcendental numbers.

(Recall that a transcendental number is a number that is not a root of any polynomial with integer coefficients)

Def. We say that a real number x is computable if there is a program such that if you enter n, you will get the n-th decimal digit of x.

Fact 7: Let $\mathbb{R}_C$ = set of all computable real numbers. Then $\mathbb{R}_C \approx \mathbb{N}$ because there are at most a countable no. of programs. So there exist real numbers which are not computable.

Fact 8: Let $\mathbb{R}_D$ = set of real numbers that have a finite description. Then

$$\mathbb{R}_D \approx \mathbb{N}.$$

From this we can see that there are real numbers which cannot even be described in finitely many words!

Lect. #16 <u>Def.</u> An ordinal α is said to be a <u>cardinal</u> if there is no ordinal $\beta < \alpha$ which is equipotent to α.

For this reason, cardinals are sometimes called <u>initial ordinals</u>.

<u>Examples</u> It is easy to see that ω is a cardinal because $\omega \not\approx n$ for any $n<\omega$. Similarly $0, 1, 2, 3, \ldots$ are cardinals. However $\omega+1$ is not a cardinal because $\omega+1 \approx \omega$. Also $\omega.2$, ω^2, ω^ω, ε are also not cardinals.

<u>Qu</u>: Are there any more cardinal?

<u>Def.</u> Let A be a set. We define the <u>Hartogs number</u> of A by

$$h(A) = \text{smallest ordinal } \alpha \text{ with } \alpha \not\preceq A.$$

It is easy to see that $h(A)$ is always a cardinal. This allows us to define a whole scale of cardinals - called the <u>alephs</u>.

<u>Def.</u> The <u>alephs</u> are the ordinals defined by by transfinite recursion as follows:

$$\omega_0 = \omega$$
$$\omega_{\alpha+1} = h(\omega)$$
$$\omega_\lambda = \sup\{\omega_\alpha : \alpha < \lambda\} \quad \text{if } \lambda \text{ is a limit ordinal.}$$

Note: Each aleph is in fact a cardinal. When we want to think of the alephs as ordinals we will denote them by ω_α. When we want to think of them as cardinals we will denote them by $\aleph_\alpha$. ($\aleph$ is the first letter of the Hebrew alphabet

Proposition 6

(a) For each α, ω_α is a cardinal

(b) For any α, $\alpha \leq \omega_\alpha$

(c) If κ is an infinite cardinal, then $\kappa = \omega_\alpha$ for some ordinal α.

Proof: (a) The proof is by ind. on α. (Do for H.W.)

(b) The proof is by ind. on α (Do for H.W.)

(c) Suppose κ is an infinite cardinal. Then κ is an ordinal. So $\kappa \leq \omega_\kappa$ by part (b). Hence $\kappa < h(\omega_\kappa)$, i.e. $\kappa < \omega_{\kappa+1}$.

So for any infinite cardinal κ, we can find an ordinal α such that $\kappa < \omega_\alpha$. We will show by ind. on α that if κ is an inf. cardinal $< \omega_\alpha$, then $\kappa = \omega_\gamma$ for some $\gamma < \alpha$.

If $\alpha = 1$, then $\kappa < \omega_1 = h(\omega_0)$ implies $\kappa \preceq \omega_0$ [because $h(\omega_0)$ = smallest ord. $\not\preceq \omega_0$] Since κ is inf. we must have $\kappa = \omega_0$. So the result is true for $\alpha = 1$.

Suppose the result is true for α. We must prove it for $\alpha+1$. Now if $\kappa < \omega_{\alpha+1} = h(\omega_\alpha)$ then $\kappa \leq \omega_\alpha$. So $\kappa = \omega_\alpha$ or $\kappa < \omega_\alpha$. In the first case take $\gamma = \alpha$ and in the second case we get a γ bec. the result is true for α.

Finally supp. the result is true for all $\alpha < \lambda$ where λ is a limit ordinal. Now if $\kappa < \omega_\lambda$, then $\kappa < \omega_{\alpha_0}$ for some $\alpha_0 < \lambda$ (otherwise we would get $\kappa \geq \omega_\lambda$). Since the result is true for all $\alpha < \lambda$ we can find a $\gamma \leq \alpha_0$ such that $\kappa = \omega_\gamma$. Thus the result is true for all α.

Hence by the Princ. of Trans. Ind. the result is true for all α. This completes the proof.

<u>The size of a set</u>:

So far we have been only comparing sets. We did not have a measure of their size.

<u>Def.</u> We define the <u>size</u> of a set A by

$$|A| = \text{the smallest ordinal } \alpha \text{ such that there is a bijection from } A \text{ to } \alpha.$$

From the definition it immediately follows that $|A|$ will be a cardinal. But there is one problem.

Maybe there is no bijection from A to <u>any</u> of the ordinals - so there wouldn't be any smallest one. Fortunately, this is not so because of the following theorem.

<u>Well-ordering Principle</u> (AC) Let A be any non-empty set. Then we can find a binary relation "$\leq$" on A such that $\langle A, \leq \rangle$ is a well-ordered set.

We will prove this theorem in the next chapter.

Since $\langle A, \leq \rangle$ is a well-ordered set, we know it is isomorphic to $\langle \alpha, \in \rangle$ for some ordinal α. So we get a bijection from A to α. Hence our definition always makes sense.

Arithmetic of the Cardinal numbers

<u>Def.</u> Let $\mathcal{F}(A, B) =$ set of all functions from A to B.

<u>Def.</u> Let κ and μ be cardinal numbers. We define $\kappa + \mu$, $\kappa \cdot \mu$ and κ^{μ} by

$$\kappa + \mu = |(\kappa \times \{0\}) \cup (\mu \times \{1\})|$$

$$\kappa \cdot \mu = |\kappa \times \mu|$$

$$\kappa^{\mu} = |\mathcal{F}(\mu, \kappa)|$$

Examples

$\kappa + 0 = \kappa \qquad |\kappa \cup \emptyset| = \kappa$

$\kappa \cdot 1 = \kappa \qquad |\kappa \times \{0\}| = \kappa$

$\kappa^0 = 1 \qquad |\mathcal{F}(\emptyset, \kappa)| = |\{\emptyset\}| = 1$

$\kappa^1 = \kappa \qquad |\mathcal{F}(\{0\}, \kappa)| \cong |\{\alpha : \alpha < \kappa\}| = \kappa$ ✓

$\{f_\alpha : f_\alpha(0) = \alpha, \alpha < \kappa\} \cong \{\alpha : \alpha < \kappa\}$

Proposition 7: for any cardinals κ, μ, ν

(a) $\kappa + \mu = \mu + \kappa$

(b) $(\kappa + \mu) + \nu = \kappa + (\mu + \nu)$

(c) $\kappa + \kappa = 2 \cdot \kappa$

Proposition 8: For any cardinals κ, μ, ν

(a) $\kappa \cdot \mu = \mu \cdot \kappa$

(b) $(\kappa \cdot \mu) \cdot \nu = \kappa \cdot (\mu \cdot \nu)$

(c) $\kappa \cdot (\mu + \nu) = \kappa \cdot \mu + \kappa \cdot \nu$

Proposition 9: For any cardinals κ, μ, ν

(a) $\kappa \cdot \kappa = \kappa^2$

(b) $\kappa^{\mu + \nu} = \kappa^\mu \cdot \kappa^\nu$

(c) $(\kappa \cdot \mu)^\nu = \kappa^\nu \cdot \mu^\nu$

(d) $(\kappa^\mu)^\nu = \kappa^{\mu \cdot \nu}$

Prove Propositions 7, 8 & 9 for H.W.

