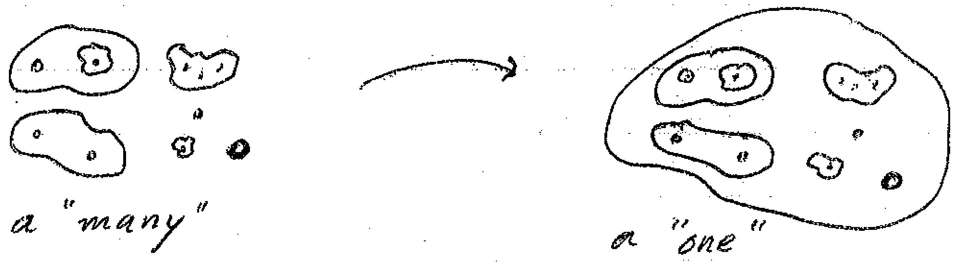
/

Lect #2

Ch. 0- Naive Set Theory

The basic principle that we have to guide us in Naive Set Theory is Cantor's notion of a set:

Cantor's Notion: A set is a "many" that can be thought of as a "one".



In Naive set theory we will assume we have a given collection of objects and that we make sets by starting out with these objects.

Notation:
If A is a set and x is an object we will write

$x \in A$ to mean x is an element of A
$x \notin A$ " " x is not " " .

We will also use the following abbreviations

$\rightarrow$ abreviates "implies"
$\leftrightarrow$ " "if and only if"
$\neg$ "not"

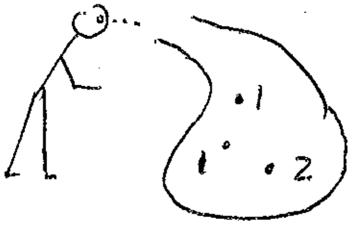
&	abbreviates	"and"
$\vee$	" "	"or" (inclusive or)
$\forall$		"for all..."
$\exists$		"there exists ... such that"

Qu: What is a set?

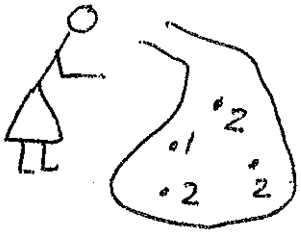
Ans: We are not in a position to say what is a set in Naive set theory - but we have Cantors notion to guide us

Qu: When are two sets equal?

Ans: $A = B$ if $(\forall x)(x \in A \leftrightarrow x \in B)$



$\{1, 1, 2\}$



$\{1, 2, 2, 2\}$

Def: We say that A is a subset of B if $(\forall x)(x \in A \rightarrow x \in B)$ and write $A \subseteq B$ when this is so.

Fact: $A = B$ if and only if $(A \subseteq B \ \& \ B \subseteq A)$

Sets of sets

Usually the elements of a set are the primary objects that we assumed given to us in Naive Set Theory - but this need not be the case. If every element of a set A is itself a set, we say that A is a set of sets (In our Axiomatic Set theory all sets will be sets of sets)

Some more operations on sets

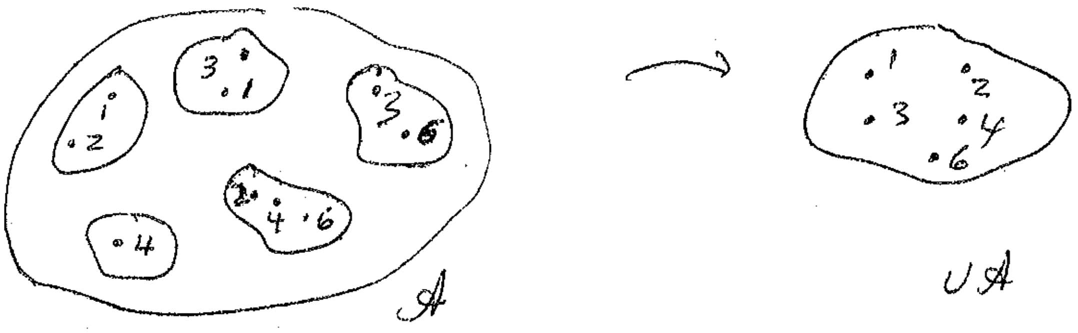
Def. We define the ordered pair $\langle a,b\rangle$ by $\langle a,b\rangle = \{\{a\},\{a,b\}\}$

Def. We define the Power set of A by $\mathcal{P}(A) = \{B : B \subseteq A\}$

Note: Both $\langle a,b\rangle$ and $\mathcal{P}(A)$ are sets of sets

Def ~~We define the union of a set of sets~~ by If $\mathcal{A}$ is a set of sets we define the union of $\mathcal{A}$ by

$$\cup\mathcal{A} = \{x : \text{there is an element } B \text{ in such that } x \in B\}$$
$$= \{x : x \text{ is a member of at least one element in}$$



Specification of sets

Let A be a set. Suppose we want to communicate A to someone, how can we do this?

Well, if A is finite we can just list the elements of A and this will do the job:

$$A = \{a_1, a_2, a_3, \dots, a_n\}$$

However if A is infinite this method will not work.

In many situations we can specify A as the set of all objects for which some property holds i.e.

$$A = \{x : P(x) \text{ holds}\}$$

This is called set building notation.

However we must be careful.

1. Is $\{x : x \neq x\}$ a set?
2. Is $\{x : x \notin x\}$ a set?

} Prove for H.W.

Some elementary operations on sets

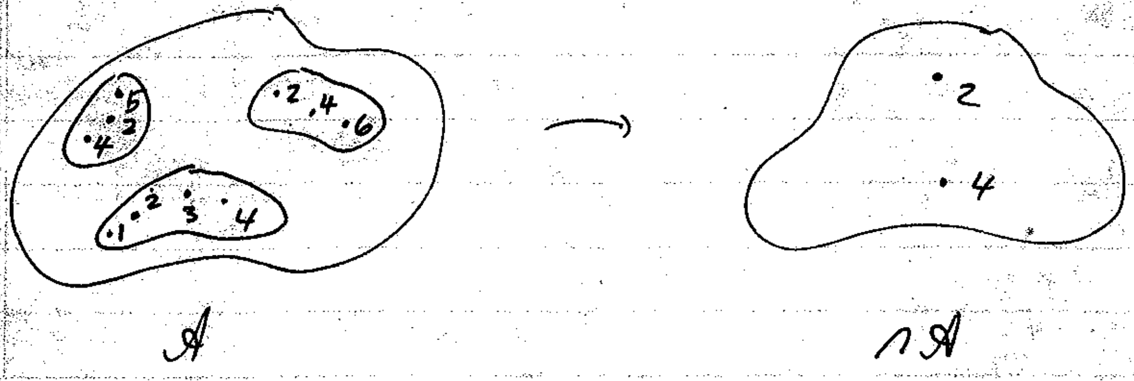
Def. We define

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$
$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$
$$A - B = \{x : x \in A \text{ and } x \notin B\}$$

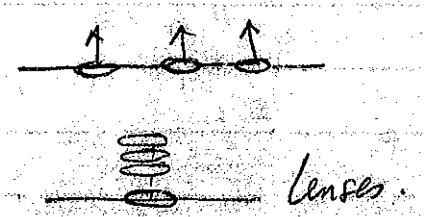
3. Is $\{x : x = x\}$ a set?
4. Is $\{x : x \in x\}$ a set?

Def. If $\mathcal{A}$ is a set of sets we define the intersection of $\mathcal{A}$ by

$$\cap\mathcal{A} = \{x : x \text{ is an element of every member of } \mathcal{A}\}$$



Qu: What is $\cup\emptyset$?
" " $\cap\emptyset$?



Skip
wait for after functions

Indexed family of sets:

If for each member i of a set I, we can associate a set A_i, we say that $\langle A_i : i \in I\rangle$ is an indexed family of sets. An index family of sets consists of as a function $f : I \to V$. I is called the indexing set.

We define $x : (\exists i \in I)(x \in A_i)$

$$\bigcup_{i\in I} A_i = \{x : x \in A_{i_0} \text{ for at least one } i_0 \in I\}$$

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ for every } i \in 1\}.$$
$$\{x : (\forall i \in I)(x \in A_i)\}$$

We usually write $f(i)$ as A_i and the indexed family as $\langle A_i : i \in I\rangle$. Wrong to write $\{A_i : i \in I\}$

1.

Lect: #3. **Binary Relations**

Def. A set R is called a binary relation if all of its elements are ordered pairs (i.e. a binary relation is just a set of ordered pairs).

Ex. 1 $R = \{\langle 1,2\rangle, \langle 3,8\rangle, \langle 1,4\rangle\}$ is a binary relation.

The set of all 1st coordinates of the ordered pairs in R is called the domain of R. The set of all 2nd coordinates of the ordered pairs in R is called the range of R

The field of R is defined by

$$\text{field}(R) = \text{dom}(R) \cup \text{ran}(R)$$

Ex. 2 In Example 1

$$\text{dom}(R) = \{1,3\} \qquad \text{ran}(R) = \{2,4,8\}$$

$$\text{field}(R) = \{1,2,3,4,8\}$$

If X and Y are any sets such that

$$\text{dom}(R) \subseteq X \quad \text{and} \quad \text{ran}(R) \subseteq Y$$

we say that R is a relation from X to Y

Ex. 3 The relation in Example 1 is from $\{1,2,3\}$ to $\{2,4,6,8\}$

A binary relation on A is just a binary relation from A to A.

Instead of writing $\langle a,b\rangle \in R$ we usually write aRb.

Def. Let R be a benary relation on A. We say that

(i) R is reflexive if for each $a\in A$, aRa

(ii) R is symmetric if for any $a,b\in A$
$aRb \Rightarrow bRa$

(iii) R is transitive if for ally $a,b,c\in A$
aRb & $bRc \Rightarrow aRc$

(iv) R is connected if for any $a,b\in A$
with $a\neq b$, aRb or bRa

(v) R is anti-symmetric if for any $a,b\in A$
with $a\neq b$, $\Rightarrow$ $aRb \Rightarrow b\not{R}a$

	a	b	c	d
a	o✓	o	o✓	o
b	o	o✓	o	o
c	o	o	o✓	o
d	o✓	o	o	o✓

Reflexive
(diagonal)

	a	b	c	d
a	o	o✓	o✓	o
b	o✓	o	o✓	o
c	o✓	o✓	o	o
d	o	o	o	o✓

Symmetric
(both or none)

	a	b	c	d
a	o	o✓	o	o✓
b	o	o	o✓	o
c	o✓	o	o✓	o✓
d	o	o	o	o

at most one of the two

anti-symm.

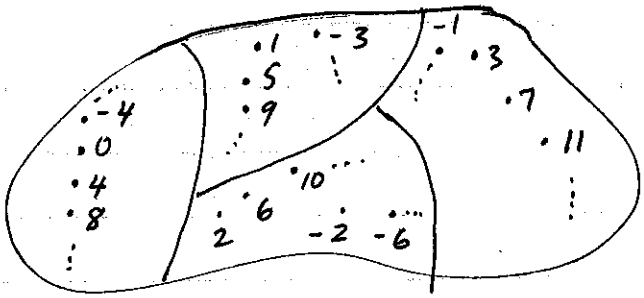
	a	b	c	d
a	o	o✓	o	o
b	o✓	o	o✓	o✓
c	o✓	o	o✓	o✓
d	o✓	o	o	o

at least one of the two

connected

Def. A binary relation on A is called an equivalence relation if it is reflexive, symmetric and transitive.

Fact: If R is an equivalence relation on A, then R partitions A into disjoint equivalence classes



Ex. Let R be the binary relation on $\mathbb{Z}$ defined by

$$aRb \quad \text{if} \quad a-b \text{ is a multiple of } 4$$

Functions:

A binary relation R is called a function if for any $a \in dom(R)$ there is only one $b \in ran(R)$ such that aRb. (i.e. if aRb & aRc then $b=c$)

If F is a function we usually write $F(a) = b$ instead of aFb.

