Ogni spazio vettoriale ha una base

Pino Vigna Suria

29 11 2004

Il titolo di questa nota dice che, per ogni spazio vettoriale, esiste un suo sottoinsieme linearmente indipendente che lo genera.

Succinto ed eclatante.

Disgraziatamente entrambi i concetti coinvolti possono essere fuorvianti, addirittura per **ogni** studente di matematica: il motivo di questa ambiguità proviene dal fatto che il concetto di spazio vettoriale viene introdotto molto presto nei corsi universitari di contenuto matematico, e, a mio avviso molto ragionevolmente, nell'intento di non vessare le giovani menti con sottigliezze che non possono ancora essere apprezzate, gli insegnanti tendono a pescare un po' nel torbido sull'idea di indipendenza lineare e di generatore. Alcuni ne sono consapevoli.

In questa nota, fino ad avviso contrario, se $f : X \longrightarrow Y$ è una funzione, l'immagine di $x \in X$ verrà denotata con f_x.

Naturalmente nei primi corsi di algebra lineare ci si accontenta di spazi vettoriali finitamente generati, per cui è sufficiente specificare, per un sottoinsieme finito A di uno spazio vettoriale V,

- Cosa significa che A è linearmente indipendente.
- Cosa significa che A genera V.

Normalmente la cosa viene affrontata n questo modo:

Sia $A = \{v_1, \ldots, v_n\}$ un **sottoinsieme finito** di uno spazio vettoriale V sul campo $\mathbb{K}$:

- Si dice che A è *linearmente indipendente* se, per ogni $n-$**upla** di scalari $\lambda_1, \ldots, \lambda_n$, se $\sum_{i=1}^{n} \lambda_i v_n = 0$ allora $\lambda_i = 0, \forall i = 1, \ldots, n$.

- Si dice che A *genera* V se ogni elemento di V è combinazione lineare degli elementi di A, cioè, per ogni $v \in V$, esistono **degli** scalari $\lambda_1, \ldots, \lambda_n$ tali che $\sum_{i=1}^{n} \lambda_i v_n = v$.

  Le parole in grassetto hanno bisogno di un'analisi più profonda: per ogni numero naturale n poniamo $\overline{n} =: \{m \in \mathbb{N}$ tali che $1 \leq m \leq n\}$; dire che un insieme A è *finito* significa che esiste un numero naturale n ed una corrispondenza biunivoca $v : \overline{n} \longrightarrow A$, non che una tale corrispondenza biunivoca sia stata fissata, come si fa implicitamente, (e truffaldinamente) nella notazione usata sopra.

- Nessuno definisce cosa sia una $n-$upla di elementi di un insieme A; i più coscienziosi dichiarano che una *$n-$upla ordinata* di elementi di A è una funzione $v : \overline{n} \longrightarrow A$. E questo è corretto.

- La terza parola scritta in grassetto, quel "degli", balza all'occhio per la sua ambiguità.

Sistemare queste imprecisioni è straordinariamente semplice.

Sia $v = (v_1, \ldots, v_n)$ una $n-$upla ordinata di vettori (cioè di elementi di uno spazio vettoriale V):

- Si dice che v è *linearmente indipendente* se per ogni $n-$upla ordinata di scalari λ, se $\sum_{i=1}^{n} \lambda_i v_n = 0$ allora $\lambda_i = 0, \forall i = 1, \ldots, n$.

- Si dice che un vettore $w \in V$ è *combinazione lineare* di v se esiste una $n-$upla ordinata di scalari λ tale che $\sum_{i=1}^{n} \lambda_i v_n = w$.

La stesse formule, ma un ben più preciso significato; il simbolo di sommatoria ovviamente deve essere interpretato così: sia $f : \mathbb{N} \longrightarrow V$ una funzione, allora $\sum_{i=1}^{n} f_i$ è definito ricorsivamente mediante $\sum_{i=1}^{0} f_i = 0$ e $\sum_{i=1}^{n+1} f_i = \sum_{i=1}^{n} f_i + f_{n+1}$. Naturalmente ogni $n-$upla ordinata, di scalari o di vettori, può essere estesa, mediante 0, a una funzione definita su tutto $\mathbb{N}$, e si coprono tutti i casi.

