§ 8 Quick Review on Linear Algebra

Vector Spaces

Definition 8.1

A vector space V over a field F consists of a set with two operations $+ : V \times V \to V$ (addition) and $\cdot : F \times V \to V$ (scalar multiplication) that satisfies

(VS 1) For all $x, y \in V$, $x+y = y+x$

(VS 2) For all $x, y, z \in V$, $(x+y)+z = x+(y+z)$

(VS 3) There exists $0_V \in V$ such that $x + 0_V = x$ for all $x \in V$

(VS 4) For all $x \in V$, there exists $y \in V$ such that $x+y = 0_V$.

(VS 5) For all $x \in V$, $1 \cdot x = x$ (Recall : 1 is the multiplicative identity in F)

(VS 6) For all $a, b \in F$, $x \in V$, $(ab) \cdot x = a \cdot (b \cdot x)$

(VS 7) For all $a \in F$, $x, y \in V$, $a \cdot (x+y) = a \cdot x + a \cdot y$

(VS 8) For all $a, b \in F$, $x \in V$, $(a+b) \cdot x = a \cdot x + b \cdot x$

(Remark : so $(V, +)$ is an abelian group.)

Example 8.1

$F^n = \{(a_1, a_2, \cdots, a_n) : a_i \in F\}$ with

$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1+b_1, a_2+b_2, \cdots, a_n+b_n)$ and $c \cdot (a_1, a_2, \cdots, a_n) = (ca_1, ca_2, \cdots, ca_n)$

where $a_i, b_i, c \in F$, is a vector space.

In particular, if $F = \mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^3$ are vector space we studied in high school.

If $F = \mathbb{Z}_p$, F^n consists of p^n elements.

Example 8.2

Let S be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$.

For $f, g \in S$, $c \in \mathbb{R}$, we define $f+g$ by $(f+g)(x) = f(x) + g(x)$ and $c \cdot f$ by $(c \cdot f)(x) = cf(x)$.

Then S is a vector space.

Example 8.3

Let F be a field.

$F[x]$ = set of all polynomials with coefficient in F with usual addition and scalar multiplication is a vector space.

Exercise 8.1

Let F be a field, $d \in \mathbb{Z}^+$. Show that

(a) the set of all polynomials of degree $\leq d$ with coefficient in F with usual addition and scalar multiplication is a vector space.

(b) the set of all polynomials of degree $= d$ with coefficient in F with usual addition and scalar multiplication is not a vector space.

Proposition 8.1

Let V be a vector space and let $x, y, z \in V$.

If $x+z = y+z$, then $x = y$.

Corollary 8.1

0_V are y described in (VS 3) and (VS 4) are unique.

(Therefore, if $x \in V$, the unique additive inverse of x is denote by $-x$)

Proposition 8.2

Let V be a vector space.

1) For all $x \in V$, $0 \cdot x = 0_V$

2) For all $x \in V$, $c \in F$, $(-c) \cdot x = -(c \cdot x)$

3) For all $a \in F$, $a \cdot 0_V = 0_V$

Definition 8.2

A subset W of a vector space V over a field F is called a subspace of V if W is a vector space over F under the operations of addition and scalar multiplication on V.

Proposition 8.3

Let V be a vector space and let W be a subset of V. W is a subspace of V if and only if all the following conditions hold:

1) $0_V \in W$

2) For all $x, y \in W$, we have $x+y \in W$.

3) For all $x \in W$, $c \in F$, we have $c \cdot x \in W$.

Linear Combination and Linear Independence of Vectors

Definition 8.3

Let V be a vector space and let S be a nonempty subset of V.

A vector $v \in V$ is called a combination of elements of S if there exist $u_1, u_2, \cdots, u_k \in S$ and $c_1, c_2, \cdots, c_k \in F$ such that $v = c_1u_1 + c_2u_2 + \cdots + c_ku_k$.

In this case, v is said to be a linear combination of $u_1, u_2, \cdots, u_k$.

Example 8.4

Let $u_1 = (2,3,1)$, $u_2 = (1,0,2) \in \mathbb{R}^3$.

$v = (7,6,8) = 2u_1 + 3u_2$ which is a linear combination of u_1 and u_2

Definition 8.4

Let V be a vector space and let S be a subset of V.

The span of S, denoted by span(S), is defined as the set of all linear combination of elements of S. In particular, if $S = \phi$, span(ϕ) is defined as $\{0_V\}$.

Proposition 8.4

span(S) is a subspace of V.

