

Algebra Lineare e Geometria

Francesco Bottacin

Indice

Capitolo 1. Teoria degli Insiemi	1
1. Insiemi finiti e infiniti	1
2. Cardinalità	10
3. Il teorema del Buon Ordinamento	24
Capitolo 2. Spazi Vettoriali	27
1. Vettori Geometrici	27
2. Spazi Vettoriali	31
Capitolo 3. Applicazioni Lineari e Matrici	61
1. Applicazioni Lineari	61
2. Matrici	70

CAPITOLO 1

Teoria degli Insiemi

1. Insiemi finiti e infiniti

Nel seguito assumeremo che il lettore abbia una certa familiarità con alcune nozioni elementari della teoria degli insiemi, quali il concetto stesso di insieme, di funzione tra insiemi, di relazione di equivalenza e di relazione d'ordine.

Indicheremo con $\mathbb{N} = \{0, 1, 2, \dots\}$ l'insieme dei numeri naturali e con J_n il sottoinsieme di \mathbb{N} costituito dai numeri naturali compresi tra 1 e n ,

$$J_n = \{x \in \mathbb{N} \mid 1 \leq x \leq n\}.$$

DEFINIZIONE 1.1. Un insieme S è *finito* se è vuoto oppure se esiste una biiezione tra J_n e S , per qualche $n \in \mathbb{N}$. Un insieme è detto *infinito* se non è finito.

La seguente proposizione ci assicura che “il numero di elementi” di un insieme finito è ben definito.

PROPOSIZIONE 1.2. *Se S è un insieme finito e non vuoto esiste un unico $n \in \mathbb{N}$ tale che S sia in biiezione con J_n .*

DIMOSTRAZIONE. Se, per assurdo, esistessero delle biiezioni tra S e J_m e tra S e J_n , con $n \neq m$, si potrebbe trovare una biiezione tra J_m e J_n . Possiamo supporre che sia $n > m$ (altrimenti basta scambiare i ruoli di m e n). Sia dunque $f : J_n \rightarrow J_m$ una funzione biiettiva. Componendo f con una opportuna permutazione σ di J_m si può ottenere una funzione biiettiva $F = \sigma \circ f : J_n \rightarrow J_m$ con la proprietà che $F(1) = 1, F(2) = 2, \dots, F(m) = m$. Ma allora $F(m+1)$ deve necessariamente coincidere con $F(i)$, per qualche $i = 1, \dots, m$, il che contraddice l'ipotesi che F sia biiettiva. \square

L'insieme \mathbb{N} non è, ovviamente, finito.

DEFINIZIONE 1.3. Un insieme S è detto *numerabile* se esiste una biiezione tra S e \mathbb{N} .

Un insieme finito non può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio (vedi la Proposizione 1.2). L'esempio seguente mostra che ciò non vale nel caso di un insieme infinito:

ESEMPIO 1.4. Sia $P = \{0, 2, 4, \dots\}$ il sottoinsieme di \mathbb{N} costituito dai numeri pari e sia D il sottoinsieme dei numeri dispari. Le funzioni $f : \mathbb{N} \rightarrow P, n \mapsto 2n$, e $g : \mathbb{N} \rightarrow D, n \mapsto 2n + 1$, sono biettive.

Se noi accettiamo il fatto che due insiemi tra i quali esiste una funzione biiettiva hanno lo stesso “numero di elementi,” allora dobbiamo necessariamente accettare il fatto che un insieme infinito quale \mathbb{N} può avere lo stesso “numero di elementi” di un suo sottoinsieme proprio (tale “numero di elementi” è allora necessariamente infinito).

Questi concetti verranno precisati nella prossima sezione.

Un insieme numerabile è, in un certo senso, il “più piccolo” degli insiemi infiniti:

PROPOSIZIONE 1.5. *Sia S un sottoinsieme di un insieme numerabile. Allora S è finito o numerabile.*

DIMOSTRAZIONE. Sia X un insieme numerabile e $S \subseteq X$. Dato che X è numerabile esiste una biiezione $f : X \rightarrow \mathbb{N}$. S può quindi essere identificato con un sottoinsieme di \mathbb{N} . È quindi sufficiente dimostrare che ogni sottoinsieme di \mathbb{N} è finito o numerabile. Sia dunque D un sottoinsieme di \mathbb{N} . Se D è finito la dimostrazione è conclusa. Supponiamo quindi che D sia infinito. Sia d_1 il più piccolo elemento di D (che esiste poiché \mathbb{N} è bene ordinato). Definiamo poi d_2 come il più piccolo elemento di $D \setminus \{d_1\}$, etc. Supponiamo quindi, induttivamente, di avere già definito $d_1 < d_2 < \dots < d_n$. Definiremo d_{n+1} come il più piccolo elemento di $D \setminus \{d_1, \dots, d_n\}$. Si ottiene in questo modo una sequenza infinita di elementi distinti di D . La funzione $f : \mathbb{N} \rightarrow D$, $n \mapsto d_n$ è dunque iniettiva. Dimostriamo che essa è anche suriettiva. Sia $d \in D$. L'insieme $D_{\leq d} = \{x \in D \mid x \leq d\}$ è finito, dato che è un sottoinsieme dell'insieme $\{0, 1, \dots, d\}$. Sia m il numero di elementi di $D_{\leq d}$. Dalle definizioni precedenti si deduce che $D_{\leq d}$ contiene gli m elementi $d_1 < d_2 < \dots < d_m$ e che necessariamente $d = d_m$. Ma ciò equivale a dire che $d = f(m)$, quindi f è suriettiva. La funzione f è dunque una biiezione tra \mathbb{N} e D . \square

Enunciamo ora un assioma che risulta essere di fondamentale importanza quando si lavora con insiemi infiniti:

ASSIOMA DELLA SCELTA. *Sia X un insieme di insiemi non vuoti. Allora è possibile scegliere un singolo elemento da ogni insieme che appartiene a X .*

Una formulazione equivalente è la seguente: *dato un qualsiasi insieme di insiemi non vuoti a due a due disgiunti, esiste almeno un insieme che ha esattamente un elemento in comune con ciascuno degli insiemi non vuoti.*

In altri termini, l'assioma della scelta afferma che, data una qualunque collezione di insiemi non vuoti, è possibile scegliere un elemento in ciascuno di questi insiemi, anche se questi sono in numero infinito e anche se non c'è nessuna “regola” che permetta di stabilire quale elemento scegliere in ciascun insieme.

ESEMPIO 1.6. Utilizzando l'assioma della scelta è possibile dimostrare che ogni funzione suriettiva tra due insiemi, $f : X \rightarrow Y$, ammette una *sezione*, cioè esiste una funzione $g : Y \rightarrow X$ tale che $f \circ g = \text{id}_Y$. Infatti, per ogni $y \in Y$ possiamo considerare il sottoinsieme $f^{-1}(y) \subseteq X$. L'assioma della scelta garantisce che, per ogni $y \in Y$, è possibile scegliere un elemento $x_y \in f^{-1}(y)$. La funzione $g : Y \rightarrow X$ definita ponendo $g(y) = x_y$ è una sezione di f .

ESEMPIO 1.7. Come altra applicazione dell'assioma della scelta dimostriamo ora che un prodotto cartesiano arbitrario di insiemi non vuoti è non vuoto.

Sia A un insieme non vuoto e, per ogni $\alpha \in A$, sia X_α un insieme non vuoto. Un elemento del prodotto cartesiano $\prod_{\alpha \in A} X_\alpha$ è $(x_\alpha)_{\alpha \in A}$, dove $x_\alpha \in X_\alpha$, per ogni $\alpha \in A$. L'assioma della scelta afferma proprio che, per ogni $\alpha \in A$, è possibile scegliere un elemento $x_\alpha \in X_\alpha$. In questo modo si ottiene un elemento $(x_\alpha)_{\alpha \in A} \in \prod_{\alpha \in A} X_\alpha$.

OSSERVAZIONE 1.8. Notiamo che, se il numero degli insiemi in questione è finito, non è necessario ricorrere all'assioma della scelta. Siano infatti A_1, A_2, \dots, A_n degli insiemi non vuoti. Poiché $A_1 \neq \emptyset$, esiste un elemento $a_1 \in A_1$. Se $a_1 \in A_2$ allora scegliamo lo stesso a_1 quale elemento di A_2 , altrimenti, dato che $A_2 \neq \emptyset$, esiste un elemento $a_2 \in A_2$, con $a_2 \neq a_1$. Ora, se A_3 contiene a_1 oppure a_2 scegliamo questo come elemento di A_3 , altrimenti, essendo $A_3 \neq \emptyset$, esiste un elemento $a_3 \in A_3$, con $a_3 \neq a_1$ e $a_3 \neq a_2$. Continuando in questo modo, dopo un numero finito di passi si ottiene un insieme di elementi $\{a_1, a_2, a_3, \dots\}$ con la proprietà richiesta.

Questo ragionamento non funziona più se il numero di insiemi è infinito.

OSSERVAZIONE 1.9. Si può dimostrare che l'assioma della scelta è indipendente dagli altri assiomi usuali della teoria degli insiemi (Assiomi di Zermelo–Fraenkel). La scelta di accettarlo quale assioma è dettata dal fatto che esso appare intuitivamente evidente. Facciamo però notare che l'assioma della scelta ha, tuttavia, delle conseguenze controintuitive, come vedremo in seguito.

Continuando la nostra discussione sugli insiemi infiniti, possiamo ora dimostrare il seguente risultato:

PROPOSIZIONE 1.10. *Ogni insieme infinito contiene un sottoinsieme numerabile.*

DIMOSTRAZIONE. Sia S un insieme infinito. Sia s_1 un elemento di S . Allora $S \setminus \{s_1\}$ è ancora un insieme infinito. Scegliamo un elemento $s_2 \in S \setminus \{s_1\}$, etc. Possiamo così supporre, induttivamente, di avere già definito gli n elementi distinti $s_1, \dots, s_n \in S$. L'insieme $S \setminus \{s_1, \dots, s_n\}$ è ancora un insieme infinito, quindi possiamo scegliere¹

¹Si noti che in questa dimostrazione si utilizza l'assioma della scelta.

un elemento $s_{n+1} \in S \setminus \{s_1, \dots, s_n\}$. Per induzione otteniamo così una sequenza infinita di elementi distinti di S , cioè una funzione iniettiva $\mathbb{N} \rightarrow S$, $n \mapsto s_n$. L'immagine di questa funzione è un sottoinsieme numerabile di S . \square

PROPOSIZIONE 1.11. *Sia S un insieme numerabile e $f : S \rightarrow Y$ una funzione suriettiva. Allora Y è finito o numerabile.*

DIMOSTRAZIONE. Per ogni $y \in Y$ la sua immagine inversa $f^{-1}(y)$ è un sottoinsieme non vuoto di S . In base all'assioma della scelta possiamo scegliere un elemento $s_y \in f^{-1}(y)$, per ogni $y \in Y$. Si ottiene così una funzione $g : Y \rightarrow S$, $y \mapsto s_y$ (g è detta una *sezione* di f). La funzione g è evidentemente iniettiva, quindi permette di identificare Y con il sottoinsieme $g(Y)$ di S . Poiché S è numerabile, dalla Proposizione 1.5 discende che $g(Y)$, e quindi anche Y , è finito o numerabile. \square

PROPOSIZIONE 1.12. *Sia S un insieme numerabile. Allora $S \times S$ è numerabile.*

DIMOSTRAZIONE. Poiché S è numerabile esiste una biiezione tra S e \mathbb{N} , da cui si ottiene una biiezione tra $S \times S$ e $\mathbb{N} \times \mathbb{N}$. Dunque è sufficiente dimostrare che $\mathbb{N} \times \mathbb{N}$ è numerabile. Una biiezione tra $\mathbb{N} \times \mathbb{N}$ e \mathbb{N} può essere costruita come suggerito nella figura 1: ad ogni coppia di numeri naturali viene associato un numero naturale ottenuto contando le coppie lungo le diagonali, nel modo indicato dalle frecce (nella figura 1, ad ogni coppia (m, n) è associato il numero scritto in grassetto in basso a sinistra). Si verifichi, come esercizio, che l'espressione esplicita di tale biiezione $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ è la seguente:

$$f : (m, n) \mapsto \frac{(m+n)(m+n+1)}{2} + n.$$

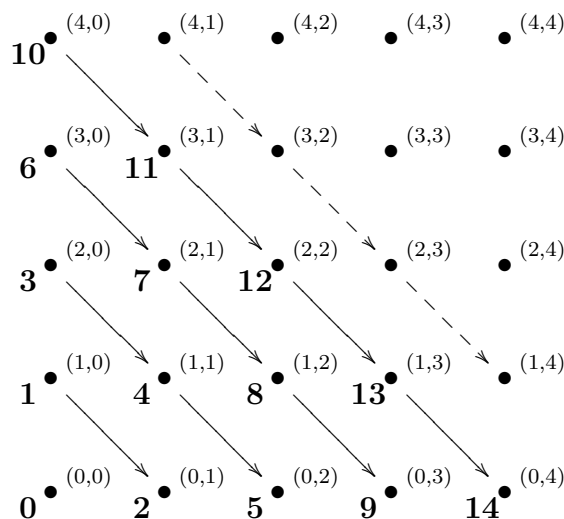
\square

OSSERVAZIONE 1.13. Un'altra dimostrazione del risultato precedente si può ottenere utilizzando il Teorema 2.2 (Teorema di Cantor–Bernstein–Shroeder).

Consideriamo la funzione $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ definita da $f(m, n) = 2^m 3^n$. È immediato verificare che f è iniettiva. Poiché esiste anche una funzione iniettiva di \mathbb{N} in $\mathbb{N} \times \mathbb{N}$, ad esempio la funzione $n \mapsto (n, 0)$, il Teorema 2.2 permette di concludere che esiste una funzione biiettiva tra $\mathbb{N} \times \mathbb{N}$ e \mathbb{N} .

Dalla proposizione precedente si deduce che un qualsiasi prodotto finito di insiemi numerabili è numerabile:

COROLLARIO 1.14. *Se S_i , per $i = 1, \dots, n$, sono insiemi numerabili, allora il prodotto $S_1 \times \dots \times S_n$ è numerabile.*

FIGURA 1. Numerazione di $\mathbb{N} \times \mathbb{N}$

PROPOSIZIONE 1.15. *L'unione di una famiglia numerabile di insiemi numerabili è numerabile, cioè, se I è un insieme numerabile e se, per ogni $i \in I$ è dato un insieme numerabile S_i , allora l'insieme $S = \bigcup_{i \in I} S_i$ è numerabile.*

DIMOSTRAZIONE. Poiché I è numerabile non è restrittivo supporre che $I = \mathbb{N}$. Per ogni $i \in \mathbb{N}$ possiamo enumerare gli elementi dell'insieme S_i utilizzando due indici, nel modo seguente:

$$S_i = \{x_{i0}, x_{i1}, x_{i2}, \dots, x_{ij}, \dots\}.$$

Consideriamo ora la funzione $f : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup_{i \in I} S_i$ definita ponendo $f(i, j) = x_{ij}$. Questa funzione è ovviamente suriettiva (anche se non necessariamente iniettiva) e, dato che l'insieme $\mathbb{N} \times \mathbb{N}$ è numerabile, utilizzando la Proposizione 1.11 si deduce che $\bigcup_{i \in I} S_i$ è numerabile. \square

1.1. Il Lemma di Zorn. In questa sezione dimostreremo un risultato di estrema utilità per lavorare con insiemi infiniti, noto come Lemma di Zorn.

Ricordiamo che un *ordine parziale* (o *preordine*) su un insieme S è una relazione tra coppie di elementi di S , che indicheremo con \leq , la quale soddisfa le tre seguenti proprietà:

- (i) $x \leq x$, per ogni $x \in S$.
- (ii) Per ogni $x, y \in S$, se $x \leq y$ e $y \leq x$, allora $x = y$.
- (iii) Per ogni $x, y, z \in S$, se $x \leq y$ e $y \leq z$, allora $x \leq z$.

La scrittura $x < y$ equivale a $x \leq y$ e $x \neq y$.

Se per ogni $x, y \in S$ si ha $x \leq y$ oppure $y \leq x$, allora l'ordine si dice *totale*. Un insieme S dotato di una relazione d'ordine parziale si dice *insieme ordinato*. S è detto *totalmente ordinato* se l'ordine è totale.

Un sottoinsieme totalmente ordinato di un insieme ordinato S è detto una *catena* di S .

Se S è un insieme ordinato, un elemento *massimale* è un elemento $m \in S$ tale che, se $m \leq s$ per qualche $s \in S$, allora deve necessariamente essere $m = s$. In altre parole, in S non ci sono elementi più grandi di m .

Sia S un insieme ordinato e T un suo sottoinsieme. Un *maggiorante* di T (in S) è un elemento $s \in S$ tale che, per ogni $t \in T$, si ha $t \leq s$. Un *estremo superiore* di T in S è un maggiorante s di T tale che, per ogni altro maggiorante r di T si abbia $s \leq r$ (l'estremo superiore è dunque il *minimo* dei maggioranti). Si noti che l'estremo superiore, quando esiste, è necessariamente unico.

Un insieme ordinato S è detto *induttivo* se ogni catena non vuota di S ammette un maggiorante. S è detto *strettamente induttivo* se ogni catena non vuota di S ammette estremo superiore.

Possiamo ora enunciare il lemma di Zorn:

LEMMA 1.16 (Lemma di Zorn). *Sia S un insieme ordinato non vuoto e induttivo. Allora esiste un elemento massimale in S .*

OSSERVAZIONE 1.17. Come vedremo nel corso della dimostrazione, il Lemma di Zorn dipende dall'Assioma della Scelta. In effetti si può dimostrare che esso è equivalente all'Assioma della Scelta.

Noi dimostreremo una versione leggermente più forte del Lemma di Zorn, la quale afferma che per ogni elemento $a \in S$ esiste un elemento massimale $m \in S$ tale che $a \leq m$. Questo risultato sarà ottenuto come corollario del Teorema 1.19.

Premettiamo una definizione che useremo nella dimostrazione del prossimo teorema.

DEFINIZIONE 1.18. Sia A un insieme non vuoto, parzialmente ordinato e strettamente induttivo. Sia $f : A \rightarrow A$ una funzione tale che $x \leq f(x)$, per ogni $x \in A$ (una tale f sarà detta *crescente*). Fissato un elemento $a \in A$, diremo che un sottoinsieme $B \subseteq A$ è *a -ammissibile* se:

- (i) $a \in B$,
- (ii) $f(B) \subseteq B$,
- (iii) per ogni catena non vuota T in B , l'estremo superiore di T in A appartiene a B .

TEOREMA 1.19. *Sia A un insieme non vuoto, parzialmente ordinato e strettamente induttivo. Sia $f : A \rightarrow A$ una funzione tale che $x \leq f(x)$, per ogni $x \in A$. Allora, per ogni $a \in A$, esiste un elemento $x_a \in A$ tale che $a \leq x_a$ e $f(x_a) = x_a$.*

DIMOSTRAZIONE. Fissiamo $a \in A$. Se A fosse totalmente ordinato esso avrebbe un estremo superiore $b \in A$. Poiché f è crescente, deve essere $b \leq f(b)$ ma, dato che b è l'estremo superiore di A , si deve anche

avere $f(b) \leq b$, da cui segue che $f(b) = b$. Dato che $a \leq b$, ponendo $x_a = b$ si ottiene l'elemento cercato.

Cercheremo allora di ridurre la dimostrazione del teorema a questo caso. Per fare ciò basta trovare un sottoinsieme totalmente ordinato a -ammissibile di A . Infatti, se $B \subseteq A$ è un tale sottoinsieme, il suo estremo superiore b soddisfa le due condizioni $a \leq b$ e $f(b) = b$.

Consideriamo quindi il sottoinsieme

$$B = \{x \in A \mid a \leq x\}.$$

Dimostriamo che B è a -ammissibile. Infatti $a \in B$ e se $y \in f(B)$, allora $y = f(x)$ per qualche $x \in B$. Ma allora si ha $a \leq x \leq f(x) = y$ (perché f è crescente), quindi $y \in B$. Questo dimostra che $f(B) \subseteq B$. Infine, se T è una catena non vuota in B e se b è il suo estremo superiore in A , si ha certamente $a \leq b$, quindi $b \in B$. Questo dimostra che B è a -ammissibile.

Arrivati a questo punto è sufficiente trovare un sottoinsieme totalmente ordinato a -ammissibile di B (questo sarà anche un sottoinsieme totalmente ordinato a -ammissibile di A).

Indichiamo con M l'intersezione di tutti i sottoinsiemi a -ammissibili di B . M non è vuoto, dato che B stesso è a -ammissibile e che tutti i sottoinsiemi a -ammissibili di B contengono a .

Dimostriamo ora che M è a -ammissibile. Infatti $a \in M$ e, se scriviamo $M = \bigcap_{i \in I} C_i$, ove gli insiemi $C_i \subseteq B$ sono a -ammissibili, si ha $f(M) = f(\bigcap_{i \in I} C_i) \subseteq \bigcap_{i \in I} f(C_i) \subseteq \bigcap_{i \in I} C_i = M$. Inoltre, se T è una catena non vuota in M , essa è anche una catena in ogni C_i , quindi il suo estremo superiore appartiene ad C_i , per ogni $i \in I$ e, di conseguenza, appartiene anche a M .

In base alla definizione, M è dunque il più piccolo sottoinsieme a -ammissibile di B , nel senso che ogni sottoinsieme a -ammissibile di B contenuto in M coincide necessariamente con M .

Per concludere la dimostrazione del teorema è ora sufficiente dimostrare che M è totalmente ordinato. Per fare ciò avremo bisogno di due risultati intermedi, che ora dimostreremo.

Prima di enunciarli ci servono alcune definizioni.

Sia $c \in M$. Diremo che c è un *punto estremo* di M se

$$x \in M, x < c \Rightarrow f(x) \leq c.$$

Notiamo che $a \in M$ è un punto estremo, dato che non esiste alcun $x \in M$ tale che $x < a$.

Per ogni punto estremo $c \in M$ poniamo

$$M_c = \{x \in M \mid x \leq c \text{ oppure } f(c) \leq x\}.$$

LEMMA 1.20. *Per ogni punto estremo $c \in M$ si ha $M_c = M$.*

DIMOSTRAZIONE. Ricordiamo che M è il più piccolo sottoinsieme a -ammissibile di B e che $M_c \subseteq M$. Basta quindi dimostrare che M_c

è a -ammissibile. Certamente si ha $a \in M_c$, dato che a è il minimo di B . Sia ora $x \in M_c$. Se $x < c$ allora $f(x) \leq c$ (per definizione di punto estremo), quindi $f(x) \in M_c$. Se $x = c$ allora $f(x) = f(c)$, quindi anche in questo caso $f(x) \in M_c$. Se invece $f(c) \leq x$ allora si ha $f(c) \leq x \leq f(x)$ (perché f è crescente), quindi anche in questo caso $f(x) \in M_c$. Sia ora T una catena non vuota in M_c . T è anche una catena in M , quindi il suo estremo superiore b appartiene a M . Se per tutti gli elementi $x \in T$ si ha $x \leq c$, allora si ha anche $b \leq c$ (per definizione di estremo superiore), quindi $b \in M_c$. Se invece qualche $x \in T$ è tale che $f(c) \leq x$, allora $f(c) \leq x \leq b$, quindi anche in questo caso $b \in M_c$. Questo dimostra che M_c è a -ammissibile, quindi coincide con M . \square

LEMMA 1.21. *Ogni elemento di M è un punto estremo.*

DIMOSTRAZIONE. Sia E l'insieme dei punti estremi di M . Basta dimostrare che E è a -ammissibile (dalla minimalità di M segue allora che $E = M$). Certamente $a \in E$ (abbiamo già osservato in precedenza che a è un punto estremo di M). Dimostriamo ora che $f(E) \subseteq E$. Sia dunque $c \in E$ e consideriamo $f(c)$. Sia $x \in M$ e supponiamo che $x < f(c)$. Dobbiamo dimostrare che $f(x) \leq f(c)$. Per il lemma precedente, $M = M_c$, quindi si deve avere $x < c$ oppure $x = c$ oppure $f(c) \leq x$. Poiché quest'ultima possibilità contraddice l'ipotesi $x < f(c)$, si può solo avere $x < c$ oppure $x = c$. Se $x < c$ allora $f(x) \leq c$ (perché c è un punto estremo), ma $c \leq f(c)$ (perché f è crescente), quindi $f(x) \leq f(c)$, che è ciò che si voleva dimostrare. Se invece $x = c$, allora $f(x) = f(c)$, il che va altrettanto bene. Abbiamo così dimostrato che $f(E) \subseteq E$.

Per finire, sia T una catena non vuota in E . T è anche una catena in M , quindi esiste il suo estremo superiore $b \in M$. Dobbiamo dimostrare che $b \in E$. Sia dunque $x \in M$, con $x < b$. Dobbiamo dimostrare che $f(x) \leq b$. Se, per ogni $c \in T$ si avesse $f(c) \leq x$, allora sarebbe $c \leq f(c) \leq x$ (perché f è crescente), quindi x sarebbe un maggiorante di T e, di conseguenza, $b \leq x$ (per definizione di estremo superiore), il che contraddice l'ipotesi $x < b$.

Dato che $M_c = M$, per ogni $c \in E$, si deve allora necessariamente avere $x \leq c$, per qualche $c \in T$. Infatti, se fosse $c < x$, $\forall c \in T$, allora si avrebbe anche $b \leq x$, il che contraddice l'ipotesi $x < b$. Se fosse $x < c$ allora si avrebbe $f(x) \leq c \leq b$, quindi b sarebbe un punto estremo, cioè $b \in E$, che è esattamente ciò che si voleva ottenere. Se invece $x = c$ allora, dato che c è un punto estremo (perché $c \in T \subseteq E$) e dato che $M_c = M$, si deduce che $f(x) = f(c) \leq b$ (in base alla definizione di M_c , e cioè perché altrimenti b sarebbe un elemento di M compreso tra c e $f(c)$, il che non è possibile per il lemma precedente). Questo dimostra che, anche in questo caso, $b \in E$, quindi E è a -ammissibile. \square

Ritornando alla dimostrazione del teorema, ricordo che dovevamo dimostrare che M è totalmente ordinato. Siano quindi $x, y \in M$. In base al Lemma 1.21, x è un punto estremo di M , quindi $y \in M = M_x$, per il Lemma 1.20. Ma, dalla definizione di M_x segue che o $y \leq x$, oppure $x \leq f(x) \leq y$ (perché f è crescente). Quindi x e y sono confrontabili tra loro, il che dimostra che M è totalmente ordinato. Questo termina la dimostrazione del teorema. \square

Come corollario possiamo, dapprima, ottenere una versione debole del Lemma di Zorn:

COROLLARIO 1.22. *Sia S un insieme non vuoto, parzialmente ordinato e strettamente induttivo. Per ogni $s \in S$ esiste un elemento massimale $m \in S$ tale che $s \leq m$.*

DIMOSTRAZIONE. Supponiamo, per assurdo, che esista $s \in S$ per il quale non esiste alcun elemento massimale $m \in S$ con $s \leq m$. Sia $A = \{x \in S \mid s \leq x\}$. A è un insieme non vuoto (contiene s) e parzialmente ordinato. Sia T una catena non vuota in A e sia b il suo estremo superiore in S . Dato che $s \leq b$, si ha che $b \in A$, quindi A è strettamente induttivo. Dall'ipotesi che non esista alcun elemento massimale $m \in S$ con $s \leq m$, si deduce che per ogni $x \in A$ esiste² un elemento $y_x \in A$ tale che $x < y_x$. La funzione $f : A \rightarrow A$, $x \mapsto y_x$ soddisfa le ipotesi del Teorema 1.19, il quale garantisce l'esistenza di un elemento $x \in A$ per cui si ha $f(x) = x$. Ma ciò contraddice il fatto che $x < y_x$, per ogni $x \in A$. \square

Il Lemma di Zorn si può ora dedurre dal corollario precedente:

COROLLARIO 1.23 (Lemma di Zorn). *Sia S un insieme non vuoto, parzialmente ordinato e induttivo. Per ogni $s \in S$ esiste un elemento massimale $m \in S$ tale che $s \leq m$.*

DIMOSTRAZIONE. Sia \mathcal{A} l'insieme di tutte le catene non vuote di S . \mathcal{A} non è l'insieme vuoto perché $\{a\} \in \mathcal{A}$, per ogni $a \in S$. Se $X, Y \in \mathcal{A}$, poniamo $X \leq Y$ se $X \subseteq Y$ (ordiniamo \mathcal{A} per inclusione). In questo modo \mathcal{A} diventa un insieme parzialmente ordinato strettamente induttivo. Infatti, se $T = \{X_i\}_{i \in I}$ è una catena in \mathcal{A} e se poniamo $Z = \bigcup_{i \in I} X_i$, Z risulta essere una catena in S . Infatti, se $x, y \in Z$, allora $x \in X_i$ e $y \in X_j$, per qualche $i, j \in I$. Ma, dato che T è una catena, si deve avere $X_i \subseteq X_j$ oppure $X_j \subseteq X_i$. In ogni caso, i due elementi x e y appartengono ad uno stesso insieme X_k (dove $k = i$ o $k = j$). Ma X_k è una catena in S , quindi si ha che $x \leq y$ oppure $y \leq x$. Ora è chiaro che Z è l'estremo superiore di T e che $Z \in \mathcal{A}$, quindi \mathcal{A} è strettamente induttivo. Applicando la versione debole del Lemma di Zorn (corollario precedente) all'insieme \mathcal{A} si conclude che, per ogni $X \in \mathcal{A}$, esiste un elemento massimale $X_0 \in \mathcal{A}$ tale che $X \subseteq X_0$. L'insieme X_0 è dunque

²Si noti che in questo punto si usa l'Assioma della Scelta.

una catena non vuota di S , massimale rispetto all'inclusione. Dato che S è induttivo, l'insieme X_0 ammette dei maggioranti. Sia dunque $m \in S$ un maggiorante di X_0 . Dimosteremo ora che m è un elemento massimale di S . Infatti, se esistesse $x \in S$ con $m \leq x$, l'insieme $X_0 \cup \{x\}$ sarebbe totalmente ordinato, cioè sarebbe una catena in S . Ma X_0 è massimale tra tali catene, pertanto si deve avere $X_0 \cup \{x\} = X_0$, cioè $x \in X_0$. Ma ciò significa che $x \leq m$, dato che m è un maggiorante di X_0 . Si conclude quindi che $x = m$, il che dimostra che m è massimale.

Abbiamo dunque dimostrato l'esistenza di un elemento massimale in S .

Per terminare la dimostrazione osserviamo che, se $s \in S$ è un elemento fissato, basta porre $X = \{s\}$ nel ragionamento precedente per dedurre che $s \in X_0$. Dato che m era un maggiorante di X_0 , si ha $s \leq m$, come richiesto. \square

2. Cardinalità

Il processo intuitivo di “contare” gli elementi di un insieme finito e non vuoto S consiste nello stabilire una biiezione tra S e $J_n = \{1, 2, \dots, n\}$, per qualche $n \in \mathbb{N}$. L'unico numero n per il quale esiste una funzione biiezione tra S e J_n è proprio il numero di elementi di S , che chiameremo la *cardinalità* di S e indicheremo con $|S|$. Nel caso dell'insieme vuoto porremo naturalmente $|\emptyset| = 0$.

