Lecture 2

CS 117, S25

Announcements:

- Office hours:
  - Mondays 2:30-3:30pm
  - Fridays 1-2pm

- Makeup lectures:
  - Friday, April 25, 11am-12:15pm
  - Friday, May 9, 11am-12:15pm

- Exams
  - Tuesday, April 29th: Midterm 1
  - Thursday, May 29th: Midterm 2
  - Monday, June 9th: Final Exam (12-3pm)

- HW1, Q10 now unstarred

Recall:

Numbers!

Natural numbers $\mathbb{N} = \{1, 2, 3, 4, \dots\}$

Integers $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

Rational numbers $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$

Real numbers $\mathbb{R} = ?$

Def: A binary operation on a set X is a function from $X \times X$ to X.

Def: (field) A set F is a field if it has two binary operations (addition and multiplication) that satisfy the following properties $\forall a, b, c \in F$:

(A1) $a+(b+c)=(a+b)+c$ associativity

(A2) $a+b=b+a$ commatativity

(A3) $\exists$ an element $0 \in F$ s.t. identity

$\forall a \in F$, $a+0=a$.

(A4) for each $a \in F$, $\exists! b \in F$ inverse

s.t. $a+b=0$; denote $-a := b$

(m1) $a(bc)=(ab)c$ associativity

(m2) $ab=ba$ commatativity

(m3) $\exists$ an element $1 \in F \setminus \{0\}$ identity

s.t. $\forall a \in F$, $a \cdot 1 = a$

(m4) for each $a \in F \setminus \{0\}$, $\exists!$ inverse

$b \in F$ s.t. $ab=1$;

denote $\frac{1}{a} = a^{-1} = b$.

(D2) $a(b+c)=ab+ac$ distributive law

<u>Thm</u>: $\mathbb{Q}$ is a field.

Using the definition of a field, you can rigorously prove familiar algebraic properties.

Thm: If F is a field, then $\forall a,b \in F$,
(i) if $a+c=b+c$, then $a=b$;
(ii) $a \cdot 0 = 0$.

Def (ordered field): A field F is an *ordered field* if it has an ordering relation $\leq$ so that, for all $a,b,c \in F$,
(O1) either $a \leq b$ or $b \leq a$ totality
(O2) if $a \leq b$ and $b \leq a$, then $a=b$ antisymmetry
(O3) if $a \leq b$ and $b \leq c$, then $a \leq c$ transitivity
(O4) if $a \leq b$, then $a+c \leq b+c$ addition
(O5) if $a \leq b$ and $c \geq 0$, then $ac \leq bc$ multiplication

Def: Given an ordered field and $a,b \in F$, if $a \leq b$ and $a \neq b$, then write $a<b$.

Thm: Suppose F is an ordered field. Then $\forall a,b,c \in F$,

(i) $a \leq b \Rightarrow -b \leq -a$

(ii) $a \leq b$ and $c \leq 0 \Rightarrow ac \geq bc$

(iii) $0 \leq a$ and $0 \leq b \Rightarrow 0 \leq ab$.

(iv) $0 \leq a^2$, where $a^2 := a \cdot a$

(v) $0 < a \Rightarrow 0 < \frac{1}{a}$.

Thm: $\mathbb{Q}$ is an ordered field.

Prop: Suppose F is an ordered field. Then $\forall p,q \in F$ with $p<q$, $\exists r \in F$ s.t. $p<r<q$.

Def: For any $a \in F$, $|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$

Thm (basic properties of $|\cdot|$): For all $a, b \in F$,

(i) $|a| \geq 0$

(ii) $|ab| = |a||b|$ ← distributes over multiplication

(iii) $|a| \geq a$ and $|a| \geq -a$

(iv) $|a+b| \leq |a| + |b|$ ← triangle inequality

Def: For any $a, b \in F$,
$\text{dist}(a,b) := |a-b|$.

On an ordered field, we can define the notion of maximum or minimum of a set.

Def (maximum, minimum): Suppose $S \subseteq F$, where F is an ordered field.

- If there exists $s_0 \in S$ satisfying $s_0 \geq s \ \forall s \in S$, then s_0 is the maximum of S and write $s_0 = \max(S)$.
  "s_0 is the largest element in the set"

- If there exists $s_0 \in S$ satisfying $s_0 \leq s \ \forall s \in S$, then s_0 is the minimum of S and write $s_0 = \min(S)$.

"s_0 is the smallest element in the set"

Ex: Let F be an ordered field. Then any finite set $\{s_1, s_2, \ldots, s_n\} \subseteq F$ has a maximum and minimum.

