Indipendenza lineare - basi - dimensione

Sia V un $\mathbf{K}$-spazio e $X \subset V$ un sottoinsieme non vuoto.

Diciamo che i vettori di X sono **linearmente indipendenti** se la combinazione lineare con supporto vuoto, cioè con tutti i coefficienti uguali a zero, è l'unica combinazione lineare di elementi di X che rappresenti $0 \in V$ come un elemento di span(X).

Se X è fatto di vettori indipendenti, lo stesso vale per ogni sottoinsieme non-vuoto $Y \subset X$.

I vettori dell'insieme X **non** sono linearmente indipendenti se esiste una combinazione lineare che esprime $0 \in V$

$0 = \sum_{x \in X} a_x x$

ed esiste $x_0 \in X$ tale che $a_{x_0} \neq 0$.

Questo succede se e solo se esiste $x_0 \in X$ tale che $x_0 \in \text{span}(X \setminus \{x_0\})$:

$x_0 = \sum_{x \neq x_0} -(a_x a_{x_0}^{-1}) x$

...

Esempi. $X = \{E(i,j)\} \subset M(m,n,\mathbf{K})$ è formato da matrici linearmente indipendenti. In particolare questo vale per

$X = \{E^1, \ldots, E^n\} \subset \mathbf{K}^n$. Verifichiamolo in questo caso

$X = x_1E^1 + \cdots + x_nE^n = 0$ se e solo se $x_j = 0$ per ogni $j = 1, \ldots, n$

L'insieme numerabile dei monomi

$\{1 = t^0, t, t^2, \ldots, t^k, \ldots\} \subset \mathbf{K}[t]$

è formato da polinomi linearmente indipendenti. I coefficienti di $p(t) = a_0t^0 + \ldots a_kt^k$ sono i coefficienti di una combinazione lineare di quei monomi; se rappresenta in polinomio nullo allora gli a_j sono tutti nulli.

Un sottoinsieme $X \subset V$ è detto una **base di** V (base **ordinata** se X è munito di un ordinamento totale), se soddisfa le seguenti proprietà:

(1) $V = \text{span}(X)$ (X genera V)

(2) X è formato da vettori linearmente indipendenti.

Negli esempi precedenti abbiamo esempi di basi ordinate, prendendo: per le matrici, l' ordinamento lessicografico degli indici; per i monomi, l' ordinamento secondo il grado.

Per questi esempi, queste sono dette le **basi canoniche, standard** dei rispettivi spazi. In particolare $\{E^1, \ldots, E^n\}$ è la base canonica di $\mathbf{K}^n$.

Se X è una base di V, per ogni $v \in V$ esiste un' **unica** *combinazione lineare di elementi di X che esprima il vettore v.*

Dim. Esiste perché X genera V. Per l'unicità,

$v = \sum_x a_x x = \sum_x b_x x$, $0 = \sum_x (a_x - b_x)x$,

$a_x - b_x = 0$, $a_x = b_x$ per ogni x, perchè gli elementi di X sono linearmente indipendenti.

$\blacksquare$

V $\mathbf{K}$-spazio.

Sia $Y = \{y_1, \ldots, y_n\}$ un sottoinsieme finito e ordinato di V. I vettori di Y non sono linearmente indipendenti se e solo se esiste $1 \leq j \leq n$ tale che y_j è combinazione lineare dei vettori di Y che lo precedono.

Dim. Se $y_j = \sum_{i<j} a_i y_i$ allora

$$y_j - \sum_{i<j} a_i y_i = 0$$

senza avere tutti i coefficienti nulli.

Viceversa, se $\sum_{i=1}^{n} a_i y_i = 0$ senza avere tutti i coefficienti nulli, sia j il massimo indice tale che $a_j \neq 0$. Allora

$$y_j = \sum_{i<j} -(a_i a_j^{-1}) y_i$$

$\blacksquare$

Costruzione di basi per gli spazi finitamente generati.

V $\mathbf{K}$-spazio finitamente generato.

Conveniamo di considerare solo *basi ordinate* di V.

Sia $X = \{x_1, \ldots, x_n\}$ un insieme **finito e ordinato** che genera V. Supponiamo anche che ogni $x_i \neq 0$.

