Intro to Top

1

Chapter 1 Set Theory and Logic   1.1 Fund Concepts

set = { objects }

some logical fund of set theory needed

$P = \{A : A \notin A\}$ $P \notin P \Rightarrow P \in P \Rightarrow P \notin P$

but not discussed here   Russell's paradox!

Basic Notation

$a \in A$ element $a \notin A$ not el. $A \ni a$ "includes"

$A \subset B$ every $a \in A$ has $a \in B$ subset
inclusion

includes $=$ $A \subset A$

if excludes $=$ write $A \subsetneq B$

proper inclusion

$B \supset A$ B superset of A   B contains A

notation of sets

{objects} $\{1, 2, 3\}$

{objects | property} $\{x \mid x \text{ even int}\}$
:

Union / Inters / or / and

$A \cup B$ union $A \cup B = \{x : x \in A \text{ or } x \in B\}$

$A \cap B$ inters. $A \cap B = \{x : x \in A \text{ and } x \in B\}$

$= \{x \in A : x \in B\}$

②

Rem: or is not exclusive

"P or Q" means one of P and Q

If we want to exclude — " —

write "either __ or __" or "__ or __ but not both"

$\emptyset$ empty set

$A \cap B = \emptyset$ A, B disjoint

for all $\forall x$ $x \notin \emptyset$

$A \cup \emptyset = A$ $A \cap \emptyset = \emptyset$

If ... then

If P then Q $P \Rightarrow Q$ means if P = true then Q = true

Q if P if P = false then Q = true or false

P if and only if Q $P \Leftrightarrow Q$ means - - - - - true

"If $x^2 < 0$, then $x = 23$"

$\forall x$ P = false " } " (vacuously) true

Contrapositive / Converse

$P \Rightarrow Q$ contrapositive

$\neg Q \Rightarrow \neg P$.

$\neg$ not

contrapositive is true if and only if statement is true

contrapositive is logically equivalent

$P \Rightarrow Q$ — converse $Q \Rightarrow P$ (not equivalent to $P \Rightarrow Q$)

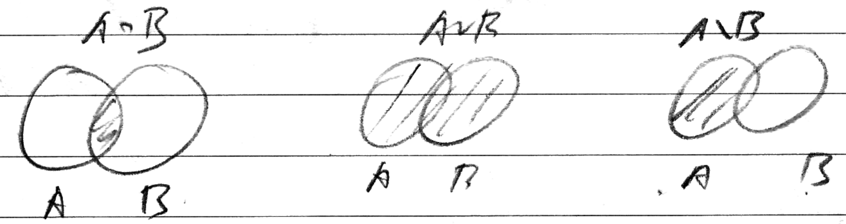
$P \Leftrightarrow Q$ means $P \Rightarrow Q$ and $Q \Rightarrow P$

<u>Negation of quantified statements</u>

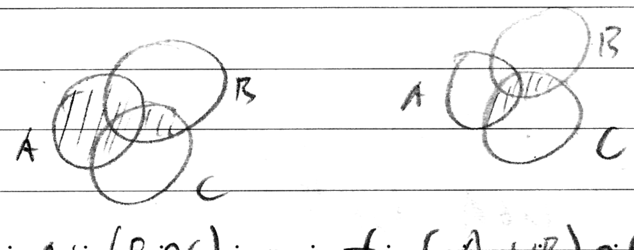
			negation
for all	$\forall x$	P	"$\neg(\forall x\ P)$" = "$\exists x\ \neg P$"
exists	$\exists x$	P	"$\neg(\exists x\ P)$" = "$\forall x\ \neg P$"

<u>Set difference</u>

$$A - B = A \setminus B = \{x \in A : x \notin B\}$$



$A \cap B = B \cap A$ $\qquad$ $A \setminus B \neq B \setminus A$



$A \cup (B \cap C) \neq (A \cup B) \cap C$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ distr. laws
$A \cup (B \cap C) \quad (A \cup B) \cap (A \cup C)$

$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ De Morgan's law
$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Collection of sets

can form sets out of sets

$\mathcal{P}(A) : \{B : B \subset A\}$ power set of A

$a \in A \iff \{a\} \subset A \iff \{a\} \in \mathcal{P}(A)$

Arbitrary Unions and $\cap$s

$\mathcal{A}$ family of sets $\quad \bigcup_{A \in \mathcal{A}} A = \{x : \exists A \in \mathcal{A} \; x \in A\}$

x is in at least one $A \in \mathcal{A}$

$\bigcap_{A \in \mathcal{A}} A = \{x : \forall A \in \mathcal{A} \; x \in A\}$

x is in all $A \in \mathcal{A}$

Cartesian Products

$A \times B = \{ (a,b) \quad a \in A, b \in B\}$

1.2. Functions

We need a bit more formal def. to make precise domain...

C, D sets. A rule of assignment is $r \subset C \times D$ with

$\forall c \in C \qquad (\{c\} \times D) \cap r$ has at most one el.

Then define

$\text{domain}(r) = \{ c \in C : (\{c\} \times D) \cap r \neq \emptyset \}$

$\text{image}(r) = \{ d \in D \quad (C \times \{d\}) \cap r \neq \emptyset \}$

<u>Def:</u> $f = (r, B)$ $\quad r$ r.o.a. $B \supset \text{image}(r)$ is a function

$A := \text{dom}(r) = \text{dom}(f)$ domain 정의역

공역 range of f $B \supset \text{image}(r) = \text{img}(f)$ image of f 치역

[<u>Rem:</u> dialect (my other lectures) analysis $\quad$ image = range 치역, range = target 공역]