Ex: Let $F = \mathbb{Q}$. Then $S := \mathbb{N} \subseteq \mathbb{Q}$ and $\min(S) = 1$ and $\max(S)$ D.N.E.

Fix $a, b \in \mathbb{Q}$, $a < b$. Let $S := \{q \in \mathbb{Q} : a \leq q < b\}$. $\min(S) = a$,

Claim: $\max(S)$ D.N.E.

Pf: Assume, for the sake of contradiction, that $s_0 \in \mathbb{Q}$ satisfies $s_0 = \max(S)$.

Since $s_0 \in S$, $a \leq s_0 < b$.
By our prop, $\exists\, r \in \mathbb{Q}$ s.t. $s_0 < r < b$.
Thus $r \in S$, and this contradicts that s_0 was the maximum.

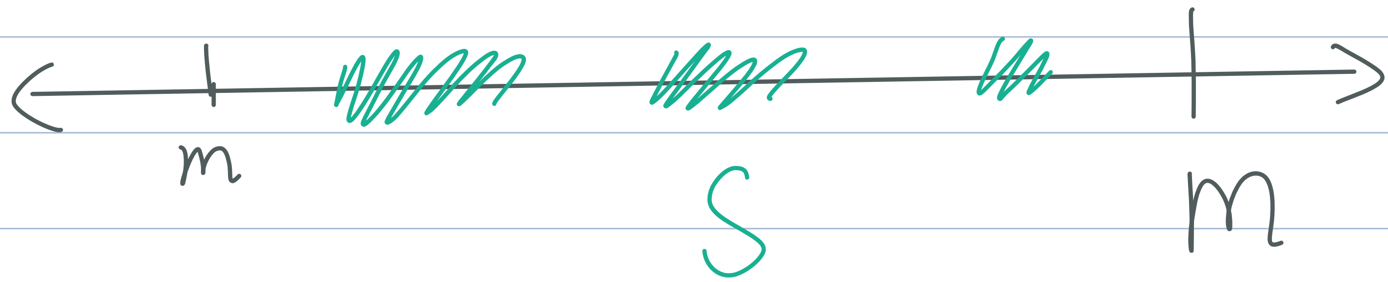
Likewise, on an ordered field, we can define what it means for a set to be bounded above or below.

Def: (bounded above/below): Suppose $S \subseteq F$, for an ordered field F,

- If there exists $M \in F$ s.t. $s \leq M$ $\forall s \in S$, then S is <u>bounded above</u> and M is an <u>upper bound</u> of S.

- If there exists $m \in F$ s.t. $s \geq m$ $\forall s \in S$, then S is <u>bounded below</u> and m is an <u>lower bound</u> of S.

• If S is bounded above <u>and</u> below, then S is <u>bounded</u>.



Ex: $F = \mathbb{Q}$, $a, b \in \mathbb{Q}$, $a < b$

$S = \{q \in \mathbb{Q} : a \leq q < b\}$ is bounded

$\mathbb{N}$ is not bounded

$S = \{q \in \mathbb{Q} : 0 \leq q < 5\}$

What about when a set "almost" has a maximum?

<u>Def</u> (supremum/infimum): Consider an ordered field F.

• If $S \subseteq F$ is bounded above and there exists $M_0 \in F$ satisfying...

(a) M_0 is an upper bound of S
(b) if M is an upper bound of S, then $M_0 \leq M$

we say M_0 is the <u>supremum</u> of S and write $M_0 = \sup(S)$.
"M_0 is the least upper bound of S"

- If $S \subseteq F$ is bounded below and there exists $m_0 \in F$ satisfying...
  (a) m_0 is a lower bound of S
  (b) if m is a lower bound of S, then $m_0 \geq m$.

we say m_0 is the <u>infimum</u> of S and write $m_0 = \inf(S)$.
"m_0 is the greatest lower bound of S"

Thm: Given $S \subseteq F$, F an ordered field,
- if $\max(S)$ exists, $\sup(S) = \max(S)$;
- if $\min(S)$ exists, $\inf(S) = \min(S)$

Pf: HW

Rmk: The supremum generalizes the idea of maximum.

Ex: $F = \mathbb{Q}$, $a, b \in \mathbb{Q}$, $a < b$
$S = \{q \in \mathbb{Q} : a \leq q < b\}$.

Claim: $\sup(S) = b$

Pf: By defn, b is an upper bound of S. Assume, for the sake of contradiction that $\exists\ M$ s.t. M is an upper bound of S and $M < b$. By Prop $\exists\ r \in \mathbb{Q}$ s.t.

