

Appunti per gli studenti del corso di Geometria

Corso di Laurea in Fisica

A.A. 2025/26

A. Lotta

1. NOZIONI DI BASE

La geometria analitica permette di trattare questioni geometriche utilizzando il linguaggio algebrico. Così \mathbb{R} fornisce un modello universale di “retta euclidea”, mentre $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ il modello categorico di “piano euclideo”. In ultima analisi, ciò che tale identificazione permette è la manipolazione e lo studio degli oggetti geometrici mediante le operazioni fondamentali tra numeri reali: somma, prodotto, differenza, passaggio al reciproco. In tale procedimento sono di basilare importanza le proprietà formali di queste operazioni. Su di esse si basa la nozione generale di *campo*, che sarà discussa in questo paragrafo.

Consideriamo un insieme X su cui sia definita un’**operazione interna** $*$, ovvero una legge che associa univocamente ad ogni coppia ordinata (x, y) di elementi di X , un ben preciso elemento dello stesso insieme, denotato con $x * y$. In tal caso diremo che $(X, *)$ è una **struttura algebrica**.

A priori, quindi, l’ordine in cui si considerano gli oggetti x e y è importante ai fini di determinare il risultato dell’operazione $*$ applicata ad essi. In altri termini, gli oggetti $x * y$ e $y * x$ possono differire.

Se $*$ è un’operazione su X , la coppia $(X, *)$ prende il nome di **struttura algebrica**.

Osservazione 1.1. Osserviamo che un’operazione interna $*$ sull’insieme X altro non è che una funzione (applicazione) $*$: $X \times X \rightarrow X$, il cui dominio è il prodotto cartesiano $X \times X = \{(x, y) : x \in X, y \in Y\}$ e il cui insieme di arrivo è lo stesso insieme X .

Più in generale, si possono considerare strutture algebriche $(X, *_1, \dots, *_k)$ dove $*_1, \dots, *_k$ sono $k \geq 1$ operazioni diverse su X .

ESEMPIO 1.2. Sono operazioni interne la somma $+$ ed il prodotto \cdot standard sugli insiemi numerici \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} . Quindi, ad esempio, sono strutture algebriche $(\mathbb{Z}, +)$, (\mathbb{Q}, \cdot) , ma anche $(\mathbb{Z}, +, \cdot)$ oppure $(\mathbb{R}, +, \cdot)$ (strutture con due operazioni).

Fissiamo ora un po' di terminologia di uso corrente. Si dice che l'operazione $*$ sull'insieme X gode della proprietà **commutativa** se:

$$\forall x, y \in X \quad x * y = y * x.$$

L'operazione $*$ è detta **associativa** se per ogni $x, y, z \in X$ risulta:

$$x * (y * z) = (x * y) * z.$$

In questo caso, è possibile scrivere, senza ambiguità:

$$x * y * z.$$

Diremo che struttura algebrica $(X, *)$ ammette **elemento neutro**, se esiste un elemento $e \in X$ tale che:

$$x * e = x = e * x$$

per ogni $x \in X$.

Un tale oggetto, se esiste, è sempre univocamente determinato. Infatti, ammettendo che e ed e' siano entrambi elementi neutri, risulta necessariamente:

$$e = e * e' = e'.$$

La prima uguaglianza è giustificata dal fatto che e' è elemento neutro, la seconda dal fatto che e gode della stessa proprietà.

I più familiari esempi di elementi neutri sono il numero 0 nel caso degli insiemi numerici $(\mathbb{N}, +)$, $(\mathbb{Q}, +)$, ecc. ed il numero 1, laddove si consideri la moltiplicazione invece della somma.

ESEMPIO 1.3. Dato un insieme A , possiamo considerare sull'insieme delle parti (cioè l'insieme di tutti i sottoinsiemi) $\mathcal{P}(A)$ di A le operazioni fondamentali di intersezione e unione che danno luogo a due differenti strutture algebriche: $(\mathcal{P}(A), \cap)$ e $(\mathcal{P}(A), \cup)$ e in entrambi i casi sussiste la proprietà associativa. Si noti che la prima di queste strutture ammette l'intero insieme A come elemento neutro, mentre per la seconda tale ruolo è svolto dall'insieme vuoto \emptyset .

ESEMPIO 1.4. Dato un insieme A , consideriamo l'insieme A^A di tutte le funzioni (applicazioni) da A in A . Questo insieme è dotato della fondamentale operazione di composizione

$$(f, g) \mapsto f \circ g.$$

Ricordiamo che $f \circ g : A \rightarrow A$ è la funzione definita ponendo

$$(f \circ g)(x) := f(g(x))$$

per ogni $x \in A$.

L'operazione di composizione \circ tra funzioni è *sempre associativa*, ma *non* è (di norma) commutativa.

La funzione identica $Id_A : A \rightarrow A$ (definita com'è noto da $Id_A(x) := x$ per ogni $x \in A$), è l'elemento neutro di (A^A, \circ) , avendosi infatti, per ogni funzione $f : A \rightarrow A$, che

$$f \circ Id_A = f = Id_A \circ f.$$

In presenza di un elemento neutro e per una struttura algebrica $(X, *)$, un elemento $x \in X$ è detto **invertibile** se in corrispondenza di esso esiste un altro $x' \in X$, detto *inverso di x* , per cui si abbia:

$$x * x' = e = x' * x.$$

Si dice anche che x **ammette un inverso** in X .

Considerato ad esempio l'insieme dei numeri reali, ogni numero $x \neq 0$ è un elemento invertibile di (\mathbb{R}, \cdot) , con inverso $\frac{1}{x}$. Invece ogni numero reale x è un elemento invertibile di $(\mathbb{R}, +)$, con inverso $-x$.

ESEMPIO 1.5. Consideriamo ancora un insieme non vuoto A e la struttura algebrica (A^A, \circ) . Data una funzione $f : A \rightarrow A$, essa è un elemento invertibile di (A^A, \circ) se e solo se esiste una funzione $g : A \rightarrow A$ tale che:

$$f \circ g = Id_A, g \circ f = Id_A.$$

Questo significa che per ogni $x \in A$ deve aversi

$$g(f(x)) = x$$

e anche:

$$f(g(y)) = y,$$

sempre per ogni $y \in A$.

Allo studente è già noto che condizione necessaria e sufficiente affinché ciò sia possibile è che f sia una funzione *bigettiva*, ovvero sia *ingettiva* che *surgettiva*. La funzione $g : A \rightarrow A$ è la funzione inversa $g = f^{-1}$ della bigezione f , che associa ad ogni $y \in A$ l'unico elemento x dello stesso insieme, tale che $f(x) = y$.

In tal caso quindi abbiamo a disposizione una caratterizzazione completa degli elementi invertibili della struttura algebrica (A^A, \circ) in esame.

Teorema 1.6. *Sia $(X, *)$ un struttura algebrica, dotata di elemento neutro e , la cui operazione $*$ è associativa. Se $x \in X$ è un elemento invertibile, allora l'inverso x' di x è univocamente determinato.*

DIMOSTRAZIONE: Supponiamo che x' e x'' siano entrambi inversi di x . Allora in particolare abbiamo

$$x * x' = e.$$

Applicando l'operazione $*$, "componendo" ambo i membri a sinistra con x'' si ottiene:

$$x'' * (x * x') = x'' * e$$

ovvero

$$x'' * (x * x') = x''$$

che si può riscrivere, stante la proprietà associativa:

$$(x'' * x) * x' = x''.$$

D'altra parte, per definizione di inverso, sappiamo anche che $x'' * x = e$ e quindi l'ultima uguaglianza si riscrive:

$$e * x' = x''$$

da cui

$$x' = x''.$$

□

Introduciamo ora una delle più importanti tipologie di struttura algebrica, rilevante non solo nell'ambito della matematica pura, ma anche in molte altre discipline.

Definizione 1.7. Si chiama **gruppo** ogni struttura algebrica $(G, *)$ soddisfacente le seguenti condizioni:

- 1) L'operazione $*$ è associativa.
- 2) $(G, *)$ ammette elemento neutro.
- 3) Tutti gli elementi di G sono invertibili.

Solitamente l'elemento neutro di un gruppo G si denota con e , mentre l'inverso di un elemento x si denota con x^{-1} , salvo diversa convenzione.

Definizione 1.8. Un gruppo $(G, *)$ si dice **abeliano** se l'operazione $*$ è commutativa.

Sono gruppi:

- $(X, +)$ dove X è uno degli insiemi numerici $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
- $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot)$ e dove $*$ indica l'insieme numerico in questione privato di 0.
Tutti questi gruppi sono abeliani.

Invece *non* sono gruppi:

- $(\mathbb{N}, +), (\mathbb{N}, \cdot)$ e (\mathbb{Z}, \cdot) .

Si osservi che l'operazione di moltiplicazione è effettivamente un'operazione interna su \mathbb{R}^* : il prodotto $a \cdot b$ di due numeri reali diversi da zero, è anch'esso diverso da zero (legge di annullamento del prodotto). Pertanto possiamo considerare l'operazione $\cdot : \mathbb{R}^* \times \mathbb{R}^* \rightarrow \mathbb{R}^*$ e la struttura algebrica (\mathbb{R}^*, \cdot) su tale insieme. Lo stesso discorso vale per \mathbb{Q}^* .

ESEMPIO 1.9. Dato un insieme qualsiasi non vuoto A , l'insieme $Sym(A)$ di tutte le *bigezioni* $f : A \rightarrow A$ è un gruppo rispetto all'operazione \circ di composizione. Si tratta di un esempio significativo di gruppo, in cui l'operazione interna *non* gode della familiare proprietà commutativa, tipica dei gruppi costruiti con gli insiemi numerici. Esso prende il nome di *gruppo delle permutazioni* di A . Ad esempio, se $A = \{1, \dots, n\}$ è un insieme finito, si tratta del gruppo delle *permutazioni su n oggetti*, un importante gruppo finito studiato ad es. nell'ambito del calcolo combinatorio.

Con riferimento all'esempio precedente, si osservi che, in analogia con quanto osservato per il gruppo (\mathbb{R}^*, \cdot) , l'operazione \circ si può considerare come operazione interna su $Sym(A)$, grazie al fatto che la composizione $f \circ g$ di due bigezioni è ancora una bigezione (la composizione di due applicazioni ingettive è ingettiva e la composizione di due funzioni surgettive è pure surgettiva). Tale operazione risulta indotta dall'operazione di composizione della struttura algebrica più grande (A^A, \circ) . La definizione seguente generalizza questo tipo di situazione.

Definizione 1.10. Data una struttura algebrica $(X, *)$, un sottoinsieme $E \subset X$ è detto **chiuso** o **stabile** (rispetto all'operazione $*$) se per ogni $x, y \in E$, si ha che

$$x * y \in E.$$

Si osservi che ogni sottoinsieme stabile E di $(X, *)$ eredita in modo naturale per restrizione da X l'operazione interna $*$, che opera allo stesso modo, ma solo su coppie di elementi di E , producendo sempre elementi di E . Evidentemente, se $*$ è associativa (risp. commutativa), tale è questa operazione indotta.

Dunque l'insieme $Sym(A)$ di tutte le bigezioni $F : A \rightarrow A$ di un insieme su sè stesso è stabile per l'operazione di composizione \circ su A^A , ovvero è un sottoinsieme stabile della struttura algebrica (A^A, \circ) .

Come altro esempio, abbiamo che $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$ è un insieme stabile di $(\mathbb{R}, +)$, mentre $\{1, 0, -1\}$ non lo è.

ESEMPIO 1.11. 1) L'insieme costituito da tutte e sole le rotazioni del piano Euclideo E intorno ad un punto fissato O è un gruppo, rispetto all'operazione di composizione di applicazioni.

2) Data una retta r del piano euclideo E , detta $\sigma : E \rightarrow E$ la simmetria assiale rispetto a r , allora $G = \{Id_E, \sigma\}$ costituisce un gruppo, costituito da soli due elementi. Ricordiamo che per ogni punto P , la sua immagine $\sigma(P)$ è il punto simmetrico di P rispetto a r .

Basta notare che σ è una bigezione che ammette se stessa come inversa: infatti abbiamo

$$\sigma \circ \sigma = Id_A$$

perchè denotando, per ogni punto P , con P' il simmetrico di esso rispetto alla retta, allora $(P')' = P$ (il simmetrico del simmetrico è il punto stesso).