Ciò che ora vogliamo fare è estendere la nozione di cardinalità agli insiemi infiniti.

Naturalmente, nel caso di un insieme infinito, non è più possibile contare i suoi elementi! Tuttavia abbiamo già osservato che per stabilire se due insiemi finiti abbiano o meno lo stesso numero di elementi non è necessario contarli; basta infatti stabilire se esiste o meno una biiezione tra i due insiemi in questione. Possiamo quindi pensare di fare una cosa analoga nel caso degli insiemi infiniti.³ Diamo quindi la seguente definizione:

DEFINIZIONE 2.1. Due insiemi A e B (finiti o infiniti) sono *equipotenti* se esiste una funzione biiezione tra A e B .

Si verifica facilmente che la relazione di equipotenza gode delle proprietà riflessiva, simmetrica e transitiva, quindi definisce una relazione di equivalenza.

Nel caso di un insieme infinito non possiamo più definire la cardinalità come il numero dei suoi elementi (poiché “infinito” non è un numero), tuttavia possiamo risolvere questo problema identificando la cardinalità con una classe di equivalenza per la relazione di equipotenza. In altre parole, la cardinalità di un insieme S (finito o meno),

³Notiamo tuttavia che il fatto di accettare che delle proprietà che valgono per gli insiemi finiti valgano anche per insiemi infiniti, su cui non abbiamo esperienza diretta, può portare a conseguenze controintuitive.

indicata sempre con $|S|$, è ora pensata come la classe di tutti⁴ gli insiemi equipotenti a S . A parte questa definizione tecnica, la cardinalità può essere intuitivamente pensata come quella “cosa” che hanno in comune tutti gli insiemi che sono equipotenti tra loro.

Possiamo anche pensare di confrontare due cardinalità stabilendo che, dati due insiemi A e B , sarà $|A| \leq |B|$ quando esiste una funzione iniettiva da A in B (si verifichi che, nel caso di insiemi finiti, questa definizione coincide con quella naturale data dal confronto tra numeri).

Arrivati a questo punto, sarebbe piuttosto utile sapere che se A e B sono due insiemi tali che $|A| \leq |B|$ e $|B| \leq |A|$, allora deve necessariamente essere $|A| = |B|$. Ciò non è affatto ovvio perché, in base alle definizioni date, richiede di sapere che l'esistenza di una funzione iniettiva $f : A \rightarrow B$ e di una funzione iniettiva $g : B \rightarrow A$ implica l'esistenza di una funzione biiettiva $h : A \rightarrow B$. Per fortuna ciò è vero:

TEOREMA 2.2 (Cantor–Bernstein–Shroeder). *Siano X e Y due insiemi tali che $|X| \leq |Y|$ e $|Y| \leq |X|$. Allora si ha $|X| = |Y|$.*

Per la dimostrazione avremo bisogno del seguente risultato:

LEMMA 2.3. *Sia X un insieme e sia $\mathcal{P}(X)$ l'insieme dei sottoinsiemi di X . Sia $f : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ una funzione tale che per ogni $A, B \subseteq X$ con $A \subseteq B$, si ha $f(A) \subseteq f(B)$. Allora esiste un sottoinsieme $Y \subseteq X$ tale che $f(Y) = Y$.*

DIMOSTRAZIONE. Sia $\mathcal{S} = \{A \in \mathcal{P}(X) \mid f(A) \subseteq A\}$. L'insieme \mathcal{S} non è vuoto, dato che sicuramente contiene X . Poniamo allora $Y = \bigcap_{A \in \mathcal{S}} A$. Allora $Y \subseteq A$, per ogni $A \in \mathcal{S}$, da cui segue che $f(Y) \subseteq f(A) \subseteq A$, per ogni $A \in \mathcal{S}$, quindi $f(Y) \subseteq Y$. Applicando f ad ambo i membri di questa inclusione si ottiene $f(f(Y)) \subseteq f(Y)$, da cui segue che $f(Y) \in \mathcal{S}$. Ma allora $Y \subseteq f(Y)$, il che dimostra che $f(Y) = Y$. \square

Possiamo ora dimostrare il Teorema 2.2:

DIMOSTRAZIONE. (T. DI CANTOR–BERNSTEIN–SHROEDER). Siano $f : X \rightarrow Y$ e $g : Y \rightarrow X$ due funzioni iniettive. Definiamo $F : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ ponendo

$$F(A) = X \setminus \left(g(Y \setminus f(A)) \right).$$

Si verifica immediatamente che, se $A \subseteq B$, allora $F(A) \subseteq F(B)$. Dal lemma precedente si deduce che esiste un sottoinsieme $Z \subseteq X$ tale che $F(Z) = Z$. Ciò significa che $X \setminus Z = g(Y \setminus f(Z))$. Pertanto $f|_Z$ è una biiezione tra Z e la sua immagine $f(Z)$, mentre $g|_{Y \setminus f(Z)}$ è una biiezione tra $Y \setminus f(Z)$ e $X \setminus Z$. Usando queste due biiezioni (più

⁴Quando si parla della “classe di tutti gli insiemi...” bisogna stare attenti a non incorrere in paradossi, quali il paradosso di Russell. Per andare sul sicuro conviene sempre considerare insiemi contenuti in un qualche universo \mathcal{U} prefissato.

precisamente, usando $f|_Z$ e l'inversa di $g|_{Y \setminus f(Z)}$ si può costruire una funzione biiettiva da X a Y . \square

Da questo teorema segue quindi che la relazione tra cardinalità definita in precedenza è, in effetti, un ordine parziale. Come ora vedremo, utilizzando il Lemma di Zorn si può dimostrare che si tratta di un ordine totale.

PROPOSIZIONE 2.4. *Dati due insiemi X e Y , si ha $|X| \leq |Y|$ oppure $|Y| \leq |X|$.*

DIMOSTRAZIONE. Possiamo supporre che X e Y non siano vuoti, altrimenti l'asserzione è banale. Sia \mathcal{A} l'insieme di tutte le coppie (A, f) , dove $A \subseteq X$ e $f : A \rightarrow Y$ è una funzione iniettiva. \mathcal{A} è non vuoto poiché contiene almeno una coppia in cui $A = \{a\}$, con $a \in X$. Definiamo un ordine parziale su \mathcal{A} ponendo $(A, f) \leq (B, g)$ se $A \subseteq B$ e la restrizione di g ad A coincide con f . L'insieme \mathcal{A} è induttivo, anzi è addirittura strettamente induttivo. Infatti se $T = \{(A_i, f_i)\}_{i \in I}$ è una catena in \mathcal{A} basta porre $V = \bigcup_{i \in I} A_i$ e definire $h : V \rightarrow Y$ ponendo $h(x) = f_i(x)$ se $x \in A_i$, per qualche indice $i \in I$ (si noti che tale definizione non dipende dal particolare indice i scelto).

Dal Lemma di Zorn si deduce quindi che in \mathcal{A} esiste un elemento massimale, che indicheremo con (M, k) . Se $k : M \rightarrow Y$ è suriettiva, allora essa è biiettiva; pertanto componendo l'inversa di k con l'inclusione di M in X si ottiene una funzione iniettiva $Y \rightarrow X$, il che significa che $|Y| \leq |X|$.

Se invece k non è suriettiva allora si deve avere $M = X$. Infatti, se esistesse un elemento $x \in X \setminus M$, poiché esiste anche un elemento $y \in Y \setminus k(M)$ (dato che abbiamo supposto che k non sia suriettiva), si potrebbe costruire una coppia (M', k') ponendo $M' = M \cup \{x\}$ e definendo $k' : M' \rightarrow Y$ ponendo $k'(x) = y$ e stabilendo poi che k' coincida con k sugli elementi di M . Ma questo sarebbe in contraddizione con la massimalità di (M, k) . Essendo pertanto $M = X$, k è una funzione iniettiva di X in Y , il che significa che $|X| \leq |Y|$. \square

Nella sezione precedente abbiamo studiato alcune proprietà degli insiemi numerabili. In particolare abbiamo dimostrato che ogni insieme infinito contiene un sottoinsieme numerabile (Proposizione 1.10), mentre un sottoinsieme di un insieme numerabile deve necessariamente essere finito o numerabile (Proposizione 1.5).

Ciò significa che la cardinalità di un insieme numerabile è la più piccola tra tutte le cardinalità infinite: una cardinalità strettamente minore della cardinalità di un insieme numerabile è necessariamente finita.

Vista la sua importanza, la cardinalità di un insieme numerabile è indicata con un simbolo particolare: \aleph_0 (aleph⁵ zero).

⁵Aleph, \aleph , è la prima lettera dell'alfabeto ebraico.

Veniamo ora allo studio di alcune proprietà delle cardinalità infinite. Premettiamo una definizione:

DEFINIZIONE 2.5. Sia S un insieme. Un *ricoprimento* di S è un insieme Γ di sottoinsiemi di S tale che si abbia $S = \bigcup_{C \in \Gamma} C$. Diremo che Γ è un *ricoprimento disgiunto* di S se esso è un ricoprimento di S e se, per ogni $C, C' \in \Gamma$, con $C \neq C'$, si ha $C \cap C' = \emptyset$.

LEMMA 2.6. *Sia S un insieme infinito. Allora esiste un ricoprimento disgiunto di S costituito da insiemi numerabili.*

DIMOSTRAZIONE. Sia \mathcal{S} l'insieme delle coppie (A, Γ) , dove A è un sottoinsieme di S e Γ è un ricoprimento disgiunto di A costituito da insiemi numerabili. L'insieme \mathcal{S} non è vuoto; infatti, dato che S è infinito, esso contiene un sottoinsieme numerabile D , quindi la coppia $(D, \{D\})$ appartiene a \mathcal{S} . Definiamo un ordine parziale in \mathcal{S} ponendo $(A, \Gamma) \leq (A', \Gamma')$ se $A \subseteq A'$ e $\Gamma \subseteq \Gamma'$. Sia ora T un sottoinsieme non vuoto totalmente ordinato di \mathcal{S} . Possiamo scrivere $T = \{(A_i, \Gamma_i)\}_{i \in I}$, per qualche insieme di indici I . Poniamo $A = \bigcup_{i \in I} A_i$ e $\Gamma = \bigcup_{i \in I} \Gamma_i$. Se $C, C' \in \Gamma$, con $C \neq C'$, allora esistono due indici $i, j \in I$ tali che $C \in \Gamma_i$ e $C' \in \Gamma_j$. Dato che T è totalmente ordinato, si ha $(A_i, \Gamma_i) \leq (A_j, \Gamma_j)$ oppure $(A_j, \Gamma_j) \leq (A_i, \Gamma_i)$. Supponiamo che valga la prima disuguaglianza (altrimenti basta scambiare il ruolo dei due indici i e j). Se ne deduce che $C, C' \in \Gamma_j$ e quindi $C \cap C' = \emptyset$, dato che Γ_j è un ricoprimento disgiunto di A_j . Se $x \in A$, allora $x \in A_i$, per qualche indice i , quindi x appartiene a qualche $C \in \Gamma_i$, dato che Γ_i è un ricoprimento disgiunto di A_i . Da ciò segue che Γ è un ricoprimento disgiunto di A . Dato che gli elementi di ciascun Γ_i sono sottoinsiemi numerabili di S , Γ è un ricoprimento disgiunto di A costituito da insiemi numerabili, quindi $(A, \Gamma) \in \mathcal{S}$ ed è, ovviamente, un maggiorante di T (anzi, ne è proprio l'estremo superiore). Ciò dimostra che \mathcal{S} è induttivamente ordinato. Sia allora (M, Δ) un elemento massimale di \mathcal{S} , la cui esistenza è garantita dal Lemma di Zorn. Se $M = S$ abbiamo finito. Supponiamo quindi che M sia diverso da S . Se il complementare di M in S è infinito, esso contiene un insieme numerabile D . Allora la coppia $(M \cup D, \Delta \cup \{D\})$ è un elemento di \mathcal{S} più grande di (M, Δ) , il che contraddice la massimalità di quest'ultimo. Quindi il complementare di M in S deve essere un insieme finito F . Sia D_0 un elemento di Δ . Poniamo $D_1 = D_0 \cup F$. Allora D_1 è un insieme numerabile. Sia Δ_1 l'insieme costituito da tutti gli elementi di Δ eccetto D_0 , assieme a D_1 . Allora Δ_1 è un ricoprimento disgiunto di S costituito da insiemi numerabili, come volevasi dimostrare. \square

TEOREMA 2.7. *Sia S un insieme infinito e sia D un insieme numerabile. Allora $|S \times D| = |S|$.*

DIMOSTRAZIONE. Per il lemma precedente possiamo esprimere S come unione disgiunta di insiemi numerabili $S = \bigcup_{i \in I} D_i$. Allora si ha:

$$S \times D = \bigcup_{i \in I} (D_i \times D).$$

Per ogni $i \in I$ esiste una biiezione tra $D_i \times D$ e D_i , in base alla Proposizione 1.12. Dato che gli insiemi $D_i \times D$ sono a due a due disgiunti, si ottiene una biiezione tra $S \times D$ e S . \square

COROLLARIO 2.8. *Sia S un insieme infinito. Per ogni insieme finito non vuoto F , si ha $|S \times F| = |S|$.*

DIMOSTRAZIONE. Sia D un insieme numerabile contenente F . Si ha:

$$|S| \leq |S \times F| \leq |S \times D| = |S|.$$

Il Teorema 2.2 permette di concludere. \square

COROLLARIO 2.9. *Sia S un insieme infinito e R un insieme non vuoto. Se $|R| \leq |S|$ allora si ha $|S \cup R| = |S|$.*

DIMOSTRAZIONE. Possiamo scrivere $S \cup R = S \cup T$, per qualche $T \subseteq R$ tale che $S \cap T = \emptyset$. Allora $|T| \leq |R| \leq |S|$. Possiamo allora costruire una funzione iniettiva di $S \cup T$ in $S \times \{1, 2\}$. Infatti si ha una biiezione tra S e $S \times \{1\}$ nel modo ovvio, ed esiste una funzione iniettiva di T in $S \times \{2\}$ per il fatto che $|T| \leq |S|$. Si ha pertanto $|S \cup T| \leq |S \times \{1, 2\}| = |S|$. Poiché si ha, ovviamente, anche $|S| \leq |S \cup T|$, dal Teorema 2.2 si conclude che deve valere l'uguaglianza. \square

COROLLARIO 2.10. *Sia S un insieme infinito e $R \subseteq S$. Se $|R| < |S|$ allora si ha $|S \setminus R| = |S|$.*

DIMOSTRAZIONE. Osserviamo che si ha $S = (S \setminus R) \cup R$. Dalle ipotesi segue che $|R| < |S \setminus R|$. Infatti, se fosse $|S \setminus R| \leq |R|$, dal corollario precedente si avrebbe $|S| = |(S \setminus R) \cup R| = |R|$, il che contraddice l'ipotesi $|R| < |S|$. Sempre dal corollario precedente segue allora che $|S| = |(S \setminus R) \cup R| = |S \setminus R|$. \square

PROPOSIZIONE 2.11. *Sia S un insieme infinito. Per ogni $i \in \mathbb{N}$ sia A_i un insieme tale che $|A_i| \leq |S|$. Supponiamo inoltre che gli insiemi A_i siano a due a due disgiunti, cioè che $A_i \cap A_j = \emptyset$, se $i \neq j$ e poniamo $A = \bigcup_{i \in \mathbb{N}} A_i$. Allora si ha $|A| \leq |S|$.*

DIMOSTRAZIONE. Per ogni $i \in \mathbb{N}$ sia $f_i : A_i \rightarrow S$ una funzione iniettiva. Osserviamo che, per ogni $x \in A$ esiste un unico indice i tale che $x \in A_i$ (qui si usa l'ipotesi che gli insiemi A_i siano a due a due disgiunti). Possiamo quindi definire una funzione $F : A \rightarrow S \times \mathbb{N}$ associando a tale $x \in A$ la coppia $(f_i(x), i)$. La funzione F è iniettiva, quindi si ha $|A| \leq |S \times \mathbb{N}|$. Dal Teorema 2.7 si ha che $|S \times \mathbb{N}| = |S|$, quindi $|A| \leq |S|$, come volevasi dimostrare. \square

OSSERVAZIONE 2.12. La proposizione precedente continua a valere anche se gli insiemi A_i non sono a due a due disgiunti. Infatti se $A = \bigcup_{i \in \mathbb{N}} A_i$, è sempre possibile trovare dei sottoinsiemi $B_i \subseteq A_i$ tali che $B_i \cap B_j = \emptyset$, per ogni $i \neq j$, e tali che $A = \bigcup_{i \in \mathbb{N}} B_i$.

TEOREMA 2.13. *Sia S un insieme infinito. Allora $|S \times S| = |S|$.*

DIMOSTRAZIONE. Sia \mathcal{S} l'insieme delle coppie (A, f) , ove A è un sottoinsieme infinito di S e $f : A \rightarrow A \times A$ è una funzione biettiva. \mathcal{S} non è vuoto perché S contiene un sottoinsieme numerabile D e, dato che D è numerabile, è sempre possibile trovare una funzione biettiva $f : D \rightarrow D \times D$. Dati due elementi (A, f) e (A', f') in \mathcal{S} , poniamo $(A, f) \leq (A', f')$ se $A \subseteq A'$ e $f'|_A = f$. In questo modo l'insieme \mathcal{S} risulta essere parzialmente ordinato. Sia ora T una catena non vuota in \mathcal{S} . Possiamo scrivere $T = \{(A_i, f_i)\}_{i \in I}$, per qualche insieme di indici I . Sia $M = \bigcup_{i \in I} A_i$. Definiremo ora una biiezione $g : M \rightarrow M \times M$. Se $x \in M$ allora $x \in A_i$ per qualche $i \in I$; poniamo allora $g(x) = f_i(x)$. Questa è una buona definizione in quanto il valore $f_i(x)$ non dipende dalla scelta di A_i . Infatti se $x \in A_j$, per qualche $j \neq i$, allora si avrà $(A_i, f_i) \leq (A_j, f_j)$ oppure $(A_j, f_j) \leq (A_i, f_i)$, perché T è totalmente ordinato. A meno di scambiare i ruoli di i e j possiamo allora supporre che sia $(A_i, f_i) \leq (A_j, f_j)$. In tal caso si ha $x \in A_i \subseteq A_j$ e $f_j|_{A_i} = f_i$, il che significa che $f_j(x) = f_i(x)$. Per dimostrare che g è suriettiva, sia $(x, y) \in M \times M$. Allora $x \in A_i$ e $y \in A_j$, per qualche $i, j \in I$. Esattamente come prima, non è restrittivo supporre che sia $(A_i, f_i) \leq (A_j, f_j)$, da cui si deduce che $x, y \in A_j$. Allora esiste un elemento $b \in A_j$ tale che $f_j(b) = (x, y)$, perché f_j è biettiva. Dalla definizione di g si deduce che $g(b) = (x, y)$, quindi g è suriettiva. La dimostrazione dell'iniettività di g è analoga. Supponiamo infatti che $x, y \in M$ siano tali che $g(x) = g(y)$. Si ha $x \in A_i$ e $y \in A_j$, per qualche $i, j \in I$. Dato che T è totalmente ordinato, non è restrittivo supporre che $(A_i, f_i) \leq (A_j, f_j)$. Da ciò segue che $x, y \in A_j$ e che $f_i(x) = f_j(x)$. Ma allora si ha $g(x) = f_j(x)$ e $g(y) = f_j(y)$, quindi $f_j(x) = f_j(y)$. Dato che f_j è iniettiva si deve avere $x = y$, il che dimostra che g è iniettiva.

Abbiamo così dimostrato che g è biettiva. Da ciò segue subito che (M, g) è un maggiorante di T in \mathcal{S} (anzi è proprio l'estremo superiore di T). Questo dimostra che l'insieme \mathcal{S} è induttivo. Sia quindi (M, g) un elemento massimale di \mathcal{S} (esiste per il Lemma di Zorn) e sia C il complemento di M in S . Se $|C| \leq |M|$, si ha

$$|M| \leq |S| = |M \cup C| = |M|,$$

per il Corollario 2.9, da cui segue che $|M| = |S|$ per il Teorema 2.2. Dato che $|M| = |M \times M|$, abbiamo concluso la dimostrazione. Rimane solo da analizzare il caso in cui $|M| \leq |C|$. In questo caso esiste un sottoinsieme M_1 di C avente la stessa cardinalità di M . Consideriamo

allora

$$(M \cup M_1) \times (M \cup M_1) = (M \times M) \cup (M_1 \times M) \cup (M \times M_1) \cup (M_1 \times M_1).$$

Per l'ipotesi su M gli ultimi tre insiemi in parentesi alla destra di questa equazione hanno la stessa cardinalità di M , quindi, per il Corollario 2.9, possiamo scrivere

$$(M \cup M_1) \times (M \cup M_1) = (M \times M) \cup M_2,$$

dove M_2 è disgiunto da $M \times M$ e ha la stessa cardinalità di M .

Ora definiamo una biiezione

$$g_1 : M \cup M_1 \rightarrow (M \cup M_1) \times (M \cup M_1).$$

Poniamo $g_1(x) = g(x)$ se $x \in M$, e definiamo g_1 in M_1 come una qualunque biiezione tra M_1 e M_2 . In questo modo abbiamo esteso g da M a $M \cup M_1$ ottenendo una coppia $(M \cup M_1, g_1) \in \mathcal{S}$, il che contraddice la massimalità di (M, g) . Questo dimostra che non può essere $|M| \leq |C|$, pertanto deve necessariamente essere $|C| \leq |M|$ (infatti abbiamo già dimostrato che le cardinalità sono totalmente ordinate). Questo conclude la dimostrazione del teorema. \square

COROLLARIO 2.14. *Sia S un insieme infinito e indichiamo con S^n il prodotto cartesiano di S per sé stesso n volte. Allora si ha $|S^n| = |S|$, per ogni $n \geq 1$.*

DIMOSTRAZIONE. Induzione su n . \square

COROLLARIO 2.15. *Se S_1, S_2, \dots, S_n sono insiemi non vuoti, con S_n infinito, e se $|S_i| \leq |S_n|$, per $i = 1, \dots, n-1$, allora $|S_1 \times \dots \times S_n| = |S_n|$.*

DIMOSTRAZIONE. Si ha:

$$|S_n| \leq |S_1 \times \dots \times S_n| \leq |S_n \times \dots \times S_n| = |S_n|,$$

per il corollario precedente. Il Teorema 2.2 permette di concludere. \square

COROLLARIO 2.16. *Sia S un insieme infinito e sia Φ l'insieme dei sottoinsiemi finiti di S . Allora $|\Phi| = |S|$.*

DIMOSTRAZIONE. Sia Φ_n l'insieme dei sottoinsiemi di S aventi esattamente n elementi, per $n = 0, 1, 2, \dots$. Dimostriamo dapprima che $|\Phi_n| \leq |S|$. Per $n = 0$, Φ_0 contiene solo l'insieme vuoto, quindi $|\Phi_0| = 1$. Supponiamo quindi che $n \geq 1$. Per ogni elemento F di Φ_n fissiamo un qualche ordinamento dei suoi elementi,

$$F = \{x_1, \dots, x_n\}.$$

A tale sottoinsieme possiamo quindi associare l'elemento $(x_1, \dots, x_n) \in S^n$. Otteniamo così una funzione $\Phi_n \rightarrow S^n$, $F \mapsto (x_1, \dots, x_n)$.

Questa funzione è iniettiva; infatti se $G = \{y_1, \dots, y_n\}$ è un altro sottoinsieme di S avente n elementi e se $G \neq F$, allora si ha necessariamente $(y_1, \dots, y_n) \neq (x_1, \dots, x_n)$. Da ciò segue che

$$|\Phi_n| \leq |S^n| = |S|,$$

per il Corollario 2.14. Ora osserviamo che Φ è l'unione disgiunta dei Φ_n , per $n = 0, 1, 2, \dots$. Dalla Proposizione 2.11 segue che $|\Phi| \leq |S|$. Poiché si ha anche $|S| \leq |\Phi|$ (basta osservare che si ha $|S| = |\Phi_1|$), dal Teorema 2.2 si conclude. \square

Possiamo osservare che, fino a questo punto, non abbiamo mai incontrato delle cardinalità più grandi di \aleph_0 . Il prossimo teorema mostra che, dato un qualsiasi insieme infinito S , esiste sempre un insieme la cui cardinalità è strettamente maggiore di quella di S .

TEOREMA 2.17. *Sia S un insieme infinito e sia M l'insieme di tutte le funzioni da S nell'insieme $\{0, 1\}$. Allora si ha $|S| < |M|$.*

DIMOSTRAZIONE. Per ogni $x \in S$ sia $f_x : S \rightarrow \{0, 1\}$ la funzione definita da $f_x(x) = 1$ e $f_x(y) = 0$ per ogni $y \neq x$. Allora la funzione $x \mapsto f_x$ è una funzione iniettiva di S in M , pertanto $|S| \leq |M|$. Supponiamo che sia $|S| = |M|$. Sia dunque $x \mapsto g_x$ una biiezione tra S e M . Definiamo ora una funzione $h : S \rightarrow \{0, 1\}$ ponendo

$$h(x) = \begin{cases} 0 & \text{se } g_x(x) = 1, \\ 1 & \text{se } g_x(x) = 0. \end{cases}$$

Allora si ha certamente $h \neq g_x$, per ogni $x \in S$, ma ciò contraddice l'ipotesi che la funzione $x \mapsto g_x$ sia biiettiva. Quindi deve essere $|S| \neq |M|$, come volevasi dimostrare. \square

OSSERVAZIONE 2.18. Se S e T sono due insiemi, l'insieme di tutte le funzioni $f : S \rightarrow T$ è indicato con il simbolo T^S . Tale notazione è consistente con il fatto che $|T^S| = |T|^{|S|}$ (quando S e T sono insiemi finiti). Usando questa notazione, il risultato del teorema precedente può essere espresso dicendo che, per ogni insieme S (finito o infinito), si ha

$$|S| < 2^{|S|}.$$

COROLLARIO 2.19. *Sia S un insieme infinito e sia $\mathcal{P}(S)$ l'insieme di tutti i sottoinsiemi di S . Allora si ha $|S| < |\mathcal{P}(S)|$.*

DIMOSTRAZIONE. Sia M l'insieme di tutte le funzioni da S in $\{0, 1\}$. Per ogni sottoinsieme $A \subseteq S$ definiamo la sua *funzione caratteristica* $\chi_A : S \rightarrow \{0, 1\}$ ponendo

$$\chi_A(x) = \begin{cases} 1 & \text{se } x \in A, \\ 0 & \text{se } x \notin A. \end{cases}$$

Si verifica facilmente che la funzione $\mathcal{P}(S) \rightarrow M, A \mapsto \chi_A$, è una biiezione, quindi $|\mathcal{P}(S)| = |M|$. Il teorema precedente permette allora di concludere. \square

2.1. La cardinalità del continuo. In questa sezione studieremo le cardinalità degli usuali insiemi numerici \mathbb{Z} , \mathbb{Q} e \mathbb{R} .

Iniziamo con l'osservare che l'insieme \mathbb{Z} dei numeri interi è numerabile. Esso è infatti unione dei due insiemi numerabili $\{0, 1, 2, 3, \dots\}$ e $\{-1, -2, -3, \dots\}$ (cf. Proposizione 1.15).

Più direttamente, è sufficiente osservare che la funzione $f : \mathbb{N} \rightarrow \mathbb{Z}$ definita ponendo

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari,} \\ -\frac{n+1}{2} & \text{se } n \text{ è dispari} \end{cases}$$

è biiettiva.

Passiamo ora dell'insieme \mathbb{Q} dei numeri razionali.

PROPOSIZIONE 2.20. *L'insieme \mathbb{Q} è numerabile.*

DIMOSTRAZIONE. Poniamo $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$ e $\mathbb{Q}^- = \{q \in \mathbb{Q} \mid q < 0\}$. La funzione $\mathbb{Q}^+ \rightarrow \mathbb{Q}^-, q \mapsto -q$, è biiettiva, quindi $|\mathbb{Q}^+| = |\mathbb{Q}^-|$. Dato che $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$, dalla Proposizione 1.15 si deduce che $|\mathbb{Q}| = |\mathbb{Q}^+|$. È quindi sufficiente dimostrare che \mathbb{Q}^+ è numerabile.

Poniamo $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ e osserviamo che ogni $q \in \mathbb{Q}^+$ si può scrivere in modo unico nella forma $q = m/n$, ove $m, n \in \mathbb{N}^*$ sono due interi relativamente primi. Se associamo a q la coppia (m, n) otteniamo una funzione iniettiva $F : \mathbb{Q}^+ \rightarrow \mathbb{N}^* \times \mathbb{N}^*$. Poiché \mathbb{N}^* è numerabile, dalla Proposizione 1.12 si deduce che $\mathbb{N}^* \times \mathbb{N}^*$ è numerabile, quindi si ha

$$|\mathbb{Q}^+| \leq |\mathbb{N}^* \times \mathbb{N}^*| = |\mathbb{N}|.$$

Dall'ovvia inclusione $\mathbb{N}^* \hookrightarrow \mathbb{Q}^+$ data da $n \mapsto n/1$, segue che $|\mathbb{N}^*| \leq |\mathbb{Q}^+|$. Per il Teorema 2.2, si ha quindi $|\mathbb{Q}^+| = |\mathbb{N}|$. \square

Consideriamo ora l'insieme \mathbb{R} dei numeri reali. Avremo bisogno di richiamare alcuni fatti elementari riguardanti la rappresentazione di un numero reale in una base N arbitraria.

Fissiamo quindi un numero naturale $N \geq 2$ (la *base*) e consideriamo un insieme S di "simboli," contenente N elementi. Assegniamo a ciascuno degli elementi di S un valore numerico distinto, preso nell'insieme $\{0, 1, 2, \dots, N-1\}$. In tal modo è possibile identificare S con l'insieme dei numeri naturali $\{0, 1, \dots, N-1\}$. Non è quindi restrittivo supporre che sia $S = \{0, 1, \dots, N-1\}$.

ESEMPIO 2.21. Nel caso in cui $N = 2$ (numerazione in base 2, o *binaria*), solitamente si prende $S = \{0, 1\}$, mentre nella usuale notazione decimale ($N = 10$), si ha $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Nella cosiddetta notazione *esadecimale* ($N = 16$), si ha

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\},$$

dove i valori numerici dei nuovi simboli sono: $A = 10$, $B = 11$, $C = 12$, $D = 13$, $E = 14$ e $F = 15$.

Un numero reale r è rappresentato (in base N) da una sequenza di simboli del tipo

$$(2.1) \quad a_m a_{m-1} \dots a_2 a_1 a_0, b_1 b_2 \dots b_j \dots$$

ove gli a_i e i b_j sono elementi di S . La corrispondenza tra $r \in \mathbb{R}$ e la sua rappresentazione simbolica (2.1) è data dalla seguente formula:

$$(2.2) \quad \begin{aligned} r &= a_m N^m + a_{m-1} N^{m-1} + \dots + a_1 N^1 + a_0 N^0 \\ &\quad + b_1 N^{-1} + b_2 N^{-2} + \dots + b_j N^{-j} + \dots \\ &= \sum_{i=0}^m a_i N^i + \sum_{j=1}^{+\infty} b_j N^{-j}. \end{aligned}$$

Si osservi che le sequenze che stiamo considerando hanno sempre un numero finito di simboli a_i a sinistra della virgola, quindi le espressioni del tipo $\sum_{i=0}^m a_i N^i$ sono in ogni caso delle somme finite. I simboli b_j che compaiono a destra della virgola possono invece essere in numero infinito, quindi un'espressione del tipo $\sum_{j=1}^{+\infty} b_j N^{-j}$ rappresenta, in realtà, una serie numerica. È però molto facile dimostrare che questo tipo di serie numeriche hanno sempre una somma finita (per ogni base $N \geq 2$).

