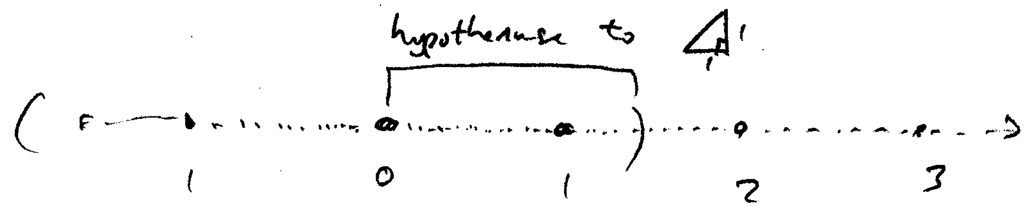
Lecture 3:4 Constructing the reals.

Technique "Dedekind cuts." (1872).



$x^2 = 2$ has no solution in $\mathbb{Q}$.

Consider the set $A = \{x \in \mathbb{Q} : x^2 < 2\}$.

Def: Say $E \subset S$, an ordered set. If there exists ($\exists$) $\beta \in S$ s.t. for all ($\forall$) $x \in E$, we have $x \leq \beta$, then β is an upper bound for E, and we say E is bounded above.

Lower bound is defined similarly (replace $\leq$ with $\geq$).

Ex: • 2 is an upper bound for A

• $\frac{3}{2}$ is an upper bound for A. (Why? If not, $\exists x \in A$ s.t. $x > \frac{3}{2}$. Then $x^2 > \left(\frac{3}{2}\right)^2 > 2$. So $x \notin A$. ↯.)

Def: If $\exists\, \alpha \in S$ s.t.

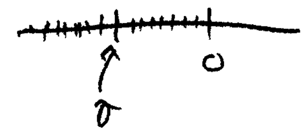
1. α is an upper bound of E
2. If $\gamma < \alpha \Rightarrow \gamma$ is not an upper bound for E

alternate defn: $\gamma \leq \alpha$ is an u.b.

Then α is a least upper bound of E, or supremum of E: $\boxed{\alpha = \sup E}$.

Ex: • $E = \{\frac{1}{2}, 1, 2\}$ $\boxed{\sup E = 2}$ (Finite sets have a sup.)

• $E = \mathbb{Q}^-$ (negative rationals). $\boxed{\sup E = 0}$

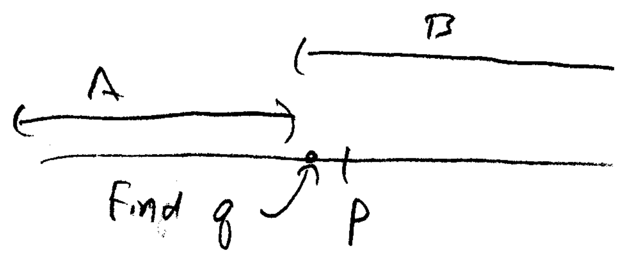


• $E = \mathbb{Q}$. $\sup E$ does not exist, because E is unbounded above. We say $\sup E = +\infty$.

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

Does this have a least upper bound (in $\mathbb{Q}$)?

No, $\sup A$ does not exist! (in $\mathbb{Q}$; say we're pre-1872).



Proof: Suppose for sake of contradiction that p is a least upper bound for A.

Let $B = \{x \in \mathbb{Q} : x^2 > 2\}$.

Question: Can we find a smaller upper bound q?

Intuition: Between $\sqrt{2}$ and p
which "doesn't exist" yet.

Better: Define $q = p - \frac{p^2 - 2}{p+2} = \frac{2p+2}{p+2}$. (*)

This means that $q^2 - 2 = \frac{2(p^2-2)}{(p+2)^2}$. (**)

• Suppose $p \in B$. Then $p^2 - 2 > 0$, so (*) implies $q > p$.

Now, (**) implies that $q^2 - 2 > 0$, so $q \in B$.

