Lezione 6

venerdì 26 marzo 2021 10:48

$(V,+,\cdot)$ spazio vettoriale su un campo K

Sia $S \subseteq V$ e $W = \mathcal{L}(S)$.

Ci siamo chiesti se è possibile ricavare da S un sistema di generatori di W che sia anche linearmente indipendente, ossia una base di W.

Questa domanda ha risposta affermativa se S è finito.

Teorema di ESTRAZIONE di una BASE (da un sistema di generatori).

$S \subseteq V$, $W = \mathcal{L}(S)$, $|S| = m$

Esiste una base di W contenuta in S.

DIM. La dimostrazione è costruttiva e dà quindi luogo ad un algoritmo

$S = \{u_1, \dots, u_m\}$

Se S è linearmente indipendente, allora S è la base cercata.
Altrimenti può accadere $\underline{0} \in S$ e poniamo $S' = S \setminus \{\underline{0}\}$

oppure $\underline{0} \notin S$ ma per il teorema della lezione precedente esiste un vettore u di S tale che $W = \mathcal{L}(S) = \mathcal{L}(S \setminus \{u\})$ e quindi poniamo $S' = S \setminus \{u\}$. Per esempio $u = u_m$.

Se S' è linearmente indipendente, allora S' è la base di W cercata
Altrimenti applichiamo ad S' lo stesso ragionamento fatto su S:

per il teorema precedente, esiste $v \in S'$: $W = \mathcal{L}(S') = \mathcal{L}(S' \setminus \{v\})$

e procediamo così fino a quando troviamo un sottoinsieme di S che è sistema di generatori di W lin. indip.

<u>Esempio</u>: $\mathbb{R}^3$ Verificare che il seguente sottoinsieme di $\mathbb{R}^3$ è un sottospazio vettoriale di $\mathbb{R}^3$ e determinarne una base:

$$X = \{\alpha(1,0,1) + \beta(1,1,1) + \gamma(0,1,0) + 1(1,-1,1) \mid \alpha,\beta,\gamma \in \mathbb{R}\} \subseteq \mathcal{L}((1,0,1),(1,1,1),(0,1,0),(1,-1,1))$$

$u, v \in V \Rightarrow \exists\, \alpha,\beta,\gamma \in \mathbb{R}$: $u = \alpha(1,0,1) + \beta(1,1,1) + \gamma(0,1,0) + (1,-1,1)$ $+$

$\exists\, \alpha',\beta',\gamma' \in \mathbb{R}$: $v = \alpha'(1,0,1) + \beta'(1,1,1) + \gamma'(0,1,0) + (1,-1,1)$

$X \neq \emptyset$

$(1,-1,1) \in X$

$$u+v = (\alpha+\alpha')(1,0,1) + (\beta+\beta')(1,1,1) + (\gamma+\gamma')(0,1,0) + 2(1,-1,1) =$$

$$= (\alpha+\alpha'+\beta+\beta'+2,\ \beta+\beta'+\gamma+\gamma'-2,\ \alpha+\alpha'+\beta+\beta'+2) \ \underline{\in X}\ ?$$

$\in X \iff \exists\, a,b,c \in \mathbb{R}$:

$$(\alpha+\alpha'+\beta+\beta'+2,\ \beta+\beta'+\gamma+\gamma'-2,\ \alpha+\alpha'+\beta+\beta'+2) = a(1,0,1) + b(1,1,1) + c(0,1,0) + 1(1,-1,1) =$$

$$(a+b+1,\ b+c-1,\ a+b+1) \iff$$

$$\iff \begin{cases} \alpha+\alpha'+\beta+\beta'+2 = a+b+1 \\ \beta+\beta'+\gamma+\gamma'-2 = b+c-1 \\ \alpha+\alpha'+\beta+\beta'+2 = a+b+1 \end{cases} \qquad \begin{cases} a = \alpha+\alpha'+\beta+\beta'+\underline{2-b-1} \\ c = \beta+\beta'+\gamma+\gamma'-2-b+1 \end{cases}$$

$$\Longleftrightarrow \begin{cases} \alpha+\alpha'+\beta+\beta'+2 = a+b+1 \\ \beta+\beta'+\gamma+\gamma'-2 = b+c-1 \\ \alpha+\alpha'+\beta+\beta'+2 = a+b+1 \end{cases} \qquad \begin{cases} a = \alpha+\alpha'+\beta+\beta'+\underline{2-b-1} \\ c = \beta+\beta'+\gamma+\gamma'-2-b+1 \end{cases}$$