Purtroppo l'espressione in una qualsiasi base N di un numero reale non è, in generale, unica.

ESEMPIO 2.22. A titolo di esempio, consideriamo l'usuale rappresentazione decimale ($N = 10$). Sia r il numero reale corrispondente alla sequenza $0,999\dots$ (infiniti 9 dopo la virgola)

$$r = 0,999\dots$$

Moltiplicando per 10 si ottiene $10r = 9,999\dots$, e quindi

$$9r = 10r - r = 9$$

da cui si deduce che $r = 1$. Si ha pertanto

$$0,999\dots = 1.$$

Un fenomeno analogo avviene anche in base N , quando i simboli b_h , per h maggiore o uguale a un qualche indice j , corrispondono tutti al numero $N - 1$.

Pertanto, se vogliamo che l'espressione di un numero reale in base N sia unica, è necessario richiedere che nell'espressione (2.1) non esista alcun indice j per cui si abbia $b_h = N - 1, \forall h \geq j$ (si consiglia al lettore di dimostrarlo, come esercizio).

Come vedremo, questo fatto ci creerà qualche complicazione in seguito.

OSSERVAZIONE 2.23. Facciamo notare che si potrebbe anche *definire* l'insieme \mathbb{R} dei numeri reali come l'insieme di tutte le sequenze di simboli del tipo sopra descritto, per le quali che non esiste alcun indice j tale che $b_h = N - 1, \forall h \geq j$.

Consideriamo ora l'intervallo dei numeri reali compresi tra 0 e 1,

$$I = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

Osserviamo che, in una qualsiasi base N , la rappresentazione di un numero $r \in I$ è del tipo

$$r = 0, b_1 b_2 \dots b_j \dots$$

Cominciamo col dimostrare che I e \mathbb{R} hanno la stessa cardinalità:

LEMMA 2.24. *Si ha $|\mathbb{R}| = |I|$.*

DIMOSTRAZIONE. È sufficiente osservare che la funzione $f : I \rightarrow \mathbb{R}$ definita da $f(x) = \tan(\pi(x - 1/2))$ è biiettiva. \square

Siamo ora in grado di dimostrare che la cardinalità dell'insieme dei numeri reali è strettamente maggiore della cardinalità di \mathbb{N} .

TEOREMA 2.25. *L'insieme \mathbb{R} dei numeri reali non è numerabile.*

DIMOSTRAZIONE. In base al lemma precedente, basta dimostrare che I non è numerabile. Per fare ciò utilizzeremo l'usuale rappresentazione dei numeri reali in base 10.

Come già osservato, ogni $r \in I$ ha una rappresentazione decimale della forma

$$r = 0, b_1 b_2 b_3 \dots b_j \dots$$

ove i $b_j \in \{0, 1, 2, \dots, 9\}$ non sono tutti nulli e ove non esiste alcun indice j tale che $b_h = 9, \forall h \geq j$.

Ragioniamo per assurdo, supponendo che I sia numerabile. Esisterà quindi una funzione biiettiva $\mathbb{N}^* \rightarrow I, i \mapsto r_i$. Questo ci permette di enumerare gli elementi di I :

$$I = \{r_1, r_2, r_3, \dots, r_j, \dots\}$$

e utilizzando la rappresentazione in base 10 possiamo anche scrivere:

$$\begin{aligned} r_1 &= 0, b_{11} b_{12} b_{13} \dots b_{1l} \dots \\ r_2 &= 0, b_{21} b_{22} b_{23} \dots b_{2l} \dots \\ r_3 &= 0, b_{31} b_{32} b_{33} \dots b_{3l} \dots \\ &\dots\dots\dots \\ r_j &= 0, b_{j1} b_{j2} b_{j3} \dots b_{jl} \dots \\ &\dots\dots\dots \end{aligned}$$

Definiamo ora un numero reale $s = 0, c_1 c_2 c_3 \dots c_l \dots$ ponendo, per ogni $i \geq 1$,

$$c_i = \begin{cases} 7 & \text{se } b_{ii} \leq 5, \\ 3 & \text{se } b_{ii} > 5. \end{cases}$$

Si noti che, per costruzione, $c_i \neq b_{ii}$, per ogni $i \geq 1$.

Poiché abbiamo supposto che la funzione $i \mapsto r_i$, sia biiettiva, e poiché ovviamente $s \in I$, deve essere $s = r_h$, per qualche $h \geq 1$. Tuttavia, dalla costruzione di s , risulta che $s \neq r_h$, per ogni $h \in \mathbb{N}^*$; infatti l' h -esima cifra decimale c_h di s è, per costruzione, diversa dalla h -esima cifra decimale b_{hh} di r_h . Questa contraddizione deriva dall'aver supposto che I sia numerabile, quindi I non può essere numerabile. \square

Dato che $\mathbb{N} \subset \mathbb{R}$ e dato che \mathbb{R} non è numerabile, si ha quindi $|\mathbb{N}| < |\mathbb{R}|$.

DEFINIZIONE 2.26. La cardinalità di \mathbb{R} è indicata con \mathfrak{c} , e detta la *cardinalità del continuo*.

Possiamo quindi scrivere

$$\aleph_0 < \mathfrak{c}.$$

Ora ci proponiamo di dimostrare che, per la precisione, è $\mathfrak{c} = 2^{\aleph_0}$, cioè che $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

TEOREMA 2.27. *La cardinalità \mathfrak{c} dell'insieme dei numeri reali è uguale alla cardinalità 2^{\aleph_0} dell'insieme delle parti di \mathbb{N} .*

DIMOSTRAZIONE. Dato che $|\mathbb{R}| = |I|$, è sufficiente dimostrare che esiste una biiezione tra I e $\mathcal{P}(\mathbb{N})$.

Sia M l'insieme di tutte le funzioni $f : \mathbb{N} \rightarrow \{0, 1\}$. Abbiamo già osservato (nel corso della dimostrazione del Corollario 2.19) che esiste una biiezione tra M e $\mathcal{P}(\mathbb{N})$. Basta quindi dimostrare che $|M| = |I|$. Per fare ciò utilizzeremo la rappresentazione dei numeri reali in base 2. Osserviamo che ogni $r \in I$ ha una rappresentazione della forma

$$r = 0, b_0 b_1 b_2 \dots b_j \dots$$

con $b_j \in \{0, 1\}$, per ogni $j \geq 0$, e ove i b_j non sono tutti nulli (dato che $0 \notin I$). Inoltre, affinché una tale rappresentazione sia unica, è necessario richiedere che non esista alcun indice j tale che $b_h = 1$ per ogni $h \geq j$.

Al numero $r = 0, b_0 b_1 b_2 \dots b_j \dots$ possiamo quindi associare la funzione $f_r : \mathbb{N} \rightarrow \{0, 1\}$, $i \mapsto b_i$. In questo modo si ottiene una funzione $F : I \rightarrow M$, definita ponendo $F(r) = f_r$. Dall'unicità della rappresentazione di r si deduce che F è iniettiva.

Indichiamo con M' l'immagine di F . M' è il sottoinsieme di M costituito da tutte le funzioni $f : \mathbb{N} \rightarrow \{0, 1\}$, non identicamente nulle, tali che non esista alcun indice j per cui si abbia $f(h) = 1$, per ogni $h \geq j$.

Vogliamo ora dimostrare che $|M'| = |M|$.

Per ogni $j \in \mathbb{N}$ poniamo

$$V_j = \{f \in M \mid f(h) = 1, \forall h \geq j\}.$$

Si noti che $V_j \subseteq V_{j+1}$, per ogni j .

Poniamo $V = \bigcup_{j \in \mathbb{N}} V_j$ e indichiamo infine con $f_0 \in M$ la funzione identicamente nulla, $f_0(h) = 0$, per ogni $h \in \mathbb{N}$. Da quanto osservato in precedenza, si deduce che

$$M' = M \setminus (V \cup \{f_0\}).$$

Tutti gli insiemi V_j hanno un numero finito di elementi. Più precisamente, $|V_j| = 2^j$, per ogni $j \geq 0$. Di conseguenza, l'insieme V è numerabile, in quanto unione numerabile di insiemi finiti (cf. Proposizione 1.15). Anche $V \cup \{f_0\}$ è dunque numerabile e, per il Teorema 2.17, si ha

$$|V \cup \{f_0\}| = \aleph_0 < |M| = 2^{\aleph_0}.$$

Ma allora, per il Corollario 2.10, si ha

$$|M'| = |M \setminus (V \cup \{f_0\})| = |M|.$$

Poiché abbiamo già dimostrato che l'insieme M' è in biiezione con I , si ha

$$|I| = |M'| = |M| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0},$$

come volevasi dimostrare. \square

OSSERVAZIONE 2.28. Possiamo osservare come la dimostrazione precedente risulti complicata dalla mancanza di unicità della rappresentazione di un numero reale in base 2 (ciò ci obbligava a considerare il sottoinsieme M' di M).

Un modo diverso per contornare questo ostacolo è il seguente. Ad ogni funzione $f \in M$, associamo la sequenza

$$0, b_0 b_1 b_2 \dots b_j \dots,$$

ove $b_i = f(i)$, ma ora interpretiamo questa come l'espressione di un numero reale r in base 3 e non in base 2. Poiché le sequenze così ottenute non contengono il numero 2, sequenze diverse rappresentano numeri reali diversi. In questo modo si ottiene una funzione iniettiva $M \rightarrow \mathbb{R}$, da cui si deduce che $|M| \leq |\mathbb{R}|$. Dato che $|M| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$, si ha quindi $2^{\aleph_0} \leq \mathfrak{c}$.

Consideriamo ora la funzione $F : \mathbb{R} \rightarrow \mathcal{P}(\mathbb{Q})$ definita ponendo

$$F(r) = \{q \in \mathbb{Q} \mid q \leq r\}.$$

Dalla densità di \mathbb{Q} in \mathbb{R} segue che F è iniettiva, quindi $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})|$. Ma \mathbb{Q} è numerabile, cioè $|\mathbb{Q}| = \aleph_0$, da cui si deduce che $|\mathcal{P}(\mathbb{Q})| = 2^{\aleph_0}$. Abbiamo così dimostrato che è anche $\mathfrak{c} \leq 2^{\aleph_0}$.

Da queste due disuguaglianze, e dal Teorema 2.2, si deduce l'uguaglianza $\mathfrak{c} = 2^{\aleph_0}$.

Per terminare questa sezione, vogliamo ora studiare la cardinalità del sottoinsieme di \mathbb{R} costituito dai numeri algebrici.

DEFINIZIONE 2.29. Un numero reale r è detto *algebrico* se esiste un polinomio non nullo a coefficienti razionali $p(x) \in \mathbb{Q}[x]$ tale che $p(r) = 0$. Un numero reale è detto *trascendente* se esso non è algebrico.

Indicheremo con $\overline{\mathbb{Q}}$ il sottoinsieme di \mathbb{R} costituito dai numeri algebrici.

OSSERVAZIONE 2.30. Ogni numero razionale $q \in \mathbb{Q}$ è un numero algebrico; esso è infatti lo zero del polinomio $p(x) = x - q$. Quindi $\mathbb{Q} \subset \overline{\mathbb{Q}}$.

\mathbb{Q} è un sottoinsieme proprio di $\overline{\mathbb{Q}}$; infatti moltissimi numeri irrazionali sono algebrici. Ad esempio $\sqrt{2}$ è uno zero del polinomio $x^2 - 2$, quindi è algebrico. Anche un numero quale $\sqrt{2} + \sqrt{3}$ è algebrico; esso è infatti uno zero del polinomio $x^4 - 10x^2 + 1$. In effetti, trovare dei numeri trascendenti non è un'impresa molto facile. Un esempio di tali numeri è dato da e e π , ma la dimostrazione della loro trascendenza è complicata.

Come ora vedremo, anche l'insieme dei numeri algebrici è numerabile.

TEOREMA 2.31. *L'insieme $\overline{\mathbb{Q}}$ è numerabile.*

DIMOSTRAZIONE. Sia $\mathbb{Q}[x]$ l'insieme dei polinomi in una indeterminata a coefficienti razionali e indichiamo con $\mathbb{Q}[x]_n$ l'insieme dei polinomi di grado $\leq n$ (compreso il polinomio nullo). Dato che ogni polinomio in $\mathbb{Q}[x]_n$ può essere scritto in modo unico nella forma

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

con $a_0, a_1, \dots, a_n \in \mathbb{Q}$, la funzione

$$\mathbb{Q}[x]_n \rightarrow \mathbb{Q}^{n+1}, \quad p(x) \mapsto (a_0, a_1, \dots, a_n)$$

è biiettiva, il che significa che $|\mathbb{Q}[x]_n| = |\mathbb{Q}^{n+1}|$.

Poiché \mathbb{Q} è numerabile, si ha $|\mathbb{Q}^{n+1}| = |\mathbb{N}|$ (cf. Corollario 1.14), quindi l'insieme $\mathbb{Q}[x]_n$ è numerabile. Di conseguenza, l'insieme

$$\mathbb{Q}[x] = \bigcup_{n \in \mathbb{N}} \mathbb{Q}[x]_n$$

è anch'esso numerabile, in quanto unione numerabile di insiemi numerabili (cf. Proposizione 1.15).

Per ogni polinomio non nullo $f \in \mathbb{Q}[x]$ indichiamo con

$$Z(f) = \{r \in \mathbb{R} \mid f(r) = 0\}$$

il suo insieme degli zeri. Osserviamo che gli insiemi $Z(f)$ sono finiti, in quanto un polinomio non nullo di grado n possiede, al più, n zeri reali.

Dalla definizione di numero algebrico si ha

$$\overline{\mathbb{Q}} = \bigcup_{0 \neq f \in \mathbb{Q}[x]} Z(f).$$

Poiché abbiamo dimostrato in precedenza che $\mathbb{Q}[x]$ è numerabile, $\overline{\mathbb{Q}}$ è dunque un'unione numerabile di insiemi finiti, quindi è anch'esso numerabile, come volevasi dimostrare. \square

COROLLARIO 2.32. *Sia $\mathbb{T} = \mathbb{R} \setminus \overline{\mathbb{Q}}$ l'insieme dei numeri trascendenti. Allora $|\mathbb{T}| = |\mathbb{R}|$.*

DIMOSTRAZIONE. Poiché $\mathbb{R} = \mathbb{T} \cup \overline{\mathbb{Q}}$, \mathbb{T} deve necessariamente essere infinito, altrimenti si avrebbe $|\mathbb{R}| = |\overline{\mathbb{Q}}| = \aleph_0$, il che non è vero. Per la Proposizione 1.10 si ha quindi $|\mathbb{N}| \leq |\mathbb{T}|$. Dato che $|\overline{\mathbb{Q}}|$ è numerabile, dal Corollario 2.9 segue che $|\mathbb{T} \cup \overline{\mathbb{Q}}| = |\mathbb{T}|$. Ma ciò significa proprio che $|\mathbb{R}| = |\mathbb{T}|$. \square

Questo corollario mostra che i numeri trascendenti non solo esistono ma sono, in realtà, molti di più dei numeri algebrici!

OSSERVAZIONE 2.33. Poiché abbiamo dimostrato che la cardinalità \aleph_0 di \mathbb{N} è strettamente minore della cardinalità \mathfrak{c} di \mathbb{R} , sorge spontanea la domanda se esistano o meno delle cardinalità strettamente comprese tra \aleph_0 e \mathfrak{c} , cioè se esista una cardinalità, che potremmo chiamare \aleph_1 , tale che

$$\aleph_0 < \aleph_1 < \mathfrak{c}$$

(la non esistenza di una tale cardinalità è nota come “ipotesi del continuo”).

La sorprendente risposta a questa domanda, trovata da P. Cohen⁶ nel 1963, è che tale questione è indipendente dagli assiomi usuali della teoria degli insiemi (assiomi di Zermelo–Fraenkel) e anche dall'Assioma della Scelta. In altre parole, all'interno della teoria classica degli insiemi non è possibile dimostrare che una tale cardinalità \aleph_1 esiste, ma nemmeno che essa non esista! Sia l'esistenza di una tale \aleph_1 , che la sua non esistenza, possono quindi essere accettate come un nuovo assioma, ottenendo due diverse teorie entrambe prive di contraddizioni.

3. Il teorema del Buon Ordinamento

In questa sezione dimostreremo un risultato, per nulla intuitivo, che dipende dall'Assioma della Scelta.

DEFINIZIONE 3.1. Un insieme parzialmente ordinato S è detto *bene ordinato* se esso è totalmente ordinato e se ogni suo sottoinsieme non vuoto ammette minimo. Cioè, se per ogni $A \subseteq S$ esiste un elemento $a \in A$ tale che $a \leq x$, per ogni $x \in A$ (tale elemento è allora necessariamente

⁶P.J. Cohen, *The independence of the continuum hypothesis*, Proc. Nat. Acad. of Sci. USA (1963), 1143–1148, (1964), 105–110.

unico). Una relazione d'ordine \leq su un insieme S è detta un *buon ordinamento* se (S, \leq) è un insieme bene ordinato.

DEFINIZIONE 3.2. Sia S un insieme totalmente ordinato e sia T un sottoinsieme di S dotato dell'ordine indotto da S . Diremo che T è un *segmento iniziale* di S se

$$x \in T, y \in S, y \leq x \Rightarrow y \in T.$$

ESEMPIO 3.3. Ogni insieme finito può essere bene ordinato, basta scegliere un qualsiasi ordine totale tra i suoi elementi.

L'insieme \mathbb{N} dei numeri naturali è bene ordinato. Da ciò si deduce che ogni insieme numerabile può essere bene ordinato. Infatti, se D è un insieme numerabile e se $f : D \rightarrow \mathbb{N}$ è una funzione biettiva, ponendo, per ogni $d_1, d_2 \in D$,

$$d_1 \leq d_2 \Leftrightarrow f(d_1) \leq f(d_2)$$

si definisce un ordine totale su D che risulta essere un buon ordinamento.

ESEMPIO 3.4. Sia S un insieme bene ordinato e sia y un elemento di qualche insieme, tale che $y \notin S$. Sia $S' = S \cup \{y\}$. Estendiamo la relazione d'ordine a S' ponendo $x \leq y$, per ogni $x \in S$. L'insieme S' risulta essere totalmente ordinato e anche bene ordinato.

TEOREMA 3.5 (T. del Buon Ordinamento). *Ogni insieme non vuoto può essere bene ordinato.*

DIMOSTRAZIONE. Sia S un insieme non vuoto. Indichiamo con \mathcal{S} l'insieme di tutte le coppie (X, ω) , dove X è un sottoinsieme di S e ω è un buon ordinamento su X . Si noti che \mathcal{S} non è vuoto dato che ogni singolo elemento di S dà luogo a una tale coppia. Se (X, ω) e (X', ω') sono due elementi di \mathcal{S} , poniamo $(X, \omega) \leq (X', \omega')$ se $X \subseteq X'$, se l'ordine indotto su X da ω' è uguale a ω e se (X, ω) è un segmento iniziale di (X', ω') . In questo modo risulta definito un ordine parziale su \mathcal{S} . Dimostriamo ora che \mathcal{S} è un insieme induttivo.

Sia $T = \{(X_i, \omega_i)\}_{i \in I}$ una catena in \mathcal{S} e poniamo $X = \bigcup_{i \in I} X_i$. Se $a, b \in X$ allora a e b appartengono a uno stesso X_i , per qualche indice i . Definiamo allora $a \leq b$ in X se è $a \leq b$ rispetto all'ordine ω_i di X_i . Si verifica facilmente che ciò non dipende dal particolare indice i scelto. L'insieme X risulta così essere totalmente ordinato. In effetti, esso è anche bene ordinato. Infatti, se Y è un sottoinsieme non vuoto di X , allora esiste un elemento $y \in Y$, quindi $y \in X_i$, per qualche $i \in I$. Consideriamo allora il sottoinsieme $Y \cap X_i$ di X_i . Dato che X_i è bene ordinato, esiste un elemento c che è il minimo di $Y \cap X_i$. Si verifica che tale elemento non dipende dall'indice i scelto ed è, in effetti, il minimo di Y . Possiamo dunque applicare il Lemma di Zorn all'insieme \mathcal{S} . Sia (X, ω) un elemento massimale in \mathcal{S} . Se fosse $X \neq S$ allora esisterebbe un elemento $s \in S$ tale che $s \notin X$.

Utilizzando il metodo descritto nell'Esempio 3.4, si può definire un buon ordinamento sull'insieme $X' = X \cup \{s\}$. Ma questo contraddice la massimalità di (X, ω) . Si deve quindi avere $X = S$, il che dimostra che esiste un buon ordinamento su S , come volevasi dimostrare. \square

Come abbiamo visto, il Teorema del Buon Ordinamento dipende dall'Assioma della Scelta. Esso infatti è una conseguenza diretta del Lemma di Zorn, il quale, a sua volta, dipende dall'Assioma della Scelta.

Ora dimostreremo che il Teorema del Buon Ordinamento implica l'Assioma della Scelta. In questo modo si prova che l'Assioma della Scelta, il Lemma di Zorn e il Teorema del Buon Ordinamento sono tra loro equivalenti.

PROPOSIZIONE 3.6. *Se ogni insieme non vuoto può essere bene ordinato allora vale l'Assioma della Scelta.*

DIMOSTRAZIONE. Sia X un insieme di insiemi non vuoti e consideriamo l'insieme $S = \bigcup_{A \in X} A$. Per ipotesi esiste un buon ordinamento su S , quindi ogni sottoinsieme non vuoto di S ammette minimo. Per ogni $A \in X$ indichiamo dunque con m_A il suo minimo rispetto all'ordine fissato su S . In questo modo si ottiene una "regola" che permette di scegliere un singolo elemento da ogni insieme A che appartiene a X . Ciò dimostra che vale l'Assioma della Scelta. \square

CAPITOLO 2

Spazi Vettoriali

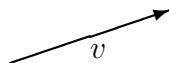
1. Vettori Geometrici

Il concetto di vettore viene spesso introdotto ricorrendo a delle motivazioni che provengono dalla fisica. In fisica infatti, accanto a grandezze che possono essere adeguatamente espresse con un singolo numero, come ad esempio la temperatura o il tempo, ce ne sono altre la cui descrizione richiede più informazioni. Per descrivere, ad esempio, lo spostamento di un punto, la sola informazione numerica relativa alla “misura” di tale spostamento non basta; è necessario specificare anche la retta lungo la quale avviene lo spostamento e, per finire, occorre specificare anche il verso di percorrenza di tale retta. In modo analogo, per specificare una forza, occorre fornire il valore numerico dell’entità di tale forza (in una qualche unità di misura) assieme alla direzione e al verso di applicazione della forza (in molti casi ciò non è ancora sufficiente, ed occorre specificare anche il punto di applicazione della forza).

Per motivare le considerazioni che faremo nel seguito, ricorreremo al concetto geometrico di “movimento” o, più precisamente, alla nozione di *traslazione* in un piano.

In base a ciò che abbiamo appena detto, per descrivere una traslazione è necessario specificare una retta (la *direzione* in cui avviene lo spostamento), un *verso* di percorrenza di tale retta e, infine, un *numero* che, in qualche modo, misura l’entità di tale traslazione.

Un modo particolarmente comodo per esprimere graficamente tutte queste informazioni è quello di utilizzare un *segmento orientato*



La retta su cui giace questo segmento individua la direzione, la freccia posta in una delle estremità specifica il verso di percorrenza e la lunghezza del segmento stesso (espressa in qualche unità di misura) determina l’entità dello spostamento.

Un oggetto di questo tipo è chiamato *vettore*. Dato un vettore v , rappresentato da un segmento orientato come sopra, la lunghezza di tale segmento è detta il *modulo* (o la *norma*) di v , ed è indicata con $|v|$ (oppure con $\|v\|$).

A questo punto è forse necessaria una precisazione. Un vettore v non descrive lo spostamento di un qualche punto fissato A verso un

qualche altro punto B ; esso descrive una traslazione di tutto il piano (o di tutto lo spazio). In tal senso, non ha alcuna importanza “dove” si disegni il segmento che rappresenta graficamente il vettore. In altre parole, due diversi segmenti orientati che abbiamo, tuttavia, la stessa direzione (cioè che si trovino su due rette parallele), lo stesso verso e la stessa lunghezza, sono due rappresentazioni grafiche diverse dello stesso vettore.

Questa idea può essere resa matematicamente precisa nel modo seguente.

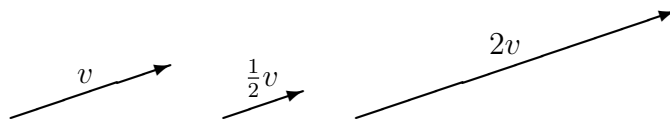
DEFINIZIONE 1.1. Due segmenti orientati sono detti *equipollenti* se hanno la stessa direzione (cioè sono contenuti in due rette parallele), lo stesso verso e la stessa lunghezza.

Si verifica facilmente che la relazione di equipollenza è una relazione di equivalenza nell'insieme di tutti i segmenti orientati. Possiamo quindi dare la seguente definizione di vettore:

DEFINIZIONE 1.2. Un *vettore (geometrico)* è una classe di equipollenza di segmenti orientati.

OSSERVAZIONE 1.3. Come abbiamo già fatto notare, a volte è importante specificare anche il punto in cui un vettore si intende “applicato” (come nel caso di una forza). Ciò porta alla definizione della nozione di *vettore applicato*, che deve essere inteso come una coppia (P, v) costituita da un punto P (il punto di applicazione) e da un vettore v .

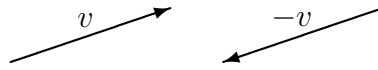
Nell'insieme dei vettori geometrici sono definite, in modo del tutto naturale, due operazioni. La prima consiste nella moltiplicazione di un vettore v per un numero (reale) λ . Se v rappresenta una determinata traslazione e se $\lambda > 0$, il vettore λv rappresenta una traslazione che avviene nella stessa direzione e nello stesso verso di quella rappresentata da v , ma determina uno spostamento pari a λ volte quello effettuato dalla traslazione rappresentata da v . Il vettore λv è quindi rappresentato da un segmento orientato che ha la stessa direzione e verso di v , ma una lunghezza pari alla lunghezza di v moltiplicata per λ .



Se $\lambda = 0$ si ottiene un vettore di lunghezza nulla, che corrisponde a una “traslazione nulla.” In questo caso le nozioni di direzione e verso non hanno più alcun significato; il segmento orientato si riduce a un punto, il quale non ha più alcuna direzione e alcun verso.

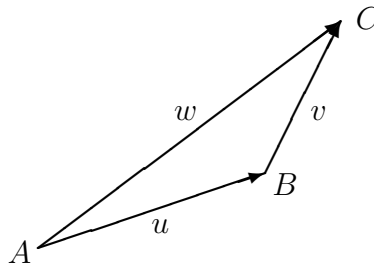
Se $\lambda < 0$ si intende che il vettore λv rappresenta una traslazione che avviene nella stessa direzione ma nel verso opposto a quella rappresentata da v , per uno spostamento pari al valore assoluto di λ moltiplicato

per lo spostamento effettuato dalla traslazione rappresentata da v .



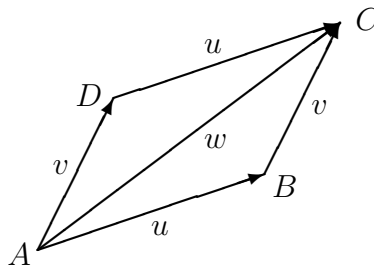
In questo modo si ha che la composizione delle traslazioni corrispondenti ai vettori λv e $-\lambda v$ è la traslazione nulla: $\lambda v + (-\lambda v) = 0$.

La seconda operazione che consideriamo è la *somma* di due vettori; essa corrisponde alla composizione di due traslazioni. Se u e v sono due vettori, la loro somma $w = u + v$ è, per definizione, il vettore che rappresenta la traslazione che si ottiene effettuando prima la traslazione rappresentata da u e poi quella rappresentata da v . L'effetto di questa composizione di traslazioni è rappresentato nella figura seguente.



Se la traslazione rappresentata da u porta il punto A nel punto B e la traslazione rappresentata da v porta il punto B nel punto C , allora la composizione delle due traslazioni, rappresentata da $w = u + v$, porta il punto A nel punto C .

Si verifica immediatamente che la somma di vettori gode della proprietà commutativa, cioè $u + v = v + u$, come si può vedere nella figura seguente.



Questa figura illustra la cosiddetta *regola del parallelogramma*: il vettore $w = u + v$ è la diagonale del parallelogramma che ha come lati i vettori u e v .

Se fissiamo un sistema di coordinate cartesiane ortogonali OXY nel piano, ogni vettore v può essere rappresentato da una coppia di numeri reali (v_x, v_y) , che individuano le proiezioni di v sugli assi coordinati (vedi figura 1).

Possiamo quindi identificare il vettore v con la coppia $(v_x, v_y) \in \mathbb{R}^2$. In termini di questa identificazione, la somma dei due vettori $u = (u_x, u_y)$ e $v = (v_x, v_y)$ è data da

$$u + v = (u_x + v_x, u_y + v_y),$$

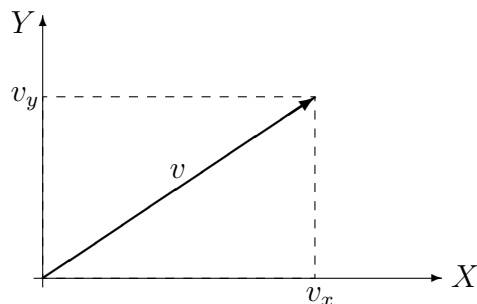


FIGURA 1. Decomposizione di un vettore nelle sue componenti

mentre il prodotto di un numero reale λ per il vettore $v = (v_x, v_y)$ è dato da

$$\lambda v = (\lambda v_x, \lambda v_y).$$

Usando queste formule è ora immediato verificare che la somma di vettori gode delle proprietà associative e commutativa. Esiste poi un elemento neutro per la somma, il *vettore nullo*, le cui componenti sono tutte nulle, e che indicheremo con $\mathbf{0} = (0, 0)$. Inoltre, per ogni vettore $v = (v_x, v_y)$ esiste il suo opposto $-v = (-v_x, -v_y)$, tale che $v + (-v) = \mathbf{0}$.

Tutto ciò si può riassumere dicendo che l'insieme dei vettori, con l'operazione di somma, forma un *gruppo abeliano*.

Consideriamo ora l'operazione di prodotto tra un numero reale e un vettore. È immediato verificare che questa operazione soddisfa le seguenti proprietà:

- (i) $(\lambda\mu)v = \lambda(\mu v)$,
- (ii) $\lambda(u + v) = \lambda u + \lambda v$,
- (iii) $(\lambda + \mu)v = \lambda v + \mu v$,
- (iv) $1v = v$,

per ogni $\lambda, \mu \in \mathbb{R}$ e per ogni coppia di vettori u e v .

