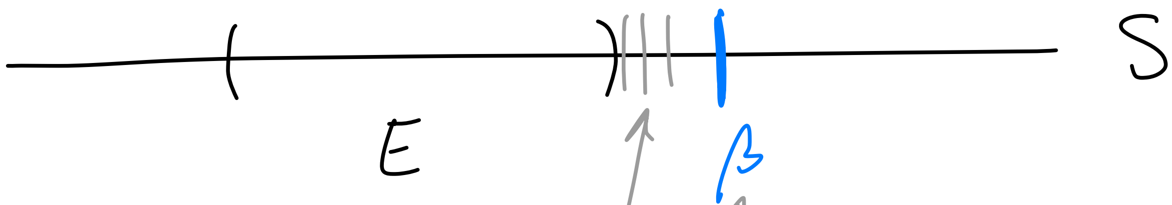
MAT320 Lecture 2 8/31/2020

Quick recap of Lecture 1:

$(S,<)$ ordered set, $E \subset S$ bounded from above:

$\exists \beta \in S$
$\forall x \in E,$
$x \leq \beta$



all of these are upper bounds for E

$\sup E$ = least upper bound for E

⚠ If $S = \mathbb{Q}$, then sup might not exist in S.

Analogously, if E is bounded from below:

all of these are lower bounds for E

$\exists \alpha \in S$
$\forall x \in E$
$\alpha \leq x$

$\inf E$ = largest lower bound for E.

⚠ Also inf's might not exist!

Example: Verify that $\mathbb{Z}_2 = \{0,1\}$ is a field with:

$+$	0	1
0	0	1
1	1	0

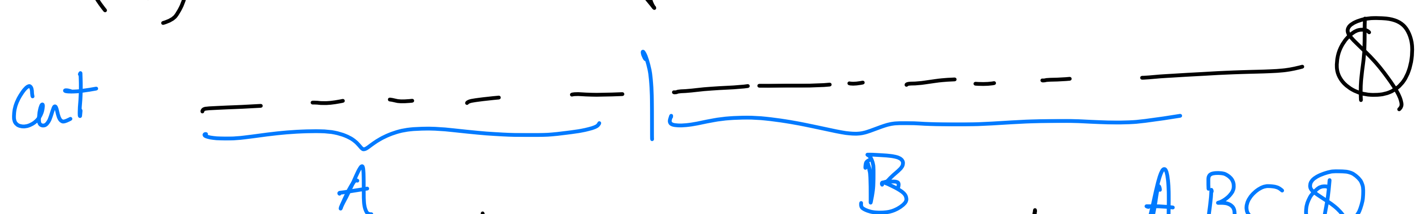
$\cdot$	0	1
0	0	0
1	0	1

The real numbers:

Recall (from Lecture 1:) i.e., every subset bounded from above has a supremum (note: get existence of inf from this "for free"!)

Thm: There exists a unique ordered field $\mathbb{R}$ which has the least-upper-bound property. Moreover, $\mathbb{R}$ contains $\mathbb{Q}$ as subfield.

Idea of proof: (1) Construction of $\mathbb{R}$: Dedekind cuts



$A, B \subset \mathbb{Q}$

$\mathbb{R} :=$ collection of all such cuts.

(2) Uniqueness: if $\mathbb{R}_1, \mathbb{R}_2$ are fields satisfying

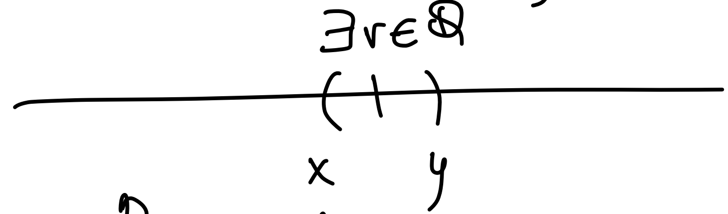
the above (ordered, w/ l.u.b. property), then $\exists \phi : \mathbb{R}_1 \longrightarrow \mathbb{R}_2$ an isomorphism of fields, i.e., ϕ preserves $+, \cdot$.