If $A = dom(F)$ and B is any set such that $ran(F) \subseteq B$, we say that F is a function from A to B. B is called a co-domain of F.

Def. Let $f: A \to B$ be a function with codomain B. We say that

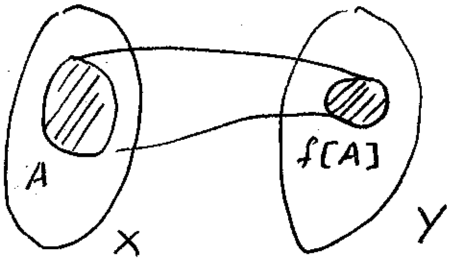
(i) f is *injective* if for any $b \in B$, there is at most one $a \in A$ such that $f(a) = b$.
(i.e. $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$)

(ii) f is *surjective* if for any $b \in B$, there is at least one $a \in A$ such that $f(a) = b$.

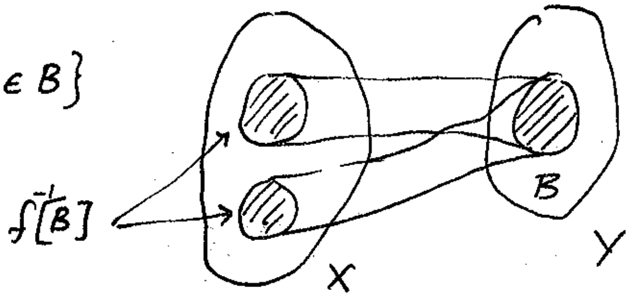
(iii) f is *bijective* if for any $b \in B$, there is *exactly one* $a \in A$ such that $f(a) = b$.

Def. If $f: A \to B$ and $g: B \to C$ are functions, we define the *composition* of g with f by
$$(g \circ f)(a) = g(f(a)).$$

Def. Let $f: X \to Y$ and suppose $A \subseteq X$ and $B \subseteq Y$. We define the *image* of A under f by
$$f[A] = \{f(a) : a \in A\}$$



We define the *inverse image* of B under f by
$$f^{-1}[B] = \{a \in X : f(a) \in B\}$$



Generalised cartesian products

Ordered pair $\langle a,b\rangle = \{\{a\},\{a,b\}\}$ ✓

Ordered triple $\langle a,b,c\rangle =$ function from $\{0,1,2\}$ to V

Ordered quadruple $\langle a,b,c,d\rangle$

ordered n-tuple $f : \{0,1,2,\dots n-1\} \to V$

Indexed family of sets $\bigcup_{i\in I} A_i$, $\bigcap_{i\in I} A_i$

ordered infinite-tuple ?? $\langle a_1, a_2, a_3, \dots \rangle$

= infinite sequence.

skip × Def. An *infinite sequence* is a function s with

$$\text{dom}(s) = \mathbb{P} = \{1,2,3,\dots\}$$

$s(1) = a_1$

$s(2) = a_2$

$\vdots$

skip × A *doubly infinite sequence* is a function s with $\text{dom}(s) = \mathbb{Z}$.

$$\langle \dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots \rangle$$

$$\langle \cdots\cdots \underset{a_{-1}}{\cdot} \underset{a_{-1/2}}{\cdot} \underset{a_0}{\cdot\cdot} \underset{a_{1/4}}{\cdot} \underset{a_{1/2}}{\cdot} \underset{a_1}{\cdot} \cdots\cdots \rangle$$

Def. Let $\langle A_i : i\in I\rangle$ be a family of sets. We define the generalised cartesian product of by

$$\mathop{\times}_{i\in I} A_i = \{f : f \text{ is a function from } I \text{ to } \bigcup_{i\in I} A_i \text{ with } f(i)\in A_i \text{ for each } i\in I\}$$

Lect. #4

Ch. 2 - The ZFC Axioms

Axiomatic Theories

An axiomatic theory in mathematics consists of

1. Logical axioms
2. Rules of inferences
3. Proper axioms

$\left.\begin{array}{l}1.\ \text{Logical axioms}\\ 2.\ \text{Rules of inferences}\end{array}\right\}$ these are the same in all mathematical theories

Ex. 1 The Theory of Arithmetic

We don't usually write this part down

1. Logical Axioms:

$(\neg q \to \neg p) \leftrightarrow (p \to q)$,

$(\forall x)(\neg p(x)) \leftrightarrow \neg(\exists x)(p(x))$,

$(p \to q) \leftrightarrow (\neg p \vee q)$,

.... etc.

2. Rules of inference:

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array}$$

modus ponens = rule of detachment,

$$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$$

(simplification),

$$\begin{array}{c} \neg p \to \text{a contradiction} \\ \hline \therefore p \end{array}$$

, etc.

3. Proper Axioms

(i) If $s(x) = s(y)$ then $x = y$

(ii) There is no natural number x such that $0 = s(x)$

$(iii)_P$ If P is a property such that (a) $P(0)$ is true (b) $P(n) \Rightarrow P(s(n))$, for any n, then $P(n)$ is true for all natural numbers n.

Structures

A structure consists of

1. a set $\mathcal{U}$ (called the universe)
2. some relations on $\mathcal{U}$
3. some functions on $\mathcal{U}$
4. some constants from $\mathcal{U}$

Ex 2. The structure of arithmetic is

$\langle \mathbb{N}, s, 0 \rangle$ $s =$ successor function

Ex. 3 The structure of the real numbers is

$\langle \mathbb{R}, <, +, \cdot, 0, 1 \rangle$

If we can find a structure such that all the proper axioms of an ~~theory~~ axiomatic theory is true, then we say that the theory is consistent

Ex. 4. The Theory of Arithmetic is consistent.

Ex. 5 Consider the theory with proper axioms

1. $s(0) \neq 0$
2. $(\forall x)[s(x) = x]$

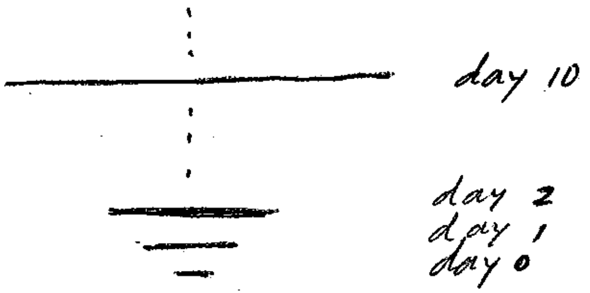
This theory cannot be consistent because there is no way for 1. & 2. to be both true in a structure.

The cumulative hierarchy

In Naive Set Theory we started with a collection of objects and built sets from them. If we want to be more precise we must answer the following questions

Q1: What do we take as our initial collection?
Q2: What operations can we use to build new sets?
Q3: How long can we keep building?

Now in building sets what we expect is to take old sets and make new ones out of them. So we can think of our initial collection as the set of all things born on day 0. Then on day 1 we can create sets from whatever we have obtained so far, and so on on day 2.



The hierarchy of births

Q2 can now be modified to
Q2': Which collections of objects from the previous days should we be able to ~~collect~~ put together and call sets?

ANS. 1: It does not seem like a bad idea to assume that no set was created on day 0.

ANS. 2': We should be able to take all possible collections of objects from the previous days and put them together as sets.

ANS. 3: We should be allowed to go on making sets as long as we like – there should be no restriction or ending day.

What we get out of all of This is the cumulative hierarchy. Let V_i = collection of all sets born on or before day i:

$V_0 = \emptyset$

$V_1 = \{\emptyset\}$

$V_2 = \{\emptyset, \{\emptyset\}\}$

$V_3 = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} = 2^2$ 4 sets

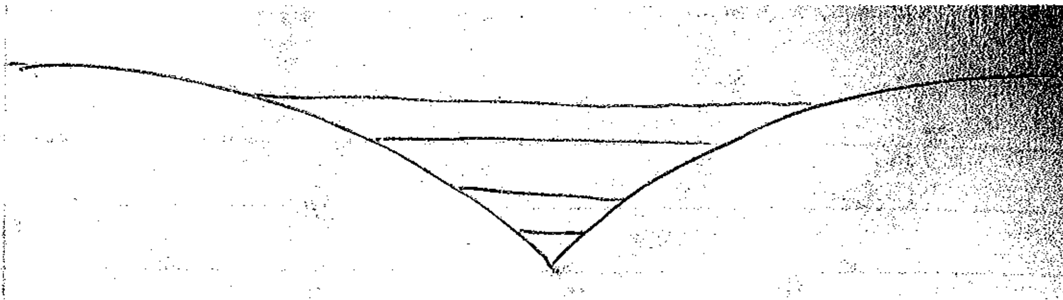
$V_4 = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots \} = 2^{2^2}$ 16 of them

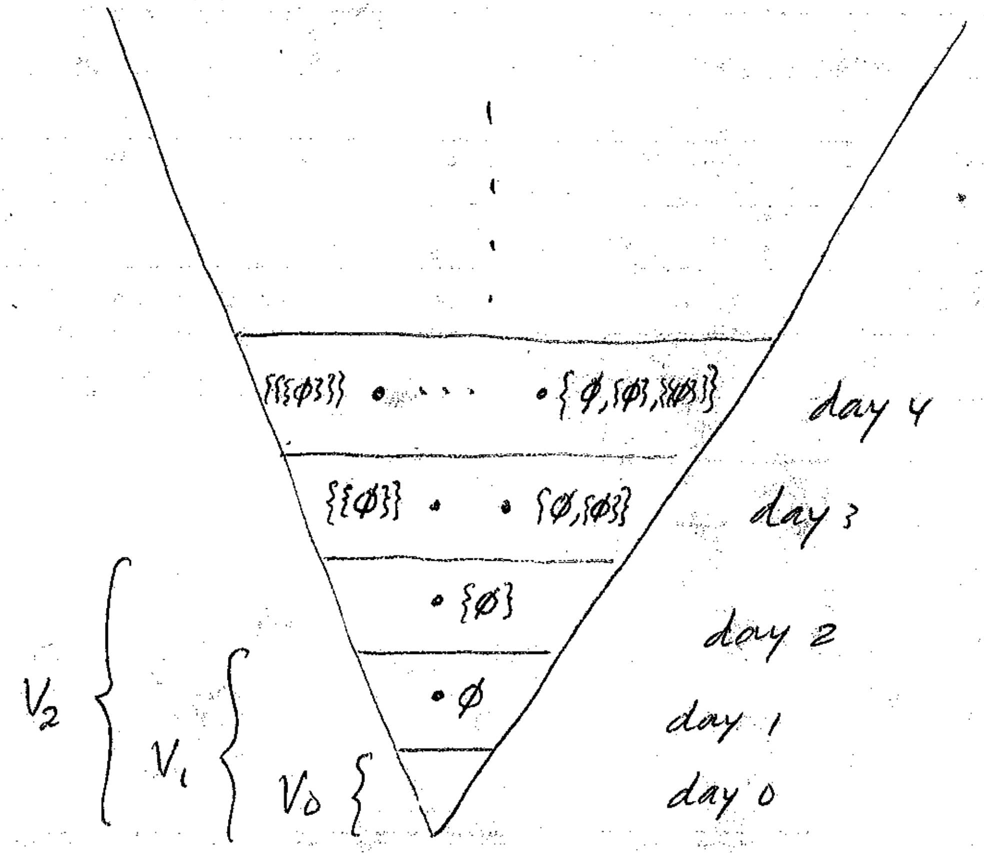
$V_5 = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{\{\{\{\emptyset\}\}\}\}, \dots\}$ $2^{16} = 65,536$ se

$V_6 = \{ \dots \quad \cdot \quad - \quad - \}$ $2^{65,536}$ sets

$\vdots$

$V_n = \underbrace{2^{\cdot^{\cdot^{\cdot^{2}}}}}_{n\text{-}1\text{times}}$





The cumulative hierarchy

Zermelian sets:

$$\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\{\{\emptyset\}\}\},\ \ldots$$
$$Z_0 \quad Z_1 \quad Z_2 \quad Z_3$$

Neumanian sets:

$$\emptyset,\ \{\emptyset\},\ \{\emptyset,\{\emptyset\}\},\ \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\},\ \ldots$$
$$N_0 \quad N_1 \quad N_2 \quad N_3$$

Lect #5 The ZFC Axioms

1. Null set Axiom : There is a set $\emptyset$ which has no elements

2. Extensionality Axiom : Two sets A and B are equal if every element of A is in B and every element of B is in A.

3. Pairing Axiom : If A and B are sets, then $\{A, B\}$ is a set.

4. Union Axiom : If A is a set, then $\cup A$ is a set.

5. Power set Axiom : If A is a set, then $\mathcal{P}(A)$ is a set.

6. Infinity Axiom : There is a set X such That (i) $\emptyset \in X$ and. (ii) $A \in X \Rightarrow \{A\} \in X$.

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

8. Foundation Axiom : If X is any non-empty set, there there is an element $A \in X$ such That A and X have no common element (i.e. $A \cap X = \emptyset$)

$(9.\varphi)$ Separation Axiom : If $\varphi(x)$ is any formula in L.O.S.T. and A is a set , then

$$\{a \in A : \varphi(a) \text{ is true}\}$$

is a set.