L'insieme dei vettori ha quindi una struttura più ricca di quella di un semplice gruppo abeliano. A questo tipo di struttura daremo il nome di *spazio vettoriale*.

Prima di concludere osserviamo che delle considerazioni del tutto analoghe si possono fare per vettori nell'usuale spazio tridimensionale. Ad ogni tale vettore v si può associare una terna di numeri $(v_x, v_y, v_z) \in \mathbb{R}^3$, i quali rappresentano le proiezioni di v sui tre assi coordinati di un opportuno sistema di riferimento $OXYZ$ fissato, come mostrato nella figura 2.

Si ottiene in questo modo un'identificazione tra vettori dello spazio tridimensionale e terne di numeri reali, in termini della quale la somma di due vettori $u = (u_x, u_y, u_z)$ e $v = (v_x, v_y, v_z)$ è data da

$$u + v = (u_x + v_x, u_y + v_y, u_z + v_z),$$

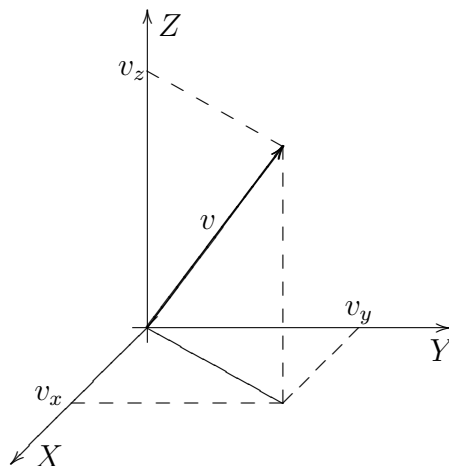


FIGURA 2. Decomposizione di un vettore nelle sue componenti

e il prodotto di un numero reale λ per un vettore $v = (v_x, v_y, v_z)$ è dato da

$$\lambda v = (\lambda v_x, \lambda v_y, \lambda v_z).$$

OSSERVAZIONE 1.4. Prendendo spunto dalle considerazioni precedenti possiamo *definire* dei vettori a n componenti (vettori di uno spazio n -dimensionale) semplicemente identificandoli con delle n -uple di numeri reali, $v = (a_1, a_2, \dots, a_n) \in \mathbb{R}^n$. Le operazioni di somma di due vettori e di prodotto di un numero reale per un vettore saranno definite in modo analogo a quanto abbiamo già visto nel caso di \mathbb{R}^2 e di \mathbb{R}^3 :

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

e

$$\lambda (a_1, a_2, \dots, a_n) = (\lambda a_1, \lambda a_2, \dots, \lambda a_n).$$

Questa costruzione verrà ampiamente studiata (e opportunamente generalizzata) nelle prossime sezioni.

2. Spazi Vettoriali

Nella sezione precedente abbiamo dunque visto che i vettori sono degli “oggetti” che possono essere sommati tra loro e possono anche essere moltiplicati per dei numeri, in modo tale che le operazioni così definite soddisfino tutta una serie di proprietà, essenzialmente analoghe alle usuali proprietà che valgono per la somma e il prodotto tra numeri.

Se ora concentriamo la nostra attenzione non tanto sulla natura di tali “oggetti” (definiti in precedenza come classi di equipollenza di segmenti orientati), quanto piuttosto sull’esistenza di determinate operazioni tra di essi e sulle proprietà che, ragionevolmente, dovrebbero essere soddisfatte da queste operazioni, possiamo fornire una definizione astratta di “insieme di vettori” come un qualche insieme nel quale

sono definite un'operazione di somma tra i suoi elementi ed un'operazione di prodotto tra un elemento di tale insieme ed un numero, in modo tale che siano soddisfatte delle proprietà analoghe a quelle elencate nella sezione precedente.

Cerchiamo ora di rendere precise le idee espresse fin'ora.

Sia K un campo¹ (tanto per fissare le idee, si può supporre che K sia il campo \mathbb{Q} dei numeri razionali, oppure il campo \mathbb{R} dei numeri reali, oppure ancora il campo \mathbb{C} dei numeri complessi).

DEFINIZIONE 2.1. Uno *spazio vettoriale* su K è un insieme non vuoto V dotato di un'operazione $+_V$, detta *somma*,

$$+_V : V \times V \rightarrow V, \quad (v_1, v_2) \mapsto v_1 +_V v_2,$$

e di un'operazione \cdot_V

$$\cdot_V : K \times V \rightarrow V, \quad (\lambda, v) \mapsto \lambda \cdot_V v,$$

detta *prodotto per uno scalare*, che soddisfano le seguenti proprietà: per ogni $\lambda, \lambda_1, \lambda_2 \in K$ e ogni $v, v_1, v_2 \in V$ si ha

- (1) $(v_1 +_V v_2) +_V v_3 = v_1 +_V (v_2 +_V v_3)$;
- (2) $v_1 +_V v_2 = v_2 +_V v_1$;
- (3) esiste un elemento $\mathbf{0}_V \in V$ tale che $v +_V \mathbf{0}_V = \mathbf{0}_V +_V v = v$;
- (4) per ogni $v \in V$ esiste un elemento $v' \in V$ tale che $v +_V v' = v' +_V v = \mathbf{0}_V$. Tale elemento v' viene indicato con $-v$ e detto l'opposto di v ;
- (5) $\lambda \cdot_V (v_1 +_V v_2) = (\lambda \cdot_V v_1) +_V (\lambda \cdot_V v_2)$;
- (6) $(\lambda_1 + \lambda_2) \cdot_V v = (\lambda_1 \cdot_V v) +_V (\lambda_2 \cdot_V v)$;
- (7) $(\lambda_1 \lambda_2) \cdot_V v = \lambda_1 \cdot_V (\lambda_2 \cdot_V v)$;
- (8) $1 \cdot_V v = v$.

Gli elementi di uno spazio vettoriale V sono detti *vettori*. Gli elementi del campo K sono detti *scalari*.

OSSERVAZIONE 2.2. Dalle proprietà sopra elencate segue che, in ogni spazio vettoriale V , si ha $0 \cdot_V v = \mathbf{0}_V$, per ogni $v \in V$. Infatti si ha:

$$v + 0 \cdot_V v = 1 \cdot_V v + 0 \cdot_V v = (1 + 0) \cdot_V v = v.$$

Sommando ad ambo i membri di questa uguaglianza l'opposto di v , si ottiene

$$-v + v + 0 \cdot_V v = -v + v = \mathbf{0}_V,$$

da cui segue $0 \cdot_V v = \mathbf{0}_V$.

Da ciò possiamo ora dedurre che $(-1) \cdot_V v = -v$. Infatti, si ha:

$$\mathbf{0}_V = 0 \cdot_V v = (1 - 1) \cdot_V v = 1 \cdot_V v + (-1) \cdot_V v = v + (-1) \cdot_V v,$$

¹Ricordiamo che un campo è un insieme dotato di due operazioni, che indicheremo con $+$ e \cdot , le quali soddisfano delle proprietà del tutto analoghe a quelle della somma e del prodotto di numeri razionali. Più precisamente, un campo è un anello commutativo con unità in cui ogni elemento diverso da 0 ammette un inverso moltiplicativo.

da cui segue che il vettore $(-1) \cdot_V v$ è l'opposto di v .

D'ora in poi l'operazione di somma in uno spazio vettoriale V sarà indicata semplicemente con $+$ mentre il simbolo del prodotto per uno scalare sarà omissivo: si scriverà quindi $v_1 + v_2$ al posto di $v_1 +_V v_2$ e λv al posto di $\lambda \cdot_V v$.

ESEMPIO 2.3. Sia $V = K^n$ e definiamo un'operazione di somma tra elementi di V ponendo

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n),$$

e un'operazione di prodotto tra elementi dal campo K ed elementi di V ponendo

$$\lambda (a_1, a_2, \dots, a_n) = (\lambda a_1, \lambda a_2, \dots, \lambda a_n).$$

È immediato verificare che V , con le operazioni appena definite, è uno spazio vettoriale su K .

ESEMPIO 2.4. Sia K un campo e indichiamo con $K[X]$ l'insieme dei polinomi a coefficienti in K nell'indeterminata X . Un generico elemento di $K[X]$ si scrive nella forma

$$p(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n,$$

per qualche $n \geq 0$, ove tutti i coefficienti a_i sono elementi di K .

Rispetto alle operazioni di somma di polinomi e di prodotto di un polinomio per un elemento di K , l'insieme $K[X]$ è uno spazio vettoriale.

ESEMPIO 2.5. Sia K un campo e sia S un insieme (non vuoto) qualsiasi. Indichiamo con K^S l'insieme di tutte le funzioni $f : S \rightarrow K$.

Date due funzioni $f, g \in K^S$ possiamo definire la loro somma ponendo

$$(f + g)(s) = f(s) + g(s),$$

e possiamo definire il prodotto di una funzione f per uno scalare $\lambda \in K$ ponendo,

$$(\lambda f)(s) = \lambda(f(s)),$$

per ogni $s \in S$.

Anche in questo caso è immediato verificare che l'insieme K^S , con le operazioni appena definite, è uno spazio vettoriale su K .

ESEMPIO 2.6. Sia $K = \mathbb{Q}$ il campo dei numeri razionali e sia $V = \mathbb{R}$. Rispetto alle usuali operazioni di somma e prodotto tra numeri, V risulta essere uno spazio vettoriale su K .

Più in generale, per ogni campo K e ogni estensione di campi $K \subset L$, L risulta essere uno spazio vettoriale su K .

OSSERVAZIONE 2.7. Vogliamo far notare che, nella definizione di spazio vettoriale, la proprietà (8) è necessaria. Infatti l'uguaglianza $1 \cdot_V v = v$ non discende dalle prime sette proprietà, come si può vedere dal seguente esempio.

Sia $V = K^n$. Definiamo la somma di vettori componente per componente (come nell'Esempio 2.3) e definiamo il prodotto di un vettore per un elemento di K come segue:

$$\lambda(a_1, a_2, \dots, a_n) = (0, 0, \dots, 0),$$

per ogni $\lambda \in K$ e ogni $(a_1, a_2, \dots, a_n) \in V$.

È immediato verificare che le due operazioni così definite verificano tutte le proprietà elencate nella definizione di spazio vettoriale, ad eccezione della (8).

OSSERVAZIONE 2.8. Si noti che nella definizione di spazio vettoriale non si usa mai il fatto che K sia un campo.

Una definizione del tutto analoga si può dare supponendo solo che K sia un anello commutativo (con unità). L'analogo di uno spazio vettoriale è chiamato, in questo caso, un *modulo* sull'anello K .

Tuttavia, come avremo occasione di osservare in seguito, molti risultati che dimostreremo per gli spazi vettoriali dipendono in modo essenziale dal fatto che K sia un campo e non valgono, invece, per un modulo su un anello. In effetti, la teoria dei moduli risulta essere profondamente diversa dalla teoria degli spazi vettoriali.

Terminiamo questa sezione con la seguente definizione:

DEFINIZIONE 2.9. Sia V uno spazio vettoriale su K . Una *combinazione lineare* di elementi di V è una somma finita del tipo

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n,$$

con $\lambda_1, \dots, \lambda_n \in K$ e $v_1, \dots, v_n \in V$.

2.1. Sottospazi vettoriali. Sia V uno spazio vettoriale definito sul campo K .

DEFINIZIONE 2.10. Un *sottospazio vettoriale* W di V è un sottoinsieme non vuoto $W \subseteq V$ tale che la restrizione a W delle operazioni di somma e di prodotto per uno scalare definite su V rende W uno spazio vettoriale sul campo K .

Dalla definizione si deduce che, affinché un sottoinsieme non vuoto W di V sia un sottospazio vettoriale, è necessario e sufficiente che valgano le seguenti proprietà:

- (1) per ogni $w_1, w_2 \in W$, si ha $w_1 + w_2 \in W$;
- (2) per ogni $w \in W$, anche $-w \in W$;
- (3) $\mathbf{0}_V \in W$;
- (4) per ogni $\lambda \in K$ e ogni $w \in W$, si ha $\lambda w \in W$.

In effetti, è sufficiente richiedere che W sia *chiuso* per le operazioni di somma e di prodotto per uno scalare, cioè che si abbia

$$w_1 + w_2 \in W, \quad \forall w_1, w_2 \in W$$

e

$$\lambda w \in W, \quad \forall \lambda \in K, \forall w \in W.$$

Queste due condizioni possono essere raggruppate in una sola:

PROPOSIZIONE 2.11. *Un sottoinsieme non vuoto W di uno spazio vettoriale V sul campo K è un sottospazio vettoriale di V se e solo se*

$$\lambda_1 w_1 + \lambda_2 w_2 \in W,$$

per ogni $\lambda_1, \lambda_2 \in K$ e ogni $w_1, w_2 \in W$.

DIMOSTRAZIONE. È immediato verificare che, sotto questa ipotesi, le operazioni di somma di vettori e di prodotto di un vettore per uno scalare definite in V rendono W un sottospazio vettoriale. \square

OSSERVAZIONE 2.12. Ogni spazio vettoriale V è, naturalmente, un sottospazio vettoriale di sé stesso. Inoltre $\{\mathbf{0}_V\}$ è banalmente un sottospazio vettoriale di V , detto il *sottospazio nullo*. A volte scriveremo semplicemente 0 per indicare il sottospazio $\{\mathbf{0}_V\}$ (il significato sarà chiaro dal contesto).

ESEMPIO 2.13. Sia $V = K^n$ e sia W l'insieme dei vettori $w = (x_1, x_2, \dots, x_n)$ che sono soluzioni di un'equazione lineare del tipo

$$a_1 x_1 + a_2 x_2 + \dots + a_n x_n = 0,$$

con $a_1, \dots, a_n \in K$ fissati.

È immediato verificare che una combinazione lineare di due elementi di W fornisce ancora una soluzione della precedente equazione, quindi appartiene a W . Ciò significa che W è un sottospazio vettoriale di V .

Al contrario, l'insieme delle soluzioni di un'equazione del tipo

$$a_1 x_1 + a_2 x_2 + \dots + a_n x_n = k,$$

con $k \neq 0$, non è un sottospazio vettoriale di V , dato che non contiene il vettore nullo $\mathbf{0}$.

PROPOSIZIONE 2.14. *Se $\{W_i\}_{i \in I}$ è una famiglia di sottospazi vettoriali di uno spazio vettoriale V , allora anche la loro intersezione W*

$$W = \bigcap_{i \in I} W_i$$

è un sottospazio vettoriale di V .

DIMOSTRAZIONE. Siano $\lambda_1, \lambda_2 \in K$ e $w_1, w_2 \in W$. Allora $w_1, w_2 \in W_i$, per ogni $i \in I$, quindi anche $\lambda_1 w_1 + \lambda_2 w_2 \in W_i$, dato che W_i è un sottospazio vettoriale di V . Da ciò segue che $\lambda_1 w_1 + \lambda_2 w_2 \in W$. \square

OSSERVAZIONE 2.15. Una proprietà analoga non vale invece per l'unione: se W_1 e W_2 sono due sottospazi vettoriali di V , la loro unione $W_1 \cup W_2$ non è, in generale, un sottospazio vettoriale di V .

A titolo di esempio, consideriamo lo spazio vettoriale $V = K^2$. Poniamo $W_1 = \{(a, 0) \mid a \in K\}$ e $W_2 = \{(0, b) \mid b \in K\}$. È immediato verificare che essi sono due sottospazi vettoriali di V . Si ha $(1, 0) \in W_1$ e $(0, 1) \in W_2$, tuttavia la loro somma $(1, 1)$ non appartiene né a W_1 né a W_2 . Ciò dimostra che l'insieme $W_1 \cup W_2$ non è chiuso per l'operazione di somma, quindi non può essere un sottospazio vettoriale.

DEFINIZIONE 2.16. Sia S un sottoinsieme di uno spazio vettoriale V . Il *sottospazio vettoriale generato da S* , che indicheremo con $L(S)$, è il più piccolo² sottospazio vettoriale di V contenente S (se S è vuoto è quindi $L(S) = \{\mathbf{0}\}$).

Dato che l'intersezione di una famiglia di sottospazi vettoriali di V è un sottospazio vettoriale di V , è immediato verificare che $L(S)$ coincide con l'intersezione di tutti i sottospazi vettoriali di V che contengono S .

Un'altra descrizione, ancora più esplicita, di $L(S)$ è data dalla seguente proposizione.

PROPOSIZIONE 2.17. Il sottospazio vettoriale $L(S)$ generato da S è l'insieme di tutte le combinazioni lineari finite di elementi di S , cioè

$$L(S) = \left\{ \sum_{i=1}^n \lambda_i v_i \mid n \in \mathbb{N}, \lambda_i \in K, v_i \in S \right\},$$

dove si intende che la combinazione lineare di zero elementi di S è il vettore nullo $\mathbf{0} \in V$.

DIMOSTRAZIONE. Poniamo

$$\Lambda(S) = \left\{ \sum_{i=1}^n \lambda_i v_i \mid n \in \mathbb{N}, \lambda_i \in K, v_i \in S \right\}.$$

Ovviamente $S \subseteq \Lambda(S)$. Notiamo che ogni sottospazio vettoriale di V contenente S contiene anche tutte le combinazioni lineari finite di elementi di S , quindi contiene $\Lambda(S)$. Da ciò segue che $\Lambda(S)$ è contenuto nell'intersezione di tutti i sottospazi vettoriali di V che contengono S , quindi $\Lambda(S) \subseteq L(S)$.

D'altra parte è evidente che $\Lambda(S)$ è anch'esso un sottospazio vettoriale di V : infatti la combinazione lineare di due combinazioni lineari finite di elementi di S è essa stessa una combinazione lineare finita di elementi di S . Poiché $L(S)$ è il più piccolo sottospazio vettoriale di V contenente S , si ha dunque $L(S) \subseteq \Lambda(S)$, da cui segue che $L(S) = \Lambda(S)$. \square

OSSERVAZIONE 2.18. Se $S = \{v_1, v_2, \dots, v_n\}$, il sottospazio vettoriale $L(S)$ viene anche indicato con $\langle v_1, v_2, \dots, v_n \rangle$.

²Più piccolo, inteso rispetto alla relazione d'ordine data dall'inclusione.

Come abbiamo già osservato, nel contesto degli spazi vettoriali l'operazione di unione di due sottospazi non ha delle buone proprietà: infatti l'unione di due sottospazi vettoriali non è, in generale, un sottospazio vettoriale (vedi l'Osservazione 2.15). Tale operazione viene quindi sostituita dall'operazione di somma:

DEFINIZIONE 2.19. Se W_1 e W_2 sono sottospazi vettoriali di V , la loro *somma* $W_1 + W_2$ è il sottospazio vettoriale $L(W_1 \cup W_2)$ generato da $W_1 \cup W_2$. Tale definizione si generalizza, in modo ovvio, al caso della somma di una famiglia qualsiasi (anche infinita) di sottospazi di V .

Una descrizione esplicita della somma di due sottospazi vettoriali è fornita dalla seguente proposizione:

PROPOSIZIONE 2.20. *Si ha*

$$W_1 + W_2 = \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}.$$

DIMOSTRAZIONE. È immediato verificare che l'insieme

$$\{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}$$

è un sottospazio vettoriale di V che contiene W_1 e W_2 , quindi contiene anche la loro unione. Poiché $W_1 + W_2$ è, per definizione, il più piccolo sottospazio vettoriale di V contenente $W_1 \cup W_2$, si ha l'inclusione

$$W_1 + W_2 \subseteq \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}.$$

D'altra parte, ogni vettore del tipo $w_1 + w_2$ appartiene necessariamente a $W_1 + W_2$. Questo dimostra che vale anche l'inclusione opposta e quindi l'uguaglianza. \square

OSSERVAZIONE 2.21. Un risultato del tutto analogo vale anche per la somma di una famiglia finita di sottospazi vettoriali di V . Si ha cioè

$$W_1 + \cdots + W_n = \{w_1 + \cdots + w_n \mid w_i \in W_i, \text{ per } i = 1, \dots, n\}.$$

Nel caso invece di una famiglia infinita $\{W_i\}_{i \in I}$ di sottospazi vettoriali, è facile verificare che la somma

$$\sum_{i \in I} W_i$$

coincide con l'insieme di tutte le somme *finite* di vettori $w_i \in W_i$.

DEFINIZIONE 2.22. La somma di due sottospazi vettoriali W_1 e W_2 di V si dice *diretta*, e si indica con $W_1 \oplus W_2$, se $W_1 \cap W_2 = \{\mathbf{0}\}$.

Più in generale, la somma di una famiglia qualsiasi $\{W_i\}_{i \in I}$ di sottospazi vettoriali di V si dice *diretta* se $W_i \cap W_j = \{\mathbf{0}\}$, per ogni $i, j \in I$ con $i \neq j$. La somma diretta di una famiglia $\{W_i\}_{i \in I}$ di sottospazi di V si indica con

$$\bigoplus_{i \in I} W_i.$$

PROPOSIZIONE 2.23. *Ogni vettore $v \in W_1 \oplus W_2$ si scrive in modo unico nella forma $v = w_1 + w_2$, per qualche $w_1 \in W_1$ e qualche $w_2 \in W_2$ (un risultato analogo vale anche per una somma diretta di un numero qualunque di sottospazi di V).*

DIMOSTRAZIONE. Nella proposizione precedente abbiamo visto che ogni $v \in W_1 \oplus W_2$ si può scrivere nella forma $v = w_1 + w_2$, per qualche $w_1 \in W_1$ e qualche $w_2 \in W_2$. Dobbiamo solo dimostrare che tale scrittura è unica.

Supponiamo che si abbia

$$v = w_1 + w_2 = w'_1 + w'_2,$$

con $w_1, w'_1 \in W_1$ e $w_2, w'_2 \in W_2$. Allora si ha

$$w_1 - w'_1 = w'_2 - w_2 \in W_1 \cap W_2.$$

Poiché la somma di W_1 e W_2 è diretta, si ha $W_1 \cap W_2 = \{\mathbf{0}\}$, quindi $w_1 - w'_1 = w'_2 - w_2 = \mathbf{0}$, da cui si deduce che $w_1 = w'_1$ e $w_2 = w'_2$. \square

OSSERVAZIONE 2.24. La somma diretta di due sottospazi di uno spazio vettoriale V , definita in precedenza, è anche detta *somma diretta interna*. Ora vedremo come sia possibile definire anche la somma diretta di due spazi vettoriali V e W qualunque, in modo tale che V e W si possano poi identificare con due sottospazi vettoriali di $V \oplus W$. Una tale somma è detta *somma diretta esterna*.

Siano dunque V e W due spazi vettoriali sul campo K . Sul prodotto cartesiano $V \times W$ definiamo un'operazione di somma ponendo

$$(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2),$$

e un'operazione di prodotto per un elemento di K ponendo

$$\lambda(v_1, w_1) = (\lambda v_1, \lambda w_1),$$

per ogni $(v_1, w_1), (v_2, w_2) \in V \times W$ e ogni $\lambda \in K$. È immediato verificare che queste operazioni definiscono una struttura di spazio vettoriale su $V \times W$. Indichiamo con $V \oplus W$ lo spazio vettoriale così ottenuto.

Le due funzioni $i_V : V \rightarrow V \oplus W$, $v \mapsto (v, \mathbf{0}_W)$ e $i_W : W \rightarrow V \oplus W$, $w \mapsto (\mathbf{0}_V, w)$ sono iniettive e permettono di identificare i due spazi vettoriali V e W con i due sottospazi vettoriali $i_V(V) = V \times \{\mathbf{0}_W\}$ e $i_W(W) = \{\mathbf{0}_V\} \times W$ di $V \oplus W$. Si verifica facilmente che lo spazio vettoriale $V \oplus W$ appena definito coincide con la somma diretta (interna) dei suoi due sottospazi $i_V(V)$ e $i_W(W)$.

Più in generale, se V_1, V_2, \dots, V_n sono una famiglia finita di spazi vettoriali sul campo K è possibile definire, in modo naturale, una struttura di spazio vettoriale sul prodotto cartesiano $V_1 \times V_2 \times \dots \times V_n$, ponendo

$$(v_1, v_2, \dots, v_n) + (w_1, w_2, \dots, w_n) = (v_1 + w_1, v_2 + w_2, \dots, v_n + w_n)$$

e

$$\lambda(v_1, v_2, \dots, v_n) = (\lambda v_1, \lambda v_2, \dots, \lambda v_n),$$

per ogni $\lambda \in K$ e ogni $(v_1, \dots, v_n), (w_1, \dots, w_n) \in V_1 \times \dots \times V_n$. Ogni V_i si identifica in modo naturale con il sottospazio V_i' del prodotto cartesiano $V_1 \times \dots \times V_n$ che consiste di tutti gli elementi del tipo $(0, \dots, 0, v, 0, \dots, 0)$, al variare di $v \in V_i$ (il vettore v si trova nella i -esima posizione). È ora immediato verificare che la somma diretta di tutti questi sottospazi V_i' coincide con il prodotto cartesiano $V_1 \times \dots \times V_n$. Si definisce pertanto la somma diretta esterna della famiglia di spazi vettoriali V_1, V_2, \dots, V_n ponendo

$$\bigoplus_{i=1}^n V_i = \prod_{i=1}^n V_i.$$

In conclusione, possiamo riassumere quanto visto finora, dicendo che, nel caso di una famiglia *finita* di spazi vettoriali, la somma diretta coincide con il prodotto cartesiano. Come vedremo in seguito, tale uguaglianza non vale nel caso della somma diretta di una famiglia di infiniti spazi vettoriali.

2.2. Spazi vettoriali quoziente. Sia V uno spazio vettoriale sul campo K e sia W un sottospazio di V . Definiamo una relazione di equivalenza su V , che indicheremo con \equiv_W , ponendo

$$v \equiv_W v' \quad \text{se e solo se} \quad v - v' \in W.$$

Se indichiamo con $[v]$ la classe di equivalenza di un vettore $v \in V$, si ha

$$[v] = v + W = \{v + w \mid w \in W\}.$$

L'insieme quoziente V/\equiv_W sarà indicato con V/W . Vedremo ora che V/W ha una struttura naturale di spazio vettoriale su K .

Dati due elementi $[v_1], [v_2] \in V/W$, definiamo la loro somma ponendo

$$[v_1] + [v_2] = [v_1 + v_2].$$

Naturalmente, affinché questa sia una buona definizione, bisogna verificare che se $[v_1] = [v_1']$ e $[v_2] = [v_2']$, allora è anche $[v_1 + v_2] = [v_1' + v_2']$.

Dire che $[v_1] = [v_1']$ e $[v_2] = [v_2']$ equivale ad affermare che esistono due vettori $w_1, w_2 \in W$ tali che $v_1 - v_1' = w_1$ e $v_2 - v_2' = w_2$. Da ciò segue che $(v_1 + v_2) - (v_1' + v_2') = w_1 + w_2 \in W$, quindi $[v_1 + v_2] = [v_1' + v_2']$.

Definiamo poi il prodotto di un elemento $\lambda \in K$ per una classe di equivalenza $[v] \in V/W$ ponendo

$$\lambda \cdot [v] = [\lambda v].$$

Anche in questo caso è facile controllare che si tratta di una buona definizione.

È ora del tutto immediato verificare che l'insieme V/W , con le due operazioni appena definite, è uno spazio vettoriale sul campo K . Esso è detto lo *spazio vettoriale quoziente* di V modulo il sottospazio W .

2.3. Insiemi di generatori e basi. Sia V uno spazio vettoriale su un campo K .

DEFINIZIONE 2.25. Un sottoinsieme $S \subseteq V$ è detto un *insieme di generatori di V* se $L(S) = V$. In tal caso si dice anche che S genera V .

Notiamo che ogni spazio vettoriale possiede dei sistemi di generatori: l'intero spazio V è banalmente un insieme di generatori di V .

Dalla Proposizione 2.17 segue che, se S è un insieme di generatori di V , ogni vettore $v \in V$ si può scrivere come combinazione lineare finita di elementi di S :

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n,$$

per qualche $v_1, \dots, v_n \in S$ e $\lambda_1, \dots, \lambda_n \in K$. Una tale espressione non è però, in generale, unica.

DEFINIZIONE 2.26. Un sottoinsieme $S \subseteq V$ è detto un *insieme libero* di vettori se esso ha la seguente proprietà: una combinazione lineare finita di elementi di S è il vettore nullo se e solo se tutti i coefficienti λ_i sono nulli. Cioè

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = \mathbf{0}$$

con $v_1, \dots, v_n \in S$, implica $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

Se $S = \{v_1, v_2, \dots, v_n\}$ è un insieme libero, diremo anche che i vettori v_1, v_2, \dots, v_n sono *linearmente indipendenti*.

Quindi i vettori $v_1, v_2, \dots, v_n \in V$ sono linearmente indipendenti se e solo se l'equazione

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = \mathbf{0}$$

ha come unica soluzione $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

OSSERVAZIONE 2.27. Se S è l'insieme costituito da un unico vettore v , dire che S è libero equivale a dire che $v \neq \mathbf{0}$.

Analogamente, si trova che se i vettori v_1, v_2, \dots, v_n sono linearmente indipendenti, essi devono essere tutti diversi da zero.

DEFINIZIONE 2.28. I vettori $v_1, v_2, \dots, v_n \in V$ si dicono *linearmente dipendenti* se essi non sono linearmente indipendenti, cioè se esistono degli scalari $\lambda_1, \lambda_2, \dots, \lambda_n \in K$, non tutti nulli, per cui si abbia

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = \mathbf{0}.$$

PROPOSIZIONE 2.29. I vettori $v_1, v_2, \dots, v_n \in V$ sono linearmente dipendenti se e solo se uno di essi può essere espresso come combinazione lineare dei rimanenti, cioè se e solo se esiste un indice i tale che si abbia

$$v_i = \sum_{j=1, j \neq i}^n \alpha_j v_j,$$

con $\alpha_j \in K$.

DIMOSTRAZIONE. Se i vettori v_1, v_2, \dots, v_n sono linearmente dipendenti, esiste una combinazione lineare

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n = \mathbf{0}$$

in cui i coefficienti λ_j non sono tutti nulli. Sia dunque i un indice tale che $\lambda_i \neq 0$. Possiamo quindi scrivere

$$\lambda_i v_i = -\lambda_1 v_1 - \dots - \lambda_{i-1} v_{i-1} - \lambda_{i+1} v_{i+1} - \dots - \lambda_n v_n,$$

da cui si ricava

$$v_i = -\frac{\lambda_1}{\lambda_i} v_1 - \dots - \frac{\lambda_{i-1}}{\lambda_i} v_{i-1} - \frac{\lambda_{i+1}}{\lambda_i} v_{i+1} - \dots - \frac{\lambda_n}{\lambda_i} v_n.$$

Viceversa, supponiamo che un vettore v_i sia combinazione lineare dei rimanenti, cioè che si abbia

$$v_i = \alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \dots + \alpha_n v_n.$$

Allora si ha

$$\alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} - v_i + \alpha_{i+1} v_{i+1} + \dots + \alpha_n v_n = \mathbf{0},$$

il che dimostra che i vettori v_1, \dots, v_n sono linearmente dipendenti. \square

OSSERVAZIONE 2.30. Notiamo che la dimostrazione della proposizione precedente dipende in modo essenziale dalla possibilità di poter dividere per un elemento non nullo $\lambda_i \in K$; è pertanto indispensabile che K sia un campo. Nel caso in cui V sia un modulo su un anello un analogo risultato non vale, come illustrato dal seguente esempio.