<u>Archimedean property</u>: $\forall x, y \in \mathbb{R}$, $x > 0$, $\exists n \in \mathbb{N}$ such that

$$nx > y.$$

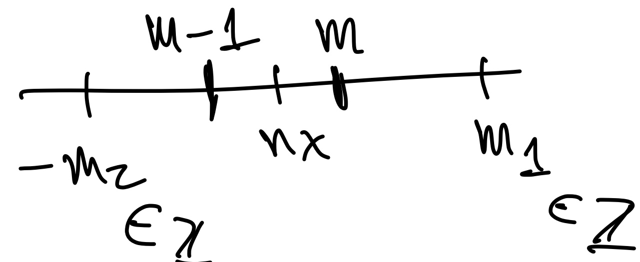
<u>Pf</u>: Given $x \in \mathbb{R}$, $x > 0$, let $A = \{ nx : n \in \mathbb{N} \}$. If the conclusion was false, then $\forall n \in \mathbb{N}$, $nx \le y$; which means that A is bounded from above. By the l.u.b property, $\exists \alpha = \sup A \in \mathbb{R}$. Since $x > 0$, $\alpha - x < \alpha$; so $\alpha - x$ is <u>not</u> an upper bound for A. Therefore $\exists m \in \mathbb{N}$ s.t. $\alpha - x < mx$. This means that $\alpha < \underbrace{(m+1)}_{\in \mathbb{N}} x \in A$. This contradiction finishes the proof. $\square$

<u>Theorem</u>: $\mathbb{Q}$ is "dense" in $\mathbb{R}$, i.e., $\forall x, y \in \mathbb{R}$, $x < y$
$\exists r \in \mathbb{Q}$, $x < r < y$.



<u>Pf</u>: Since $x < y$, we have $y - x > 0$. By Archimedean prop., $\exists n \in \mathbb{N}$ s.t. $n(y-x) > 1$. Again by Archimedean prop., $\exists m_1, m_2 \in \mathbb{N}$ s.t. $m_1 > nx$ and $m_2 > -nx$. Then

$$-m_2 < nx < m_1$$



Therefore $\exists m \in \mathbb{Z}$, s.t.

$$m - 1 \le nx < m$$

Putting the above together:

$$nx < m \le 1 + nx < ny$$

Divide by n: $x < \frac{m}{n} < y$. $(n \in \mathbb{N},\ m \in \mathbb{Z})$.

So we found $r = \frac{m}{n} \in \mathbb{Q}$ s.t. $x < r < y$. $\square$

<u>Existence of n^{th} root of any positive! real number, $\forall n \in \mathbb{N}$.</u>

<u>Lemma</u>: If $0 < a < b$, then $b^n - a^n < (b-a) n b^{n-1}$ for all $n \in \mathbb{N}$.

<u>Pf</u>: Recall $b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \dots + a^{n-1})$.

This can be proven by induction on n.

$0 < a < b \Rightarrow a^j b^{n-1-j} < b^{n-1}$, $\forall j = 1, \dots, n-1$

Thus: $b^n - a^n < (b-a)(\underbrace{b^{n-1} + b^{n-1} + \dots + b^{n-1}}_{n}) = (b-a) n b^{n-1}$.

$\square$

Thm: For all $x \in \mathbb{R}$, $x > 0$, and $n \in \mathbb{N}$ there exists a unique $y \in \mathbb{R}$, s.t. $y > 0$ and $y^n = x$

(Notation: $y = \sqrt[n]{x} = x^{1/n}$)

Pf: (Uniqueness). If $y_1, y_2 \in \mathbb{R}$ satisfied $y_1^n = x = y_2^n$, then $y_1 = y_2$. If not: $y_1 < y_2$ or $y_1 > y_2$.