From this we see that cardinal arithmetic is very much like ordinary arithmetic. But a lot of strange things will show up later.

Lect. #17 Ch. 5 - The axiom of choice and Cardinal Arithmetic

Def. Let S be a set and f be any function with domain S. We say that f is a choice function for S if
$f(A) \in A$ for each non-empty $A \in S$.

Note:
A set can have many choice functions.
Ex. Let $S = \{\emptyset, \{1\}, \{0,1\}\}$ and f and g be defined by

$$f(\emptyset) = \emptyset, \quad f(\{1\}) = 1, \quad f(\{0,1\}) = 0$$
$$g(\emptyset) = \{4\}, \quad g(\{1\}) = 1, \quad g(\{0,1\}) = 1$$

Then f and g are both choice functions for S.

Qu: Does every set has a choice function?

Recall that the axiom of choice was the statement:

(AC): If $\mathcal{A}$ is a set of pairwise disjoint non-empty sets, then there is a set M which consists of one element of each member of $\mathcal{A}$.

Let AC′ be the statement given by

(AC′): Every set has a choice function

<u>Proposition 1</u>. $(AC') \Leftrightarrow (AC)$

<u>Proof</u>: $(\Longrightarrow)$ Suppose (AC′) is true. Let $\mathcal{A}$ be a set of pairwise disjoint non-empty sets. Then we can find a choice function f for $\mathcal{A}$. Let

$$M = \{f(A) : A \in \mathcal{A}\} = \text{range}(f)$$

Then by the Replacement Axiom, M is a set and because f is a choice function M consists of exactly one element from each member of $\mathcal{A}$.

$(\Longleftarrow)$ Suppose (AC) is true. Let S be any set. For each $A \in S$, let

$$A^* = \{\langle a, A\rangle : a \in A\}$$

and put $S^* = \{A^* : A \in S\}$

Then the elements of S^* will be pairwise disjoint and $\phi \in S$ $\phi \in S^*$

By (AC) we can find a set M such that M has exactly one member of each non-empty set in S^*. Let f be defined by

$$f(A) = a_0 \quad \text{if} \quad A^* \cap M = \{\langle a_0, A\rangle\}$$

$f(\phi) = \phi$. Then f is a choice function for S.

Example

$$S = \Big\{ \underbrace{\{a\}}_{A} \quad \underbrace{\{b\}}_{B} \quad \underbrace{\{a, b\}}_{C} \quad \underbrace{\{b, d\}}_{D} \Big\}$$

$$S^* = \Big\{ \underbrace{\{\langle a, A\rangle\}}_{A^*} \quad \underbrace{\{\langle b, B\rangle\}}_{B^*} \quad \underbrace{\{\langle a, C\rangle, \langle b, C\rangle\}}_{C^*} \quad \underbrace{\{\langle b, D\rangle, \langle d, D\rangle\}}_{D^*} \Big\}$$

Say $M = \{ \langle a, A\rangle \quad \langle b, B\rangle \quad \langle a, C\rangle \quad \langle b, D\rangle \}$

Then

$$f(A) = a, \quad f(B) = b, \quad f(C) = a, \quad f(D) = b.$$

We want to show that the every set can be well-ordered. We need the following Lemma

<u>Lemma 2</u> (AC): If A is any set then there is a function $f : \mathcal{P}(A) \to A \cup \{A\}$ such $f(A) = A$ and $f(X) \in A - X$ for each $X \subsetneq A$.

<u>Proof:</u> Let $\mathcal{B} = \{ A - X : X \subsetneq A \}$. Since AC′ is equiv. to AC, we know that we can find a choice function $g : \mathcal{B} \to \cup \mathcal{B}$.

Define $f: \mathcal{P}(A) \to A \cup \{A\}$ by

$$f(A) = A$$
$$f(X) = g(A - X) \quad \text{if} \quad X \subsetneq A.$$

Since g was a choice function $g(A-X) \in A - X$. So $f(X) \in A - X$ and we are done.

<u>Theorem 3</u> (AC): Every set can be well-ordered.

<u>Proof</u>: Let A be any set. Then by Lemma 2, we can find a function $f: \mathcal{P}(A) \to A \cup \{A\}$ such that $f(A) = A$ and $f(X) \in A - X$ for each $X \subsetneq A$

Define the class-function $h: \Omega \to V$ by

$$h(\alpha) = \begin{cases} f(h[\alpha] \cap A) & \text{if } A \nsubseteq h[\alpha] \\ \{A\} & \text{if } A \subseteq h[\alpha] \end{cases}$$

Then $h(\alpha) = \{A\}$ for some $\alpha \in \Omega$.

[Indeed, supp. $h(\alpha) \neq \{A\}$ for any $\alpha \in \Omega$. Then we have $h(\alpha) = f(h[\alpha] \cap A) \in A$ for each $\alpha \in \Omega$. So $h[\Omega]$ is a subset B of A. Also h will be an injective class-function because $f(X) \in A - X$ for each $X \subsetneq A$. So h^{-1} will be a bijection from B to Ω,

[illegible]

But then $h^{-1}[B] = \Omega$! will be a set by the Replacement axiom. Since we know Ω is not a set we have a contradiction

Now let α_0 = smallest ordinal α such that $h(\alpha) = \{A\}$.

Then
$h(\beta) \in A$ for each $\beta < \alpha$.

So $h[\alpha_0] \subseteq A$.

But $h(\alpha_0)$, so by def. of h, $h[\alpha_0] \supseteq A$.
Hence $h[\alpha_0] = A$.

We will now show that h is a bijective function from α_0 to A. Suppose $\beta < \gamma$ are elements of α_0. Then
$h(\beta) \in h[\gamma]$ bec. $\beta < \gamma \Rightarrow \beta \in \gamma$.

So $h(\gamma) = f(h[\gamma] \cap A)$
$\in A - h[\gamma] \cap A$ by the choice of f
and since $h(\beta) \in h[\gamma] \cap A$,
$h(\gamma)$ cannot be equal to $h(\beta)$.

Thus h is injective and as $h[\alpha_0] = A$, h is surjective. Hence h is a bijection.

Now we define a well ordering "$\prec$" on A by $a \prec b$ if $h^{-1}(a) < h^{-1}[b]$. Note A inherits this well-ordering from the ordinal α_0.

Lect 18 The statement "Every set can be well-ordered" is usually referred to as the <u>Well Ordering Principle</u> (WOP). We can actually prove the following result.

<u>Corollary 4</u>: $(AC) \Leftrightarrow (WOP)$

<u>Proof</u>: We have already seen in Thm 3 that $AC \Rightarrow WOP$. We will show that $WOP \Rightarrow AC$

Suppose WOP is true. Let $\mathcal{A}$ be any set of pairwise disjoint non-empty set. Then $\cup\mathcal{A}$ is a set. So we can find a well-ordering "$\prec$" on $\cup\mathcal{A}$.
For each $A \in \mathcal{A}$, let

$$f(A) = \text{smallest element of } A \text{ according to } "\prec"$$

Then put $M = \{f(A) : A \in \mathcal{A}\}$. Then M will be a set which contains exactly one element from each member of $\mathcal{A}$. So we indeed have $WOP \Rightarrow AC$.