Qualcuno, diciamo il signor Simplicio, potrà argomentare che queste sono inutili complicazioni di un concetto così semplice da non meritare alcuna riflessione; la sua convinzione non può che essere rafforzata dall'osservazione che segue: il fatto che una $n-$upla ordinata di vettori v generi V (rispettivamente sia linearmente indipendente) "non dipende dall' ordine in cui si presentano i suoi elementi", affermazione euristica che può facilmente essere precisata come segue: sia σ una permutazione di $\overline{n}$, cioè $\sigma : \overline{n} \longrightarrow \overline{n}$ è una corrispondenza biunivoca; se v è linearmente indipendente (genera V) allora anche $v \circ \sigma$ è linearmente indipendente (genera V).

Sembrerebbe proprio che i due predicati che stiamo discutendo siano in realtà attribuibili più a un insieme finito di vettori con n elementi piuttosto che a una $n-$upla ordinata; tuttavia c'è un argomento per mostrare che non è così: negli appunti di algebra lineare di Simplicio, poco dopo le sue definizioni, comparirà quasi certamente un'affermazione che suona pressapoco così: se in $\{v_1, \ldots, v_n\}$ c'è una ripetizione, allora tale insieme non è linearmente indipendente: il che ovviamente contrasta con la sua sbandierata convinzione che un insieme è completamente determinato dai suoi elementi, e quindi, in insiemistica, la parola ripetizione non significa nulla. Per metterla giù pesante, parlando ad esempio di $\mathbb{R}^2$, Simplicio, se coerente, deve ammettere che l'insieme di vettori $\{(1,1),(1,1),(1,1)\}$ è linearmente indipendente; e questo, si sa, provoca disastri inenarrabili. La scappatoia di non menzionare questo risultato ha le gambe corte: leggendo la continuazione degli appunti di Simplicio, troverete facilmente qualche punto in cui lo usa .

Naturalmente la versione purificata dello stesso risultato è perfettamente vera e dice solo che una $n-$upla ordinata linearmente indipendente è iniettiva.

Rigore è fatto, ad un prezzo irrisorio. Disgraziatamente l'eclatante risultato che appare nelle prime due righe di queste note parla di un **insieme** linearmente indipendente che genera il nostro spazio vettoriale.

Definizione 1. *Sia V uno spazio vettoriale e $A \subseteq V$; denotiamo con $\mathcal{L}(A)$ l'intersezione di tutti i sottospazi vettoriali di V che contengono A. Si dice che l'insieme A* genera *V se $\mathcal{L}(A) = V$.*

Anche se A non genera V è facile vedere che $\mathcal{L}(A)$ è il più piccolo sottospazio vettoriale di V che contiene A, cioè:

- $\mathcal{L}(A) \triangleleft V$, in quanto un'intersezione qualunque di sottospazi è un sottospazio.
- $A \subseteq \mathcal{L}(A)$.
- Se $W \triangleleft V$ e $A \subseteq W$ allora $\mathcal{L}(A) \subseteq W$.

In particolare se $B \subseteq A$ allora $\mathcal{L}(B) \triangleleft \mathcal{L}(A)$.

Usando questo piccolo risultato,le proprietà elencate sopra e quelle della somma di due sottospazi si vede, con facili ed eleganti giochetti, che

$\mathcal{L}(A \cup B) = \mathcal{L}(A) + \mathcal{L}(B)$; se $A = \{v\}$ è un singoletto scriveremo $\mathcal{L}(v)$ per $\mathcal{L}(\{v\})$. È immediato verificare che $\mathcal{L}(v) = \{\lambda v \text{ con } \lambda \in \mathbb{K}\}$.

