Math 3340
Spring 2021
Lecture #24

Fields!

5 April 2021
Lecture #24

1

Question: what operations on numbers do we need to state / solve:

$$2x + 3y = 13$$
$$4x + 5y = 23 \quad ?$$

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ are all "possible scalars".

$+$, $-$

$\cdot$, $/$

get $-$ from $+$: $a-b$ same as $a+(-b)$

get $/$ from $\cdot$: a/b is the number s.t. $(a/b)\cdot b = a$

$(b \neq 0)$!

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ all have ops $+$, $\cdot$

$\mathbb{Z}$ does too

matrices too (square $n \times n$ matrices)

$\mathbb{N}$

$\mathbb{Z}_n$

5 April 2021
Lecture #24

Def (field, short form)

A field $(\mathbb{F}, +, \cdot)$ is a set $\mathbb{F}$, equipped with 2 binary operations $+ : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$

$$\cdot : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$$

satisfying:

(a) $(\mathbb{F}, +)$ is an Abelian group

Let $0 = 0_{\mathbb{F}}$ denote the identity elem for $+$.

(b) $(\mathbb{F} \setminus \{0\}, \cdot)$ is an Abelian group.

Let $1 = 1_{\mathbb{F}}$ denote the identity elem for $\cdot$.

(c) $\forall\, a, b, c \in \mathbb{F}$, then

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

(notation: $ab + ac = a(b + c)$)

Examples (you may assume these):

$\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are all fields

Long form definition

A field $(\mathbb{F}, +, \cdot)$ is a set $\mathbb{F}$ equipped with 2 binary ops s.t.

F1 (closure) $\forall\, a, b \in \mathbb{F}$, $a+b \in \mathbb{F}$, $a \cdot b \in \mathbb{F}$.

F2 (associativity) $\forall\, a, b, c \in \mathbb{F}$:

$$a + (b + c) = (a+b) + c$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

F3 (commutativity) $\forall\, a, b \in \mathbb{F}$

$$a + b = b + a$$

$$a \cdot b = b \cdot a$$

F4 (distributivity) $\forall\, a, b, c \in \mathbb{F}$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

F5 (identity elems)

$\exists$ element $0 \in \mathbb{F}$ s.t. $\forall\, a \in \mathbb{F}$, $a + 0 = a$

$\exists$ element $1 \in \mathbb{F}$ s.t. $\forall\, a \in \mathbb{F}$ $a \cdot 1 = a$

$\neq 0$

(not needed)

ALSO: $0 \neq 1$

F6 (inverses)

$\forall a \in \mathbb{F}, \exists x \in \mathbb{F}$ s.t. $a + x = 0$

(write this x as $-a$)

$\forall a \in \mathbb{F}, a \neq 0, \exists x \in \mathbb{F}$ s.t. $ax = 1$

(denote this x by $\frac{1}{a}$ or a^{-1})

Examples Let $\mathbb{F}_2 = \{0, 1\}$

can you find $+, \cdot$ on $\mathbb{F}_2$ that makes $\mathbb{F}_2$ into a field?

$+$	0	1
0	0	1
1	1	0

addition table

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

mult. table

(assuming: $0 \cdot a = 0 \quad \forall a \in \mathbb{F}$)

$1 + 1 = ??$

case 1 : $1 + 1 = 0$

must have

$\boxed{1 + 1 = 0}$

case 2 : $1 + 1 = 1$ X

$(1+1) + (-1) = 1 + (-1) = 0$

$(-1) = 1$

$1 + (1 + (-1))$
$\parallel$
1

but $1 \neq 0$ c!

5 April 2021
Lecture #24

Properties Let $\mathbb{F}$ be a field, $a, b, c \in \mathbb{F}$

ⓐ cancellation laws hold:

$$a + c = b + c \implies a = b$$

$$\left.\begin{array}{l} ac = bc \\ \text{AND } c \neq 0 \,!! \end{array}\right\} \implies a = b$$

ⓑ uniqueness of $0, 1$:

if $a + b = a$ then $b = 0$

$$\left.\begin{array}{l} \text{if } a \cdot c = a \\ (\text{AND } a \neq 0) \end{array}\right\} \implies \text{then } c = 1$$

ⓒ uniqueness of inverses!

if $a + b = 0$ then $b = -a$

if $a \cdot b = 1$ AND $a \neq 0$ then $b = \frac{1}{a}$ (or a^{-1})

5 April 2021
Lecture #24

Questions: For any field $\mathbb{F}$, $a, b \in \mathbb{F}$

1. is $a \cdot 0 = 0$?
2. What is $(-1)(-1) = ??$ (also $(-1)\cdot a = -a$)
3. if $a, b \neq 0$, can $ab = 0$? (think about this)

proofs

1. $$0 = 0 + 0 \quad (\text{since } 0 = \text{additive identity})$$

$$\therefore \; a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$$

add $-(a \cdot 0)$ to both sides

get
$$0 = a \cdot 0 + 0$$
$$\boxed{0 = a \cdot 0}$$

2. $$(-1)(-1) + (-1)\cdot 1$$
$$= (-1)((-1) + 1)$$
$$= (-1)\cdot 0 = 0$$

$$\therefore \; (-1)(-1) = -(-1) = 1 \; !$$

since $1 + (-1) = 0$

$$\therefore \; -(-1) = 1$$

$\therefore (-1)(-1) = 1$

Next time: $\mathbb{Z}_n$ when is this a field?

$\mathbb{Z}_4$ $\quad [2]_4 [2]_4 = [4]_4 = [0]_4$