Set Theory
Third Lecture

27 September 2021

Zermelo Set Theory Z:

Ext, Pair, Union, Pow, Sep, Inf.

Z proves there is a unique smallest inductive set, call it $\mathbb{N}$.

X is inductive if $\emptyset \in X$ and for all x, if $x \in X$, then $s(x) = x \cup \{x\} \in X$.
successor

$\mathbb{N}$ satisfies the INDUCTION PRINCIPLE:

if $X \subseteq \mathbb{N}$ is inductive,
then $X = \mathbb{N}$.

We proved (1) For every $n \in \mathbb{N}$, either $n = \emptyset$ or $\emptyset \in n$.

A set x is transitive if f.a. y ($y \in x \rightarrow y \subseteq x$)

(2) Every $n \in \mathbb{N}$ is transitive.

Elements of $\mathbb{N}$:

$$\boxed{\emptyset} \in \mathbb{N}$$

has zero elements, why not call it 0?

$$0 := \emptyset.$$

Also:

$$\boxed{\{0\}}$$
$$\|$$
$$s(0) = s(\emptyset) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$$

has one element, why not call it 1?

$$1 := \{\emptyset\}.$$

Also:

$$s(1) = s(\{\emptyset\}) = \{\emptyset\} \cup \{\{\emptyset\}\}$$
$$= \{\emptyset, \{\emptyset\}\}$$
$$= \boxed{\{0, 1\}}$$

has two elements, why not call it 2?

$$2 := \{\emptyset, \{\emptyset\}\}$$

$$\boxed{\{0,1,2\}}$$
$$\|$$
$$3 := s(2) := 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

Define a relation $<$ on $\mathbb{N}$ by

$$n < m \;:\Longleftrightarrow\; n \in m.$$

$$n \leq m \;:\Longleftrightarrow\; n \subseteq m$$

First goal (related to HW (9) on sheet #2)

Show that $<$ is a strict total order, i.e., irreflexive, transitive, total.

Further properties of natural numbers:

(3) Every elt of a natural number is a natural number.

[$Z := \{ n \in \mathbb{N} ;$ every elt. of n is a natural number $\}$

Prove that Z is inductive.

$n = \emptyset \implies$ trivially true.

Suppose $n \in Z$, so $n \subseteq \mathbb{N}$.

$s(n) = n \cup \{ \underset{\in \mathbb{N}}{n} \} \subseteq \mathbb{N}$. So Z is inductive. Done!]

(4) Every natural number is either 0 or the successor of another number.

[$Z := \{ n \in \mathbb{N};\ n = 0$ or $\exists m \in \mathbb{N}\ n = s(m) \}$

$n = 0$ ✓

Suppose $n \in Z$, so $n \in \mathbb{N}$, and thus $s(n) \in Z$.]

(5) [DISCRETENESS OF THE ORDER]

If $n < m$, then $s(n) \leq m$.

[$n < m \iff n \in m$.

$s(n) \leq m \iff s(n) \subseteq m$.

Suppose $n \in m$. By transitivity (2), we have $n \subseteq m$.

$$\underbrace{s(n)}_{} = \underbrace{n}_{\subseteq m} \cup \underbrace{\{\underbrace{n}_{\in m}\}}_{\subseteq m} \subseteq m. \quad]$$

Theorem $(\mathbb{N}, <)$ is a strict total order with minimal element 0.

Proof. Minimality of 0:

Property ①: For each $n \in \mathbb{N}$, either $\underbrace{\emptyset = n}_{n=0}$ or $\underbrace{\emptyset \in n}_{0<n}$.

Transitivity: Need to show: if $n, m, k \in \mathbb{N}$ and $\underset{n \in m}{n < m}$ and $\underset{m \in k}{m < k}$, then $\underset{n \in k}{n < k}$

So it follows directly from property ②.

Totality of $\leq$: Homework assignment (9), sheet #2

Irreflexivity. For all $n \in \mathbb{N}$, $\underbrace{n \not< n}_{n \notin n}$.

Therefore consider

$$Z := \{ n \in \mathbb{N} ; n \notin n \}$$

and show that Z is inductive.