We will return to the applications of AC in a little while. For now, let us turn to the Arithmetic of Cardinals. Below are some basic questions:

Qu: What are $\aleph_0 + \aleph_0$, $\aleph_0 \cdot \aleph_0$, and $\aleph_0^{\aleph_0}$?

We will shortly see that $\aleph_0 + \aleph_0 = \aleph_0$

$\aleph_0 \cdot \aleph_0 = \aleph_0$

but $\aleph_0^{\aleph_0}$ is not at all easy. We can show (see homework problems in Ch. 4) that

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

but this does not answer the question. What we want is an α such that $2^{\aleph_0} = \aleph_\alpha$!

Proposition 5: If κ is an infinite cardinal then $\kappa + \kappa = \kappa$.

Proof: Recall that each ordinal α can be uniquely written in the form

$$\alpha = \lambda + n$$

where λ is a limit ordinal and $n \in \mathbb{N}$. We say that the ordinal is <u>even</u> if n is even, and that α is <u>odd</u> if n is odd.

Now let κ_O = set of all odd ordinals in κ

and κ_E = set " " even " in κ.

Then $\kappa = \kappa_O \cup \kappa_E$. Now define the functions f and g by

$$f : \kappa \times \{0\} \to \kappa_O \qquad f(\langle \alpha, 0 \rangle) = \lambda + 2n + 1 \quad \text{if } \alpha = \lambda + n$$

$$g : \kappa \times \{1\} \to \kappa_E \qquad g(\langle \alpha, 1 \rangle) = \lambda + 2n \quad \text{if } \alpha = \lambda + n$$

Then it is easy to see that f and g are bijections. So

$$\begin{aligned} \kappa + \kappa &= \left| (\kappa \times \{0\}) \cup (\kappa \times \{1\}) \right| \\ &= \left| \kappa_O \cup \kappa_E \right| \\ &= |\kappa| = \kappa \end{aligned}$$

and we are done.

<u>Corollary 6</u>: If at least one of the two cardinals κ and μ is infinite, then

$$\kappa + \mu = \max(\kappa, \mu)$$

<u>Proof</u>: We have

$$\begin{aligned} \max(\kappa, \mu) &\leq \kappa + \mu \\ &\leq \max(\kappa, \mu) + \max(\kappa, \mu) \\ &= \max(\kappa, \mu) \qquad \text{by Prop. 5.} \end{aligned}$$

So we must have $\kappa + \mu = \max(\kappa, \mu)$

<u>Proposition 7</u>: If κ is an infinite cardinal, then $\kappa . \kappa = \kappa$

<u>Proof</u>: First observe that the function $j : \kappa \to \kappa \times \kappa$ defined by $j(\alpha) = \langle \alpha, 0 \rangle$ is an injection. So $\kappa \leq |\kappa \times \kappa| = \kappa . \kappa$

Now suppose $\kappa < \kappa . \kappa$. Wlog we may assume that κ is the smallest infinite cardinal for which this is true. Then

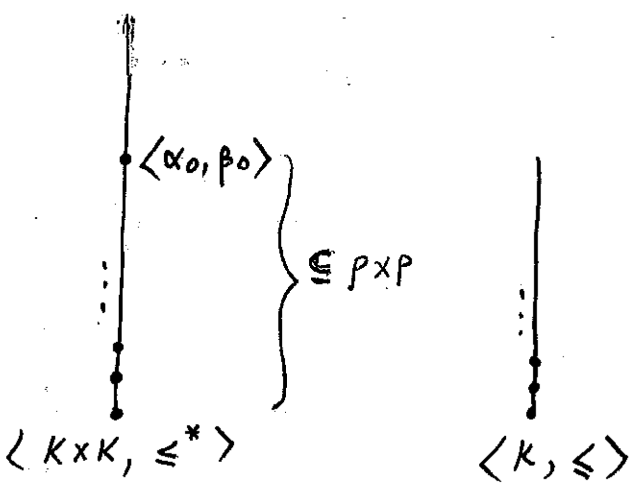
$$\mu = \mu \cdot \mu$$

for all inf. cardinals $\mu < \kappa$. Now define a well-ordering $\leq^*$ on $\kappa \times \kappa$ as follows:

$$\langle \alpha, \beta \rangle \leq^* \langle \gamma, \delta \rangle \quad \text{if} \quad \begin{array}{l} \alpha+\beta < \gamma+\delta; \text{ or} \\ \alpha+\beta = \gamma+\delta \text{ and } \alpha < \gamma. \end{array}$$

Let ζ = ordinal isomorphic to $\langle \kappa \times \kappa, \leq^* \rangle$

Then $\zeta > \kappa$ (because the $\kappa < \kappa . \kappa$ and consequently the shortest well-ordering on $\kappa \times \kappa$ has to be $> \kappa$)



So there must be an ordered pair $\langle \alpha_0, \beta_0 \rangle \in \kappa \times \kappa$ such that $\langle [\kappa \times \kappa]_{\langle \alpha_0, \beta_0 \rangle}, \leq^* \rangle \cong \langle \kappa, \leq \rangle$

Let $\rho = \alpha_0 + \beta_0 + 1$. Then $\rho < \kappa$ and

$$[\kappa \times \kappa]_{\langle \alpha_0, \beta_0 \rangle} \subseteq \{ \langle \gamma, \delta \rangle : \ \gamma < \rho \text{ and } \delta < \rho \} = \rho \times \rho$$

$$|\rho \times \rho| = |\rho| \cdot |\rho| = |\rho| \quad (\text{bec. } |\rho| < \kappa)$$

So $|\rho \times \rho| < \kappa$. But this contradicts the fact that $\langle [\kappa \times \kappa]_{\langle \alpha_0, \beta_0 \rangle}, \leq^* \rangle \cong \langle \kappa, \leq \rangle$. Hence we must have $\kappa = \kappa . \kappa$ for all infinite cardinals κ.

Corollary 8: If κ & μ are > 0 and at least one of them is infinite, then
$$\kappa \cdot \mu = \max(\kappa, \mu)$$

Proof: Do for H.W.

Proposition 9: For any cardinal κ

(a) $2^{\kappa} = |\mathcal{P}(\kappa)|$

(b) $\kappa < 2^{\kappa}$

Proof: (a) By definition we know that $2^{\kappa} = |\mathcal{F}(\kappa, 2)| = |\mathcal{F}(\kappa, \{0,1\})|$. So all we have to do is to find a bijection from $\mathcal{P}(\kappa)$ to $\mathcal{F}(\kappa, \{0,1\})$ — Do for H.W.

(b) We know from Cantor's diagonal theorem that $\kappa \prec \mathcal{P}(\kappa)$. So $|\kappa| < |\mathcal{P}(\kappa)|$. Thus $\kappa < 2^{\kappa}$.

So $2^{\aleph_0} = |\mathcal{P}(\aleph_0)|$ and $2^{\aleph_0} > \aleph_0$. Since $\aleph_1$ is the first cardinal $> \aleph_0$, we see that $2^{\aleph_0} \geq \aleph_1$. This is all we can say.

