

21/5/23

## Construction of Real number system

$\mathbb{N}$  = Set of natural numbers

$$\emptyset \longleftrightarrow 0$$

$$0, 1, 2, \dots$$

$$\{\emptyset\} = \{0\} \longleftrightarrow 1$$

$$n \in \mathbb{N} = n \cup \{n\}$$

$$\{0, 1\} \longleftrightarrow 2$$

...

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}$$

$$(n, m) \sim (n', m')$$

$$n+m = n'+m'$$

This  $\sim$  is equivalence relation

$$\text{reflexive } \forall (n, m) \sim (n, m) \quad (n+m = n+m)$$

$$\text{symmetry } (n, m) \sim (n', m')$$

$$\Rightarrow (n', m) \sim (n, m) \quad (n+m' = n'+m)$$

$$n'+m = n+m'$$

$$\text{transitive } (n, m) \sim (n', m')$$

$$(n', m) \sim (n'', m'')$$

$$\Rightarrow (n, m) \sim (n'', m'')$$

$$\begin{aligned} \overline{[(n, m)] + [(\nu, s)]} &= \overline{[(n+\nu), (m+s)]} \\ \overline{[(n+m)] \cdot [(\nu, s)]} &= \overline{[(nr+ms), (nr+ns)]} \end{aligned}$$

Ex:  $(\mathbb{Z}, +, \cdot)$  is commutative ring

$$\text{Proof: } \overline{[(1, 1)]} = 0 = \overline{[(n, 0)]} ; \text{ additive identity}$$

$$\overline{[(2, 1)]} = \overline{[(n+1, n)]} ; \text{ multiplicative identity.}$$

$$\overline{[(n+1, 1)]} \longleftrightarrow n$$

$$\overline{[(1, n+1)]} \longleftrightarrow -n \quad \text{Inverse}$$

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$$

$$\begin{aligned} \overline{[(n+1, 1)] \cdot [(\nu+1, 1)]} &\rightarrow \overline{[(nm+n\nu+n+\nu+2, m+\nu+2)]} \\ n \cdot \nu &\rightarrow \overline{[(nm+1, 1)]} \\ hm & \end{aligned}$$

$\mathbb{Q}$  = field of rational numbers

$\mathbb{Z} \times \mathbb{Z}^*$ ,  $\approx$

$$(p, q) \approx (r, s) \text{ if } ps = qr$$

Ex: i)  $\approx$  is equivalence.

ii)  $\approx (p, q) = p/q$  is the equivalence class of  $(p, q)$

$$\mathbb{Q} = \frac{\mathbb{Z} \times \mathbb{Z}^*}{\approx} = \text{Set of equivalence classes of } \approx$$

Define

$$p/q + r/s = \frac{ps + qr}{qs}, \quad p/q \cdot r/s = \frac{pr}{qs}$$

iii)  $(\mathbb{Q}, +, \cdot)$  is field

$$(0, p) = 0/r \text{ additive}$$

$$(p, p) = p/p = 1 \text{ multiplicative}$$

$$p = p_1 d, \quad q = q_1 d; \quad d = \gcd(p, q)$$

$$\frac{p}{q} = \frac{p_1}{q_1} = -\frac{p_1}{q_1}$$

Standard forms

$$p/q > r/s \quad \text{if} \quad ps > qr$$

$$\text{otherwise} \quad p/q > 0 \quad \text{if} \quad pq > 0$$

Ex: Show that  $\mathbb{Q}$  is an ordered field

Ex: Show that  $\mathbb{Q}$  is not Dedekind complete

$$A = \{x \in \mathbb{Q} : x > 0 \text{ and } x^2 > 2\}$$

Let  $p \in \mathbb{Q}$ . (There exist rational numbers whose square is 2)

$$q = p - \left( \frac{p^2 - 2}{p+2} \right) = \frac{2(p+1)}{p+2} > 0$$

$$q^2 - 2 = \frac{4(p+1)^2}{(p+2)^2} - 2 = \frac{2(p^2 - 2)}{(p+2)^2}$$

If  $p^2 < 2$ , then  $p < \sqrt{2}$  and  $q < \sqrt{2}$

If  $p^2 > 2$ , then  $q < p$  and  $q^2 > 2$

### Dedekind construction of Real numbers

We consider the set of real numbers  $\mathbb{R}$  as a subset of the power set  $P(\mathbb{Q})$  of  $\mathbb{Q}$