$f : A \xrightarrow{(r,B)} B$

$a \in B$. Let $b \in B$ be so that $(a, b) \in r$

(b unique!) $f(a) = b$ image of a under f, value of f at a

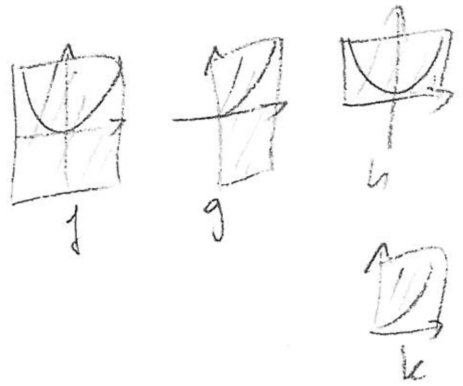
$f: A \longrightarrow B \qquad A_0 \subset A$

$\overset{\shortparallel}{(r, B)}$

$r \subset C \times D$

$f: A_0 \longrightarrow B$ def. by $(r \cap A_0 \times D, B)$

f/A_0 restriction of f to A_0



Ex. $\quad f: \mathbb{R} \to \mathbb{R} \qquad f(x) = x^2$

$\overline{\mathbb{R}}_+ = [0, \infty) \quad g: \overline{\mathbb{R}}_+ \to \mathbb{R} \qquad g(x) = x^2$

$h: \mathbb{R} \to \overline{\mathbb{R}}_+ \qquad h(x) = x^2$

$k: \overline{\mathbb{R}}_+ \to \overline{\mathbb{R}}_+ \qquad k(x) = x^2$

(for us) are all diff., $g = f/_{\overline{\mathbb{R}}_+}$, $k = h/_{\overline{\mathbb{R}}_+}$

(we keep record of range!)

Def: $f: A \longrightarrow B \qquad g: B \to C$

The composite $g \circ f: A \to C \qquad g \circ f(a) = g(f(a))$

rule of ass $r_{g \circ f} = \{ (a, c) \in A \times C : \exists b \in B \quad (a, b) \in r_f \ (b, c) \in r_g \}$

note: we define $g \circ f$ only if range$(f) \underset{!}{=}$ dom(g) (not $\subset$)

$f: A \longrightarrow B$ injective if $\forall a \neq b \quad a, b \in A \quad f(a) \neq f(b)$
(one-to-one)

$(\Longleftrightarrow \quad f(a) = f(b) \Longrightarrow a = b)$

$f: A \to B$ onto $\forall b \in B \ \exists a \in A \ f(a) = b$

$(\Leftrightarrow \text{image}(f) \overset{!}{=} \text{range}(f) = B)$

$f: A \to B$ bijective if f inj & surj
1-to-1 corresp.

If $f: A \to B$ bij $\exists f^{-1}: B \to A$ inverse

$b \in B$ $\quad f^{-1}(b) = a$ with $f(a) = b$

$(f \text{ bij} \Rightarrow \exists! a)$

$f: A \to A$ $\quad f(x) = x$ $\quad i_A$ identity fct

Lemma Let $f: A \to B$

If $\exists g, h: B \to A$ $\quad g \circ f = Id_A$ left inverse
$f \circ h = Id_B$ right inverse

Then f bijective and $g = h = f^{-1}$.

Def: $f: A \to B$ $\quad A_0 \subset A$

$f(A_0) = \{ f(a) : a \in A_0 \}$

$= \{ b \in B : \exists a \in A \ f(a) = b \}$

image of A_0

$B_0 \subset B$ $\quad f^{-1}(B_0) = \{ a \in A : f(a) \in B_0 \}$

Rem. If f bij then $\underset{\text{preimage}}{f^{-1}(B_0)} = \underset{\text{image under inverse map}}{(f^{-1})(B_0)}$

Rem $\quad f(f^{-1}(B_0)) \subset B_0 \quad$ "=" if f surjective

$\qquad f^{-1}(f(A_0)) \supset A_0 \quad$ "=" if f injective

§ 1.3 Relations

(1) equiv rel. $\quad$ (2) order rel.

Def: A relation on a set A is a subset $C \subset A \times A$

$x C y$ if $(x,y) \in C$ "x is in the rel C to y"

$x \sim_C y$ and $x \not\sim_C y$ $(x,y) \notin C$ "x is not in rel C to y"

(1)

Def: $C \subset A \times A$ equivalence rel if

(1) reflexivity $\quad x \sim_C x \quad \forall x \in A$

(2) symmetry $\quad \forall x, y \in A \quad x \sim_C y \Rightarrow y \sim_C x$

(3) transitivity $\quad \forall x, y, z \in A \quad x \sim_C y, y \sim_C z \Rightarrow x \sim_C z$

Ex. $C = A \times A$ $\quad$ trivial equivalences

$C = \{(x,x) : x \in A\}$

$A = \mathbb{Z} \quad x \sim y \Leftrightarrow y - x$ is even

Def: $C \subset A \times A$ equiv rel.

$a \in A \qquad [a] = [a]_{\sim_C} = \{ b \in A : b \sim_C a \} \subset A$

$[a] \ni a$

Lemma $\forall a,b \in A$ $\quad [a]=[b]$ or $[a]\cap[b]=\phi$

two equiv classes are equal or disjoint

Def: A set. $\mathcal{E}$ family of sets is partition of A if

a) $\forall A' \in \mathcal{E}$ $\quad \phi \neq A' \subset A$ non-empty subsets of A

b) $\forall A', A'' \in \mathcal{E}$ if $A' \neq A'' \Rightarrow A' \cap A'' = \phi$ disjoint

c) $\bigcup_{A' \in \mathcal{E}} A' = A$

$\{$equiv rels of $A\} \Longleftrightarrow \{$partitions of $A\}$

If $\sim_c$ is equiv. rel. of A $\Rightarrow \mathcal{E} = \{$equiv classes$\}$ is a part of A

$\mathcal{E} = \{[a] : a \in A\}$ (removing duplicates)

If $\mathcal{E}$ partition of A, define $\forall a,b \in A$

$a \sim_{\mathcal{E}} b$ if $\exists A' \in \mathcal{E}$ $a,b \in A'$

is an equiv rel.

