Lecture #3

- Office hours are posted
  zoom links are on canvas
- fields
- vector spaces

Fields

Example $\mathbb{F}_2$: a field with 2 elements

give $+$, $\cdot$ say which is $0, 1$ elements.

+	0	1
0	0	1
1	1	0

0, 1 are the 2 elements

·	0	1
0	0	0
1	0	1

$0 \cdot 0 = ?$

in fact $0 \cdot a = 0 \;\; \forall a \in \mathbb{F}$.

what is $1+1$?!

case 1: $1+1=0$

case 2: $1+1=1$
$\Rightarrow 1=0$ c!

$\therefore 1+1=0$

note $(-1)=1$

need to check:
F1, F2, F3, F4, F5.

$\boxed{\text{example}}$ $\mathbb{Z}_n$ for $n \geq 2$.

if $a \in \mathbb{Z}$, we can divide a by n

get a remainder $a \text{ rem } n \in \{0, 1, \dots, n-1\}$.

<u>define</u> $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ n elements

addition. $\underset{\text{in } \mathbb{Z}_n}{a + b} := \underset{\text{usual + in } \mathbb{Z}}{(a + b)} \text{ rem } n$

$\mathbb{Z}$: integers.

multiplication:

$$\underset{\text{in } \mathbb{Z}_n}{a \cdot b} := \underset{\text{in } \mathbb{Z}}{(a \cdot b)} \text{ rem } n.$$

what is $0_{\mathbb{Z}_n} = 0 \in \mathbb{Z}_n$

$$1_{\mathbb{Z}_n} = 1 \in \mathbb{Z}_n.$$

is this a field?

<u>example</u> $\mathbb{Z}_4$ $2 \cdot 2 = 0$ in $\mathbb{Z}_4$

is $\mathbb{Z}_4$ a field?!

<u>NO</u>

<u>theorem/fact</u>

$\mathbb{Z}_n$ is a field $\iff$ n = a prime number.

problem is: existence of mult. inverse.

<u>example</u>

(a) $\mathbb{Z}_5$ what is the mult + additive inverse of each element?

(b) $\mathbb{Z}_6$ same question, but which exist.

(breakout rooms to discuss).

$\mathbb{Z}_5$

0	1	2	3	4	
0	4	3	2	1	add inverse
×	1	3	2	4	mult inv.

$4 = (-1)$. " " -1.

$\mathbb{Z}_6$

0	1	2	3	4	5	
0	5	4	3	2	1	add
×	1	×	×	×	5	mult inverses

7 Sep 2020
Lecture 3

cancellation theorem

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

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

(b) if $a \cdot b = a \cdot c$ AND $a \neq 0$! then $b = c$.

will be an exercise (use axioms).

Simple facts:

$\boxed{a \cdot 0 = 0}$!? Better be true.

proof

$a \cdot 0 = a \cdot (0 + 0)$ (F3)

$\| \quad = a \cdot 0 + a \cdot 0$ (F5)

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

cancel $\Rightarrow 0 = a \cdot 0$ ✓

Sep 2020 Lecture ⑤

<u>other simple facts</u> :

$\boxed{\text{(try these yourself)}}$:

ⓐ $0, 1, -a, \frac{1}{a}$ are all unique

$a \neq 0$.

ⓑ $(-1) \cdot a = -a$

additive inverse.

$(-1)\cdot(-1) = 1$

$(-a)\,b = -ab$

$(-a)(-b) = ab$.

Vector spaces

you know $\mathbb{R}^n$

$$\vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \qquad \vec{w} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

both in $\mathbb{R}^n$

$$\vec{v} + \vec{w} = \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix}$$

addition

$$c\vec{v} = \begin{pmatrix} cv_1 \\ cv_2 \\ \vdots \\ cv_n \end{pmatrix}$$

$c \in \mathbb{R}$.

$$0_{\mathbb{R}^n} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Let $\mathbb{F}$ be a field (think: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_p$)
(p prime)

n-tuple

Def: $\mathbb{F}^n = \left\{ \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} : v_1, \ldots, v_n \in \mathbb{F} \right\}$

define $+$, scalar multiplication as above notes: $\begin{pmatrix}4\\3\end{pmatrix} \in \mathbb{Q}^2$

$\begin{pmatrix}4\\3\\0\end{pmatrix} \in \mathbb{Q}^3$.

is $\begin{pmatrix}4\\3\end{pmatrix} = \begin{pmatrix}4\\3\\0\end{pmatrix}$? NO

e.g: $\begin{pmatrix}4\\3\end{pmatrix} + \begin{pmatrix}2\\1\\1\end{pmatrix} =$ NOT WELL DEFINED

can only add, compare tuples with the same number of entries