Sia $K = \mathbb{Z}$ e $V = \mathbb{Z}^2$. Consideriamo i tre elementi $u = (1, 2)$, $v = (2, 1)$ e $w = (3, 4)$. Essi sono linearmente dipendenti, infatti

$$5(1, 2) + 2(2, 1) - 3(3, 4) = 0,$$

tuttavia è facile verificare che nessuno di essi può essere espresso come combinazione lineare degli altri due.

Dimostriamo ora che, se un vettore si può scrivere come combinazione lineare di un insieme di vettori linearmente indipendenti, tale espressione è unica.

PROPOSIZIONE 2.31. *Siano $v_1, v_2, \dots, v_n \in V$ dei vettori linearmente indipendenti. Se $v \in V$ si può scrivere come combinazione lineare dei vettori v_1, v_2, \dots, v_n ,*

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n,$$

allora gli scalari $\lambda_1, \lambda_2, \dots, \lambda_n$ sono determinati in modo unico.

DIMOSTRAZIONE. Supponiamo che sia possibile scrivere v in due modi, come

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n,$$

e come

$$v = \mu_1 v_1 + \mu_2 v_2 + \dots + \mu_n v_n.$$

Allora si ha

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = \mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_n v_n,$$

che si può riscrivere come

$$(\lambda_1 - \mu_1)v_1 + (\lambda_2 - \mu_2)v_2 + \cdots + (\lambda_n - \mu_n)v_n = 0.$$

Poiché i vettori v_1, v_2, \dots, v_n sono linearmente indipendenti, si ha dunque

$$\lambda_1 - \mu_1 = 0, \lambda_2 - \mu_2 = 0, \dots, \lambda_n - \mu_n = 0,$$

il che dimostra che $\lambda_i = \mu_i$, per ogni $i = 1, \dots, n$. \square

Dalla proposizione appena dimostrata discende quindi che, se consideriamo un insieme di generatori S di V con la proprietà aggiuntiva che i vettori di S siano linearmente indipendenti, allora ogni vettore di V si può scrivere, in modo *unico*, come combinazione lineare finita di elementi di S .

DEFINIZIONE 2.32. Un insieme libero di generatori di uno spazio vettoriale V è detto una *base* di V . In altri termini, una base di V è un insieme di vettori linearmente indipendenti i quali generano l'intero spazio V .

Da quanto visto in precedenza, si deduce il seguente risultato:

COROLLARIO 2.33. *Sia S una base di V . Ogni vettore $v \in V$ si può scrivere, in modo unico, come combinazione lineare finita di elementi di S .*

OSSERVAZIONE 2.34. Supponiamo che $S = \{v_1, v_2, \dots, v_n\}$ sia una base di uno spazio vettoriale V . Allora, per ogni $v \in V$, si ha

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n,$$

e gli scalari $\lambda_i \in K$ sono unicamente determinati da v . Tali scalari sono anche detti le *coordinate* del vettore v rispetto alla base v_1, v_2, \dots, v_n fissata.

2.4. Spazi vettoriali finitamente generati. Nella sezione precedente non abbiamo fatto nessuna ipotesi sul numero di generatori di uno spazio vettoriale. Ora ci occuperemo in dettaglio del caso in cui tale numero è finito.

DEFINIZIONE 2.35. Uno spazio vettoriale V è detto *finitamente generato* se esiste un insieme finito di generatori di V .

Cominciamo col dimostrare che ogni uno spazio vettoriale V finitamente generato ammette una base. Più precisamente, dimostreremo che da ogni insieme di generatori di V si può estrarre una base.

PROPOSIZIONE 2.36. *Sia $S = \{v_1, v_2, \dots, v_n\}$ un insieme di generatori di V . Allora S contiene dei vettori $v_{i_1}, v_{i_2}, \dots, v_{i_r}$, per qualche $r \leq n$, che formano una base di V .*

DIMOSTRAZIONE. Se i vettori v_1, v_2, \dots, v_n sono linearmente indipendenti, essi sono una base di V e la dimostrazione è così terminata. Se invece essi sono linearmente dipendenti, uno di essi può essere espresso come combinazione lineare dei rimanenti. A meno di rinominarli, possiamo supporre che questo vettore sia v_n . Possiamo quindi scrivere

$$v_n = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_{n-1} v_{n-1}.$$

Da ciò segue che i vettori v_1, v_2, \dots, v_{n-1} generano lo spazio vettoriale V ; infatti ogni vettore che si scrive come combinazione lineare dei vettori v_1, v_2, \dots, v_n si può anche scrivere come combinazione lineare dei soli vettori v_1, v_2, \dots, v_{n-1} . Ora, se i vettori v_1, v_2, \dots, v_{n-1} sono linearmente indipendenti, essi sono una base di V e la dimostrazione è terminata. In caso contrario uno di essi può essere espresso come combinazione lineare dei rimanenti. Anche in questo caso, a meno di riordinare i vettori, possiamo supporre che sia v_{n-1} a potersi scrivere come combinazione lineare dei vettori v_1, v_2, \dots, v_{n-2} . Ma ciò significa che i vettori v_1, v_2, \dots, v_{n-2} sono un insieme di generatori di V .

Ripetendo il ragionamento sopra descritto si arriverà, prima o poi, ad un insieme di vettori v_1, v_2, \dots, v_r , per qualche $r \leq n$, che generano tutto lo spazio V e sono linearmente indipendenti. Essi costituiscono quindi una base di V . \square

Il seguente risultato chiarisce le relazioni che esistono tra insiemi di vettori linearmente indipendenti, basi e insiemi di generatori.

PROPOSIZIONE 2.37. *Sia V uno spazio vettoriale finitamente generato. Consideriamo un insieme $\{v_1, v_2, \dots, v_n\}$ di generatori di V e siano w_1, w_2, \dots, w_r dei vettori linearmente indipendenti. Allora $r \leq n$.*

DIMOSTRAZIONE. Poiché i vettori v_1, v_2, \dots, v_n generano V , il vettore w_1 si può scrivere come una loro combinazione lineare,

$$w_1 = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n.$$

Dato che $w_1 \neq 0$, gli scalari $\lambda_1, \dots, \lambda_n$ non possono essere tutti nulli, quindi esiste un indice i tale che $\lambda_i \neq 0$. Da ciò si deduce che il vettore v_i può essere espresso come combinazione lineare dei vettori $w_1, v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$.

A meno di rinominare i vettori v_j , possiamo supporre che sia $i = n$, cioè che v_n si possa scrivere come combinazione lineare dei vettori w_1, v_1, \dots, v_{n-1} ; ma ciò significa che anche $\{w_1, v_1, \dots, v_{n-1}\}$ è un insieme di generatori di V . Il vettore w_2 si può quindi scrivere come combinazione lineare dei vettori w_1, v_1, \dots, v_{n-1} :

$$w_2 = \alpha_1 w_1 + \lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1},$$

e gli scalari $\lambda_1, \dots, \lambda_{n-1}$ non possono essere tutti nulli, perché altrimenti i vettori w_1 e w_2 sarebbero linearmente dipendenti, contro l'ipotesi.

Esiste quindi un indice i per il quale $\lambda_i \neq 0$ e, ancora una volta, possiamo supporre che sia $i = n - 1$ (a meno di riordinare i vettori v_j). Da

ciò segue che il vettore v_{n-1} si può scrivere come combinazione lineare dei vettori $w_1, w_2, v_1, \dots, v_{n-2}$, quindi anche $\{w_1, w_2, v_1, \dots, v_{n-2}\}$ è un insieme di generatori di V .

Continuando in questo modo, si dimostra che tutti gli insiemi

$$\{w_1, w_2, \dots, w_h, v_1, \dots, v_{n-h}\}$$

sono insiemi di generatori di V .

Se, per assurdo, fosse $n < r$, ponendo $h = n$ si avrebbe che i vettori w_1, w_2, \dots, w_n generano tutto lo spazio V , quindi il vettore w_{n+1} si potrebbe scrivere come combinazione lineare dei vettori w_1, w_2, \dots, w_n , il che contraddice l'ipotesi che i vettori w_1, w_2, \dots, w_r siano linearmente indipendenti. Deve quindi essere $r \leq n$. \square

COROLLARIO 2.38. *Sia V uno spazio vettoriale finitamente generato e sia $\{v_1, v_2, \dots, v_n\}$ una base di V . Allora, per ogni insieme di vettori linearmente indipendenti $\{w_1, w_2, \dots, w_r\}$, si ha $r \leq n$ e, per ogni insieme $\{u_1, u_2, \dots, u_s\}$ di generatori di V , si ha $s \geq n$.*

DIMOSTRAZIONE. Questo risultato è una conseguenza immediata della proposizione precedente; basta ricordare che i vettori v_1, v_2, \dots, v_n sono linearmente indipendenti e sono anche un insieme di generatori di V . \square

COROLLARIO 2.39. *Due basi qualunque di uno spazio vettoriale V (finitamente generato) hanno lo stesso numero di elementi.*

DIMOSTRAZIONE. Siano $\{v_1, v_2, \dots, v_r\}$ e $\{w_1, w_2, \dots, w_s\}$ due basi di V . Allora, dato che i vettori v_1, v_2, \dots, v_r sono linearmente indipendenti e i vettori w_1, w_2, \dots, w_s sono dei generatori di V , si ha $r \leq s$. Scambiando il ruolo delle due basi, si ottiene anche $s \leq r$, da cui segue l'uguaglianza $r = s$. \square

Il numero di vettori che compongono una base di uno spazio vettoriale finitamente generato V è dunque indipendente dalla base scelta e dipende dunque solo dallo spazio V . Possiamo quindi dare la seguente definizione:

DEFINIZIONE 2.40. La *dimensione* di uno spazio vettoriale (finitamente generato) V , che indicheremo con $\dim V$, è il numero di elementi di una base di V .

ESEMPIO 2.41. Consideriamo lo spazio vettoriale $V = K^n$, definito nell'Esempio 2.3. Per ogni $i = 1, \dots, n$, indichiamo con e_i la n -upla di elementi di K le cui componenti sono tutte nulle tranne la i -esima, che

è uguale a 1:

$$\begin{aligned} e_1 &= (1, 0, 0, 0, \dots, 0, 0), \\ e_2 &= (0, 1, 0, 0, \dots, 0, 0), \\ e_3 &= (0, 0, 1, 0, \dots, 0, 0), \\ &\dots \\ e_n &= (0, 0, 0, 0, \dots, 0, 1). \end{aligned}$$

Notiamo che, per ogni $\lambda_1, \dots, \lambda_n \in K$, si ha

$$\lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_n e_n = (\lambda_1, \lambda_2, \dots, \lambda_n).$$

Da questa uguaglianza si deduce che i vettori e_1, e_2, \dots, e_n sono linearmente indipendenti e generano lo spazio vettoriale V ; essi sono pertanto una base di $V = K^n$. Questa base è detta la *base canonica* di K^n . Si ha pertanto $\dim K^n = n$.

ESEMPIO 2.42. Lo spazio vettoriale nullo, $V = \{\mathbf{0}\}$, ha dimensione pari a zero. Esso infatti contiene un solo vettore $v = \mathbf{0}$, ma tale vettore non forma una base di V dato che esso non è linearmente indipendente! Infatti un insieme costituito da un solo vettore v è un insieme libero (cioè v è linearmente indipendente) se e solo se $v \neq \mathbf{0}$.

Dalla Proposizione 2.37 derivano anche i prossimi due risultati.

COROLLARIO 2.43. *Sia V uno spazio vettoriale finitamente generato. Allora ogni sottospazio vettoriale W di V è finitamente generato e si ha $\dim W \leq \dim V$.*

DIMOSTRAZIONE. Poniamo $n = \dim V$. Se $\{w_1, \dots, w_r\}$ è un insieme di vettori linearmente indipendenti di W , essi sono anche dei vettori linearmente indipendenti di V ; deve quindi essere $r \leq n$. Se questi vettori non sono un insieme di generatori di W , ciò significa che esiste un vettore $w_{r+1} \in W$ che non può essere espresso come combinazione lineare di w_1, \dots, w_r . Da ciò segue che i vettori w_1, \dots, w_r, w_{r+1} sono linearmente indipendenti. Se essi non sono ancora un insieme di generatori di W , deve esistere un vettore $w_{r+2} \in W$ che non può essere espresso come combinazione lineare di w_1, \dots, w_r, w_{r+1} . Ma allora anche i vettori $w_1, \dots, w_r, w_{r+1}, w_{r+2}$ sono linearmente indipendenti.

Poiché il numero di vettori linearmente indipendenti non può eccedere n , ripetendo il ragionamento precedente si arriva, dopo un numero finito di passi, a costruire un insieme di vettori linearmente indipendenti $\{w_1, \dots, w_s\}$, con $s \leq n$, i quali generano il sottospazio W e sono quindi una base di W . Ciò dimostra che $\dim W \leq \dim V$. \square

COROLLARIO 2.44. *Sia V uno spazio vettoriale finitamente generato. Allora ogni insieme di vettori linearmente indipendenti v_1, \dots, v_r può essere completato a una base di V . In altri termini, esistono dei vettori v_{r+1}, \dots, v_n tali che l'insieme $\{v_1, \dots, v_r, v_{r+1}, \dots, v_n\}$ sia una base di V .*

DIMOSTRAZIONE. La dimostrazione di questo risultato è essenzialmente analoga a quella del corollario precedente. Supponiamo che $v_1, \dots, v_r \in V$ siano dei vettori linearmente indipendenti. Se questi vettori non sono un insieme di generatori di V , ciò significa che esiste un vettore $v_{r+1} \in V$ che non può essere espresso come combinazione lineare di v_1, \dots, v_r . Da ciò segue che i vettori v_1, \dots, v_r, v_{r+1} sono linearmente indipendenti. Se essi non sono ancora un insieme di generatori di V , deve esistere un vettore $v_{r+2} \in V$ che non può essere espresso come combinazione lineare di v_1, \dots, v_r, v_{r+1} . Ma allora anche i vettori $v_1, \dots, v_r, v_{r+1}, v_{r+2}$ sono linearmente indipendenti. Continuando in questo modo, si deve necessariamente ottenere un insieme di vettori linearmente indipendenti $\{v_1, \dots, v_r, v_{r+1}, \dots, v_n\}$ che sono anche un insieme di generatori di V , altrimenti si otterrebbe un insieme infinito di vettori linearmente indipendenti, contro l'ipotesi che V sia finitamente generato. \square

Se la dimensione di uno spazio vettoriale V è nota, la verifica che un determinato insieme di vettori di V forma una base risulta semplificata. Vale infatti il seguente risultato:

PROPOSIZIONE 2.45. *Sia V uno spazio vettoriale di dimensione n e siano v_1, \dots, v_n dei vettori di V .*

- (a) *Se i vettori v_1, \dots, v_n sono linearmente indipendenti, allora essi sono anche un sistema di generatori di V , quindi sono una base di V .*
- (b) *Se i vettori v_1, \dots, v_n sono un sistema di generatori di V , allora essi sono anche linearmente indipendenti, quindi sono una base di V .*

DIMOSTRAZIONE. (a) Supponiamo che i vettori v_1, \dots, v_n siano linearmente indipendenti. Per il corollario precedente, essi sono contenuti in una base $\{v_1, \dots, v_n, v_{n+1}, \dots, v_{n+r}\}$ di V . Ma, poiché V ha dimensione n , ogni base di V deve avere n elementi. Da ciò si deduce che $r = 0$ e quindi i vettori v_1, \dots, v_n sono, in effetti, una base di V .

(b) Supponiamo che i vettori v_1, \dots, v_n siano un insieme di generatori di V . Se, per assurdo, essi fossero linearmente dipendenti, uno di essi sarebbe combinazione lineare dei rimanenti. A meno di riordinare i vettori, non è restrittivo supporre che v_n sia combinazione lineare di v_1, \dots, v_{n-1} . Ma allora i vettori v_1, \dots, v_{n-1} sarebbero anch'essi un insieme di generatori di V . Questo però è assurdo; infatti la cardinalità di un insieme di generatori di V deve essere $\geq \dim V$ (vedi Corollario 2.38). Quindi i vettori v_1, \dots, v_n sono linearmente indipendenti, cioè sono una base di V . \square

COROLLARIO 2.46. *Sia V uno spazio vettoriale finitamente generato e sia $W \subset V$ un suo sottospazio proprio. Allora $\dim W < \dim V$.*

DIMOSTRAZIONE. Nel Corollario 2.43 abbiamo dimostrato che si ha $\dim W \leq \dim V$. Supponiamo, per assurdo, che si abbia $\dim W = \dim V = n$. Consideriamo quindi una base w_1, \dots, w_n di W . Dato che questi sono n vettori linearmente indipendenti di V , e dato che n è proprio la dimensione di V , per il punto (a) della proposizione precedente essi sono una base di V . Ma da ciò segue che $W = V$, contro l'ipotesi che W sia un sottospazio proprio di V . \square

Occupiamoci ora della dimensione di uno spazio vettoriale quoziente.

PROPOSIZIONE 2.47. *Sia V uno spazio vettoriale di dimensione n sul campo K e sia W un sottospazio vettoriale di dimensione r di V . Allora lo spazio vettoriale quoziente V/W ha dimensione $n - r$.*

DIMOSTRAZIONE. Sia $\{w_1, \dots, w_r\}$ una base di W . Per il Corollario 2.44, è possibile completare questo insieme di vettori ad una base $\{w_1, \dots, w_r, v_{r+1}, \dots, v_n\}$ di V .

Se consideriamo le classi di equivalenza di questi vettori nel quoziente V/W , si ha

$$[w_1] = [w_2] = \dots = [w_r] = [\mathbf{0}].$$

Dimostriamo ora che gli elementi $[v_{r+1}], [v_{r+2}], \dots, [v_n]$ sono una base di V/W .

Che essi siano un insieme di generatori è del tutto ovvio: dato che ogni vettore $v \in V$ si può scrivere come una combinazione lineare del tipo

$$v = \alpha_1 w_1 + \dots + \alpha_r w_r + \beta_1 v_{r+1} + \dots + \beta_{n-r} v_n,$$

da ciò si deduce che

$$[v] = \beta_1 [v_{r+1}] + \dots + \beta_{n-r} [v_n].$$

Se, per assurdo, i vettori $[v_{r+1}], \dots, [v_n]$ fossero linearmente dipendenti, esisterebbe una combinazione lineare (con coefficienti non tutti nulli)

$$\lambda_1 [v_{r+1}] + \dots + \lambda_{n-r} [v_n] = [\mathbf{0}],$$

il che equivale a

$$\lambda_1 v_{r+1} + \dots + \lambda_{n-r} v_n \in W.$$

Ma ciò significa che è possibile scrivere

$$\lambda_1 v_{r+1} + \dots + \lambda_{n-r} v_n = \mu_1 w_1 + \dots + \mu_r w_r,$$

per qualche $\mu_1, \dots, \mu_r \in K$. I vettori $w_1, \dots, w_r, v_{r+1}, \dots, v_n$ sarebbero quindi linearmente dipendenti, il che non è possibile dato che essi sono una base di V .

Avendo così dimostrato che i vettori $[v_{r+1}], [v_{r+2}], \dots, [v_n]$ sono una base di V/W , si deduce che $\dim V/W = n - r$. \square

OSSERVAZIONE 2.48. Se $K \subset L$ è una estensione³ di campi, ogni spazio vettoriale V sul campo L può essere anche considerato come spazio vettoriale sul campo K . Se $\{v_1, \dots, v_n\}$ è una base di V in quanto K -spazio vettoriale, questi stessi vettori generano V anche in quanto spazio vettoriale su L , tuttavia, in questo caso, essi potrebbero non essere più linearmente indipendenti, come vedremo nel successivo esempio. In generale, possiamo pertanto affermare che la dimensione di V in quanto L -spazio vettoriale è minore o uguale alla dimensione di V considerato come spazio vettoriale su K , cioè

$$\dim_L V \leq \dim_K V.$$

Illustriamo quanto appena affermato con un esempio concreto. Sia $K = \mathbb{R}$ il campo dei numeri reali e $L = \mathbb{C}$ il campo dei numeri complessi. L'insieme \mathbb{C} è identificato in modo naturale con l'insieme \mathbb{R}^2 , associando ad ogni numero complesso $z = x + iy$ la coppia di numeri reali (x, y) . Poniamo quindi $V = \mathbb{C} \cong \mathbb{R}^2$. Lo spazio vettoriale $V = \mathbb{C}$, in quanto spazio vettoriale sul campo \mathbb{C} , ha naturalmente dimensione 1, e una sua base è costituita dal vettore $v = 1$. Se invece consideriamo \mathbb{C} in quanto spazio vettoriale su \mathbb{R} , esso ha dimensione 2. Una sua base è infatti costituita dai vettori $v_1 = 1$ e $v_2 = i$, i quali corrispondono, nell'identificazione $\mathbb{C} \cong \mathbb{R}^2$ descritta in precedenza, ai due vettori $(1, 0)$ e $(0, 1)$ della base canonica di \mathbb{R}^2 .

Notiamo che i vettori $v_1 = 1$ e $v_2 = i$ sono linearmente indipendenti sul campo \mathbb{R} dei numeri reali; infatti se $\alpha v_1 + \beta v_2 = \alpha + i\beta = 0$, con $\alpha, \beta \in \mathbb{R}$, si deve necessariamente avere $\alpha = \beta = 0$.

Essi sono invece linearmente dipendenti sul campo \mathbb{C} : si ha infatti

$$v_1 + iv_2 = 1 + i^2 = 1 - 1 = 0.$$

Più in generale, se $V = \mathbb{C}^n$, si ha $\dim_{\mathbb{C}} V = n$ e $\dim_{\mathbb{R}} V = 2n$.

OSSERVAZIONE 2.49. Sia V uno spazio vettoriale di dimensione n sul campo K . Se fissiamo una base v_1, \dots, v_n di V , ad ogni vettore $v \in V$ possiamo associare l'unica n -upla di elementi di K , $(\lambda_1, \dots, \lambda_n) \in K^n$, per cui si ha $v = \lambda_1 v_1 + \dots + \lambda_n v_n$. Si ottiene in questo modo una funzione biiettiva

$$V \rightarrow K^n, \quad v \mapsto (\lambda_1, \dots, \lambda_n),$$

da cui si deduce che la cardinalità di V coincide con la cardinalità dell'insieme K^n :

$$|V| = |K^n| = n |K|.$$

Se K è un campo infinito, si ha $|K^n| = |K|$ (vedi Capitolo 1, Corollario 2.14).

Abbiamo così dimostrato che ogni spazio vettoriale di dimensione finita su un campo infinito K ha cardinalità pari alla cardinalità di K .

³Ciò significa semplicemente che L è un campo e K è un suo sottocampo.

Terminiamo questa sezione dimostrando un risultato che mette in relazione le dimensioni di due sottospazi vettoriali di V con le dimensioni della loro somma e della loro intersezione:

PROPOSIZIONE 2.50. *Siano W_1 e W_2 due sottospazi vettoriali di uno spazio vettoriale finitamente generato V . Allora si ha:*

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2).$$

DIMOSTRAZIONE. Poniamo

$$r = \dim W_1, \quad s = \dim W_2, \quad t = \dim(W_1 \cap W_2).$$

Consideriamo una base $\{v_1, \dots, v_t\}$ di $W_1 \cap W_2$. Per il Corollario 2.44, questo insieme di vettori può essere completato, tramite aggiunta di altri vettori, in modo da ottenere una base $\{v_1, \dots, v_t, v_{t+1}, \dots, v_r\}$ di W_1 e una base $\{v_1, \dots, v_t, v'_{t+1}, \dots, v'_s\}$ di W_2 .

Dato che ogni vettore di $W_1 + W_2$ può essere scritto come somma di un vettore di W_1 e di uno di W_2 , esso può quindi essere espresso come combinazione lineare dei vettori $v_1, \dots, v_t, v_{t+1}, \dots, v_r, v'_{t+1}, \dots, v'_s$. Vogliamo ora dimostrare che questi vettori, oltre a essere dei generatori di $W_1 + W_2$, sono anche linearmente indipendenti.

Supponiamo quindi che sia

$$\alpha_1 v_1 + \dots + \alpha_t v_t + \beta_1 v_{t+1} + \dots + \beta_{r-t} v_r + \gamma_1 v'_{t+1} + \dots + \gamma_{s-t} v'_s = \mathbf{0}.$$

Da ciò segue che

$$\alpha_1 v_1 + \dots + \alpha_t v_t + \beta_1 v_{t+1} + \dots + \beta_{r-t} v_r = -(\gamma_1 v'_{t+1} + \dots + \gamma_{s-t} v'_s).$$

Se chiamiamo w il vettore precedente, si ha che $w \in W_1 \cap W_2$. Poiché $\{v_1, \dots, v_t\}$ è una base di $W_1 \cap W_2$, il vettore w si può scrivere, in modo unico, nella forma

$$w = \lambda_1 v_1 + \dots + \lambda_t v_t.$$

Si hanno quindi le seguenti uguaglianze:

$$\lambda_1 v_1 + \dots + \lambda_t v_t = \alpha_1 v_1 + \dots + \alpha_t v_t + \beta_1 v_{t+1} + \dots + \beta_{r-t} v_r$$

e

$$\lambda_1 v_1 + \dots + \lambda_t v_t = -(\gamma_1 v'_{t+1} + \dots + \gamma_{s-t} v'_s).$$

Poiché, per ipotesi, i vettori $v_1, \dots, v_t, v_{t+1}, \dots, v_r$ sono una base di W_1 e i vettori $v_1, \dots, v_t, v'_{t+1}, \dots, v'_s$ sono una base di W_2 , dalle uguaglianze precedenti segue che

$$\begin{aligned} \lambda_1 = \dots = \lambda_t = 0, & \quad \alpha_1 = \dots = \alpha_t = 0, \\ \beta_1 = \dots = \beta_{r-t} = 0, & \quad \gamma_1 = \dots = \gamma_{s-t} = 0. \end{aligned}$$

Abbiamo così dimostrato che l'insieme dei vettori

$$\{v_1, \dots, v_t, v_{t+1}, \dots, v_r, v'_{t+1}, \dots, v'_s\}$$

è una base di $W_1 + W_2$. Si ha pertanto

$$\dim(W_1 + W_2) = r + s - t = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2).$$

□

OSSERVAZIONE 2.51. Sia V uno spazio vettoriale finitamente generato. Notiamo che, per ogni sottospazio $W \subseteq V$, è possibile trovare un sottospazio W' di V tale che $V = W \oplus W'$, cioè tale che si abbia $V = W + W'$ e $W \cap W' = \{\mathbf{0}\}$. Un tale W' è detto un *sottospazio complementare* di W .

A tal fine, è sufficiente considerare una base $\{w_1, \dots, w_r\}$ di W e completarla ad una base $\{w_1, \dots, w_r, v_{r+1}, \dots, v_n\}$ di V (cf. Corollario 2.44). Il sottospazio $W' = \langle v_{r+1}, \dots, v_n \rangle$, generato dai vettori v_{r+1}, \dots, v_n , è il sottospazio cercato.

Notiamo infine che un tale sottospazio W' non è unico. Ad esempio, se $V = K^2$ e se W è il sottospazio generato dal vettore $(1, 0)$, qualunque vettore (a, b) , con $b \neq 0$, genera un sottospazio W' tale che $V = W \oplus W'$.

2.5. Spazi vettoriali non finitamente generati. Nella sezione precedente ci siamo occupati esclusivamente di spazi vettoriali di dimensione finita. Ora vedremo che alcuni risultati, come ad esempio il fatto che ogni spazio vettoriale ammetta una base e che due basi dello stesso spazio vettoriale abbiano la stessa cardinalità, valgono anche per spazi vettoriali non finitamente generati. Le dimostrazioni, tuttavia, sono più complicate.

Cominciamo col dimostrare l'analogo della Proposizione 2.36 e del Corollario 2.44 per uno spazio vettoriale V non necessariamente finitamente generato; dimostriamo cioè che ogni insieme di generatori di V contiene una base e che ogni insieme libero di vettori può essere completato ad una base di V .

TEOREMA 2.52. *Sia V uno spazio vettoriale (non finitamente generato) sul campo K . Allora:*

- (a) *Ogni insieme libero S di vettori di V è contenuto in una base. Cioè, esiste una base B di V tale che $S \subseteq B$.*
- (b) *Ogni insieme S di generatori di V contiene una base. Cioè, esiste una base B di V tale che $B \subseteq S$.*

DIMOSTRAZIONE. (a) Indichiamo con \mathcal{S} il sottoinsieme di $\mathcal{P}(V)$ formato da tutti i sottoinsiemi liberi S di V . Notiamo che \mathcal{S} non è l'insieme vuoto, perché in V esiste almeno un vettore non nullo. Definiamo un ordine parziale su \mathcal{S} ponendo $S_1 \leq S_2$ se $S_1 \subseteq S_2$. Ora dimostreremo che l'insieme \mathcal{S} è (strettamente) induttivo.

Sia T una catena non vuota in \mathcal{S} , e scriviamo $T = \{S_i\}_{i \in I}$. Poniamo

$$S = \bigcup_{i \in I} S_i.$$

Dimostriamo che S è un sottoinsieme libero di V . Se così non fosse, S conterrebbe un insieme finito di vettori linearmente dipendenti $\{v_1, v_2, \dots, v_n\}$. Per definizione di S , ogni v_i deve appartenere a un insieme S_j , per qualche indice $j \in I$. Poiché T è una catena, e poiché i vettori v_1, v_2, \dots, v_n sono in numero finito, esiste un indice $h \in I$ tale

che $v_1, v_2, \dots, v_n \in S_h$. Ma S_h è un sottoinsieme libero di V , quindi i vettori v_1, v_2, \dots, v_n non possono essere linearmente dipendenti. Da ciò si deduce che S è un insieme libero, quindi appartiene a \mathcal{S} .

È ora immediato verificare che S è proprio l'estremo superiore di T , il che dimostra che \mathcal{S} è un insieme strettamente induttivo.

Possiamo quindi applicare il Lemma di Zorn, il quale afferma che per ogni insieme libero $S \in \mathcal{S}$ esiste un elemento massimale $M \in \mathcal{S}$, con $S \subseteq M$. Si tratta ora di dimostrare che M è una base di V .

Osserviamo, innanzitutto, che M è un insieme libero, dato che $M \in \mathcal{S}$; bisogna quindi dimostrare che M è un insieme di generatori di V . Se così non fosse, esisterebbe un vettore $v \in V$ che non può essere espresso come combinazione lineare finita di elementi di M . Ma, in tal caso, l'insieme $M' = M \cup \{v\}$ sarebbe un insieme libero che contiene strettamente M , il che contraddice la massimalità di M . M è pertanto una base di V .

(b) La dimostrazione è simile a quella del punto (a). In questo caso definiamo \mathcal{S} come l'insieme di tutti i sottoinsiemi di V che sono insiemi di generatori di V ; \mathcal{S} non è l'insieme vuoto dato che $V \in \mathcal{S}$. Ordiniamo \mathcal{S} per inclusione rovesciata, cioè poniamo $S_1 \leq S_2$ se $S_1 \supseteq S_2$. In questo modo \mathcal{S} risulta essere un insieme parzialmente ordinato (strettamente) induttivo. Infatti, se $T = \{S_i\}_{i \in I}$ è una catena non vuota in \mathcal{S} , si verifica facilmente che l'insieme

$$S = \bigcap_{i \in I} S_i$$

è proprio l'estremo superiore di T (la verifica è lasciata al lettore, per esercizio).