② Order relations (more important for us)

Def: $C \subset A \times A$ (simple) order, linear order if

(1) Comparability $\forall x,y \in A$ $x \neq y$ $\quad x \sim_c y$ or $y \sim_c x$

(2) Nonreflexivity $\forall x \in A$ $\quad x \not\sim_c x$

(3) Transitivity $\forall x,y,z \in A$ $\quad x \sim_c y$ $\quad y \sim_c z \Rightarrow x \sim_c z$

Rem (2), (3) $\Rightarrow$ "or" in (1) is either or

($\nexists x, y \in A$: $x \sim_c y$ and $y \sim_c x$) (10)

Ex. $A = \mathbb{R}$ $<$ usual order rel.

$A = \mathbb{R}$ $x \sim_c y \Leftrightarrow x^2 < y^2$ or $x^2 = y^2$ $x < y$

unusual order rel.

Ex. (A, C) C order rel. $B \subset A$ $(B, C \cap (B \times B))$ restriction

usually use '<' for order rel.

$x < y$ x less than y

Def: $x \leq y \Leftrightarrow x < y$ or $x = y$ $(A, <)$ ordered set

$y > x \Leftrightarrow x < y$

$y \geq x \Leftrightarrow y > x$ or $y = x$

write $x < y < z$ for $x < y$ and $y < z$

Def: $a, b \in (A, <)$ $a < b$

Define $(a, b) = \{ x \mid a < x < b \}$

open interval

if $(a, b) = \emptyset$ call b immediate successor of a

a immediate predecessor of b

<u>Ex.</u> $(\mathbb{R}, <)$ no el. has immed. succ. or pred.

bec $\forall a<b \quad (a,b) \neq \emptyset$

$(\mathbb{Q}, <)$ similar

$(\mathbb{Z}, <)$ immed succ of $a \in \mathbb{Z}$ is $a+1$

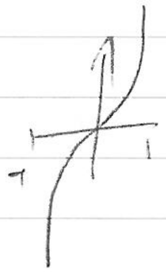
pred $a-1$

<u>Def:</u> $(A, <_A) \simeq (B, <_B)$ same order type

iff

$\exists f: A \to B$ bijective w/ $a_1 <_A a_2 \Leftrightarrow f(a_1) <_B f(a_2)$

<u>Ex.</u> $\mathbb{R} \simeq (-1,1)$ $\quad f(x) = \dfrac{x}{1-x^2}$



$[0,1) \simeq \{0\} \cup (1,2)$ $\quad f(0) = 0$

$f(x) = x+1$

<u>Def:</u> $(A, <_A), (B, <_B)$ ordered sets

Define $<_{A\times B}$ on $A \times B$ by

$(a_1, b_1) < (a_2, b_2)$ if $a_1 <_A a_2$ or

$a_1 = a_2$ and $b_1 <_B b_2$

dictionary (lexicographic) order

$$\overset{<}{\mathbb{Z}} \times \overset{<}{[0,1)} \quad \text{usual order}$$

<u>Ex.</u> $\mathbb{Z} \times [0,1)$ has the order type of $\mathbb{R}$ with lexicogr. order

$$f(z, \varepsilon) = z + \varepsilon$$

$[0,1) \times \mathbb{Z}$ has very diff order type

every el. has an immediate pred. & succ.

<u>Bounds, maxima, suprema, ...</u>

$(A, <)$ $\quad A_0 \subset A$

$b = \max A_0$ largest element of A_0

if $b \in A_0$ $\quad b \geq x \quad \forall x \in A_0$

$b = \min A_0$ smallest element

$b \in A_0 \quad b \leq x \quad \forall x \in A_0$

(does not need to exist!)

$b \in A$ upper bound for A_0 if $\quad b \geq x \quad \forall x \in A_0$

lower $\quad b \leq x$

A_0 bounded above if it has upper bound

below $\quad$ lower

bounded $\Leftrightarrow$ above + below

A_0 has least upper bound b if
b upper bound for A_0 and
$\forall x \in A$ $x < b$ x is not upper bound for A_0

$b = \min \{ x : x \text{ upper bound for } A_0 \}$

$b = \sup A_0$ supremum

A_0 has greatest lower bound b if
b lower bound for A_0 and
$\forall x \in A$ $x > b$ x not lower bound for A_0

$b = \max \{ x : x \text{ lower bound for } A_0 \}$

$b = \inf A_0$ infimum

Rem: If $b = \sup A_0 \in A_0$, then $b = \max A_0$
$b = \inf A_0 \in A_0$ $\quad$ $b = \min A_0$

Def: $(A, <)$ has least upper bound property (l.u.b.p)
if $\forall A_0 \subset A$ $\left\{ \begin{array}{l} A_0 \neq \emptyset \\ A_0 \text{ bounded above} \end{array} \right\}$

$\exists \sup A_0 \in A$

$(A, <)$ has greatest lower bound (g.l.b.) property if (14)

$\forall A_0 \subset A$ $\quad$ $A_0 \neq \emptyset$
A_0 bounded below

$\exists \inf A_0 \in A$

<u>Th.</u> $(A, <)$ has g.l.b.p. $\iff$ l.u.b.p.

<u>Ex.</u> Assume $(\mathbb{R}, <)$ has l.u.b.p. (discuss this later!)

then $A = (-1, 1), <$ has l.u.b.p.

<u>Proof:</u> $A_0 \subset (-1,1)$ $\quad A_0 \neq \emptyset$ bounded above in A_0

$\exists b \in (-1,1)$ $\quad b \geq x \quad \forall x \in A_0$

$b \in A_0 \subset \mathbb{R} \implies A_0$ bound. above in $\mathbb{R}$

$\mathbb{R}$ has lubp $\implies \exists$ least upper bound $\tilde{b}$ of A_0 in $\mathbb{R}$

$A_0 \neq \emptyset \quad \exists a \in A_0 \qquad a \leq \tilde{b} \leq b$

now $\quad a, b \in A_0 = (-1, 1) \implies \tilde{b} \in (-1, 1) = A$

$\tilde{b}$ is least upper bound of A_0 in A

Similarly all intervals in $\mathbb{R}$ have lubp

Ex. $A = (-1,0) \cup (0,1)$

$A_0 = \{-1/n : n > 1\}$ has upper bound but no least upper bound

1.4. Integers and real numbers

need a bit more formal approach to real #s via axioms

Def: $f : A \times A \longrightarrow A$ binary operation on A

$f(a,a') = a f a'$

define group, Ab. group, field

Def: The real #s $(\mathbb{R}, +, \cdot, <)$ is a set with two binary oper

$+$ addition $\cdot$ mult

and one ordering relation $<$ s.t.