$n=0$ is true since $0=\emptyset$.
and therefore $0\notin 0$.

Suppose $n\notin n$. Show $s(n)\notin s(n)$.

Towards a contradiction, let

$$s(n) \in s(n) = n \cup \{n\}.$$

<u>Case 1.</u> $\underset{\underset{n\cup\{n\}}{\shortparallel}}{s(n)} = n.$

$\implies n \in n.$

Contradiction to assumption.

<u>Case 2.</u> $s(n) \in n$

By transitivity

$n\cup\{n\} = s(n) \subseteq n$

$\implies n \in n.$ Contradiction to assumption.

q.e.d.

<u>Definition</u> A set x is called <u>finite</u> if there is a natural number $n\in\mathbb{N}$ such that there is a bijection between x and n. It is called <u>infinite</u> if it's not finite.

We hope that

$Z \vdash$ "there is an infinite set".

More concretely,

$Z \vdash$ "$\mathbb{N}$ is infinite".

<u>Theorem</u> $\mathbb{N}$ is infinite.

<u>Proof.</u> On sheet #3, homework q. (10), we'll look at the relation between Dedekind-finiteness and finiteness.

<u>Remember</u> X is called <u>Dedekind-infinite</u> if there is $f: X \to X$ injective not bijective.

So X is <u>Dedekind-finite</u> if every $f: X \to X$ that is inj. is bijective.

HW (10): Every $n \in \mathbb{N}$ is Dedekind-finite.

All four notions are "closed under bijections": if x is D-i/D-f/i/f and there is a bij. between x & y, then y is D-i/D-f/i/f.

Put together: every finite set is D-finite.

So, it is enough to show that $\mathbb{N}$ is D-infinite. Because then it can't be finite.

Answer: the successor function.

$$f := \{ (n,m) \in \mathbb{N} \times \mathbb{N} \ ; \ m = s(n) \}$$

[separate f from the Cartesian product]

We could show that f is an injection [another one of the Peano axioms] and it is clearly not a surjection since $\emptyset \notin \operatorname{ran}(f)$.

q.e.d.

Remark Strengthening the argument about closure under bij.:

E.g. if X is infinite and $f : X \to Y$ is an injection, then Y is infinite.

ARITHMETIC

How do we add natural numbers?
Two very different definitions that end up being equivalent:

SYNTHETIC DEFINITION
CARDINAL DEFINITION

Define for sets X and Y a disjoint union:

$$X \uplus Y := \{0\}\times X \cup \{1\}\times Y$$

<u>Remark</u> There there nothing canonical about this definition and it implies in general that $X \not\subseteq X \uplus Y$.

Define a function

$$\oplus : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$$

by $n \oplus m = k$ if and only if

k is <u>the unique number</u> in bij. with $n \uplus m$.

<u>Note</u>: We would need to prove that such a number exists and is unique.
(cf. HW (10)).

INDUCTIVE DEFINITION
ORDINAL DEFINITION

Remark Properly speaking, INDUCTION is a proof principle; RECURSION is a definition principle.

RECURSION EQUATIONS

Example.

$$\boxed{\begin{aligned} 0! &:= 1. \\ (n+1)! &:= n! \cdot (n+1) \end{aligned}}$$

Caution In set theory, to define a function $f: \mathbb{N} \to \mathbb{N}$, we need a formula φ s.t.

$$f = \{(n,m);\ \varphi(n,m)\}$$

The recursion equations have a circular reference to the object we try to define.

$\Longrightarrow$ We need to prove a RECURSION THEOREM that says that these functions exist.

That's what happens after the break.
Then we use the so called
GRASSMANN EQUATIONS:

$$\boxed{\begin{aligned} n+0 &:= n \\ n+s(m) &:= s(n+m). \end{aligned}}$$

MULTI-PLICA-TION

$$\boxed{\begin{aligned} n\cdot 0 &:= 0 \\ n\cdot s(m) &:= n\cdot m + n \end{aligned}}$$

RECURSION THEOREM

Suppose $f: \mathbb{N} \longrightarrow \mathbb{N}$ is a function and $x_0 \in \mathbb{N}$.
Then there is a unique function

$$F: \mathbb{N} \longrightarrow \mathbb{N}$$

satisfying the RECURSION EQUATIONS:

$$F(0) = x_0$$

$$F(s(n)) = f(F(n)).$$

Remark. You get the function

$$+ : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$$

by defining it from the functions

$$+_n : \mathbb{N} \longrightarrow \mathbb{N}$$
$$k \longmapsto n+k$$

defined via the Grassmann equations.