Proviamo a porre $b=1$: $\begin{cases} a = \alpha+\alpha'+\beta+\beta' \\ c = \beta+\beta'+\gamma+\gamma'-2 \end{cases}$

Quindi X è sottosp. vett. di $\mathbb{R}^3$

Si può vedere che X è chiuso anche rispetto alla moltiplicazione.

Vediamo se $(1,-1,1)$ si può esprimere come comb. lineare degli altri vettori:

$$(1,-1,1) = \underline{\alpha_1}(1,0,1) + \alpha_2(1,1,1) + \underline{\alpha_3}(0,1,0) = (\alpha_1+\alpha_2, \alpha_2+\alpha_3, \alpha_1+\alpha_2) \Longleftrightarrow$$

$$\Longleftrightarrow \begin{cases} 1 = \alpha_1+\alpha_2 \\ -1 = \alpha_2+\alpha_3 \\ 1 = \alpha_1+\alpha_2 \end{cases} \qquad \begin{cases} \alpha_1 = 1-\alpha_2 \\ \alpha_3 = -1-\alpha_2 \end{cases} \qquad \text{quindi:}$$

$$\forall \alpha_2 \in \mathbb{R}, \quad (1,-1,1) = (1-\alpha_2)(1,0,1) + \alpha_2(1,1,1) + (-1-\alpha_2)(0,1,0)$$

Dal ragionamento su $u+v$, vediamo che $\underline{0} \in X$ e quindi i vettori $(1,0,1), (1,1,1), (0,1,0), (1,-1,1)$ sono lin. dip. e quindi c'è un vettore che si può esprimere con comb. lineare degli altri. Noi abbiamo trovato che $(1,-1,1)$ è uno di questi vettori. Possiamo scrivere:

$\alpha_2 = 1$: $\quad (1,-1,1) = 0\,(1,0,1) + 1\,(1,1,1) + (-2)(0,1,0)$

$$X = \{\alpha(1,0,1) + \beta(1,1,1) + \gamma(0,1,0) + \overbrace{1(1,1,1) + (-2)(0,1,0)}^{(1,-1,1)=} \mid \alpha,\beta,\gamma \in \mathbb{R}\} =$$

$$\alpha(1,0,1) + (\beta+1)(1,1,1) + (\gamma-2)(0,1,0)$$
$$\alpha = h,\quad \beta+1 = k,\quad \gamma-2 = j$$

$$= \{h(1,0,1) + k(1,1,1) + j(0,1,0) \mid h,k,j \in \mathbb{R}\} = \mathcal{L}((1,0,1),(1,1,1),(0,1,0))$$

X è sottosp. vett. e $X = \mathcal{L}(S)$ con $S = \{(1,0,1),(1,1,1),(0,1,0)\}$

? S è lin. indip.? No, perché $(1,1,1) = (1,0,1) + (0,1,0)$ e per il teorema della lezione precedente:

$$\mathcal{L}(S) = \mathcal{L}(S \setminus \{(1,1,1)\})$$

Allora poniamo $S' = S \setminus \{(1,1,1)\} = \{(1,0,1),(0,1,0)\}$ che è lin. indip.

Quindi S' è la base di X cercata.

__Esempio__: $\mathbb{R}^2$ $\quad S = \{\underline{0}, (1,1), (2,3), (0,1)\}$ $\quad W = \mathcal{L}(S)$.

$\underline{0} \in S$. Allora $S' = S \setminus \{\underline{0}\} = \{(1,1),(2,3),(0,1)\}$ e $W = \mathcal{L}(S')$

S' è lin. indip? NO $\quad (2,3) = 2(1,1) + (0,1)$

Allora: $S'' = S' \setminus \{(2,3)\} = \{(1,1),(0,1)\}$ è lin. indip.

