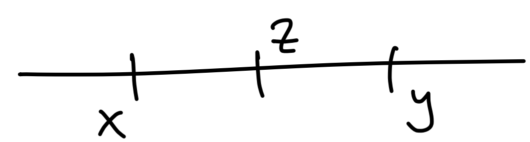
MAT 320 Lecture 1 8/26/2020

Numbers:

- Natural numbers $\mathbb{N}$: $1, 2, 3, 4, \ldots$
- Integer numbers $\mathbb{Z}$: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$
- Rational numbers $\mathbb{Q}$: numbers that can be expressed as an irreducible fraction m/n; where $m, n \in \mathbb{Z}$, $n \neq 0$.
- Real numbers $\mathbb{R}$

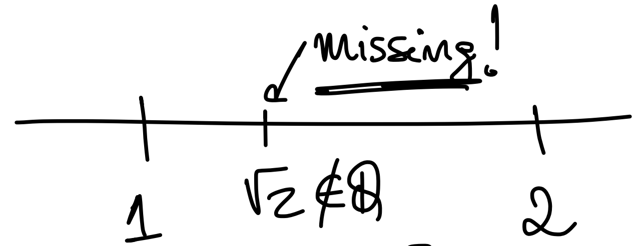
Q: Can you find a rational number strictly between any two given rational numbers?



$\forall x, y \in \mathbb{Q}, \ \exists z \in \mathbb{Q}, \ x < z < y$, e.g., take $z = \frac{x+y}{2} \in \mathbb{Q}$.

Q: Are "all numbers" between $x, y \in \mathbb{Q}$ also rational?

A: No, e.g., there exists no rational number $z \in \mathbb{Q}$ such that $z^2 = 2$.



Pf: Suppose, by contradiction, that $\exists z \in \mathbb{Q}$, $z^2 = 2$.

Then $z = m/n$, where $m, n \in \mathbb{Z}$, $n \neq 0$ and m, n share no common prime factors.

$$2 = z^2 = m^2/n^2 \implies m^2 = 2n^2$$

$\implies m^2$ is even. $\implies m$ is even $\implies m^2$ is divisible by 4.

$\implies 2n^2 = m^2$ is also divisible by 4.

$\implies n^2$ is divisible by 2 $\implies n$ is even. Contradiction.

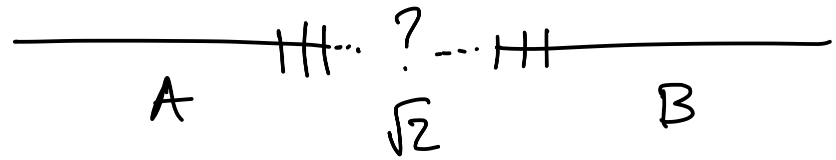
$\square$

Least upper bound / Largest lower bound might not exist in $\mathbb{Q}$:

(sup / inf)

$$A := \{ x \in \mathbb{Q} : x^2 < 2 \}$$

$$B := \{ y \in \mathbb{Q} : y^2 > 2 \}$$



Claim: A has no least upper bound in $\mathbb{Q}$.

Pf: Choose $p \in A$. We will find $q \in A$, s.t. $q > p$.

Let

$$\underbrace{q = p - \frac{p^2 - 2}{p+2}}_{\Rightarrow\ q > p.} = \frac{p^2 + 2p - p^2 + 2}{p+2} = \frac{2p+2}{p+2} \in \mathbb{Q}$$

Then

$$q^2 - 2 = \frac{4p^2 + 8p + 4}{p^2 + 4p + 4} - 2 = \frac{4p^2 + \cancel{8p} + 4 - 2p^2 - \cancel{8p} - 8}{p^2 + 4p + 4} =$$

$$= \frac{2p^2-4}{(p+2)^2} = \frac{2(p^2-2)}{(p+2)^2} < 0 \quad \begin{matrix} p\in A \\ (p^2<2) \end{matrix}$$

So $q^2 < 2$. Thus, $q \in A$ and $q > p$ as desired. $\square$

Ordered sets

<u>Def</u>: An <u>order</u> on a set S is a relation $<$ on S, s.t.:

(i) $\forall x, y \in S$ one (and only one) of the following holds:

$$x < y, \qquad x = y, \qquad y < x$$

(ii) transitivity: $\forall x, y, z \in S$: $x < y,\ y < z \implies x < z$.