It is possible to have $2^{\aleph_0} = \aleph_1$ in one universe and $2^{\aleph_0}$ $\aleph_4$ in another universe. But $2^{\aleph_0}$ cannot be "any thing" $> \aleph_0$. We can't have $2^{\aleph_0} = \aleph_\omega$.

<u>Lect #19</u> We know that $\mu \cdot \mu = \mu$ for any inf. card. So by repeatedly using this fact we can see that for $n \in \mathbb{N}$

$$\mu^n = \mu \cdot \mu \cdots \mu \quad (n \text{ times})$$
$$= \mu .$$

The basic question about cardinal exponentiatio[n] then becomes:

What is μ^κ, if κ is infinite?

<u>Def.</u> The <u>successor</u> of a cardinal κ is defined by

$$\kappa^+ = \text{"smallest cardinal } > \kappa\text{"}$$

A cardinal κ is called a <u>successor cardinal</u> if $\kappa = \mu^+$ for some cardinal μ. If κ is not a succ. card., we say it is a <u>limit cardina[l]</u>

<u>Ex.</u> $\aleph_1, \aleph_2, \aleph_3, \ldots, \aleph_{\omega+6}, \ldots, \aleph_{\omega_1+1}, \ldots$ are all succ. card.

$\aleph_0, \aleph_\omega, \aleph_{\omega \cdot 2}, \aleph_{\omega_1}$ are all limit cardina[ls]

<u>Proposition 10</u>: If κ is an infinite cardinal, then $\mu^\kappa = 2^\kappa$ for all $2 \leq \mu \leq \kappa^+$

<u>Proof:</u> First observe that since $\mu \geq 2$, $\mathcal{F}(\kappa, 2) \subseteq \mathcal{F}(\kappa, \mu)$.

So $2^\kappa = |\mathcal{F}(\kappa, 2)|$
$\leq |\mathcal{F}(\kappa, \mu)| = \mu^\kappa$

Thus $2^\kappa \leq \mu^\kappa$

Similarly
$$\begin{aligned} \mu^\kappa &\leq (\kappa^+)^\kappa && \text{bec. } \mu \leq \kappa^+ \\ &\leq (2^\kappa)^\kappa && \text{bec. } \kappa^+ \leq 2^\kappa \\ &= 2^{\kappa \cdot \kappa} && \text{by Prop. 4.9(d)} \\ &= 2^\kappa && \text{bec. } \kappa \cdot \kappa = \kappa \end{aligned}$$

Thus $\mu^\kappa \leq 2^\kappa$

Hence $\mu^\kappa = 2^\kappa$ and we are done.

So we would really like to know what is 2^κ for κ infinite. (We would also like to know what is μ^κ if $\mu > \kappa^+$ - but this a more complicated problem.)

Cantor thought that $2^{\aleph_0} = \aleph_1$, but he couldn't prove this.

<u>Continuum Hypothesis</u> (CH): $2^{\aleph_0} = \aleph_1$

It can be shown that CH is independent of ZFC. This means that there some universes ~~of~~ ZFC in which CH is true and some in which CH is false.

<u>Generalised Continuum Hypothesis</u> (GCH):
For each α, $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

<u>Def.</u> We define the <u>cofinality</u> of a limit ordinal λ by

$cof(\lambda) =$ smallest ordinal θ such that there is a seq. $\langle \alpha_\beta : \beta < \theta \rangle$ of <u>ordinals in λ</u> such that $\sup\{\alpha_\beta : \beta < \theta\} =$

<u>Ex.</u>

1. Consider $\omega \cdot 2$. We know that
$$\omega, \omega+1, \omega+2, \omega+3, \ldots = \langle \omega+n : n<\omega \rangle$$
is a sequence ordinals in $\omega \cdot 2$ with limit $\omega \cdot 2$. Since no shorter sequence will produce $\omega \cdot 2$, $cof(\omega \cdot 2) = \omega$.

2. Consider ω_ω. We know that
$$\langle \omega_n : n<\omega \rangle = \omega_0, \omega_1, \omega_2, \ldots$$
is a seq. of ordinals in ω_ω with limit ω_ω. Again no shorter seq. will produce ω_ω, so $cof(\omega_\omega) = \omega$.

3. Consider ω_1. We know that
$$\omega_1 = \sup\{\alpha : \alpha < \omega_1\}$$
and no shorter seq. will produce ω_1. (bec. if $\omega_1 = \sup\{\alpha_\beta : \beta < \theta\}$ and $\alpha_\beta \in \omega_1$ and $\theta < \omega_1$, then
$$\omega_1 = \bigcup_{\beta<\theta} \alpha_\beta = \text{countable union of countable sets}$$
and ω_1 would be countable. But we know ω_1 is uncountable).

So $cof(\omega_1) = \omega_1$.

Proposition 11: $\mathrm{cof}(\lambda)$ is always a cardinal.

Proof: Let $\theta = \mathrm{cof}(\lambda)$. Supp. θ is not a cardinal. Then $|\theta| < \theta$. Now by def. of $\mathrm{cof}(\lambda)$, we can find a seq. $\langle \alpha_\beta : \beta < \theta \rangle$ of ordinals in λ s.t. $\lambda = \sup\{\alpha_\beta : \beta < \theta\}$.

Let $\kappa = |\theta|$ and $i : \kappa \to \theta$ be a bijection. Then $\langle \alpha_{i(\beta)} : \beta < \kappa \rangle$ is a seq. of ord. in λ with

$$\sup \langle \alpha_{i(\beta)} : \beta < \kappa \rangle = \lambda.$$

So $\mathrm{cof}(\lambda) \leq \kappa < \theta$. But this contradicts the fact that $\mathrm{cof}(\lambda) = \theta$. Hence θ must be a cardinal.

Def. A cardinal κ is said to be regular if $\mathrm{cof}(\kappa) = \kappa$, and singular if $\mathrm{cof}(\kappa) < \kappa$.

Theorem 12: If κ is a successor cardinal, then κ is regular.

Proof: Supp. κ is a succ. cardinal. Then $\kappa = \mu^+$ for some cardinal μ.

Now suppose $\mathrm{cof}(\kappa) = \theta < \kappa$. Then we can find a seq. $\langle \alpha_\beta : \beta < \theta \rangle$ of ordinals in κ such that

$$\sup\{\alpha_\beta : \beta < \theta\} = \kappa.$$

Now for each β, $|\alpha_\beta| < \kappa$, so $|\alpha_\beta| \leq \mu$.
Also $|\theta| < \kappa$, so $|\theta| \leq \mu$.
Thus

$$\begin{aligned} \left| \bigcup_{\beta<\theta} \alpha_\beta \right| &\leq \sum_{\beta<\theta} |\alpha_\beta| \\ &\leq \sum_{\beta<\theta} \mu \\ &= \mu . |\theta| \\ &\leq \mu . \mu = \mu \end{aligned}$$

Hence

$\left| \bigcup_{\beta<\theta} \alpha_\beta \right| \leq \mu < \kappa$ which contradicts the fact that

$$\bigcup_{\beta<\theta} \alpha_\beta = \kappa .$$

So $cof(\kappa) = \kappa$.

