Topic#4
Basis & dimension

Def. $(V, +, \cdot)$: v.s. over $\mathbb{F}$. $\beta \subset V$. β is a **basis** if
(a) β is l. indep.
(b) $V = \text{span}\beta$.

Examples:

(1) $\mathbb{F}^n$: $\{e_1, \cdots, e_n\}$ is a bsis (standard basis)
note: span$\{e_1, e_2, \cdots\}$ = a v.s. of all sequences $(x_1, x_2, \cdots) \in \mathbb{F}^\infty$ with finite many non-zero terms

(2) $P_n(\mathbb{F}) : \{1, x, \cdots, x^n\}$ is a basis
$P(\mathbb{F}) = \{1, x, \cdots\}$ is a basis

(3) $M_{m\times n}(\mathbb{F}) : \{E_{ij} : 1 \le i \le m, 1 \le j \le n\}$ is a basis, where

$$E_{ij} = i^{th} \begin{pmatrix} & \overset{j^{th}}{\vdots} & \\ \cdots & \cdot & \cdots \\ & \vdots & \end{pmatrix}.$$

Def.: A v.s. V is **finite-dimensional** if V has a finite spanning set, i.e., $\exists$ a finite set $S \subset V$ s.t.

$$V = \mathrm{span}(S).$$

Otherwise, V is **infinite-dimensional**.

Thm. A finite spanning set can be reduced to a basis, namely, let $(V, +, \cdot)$: v.s. over $\mathbb{F}$. If $V = \text{span}(S)$ where $S \subset V$ is of finite size, then $\exists \beta \subset S$ which is a basis for V.

Proof.

- If S is l. indep., take $\beta = S$, done.

- Otherwise, S is l. dep.

By a previous prop., $\exists v_1 \in S$ s.t. span$S$=span$(S \setminus \{v_1\})$.
If $S \setminus \{v_1\}$ is l. indep., take $\beta = S \setminus \{v_1\}$, done.

- Otherwise, repeat the same process.

$\because$ S is finite
$\therefore$ After finite steps, we reach a l. indep. subst $S' \subset S$ s.t.

$$\text{span}S' = \text{span}S,$$

then take $\beta = S'$, done! $\square$

Coro.: V is finite-dimensional **iff** V has a finite basis.

Prop. $(V, +, \cdot)$: v.s. over $\mathbb{F}$. $\beta = \{u_1, u_2, \cdots, u_n\} \subset V$.
Then β is a basis for V **iff** $\forall v \in V$, $\exists! a_1, a_2, \cdots, a_n \in \mathbb{F}$ s.t.

$$v = a_1 u_1 + a_2 u_2 + \cdots + a_n u_n.$$

Proof. "$\Rightarrow$" Assume: β is a basis. Let $v \in V$.
$V = \text{span}\beta \Rightarrow v$ is a linear combination of $u_1, \cdots, u_n$.
If $v = a_1 u_1 + \cdots + a_n u_n = b_1 u_1 + \cdots + b_n u_n$ are two representations, then $(a_1 - b_1)u_1 + \cdots + (a_n - b_n)u_n = 0$
$\because \beta$ is l. indep.
$\therefore a_i - b_i = 0, 1 \leq i \leq n$, i.e. $a_i = b_i, 1 \leq i \leq n$.

$\Leftarrow$ Let $\forall v \in V$. Then, $\exists! a_1, \cdots, a_n \in \mathbb{F}$ s.t. $v = \sum_{i=1}^{n} a_i u_i$,
$\therefore v \in \text{span}\beta$
$\therefore V \subset \text{span}\beta$. $\therefore V = \text{span}\beta$
Also, let $a_1 u_1 + \cdots + a_n u_n = 0$.
Then, $a_i = 0$ $(1 \leq i \leq n)$ by uniqueness.
$\therefore \beta$ is l. indep.
$\therefore \beta$ is a bsis for V. $\square$

Thm. (Replacement Theorem)

$(V, +, \cdot)$: v.s. over $\mathbb{F}$.
$V =$span$G$ with $\sharp G = n$.
$L \subset V$ is l. indep. with $\sharp L = m$.