(1) - (5.) $(\mathbb{R}, +, \cdot)$ is a field

mixed alg. and order property

(6) $\forall x, y, z \in \mathbb{R}$ $x > y \Rightarrow x + z > y + z$

$x > y, z > 0 \Rightarrow x \cdot z > y \cdot z$

ordered field

Order properties

(7) $<$ has least upper bound property

(8) if $x < z$ $\exists y$: $x < y$ and $y < z$

$-x$ is the additive inverse $x+(-x)=0$

$a-b = a+(-b)$ subtraction

$x \neq 0$ $\frac{1}{x} = x^{-1}$ is mult. inverse

$x \cdot \frac{1}{x} = 1$

$b \neq 0$ $\frac{a}{b} = a \cdot b^{-1} = b^{-1} \cdot a$ quotient

all other common properties of real #s can be derived from these axioms (1)-(18)

for ex.

if $x > y$ $z < 0$ $\Rightarrow$ $x \cdot z < y \cdot z$

$-1 < 0 < 1$

(1) - (5) field } ordered field ($\Rightarrow$ char $= 0$!)

(6)

(7), (8) } linear continuum (topol. term)

<u>Rem:</u> (8) $\Leftarrow$ (1) - (7)

given $x \neq z$ build $y = \frac{x+z}{2}$ with $2 = 1+1 \neq 0$ (!!)

<u>Def:</u> $x > 0$ positive

$x < 0$ negative

formal def of integers

$A \subset \mathbb{R}$ inductive if $1 \in A$
and $\forall x \in A \quad x+1 \in A$

$\mathcal{A} = \{A \subset \mathbb{R} : A \text{ inductive}\}$

$$(\mathbb{N}_+ =)\ \mathbb{Z}_+ = \bigcap_{A \in \mathcal{A}} A$$

positive integers (natural #s $\mathbb{N}$)

$$\mathbb{Z} = \mathbb{Z}_+ \cup \{0\} \cup \underbrace{-\mathbb{Z}_+}_{\{-a\,:\,a \in \mathbb{Z}_+\}}$$

Rem: $\mathbb{Z}_+ \subset \overset{=(0,\infty)}{\mathbb{R}_+}$ bec $(0,\infty)$ ind.

$\min \mathbb{Z}_+ = 1$ bec. $[1,\infty)$ is inductive
so $\mathbb{Z}_+ \subset [1,\infty)$

define rat. #s

$$\mathbb{Q} = \left\{ m/n : m,n \in \mathbb{Z},\ n \neq 0 \right\}$$

Theo 4.1 (well-ordering prop)

$A \subset \mathbb{Z}_+ \quad A \neq \emptyset \implies \exists \min A$
$A \ni$ smallest el.

$\{1, \dots, n\} = S_{n+1}$ section of pos. ints, $S_1 = \emptyset$

Th. 4.2 (Strong ind. prop.)

$A \subset \mathbb{Z}_+$ and $\forall n \in \mathbb{Z}_+ \; S_n \subset A \Rightarrow S_{n+1} \subset A$

(i.e. $n=1$ $\underbrace{\emptyset}_{S_1} \subset A \Rightarrow \underbrace{S_2}_{\{1\}} \subset A \Rightarrow 1 \in A$)

then $A = \mathbb{Z}_+$

l.u.b. axiom (7) $\Rightarrow$ $\mathbb{Z}_+$ has no upper bound
(Archimedean ordering prop.)

$\Rightarrow \exists \sqrt{x} \quad x > 0 \quad \cdots \quad \sqrt{a} = \sup\{x : x \cdot x \leq a\}$

1.S. Cartesian products

generalize $A \times B$

Def: $\mathcal{A}$ family of sets, index set
indexing function $f: J \to \mathcal{A}$
f surjective

$\alpha \in J$ write $f(\alpha) \in \mathcal{A}$ as A_α

$$\mathcal{A} = \{A_\alpha\}_{\alpha \in J}$$

we don't need f bij so same set can be indexed multiply!

$$\cancel{\bigcup_{\alpha\in J} A_\alpha = \bigcup_{A\in\mathcal{A}} A = \{x : A \ni x_\alpha \text{ for at least one } \alpha\in J\}}$$

all

$$\bigcap_{\alpha\in J} A_\alpha = \bigcap_{A\in\mathcal{A}} A$$

Ex. $J=\{1,2\}$ $\quad \mathcal{A}=\{A_1, A_2\}$

$$\bigcap_{\alpha\in J} A_\alpha = A_1\cap A_2 \qquad \bigcup_{\alpha\in J} A_\alpha = A_1\cup A_2$$

Def: $m\in\mathbb{Z}_+=\mathbb{N}$ $\quad X$ set

m-tuple x of els in X is

$$x:\{1,\dots,m\}\to X$$

$x=(x(1),\dots,x(m))$ $\quad x(i)\in X$ i-th coord of x

$\mathcal{A}=\{A_1,\dots,A_m\}$ family indexed by $\{1,\dots,m\}$

$$A_1\times\dots\times A_m = \{x \text{ } m\text{-tuple of } X=\bigcup_{i=1}^m A_i \text{ with } x(i)\in A_i \ \forall i=1,\dots,m\}$$

Rem $(A\times B)\times C \simeq A\times(B\times C)\simeq A\times B\times C$

$$((a,b),c)\longleftrightarrow(a,(b,c))\longleftrightarrow(a,b,c)$$

$n\in\mathbb{Z}_+$ $\quad A^n = A\times A\times\dots\times A = \{(x_1,\dots,x_n) : x_i\in A\}$