$(10.\varphi)$ Replacement Axiom : If $\varphi(x, y)$ is any function-type formula and A is a set, then

$$\{b : \varphi(a,b) \text{ is true for at least one } a \in A\}$$

is a set.

Def. A formula $\varphi(x,y)$ is said to be a function-type formula if for any set a there is at most one set b such that $\varphi(a,b)$ is true.

The language of set theory (L.O.S.T) is based on the alphabet given below:

variables : $x_1, x_2, x_3 \cdots$
parameters (names of specific sets) : $a_1, a_2, a_3,$
connectives : $\neg, \&, \vee, \rightarrow, \leftrightarrow$
quantifiers : $\forall$, $\exists$
membership symbol : $\in$
equality symbol : $=$
parenthesis : $($, $)$, $[$, $]$

L.O.S.T is defined recursively as follows:

1. Any expression of the form:

   $(x_i = x_j)$ $(a_i = a_j)$ $(a_i = x_j)$ $(x_i = a_j)$

   $(a_i \in a_j)$ $(a_i \in a_j)$ $(a_i \in x_j)$ $(x_i \in a_j)$

   is a formula in LOST.

2. If φ and ψ are formulas in LOST then so are $(\neg\varphi)$, $(\varphi \& \psi)$, $(\varphi \vee \psi)$

   $(\varphi \rightarrow \psi)$, $(\varphi \leftrightarrow \psi)$

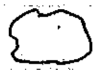
   $(\exists x_i)(\varphi)$, $(\forall x_i)(\varphi)$

3. An expression is a formula in LOST only if can be formed from the atomic formulas in 1. by using the methods in step 2 a finite number of times.

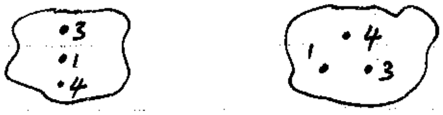
<u>Note:</u> If an object or statement has a mathematical description, it can be shown that there is a formula in LOST which will describe it.

Justification of the axioms

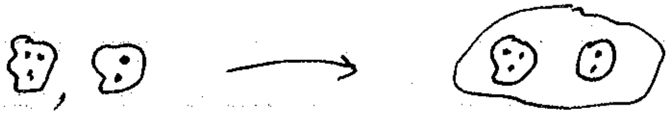
1. Null set axiom :



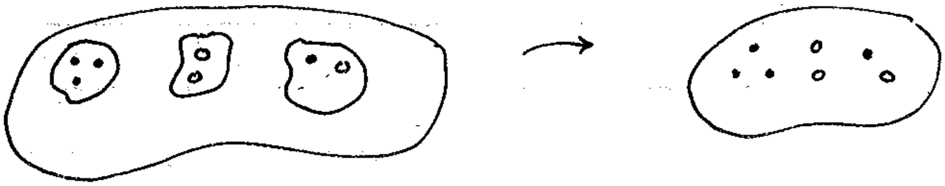
2. Extensionality Axiom :



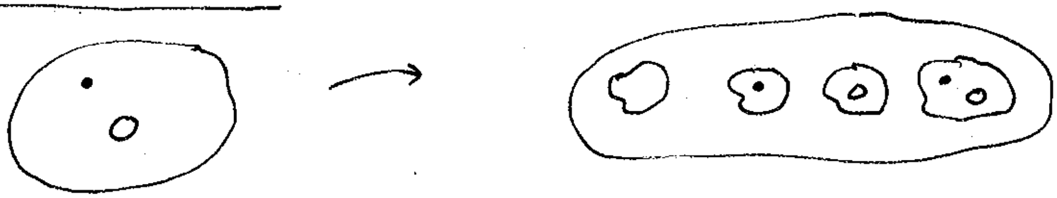
3. Pairing axiom :



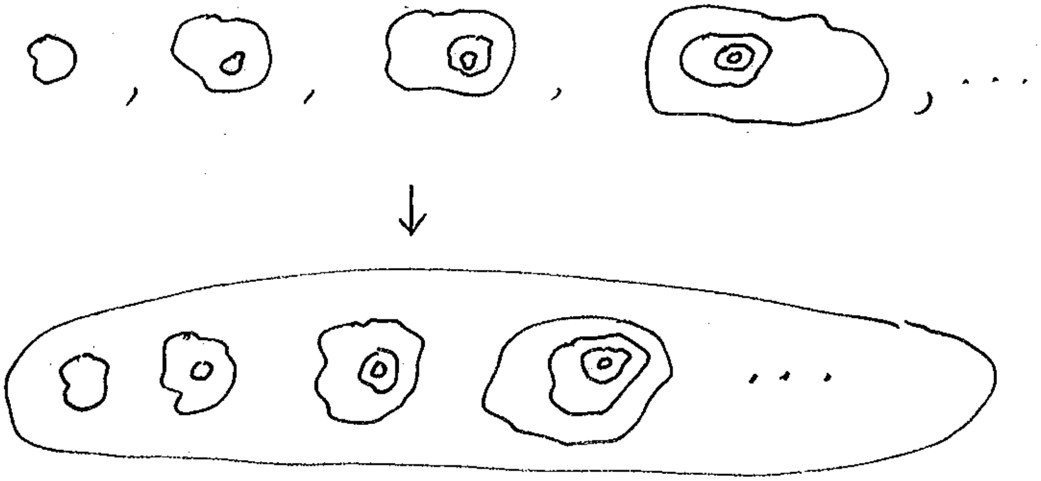
4. Union axiom :



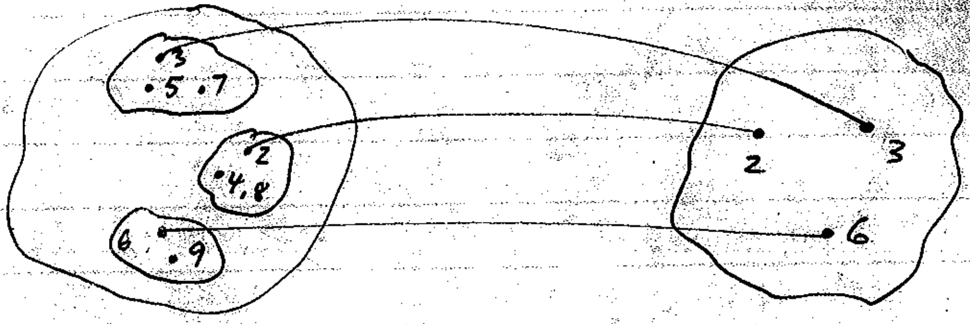
5. Power Set Axiom :



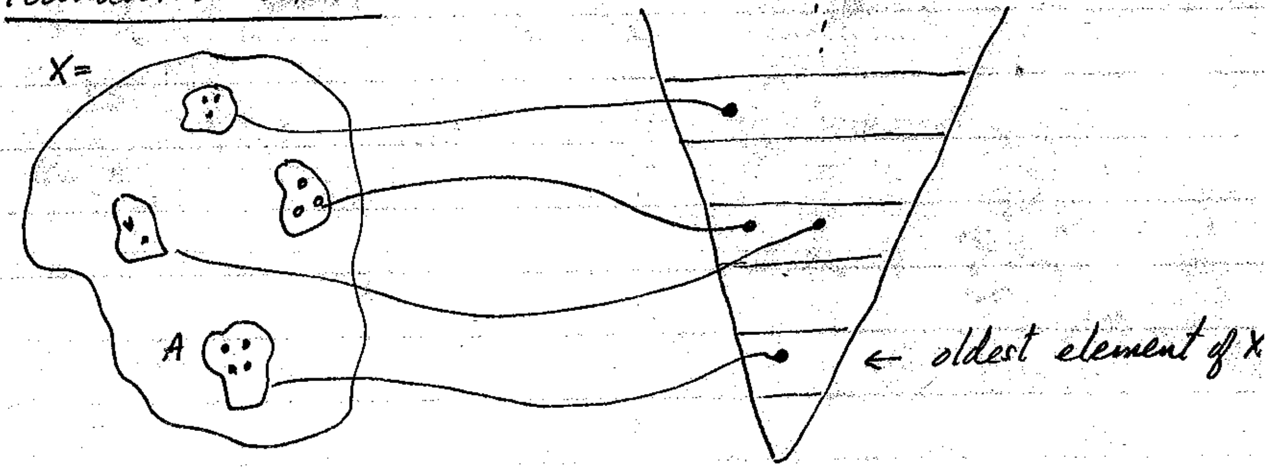
6. Infinity axiom :



7. Axiom of choice



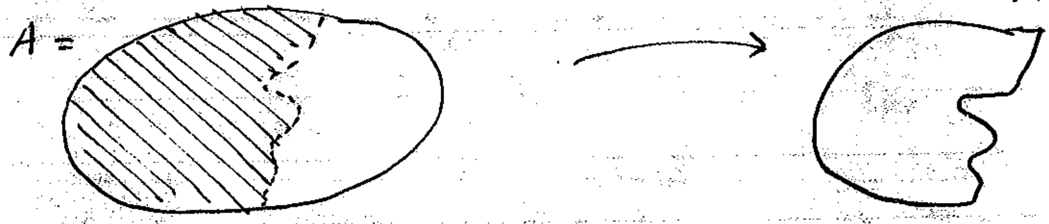
8. Foundation axiom



A and X cannot have elements in common

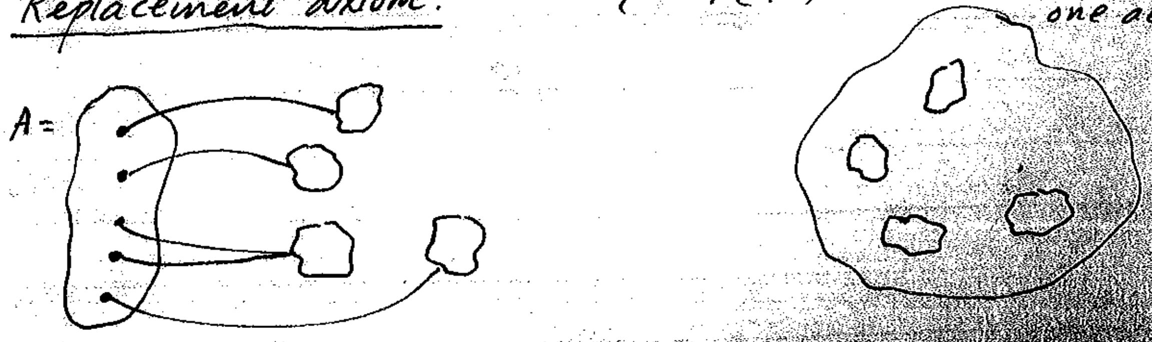
9. Separation Axiom

$\{x \in A : \varphi(x) \text{ is true}\}$



10. Replacement axiom.

$\{b : \varphi(a,b) \text{ is true for at least one } a \in A\}$



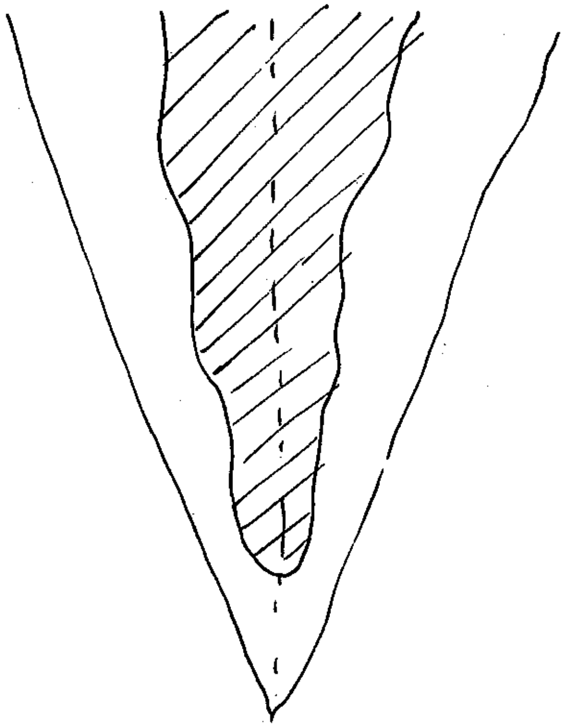
Lect. #6 Sets & Proper classes

In many situations we usually want to talk about certain collections which are too "big" to be sets

