Def A field F is a set with two operations $\oplus$ and $\odot$ s.t.

I. F is closed under $\oplus$ and $\odot$

$\forall a, b \in F$, $a \oplus b \in F$, $a \odot b \in F$

II. $\forall a, b, c \in F$,

(F1) $a \oplus b = b \oplus a$, $a \odot b = b \odot a$

(F2) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

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

(F3) There exist elements called 0 and 1 s.t. $0 \oplus a = a$

$1 \odot a = a$

(F4) $\forall a \in F, \exists c \in F$, s.t. $a \oplus c = 0$

$\forall b \in F$, $b \neq 0$, $\exists d \in F$ s.t. $b \odot d = 1$

(F5) $a \odot (b \oplus c) = a \odot b \oplus a \odot c$

Ex: ① $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ $+$, $\cdot$

② $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ is a field.

$a \oplus b = \mathrm{mod}(a+b, 3)$

$a \odot b = \mathrm{mod}(ab, 3)$

$1 \oplus 2 = 0$

$2 \oplus 1 = 0$

$1 \odot 1 = 1$

$2 \odot 2 = 1$

③ $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$ is a field if n is prime.

$a \oplus b = \mathrm{mod}(a+b, n) \quad a \odot b = \mathrm{mod}(ab, n)$

Examples of Vector Space

① $V = F$ is a vector space over F.

$V = \mathbb{R}$ is a V.S. over $\mathbb{R}$.
$\mathbb{C}$ - - - $\mathbb{C}$
$\mathbb{Q}$ - - - $\mathbb{Q}$
$\mathbb{Z}/3\mathbb{Z}$ - - - $\mathbb{Z}/3\mathbb{Z}$

② $V = F^{m \times n}$ is a V.S. over F.

③ Can $V = \mathbb{R}$ be a V.S. over $\mathbb{C}$?
No, not closed.

④ $V = \{$All polynomials with coef in $F\}$ is a V.S. over F.

Def y in (VS4) is defined as $-x$.

Theorem 1.2 V is a V.S.

(a) $0 \cdot x = \vec{0} \quad \forall x \in V$

(b) $(-a)x = -(ax) = a(-x)$

(c) $a\vec{0} = \vec{0}, \ \forall a \in F$.

Proof: (a) $0 \cdot x + 0 \cdot x = (0+0) \cdot x = 0 \cdot x = 0 \cdot x + \vec{0}$

$\Downarrow$ (canellation Thm)

$0 \cdot x = \vec{0}$

(b) $ax + [-(ax)] = \vec{0}$ ①

$ax + (-a)x = (a-a) \cdot x = 0 \cdot x = \vec{0}$ ②

①② $\Rightarrow ax + [-(ax)] = ax + (-a)x$

Cancellation Thm $\Rightarrow$ $-(ax) = (-a)x$.

Section 1.3

Def V is a V.S. over F

$W \subseteq V$ is a subspace of V if

W is a V.S. over F.

Remark: (VS1), (VS2), (VS6), (VS7), (VS8)

hold for W trivially.

For W to be a subspace,

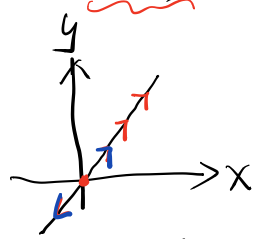
I. W is closed under $\oplus$ and $\odot$.

II. (VS3) $\vec{0} \in W$.

(VS4) $\forall x \in W$, $\exists y \in W$ s.t. $x + y = \vec{0}$

$-x \in W$.

Ex: $V = \mathbb{R}^2$



Any line passing $(0,0)$ is a subspace.

Theorem $W \subseteq V$ is a subspace iff

(a) $\vec{0} \in W$

(b) W is closed under $\oplus$ and $\odot$.

Proof: "if" $\forall x \in W$, closeness $\underset{\text{(Thm 1.2)}}{\Rightarrow}$ $-x = (-1)\cdot x \in W$

$\Rightarrow$ (VS4) holds.

"only if" Trivial.