$(\mathcal{A}=\{A\} \quad f:\{1,\dots,n\}\to\mathcal{A} \quad f(i)=A \quad i=1,\dots,n)$

<u>Def:</u> (sequence set) X set

$x : \mathbb{Z}_+ \to X$ (infinite) sequence, ω-tuple of els in X

$\mathbb{Z}_+ = \mathbb{N}$

$$x = (x(1), x(2), \dots) = (x_1, x_2, \dots) = (x_n)_{n \in \mathbb{N}}$$

$$X^\omega = \{ x : x \text{ sequence in } X \}$$

$\mathcal{A} = \{A_i\}_{i \in \mathbb{Z}_+}$ $\quad A_1 \times A_2 \times \dots = \prod_{i=1}^{\infty} A_i = \prod_{i \in \mathbb{Z}_+} A_i = \{ x \in X^\omega \text{ for } X = \bigcup_{i=1}^{\infty} A_i$

$x_i \in A_i \ \forall i \in \mathbb{Z}_+ \}$

$$X^\omega = \prod_{i=1}^{\infty} X = \prod_{i \in \mathbb{Z}_+} X$$

(later define $\prod_{\alpha \in J} A_\alpha$ for $\mathcal{A} = \{A_\alpha\}_{\alpha \in J}$)

1.6. Finite sets and cardinalities

<u>Def:</u> set A finite $\exists n \in \mathbb{N}$ $\exists f : S_n \to A$ bijective

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

$|A| := n-1$ cardinality of A

$n - 1 \in \mathbb{N} \cup \{0\}$

$|A| < \infty$

caution: why is this well defined?

Can $S_m \xleftrightarrow{f'} A \xleftrightarrow{f} S_n$ with

to prove is $\nexists f: S_m \to S_n$ bijective if $m \neq n$

this is intuitively clear, but it is good to prove it formally using the tools from set theory we developed

I skip details but it requires some steps which are important for other reasons

Th 6.2 Let A be a set. Assume $\exists f: A \to \{1,\dots,n\}$ bijective. Let $B \subsetneq A$, $B \neq \emptyset$.
Then (1) $\exists m \in \mathbb{N}$ $m<n$ $\tilde{f}: B \to \{1,\dots,m\}$ bijective and (2) $\nexists \hat{f}: B \to \{1,\dots,n\}$ bij

The proof uses induction.

$C = \{ n \in \mathbb{Z}_+ : \text{Th. holds} \}$

prove that C is inductive

$1 \in C$ if $n \in C \Rightarrow n+1 \in C$

$\Rightarrow C = \mathbb{Z}_+$

<u>Cor.</u> If A is finite, $\nexists$ bijection betw A and a proper subset B of itself.

Pf. If $A \simeq B$, $A \simeq \{1,\dots,n\}$ $\Rightarrow$ $B \subsetneq A$, $B \simeq \{1,\dots,n\}$
Prev th. (2) $\Rightarrow$ ↯ $\boxtimes$

<u>Cor</u> $\mathbb{Z}_+ = \mathbb{N}$ is not finite

bc. $n \mapsto n+1$ $\quad f: \mathbb{Z}_+ \to \mathbb{Z}_+ \setminus \{1\}$ bijective

<u>Cor</u> $|A|$ is well defined (for A finite)

Pf. otherw $\{1,\dots,n\} \simeq \{1,\dots,m\}$ $\quad m<n$

$\subsetneq$ · ↯

<u>Cor</u> A finite $B \subsetneq A$ $\quad$ B finite and $|B|<|A|$

<u>Cor.</u> The foll are equivalent $\forall B \neq \emptyset$

(1) B is finite
(2) $\exists f: S_n \to B$ surjective for some n
(3) $\exists f: B \to S_m$ injective — " — m

<u>Cor</u> Finite unions of finite sets are finite

$\mathcal{A} = \{A_\alpha\}_{\alpha \in J}$ $\quad |J| < \infty$ $\quad \forall \alpha \in J$ $|A_\alpha| < \infty$

$$\Rightarrow \left|\bigcup_{\alpha \in J} A_\alpha\right| = \left|\bigcup_{A \in \mathcal{A}} A\right| < \infty$$

ind on $|\mathcal{A}|=n$

Pf. $|\mathcal{A}|=2$ $\mathcal{A}=\{A,B\}$

$\{1,\dots,p\} \leftrightarrow A$ $\{1,\dots,p+n\} \xrightarrow{\text{surj}} A\cup B$

$\{1,\dots,n\} \to B$

induction set $A_1\cup\dots\cup A_n = (\underbrace{A_1\cup\dots\cup A_{n-1}}_{A})\cup \underbrace{A_n}_{B}$

§1.7. Countable and uncountable sets

Def: A set infinite if not finite $\forall n$ $\nexists f: S_n \to A$ bijective

$\underbrace{A \quad\quad\quad \text{if } \exists f: A \to \mathbb{Z}_+ \text{ bijective}}$ countably infinite ∞

Rem countably inf. $\Rightarrow$ infinite

Pf. if $\exists$ bij (surj) $\mathbb{Z}_+ \to \{1,\dots,n\}$

$\Rightarrow \exists$ inj i $\mathbb{Z}_+ \to \{1,\dots,n\}$

$\{1,\dots,n\} \subsetneq \mathbb{Z}_+$ $i|_{\{1,\dots,n\}} : \{1,\dots,n\} \to I$ bij

$I = i(\{1,\dots,n\}) \subsetneq \{1,\dots,n\}$

$\{1,\dots,n\}$ has bij to proper subset by ⊠

Def: A countable $\Leftrightarrow$ A finite or countably ∞

uncountable otherwise

Lemma $C \subset \mathbb{Z}_+$ infinite $\Rightarrow C$ countably ∞te

Pf. Construct $h : \mathbb{Z}_+ \xrightarrow{\text{bij}} C$ with recursive definite

$$h(n) = \overbrace{\text{smallest el. of}}^{\min} \underbrace{C \setminus h(\{1, \dots, n-1\})}_{C_{n-1}} \rightarrow \begin{array}{l}\text{ex. bec.}\\ \subset \mathbb{Z}_+\end{array}$$

$\blacksquare$

and prove h is bij!

recursive in terms of itself but care is needed e.g. $h(n) = \min C_{n+1}$ nonsense since $h(n) \notin C_{n+1}$

Principle of recursive def. $\rightsquigarrow$ (1.8 more detail skip here)

Let A set.