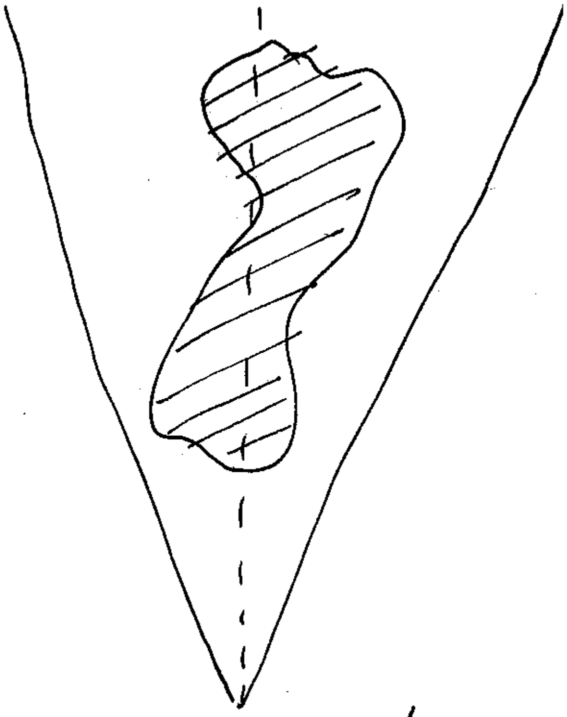
For example, consider the following collections

1. $V = \{x : x = x\}$
2. $\Sigma = \{x : x \text{ has exactly one element}\}$
3. $\Omega = \{x : x \text{ is an ordinal}\}$

It can be shown that none of these collections is a set - yet we know exactly what is and what isn't in each collection.



A typical class



A typical set.

Def. A class is any collection of the form $\{x : \varphi(x) \text{ holds}\}$, where $\varphi(x)$ is a formula in L.O.S.T. (with parameters allowed)

Fact: All sets are classes.

If a_i is a particular set, then $\{x_j : x_j \in a_i\}$ is a class because $x_j \in a_i$ is a formula in LOST

Def. A class that is not a set is called a proper class.

Examples

$V = \{x : x = x\}$ is a proper class

$\Omega = \{x : x \text{ is an ordinal}\}$ is a proper class

$D = \{x : \text{cardinality of } x = \omega\}$ is a proper class

Qu: 1. Is $\{x : x \neq x\}$ a proper class?

2. Is $\{x : x \notin x\}$ a proper class?

Proof:

1. We know from logic that $x = x$ for any x. So $\{x : x \neq x\} = \emptyset$ and is not a proper class.

2. Let $R = \{x : x \notin x\}$. Suppose R is a set. Then $R \in R$ or $R \notin R$

But if $R \in R$ then $R \notin R$ by the def. of R.

And if $R \notin R$, then $R \in R$ by the def. of R. Hence we have a contradiction. So R cannot be a set. So R is a proper class.

(It can be shown that $R = V$ because of the Foundation Axiom.)

Using the notion of a class we can greatly simplify the Separation Axiom and the Replacement Axiom.

<u>Separation Axiom</u> If $\varphi(x)$ is any formula in L.O.S.T. and A is a set then

$\{x \in A : \varphi(x) \text{ holds}\}$ is a set

<u>Separation Axiom (class form)</u>. If $\mathscr{C}$ is any class and A is a set then

$\mathscr{C} \cap A$ is a set

<u>Replacement Axiom</u>: If $\varphi(x, y)$ is any <u>function-type formula</u> in L.O.S.T. and A is a set, then $\{b : \varphi(a, b)$ is true for at least one a in $A\}$ is a set.

<u>Replacement Axiom (class form)</u>: If $\mathcal{F}$ is any <u>class-function</u> and A is a set, then

$\mathcal{F}[A]$ is a set

Operations on classes:

A proper classes is in a sense an "incomplete object". In Cantor's words, it is a "many" that cannot be considered as a "one".

So it is meaningless to ask questions such as: Is $V \in V$?
This is because only "completed objects" (or sets) are allowed to be members.

We can however define many natural operations on classes.

Def. Let $\mathcal{A} = \{x : \varphi(x) \text{ holds}\}$
$\mathcal{B} = \{x : \psi(x) \text{ holds}\}$ $\varphi, \psi \in L.O.S.T.$

We define

$$\mathcal{A} \cap \mathcal{B} = \{x : \varphi(x) \& \psi(x) \text{ holds}\}$$
$$\mathcal{A} \cup \mathcal{B} = \{x : \varphi(x) \vee \psi(x) \text{ holds}\}$$
$$\mathcal{A} - \mathcal{B} = \{x : \varphi(x) \& (\neg\psi(x)) \text{ holds}\}$$
$$\mathcal{A}^c = \{x : \neg\varphi(x) \text{ holds}\}$$

We say that

$\mathcal{A} \subseteq \mathcal{B}$ if $\varphi(x) \Rightarrow \psi(x)$ and

$\mathcal{A} = \mathcal{B}$ if $(\varphi(x) \Rightarrow \psi(x)) \& (\psi(x) \Rightarrow \varphi(x))$.

Lect. #7 Ordered sets:

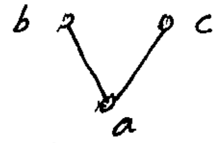
Recall that a relation R on a set A is anti-symmetric if for any $a, b \in A$ with $a \neq b$, $aRb \Rightarrow b \not R a$.

We say that R is asymmetric if for any $a, b \in A$, $aRb \Rightarrow b \not R a$.

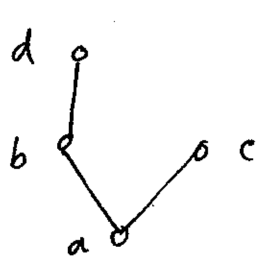
Def. An ordering on a set A is a binary relation on A which is reflexive, anti-symmetric, and transitive.
A strict ordering on A is a binary relation on A which is asymmetric and transitive.

Example

1. Let $R = \{\langle a,a\rangle, \langle a,b\rangle, \langle a,c\rangle, \langle b,b\rangle, \langle c,c\rangle\}$
Then R is an ordering on $\{a,b,c\}$



2. Let $S = \{\langle a,b\rangle, \langle a,c\rangle, \langle a,d\rangle, \langle b,d\rangle\}$.
Then S is a strict ordering on $\{a,b,c,d\}$



With any ordering R on A we can associate a strict ordering R_s on A by letting

$$R_S = R - \{\langle a,a\rangle : a \in A\}$$

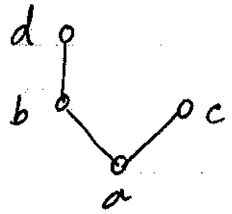
And with any strict ordering S we can assocate an ordering S_R by letting

$$S_R = S \cup \{\langle a,a\rangle : a \in A\}.$$

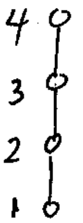
We usually denote ordering by "$\leq$" and strict ordering by "$<$". Basically "$a < b$" means "$a \neq b$ and $a \leq b$."

<u>Def.</u> Let $\langle A, \leq\rangle$ be an ordered set. We say that a and b are <u>comparable</u> if $a \leq b$ or $b \leq a$.

An ordering on A is called a <u>linear order</u> if any two elements of are comparable.



b & c are not comparable
d & c are not comparable



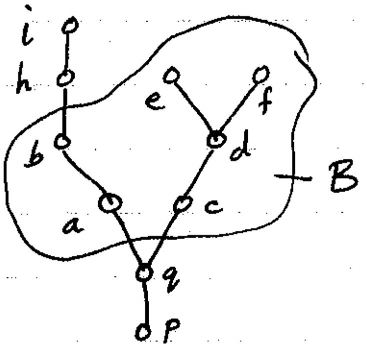
A linear ordering.

Def. Let $\langle A, \le \rangle$ be an ordered set and B be a subset of A. We say that

(i) b is the smallest element of B if
$b \le x$ for all $x \in B$

(ii) b is a minimal element of B if
there is no x in B with $x < b$.

Example



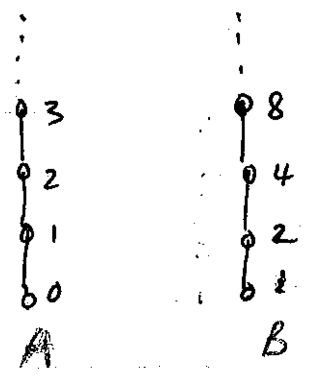
$A = \{a, b, c, d, e, f, g, h$
$i, p, q\}$

a & c are both minimal elements of B
B has no smallest element.

p is the smallest element of A
p is also a minimal element of A

Def. We say that two ordered sets $\langle A, <_1 \rangle$ & $\langle B, <_2 \rangle$ isomorphic if we can find a bijection $f: A \to B$ such that for any $x, y \in A$

$$x <_1 y \Rightarrow f(x) <_2 f(y)$$



$f: A \to B$
$f(k) = 2^k$

These two ordering are isomorphic.

Def. An ordered set $\langle A, \leq \rangle$ is said to be well-founded if every non-empty subset of A has a minimal element

Ex. $\langle \mathbb{N}, \leq \rangle$ is well-founded
$\langle \mathbb{Z}, \leq \rangle$ is not well-founded

Proposition 1 (AC) $\langle A, \leq \rangle$ is well-founded $\Leftrightarrow$ there is no sequence $\langle a_n \rangle$ in A such that $a_1 > a_2 > a_3 > \cdots$

Proof: ($\Rightarrow$): Suppose there is a sequence $\langle a_n \rangle$ in A such that $a_1 > a_2 > a_3 > \cdots$. Let $B = \{a_1, a_2, a_3, \cdots\}$. Then B clearly has no minimal element. Hence $\langle A, \leq \rangle$ is not well-founded.

($\Leftarrow$) Suppose $\langle A, \leq \rangle$ is not well-founded. Then we can find a subset B which has no minimal element. Let a_1 be any element of B. Since a_1 is not a minimal element of B we can find an element $a_2 \in B$ such that $a_1 > a_2$. Again since a_2 is not a minimal element of B we can find $a_3 \in B$ such that $a_1 > a_2 > a_3$ Proceeding inductively in this manner we will get a sequence $\langle a_n \rangle$ such that $a_1 > a_2 > a_3 > \cdots$ Hence the results follow.