Vogliamo mostrare che eliminando, se necessario e in modo costruttivo, alcuni elementi di X, l'insieme rimanente con l'ordinamento indotto è una base (ordinata) di V.

Algoritmo di estrazione di una base

Sia $X = \{x_1, \ldots, x_n\}$ come sopra.

Conveniamo che ogni sottoinsieme di X erediti da X l' ordinamento indotto.

Prima descriviamo qualitativamente l'algoritmo, poi lo espliciteremo.

Uno *stato* di X è della forma $\{T|Y\}$, dove $\{T, Y\}$ è un sottoinsieme di X (con l'ordinamento indotto); la barra di separazione corrisponde ad un ruolo diverso dei due sottoinsiemi T e Y. Per esempio, se $X = \{x_1, x_2, x_3, x_4, x_5\}$, $\{x_1|x_4, x_5\}$ è uno stato di X.

L'algoritmo esegue successivamente un numero finito di passi, $p_1, \ldots, p_k$.

Ogni passo p_j ha uno *stato iniziale* $\{T_j | Y_j\}$ e uno *stato finale* $\{T_{j+1} | Y_{j+1}\}$ che è anche lo stato iniziale di p_{j+1}.

Y_{j+1} è **strettamente contenuto** in Y_j, mentre T_{j+1} contiene T_j (non necessariamente strettamente).

L'algoritmo si arresta al passo p_k per il quale $Y_k \neq \emptyset$, mentre $Y_{k+1} = \emptyset$. Cioè lo stato finale di p_k è $\{T_{k+1} | \emptyset\}$.

T_{k+1} sarà la base (ordinata) estratta dall'insieme X.

T_j va pensato come il sottonsieme di X dei vettori **già selezionati** nei passi precedenti; T_{j+1} quello dei selezionati dopo il passo p_j.

Veniamo alla costruzione dell'algoritmo di estrazione.

Passo iniziale :

$\{T_1|Y_1\} = \{x_1|x_2, \dots, x_n\}$

Test 1: Esiste $\lambda \in \mathbf{K}$ tale che $x_2 = \lambda x_1$?

Se "SI", allora $\{T_2|Y_2\} = \{x_1|x_3, \dots, x_n\}$;

Se "NO", allora $\{T_2|Y_2\} = \{x_1, x_2|x_3, \dots, x_n\}$.

Procediamo per induzione.

Supponiamo di avere eseguito il passo p_{j-1}, per cui $\{T_j|Y_j\}$ è lo stato iniziale del passo p_j.

Test j: Sia $\bar{x}(j)$ il più piccolo elemento di Y_j, cioè lo stato iniziale di p_j è della forma $\{T_j|\bar{x}(j),\dots\}$. Ci chiediamo: $\bar{x}(j) \in \mathrm{Comb}(T_j)$?

Se "SI", allora $T_{j+1} = T_j$ mentre Y_{j+1} si ottiene da Y_j eliminando $\bar{x}(j)$;

Se "NO", allora T_{j+1} si ottiene aggiungendo $\bar{x}(j)$ a T_j, mentre Y_{j+1} si ottiene da Y_j eliminando $\bar{x}(j)$ (in pratica, semplicemente si sposta la barra di un passo verso destra).

Resta da dimostrare che eseguendo l'algoritmo, T_{k+1}, ottenuto quando si arresta, è effettivamente una base di V.

Dimostriamo per induzione sul numero di passi che T_{k+1} genera V. Poiché X genera V per ipotesi, basta dimostrare, per ogni j, che se gli elementi dello stato iniziale di p_j generano V (dimenticando la barra di divisione), allora anche gli elementi dello stato finale di p_j generano V.

Se la risposta al Test j è NO, cambia la posizione della barra ma non cambia l'insieme degli elementi dei due stati.

Se la risposta al Test j è SI, se esprimiamo v come una combinazione lineare degli elementi di $\{T_j, Y_j\}$, sostituendo $\bar{x}(i)$ con una sua espressione come combinazione lineare degli elementi di T_j, otteniamo una espressione di v come combinazione lineare degli elementi dello stato finale.