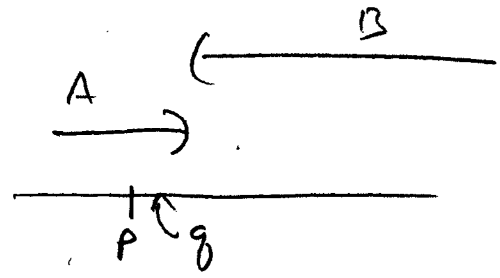
We have produced a smaller upper bound for A.

- Thus, it must be that $p \in A$, so $p^2 - 2 < 0$.

  Now, by (*), $q = p - \frac{p^2-2}{p+2} > p$.

  But by (**), $q^2 - 2 < 0$, so $q \in A$.

  This contradicts the assumption that q was an upper bound for A.



Thus, $A \subset \mathbb{Q}$ has no supremum. $\square$

Next: We'll construct $\mathbb{R}$ involving only $\mathbb{Q}$, and prove:

Theorem (Rudin 1.19) $\mathbb{R}$ is an ordered field with the l.u.b. property and contains $\mathbb{Q}$ as a subfield.

Def: A set S has the lub property (or satisfies the "completeness axiom") if every nonempty subset of S that has an upper bound also has a least upper bound (lub, or sup) in S.

Dedekind: A cut α is a subset of $\mathbb{Q}$ s.t.

1. $\alpha \neq \emptyset$ and $\alpha \neq \mathbb{Q}$ [nontrivial]
2. If $p \in \alpha$, $q \in \mathbb{Q}$, $q < p$, then $q \in \alpha$. [closed downwards]
3. If $p \in \alpha$, then $p < r$ for some $r \in \alpha$. [no largest element].

4

Ex: • The set A is not a cut (fails ②).

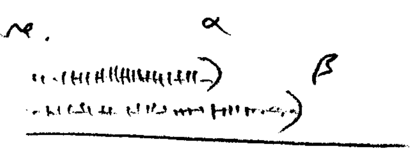
• $\alpha = \mathbb{Q}^-$ is a cut.

• $\beta = \{r \in \mathbb{Q} : r \leq 2\}$ is not a cut (fails ③).

Idea: Look at the set of all cuts, and declare those to be the real numbers.

Def: Let $\boxed{\mathbb{R} = \{\alpha : \alpha \text{ is a cut}\}}$.

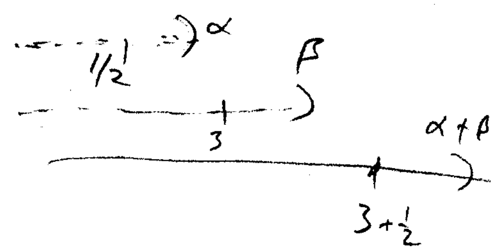
Need to show this set has some structure.



Define: • order $\boxed{\alpha < \beta \text{ means } \alpha \subsetneq \beta}$

(easy to check that this is an order: trichotomy ✓ transitivity ✓)

* addition: $\alpha + \beta := \{r+s : r \in \alpha, s \in \beta\}$.



check: Is a cut?

nontrivial (check)

closed downwards: If $p \in \alpha+\beta$, say $q < r+s$ $(r \in \alpha, s \in \beta)$.

Why is $q \in \alpha + \beta$? Note: $q - s < r \in \alpha$, so $q - s \in \alpha$.

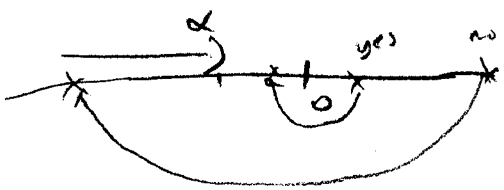
Thus $q = (q-s) + s \in \alpha + \beta$, as desired. ✓

Show axioms (A1)–(A5) for addition (most left as exercises).

- Add. <u>identity</u>: 0^* is $\mathbb{Q}_-$, neg. rationals.

  Check: $\alpha + 0^* = \alpha$. To verify show $\overbrace{\alpha + 0^* \subset \alpha \text{ and } \alpha \subset \alpha + 0^*}^{\text{explain.}}$

- Add. <u>inverse</u> for α:



<u>Hint</u>: Define $\beta = \{p : \exists r > 0 \text{ s.t. } -p - r \notin \alpha\}$.