Si osservi che un altro esempio di gruppo costituito da due soli elementi è $(\{0, 1\}, +)$, la cui operazione è definita ponendo:

$$0 + 0 := 0, \quad 0 + 1 := 1 = 1 + 0, \quad 1 + 1 := 0.$$

Tale gruppo si denota con \mathbb{Z}_2 (gruppo additivo dell'aritmetica modulo 2). Il ruolo che svolge la funzione identica nell'esempio precedente $G = \{Id_E, \sigma\}$ è qui svolto da 0, mentre la simmetria assiale è rimpiazzata da 1. Evidentemente i due gruppi sono identificabili (il termine preciso è isomorfi). Anzi, qualsiasi gruppo $(G, *)$ costituito da esattamente due elementi distinti ha lo stesso tipo di struttura: detto x l'elemento diverso dall'elemento neutro, x deve necessariamente ammettere se stesso come inverso.

3) Si chiama *gruppo banale* ogni struttura algebrica del tipo $(G = \{e\}, *)$, costituita da un solo elemento, la cui operazione è definita semplicemente ponendo

$$e * e = e.$$

Notazione e convenzioni riguardanti i gruppi:

Dato un gruppo $(G, +)$ la cui operazione è denotata con notazione **additiva** $+$, si usano di solito le seguenti **convenzioni**:

-L'elemento neutro si denota preferibilmente con 0.

-L'inverso di $a \in G$ si denota con $-a$ e si chiama **l'opposto di a** .

Inoltre, dati due oggetti qualsiasi x e y , in tal caso si scriverà:

$$x - y$$

in luogo di

$$x + (-y).$$

Dato un gruppo (G, \cdot) la cui operazione è denotata mediante notazione **moltiplicativa** \cdot , si usano le seguenti convenzioni:

-L'elemento neutro si denota preferibilmente con 1 (talvolta è utilizzato anche il simbolo e).

-L'inverso di $a \in G$ si denota con a^{-1} .

Osservazione 1.12. Osserviamo che, dato un gruppo abeliano $(G, +)$ le convenzioni precedenti sulla notazione additiva permettono di effettuare operazioni nel gruppo in modo naturale, operando con le usuali regole del calcolo letterale. Ad es. se a, b, c sono elementi qualsiasi, allora si ha

$$a + b = c$$

se e solo se

$$a - c = -b.$$

Enunciamo ora una proprietà basilare dei gruppi, nota come *legge di cancellazione*.

Teorema 1.13. *Siano a, b, c elementi di un gruppo $(G, *)$ e si assuma che*

$$a * c = b * c$$

oppure che

$$c * a = c * b.$$

Allora $a = b$.

DIMOSTRAZIONE: Denotato con e l'elemento neutro di G , assumendo ad esempio che

$$a * c = b * c,$$

allora componendo ambo i membri con l'inverso c^{-1} di c segue:

$$(a * c) * c^{-1} = (b * c) * c^{-1}$$

da cui

$$a * (c * c^{-1}) = b * (c * c^{-1})$$

ovvero

$$a * e = b * e$$

e quindi in definitiva

$$a = b.$$

□

Proposizione 1.14. *Dato un gruppo $(G, *)$, per ogni a, b in G l'inverso di $a * b$ è dato da:*

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

DIMOSTRAZIONE: Tenendo presente che l'inverso di $a * b$ è univocamente determinato, basta fare la seguente verifica:

$$(a * b) * (b^{-1} * a^{-1}) = e = (b^{-1} * a^{-1}) * (a * b).$$

Infatti, sfruttando la proprietà associativa, abbiamo:

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = (a * e) * a^{-1} = a * a^{-1} = e.$$

In modo completamente analogo si controlla la validità della seconda uguaglianza richiesta. \square

ESEMPIO 1.15. Discutiamo ora un esempio importante di gruppo abeliano, che incontreremo e generalizzeremo presto nel contesto degli spazi vettoriali; sul prodotto cartesiano $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ si definisce un'operazione naturale di somma $+$ ponendo:

$$(x, y) + (x', y') := (x + x', y + y'),$$

per ogni (x, y) e (x', y') in \mathbb{R}^2 .

Risulta che $(\mathbb{R}^2, +)$ è un gruppo abeliano. L'elemento neutro è la coppia $(0, 0)$; per ogni $A = (x, y)$, esiste l'elemento inverso dato dalla coppia $(-x, -y)$. La verifica dell'associatività dell'operazione $+$ è semplice, ed è basata sulla proprietà associativa dell'addizione in \mathbb{R} ; si ha infatti:

$$[(x, y) + (x', y')] + (x'', y'') = (x + x', y + y') + (x'', y'') = (x + x' + x'', y + y' + y'')$$

e d'altra parte

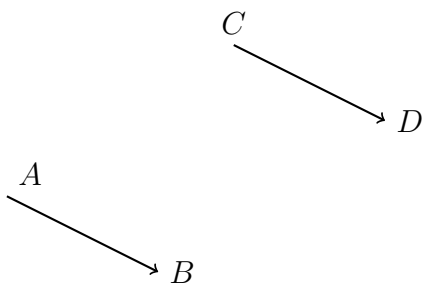
$$(x, y) + [(x', y') + (x'', y'')] = (x, y) + (x' + x'', y' + y'') = (x + x' + x'', y + y' + y'').$$

È altresì immediato constatare che $+$ gode della proprietà commutativa.

A questa operazione si può dare un significato geometrico, se interpretiamo ogni coppia (x, y) in \mathbb{R}^2 come un punto di un piano Cartesiano, $P(x, y)$ di ascissa x e ordinata y in un fissato sistema di riferimento.

Ricordiamo che nel piano della geometria elementare vi è una nozione puramente sintetica di vettore: dati due punti distinti A e B , il *vettore applicato* \overrightarrow{AB} è il segmento orientato AB . Nel caso generale $A \neq B$ esso ha tre caratteristiche: la *direzione*, che è quella individuata dalla retta per A e B , il *verso*, che è quello sulla stessa retta secondo cui A precede B , e la *lunghezza*, che è la lunghezza del segmento stesso (fissata una unità di misura) che è un numero strettamente positivo. Se invece $A = B$ tale vettore è detto *vettore nullo* ed ha lunghezza 0, mentre non gli si attribuisce nè direzione, nè verso. In ogni caso il punto A è il *punto di applicazione* del vettore \overrightarrow{AB} , mentre il punto B si dice punto di arrivo o punto finale dello stesso.

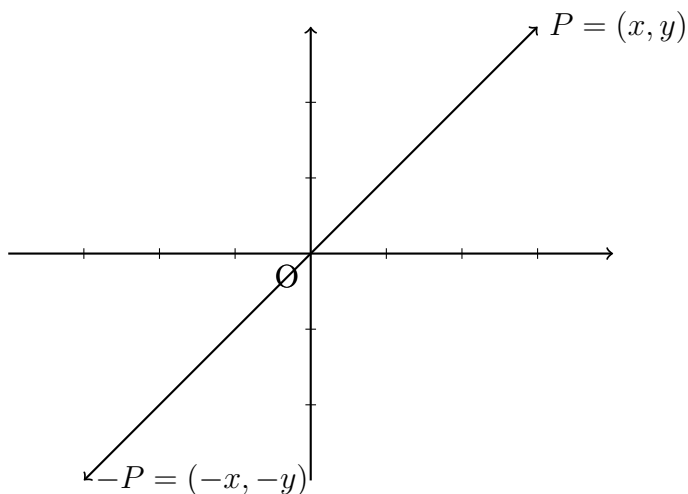
Dato un vettore \overrightarrow{AB} e un punto C , esiste un unico vettore \overrightarrow{CD} che ha le stesse caratteristiche di \overrightarrow{AB} (direzione, lunghezza e verso): esso si dice *equipollente ad* \overrightarrow{AB} . I vettori equipollenti \overrightarrow{AB} e \overrightarrow{CD} sono due rappresentanti dello stesso vettore *libero*.



La somma $\vec{AB} + \vec{AC}$ di due vettori \vec{AB} e \vec{AC} applicati nello stesso punto A , si definisce come il vettore \vec{AD} dove D è il punto finale del vettore applicato in B equipollente ad \vec{AC} .

Questa regola prende il nome di *regola del parallelogramma* in quanto, nel caso generico in cui A, B e C non sono allineati, detto D il punto finale di $\vec{AB} + \vec{AC}$, allora A, C, D e B sono i vertici di un parallelogramma.

Tenendo presente ciò possiamo dare un significato geometrico all'operazione di somma in \mathbb{R}^2 . Osserviamo innanzitutto che l'elemento neutro $(0, 0)$ corrisponde all'origine O del nostro riferimento. Inoltre, l'opposto $-P$ di un punto coincide con il simmetrico di P rispetto a O .



Proposizione 1.16. 1) Siano A, B di \mathbb{R}^2 e sia C un altro punto. Allora l'unico punto D tale che

$$\vec{AB} \text{ è equipollente a } \vec{CD}$$

è il punto

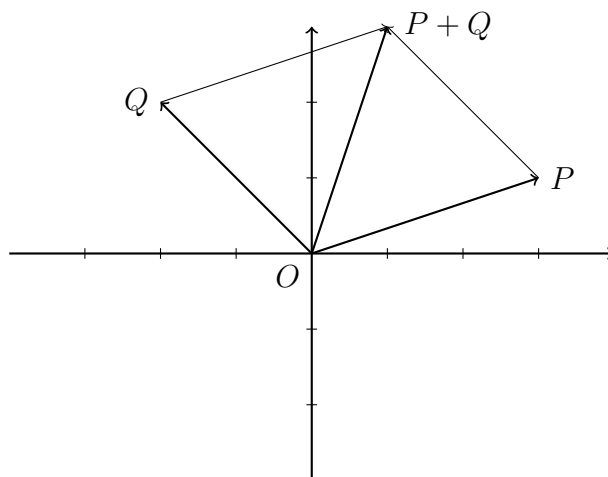
$$D = C + B - A.$$

2) Dati i punti A, B, C, D si ha:

$$\vec{AB} \text{ è equipollente a } \vec{CD} \iff B - A = D - C.$$

3) Dati i punti P e Q , la somma $P+Q$ coincide con il secondo estremo del vettore somma $\overrightarrow{OP} + \overrightarrow{OQ}$, effettuata secondo la regola del parallelogramma, ovvero:

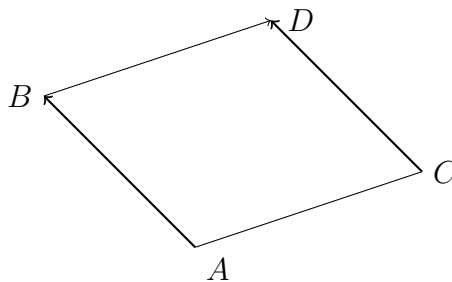
$$\overrightarrow{OP} + \overrightarrow{OQ} = \overrightarrow{O(P+Q)}.$$



Si osservi che in questa uguaglianza, la somma $P+Q$ è quella effettuata nel gruppo $(\mathbb{R}^2, +)$ che abbiamo introdotto, mentre la somma al primo membro è quella tra vettori applicati.

Notiamo anche che la proprietà 2) suggerisce che ogni differenza $B-A$ tra punti nel nostro gruppo si può interpretare come un vettore libero, di cui un rappresentante è il vettore applicato \overrightarrow{AB} .

DIMOSTRAZIONE: Per ogni coppia di punti (A, B) distinti, denotiamo con $r_{A,B}$ la retta passante per questi punti. Nel provare 1), possiamo supporre che $A \neq B$, perchè nel caso $A = B$ il risultato è evidente, perchè in tal caso necessariamente $D = C$. Consideriamo dapprima il caso generico in cui C non è allineato con A e B . Dato il vettore \overrightarrow{AB} , sappiamo che il punto D in questione è univocamente determinato dalla condizione che A, B, D, C , siano i vertici di un parallelogramma:

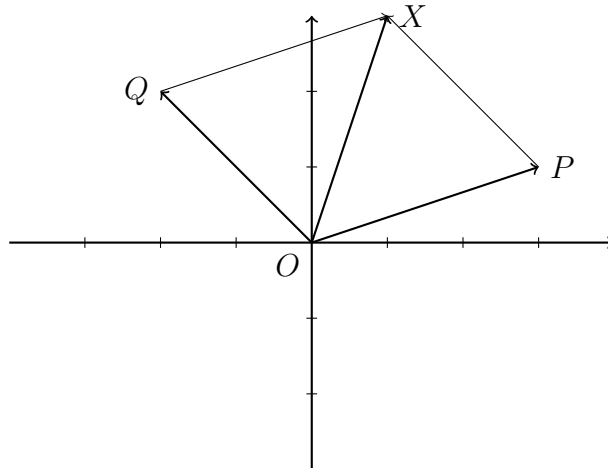


Affermiamo che tale punto è $X := C + B - A$. Per far ciò, posto $A(a_1, a_2)$, $B(b_1, b_2)$ e $C(c_1, c_2)$, basta controllare che la retta $r_{A,B}$ è parallela alla retta $r_{C,X}$ e che la retta $r_{B,X}$ è parallela alla retta $r_{A,C}$. Infatti, abbiamo che il punto X ha coordinate $(b_1 + c_1 - a_1, b_2 + c_2 - a_2)$ e un rapido confronto dei coefficienti angolari delle rette in questione ci dà conferma in merito. Ad esempio, tranne che nel caso in cui $a_1 = b_1$, il coefficiente angolare di $r_{A,B}$ è $m = \frac{b_2 - a_2}{b_1 - a_1}$; mentre quello della retta $r_{C,X}$ è $m' = \frac{b_2 + c_2 - a_2 - c_2}{b_1 + c_1 - a_1 - c_1} = m$. Nel caso particolare $a_1 = b_1$, la retta $r_{A,B}$ è comunque parallela a $r_{C,X}$ perchè entrambe sono parallele all'asse delle ordinate. La verifica per le rette $r_{B,X}$ e $r_{A,C}$ è analoga.