Then $m \leq n$ and $\exists H \subset G$ with $\sharp H = n - m$ such that

$$V = \text{span}(L \cup H).$$

Proof. Induction in m:

$m = 0 : L = \emptyset$, take $H = G$.

Assume "TRUE" for some $m \geq 0$, to show "TRUE" for $m+1$.

Assume: $L = \{v_1, \cdots, v_{m+1}\} \subset V$ l. indep. with $\sharp L = m+1$.

$\therefore L' = \{v_1, \cdots, v_m\}$ l. indep. with $\sharp L' = m$

$\therefore$ By I.A., $m \leq n$ & $\exists H' = \{u_1, \cdots, u_{n-m}\} \subset G$ s.t.

$$V = \text{span}(L' \cup H') = \text{span}(\{v_1, \cdots, v_m, u_1, \cdots, u_{n-m}\}).$$

Consider $v_{m+1} \in V$.

$$\therefore v_{m+1} = a_1 v_1 + \cdots + a_m v_m + b_1 u_1 + \cdots + b_{n-m} u_{n-m}$$
$$\text{for some } a_1, \cdots, a_m, b_1, \cdots, b_{n-m} \in \mathbb{F}$$

$\because L = \{v_1, \cdots, v_{m+1}\}$ l. indep.

$\therefore b_1, \cdots, b_{n-m}$ not all zero, i.e. $n - m > 0$, i.e. $n \geq m+1$.

For instance, $b_1 \neq 0$, then

$$u_1 \in \text{span}\{v_1, \cdots, v_m, v_{m+1}, u_2, \cdots, u_{n-m}\}.$$

Take $H \overset{def}{=} \{u_2, \cdots, u_{n-m}\}$.

Then $V = \text{span}(\{v_1, \cdots, v_{m+1}, u_2, \cdots, u_{n-m}\}) = \text{span}(L \cup H)$.

$\therefore$ TRUE for $m+1$. $\square$

Two quick consequences of R.T.:

(1) Let V be a **finite-dimensional** v.s., then **any linearly independent subset of V must be finite.** Indeed, otherwise, let $\{v_1, v_2, ...\} \subset V$ be a linear independent infinite subset. Let β be a finite basis for V with $\#\beta = n$. Note that $\{v_1, ..., v_{n+1}\}$ is linearly independent with $\# = n + 1$. By R.T., $n + 1 \leq m = n$, which is a contradiction.

(2) By (1), one then can conclude that **if V has an infinite linearly independent subset, then V must be infinite-dimensional.**

Fact: Let V be a **finite-dimensional** v.s., then all bases for V have the same size, for instance, let β, γ be two finite bases for V, then $\sharp\beta = \sharp\gamma$.

Pf. Direct consequence of Replacement Theorem:

let $V =$spanβ. $\gamma \subset V$ l. indep. $\Rightarrow \sharp\gamma \leq \sharp\beta$
$V =$spanγ. $\beta \subset V$ l. indep. $\Rightarrow \sharp\beta \leq \sharp\gamma$ □

Def. $(V, +, \cdot)$: v.s. over $\mathbb{F}$. When V is **finite-dimensional**, we write the **dimension** of V as

$$\dim(V) = \sharp\beta$$

where β is a finite basis of V.

Examples:

(1) $\dim(\mathbb{F}^n) = n$.
$\mathbb{F}^\infty$ is ∞-dimensional.

(2) $\dim P_n(\mathbb{F}) = n$.
$P(\mathbb{F})$ is ∞-dimensional.

(3) $\dim M_{m\times n}(\mathbb{F}) = mn$.

(4) $(\mathbb{C}, +, \cdot)$: v.s. over $\mathbb{F}$.
When $\mathbb{F} = \mathbb{C}$, $\dim \mathbb{C} = 1$ (why?);
When $\mathbb{F} = \mathbb{R}$, $\dim \mathbb{C} = 2$ (why?).

Basic Facts: Let $(V, +, \cdot)$: v.s over $\mathbb{F}$ with dim $V = n$.