If $h(1) \in A$

and $\exists$ formula defining

$h(n)$ in terms of $h(1), \dots, h(n-1)$

then this formula determines a unique

fct. $h : \mathbb{Z}_+ \to A$

Th. Let $B \neq \emptyset$ then the foll are equiv

(1) B countable (incl. finite!)

(2) $\exists f : \mathbb{Z}_+ \to B$ surj

(3) $\exists f : B \to \mathbb{Z}_+$ inj

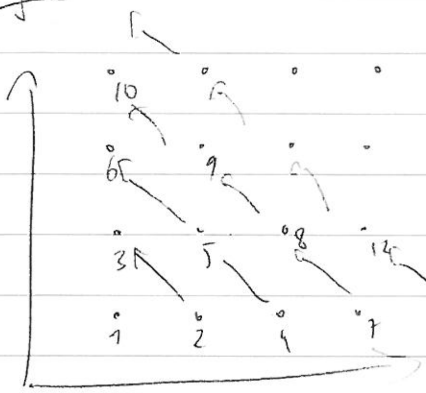
(3)

Cor B countable $C \subseteq B$ C countable

Cor $\mathbb{Z}_+ \times \mathbb{Z}_+$ countably infinite

Proof:

(1)



$j = h(i)$ describe $\mathbb{Z}_+ \xleftrightarrow{h} \mathbb{Z}_+ \times \mathbb{Z}_+$

(2) define $f: \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ by $f(m,n) = 2^m 3^n$ injective (bec prime factor is unique).

Exer $\mathbb{Q}$ countably ∞

Th. Countable union of countable sets is countable

i.e. $\mathcal{A} = \{A_\alpha\}_{\alpha \in J}$ J count. $\forall \alpha \in J$ A_α count.

$\Rightarrow \bigcup_{A \in \mathcal{A}} A$ countable

Pf. fix $g: \mathbb{Z}_+ \to J$ surj

$\forall \alpha \in J$ $f_\alpha: \mathbb{Z}_+ \to A_\alpha$ surj

cons $h: \mathbb{Z}_+ \times \mathbb{Z}_+ \to \bigcup_{\alpha \in J} A_\alpha$

$h(k,m) = f_{g(k)}(m)$ & h surj

Th. finite product of c. set is c.

i.e. $\{A_1, \dots, A_n\}$ countable $\longrightarrow \prod_{i=1}^{n} A_i$ c

<u>Thm</u> not true for ∞ products

$$\prod_{i=1}^{\infty} \{0,1\} = \{0,1\}^{\omega} \quad \text{uncountable}$$

$$\{0,1\}^{\omega} \underset{h}{\longleftrightarrow} \mathcal{P}(\mathbb{Z}_+) = \{A : A \subset \mathbb{Z}_+\}$$

$$h((x_1, x_2, \dots, x_n, \dots)) = \{n \in \mathbb{Z}_+ : x_i = 1\}$$

$$h^{-1}(A) = (x_1, x_2 \dots) \text{ with } x_n = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}$$

<u>Th.</u> $\forall A$ $\exists$ no bijection betw A and $\mathcal{P}(A)$

<u>Pf.</u> assume $A \underset{f}{\simeq} \mathcal{P}(A)$

consider $B = \{a \in A : a \notin f(a)\} \subset A \quad B \in \mathcal{P}(A)$

$\exists A \quad b = f^{-1}(B) \in A$

If $b = f^{-1}(B) \in B \implies b \notin f(b) = f(f^{-1}(B)) = B$ ↯

If $b \notin B \implies b \in f(b) = B$ ↯ $\boxtimes$

Pf. can be modified to f surjection $A \longrightarrow \mathcal{P}(A)$ (Exer.)

<u>Th (dual)</u> $\exists$ no surj $A \longrightarrow \mathcal{P}(A)$

$\exists$ no inj. $\mathcal{P}(A) \longrightarrow A$

Th $\mathbb{R}$ uncountable

Pf. describe $\{0,1\}^\omega \xrightarrow[h]{} \mathbb{R}$ injective

$(x_1, \dots, x_n, \dots) \longmapsto \sum_{i=1}^{\infty} \frac{x_i}{3^i}$

[not 2 bec $(0,1,1,1,\dots)$
$\updownarrow$
$1/2$
$\updownarrow$
$(1,0,\dots,0,\dots)$]

now if $\mathbb{R}$ countable

$\exists f: \mathbb{R} \to \mathbb{Z}_+$ inj.

$h \circ f : \{0,1\}^\omega \to \mathbb{Z}_+$ inj $\lightning$ ∎

but this makes use of ~~analytic~~ alg propr of $\mathbb{R}$ etc.
(convergence ...)

later proof only using order properties.

Def: If f. A $\exists$ $f: A \to \mathbb{R}$ bijective say
A has the cardinality ω of the continuum

here not of bijections preserve order

Ex. $\{0,1\}^\omega$ has card of the continuum
(needs a bit of proof!)

Rem: a) $\{A \subseteq \mathbb{Z}_+ : |A| < \infty\}$ all finite subsets of $\mathbb{Z}_+$

is countable!

b) $(\mathbb{Z}_+)^\infty_0 = \{(x_1, \dots) \quad x_i \in \mathbb{Z}_+ \ \underbrace{\exists n \ \forall N \geq n \ x_N = 0}_{\text{eventually zero int seq.}}\}$

countable!