Nel caso in cui A, B e C siano allineati, la verifica che $D = X$ va fatta direttamente con la definizione di equipollenza: si tratta di controllare che il segmento AB sia congruente a CX e che C preceda X nel verso sulla retta $r_{A,B}$ secondo cui A precede B . Quest'ultima verifica consiste nel confrontare le ascisse dei punti (o, in caso siano uguali, le ordinate). Ad esempio, supponiamo che $a_1 < b_1$; bisogna controllare che anche l'ascissa di C sia minore dell'ascissa di X . Infatti, si ha: $c_1 < c_1 + (b_1 - a_1)$. La prima verifica si lascia al lettore, e si fa agevolmente calcolando le distanze $d(A, B)$ e $d(C, X)$. Dunque, in ogni caso resta provato che $D = C + B - A$.

La 2) consegue come immediata conseguenza: infatti, stante la 1) abbiamo che \overrightarrow{AB} è equipollente a \overrightarrow{CD} se e solo se e solo se $D = C + B - A$ e tale uguaglianza, operando nel gruppo $(\mathbb{R}^2, +)$, si può riscrivere come $B - A = D - C$.

La 3) è un caso particolare, in quanto effettuando la somma dei vettori \overrightarrow{OP} e \overrightarrow{OQ} con la regola del parallelogramma si ottiene un vettore \overrightarrow{OX} dove X è tale che \overrightarrow{OQ} e \overrightarrow{PX} sono equipollenti:



Pertanto, applicando 1) il punto X in questione è $X = P + (Q - O) = P + Q$. \square

Possiamo ora introdurre il concetto di campo, i cui esempi più noti sono il campo dei numeri razionali \mathbb{Q} , quello dei numeri reali \mathbb{R} e il campo dei numeri complessi \mathbb{C} .

Definizione 1.17. Si chiama **campo** ogni struttura algebrica $(K, +, \cdot)$ le cui operazioni soddisfano i seguenti requisiti:

- a) $(K, +)$ è un gruppo abeliano, il cui elemento neutro si denota con 0.
- b) L'operazione di moltiplicazione \cdot è associativa, commutativa e (K, \cdot) ammette l'elemento neutro, denotato con 1, tale che $1 \neq 0$.
- c) Ogni $x \in K$, tale che $x \neq 0$ ammette un inverso rispetto al prodotto, denotato con x^{-1} .
- d) Sussiste la *proprietà distributiva* del prodotto rispetto alla somma:

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

per ogni $x, y, z \in K$.

Proposizione 1.18. Sia $(K, +, \cdot)$ un campo. Sussistono le seguenti proprietà:

1) Per ogni $a \in K$ si ha: $0 \cdot x = 0 = x \cdot 0$.

2) Vale la legge di annullamento del prodotto:

$$a \cdot b = 0 \Rightarrow a = 0 \text{ oppure } b = 0.$$

3) L'insieme $K^* = K - \{0\}$ è stabile rispetto all'operazione di moltiplicazione, e (K^*, \cdot) è un gruppo abeliano.

DIMOSTRAZIONE: 1) Abbiamo, utilizzando la prima delle proprietà distributiva (assioma d) della definizione di campo):

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0,$$

che porta a $x \cdot 0 = 0$ in forza della legge di cancellazione nel gruppo $(K, +)$.

2) Siano $a, b \in K$ tali che

$$a \cdot b = 0.$$

Vogliamo provare che $a = 0$ oppure $b = 0$. Se $a = 0$, non c'è nulla da provare; assumiamo quindi $a \neq 0$; in tal caso l'assioma c) garantisce che a ammette l'inverso a^{-1} rispetto alla moltiplicazione; utilizzando tale inverso si ottiene:

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0,$$

da cui, stante la 1)

$$a^{-1} \cdot (a \cdot b) = 0,$$

e quindi, in forza della proprietà associativa del prodotto:

$$(a^{-1} \cdot a) \cdot b = 0,$$

ovvero

$$1 \cdot b = 0$$

e resta provato che $b = 0$.

3) La legge di annullamento del prodotto si può reinterpretare esattamente come la circostanza che il prodotto di due oggetti a, b entrambi diversi da zero, è anch'esso diverso da zero:

$$a \neq 0 \text{ e } b \neq 0 \Rightarrow a \cdot b \neq 0.$$

Ciò significa proprio che K^* è stabile rispetto al prodotto. Ciò detto, in forza degli assiomi b) e c), è immediato riconoscere che (K^*, \cdot) è un gruppo abeliano. Infatti, l'operazione \cdot ristretta a K^* è associativa e commutativa, e ammette ancora 1 come elemento neutro: si noti infatti che $1 \in K^*$ in quanto l'assioma 2) garantisce che $1 \neq 0$. Infine, osserviamo che dato $x \in K^*$, allora anche il suo inverso x^{-1} previsto nell'assioma b) appartiene a K^* , perchè se fosse $x^{-1} = 0$, dalla relazione

$$x \cdot x^{-1} = 1$$

seguirebbe

$$x \cdot 0 = 1$$

ovvero, in forza di 1)

$$0 = 1$$

il che viola l'assioma b). Pertanto ogni $x \in K^*$ risulta invertibile (K^*, \cdot) con lo stesso x^{-1} come inverso, e con ciò resta verificato che questa struttura algebrica è un gruppo abeliano. \square

Coerentemente con le convenzioni generali sui gruppi, dato un campo $(K, +, \cdot)$ l'opposto di un elemento a , rispetto al gruppo $(K, +)$, si denoterà sempre con $-a$. Se $a \neq 0$, il suo inverso rispetto alla moltiplicazione, ovvero il suo inverso in (K^*, \cdot) , si denoterà sempre con a^{-1} . Utilizzando la Prop. 1.14, sappiamo che dati a, b elementi qualsiasi diversi da 0, si ha:

$$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1} = b^{-1} \cdot a^{-1}.$$

Un'altra proprietà naturale che si deduce dagli assiomi di campo, e che lega tra loro l'addizione e la moltiplicazione, è la seguente.

Proposizione 1.19. *Se $(K, +, \cdot)$ è un campo, allora per ogni $x \in K$ risulta:*

$$-x = (-1) \cdot x.$$

DIMOSTRAZIONE: Stante l'unicità dell'opposto di x nel gruppo $(K, +)$, e la commutatività di $+$, basta verificare che

$$(-1) \cdot x + x = 0.$$

Ma ciò è conseguenza della proprietà distributiva e della proposizione precedente:

$$(-1) \cdot x + x = (-1) \cdot x + 1 \cdot x = (-1 + 1) \cdot x = 0 \cdot x = 0.$$

\square

Osservazione 1.20. Nei campi numerici, dato un numero $a \neq 0$, siamo abituati a scrivere

$$\frac{1}{a}$$

per denotare l'inverso a^{-1} di a . Questa notazione è ammissibile anche in un campo astratto K . Inoltre, dati $a, b \in K$ con $b \neq 0$ si può anche scrivere $\frac{a}{b}$ in luogo di $a \cdot b^{-1}$, ovvero in luogo di $a \cdot \frac{1}{b}$. Con questa notazione, dati a, b, c, d con $c \neq 0$ e $d \neq 0$, vale:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d},$$

dove il secondo membro ha senso in forza della legge di annullamento del prodotto. Si lascia la verifica come esercizio.

2. SPAZI VETTORIALI

L'algebra lineare è la disciplina matematica il cui oggetto principale di studio è la teoria degli *spazi vettoriali* e delle *applicazioni lineari*. Gli spazi vettoriali sono oggetti di natura algebrica su cui non solo si può fondare l'ordinaria geometria elementare e le sue generalizzazioni, ma sono strutture basilari utilizzate in tutti i campi della Matematica, della Fisica e numerose altre discipline. Uno dei temi più importanti dell'algebra lineare è lo studio dei sistemi di equazioni lineari.

Sia \mathbb{K} un campo. Denoteremo, in accordo con quanto discusso nel paragrafo precedente, con 0 e 1 gli elementi neutri di \mathbb{K} rispettivamente per la somma ed il prodotto, che denotiamo sempre con $+$ e \cdot . Se $x \in \mathbb{K}$, allora $-x$ denoterà l'opposto di x (rispetto alla somma) mentre se $x \in \mathbb{K}^*$, usiamo x^{-1} per denotare l'inverso di x (rispetto al prodotto).

In precedenza abbiamo introdotto il concetto di operazione interna su un insieme. Introduciamo ora un altro tipo di operazione, che coinvolge il campo \mathbb{K} .

Definizione 2.1. Sia V un insieme non vuoto. Chiameremo *prodotto esterno* o *moltiplicazione per gli scalari di \mathbb{K}* ogni applicazione del tipo

$$\cdot : \mathbb{K} \times V \rightarrow V.$$

Per ogni coppia (λ, v) con $\lambda \in \mathbb{K}$ e $v \in V$, scriveremo

$$\lambda \cdot v$$

oppure più semplicemente, omettendo il simbolo \cdot :

$$\lambda v$$

in luogo di $\cdot((\lambda, v))$.

Nel seguito quindi ammetteremo strutture algebriche su insiemi che presentino operazioni di tipo misto, interne e/o esterne.

Definizione 2.2. Si chiama *spazio vettoriale sul campo* \mathbb{K} ogni struttura algebrica $(V, +, \cdot)$, dove

$$+ : V \times V \rightarrow V, \quad \cdot : \mathbb{K} \times V \rightarrow V$$

sono rispettivamente un'operazione interna ed una esterna, dette operazioni di *somma* e *prodotto per scalari*, verificanti le seguenti proprietà (assiomi di spazio vettoriale):

- A) $(V, +)$ è un gruppo abeliano.
- B) Il prodotto per scalari soddisfa, per ogni $\lambda, \mu \in \mathbb{K}$ e $v \in V$:
 - 1) $\lambda(\mu v) = (\lambda\mu)v$
 - 2) $1v = v$.
- C) Le due operazioni sono legate dalle seguenti relazioni, valide per ogni $\lambda, \mu \in \mathbb{K}$ e per ogni $v, w \in V$:
 - 3) $(\lambda + \mu)v = \lambda v + \mu v$
 - 4) $\lambda(v + w) = \lambda v + \lambda w$.

Notiamo esplicitamente che negli assiomi di spazio vettoriale sono coinvolte, riconoscibili senza ambiguità, anche le operazioni di somma e prodotto del campo \mathbb{K} . In questo contesto gli elementi di \mathbb{K} vengono di solito chiamati *scalari*.

Spesso uno spazio vettoriale $(V, +, \cdot)$ sarà denotate semplicemente con il simbolo V , sottintendendo le due operazioni di cui è dotato. Diremo anche V è un \mathbb{K} -spazio vettoriale. Gli elementi di V si diranno *vettori* di V .

Nel caso in cui $\mathbb{K} = \mathbb{R}$, parleremo di spazio vettoriale *reale*, mentre se $\mathbb{K} = \mathbb{C}$, la terminologia è spazio vettoriale *complesso*.

Se $\lambda \in \mathbb{K}$ e $v \in V$, il vettore λv è detto *prodotto di v per lo scalare λ* . L'elemento neutro di V rispetto all'operazione di somma verrà denotato con 0_V o con 0 e sarà chiamato il *vettore nullo* di V .

Ricordiamo inoltre che l'assioma A) garantisce la validità delle proprietà commutativa e associativa dell'operazione di somma; inoltre per ogni vettore $v \in V$ esiste un unico vettore $-v \in V$ tale che

$$v + (-v) = 0_V;$$

tale vettore sarà chiamato il *vettore opposto* di v .