Quindi S'' è la base di W cercata.

Esempio $\mathbb{R}^2$ $\quad T = \{(1,0)\}$ è linearm. indip.

Esempio $\mathbb{R}^2$ $T=\{(1,0)\}$ è linearm. indip.

$(0,1) \notin \mathcal{L}(T)$ $T\cup\{(0,1)\}$ è lin. indip.

$\{(1,0),(0,1)\}$ è base di $\mathbb{R}^2$

<u>Lemma</u> (importante): $(V,+,\cdot)$, $S=\{u_1,\dots,u_n\}\subseteq V$

Supponiamo che S è lin. indip.

Se $u\in V$ tale che $u\notin\mathcal{L}(S)$, allora $S\cup\{u\}$ è lin. indip.

<u>DIM</u> p.a. $S\cup\{u\}=\{u_1,\dots,u_n,u\}$ lin. dipendente.

Allora, per definizione, esistono degli scalari $\alpha_1,\dots,\alpha_n,\alpha\in K$ NON TUTTI NULLI tali che: $\underline{0}=\alpha_1u_1+\dots+\alpha_nu_n+\alpha u$

non può accadere che sia $\alpha=0$, altrimenti: $\underline{0}=\alpha_1u_1+\dots+\alpha_nu_n$ con SCALARI NON TUTTI NULLI

e questo è impossibile perché $S=\{u_1,\dots,u_n\}$ è lin. indip.

Allora: $\alpha\neq0$. Quindi, $\exists\,\alpha^{-1}\in K$:

$$\underline{0}=\alpha^{-1}\underline{0}=\alpha^{-1}(\alpha_1u_1+\dots+\alpha_nu_n+\alpha u)=$$
$$=\alpha^{-1}(\alpha_1u_1)+\dots+\alpha^{-1}(\alpha_nu_n)+\alpha^{-1}(\alpha u)=$$
$$=(\alpha^{-1}\alpha_1)u_1+\dots+(\alpha^{-1}\alpha_n)u_n+\underbrace{(\alpha^{-1}\alpha)}_{=1}u \implies$$

$$\implies -(\alpha^{-1}\alpha_1)u_1+\dots-(\alpha^{-1}\alpha_n)u_n=u \in\mathcal{L}(u_1,\dots,u_n)=\mathcal{L}(S) \rightsquigarrow \text{ASSURDO}$$

Esempio: $\mathbb{R}^3$ $S=\{(1,1,0)\}$ è lin. indip.

$u\notin\mathcal{L}(S)=\{\alpha(1,1,0)\mid\alpha\in\mathbb{R}\}$. Per esempio, $u=(0,0,1)$

Per il Lemma precedente: $T=S\cup\{(0,0,1)\}=\{(1,1,0),(0,0,1)\}$ è lin. indip.

$w\notin\mathcal{L}(T)=\{\underbrace{\alpha(1,1,0)+\beta(0,0,1)}_{=(\alpha,\alpha,\beta)}\mid\alpha,\beta\in\mathbb{R}\}\not\ni(1,0,1)$

Per esempio $w=(1,0,1)$ e per il Lemma precedente

$U=T\cup\{(1,0,1)\}$ è lin indip.

Possiamo continuare o è impossibile? Oppure U è una base di $\mathbb{R}^3$?

Lemma di Steinitz: $(V,+,\cdot)$ su K

Sia W un sottosp. vett. di V f.g. con sistema di generatori $S=\{u_1,\dots,u_n\}$.

Se $X=\{v_1,\dots,v_m\}\subseteq W$ con $m>n$, allora X è lin. dipendente.

DIM. lezione prossima.

Tornando all'esempio precedente, sappiamo che $B = \{(1,0,0),(0,1,0),(0,0,1)\}$ è un sist. di gen. di $\mathbb{R}^3$ per cui:

$$\forall z \in \mathbb{R}^3 \setminus U, \quad |U \cup \{z\}| = 4 > |B|, \text{ e quindi } U \cup \{z\} \text{ è lin. dip.}$$

<u>Corollario</u>: $(V,+,\cdot)$ f.g. e sia $S = \{u_1, \dots, u_m\}$ sist. di gen. di V:
(**) $V = \mathcal{L}(S)$.

