Welcome to Math 104!!

Goal: study the following in a mathematically rigorous manner:

- definitions of limit, continuity, differentiation, integration, etc.
- proofs of important results in analysis, e.g. intermediate value theorem, mean value theorem, etc.

Today: What are real numbers?

- Intuitively, the set of real numbers (denoted by $\mathbb{R}$) has 1-1 correspondence with points on the "real line"

- This is not a completely rigorous definition of $\mathbb{R}$. We'll introduce the properties that uniquely characterize $\mathbb{R}$. (see §6 for the precise definition).

Def: A field is a set F along with two operations, denoted "$+$" and "$\cdot$", satisfying:

1) $a, b \in F \Rightarrow a+b,\ a \cdot b \in F$.
   (F is closed under "$+$" and "$\cdot$")

2) "$+$" and "$\cdot$" are associative $\begin{pmatrix}(a+b)+c = a+(b+c),\\ (a\cdot b)\cdot c = a\cdot(b\cdot c)\end{pmatrix}$,
   commutative $\begin{pmatrix}a+b=b+a,\\ a\cdot b = b\cdot a\end{pmatrix}$, distributive $\left(a\cdot(b+c) = a\cdot b + a\cdot c\right)$.

3) F has identity elements "0" and "1" for "$+$" and "$\cdot$"

where $a + 0_F = a$, $a \cdot 1_F = a$; and $0_F \neq 1_F$

4) $\forall a \in F$, $\exists b \in F$ s.t. $a + b = 0_F$. ($\exists$ additive inverse).

5) $\forall a \in F \setminus \{0\}$, $\exists b \in F$ s.t. $a \cdot b = 1_F$ ($\exists$ mult. inverse)

Notations:

- "$a \in S$": a is an element in S.
- "$\Rightarrow$": implies
- "$\forall$": for all
- "$\exists$": there exists
- "s.t.": such that
- "$S \subseteq T$": S is a subset of T. ($\forall a \in S$, we have $a \in T$)

- $\mathbb{N} = \{1, 2, 3, 4, \dots\}$
  $\cap$
  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ } NOT
  $\cap$
  $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0\}$.
  $\cap$
  $\mathbb{R}$ } fields.

- $\exists$ fields w/ only finitely many elements.

e.g. p prime, $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}$

$$\bar{a} + \bar{b} := \overline{a+b} \mod p$$

$$\bar{a}\bar{b} := \overline{ab} \mod p.$$

$\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$

$\bar{0}+\bar{0}=\bar{0}$	$\bar{0}\cdot\bar{0}=\bar{0}$
$\bar{0}+\bar{1}=\bar{1}$	$\bar{0}\cdot\bar{1}=\bar{0}$
$\bar{1}+\bar{0}=\bar{1}$	$\bar{1}\cdot\bar{0}=\bar{0}$
$\bar{1}+\bar{1}=\bar{0}$	$\bar{1}\cdot\bar{1}=\bar{1}$

If $\bar{0} \leq \bar{1}$,
then $\bar{1}+\bar{0} \leq \bar{1}+\bar{1}$
$\bar{1} \quad \bar{0}$

Def: A field F is called <u>ordered</u> if there exists an ordering, denoted "$\leq$", satisfying:

1) $\forall a, b \in F$, at least one of the following is true:
"$a \leq b$" or "$b \leq a$"

Moreover, if $a \leq b$ and $b \leq a$, then $a = b$.

2) $a \leq b$, $b \leq c \Rightarrow a \leq c$.

3) $a \leq b \Rightarrow a + c \leq b + c$.

4) $a \leq b$, $0 \leq c \Rightarrow ac \leq bc$

e.g. $\mathbb{Q}$, $\mathbb{R}$ ordered field.

$\Rightarrow \mathbb{Z}/p\mathbb{Z}$ not ordered field.

Rmks: Any ordered <u>field</u> contains a copy of $\mathbb{Z}$.

$$-2_F < -1_F < 0_F < 1_F < 2_F < \cdots\cdots$$

$-2_F = -1_F - 1_F$ $\qquad$ $2_F = 1_F + 1_F$

In particular, any finite field can't be ordered.

---

§ Least upper bound property. ("secret sauce of $\mathbb{R}$")
(a.k.a. completeness axiom).

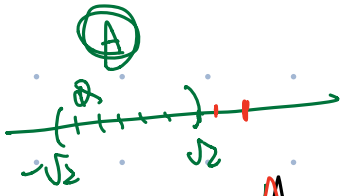
Def Let F be an ordered field. (e.g. $\mathbb{Q}, \mathbb{R}$)
Let $A \subseteq F$ subset of F.

We say $z \in F$ is an upper bound of A
if $a \leq z \quad \forall a \in A$.