ESEMPIO 2.3. Ogni campo \mathbb{K} è dotato di una struttura canonica di spazio vettoriale su se stesso; le operazioni sono esattamente quelle di somma e prodotto del campo; quest'ultima infatti si può interpretare, in questo caso, anche come operazione esterna.

Gli assiomi di campo garantiscono infatti la validità delle proprietà A) e B) e C).

Spesso tale spazio si chiama *spazio vettoriale 1-dimensionale canonico* su \mathbb{K} o anche *retta* sul campo \mathbb{K} .

ESEMPIO 2.4. Sappiamo che il piano cartesiano reale \mathbb{R}^2 ha una struttura canonica di gruppo abeliano, discussa nell'Esempio 1.15. Si definisce anche in modo naturale una moltiplicazione esterna $\cdot : \mathbb{R} \times \mathbb{R}^2 \rightarrow \mathbb{R}^2$ ponendo

$$\lambda \cdot (x, y) := (\lambda x, \lambda y)$$

per ogni $\lambda \in \mathbb{R}$ e per ogni $(x, y) \in \mathbb{R}^2$. Risulta quindi che $(\mathbb{R}^2, +, \cdot)$ è uno spazio vettoriale reale.

Per interpretare geometricamente le operazioni qui introdotte, è sufficiente rappresentare ogni (x, y) mediante il vettore applicato \vec{OP} , dove P è il punto di coordinate (x, y) . Dunque ogni elemento di \mathbb{R}^2 ha due interpretazioni: punto o vettore. Quando usiamo la seconda interpretazione, stiamo dando una veste geometrica ai vettori dello *spazio vettoriale* \mathbb{R}^2 . Come già visto in precedenza, la somma di due vettori corrisponde alla somma dei corrispondenti vettori applicati secondo la regola del parallelogramma. Dato poi un vettore $v = (x, y) \in \mathbb{R}^2$ rappresentato da \vec{OP} e uno scalare $\lambda \in \mathbb{R}$ non nullo, allora $\lambda \cdot v$ corrisponde al vettore geometrico \vec{OQ} , dove il punto Q è allineato con O e P , il rapporto delle misure dei segmenti OQ e OP è λ , e il verso di \vec{OQ} è concorde con quello di \vec{OP} se $\lambda > 0$, mentre è il verso opposto a quello di \vec{OP} se $\lambda < 0$.

ESEMPIO 2.5. L'esempio precedente ammette una naturale generalizzazione. Dato un campo qualsiasi \mathbb{K} , possiamo introdurre una struttura di \mathbb{K} -spazio vettoriale sul prodotto cartesiano $\mathbb{K}^2 := \mathbb{K} \times \mathbb{K}$ introducendo due operazioni

$$+ : \mathbb{K}^2 \times \mathbb{K}^2 \rightarrow \mathbb{K}^2, \quad \cdot : \mathbb{K} \times \mathbb{K}^2 \rightarrow \mathbb{K}^2,$$

definite allo stesso modo di \mathbb{R}^2 come segue:

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \quad \lambda(x, y) := (\lambda x, \lambda y).$$

La verifica della validità degli assiomi di spazio vettoriale per $(\mathbb{K}^2, +, \cdot)$ non presenta particolari difficoltà. In particolare, l'associatività e la commutatività di $+$ vengono ereditate dalle analoghe proprietà della somma nel campo \mathbb{K} (che viene utilizzata contemporaneamente e separatamente sulle due coordinate delle coppie di scalari coinvolte).

Risulta che $(\mathbb{K}^2, +)$ è un gruppo, in quanto ammette la coppia:

$$(0, 0)$$

come elemento neutro, e ogni $(x, y) \in \mathbb{K}^2$ ammette come opposto:

$$(-x, -y).$$

Dunque $(\mathbb{K}^2, +)$ è effettivamente un gruppo abeliano. Si lascia al lettore la verifica completa delle restanti proprietà B) e C) nella definizione di spazio vettoriale. A titolo di esempio, controlliamo la prima delle B): se $\lambda, \mu \in \mathbb{K}$ e $(x, y) \in \mathbb{K}^2$, allora per definizione della moltiplicazione esterna risulta:

$$\lambda(\mu(x, y)) = \lambda(\mu x, \mu y) = (\lambda(\mu x), \lambda(\mu y)) = (\lambda\mu x, \lambda\mu y),$$

e d'altra parte:

$$(\lambda\mu)(x, y) = ((\lambda\mu)x, (\lambda\mu)y) = (\lambda\mu x, \lambda\mu y).$$

In tale verifica ci siamo avvalsi della proprietà associativa del prodotto nel campo.

ESEMPIO 2.6. Generalizzando quanto fatto nell'esempio precedente, possiamo introdurre una struttura di \mathbb{K} -spazio vettoriale sul prodotto cartesiano di più copie del campo \mathbb{K} , ovvero sull'insieme

$$\mathbb{K}^n = \underbrace{\mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ volte}} = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{K} \text{ per ogni } i\}.$$

Le operazioni di tale spazio vettoriale sono definite quindi come segue:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n),$$

$$\lambda(x_1, \dots, x_n) := (\lambda x_1, \dots, \lambda x_n).$$

Il vettore nullo è:

$$(0, 0, \dots, 0),$$

mentre per ogni vettore $(x_1, \dots, x_n) \in \mathbb{K}^n$ il suo opposto è:

$$(-x_1, \dots, -x_n).$$

In simboli:

$$-(x_1, \dots, x_n) = (-x_1, \dots, -x_n).$$

Lo spazio vettoriale \mathbb{K}^n sarà chiamato *spazio vettoriale n -dimensionale canonico* (talvolta *numerico*) sul campo \mathbb{K} .

3. PRODOTTI DIRETTI

Siano V_1 e V_2 spazi vettoriali sullo stesso campo \mathbb{K} . Definiamo sul prodotto cartesiano $V_1 \times V_2$ due operazioni

$$+ : (V_1 \times V_2) \times (V_1 \times V_2) \rightarrow V_1 \times V_2, \quad \cdot : \mathbb{K} \times (V_1 \times V_2) \rightarrow V_1 \times V_2$$

nel modo seguente

$$(1) \quad (v_1, v_2) + (w_1, w_2) := (v_1 + w_1, v_2 + w_2), \quad \lambda(v_1, v_2) := (\lambda v_1, \lambda v_2).$$

È facile verificare che tali operazioni godono delle proprietà A), B) e C) della Definizione 2.2. In particolare, riguardo A), l'elemento neutro per la somma è la coppia $(0_{V_1}, 0_{V_2})$; per ogni vettore $(v_1, v_2) \in V_1 \times V_2$, il suo opposto è la coppia $(-v_1, -v_2)$.

Definizione 3.1. Lo spazio vettoriale $V_1 \times V_2$ dotato delle operazioni (1) si chiama *prodotto diretto* di V_1 e V_2 .

4. SPAZI VETTORIALI DI FUNZIONI

Introduciamo ora un'altra importante tipologia di spazi vettoriali. Siano X un insieme non vuoto e V uno spazio vettoriale sul campo \mathbb{K} . Denoteremo con

$$V^X$$

l'insieme di tutte le funzioni $F : X \rightarrow V$. Su tale insieme si definiscono in modo naturale un'operazione interna di somma e una moltiplicazione esterna per scalari, come segue. Date due funzioni $F : X \rightarrow V$ e $G : X \rightarrow V$, allora la *funzione somma* $F + G$ si definisce come la funzione denotata con $F + G : X \rightarrow V$ che opera come segue:

$$(F + G)(x) := F(x) + G(x) \quad \forall x \in X.$$

Invece se $F : X \rightarrow V$ e $\lambda \in \mathbb{K}$, allora il *prodotto* $\lambda \cdot F$ si definisce come la funzione $\lambda \cdot F : X \rightarrow V$ tale che:

$$(\lambda \cdot F)(x) := \lambda F(x) \quad \forall x \in X.$$

Risulta allora che $(V^X, +, \cdot)$ è uno spazio vettoriale sul campo \mathbb{K} . Si osserva che le proprietà di associatività della somma tra funzioni discende dall'analoga proprietà della somma tra vettori di V . Lo stesso vale per quel che riguarda la proprietà commutativa.

Il vettore nullo di tale spazio è la funzione costante di valore 0_V , che denotiamo con 0_{V^X} . Dunque si tratta della funzione definita da:

$$0_{V^X}(x) := 0_V \quad \forall x \in X,$$

che associa ad ogni x il vettore nullo di V .

Infatti, risulta che

$$F + 0_{V^X} = F$$

in quanto per ogni $x \in X$, calcolando il valore in x della funzione somma $F + 0_{V^X}$ si ottiene:

$$(F + 0_{V^X})(x) = F(x) + 0_{V^X}(x) = F(x) + 0_V = F(x).$$

Per ogni $F : X \rightarrow V$ il vettore opposto $-F$ è la funzione così definita:

$$(-F)(x) := -F(x) \quad \forall x \in X,$$

che associa cioè ad ogni punto x in X il vettore opposto di $F(x)$ in V . Anche in questo caso la verifica di ciò consiste nel giustificare un'uguaglianza tra funzioni:

$$F + (-F) = 0_{V^X}.$$

Questa uguaglianza sussiste in quanto per ogni $x \in X$ si ha:

$$(F + (-F))(x) = F(x) + (-F)(x) = F(x) - F(x) = 0_V.$$

La verifica della validità di tutti gli altri assiomi di spazio vettoriale per tale struttura algebrica $(V^X, +, \cdot)$ è un esercizio molto istruttivo per prendere confidenza con la nozione di spazio vettoriale.

5. MATRICI

Discutiamo ora un altro esempio fondamentale di spazio vettoriale. Sia \mathbb{K} un campo e siano m, n interi positivi.

Definizione 5.1. Una **matrice** A di tipo $m \times n$ (oppure (m, n)) a coefficienti in \mathbb{K} è una tabella rettangolare costituita da $m \cdot n$ elementi di \mathbb{K} disposti in m righe ed n colonne, e rappresentata nel modo seguente:

$$(2) \quad A = \begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_n^1 \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ a_1^m & a_2^m & \cdots & a_n^m \end{pmatrix}$$

Si scrive anche in modo compatto $A = (a_j^i)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ o più semplicemente $A = (a_j^i)$.

Nella scrittura $A = (a_j^i)$ converremo sempre che l'indice in alto (in basso) indichi la riga (risp. la colonna) occupata dall'elemento a_j^i . L'insieme di tutte le matrici di tipo $m \times n$ ad elementi in \mathbb{K} verrà denotato col simbolo $M_{m,n}(\mathbb{K})$.

Se $m = n$, tale insieme si denota più semplicemente con $M_n(\mathbb{K})$ e i suoi elementi sono detti *matrici quadrate* di ordine n .

Una matrice $(a_1 \dots a_n)$ di tipo $1 \times n$ è chiamata *vettore riga* (di lunghezza n) ed è identificata con il vettore (a_1, \dots, a_n) dello spazio \mathbb{K}^n . Analogamente, ogni matrice

$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$ è detta *vettore colonna* ed è identificabile anch'essa con $(a_1, \dots, a_m) \in \mathbb{K}^m$.

Nel seguito tali identificazioni saranno utilizzate spesso senza ulteriori commenti.

Fissato $i \in \{1, \dots, m\}$, l' i -ma riga di A è dunque la matrice di tipo $1 \times n$

$$A^{(i)} := (a_1^i \quad a_2^i \quad \cdots \quad a_n^i)$$

mentre, fissato $j \in \{1, \dots, n\}$, la j -ma colonna di A è la matrice di tipo $m \times 1$:

$$A_{(j)} := \begin{pmatrix} a_j^1 \\ a_j^2 \\ \vdots \\ a_j^m \end{pmatrix}.$$

Possiamo rappresentare A per colonne nel modo seguente:

$$A = (A_{(1)} \quad A_{(2)} \quad \cdots \quad A_{(n)})$$

oppure per righe:

$$A = \begin{pmatrix} A^{(1)} \\ A^{(2)} \\ \vdots \\ A^{(m)} \end{pmatrix}.$$

Teorema 5.2. *L'insieme $M_{m,n}(\mathbb{K})$ ammette una struttura canonica di spazio vettoriale su \mathbb{K} , le cui operazioni di somma e prodotto esterno sono definite come segue: per ogni $A = (a_j^i)$, $B = (b_j^i)$ e $\lambda \in \mathbb{K}$ si pone:*

$$A + B := (a_j^i + b_j^i), \quad \lambda A := (\lambda a_j^i).$$

Lasciamo al lettore la cura di verificare, per le operazioni descritte sopra, la validità degli assiomi A), B) e C) della definizione di spazio vettoriale. Ci limitiamo a mettere in evidenza due fatti salienti: il vettore nullo dello spazio vettoriale $M_{m,n}(\mathbb{K})$ in questione è la *matrice nulla* ovvero la matrice, denotata semplicemente con 0 , i cui elementi sono tutti uguali allo zero di \mathbb{K} :

$$0 := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Per ogni $A = (a_j^i) \in M_{m,n}(\mathbb{K})$, il vettore opposto di A in $M_{m,n}(\mathbb{K})$ è la matrice

$$-A = (-a_j^i).$$

D'ora in avanti considereremo sempre l'insieme $M_{m,n}(\mathbb{K})$ munito della struttura di spazio vettoriale appena descritta.

