Set Theory I

Yeheli Fomberg

Contents

1 Permutations

Permutation σ is a bijection from a set S onto iteself.
Every permutation can be decomposed into one or more disjoint cycles(or orbits), thus, they can also be defined by them like this:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (3\ 4)(1\ 2\ 5)$$

1. A cycle of one element is call a **fixed point**
2. A permutation without fixed points is called a **derangement**
3. A permutation that's an orbit of 2 elements is called a **transposition**

1.1 The symmetric group

A symmetric group defined over a set is the group whose elements are all the permutation over the set, and whose group operation is the composition of functions.

Reminder: A group is an algebric structure with the following charachteristics:

- Closure
- Associativity
- An Idenentity permutation exists
- $\forall \sigma \in S_n (\exists \pi : \sigma \circ \pi = Id)$

2 Hall's theorem

Hall's theorem - *In a finite bipartite graph* $G(X, Y, E)$
$\forall W \subseteq X(|W| \leq |N_g(W)|) \iff$ *An* X*-perfect matching exists.*

($\Leftarrow$) Suppose we have an X perfect matching M, since for any given W all vertices in W have a distinct matching vertice in Y by M we get

$$\forall W \subseteq X(|W| \leq |N_g(W)|)$$

($\Rightarrow$) We'll prove by contradiction. Assume an X-perfect matching doesn't exist, we'll denote the maximal matching M,and the sets of vertices in X, Y that appear in M as S, T. An X-perfect matching doesn't exist $\Rightarrow X \setminus S \neq \emptyset$, so we can choose a vertice $u_0 \in X \setminus S$ and consider all alternating paths of the form $P = (u_0, v_1, v_2, \ldots)$ such that odd edges are not in M and even edges are in M. Denote:

$$A = \{u : u \in P \wedge u \in X\}, \quad B = \{v : v \in P \wedge v \in Y\}$$

We know every vertice in B is matched by M to a vertice in A because otherwise we could create a bigger matching by toggling whether each of the edges belong to M or not.

$$\Rightarrow |B| \leq |A \setminus \{u_0\}| \Rightarrow |B| < |A|$$

but also for any vertice in $a \in A$ any of its neighbors b are in B. We can show that an alternating path to b exists either by removing the matched edge ab from the alternating path to a, or by adding the unmatched edge ab to the alternating path to a.

$$\Rightarrow B = N_g(A)$$

$$\Rightarrow |N_g(A)| < |A|$$

That's a contradiction so an X-perfect matching must exist.

3 Cantor's theorem

$$|A| < |P(A)|$$

We can define $f : A \to P(A)$ as such

$$f(a) = a$$

$$\Rightarrow |A| \leq |P(A)|$$

Assume $|A| = |P(A)|$. That means there's a bijection $g : A \to P(A)$.
consider the following set:

$$D = \{a : a \notin g(a)\}$$

Since g is a bijection $\exists b \in A : f(b) = D$. Now look at the different cases:

$$\begin{cases} b \in D, & b \notin g(b) = D \Rightarrow \textit{contradiction} \\ b \notin D = g(b), & b \in D \Rightarrow \textit{contradiction} \end{cases}$$

Therefore $|A| \neq |P(A)| \Rightarrow |A| < |P(A)|$

4 Equivalence Relations

An equivalence relation is a binary relation(a set of ordered pairs) that is

- Reflexive
- Symmetric
- Transitive

4.1 Some Terminology

Suppose we have an equivalnce relation R on a set X:

Equivalence Class: $[a]_R = \{b \in X : bRa = 1\}$
Quotient Set: $X/R = \{[a]_R : a \in X\}$
Projection: The projection of R is $\pi : X \to X/R$ such that $\pi(x) = [x]_R$
A Cut: A cut of X is a set with only one element of each Equivalence class.

Equivalence relations can be defined by their Quotient set. Thus they can also be defined by a function or a partition. The numbers of partitions of a set $|X| = n$ are known as Bell's numbers and can be calculated recursivly as such:

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

Think why.