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

* <u>Multiplication</u>:

  If $\alpha, \beta \in \mathbb{R}^+$ (i.e., $\alpha, \beta > 0^*$), define

  $$\alpha\beta = \{p \in \mathbb{Q} : p < rs \text{ for some } r \in \alpha,\ s \in \beta,\ r, s > 0\}.$$

  Let $1^* = \{q \in \mathbb{Q} : q < 1\}$.

  <u>Negative reals</u>: not quite as obvious, but similar (exercise).

Need to show axioms (M1)–(M5) for multiplication and (D) for distributive property.

We conclude that $\mathbb{R}$ is a <u>field</u>.

Additionally, we claim that $\mathbb{R}$ is an <u>ordered</u> field, i.e, order is preserved by $+$, $\times$. (Verbal explanation).

- Also, $\mathbb{R}$ <u>contains</u> $\mathbb{Q}$ as a subfield ($\mathbb{R}$ "extends" $\mathbb{Q}$).

Associate to $q \in \mathbb{Q}$ the cut $q^* = \{r \in \mathbb{Q} : r < q\}$.

This shows how $\mathbb{Q}$ is embedded in $\mathbb{R}$

Check: $f : \mathbb{Q} \longrightarrow \mathbb{R}$
$q \longmapsto q^*$

This map is clearly 1-1, and it also preserves $+$, $*$, order.

That is,
$$(r+s)^* = r^* + s^*$$
$$(rs)^* = r^* s^*$$
$$r < s \Rightarrow r^* < s^*.$$

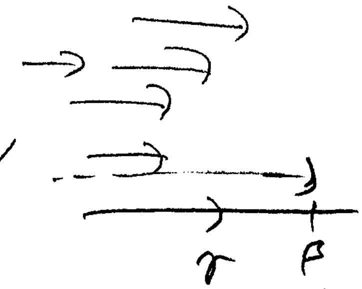
Thus, $\mathbb{Q}^* := \{q^* : q \in \mathbb{Q}\}$ is a <u>subfield</u> of $\mathbb{R}$.

<u>Notice</u>: The length "$\sqrt{2}$" sits in $\mathbb{R}$ as $\gamma = \{q : q^2 < 2, \text{ or } q < 0\}$.

<u>Check</u> (Using def'n of mult) that $\gamma^2 = 2^*$.

* $\mathbb{R}$ has the least upper bound (lub) property.

If A is a collection of cuts, with upper bound β, let $\gamma = \bigcup \{\alpha : \alpha \in A\}$, which is a subset of $\mathbb{Q}$

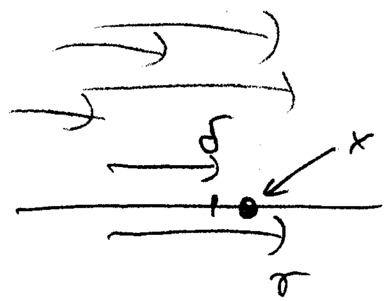


Check: γ is a cut, and $\gamma = \sup A$.

γ nonempty? ✓ closed downwards? ✓

γ not everything? ✓ no largest element? ✓

- γ is an upper bound, clearly, since γ contains each $\alpha \in A$. ✓
- γ is a least upper bound because if $\delta < \gamma$, then there is some $x \in \gamma \setminus \delta$, so δ is not an upper bound for α, and hence not for A. ✓



Summary: We have an ordered field that extends $\mathbb{Q}$, and has the least upper bound property. (Rudin, Thm 1.19).

Fact: $\mathbb{R}$ is the only ordered field with the lub property.

"algebraic property"

$$\mathbb{Q} \subseteq \ldots \mathbb{A} \ldots \subseteq \mathbb{R} \subseteq \ldots \mathbb{C} \subseteq \ldots$$

⟵ to "small" to have lub property. ⟶ too big to be ordered

Consequence: length "$\sqrt{2}$" = $\sup\{1, 1.4, 1.41, 1.414, 1.4142, \ldots\}$.

More generally, define $a^{1/n} = \sup\{r \in \mathbb{Q} : r^n < a\}$, if this set is $\neq \emptyset$.

Check: $(a^{1/n})^n = a$. [Note: This fails if $a \leq 0$... why?]