Infine, supponiamo per assurdo che gli elementi di T_{k+1} non siano linearmente indipendenti. Ci sarebbe allora il più piccolo elemento di T_{k+1} che si può esprimere come combinazione lineare degli elementi che lo precedono. Ma allora l'esecuzione dell'algoritmo avrebbe eliminato tale elemento. Assurdo.

$\blacksquare$

Algoritmo di completamento ad una base.

Sia $X = \{x_1, \ldots, x_n\}$ un insieme finito ordinato che genera V come prima.

Sia $Z = \{z_1, \ldots, z_k\}$ un insieme finito e ordinato di vettori linearmente indipendenti di V. Vogliamo dimostrare che aggiungendo, se necessario e in modo costruttivo, un po' di vettori di X, si può estendere Z ad una base di V.

Consideriamo l'insieme ordinato $X' := \{Z, X\}$, Esso genera V perché contiene X che già genera. Applichiamo ad X' l' algoritmo di estrazione di una base. Poiché gli elementi di Z sono linearmente indipendenti, essi vengono conservati durante l'esecuzione dell'algoritmo, per cui la base estratta alla fine sarà della forma $\{Z, X''\}$, $X'' \subset X$, come voluto.

La dimensione di uno spazio finitamente generato.

Se $X = \{x_1, \ldots, x_n\}$ *genera* V *e* $Z = \{z_1, \ldots, z_k\} \subset V$ *è formato da vettori linearmente indipendenti, allora* $n \geq k$

Corollario. *Una base di uno spazio finitamente generato* V *è finita. Se* B *e* B' *sono due basi (necessariamente finite) di* V*, allora hanno lo stesso numero di elementi. Questo numero è un carattere intrinseco dello spazio* V *ed è detto la sua* **dimensione***:* $\dim V$.

Dimostriamo intanto il corollario. Una base di V è finita perché il suo numero di elementi non può eccedere quello di un insieme generatore finito che esiste per ipotesi.

Siano m e m' il numero di elementi di B e di B' rispettivamente. Siccome ogni base genera ed è linearmente indipendente, applicando due volte la proposizione, scambiando i ruoli, abbiamo $m \leq m'$, $m' \leq m$.

$\blacksquare$

Dimostriamo ora la proposizione.

L'insieme $\{z_1, X\}$ genera e non è linearmente indipendente perché X genera. Applichiamo parzialmente l'algoritmo di estrazione; sicuramente z_1 viene conservato e ci fermiamo nel momento in cui viene eliminato un elemento di X. Otteniamo $\{z_1, X_1\}$ che genera. Consideriamo $\{z_1, z_2, X_1\}$. Operando come prima otteniamo $\{z_1, z_2, X_2\}$. Iteriamo aggiungendo uno z_j (ed eliminando uno $x_{i(j)}$) alla volta, fino a che è possibile. Ci sono, a priori, due possibilità:

1) Riusciamo ad inserire tutti gli z_j, ottenendo $\{z_1, \ldots, z_k, X_k\}$ dove X_k è ottenuto eliminando k elementi di X. Quindi $n \geq k$.

2) Esauriamo gli elementi di X avendo inserito solo $z_1, \ldots z_h$, $h < k$. Ma questo è impossibile. Infatti poiché $\{z_1, \ldots, z_h\}$ genererebbero, z_{h+1} sarebbe combinazione lineare degli z_j che lo precedono, contro il fatto che i vettori di Z sono linearmente indipendenti.

$\blacksquare$

$\dim V = n$, W *sottospazio di* V, *allora* W *è finitamente generato e* $\dim W \leq \dim V$*.*

$\dim W = \dim V$ *se e solo se* $W = V$*.*

Dim. Se $W = \{0\}$ tutto è evidente. Se $w_1 \in W$ non genera W, esite $w_2 \in W$ tale che w_1, w_2 sono linearmente indipendenti (in W quindi in V). Se non generano, troviamo in W w_1, w_2, w_3 linearmente indipendenti. Questo procedimento può essere iterato al più $\dim V$ - volte. Quindi W è finitamente generato e $\dim W \leq \dim V$.

Se $\dim W = \dim V = n$, sia $\{w_1, \ldots, w_n\}$ una base di W. Se non fosse una base di V, esisterebbe $v_{n+1} \in V$ tale che $\{w_1, \ldots w_n, v_{n+1}\}$ sono linearmente indipendenti, quindi sarebbe $\dim V \geq n + 1$. Assurdo.