6. PROPRIETÀ ELEMENTARI DEGLI SPAZI VETTORIALI

Prima di procedere oltre, mettiamo in evidenza alcune proprietà basilari degli spazi vettoriali che si deducono dagli assiomi.

Proposizione 6.1. *Sia V uno spazio vettoriale sul campo \mathbb{K} . Allora per ogni $v \in V$ e per ogni $\lambda \in \mathbb{K}$, risulta:*

- a) $\lambda 0_V = 0_V$
- b) $0v = 0_V$
- c) $-v = (-1)v$.
- d) $\lambda v = 0_V \Rightarrow \lambda = 0 \vee v = 0_V$.

DIMOSTRAZIONE: a) Abbiamo $\lambda 0_V = \lambda(0_V + 0_V) = \lambda 0_V + \lambda 0_V$ da cui, per la legge di cancellazione: $0_V = \lambda 0_V$.

b) Possiamo scrivere $0v = (0 + 0)v = 0v + 0v$ da cui ancora per la legge di cancellazione $0_V = 0v$.

c) Per l'unicità dell'opposto di v nel gruppo abeliano $(V, +)$, si tratta di provare che

$$v + (-1)v = 0_V.$$

Infatti,

$$v + (-1)v = 1v + (-1)v = (1 - 1)v = 0v = 0_V$$

dove l'ultimo passaggio è giustificato dalla proprietà b) già provata.

d) Si supponga $\lambda v = 0_V$. Se $\lambda = 0$, la tesi è provata. Supponiamo quindi $\lambda \neq 0$; allora esiste l'inverso λ^{-1} di λ in \mathbb{K} . Dalla relazione $\lambda v = 0_V$ moltiplicando ambo i membri per λ^{-1} otteniamo

$$\lambda^{-1}(\lambda v) = \lambda^{-1}0_V$$

da cui per la a):

$$(\lambda^{-1}\lambda)v = 0_V$$

che possiamo riscrivere

$$1v = 0_V$$

ovvero $v = 0_V$.

□

7. SOTTOSPAZI

Sia V uno spazio vettoriale sul campo \mathbb{K} .

Definizione 7.1. Un sottoinsieme non vuoto W di V si dice *sottospazio vettoriale* di V se è stabile rispetto ad entrambe le operazioni $+$ e \cdot di V , il che significa che sono soddisfatte le seguenti condizioni:

- a) $\forall u, v \in W : u + v \in W.$
- b) $\forall u \in W \forall \lambda \in \mathbb{K} : \lambda u \in W.$

La terminologia “sottospazio” è chiarita dalla seguente proposizione.

Proposizione 7.2. *Sia $W \subset V$ un sottospazio vettoriale del \mathbb{K} -spazio vettoriale V . Allora si ha che $0_V \in W$. Inoltre W eredita in modo canonico una struttura di spazio vettoriale su \mathbb{K} , le cui operazioni sono ottenute dalle operazioni dello spazio vettoriale ambiente V per restrizione.*

DIMOSTRAZIONE: Sia $u \in W$; allora, utilizzando la proprietà b) di sottospazio, abbiamo che anche il vettore opposto $-u$ appartiene anch'esso a W , in quanto, ricordando quanto stabilito nella Prop. 6.1, possiamo scrivere $-u = (-1)u \in W$. In particolare, fissato un tale elemento $u \in W$ (è possibile perchè W non è vuoto), usando la proprietà a) si evince che $0_V \in W$; infatti:

$$0_V = u + (-u) \in W.$$

Con ciò resta provata la prima affermazione. Le condizioni a) e b) permettono di restringere le operazioni di somma e prodotto esterno su W , ottenendo le operazioni indotte

$$+ : W \times W \rightarrow W, \cdot : \mathbb{K} \times W \rightarrow W$$

con cui si opera allo stesso modo. Come sappiamo, l'operazione di somma così ottenuta continua a essere associativa e commutativa sull'insieme stabile W . Evidentemente 0_V è anche elemento neutro di $(W, +)$ e ogni $u \in W$ risulta invertibile in $(W, +)$ grazie al fatto, già stabilito, che $-u \in W$. Dunque $(W, +)$ è un gruppo abeliano. Infine, le proprietà B) e C) nella definizione di spazio vettoriale sono ancora manifestamente soddisfatte anche dalle operazioni qui coinvolte, ristrette a W . \square

ESEMPIO 7.3. Pensando a \mathbb{R}^2 come ad un piano cartesiano, abbiamo che ogni retta $r \subset \mathbb{R}^2$ passante per l'origine è un sottospazio vettoriale di \mathbb{R}^2 .

Infatti, supponiamo che r abbia equazione:

$$r : ax + by = 0,$$

dove le costanti reali a, b non sono entrambe zero. Dunque r è il luogo geometrico:

$$r = \{(x, y) \in \mathbb{R}^2 : ax + by = 0\}.$$

Dati $(x_1, y_1) \in r$ e $(x_2, y_2) \in r$, bisogna verificare innanzitutto che

$$(x_1, y_1) + (x_2, y_2) \in r.$$

Infatti, per definizione $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ e risulta

$$a(x_1 + x_2) + b(y_1 + y_2) = (ax_1 + by_1) + (ax_2 + by_2) = 0 + 0 = 0.$$

Analogamente, se $\lambda \in \mathbb{R}$ e $(x_1, y_1) \in r$, allora anche $\lambda(x_1, y_1) = (\lambda x_1, \lambda y_1)$ appartiene alla retta perchè

$$a(\lambda x_1) + b(\lambda y_1) = \lambda(ax_1 + by_1) = \lambda \cdot 0 = 0.$$

Questo esempio ci fa intuire che la stessa nozione di retta, così come quella di piano, e tutta la geometria elementare si possono fondare, in modo indipendente dal metodo assiomatico classico, sulla nozione di spazio vettoriale reale.

ESEMPIO 7.4. Una matrice quadrata $A = (a_j^i)$ di ordine n a coefficienti in un campo assegnato \mathbb{K} si dice *simmetrica* se:

$$a_j^i = a_i^j, \text{ per ogni } i, j \in \{1, \dots, n\}.$$

Ciò significa che gli elementi della matrice sono disposti in modo simmetrico rispetto alla cosiddetta *diagonale principale*, formata dagli ingressi del tipo a_1^1, \dots, a_n^n , aventi indice riga e colonna uguali.

Così ad es. la generica matrice simmetria 3x3 è del tipo:

$$A = \begin{pmatrix} a_1^1 & a_2^1 & a_3^1 \\ a_2^1 & a_2^2 & a_3^2 \\ a_3^1 & a_3^2 & a_3^3 \end{pmatrix}.$$

Non è difficile verificare che l'insieme $Sym_n(\mathbb{K})$ di tutte le matrici simmetriche di un fissato ordine n è un sottospazio vettoriale di $M_n(\mathbb{K})$. Infatti, tale insieme è non vuoto in quanto la matrice nulla 0 è banalmente simmetrica. Date due matrici simmetriche $A = (a_j^i)$ e $B = (b_j^i)$, allora $A + B$ è simmetrica in quanto

$$a_j^i + b_j^i = a_i^j + b_i^j.$$

Analogamente, per ogni $\lambda \in \mathbb{K}$ e $A = (a_j^i) \in Sym_n(\mathbb{K})$, risulta che anche λA è simmetrica avendosi

$$\lambda a_j^i = \lambda a_i^j.$$

In particolare, si ottiene anche $Sym_n(\mathbb{K})$ è canonicamente uno spazio vettoriale su \mathbb{K} .

8. SOMMA E INTERSEZIONE DI SOTTOSPAZI

Discutiamo ora due metodi standard per costruire sottospazi vettoriali di uno spazio vettoriale assegnato.

Proposizione 8.1. *Siano U e W due sottospazi di un assegnato \mathbb{K} -spazio vettoriale V .*

a) *Il sottoinsieme di V definito da*

$$U + W := \{u + w \mid u \in U, w \in W\}$$

è un sottospazio vettoriale di V , detto somma di U e W .

b) *L'intersezione insiemistica $U \cap W$ è un sottospazio vettoriale di V .*

DIMOSTRAZIONE:

a) Naturalmente $U + W \neq \emptyset$ perchè entrambi i sottospazi non sono vuoti. Considerati due vettori $u + w$ e $u' + w'$ di $U + W$, dove $u, u' \in U$ e $w, w' \in W$, allora:

$$(u + w) + (u' + w') = (u + u') + (w + w') \in U + W$$

perchè sia U che W sono stabili rispetto alla somma. Analogamente, dato uno scalare λ si ha

$$\lambda(u + w) = (\lambda u) + (\lambda w) \in U + W.$$

b) L'intersezione in questione è non vuota, in quanto il vettore nullo appartiene a entrambi i sottospazi. Dati due vettori u e w in $U \cap W$ allora il vettore $u + w$ appartiene ad U , in quanto U è sottospazio, e i vettori in questione vi appartengono; per lo stesso motivo $u + w$ appartiene anche a W , dunque appartiene a $U \cap W$. Lo stesso argomento mostra che, se $\lambda \in \mathbb{K}$ e $u \in U \cap W$, anche λu appartiene a $U \cap W$.

□

Si osservi che risulta:

$$U \subset U + W, \quad W \subset U + W,$$

perchè ogni vettore u di U può essere scritto nella forma $u = u + 0_W$ e analogamente per W .

9. COMBINAZIONI LINEARI DI VETTORI

Definizione 9.1. Siano V un \mathbb{K} -spazio vettoriale e

$$v_1, \dots, v_k$$

una sequenza finita di vettori di V . Si chiama *combinazione lineare* dei vettori v_1, \dots, v_k ogni vettore del tipo

$$\lambda_1 v_1 + \dots + \lambda_k v_k$$

dove $\lambda_1, \dots, \lambda_k$ sono arbitrari scalari, detti *coefficienti* della combinazione lineare.

ESEMPIO 9.2. Ad esempio tutte le combinazioni lineari dei vettori

$$(1, 2, 0), (0, 0, 1), (\sqrt{2}, 0, \sqrt{3})$$

di \mathbb{R}^3 sono i vettori del tipo:

$$(\alpha + \sqrt{2}\gamma, 2\alpha, \beta + \sqrt{3}\gamma)$$

al variare di α, β, γ in \mathbb{R} .

Invece, date le funzioni $\sin : \mathbb{R} \rightarrow \mathbb{R}$, $\cos : \mathbb{R} \rightarrow \mathbb{R}$, pensate come vettori di $\mathbb{R}^{\mathbb{R}}$, ogni funzione del tipo:

$$f(x) = a \sin(x) + b \cos(x),$$

con a e b costanti reali, è una loro combinazione lineare.

Sussiste la seguente caratterizzazione dei sottospazi, che utilizza la nozione di combinazione lineare di due vettori:

Proposizione 9.3. Sia W un sottoinsieme non vuoto di un \mathbb{K} -spazio vettoriale V . Allora sono proprietà equivalenti:

- a) W è sottospazio vettoriale di V ;
- b) Per ogni $u, v \in W$ e $\lambda, \mu \in \mathbb{K}$ si ha $\lambda u + \mu v \in W$.

Si lascia la verifica come esercizio.

10. SOTTOSPAZIO GENERATO DA UN NUMERO FINITO DI VETTORI

Definizione 10.1. Sia V uno spazio vettoriale sul campo \mathbb{K} e sia v_1, \dots, v_m , $m \geq 1$, una successione finita di vettori.

Si chiama *sottospazio vettoriale di V generato da v_1, \dots, v_m* il sottoinsieme di V

$$L(v_1, \dots, v_m) := \{\lambda_1 v_1 + \dots + \lambda_m v_m \mid \lambda_1, \dots, \lambda_m \in \mathbb{K}\}$$

costituito da tutte le combinazioni lineari dei vettori v_1, \dots, v_m .

