1. Dipendenza lineare e basi

Sia V uno spazio vettoriale sul campo K. Sia $\mathcal{F} = \{v_i\}_{i\in I}$ una famiglia di elementi di V. Una *combinazione lineare* di elementi di $\mathcal{F}$ è una somma $\sum_{i\in I} \alpha_i v_i$, dove i coefficienti α_i sono scalari, e tutti gli α_i, tranne al più un numero finito, sono nulli; si tratta dunque di una somma finita. Diremo che $\mathcal{F}$ è *linearmente dipendente*, o anche che i v_i sono linearmente dipendenti, se esiste una combinazione lineare di elementi di $\mathcal{F}$ che sia nulla, ma nella quale compaia qualche coefficiente non nullo. In caso contrario diremo che $\mathcal{F}$ è *linearmente indipendente*, o anche che i v_i sono linearmente indipendenti. Nel seguito ometteremo spesso la parola "linearmente" e scriveremo semplicemente "dipendente" o "indipendente".

Diremo che un elemento v di V è *linearmente dipendente da* $\mathcal{F}$ se esiste una combinazione lineare di elementi di $\mathcal{F}$ il cui valore sia v; in particolare, se ciò accade, $\mathcal{F} \cup \{v\}$ è linearmente dipendente. Viceversa, supponiamo che esista una combinazione lineare $\alpha v + \sum \alpha_i v_i$ di v e di elementi di $\mathcal{F}$ il cui valore sia zero, ma nella quali il coefficiente di v, cioè α, non sia nullo. Allora

$$v = -\sum_{i\in I} \frac{\alpha_i}{\alpha} v_i \,,$$

e dunque v è linearmente dipendente da $\mathcal{F}$. Se $\mathcal{F}$ è dipendente e $\mathcal{G} = \{v_j\}_{j\in J}$, dove $J \subset I$, è una sua sottofamiglia indipendente, allora esiste un indice $h \notin J$ tale che v_h sia linearmente dipendente da $\mathcal{F} - \{v_h\}$. Infatti le ipotesi dicono che esiste una relazione di dipendenza lineare $\sum \alpha_i v_i = 0$, ma che questa non può coinvolgere solo i v_i con $i \in J$, perchè questi sono indipendenti. In altre parole si deve avere che $\alpha_h \neq 0$ per qualche $h \notin J$.

La dipendenza lineare è transitiva, nel senso seguente. Se $\mathcal{G} = \{w_j\}_{j\in J}$ è una famiglia di elementi di V diremo che $\mathcal{G}$ è linearmente dipendente da $\mathcal{F}$ se ogni suo elemento è linearmente dipendente da $\mathcal{F}$. Allora, se v è dipendente da $\mathcal{G}$ e $\mathcal{G}$ è dipendente da $\mathcal{F}$, v è dipendente da $\mathcal{F}$. In effetti, se $v = \sum_j \beta_j w_j$ e $w_j = \sum_i \alpha_{ji} v_i$, si ha che

$$v = \sum_j \sum_i \beta_j \alpha_{ji} v_i = \sum_i \Big(\sum_j \beta_j \alpha_{ji} \Big) v_i \,.$$

Diremo che la famiglia $\mathcal{F}$ *genera* V, o che è un *sistema di generatori per* V se ogni elemento di V è combinazione lineare di elementi di $\mathcal{F}$. Più in generale possiamo notare che l'insieme delle combinazioni lineari di elementi di $\mathcal{F}$ è un sottospazio vettoriale di V, che viene chiamato il *sottospazio generato da* $\mathcal{F}$. In effetti la somma di due combinazioni lineari

$$\sum_{i\in I} \alpha_i v_i + \sum_{i\in I} \beta_i v_i = \sum_{i\in I} (\alpha_i + \beta_i) v_i$$

è anch'essa una combinazione lineare di elementi di $\mathcal{F}$, e lo stesso vale per un prodotto $k \sum \alpha_i v_i = \sum k \alpha_i v_i$, dove k è uno scalare. Diremo che V ha *dimensione finita* se ammette un sistema di generatori finito.