- Transpose of a matrix

$$\begin{pmatrix} 1 & -2 & 3 \\ 0 & 5 & 1 \end{pmatrix}^T_{m\times n} = \begin{pmatrix} 1 & 0 \\ -2 & 5 \\ 3 & 1 \end{pmatrix}_{n\times m}$$

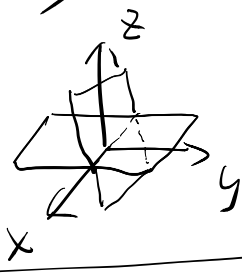
- Symmetric $n\times n$ matrix : $A^T = A$. $\begin{pmatrix} 1 & 4 & 5 \\ 4 & 2 & 6 \\ 5 & 6 & 3 \end{pmatrix}$

$a_{ij} = a_{ji}$

Ex: All real symmetric $n\times n$ matrices form a subspace of $V = \mathbb{R}^{n\times n}$.

Theorem 1.4 W_1, W_2 are subspaces of V
$\Rightarrow W_1 \cap W_2$ is a subspace.

Ex: $V = \mathbb{R}^3$

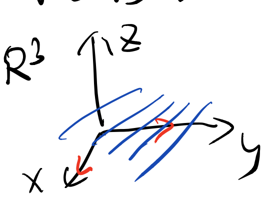


Section 1.4

Def A linear combination vectors $v_i \in V$ is
$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \in V$
where $a_i \in F$.

Def $S \neq \phi$, $S \subseteq V$
Span(S) is the set of all linear combinations of vectors in S.

Ex: $V = \mathbb{R}^3$



$S = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right\}$

$\text{Span}(S) = \left\{ a\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + b\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \ \forall a, b \in F \right\}$

$= \left\{ \begin{bmatrix} a \\ b \\ 0 \end{bmatrix}, \forall a, b \in F \right\}$

Def If $\mathrm{Span}(S) = V$, we say S spans/generates V.

Ex: $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ spans $\mathbb{R}^{2\times 2}$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Ex: $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ spans all real symmetric 2×2 matrices.

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Theorem 1.5 ① $S \subseteq V$, $\mathrm{Span}(S)$ is a subspace of V.

② Any subspace containing S must also contain $\mathrm{Span}(S)$.

Sketchy Proof: ① $\forall x \in S$, $\underset{\overset{\|}{0}}{0 \cdot x} \in \mathrm{Span}(S)$

$\forall x, y \in \mathrm{Span}(S)$, then

$x = a_1 u_1 + a_2 u_2 + \cdots + a_n u_n$

$y = b_1 v_1 + \cdots + b_m v_m$

$a_i, b_j \in F$, $u_i, v_j \in S$

$x + y = a_1 u_1 + \cdots + a_n u_n + b_1 v_1 + \cdots + b_m v_m \in \mathrm{Span}(S)$.

Def Linear Dependence.

$S \subseteq V$ is called linearly dependent if

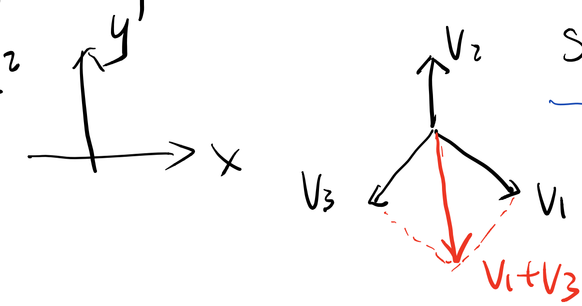
$\exists$ distinct vectors $u_i \in S$, and $a_i \in F$ s.t.

$a_1 u_1 + a_2 u_2 + \cdots + a_n u_n = \vec{0}$

where a_i are not all zero.

Linear Independence: no such linear comb.

Ex: $V = \mathbb{R}^2$



$S = \{V_1, V_2, V_3\}$

$V_1 + V_3 + aV_2 = \vec{0}$ $\quad a \neq 0$

$\Downarrow$

$V_1 = -V_3 - aV_2$

Theorem 1.7 S is a linearly independent subset of V. $v \in V$, $v \notin S$. Then $S \cup \{v\}$ is linearly dependent iff $v \in \mathrm{Span}(S)$.

Proof: "if" $v \in \mathrm{Span}(S)$

$\Rightarrow v = a_1 u_1 + \cdots + a_n u_n$, $u_i \in S$, $a_i \in F$.

$\Rightarrow (-v) + v = -v + a_1 u_1 + \cdots + a_n u_n$

$\Rightarrow \vec{0} = \underbrace{(-1)}_{\neq 0} v + a_1 u_1 + \cdots + a_n u_n.$