GTLA lecture 13.08.2020

Fields: Examples:

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where $p \in \mathbb{Z}_{>0}$ is prime.

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$$

$\mathbb{R}$ 

Vector spaces (Field actions)

(in week 7 or 8 we will do group actions so field actions is a "warm up")

Let $\mathbb{F}$ be a field.

An $\mathbb{F}$-vector space is a set V with functions

$$V \times V \to V \qquad \text{and} \qquad \mathbb{F} \times V \to V$$
$$(v_1, v_2) \mapsto v_1 + v_2 \qquad\qquad (c, v) \mapsto cv$$

addition   scalar multiplication

such that

(a) If $v_1, v_2, v_3 \in V$ then

$$(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$$

(b) If $v_1, v_2 \in V$ then

$$v_1 + v_2 = v_2 + v_1$$

(c) There exist $0 \in V$ such that if $v \in V$ then $0 + v = v$

(c') If $v \in V$ then there exists $-v \in V$ such that $v + (-v) = 0$.

(d) If $c_1, c_2 \in \mathbb{F}$ and $v \in V$ then

$$c_1(c_2 v) = (c_1 c_2) v,$$

(e) If $c_1, c_2 \in \mathbb{F}$ and $v \in V$ then

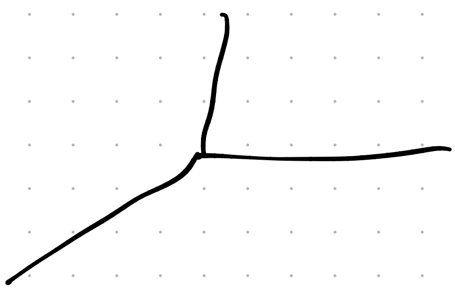
$$(c_1 + c_2) v = c_1 v + c_2 v$$

(f) If $v \in V$ then $1 \cdot v = v$.