Proof of the Recursion Theorem.

Idea: Finite fragments are fine, putting them together to an infinite object is the problem to be solved.

Def. Let's call a function

$$g : n \longrightarrow \mathbb{N}$$

a germ if it satisfies the recursion equations everywhere on its domain.

These exist: $\emptyset$ is a germ

$\{(0, \underline{x_0})\}$ is a germ.

from thm

__Lemma 1__ If g, g' are germs and $x \in \mathrm{dom}(g) \cap \mathrm{dom}(g')$, then $g(x) = g'(x)$.

[By induction:

$Z := \{ k \in \mathbb{N} ;$ for all g, g' germ s.t. $k \in \mathrm{dom}(g) \cap \mathrm{dom}(g')$, we have $g(k) = g'(k) \}$.

$k = 0$. $\left(g(0) = \underset{\text{from thm}}{\underline{x_0}} = g'(0). \right)$ ✓

Suppose $k \in Z$, i.e., $g(k) = g'(k)$ f.a. g, g' germ with k in domain

If $s(k) \in \mathrm{dom}(g) \cap \mathrm{dom}(g')$, then by <u>assumption</u>, we know $g(k) = g'(k)$

$$g(s(k)) = \underline{f}(g(k)) = \underline{f}(g'(k)) = g'(s(k)).$$

from thm]

<u>Lemma 2</u> For every $n \in \mathbb{N}$, there is a germ g s.t. $n \in \mathrm{dom}(g)$.

[$Z := \{ n \in \mathbb{N};$ there is a germ g s.t. $n \in \mathrm{dom}(g) \}$

$n = 0$ Done in pink on page 12.

Suppose $n \in Z$. That means there is g s.t. $n \in \mathrm{dom}(g)$.

By the recursion eq., we need germ g' s.t.

$$g'(s(n)) = f(g(n))$$

and $g'(k) = g(k)$ f.a. $k \leq n$.

$$g' := g \cup \{ (s(n), f(g(n))) \}$$

Then g' is a germ and $s(n) \in \mathrm{dom}(g')$.]

Now define $F : \mathbb{N} \longrightarrow \mathbb{N}$ by
SEPARATION

$$F := \{ (n,m) \in \mathbb{N} \times \mathbb{N} \; ; \text{ there is a germ } g \text{ s.t. } n \in \mathrm{dom}(g) \text{ and } g(n) = m \}$$

Lemma 1 proves that F is a function.
Lemma 2 proves that $\mathrm{dom}(F) = \mathbb{N}$.

q.e.d.

This allows us to define ("inductively") the operation

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

and we can check the usual properties

Associativity: $(x+y)+z = x+(y+z)$

Commutative: $x+y = y+x$

HW (11) on sheet #3

Since the definition is asymmetric (recursion in the right parameter, not left), this could be surprising.

Similarly for multiplication:

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

by the Grassmann equation.

<u>Proposition</u> For all n, m:

$$n \oplus m = n + m.$$

$\left[Z_n = \{ m \in \mathbb{N} ; n + m = n \oplus m \} \right.$
Show [for each fixed n] that this is inductive.]

THE LEAST NUMBER PRINCIPLE

<u>Definition</u> A strict total order $(X, <)$ has the <u>least number principle</u> (or is <u>wellfounded</u>) if every nonempty subset $Z \subseteq X$ has a least element.

<u>Remark</u> Many proof for $\mathbb{N}$ called "inductive" are instead using the least number principle.

Theorem $(\mathbb{N}, <)$ satisfy the least number principle.