Anche in questo caso possiamo dunque applicare il Lemma di Zorn, il quale, nella sua versione più forte, afferma che per ogni insieme di generatori $S \in \mathcal{S}$, esiste un elemento massimale $M \in \mathcal{S}$, con $S \leq M$, il che equivale a dire $S \supseteq M$. Ora dimostreremo che M è, in effetti, una base di V .

Dato che, per definizione di \mathcal{S} , M genera V , è sufficiente dimostrare che M è un insieme libero. Per assurdo, supponiamo che M contenga dei vettori linearmente dipendenti, v_1, v_2, \dots, v_n . In tal caso, uno di questi vettori si può scrivere come combinazione lineare dei rimanenti. A meno di riordinarli, non è restrittivo supporre che sia

$$v_n = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_{n-1} v_{n-1}.$$

Da ciò si deduce che anche $M' = M \setminus \{v_n\}$ è un insieme di generatori di V . Ma M' è contenuto propriamente in M , il che significa che $M < M'$. Ciò, tuttavia, contraddice la massimalità di M . Abbiamo così dimostrato che M è una base di V . \square

Da questo risultato si ottiene immediatamente l'esistenza di una base di V .

COROLLARIO 2.53. *Ogni spazio vettoriale V su un campo K possiede una base.*

OSSERVAZIONE 2.54. Notiamo che la dimostrazione dell'esistenza di una base per uno spazio vettoriale non finitamente generato utilizza il Lemma di Zorn e quindi dipende dall'Assioma della Scelta.

ESEMPIO 2.55. Sia $V = K[X]$ lo spazio vettoriale dei polinomi in una indeterminata, a coefficienti nel campo K (che è già stato introdotto nell'Esempio 2.4).

Ricordando che ogni polinomio in $K[X]$, per definizione, si scrive in modo unico nella forma

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n,$$

per qualche $n \geq 0$, e per qualche $a_1, \dots, a_n \in K$, si deduce che l'insieme degli infiniti polinomi

$$q_0(X) = 1, q_1(X) = X, q_2(X) = X^2, \dots, q_i(X) = X^i, \dots$$

è una base di V . Lo spazio vettoriale $V = K[X]$ non è quindi finitamente generato. Più precisamente, abbiamo dimostrato che V ha una base costituita da un insieme numerabile di vettori.

OSSERVAZIONE 2.56. Sia V uno spazio vettoriale sul campo K e supponiamo che V abbia una base numerabile

$$\{v_1, v_2, \dots, v_i, \dots\}.$$

Per ogni intero $n \geq 1$ indichiamo con V_n il sottospazio di V generato dai vettori v_1, v_2, \dots, v_n ; si ha quindi $\dim V_n = n$. Notiamo che

$$V = \bigcup_{n \geq 1} V_n.$$

Se K è un campo finito, tutti gli insiemi V_n sono finiti, come dimostrato nell'Osservazione 2.49. L'insieme V è dunque numerabile, essendo unione numerabile di insiemi finiti (vedi Cap. 1, Proposizione 1.15).

Se invece K è un campo infinito, abbiamo già dimostrato nell'Osservazione 2.49 che $|V_n| = |K|$, per ogni $n \geq 1$. Poiché V è unione dei sottospazi V_n , dalla Proposizione 2.11 del Cap. 1 (e dall'osservazione successiva), si deduce che la cardinalità di V coincide con la cardinalità di K , esattamente come accade nel caso in cui V ha dimensione finita.

ESEMPIO 2.57. Sia $K = \mathbb{Q}$ il campo dei numeri razionali e sia $V = \mathbb{R}$ l'insieme dei numeri reali. Consideriamo V in quanto spazio vettoriale su K . Se esistesse una base finita o numerabile di V si avrebbe, in base all'osservazione precedente, $|V| = |K| = \aleph_0$, il che è falso, dato che \mathbb{R} non è numerabile. In effetti, è facile dimostrare che ogni base di V deve avere la stessa cardinalità di \mathbb{R} .

ESEMPIO 2.58. Sia $K = \mathbb{Z}/2\mathbb{Z}$ il campo finito con due elementi e sia V l'insieme di tutte le funzioni da $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ in K . V è, in modo naturale, uno spazio vettoriale su K (vedi Esempio 2.5).

Ad ogni funzione $f : \mathbb{N}^* \rightarrow K$ possiamo associare una sequenza infinita $(a_1, a_2, \dots, a_i, \dots)$ di elementi di K , ponendo $a_i = f(i)$, per ogni $i \geq 1$. Lo spazio vettoriale V può quindi essere identificato con l'insieme di tali sequenze, cioè con il prodotto cartesiano

$$K^\infty = \prod_{i=1}^{\infty} K.$$

di infinite copie di K .

Per ogni intero $i \geq 1$ indichiamo con e_i la sequenza i cui elementi sono tutti nulli tranne quello nella i -esima posizione, che è uguale a 1 (la sequenza e_i corrisponde alla funzione f_i definita da $f_i(n) = 0$ per ogni $n \neq i$ e $f_i(i) = 1$).

Per analogia con quanto accade nel caso degli spazi vettoriali K^n , si potrebbe, ingenuamente, pensare che l'insieme degli infiniti vettori

$$\{e_1, e_2, \dots, e_i, \dots\}$$

costituisse una base numerabile di $V \cong K^\infty$. Ciò è falso! Infatti se consideriamo il vettore $v = (1, 1, \dots, 1, \dots)$, esso non può, in nessun modo, essere espresso come combinazione lineare *finita* dei vettori e_i ; infatti ogni tale combinazione lineare finita produce una sequenza che ha solo un numero finito di elementi diversi da zero.

Formalmente si avrebbe

$$v = \sum_{i=1}^{\infty} e_i,$$

ma, nelle definizioni relative agli spazi vettoriali, non sono ammesse delle combinazioni lineari infinite⁴ di vettori.

In realtà lo spazio vettoriale V che abbiamo considerato non possiede una base numerabile. Infatti, se esistesse una base numerabile di V , V stesso sarebbe un insieme numerabile. Invece l'insieme V può essere identificato con l'insieme delle parti di \mathbb{N} , la cui cardinalità è $2^{\aleph_0} = \mathfrak{c}$. Da ciò si deduce che ogni base di V deve avere la cardinalità \mathfrak{c} del continuo.

Ora dimostreremo che, anche nel caso di spazi vettoriali non finitamente generati, due basi di uno stesso spazio vettoriale sono equipotenti. È quindi ancora possibile definire la dimensione di uno spazio vettoriale, identificandola con la cardinalità di una base.

⁴Per dare un senso ad una somma infinita occorre introdurre una topologia e definire la somma infinita come un limite di opportune somme finite. Dopodiché bisogna stabilire se un tale limite esiste oppure no.

TEOREMA 2.59. *Siano B_1 e B_2 due basi di uno spazio vettoriale V sul campo K . Allora $|B_1| = |B_2|$.*

DIMOSTRAZIONE. Dato che la dimostrazione è piuttosto lunga, riteniamo utile descrivere subito la strategia che seguiremo. Quello che vogliamo dimostrare è che esiste una funzione iniettiva $\psi : B_1 \rightarrow B_2$. Dopodiché, scambiando i ruoli delle due basi, si ottiene anche l'esistenza di una funzione iniettiva da B_2 in B_1 . Il Teorema di Cantor–Bernstein–Shroeder (Cap. 1, Teorema 2.2) permette quindi di concludere che esiste una funzione biiettiva $B_1 \rightarrow B_2$, il che equivale a dire che B_1 e B_2 hanno la stessa cardinalità.

Per ottenere l'esistenza di una funzione iniettiva $\psi : B_1 \rightarrow B_2$, considereremo un opportuno insieme di coppie (S, ϕ) , ove S è un sottoinsieme di B_1 e $\phi : S \rightarrow B_2$ è una funzione iniettiva. È possibile ordinare parzialmente tale insieme di coppie in modo da ottenere un insieme induttivo a cui si può applicare il Lemma di Zorn. Se indichiamo con (M, ψ) un elemento massimale di tale insieme, basterà solo dimostrare che $M = B_1$ per ottenere la funzione iniettiva $\psi : B_1 \rightarrow B_2$ cercata.

Sia dunque \mathcal{S} l'insieme delle coppie (S, ϕ) , dove $S \subseteq B_1$ e $\phi : S \rightarrow B_2$ è una funzione iniettiva, che soddisfano la seguente condizione:

$$(B_1 \setminus S) \cup \phi(S) \text{ è un insieme libero.}$$

Innanzitutto dimostriamo che \mathcal{S} non è l'insieme vuoto.

Consideriamo un vettore $v \in B_1$. Dato che B_2 è una base di V , esistono dei vettori $w_1, \dots, w_n \in B_2$ e degli scalari $\lambda_1, \dots, \lambda_n \in K$ tali che

$$v = \lambda_1 w_1 + \lambda_2 w_2 + \dots + \lambda_n w_n.$$

Poniamo $C = B_1 \setminus \{v\}$; C è un insieme libero in quanto sottoinsieme della base B_1 . Tra i vettori w_1, \dots, w_n che compaiono nell'espressione di v ce ne deve essere almeno uno, chiamiamolo w_k , che non appartiene all'insieme C e tale che $C \cup \{w_k\}$ sia un insieme libero. Infatti, in caso contrario, si avrebbe che ogni w_i o appartiene a C oppure si può scrivere come combinazione lineare di elementi di C . Ma da ciò seguirebbe che il vettore v è combinazione lineare di elementi di C , quindi l'insieme $C \cup \{v\} = B_1$ non sarebbe libero, contro l'ipotesi che B_1 sia una base.

Definiamo ora una funzione $\phi : \{v\} \rightarrow B_2$, ponendo $\phi(v) = w_k$. Questa funzione è ovviamente iniettiva, inoltre si ha che l'insieme

$$(B_1 \setminus \{v\}) \cup \{\phi(v)\} = C \cup \{w_k\}$$

è libero. Ciò significa che la coppia $(\{v\}, \phi)$ appartiene all'insieme \mathcal{S} , che non è dunque l'insieme vuoto.

Possiamo ora definire un ordine parziale su \mathcal{S} ponendo

$$(S_1, \phi_1) \leq (S_2, \phi_2) \quad \text{se } S_1 \subseteq S_2 \text{ e } \phi_2|_{S_1} = \phi_1.$$

Il prossimo passo consiste nel dimostrare che \mathcal{S} è un insieme (strettamente) induttivo.

Sia $T = \{(S_i, \phi_i)\}_{i \in I}$ una catena non vuota in \mathcal{S} . Poniamo

$$S = \bigcup_{i \in I} S_i$$

e definiamo una funzione $\phi : S \rightarrow B_2$ ponendo $\phi(v) = \phi_i(v)$ per qualche indice $i \in I$ per cui si abbia $v \in S_i$. Notiamo che se $i \neq j$ sono due indici tali che $v \in S_i$ e $v \in S_j$, dato che T è una catena deve essere $(S_i, \phi_i) \leq (S_j, \phi_j)$ oppure $(S_j, \phi_j) \leq (S_i, \phi_i)$. In entrambi i casi si ha dunque $\phi_i(v) = \phi_j(v)$, il che dimostra che la funzione $\phi : S \rightarrow B_2$ è ben definita.

Verifichiamo ora che ϕ è iniettiva. Siano dunque $v, v' \in S$ tali che $\phi(v) = \phi(v')$. Esisteranno due indici $i, j \in I$ tali che $v \in S_i$ e $v' \in S_j$ ma, dato che T è una catena, deve necessariamente essere $S_i \subseteq S_j$ oppure $S_j \subseteq S_i$. In entrambi i casi, esiste un indice $h \in I$ tale che $v, v' \in S_h$ e si ha quindi $\phi(v) = \phi_h(v)$ e $\phi(v') = \phi_h(v')$. Poiché ϕ_h è iniettiva, dall'uguaglianza $\phi_h(v) = \phi_h(v')$ segue che $v = v'$. Ciò dimostra che la funzione ϕ è iniettiva.

Per concludere che la coppia (S, ϕ) appartiene a \mathcal{S} rimane solo da verificare che l'insieme $(B_1 \setminus S) \cup \phi(S)$ è libero. Per assurdo, supponiamo che ciò sia falso. Questo insieme contiene quindi una famiglia finita di vettori linearmente dipendenti. Possiamo quindi supporre che esistano dei vettori $v_1, \dots, v_r \in B_1 \setminus S$ e dei vettori $w_1, \dots, w_s \in \phi(S)$ tali che l'insieme

$$\{v_1, \dots, v_r, w_1, \dots, w_s\}$$

non sia libero. Notiamo inoltre che non è restrittivo supporre che $w_1, \dots, w_s \notin B_1 \setminus S$. Dall'ipotesi $w_1, \dots, w_s \in \phi(S)$ segue che esistono dei vettori $u_1, \dots, u_s \in S$ tali che $w_1 = \phi(u_1)$, $w_2 = \phi(u_2)$, \dots , $w_s = \phi(u_s)$. Poiché i vettori u_1, \dots, u_s sono in numero finito, dall'ipotesi che T sia una catena si deduce che deve esistere un indice $h \in I$ tale che $u_1, \dots, u_s \in S_h$. Ciò significa che $w_1, \dots, w_s \in \phi(S_h)$ e, poiché si ha anche $v_1, \dots, v_r \in B_1 \setminus S_h$, l'insieme di vettori linearmente indipendenti

$$\{v_1, \dots, v_r, w_1, \dots, w_s\}$$

è contenuto in $(B_1 \setminus S_h) \cup \phi(S_h)$, il che è assurdo perché, per ipotesi, questo insieme è libero.

Abbiamo così dimostrato che $(S, \phi) \in \mathcal{S}$. Dato che, dalla definizione di S e di ϕ , si deduce immediatamente che la coppia (S, ϕ) è l'estremo superiore di T , questo dimostra che \mathcal{S} è un insieme strettamente induttivo. Per il Lemma di Zorn esiste dunque un elemento massimale (M, ψ) in \mathcal{S} . Come già spiegato all'inizio, si tratta ora di dimostrare che $M = B_1$.

Supponiamo, per assurdo, che M sia un sottoinsieme proprio di B_1 . In tal caso esiste un vettore $v \in B_1 \setminus M$. Poiché B_2 è una base, si ha

$$v = \lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_n w_n,$$

per qualche $w_1, \dots, w_n \in B_2$ e qualche $\lambda_1, \dots, \lambda_n \in K$.

Se tutti i vettori w_1, \dots, w_n appartenessero al sottospazio generato dall'insieme $(B_1 \setminus (M \cup \{v\})) \cup \psi(M)$, anche v dovrebbe appartenere a tale sottospazio. Ma da ciò seguirebbe che l'insieme

$$(B_1 \setminus (M \cup \{v\})) \cup \psi(M) \cup \{v\} = (B_1 \setminus M) \cup \psi(M)$$

non è libero, il che contraddice il fatto che $(M, \psi) \in \mathcal{S}$.

Si conclude pertanto che almeno uno dei vettori w_1, \dots, w_n , che chiameremo w_h , non appartiene a $L((B_1 \setminus (M \cup \{v\})) \cup \psi(M))$. Ora poniamo $M' = M \cup \{v\}$ e definiamo una funzione $\psi' : M' \rightarrow B_2$ ponendo $\psi'(u) = \psi(u)$ per ogni $u \in M$ e $\psi'(v) = w_h$. Vogliamo dimostrare che ψ' è iniettiva.

Supponiamo, per assurdo, che ψ' non sia iniettiva. Dato che $\psi'|_M = \psi$ è iniettiva, si deve avere $\psi'(v) = \psi'(u)$, per qualche $u \in M$, il che equivale a dire che $\psi(u) = w_h$. Quindi $w_h \in \psi(M)$, il che è assurdo dato che avevamo supposto che il vettore w_h non appartenesse al sottospazio vettoriale generato dall'insieme $(B_1 \setminus (M \cup \{v\})) \cup \psi(M)$.

Per concludere che la coppia (M', ψ') appartiene a \mathcal{S} rimane ora solo da dimostrare che $(B_1 \setminus M') \cup \psi'(M')$ è un insieme libero. Per assurdo, supponiamo che tale insieme non sia libero. Ricordando che $(B_1 \setminus M) \cup \psi(M)$ è un insieme libero e che $\psi'(M') = \psi(M) \cup \{w_h\}$, si deduce che devono esistere dei vettori $u_1, \dots, u_m \in (B_1 \setminus M') \cup \psi(M)$ e una combinazione lineare

$$\alpha w_r + \beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_m u_m = 0,$$

con $\alpha \neq 0$ (e naturalmente con β_1, \dots, β_m non tutti nulli). Ma da ciò segue che w_r si può scrivere come combinazione lineare dei vettori u_1, \dots, u_m , quindi $w_r \in L((B_1 \setminus M') \cup \psi(M)) = L((B_1 \setminus (M \cup \{v\})) \cup \psi(M))$, il che è assurdo, dato che w_r è stato scelto proprio in modo da non appartenere a tale sottospazio.

Abbiamo così dimostrato che $(M', \psi') \in \mathcal{S}$, ma ciò contraddice il fatto che la coppia (M, ψ) è un elemento massimale di \mathcal{S} . Si conclude pertanto che $M = B_1$ e quindi ψ è una funzione iniettiva di B_1 in B_2 , come volevasi dimostrare. \square

OSSERVAZIONE 2.60. Ci sono, naturalmente, altri modi di dimostrare il teorema precedente. Una dimostrazione per certi aspetti più semplice è la seguente.⁵

Innanzitutto notiamo che se lo spazio vettoriale V è finitamente generato, il fatto che due basi di V abbiano la stessa cardinalità è già

⁵Questa dimostrazione è tratta da Jacobson, "Lectures in Abstract Algebra, vol. 2."

stato dimostrato (vedi Corollario 2.39). Possiamo quindi supporre che V non sia finitamente generato e quindi che le due basi B_1 e B_2 siano insiemi infiniti. Poniamo quindi $B_1 = \{v_i\}_{i \in I}$ e $B_2 = \{w_j\}_{j \in J}$, per opportuni insiemi infiniti di indici I e J .

Dato che B_2 è una base di V , ogni vettore $v_i \in B_1$ si può scrivere come combinazione lineare di un numero finito di vettori di B_2

$$v_i = \lambda_1 w_{j_1} + \lambda_2 w_{j_2} + \cdots + \lambda_m w_{j_m},$$

per qualche $w_{j_1}, \dots, w_{j_m} \in B_2$ e qualche $\lambda_1, \dots, \lambda_m \in K$.

Si noti che ogni vettore $w_j \in B_2$ deve comparire in almeno una di queste espressioni. Infatti, se esistesse un vettore $w_h \in B_2$ che non compare nell'espressione di nessun $v_i \in B_1$, sarebbe possibile esprimere tale w_h come combinazione lineare di un numero finito di tali v_i (perché B_1 è una base) e quindi, poiché tutti questi v_i sarebbero a loro volta combinazioni lineari finite dei $w_j \in B_2$, con $j \neq h$, il vettore w_h sarebbe una combinazione lineare finita di vettori $w_j \in B_2$, con $j \neq h$. Ma ciò è assurdo, perché B_2 è una base quindi, in particolare, è un insieme libero. Si conclude quindi che, per ogni $w_h \in B_2$, esiste almeno un vettore $v_i \in B_1$ il quale contiene w_h nella sua espressione come combinazione lineare finita di elementi di B_2 . Possiamo allora definire una funzione $f: B_2 \rightarrow B_1$ ponendo $f(w_h) = v_i$, per qualche v_i come sopra descritto (naturalmente una siffatta funzione f non sarà, in generale, né iniettiva, né suriettiva).

Indichiamo con $B'_1 \subseteq B_1$ l'immagine di f e, per ogni $v_i \in B'_1$ consideriamo l'immagine inversa $f^{-1}(v_i) \subset B_2$. Questi insiemi costituiscono una partizione di B_2 :

$$B_2 = \bigcup_{v_i \in B'_1} f^{-1}(v_i).$$

Notiamo che tutte le immagini inverse dei vettori $v_i \in B'_1$ sono insiemi finiti; $f^{-1}(v_i)$ consiste infatti di alcuni tra i vettori w_h che compaiono nell'espressione di v_i come combinazione lineare finita di elementi della base B_2 .

Dato che B_2 è un insieme infinito, anche B'_1 deve essere infinito e, dai risultati sulle cardinalità dimostrati nel Cap. 1 (vedi in particolare la Proposizione 2.11), si deduce che

$$|B_2| = \left| \bigcup_{v_i \in B'_1} f^{-1}(v_i) \right| = |B'_1|.$$

Infine, poiché $B'_1 \subseteq B_1$, si ha $|B'_1| \leq |B_1|$, e quindi $|B_2| \leq |B_1|$.

Per concludere basta notare che scambiando i ruoli di B_1 e B_2 si ottiene anche la disuguaglianza $|B_1| \leq |B_2|$ e, dal Teorema di Cantor–Bernstein–Shroeder, si deduce infine che $|B_1| = |B_2|$.

2.5.1. *Somma diretta e prodotto cartesiano.* Per terminare questa sezione occupiamoci della somma diretta (esterna) di una famiglia infinita di spazi vettoriali.

Nell'Osservazione 2.24, abbiamo già visto che, nel caso di una famiglia finita di spazi vettoriali V_1, V_2, \dots, V_n sul campo K , la loro somma diretta coincide con il loro prodotto cartesiano, cioè si ha

$$\bigoplus_{i=1}^n V_i = \prod_{i=1}^n V_i.$$

Vedremo ora che, nel caso di una famiglia infinita $\{V_i\}_{i \in I}$ questa uguaglianza non vale.

Iniziamo considerando il prodotto cartesiano infinito $\prod_{i \in I} V_i$. Tale prodotto è non vuoto (a causa dell'Assioma della Scelta, vedi Cap. 1, Esempio 1.7) ed è, in modo naturale, uno spazio vettoriale su K , per le operazioni definite da

$$(v_i)_{i \in I} + (w_i)_{i \in I} = (v_i + w_i)_{i \in I}$$

e

$$\lambda(v_i)_{i \in I} = (\lambda v_i)_{i \in I},$$

per ogni $\lambda \in K$ e ogni $(v_i)_{i \in I}, (w_i)_{i \in I} \in \prod_{i \in I} V_i$.

Esattamente come nel caso di una famiglia finita (cf. Osservazione 2.24), ogni V_i si identifica in modo naturale con il sottospazio V'_i del prodotto $\prod_{i \in I} V_i$ che consiste di tutte le sequenze infinite $(v_i)_{i \in I}$ in cui i vettori v_j sono il vettore nullo di V_j , per ogni indice $j \neq i$. Definiremo quindi la somma diretta esterna della famiglia di spazi vettoriali $\{V_i\}_{i \in I}$ come la somma diretta interna della famiglia $\{V'_i\}_{i \in I}$ di sottospazi vettoriali del prodotto cartesiano $\prod_{i \in I} V_i$, cioè come il più piccolo sottospazio vettoriale di $\prod_{i \in I} V_i$ che contiene tutti i sottospazi V'_i , per ogni $i \in I$.

Ora dimostreremo che questa somma diretta coincide con il sottoinsieme proprio del prodotto cartesiano $\prod_{i \in I} V_i$ costituito da tutte le sequenze infinite $(v_i)_{i \in I}$ *quasi-ovunque nulle*, cioè quelle sequenze che contengono solo un numero finito di elementi v_i diversi dal vettore nullo.

Sia dunque $W \subset \prod_{i \in I} V_i$ l'insieme delle sequenze quasi-ovunque nulle. Poiché una combinazione lineare di due sequenze quasi-ovunque nulle è ancora una sequenza quasi-ovunque nulla, l'insieme W è, in effetti, un sottospazio vettoriale del prodotto $\prod_{i \in I} V_i$.

Dato che W contiene tutti i sottospazi V'_i esso contiene anche la loro somma diretta. D'altra parte, ogni sottospazio del prodotto $\prod_{i \in I} V_i$ che contiene tutti i sottospazi V'_i deve contenere anche tutte le combinazioni lineari finite di loro elementi, ma queste sono precisamente tutte le sequenze $(v_i)_{i \in I}$ quasi-ovunque nulle. Ciò dimostra che

$$W = \bigoplus_{i \in I} V'_i = \bigoplus_{i \in I} V_i.$$

Da quanto sopra detto, si deduce che se, per ogni $i \in I$, B_i è una base di V_i , allora l'insieme di tutte le sequenze $(v_i)_{i \in I}$ tali che esiste $j \in I$ per

cui $v_j \in B_j$ e $v_i = \mathbf{0}$, per ogni $i \neq j$, costituisce una base dello spazio vettoriale $\bigoplus_{i \in I} V_i$, ma non è invece una base del prodotto $\prod_{i \in I} V_i$.

CAPITOLO 3

Applicazioni Lineari e Matrici

1. Applicazioni Lineari

In questo capitolo ci occuperemo dello studio delle funzioni, definite tra due spazi vettoriali, che “rispettano” la struttura di spazio vettoriale, cioè che sono compatibili con le operazioni di somma di vettori e di prodotto di un vettore per uno scalare.

DEFINIZIONE 1.1. Siano V e W due spazi vettoriali su un campo K . Una funzione $f : V \rightarrow W$ è detta *additiva* se

$$f(v_1 + v_2) = f(v_1) + f(v_2),$$

per ogni $v_1, v_2 \in V$.

Una tale funzione è detta *K -lineare* (o, più semplicemente, *lineare*) se, oltre ad essere additiva, essa soddisfa la seguente uguaglianza:

$$f(\lambda v) = \lambda f(v),$$

per ogni $v \in V$ e ogni $\lambda \in K$.

Una funzione lineare tra due spazi vettoriali è anche detta un *omomorfismo* di spazi vettoriali.

OSSERVAZIONE 1.2. Supponiamo che f sia una funzione additiva tra due spazi vettoriali V e W definiti sul campo K , e supponiamo che $\mathbb{Q} \subseteq K$. Per ogni intero positivo n ed ogni $v \in V$, si ha

$$f(nv) = f(\underbrace{v + v + \cdots + v}_n) = \underbrace{f(v) + f(v) + \cdots + f(v)}_n = nf(v).$$

Si ha inoltre $f(\mathbf{0}_V) = \mathbf{0}_W$: infatti dall’additività di f si deduce che

$$f(v) = f(v + \mathbf{0}_V) = f(v) + f(\mathbf{0}_V),$$

da cui, sommando ad ambo i membri il vettore $-f(v)$, si conclude.

Utilizzando questo risultato si può dimostrare che $f(-v) = -f(v)$: si ha infatti

$$\mathbf{0}_W = f(\mathbf{0}_V) = f(v + (-v)) = f(v) + f(-v),$$

da cui segue che $f(-v)$ è l’opposto di $f(v)$.

Combinando questi risultati, si conclude che l’uguaglianza $f(nv) = nf(v)$ vale per ogni vettore $v \in V$ ed ogni $n \in \mathbb{Z}$: una funzione additiva è quindi automaticamente \mathbb{Z} -lineare.

In effetti una funzione additiva è anche \mathbb{Q} -lineare. Infatti, per ogni $n \neq 0$, si ha

$$f(v) = f\left(n \frac{1}{n} v\right) = n f\left(\frac{1}{n} v\right),$$

da cui segue che $f\left(\frac{1}{n} v\right) = \frac{1}{n} f(v)$. Infine, per ogni $\frac{m}{n} \in \mathbb{Q}$, si ha

$$f\left(\frac{m}{n} v\right) = m f\left(\frac{1}{n} v\right) = \frac{m}{n} f(v).$$

Tuttavia, se K contiene propriamente \mathbb{Q} , dall'additività di una funzione non si può dedurre, in generale, la sua K -linearità. Ad esempio, dimostreremo in seguito (vedi Esempio 1.22) che esistono delle funzioni additive (e quindi \mathbb{Q} -lineari) che non sono \mathbb{R} -lineari!

Veniamo ora alla definizione di isomorfismo di spazi vettoriali.

DEFINIZIONE 1.3. Sia $f : V \rightarrow W$ un omomorfismo di spazi vettoriali. f è un *isomorfismo* se esiste un omomorfismo $g : W \rightarrow V$ tale che $g \circ f = \text{id}_V$ e $f \circ g = \text{id}_W$.

In altre parole, dire che f è un isomorfismo di spazi vettoriali equivale a dire che f è un omomorfismo invertibile e che la sua funzione inversa è lineare.

Due spazi vettoriali V e W su K si dicono *isomorfi* se esiste un isomorfismo $f : V \rightarrow W$. Quando vorremo indicare che V e W sono isomorfi senza specificare quale sia l'isomorfismo, scriveremo semplicemente $V \cong W$.

Dalla definizione data segue che un isomorfismo di spazi vettoriali è una funzione biiettiva. Dimostriamo ora il viceversa:

PROPOSIZIONE 1.4. *Sia $f : V \rightarrow W$ un omomorfismo di spazi vettoriali. Se la funzione f è biiettiva essa è un isomorfismo.*

DIMOSTRAZIONE. Poiché f è biiettiva essa è invertibile. Rimane quindi solo da dimostrare che la funzione inversa $f^{-1} : W \rightarrow V$ è lineare.

Siano dunque $w_1, w_2 \in W$ e poniamo $v_1 = f^{-1}(w_1)$ e $v_2 = f^{-1}(w_2)$. Dall'additività di f si deduce che $f(v_1 + v_2) = f(v_1) + f(v_2) = w_1 + w_2$, da cui segue che $f^{-1}(w_1 + w_2) = v_1 + v_2 = f^{-1}(w_1) + f^{-1}(w_2)$; ciò dimostra che f^{-1} è additiva.

Consideriamo ora uno scalare $\lambda \in K$. Dalla linearità di f segue che $f(\lambda v_1) = \lambda f(v_1) = \lambda w_1$, da cui si deduce che $f^{-1}(\lambda w_1) = \lambda v_1 = \lambda f^{-1}(w_1)$. Abbiamo così dimostrato che f^{-1} è lineare. \square

OSSERVAZIONE 1.5. Un omomorfismo iniettivo di spazi vettoriali è anche detto un *monomorfismo*, mentre un omomorfismo suriettivo è chiamato *epimorfismo*. Un monomorfismo che sia anche epimorfismo è dunque un omomorfismo biiettivo e quindi, in base alla proposizione precedente, è un isomorfismo.

L'importanza della nozione di isomorfismo è data dal fatto che esso permette di "identificare" spazi vettoriali diversi, a patto che siano isomorfi. Si può così arrivare ad una classificazione degli spazi vettoriali, come descritto nel seguente risultato:

PROPOSIZIONE 1.6. *Sia V uno spazio vettoriale di dimensione n sul campo K . Allora V è isomorfo (non canonicamente) allo spazio vettoriale K^n .*

DIMOSTRAZIONE. Fissiamo una base $\{v_1, v_2, \dots, v_n\}$ di V . Facciamo notare che ciò è sempre possibile, anche se non c'è, in generale, nessuna scelta "canonica" per una tale base.

Ora possiamo definire una funzione $f : V \rightarrow K^n$ la quale associa ad un vettore $v \in V$ l'unica n -upla $(\lambda_1, \dots, \lambda_n) \in K^n$ per cui si ha

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n.$$

È immediato verificare che la funzione f è lineare. Essa è inoltre biiettiva, dato che $\{v_1, v_2, \dots, v_n\}$ è una base di V . Dalla Proposizione 1.4 si deduce quindi che f è un isomorfismo.