Se $T = \{w_1, \dots, w_h\} \subseteq V$ è lin. indip., allora $h \leq m$.

DIM. Se $h > m$, allora T sarebbe lin. dip. per il Lemma di Steinitz e questo è assurdo.

Esempio $\mathbb{R}[x]_{\leq 3}$ $\quad S = \{1, x, x^2, x^3\}$ è un sist. di gen. di $\mathbb{R}[x]_{\leq 3}$
$|S| = 4$

Allora <u>ogni</u> sottoinsieme lin. indip. di $\mathbb{R}[x]_{\leq 3}$ ha al più 4 vettori.

Teorema di equipotenza delle basi:

Sia $(V,+,\cdot)$ uno sp. vett. f.g. su un campo K.
Allora tutte le basi di V sono finite e hanno la stessa cardinalità.

<u>DIM</u>. V è f.g. per cui ha almeno un sistema di generatori finito S: $V = \mathcal{L}(S)$.
Per il Teorema di estrazione di una base, esiste una base B di V contenuta in S. Quindi B è una base finita: $m = |B|$.
Sia B' un'altra base di V. Siccome B' è lin. indip., ogni suo sottoinsieme finito è lin. indip. e per il Corollario (**) ha al più m vettori: $|B'| \leq m = |B|$
Scambiamo il ruolo di B e B', per cui $|B| \leq |B'|$.
Da cui $|B| = |B'|$. $\square$

Def. Sia $(V,+,\cdot)$ uno sp. vett. f.g.. La cardinalità di una qualsiasi base di V è detta dimensione di V.

Esempi:

K^n una base è $\{(1,0,\dots),(0,1,\dots),\dots,(0,\dots,1)\}$ detta base canonica
$\dim(K^n) = n$

$K[x]_{\leq h}$ $\quad \dim(K[x]_{\leq h}) = h+1 \quad \{1, x, \dots, x^h\}$ base canonica

$M_{m \times n}(K)$ $\quad \left\{ \begin{pmatrix} 1 & 0 & \cdots \\ 0 & \cdots & \end{pmatrix}, \begin{pmatrix} 0 & 1 & \cdots \\ \cdots & & \end{pmatrix}, \dots, \begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 1 \end{pmatrix} \right\}$ base canonica

$$\dim(M_{m \times n}(K)) = mn.$$

<u>Proposizione</u>. $(V,+,\cdot)$ su K $\quad \dim V = n$
$S = \{u_1, \dots, u_m\} \subseteq V$ $\quad |S| = n$

- S è lin. indip. $\Rightarrow$ S è base di V
- S è sist. di gen. $\Rightarrow$ S è base di V

<u>DIM</u>: • S è lin. indip. per ipotesi:

p.a. S non è base, e quindi non è un sist. di gen. di V:

$\mathcal{L}(S) \subsetneq V$. Allora $\exists\, u \in V : u \notin \mathcal{L}(S)$;

quindi per il Lemma importante:

$S \cup \{u\}$ è lin. indip.

con $|S \cup \{u\}| = n+1 > \dim V$

Ma questo è assurdo per il Corollario $(**)$

• S è un sist. di gen per ipotesi.

p.a. S non è base, e quindi non è lin. indip e per il Teorema di estrazione di una base contiene propriamente una base:

$\exists\, B \subsetneq S$: B è base di V

$\Downarrow$

$|B| = k < n = |S| = \dim V$ $\rightsquigarrow$ assurdo. $\square$

Durante la prossima lezione dimostreremo il lemma di Steinitz e parleremo di un'altra importante conseguenza:

Teorema di completamento in una base:

$(V, +, \cdot)$ su $\mathbb{K}$, $\dim V = n$.

Sia $S = \{u_1, \dots, u_t\} \subseteq V$ lin. indip.

Se $t = |S| < n$, allora esiste $X = \{u_{t+1}, \dots, u_n\} \subseteq V$, $|X| = n-t$,

tale che $S \cup X$ è base di V.