Constructing of so called cuts

Def: A subset  $\alpha \subseteq \mathbb{Q}$  is called Dedekind cut if

i)  $\emptyset \neq \alpha \neq \mathbb{Q}$

ii) If  $p \in \alpha$  &  $q < p$ , then  $q \in \alpha$ .

iii) If  $p \in \alpha$ , then  $\exists r \in \alpha$  s.t.  $p \in r$

Ex: Show that  $\mathbb{Q}$  is an ordered field

Ex: Show that  $\mathbb{Q}$  is not Dedekind complete

Proof:  $\mathbb{Q}$  is ordered field.

PC f subset such

$x \in f$ , exactly one of the following

$x \in P$ ,  $-x \in D$   $x=0$

$x, y \in P$ ,  $x+y \in P$   $x+y \in D$

$x \leq y \Leftrightarrow y-x \in P \vee x=y$ .

Let  $a, b \in S$   $\cup S \subset Q$

$a+b \in S$ ,  $a \cdot b \in S$ ,

so  $\mathbb{Q}$  is ordered field

Dedekind Complete (LUB)  $\forall$  non empty bounded above subset of  $K$  has supremum in itself ( $K$ ). Then  $K$  is dedekind complete

complete field:- If  $\forall$  cauchy sequence of element in  $K$  converges to a limit that is also in  $K$ . i.e.  $\forall (a_n) \lim_{n \rightarrow \infty} (a_n) \in K$ .

Example  $\mathbb{R}(x)$  complete but not dedekind complete

$A$  (field of algebraic numbers) is dedekind complete

but not complete or constructive numbers

$\mathbb{Q}$  is not dedekind. : for  $\forall$  non empty bounded above subset of  $K$  isn't have supremum in  $K$ .

$$A = \{x : x > 0, x^2 \leq 2 \quad x \in \mathbb{Q}\}$$

let  $x=1$ ,  $x^2=1$

$\Rightarrow x \in A$

$A$  is nonempty.

consider  $x=3$

$x > 3$  but  $x^2 = 9 \notin A$

so  $x \notin A$

$A$  is bounded above.

Since  $A$  is nonempty bounded above set,

let  $U = \sup(A)$

let  $x = \sqrt{2}$ ,  $x^2 = 2$

clai  $\sup(A) = \sqrt{2}$

If  $b, \sup(A)$

$\Rightarrow b < \sqrt{2}$ ,

by defn  $b < c < \sqrt{2}$

squaring  $b^2 < c^2 < 2$

$c \in A, b < c$ .

so  $b$  is not sup(A).

so  $\sup(A) = \sqrt{2}$

but  $\sqrt{2}$  doesn't belong

$+ \mathbb{Q}$ . so

$\mathbb{Q}$  is not dedekind comp

$$\{r \in \mathbb{Q} : r < 1\}$$

$$R = \{ \alpha \leq \mathbb{Q} : \alpha \text{ is a cut}\}$$

define an order on  $R$  by

$$\alpha \leq \beta \text{ if } \alpha \subseteq \beta$$

Ex: 1) Show that  $\leq$  is total order on  $R$

2)  $\forall$  nonempty bdd rc subset of  $R$  has the supremum in  $R$

$$\left. \begin{array}{l} A \subseteq R \\ \exists r \in R \\ \alpha \in A \Rightarrow \alpha \subseteq r \\ \bigvee \alpha = \beta \\ \alpha \in A \end{array} \right\} \begin{array}{l} \text{try} \\ \text{to complete } R \text{ order} \\ \& \text{& then...} \end{array}$$

