18.100A: Typed Lecture Notes

Lecture 4:
The Characterization of the Real Numbers

Question 1. *Last time we stated that $\mathbb{Q}$ was an example of a field, but what is a* ***field****?*

Definition 2 (Field)
A set F is a **field** if it has two operations: addition $(+)$ and multiplication $(\cdot)$ with the following properties.

A1) If $x, y \in F$ then $x + y \in F$.

A2) *(Commutativity)* $\forall x, y \in F$, $x + y = y + x$.

A3) *(Associativity)* $\forall x, y, z \in F$, $(x + y) + z = x + (y + z)$.

A4) $\exists$ an element $0 \in F$ such that $0 + x = x = x + 0$.

A5) $\forall x \in F$, $\exists y \in F$ such that $x + y = 0$. We denote $y = -x$.

M1) If $x, y \in F$, then $x \cdot y \in F$.

M2) *(Commutativity)* $\forall x, y \in F$, $x \cdot y = y \cdot x$.

M3) *(Associativity)* $\forall x, y, z \in F$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

M4) $\exists 1 \in F$ such that $1 \cdot x = x = x \cdot 1$ for all $x \in F$.

M5) $\forall x \in F \setminus \{0\}$, $\exists x^{-1}$ such that $x \cdot x^{-1} = 1$.

D) *(Distributativity)* $\forall x, y, z \in F$, $(x + y)z = xz + yz$.

These may seem like trivial properties, but consider the following non-example: $\mathbb{Z}$. $\mathbb{Z}$ fails M5)– multiplicative inverses do not exist in the integers.

Example 3
Here are two examples of fields:

1. $\mathbb{Z}_2 = \{0, 1\}$ where $1 + 1 = 0$.
2. $\mathbb{Z}_3 = \{0, 1, 2\}$ with $c := a + b \pmod 3$. In other words,

$$2 + 1 = 3 = 0 \pmod 3 \quad \text{and} \quad 2 \cdot 2 = 4 = 3 + 1 = 1 \pmod 3.$$

Simple properties follow from the properties of a field!

Theorem 4
If $x \in F$ where F is a field, $0x = 0$.

Proof: If $x \in F$, then

$$0 = 0 \cdot x - 0 \cdot x = (0+0) \cdot x - 0 \cdot x = 0 \cdot x + 0 \cdot x - 0 \cdot x = 0 \cdot x.$$

$\square$

Definition 5 (Ordered field)

A field F is an **ordered field** if F is also an ordered set with ordering $<$ and

i) $\forall x, y, z \in F$, $x < y \implies x + z < y + z$.

ii) If $x > 0$ and $y > 0$ then $xy > 0$.

If $x > 0$ we say x is **positive**, and if $x \geq 0$ we say x is **non-negative**.

Example 6

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

A non-example would be $\mathbb{Z}_2$. For instance, consider $0 < 1$. If $0 < 1$, then $1 + 0 < 1 + 1 = 0 \implies 1 < 0$ which is a contradiction. If $1 < 0$, then $0 = 1 + 1 < 0 + 1 \implies 0 < 1$ which is a contradiction. Hence, $\mathbb{Z}_2$ is not an ordered field.

Using the definition of an ordered field, one can easily prove all of the usual facts about inequalities.

Theorem 7

If $x > 0$, then $-x < 0$ (and vice versa).

Proof: If $x \in F$ and $x > 0$, then by i),

$$-x + x > -x \implies 0 > -x.$$

$\square$

One can see Proposition 1.1.8 **[L]** for a list of other simple inequality facts.

Theorem 8

Let $x, y \in F$ where F is an ordered field. If $x > 0$ and $y < 0$ or $x < 0$ and $y > 0$, then $xy < 0$.

Proof: Suppose $x > 0$ and $y < 0$. Then, $x > 0$ and $-y > 0$. Hence, $-xy = x(-y) > 0$. Thus, $xy < 0$. If $x < 0$ and $y > 0$, then $-x > 0$ and $y > 0 \implies -xy = (-x)y > 0 \implies xy < 0$. $\square$

Question 9. *Is there a greatest lower bound property?*

For an ordered field F, if F has the least upper bound property then F has a greatest lower bound property.

Theorem 10

Let F be an ordered field with the least upper bound property. If $A \subset F$ is nonempty and bounded below, then $\inf A$ exists in F.

Proof: Suppose $A \subset F$ is nonempty and bounded below, i.e. $\exists a \in F$ such that $\forall x \in A$, $a \leq x$. Let $B = \{-x \mid x \in A\}$. Then, $\forall x \in A$, $-x \leq -a \implies -a$ is an upper bound for B. Since F has the least upper bound property, $\exists c \in F$ such that $c = \sup B$. Then, $\forall x \in A$, $-x \leq c \implies \forall x \in A$, $-c \leq x$. Hence, $-c$ is a lower bound for A. We have also shown that if a is a lower bound for A, then $-a$ is an upper bound for B. Therefore, $c \leq -a$ since $c = \sup B \implies a \leq -c$. Hence, $-c$ is the greatest lower bound for A. $\square$

Real Numbers

Theorem 11

There exists a "unique" ordered field, labeled $\mathbb{R}$, such that $\mathbb{Q} \subset \mathbb{R}$ and $\mathbb{R}$ has the least upper bound property.

One can construct $\mathbb{R}$ using Dedekind cuts or as equivalence classes of Cauchy sequences. (We will define Cauchy sequences later in the course.)

Theorem 12

$\exists! r \in \mathbb{R}$ such that $r > 0$ and $r^2 = 2$. In other words, $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \notin \mathbb{Q}$.

Proof: Let $\tilde{E} = \{x \in \mathbb{R} \mid x > 0 \text{ and } x^2 < 2\}$. Then, since $\tilde{E}$ is bounded above (by 2 for instance), we have that $r := \sup \tilde{E}$ exists in $\mathbb{R}$. Then, one can show that $r > 0$ and $r^2 = 2$. This is left as an exercise.

We now prove uniqueness. Suppose that there is a $\tilde{r} > 0$ with $\tilde{r}^2 = 2$. Then, since $(r + \tilde{r}) > 0$,

$$0 = r^2 - \tilde{r}^2 = (r + \tilde{r})(r - \tilde{r}) \implies r - \tilde{r} = 0 \implies r = \tilde{r}.$$

$\square$

Remark 13. *In Assignment 2 Exercise 7, you will show that* $\sqrt[3]{2} \in \mathbb{R}$.