Math 600 Lecture 2

Does $\mathbb{Z}$, with the usual order, satisfy the least-upper-bound property?

Definition: Let S be an ordered set and let $E \subset S$ be nonempty.

We say that E is <u>well ordered</u> iff every nonempty subset of E contains a smallest element $\left(\forall A \subseteq E,\ A \neq \emptyset \Rightarrow \left(\exists x \in A\ \forall y \in A,\ x \leq y \right) \right)$

We assume that the definitions and basic properties of rings, integral domains, and fields are known (see handout).

Definition: An ordered field (ring) F is a field (ring) that is an ordered set and in which

- $\alpha, \beta, \gamma \in F$ and $\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$
- $\alpha, \beta \in F$ and $\alpha > 0$ and $\beta > 0 \Rightarrow \alpha\beta > 0$.

We say that $\alpha \in F$ is <u>positive</u> iff $\alpha > 0$.

Theorem: Let F be an ordered field and let $\alpha, \beta, \gamma \in F$. Then

1. $\alpha > 0 \Leftrightarrow -\alpha < 0$
2. $\alpha > 0$ and $\beta < \gamma \Rightarrow \alpha\beta < \alpha\gamma$
3. $\alpha, \beta, \gamma, \delta > 0$ and $\alpha < \beta$ and $\gamma < \delta \Rightarrow \alpha\gamma < \beta\delta$
4. $\alpha < 0$ and $\beta < \gamma \Rightarrow \alpha\beta > \alpha\gamma$
5. $\alpha \neq 0 \Rightarrow \alpha^2 > 0$
6. $1 > 0$
7. $0 < \alpha < \beta \Rightarrow 0 < \frac{1}{\beta} < \frac{1}{\alpha}$

Also: $\alpha, \beta, \gamma, \delta \in F$ and $\alpha < \beta$ and $\gamma < \delta \Rightarrow \alpha + \gamma < \beta + \delta$.

Proof: 1. Suppose $\alpha > 0$. Then

$$\begin{aligned} & 0 < \alpha \\ \Rightarrow\ & 0 + (-\alpha) < \alpha + (-\alpha) && \text{(by definition of ordered field)} \\ \Rightarrow\ & -\alpha < 0, && \text{(by definition of } 0, -\alpha) \end{aligned}$$

as desired.

2. We have

$$\begin{aligned} \beta < \gamma \Rightarrow\ & \beta + (-\beta) < \gamma + (-\beta) && \text{(by definition of ordered field)} \\ \Rightarrow\ & 0 < \gamma - \beta && \text{(by definitions of } -\beta\text{, subtraction)} \\ \Rightarrow\ & 0 < \alpha(\gamma - \beta) && \text{(by definition of ordered field)} \\ \Rightarrow\ & 0 < \alpha\gamma - \alpha\beta && \text{(distributive laws)} \\ \Rightarrow\ & 0 + \alpha\beta < \alpha\gamma - \alpha\beta + \alpha\beta && \text{(by definition of ordered field)} \\ \Rightarrow\ & \alpha\beta < \alpha\gamma && \text{(by definition of } 0, -\alpha\beta), \end{aligned}$$

as desired.

3. We have (since $\alpha, \delta > 0$)

$$\gamma < \delta \Rightarrow \alpha\gamma < \alpha\delta \text{ and } \alpha < \beta \Rightarrow \alpha\delta < \beta\delta.$$

But then

$$\alpha\gamma < \alpha\delta \text{ and } \alpha\delta < \beta\delta \Rightarrow \alpha\gamma < \beta\delta.$$

4. Since $\alpha < 0$, we know that $-\alpha > 0$; thus

$$\begin{aligned} \beta < \gamma \Rightarrow\ & (-\alpha)\beta < (-\alpha)\gamma && \text{(by the previous result)} \\ \Rightarrow\ & -\alpha\beta < -\alpha\gamma && \text{(by general field properties)} \\ \Rightarrow\ & 0 < \alpha\beta - \alpha\gamma && \text{(by definition of ordered field)} \\ \Rightarrow\ & \alpha\gamma < \alpha\beta. && \text{(by definition of ordered field)} \end{aligned}$$