Vogliamo far notare che la funzione f dipende dalla base di V che è stata scelta. La non esistenza, in generale, di una base canonica ha quindi come conseguenza la non esistenza di una scelta canonica di un isomorfismo tra V e K^n . \square

COROLLARIO 1.7. *Due spazi vettoriali di dimensione finita sul campo K sono isomorfi (non in modo canonico) se e solo se hanno la stessa dimensione.*

1.1. Nucleo, Conucleo e Immagine. Introduciamo ora alcuni sottospazi vettoriali particolarmente importanti associati ad una funzione lineare:

DEFINIZIONE 1.8. Sia $f : V \rightarrow W$ una funzione lineare tra due spazi vettoriali. Il *nucleo* di f è l'insieme

$$\text{Ker}(f) = \{v \in V \mid f(v) = \mathbf{0}\}.$$

L'*immagine* di f è l'insieme

$$\text{Im}(f) = \{w \in W \mid w = f(v), \text{ per qualche } v \in V\}.$$

PROPOSIZIONE 1.9. *Il nucleo di una funzione lineare $f : V \rightarrow W$ è un sottospazio vettoriale di V , mentre l'immagine di f è un sottospazio vettoriale di W .*

DIMOSTRAZIONE. Siano $v_1, v_2 \in \text{Ker}(f)$ e consideriamo una combinazione lineare $\lambda_1 v_1 + \lambda_2 v_2$, con $\lambda_1, \lambda_2 \in K$. Dalla linearità di f segue che

$$f(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 f(v_1) + \lambda_2 f(v_2) = \mathbf{0},$$

quindi $\lambda_1 v_1 + \lambda_2 v_2 \in \text{Ker}(f)$. Questo dimostra che $\text{Ker}(f)$ è un sottospazio vettoriale di V .

Passiamo ora all'immagine di f . Siano $w_1, w_2 \in \text{Im}(f)$ e siano $v_1, v_2 \in V$ tali che $w_1 = f(v_1)$ e $w_2 = f(v_2)$. Dalla linearità di f segue che

$$f(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 f(v_1) + \lambda_2 f(v_2) = \lambda_1 w_1 + \lambda_2 w_2,$$

il che significa che $\lambda_1 w_1 + \lambda_2 w_2 \in \text{Im}(f)$, per ogni $\lambda_1, \lambda_2 \in K$. Ciò dimostra che $\text{Im}(f)$ è un sottospazio vettoriale di W . \square

Poiché l'immagine di f è un sottospazio vettoriale di W , possiamo considerare lo spazio vettoriale quoziente $W/\text{Im}(f)$:

DEFINIZIONE 1.10. Il *conucleo* di una funzione lineare $f : V \rightarrow W$ è lo spazio vettoriale quoziente

$$\text{Coker}(f) = W/\text{Im}(f).$$

Il seguente risultato fornisce una caratterizzazione dei monomorfismi e degli epimorfismi in termini di annullamento del nucleo e del conucleo, rispettivamente.

PROPOSIZIONE 1.11. *Sia $f : V \rightarrow W$ una funzione lineare. Allora:*

- (i) f è iniettiva se e solo se $\text{Ker}(f) = \{\mathbf{0}\}$,
- (ii) f è suriettiva se e solo se $\text{Coker}(f) = \{\mathbf{0}\}$.

DIMOSTRAZIONE. (i) Supponiamo che f sia iniettiva. Sia $v \in \text{Ker}(f)$: si ha quindi $f(v) = \mathbf{0}$. Ricordando che $f(\mathbf{0}) = \mathbf{0}$, dall'iniettività di f si deduce che $v = \mathbf{0}$, il che dimostra che $\text{Ker}(f) = \{\mathbf{0}\}$.

Viceversa, supponiamo che $\text{Ker}(f) = \{\mathbf{0}\}$. Siano $v_1, v_2 \in V$ tali che $f(v_1) = f(v_2)$. Dalla linearità di f si ha

$$f(v_1 - v_2) = f(v_1) - f(v_2) = \mathbf{0},$$

quindi $v_1 - v_2 \in \text{Ker}(f)$. Poiché, per ipotesi, $\text{Ker}(f) = \{\mathbf{0}\}$, si ha $v_1 - v_2 = \mathbf{0}$, cioè $v_1 = v_2$. Questo dimostra che f è iniettiva.

(ii) Dire che f è suriettiva equivale a dire che $\text{Im}(f) = W$. Ma, per la definizione del conucleo di f , ciò equivale ad affermare che $\text{Coker}(f) = \{\mathbf{0}\}$. \square

Dimostriamo ora un importante risultato, noto anche come il “Primo Teorema di Isomorfismo” per gli spazi vettoriali.

TEOREMA 1.12 (Primo Teorema di Isomorfismo). *Sia $f : V \rightarrow W$ un omomorfismo di spazi vettoriali. Esiste un unico omomorfismo $\bar{f} : V/\text{Ker}(f) \rightarrow W$ che rende commutativo il seguente diagramma*

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ & \searrow \pi & \nearrow \bar{f} \\ & V/\text{Ker}(f) & \end{array}$$

cioè tale che $\bar{f} \circ \pi = f$, ove $\pi : V \rightarrow V/\text{Ker}(f)$ è la proiezione canonica.

Inoltre, la funzione \bar{f} è iniettiva e induce un isomorfismo

$$V/\text{Ker}(f) \cong \text{Im}(f).$$

DIMOSTRAZIONE. Per ogni $v \in V$ indichiamo con $[v] = \pi(v)$ la sua classe di equivalenza nel quoziente $V/\text{Ker}(f)$. Ricordiamo che

$$[v] = \{v + u \mid u \in \text{Ker}(f)\}.$$

Definiamo la funzione \bar{f} ponendo $\bar{f}([v]) = f(v)$. La funzione \bar{f} è ben definita: infatti se $[v_1] = [v_2]$ si ha $v_1 = v_2 + u$, per qualche $u \in \text{Ker}(f)$, quindi

$$f(v_1) = f(v_2 + u) = f(v_2) + f(u) = f(v_2),$$

il che dimostra che $\bar{f}([v_1]) = \bar{f}([v_2])$. Dalla definizione segue inoltre che $(\bar{f} \circ \pi)(v) = \bar{f}([v]) = f(v)$, per ogni $v \in V$.

La linearità di \bar{f} è conseguenza della linearità di f :

$$\begin{aligned} \bar{f}(\lambda_1[v_1] + \lambda_2[v_2]) &= \bar{f}([\lambda_1v_1 + \lambda_2v_2]) \\ &= f(\lambda_1v_1 + \lambda_2v_2) \\ &= \lambda_1f(v_1) + \lambda_2f(v_2) \\ &= \lambda_1\bar{f}([v_1]) + \lambda_2\bar{f}([v_2]). \end{aligned}$$

Dimostriamo ora che \bar{f} è iniettiva. Per la Proposizione 1.11, basta dimostrare che se $\bar{f}([v]) = \mathbf{0}$ allora deve essere $[v] = \mathbf{0}$. Ma $\bar{f}([v]) = f(v) = \mathbf{0}$ equivale a dire che $v \in \text{Ker}(f)$, che significa proprio $[v] = \mathbf{0}$.

Infine, la funzione indotta $\bar{f} : V/\text{Ker}(f) \rightarrow \text{Im}(f)$ è ovviamente suriettiva, per definizione di $\text{Im}(f)$. Essa è quindi un omomorfismo biiettivo e dunque un isomorfismo. \square

COROLLARIO 1.13. Sia $f : V \rightarrow W$ una funzione lineare. Se V ha dimensione finita, si ha

$$\dim(V) = \dim \text{Ker}(f) + \dim \text{Im}(f).$$

DIMOSTRAZIONE. Il teorema precedente afferma che gli spazi vettoriali $V/\text{Ker}(f)$ e $\text{Im}(f)$ sono isomorfi; essi hanno quindi la stessa dimensione. Ricordando che (vedi Cap. 2, Proposizione 2.47)

$$\dim(V/\text{Ker}(f)) = \dim(V) - \dim \text{Ker}(f),$$

si ha $\dim(V) - \dim \text{Ker}(f) = \dim \text{Im}(f)$. \square

OSSERVAZIONE 1.14. Sia $f : V \rightarrow W$ una funzione lineare tra due spazi vettoriali.

La dimensione dell'immagine di f è detta il *rango* di f ,

$$\text{rk}(f) = \dim \text{Im}(f)$$

mentre la dimensione del nucleo di f è detta la *nullità* di f ,

$$\text{null}(f) = \dim \text{Ker}(f).$$

Il corollario precedente afferma quindi che, per ogni omomorfismo $f : V \rightarrow W$, si ha

$$\text{rk}(f) + \text{null}(f) = \dim(V).$$

Dimostriamo ora altri due teoremi di isomorfismo, che sono delle facili conseguenze del primo.

TEOREMA 1.15 (Secondo Teorema di Isomorfismo). *Sia V uno spazio vettoriale e siano U e W due sottospazi di V , con $U \subseteq W \subseteq V$. Allora esiste un isomorfismo*

$$\frac{V/U}{W/U} \cong \frac{V}{W}.$$

DIMOSTRAZIONE. Per ogni vettore $v \in V$ indichiamo con $[v]_U$ la sua classe di equivalenza in V/U e con $[v]_W$ la sua classe di equivalenza in V/W .

Consideriamo la funzione

$$f : V/U \rightarrow V/W$$

definita ponendo $f([v]_U) = [v]_W$. Si verifica facilmente che f è ben definita e che è un omomorfismo.

Consideriamo ora un elemento $[v]_U \in V/U$ che appartenga al nucleo di f . Ciò significa che $f([v]_U) = [v]_W = \mathbf{0}$, il che equivale a dire che $v \in W$. Da ciò segue che $\text{Ker}(f) = W/U$. Dal primo teorema di isomorfismo si deduce allora l'esistenza di un isomorfismo tra $(V/U)/\text{Ker}(f) = (V/U)/(W/U)$ e $\text{Im}(f)$. A questo punto basta osservare che $\text{Im}(f) = V/W$, dato che f è suriettiva. \square

TEOREMA 1.16 (Terzo Teorema di Isomorfismo). *Sia V uno spazio vettoriale e siano U e W due sottospazi di V . Esiste un isomorfismo*

$$\frac{U+W}{U} \cong \frac{W}{U \cap W}.$$

DIMOSTRAZIONE. Osserviamo che, poiché $W \subseteq U+W$, la restrizione a W della proiezione canonica $\pi : U+W \rightarrow (U+W)/U$ definisce una funzione lineare

$$f : W \rightarrow \frac{U+W}{U}.$$

Per prima cosa dimostriamo che f è suriettiva. Ricordiamo che ogni elemento di $U+W$ può essere scritto nella forma $u+w$, per qualche $u \in U$ e qualche $w \in W$. Indichiamo dunque con $[u+w]_U$ la classe di equivalenza dell'elemento $u+w$ nel quoziente $(U+W)/U$. Dato che $u \in U$, si ha $[u]_U = \mathbf{0}$, da cui segue che $[u+w]_U = [w]_U$. Si ha pertanto $[u+w]_U = [w]_U = f(w)$, il che dimostra che $\text{Im}(f) = (U+W)/U$.

Determiniamo ora il nucleo di f . Sia $w \in W$ tale che $f(w) = [w]_U = \mathbf{0}$. Ciò equivale a dire che $w \in U$, il che prova che $\text{Ker}(f) = U \cap W$.

Applicando ora il primo teorema di isomorfismo alla funzione lineare f si conclude. \square

OSSERVAZIONE 1.17. Siano V e W due spazi vettoriali su K e indichiamo con $\text{Hom}(V, W)$ l'insieme delle applicazioni lineari da V a W . Definiamo la somma di due applicazioni lineari $f, g \in \text{Hom}(V, W)$ ponendo $(f + g)(v) = f(v) + g(v)$, per ogni $v \in V$; essa è ancora una funzione lineare. Definiamo poi il prodotto di uno scalare $\lambda \in K$ per una funzione lineare $f \in \text{Hom}(V, W)$ ponendo $(\lambda f)(v) = \lambda(f(v))$, per ogni $v \in V$. Si verifica facilmente che l'insieme $\text{Hom}(V, W)$, dotato delle due operazioni appena definite, è uno spazio vettoriale su K .

Notiamo infine che, se $W = V$, la composizione di due applicazioni lineari $f, g : V \rightarrow V$ è ancora una funzione lineare, cioè $g \circ f \in \text{Hom}(V, V)$, per ogni $f, g \in \text{Hom}(V, V)$. L'insieme $\text{Hom}(V, V)$, dotato dell'operazione di somma e dell'operazione di composizione, risulta essere un anello (unitario) non commutativo. Se, in aggiunta a queste due operazioni, consideriamo anche il prodotto di una funzione lineare per uno scalare $\lambda \in K$, si ottiene una struttura nota con il nome di K -algebra.

OSSERVAZIONE 1.18. Un omomorfismo di uno spazio vettoriale V in sé stesso, $f : V \rightarrow V$, è anche detto *endomorfismo*. Se esso è invertibile, si parla allora di *automorfismo*. L'insieme degli endomorfismi di uno spazio vettoriale V è indicato con $\text{End}(V)$ e il sottoinsieme costituito dagli automorfismi è indicato con $\text{Aut}(V)$.

OSSERVAZIONE 1.19. Nell'enunciato del Teorema 1.12 abbiamo usato l'espressione "diagramma commutativo." Riteniamo utile precisarne il significato.

Un *diagramma* costituito da spazi vettoriali e omomorfismi tra di essi è detto *commutativo* se, per ogni coppia di spazi vettoriali, tutte le funzioni tra di essi che si possono ottenere come composizione di omomorfismi del diagramma, sono uguali.

A titolo di esempio, consideriamo il seguente diagramma:

$$\begin{array}{ccccc}
 V_1 & \xrightarrow{f_1} & V_2 & \xrightarrow{f_2} & V_3 \\
 f_3 \downarrow & \searrow f_4 & \downarrow f_5 & & \downarrow f_6 \\
 V_4 & \xrightarrow{f_7} & V_5 & \xrightarrow{f_8} & V_6
 \end{array}$$

Dire che esso è commutativo significa che $f_5 \circ f_1 = f_4$, $f_7 \circ f_3 = f_4$, $f_6 \circ f_2 = f_8 \circ f_5$, etc.

1.2. Applicazioni lineari e basi. Ci proponiamo ora di studiare le proprietà di una funzione lineare $f : V \rightarrow W$, in relazione alla scelta di basi per gli spazi vettoriali V e W .

Iniziamo col dimostrare che una funzione lineare $f : V \rightarrow W$ è completamente determinata dalla conoscenza delle immagini dei vettori di una base di V , le quali possono essere scelte arbitrariamente in W .

PROPOSIZIONE 1.20. *Siano V e W due spazi vettoriali sul campo K e sia $\{v_i\}_{i \in I}$ una base (non necessariamente finita) di V .*

- (i) *Un omomorfismo $f : V \rightarrow W$ è determinato, in modo unico, dalle immagini dei vettori v_i , per ogni $i \in I$.*
- (ii) *Scelti arbitrariamente dei vettori $\{w_i\}_{i \in I}$ in W , esiste un unico omomorfismo $f : V \rightarrow W$ tale che $f(v_i) = w_i$, per ogni $i \in I$.*

DIMOSTRAZIONE. (i) Sia $f : V \rightarrow W$ una funzione lineare e supponiamo di conoscere $f(v_i)$, per ogni $i \in I$. Poiché $\{v_i\}_{i \in I}$ è una base di V , ogni vettore $v \in V$ si può scrivere, in modo unico, come combinazione lineare finita dei vettori v_i :

$$v = \lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \cdots + \lambda_n v_{i_n}.$$

Dalla linearità di f segue che

$$(1.1) \quad f(v) = \lambda_1 f(v_{i_1}) + \lambda_2 f(v_{i_2}) + \cdots + \lambda_n f(v_{i_n}),$$

il che dimostra che la conoscenza di $f(v_i)$, per ogni $i \in I$, determina, in modo unico, $f(v)$, per ogni $v \in V$. In altre parole, se $g : V \rightarrow W$ è un omomorfismo tale che $g(v_i) = f(v_i)$, per ogni $i \in I$, da (1.1) segue che $g(v) = f(v)$, per ogni $v \in V$.

(ii) Per ogni $i \in I$ scegliamo arbitrariamente un vettore $w_i \in W$. Definiamo una funzione $f : V \rightarrow W$ ponendo $f(v_i) = w_i$, per ogni $i \in I$, ed estendendo f per linearità a tutto V , cioè ponendo

$$f(v) = \lambda_1 f(v_{i_1}) + \lambda_2 f(v_{i_2}) + \cdots + \lambda_n f(v_{i_n}),$$

se $v = \lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \cdots + \lambda_n v_{i_n}$.

Si verifica immediatamente che f è ben definita ed è lineare. L'unicità di una tale f discende dal punto (i). \square

COROLLARIO 1.21. *Siano V e W due spazi vettoriali sul campo K , sia $\{v_i\}_{i \in I}$ una base (non necessariamente finita) di V e sia $f : V \rightarrow W$ un'applicazione lineare.*

- (i) *f è iniettiva se e solo se $\{f(v_i)\}_{i \in I}$ è un insieme libero;*
- (ii) *f è suriettiva se e solo se $\{f(v_i)\}_{i \in I}$ è un insieme di generatori di W ;*
- (iii) *f è un isomorfismo se e solo se $\{f(v_i)\}_{i \in I}$ è una base di W .*

DIMOSTRAZIONE. (i) Ricordiamo, dalla Proposizione 1.11, che f è iniettiva se e solo se $\text{Ker}(f) = \{\mathbf{0}\}$. Dimostriamo quindi l'implicazione $\text{Ker}(f) = \{\mathbf{0}\} \Rightarrow \{f(v_i)\}_{i \in I}$ è un insieme libero.

Consideriamo una combinazione lineare

$$\lambda_1 f(v_{i_1}) + \lambda_2 f(v_{i_2}) + \cdots + \lambda_n f(v_{i_n}) = \mathbf{0}.$$

Si ha

$$\lambda_1 f(v_{i_1}) + \lambda_2 f(v_{i_2}) + \cdots + \lambda_n f(v_{i_n}) = f(\lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \cdots + \lambda_n v_{i_n}),$$

da cui segue

$$\lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \cdots + \lambda_n v_{i_n} \in \text{Ker}(f).$$

Dato che, per ipotesi, $\text{Ker}(f) = \{\mathbf{0}\}$, si ha

$$\lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \cdots + \lambda_n v_{i_n} = \mathbf{0},$$

da cui segue

$$\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0,$$

perché i vettori $\{v_i\}_{i \in I}$ sono una base di V .

Dimostriamo ora l'implicazione opposta. Sia $v \in \text{Ker}(f)$ e scriviamo

$$v = \lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \cdots + \lambda_n v_{i_n},$$

per qualche n e qualche $\lambda_1, \dots, \lambda_n \in K$. Poiché $f(v) = \mathbf{0}$, dalla linearità di f si deduce che

$$\lambda_1 f(v_{i_1}) + \lambda_2 f(v_{i_2}) + \cdots + \lambda_n f(v_{i_n}) = \mathbf{0}.$$

Poiché, per ipotesi, l'insieme $\{f(v_i)\}_{i \in I}$ è libero, si ha

$$\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$$

e dunque $v = \mathbf{0}$, il che dimostra che $\text{Ker}(f) = \{\mathbf{0}\}$.

(ii) Ricordiamo che affermare che f è suriettiva equivale a dire che $\text{Im}(f) = W$. Osserviamo inoltre che $\text{Im}(f)$ è generata dai vettori $f(v_i)$, al variare di $i \in I$. Infatti, per ogni $w \in \text{Im}(f)$ esiste un vettore $v \in V$ tale che $w = f(v)$. Poiché $\{v_i\}_{i \in I}$ è una base di V , è possibile esprimere v come combinazione lineare di un numero finito di v_i ,

$$v = \lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \cdots + \lambda_n v_{i_n}.$$

Si ha dunque

$$w = f(v) = \lambda_1 f(v_{i_1}) + \lambda_2 f(v_{i_2}) + \cdots + \lambda_n f(v_{i_n}),$$

il che dimostra che l'insieme dei vettori $\{f(v_i)\}_{i \in I}$ genera l'immagine di f .

Da quanto detto segue quindi che $\text{Im}(f) = W$ se e solo se $\{f(v_i)\}_{i \in I}$ è un insieme di generatori di W .

(iii) Poiché f è un isomorfismo se e solo se essa è biiettiva (vedi Proposizione 1.4), dai punti (i) e (ii) segue che f è un isomorfismo se e solo se $\{f(v_i)\}_{i \in I}$ è un insieme libero di generatori di W , cioè una base di W . \square

ESEMPIO 1.22. In questo esempio vedremo come si possa costruire una funzione additiva $f : \mathbb{R} \rightarrow \mathbb{R}$ che non sia \mathbb{R} -lineare.

Consideriamo \mathbb{R} come spazio vettoriale sul campo \mathbb{Q} . I due "vettori" $v_1 = 1$ e $v_2 = \pi$ sono linearmente indipendenti su \mathbb{Q} (ciò deriva dal fatto che π è irrazionale), quindi esiste una base $\{v_i\}_{i \in I}$ di \mathbb{R} su \mathbb{Q} che contiene i numeri 1 e π (osserviamo che una base di \mathbb{R} su \mathbb{Q} non può essere numerabile).

Per la Proposizione 1.20 è possibile definire una funzione \mathbb{Q} -lineare $f : \mathbb{R} \rightarrow \mathbb{R}$ fissando arbitrariamente i valori di $f(v_i)$, per ogni $i \in I$. Se poniamo $f(1) = 1$ e $f(\pi) = 2$ (e fissiamo arbitrariamente i rimanenti

$f(v_i) \in \mathbb{R}$), otteniamo una funzione additiva (e quindi \mathbb{Q} -lineare) la quale non è \mathbb{R} -lineare. Se lo fosse si avrebbe infatti

$$f(\pi) = f(\pi 1) = \pi f(1) = \pi,$$

contro l'ipotesi che $f(\pi) = 2$.

2. Matrici

Siano V e W due spazi vettoriali sul campo K , di dimensioni n e m , rispettivamente, e fissiamo delle basi $\{v_1, \dots, v_n\}$ di V e $\{w_1, \dots, w_m\}$ di W .

In base alla Proposizione 1.20, una funzione lineare $f : V \rightarrow W$ è determinata, in modo unico, dalla conoscenza dei vettori $f(v_j)$, per $j = 1, \dots, n$. Poiché $\{w_1, \dots, w_m\}$ è una base di W , per ogni $j = 1, \dots, n$ possiamo scrivere

$$f(v_j) = \sum_{i=1}^m a_{ij} w_i,$$

per degli opportuni $a_{ij} \in K$, con $i = 1, \dots, m$ e $j = 1, \dots, n$.

Da quanto detto si deduce quindi che una funzione lineare $f : V \rightarrow W$ è determinata in modo unico dal dato di mn elementi a_{ij} del campo K . Tali elementi costituiscono ciò che va sotto il nome di *matrice*.

DEFINIZIONE 2.1. Una *matrice*, con m righe e n colonne (o matrice $m \times n$) a coefficienti in K è il dato di mn elementi di K , scritti solitamente sotto forma di tabella rettangolare costituita da m righe e n colonne:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Una matrice A di questo tipo sarà spesso indicata semplicemente con la scrittura

$$A = (a_{ij}),$$

dove $i = 1, \dots, m$ è detto *indice di riga* mentre $j = 1, \dots, n$ è detto *indice di colonna*.

Ad ogni funzione lineare $f : V \rightarrow W$ può dunque essere associata una matrice $m \times n$ a coefficienti in K . Naturalmente tale matrice dipende, oltre che dalla funzione f , anche dalla scelta delle basi di V e W .

OSSERVAZIONE 2.2. Ricordiamo che se un vettore $v \in V$ si scrive come combinazione lineare

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n$$

degli elementi di una base $\{v_1, \dots, v_n\}$ di V , i coefficienti $\lambda_1, \dots, \lambda_n$ che compaiono in una tale espressione si dicono le *coordinate* di v rispetto alla base fissata.

Possiamo allora osservare che, dalla definizione della matrice A associata ad un omomorfismo $f : V \rightarrow W$, rispetto a delle basi $\{v_1, \dots, v_n\}$ di V e $\{w_1, \dots, w_m\}$ di W , segue che le coordinate del vettore $f(v_j)$, rispetto alla base di W fissata, costituiscono la j -esima colonna della matrice A . Questa osservazione si rivela utile quando è necessario scrivere esplicitamente la matrice associata ad una data funzione lineare.

OSSERVAZIONE 2.3. In tutta questa sezione supporremo sempre che gli spazi vettoriali abbiano dimensione finita. Facciamo comunque notare che molti risultati si possono estendere, con opportune modifiche, anche a spazi vettoriali di dimensione infinita.

Consideriamo ora due applicazioni lineari $f, g : V \rightarrow W$ e indichiamo con $A = (a_{ij})$ e $B = (b_{ij})$ le matrici ad esse associate. La somma di f e g è l'applicazione lineare definita da $(f + g)(v) = f(v) + g(v)$, per ogni $v \in V$. In particolare, per ogni vettore v_j della base di V , si ha

$$\begin{aligned} (f + g)(v_j) &= f(v_j) + g(v_j) = \sum_{i=1}^m a_{ij}w_i + \sum_{i=1}^m b_{ij}w_i \\ &= \sum_{i=1}^m (a_{ij} + b_{ij})w_i. \end{aligned}$$

La matrice associata alla funzione $f + g$ ha quindi come coefficienti le somme $a_{ij} + b_{ij}$ dei coefficienti delle matrici A e B , associate rispettivamente a f e g . Questo risultato motiva la seguente definizione:

DEFINIZIONE 2.4. Siano $A = (a_{ij})$ e $B = (b_{ij})$ due matrici $m \times n$ a coefficienti in K . La loro somma è la matrice

$$A + B = (a_{ij} + b_{ij}),$$

ottenuta sommando i coefficienti di A e B che si trovano nelle stesse posizioni.

Sia ora $\lambda \in K$ e consideriamo la funzione λf definita da $(\lambda f)(v) = \lambda f(v)$, per ogni $v \in V$. Valutando questa funzione sui vettori della base di V , si ha

$$(\lambda f)(v_j) = \lambda f(v_j) = \lambda \sum_{i=1}^m a_{ij}w_i = \sum_{i=1}^m (\lambda a_{ij})w_i,$$

da cui si deduce che la matrice associata alla funzione λf è la matrice i cui coefficienti sono dati dal prodotto di λ per i coefficienti della matrice A di f .

DEFINIZIONE 2.5. Per ogni $\lambda \in K$, il prodotto di λ per una matrice $A = (a_{ij})$ a coefficienti in K è la matrice

$$\lambda A = (\lambda a_{ij}).$$

Indicheremo con $M_{m,n}(K)$ l'insieme delle matrici con m righe e n colonne, a coefficienti in K . Da quanto visto sopra si deduce che esiste una biiezione tra l'insieme $\text{Hom}(V, W)$ e $M_{m,n}(K)$. Dato che $\text{Hom}(V, W)$, con le operazioni di somma di funzioni e di prodotto di una funzione per uno scalare, è uno spazio vettoriale su K , anche l'insieme $M_{m,n}(K)$, con le due operazioni sopra definite, risulta essere un K -spazio vettoriale. Inoltre, i due spazi vettoriali $\text{Hom}(V, W)$ e $M_{m,n}(K)$ sono isomorfi.

Per analogia con la definizione della base canonica di K^n , definiamo delle matrici E_{ij} , con $i = 1, \dots, m$ e $j = 1, \dots, n$, i cui coefficienti sono tutti nulli eccetto quello di posto (i, j) (cioè quello che si trova sulla i -esima riga e sulla j -esima colonna), che è uguale a 1. È immediato verificare che le mn matrici E_{ij} appena definite formano una base dello spazio vettoriale $M_{m,n}(K)$. Ciò è conseguenza del fatto che ogni matrice $A = (a_{ij})$ si scrive, in modo unico, come segue:

$$A = \sum_{i,j} a_{ij} E_{ij}.$$

Possiamo riassumere quanto appena visto nel seguente risultato:

PROPOSIZIONE 2.6. $M_{m,n}(K)$ è uno spazio vettoriale di dimensione mn su K . Se V e W sono due K -spazi vettoriali di dimensioni n e m rispettivamente, vi è un isomorfismo $\text{Hom}(V, W) \cong M_{m,n}(K)$. Tale isomorfismo non è canonico, in quanto dipende dalla scelta di una base di V e di una base di W .

In particolare, se $V = W$ e quindi $m = n$, lo spazio vettoriale $\text{End}(V) = \text{Hom}(V, V)$ è isomorfo a $M_n(K) = M_{n,n}(K)$ ed ha dimensione n^2 .

Vediamo ora quale operazione tra matrici corrisponde alla composizione di due funzioni lineari. A tal fine consideriamo tre spazi vettoriali U, V e W , di dimensioni rispettivamente r, n e m , e fissiamo delle loro basi $\{u_1, \dots, u_r\}$, $\{v_1, \dots, v_n\}$ e $\{w_1, \dots, w_m\}$. Siano $f : V \rightarrow W$ e $g : U \rightarrow V$ due applicazioni lineari e indichiamo con A la matrice di f , con B la matrice di g e con C la matrice di $f \circ g : U \rightarrow W$, rispetto alle basi indicate. Ricordiamo che A è una matrice $m \times n$, B è una matrice $n \times r$, mentre C è una matrice $m \times r$.

Per ogni vettore u_j della base di U si ha:

$$\begin{aligned} (f \circ g)(u_j) &= f(g(u_j)) = f\left(\sum_{h=1}^n b_{hj}v_h\right) \\ &= \sum_{h=1}^n b_{hj}f(v_h) = \sum_{h=1}^n b_{hj}\left(\sum_{i=1}^m a_{ih}w_i\right) \\ &= \sum_{i=1}^m \left(\sum_{h=1}^n a_{ih}b_{hj}\right)w_i. \end{aligned}$$

Poiché $C = (c_{ij})$ è la matrice di $f \circ g$, si ha anche

$$(f \circ g)(u_j) = \sum_{i=1}^m c_{ij}w_i.$$

Dall'uguaglianza di queste due ultime espressioni (e dal fatto che i vettori $\{w_1, \dots, w_m\}$ sono una base di W) segue che

$$c_{ij} = \sum_{h=1}^n a_{ih}b_{hj},$$

per ogni $i = 1, \dots, m$ e $j = 1, \dots, r$. Utilizzeremo dunque questa formula per definire un prodotto di matrici, in modo che il prodotto delle matrici A e B associate agli omomorfismi f e g fornisca proprio la matrice associata all'omomorfismo composto $f \circ g$.

DEFINIZIONE 2.7. Date due matrici $A \in M_{m,n}(K)$ e $B \in M_{n,r}(K)$, il loro *prodotto* è la matrice $C \in M_{m,r}(K)$ i cui coefficienti sono dati da

$$(2.1) \quad c_{ij} = \sum_{h=1}^n a_{ih}b_{hj},$$

per ogni $i = 1, \dots, m$ e $j = 1, \dots, r$. Questo prodotto di matrici è anche detto *prodotto righe per colonne*.