### Addition

$$\alpha, \beta \in R$$

$$\alpha + \beta = \{ p+q : p \in \alpha, q \in \beta \} \text{ is cut}$$

$$p \in \mathbb{Q}, \quad p^+ = \{ r \in \mathbb{Q} : r < p \} \rightarrow \text{rational cut}$$

$$0^*, 1^*$$

$$\alpha \in R$$

Let  $\gamma$  be given by

$$\gamma = \{ p \in \mathbb{Q} : -p - \gamma \notin \alpha \text{ for some } r \in \mathbb{Q} \text{ with } r > \gamma \}$$

$$\text{Check: } \alpha + \gamma = \gamma + \alpha = 0^* \quad r = -\alpha$$

Exercise  $(R, +, 0^*)$  is an Abelian group

$$\alpha > 0^*, \beta > 0^*$$

$$\alpha \beta = \{ r \in \mathbb{Q} : r \leq p q \text{ for some positive } p \in \alpha \text{ and } \text{positive } q \in \beta \} \text{ is a cut}$$

$$\alpha \beta^{-1} = \beta^{-1} \alpha = \alpha$$

$$S = \{ r \in \mathbb{Q} : rp < 1-s \text{ & } 0 < p < \alpha \quad \text{if } \alpha \in S \text{ with } s > 0 \}$$

zu 8/23

## Dedekind construction of Real number

$\mathbb{Q} \rightarrow \mathcal{P}(\mathbb{Q}) =$  the set of all subsets of  $\mathbb{Q}$   
powerset of  $\mathbb{Q}$

$\mathbb{R} = \{ \alpha \in \mathcal{P}(\mathbb{Q}) : \alpha \text{ is a Dedekind cut} \}$

$$\alpha \subseteq \mathbb{Q} \quad \emptyset \neq \alpha \neq \mathbb{Q}$$

$$\alpha \subseteq \beta \text{ if } \Rightarrow \alpha \subseteq \beta$$

$$\mathcal{A} = \{ \alpha_j \mid j \in \mathbb{N} \} \subseteq \mathbb{R}$$

$$\alpha_j \subseteq \Rightarrow \bigcup_{j \in \mathbb{N}} \alpha_j$$

$$\alpha + \beta = \{ p+q ; p \in \alpha, q \in \beta \}$$

$$p^* = \{ r \in \mathbb{Q} ; r < p \}$$

$0^*$  → additive identity

$$\alpha + 0^* = 0^* + \alpha = \alpha$$

do what

$$\alpha \in \mathbb{R}$$

$$\gamma = \{ p \in \mathbb{Q} : \exists r \in \mathbb{Q} ; r >_0 \text{ with } -p-r \notin \alpha \} \\ - (\mathbb{Q} \setminus \alpha)$$

$$\alpha > 0^*, \beta > 0^*$$

$$\alpha \beta = \{ r \in \mathbb{Q} : r \leq pq \text{ for } p \in \alpha, q \in \beta \\ \text{ both } p >_0, q >_0 \}$$

$$\alpha^{-1} = \bigcap \alpha = \alpha$$

$$p \in \alpha ; \exists p' \in \alpha \text{ with } p < p'$$

$$p = p'(p/p')$$

$$\alpha >_0$$

$$\exists s \in \mathbb{Q} ; s >_0$$

$$\delta = \{ p \in \mathbb{Q} : pr < 1-s, \forall r \in \alpha, r >_0 \}$$

$$\alpha \delta = \delta \alpha = 1^*$$

$$\alpha \beta = \begin{cases} (-\alpha) \beta & \alpha < 0^* \quad \beta > 0^* \\ -(\alpha) (-\beta) & \alpha > 0^* \quad \beta < 0^* \\ (\alpha) (-\beta) & \alpha < 0^* \quad \beta < 0^* \\ (\alpha) (\beta) & \alpha > 0^* \quad \beta > 0^* \end{cases}$$

$$\alpha 0^* = 0^* \alpha = 0^*$$

$$\mathbb{Q} \rightarrow \mathbb{R}$$

$$p \mapsto p^*$$

$$(p+q^*) = p^* + q^* ; (pq^*) = p^* q^*$$

$$p_1 < p_2 \Rightarrow p_1^* < p_2^*$$

$$\mathbb{R} \xrightarrow{f} \mathbb{Q}$$

$$f(r) = j(r) \text{ if } r \in \mathbb{Q}$$

down

$$\omega = \{ p \in \mathbb{Q} : p \not\in \omega \}$$

$$f(\omega) = \sup \{ f(r) : r < \omega \}$$

$$x - \frac{\lfloor 2^n x \rfloor}{2^n} = \frac{2^n x - \lfloor 2^n x \rfloor}{2^n} \leq \frac{1}{2^n}$$