5 Kőnig's Theorem

Kőnig's Theorem - *For an index set I, suppose $\forall i \in I$ and κ_i, λ_i we know* $\kappa_i < \lambda_i$ then $\sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i$
We'll show this by proving for any

$$f : \sum_{i \in I} B_i \to \prod_{i \in I} C_i \quad |B_i| = \kappa_i, |C_i| = \lambda_i$$

That f is not surjective. Let's define the function f_i as such:

$$f_i : B_i \to C_i$$

$$f_i(x) = f(x)_i$$

$\forall i \in I(|B_i| < |C_i|) \Rightarrow \forall i \in I(f_i \text{ is not surjective}) \Rightarrow \exists c_i \in C_i \setminus Imf_i$
Consider the vector:

$$\hat{c} = < c_i : i \in I >$$

If $\hat{c} \in Imf \Rightarrow \exists i \in I, b \in B_i : f(b) = \hat{c}$
$\Rightarrow f(b)_i = c_i \Rightarrow f_i(b) = c_i$ but $c_i \in C_i \setminus Imf_i$
That's a contradiction so we got

$$|\sum_{i \in I} B_i| < |\prod_{i \in I} C_i| \Rightarrow \sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i$$

6 Partial Orders

A **Weak/Non-Strict** Partial Order is a homogeneous relation $\leq$ on a set P that is:

- Reflexive
- Antisymmetric[1]
- Transitive

A **Strong/Strict Partial** Order is a homogeneous relation $<$ on a set P that is:

- Irreflexive
- Asymmetric[2]
- Transitive

note: $< \bigcup \leq_{Id} = \leq$

7 Partially Ordered Sets

A Partially Ordered Set(aka a poset) is a set on which a partial order is defined $(A, \leq)$. We say two elements $a, b \in A$ are comparable $\iff a \leq b \vee b \leq a$
If two elements are incomparable they're linearly independent. A **linear/total order** is a partial order under which every pair of elements is comparable. All ordered subsets(chains) are linearly independent of each other.

7.1 Extrema

Greatest Element - *an element that's comparable and greater than all other elements*
Maximal Element - *an element that doesn't have a greater element than him*
Upper/Lower Bounds in sets - *a is a bound in A of* $B \subseteq A$ *if* $a \in A \wedge \forall b \in B(b \leq a)$

7.1.1 About Lattices

Let A be a partially ordered set:
A is a lattice $\iff \forall S \subseteq A(|S| = 2 \Rightarrow SupS, InfS \quad \text{exist})$

[1] $a \leq b \wedge b \leq a \Rightarrow a = b$
[2] $a < b \Rightarrow \neg b < a$

8 Cardinals

Cardinal numbers are the "numbers" we use to represent the cardinality of sets. Their "size". All cardinal numbers are based on the size of $\mathbb{N}$ that is $\aleph_0$. This subject is rather simple, yet hard to start from scratch. Thus I encourage you to try to prove the following:

1. $|\mathbb{N}| < |\mathbb{R}|$
2. $\aleph_0 = \aleph_0 + n = \aleph_0 \times n = \aleph_0 \times \aleph_0 = |\mathbb{Z}| = |\mathbb{Q}|$
3. $\aleph = 2^{\aleph_0} = |(0,1)^{\aleph_0}| = \aleph \times \aleph_0 = \aleph \times \aleph = |(0,1)| = |[0,1]|$
4. A plane can't be covered by $\aleph_0$ lines.
5. Let A be an infinte set, $\exists S \subseteq A : |S| = \aleph_0$
6. $\aleph = |P(\mathbb{N})| = |P(\mathbb{Q})|$
7. let A = {The set of all finite subsets of $\mathbb{N}$} prove $|A| = \aleph_0$
8. $\aleph_0^{\aleph} = \aleph$
9. $|\mathbb{R}^{\mathbb{R}}| = |P(\mathbb{R})| = 2^{\aleph}$
10. |The disjoint union of $\mathbb{N}$ sets of size $\mathbb{N}$|= $\aleph_0$
11. $\aleph_0^{\aleph_0} = \aleph$
12. |The set of all invertible functions $\mathbb{R} \to \mathbb{R}$|= $2^{\aleph}$
13. $|A| =$ |The set of all algebric numbers| $= \aleph_0$
14. $|B| = |\mathbb{R} \setminus A| =$ |The set of all transcedental number| $= \aleph$
15. |All subsets of $\mathbb{R}$ with cardinality $\aleph/\aleph_0$|
16. Let $\aleph_0$ people with a natural number of hats on their head guess how many hats they have. How many options are there, given only a finite number of people guessed right/wrong?