Principle of Mathematical Induction

Let $P(n)$ be a statement for each $n \in \mathbb{N}$. If

1. $P(0)$ is true and
2. $(\forall n \in \mathbb{N})\ [P(n) \Rightarrow P(n+1)]$

then $(\forall n \in \mathbb{N})\ P(n)$ is true.

Proof: Suppose the conclusion does not hold Then we can find an n such that $P(n)$ is false. Let n_0 be the smallest n such that $P(n)$ is false. Then $n_0 > 0$ because $P(0)$ is true. And $P(n_0 - 1)$ must be true (because n_0 was the smallest n for which $P(n)$ is false). But from 2. we get

$$P(n_0 - 1) \Rightarrow P(n_0)$$

Hence $P(n_0)$ must be true. Hence we have a contradiction. So the conclusion follows.

Def. We say that the ordered set $\langle A, \leq \rangle$ is *well-ordered* if any non-empty subset of A has a *smallest* element.

Proposition 2: (Induction on well-ordered sets)
Let $\langle A, \leq \rangle$ be a well-ordered set, and for any element $x \in A$, let $A_x = \{a \in A : a < x\}$
Also let $a_0 =$ smallest element of A and P be a property. If

1. $P(a_0)$ is true, and
2. for each $x \in A$, $[P(a)$ true for each $a \in A_x] \Rightarrow P(x)$

then $P(x)$ is true for all $x \in A$.

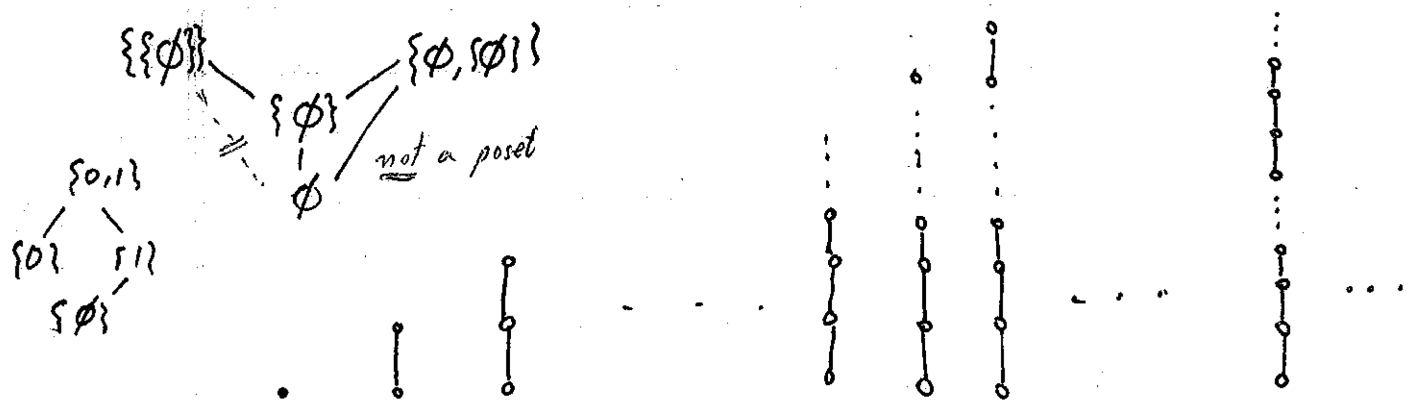
Lect. #8

Ch. 3 - Ordinal Numbers

Recall that an ordered set $\langle A, < \rangle$ was said to be <u>well-ordered</u> if every <u>non-empty</u> subset of A has a smallest element.

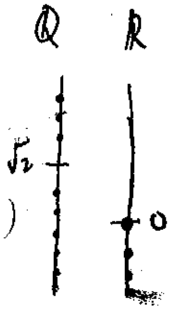
<u>Examples</u>

1. $\langle \mathbb{N}, <_{\mathbb{N}} \rangle$ is a well-ordered set.
2. $\langle \mathcal{P}(\{0,1\}), \subseteq \rangle$ is well-founded but not well-ordered
3. $\langle \mathbb{Z}, <_{\mathbb{Z}} \rangle$ and $\langle \mathbb{R}, <_{\mathbb{R}} \rangle$ are not well-ordered.



<u>Some well-ordered sets.</u> (above)
(Notice that each set has a certain "length" associated with it.)

<u>Fact:</u> Every well-ordered set is linearly ordered (see exercises for ch. 2)



<u>Def.</u> Let $\langle A, < \rangle$ be a linearly ordered set. A set $B \subseteq A$ is called an <u>initial segment</u> if (i) $B \neq A$ and
(ii) for any $b \in B$, $x < b \Rightarrow x \in B$

$(-\infty, 0] \neq \mathbb{R}_a = \{x : x < a\}$ for any a , $(-\infty, \sqrt{2}) \cap \mathbb{Q} \neq \mathbb{Q}_a$ for any $a \in \mathbb{Q}$

Proposition 1: Let $\langle W, < \rangle$ be a well-ordered set and S be an initial segment of $\langle W, < \rangle$. Then there is an element $a \in W$ such that

$$S = \{x \in W : x < a\}$$

Proof: Let $A = W - S$. Since $S \neq W$, A is a non-empty set and as $\langle W, < \rangle$ is a wellorderd set, A has a smallest element. Let a be the smallest elemant of A.
Now if $x < a$, then $x \notin A$ (because a was the smallest element of A), so $x \in S$
And if $x \geq a$, then $x \notin S$ (because if $x \in S$, then a would have to be in S since S is an initial segment). Hence

$$S = \{x \in W : x < a\}$$

Recall that $\langle W_1, <_1 \rangle$ and $\langle W_2 <_2 \rangle$ are *isomorphic* if there is a bijection $f : W_1 \to W_2$ such that $a <_1 b \Rightarrow f(a) <_2 f(b)$. The function f is called an *isomorphism* from W_1 to W_2.
We will denote the initial segment $\{x \in W : x < a\}$ by $W[a]$
Let $f : W \to W$ be a function on a well-ordered set $\langle W, < \rangle$. We say that f is *increasing* if $a < b \Rightarrow f(a) < f(b)$.

Proposition 2: If $\langle W, < \rangle$ is a w.o. set and $f : W \to W$ is an increasing function, then $f(x) \geq x$ for each $x \in W$.

Proof: Let $A = \{x \in W : f(x) < x\}$. We will show that $A = \emptyset$. This will prove the result. Suppose $A \neq \emptyset$. Then A has a smallest element, a say.

Now $f(a) < a$ bec. $a \in A$

So $f(f(a)) < f(a)$ bec. f is increasing.

Hence $f(a) \in A$. But this contradicts the fact that a was the smallest element of A. Hence $A = \emptyset$ and we are done.

Corollary 3:

(a) No w.o. set $\langle W, < \rangle$ is isomorphic to an initial segment of itself.

(b) The identity function is the only isomorphism from a w.o. set to itself

(c) If $\langle W_1, <_1 \rangle$ and $\langle W_2, <_2 \rangle$ are isomorphic, then there is only one isomorphism from W_1 to W_2.

Proof: Do for Home work (Provide all details)

(Hint: See textbook p. 137)

Theorem 4: Let W_1 and W_2 be w.o. sets. Then exactly one of the following holds.

(a) $W_1 \cong W_2$

(b) $W_1 \cong W_2[b]$ for some $b \in W_2$

(c) $W_2 \cong W_1[a]$ for some $a \in W_1$.

Skip

Proof: Define the set of ordered pairs $f \subseteq W_1 \times W_2$ as follows: Let

$$f = \{\langle x, y\rangle \in W_1 \times W_2 : \quad W_1[x] \cong W_2[y]\}$$

We will first show that f is an injective function.

Suppose $\langle x, y\rangle$ and $\langle x, y'\rangle$ are both in f.
Then $W_1[x] \cong W_2[y]$ and $W_1[x] \cong W_2[y']$.
So $W_2[y] \cong W_2[y']$. Hence $y = y'$
(If $y < y'$ then $W_2[y']$ would be isom. to an initial seg. of itself and if $y' < y$, then $W_2[y]$ would be isom. to an init. seg. of itself And both are forbidden by Cor. 3(a)]
Hence f is a function.

Now suppose $f(x_1) = f(x_2)$. TLet $y = f(x_1)$.
Then $W_1[x_1] \cong W_2[y]$ and $W_1[x_2] \cong W_2[y]$
So $W_1[x_1] \cong W_2[x_2]$ and hence $x_1 = x_2$ just as above. So f is injective.

Now suppose $x_1 < x_2$. Let $y_1 = f(x_1)$ and $y_2 = f(x_2)$. Then $y_1 \neq y_2$ bec. f is injective. And If $y_1 > y_2$, then

$$\begin{aligned} W_1[x_2] \cong W_2[y_2] &= \text{an init. seg. of } W_2[y_1] \\ &\cong \text{an init seg. of } W_1[x_1] \\ &= \text{an init seg. of } W_2[x_2] \end{aligned}$$

which is forbidden by Cor. 3(a).
Hence $y_2 > y_1$. Thus

$$x_1 < x_2 \implies f(x_1) < f(x_2)$$

From this it follows that f is an isomorphism from $dom(f)$ to $ran(f)$. There are cases:

<u>Case (a)</u> : $dom(f) = W_1$ and $ran(f) = W_2$.
In this case $W_1 \cong W_2$ and we are done.

<u>Case (b)</u> : $dom(f) = W_1$ and $ran(f) \neq W_2$
In this case we must show that $ran(f)$ is an init. seg. of W_2.
Supp. $y \in ran(f)$ and $y' < y$. Then
$$W_2[y] \cong W_1[x] \quad \text{for some } x \in W_1$$
Let $h: W_2[y] \to W_1[x]$ be this isomorphism.
Then $W_2[y'] \cong W_1[h(y')]$. So $y' \in ran(f)$
Hence vran(f) is an init. seg. of W_2.
So $W_1 \cong$ an init. seg. of W_2.

<u>Case (c)</u> : $dom(f) \neq W_1$ and $ran(f) = W_2$.
This is similar to case (b) above. We get $W_2 \cong$ an init. seg. of W_1

<u>Case (d)</u> : $dom(f) \neq W_1$ and $ran(f) \neq W_2$
This case cannot happen.
Let $a =$ smallest element not in $dom(f)$
$b =$ " " in $ran(f)$.
Then we can show that
$$W_1[a] \cong W_2[b]$$
But this would mean that $\langle a, b\rangle \in f$
i.e. $a \in dom(f)$ & $b \in ran(f)$ which is a contradiction.

Example: Supp. $x \in x$, ~~then~~ let $a = \{x\}$. Then by the Foundation axiom, a must have a minimal (w.r.t "$\in$") element. ~~But a has only one element x~~, so x must be the minimal element ~~and x~~ ~~So~~ $\therefore a \cap x$ must be $\emptyset$. But $x \in a$ & $x \in x$, so $x \in a \cap x$. $\therefore a \cap x \neq \emptyset$ a contradiction. Hence $(\neg \exists x)(x \in x)$.

Lect. #9

Ordinals

In set theory all the objects we consider are made up of sets. The natural numbers themselves are sets. We define

$$0 = \emptyset$$
$$1 = \{0\}$$
$$2 = \{0,1\}$$
$$3 = \{0,1,2\}$$
$$\vdots$$
$$n = \{0,1,2,\ldots,n-1\}$$
$$\vdots$$

Notice that each natural number is just the set of all preceding nat. nos. So we might try to define more objects by following this idea

← all the nat. nos.!

$$\omega = \{0,1,2,3,\ldots\}$$
$$\omega+1 = \{0,1,2,3,\ldots,\omega\}$$
$$\vdots$$

This naive construction gives us an idea of what are ordinals. We will see later that the ordinals are the "back-bone" of the universe of sets.