Example 8.5

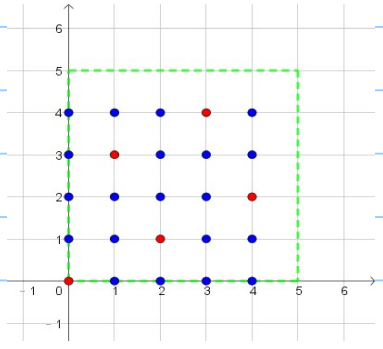
Let $u_1 = (1,0,1)$, $u_2 = (0,1,2) \in \mathbb{R}^3$.

Then $\text{span}(\{u_1, u_2\}) = \{v = c_1u_1 + c_2u_2 : c_1, c_2 \in \mathbb{R}\}$ which is the plane containing u_1 and u_2.

Example 8.6

Let $F = \mathbb{Z}_5$ and let $u = (1,3) \in F^2$

$\text{span}(\{u\}) = \{v = cu : c \in F\} = \{(0,0), (1,3), (2,1), (3,4), (4,2)\}$



All marked lattice points are points of F^2

Red points are points of span($\{u\}$)

Definition 8.5

A subset S of a vector space V spans V if $\text{span}(S) = V$.

Example 8.7

Let $u_1 = (1,0,0)$, $u_2 = (2,1,0)$, $u_3 = (1,1,1) \in \mathbb{R}^3$.

Let $v = (a_1, a_2, a_3) \in \mathbb{R}^3$ Find $c_1, c_2, c_3 \in \mathbb{R}$ such that $v = c_1u_1 + c_2u_2 + c_3u_3$.

$$\begin{aligned} 1\cdot c_1 + 2\ c_2 + 1\cdot c_3 &= a_1 \\ 0\cdot c_1 + 1\ c_2 + 1\cdot c_3 &= a_2 \\ 0\cdot c_1 + 0\cdot c_2 + 1\cdot c_3 &= a_3 \end{aligned} \longrightarrow \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \quad \text{or} \quad \left(\begin{array}{ccc|c} 1 & 2 & 1 & a_1 \\ 0 & 1 & 1 & a_2 \\ 0 & 0 & 1 & a_3 \end{array}\right)$$

$c_1 = a_1 - 2a_2 + a_3$, $c_2 = a_2 - a_3$, $c_3 = a_3$

$\therefore$ Any vector $(a_1, a_2, a_3) \in \mathbb{R}^3$ can be expressed as a linear combination of u_1, u_2, u_3,

$\text{span}(\{u_1, u_2, u_3\}) = \mathbb{R}^3$.

In general, if we have $u_1, u_2, \ldots, u_n \in \mathbb{R}^m$ and we want to express $v \in \mathbb{R}^m$ in a linear combination of $u_1, u_2, \ldots, u_m$, we have to solve a system of linear equations with m equations, n unknowns

Example 8.8

Let $u_1 = (2,3,0)$, $u_2 = (3,1,0)$, $u_3 = (4,0,3) \in F^3$, where $F = \mathbb{Z}_5$

Find $c_1, c_2, c_3 \in F$ such that $v = (2,1,4) = c_1u_1 + c_2u_2 + c_3u_3$

$$\begin{aligned} 2\cdot c_1 + 3\ c_2 + 4\cdot c_3 &= 2 \\ 3\cdot c_1 + 1\ c_2 + 0\cdot c_3 &= 1 \\ 0\cdot c_1 + 0\ c_2 + 3\cdot c_3 &= 4 \end{aligned} \longrightarrow \left(\begin{array}{ccc|c} 2 & 3 & 4 & 2 \\ 3 & 1 & 0 & 1 \\ 0 & 0 & 3 & 4 \end{array}\right) \begin{matrix} 3R_1 \to R_1 \\ \sim \\ 2R_2 \to R_2 \end{matrix} \left(\begin{array}{ccc|c} 1 & 4 & 2 & 1 \\ 1 & 2 & 0 & 2 \\ 0 & 0 & 3 & 4 \end{array}\right)$$

(Note: $2^{-1} = 3$, $3^{-1} = 2$ in F)

$$\begin{matrix} R_2 - R_1 \to R_2 \\ \sim \end{matrix} \left(\begin{array}{ccc|c} 1 & 4 & 2 & 1 \\ 0 & 3 & 3 & 1 \\ 0 & 0 & 3 & 4 \end{array}\right)$$

$$\begin{matrix} 2R_2 \to R_2 \\ \sim \end{matrix} \left(\begin{array}{ccc|c} 1 & 4 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 3 & 4 \end{array}\right)$$

$$\begin{matrix} 2R_3 \to R_3 \\ \sim \end{matrix} \left(\begin{array}{ccc|c} 1 & 4 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