Notiamo che $L(v_1, \dots, v_m)$ è effettivamente un sottospazio di V . Chiaramente $L(v_1, \dots, v_m)$ non è vuoto; notiamo in particolare che $0 \in L(v_1, \dots, v_m)$ in quanto

$$0 = 0v_1 + \dots + 0v_m.$$

Date due combinazioni lineari $u = \lambda_1 v_1 + \dots + \lambda_m v_m$ e $w = \mu_1 v_1 + \dots + \mu_m v_m$, la loro somma è ancora una combinazione lineare degli stessi vettori, infatti:

$$\begin{aligned} u + w &= (\lambda_1 v_1 + \dots + \lambda_m v_m) + (\mu_1 v_1 + \dots + \mu_m v_m) \\ &= (\lambda_1 v_1 + \mu_1 v_1) + \dots + (\lambda_m v_m + \mu_m v_m) = \\ &= (\lambda_1 + \mu_1)v_1 + \dots + (\lambda_m + \mu_m)v_m. \end{aligned}$$

Si noti l'utilizzo delle proprietà commutativa e associativa della somma e dell'assioma C) di spazio vettoriale. Analogamente, per ogni $\lambda \in \mathbb{K}$ abbiamo

$$(3) \quad \lambda u = \lambda(\lambda_1 v_1 + \dots + \lambda_m v_m) = (\lambda \lambda_1)v_1 + \dots + (\lambda \lambda_m)v_m$$

per cui anche λu appartiene a $L(v_1, \dots, v_m)$.

Notiamo esplicitamente che ciascun vettore v_i della sequenza appartiene a $L(v_1, \dots, v_m)$, potendosi scrivere

$$v_i = 0v_1 + \dots + 0v_{i-1} + 1v_i + 0v_{i+1} + \dots + 0v_m.$$

Sussiste anzi la seguente proprietà:

Proposizione 10.2. *Data una sequenza di vettori v_1, \dots, v_m dello spazio vettoriale V ed un sottospazio vettoriale W di V contenente tutti i vettori v_1, \dots, v_m , si ha che*

$$L(v_1, \dots, v_m) \subset W.$$

Dunque il sottospazio generato da v_1, \dots, v_m è il più piccolo sottospazio che contiene gli stessi vettori.

DIMOSTRAZIONE: Basta osservare che ogni vettore del tipo $\lambda_1 v_1 + \dots + \lambda_m v_m$ deve appartenere a W in quanto, stante l'ipotesi su W , per definizione di sottospazio vettoriale ogni $\lambda_i v_i$ vi appartiene e W è stabile rispetto all'operazione di somma. \square

11. APPLICAZIONI LINEARI

Nello studio degli spazi vettoriali è essenziale lavorare con funzioni che permettano di mettere in relazione spazi diversi non solo come insiemi, ma tenendo conto della struttura algebrica aggiuntiva.

Definizione 11.1. Siano V e V' due spazi vettoriali sullo stesso campo \mathbb{K} . Un' applicazione $F : V \rightarrow V'$ si dice \mathbb{K} -lineare o semplicemente *lineare* se ha le proprietà seguenti:

$$\begin{aligned} 1) \quad \forall u, v \in V : & \quad F(u + v) = F(u) + F(v). \\ 2) \quad \forall v \in V \forall \lambda \in \mathbb{K} : & \quad F(\lambda v) = \lambda F(v). \end{aligned}$$

Ogni applicazione lineare deve soddisfare il seguente vincolo:

Proposizione 11.2. Sia $F : V \rightarrow V'$ un'applicazione lineare tra \mathbb{K} -spazi vettoriali. Allora

$$F(0_V) = 0_{V'}.$$

DIMOSTRAZIONE: Infatti,

$$F(0_V) = F(0_V + 0_V) = F(0_V) + F(0_V).$$

Utilizzando la legge di cancellazione nel gruppo $(V', +)$ segue che $0_{V'} = F(0_V)$. \square

ESEMPIO 11.3. Sono lineari tutte le funzioni $\mathbb{R} \rightarrow \mathbb{R}$ del tipo:

$$x \in \mathbb{R} \mapsto ax,$$

dove $a \in \mathbb{R}$ è una costante assegnata. Si noti che invece un polinomio di primo grado

$$x \in \mathbb{R} \mapsto ax + b$$

con $b \neq 0$ non è lineare secondo la definizione che abbiamo introdotto, stante la proposizione precedente.

ESEMPIO 11.4. Ogni funzione polinomiale $F : \mathbb{R}^2 \rightarrow \mathbb{R}$ del tipo

$$F(x, y) := ax + by$$

con a, b costanti assegnate, è lineare.

La verifica di questo fatto ricalca quanto fatto nell'Es. 7.3 per giustificare che ogni retta per l'origine è un sottospazio vettoriale di \mathbb{R}^2 . Infatti, dati i vettori (x_1, y_1) e (x_2, y_2) risulta:

$$\begin{aligned} F((x_1, y_1) + (x_2, y_2)) &= F(x_1 + x_2, y_1 + y_2) = a(x_1 + x_2) + b(y_1 + y_2) = \\ &= (ax_1 + by_1) + (ax_2 + by_2) = F(x_1, y_1) + F(x_2, y_2). \end{aligned}$$

E ancora in modo simile:

$$F(\lambda(x_1, y_1)) = F(\lambda x_1, \lambda y_1) = a(\lambda x_1) + b(\lambda y_1) = \lambda(ax_1 + by_1) = \lambda F(x_1, y_1).$$

Osservazione 11.5. Notiamo che ogni applicazione lineare $F : V \rightarrow V'$ soddisfa anche:

$$F(u - v) = F(u) - F(v),$$

per ogni $u, v \in V$.

$$\text{Infatti: } F(u - v) = F(u + (-1)v) = F(u) + (-1)F(v) = F(u) - F(v).$$

Ad ogni applicazione lineare si associa in modo naturale un insieme notevole di vettori, definito come segue:

Definizione 11.6. Sia $F : V \rightarrow V'$ un'applicazione lineare tra \mathbb{K} -spazi vettoriali. Si chiama *nucleo di F* il seguente sottoinsieme di V :

$$\text{Ker}(F) := \{v \in V \mid F(v) = 0_{V'}\}.$$

Il seguente risultato è basilare:

Teorema 11.7. Sia $F : V \rightarrow V'$ un'applicazione lineare tra \mathbb{K} -spazi vettoriali. Allora:

- 1) $\text{Ker}(F)$ è un sottospazio vettoriale di V .
- 2) F è iniettiva $\iff \text{Ker}(F) = \{0_V\}$.

DIMOSTRAZIONE: a) Sappiamo che $0_V \in \text{Ker}(F)$, per cui $\text{Ker}(F)$ è non vuoto. Siano $u, v \in \text{Ker}(F)$; allora

$$F(u + v) = F(u) + F(v) = 0_{V'} + 0_{V'} = 0_{V'},$$

e ciò mostra che $u + v \in \text{Ker}(F)$. Inoltre, dato un arbitrario scalare λ abbiamo:

$$F(\lambda u) = \lambda F(u) = \lambda 0_{V'} = 0_{V'}.$$

b) Cominciamo con l'osservare che l'inclusione $\{0_V\} \subset \text{Ker}(F)$ è sempre vera. Supponiamo dapprima che F sia iniettiva. Sia $u \in \text{Ker}(F)$; allora $F(u) = 0_{V'}$, ovvero stante la Prop. 11.2:

$$F(u) = F(0_V),$$

da cui $u = 0_V$ per l'iniettività di F . Resta così provato che $\text{Ker}(F) = \{0_V\}$.

Supponiamo ora $\text{Ker}(F) = \{0_V\}$; siano $u, v \in V$ tali che

$$F(u) = F(v).$$

Utilizzando le proprietà del gruppo $(V', +)$, segue:

$$F(u) - F(v) = 0_{V'}$$

e quindi

$$F(u - v) = 0_{V'},$$

pertanto $u - v \in \text{Ker}(F)$ e per l'ipotesi segue necessariamente che $u - v = 0_V$, ovvero $u = v$. \square

Tornando all'esempio delle rette per l'origine in \mathbb{R}^2 , ogni retta del piano di assegnata equazione $r : ax + by = 0$ coincide con il nucleo dell'applicazione lineare $F : \mathbb{R}^2 \rightarrow \mathbb{R}$ di cui nell'esempio precedente. Quindi il fatto che ogni retta in questione è uno spazio vettoriale è fondato su un principio generale.

Si noti anche la seguente caratterizzazione delle applicazioni lineari, che coinvolge combinazioni lineari di vettori:

Proposizione 11.8. *Sia $F : V \rightarrow V'$ un'applicazione tra due \mathbb{K} -spazi vettoriali. Sono proprietà equivalenti:*

- a) F è lineare;
- b) Per ogni $\lambda, \mu \in \mathbb{K}$ e $u, v \in V$ si ha: $F(\lambda u + \mu v) = \lambda F(u) + \mu F(v)$.

La dimostrazione è un esercizio: per provare che b) implica a), basta particularizzare b) nel caso $\lambda = \mu = 1$ e nel caso $\mu = 0$.

ESEMPIO 11.9. (Proiezioni) Fissato $n \geq 1$, le n funzioni

$$p_i : \mathbb{K}^n \rightarrow \mathbb{K}, \quad p_i(x_1, \dots, x_n) := x_i, \quad i \leq i \leq n$$

che associano ad ogni vettore di \mathbb{K}^n la sua coordinata i -ma sono tutte lineari. Esse si chiamano *proiezioni naturali* o semplicemente *proiezioni*.

La verifica di ciò è semplice: dati $x = (x_1, \dots, x_n)$ e $y = (y_1, \dots, y_n)$ e due scalari λ, μ allora:

$$\lambda x + \mu y = (\lambda x_1 + \mu y_1, \dots, \lambda x_i + \mu y_i, \dots, \lambda x_n + \mu y_n)$$

sicchè

$$p_i(\lambda x + \mu y) = \lambda x_i + \mu y_i = \lambda p_i(x) + \mu p_i(y).$$

12. MONOMORFISMI, EPIMORFISMI E ISOMORFISMI

Definizione 12.1. Si consideri un'applicazione lineare $F : V \rightarrow V'$ tra due \mathbb{K} -spazi vettoriali.

Se F è iniettiva, prende il nome di **monomorfismo**, mentre se è surgettiva prende il nome di **epimorfismo**; infine, se F è bigettiva, essa prende il nome di **isomorfismo**.

Sappiano che i monomorfismi sono caratterizzati dall'aver nucleo banale; gli epimorfismi si caratterizzano, stante la definizione, mediante un altro sottospazio notevole:

Definizione 12.2. Sia $F : V \rightarrow V'$ un'applicazione lineare tra \mathbb{K} -spazi vettoriali. Si chiama **immagine di F** il sottoinsieme $Im(F) := F(V)$ di V' . Pertanto:

$$Im(F) = \{F(v) \mid v \in V\}.$$

Dunque F è un epimorfismo se e solo se $Im(F) = V'$.

Proposizione 12.3. *Per ogni applicazione lineare $F : V \rightarrow V'$, $Im(F)$ è un sottospazio vettoriale di V' .*

La dimostrazione è semplice: dati due vettori $u' = F(u)$ e $v' = F(v)$ di $Im(F)$ e due scalari λ e μ risulta:

$$\lambda u' + \mu v' = \lambda F(u) + \mu F(v) = F(\lambda u + \mu v) \in Im(F).$$

Due \mathbb{K} -spazi vettoriali V e V' si diranno **isomorfi** se esiste almeno un isomorfismo $F : V \rightarrow V'$. In tal caso, scriveremo

$$V \cong V'$$

o anche, volendo mettere in evidenza un particolare isomorfismo:

$$F : V \xrightarrow{\sim} V'.$$

Due spazi vettoriali isomorfi sono da considerarsi due diverse manifestazioni del medesimo oggetto matematico; dal punto di vista dell'algebra lineare, essi avranno le stesse proprietà e si potranno opportunamente identificare.

Vale il seguente risultato, la cui dimostrazione è un utile esercizio:

Teorema 12.4. *Sia $F : V \rightarrow V'$ un isomorfismo. Allora anche l'applicazione inversa $F^{-1} : V' \rightarrow V$ è lineare, e quindi è anch'essa un isomorfismo.*

Concludiamo questo paragrafo con la seguente osservazione:

Proposizione 12.5. *Sia $F : V \rightarrow V'$ un'applicazione lineare tra due \mathbb{K} -spazi vettoriali. Allora F trasforma combinazioni lineari di vettori in combinazioni lineari delle rispettive immagini, mantenendo gli stessi coefficienti. Ovvero per ogni $v_1, \dots, v_k \in V$ e per ogni $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ si ha:*

$$F(\lambda_1 v_1 + \dots + \lambda_k v_k) = \lambda_1 F(v_1) + \dots + \lambda_k F(v_k).$$

Per provarlo è sufficiente applicare più volte la b) della Proposizione 11.8. Una dimostrazione più rigorosa si può fare agevolmente per induzione sul numero k dei vettori coinvolti.