<u>Qu:</u> Is there a <u>limit cardinal</u> which is regular?
<u>Ans:</u> Yes. ω.

<u>Qu:</u> Is there any more? We don't know

<u>Def.</u> A cardinal κ is said to be <u>weakly-inaccessible</u> if
(i) $\kappa > \aleph_0$,
(ii) κ is regular, and
(iii) κ is a limit cardinal
[i.e. $(\forall \mu < \kappa)(\mu^+ < \kappa)$]

<u>Def.</u> A cardinal κ is said to be <u>strongly-inaccessible</u> if
(i) $\kappa > \aleph_0$,
(ii) κ is regular, and
(iii) $(\forall \mu < \kappa)(2^\mu < \kappa)$.

Lect. #20 Recall that a cardinal κ is strongly inaccessible if

(i) $\kappa > \aleph_0$

(ii) κ is regular, and

(iii) $(\forall \mu < \kappa)\ (2^\mu < \kappa)$.

Models of ZFC

1. $\langle V_\omega, \in \rangle$: satisfies all of ZFC except Inf. Ax.

2. $\langle V_{\omega+\omega}, \in \rangle$ satisfies all of ZFC except Repl. Ax. More generally if λ is any limit ord. $> \omega$, then $\langle V_\lambda, \in \rangle$ satisfies all of ZF except Repl. Ax

3. $\langle V_\kappa, \in \rangle$ satisfies all of ZFC if κ is strongly inaccessible.

König's Theorem: Suppose $\langle \kappa_i \rangle$ and $\langle \mu_i \rangle$ are seq. of cardinals such that $\kappa_i < \mu_i$ for each $i \in I$. Then

$$\sum_{i \in I} \kappa_i < \prod_{i \in I} \mu_i$$

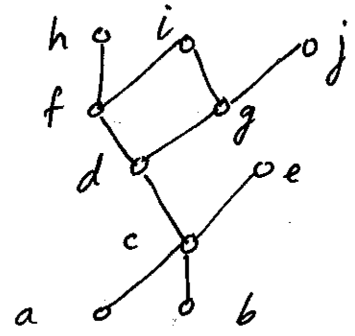
Proof: See textbook p. 190-191

Corollary: For any α, $\operatorname{cof}(2^{\aleph_\alpha}) > \aleph_\alpha$.

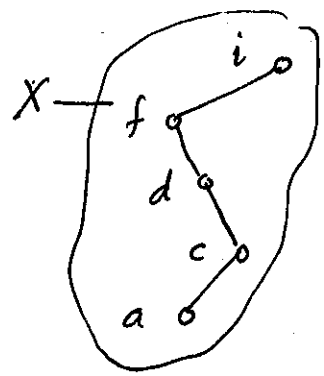
Proof: Let $\theta = \operatorname{cof}(2^{\aleph_\alpha})$. Supp. $\theta \leq \aleph_\alpha$.
Then we can find a seq. $\langle \kappa_\beta : \beta \in \theta \rangle$ with $\kappa_\beta < 2^{\aleph_\alpha}$ s.t. $2^{\aleph_\alpha} = \sum_{\beta < \theta} \kappa_\beta$. So by König's Thm. $\sum_{\beta<\theta} \kappa_\beta < \prod_{\beta<\theta} (2^{\aleph_\alpha})$
So $2^{\aleph_\alpha} < (2^{\aleph_\alpha})^\theta \leq (2^{\aleph_\alpha})^{\aleph_\alpha} = 2^{\aleph_\alpha}$ a contradiction. $\therefore$ results follow.

Lect #20 **Def.** Let $\langle A, \leq \rangle$ be a partially ordered set. A subset $X \subseteq A$ is said to be a <u>chain</u> in A if $\langle X, \leq \rangle$ is linearly ordered.

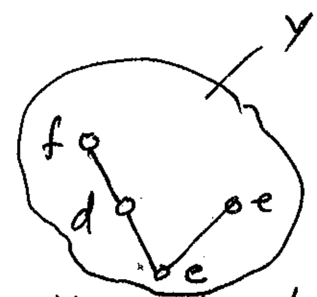
Ex.



$\langle A, \leq \rangle$



X is a chain A.



Y is <u>not</u> a chain

Recall that an element $a \in A$ was said to be <u>maximal in A</u> if there is no $b \in A$ with $a < b$.

Def. An element $b \in A$ is said to be an <u>upper bound</u> for the chain X if

$$x \leq b \quad \text{for each } x \in X.$$

<u>Zorn's Lemma</u>: Let $\langle A, \leq \rangle$ be a partially ordered set. If every chain X in A has an upper bound in A, then A has a maximal element.

Example

Recall that V_ω was equal to the collection of all heriditarily finite sets. Not every chain in V_ω has an upper bound. So we shouldn't expect V_ω to have a maximal element. And V_ω indeed has no maximal element.

Proposition 13: AC $\Rightarrow$ Zorn's Lemma

Proof: We will prove that WOP $\Rightarrow$ Zorn's Lemma. Since WOP $\Leftrightarrow$ AC the result will follow.

Supp. WOP is true. Let $(A, \leq)$ be a partially ordered set in which every chain X has an upper bound. Since WOP is true we can find a bijection $f: \beta \to A$ for ordinal β. Now ~~for~~ each $\alpha \in \beta$, define a chain X_α by

$$X_0 = \{f(0)\}$$

$$X_\alpha = \begin{cases} \left(\bigcup_{\gamma < \alpha} X_\gamma\right) \cup \{f(\alpha)\} & \text{if } x < f(\alpha) \text{ for each } x \text{ in } \bigcup_{\gamma<\alpha} X_\gamma \\ \left(\bigcup_{\gamma<\alpha} X_\gamma\right) & \text{otherwise.} \end{cases}$$

Then $X = \bigcup_{\alpha<\beta} X_\alpha$ will be a chain in A. So we can find an element $b \in A$ which is an upper bound for X. This b must be a maximal element of A bec. of the def. of X

Def. A vector space is an ordered 4-tuple $\langle V, F, +, \cdot \rangle$ where $V \neq \emptyset$, F is a field, and $+ : V \times V \to V$ is a binary operation (called vector addition) and $\cdot : \times V \to V$ is a binary operation (called scalar mult.) such that the following hold.

1. $(u + v) + w = u + (v + w)$ $\qquad u, v, w \in V$
2. $u + v = v + u$
3. $\exists$ an element $\underline{0} \in V$ such that $\underline{0} + u = \underline{u}$
4. For each $u \in V$, $\exists$ $v \in V$ such that $u + v = \underline{0}$
5. $1 . v = v$
6. $(a + b) . v = a . v + b . v$ $\qquad a, b \in F$
7. $(ab) . v = a . (b . v)$
8. $a(u + v) = a . u + a . v$

Def. Let $\mathcal{U} \subseteq V$. The span of $\mathcal{U}$ is defined by $\text{span}(\mathcal{U}) = \{ v : v = c_1 u_1 + \cdots + c_k u_k$ for some $u_1, \ldots, u_k \in \mathcal{U}$ and $c_1, \ldots, c_k \in \mathbb{R} \}$

Def. Let $\mathcal{U} \subseteq V$. We say that $\mathcal{U}$ is linearly independent if there is no $u_1, \ldots, u_k$ in $\mathcal{U}$ such that $c_1 u_1 + \cdots + c_k u_k = \underline{0}$ and $\langle c_1, \ldots, c_k \rangle \neq \langle 0, \ldots, 0 \rangle$.