<u>Def</u>: If $(S, <)$ is an ordered set and $E \subset S$ such that $\exists \beta \in S$ s.t. $\forall x \in E$, $x \leq \beta$, then E is <u>bounded from above</u>.

Def: Suppose $(S, <)$ is an ordered set, $E \subset S$ bounded from above, if $\exists\, \alpha \in S$ s.t.

(i) α is an upper bound for E

(ii) If $\gamma < \alpha$, then γ is not an upper bound for E

then α is called the least upper bound of E, also denoted

$\alpha = \sup E.$ ← "supremum"

(Similarly, define largest lower bound for sets which are bounded from below, "infimum", $\alpha = \inf E$)

Examples: $E = \{\frac{1}{n} : n \in \mathbb{N}\} = \{1, \frac{1}{2}, \frac{1}{3}, \dots\} \subset \mathbb{Q}$

$\inf E = 0 \notin E$

$\sup E = 1 \in E$

Example: The set $A = \{x \in \mathbb{Q} : x^2 < 2\}$ does not have a sup in $\mathbb{Q}$; $B = \{y \in \mathbb{Q} : y^2 > 2\}$ does not have an inf in $\mathbb{Q}$.

Definition: An ordered set $(S, <)$ has the least-upper-bound property if $\forall E \subset S$, $E \neq \emptyset$, E bounded from above, the least upper bound $\sup E$ exists in S.

Q: Does the least-upper-bound property (i.e., existence of sup) guarantee the analogous "largest-lower-bound property" (existence of inf)?

A: Yes!

Thm: Suppose $(S, <)$ is an ordered set w/ least-upper-bound property, $B \subset S$, $B \neq \emptyset$, bounded from below. Let L be

the set of all lower bounds of B; $\alpha := \sup L \in S$.
Then $\alpha = \inf B$.

<u>Pf:</u> B bounded from below $\Rightarrow L \neq \phi$

$\forall b \in B$, b is an upper bound for L; so L is bounded from above, so $\exists \alpha = \sup L \in S$.

If $\gamma < \alpha$, then γ is <u>not</u> an upper bound for L; so $\gamma \notin B$. Thus, $\forall b \in B$, $\alpha \leq b$; that is $\alpha \in L$.

If $\alpha < \beta$, then $\beta \notin L$ since α is an upper bound for L.

Altogether, we showed $\alpha = \sup L \in L$, but $\beta \notin L$ if $\beta > \alpha$; this means that $\alpha = \inf B$.

$\square$

Fields

Def: A <u>field</u> is a set F with an addition $+ : F \times F \to F$ and a multiplication $\times : F \times F \to F$ satisfying the following axioms:

(A1) $x, y \in F$, $x + y \in F$

(A2) $x + y = y + x$, $\forall x, y \in F$

(A3) $(x+y) + z = x + (y+z)$, $\forall x, y, z \in F$

(A4) $\exists\, 0 \in F$ s.t. $0 + x = x$, $\forall x \in F$

(A5) $\forall x \in F$ $\exists -x \in F$ s.t. $x + (-x) = 0$

(M1) $x, y \in F$, $x \cdot y \in F$

(M2) $xy = yx, \quad \forall x, y \in F$

(M3) $(xy)z = x(yz), \quad \forall x, y, z \in F$

(M4) $\exists\, 1 \in F$ s.t. $1 \neq 0$ and $1 \cdot x = x, \quad \forall x \in F$

(M5) $\forall x \in F,\ x \neq 0 \quad \exists\, 1/x \in F$ s.t. $x \cdot \frac{1}{x} = 1$

(D) $x(y+z) = xy + xz, \quad \forall x, y, z \in F$

<u>Examples</u>: $\mathbb{Q}$ rational numbers

$\mathbb{R}$ real numbers

$\mathbb{C}$ complex numbers

$\left.\begin{matrix} \mathbb{R} \\ \mathbb{C} \end{matrix}\right\}$ (to be defined soon)

<u>Def</u>: An <u>ordered field</u> is a field and an ordered set s.t. $x + y < x + z \quad \forall x, y, z \in F$ s.t. $y < z$

$xy > 0$ if $x, y \in F$ s.t. $x > 0$, $y > 0$.

<u>Next lecture:</u> $\mathbb{R}$ will be defined as the (unique) ordered field that has the least-upper-bound prop.