$$j\left(\frac{\lfloor 2^n x \rfloor}{2^n}\right) \rightarrow x \quad n \rightarrow \infty$$

$$f(n) = \lim_{n \rightarrow \infty} j\left(\frac{\lfloor 2^n x \rfloor}{2^n}\right)$$

$$q \leq \omega \leq \mathbb{Q}$$

$$-\omega < \quad < \omega$$

$$\mathbb{R}^- = \mathbb{R} \cup \{-\omega, \omega\}$$

$$\omega + \omega = \omega + \omega - \omega ; \quad \omega - \omega = (\omega) + \omega = -\omega$$

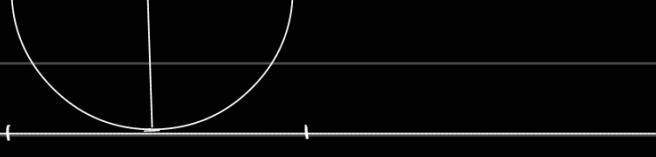
$$\omega \omega = \omega \omega = \begin{cases} \omega & \omega > 0 \\ -\omega & \omega < 0 \end{cases}$$

$$\omega(-\omega) = (-\omega)\omega = \begin{cases} \omega & \omega < 0 \\ -\omega & \omega > 0 \end{cases}$$

$$\omega \omega = (-\omega)(-\omega) = \omega$$

$$(-\omega)(\omega) = (\omega)(-\omega) = (-\omega)$$

$$\omega - \omega \quad \left[ \begin{array}{l} \text{not defined} \\ 0 \omega \end{array} \right]$$



## Set theory

If  $A \rightarrow B$  is bijection, then we say that  $A \& B$  are equivalent  
 $A \sim B$

$\sim X$  is if  $X$  is equivalent to proper subset

$X \rightarrow X$  injective but not surjective

$X$  is finite, if it not infinite

example :  $\mathbb{N}$ 's infin

are  $\mathbb{N}$  is hh

25/6/23  
 $A \sim B$  if  $\exists f: A \rightarrow B$ ,  $f$  is bijection  
↳ equipotent

ex:  $a < b$  are real numbers

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}$$

$$(-\infty, b) = \{x \in \mathbb{R} : x < b\}$$

$$(-\infty, \infty) = \mathbb{R}$$

$$[0, 1] \sim [a, b]$$

$$t \mapsto (1-t)a + tb$$

$$(0, 1) \sim \mathbb{R} ?$$

$X$  is equipotent to a proper subset of  $X$

$$X \sim A ; A \subsetneq X$$

Def:  $X$  is infinite [ $\exists f: X \rightarrow$  injective but not bijective]

Ex:  $\mathbb{N}$  is infinite

$$X \subset Y$$

If  $X$  is infinite  $\rightarrow Y$  is infinite

If  $Y$  is finite  $\rightarrow X$  is finite

$X$  is infinite  $\rightarrow X \cdot \{x\}$  is infinite

\*  $X$  is denumerable if  $X \sim \mathbb{N}$

Countable if either finite or denumerable

Uncountable if it is not countable

$$\text{Ex: } \mathbb{N} \times \mathbb{N} \leftarrow \mathbb{N}$$

$$(m, n) \leftarrow p = 2^{m-1}(2n-1)$$

$$(m, n) \longrightarrow 2^{m-1}(2n-1)$$

Ex: Countable union of countable sets are countable

abcdefghijklmnopqrstuvwxyz

$[0, 1]$  is uncountable

$$x_1 \rightarrow 0.x_{11} x_{12} x_{13} \dots$$

$$x_2 \rightarrow 0.x_{21} x_{22} x_{23} \dots$$

$$x_3 \rightarrow 0.x_{31} x_{32} x_{33} \dots$$

We take  $y = 0.y_1 y_2 y_3 \dots$

$$y_i = \begin{cases} \frac{1}{2} & \text{if } x_{ii} \neq 1 \\ 1 & \text{if } x_{ii} = 1 \end{cases}$$

Then  $y$  would be different from  $x_1, x_2, \dots$  [complete different from the list]

This is called Cantor's diagonal trick.

