# Math 600 Lecture 1

**Prove**: If $x, y \in \mathbb{R}$ and $x < y$, then there exists a rational number $r$ such that

$$x < r < y.$$

(For convenience, you can assume that $0 < x < y$.)

---

The purpose of analysis is to discover theorems (such as the above statement) and to rigorously prove them. To give a rigorous (i.e. logically sound) proof, it is necessary to state the foundations (undefined terms and axioms) clearly. That is the purpose of this introduction.

<u>Set</u> and <u>element of a set</u> are undefined terms. Informally, a set $S$ is a collection of objects that are called the elements of $S$. We write $x \in S$ to indicate that $x$ is an element of $S$ and $x \notin S$ to indicate that $x$ is not an element of $S$.

$A \subset B$ ($A$ is a subset of $B$) means every element of $A$ is also an element of $B$. Thus $A \subset B$ means

$$x \in A \Rightarrow x \in B$$

or

$$\forall x \in A, x \in B.$$

By definition,

$$A = B \Longleftrightarrow (A \subset B \wedge B \subset A).$$

That is,

$$A = B \Longleftrightarrow (x \in A \Longleftrightarrow x \in B).$$

If $A \subset B$ and $A \neq B$, we say that $A$ is a <u>proper subset</u> of $B$.

<u>Examples</u>

- $\mathbb{Z}$ = the set of all integers $= \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is a set.

  $\mathbb{Z}^+$ = the set of positive integers $= \{1, 2, 3, \ldots\}$ is a subset of $\mathbb{Z}$.
- $\mathbb{Q}$ = the set of rational numbers $= \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$ is a set.

  $\mathbb{Q}^+$ = the set of positive rational numbers

  $= \{\frac{m}{n} : m, n \in \mathbb{Z},\ m, n \text{ are both positive}\}$ is a subset of $\mathbb{Q}$.

<u>Definition</u>: Let $S$ be a set. An <u>order</u> on $S$ is a relation, denoted by $<$, satisfying

(1) If $x, y \in S$, then exactly one of the following is true:

$$x < y \text{ or } x = y \text{ or } y < x$$

(trichotomy law);

(2) If $x, y, z \in S$, then

$$(x < y) \wedge (y < z) \Rightarrow x < z.$$

(What is a relation? If $S$ is a set, a relation $R$ on $S$ is just a subset of $S \times S$. We usually choose a binary symbol such as $\sim$ and write $x \sim y$ to mean $(x,y) \in R$.)

An <u>ordered set</u> is a set on which an order is defined.

Note that $x \leq y$ is shorthand for "$x < y$ or $x = y$".

<u>Example</u>: We can define an order on $\mathbb{Z}$ by

$$m < n \iff n - m \in \mathbb{Z}^+.$$

Assuming that, for all $p \in \mathbb{Z}$, exactly one of

$$p \in \mathbb{Z}^+ \text{ or } p = 0 \text{ or } -p \in \mathbb{Z}^+$$

*

holds, it follows that, given $m, n \in \mathbb{Z}$, exactly one of

$$n - m \in \mathbb{Z}^+ \text{ or } n - m = 0 \text{ or } -(n-m) \in \mathbb{Z}^+$$

holds. Equivalently, exactly one of

$$m < n \text{ or } m = n \text{ or } n < m$$

holds.

Also,

$$\begin{aligned} k < m \wedge m < n &\Rightarrow m - k, n - m \in \mathbb{Z}^+ \\ &\overset{*}{\Rightarrow} m - k + n - m \in \mathbb{Z}^+ \\ &\Rightarrow n - k \in \mathbb{Z}^+ \\ &\Rightarrow k < n. \end{aligned}$$

Thus $<$ is a valid order on $\mathbb{Z}$.

* Note that we are relying on familiar properties of $\mathbb{Z}$.

**Definition** Let $S$ be an ordered set and suppose $E \subset S$. If there exists $\beta \in S$ such that

$$x \le \beta \quad \forall x \in E,$$

then we say that $E$ is bounded above and that $\beta$ is an upper bound for $E$. If $E$ is bounded above, $\alpha$ is an upper bound for $E$, and

$$\beta \text{ is an upper bound for } E \Rightarrow \alpha \le \beta,$$

then we say that $\alpha$ is the least upper bound or supremum of $E$ and write

$$\alpha = \sup E.$$

(Bounded below, lower bound, greatest lower bound, and infimum are defined analogously.)

**Example**: Let $E = \{x \in \mathbb{Q}^+ \mid x^2 < 2\}$. Then $E$ is bounded above. For example, $1.5$ is an upper bound for $E$:

$$x \ge 1.5 \Rightarrow x^2 \ge 2.25 > 2 \Rightarrow x \notin E.$$

$$\left[ (x \ge 1.5 \Rightarrow x \notin E) \Longleftrightarrow (x \in E \Rightarrow x < 1.5) \Longleftrightarrow (x < 1.5 \ \forall x \in E) \right]$$

However, $E$ has no least upper bound in $\mathbb{Q}^+$.