$\{\mathbb{Z}_+ \to \mathbb{Z}$

c) $\mathbb{Z}[t] = \{\text{poly. with int coeffs.}\}$ countable

$\{\text{alg. \#s.}\} = \bigcup_{P \in \mathbb{Z}[t]} \{\text{roots of } P\} \subset \mathbb{R}$ countable

d) transcendental #s $= \mathbb{R} \setminus \{\text{alg. \#s}\}$ are uncountable ◁ Cantor's proof of existence of transc. #s

even though very hard to find explicit transcendental #s

π, e, a^b a rat.
b alg & not rat.

e.g. 2^{e} (Baker's theo)

but proofs are very hard!!

1.9 Infinite sets and Axiom of choice

Some criteria for infinite sets we had are sufficient to exactly characterise ∞ sets

Th. 9.1 A set. The foll. equiv:

(1) $\exists\, f: \mathbb{Z}_+ \to A$ injective
(2) $\exists\ A \leftrightarrow B$ bijective $B \subsetneq A$
(3) $|A| = \infty$

Pf. Insert proof we saw on $(3) \Rightarrow (1)$. Ass $|A| = \infty$
Cont $f(n)$ by ind. on n.
$\exists\, a_1 \in A$ set $f(1) := a_1$
$\exists\, a_n \in \underbrace{A \setminus f(\{1, \dots, n-1\})}_{A_n}$ set $f(n) := a_n$ $\square$

This pf. uses a choice of el. in an ∞ family of sets $\{A_n\}$.
The freedom of such choice does not follow from prev. set constructions. So we need a new method.

Axiom of choice (AC) $\mathcal{A} = \{A_i\}_{i \in I}$ $A_i \neq \emptyset$
$A_i \cap A_j = \emptyset$ $i \neq j$ $(*)$

$\Rightarrow \exists\, C \subset \bigcup_{i \in I} A_i$ with $|C \cap A_i| = 1$ $\forall i \in I$ $(**)$
$\bigcup_{i \in I} A_i =: \bigcup \mathcal{A} = \bigcup_{A \in \mathcal{A}} A$

This is the same as saying $\exists\, f: \mathcal{A} \to \bigcup \mathcal{A}$ with
$f(A) \in A$ $\forall A \in \mathcal{A}$

bec. given f take $C = \operatorname{im}(f)$ which sat. $(**)$ bec. of $(*)$

and given C define $f(A) = x$ for $x \in C \cap A$

One can show (Lemma 9.2 in book) that when one uses a choice fct. we can get rid of the card (a)

<u>Lemma</u> $\mathcal{B}$ family of sets $\exists f : \mathcal{B} \to \cup\mathcal{B}$ with $c(B) \in B \quad \forall B \in \mathcal{B}$

and now with this one can make Pf of (3) ⇒ (1) in Th 9.1 more precise

let $\mathcal{C} = \{ A' \subset A \quad A' \neq \emptyset \}$

take $c : \mathcal{C} \to \cup \mathcal{C}$

$f(i) = c(A \setminus f(\{1, \dots, i-1\})) \dots$

AC did generate some controversy as to bizarre conseq like the well-ordering thm, but now it is widely accepted.

10. well-ordered sets

<u>Def:</u> $(A, <)$ well ordered if $\exists \emptyset \neq A' \subset A$ smallest el. $a = \min A' \in A'$ exists.

<u>Ex.</u> $(\mathbb{Z}_+, <)$.

$(\mathbb{Z}, <)$ is not well ordered, unlike $([0,1], <) \quad ((0,1), <) \quad (\mathbb{R}, <)$

Construction of w.o. sets

(a) If $(A, <)$ w.o. and $B \subset A$

$$(B, <|_{B \times B}) \text{ is w.o.}$$

(b) A, B w.o. $\Rightarrow$ $A \times B$ with dictionary order is w.o.

Th. Every non-empty finite ordered set has the order type of $(S_n, <)$ so is w.o.

Ex. $\mathbb{Z}_+^n$ is w.o. with dict order

$\mathbb{Z}_+^\omega$ also has a "dict order"

$(a_1, \dots, a_n, \dots) < (b_1, \dots, b_n, \dots)$

if $\exists i$ $a_1 = b_1 \dots a_{i-1} = b_{i-1}$ $a_i < b_i$

but is not w.o. e.g. $\{(1, \dots, 1, 2, 1, \dots 1) \quad i \in \mathbb{Z}_+\}$ has no smallest el.

Is there another $<$ such $\mathbb{Z}_+^\omega$ w.o.?

Th. (Zermelo 1904) For every set A $\exists <$ s.t. $(A, <)$ w.o.

This proof only uses the AC and shocked many math. at the time which led to suspicion about AC.

Unf, the proof (as the AC) is not constructive, so one can't know what is $<$?!

Cor $\exists$ a well-ordered uncountable set.

Def: X w.o. set. $\alpha \in X$ let $S_\alpha = \{x \in X : x < \alpha\}$
section of X by α

(needed later)

Lemma $\exists$ w.o. set A with largest element Ω
s.t. $S_\Omega = \{a \in A : a < \Omega\} = A \setminus \{\Omega\}$
is uncountable, but all other sections of A
$S_a = \{a' \in A : a' < a\}$

are countable

Write $A = S_\Omega \cup \{\Omega\} = \overline{S_\Omega}$.

Ex (of sth. similar)

$(\overbrace{\{1\} \cup \{1 - 1/n : n \in \mathbb{Z}_+\}}^{A}, <)$ w.o.

Then $\Omega = 1$ and $|S_\Omega| = \infty$ but $\forall a < 1$
$|S_a| < \infty$

Th. If $A \subset S_\Omega$ countable then
A has an upper bound in S_Ω

1.11 The Maximum Principle

AC has several consequences (later proved equivalent to it) of the type "max principle".
Two versions here.

Def. A set $< \subset A \times A$ is strict partial order (s.p.o.) if

(1) $\forall a \in A \quad a \not< a$ (nonreflex.)
(2) $\forall a,b,c \quad a<b, b<c \Rightarrow a<c$ (transit.)