9 Schröder–Bernstein Theorem

Schröder–Bernstein Theorem - $|A| \leq |B| \wedge |B| \leq |A| \iff |A| = |B|$ There are more proofs that rely on similiar ideas. Here's one:
We're given two injective functions

$$f : A \to B$$

$$g : B \to A$$

Without loss of generality assume A,B are disjoint(Why can we do this?)
Considering the partially defined functions f^{-1}, g^{-1} we can create a sequence for every element of $A \bigcup B$ in the following way:

$$\dots f^{-1}g^{-1}(a) \to g^{-1}(a) \to a \to f(a) \to g(f(a)) \dots$$

The sequence can keep going forever to the right, but to the left it may stop eventually since the inverse functions are partial[1]. We can see that every element in $A \bigcup B$ has a sequence and that if an element appears in two sequnces they'll be identical since they're injective and by our construction. Thus those sequences form a partition of $A \bigcup B$ so it's sufficient to create bijections for all partitions, and we're finished. Our bijection will be:

$$h(x) = \left\{ \begin{array}{ll} f(x), & \text{for } x \in A \text{ in an A-stop} \\ g^{-1}(x), & \text{for } x \in A \text{ in a B-stop} \\ f^{-1}(x), & \text{for } x \in B \text{ in an A-stop} \\ g(x), & \text{for } x \in B \text{ in a B-stop} \end{array} \right\}$$

And of course any element of an A-stop can go one step right with f and we can get any element's left neighbor by applying f^{-1}, and so we get a bijection for any A-stop sequence. The proof for B-stops is similiar. Finally, we get that h is the bijection we looked for and that $|A| = |B|$.

[1] We'll call those who stop from the left on an element of A A-stops and the rest B-stops - even though they may not always stop!

10 Homomorphism and Isomorphosm of Ordered Sets

10.1 Homomorphisms

Let $(X, \leq_1), (Y, \leq_2)$ be partially ordered sets.

$$F \text{ is a Homomorphism } \iff \forall x_1, x_2 \in X(x_1 \leq_1 x_2 \Rightarrow F(x_1) \leq_2 F(x_2)$$

10.2 Isomorphisms

Let $(X, \leq_1), (Y, \leq_2)$ be partially ordered sets.

$$F \text{ is an Isomorphism } \iff F : X \to Y \text{ is a bijection} \wedge \forall x_1, x_2 \in X(x_1 \leq_1 x_2 \Rightarrow F(x_1) \leq_2 F(x_2)$$

An isomorphism is reflexive, symmetric and transitive so it's an equivalnce relation.
If F is an Isomorphism and the orders are total orders, F^{-1} is also an isomorphism.

10.3 Lexicographic Order

Also known as a Dictonary Order, is an order That's defined as such:

$$(x_1, y_1) \leq (x_2, y_2) \iff x_1 <_x x_2 \vee (x_1 = x_2 \wedge y_1 \leq_y y_2)$$

This is a partial order on $X \times Y$

11 Zorn's Lemma

Zorn's lemma - *Let F be a non-empty poset. If for every chain*[1] *in F exists an upper bound in F, then F has at least one maximal element.*

11.1 Proof All Vector Spaces Have a Base

Let V be a vector space: If $V = \{0\}$ then $\emptyset$ is its basis. If V is finitely generated then we can add vectors from V to $\emptyset$ until it's spanning V. Suppose V is not finitely generated, let's Define F as the set of all linearly independant sets of vectors. F is partially ordered by the order of inclusion of sets. Let $C = (A_i)_{i \in I}$ be a chain in F, $A = \bigcup_{i \in I} A_i$. A is clearly a maximal element of the chain. Let's prove it's in F. Assume A isn't in $F \Rightarrow$ there exists a finite series of linearly dependent vectors, each is an element of a finite series of elements of C. Since that series is finite, and linearly ordered as a subset of C, There exists a maximal element that must contain all the vectors in the linearly independent vector series, but that element is in F so it's both linearly dependent and independent at the same time! contradiction! We get that $A \in F$ so by Zorn's lemma F has a maximal element T. That T is our basis.

11.2 Comparing Cardinals

We'll show that for every two cardinals α, β other than 0 we get $\alpha \leq \beta \vee \beta \leq \alpha$ Let A, B be two sets of cardinality α, β Define F to be the set of all ordered pairs (X, f) such that $f : X \to B$ is an injective function($X \subseteq A$). Now we'll define an order in the following way:

$$(X_1, f_1) \leq (X_2, f_2) \iff X_1 \subseteq X_2 \wedge f_2|_{X_1} = f_1$$

Let $C = ((X_1, f_1), (X_2, f_2), \ldots)$ be a chain in F, $(X, g) = (\bigcup A_i, \bigcup f_i)$

$$\Rightarrow \forall i((X_i, f_i) \leq (X, g)).$$

Assume g isn't a function, we get $(x, y), (x, z) \in G$

$$\Rightarrow \exists i, j \text{ such that: } f_i(x) = y, f_j(x) = z$$

C is a chain so we without lose of generailty we get:

$$f_i \leq f_j$$

$$\Rightarrow f_j|_{X_i} = f_i$$

$$\Rightarrow f_i(x) = f_j(x)$$

$$\Rightarrow y = z$$

[1] a totally ordered subset

That means g is a function, and since it's a union of injective functions, it must also be injective. That means it's in F and using Zorn's lemma we get a maximal element in F, which we'll denote (D, h). If $D = X$ then h is injective and we get $A \leq B$. If it's not, it must be surjective or we get a contradiction to (D, h)'s maximality and thus $B \leq A$