Def. A set T is said to be transitive if $a \in b$ and $b \in T \Rightarrow a \in T$.

$C = \{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}$ is also transitive

Ex. $A = \{\phi, \{\phi\}\}$ is a transitive set

$B = \{\{\phi\}, \{\{\phi\}\}\}$ is not transitive

beeause $\phi \in \{\phi\}$ & $\{\phi\} \in B$ but $\phi \notin B$.

Def. A set α is said to be an ordinal if (i) α is transitive

(ii) $\in$ is a strict well-ordering on α

Ex. 1. All the natural numbers and ω and $\omega+1$ are ordinals

2. $\{\phi, \{\phi\}, \{\{\phi\}\}\}$ is a transitive set but it is not well-ordered by $\in$.
(Prove for H.W.)

Proposition 5:

(a) If α is an ordinal then $\alpha \notin \alpha$

(b) If α is an ordinal, then so is $\alpha \cup \{\alpha\}$

(c) If α is an ordinal and $x \in \alpha$, then x is also an ordinal.

Proof.

(a) Suppose $\alpha \in \alpha$. Let $x = \alpha$. Then $x \in \alpha$. But since $x = \alpha$, $x \in x$. So α has an element x such that $x \in x$. But this contradicts the fact that $\in$ is a strict well-ordering on α

(b) Let $T = \alpha \cup \{\alpha\}$. We want to show that T is transitive. Suppose $a \in b$ and $b \in T$. There are two cases:

<u>Case (i)</u> : $b \in \alpha$

In this case $a \in b$ and $b \in \alpha$. Since α is transitive $a \in \alpha$. $\therefore$ $a \in T$

<u>Case (ii)</u> $b \in \{\alpha\}$, i.e. $b = \alpha$

In this case $a \in b$ and $b = \alpha$. $\therefore$ $a \in \alpha$ So $a \in T$

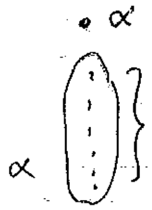
So in either case $a \in b \wedge b \in T \rightarrow a \in T$.

$\therefore$ T is transitive.

We must show that $\langle T, \in \rangle$ is a w.o. set.

We know that $\langle \alpha, \in \rangle$ is w.o. set and since $\alpha \in T$, we see that

for each $\beta \in \alpha$, $\beta \in \alpha$.



Also $\langle T, \in \rangle$ is a p.o. set

<u>Let</u> S be any non-empty subset of T.

<u>Case (i)</u> $S - \{\alpha\} = \emptyset$

In this case $S = \alpha$ and α is the smallest member of

<u>Case (ii)</u> $S - \{\alpha\} \neq O$.

In this case $S - \{\alpha\}$ is a non-empty subset of α.

So $S - \{\alpha\}$ has a smallest element bec. $\langle \alpha, \in \rangle$ is w.o.

This smallest element will be the smallest element of S bec. α is the largest element of T.

(b) We have to show that $\alpha \cup \{\alpha\}$ is a transitive set and $\in$ is a strict well-ordering on α. (Provide the details for H.W.)

(c) Let α be an ordinal and $x \in \alpha$. We first show that x is transitive. Suppose $u \in v$ and $v \in x$. Since $v \in x$ and $x \in \alpha$, we get $v \in \alpha$. And since $u \in v$ and $v \in \alpha$, we get $u \in \alpha$. So $u, v,$ and x are all elements of α. But $\in$ is a strict well-ordering on α. So we must have

$u \in x$ bec. $u \in v$ and $v \in x$

We will now show that $\in$ is a strict well-ordering on x. Since α is transitive and $x \in \alpha$, we must have $x \subseteq \alpha$. So x will inherit the well-ordering property of $\in$ from α.

Hence x is an ordinal.

<u>Conventions</u>:

1. The ordinal $\alpha \cup \{\alpha\}$ is called the <u>successor</u> of α and is denoted by $\alpha+1$.
2. If α is an ordinal, we usually write $\beta < \alpha$ instead of "$\beta \in \alpha$" because we want to focus on the order in α – we don't want to focus on the elements of α.

Def. An ordinal α is said to be a successor ordinal if there is a an ordinal β such that $\alpha = \beta + 1$.

An ordinal that is not a successor ordinal is called a limit ordinal

Examples

$1, 2, 3, \omega+1, \omega+12$ are all succ. ord.

$0, \omega, \omega+\omega, \omega+\omega+\omega$ are limit ordinals

0 is called the trivial limit ordinal. From now on all limit ordinals will be non-trivial

Theorem 6: Let α, β and γ be ordinals

(a) If $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$

(b) If $\alpha < \beta$, then $\beta \not< \alpha$

(c) Every non-empty set of ordinals has a smallest element.

Proof: (a) Suppose $\alpha < \beta$ and $\beta < \gamma$. Then $\alpha \in \beta$ and $\beta \in \gamma$. Since γ is transitive we get $\alpha \in \gamma$. Hence $\alpha < \gamma$.

(b) Suppose $\alpha < \beta$. If $\beta < \alpha$ also, then we would have $\alpha < \beta$ and $\beta < \alpha$. So by part (a) $\alpha < \alpha$. But this means that $\alpha \in \alpha$ which contradict. Proposition 5(a). Hence we must have $\beta \not< \alpha$.

(c) Let A be any non-empty set of ordinals. Then we can find an ordinal $\alpha \in A$. Now consider the set $\alpha \cap A$.
If $\alpha \cap A = \emptyset$, then α will be the smallest element of A.
And if $\alpha \cap A \neq \emptyset$, then $\alpha \cap A \subseteq \alpha$
But we know that $\langle \alpha, \in \rangle$ is a well-ordered set. So $\alpha \cap A$ will have a smallest element, β say, in $\langle \alpha, \in \rangle$. This β will be the smallest element of A

[If A had some element γ which was smaller than β, then $\gamma < \beta$ and $\beta < \alpha$ So $\gamma < \alpha$, i.e. $\gamma \in \alpha$. So $\gamma \in \alpha \cap A$ and this would contradict β being the smallest element of $\alpha \cap A$.]

Lect. #10
skip

Def. If $\langle W_1, \leq_1 \rangle \cong$ an init. seg. of $(W_2, \leq_2)$ we say that W_1 is shorter than W_2 and write $W_1 \prec W_2$.

Induction Principle: (for W.O. SETS)
Let P be a property of sets. Suppose that for every well-ordered set W we have

(*) If every w.o. set W' with $W' \prec W$ has property P, then W has property P.

Then every w.o. set has property P.

Proof: Suppose there is a w.o. set W which fails to have property P. Then by (*) there must be a shorter w.o. set which does not have property P.
Let $a \in W$ be the smallest element of W such that $P(W[a])$ fails.
Then $P(W[b])$ is true for all $b < a$.
So by (*) we must have $P(W[a])$ is true, which is a contradiction.
Hence there is no. w.o. set W ~~which~~ for which property P fails.

Theorem 7: Every well-ordered set $\langle W, < \rangle$ is isomorphic to a unique ordinal.

skip. Proof: First observe that if $\langle W, < \rangle \cong \langle \alpha, \in \rangle$ and $\langle W, < \rangle \cong \langle \beta, \in \rangle$ then $\langle \alpha, \in \rangle \cong \langle \beta, \in \rangle$. And since no ordinal isomorphic to a smaller ordinal (= an init. seg. of the first ordinal) it follows that $\alpha = \beta$. So if $\langle W, < \rangle$ is isomorphic to an ordinal that ordinal will be unique.

We will prove that every well-ordered set is isom. to an ordinal by the Ind. Princ. for w.o. sets.

Let $P(W,<)$ be the property:
"There exist an ordinal α such that $\langle W, < \rangle \cong \langle \alpha, \in \rangle$"

We will show that
(*) If every w.o. set W' with $W' \prec W$ has property P, then W has property P.

The result will follow from this. So suppose that every w.o. set W' with $W' \prec W$ has property P. Then $W[a]$ will have property P for each $a \in W$. Let α_a be the unique ordinal $\cong W[a]$ and put

$$\beta = \{\alpha_a : a \in W\}.$$

Then β is a set because of the Replacement Ax.

Also β is strictly well-ordered by "$\in$" because it is a set of ordinals. We further claim that β is a transitive set.

Indeed suppose $\gamma \in \alpha_a$ and $\alpha_a \in \beta$. Let $f: W[a] \to \alpha_a$ be the isom. from $W[a]$ to α_a and put $c = f^{-1}(\gamma)$. Then $W[c]$ will be isom. to γ. So γ will be in β. Hence β is a transitive set. Thus β is an ordinal.

Now let $g: W \to \beta$ be defined by

$$g = \{\langle a, \alpha_a \rangle : a \in W\}$$

Then it is easy to see that g will be an isomorphism from $\langle W, < \rangle$ to $\langle \beta, \in \rangle$. Thus W will have property and we will be done.

Let us now recall two basic theorems of Arithmetic.

Recall

<u>Induction Principle (for $\mathbb{N}$)</u> Let $P(x)$ be a property such that

(a) $P(0)$ is true and

(b) $(\forall n \in \mathbb{N})\ [P(n) \Rightarrow P(n+1)]$ is true

Then $P(n)$ will be true for each $n \in \mathbb{N}$.

<u>Recursion Principle</u> (for $\mathbb{N}$). Let $G : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a function and c be any constant in $\mathbb{N}$. Then we can define a unique seq. $\langle a_n \rangle$ by letting

(a) $a_0 = c$ and

(b) $a_{n+1} = G(a_n, n)$ for all $n \in \mathbb{N}$.

We have the following analogues for ordinals

<u>The Transfinite Induction Principle</u>:

Let $P(\alpha)$ be a property such that

(a) $P(0)$ is true,

(b) for any ordinal α, $P(\alpha) \Rightarrow P(\alpha+1)$

(c) for any limit ordinal $\lambda > 0$,

$$[(\forall \beta < \lambda)\ P(\beta)] \Rightarrow P(\lambda)$$

Then $P(\alpha)$ will be true for all ordinals

Lect. #11. <u>Ordinal Arithmetic</u>

Recall that if α was an ordinal we define $\alpha \cup \{\alpha\}$ to be the <u>successor</u> of α. We usually denote $\alpha \cup \{\alpha\}$ by $s(\alpha)$ [or by $\alpha+1$ when there is no room for confusion]

<u>Def.</u> (<u>Ordinal addition</u>)

For each ordinal β we define $\beta+\alpha$ by transfinite recursion on α as follows:

(a) $\beta + 0 = \beta$ $\qquad \alpha+0=\alpha$

(b) $\beta + (\alpha+1) = S(\beta+\alpha)$ $\qquad \alpha+(\beta+1) = (\alpha+\beta)+1$

(c) $\beta + \lambda = \sup\{\beta+\alpha : \alpha<\lambda\}$ if λ is a limit ordinal

<u>Examples</u>:

$$\beta+1 = S(\beta) = \xrightarrow{\beta} \cdot$$

$$\beta+2 = S(S(\beta)) = \xrightarrow{\beta} \cdot\ \cdot$$

$$\beta+\omega = \sup\{\beta+n : n<\omega\} = \xrightarrow{\beta} \cdot\ \cdot\ \overset{\omega}{\cdot} \cdots\cdots$$

<u>NB</u> $\times$ $0+\alpha = \alpha$ (not obvious) can be proved by transf. ind.

$$2+\omega = \sup\{2+n : n<\omega\} = \omega$$

$$\omega+2 = s(s(\omega)) \neq \omega = 2+\omega$$

<u>Interpretation</u>

$$\beta+\alpha = \xrightarrow{\beta}\ \xrightarrow{\alpha}$$

= order type of set with two parts: a w.o. set with order type β and a w.o. set with order type α above

Question: What is $0+\beta$? $\qquad 0+\beta = \beta$
(proved by transf. induction on β)

<u>Proposition 8</u> : For any ordinals α, β, and γ we have $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$

<u>Proof</u>: Let α and β be arbitrary but fixed (i.e. α and β are considered as parameters) We will prove the result by transfinite ind. on γ.