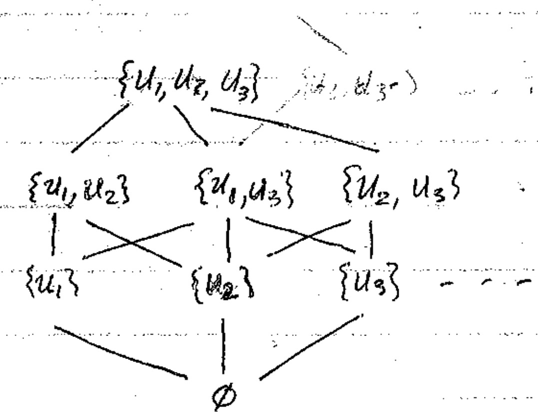
Def. A subset $\mathcal{U}$ of V is said to be a basis of V if

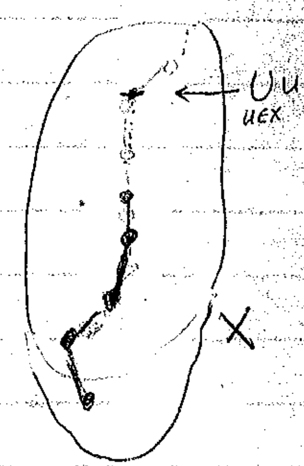
1. $\text{span}(\mathcal{U}) = V$ and
2. $\mathcal{U}$ is linearly independent.

Theorem (AC) Every vector space has a basis (This cannot be proved without AC)

Proof: The proof will use "Zorn's lemma". Let P be the collection of all linearly independent subsets of V. We want to find an element U_0 of P such that $\text{span}(U_0) = V$. First observe that $\langle P, \subseteq \rangle$ is a poset.

Now let X be a chain in P





Then $\bigcup_{U \in X} U$ is an upper bound for X.

So every chain X in P has an upper bound in P. Hence by Zorn's lemma, it follows that P has a maximal element U_0. We claim that U_0 is a basis of V.

Suppose $\text{span}(U_0) \neq V$. Then we can find an element $w \in V$ such that $w \notin \text{span}(U_0)$. But then $U_0 \cup \{w\}$ will be linearly indep. and this contradicts the fact that U_0 was a maximal element of U_0. Hence $\text{span}(U_0) = V$ and so U_0 is a basis of V.

Lect. #21

SOME OTHER EQUIVALENTS OF AC

AC is equivalent to each of the following statements

1. The Power set of every ordinal can be well-ordered
2. For all infinite cardinals κ, $\kappa \cdot \kappa = \kappa$
3. For all infinite cardinals μ & κ, $\kappa + \mu = \kappa \cdot \mu$

SOME WEAKER VERSIONS OF AC

1. AC_ω – The axiom of choice for countable sets
Every countable set of non-empty sets has a choice function.

It can be shown that

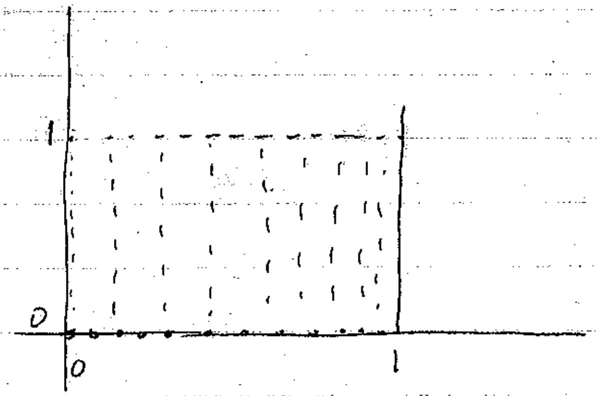
1. $AC_\omega \Rightarrow$ Any countable union of countable sets is countable
2. $AC_\omega \Rightarrow$ $\aleph_1$ is a regular cardinal
3. $AC_\omega \Rightarrow$ every infinite set has a countably infinite subset.

2. DC_ω (axiom of ω dependent choice)
Let A be a set, $u \in A$, and R be a relation on A. If for every $x \in A$, there is a $y \in a$ such that xRy, then there is a seq. $\langle z_n : n < \omega \rangle$ of elements of A such that

$$z_0 = u \quad \text{and}$$
$$z_n R z_{n+1} \quad \text{for all } n \in \omega.$$

Fact: $AC \Rightarrow DC_\omega \Rightarrow AC_\omega$. The converses are not true.

Areas. Let $f(x) = \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x \in \mathbb{R} \sim \mathbb{Q} \end{cases}$



Let $A = \{\langle x, y \rangle : 0 \leq y \leq f(x) \text{ and } x \in [0,1]\}$

Qu: What is the "area" of A?

Note: f is not Riemann-integrable, so we cannot find the area of A by using the formula Area $(A) = \int_0^1 f(x)\,dx$.

Ans: Area $(A) = 0$.

Let $\varepsilon > 0$ be given. ~~List the elements of Q in some order~~ Since $\mathbb{Q}$ is countable we can list the elements of $\mathbb{Q}$ as a sequence $r_1, r_2, r_3, \dots$

Now cover the vertical line over r_1 by a thin rectangle of length 1 and width $\frac{\varepsilon}{2}$. In general cover the line over r_n by a rectangle of length 1 and width $\frac{\varepsilon}{2^n}$. Then A can be completely covered by strips of total area $\frac{\varepsilon}{2} + \frac{\varepsilon}{4} + \dots + \frac{\varepsilon}{2^n} + \dots = \varepsilon$.

So Area $(A) \leq \varepsilon$. Since this is true for all $\varepsilon > 0$, it follows that Area $(A) = 0$.

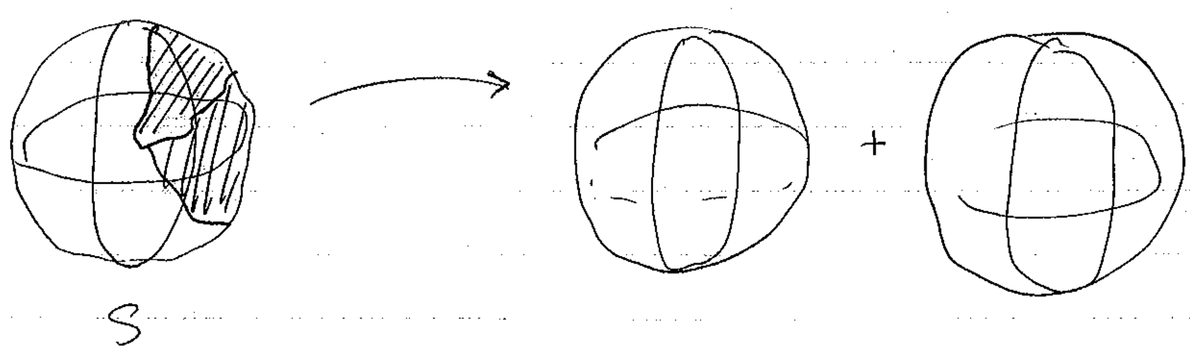
We have not defined what "area" means — but "area" should clearly satisfy the following

1. Area $(A) \geq 0$ for each $A \subseteq$ unit square
2. Area (unit sq.) $= 1$
3. If $B \subseteq A$, then area $(B) \leq$ area(B)
4. If $\langle A_n \rangle_{n \in \mathbb{P}}$ is a seq. of pairwise disjoint subsets of the unit sq., then
$$\text{area}\left(\bigcup_{n \in \mathbb{P}} A_n\right) = \sum_{n=1}^{\infty} \text{area}(A_n)$$

Fact: It can be shown, by using AC, that there are subsets of the unit square which cannot be assigned an "area" as long as "area" satisfies properties 1–4.