We can also prove $\alpha + \alpha = \alpha$. We know that $\alpha + \alpha = 2\alpha$ so we'll just prove $\alpha = 2\alpha$. We'll build F using bijections this time. Denote the maximal element $M = (X, g)$. If $|X| = 2\alpha$ We finished, else we get that there's a set of size $\aleph_0$ that can be mapped "bijectively" to the set of 2α contradicting M's maximality.

11.3 Corollaries

- $\alpha + \beta = max\{\alpha, \beta\}$
- $|A \setminus B| = |A| \iff |B| \leq |A|$
- $\alpha * \alpha = \alpha$ (not a direct corollary)
- $\alpha^\alpha = 2^\alpha$

12 Axiom of Choice

First let's define what is a choice function. A Choice Function - is a function from an indexed family of sets $(S_i)i \in I$ to their union such that $\forall i \in I(f(S_i) \in S_i)$. Now for the axiom itself, The Axiom of Choice:

$$\forall X[\emptyset \notin X \Rightarrow \exists f : X \to \bigcup X \ \forall A \in X(f(A) \in A)]$$

12.1 Nomenclature

AC - *Axiom of Choice*
ZF - *Zermelo-Fraenkel set theory omitting AC*
ZFC - *ZF extended to include AC*

13 More Axioms In ZF

Axiom of extensionality

$$\forall A \forall B(\forall x(x \in A \iff x \in B) \Rightarrow A = B)$$

Axiom of union

$$\forall A \exists B \forall c(c \in B \iff \exists D(c \in D \wedge D \in A))$$

Axiom of infinity

$$\exists I(\emptyset \in I \wedge \forall x \in I(x \cup \{x\} \in I))$$

Axiom of power set

$$\forall x \exists y \forall z[z \in y \iff \forall w(w \in z \Rightarrow w \in x)]$$

Axiom of regularity

$$\forall x(x \neq \emptyset \rightarrow \exists y(y \in x \wedge y \cap x = \emptyset))$$

Axiom of pairing

$$\forall A \forall B \exists C \forall D[D \in C \iff (D = A \wedge D = B)]$$

Axiom schema of specification - *any definable subclass of a set is a set.* **Axiom schema of replacement** - *the image of any set under any definable mapping is also a set*

14 Measure

Measure theory is complex and goes well beond what I can show in this section but let's talk about it anyway. A measure is a way to generalize the length, volume, and such for sets. Let X be a set and Σ a σ-algebra over X. A set function μ from Σ to the extended real number line is called a measure if

- $\forall E \in \Sigma : \mu(E) \geq 0$
- $\mu(\emptyset) = 0$
- σ-additivity: For all countable collections $\{E_k\}_{k=1}^{\infty}$ of pairwise disjoint sets in Σ,
$$\mu(\bigcup_{k=1}^{\infty} E_k) = \sum_{k=1}^{\infty} \mu(E_k)$$

If the condition of non-negativity is dropped then μ is called a signed measure. The pair (X, Σ) is called a measurable space, and the members of Σ are called measurable sets. A triple (X, Σ, μ) is called a measure space. A probability measure is a measure with total measure $\mu(X) = 1$. A probability space is a measure space with a probability measure.

14.1 Lebesgue Measure

Now we have to simplify things so we'll consider only Lebesgue measure of bounded sets on the real number line. First, if the set is of the form $X = (a, b)$ or $X = [a, b]$ and such the measure must satisfy $\mu(X) = b - a$, if $Y = f(X)$ and f is an isometric function then $\mu(X) - \mu(Y)$. Denote $\mathcal{Y} = (Y_i)_{i \in I}$ such that $|I| < \aleph_0$ and $X \subseteq \bigcup_{i \in I} Y_i$ and each Y_i is an interval on R. Denote $s(\mathcal{Y})$ The sum of lengths of intervals in $\mathcal{Y}$. The outer measure of X is

$$\mu^*(X) = \inf_{\mathcal{Y}} s(\mathcal{Y})$$

And the inner measure is defined with an interval $X \subseteq [a, b]$ and $X' = [a, b] \setminus X$

$$\mu_*(X) = (b - a) - \mu^*(X')$$

It's easy to show that the outer measure is always greater than the inner measure. The Lebesgue measure is defined if they are equal and is equal to

$$\mu_*(X) = \mu^*(X) = \mu(X)$$

15 Well Order

A partially ordered set $(X, \leq)$ is well ordered

$$\iff$$

$$\forall S \subseteq X(S \neq \emptyset \rightarrow \exists b \in S(\text{b is a minimal element is S}))$$