Q have bijection with  $\mathbb{N}$ .?

Proj construct set with all the from  $\mathbb{N}$  are countable

### Thm: Schröder - Bernstein

If  $f: X \rightarrow Y$  and  $g: Y \rightarrow X$  are injective maps, then  $X \sim Y$ .  
They have same cardinal.

$$[0, 1] \subseteq \mathbb{R} \quad \text{and} \quad \tan: (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R} \quad (0, 1) \subseteq [0, 1]$$

$$[0, 1] \setminus \{0, 1, \frac{1}{2}, \frac{1}{3}, \dots\} \quad (0, 1) \setminus \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$$

Norms :- a function  $f: \mathbb{R}/\{0\} \rightarrow \mathbb{R}^+ \cup \{0\}$   
absolute value on R      vector space      behave like distance from origin.

$$|x| = \max \{|x|, -x|\}$$

$$\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \dots \times \mathbb{R} = \{(a_1, a_2, \dots, a_n) \mid a_i \in \mathbb{R}\}$$

$\mathbb{R}^n$  is vector space over  $\mathbb{R}$

$$(a_1, a_2, a_3, \dots, a_n) + (b_1, b_2, b_3, \dots, b_n) = (a_1+b_1, a_2+b_2, \dots, a_n+b_n)$$

$$\alpha(a_1, a_2, \dots, a_n) = (\alpha a_1, \alpha a_2, \alpha a_3, \dots, \alpha a_n)$$

$$e_1 = (1, 0, 0, \dots, 0)$$

$$e_2 = (0, 1, 0, \dots, 0)$$

$$e_n = (0, 0, \dots, 1)$$

$\{e_1, e_2, \dots, e_n\}$  is basis of  $\mathbb{R}^n$

$$a = (a_1, a_2, a_3, \dots, a_n)$$

$$b = (b_1, b_2, b_3, \dots, b_n) \in \mathbb{R}^n$$

$$\langle a, b \rangle = \text{inner product of } a \& b \quad |a \cdot b|$$

Euclidean inner product in  $\mathbb{R}^n$

$$= a_1 b_1 + a_2 b_2 + \dots + a_n b_n = \sum_{i=1}^n a_i b_i$$

$(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$  is  $n$ -dimensional Euclidean space

### Euclidean norm on $\mathbb{R}^n$

$$\|a\| = \sqrt{\langle a, a \rangle} = \sqrt{\sum_{i=1}^n a_i^2}$$

#### Properties

$$1) \|a\| \geq 0 \quad \text{and} \quad \|a\| = 0 \iff a = 0$$

$$2) \|\alpha a\| = |\alpha| \|a\|$$

$$3) \|a+b\| \leq \|a\| + \|b\| \quad (\text{Triangle inequality})$$

$$\begin{aligned} 0 &\leq (\|a+b\|)^2 = \langle a+b, a+b \rangle \\ &= \sum (a+b)^2 \\ &= \sum a_i^2 + 2 \sum b_i + 2 \sum a_i b_i \\ &= A + C + 2B \end{aligned}$$

Then  $A + C + 2B \leq 0 \Rightarrow (B^2 - C)A \leq 0$

$$B^2 \leq A C$$

$$\left| \sum_{i=1}^n a_i b_i \right| \leq \sqrt{\left( \sum_{i=1}^n a_i^2 \right)} \sqrt{\left( \sum_{i=1}^n b_i^2 \right)}$$

$$|\langle a, b \rangle| \leq \|a\| \|b\| \rightarrow \text{Cauchy-Schwarz Inequality}$$

$$\Rightarrow |a \cdot b| \leq \|a\| \|b\|$$

Proof:  $\langle a, b \rangle = \sum_{i=1}^n a_i b_i$

$$\|a\| = \left( \sum_{i=1}^n a_i^2 \right)^{1/2}$$

$$\|b\| = \left( \sum_{i=1}^n b_i^2 \right)^{1/2}$$

*Awst*

we know

$$\left( \sum_{i=1}^n a_i b_i \right)^2 \leq \left( \sum_{i=1}^n a_i^2 \right) \left( \sum_{i=1}^n b_i^2 \right) \rightarrow \text{by Lagrange Identity}$$