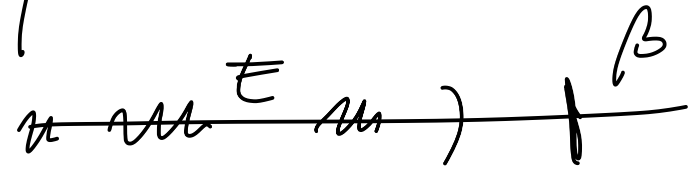
$$\begin{array}{ccc} y_1 < y_2 & & y_1 > y_2 \\ \Downarrow & & \Downarrow \\ y_1^n < y_2^n & & y_1^n > y_2^n \\ \text{(contradiction)} & & \text{(contradiction)} \end{array}$$

(Existence). To define $y \in \mathbb{R}$ we shall use the l.u.b. property of $\mathbb{R}$

Let $E = \{t \in \mathbb{R} : t > 0 \text{ and } t^n < x\}$

(1) <u>$E \neq \emptyset$</u>: Set $t = \dfrac{x}{1+x} \in \mathbb{R}$, note $0 < t < 1$. Also, $t^n < t < x$. Thus, $t = \dfrac{x}{1+x} \in E$.

(2) <u>E is bounded from above</u>: If $t > 1 + x$, then $t^n > t > x$ so $t \notin E$. Thus $\beta = 1 + x$ is an upper bound for E.



By the l.u.b.-property, $\exists\, y := \sup E \in \mathbb{R}$.

Now we show $y^n = x$. If not, then either

$y^n < x$ or $y^n > x$.

If $y^n < x$; then choose $h \in \mathbb{R}$ s.t. $0 < h \leq 1$ and

$h \leq \dfrac{x - y^n}{n(y+1)^{n-1}}$; e.g., $h = \min\left\{1, \dfrac{x-y^n}{n(y+1)^{n-1}}\right\}$

Set $a = y$, $b = y+h$ in the Lemma: $(0<a<b)$

$b^n - a^n < (b-a)\,n\,b^{n-1}$

$(y+h)^n - y^n < (y+h-y).n.(y+h)^{n-1} = hn(y+h)^{n-1}$

$\underset{(h \leq 1)}{\leq} hn(y+1)^{n-1} \leq x - y^n$

$$\Rightarrow \quad \underbrace{(y+h)^n}_{\in E} < x, \qquad y+h > y = \sup E.$$

contradicts $y = \sup E$.
(in particular, y is an upper bound for E)

If $y^n > x$: Set $k = \dfrac{y^n - x}{n y^{n-1}}$, note $0 < k < y$.

If $t \geq y - k$, then by the Lemma:

$$y^n - t^n \leq \underbrace{y^n}_{= b} - (\underbrace{y-k}_{= a})^n < \underbrace{n k y^{n-1}}_{n(b-a)b^{n-1}} = y^n - x.$$

Thus $t^n > x$; in particular, $t \notin E$.

Therefore $y-k$ is an upper bound for E.
This contradicts the fact that $y = \sup E$ is the <u>least</u> upper bound for E.
Hence $y^n = x$, completing the proof. $\square$.

<u>Extensions of real numbers:</u>

(1) "Extended" real line: $\overline{\mathbb{R}} := \mathbb{R} \cup \{+\infty, -\infty\}$.

Define $-\infty < x < +\infty$, $\forall x \in \mathbb{R}$, with the "intuitive" definitions for arithmetic operations with $\pm\infty$:

$$x + \infty = +\infty, \quad x - \infty = -\infty, \quad \frac{x}{\pm\infty} = 0.$$

⚠ $\overline{\mathbb{R}}$ is <u>not</u> a field.

(2) Complex numbers $\mathbb{C} = \mathbb{R} \oplus \mathbb{R} = \mathbb{R}^2$

$x = (a, b)$, $y = (c, d) \in \mathbb{C}$ $\quad a, b, c, d \in \mathbb{R}$

$x + y := (a + c, b + d)$, $x \cdot y := (ac - bd, ad + bc)$

It can be shown that $\mathbb{C}$ is a <u>field</u>.

However, $\mathbb{C}$ is <u>not</u> ordered. (Hint: $i := (0, 1) \in \mathbb{C}$
$i^2 = (-1, 0)$)
$(= -1 \in \mathbb{R})$

(3) Cayley-Dickson construction

$\mathbb{C} = \mathbb{R} \oplus \mathbb{R}$, $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}$, $\mathbb{C}a = \mathbb{H} \oplus \mathbb{H}$

"Quaternions" (not a field!) "Octonions" (not a field!)