Think about the following theorems:

1. Every finite totally ordered set is well ordered.
2. If $\leq$ is a well order then it's a linear order as well.
3. Let $(X, \leq)$ be a linearly ordered set. It's well ordered $\iff$ it doesn't include an infinite decreasing series.

We'll proceed to define two very similar terms.
Risha - If X is well ordered $A \subseteq X$(usually we mean $A \subset X$) is a Risha if $x \in A \wedge y < x \rightarrow y \in A$
Initial segment - $I_x(a) = \{x \in X : x < a\}$ aka initial segement of a in X

note: $[0, 0.5]$ in $[0, 1] \in \mathbb{R}$ is a Risha but not an initial segment. Prove a Risha and an initial segment are the same in wosets.

15.1 Some Lemmas

1. let X be a woset, $f : X \rightarrow X$ a one-to-one homomorphism $\rightarrow \forall x \in X(x \leq f(x))$
2. let $(X, \leq_x) \cong (Y, \leq_y)$ be isomorphic wosets, there's only one unique isomorphism betweem them (proof using previous theorem)
3. in a woset X a risha can't be have an isomorphism with X
4. in wosets $I_x(a) \cong I_x(b) \Rightarrow a = b$
5. let $f : X \rightarrow Y$ be an isomorphism between wosets s.t. $y_0 = f(x_0) \Rightarrow I_x(x_0) = I_y(y_0)$

15.2 A lemma about partial orders

If $(X, \leq_x), (Y, \leq_y)$ are partial orders, and $\leq_x$ is a total order, then if f is an inversible homomorphism then it's an isomorphism, and $\leq_y$ is a total order.

16 Comparison of Well Ordered Sets

If X, Y are wosets then exatcly one of the following is true

1. $(X, \leq_x) \cong (Y, \leq_y)$
2. $\exists y_0 \in Y : (X, \leq_x) \cong (I_y(y_0), \leq_y)$
3. $\exists x_0 \in X : (Y, \leq_y) \cong (I_x(x_0), \leq_x)$

If $X = \emptyset \vee Y = \emptyset$ the proof is trivial. Assuming they're not empty we'll define:

$$A = \{x \in X : \exists y \in Y (I_X(x) \cong I_Y(y))\}$$

$$B = \{y \in Y : \exists x \in X (I_X(x) \cong I_Y(y))\}$$

$$\phi : A \to B$$

$$\phi(x) = y : I_X(x) \cong I_Y(y)$$

It's clear why ϕ is a bijection, we will show it's an isomorphism. Consider $a_1 < a_2 \in A$ and $\phi(a_1) = b_1, \phi(a_2) = b_2$. Since $I_X(a_2) \cong I_Y(b_2)$ we'll denote their isomorphism α. $a_1 < a_2 \Rightarrow a_1 \in Dom\alpha \Rightarrow \alpha(a_1) \in Im\alpha = I_Y(b_2) \Rightarrow \alpha(a_1) < b_2$. By one of our previous lemmas[0] $I_X(a_1) \cong I_Y(\alpha(a_1))$ and we know $I_X(a_1) \cong I_Y(b_1) \Rightarrow b_1 = \alpha(a_1)$. Recall that $\alpha(a_1) < b_2 \Rightarrow b_1 < b_2$. Since ϕ is a bijection and a homomorphism it's an isomorphism $\Rightarrow A \cong B$.
By cases we'll get:

1. If $A = X, B = Y \Rightarrow (1)$.
2. If $B = Y \wedge A \subset X \neq \emptyset$ denote $A \setminus X$'s minimal element c and then $\Rightarrow I_X(c) = A$ [1] $\Rightarrow (3)$[2]
3. If $A = X \wedge B \subset Y \neq \emptyset$ denote $Y \setminus B$ minimal element d and then $\Rightarrow I_X(d) = B \Rightarrow (2)$
4. If $A \subset X \wedge B \subset Y \Rightarrow I_X(c) \cong A \wedge I_Y(d) \cong B.A \cong B \Rightarrow I_X(c) \cong I_Y(d) \Rightarrow c \in A$ but $c \notin A$ by our construction $\Rightarrow$ contradiction.