(g) If $c \in \mathbb{F}$ and $v_1, v_2 \in V$ then $c(v_1 + v_2) = cv_1 + cv_2$

<u>Examples</u> $\mathbb{R}^2$

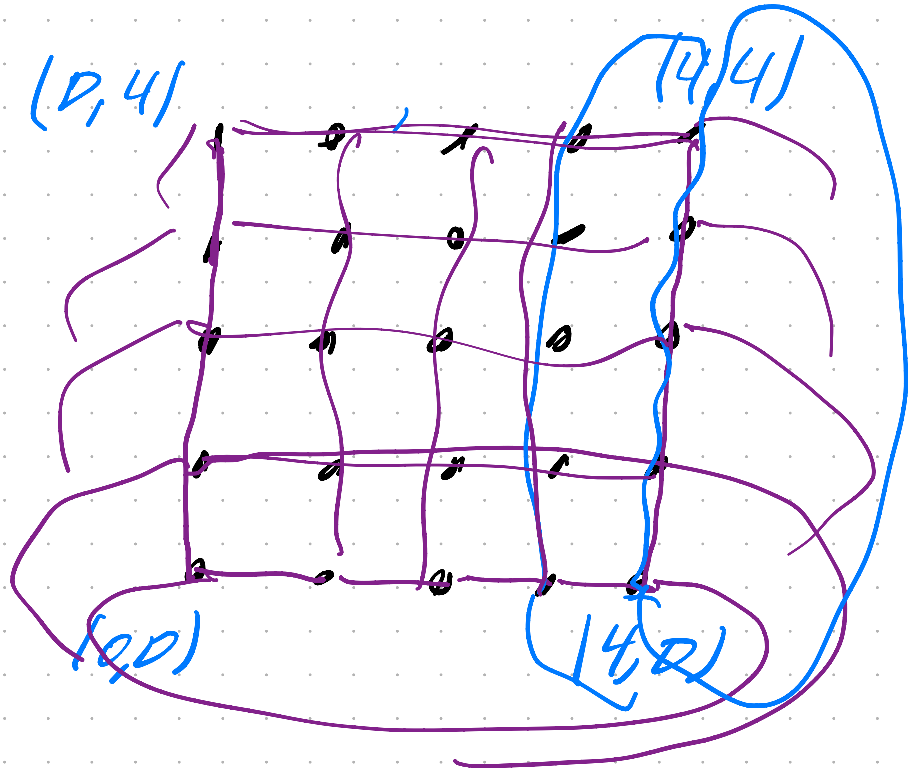
$\mathbb{R}^3$

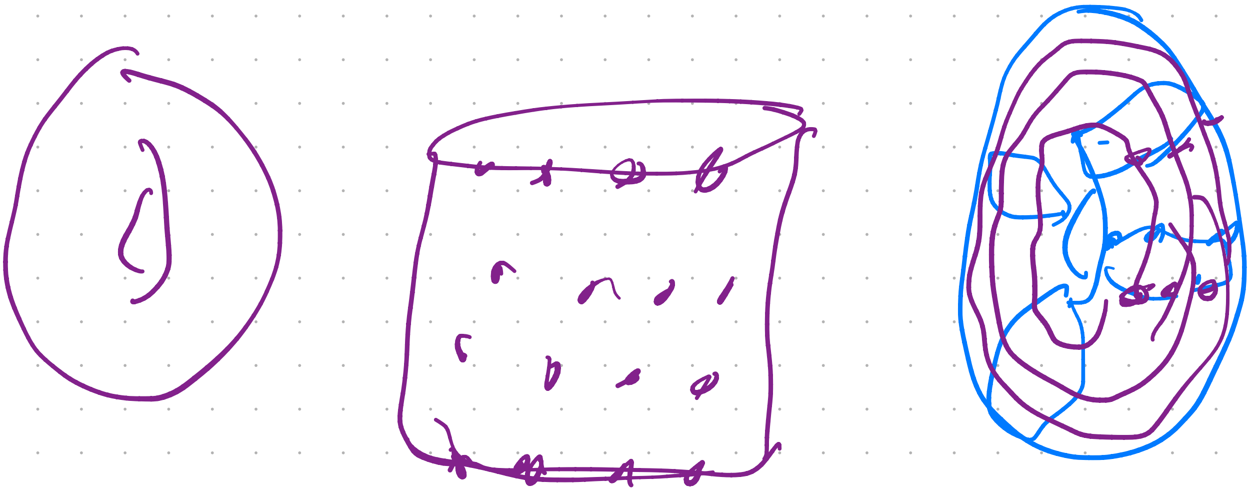


$$\mathbb{R}^2 = \{(c_1, c_2) \mid c_1, c_2 \in \mathbb{R}\}$$

$$\mathbb{F}_5^2 = \{(c_1, c_2) \mid c_1, c_2 \in \mathbb{F}_5\}$$

$\mathbb{F}_5^2 =$





Except for the "geometry" $\mathbb{F}_5^2$ acts the same as $\mathbb{R}^2$.

<u>Subspaces</u> Let $\mathbb{F}$ be a field and V an $\mathbb{F}$-vector space.

A <u>subspace</u> of V is a subset $W \subseteq V$ such that

(0) $0 \in W$ and if $w \in V$ then $-w \in W$.

(a) If $w_1, w_2 \in W$ then $w_1 + w_2 \in W$

(b) If $c \in \mathbb{F}$ and $w \in W$ then

$$cw \in W.$$

Example: $\mathbb{R}^2 \subseteq \mathbb{R}^3$

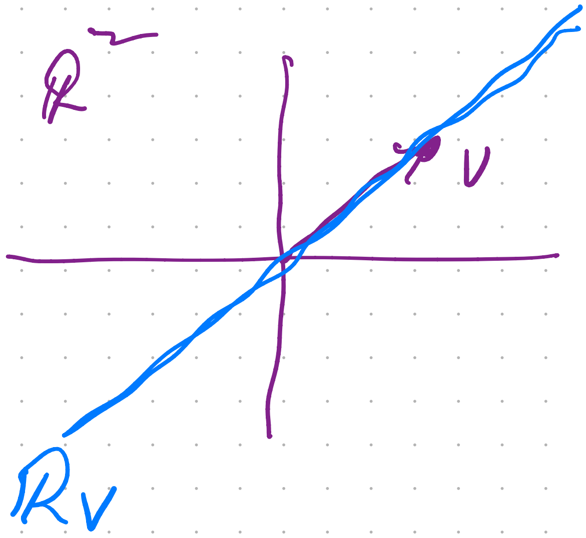
or $\mathbb{F}_5^2 \subseteq \mathbb{F}_5^3$

Example

If $v \in V$ then

$$\mathbb{F}v = \{cv \mid c \in \mathbb{F}\} \quad \text{(a line)}$$

a subspace



Let V be an $\mathbb{F}$-vector space and M and N subspaces of V.

$$M+N = \left\{ \cancel{m+n}\, m+n \;\middle|\; \begin{matrix} m \in M \\ n \in N \end{matrix} \right\}$$

(reminds us of $a\mathbb{Z} + b\mathbb{Z}$).

$$M \cap N = \{v \in V \mid v \in M \text{ and } v \in N\}$$

which are also subspaces of V.

Write $V = M \oplus N$

if $V = M + N$ and $0 = M \cap N$.

Let V be a $\mathbb{F}$-vector space.