Proof. Suppose $X \subseteq \mathbb{N}$. Show that if X has no least element, then $X = \emptyset$.
Suppose that X does not have a least element:

$$Z := \{ x \in \mathbb{N} ; \forall y \, (y \leq x \longrightarrow y \notin X) \}$$

If we can show that $Z = \mathbb{N}$, then by $\mathbb{N} \setminus X \supseteq Z$, we get $X = \emptyset$.

Thus, we only need to show that Z is inductive.

$x = 0$. If $0 \notin Z$, then $0 \in X$.
But then X has a least number,
Contradiction.

Suppose $x \in Z$, show that $s(x) \in Z$.
If $x \in Z$, but $s(x) \notin Z$, then by discreteness, this implies $s(x) \in X$.
But then $s(x)$ is the least elt of X.
Contradiction! q.e.d.

The least number principle allows us to define a slightly different notion of induction.

If $(X,<)$ is a strict total order and for $x \in X$, we define

$$<[x] := \{y \in X \,;\, y < x\}$$

[the proper initial segment defined by x]

Say that $Z \subseteq X$ is order inductive if for all $x \in X$:

if $<[x] \subseteq Z$, then $x \in Z$.

The PRINCIPLE OF ORDER INDUCTION

if $Z \subseteq X$ is order inductive, then $Z = X$.

[Cf. homework sheet #3.]

Claim $(\mathbb{N},<)$ satisfies the principle of order induction.

RECOVERING ORDINARY MATHEMATICS

$\mathbb{N}$

Want integers $\mathbb{Z}$

rationals $\mathbb{Q}$

reals $\mathbb{R}$

complex numbers $\mathbb{C}$

function spaces ...

INTEGERS

Integers are $\pm n$ where $n \in \mathbb{N}$.
[Except 0 which should not be counted double.]

Interpret $(0,n)$ as $+n$
$(1,n)$ as $-n$

then $\mathbb{Z} := \{0\} \times \mathbb{N} \cup \{1\} \times (\mathbb{N} \setminus \{0\})$

Again: no canonicity.

I now need to define $+, \cdot, <$ to make sure that $\mathbb{Z}$ is given the right structure.

Note that only the structure of $+, \cdot, <$ really makes the set $\mathbb{Z}$ behave like the integers, so if

$(Y, \oplus, \otimes, \prec)$ is a structure

& s.t. there is an isomorphism, i.e., a bij. $f : \mathbb{Z} \longrightarrow Y$ preserving the $+, \cdot, <$ - structure, then Y has the same right to be called the integers as $\mathbb{Z}$.

<u>Remark.</u> If Y is any $\boxed{\text{countably infinite}}$ set, then we find $\oplus, \otimes, \prec$ s.t.

$$(Y, \oplus, \otimes, \prec) \cong (\mathbb{Z}, +, \cdot, <).$$

<u>Definition</u> A set X is called <u>countable</u> if there is an injection

$$f : X \longrightarrow \mathbb{N}.$$

It is called <u>countably infinite</u> if there is a bijection

$$f : X \longrightarrow \mathbb{N}.$$

Theorem A set X is <u>countably infinite</u> iff it is <u>countable</u> and <u>infinite</u>.

there is a bij. $X \to \mathbb{N}$

there is an inj. $X \to \mathbb{N}$

not finite: no bij. to any $n \in \mathbb{N}$.

Proof. "$\Longrightarrow$": • Every bij. is an inj., so it's countable.

• X is in bij. with an infinite set, viz. $\mathbb{N}$, so infinite.

"$\Longleftarrow$":

Preliminary remarks.

$\boxed{\text{Let try to show that each infinite subset of } \mathbb{N} \text{ is in bij. with } \mathbb{N}.}$

Need a slightly different recursion theorem for this:

Let $P := \{f ; \operatorname{dom}(f) \in \mathbb{N}$ and $\operatorname{ran}(f) \subseteq \mathbb{N}\}$

(Ordertheoretic) Recursion Theorem

Let $f : P \longrightarrow \mathbb{N}$.

Then there is a unique

$F : \mathbb{N} \longrightarrow \mathbb{N}$ s.t.

for all n $\boxed{F(n) = \underline{f(F \upharpoonright n)}}$

$f(F \upharpoonright <[n])$

Proof idea Exactly the same as the other Recursion, except that we use order induction / least number principle where we use induction in the other proof.