We say a subset $A \subseteq F$ is bounded above
if an upper bound of A exists.

e.g. $F = \mathbb{Q}$

- $A = \{1, 2, 3\}$ is bounded above: $\sup A = 3$
  any number ≥ 3 is an upper bound of A.
- $A = \{1 - \frac{1}{n} \mid n \in \mathbb{N}\}$ (HW: $\sup A = 1$)
  $= \{0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \cdots, \frac{n-1}{n}, \cdots\}$ is bounded above.



any number ≥ 1 is an upper bound of A.

- $A = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$ is bounded above

  any rational number $> \sqrt{2}$ is an upper bound of A

  ↓ the least upper bound does not exist in $\mathbb{Q}$.

- $A = \mathbb{N} \subseteq \mathbb{Q}$ is not bounded above.

~~$A \subseteq F$, F is ordered field.~~

Def We say $z \in F$ is the **least upper bound** of A if $z \leq z'$ for any upper bound z' of A.

($\sup A :=$ least upper bound of A (supremum))

Def We say an ordered field F has the **least upper bound property** if for any nonempty subset $A \subseteq F$ that's bounded above, ~~there exists~~ the least upper bound of A exists in F.

~~Ex~~ $\mathbb{Q}$ doesn't satisfy the least upper bound property.

Thm (Completeness Axiom) $\mathbb{R}$ is the unique ordered field satisfying the least upper bound property.

Rmk: "$\mathbb{N} \subseteq \mathbb{R}$ is not bounded above" is not trivial to prove

(Why?
$\exists$ ordered field F s.t. $\mathbb{N} \subseteq F$ is bounded above.)

We need the ~~Completeness~~ least upper bound property to prove it:

pf: Assume the contrary; i.e. $\mathbb{N} \subseteq \mathbb{R}$ is bounded above.

By LUB property, $\exists\ z := \sup \mathbb{N} \in \mathbb{R}$

$$n \leq z \quad \forall\ n \in \mathbb{N}$$

$$n+1 \leq z \quad \forall\ n \in \mathbb{N}$$

(in $\mathbb{N}$)

$$\Rightarrow \quad n \leq z-1 \quad \forall\ n \in \mathbb{N}$$

$\Rightarrow$ $z-1$ is an upper bound of $\mathbb{N}$

This contradicts w/ the assumption that z is the least upper bound of $\mathbb{N}$. $(z-1 < z)$

$\square$

Rmk: The least upper bound $A \subseteq F$ is unique (if exists).

pf: Say z, z' are both least upper bound of A

$z = z'$ $\Leftarrow$ $z \leq z'$ $(\because z$ is a least upper bound)
$z' \leq z$

Denseness of $\mathbb{Q}$ in $\mathbb{R}$.

$\forall\, a, b \in \mathbb{R}$, say $a < b$.

$\exists\, r \in \mathbb{Q}$ s.t. $a < r < b$.

---

pf: We want to find $m, n \in \mathbb{Z}$, $n > 0$

$$a < \frac{m}{n} < b$$

$$an < m < bn$$

Step 1: Find $n \in \mathbb{N}$ s.t. $bn - an > 1$

$n(b-a)$

Step 2: If $r_1, r_2 \in \mathbb{R}$, $r_2 - r_1 > 1$,
then $\exists\, m \in \mathbb{Z}$ s.t. $r_1 < m < r_2$

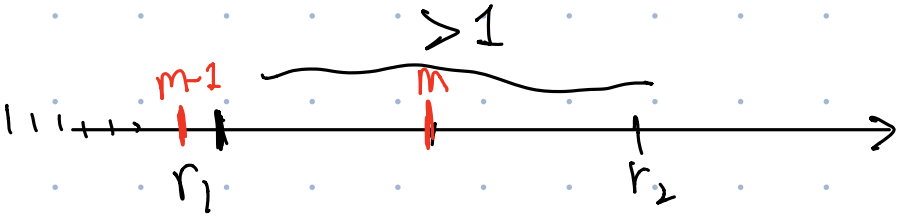
(is not true for arbitrary ordered fields)

We can always find $n \in \mathbb{N}$ big enough s.t. $n(b-a) > 1$

$\Updownarrow$

($\because$ $\mathbb{N} \subseteq \mathbb{R}$ not bounded above) $\quad n > \frac{1}{b-a}$

The proof relies on least upper bound property of $\mathbb{R}$.



$A := \{a \in \mathbb{Z} \mid a \leq r_1\}$ is bounded above

$m-1 := \sup A \in \mathbb{R}$ exists by LUB prpty of $\mathbb{R}$

$\mathbb{Z}$

Claim: $r_1 < m < r_2$

pf: "$r_1 < m$": if $r_1 \geq m$, then $m \in A$

contradicts w/ $m-1$ is an upper bound of A.

"$m < r_2$": $m \leq r_1 + 1 < r_2$

$r_2 - r_1 > 1$