5. We know that

$$(-\alpha)^2 = (-\alpha)(-\alpha) = \alpha^2 \quad \text{(property of fields)}$$

and

$$\alpha > 0 \Rightarrow \alpha \cdot \alpha > 0 \Rightarrow \alpha^2 > 0 \quad \text{(by definition of ordered field)},$$

$$-\alpha > 0 \Rightarrow (-\alpha)(-\alpha) > 0 \Rightarrow \alpha^2 > 0 \quad (\text{" \quad " \quad " \quad " \quad "}).$$

Thus, if $\alpha \neq 0$, then $\alpha^2 > 0$.

6. By the definition of a field, $1 \neq 0$, and hence $1 = 1^2 > 0$ by the previous result.

7. Assume $\alpha, \beta > 0$. If $\gamma \leq 0$, then $-\gamma \geq 0$ and hence

$$\alpha(-\gamma) \geq 0 \Rightarrow -\alpha\gamma \geq 0 \Rightarrow \alpha\gamma \leq 0.$$

Thus $\alpha(\alpha^{-1}) = 1 > 0$ implies that $\alpha^{-1} > 0$. Similarly, $\beta^{-1} > 0$. Thus

$$\begin{aligned} \alpha < \beta &\Rightarrow \alpha^{-1}\alpha < \alpha^{-1}\beta && \text{(by 2)} \\ &\Rightarrow 1 < \alpha^{-1}\beta && \text{(by definition of } \alpha^{-1}) \\ &\Rightarrow 1 \cdot \beta^{-1} < \alpha^{-1}\beta\beta^{-1} && \text{(by 2)} \\ &\Rightarrow \beta^{-1} < \alpha^{-1}, && \text{(by definition of } 1, \beta^{-1}) \end{aligned}$$

as desired. //

Now we can state our assumptions (the foundations for this course):

- $\mathbb{Z}$ is an ordered integral domain in which $\mathbb{Z}^+$ is well ordered. (Moreover, if D is an ordered integral domain and D^+ is well ordered, then D is isomorphic to $\mathbb{Z}$.)

- $\mathbb{R}$ is an ordered field that satisfies the least-upper-bound property. (Moreover, if F is an ordered field that satisfies the least-upper-bound property, then F is isomorphic to $\mathbb{R}$.)

Interestingly, it is not as easy to characterize $\mathbb{Q}$. We can <u>define</u> $\mathbb{Q}$ as the <u>field of quotients</u> of $\mathbb{Z}$. Or we can say that $\mathbb{Q}$ is the smallest ordered field containing $\mathbb{Z}$ as a subring (i.e. if F is an ordered field that contains $\mathbb{Z}$ as a subring, then $\mathbb{Q} \subset F$).

Basic properties of $\mathbb{R}$

<u>Theorem</u> (Archimedean property of $\mathbb{R}$): If $x, y \in \mathbb{R}$ and $x > 0$, then there exists $n \in \mathbb{Z}^+$ such that $nx > y$.

<u>Proof:</u> We argue by contradiction and assume that $nx \leq y$ for all $n \in \mathbb{Z}^+$. It follows that

$$E = \{nx \mid n \in \mathbb{Z}^+\}$$

is bounded above. Hence $\alpha = \sup E$ exists. Since $x > 0$, $\alpha - x < \alpha$ and hence $\alpha - x$ is not an upper bound of E. Choose $n \in \mathbb{Z}^+$ such that $nx > \alpha - x$. But then

$$nx + x > \alpha \Rightarrow (n+1)x > \alpha$$

and $(n+1)x \in E$, contradicting that α is an upper bound for E. Thus E cannot be bounded above, and the proof is complete. //

<u>Theorem</u>: Suppose $x, y \in \mathbb{R}$ and $x < y$. Then there exists $r \in \mathbb{Q}$ such that $x < r < y$.