$c_3 = 3$,

$c_2 + c_3 = 2 \Rightarrow c_2 = 1$

$c_1 + 4c_2 + 2c_3 = 1 \Rightarrow c_1 + 4(1) + 2(3) = 1 \Rightarrow c_1 = 1$

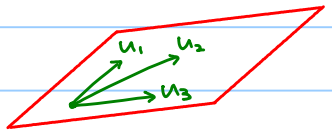
Question: Given $u_1, u_2 \in \mathbb{R}^3 \setminus \{0\}$, is $\text{span}(\{u_1, u_2\})$ always a plane?

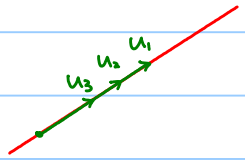
Answer: No! If $u_1 \parallel u_2$ (i.e. $u_2 = ku_1$ for some $k \in \mathbb{R}$), then $\text{span}(\{u_1, u_2\})$ is just a line.

($\because v = c_1u_1 + c_2u_2 = (c_1 + kc_2)u_1$)

Question: Given $u_1, u_2, u_3 \in \mathbb{R}^3 \setminus \{0\}$, is $\text{span}(\{u_1, u_2, u_3\})$ always $\mathbb{R}^3$?

Answer: No! If u_1, u_2, u_3 lie on a plane or a line, $\text{span}(\{u_1, u_2, u_3\}) \neq \mathbb{R}^3$.





One of u_i can be expressed as a linear combination of the others.

Definition 8.6

A subset S of a vector space V is called linearly independent if for all finite number of distinct vectors $u_1, u_2, \cdots, u_k \in S$, $c_1u_1 + c_2u_2 + \cdots + c_ku_k = 0_V \Rightarrow c_1 = c_2 = \cdots = c_k = 0$.

(Conversely, S is linearly dependent if there exists $u_1, u_2, \cdots, u_k \in S$ and $c_1, c_2, \cdots, c_k \in F$ but not all zero such that $c_1u_1 + c_2u_2 + \cdots + c_ku_k = 0_V$.

Assume $c_i \neq 0$, then $u_i = \sum_{j \neq i} -\frac{c_j}{c_i} u_j$,

i.e u_i can be expressed as a linear combination of the others.)

Exercise 8.2

Let V be a vector space and let $S_1 \subseteq S_2 \subseteq V$. Show that if S_2 is linearly independent, then S_1 is also linearly independent.

Definition 8.7

Let V be a vector space and let $\beta \subseteq V$.

β is said to be a basis for V if β is linearly independent and $\text{span}(\beta) = V$.

Example 8.9

Let $e_i = (0, \cdots, 0, \underset{\text{i-th}}{1}, 0, \cdots, 0) \in F^n$ for $i = 1, 2, \cdots, n$. $\{e_1, e_2, \cdots, e_n\}$ is a basis for F^n, which is called the standard basis for F^n

Exercise 8.3

Show that $\{u_1, u_2, u_3\}$ in example 8.7 is a linearly independent set of vectors.
Also, since $\text{span}(\{u_1, u_2, u_3\}) = \mathbb{R}^3$, $\{u_1, u_2, u_3\}$ is a basis for $\mathbb{R}^3$.

Proposition 8.4

Let V be a vector space and let $\beta = \{u_1, u_2, \cdots, u_n\}$ be a subset of V.
Then β is a basis for V if and only if for all $v \in V$, there exist unique $c_1, c_2, \cdots, c_n \in F$ such that $v = c_1u_1 + c_2u_2 + \cdots + c_nu_n$.

Proposition 8.5

Let V be a vector space having a finite basis. Then every basis for V contains the same number of elements.

Definition 8.8

A vector space is called finite dimensional if it has a finite basis. The unique number of elements in each basis for V is called the dimension of V and is denoted by $\dim(V)$.
A vector space is infinite dimensional if it is not finite dimensional.

Example 8.10

$\dim(F^n) = n$ (Recall : the standard basis has n vectors.)
Let $S = \{u_1, u_2, \cdots, u_k\}$ be a linearly independent set of vectors in F^n, where $1 \le k \le n$.
If $W = \text{span}(S)$, then W is a k-dimensional subset of V.