Banach-Tarski Paradoxical Decomposition

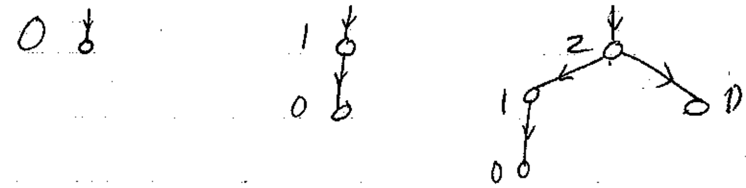
Let $S = \{\langle x, y, z\rangle : x^2 + y^2 + z^2 \leq 1\}$ be the unit sphere. It can be shown, by using AC, that we can partition S into a finite number of pieces and then rearrange these pieces and form two unit spheres.



Non-well-founded Sets

One way of representing sets is by using rooted digraphs.

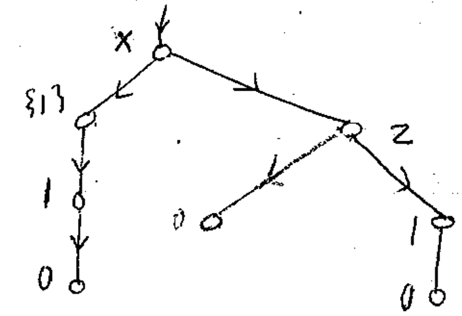
Examples



An edge from u to v in G means that v is an element of G. The root tells you the set that is defined.

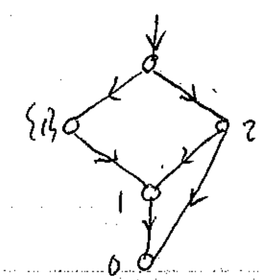
Note by the Ax. of Foundation, we cannot have any directed cycles or loops in the digraph.

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



Note: Any rooted digraph which has no directed cycles or loops will produce a set. A set can be represented by many rooted digraph.

For example: $\{\{1\}, 2\} =$



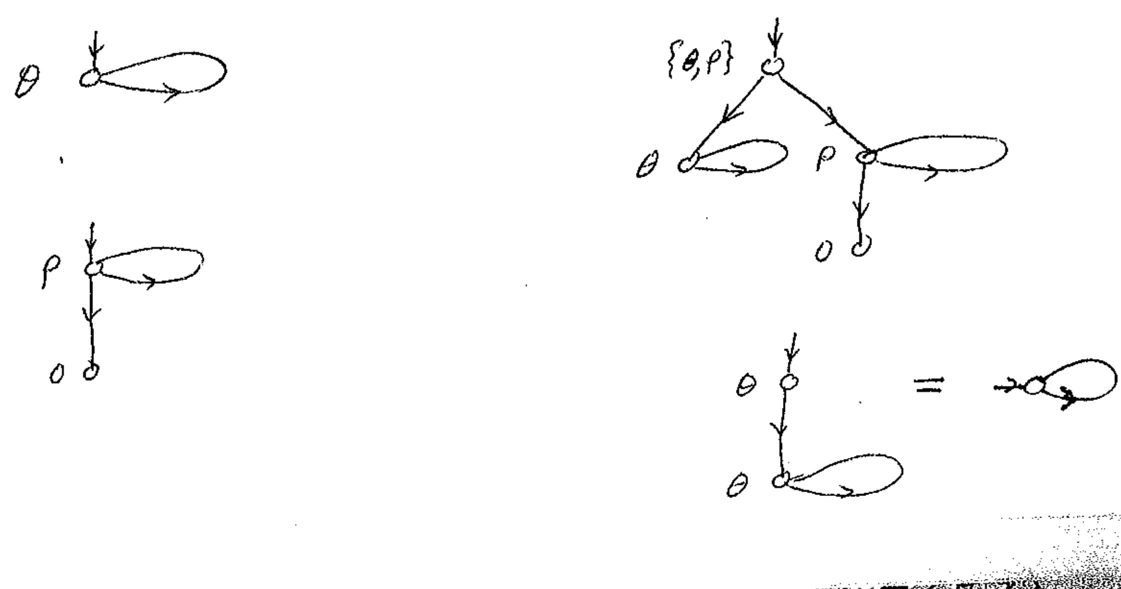
Qu: How can we tell if two digraphs represent the same set

Def. A digraph $G = \langle V, E \rangle$ is an ordered pair in which V is a non-empty set of objects called vertices and E is a set of ordered pairs of elements of V. The elements of E are called (directed) edges

Def. A pseudo-set is an ordered pair $\langle G, v_0 \rangle$ where G is a digraph and v_0 is a distinguished vertex in G called the root, i.e. a pseudoset is a rooted digraph

Note: All sets are pseudo-sets because we can show that any set can be represented by a rooted digraph

Some non-well-founded sets

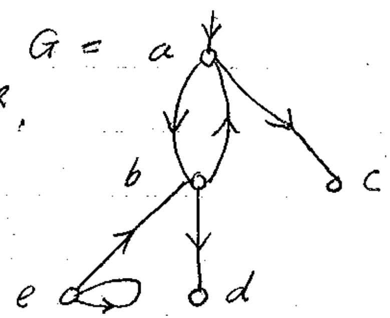


How to determine if $\langle G, v_0 \rangle$ and $\langle H, u_0 \rangle$ are the same pseudo-set.

Basic idea

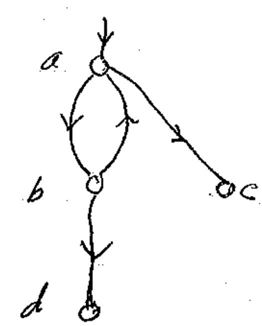
1. Remove all vertices in G and H which are not <u>accessible</u> from v_0 and u_0 resp. This will produce two new rooted digraphs $\langle G', v_0 \rangle$ and $\langle H', u_0 \rangle$.
2. Reduce $\langle G', v_0 \rangle$ and $\langle H', u_0 \rangle$ to minimal digraphs $\langle G^R, v_0 \rangle$ and $\langle H^R, u_0 \rangle$ by removing all redundant vertices.
3. Check if $\langle G^R, v_0 \rangle \cong \langle H^R, u_0 \rangle$.

<u>Example</u>: Let $G =$



We will find G^R.

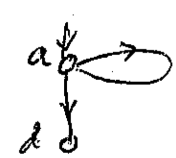
$G' =$



First e is inaccessible from ~~root~~ a.