Let $b_1, \ldots, b_k \in V$ or $\{$Let $B \subseteq V\}$

The set of __linear combinations__ of $b_1, \ldots, b_k$ is

$$\mathrm{span}_{\mathbb{F}}(b_1, \ldots, b_k) = \mathbb{F}b_1 + \cdots + \mathbb{F}b_k$$
$$= \{c_1 b_1 + \cdots + c_k b_k \mid c_1, \ldots, c_k \in \mathbb{F}\}.$$

The set $\{b_1, \ldots, b_k\}$ is __linearly independent__ if it satisfies

if $c_1, \ldots, c_k \in \mathbb{F}$ and
$c_1 b_1 + \cdots + c_k b_k = 0$
then $c_1 = 0, c_2 = 0, \ldots, c_k = 0$.

The set $\{b_1, \ldots, b_k\}$ is a __basis__ of V if

(a) $\mathbb{F}b_1 + \cdots + \mathbb{F}b_k = V$ and
(b) $\{b_1, \ldots, b_k\}$ is linearly independent.

The <u>dimension of V</u> is

$$\dim(V) = \operatorname{Card}(B)$$

where B is a basis of V.

F.2.7 in the notes reminds us:

to build bases either

(1) start with a linearly independent set and add more linearly indep. elements

(2) start with a spanning set and remove elements one at a time until ~~the~~ what's left is linearly independent

$$M_n(\mathbb{F}) = \left\{ \begin{array}{l} n\times n \text{ matrices with} \\ \text{entries in } \mathbb{F} \end{array} \right\}$$

The <u>general linear group</u>

$GL_n(\mathbb{F}) = \{ P \in M_n(\mathbb{F}) \mid P \text{ is invertible} \}$

P is <u>invertible</u> if there exists $Q \in M_n(\mathbb{F})$ such that $QP = 1$ and $PQ = 1$.

<u>Theorem</u> Let $V = \mathbb{F}^n$

$$\mathbb{F}^n = \left\{ \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \,\middle|\, c_1, \dots, c_n \in \mathbb{F} \right\}.$$

Then

$$\{\text{bases of } \mathbb{F}^n\} \longrightarrow GL_n(\mathbb{F})$$

$$(p_1, p_2, \dots, p_n) \longmapsto \begin{pmatrix} | & | & & | \\ p_1 & p_2 & \cdots & p_n \\ | & | & & | \end{pmatrix}$$

is a bijection

In English: A matrix $P \in M_n(\mathbb{F})$ is invertible if and only if its columns are linearly independent.

<u>Example</u> $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ is a field.

$\mathbb{F}_5^2 = \left\{ \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \middle| \, c_1, c_2 \in \mathbb{F}_5 \right\}$

$\mathrm{Card}(\mathbb{F}_5^2) = 25$ $\quad$ ($\mathrm{Card}(\mathbb{R}^2)$ HUGE)

A basis of $\mathbb{F}_5^2$ has two vectors in it $\{P_1, P_2\}$

For example

$P_1 = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \quad P_2 = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$

$P = \begin{pmatrix} 2 & 4 \\ 3 & 0 \end{pmatrix}$ To determine whether $\{P_1, P_2\}$ is a basis of $\mathbb{F}_5^2$

check if P is invertible.

Since

$$\begin{pmatrix} 2 & 4 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} 2\cdot 0 + 4\cdot 4 & 2\cdot 2 + 4\cdot 4 \\ 3\cdot 0 + 0\cdot 4 & 3\cdot 2 + 0\cdot 4 \end{pmatrix}$$

$$= \begin{pmatrix} 16 & 20 \\ 0 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

then $\begin{pmatrix} 0 & 2 \\ 4 & 4 \end{pmatrix}$ is the inverse of $\begin{pmatrix} 2 & 4 \\ 3 & 0 \end{pmatrix}$

and $\left\{ \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \end{pmatrix} \right\}$ is a basis of $\mathbb{F}_5^2$.

HW Show that if $A, B \in M_n(\mathbb{F})$ and $AB = I$ then $BA = I$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= (ad-bc)^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\begin{pmatrix} 2 & 4 \\ 3 & 0 \end{pmatrix}^{-1} = \frac{1}{2\cdot 0 - 4\cdot 3}\begin{pmatrix} 0 & -4 \\ -3 & 2 \end{pmatrix}$$

$$= \frac{1}{-12}\begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}$$

$$= \frac{1}{-2}\begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}$$

$$= 2\begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 4 & 4 \end{pmatrix}$$

since $3 \cdot 2 = 1$ then $\frac{1}{3} = 2$

$0 = 5$ in $\mathbb{F}_5$.

$0 \equiv 5$ in $\mathbb{F}_5$