**Proof** (sketch): Suppose $\alpha \in \mathbb{Q}^+$ is the least upper bound for $E$. Then $\alpha^2 = 2$ must hold (If $\alpha^2 < 2$, there exists $\beta \in \mathbb{Q}^+$ such that $\alpha^2 < \beta^2 < 2$, so $\alpha$ is not an upper bound. If $\alpha^2 > 2$, there exists $\beta \in \mathbb{Q}^+$ such that $2 < \beta^2 < \alpha^2$, so $\alpha$ is not the least upper bound. See text, page 2.) But no rational number $\alpha$ satisfies $\alpha^2 = 2$. //

Definition: Let $S$ be an ordered set. We say that $S$ satisfies the least-upper-bound property iff

$$E \subset S,\ E \neq \emptyset,\ E \text{ bounded above} \Longrightarrow \sup E \text{ exists in } S.$$

Note that the previous example proves that $\mathbb{Q}$ does not satisfy the least-upper-bound property.

Theorem: Suppose $S$ is an ordered set that satisfies the least-upper-bound property, $E \subset S$ is nonempty, and $E$ is bounded below. If $L$ is the set of all lower bounds of $E$, then $\alpha = \sup L$ exists in $S$ and $\alpha = \inf E$.

Proof: For all $x \in L$, $x \leq y$ for all $y \in E$. In other words, if $y \in E$, then $x \leq y$ for all $x \in L$. Thus every $y \in E$ is an upper bound for $L$. Since $E$ is nonempty, it follows that $L$ is bounded above and hence $\alpha = \sup L$ exists in $S$. Note that $\alpha \leq x$ for all $x \in E$, since we already know that every $x \in E$ is an upper bound for $L$, and $\alpha$ is the least upper bound of $L$. Thus $\alpha$ is a lower bound for $E$. Moreover, every lower bound $\beta$ of $E$ belongs to $L$, and $\alpha$ is an upper bound for $L$. Thus $\beta \leq \alpha$ for all lower bounds $\beta$ of $E$, and hence $\alpha = \inf E$. //

Corollary: If $S$ is an ordered set that satisfies the least-upper-bound property, then $S$ satisfies the greatest-lower-bound property.

<u>Definition</u>: Let $S$ be an ordered set and let $E \subset S$ be nonempty. We say that $E$ is <u>wellordered</u> iff every nonempty subset of $E$ contains a smallest element $(\forall A \subseteq E, A \neq \emptyset \Rightarrow (\exists x \in A \ \forall y \in A, x < y))$.

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

<u>Definition</u>: 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 $\alpha > 0$.

<u>Theorem</u>: 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. $\alpha < 0$ and $\beta < \gamma \Rightarrow \alpha\beta > \alpha\gamma$
4. $\alpha \neq 0 \Rightarrow \alpha^2 > 0$
5. $1 > 0$
6. $0 < \alpha < \beta \Rightarrow 0 < \frac{1}{\beta} < \frac{1}{\alpha}$

<u>Proof</u>: 1. Suppose $\alpha > 0$. Then

$$0 < \alpha$$

$$\Rightarrow 0 + (-\alpha) < \alpha + (-\alpha) \quad \text{(by definition of ordered field)}$$

$$\Rightarrow -\alpha < 0, \quad \text{(by definition of } 0, -\alpha\text{)}$$

as desired.

2. We have

$$\beta < \gamma \Rightarrow \beta + (-\beta) < \gamma + (-\beta) \quad \text{(by definition of ordered field)}$$

$$\Rightarrow 0 < \gamma - \beta \quad \text{(by definitions of } -\beta \text{, subtraction)}$$

$$\Rightarrow 0 < \alpha(\gamma - \beta) \quad \text{(by definition of ordered field)}$$

$$\Rightarrow 0 < \alpha\gamma - \alpha\beta \quad \text{(distributive law)}$$

$$\Rightarrow 0 + \alpha\beta < \alpha\gamma - \alpha\beta + \alpha\beta \quad \text{(by definition of ordered field)}$$

$$\Rightarrow \alpha\beta < \alpha\gamma \quad \text{(by definition of } 0, -\alpha\beta\text{),}$$

as desired.

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

$$\beta < \gamma \Rightarrow (-\alpha)\beta < (-\alpha)\gamma \quad \text{(by the previous result)}$$

$$\Rightarrow -\alpha\beta < -\alpha\gamma \quad \text{(by general field properties)}$$

$$\Rightarrow 0 < \alpha\beta - \alpha\gamma \quad \text{(by definition of ordered field)}$$

$$\Rightarrow \alpha\gamma < \alpha\beta. \quad \text{(by definition of ordered field)}$$

4. We know that

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

and

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

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

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

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

6. 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

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

as desired. //