Now we'll show only one of $(1), (2), (3)$ can be true for any X, Y:
$(2) + (3) \Rightarrow \exists \delta : X \to I_Y(d)$ isomorphism $\Rightarrow^0 I_X(c) \cong I_Y(\delta(c))$ and since we know $Y \cong I_X(c)$ we get that $Y \cong I_Y(\delta(c))$ which we know can't be.
$(1) + (3)/(1) + (2) \Rightarrow$ an initial segment of X/Y is isomorphic to X/Y and that can't be!

[0] Refer to 15.1.5
[1] Think why(two sided inclusion).
[2] since $A \cong B$

17 Ordinals

Ordinals are the generalization of ordinal numerals aimed to extend enumeration to infinite sets. The finite ordinals will be defined as such:

$$k = ord(\{0, 1, \ldots, k-1\}) = ord(I_{\mathbb{N}}(k))$$

$$ord(\emptyset) = 0$$

$$ord(\mathbb{N}) = \omega$$

By the comparability of wosets we can define an order on the ordinals as such:

$A \cong B \iff ord(A) = ord(B)$
$A < B \iff ord(A) < ord(B)$
$A > B \iff ord(A) > ord(B)$

Now we'll define a new set function on ordinals $W(\alpha)$

$$W(\alpha) = \{\beta : \beta < \alpha\}$$

$W(\alpha)$ is a woset and $ord(W(\alpha)) = \alpha$
proof by constructing the isomorphism: $\phi : A^1 \to W(\alpha)$

$$\phi(a) = W(ord(I_A(a)))$$

So by our construction, every set of ordinals A is a woset. A proof can be made by showing that every $A' \subseteq A$ has an element a, which if not already minimal, has a $W(a) \bigcup A'$ that contains the minimal element since it's a woset as a subset of a woset.

17.1 Cesare Burali-Forti Paradox

The set of all ordinals can't be well defined. Suppose it were a set, it'll be a woset, we'll denote it $O \Rightarrow ord(O) \in O \Rightarrow W(O) \subseteq O$ but we know $ord(W(O)) = O$ and that means $I_O(ord(O)) \cong O$ Thus an initial segment of the set is isomorphic to it which is a contradiction.

17.2 Russell's Paradox

Russell's Paradox - *Let R be the set than contains all the sets that don't contain themselves.*
If R contains itself, it must not contain itself.
If R doesn't contain itself, then it must contain itself.
Paradox.

[1] $|A| = \alpha$ and A is a woset

17.3 Kinds of Ordinals

There are two kinds of ordinals:
Successor Ordinals - *ordinals that immediatly success another ordinal*
Limit Ordinals - *the rest.*

17.4 Ordinal Arthimetic

17.4.1 addition

Let $(X, \leq_x), (Y, \leq_y)$ be two **disjoint** wosets such that $(ord(A), ord(B) = (\alpha, \beta))$.
We denote:$(X \bigcup Y, \leq)$:

$$a \leq b \iff \begin{Bmatrix} a, b \in X & a \leq_x b \\ a, b \in Y & a \leq_y b \\ a \in X & b \in Y \end{Bmatrix}$$

As $X \oplus Y$, And by definition $\alpha + \beta = ord(X \oplus Y)$
Oridnals are associative but not commutative with addition

- $n + \omega = \omega$
- $\alpha + 0 = \alpha$
- $\omega < \omega + 1 < \omega + 2 < \ldots < \omega + k < \ldots < 2\omega$

17.4.2 multiplication

Let $(X, \leq_x), (Y, \leq_y)$ be two **disjoint** wosets such that $(ord(A), ord(B) = (\alpha, \beta))$.
We denote:$(X \times Y, \leq_{dictionary})$ As $X \odot Y$, and by definition $\alpha * \beta = ord(X \odot Y)$
It's possible to show $\omega = k\omega$ by constructing an isomorphism

$$\phi : \mathbb{N} \to \{0, 1, \ldots, k-1\} \times \mathbb{N}$$

$$\phi(n) = (\lfloor n/k \rfloor, n \bmod k)$$

- $\omega * 0 = 0$
- $\alpha * 1 = \alpha$
- $2\omega = \omega < \omega 2 = \omega + \omega < \omega 3 < \ldots < \omega k < \ldots < \omega^2$

Ordinals are left distribuitive but not right distributive. Why?