13. ULTERIORI PROPRIETÀ DELLE APPLICAZIONI LINEARI

Proposizione 13.1. *Sia $F : V \rightarrow V'$ un'applicazione lineare tra \mathbb{K} -spazi vettoriali. Sia U un sottospazio vettoriale di V . Allora:*

- a) la restrizione $F|_U : U \rightarrow V'$ è lineare.
- b) L'immagine $F(U)$ di U è sottospazio vettoriale di V' .

DIMOSTRAZIONE: a) La dimostrazione è immediata, in quanto la restrizione di F opera come F sui vettori di U : quindi per ogni $u, w \in U$ e λ, μ scalari abbiamo ancora

$$F|_U(\lambda u + \mu w) = F(\lambda u + \mu w) = \lambda F(u) + \mu F(w) = \lambda F|_U(u) + \mu F|_U(w).$$

b) Ricordiamo che, per definizione:

$$F(U) = \{F(u) \mid u \in U\},$$

e chiaramente tale insieme coincide con $Im(F|_U)$, avendosi:

$$\{F(u) \mid u \in U\} = \{F|_U(u) \mid u \in U\}.$$

□

La seguente proprietà è fondamentale nella teoria degli spazi vettoriali.

Teorema 13.2. *Siano V, V' e V'' spazi vettoriali sullo stesso campo \mathbb{K} e siano $F : V \rightarrow V', G : V' \rightarrow V''$ applicazioni lineari. Allora anche $G \circ F : V \rightarrow V''$ è lineare.*

DIMOSTRAZIONE: Siano $u, v \in V$ e λ, μ scalari. Allora si ha:

$$\begin{aligned} (G \circ F)(\lambda u + \mu v) &= G(F(\lambda u + \mu v)) = G(\lambda F(u) + \mu F(v)) \\ &= \lambda G(F(u)) + \mu G(F(v)) = \lambda(G \circ F)(u) + \mu(G \circ F)(v). \end{aligned}$$

□

Occupiamoci ora di ulteriori importanti proprietà delle applicazioni lineari, che coinvolgono le operazioni di somma di funzioni e moltiplicazione di scalari per funzioni, già considerate nel §4.

Proposizione 13.3. *Siano V e W due \mathbb{K} -spazi vettoriali.*

a) *Se $F : V \rightarrow W$ e $G : V \rightarrow W$ sono due applicazioni lineari, allora anche $F + G : V \rightarrow W$ è lineare.*

b) *Se $F : V \rightarrow W$ è un'applicazione lineare e $\lambda \in \mathbb{K}$, allora anche λF è lineare.*

DIMOSTRAZIONE: a) Date le applicazioni lineari $F : V \rightarrow W$ e $G : V \rightarrow W$, due vettori u, v di V e scalari λ, μ , si tratta di verificare che:

$$(F + G)(\lambda u + \mu v) = \lambda(F + G)(u) + \mu(F + G)(v).$$

Infatti, per definizione della funzione somma $F + G$, e la linearità delle due funzioni abbiamo:

$$\begin{aligned} (F + G)(\lambda u + \mu v) &= F(\lambda u + \mu v) + G(\lambda u + \mu v) = \\ &= \lambda F(u) + \mu F(v) + \lambda G(u) + \mu G(v) = \\ &= \lambda(F(u) + G(u)) + \mu(F(v) + G(v)) = \\ &= \lambda(F + G)(u) + \mu(F + G)(v). \end{aligned}$$

La verifica di b) è simile:

$$\begin{aligned}(\lambda F)(\alpha u + \beta v) &= \lambda(F(\alpha u + \beta v)) = \lambda(\alpha F(u) + \beta F(v)) = \\ &= \lambda\alpha F(u) + \lambda\beta F(v) = \alpha\lambda F(u) + \beta\lambda F(v) = \alpha(\lambda F)(u) + \beta(\lambda F)(v).\end{aligned}$$

□

Fissati i due spazi vettoriali V e W sullo stesso campo \mathbb{K} denoteremo con il simbolo

$$\text{Hom}(V, W)$$

l'insieme di tutte le applicazioni lineari da V in W , ovvero

$$\text{Hom}(V, W) := \{F : V \rightarrow W \mid F \text{ è lineare}\}.$$

Si tratta di un sottoinsieme dello spazio vettoriale W^V di tutte le funzioni $F : V \rightarrow W$: esso è certamente non vuoto, perchè l'applicazione nulla $0 : V \rightarrow W$ è lineare. Le proprietà a) e b) appena stabilite garantiscono quindi che:

Corollario 13.4. *Dati due \mathbb{K} -spazi vettoriali, $\text{Hom}(V, W)$ è un sottospazio vettoriale di W^V .*

In particolare anche $\text{Hom}(V, W)$ è canonicamente un \mathbb{K} -spazio vettoriale, in cui le operazioni di somma tra funzioni lineari e moltiplicazione per scalari sono esattamente quelle discusse sopra. Il vettore nullo di tale spazio è la funzione nulla $0 : V \rightarrow W$.

Concludiamo questo paragrafo discutendo le seguenti proprietà utili che coinvolgono somme e composizioni di applicazioni lineari:

Proposizione 13.5. *Siano $F : V \rightarrow V'$ e $G : V \rightarrow V'$ due applicazioni \mathbb{K} -lineari e $T : U \rightarrow V$, $L : V' \rightarrow W$ due altre applicazioni lineari, dove U e W sono altri \mathbb{K} -spazi vettoriali. Allora:*

$$(F + G) \circ T = F \circ T + G \circ T, \quad L \circ (F + G) = L \circ F + L \circ G.$$

DIMOSTRAZIONE: La dimostrazione è ancora una semplice applicazione della definizione di somma di due funzioni; ad esempio, per ogni $u \in U$ si ha:

$$\begin{aligned}((F + G) \circ T)(u) &= (F + G)(T(u)) = F(T(u)) + G(T(u)) = \\ &= (F \circ T)(u) + (G \circ T)(u) = (F \circ T + G \circ T)(u).\end{aligned}$$

Similmente, per ogni $v \in V$ ricaviamo che:

$$\begin{aligned}(L \circ (F + G))(v) &= L((F + G)(v)) = L(F(v) + G(v)) = L(F(v)) + L(G(v)) = \\ &= (L \circ F)(v) + (L \circ G)(v) = (L \circ F + L \circ G)(v).\end{aligned}$$

□

14. LA BASE CANONICA DI \mathbb{K}^n

Lo spazio vettoriale \mathbb{K}^n contiene un insieme di vettori particolarmente importante; esso costituisce il prototipo della nozione di “base” di uno spazio vettoriale qualsiasi che verrà studiata in seguito.

Definizione 14.1. Sia $n \geq 1$. Si chiama *base canonica* di \mathbb{K}^n la sequenza di n vettori

$$e_1, \dots, e_n$$

così definiti:

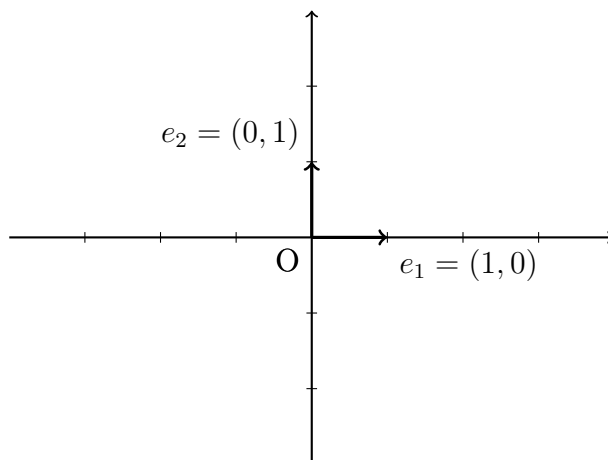
$$(4) \quad e_1 := (1, 0, \dots, 0), \quad e_2 := (0, 1, 0, \dots, 0), \dots, \quad e_n := (0, 0, \dots, 0, 1).$$

Dunque per ogni $j \in \{1, \dots, n\}$, il vettore e_j ha tutte le coordinate nulle tranne la j -ma che coincide con 1.

Ad esempio, la base canonica di \mathbb{K}^2 è costituita dai vettori

$$e_1 := (1, 0), \quad e_2 := (0, 1).$$

Nel caso $n = 1$, corrispondente al campo \mathbb{K} pensato come spazio vettoriale, abbiamo l'unico vettore $e_1 = 1$.



Illustriamo ora una proprietà fondamentale della base canonica:

Teorema 14.2. Ogni vettore $x = (x_1, \dots, x_n) \in \mathbb{K}^n$ si può scrivere in modo unico come combinazione lineare dei vettori della base canonica, nel modo seguente:

$$(5) \quad x = x_1 e_1 + \dots + x_n e_n = \sum_{i=1}^n x_i e_i,$$

le cui coefficienti della combinazione lineare essendo le coordinate stesse del vettore.

DIMOSTRAZIONE: La verifica di (5) è semplice: sviluppando il secondo membro abbiamo

$$\begin{aligned} x_1 e_1 + \cdots + x_n e_n &= \\ x_1(1, 0, \dots, 0) + x_2(0, 1, \dots, 0) + \cdots + x_n(0, 0, \dots, 0, 1) &= \\ (x_1, 0, \dots, 0) + (0, x_2, \dots, 0) + \cdots + (0, 0, \dots, 0, x_n) &= \\ (x_1 + 0 + \cdots + 0, 0 + x_2 + 0 + \cdots + 0, \dots, 0 + \cdots + 0 + x_n) &= \\ (x_1, x_2, \dots, x_n). \end{aligned}$$

Riguardo l'unicità della decomposizione, supponiamo che x si possa anche scrivere

$$x = \lambda_1 e_1 + \cdots + \lambda_n e_n$$

mediante altri coefficienti; osserviamo che in base a quanto appena provato, il secondo membro di questa uguaglianza altri non è che il vettore $(\lambda_1, \dots, \lambda_n)$, quindi abbiamo

$$(x_1, x_2, \dots, x_n) = (\lambda_1, \dots, \lambda_n)$$

e pertanto necessariamente $\lambda_i = x_i$ per ogni $i = 1, \dots, n$. \square

Come applicazione di questo risultato, determiniamo esplicitamente tutte le applicazioni lineari $\mathbb{K}^n \rightarrow \mathbb{K}$, dove $n \geq 1$ è un intero fissato.

Teorema 14.3. *Sia $n \geq 1$ un intero. Allora le applicazioni lineari $F : \mathbb{K}^n \rightarrow \mathbb{K}$ sono tutte e sole le funzioni del tipo*

$$(6) \quad F(x_1, \dots, x_n) := a_1 x_1 + \cdots + a_n x_n$$

l dove a_1, \dots, a_n sono delle costanti appartenenti al campo \mathbb{K} . Data inoltre una tale funzione, risulta $a_i = F(e_i)$.

DIMOSTRAZIONE: La dimostrazione del fatto che ogni funzione F del tipo (6) è effettivamente un'applicazione lineare può farsi direttamente, oppure si può far uso delle proiezioni $p_i : \mathbb{K}^n \rightarrow \mathbb{K}$, $i = 1, \dots, n$ e osservare che

$$F = a_1 p_1 + \cdots + a_n p_n.$$

Infatti per ogni x si ha $a_i p_i(x) = a_i p_i(x) = a_i x_i$ e quindi

$$F(x) = a_1 x_1 + \cdots + a_n x_n = a_1 p_1(x) + \cdots + a_n p_n(x) = (a_1 p_1 + \cdots + a_n p_n)(x).$$

Siccome le p_i sono lineari possiamo concludere che anche F è lineare.

Proviamo ora il viceversa. Sia assegnata ora un'applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}$. Utilizzando il fatto che

$$x = x_1 e_1 + \cdots + x_n e_n$$

otteniamo, applicando la Proposizione 12.5:

$$F(x) = x_1 F(e_1) + \cdots + x_n F(e_n)$$

da cui segue che F è della forma richiesta (6), ponendo $a_i := F(e_i)$ per ogni i .