$m < r < b$.
Since m is an upper bound of S, $m \geq a$. Thus, by transitivity, $a \leq r < b$, so $r \in S$. This contradicts that m is an upper bound of S.

__Def__ (real numbers): The real numbers is the ordered field containing $\mathbb{Q}$ with the property that every nonempty subset $S \subseteq \mathbb{R}$ that is bounded above has a supremum.

"The least upper bound property of $\mathbb{R}$"

Ex: $\{q \in \mathbb{Q} : 0 \leq q^2 < 2\} \subseteq F := \mathbb{Q}$
We will show that $\mathbb{Q}$ does not have this property

Thm: The real numbers exist and are unique.

Pf: Spivak, <u>Calculus</u>, last chapter.

How does $\mathbb{R}$ relate to other numbers?

By def, $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$.

In fact, $\mathbb{Q} \subsetneq \mathbb{R}$.

Homework: $\sqrt{2} \in \mathbb{R}$

that is, $\nexists\, a \in \mathbb{Q}$ s.t. $a \cdot a = 2$

Prop: $\sqrt{2} \notin \mathbb{Q}$

Pf: Previous course ☺

Thm: The natural numbers $\mathbb{N}$ is the smallest subset of $\mathbb{R}$ having the properties that

(i) $1 \in \mathbb{N}$

(ii) $n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$

"smallest", in the sense of set inclusion.

Note: $|X| < +\infty$, then $|2^X| = 2^{|X|}$

Pf: $2^X = \{\text{all subsets of } X\}$

Let $\mathcal{A} \subseteq 2^{\mathbb{R}}$ be

$\mathcal{A} := \{A \subseteq \mathbb{R} : 1 \in A \text{ and } n \in A \Rightarrow n+1 \in A\}$.

Define

$\bigcap \mathcal{A} := \{x \in \mathbb{R} : x \in A \quad \forall A \in \mathcal{A}\}$

By defn, $1 \in \bigcap \mathcal{A}$. Suppose $n \in \bigcap \mathcal{A}$. Then $n+1 \in \bigcap \mathcal{A}$.

Therefore $\bigcap \mathcal{A} \in \mathcal{A} \Rightarrow \mathbb{N} \subseteq \bigcap \mathcal{A}$.

For any subset of $\mathbb{R}$ satisfying the conditions of the theorem, we see that it contains $\bigcap \mathcal{A}$.

It remains to show $\bigcap \mathcal{A} \subseteq \mathbb{N}$. Since $\mathbb{N} \in \mathcal{A}$, we must have $\bigcap \mathcal{A} \subseteq \mathbb{N}$.

$\square$

Rmk: This property of $\mathbb{N}$ forms the basis for proof by induction...

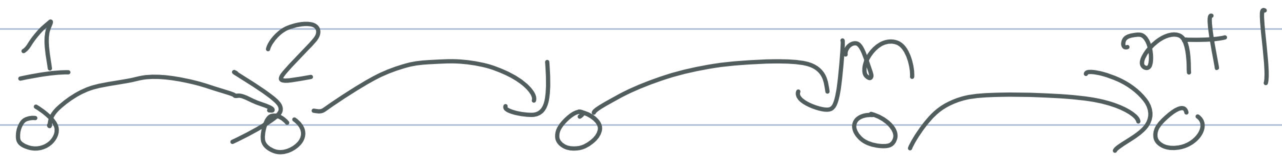
Suppose you have a list of statements

$$\{P_1, P_2, \ldots\} = \{P_k : k \in \mathbb{N}\}$$

Suppose that you show

- P_1 is true
- $\forall n \in \mathbb{N}$, P_n is true $\Rightarrow$ P_{n+1} is true.

Consider $S := \{k : P_k \text{ is true}\} \subseteq \mathbb{N}$.
Then we have shown S satisfies (i) and (ii) of previous thm, so $\mathbb{N} \subseteq S$. $\Rightarrow$ $\mathbb{N} = S$.



We'll study two major theorems for $\mathbb{R}$:

<u>Archimedean Property</u>

<u>$\mathbb{Q}$ is dense in $\mathbb{R}$</u>

Thm (Archimedean Property):
If $a, b \in \mathbb{R}$ satisfy $a > 0$, $b > 0$, then $\exists\, n \in \mathbb{N}$ s.t. $na > b$. ← bathtub

spoon

"even with a very small spoon,
you can fill a large bathtub"