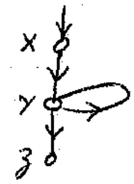
P_0 : $\{a, b, c, d\}$

P_1 : $\{a, b\}\{c, d\}$ $\longrightarrow$ $G^R =$



P_2 : $\{a, b\}\{c, d\}$

<u>Qu</u>: Is $\langle G, a \rangle = \langle H, x \rangle$? $H =$



<u>For H</u>: P_0 : $\{x, y, z\}$

P_1 : $\{x, y\}\{z\}$ $\longrightarrow$ $H^R = H$.

P_2 : $\{x\}\{y\}\{z\}$

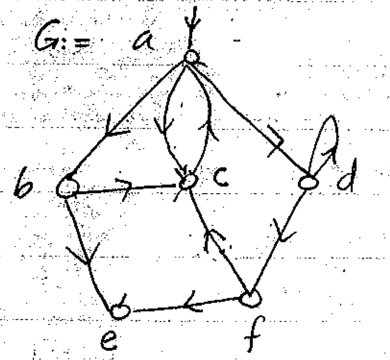
$\therefore$ $\langle G^R, a \rangle \not\cong \langle H^R, x \rangle$ So $\langle G, a \rangle \neq \langle H, x \rangle$

Partition Algorithm

1. Let V = set of vertices of G. Put
$P_0 = V$ and
$P_1 = \{v \in V : \text{outdeg}(v) > 0\}, \{v \in V : \text{outdeg}(v) = 0\}$
2. If $P_{\alpha+1} = P_\alpha$ for some $\alpha \geq 0$ STOP

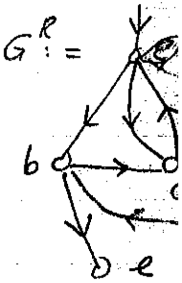
3. Now define $P_{\alpha+1}$ from P_α as follows:
The vertices a and b will be in the same block of $P_{\alpha+1}$ if
   1. a and b are in the same block of P_α
   2. If a has an edge to an element in a block of P_α, then b must have an edge an element of the same block; and vice versa
4. If λ is a limit ordinal and P_α has been defined for all $\alpha < \lambda$, define P_λ follows:
a and b are in the same block of P_λ iff a & b are in the same block of P_α for each $\alpha < \lambda$.
5. Go to step 2.

Ex: $G :=$



$P_0 : \{a, b, c, d, e, f\}$
$P_1 : \{a, b, c, d, f\} \ \{e\}$
$P_2 : \{a, c, d\} \{b, f\} \ \{e\}$
$P_3 : \{a, d\} \{c\} \{b, f\} \ \{e\}$
$P_4 : \{a\}\{d\} \{c\} \{b, f\} \ \{e\}$
$P_5 : \{a\}\{d\}\{c\} \{b, f\} \ \{e\}$

$G^R =$



Lect. #23 Forcing and the Continuum Hypothesis

V = universe of all sets
L = universe of all sets which we are forced to have so that all the ZFC axioms are satisfied.

Godel (1938): $\langle L, \in\rangle$ is a model of the ZFC axioms. In $\langle L ; \in\rangle$, GCH is also true.

So we have $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ (for each $\alpha \in \Omega$) in L. In particular $2^{\aleph_0} = \aleph_1$ in L.

Question: Is $V = L$? Ans: We don't know

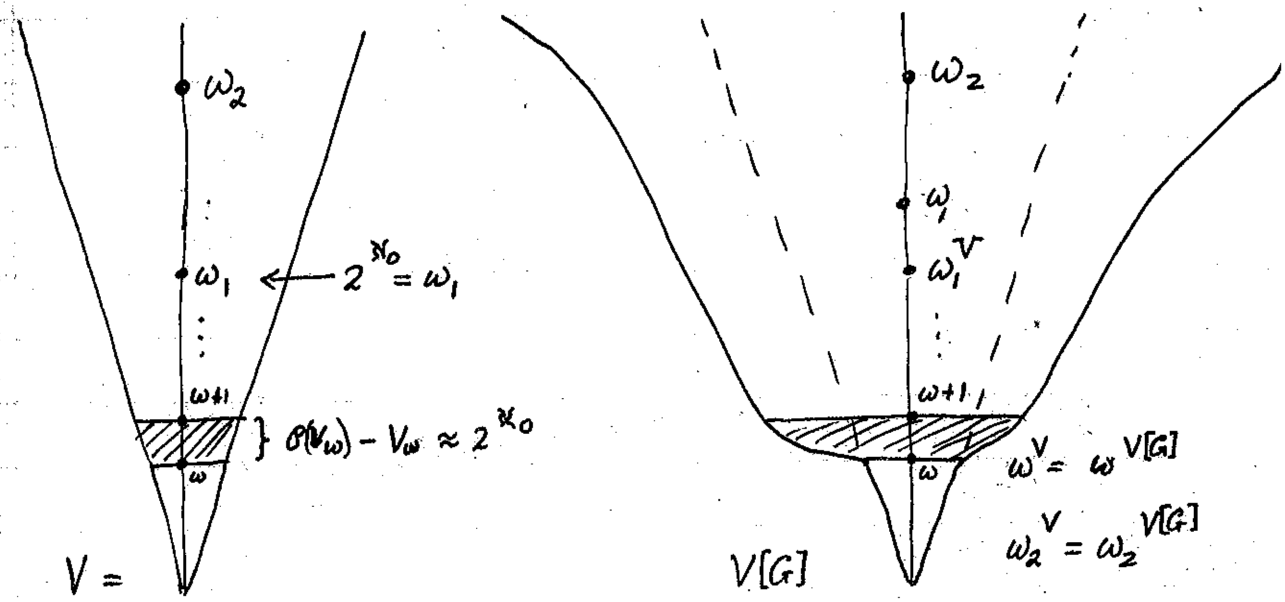
1. We could add "$V=L$" as an axiom. Then we would have $\langle L,\in\rangle$ is a model of ZFC + "$V=L$"

2. We could add an axiom call MC = There exists a measurable cardinal. Then we have
Scott (1961) ZFC + MC $\Rightarrow$ $V \neq L$.
[A measurable cardinal is $^1/_y$ an extremely huge strongly inaccessible cardinal.]

Question: Can $2^{\aleph_0} = \aleph_2$. Ans: Yes.

Cohen (1963): There is a model $\langle M, \in\rangle$ in which $2^{\aleph_0} = \aleph_2$.

Cohen used the <u>method of forcing</u> to prove that $2^{\aleph_0}$ can be equal to $\aleph_2$ in some models. He made a model $V[G]$ in such a way that $2^{\aleph_0}$ is forced to be $\aleph_2$. Start with a model V.



The empty set of V must be the same thing in $V[G]$. In fact the collection of all <u>heriditarily finite sets</u> in V will be the same as those in $V[G]$. Also $\omega^V = \omega^{V[G]}$

In V we know $\omega_1 = 2^{\aleph_0} \approx \mathcal{P}(V_\omega)$ (take $V = L$)
In $V[G]$ we have more sets. Some of these new sets will be bijections from ω_1^V to ω^V. Since $\omega_1 > \omega$, these bijections don't exist in V.

Cohen use partial functions from ω to ω_2 in V to end up with a limiting function out of V which maps ω^V to ω_1^V in $V[G]$. Cohen also had to make sure $\mathcal{P}(V_\omega^{[G]}) \approx \omega_2$. This gave $2^{\aleph_0} = \aleph_2$ (in $V[G]$).