Vediamo più in dettaglio come si calcola un tale prodotto di matrici. Siano A e B due matrici come sopra e vogliamo determinare il loro prodotto $C = AB$. Per calcolare l'elemento c_{ij} , che si trova sulla i -esima riga e sulla j -esima colonna della matrice C , dobbiamo selezionare la i -esima riga della matrice A e la j -esima colonna della matrice B :

$$(a_{i1}, a_{i2}, \dots, a_{in}) \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{pmatrix}$$

dopodiché dobbiamo “moltiplicare” questa riga per questa colonna nel modo indicato dalla formula (2.1), cioè dobbiamo effettuare la somma

dei prodotti componente per componente dei due vettori indicati:

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Osserviamo che per fare ciò è indispensabile che la lunghezza delle righe di A coincida con la lunghezza delle colonne di B . La matrice risultante dal prodotto di A per B avrà un numero di righe pari a quello della matrice A e un numero di colonne pari a quello della matrice B .

Un caso particolare di prodotto tra matrici si ha quando la matrice B ha una sola colonna, cioè quando B si riduce ad un vettore (scritto in colonna): si ottiene in questo modo il prodotto di una matrice per un vettore, il cui risultato è ancora un vettore. Più precisamente, data una matrice $A \in M_{m,n}(K)$ e un vettore $v = (x_1, x_2, \dots, x_n) \in K^n$ (che scriveremo in colonna), il prodotto Av è un vettore $w = (y_1, y_2, \dots, y_m) \in K^m$ dato da

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Si ottiene in questo modo un'applicazione lineare

$$F: K^n \rightarrow K^m, \quad v \mapsto w = F(v) = Av.$$

La matrice associata a questa applicazione lineare (rispetto alle basi canoniche di K^n e K^m) è proprio la matrice A .

OSSERVAZIONE 2.8. In modo del tutto equivalente si può considerare il caso particolare del prodotto di A per B , quando la matrice A si riduce ad un vettore (questa volta scritto in riga).

Consideriamo dunque una matrice $B \in M_{n,r}(K)$ ed un vettore $v = (x_1, x_2, \dots, x_n) \in K^n$ (che scriveremo in riga), il prodotto vB è un vettore $w = (y_1, y_2, \dots, y_r) \in K^r$ dato da

$$(y_1, y_2, \dots, y_r) = (x_1, x_2, \dots, x_n) \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1r} \\ b_{21} & b_{22} & \cdots & b_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nr} \end{pmatrix}$$

Anche in questo caso si ottiene un'applicazione lineare

$$g: K^n \rightarrow K^r, \quad v \mapsto w = g(v) = vB.$$

Si conclude pertanto che un omomorfismo tra due spazi vettoriali quali K^n e K^m può essere descritto sia dal prodotto di un vettore *riga* per una certa matrice, sia dal prodotto di un'altra matrice per un vettore *colonna*. Naturalmente si passa da una descrizione all'altra semplicemente scambiando tra loro i ruoli delle righe con quelli delle colonne. L'operazione che trasforma una matrice $m \times n$ in una matrice $n \times m$ scambiando tra di loro le righe con le colonne si chiama *trasposizione*.

DEFINIZIONE 2.9. Sia $A = (a_{ij}) \in M_{m,n}(K)$. La *trasposta* di A è la matrice ${}^tA \in M_{n,m}(K)$ il cui coefficiente di posto (i, j) è a_{ji} , cioè è il coefficiente di posto (j, i) della matrice A .

Il trasposto di un vettore scritto in colonna è dunque un vettore scritto in riga, e viceversa. Per comodità di notazione, d'ora in poi i vettori di K^n verranno sempre pensati come vettori colonna:

$$v = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Per indicare invece un analogo vettore pensato come vettore riga, scriveremo quindi tv :

$${}^tv = (x_1, x_2, \dots, x_n).$$

Come ultimo caso particolare del prodotto di due matrici, vediamo cosa succede quando sia A che B si riducono a dei vettori (scritti, naturalmente, il primo in riga e il secondo in colonna). In questo caso il risultato del prodotto è uno scalare, cioè un elemento di K :

$$(a_1, a_2, \dots, a_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1b_1 + a_2b_2 + \dots + a_nb_n \in K.$$

Si ottiene in questo modo la definizione di un prodotto tra due vettori di K^n , il cui risultato è uno scalare: questo è il cosiddetto *prodotto scalare* di due vettori.

DEFINIZIONE 2.10. Siano $v = (x_1, x_2, \dots, x_n)$ e $w = (y_1, y_2, \dots, y_n)$ due elementi di K^n . Il loro *prodotto scalare*, che indicheremo con $v \cdot w$ (o, a volte, con $\langle v, w \rangle$) è definito da

$$v \cdot w = {}^tvw = \sum_{i=1}^n x_i y_i.$$

Di questa nozione di prodotto scalare, e delle sue generalizzazioni, ci occuperemo in seguito.

Vediamo ora alcune proprietà dell'operazione di trasposizione.

PROPOSIZIONE 2.11. Siano $A, B \in M_{m,n}(K)$ e sia $\lambda \in K$. Si ha:

- (i) ${}^t({}^tA) = A$;
- (ii) ${}^t(A + B) = {}^tA + {}^tB$;
- (iii) ${}^t(\lambda A) = \lambda {}^tA$;
- (iv) ${}^t(AB) = {}^tB {}^tA$.

DIMOSTRAZIONE. Le prime tre proprietà sono ovvie, dimostriamo quindi la quarta. Indichiamo con a_{ij} i coefficienti di A e con \tilde{a}_{ij} i coefficienti di tA : si ha quindi $\tilde{a}_{ij} = a_{ji}$. Analogamente indichiamo con

b_{ij} e con \tilde{b}_{ij} i coefficienti di B e tB , rispettivamente. Indichiamo poi con c_{ij} i coefficienti del prodotto AB e con \tilde{c}_{ij} i coefficienti di ${}^t(AB)$. Infine, indichiamo con d_{ij} i coefficienti della matrice ${}^tB{}^tA$.

Ricordando la definizione del prodotto di due matrici, si ha:

$$\tilde{c}_{ij} = c_{ji} = \sum_h a_{jh} b_{hi},$$

mentre

$$d_{ij} = \sum_h \tilde{b}_{ih} \tilde{a}_{hj} = \sum_h a_{jh} b_{hi},$$

da cui segue che $d_{ij} = \tilde{c}_{ij}$, per ogni i e j . \square

Ritorniamo ora al prodotto di matrici e studiamo più in dettaglio alcune delle sue proprietà.

PROPOSIZIONE 2.12. *Siano A, B e C tre matrici e siano $\lambda, \mu \in K$. Ogni volta che le somme e i prodotti indicati sono definiti, si ha:*

- (i) $(AB)C = A(BC)$;
- (ii) $(A + B)C = AC + BC$;
- (iii) $A(B + C) = AB + AC$;
- (iv) $\lambda(AB) = (\lambda A)B = A(\lambda B)$;
- (v) $(\lambda + \mu)A = \lambda A + \mu A$;
- (vi) $(\lambda\mu)A = \lambda(\mu A)$.

DIMOSTRAZIONE. Tutte queste proprietà discendono dalle analoghe proprietà delle operazioni definite sulle funzioni lineari: ad esempio, la proprietà associativa del prodotto di matrici $(AB)C = A(BC)$ equivale alla proprietà associativa del prodotto di composizione $(f \circ g) \circ h = f \circ (g \circ h)$ delle funzioni. In ogni caso, si possono dimostrare direttamente mediante un semplice calcolo. A titolo di esempio, dimostriamo la prima.

Indichiamo con a_{ij} i coefficienti della matrice A , con b_{ij} quelli di B e con c_{ij} i coefficienti di C . Indichiamo inoltre con d_{ij} i coefficienti della matrice prodotto di A e B e con e_{ij} quelli del prodotto $(AB)C$. Dalla definizione del prodotto di due matrici si ha:

$$e_{ij} = \sum_h d_{ih} c_{hj} = \sum_h \left(\sum_k a_{ik} b_{kh} \right) c_{hj} = \sum_{h,k} a_{ik} b_{kh} c_{hj}.$$

Ora basta osservare che se calcoliamo, in modo analogo, i coefficienti del prodotto $A(BC)$, troviamo esattamente la stessa espressione. \square

Sia $f : V \rightarrow W$ un'applicazione lineare tra due spazi vettoriali di dimensioni n e m rispettivamente. Abbiamo già osservato che la scelta di una base $\mathbf{v} = \{v_1, \dots, v_n\}$ di V determina un isomorfismo $\alpha_{\mathbf{v}} : V \xrightarrow{\sim} K^n$ che associa ad ogni vettore $v \in V$ la n -upla $(\lambda_1, \dots, \lambda_n)$ delle sue coordinate rispetto alla base \mathbf{v} . Analogamente la scelta di una base $\mathbf{w} = \{w_1, \dots, w_m\}$ di W determina un isomorfismo $\beta_{\mathbf{w}} : W \xrightarrow{\sim} K^m$

che associa ad ogni vettore $w \in W$ la m -upla (μ_1, \dots, μ_m) delle sue coordinate rispetto alla base \mathbf{w} .

Sia dunque A la matrice di f rispetto alle basi scelte. Essa determina un'applicazione lineare $F : K^n \rightarrow K^m$, definita da

$$F : \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \mapsto \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_m \end{pmatrix} = A \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

PROPOSIZIONE 2.13. *Con le notazioni precedenti, il diagramma*

$$(2.2) \quad \begin{array}{ccc} V & \xrightarrow{f} & W \\ \alpha_{\mathbf{v}} \downarrow \wr & & \wr \downarrow \beta_{\mathbf{w}} \\ K^n & \xrightarrow{F} & K^m \end{array}$$

è commutativo

DIMOSTRAZIONE. Dobbiamo dimostrare che $\beta_{\mathbf{w}} \circ f = F \circ \alpha_{\mathbf{v}}$. Sia dunque $v \in V$ ed esprimiamo v come combinazione lineare dei vettori della base \mathbf{v} :

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n.$$

Per definizione della funzione $\alpha_{\mathbf{v}}$, si ha $\alpha_{\mathbf{v}}(v) = {}^t(\lambda_1, \dots, \lambda_n)$ (si ricordi che abbiamo deciso di scrivere gli elementi di K^n come vettori colonna). Calcolando ora $F(\alpha_{\mathbf{v}}(v))$ si ottiene il vettore

$$A \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix},$$

la cui i -esima componente è

$$(2.3) \quad a_{i1}\lambda_1 + a_{i2}\lambda_2 + \dots + a_{in}\lambda_n = \sum_{j=1}^n a_{ij}\lambda_j.$$

Calcoliamo ora $f(v)$. Dalla linearità di f e dalla definizione della matrice $A = (a_{ij})$ associata a f , si ha:

$$\begin{aligned} f(v) &= f(\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n) \\ &= \sum_{j=1}^n \lambda_j f(v_j) \\ &= \sum_{j=1}^n \lambda_j \left(\sum_{i=1}^m a_{ij} w_i \right) \\ &= \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} \lambda_j \right) w_i. \end{aligned}$$

Poniamo

$$(2.4) \quad \mu_i = \sum_{j=1}^n a_{ij} \lambda_j,$$

per $i = 1, \dots, m$, in modo che si abbia

$$f(v) = \sum_{i=1}^m \mu_i w_i.$$

La m -upla (μ_1, \dots, μ_m) rappresenta le coordinate del vettore $f(v)$ rispetto alla base \mathbf{w} e si ha pertanto $\beta_{\mathbf{w}}(f(v)) = {}^t(\mu_1, \dots, \mu_m)$. A questo punto basta osservare che l'espressione di μ_i in (2.4) coincide con l'espressione (2.3) per la i -esima componente del vettore $F(\alpha_{\mathbf{v}}(v))$. Abbiamo così dimostrato che $F(\alpha_{\mathbf{v}}(v)) = \beta_{\mathbf{w}}(f(v))$, per ogni $v \in V$. \square

OSSERVAZIONE 2.14. Questo risultato fornisce un metodo diretto per calcolare l'immagine tramite $f : V \rightarrow W$ di un qualsiasi vettore $v \in V$, nota la matrice di f rispetto a delle basi prefissate dei due spazi vettoriali V e W .

Dapprima si determinano le coordinate $(\lambda_1, \dots, \lambda_n)$ del vettore v rispetto alla base di V , poi si moltiplica la matrice A associata a f per il vettore $(\lambda_1, \dots, \lambda_n)$, scritto in colonna. Il vettore risultante è costituito dalle coordinate di $f(v)$ rispetto alla base di W .

Dal diagramma commutativo (2.2) segue che il nucleo di f e il nucleo di F sono tra loro isomorfi, essendo tale isomorfismo indotto dall'isomorfismo $\alpha_{\mathbf{v}}$. Analogamente, l'isomorfismo $\beta_{\mathbf{w}}$ induce un isomorfismo tra $\text{Im}(f)$ e $\text{Im}(F)$. In particolare questi spazi vettoriali hanno la stessa dimensione. Si ha pertanto

$$\text{null}(f) = \text{null}(F) \quad \text{e} \quad \text{rk}(f) = \text{rk}(F).$$

Dato che l'applicazione lineare $F : K^n \rightarrow K^m$ è data dalla moltiplicazione per la matrice A , diamo la seguente definizione:

DEFINIZIONE 2.15. Sia A una matrice $m \times n$ a coefficienti in K e sia $F : K^n \rightarrow K^m$ l'applicazione lineare data dalla moltiplicazione di un vettore (colonna) per la matrice A (a sinistra). Definiamo il *rango* e la *nullità* della matrice A ponendo

$$\begin{aligned} \text{rk}(A) &= \text{rk}(F) = \dim \text{Im}(F), \\ \text{null}(A) &= \text{null}(F) = \dim \text{Ker}(F). \end{aligned}$$

Osserviamo che il sottospazio $\text{Im}(F)$ di K^m è generato dalle *colonne* di A (possiamo anche osservare che nell'isomorfismo $\beta_{\mathbf{w}} : W \xrightarrow{\sim} K^m$ le colonne della matrice A corrispondono alle immagini, tramite $f : V \rightarrow W$, dei vettori della base di V , le quali generano il sottospazio $\text{Im}(f)$ di W). Pertanto la dimensione di $\text{Im}(F)$, cioè il rango di F , coincide con

il massimo numero di colonne linearmente indipendenti della matrice A . Abbiamo così dimostrato il seguente risultato:

PROPOSIZIONE 2.16. *Il rango di una matrice A è il massimo numero di colonne linearmente indipendenti di A .*

OSSERVAZIONE 2.17. Il risultato della proposizione precedente viene spesso usato come definizione del rango di una matrice. Si parla allora di *rango per colonne*, per distinguerlo da un analogo *rango per righe*, definito come il massimo numero di righe linearmente indipendenti. Vedremo in seguito che, in effetti, queste due nozioni di rango coincidono sempre, cioè in ogni matrice il massimo numero di colonne linearmente indipendenti è sempre uguale al massimo numero di righe linearmente indipendenti.

2.1. Matrici quadrate. Abbiamo visto che il prodotto di due matrici (così come la composizione di due applicazioni) non è sempre definito: affinché il prodotto AB sia definito è necessario (e sufficiente) che il numero di colonne della matrice A sia uguale al numero di righe di B . Se ci restringiamo a considerare solo matrici di tipo $n \times n$, questi problemi scompaiono e il prodotto di due matrici è sempre definito.

DEFINIZIONE 2.18. Una matrice a coefficienti in K si dice *quadrata di ordine n* se essa ha n righe e n colonne. L'insieme delle matrici quadrate di ordine n è indicato semplicemente con $M_n(K)$, al posto di $M_{n,n}(K)$.

OSSERVAZIONE 2.19. Se V è uno spazio vettoriale di dimensione n su K , e se è stata fissata una base $\{v_1, \dots, v_n\}$ di V , ad ogni endomorfismo $f : V \rightarrow V$ corrisponde una matrice quadrata $A \in M_n(K)$. Questa corrispondenza stabilisce una biiezione tra $\text{End}(V)$ e $M_n(K)$. Poiché $\text{End}(V)$, con le operazioni di somma di funzioni, di prodotto di una funzione per uno scalare e di composizione di due funzioni, è una K -algebra, lo stesso vale per l'insieme delle matrici quadrate $M_n(K)$.

PROPOSIZIONE 2.20. *L'insieme $M_n(K)$ delle matrici quadrate di ordine n a coefficienti in K , dotato delle operazioni di somma e di prodotto di matrici e dell'operazione di prodotto di una matrice per un elemento di K , è una K -algebra.*

Facciamo notare che l'elemento neutro per l'operazione di somma è la *matrice nulla*

$$\mathbf{0} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

(la quale corrisponde all'applicazione nulla $f : V \rightarrow V$, $f(v) = \mathbf{0}$, per ogni $v \in V$), mentre l'elemento neutro per l'operazione di prodotto di

matrici è la *matrice identica*, definita da

$$\mathbf{1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

(che corrisponde all'identità $\text{id} : V \rightarrow V$), cioè la matrice avente tutti i coefficienti sulla cosiddetta *diagonale principale* pari a 1, mentre tutti gli altri coefficienti sono nulli. Infatti è immediato verificare che, per ogni matrice $A \in M_n(K)$, si ha

$$\mathbf{1}A = A\mathbf{1} = A.$$

Infine notiamo che il prodotto di matrici non gode della proprietà commutativa: se A e B sono due matrici in $M_n(K)$ si ha, in generale,

$$AB \neq BA.$$

Ciò non deve stupire in quanto riflette semplicemente il fatto che la composizione di due funzioni lineari $f, g : V \rightarrow V$ non è, in generale, commutativa, cioè $f \circ g \neq g \circ f$.

Una matrice del tipo $\lambda\mathbf{1}$, cioè

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda \end{pmatrix},$$

con $\lambda \in K$, è detta *matrice scalare*. Essa corrisponde all'omomorfismo $f : V \rightarrow V$ definito da $f(v) = \lambda v$. È immediato verificare che una matrice scalare commuta con ogni altra matrice, cioè

$$(\lambda\mathbf{1})A = A(\lambda\mathbf{1}),$$

per ogni $A \in M_n(K)$.

Più in generale, una matrice del tipo

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

cioè una matrice in cui tutti i coefficienti sono nulli, tranne al più quelli sulla diagonale principale, è detta *matrice diagonale*. Si noti che, in generale, una matrice diagonale *non* commuta con un'altra matrice qualsiasi. Tuttavia le matrici diagonali commutano tra loro.

Una matrice *triangolare superiore* è una matrice in cui tutti i coefficienti che si trovano al di sotto della diagonale principale sono nulli,

cioè una matrice del tipo

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix}.$$

Analogamente si definisce una matrice *triangolare inferiore* come una matrice in cui tutti i coefficienti che si trovano al di sopra della diagonale principale sono nulli, cioè una matrice del tipo

$$\begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & a_{32} & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix}.$$

Si noti che la somma e il prodotto di due matrici triangolari superiori (rispettivamente, inferiori) è ancora una matrice dello stesso tipo.

OSSERVAZIONE 2.21. Consideriamo, a titolo di esempio, il caso di matrici quadrate di ordine 2, a coefficienti razionali. Siano, ad esempio,

$$A = \begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix}.$$

Si verifica immediatamente che il prodotto AB è la matrice nulla, tuttavia né A né B sono nulle! Ciò mostra che, in generale, nell'anello $M_n(K)$ delle matrici quadrate possono esistere degli elementi diversi da zero, con la proprietà che il loro prodotto è uguale a zero (elementi di questo tipo sono detti *divisori di zero*): non vale quindi la cosiddetta “legge di annullamento del prodotto,” secondo la quale il prodotto di due fattori è nullo se e solo se almeno uno dei due fattori è nullo.

Consideriamo ora la matrice

$$C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

La matrice C non è nulla, tuttavia si ha $C^2 = CC = \mathbf{0}$. Più in generale, si può dimostrare che nell'anello $M_n(K)$ esistono delle matrici $C \neq \mathbf{0}$ con la proprietà che $C^r = \mathbf{0}$, per qualche $r > 1$. Tali elementi sono detti *nilpotenti*.

Veniamo ora alla questione dell'esistenza degli inversi degli elementi di $M_n(K)$. Dato che l'elemento neutro per il prodotto è la matrice identica $\mathbf{1}$, l'inversa di una matrice $A \in M_n(K)$ è una matrice $B \in M_n(K)$ tale che si abbia

$$AB = BA = \mathbf{1}.$$

Naturalmente l'esistenza in $M_n(K)$ di divisori dello zero impedisce che esistano gli inversi di tutte le matrici non nulle. Infatti, se $A \in M_n(K)$ è un divisore dello zero e se B è una matrice non nulla tale che $AB = \mathbf{0}$, allora, se per assurdo esistesse la matrice A^{-1} inversa di A , si avrebbe

$$B = \mathbf{1}B = (A^{-1}A)B = A^{-1}(AB) = A^{-1}\mathbf{0} = \mathbf{0},$$

contro l'ipotesi che $B \neq \mathbf{0}$.

D'altra parte, se ripensiamo all'isomorfismo esistente tra $\text{End}(V)$ e $M_n(K)$, ove V è uno spazio vettoriale di dimensione n con una base fissata, notiamo che affermare che una matrice A sia invertibile equivale ad affermare che la corrispondente funzione lineare $f : V \rightarrow V$ sia invertibile, ma ciò è vero se e solo se f è biiettiva, cioè se e solo se f è un isomorfismo.

Ricordiamo che il sottoinsieme di $\text{End}(V)$ costituito dalle funzioni lineari invertibili (cioè dagli isomorfismi) $f : V \rightarrow V$, è stato indicato con $\text{Aut}(V)$. Il corrispondente sottoinsieme di $M_n(K)$, costituito dalle matrici associate ad elementi di $\text{Aut}(V)$, cioè dalle matrici invertibili, sarà indicato con $\text{GL}_n(K)$, o con $\text{GL}(n, K)$, e detto il *gruppo generale lineare* di ordine n a coefficienti in K . Esso è infatti un gruppo (non commutativo), rispetto all'operazione di prodotto tra matrici.

2.2. Cambiamenti di base. Abbiamo più volte fatto notare che la matrice associata ad una funzione lineare $f : V \rightarrow W$ dipende dalla scelta di una base dello spazio vettoriale V e di una base di W : cambiando scelta delle basi cambia anche la matrice associata a f . In questa sezione ci proponiamo di scoprire in che modo cambia la matrice di f se cambiamo la nostra scelta delle basi di V e W .

Siano dunque V e W due spazi vettoriali su K , di dimensioni rispettivamente n e m e sia $f : V \rightarrow W$ un'applicazione lineare. Siano $\mathbf{v} = \{v_1, \dots, v_n\}$ e $\mathbf{v}' = \{v'_1, \dots, v'_n\}$ due basi di V e siano $\mathbf{w} = \{w_1, \dots, w_m\}$ e $\mathbf{w}' = \{w'_1, \dots, w'_m\}$ due basi di W . Infine, indichiamo con $A = (a_{ij})$ la matrice di f rispetto alle basi \mathbf{v} e \mathbf{w} e con $A' = (a'_{ij})$ la matrice di f rispetto alle basi \mathbf{v}' e \mathbf{w}' . Ricordiamo che ciò significa che

$$f(v_j) = \sum_{i=1}^m a_{ij}w_i, \quad \text{e} \quad f(v'_j) = \sum_{i=1}^m a'_{ij}w'_i,$$

per ogni $j = 1, \dots, n$.

Indichiamo con $\alpha_{\mathbf{v}} : V \xrightarrow{\sim} K^n$ l'isomorfismo che associa ad ogni vettore $v \in V$ la n -upla $(\lambda_1, \dots, \lambda_n)$ delle sue coordinate rispetto alla base \mathbf{v} e con $\alpha_{\mathbf{v}'} : V \xrightarrow{\sim} K^n$ l'isomorfismo che associa ad ogni $v \in V$ la n -upla $(\lambda'_1, \dots, \lambda'_n)$ delle sue coordinate rispetto alla base \mathbf{v}' .

Indichiamo analogamente con $\beta_{\mathbf{w}} : W \xrightarrow{\sim} K^m$ l'isomorfismo che associa ad ogni vettore $w \in W$ la m -upla (μ_1, \dots, μ_m) delle sue coordinate rispetto alla base \mathbf{w} e con $\beta_{\mathbf{w}'} : W \xrightarrow{\sim} K^m$ l'isomorfismo che

associa ad ogni $w \in W$ la m -upla (μ'_1, \dots, μ'_m) delle sue coordinate rispetto alla base \mathbf{w}' .

Componendo $\alpha_{\mathbf{v}'}$ con l'inverso dell'isomorfismo $\alpha_{\mathbf{v}}$ otteniamo un isomorfismo di K^n in sé, il quale corrisponde alla moltiplicazione per una qualche matrice $P \in M_n(K)$. Indicheremo questo isomorfismo con $F_P : K^n \xrightarrow{\sim} K^n$. Si ottiene così il seguente diagramma commutativo:

$$\begin{array}{ccc} & V & \\ \alpha_{\mathbf{v}} \swarrow & & \searrow \alpha_{\mathbf{v}'} \\ K^n & \xrightarrow{F_P} & K^n \end{array}$$

Analogamente, componendo $\beta_{\mathbf{w}'}$ con l'inverso dell'isomorfismo $\beta_{\mathbf{w}}$ otteniamo un isomorfismo di K^m in sé, il quale corrisponde alla moltiplicazione per una qualche matrice $Q \in M_m(K)$. Indicheremo questo isomorfismo con $F_Q : K^m \xrightarrow{\sim} K^m$. Si ottiene così il seguente diagramma commutativo:

$$\begin{array}{ccc} & W & \\ \beta_{\mathbf{w}} \swarrow & & \searrow \beta_{\mathbf{w}'} \\ K^m & \xrightarrow{F_Q} & K^m \end{array}$$

Facciamo notare che le due matrici P e Q sono invertibili, dato che le corrispondenti applicazioni lineari F_P e F_Q sono degli isomorfismi.

Vediamo ora di ottenere una descrizione più esplicita delle matrici P e Q . Cominciamo dalla matrice P , la quale corrisponde all'isomorfismo

$$F_P : K^n \xrightarrow{\sim} K^n.$$

Abbiamo già osservato che le colonne di P sono date dalle immagini dei vettori della base canonica di K^n . Sia $e_j = {}^t(0, \dots, 0, 1, 0, \dots, 0)$ il j -esimo vettore della base canonica di K^n (tutte le coordinate sono nulle tranne la j -esima che è uguale a 1). Tramite l'isomorfismo $\alpha_{\mathbf{v}}$, il vettore $e_j \in K^n$ corrisponde al j -esimo vettore v_j della base \mathbf{v} di V . Si ha quindi

$$F_P(e_j) = \alpha_{\mathbf{v}'}(\alpha_{\mathbf{v}}^{-1}(e_j)) = \alpha_{\mathbf{v}'}(v_j),$$

dove ricordiamo che $\alpha_{\mathbf{v}'}(v_j) \in K^n$ è il vettore costituito dalle coordinate del vettore v_j calcolate rispetto alla base \mathbf{v}' ; questo vettore è la j -esima colonna di P .

In conclusione, possiamo affermare che le *colonne* della matrice P non sono altro che le coordinate dei vettori v_1, \dots, v_n della base \mathbf{v} di V calcolate rispetto alla seconda base \mathbf{v}' . Con un analogo ragionamento, scambiando i ruoli delle due basi, si potrebbe dimostrare che le colonne della matrice inversa P^{-1} sono precisamente le coordinate dei vettori v'_1, \dots, v'_n della base \mathbf{v}' di V calcolate rispetto alla prima base \mathbf{v} .

In modo del tutto analogo si dimostra che la j -esima colonna della matrice Q è costituita dal vettore delle coordinate del j -esimo vettore w_j della base \mathbf{w} calcolate rispetto alla base \mathbf{w}' . In altre parole, la matrice Q è la matrice le cui *colonne* sono date dalle coordinate dei vettori w_1, \dots, w_m della base \mathbf{w} di W calcolate rispetto alla seconda base \mathbf{w}' . Analogamente si dimostra che le colonne della matrice inversa Q^{-1} sono le coordinate dei vettori w'_1, \dots, w'_m della base \mathbf{w}' di W calcolate rispetto alla prima base \mathbf{w} .

Ricordando il risultato enunciato nella Proposizione 2.13, possiamo riassumere quanto detto finora nel seguente diagramma commutativo

$$\begin{array}{ccc}
 K^n & \xrightarrow{F_A} & K^m \\
 \downarrow F_P \wr & \swarrow \alpha_{\mathbf{v}} & \nearrow \beta_{\mathbf{w}} \\
 & V \xrightarrow{f} W & \\
 \downarrow F_P \wr & \swarrow \alpha_{\mathbf{v}'} & \nearrow \beta_{\mathbf{w}'} \\
 K^n & \xrightarrow{F_{A'}} & K^m
 \end{array}$$

ove F_A e $F_{A'}$ sono le applicazioni lineari date dalla moltiplicazione per A e per A' , rispettivamente.

Dalla commutatività di questo diagramma si deduce che

$$F_{A'} \circ F_P = F_Q \circ F_A,$$

che equivale alla seguente uguaglianza tra matrici

$$A'P = QA.$$

Da ciò segue che

$$(2.5) \quad A' = QAP^{-1} \quad \text{e} \quad A = Q^{-1}A'P.$$

Queste due espressioni equivalenti permettono di determinare la matrice A' di un'applicazione lineare $f : V \rightarrow W$ rispetto alle basi \mathbf{v}' di V e \mathbf{w}' di W quando è nota la matrice A di f rispetto a delle basi \mathbf{v} e \mathbf{w} e quando sono note le matrici di cambiamento di base P e Q .

Nel caso particolare in cui $W = V$, cioè quando f è un endomorfismo di uno spazio vettoriale V , il diagramma commutativo precedente si riduce al seguente

$$\begin{array}{ccc}
 K^n & \xrightarrow{F_A} & K^n \\
 \downarrow F_P \wr & \swarrow \alpha_{\mathbf{v}} & \nearrow \alpha_{\mathbf{v}} \\
 & V \xrightarrow{f} V & \\
 \downarrow F_P \wr & \swarrow \alpha_{\mathbf{v}'} & \nearrow \alpha_{\mathbf{v}'} \\
 K^n & \xrightarrow{F_{A'}} & K^n
 \end{array}$$

e le uguaglianze (2.5) diventano

$$(2.6) \quad A' = PAP^{-1} \quad \text{e} \quad A = P^{-1}A'P.$$

Diamo ora la seguente definizione:

DEFINIZIONE 2.22. Due matrici quadrate A e A' di ordine n a coefficienti in K si dicono *simili* se esiste una matrice invertibile $P \in M_n(K)$ (cioè $P \in \text{GL}_n(K)$) tale che

$$A' = PAP^{-1}$$

o, equivalentemente,

$$A = P^{-1}A'P.$$

Da quanto sopra detto si deduce il seguente risultato:

COROLLARIO 2.23. Due matrici $A, A' \in M_n(K)$ rappresentano lo stesso endomorfismo f di uno spazio vettoriale V di dimensione n su K , rispetto a basi diverse, se e solo se sono simili.

OSSERVAZIONE 2.24. Si noti che la relazione di similitudine è una relazione di equivalenza sull'insieme $M_n(K)$ delle matrici quadrate di ordine n a coefficienti in K .