Proof: Since $x<y$, $y-x>0$ and hence, by the previous theorem, there exists $n\in\mathbb{Z}^+$ such that

$$n(y-x)>1 \iff \frac{1}{n}<y-x.$$

Recall that $\frac{1}{n}>0$; hence there exists $k\in\mathbb{Z}^+$ such that $\frac{k}{n}=k\cdot\frac{1}{n}>x$;

let m be the largest nonnegative integer such that

How do we know (precisely) that such an m exists?

$$\frac{m}{n}\leq x.$$

Then, by definition of m,

$$\frac{m+1}{n}=\frac{m}{n}+\frac{1}{n}>x$$

and

$$\frac{m+1}{n}=\frac{m}{n}+\frac{1}{n}<x+(y-x)=y \quad \left(\text{since } \frac{m}{n}\leq x \text{ and } \frac{1}{n}<y\right).$$

Thus $x<\frac{m+1}{n}<y$, as desired. //

Theorem: If $x\in\mathbb{R}^+$ and $n\in\mathbb{Z}^+$, then there exists a unique $y\in\mathbb{R}^+$ such that $y^n=x$.

Proof: If $0<y_1<y_2$, then $0<y_1^n<y_2^n$ (why?). This shows that there is at most one such y.

Now, define $E=\{t\in\mathbb{R}^+ \mid t^n\leq x\}$. Note that

$$t=\frac{x}{1+x} \Rightarrow t^n<t<x,$$

which shows that $E \neq \emptyset$. Also,

$$s = x+1 \Rightarrow s^n > s > x \Rightarrow s \notin E.$$

It follows that E is bounded above $(t > s \Rightarrow t^n > s^n > x \Rightarrow t \notin E)$. Thus, by the least-upper-bound property, $y = \sup E$ exists.

It remains to prove that $y^n = x$. We argue by contradiction.

<u>Case 1</u>: $y^n < x$. To obtain a contradiction, we will find $h > 0$ such that $(y+h)^n < x$. Then $y+h \in E$ and $y+h > y$, contradicting that $y = \sup E$.

Note that

Using the identity
$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$

$$
\begin{aligned}
& (y+h)^n < x \\
\Leftrightarrow\ & (y+h)^n - y^n < x - y^n \\
\Leftrightarrow\ & (y+h-y)\left((y+h)^{n-1} + (y+h)^{n-2}y + \cdots + (y+h)y^{n-2} + y^{n-1}\right) < x - y^n \\
\Leftarrow\ & h\,n(y+h)^{n-1} < x - y^n \\
\Leftrightarrow\ & h < \frac{x-y^n}{n(y+h)^{n-1}} \\
\Leftarrow\ & h < \frac{x-y^n}{n(y+1)^{n-1}} \text{ and } 0 < h < 1.
\end{aligned}
$$

Since there exists h such that

$$0 < h < \min\left\{\frac{x-y^n}{n(y+1)^{n-1}}, 1\right\},$$

this yields the desired contradiction.

Case 2: $y^n > x$. To obtain a contradiction, we will find $h>0$ such that $(y-h)^n > x$. Then $y-h$ is an upper bound for E and $y-h<y$, a contradiction. We have

$$(y-h)^n > x$$

$$\iff (y-h)^n - y^n > x - y^n$$

$$\iff y^n - (y-h)^n < y^n - x$$

$$\iff (y-(y-h))\left(y^{n-1} + y^{n-2}(y-h) + \cdots + y(y-h)^{n-2} + (y-h)^{n-1}\right) < y^n - x$$

$$\Longleftarrow \quad h n y^{n-1} < y^n - x$$

$$\iff h < \frac{y^n - x}{n y^{n-1}}.$$

Since there clearly exists h satisfying $0 < h < \frac{y^n-x}{ny^{n-1}}$, this yields the contradiction. //

For $x>0$, $n \in \mathbb{Z}^+$, we write

$$y = x^{1/n} \iff y>0 \text{ and } y^n = x.$$

By the previous theorem, $x^{1/n}$ is well defined (the <u>positive</u> nth root of x).