Question: what restrictions should we impose on a, n?

$\neq 0$? >0? even/odd?

Greatest lower bound, or infimum, write $\inf A$.

HW: $\inf A = -\sup(-A)$.

- In $\mathbb{R}$, $\inf A$ exists if set is bounded below. [$\mathbb{R}$ has glb property].

Consequences of lub property

Thm 1.20(a)

- Archimedean property of $\mathbb{R}$: [holds for $\mathbb{Q}$ too]

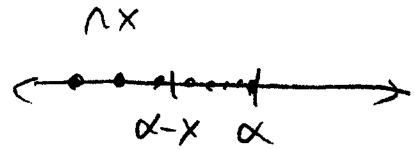
If $x, y \in \mathbb{R}$, $x > 0$, then $\exists$ pos. integer n s.t. $nx > y$.

Equiv: If $x > 0$, then $\exists x \in \mathbb{N}$ s.t. $\frac{1}{n} < x$.

Proof (by contradiction): Consider $A = \{nx : n \in \mathbb{N}\}$.

Suppose A were bounded by y (e.g., $nx < y \ \forall n \in \mathbb{N}$)

So A has a lub, call it α.



Then $\alpha - x$ is not an u.b. for A.

Hence $\alpha - x < mx$ for some $m \in \mathbb{N}$.

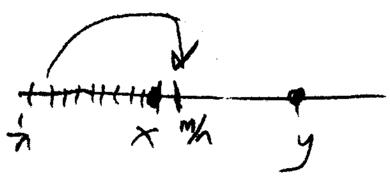
So $\alpha < (m+1)x$, so α is not an u.b. for A, ↯ □

Remark: $\mathbb{Q}$ has this property too, but this proof won't work. (Why?)

(1.20(b))

Theorem: Between any two $x, y \in \mathbb{R}$, $x < y$, $\exists\ q \in \mathbb{Q}$ s.t. $x < q < y$. [$\mathbb{Q}$ is dense in $\mathbb{R}$]

Proof: Choose n s.t. $\frac{1}{n} < y - x$ [Arch. prop.]



Consider multiples of $\frac{1}{n}$; these are unbounded [by Arch. prop.]

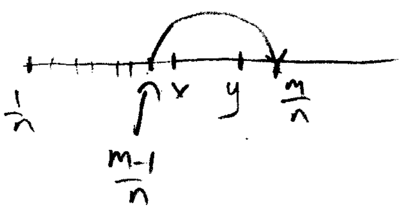
Choose the first multiple s.t. $\frac{m}{n} > x$.

Claim: $\frac{m}{n} < y$. If not, then $\underbrace{\frac{m-1}{n} < x \text{ and } \frac{m}{n} > y}$.

$$\Downarrow$$

$$-\frac{(m-1)}{n} > -x, \quad \frac{m}{n} > y$$

Impossible.



$$\Rightarrow \frac{m}{n} - \frac{(m-1)}{n} = \boxed{\frac{1}{n} > y - x}. \quad \checkmark$$

Contradiction! □

(10)

Properties of sup:

(a) r is an u.b. for $A \Leftrightarrow \sup A \le r$.

(b) $\forall a \in A,\ a \le r \Rightarrow \sup A \le r$. [Does $\Leftarrow$ hold? Yes]

(c) $\forall a \in A,\ a < r \Rightarrow \sup A \le r$. [ex: $A = \mathbb{R}^-$.]

(d) If $r < \sup A \Rightarrow \exists a \in A$ s.t. $r < a \le \sup A$.

(e) If $A \subset B$, then $\sup A \le \sup B$.

[Why? Use (a) or (b).

For all $a \in A$, $a \in B \Rightarrow a \le \boxed{\sup B} \xRightarrow{(b)} \sup A \le \boxed{\sup B}$

OR $A \subset B \Rightarrow \boxed{\sup B}$ is an u.b. for $A \xRightarrow{(a)} \sup A \le \boxed{\sup B}$

(f) To show $\sup A = \sup B$. [How?]

* One way: [Show $\forall a \in A,\ \exists b \in B$ s.t. $a \le b$.]

This shows $\sup A \le \sup B$.

Similar method for $\ge$.