Diremo che la famiglia $\mathcal{F}$ è una *base* di V se è indipendente e genera V. Ogni spazio vettoriale possiede una base. La dimostrazione nel caso generale usa il lemma di Zorn;

più avanti mostreremo che si può evitare di ricorrere a questo lemma quando si ha a che fare con spazi vettoriali di dimensione finita. Sia dunque V uno spazio vettoriale, non necessariamente di dimensione finita, sia S un insieme di generatori di V (ad esempio V stesso), e sia T un sottoinsieme indipendente di S (ad esempio l'insieme vuoto). Indichiamo con X l'insieme dei sottoinsiemi indipendenti di S contenenti T, semiordinato per inclusione. Notiamo che X non è vuoto, perchè contiene almeno T. Ogni catena in X, cioè ogni sottoinsieme totalmente ordinato di X, ammette un maggiorante in X. In effetti, se $Y \subset X$ è una catena, $A = \cup Y$ appartiene a X. Per dimostrarlo osserviamo che, se A fosse dipendente, vi sarebbero $v_1, \ldots, v_n \in A$ e scalari non nulli $\alpha_1, \ldots, \alpha_n$ tali che $\sum \alpha_i v_i = 0$. Data la definizione di A, per ogni i vi è un $B_i \in Y$ tale che $v_i \in B_i$. Ma allora tutti i v_i appartengono al più grande tra i B_i, che esiste perchè Y è totalmente ordinato; questo B_i sarebbe dunque dipendente, contro ciò che si è supposto. L'insieme X soddisfa quindi le ipotesi del lemma di Zorn, e perciò contiene un elemento massimale B. Dico che B è una base di V. In effetti, sappiamo già che B è indipendente. La massimalità di B dice inoltre che, per ogni $s \in S$, l'insieme $\{s\} \cup B$ è dipendente; dunque S dipende da B. D'altra parte, V dipende da S e quindi, per la transitività della dipendenza lineare, B genera V. Quanto si è dimostrato può essere enunciato come segue.

Teorema (1.1). *Sia V uno spazio vettoriale, sia S un insieme di generatori di V, e sia T un sottoinsieme indipendente di S. Esiste una base di V contenuta in S e contenente T. In particolare, ogni sistema di generatori di V contiene una base, e ogni sottoinsieme indipendente di V è contenuto in una base.*

Due basi di uno stesso spazio vettoriale possiedono sempre lo stesso numero di elementi. Si può dare un senso preciso a questa affermazione anche quando le basi in questione sono insiemi infiniti, ma ci limiteremo al caso finito. Il risultato chiave è il seguente.

Teorema (1.2). *Sia V uno spazio vettoriale, siano $v_1, \ldots, v_n$ elementi indipendenti di V, e sia $\{w_1, \ldots, w_m\}$ un sistema di generatori di V. Allora $n \leq m$.*

La dimostrazione è semplice. Possiamo naturalmente supporre che $n \geq m$, e dobbiamo dimostrare che $n = m$. Poiché $\{w_1, \ldots, w_m\}$ genera V, $\{v_1, w_1, \ldots, w_m\}$ è dipendente e quindi esiste un j tale che w_j sia linearmente dipendente da $v_1, w_1, \ldots, w_{j-1}, w_{j+1}, \ldots, w_m$. Riordinando i w_i, se necessario, possiamo supporre che $j = 1$. Dunque w_1 dipende da $v_1, w_2, \ldots, w_m$. Ne segue che $v_1, w_2, \ldots, w_m$ generano V. Quindi $\{v_1, v_2, w_2, \ldots, w_m\}$ è dipendente. Poiché $\{v_1, v_2\}$ è indipendente ne segue che uno dei w_i, che dopo riordinamento possiamo supporre essere w_2, dipende dai rimanenti elementi di questo sistema di vettori. In altre parole, $v_1, v_2, w_3, \ldots, w_m$ generano V. Ripetendo questo procedimento si possono sostituire, uno dopo l'altro, tutti i w_i con i corrispondenti v_i, ottenendo ad ogni passo un sistema di generatori di V. La conclusione è che $v_1, \ldots, v_m$ generano V. Ma allora deve essere $n = m$. Infatti in caso contrario v_{m+1} sarebbe linearmente dipendente da $v_1, \ldots, v_m$, contro le ipotesi.