Suppose $\gamma = 0$. Then

$$\begin{aligned}(\alpha+\beta)+0 &= \alpha+\beta \\ &= \alpha+(\beta+0).\end{aligned}$$

So the result is true for $\gamma = 0$.

Suppose that the result is true for γ. We must prove it for $\gamma+1$. Now we have

$$\begin{aligned}(\alpha+\beta)+(\gamma+1) &= \big((\alpha+\beta)+\gamma\big)+1 && \text{by the def. of additio} \\ &= \big(\alpha+(\beta+\gamma)\big)+1 && \text{bec. result is true for } \gamma \\ &= \alpha+\big((\beta+\gamma)+1\big) && \text{by the def. of addition} \\ &= \alpha+\big(\beta+(\gamma+1)\big) && \text{by the def. of add. again.}\end{aligned}$$

Finally suppose that the result is true for all $\gamma < \lambda$ where λ is a limit ordinal. We must prove it for λ. Now

$$\begin{aligned}(\alpha+\beta)+\lambda &= \sup\{(\alpha+\beta)+\gamma : \gamma<\lambda\} \\ &= \sup\{\alpha+(\beta+\gamma) : \gamma<\lambda\} && \text{bec. result is true for all } \alpha<\lambda. \\ &= \alpha+\sup\{\beta+\gamma : \gamma<\lambda\} && \text{bec. } \sup\{\beta+\gamma : \gamma<\lambda\} \\ & && \text{is a limit ordinal} \\ &= \alpha+(\beta+\lambda)\end{aligned}$$

So by the Transfinite Ind. Princ. the result is true for all γ. Since α & β were arb., it is true for all α, β, and γ.

Prop 8! (g) $0+\alpha = \alpha$ Use ind. on α

(a) $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$ Ind. on γ

(b) $\beta < \gamma \Rightarrow \alpha+\beta < \alpha+\gamma$ Ind. on γ, start at $\gamma = 1$

(c) $\alpha+\beta < \alpha+\gamma \Rightarrow \beta < \gamma$,

Supp. $\beta \not< \gamma$. Then $\gamma \leq \beta$

$\gamma = \beta \Rightarrow \alpha+\beta = \alpha+\gamma$ contradic.

$\gamma < \beta \rightarrow \alpha+\gamma < \alpha+\beta$ contradic

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

$\Rightarrow \beta = \gamma$

Supp. $\beta < \gamma$

then $\alpha+\beta < \alpha+\gamma$ contra

Supp. $\gamma < \beta$

then $\alpha+\gamma < \alpha+$, contradiction.

(e) $\alpha \leq \beta \Rightarrow \alpha+\gamma \leq \beta+\gamma$ Ind. on γ

(f) $\alpha+\gamma < \beta+\gamma \Rightarrow \alpha < \beta$

Supp. $\alpha \not< \beta$. Then $\beta \leq \alpha$

$\therefore \beta+\gamma \leq \alpha+\gamma$ — contradiction.

In general (a) $\alpha+\beta \neq \beta+\alpha$ $\omega = 2+\omega \neq \omega+2$

(b) $\alpha < \beta \not\Rightarrow \alpha+\gamma < \beta+\gamma$

$2 < 5$ but $\omega = 2+\omega \not< 5+\omega = \omega$

(c) $\alpha+\gamma = \beta+\gamma \not\Rightarrow \alpha = \beta$.

$\alpha \leq \beta \Rightarrow \alpha+\gamma \leq \beta+\gamma$

Let $\alpha \leq \beta$ be fixed

$\underline{\gamma = 0}$: $\alpha+\gamma = \alpha+0 = \alpha \leq \beta = \beta+0 = \beta+\gamma$

Assume $\alpha+\gamma \leq \beta+\gamma$. Then

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

Assume $\alpha+\gamma \leq \beta+\gamma$ for all $\gamma < \lambda$

$$\begin{aligned}\alpha+\lambda &= \sup\{\alpha+\gamma : \gamma < \lambda\} \\ &\leq \sup\{\beta+\gamma : \gamma < \lambda\} \\ &= \beta+\lambda.\end{aligned}$$

Questions: Is it always true that

1. $\alpha+\beta = \beta+\alpha$? False
2. $\alpha<\beta \Longrightarrow \alpha+\gamma<\beta+\gamma$? False
3. $\beta<\gamma \Longrightarrow \alpha+\beta<\alpha+\gamma$? true use ind on γ

Facts: ① $\alpha+\beta<\alpha+\gamma \overset{\Leftarrow}{\Longleftrightarrow} \beta<\gamma$ ④ $\alpha+\gamma<\beta+\gamma \Rightarrow \alpha<\beta$

② $\alpha+\beta=\alpha+\gamma \Longleftrightarrow \beta=\gamma$ ③ $\alpha\leq\beta \Rightarrow \alpha+\gamma\leq\beta+\gamma$ use ind. on γ

$\Leftarrow$ ✓ use ind. on γ

(⟹) ~~is~~ easily follows.

Def. (Ordinal multiplication)

For each ordinal β we define $\beta.\alpha$ by transfinite recursion on α as follows

(a) $\beta.0 = 0$ $\alpha.0=0$

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

(c) $\beta.\lambda = \sup\{\beta.\alpha : \alpha<\lambda\}$ if λ is a limit ordinal.

Examples

$\beta.1 = \beta$

$\beta\,2 = \beta+\beta$ $\xrightarrow{\beta}\xrightarrow{\beta}$ β (2 times)

$\beta.3 = (\beta+\beta)+\beta$ $\xrightarrow{\beta}\xrightarrow{\beta}\xrightarrow{\beta}$ β (3 times)

$\vdots$

$\beta.\omega = \sup\{\beta.n : n<\omega\}$ β (ω times)

$0.\beta = 0$ proved by transf. ind. on β

$1.\beta = \beta$ (proved by transf. ind.) 1 (β times)

$2.\omega = \sup\{2.n : n<\omega\} = \omega$

$\omega.2 = \omega+\omega \neq \omega.$

Interpretation:

$\beta.\alpha =$ order type of the set which is made up up β laid out α times

$$\underbrace{\xrightarrow{\beta}\ \xrightarrow{\beta}\ \xrightarrow{\beta}\ \cdots}_{(\alpha \text{ times})}.$$

Prop. 9' (a) $\alpha.(\beta+\gamma) = \alpha.\beta + \alpha.\gamma$ Ind on γ

(b) $(\alpha.\beta)\gamma = \alpha.(\beta.\gamma)$ Ind. on γ

(c) $(\beta < \gamma \wedge \alpha \neq 0) \Rightarrow \alpha.\beta < \alpha.\gamma$ Use Ind on γ

(d) $\alpha.\beta < \alpha.\gamma \Rightarrow (\beta < \gamma \wedge \alpha \neq 0)$

$\alpha \neq 0$ bec. $0.\beta \not< 0.\gamma$

Supp. $\beta \geq \gamma$. Then $\beta = \gamma$ or $\beta > \gamma$

$\therefore$ $\alpha.\beta = \alpha.\gamma$ or $\alpha.\gamma < \alpha.\beta$ – contrad.

(e) $\alpha \leq \beta \Rightarrow \alpha.\gamma \leq \beta.\gamma$ Ind. on γ

(f) $\alpha.\gamma < \beta.\gamma \Rightarrow \alpha < \beta$

Sup $\alpha \geq \beta$. Then $\beta.\gamma \leq \alpha.\gamma$ contradict

In general

$\alpha.\beta \neq \beta.\alpha$

$(\alpha+\beta).\gamma \neq \alpha.\gamma + \beta.\gamma$ $(2+3).\omega \neq 2.\omega + 3.\omega$

$\alpha.\gamma = \beta.\gamma \not\Rightarrow \alpha = \beta$ $2.\omega = 5.\omega \not\Rightarrow 2 \neq 5.$

Proposition 9: For any ordinals α, β, and γ γ we have

(a) $\alpha.(\beta+\gamma) = (\alpha.\beta)+(\alpha.\gamma)$ $\qquad (\beta+\gamma).\alpha \neq \beta.\alpha+\gamma.$

(b) $(\alpha.\beta).\gamma = \alpha.(\beta.\gamma)$ $\qquad \underbrace{(\omega+3).2}_{\omega+3+\omega.2+3 \; =\omega.2+3} \neq \underbrace{\omega.2+3.}_{\omega.2+6}$

Proof: Do for H.W.

(a) Hint: use transfinite induction on γ (You'll need Proposition 8

use ind. on γ for $\Leftarrow$ (b) Hint: use transfinite induction on γ

$\Rightarrow$ easily follows (you will need ; Prop. 9(a))

Facts: ① $\alpha.\beta < \alpha.\gamma \Leftrightarrow (\beta<\gamma \wedge \alpha\neq 0)$ ④ $\alpha.\gamma < \beta.\gamma \Rightarrow \alpha<\beta$ ind. on

② $\alpha.\beta = \alpha.\gamma \Rightarrow (\beta=\gamma \vee \alpha=0)$ ③ $\alpha<\beta \Rightarrow \alpha.\gamma \leq \beta.\gamma$

③ ⇒ ④ More questions: Is it always true that

1. $\alpha.\beta = \beta.\alpha$? ✓ false
2. $(\alpha+\beta).\gamma = (\alpha.\gamma)+(\beta.\gamma)$? proj. 3 a (false)
3. $\alpha.\beta = \alpha.\gamma$ and $\alpha\neq 0 \Rightarrow \beta=\gamma$? proj 3 b (true)
4. $\alpha.\gamma = \beta.\gamma$ and $\gamma\neq 0 \Rightarrow \alpha=\beta$? proj. 3 c (false)

Def. (Ordinal exponentiation)
For each ordinal β, we define β^α by transfinite recursion on α as follows:

(a) $\beta^0 = 1$

(b) $\beta^{\alpha+1} = \beta^\alpha.\beta$

(c) $\beta^\lambda = \sup\{\beta^\alpha : \alpha<\lambda\}$ if λ is a limit ordinal.

Examples

$\beta^1 = \beta^0.\beta = 1.\beta = \beta \qquad \beta^2 = \beta.\beta \qquad \beta^3 = \beta^2.\beta = \beta.\beta.\beta$

$1^\alpha = 1$ (can be proved by transf. ind.) on α

$2^\omega = \sup\{2^n : n<\omega\} = \omega$

$\omega^2 = \omega.\omega \neq \omega.$

Proposition 10 : For any ordinals α, β, and [illegible]
we have (a) $(\alpha^{\beta}).(\alpha^{\gamma}) = \alpha^{(\beta+\gamma)}$
(b) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta.\gamma}$

$(\alpha.\beta)$ [illegible]
$(\omega.3)$ [illegible]
$\underbrace{\omega.3.\omega.3}_{\omega^2.3}$ [illegible]

Proof: Do for H.W.

Hints : For (a) you will need Prop. 8 and Prop. 9(b)
For (b) you will need Prop. 9(a) and Prop. 10(a)

Even more questions : Is it always true that

1. $\alpha^{\gamma}.\beta^{\gamma} = (\alpha.\beta)^{\gamma}$? proj 4a (F)
2. $\alpha < \beta$ and $\gamma > 0 \Rightarrow \alpha^{\gamma} < \beta^{\gamma}$? 4b (F
3. $\beta < \gamma$ and $\alpha > 1 \Rightarrow \alpha^{\beta} < \alpha^{\gamma}$? 4c (T

Facts ① $\alpha^{\beta} < \alpha^{\gamma} \overset{\Leftarrow}{\Leftrightarrow} \beta < \gamma \wedge \alpha > 1$ ④ $\alpha^{\gamma} < \beta^{\gamma} \Rightarrow \alpha < \beta$
② $\alpha^{\beta} = \alpha^{\gamma} \Rightarrow (\beta = \gamma \vee \alpha \leq 1)$ ③ $\alpha \leq \beta \Rightarrow \alpha^{\gamma} \leq \beta^{\gamma}$.

use ind. on γ for $\Leftarrow$ ($\Rightarrow$ is easily) follows.