$$\left( \sum_{i=1}^n a_i b_i \right)^2 \leq \left( \sum_{i=1}^n a_i^2 \right)^{1/2} \left( \sum_{i=1}^n b_i^2 \right)^{1/2}$$

$$|\langle a, b \rangle| \leq \|a\| \|b\|$$

Lagrange

$$\left( \sum_{i=1}^n a_i b_i \right)^2 = \left( \sum_{i=1}^n a_i^2 \right) + \left( \sum_{i=1}^n b_i^2 \right)^2 - 2 \left( \sum_{1 \leq i < j \leq n} a_i b_j - a_j b_i \right)$$

$$a = (a_1, a_2, a_3, \dots, a_n) \in \mathbb{R}^n, b = (b_1, b_2, \dots, b_n) \in \mathbb{R}^n$$

$$\left( \sum_{i=1}^n a_i^2 \right) \left( \sum_{k=1}^n b_k^2 \right) = \sum_{i=1}^n \sum_{j=1}^n a_i^2 b_j^2 =$$

$$= \sum_{i=1}^n a_i^2 b_i^2 + \sum_{i=1}^{n-1} \sum_{j=i+1}^n a_i^2 b_j^2$$

$$\sum_{j=1}^n \sum_{i=j+1}^n a_i^2 b_j^2$$

$$\left( \sum_{i=1}^n a_i b_i \right)^2 = \sum_{i=1}^n a_i^2 b_i^2 + 2 \sum_{i=1}^n \sum_{j=i+1}^n a_i b_i a_j b_j$$

$$\sum_{i=1}^n \sum_{j \neq i} (a_i b_j - a_j b_i)^2 = \sum_{i=1}^n \sum_{j=i+1}^n (a_i^2 b_j^2 + a_j^2 b_i^2) - 2 \sum_{i=1}^n \sum_{j \neq i} a_i b_j a_j b_i$$

$$\sum_{i=1}^n \sum_{j=i+1}^n (a_i b_j - a_j b_i)^2 = \sum_{i=1}^n \sum_{j=i+1}^n a_i^2 b_j^2 + \sum_{j=1}^n \sum_{i=j+1}^n a_i^2 b_j^2 - 2 \sum_{i=1}^n \sum_{j=i+1}^n a_i b_j a_j b_i$$

$$\rightarrow \left( \sum_{i=1}^n a_i b_i \right)^2 - \left( \sum_{i=1}^n a_i^2 \sum_{k=1}^n b_k^2 \right) = \sum_{j=1}^n \sum_{i=1}^j (a_i b_j - a_j b_i)^2$$

By this

$$\begin{aligned} \|a+b\|^2 &= \langle a+b, a+b \rangle \\ &= \langle a, a \rangle + 2 \langle a, b \rangle + \langle b, b \rangle \\ &= \|a\|^2 + 2 \langle a, b \rangle + \|b\|^2 \\ &= (\|a\|^2 + 2 \langle a, b \rangle + \|b\|^2)^{1/2} \\ &\leq (\|a\|^2 + 2\|a\|(\|b\|) + \|b\|^2)^{1/2} \\ &\leq (\|a\| + \|b\|) \end{aligned}$$

$\rightarrow \|a+b\| \leq \|a\| + \|b\| \rightarrow \text{triangle Inequality}$

$\|\cdot\| : V \rightarrow \mathbb{R}$

$V$  is a vector space over  $\mathbb{R}$

$1 \leq p < \infty$

$$\|a\|_p = \left[ \sum_{i=1}^n |a_i|^p \right]^{1/p}$$

Other norms

$$\|a\|_2 = \left( \sum_{i=1}^n a_i^2 \right)^{1/2}$$

$$\|a\|_1 = \sum_{i=1}^n |a_i|$$

$$\|a\|_\infty = \sup \{|a_i| : 1 \leq i \leq n\}$$

$$d_C(a, b) = \|a-b\|_2$$

$$d_1(a, b) = \|a-b\|_1$$

$$d_\infty(a, b) = \|a-b\|_\infty$$