Corollario (1.3). *Sia V uno spazio vettoriale di dimensione finita. Tutte le basi di V hanno lo stesso numero di elementi.*

Se V ha dimensione finita, il numero di elementi di una sua base si chiama *dimensione* di V, e si indica con $\dim(V)$. Il teorema (1.2) mostra tra l'altro che, nel dimostrare (1.1), si può evitare di usare il lemma di Zorn quando si ha a che fare con spazi vettoriali di dimensione finita. In effetti, riprendendo le notazioni della dimostrazione di (1.2), il lemma di Zorn serve a mostrare l'esistenza di un insieme massimale fra quelli indipendenti contenuti in S e contenenti T. Se V ha dimensione finita, visto che ogni insieme indipendente contiene al più $\dim(V)$ elementi, l'insieme cercato non è altro che un insieme indipendente, contenuto in S e contenente T, con il massimo numero possibile di elementi.

Diamo ora qualche altra conseguenza dei risultati finora dimostrati. La prima è la seguente.

LEMMA (1.4). *Sia V uno spazio vettoriale di dimensione finita, e sia W un suo sottospazio. Allora W ha dimensione finita,* $\dim(W) \leq \dim(V)$, *e si ha uguaglianza se e solo se $W = V$. Inoltre ogni base di W è contenuta in una di V.*

Il lemma è una conseguenza immediata di (1.1). Se si vuole evitare di ricorrere a questo risultato in tutta la sua generalità, ma usare solo il caso in cui si abbia a che fare con spazi di dimensione finita, occorre mostrare innanzitutto che W ha dimensione finita. Ogni sottoinsieme indipendente di W è anche un sottoinsieme indipendente di V, e quindi contiene al più $\dim(V)$ elementi. D'altra parte un sottinsieme B di W che sia indipendente e con il massimo numero possibile di elementi è una base. Infatti se non generasse W ci sarebbe almeno un elemento w di W che è indipendente da B, e quindi $B \cup \{w\}$ sarebbe un sottinsieme indipendente di W strettamente più grande di B, contro quanto supposto. Che ogni base di W sia contenuta in una di V segue di (1.1). Di conseguenza $\dim(W) \leq \dim(V)$, e se $\dim(W) = \dim(V)$ ogni base di W è anche una base di V, e dunque $W = V$.

PROPOSIZIONE (1.5) (FORMULA DI GRASSMANN). *Siano U e W sottospazi di dimensione finita di uno stesso spazio vettoriale V. Allora $U + W$ ha dimensione finita e*

$$\dim(U + W) + \dim(U \cap W) = \dim(U) + \dim(W)\,.$$

Per dimostrare la proposizione scegliamo innanzitutto una base $\{v_1, \dots, v_a\}$ di $U \cap W$. Segue da (1.4) che esistono una base di U della forma $\{v_1, \dots, v_a, u_1, \dots, u_b\}$ e una di W della forma $\{v_1, \dots, v_a, w_1, \dots, w_c\}$. Per concludere basta mostrare che $\{v_1, \dots, v_a, u_1, \dots, u_b, w_1, \dots, w_c\} = B$ è una base di $U + W$, dato che allora

$$\dim(U + W) + \dim(U \cap W) = (a + b + c) + a = (a + b) + (a + c) = \dim(U) + \dim(W)\,.$$

Che B generi $U + W$ è chiaro. D'altra parte, se

$$\sum a_i v_i + \sum b_i u_i + \sum c_i w_i = 0\,,$$

$\sum b_i u_i = -\sum a_i v_i - \sum c_i w_i$ appartiene a $U \cap W$, e quindi si può scrivere

$$\sum b_i u_i = \sum d_i v_i\,,$$

per opportuni coefficienti d_i. Dato che $\{v_1, \dots, v_a, u_1, \dots, u_b\}$ è una base di U, ciò implica che $b_i = 0$ per ogni i. Ne segue che $\sum a_i v_i + \sum c_i w_i = 0$, e quindi che anche gli a_i e i c_i sono tutti nulli, visto che $\{v_1, \dots, v_a, w_1, \dots, w_c\}$ è una base di W. Ciò conclude la dimostrazione della formula di Grassmann.