The ordinals so far : ④ follows from ③

$0, 1, 2, 3, \ldots$ $\sup\{0,1,2,3,\ldots\} = \omega$

$\omega, \omega+1, \omega+2, \ldots$ $\sup\{\omega+n : n<\omega\} = \omega+\omega = \omega.2$

$\omega.2, \omega.3, \omega.3, \ldots$ $\sup\{\omega.n : n<\omega\} = \omega.\omega = \omega^2$

$\omega^2, \omega^3, \omega^4, \ldots$ $\sup\{\omega^n : n<\omega\} = \omega^{\omega}$

$\omega^{\omega}, \omega^{\omega^{\omega}}, \omega^{\omega^{\omega^{\omega}}}, \ldots$ $\sup\{\omega^{\omega}, \omega^{\omega^{\omega}}, \omega^{\omega^{\omega^{\omega}}}, \ldots\} = \varepsilon$

What next ? Well, $\omega^{\varepsilon} = \varepsilon$ — no advance!

$\varepsilon+1, \ldots, \varepsilon+\varepsilon = \varepsilon.2, \ldots, \varepsilon.\varepsilon = \varepsilon^2, \ldots$
$\varepsilon^{\omega}, \ldots, \varepsilon^{\omega.2}, \ldots, \varepsilon^{\omega^2}, \ldots \ldots \varepsilon^{\omega^{\omega}}, \ldots, \varepsilon^{\varepsilon}, \ldots$

1. $(\omega+2)(\omega+3) = (\omega+2).\omega + (\omega+2).3$ by Prop. 9(a)

$= \sup\{(\omega+2).n : n<\omega\} + (\omega+2)+(\omega+2)+(\omega+2)$

$= \sup\{(\omega.n)+2 : n<\omega\} + \omega + (2+\omega) + (2+\omega) + 2$ by

$= \omega.\omega + \omega + \omega + \omega + 2$ bec.

$2+\omega = $

$= \omega^2 + \omega.3 + 2$

$$\sup\{\omega.n : n<\omega\} \leqslant \sup\{(\omega.n)+2 : n<\omega\} \leqslant \sup\{\omega.(n+1) : n<\omega\}$$

$$\omega.\omega \leqslant \sup\{(\omega.n)+2 : n<\omega\} \leqslant \omega.\omega$$

$$\therefore \sup\{(\omega.n)+2 : n<\omega\} = \omega.\omega$$

$$2+\omega = \sup\{2+n : n<\omega\} = \omega$$

2. $(\omega+3)^2 = (\omega+3).(\omega+3)$

$= (\omega+3).\omega + (\omega+3).3$

$= \sup\{(\omega+3).n : n<\omega\} + (\omega+3)+(\omega+3)+(\omega+3)$

$= \omega^2 + \omega + \omega + \omega + 3$

$= \omega^2 + \omega.3 + 3$

3. $(\omega+2)^\omega = \sup\{(\omega+2)^n : n<\omega\}$

Now $\omega^n \leq (\omega+2)^n \leq (\omega^2)^n = \omega^{2n}$

So $\underbrace{\sup \omega^n}_{=\omega^\omega} \leq \sup\{(\omega+2)^n : n<\omega\} \leq \underbrace{\sup\{\omega^{2n} : n<\omega\}}_{=\omega^\omega}$

$\therefore (\omega+2)^\omega = \omega^\omega$

4. $(\omega+3)^{\omega+2} = (\omega+3)^\omega.(\omega+3)^2$

$= \omega^\omega.(\omega^2 + \omega.3 + 3)$

$= \omega^{\omega+2} + \omega^\omega.\omega.3 + \omega^\omega.3$

Lect #12 Recall that there is a theorem of Arithmetic which says that every number ≥ 1 can be uniquely represented in base a. (for $n>1$)

Let $a>1$ be a nat. no. Then for every natural no. $b \geq 1$ we can find a unique nat. no. $k \geq 1$ and unique sequences $p_1 > p_2 > p_3 \cdots > p_k$ and $q_1, q_2, \ldots, q_k$ with $1 \leq q_i \leq a-1$ such that

$$n = a^{p_1} \cdot q_1 + a^{p_2} \cdot q_2 + a^{p_3} \cdot q_3 + \cdots + a^{p_k} \cdot q_k$$

$$200{,}807 = 10^{5} \cdot 2 + 10^{2} \cdot 8 + 10^{0} \cdot 7$$

Ex. $173 = 3^4 \cdot 2 + 3^2 \cdot 1 + 3^0 \cdot 2$

$$34 = 3^3 \cdot 1 + 3^1 \cdot 2 + 3^0 \cdot 1$$

Cantor's Normal Form Theorem:

Let $\alpha > 1$ be any ordinal. Then for every ordinal $\beta \geq 1$ we can find a unique finite ordinal $k \geq 1$ and unique sequences $\gamma_1 > \gamma_2 > \cdots > \gamma_k$ and $\delta_1, \ldots, \delta_k$ with $1 \leq \delta_i \leq k-1$ such that

$$\beta = \alpha^{\gamma_1} \cdot \delta_1 + \alpha^{\gamma_2} \cdot \delta_2 + \cdots + \alpha^{\gamma_k} \cdot \delta_k$$

Ex. $(\omega+2) \cdot (\omega+3) = \omega^2 \cdot 1 + \omega^1 \cdot 3 + \omega^0 \cdot 2$ [base ω]

$$(\omega+2)(\omega+3) = 2^{\omega+\omega} \cdot 1 + 2^{\omega+1} \cdot 1 + 2^{\omega} \cdot 1 + 2^1 \cdot 1 \text{ [base 2]}$$

Goodstein Sequences

12B First observe that every natural number $m \geq 1$ can be uniquely expressed in base b with $b \geq 2$

$$m = b^{a_n} \cdot c_n + b^{a_{n-1}} \cdot c_{n-1} + \cdots + b^{a_1} \cdot c_1$$

with $1 \leq c_i \leq b-1$, $a_n > a_{n-1} > \cdots > a_2 > a_1$.

Def. The weak Goodstein sequence starting at $m \geq 1$ is defined as follows:

We take $m_0 = m$ and write m_0 in base 2.

$$m_0 = 2^{a_n} + 2^{a_{n-1}} + \cdots + 2^{a_1}$$

To get m_1 replace all the 2's by 3's and subtract 1

$$m_1 = \left(3^{a_n} + 3^{a_{n-1}} + \cdots + 3^{a_1}\right) - 1$$

Then rewrite m_1 in base 3

In general m_{k+1} is obtained from m_k which is writte in base k+ by replacing all the bases $(k+2)$ by $(k+3)$ and then subtracting 1.

Example: The weak Goodstein sequence starting at $m = 21$ begins as follows.

$$m_0 = 21 = 2^4 + 2^2 + 1$$

$$m_1 = (3^4 + 3^2 + 1) - 1 = 3^4 + 3^2 = 90$$

$$m_2 = (4^4 + 4^2) - 1 = 4^4 + 4^1 \cdot 3 + 3 = 271$$

$$m_3 = (5^4 + 5^1 \cdot 3 + 3) - 1 = 5^4 + 5^1 \cdot 3 + 2 = 642$$

$$m_4 = (6^4 + 6^1 \cdot 3 + 2) - 1 = 6^4 + 6^1 \cdot 3 + 1 = 1315$$

$$m_5 = \qquad = 7^4 + 7^1 \cdot 3 = 2422$$

$$m_6 = \qquad = 8^4 + 8 \cdot 2 + 7 = 4119$$

$$m_7 = \qquad = 9^4 + 9 \cdot 2 + 6 = 6585$$

$$m_8 = \qquad = 10^4 + 10 \cdot 2 + 5 = 10,025$$

Theorem 11 For each $m > 0$, the weak Goodstein sequence starting at m eventually terminates with $m_{k_0} = 0$ for some k_0

Proof: Let $\langle m_k \rangle_{k \geq 0}$ be the weak Goodstein sequence with $m_0 = m$. Let

$$m_k = (k+2)^{a_n} \cdot c_n + (k+2)^{a_{n-1}} \cdot c_{n-1} + \cdots + (k+2)^{a_2} \cdot c_1$$

Put

$$\alpha_k = \omega^{a_n} \cdot c_n + \omega^{a_{n-1}} \cdot c_{n-1} + \cdots + \omega^{a_1} \cdot c_1$$

Then $\alpha_0 > \alpha_1 > \alpha_2 > \cdots$. Since the ordinals are well founded this sequence of ordinals must terminate at $\alpha_{k_0} = 0$ for some k_0. Note also that $m_k \leq \alpha_k$ for each k, so $m_{k_0} \leq \alpha_{k_0} = 0 \Rightarrow m_{k_0} = 0$. This completes the proof.

Def. The strong Goodstein sequence starting at $m \geq 1$ is define in the same way as the weak one except m_k is expresed completely in base $k+2$, for each $k \geq 2$, and then we replace all the $k+2$'s by $k+3$'s and subtract 1

Example The strong Goodstein Sequence starting at 21 begins as follows:

$$m_0 = 21 = 2^{2^2} + 2^2 + 1 \qquad \approx 7.6 \times 10^{12}$$
$$m_1 = (3^{3^3} + 3^3 + 1) - 1 = 3^{3^3} + 3^3 = 7,625,597,4\ldots,\ldots$$
$$m_2 = (4^{4^4} + 4^4) - 1 \simeq 1.3 \times 10^{154} = 4^{4^4} + 4^3 \cdot 3 + 4^2 \cdot 3 + 4^1 \cdot 3 + 3$$
$$m_3 = 5^{5^5} + 5^3 \cdot 3 + 5^2 \cdot 3 + 5^1 \cdot 3 + 2 \approx 1.9 \times 10^{2184}$$
$$m_4 = 6^{6^6} + 6^3 \cdot 3 + 6^2 \cdot 3 + 6 \cdot 3 + 1 \approx 2.6 \times 10^{36,305}$$

Theorem 12: For each $m>0$, the strong Goodstein sequence starting at $m_0 = m$ eventually terminates with $m_{k_0} = 0$ for some k_0.

Proof: The proof is similar to the previous one, but in this case α_k is obtained from m_k by writing m_k completely in base $k+2$ and then replacing each $k+2$ by ω. For example the ordinals corresponding to the Strong Goodstein seq. starting at $m_0 = 21$ is as follows:

$$\begin{aligned}
\alpha_0 &= \omega^{\omega^{\omega}} + \omega^{\omega} + 1 \\
\alpha_1 &= \omega^{\omega^{\omega}} + \omega^{\omega} \\
\alpha_2 &= \omega^{\omega^{\omega}} + \omega^3 . 3 + \omega^2 . 3 + \omega^1 . 3 + 3 \\
\alpha_3 &= \omega^{\omega^{\omega}} + \omega^3 . 3 + \omega^2 . 3 + \omega . 2 + 2 \\
\alpha_4 &= \omega^{\omega^{\omega}} + \omega^3 . 3 + \omega^2 . 3 + \omega . 3 + 1 \\
\alpha_5 &= \omega^{\omega^{\omega}} + \omega^3 . 3 + \omega^2 . 3 + \omega . 3 \\
\alpha_6 &= \omega^{\omega^{\omega}} + \omega^3 . 3 + \omega^2 . 3 + \omega . 2 + 7
\end{aligned}$$

Again it is easy to see that $\alpha_0 > \alpha_1 > \alpha_2 \cdots$ so the sequence must terminate at $\alpha_{k_0} = 0$ for some k_0. And again since $m_k \leq \alpha_k$, we get that $m_{k_0} = 0$.