Lecture #2

4 Sep 2020
Lecture 2 (1)

- Zoom suggestions
- HW #1 is available.

Last time: defined a field $\mathbb{F}$ $(\mathbb{F}, +, \cdot, 0, 1)$
$0 \neq 1$

axioms: F1 $+, \cdot$ commutative
F2 $+, \cdot$ associative
F3 $0, 1$ additive, mult. identity
F4 $\exists$ additive inverse $(-a)$ any $a \in \mathbb{F}$.
$\exists$ mult. inverse $\frac{1}{a}$ $(a \neq 0)$
F5 distributive property

Question: is $0 \cdot a = 0$? (yes: prove it!)

In this course: when you are asked to prove that something is a field, don't need to prove F1, F2, F5. (but they need to hold!)

Examples of fields!

(1) $\mathbb{R}$ real numbers $(\mathbb{R}, +, \cdot, 0, 1)$
this is a field. Proof ??! We are going to assume this.
We can't prove it without a construction of $\mathbb{R}$.

(2) What about the rational numbers?

$\mathbb{Q} = \{ a \in \mathbb{R} : a = \frac{p}{q} , p,q \in \mathbb{Z} , q \neq 0 \}$

integers

this is a field. (will see why in a second)

<u>prop</u> If $A \subseteq \mathbb{F}$, $\mathbb{F}$ is a field, s.t.

(a) $0, 1 \in A$

(b) $a+b \in A \quad \forall a,b \in A$

(c) $a \cdot b \in A \quad \forall a,b \in A$.

then A satisfies [which of (F1)—(F5)? (breakout rooms)]

(F1), (F2), (F3), (F5) hold

and A is a field (with these ops) $\iff$ (F4) holds

$\mathbb{Q}$: is a field

$\mathbb{Z} = \{0,1,2,\ldots,-1,-2,\ldots\} \subseteq \mathbb{Q}$ has additive inverse
not a field. but $\frac{1}{2} \notin \mathbb{Z}$, no mult inverse.

$\mathbb{Q}_{\geq 0} = \{ a \in \mathbb{Q} : a \geq 0 \}$ no additive inverse

not fields.

$\mathbb{C} := \{a+bi : a,b \in \mathbb{R}\}$ $\{(a,b) : a,b \in \mathbb{R}\}$ "$\mathbb{C}$"

(idea : $i^2 = -1$)

define :

$(a+bi) + (c+di) = (a+c) + (b+d)i$

(really : $(a,b) + (c,d) = (a+c, b+d)$)

$(a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i$

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

0 element in $\mathbb{C}$ = $0 + 0i$ = $(0,0)$

1 element in $\mathbb{C}$ = $1 + 0i$ = $(1,0)$

think of $\mathbb{R} \subseteq \mathbb{C}$ if $a \in \mathbb{R}$, think of $a = a + 0 \cdot i$
$= (a,0)$

F1, F2, F5 brute force check.

F3 easy (needs to be checked).

F4 $-(a+bi) = (-a)+(-b)i$ $-(a,b) = (-a,-b)$.

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2}$$

$(a,b) \neq 0$

$$= \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$$

inverses exist.

<u>Prop</u> $\mathbb{C}$ is a field. (with these operations).

(solve : $x^2 = i$ for x). $\leftarrow$ try this

Next time : $\mathbb{F}_2$. $\leftarrow$ field with 2 elements?