Definizione 2. *Sia V uno spazio vettoriale e $A \subseteq V$; si dice che l'insieme A è* linearmente indipendente *se, per ogni sottoinsieme proprio $B \subsetneq A$, si ha che $\mathcal{L}(B) \subsetneq \mathcal{L}(A)$.*

Un'utile strumento per maneggiare l'ultimo concetto che abbiamo esposto è dato dal seguente

Lemma 1. *$A \subseteq V$ è linearmente indipendente se e solo se, per ogni $v \in A$, $v \notin \mathcal{L}(A - \{v\})$.*

Dimostrazione. $\Leftarrow$ Sia $B \subsetneq A$ e $v \in A - B$; allora $v \in \mathcal{L}(A)$ ma $v \notin \mathcal{L}(B) \subseteq \mathcal{L}(A - \{v\})$.

$\Rightarrow$ Se esiste $v \in A$ tale che $v \in \mathcal{L}(A - \{v\})$, allora $\mathcal{L}(v) \subseteq \mathcal{L}(A - \{v\})$ e quindi

$$\mathcal{L}(A) = \mathcal{L}(A - \{v\}) + \mathcal{L}(v) \subseteq \mathcal{L}(A - \{v\}) + \mathcal{L}(A - \{v\}) = \mathcal{L}(A - \{v\})$$

e A non è linearmente indipendente. $\square$

Corollario 1. *Se A è linearmente indipendente e $B \subseteq A$ allora anche B è linearmente indipendente.*

Dimostrazione. Sia, per assurdo, $v \in B$ tale che $v \in \mathcal{L}(B - \{v\})$; allora

$$v \in \mathcal{L}(B - \{v\}) + \mathcal{L}(A - B) = \mathcal{L}((A - B) \cup (B - \{v\})) = \mathcal{L}(A - \{v\})$$

e A non è linearmente indipendente. $\square$

Quindi un sottoinsieme di V linearmente indipendente può perdere la sua virtù aumentando, e un sottoinsieme che generi V rischia diminuendo. Il titolo di queste note dice che è sempre possibile trovare un compromesso.

Corollario 2. *Se A è linearmente indipendente e $v \notin \mathcal{L}(A)$ allora anche $A \cup \{v\}$ è linearmente indipendente.*

Dimostrazione. Supponiamo che $C \subseteq A \cup \{v\}$ soddisfi $\mathcal{L}(C) = \mathcal{L}(A \cup \{v\})$; se $v \notin C$ allora $C \subseteq A$ per cui $v \in \mathcal{L}(A \cup \{v\}) = \mathcal{L}(C) \subseteq \mathcal{L}(A)$, assurdo. Quindi, se poniamo, $C' = C - \{v\}$ avremo che $C' \subseteq A$. Inoltre $\mathcal{L}(A) \subseteq \mathcal{L}(C) = \mathcal{L}(C') + \mathcal{L}(v)$, per cui ogni $w \in \mathcal{L}(A)$ può essere scritto come $w = w' + \lambda v$, con $w' \in \mathcal{L}(C')$ e $\lambda \in \mathbb{K}$; se $\lambda \neq 0$ allora $v = \lambda^{-1}w - \lambda^{-1}w' \in \mathcal{L}(A) + \mathcal{L}(C') = \mathcal{L}(A)$, assurdo; quindi deve essere $w \in \mathcal{L}(C')$. Abbiamo dunque provato che $\mathcal{L}(A) = \mathcal{L}(C')$; siccome A è linearmente indipendente ne segue che $C' = A$ e quindi $C = A \cup \{v\}$, che è quanto si doveva mostrare. $\square$

Infine ci serve una caratterizzazione di $\mathcal{L}(A)$.