(Like order but don't need to compare all els.)

Ex. $(\mathcal{P}(A), \subsetneq)$

Rem: $a \leq b :\Leftrightarrow a<b \lor a=b$ defines a partial order (non-strict)

Def. $(A,<)$ s.p.o. set $B \subset A$ is (simply) ordered subset if

I use the word 'chain'

$<|_{B \times B}$ is an order on B

(i.e. $\forall b,c \in B \quad b<c$ or $c<b$)

Ex. $\{ \subset S_n : n \in \mathbb{Z}_+ \} \subset \mathcal{P}(\mathbb{Z}_+)$ with $\subsetneq$

Def. B is maximal ordered subset if ('max chain')
B is ordered subset and

$\forall B' \supsetneq B \quad B'$ is not order subset of A

Ex. $\mathcal{A} = \{ S_n \;\; n\in\mathbb{Z}_+ \}$ is not max ordered

bec. $\mathcal{A} \cup \{\mathbb{Z}_+\}$ ordered

but $\mathcal{A}' = \{S_n\}_{n\in\mathbb{N}} \cup \{\mathbb{Z}_+\}$ is m.o. in $(\mathcal{P}(\mathbb{Z}_+), \subsetneq)$

Pf. $A \notin \mathcal{A}'$ $\quad A \subset \mathbb{Z}_+$ $\quad$ ass. $\mathcal{A}' \cup \{A\}$ is o.

If $|A| = \infty$ $\quad A \supset S_n \;\forall n \Rightarrow A = \mathbb{Z}_+ \in \mathcal{A}'$ ↯

If $|A| < \infty$ let $m = \max A$ $(\in A)$

Then $S_m \subset A$ or $\underset{\not\ni m}{A} \subset \underset{\not\ni m}{S_m}$ ↯

so $\underbrace{S_m \cup \{m\}}_{S_{m+1}} \subset A \subset S_{m+1}$

$\Rightarrow A = S_{m+1} \in \mathcal{A}'$ ↯

AC $\Updownarrow$

Th. $(A, <)$ s.p.o. set $\Rightarrow \exists B \subset A$ max (simply) ordered subset.

Def. $(A, \leq)$ s.p.o. set $\quad B \subset A$ subset

$c \in A$ upper bound for B if

$\forall b \in B$ $\quad b = c$ or $b < c$

$\Omega \in A$ is max. el. if $\nexists a \in A$ $\quad \Omega < a$

Rem. If A is ordered, max el. is unique (if $\exists$), but not when Ω is s.p.o.

<u>Lemma</u> (Zorn) $(A, <)$ s.p.o.

$\Updownarrow$ if $\forall B \subset A$ ordered $\exists$ upper bound of B in A

AC $\Downarrow$ $\Longrightarrow A$ has a max. element

This has some important applications:

① LA $\swarrow$ ② $\searrow$ funct. analysis

every vector space (∞ dim) has a basis (next page)

Hahn-Banach

$T': V' \to W$ $V' \subset V$. linear

$\exists T: V \to W$ $T' = T|_{V'}$ with $\|T\| = \|T'\|$.

W.O.T. $\Downarrow$

③ <u>Def:</u> cardinality

We say $|A| < |B|$ B has greater card than A

if $\exists \iota: A \to B$ inj $\nexists \kappa: B \to A$ inj

$\overset{AC}{\Updownarrow}$ $\exists: B \to A$ surj $\quad$ $\Updownarrow$ AC $\nexists \kappa\ A \to B$ surj

We say $|A| = |B|$ B has same card as A

if $\exists \iota: A \to B$ bij

<u>Th:</u> For any two sets A, B

$\Updownarrow$ either $|A| < |B|$, $|A| = |B|$ or $|B| < |A|$.

W.O.T. (Ex. 1.10.11)

cardinality = eq. class of eq. relation on {all sets} $A \sim B \iff |A| = |B|$ given by

$|\mathbb{Z}_+| = \omega$ countable cardinality

$|\mathbb{R}| = \aleph_0$ "aleph zero" cardinality of the continuum

Th V VS/F V has a basis

Pf. (use AC)

$$\mathcal{K} = \{ A \subset \mathcal{K} \quad A \text{ lin. indep.} \}$$

$(\mathcal{K}, \subsetneq) \subset P(V)$ is s.p.o. set

$\exists$ max chain $\mathcal{E} \subset \mathcal{K}$.

$\boxed{\text{chain} = \text{(singly) ordered subset}}$

Let $B = \bigcup_{E \in \mathcal{E}} E \subset V$.

1) we claim B lin. indep.

$\lambda_i \in F \qquad \sum_{i=1}^{n} \lambda_i v_i = 0 \qquad v_i \in E_i \quad E_i \in \mathcal{E}$

$\mathcal{E}$ chain $\Rightarrow \exists j \quad E_j = \max(E_i) \supset E_i \ \forall i$

$v_i \in E_j \qquad E_j \in \mathcal{E} \subset \mathcal{K}$ lin. indep. $\Rightarrow \lambda_i = 0$.

2) B generating

Assume B not gen. $\exists v \notin \operatorname{span}(B)$ $\quad v \in V$

$\Rightarrow B \cup \{v\}$ linearly indep. $\quad B \cup \{v\} \supset E \ \forall E \in \mathcal{E}$

$\in \mathcal{K}$

$\mathcal{K} \supset \mathcal{E}' = \mathcal{E} \cup \{B \cup \{v\}\} \supset \mathcal{E}$ is a chain in $(\mathcal{K}, \subsetneq)$

$\mathcal{E}$ max $\Rightarrow \mathcal{E}' = \mathcal{E} \Rightarrow B \cup \{v\} \in \mathcal{E}$

$v \in \bigcup_{E \in \mathcal{E}} E = B$ $\quad ⚡$

$\Rightarrow B$ basis

Rem: highly non-constructive: what is a basis of $\mathbb{R}$ over $\mathbb{Q}$??