17.4.3 Powers

$$\alpha^\gamma = \begin{pmatrix} 1 & \gamma = 0 \\ \alpha^{\gamma - 1}\alpha & \gamma \text{ is a succesor ordinal} \\ min_{\delta < \gamma}\{\mu : \alpha^\delta < \mu\} & \gamma \text{ is a limit ordinal} \end{pmatrix}$$

From that we infer the biggest ordinal so far is ω^ω
Ordinals are usually expressed as polynomials of powers of ω with natural coefficients. And I lied earlier...

$$\omega^\omega < \omega^\omega + 1 < \omega^\omega + 2 < \ldots < \omega^{\omega^\omega} < \ldots$$

17.4.4 2^ω and ω^ω

By our previous definition we can conclude that 2^ω is

$$min_{\delta<\omega}\{\mu : 2^\delta < \mu\}$$

$$= min\{2^1, 2^2, \ldots, 2^k, \ldots\}$$

Since this series doesn't have an upper bound the result is the smallest infinite ordinal or $2^\omega = \omega$

By our previous definition we can conclude that ω^ω is

$$min_{\delta<\omega}\{\mu : \omega^\delta < \mu\}$$

$$= min\{\omega^1, \omega^2, \ldots, \omega^k, \ldots\}$$

Let's consider

$$X = X_1 \oplus X_2 \oplus X_3 \ldots (\forall n \in \mathbb{N}, ord(X_n) = \omega^n)$$

We see that this is what we looked for[1] thus $ord(X) = \omega^\omega$ but also this is a sum of a countable amount of groups of a countable size so surprisingly $|X| = \aleph_0$ and this is the case for sets of ordinals ω^{ω^ω} and so on...

[1] Verify this is indeed what we looked for

18 The Well Ordering Theorem

The Well Ordering Theorem(WOT) states that any set can be well ordered and is equivalent to Zorn's lemma and AC.

18.1 Proof Form AC

Let the set we're trying to well-order be A and let f be a choice function for the family of non-empty subsets of A. Now for every ordinal α define:

$$\begin{cases} a_\alpha = f(A \setminus \{a_\xi | \xi < \alpha\}), & A \setminus \{a_\xi | \xi < \alpha\} \neq \emptyset \\ a_\alpha = \text{UNDEFINED}, & \text{otherwise} \end{cases}$$

Then

$$\langle a_\alpha | a_\alpha \text{ is defined} \rangle$$

Is a well order on A.

18.2 Proof of AC using WOT

To make a choice function for a collection of non-empty sets, E, take the union of the sets in E and call it X. There exists a well-ordering of X; let R be such an ordering. The function that to each set S of E associates the smallest element of S, as ordered by (the restriction to S of) R, is a choice function for the collection E.[2]

It's worth noting the difference between choosing this one choice function here (R), and applying the WOT to all the sets $S \in E$ seperately, and choosing the minimal element in each set seperately. While the first is allowed under ZF since we're only making a single choice, the latter is not allowed when there are infinitely many elements in E without assuming the axiom of choice itself, and thus is not a valid way to prove AC.

[2]This proof was taken straight from wikipedia.

19 The Continuum Conjecture

Suppose X is a set of cardinality $\aleph$, and consider the set of all Risha's with a cardinality greater then $\aleph_0$[1], since X can be a woset, that set has a minimal element m and $|m| = \aleph_1$. The conjecture is that $\aleph = \aleph_1$. This was proven to be unsolvable under ZFC. We can also define an $\aleph$ greater than all $\aleph$ of the form $\aleph_n$ where $n \in \mathbb{N}$ by looking at sets $|A_n| = \aleph_n$ and at $B = \bigcup_{1\in\mathbb{N}} \aleph_i$. $|B| > \aleph_n (\forall n \in N) \Rightarrow \exists x \in B : |I_B(x)| > \aleph_n (\forall n \in N)$. We denote the minimal element of the set of all such x's M, and $|M| = \aleph_\omega = \sum_{i\in\mathbb{N}} \aleph_i$ and after all countable ordinals we'll reach $\aleph_\Omega$, the $\aleph_1$-th ordinal, and the fisrt uncountable one. The generalized Continuum Conjecture is:

$$2^{\aleph_\alpha} = \aleph_{\alpha+1}$$

[1]If it's empty define any one element to be maximal

20 Transfinite Induction

Transfinite induction is an extension of mathematical induction to well-ordered sets, for example to sets of ordinal numbers or cardinal numbers. Its correctness is a theorem of ZFC. When given X a set, and P the set of elements who have a certain property, the principle that's derived by the WOT can be written like this:

$$\forall x \in X(\forall y < x(y \in P)) \Rightarrow x \in P$$

The steps of transfinite induction:

1. the 0 case($0 \in P$)
2. The succesor ordinal case($\alpha \in P \Rightarrow \alpha + 1 \in P$)
3. The limit ordinal case case($\forall\beta < \gamma(\beta \in P) \Rightarrow \gamma \in P$)

20.1 Proof That The Only Isomorphism from a Well-Ordered Set to Itself is the Identity Isomorphism

Consider the propety P that "*this element is transformed to itself under all iso- morphisms*". Now consider an element a such that all elements that are lesser than a are in P . This can always be done by choosing the minimal element by WOT. a can't be transformed to an element lesser than a because than the isomorphism won't be injective, and also not to an element greater than it, because a must also have a source, since the isomorphism is surjective, but then we get a contradiction to the the fact the isomorphism is a homomorphism.

note: transfinite induction works because of WOT but there are of course sets like $\mathbb{R}$ with normal ordering that isn't a woset so we can't use transfinite induction on it. A counter example for our proof may be f (x) = x + 1

21 Extras

21.1 A Bit About Constructions

Constructions of sets are the way to formally define sets like $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

21.1.1 Construction of $\mathbb{N}$

There are multiple ways[3] to define $\mathbb{N}$ one in ZF is recursivly defining the natural numbers as such:

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

And so on defining numbers unsing the succesor function $S(n) = n \cup \{n\}$. $\mathbb{N}$ is the smallest set containing 0 and closed under $S(n)$

21.1.2 Construction of $\mathbb{Z}$

$\mathbb{Z}$ was constructed as $\mathbb{N} \times \mathbb{N}/R$

$$\langle a, b\rangle \, R \, \langle c, d\rangle \iff c - d = a - b$$

For example $-1 = \{\langle 2, 3\rangle, \langle 5, 6\rangle, \ldots, \langle n, n+1\rangle\}$
Define $\mathbb{Z}_+, \mathbb{Z}_*$

21.1.3 Construction of $\mathbb{Q}$

$\mathbb{Z}$ was constructed as $\mathbb{Z} \times \mathbb{Z}'$[4]$/R$

$$\langle a, b\rangle \, R \, \langle c, d\rangle \iff ad = cb$$

For example $\frac{1}{2} = \{\langle 1, 2\rangle, \langle -2, -4\rangle, \ldots, \langle n, 2n\rangle\}$
Define $\mathbb{Q}_+, \mathbb{Q}_*$

21.1.4 About the Construction of $\mathbb{R}$

The construction of $\mathbb{R}$ is more difficult than you may expect. It should be studied in a number theory course, and is usually very unrigoursly defined as all numbers in the interval $(-\infty, \infty)$

21.2 Discrete Functions

Discrete Function - A function that is defined only for a set of numbers that can be listed, such as the set of whole numbers or the set of integers.

[3] One of them is by isomorphism classes of finite sets
[4] $\mathbb{Z}' = \mathbb{Z} \setminus \{0\}$

21.3 More Definitions

21.3.1 Saturated Functions

For a function $f : X \to Y$

$$\forall A \subseteq X, f_\star(A) = \{f(x) : x \in A(A \in P(X))\}$$

$$\forall B \subseteq X, f^\star(A) = \{x : f(x) \in B(B \in P(Y))\}$$

21.3.2 Hasse Diagrams

Hasse diagrams represent posets. For example the Hasse Diagram of the the set $\{1, 2, 3\} \times \{1, 2\}$ with the standard order.

$$\begin{tikzcd}
 & & \{3,2\} \arrow[dl, dash] \arrow[dr, dash] & \\
 & (2,2) \arrow[dl, dash] \arrow[dr, dash] & & (3,1) \arrow[dl, dash] \\
(1,2) \arrow[dr, dash] & & (2,1) \arrow[dl, dash] & \\
 & (1,1) & &
\end{tikzcd}$$

21.3.3 Some Denotions

- A Singleton is a set containing only one element.
- $P(A) = \{B : B \subseteq A\}$
- $A \triangle B = \{A \cup B\} \setminus \{A \cap B\}$
- $|\mathbb{R}| = c = \beth_1 = \aleph$
- $A^c = \{b : b \notin A\}$
- $\prod_{i \in I} X_i = \{f : I \to \bigcup_{i \in I} X_i | \forall i \in I(f(i) \in X_i)\}$
- A pairing function is a bijection $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- The indicator function of $A \subseteq X$ is $1_A(x) = I_A(x) = \chi_A(x) = 1 \iff x$ is in A and equals 0 otherwise