(1) If $V =$span$S$ with finite S, then $\sharp S \geq n$.

(2) If $V =$span$S$ with $\sharp S = n$, then$S$ is a basis for V.

(3) If $S \subset V$ is l. indep. with $\sharp S = n$, then S is a basis for V.

(4) Every l. indep. subset of V can be extended to a basis for V.

Proof. Let β be a basis for V with $\sharp\beta = n$.

(1) direct consequence of R.T.

(2) S must be l. indep.,
otherwise $\exists G \subsetneq S$ l. indep. s.t. $V =$span$G$.
$\therefore n = \dim(V) = \sharp G < \sharp S = n$: contradiction!
$\therefore S$ is a basis for V.

(3) Replacement Theorem $\Rightarrow$
$\exists H \subset \beta$ with $\sharp H = n - \sharp S = n - n = 0$ s.t. $V =$span$(S \cup H)$.
$\because H = \emptyset \therefore V =$span$S$. $\therefore S$ is a basis.

(4) Let $L \subset V$ be l. indep. with $\sharp L = m$.
Replacement Theorem $\Rightarrow m \leq n$ &
$\exists H \subset \beta$ with $\sharp H = n - \sharp L = n - m$ s.t. $V =$span$(L \cup H)$.
Note: $\sharp(L \cup H) = n$.
(why? $\leq$ by $\sharp(L \cup H) \leq \sharp L + \sharp H = n$ and $\geq$ by (1))
(2) $\Rightarrow L \cup H$ is a basis. $\square$

Thm.: $(V, +, \cdot)$: v.s. over $\mathbb{F}$ with $\dim(V) < \infty$. W is a subspace of V. Then

(1) W is finite-dimensional with $\dim(W) \leq \dim(V)$.

(2) If $\dim(W) = \dim(V)$ then $W = V$.

Proof. Let $n = \dim(V)$.

IF $W = \{0\}$: W is finite-dim & $\dim W = 0 \leq n$.
Otherwise, $W \neq \{0\}$: $\exists u_1 \neq 0$ s.t. $u_1 \in W$. $\{u_1\}$ is l. indep.

IF $W =$span$(\{u_1\})$: $\{u_1\}$ is a basis of W. W is finite-dim & $\dim W = 1 \leq n$.
Otherwise, $\exists u_2 \in W \setminus \text{span}(\{u_1\})$. $\therefore \{u_1, u_2\}$ l. indep.

IF $W =$span$(\{u_1, u_2\})$: $\{u_1, u_2\}$ is a basis of W. W is finite-dim & $\dim W = 2 \leq n$.
Otherwise, $\exists u_3 \in W \setminus \text{span}(\{u_1, u_2\})$, repeat the procedure.

Note: $\sharp$ of a l. indep. subset of $V \leq n$.

$\therefore$ the above process must stop with some k such that

$$W = \text{span}(\{u_1, u_2, \cdots, u_k\}): \{u_1, \cdots, u_k\} \text{ l. indep.}$$

$\therefore \{u_1, \cdots, u_k\}$ is a basis for W, $\dim(W) = k \leq n$. □

If $\dim(W) = n$, then $\beta = \{u_1, \cdots, u_n\}$ is l. indep. subset of size n in V, so β is also a basis for V. $\therefore W = \text{span}\beta = V$. □□

e.g.: $M_{n\times n}(\mathbb{F})$, $\dim(M_{n\times n}(\mathbb{F})) = n^2$:

(1) $W \overset{def}{=} \{\text{all diagonal matrices}\}$ is a subspace.
$\dim(W) = n$.

(2) $W \overset{def.}{=} \{\text{all symmetric matrices}\}$ is also a subspace
$\dim(W) = n + (n-1) + \cdots + 1 = \frac{1}{2}n(n+1)$

Cor.: $(V, +, \cdot)$: v.s. over $\mathbb{F}$ with $\dim V < \infty$. W is a subspace of V. Then any basis for W can be extent to be a basis for V.

RK: This implies: $\exists$ a subspace $Q \subset V$ s.t. $V = W \oplus Q$.