Row Vectors and Column Vectors of Matrices

Let $M_{m\times n}(F)$ be the set of all $(m\times n)$-matrices with entries in F and let $A \in M_{m\times n}(F)$

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Then the rows and columns can be regarded as vectors of F^n and F^m respectively.

Example 8.11

Consider $A = \begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 2 & 4 & 3 & 1 & 0 \\ 3 & 6 & 4 & 1 & 5 \end{pmatrix} \in M_{3\times 5}(\mathbb{R})$

There are five column vectors $v_1, v_2, \cdots, v_5 \in \mathbb{R}^3$

We perform elementary row operations on A until it is of the reduced row echelon:

$$\begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 2 & 4 & 3 & 1 & 0 \\ 3 & 6 & 4 & 1 & 5 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 & -4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \cdots \sim \underbrace{\begin{pmatrix} \textcircled{1} & 2 & 0 & -1 & 0 \\ 0 & 0 & \textcircled{1} & 1 & 0 \\ 0 & 0 & 0 & 0 & \textcircled{1} \end{pmatrix}}_{\text{reduced row echelon form}}$$

① : leading 1's

Three leading 1's are located at 1st, 3rd and 5th column and so $\{v_1, v_3, v_5\}$ forms a linear independent set of vectors.

Also $v_2 = 2v_1$ and $v_4 = -v_1 + v_3$.

Explanation:

$$\begin{pmatrix} 1 & 2 & 1 & 0 & 2 \\ 2 & 4 & 3 & 1 & 0 \\ 3 & 6 & 4 & 1 & 5 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 2 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

forget forget

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 2 & 0 & 3 & 1 \\ 3 & 5 & 4 & 1 \end{array}\right) \sim \cdots \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

Finding c_1, c_3, c_5 such that $\therefore c_1 = -1, c_3 = 1, c_5 = 0$

$c_1v_1 + c_3v_3 + c_5v_5 = v_4$

Similarly,

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 2 & 0 & 3 & 0 \\ 3 & 5 & 4 & 0 \end{array}\right) \sim \cdots \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

which means $c_1v_1 + c_3v_3 + c_5v_5 = 0_v \Rightarrow c_1 = c_3 = c_5 = 0$

so $\{v_1, v_3, v_5\}$ is linearly independent.

Remark:

To study row vectors, we can perform elementary column operations or simply study A^T.

Example 8.12

Let $G = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right) \in M_{3\times 5}(F)$, where the left block is I_3.

Claim: Row vectors of G form a linearly independent set of vectors in F^5

$$G^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \overset{\text{(Ex.)}}{\sim \cdots \sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

In general, let $I_k \in M_{k\times k}(F)$ be the identity matrix, $P \in M_{k\times(n-k)}(F)$.

Then $G = (I_k, P) \in M_{k\times n}(F)$ and the row vectors form a linearly independent set of vectors in F^n since $G^T = \begin{pmatrix} I_k \\ P^T \end{pmatrix} \sim \begin{pmatrix} I_k \\ 0 \end{pmatrix}$

Exercise 8.4

Let $G = \begin{pmatrix} 6 & 1 & 3 & 1 & 0 & 0 \\ 0 & 6 & 1 & 3 & 1 & 0 \\ 0 & 0 & 6 & 1 & 3 & 1 \end{pmatrix} \in M_{3\times 6}(F)$, where $F = \mathbb{Z}_7$

Show that the row vectors of G form a linearly independent set of vectors in F^6.

Dot Product

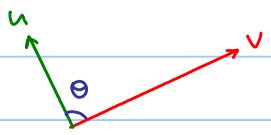
Definition 8.9

Let $u = (a_1, a_2, \cdots, a_n)$, $v = (b_1, b_2, \cdots, b_n) \in F^n$.

The dot product $u \cdot v$ is defined as $\sum_{i=1}^{n} a_i b_i$.

Recall: In particular, for $u, v \in \mathbb{R}^n$, we have $u \cdot v = |u||v|\cos\theta$ where θ is the angle between u and v and $|u|^2 = \sum_{i=1}^{n} a_i^2$, $|v|^2 = \sum_{i=1}^{n} b_i^2$.

Therefore, if $u, v \in \mathbb{R}^n \setminus \{0\}$, we have $u \cdot v = 0 \Leftrightarrow \cos\theta = 0 \Leftrightarrow u \perp v$.