■

Due $\mathbf{K}$*-spazi* V*,* W *finitamente generati sono isomorfi se e solo se* $\dim V = \dim W$*.*

Dim. Sia $f : V \to W$ un isomorfismo.

Sia $B = \{v_1, \ldots, v_n\}$ una base di V (per cui $\dim V = n$).

Affermiamo che

$f(B) := \{w_1 = f(v_1), \ldots, w_n = f(v_n)\}$ è una base di W (quindi $\dim W = n$).

Poichè f è surgettiva, per ogni $w \in W$, esiste $v \in V$, $f(v) = w$.

$v = \sum_j a_j v_j$, allora $w = \sum_j a_j w_j$, quindi $f(B)$ genera W.

Se $\sum_j a_j w_j = 0$, allora $f(\sum_j a_j v_j) = 0$, $\sum_j a_j v_j \in \ker f = \{0\}$, perché f è iniettiva. Dunque $a_j = 0$ per ogni j, perché i v_j sono linearmente indipendenti.

Mostriamo ora l'altra implicazione.

Se $\dim V = \dim W = n$, siano $B = \{v_1, \ldots, v_n\}$, $D = \{w_1, \ldots, w_n\}$ basi di V e W rispettivamente.

Ogni $v \in V$ si esprime in modo unico nella forma $v = \sum_j a_j v_j$.

Definiamo $f : V \to W, f(v) = \sum_j a_j w_j$.

f è un isomorfismo. Lasciamo per esercizio la verifica che sia lineare.

$\ker f = \{0\}$, infatti se $0 = f(v) = \sum_j a_j w_j$, allora tutti gli a_j sono nulli perché i vettori di D sono linearmente indipendenti.

Se $w = \sum_j a_j w_j$ allora $w = f(\sum_j a_j v_j) \in \mathrm{Im}(f)$.

■

Segue dalla discussione precedente che:

se $\dim V = n$, $f : V \to W$ è lineare, allora $\mathrm{Im}(f)$ è finitamente generata e $\dim \mathrm{Im}(f) \leq n$.

Se $\{v_1, \ldots, v_n\}$ è una base di V, $\{w_1, \ldots, w_n\}$ è un sottoinsieme di W, allora esiste ed è unica $f : V \to W$ lineare tale che

$f(v_j) = w_j$, $j = 1, \ldots n$.

Inoltre $\mathrm{Im}(f) = \mathrm{span}\{w_1, \ldots, w_n\}$.

Possiamo riassumere quanto visto dicendo che $f : V \to W$ lineare è un isomorfismo se e solo, comunque si fissi una base di V, essa viene inviata da f in una base di W.

Come caso particolare abbiamo che

$A \in \text{End}(\mathbf{K}^n) = M(n, \mathbf{K})$ è invertibile, cioè $A \in GL(n, \mathbf{K})$, se e solo se le colonne di A sono linearmente indipendenti.

Sia $\dim V = n$, fissiamo una base B di V.

Consideriamo $\mathbf{K}^n$ lo spazio standard di dimensione n, con la base canonica $C = \{E^1, \ldots, E^n\}$.

Applichiamo la costruzione precedente dell' isomorfismo f sostituendo (W, D) con $(\mathbf{K}^n, C)$. Otteniamo l'isomorfismo

$[*]_B : V \to \mathbf{K}^n$

per ogni $v = \sum_j a_j v_j$ (in modo unico),

$[v]_B = (a_1, a_2, \ldots, a_n)^t$.

Queste sono dette le **coordinate del vettore** v **rispetto alla base** B. L'isomorfismo è detto **isomorfismo di passaggio alle coordinate rispetto alla base** B.

V, W $\mathbf{K}$-spazi, $\dim V = n$, $\dim W = m$,

$B = \{v_1, \ldots, v_n\}$ una base di V,

$D = \{w_1, \ldots, w_m\}$ una base di W,

$f \in \mathrm{Hom}(V, W)$.