Proposizione 1. *Sia $W = \{w \in V$ tali che $\exists n \in \mathbb{N},\ \exists v : \overline{n} \longrightarrow A,\ \exists \lambda : \overline{n} \longrightarrow \mathbb{K}$ tali che $w = \sum_{i=1}^{n} \lambda_i v_i\}$. Allora $\mathcal{L}(A) = W$.*

Dimostrazione. Basta provare che W è il più piccolo sottospazio vettoriale che contiene A; l'unica verifica che merita un commento è che W è chiuso rispetto alla somma: siano $v' = \sum_{i=1}^{n} \lambda_i v_i$ e $w' = \sum_{i=1}^{m} \mu_i w_i$, definiamo $\tau : \overline{n+m} \longrightarrow \mathbb{K}$ mediante $\tau_i = \lambda_i$ se $1 \leq i \leq n$ e $\tau_i = \mu_{i-n}$ se $n+1 \leq i \leq n+m$ e definiamo $u : \overline{n+m} \longrightarrow A$ mediante $u_i = v_i$ se $1 \leq i \leq n$ e $u_i = w_{i-n}$ se $n+1 \leq i \leq n+m$; così si ottiene $v' + w' = \sum_{i=1}^{n+m} \tau_i u_i$. $\square$

Abbiamo quanto ci serve per dimostrare che ogni spazio vettoriale ha una base

Teorema 1. *Sia V uno spazio vettoriale sul campo $\mathbb{K}$; esiste un sottoinsieme $A \subseteq V$ linearmente indipendente che genera V.*

Dimostrazione. Sia $\mathcal{X} = \{B \subseteq V$ tale che B è linearmente indipendente$\}$. Non è l'insieme vuoto perchè $\emptyset \in \mathcal{X}$. Ordiniamo $\mathcal{X}$ mediante l'inclusione. Otteniamo un insieme induttivo; sia infatti $\mathcal{C}$ una catena in $\mathcal{X}$ (vuol dire che $\mathcal{C}$ è totalmente ordinato). Affermo che $B = \bigcup_{C \in \mathcal{C}} C$ è ancora linearmente indipendente.

Usiamo il lemma 1: sia $v' \in B$, proveremo che $v' \notin \mathcal{L}(B - \{v'\})$. Esiste $D \in \mathcal{C}$ tale che $v' \in D$ e supponiamo per assurdo che $v' \in \mathcal{L}(B - \{v\})$ allora per la proposizione 1 esiste $n \in \mathbb{N}$, esiste $v : \overline{n} \longrightarrow B - \{v'\}$, esiste $\lambda : \overline{n} \longrightarrow \mathbb{K}$, tali che $v' = \sum_{i=1}^{n} \lambda_i v_i$; siccome $\mathcal{C}$ è una catena esiste $C \in \mathcal{C}$ tale che $v_i \in C,\ \forall i = 1, \ldots, n$; per lo stesso motivo avremo che $C \subseteq D$ o $D \subseteq C$; chiamiamo E il più grande dei due; facciamo il punto: abbiamo trovato $E \in \mathcal{C}$ tale che

- $v' \in E$
- $v : \overline{n} \longrightarrow E - \{v'\}$
- $v' = \sum_{i=1}^{n} \lambda_i v_i$

Cioè $v' \in \mathcal{L}(E - \{v'\})$ contraddicendo il fatto che E è linearmente indipendente. Dunque $B \in \mathcal{X}$ ed è un maggiorante di $\mathcal{C}$.

Per il lemma di Zorn $\mathcal{X}$ ha un elemento massimale A. Affermo che $\mathcal{L}(A) = V$, infatti, se $v \in V - \mathcal{L}(A)$ allora, , $A \cup \{v\}$ contiene A ed è linearmente indipendente per il corollario 2;impossibile perché A è massimale in $\mathcal{X}$. $\square$

La dimostrazione precedente può essere facilmente modificata per ottenere il seguente risultato: siano $C \subseteq B \subseteq V$ tali che C è linearmente indipendente e B genera V. Allora esiste una base A di V tale che $C \subseteq A \subseteq B$, da cui segue in particolare che ogni insieme linearmente indipendente può essere completato a base e ogni insieme di generatori può essere sfoltito a base, come per gli spazi vettoriali finitamente generati: basta infatti scegliere $\mathcal{X} = \{D \subseteq V$ tale che D è linearmente indipendente e $C \subseteq D \subseteq B\}$ e comportarsi esattamente come nella dimostrazione appena finita.