Recall: Let $A \in M_{m\times n}(F)$, $B \in M_{n\times q}(F)$, then $C = AB \in M_{m\times q}(F)$ is defined by

$$c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj} = \text{dot product of the } i\text{-th row vector of } A \text{ and the } i\text{-th column vector of } B.$$

$$C = \begin{matrix} \\ m \end{matrix}\overbrace{\begin{pmatrix} \vdots \\ \cdots\ c_{ij}\ \cdots \\ \vdots \end{pmatrix}}^{q} = \begin{matrix} \\ m \end{matrix}\overbrace{\begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{bmatrix}}^{n} \begin{matrix} \\ n \end{matrix}\overbrace{\begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{bmatrix}}^{q}$$

Example 8.13

Let $A \in M_n(\mathbb{R})$ such that $AA^T = A^TA = I$.

$$\underbrace{\begin{pmatrix} — v_1 — \\ — v_2 — \\ \vdots \\ — v_n — \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} | & | & & | \\ v_1 & v_2 & \cdots & v_n \\ | & | & & | \end{pmatrix}}_{A^T} = I$$

$$v_i \cdot v_j = \begin{cases} 1 & \text{if } i=j \Rightarrow |v_i| = 1 \\ 0 & \text{if } i\neq j \Rightarrow v_i \perp v_j \text{ if } i\neq j \end{cases}$$

Proposition 8.6

Let C be a k-dimensional subspace of F^n.

Then $C^\perp = \{v \in F^n : v\cdot u = 0 \text{ for all } u \in C\}$ is a $(n-k)$-dimensional subspace of F^n.

Exercise 8.5

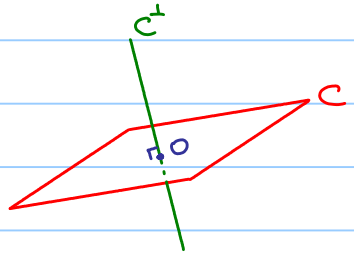
Suppose that $\beta = \{u_1, u_2, \cdots, u_k\}$ is a basis for C.

Let $v \in V$. Show that $v\cdot u = 0$ for all $u \in C$ if and only if $v\cdot u_i = 0$ for all $i = 1, 2, \cdots, k$.

Example 8.14

Let C be a 2-dimensional subspace (a plane) of $\mathbb{R}^3$.

$C^\perp$ is a line which is perpendicular to C.



However, the above picture is not that correct in some situations.

Example 8.14

Let $u_1=(1,0,0,1)$, $u_2=(0,1,1,0)\in F$, where $F=\mathbb{Z}_2$.

Suppose that $C=\text{span}(\{u_1,u_2\})$, then $\dim(C)=2$.

Then, $v=(x_1,x_2,x_3,x_4)\in C^\perp$, then $\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$ or $\left(\begin{array}{cccc|c}1&0&0&1&0\\0&1&1&0&0\end{array}\right)$

Let $x_3=s$, $x_4=t$ where $s,t\in F$

$x_1+x_4=0 \Rightarrow x_1=x_4=t$

$x_2+x_3=0 \Rightarrow x_2=x_3=s$

$\therefore (x_1,x_2,x_3,x_4)=(t,s,s,t)=t(1,0,0,1)+s(0,1,1,0)$ and $C^\perp=C$.

Example 8.15

Let $I_k\in M_k(F)$, $I_{n-k}\in M_{n-k}(F)$ be identity matrices, and let $P\in M_{k\times(n-k)}(F)$.

Then $G=(I_k,P)\in M_{k\times n}(F)$ and $H=(-P^T,I_{n-k})\in M_{(n-k)\times n}(F)$.

Also we have $GH^T=(I_k,P)\begin{pmatrix}-P\\I_{n-k}\end{pmatrix}=P-P=0$.

That means each row vector of G $\perp$ each column vector of H^T

(i.e. each row vector of H)

If C is the subspace spanned by row vectors of G,

then $C^\perp$ is the subspace spanned by row vectors of H.

Let $G=\begin{pmatrix}1&0&0&1&1\\0&1&0&1&0\\0&0&1&0&1\end{pmatrix}\in M_{3\times5}(\mathbb{Z}_2)$

Then $H=\begin{pmatrix}1&1&0&1&0\\1&0&1&0&1\end{pmatrix}\in M_{2\times5}(\mathbb{Z}_2)$ (Remark: In $\mathbb{Z}_2$, $-1=1$)