Allora

$[*]_D \circ f \circ [*]_B^{-1} \in \mathrm{Hom}(\mathbf{K}^n, \mathbf{K}^m) = M(m, n, \mathbf{K})$

Questa matrice $m \times n$ viene indicata con $M_D^B(f)$ e, per definizione, soddisfa la seguente proprietà:

Per ogni $v \in V$, $[f(v)]_D = M_D^B(f)[v]_B$.

$M_D^B(f) = ([f(v_1)]_D, \ldots, [f(v_n)]_D)$.

È detta la **matrice associata ad f (o che rappresenta f) rispetto alle basi B, D.**

Abbiamo così definito l'applicazione

$M^B_D(*) : \mathrm{Hom}(V, W) \to M(m, n, \mathbf{K})$

È un isomorfismo di $\mathbf{K}$-spazi vettoriali. La verifica è lasciata per esercizio.

Cambiamenti di base.

Domande: Date due basi B e B' di V, per ogni $v \in V$, come sono correlate le coordinate $[v]_B$ e $[v]_{B'}$?

Date basi B e B' di V, D e D' di W rispettivamente, come sono correlate le matrici $M_D^B(f)$ e $M_{D'}^{B'}(f)$?

Sia $M^B_{B'}(\mathrm{Id}_V) = ([v_1]_{B'}, \ldots, [v_n]_{B'})$. Allora, per ogni $v \in V$

$$[v]_{B'} = M^B_{B'}(\mathrm{Id}_V)[v]_B$$

Questo risponde alla prima domanda; la matrice $M^B_{B'}(\mathrm{Id}_V)$ è detta **matrice di cambiamento di base (o di coordinate)**.

$f = \mathsf{Id}_W \circ f \circ \mathsf{Id}_V$; quindi

$$M^{B'}_{D'}(f) = M^{D'}_{D}(\mathsf{Id}_W) M^{B}_{D}(f) M^{B}_{B'}(\mathsf{Id}_V)$$

Questo risponde alla seconda domanda.

$M_B^B(\mathsf{Id}_V) = I_n$;

$M_{B'}^B(\mathsf{Id}_V) M_B^{B'}(\mathsf{Id}_V) = M_B^{B'}(\mathsf{Id}_V) M_{B'}^B(\mathsf{Id}_V) = I_n$

Tutte le matrici di cambiamento di base sono invertibili (appartengono a $GL(n, \mathbf{K})$).

“Relatività”.

Sia $\dim V = n$, B una base di V, $A \in GL(n, \mathbf{K})$. $GL(n, \mathbf{K})$ è il gruppo delle trasformazioni (*automorfismi*) lineari di $\mathbf{K}^n$.

$M_B^B : GL(V) \to GL(n, \mathbf{K}),\ f \to M_B^B(f)$

è un isomorfismo di gruppi. In particolare esiste un unico automorfismo f di V tale che

$A = M_B^B(f)$.

Fatto: *Esistono uniche basi B' e B'' di V, tali che* $A = M_B^{B'}(\mathrm{Id}_V) = M_{B''}^{B}(\mathrm{Id}_V)$

Dunque, fissata una base B di V e assegnata una matrice invertibile A come sopra, possiamo interpretare A come la matrice di un automorfismo (trasformazione lineare) dello spazio V letto nel sistema di coordinate dato da B, **oppure** come una matrice di cambiamento di coordinate, essendo liberi di specificare il ruolo iniziale o finale della base B.

Quale è l'interpretazione "vera"? Lo spazio si "muove" (subisce una trasformazione) oppure "resta fermo" mentre cambiamo il sistema di coordinate con cui lo leggiamo?

Entrambe !

Dim (del Fatto). Consideriamo l'insieme di vettori di V, $B' = \{w_1, \ldots, w_n\}$ univocamente determinata dal fatto che $A = ([w_1]_B, \ldots, [w_n]_B)$. Se dimostriamo che B' è una base, abbiamo dimostrato il primo punto. Basta dimostrare che sono linearmente indipendenti.

Se $\sum_j a_j w_j = 0$, allora $\sum_j a_j [w_j]_B = 0$; quindi i coefficienti a_j sono tutti nulli perché le colonne della matrice invertibile A sono linearmente indipendenti. Per ottenere il secondo punto, basta applicare lo stesso argomento determinando l'unica base B'' per cui

$M_B^{B''}(\mathrm{Id}_V) = A^{-1}$.

■