Use this to show $X \subseteq \mathbb{N}$, X infinite $\Longrightarrow$ X in bij. with $\mathbb{N}$.

[By the least number principle for $\mathbb{N}$, we know that for $I \subseteq \mathbb{N}$, $I \neq \emptyset$, there is a least element $m(I)$.

Use the ordertheoretic recursion principle to define

$$F(n) := m\left(\boxed{X \setminus \operatorname{ran}(F \upharpoonright n)}\right)$$

Note that the fact that X is infinite implies that $F(n)$ is always defined.

By construction

$F : \mathbb{N} \longrightarrow \mathbb{N}$ is an injection with $\underline{\operatorname{ran}(F) = X}$.

Therefore X is countably infinite.

Now show "$\Longleftarrow$". So X is infinite and $h : X \longrightarrow \underline{\underline{\mathbb{N}}}$ is injective.

Consider $Y := \operatorname{ran}(h) \subseteq \mathbb{N}$.

By our earlier remark, Y is an infinite subset of $\mathbb{N}$, so there is bij. betw. Y and $\mathbb{N}$.

Clearly, $h : X \longrightarrow Y$ is a bijection.

Thus, X is in bij. with $\mathbb{N}$. q.e.d.

Theorem. If X is any countably infinite set, there are $\oplus, \otimes, \prec$ s.t.

$$(X, \oplus, \otimes, \prec) \cong (\mathbb{Z}, +, \cdot, <).$$

Proof. Suppose $f : X \longrightarrow \mathbb{N}$ is a bijection. Pick your favourite bijection between $\mathbb{N}$ and $\mathbb{Z}$.

$$\boxed{\begin{array}{l} 2n \longmapsto (0, n) \\ 2n+1 \longmapsto (1, n+1) \end{array}}$$

Compose them to get bij.

$$\hat{f} : X \longrightarrow \mathbb{Z}.$$

If $x, x' \in X$ define

$$x \oplus x' := \hat{f}^{-1}(\hat{f}(x) + \hat{f}(y))$$
$$x \otimes x' := \hat{f}^{-1}(\hat{f}(x) \cdot \hat{f}(y))$$
$$x \prec x' :\Longleftrightarrow \hat{f}(x) < \hat{f}(y).$$

Then $\hat{f}$ becomes an isomorphism between $(X, \oplus, \otimes, \prec)$ and $(\mathbb{Z}, +, \cdot, <)$.

q.e.d.

Once we have the integers, we can continue with the rationals

$\mathbb{Q}$ [e.g., as quotient field]

and $\mathbb{R}$ [e.g., Dedekind completion or Cauchy completion].

$\longrightarrow$ GI #2.

[Note that by usual results from ordinary maths: $\mathbb{Q}$ is countable whereas $\mathbb{R}$ is not. More on this later.]

Next topic: induction & recursion on other sets that are not equal to $\mathbb{N}$.

Note that $\mathbb{N}$ are not unique in satisfying the least number principle:

Examples $n \in \mathbb{N}$ satisfies the least number principle

$s(\mathbb{N}) = \mathbb{N} \cup \{\mathbb{N}\}$

$s(\mathbb{N}) = \mathbb{N} \cup \{\mathbb{N}\}$ satisfies the least number principle:

If $\underset{\neq \emptyset}{Z} \subseteq s(\mathbb{N})$, then

Case 1. $Z \cap \mathbb{N} \neq \emptyset$. Then by the the least number principle in $\mathbb{N}$, $Z \cap \mathbb{N}$ has a least number and thus that is the least number of Z.

Case 2 $Z \cap \mathbb{N} = \emptyset$. So since $Z \neq \emptyset$, $Z = \{\mathbb{N}\}$.
So Z has a least element.

Clearly $s(\mathbb{N})$ has a proper inductive subset, so it cannot satisfy the principle of complete induction, but it satisfies the least number principle.

$\rightsquigarrow$ generalised induction & recursion for wellfounded structures