Infine, data una qualsiasi funzione del tipo (6), è immediato dalla definizione che $F(e_i) = a_i$: infatti, l'unica coordinata non nulla di e_i è la i -ma e quindi

$$F(e_i) = a_1 \cdot 0 + \cdots + a_i \cdot 1 + \cdots + a_n \cdot 0 = a_i.$$

□

Vale la pena osservare esplicitamente che, stante il risultato appena provato, ogni funzione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}$ è completamente determinata dagli n scalari $a_i = F(e_i)$. La stessa cosa si può riformulare anche sotto forma di criterio di uguaglianza tra due funzioni lineari $F, G : \mathbb{K}^n \rightarrow \mathbb{K}$:

$$F = G \iff F(e_i) = G(e_i) \quad \forall i = 1, \dots, n.$$

Consideriamo ora lo spazio $\text{Hom}(\mathbb{K}^n, \mathbb{K}^m)$, determinandone in modo esplicito tutti gli elementi:

Teorema 14.4. *Dati due interi $n, m \geq 1$ le applicazioni lineari $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$ sono tutte e sole le funzioni del tipo*

$$(7) \quad F(x) := (F_1(x), \dots, F_m(x)), \quad \forall x = (x_1, \dots, x_n) \in \mathbb{K}^n,$$

dove le F_1, \dots, F_m sono tutte funzioni lineari $F_i : \mathbb{K}^n \rightarrow \mathbb{K}$.

Così, ad esempio le seguenti sono funzioni lineari $F \in \text{Hom}(\mathbb{R}^3, \mathbb{R}^2)$, e $G \in \text{Hom}(\mathbb{R}^2, \mathbb{R}^3)$:

$$F(x, y, z) = (x + 3y + z, y - \sqrt{3}z), \quad G(x, y) = (0, x + \frac{1}{3}y, x - y).$$

Nel caso di questa F abbiamo $F_1(x, y, z) = x + 3y + z$ e $F_2(x, y, z) = y - \sqrt{3}z$, tali funzioni $\mathbb{R}^3 \rightarrow \mathbb{R}$ essendo lineari in base al Teorema 14.3.

DIMOSTRAZIONE: Ogni funzione del tipo (7) è lineare, grazie alla linearità di tutte le F_i ; infatti dati $x, y \in \mathbb{K}^n$ e scalari λ, μ risulta:

$$\begin{aligned} F(\lambda x + \mu y) &= (F_1(\lambda x + \mu y), \dots, F_m(\lambda x + \mu y)) = \\ &= (\lambda F_1(x) + \mu F_1(y), \dots, \lambda F_m(x) + \mu F_m(y)) = \\ &= (\lambda F_1(x), \dots, \lambda F_m(x)) + (\mu F_1(y), \dots, \mu F_m(y)) = \\ &= \lambda(F_1(x), \dots, F_m(x)) + \mu(F_1(y), \dots, F_m(y)) = \\ &= \lambda F(x) + \mu F(y). \end{aligned}$$

Viceversa, sia assegnata una qualunque applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$; per ogni $x \in \mathbb{K}^n$, denotiamo con $F_1(x), \dots, F_m(x)$ le m coordinate del vettore $F(x) \in \mathbb{K}^m$, che sono univocamente determinate. Quindi restano definite m funzioni scalari $F_1, \dots, F_m : \mathbb{K}^n \rightarrow \mathbb{K}$: ciascuna F_i associa ad x la i -ma coordinata del vettore $F(x)$. Per costruzione, abbiamo pertanto:

$$F(x) = (F_1(x), \dots, F_m(x))$$

per ogni $x \in \mathbb{K}^n$. Resta da controllare che tali funzioni F_i sono lineari. Basta notare che esse non sono altro che le funzioni composte:

$$F_i = p_i \circ F,$$

dove per ogni $i = 1, \dots, m$, $p_i : \mathbb{K}^m \rightarrow \mathbb{K}$ è la i -ma proiezione

$$p_i(y_1, \dots, y_m) := y_i.$$

Per concludere basta utilizzare il fatto che la composizione di applicazioni lineari è lineare. \square

Data una funzione $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$ data dalla (7), scriveremo

$$F = (F_1, \dots, F_m)$$

e chiameremo le F_i le *funzioni componenti* di F .

Notiamo ancora esplicitamente che una funzione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$ è completamente determinata dai valori che assume sulla base canonica e_1, \dots, e_n di \mathbb{K}^n ; in altri termini, se $G : \mathbb{K}^n \rightarrow \mathbb{K}^m$ è un'altra applicazione lineare, allora

$$F = G \iff F(e_i) = G(e_i) \quad i = 1, \dots, n.$$

Questo segue immediatamente dall'analogo criterio di confronto per le funzioni coordinate F_i e G_i .

15. IL PRODOTTO RIGHE PER COLONNE TRA MATRICI

Si definisce ora un'operazione fondamentale tra matrici, detta prodotto righe per colonne; come vedremo, essa è strettamente correlata con l'operazione di composizione di applicazioni lineari.

Consideriamo dapprima il caso più semplice che coinvolge un vettore riga e un vettore colonna.

Definizione 15.1. Siano $A = (a_1 \ \dots \ a_n)$ un vettore riga e $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ un vettore

colonna della stessa lunghezza $n \geq 1$, a coefficienti nello stesso campo \mathbb{K} . Si definisce il loro **prodotto** AB come lo scalare

$$AB := a_1 b_1 + a_2 b_2 + \dots + a_n b_n \in \mathbb{K}.$$

È chiaro che questa operazione di prodotto è direttamente connessa con la nozione di applicazione lineare. Consideriamo infatti una generica applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}$. Sappiamo che una tale funzione è del tipo (6), ed è completamente determinata dagli n scalari a_1, \dots, a_n . Possiamo rappresentare quindi tale funzione

in modo sintetico mediante il vettore riga $(a_1 \cdots a_n)$, sapendo che, noto tale vettore, la funzione è ricostruita da

$$F(x) = a_1x_1 + \cdots + a_nx_n.$$

D'altra parte il secondo membro è semplicemente il prodotto tra $(a_1 \cdots a_n)$ e il

vettore colonna $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. Questo fatto suggerisce di definire, per ogni vettore

riga $A = (a_1 \cdots a_n)$ la seguente applicazione lineare

$$L_A = L_{(a_1 \cdots a_n)} : \mathbb{K}^n \rightarrow \mathbb{K}$$

definita ponendo, per ogni $x = (x_1, \dots, x_n)$:

$$L_A(x) := (a_1 \cdots a_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Così facendo ogni applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}$ è rappresentabile con questa notazione, cioè $F = L_{(a_1 \cdots a_n)}$ dove il vettore riga $(a_1 \cdots a_n)$ corrispondente è univocamente determinato e $a_i = F(e_i) = L_{(a_1 \cdots a_n)}(e_i)$.

La definizione di prodotto si estende al caso di due matrici di tipo generale nel modo seguente:

Definizione 15.2. Siano $A \in M_{m,n}(\mathbb{K})$ e $B \in M_{n,q}(\mathbb{K})$ due matrici tali che il numero di colonne di A coincida con il numero di righe di B . Si definisce **prodotto righe per colonne** o semplicemente **prodotto** di A per B la matrice di tipo $m \times q$ il cui elemento di posto (i, j) è dato dal prodotto della riga i -ma di A per la colonna j -ma di B . In simboli:

$$(8) \quad AB := (A^{(i)}B_{(j)}).$$

ESEMPIO 15.3. Posto $A = \begin{pmatrix} \sqrt{2} & 3 & -1 \\ 0 & 1 & 5 \end{pmatrix}$ e $B = \begin{pmatrix} 4 & \sqrt{2} & 0 \\ -2 & 1 & -2 \\ 0 & 1 & 0 \end{pmatrix}$, risulta che AB

è di tipo 2×3 e si calcola come segue:

$$AB = \begin{pmatrix} \sqrt{2} \cdot (4) + 3 \cdot (-2) + (-1) \cdot 0 & \sqrt{2} \cdot \sqrt{2} + 3 \cdot 1 + (-1) \cdot 1 & \sqrt{2} \cdot 0 + 3 \cdot (-2) + (-1) \cdot 0 \\ 0 \cdot 4 + 1 \cdot (-2) + 5 \cdot 0 & 0 \cdot \sqrt{2} + 1 \cdot 1 + 5 \cdot 1 & 0 \cdot 0 + 1 \cdot (-2) + 5 \cdot 0 \end{pmatrix}$$

$$AB = \begin{pmatrix} 4\sqrt{2} - 6 & 6 & -6 \\ -2 & 6 & -2 \end{pmatrix}.$$

Notiamo anche che in questo caso il prodotto BA non ha senso.

Utilizzando questa nozione di prodotto, anche la definizione delle funzioni L_A si generalizza come segue:

Definizione 15.4. Sia $A \in M_{m,n}(\mathbb{K})$ una matrice fissata; ad essa si associa un'applicazione

$$L_A : \mathbb{K}^n \rightarrow \mathbb{K}^m$$

definita come segue:

$$(9) \quad \forall x \in \mathbb{K}^n \quad L_A(x) := Ax.$$

Qui i vettori di \mathbb{K}^n e di \mathbb{K}^m sono identificati sempre con i corrispondenti *vettori colonna* ed il prodotto Ax è il prodotto righe per colonne.

Proposizione 15.5. Per ogni matrice $A \in M_{m,n}(\mathbb{K})$, l'applicazione $L_A : \mathbb{K}^n \rightarrow \mathbb{K}^m$ ad essa associata è lineare.

DIMOSTRAZIONE: Notiamo infatti che per ogni vettore colonna $x \in \mathbb{K}^n$ risulta

$$L_A(x) = Ax = \begin{pmatrix} A^{(1)}x \\ \vdots \\ A^{(m)}x \end{pmatrix},$$

e quindi

$$L_A(x) = (L_{A^{(1)}}(x), \dots, L_{A^{(m)}}(x)).$$

Pertanto, in base al Teorema 14.4, tale applicazione è lineare, in quanto tutte le sue funzioni componenti sono lineari.

□

A questo punto possiamo riformulare il Teorema 14.4 come segue:

Teorema 15.6. Tutte e sole le applicazioni lineari $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$ sono le funzioni del tipo

$$F = L_A$$

con $A \in M_{m,n}(\mathbb{K})$ matrice assegnata di tipo (m, n) .

Per provarlo, resta da giustificare che ogni $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$ lineare è del tipo $F = L_A$. Sappiamo che F è della forma

$$F(x) = (F_1(x), \dots, F_m(x)), \quad \forall x = (x_1, \dots, x_n) \in \mathbb{K}^n,$$

dove ciascuna F_i è lineare; ma a sua volta, come già stabilito sopra, F_i è del tipo

$$(10) \quad F_i = L_{u^i} \quad i = 1, \dots, m$$

per un certo vettore riga $u^i \in \mathbb{K}^n$. Consideriamo quindi la matrice

$$A := \begin{pmatrix} u^1 \\ \vdots \\ u^m \end{pmatrix}$$

che ha m righe (una per ogni funzione F_i) e n colonne. Per costruzione si ha immediatamente che $F = L_A$.

ESEMPIO 15.7. Data la matrice $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, allora la funzione L_A associata è $L_A : \mathbb{R}^3 \rightarrow \mathbb{R}^2$, data da

$$L_A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 + 2x_2 + 3x_3 \\ 4x_1 + 5x_2 + 6x_3 \end{pmatrix}$$

ovvero

$$L_A(x_1, x_2, x_3) = (x_1 + 2x_2 + 3x_3, 4x_1 + 5x_2 + 6x_3).$$

Facciamo qualche ulteriore osservazione sul prodotto righe per colonne.

Osservazione 15.8. a) Date le matrici $A \in M_{m,n}(\mathbb{K})$ e $B \in M_{n,q}(\mathbb{K})$ le righe e le colonne della matrice prodotto AB si possono ricavare come segue:

$$(AB)^{(i)} = A^{(i)}B$$

$$(AB)_{(j)} = AB_{(j)}.$$

La verifica è semplice conseguenza della definizione del prodotto; ad esempio:

$$(AB)^{(i)} = (A^{(i)}B_{(1)} \cdots A^{(i)}B_{(q)}) = A^{(i)}B.$$

b) Data $A \in M_{m,n}(\mathbb{K})$ le sue righe e colonne si possono ricostruire mediante moltiplicazione con i vettori della base canonica di \mathbb{K}^m e di \mathbb{K}^n ; precisamente si ha:

$$Ae_i = A_{(i)},$$

dove i vettori della base canonica di \mathbb{K}^n sono identificati con vettori colonna, mentre

$$e_i A = A^{(i)},$$

dove ciascun vettore della base canonica di \mathbb{K}^m è pensato come vettore riga.

Per giustificarlo, basta ricordare che per ogni vettore riga $u = (u_1 \dots u_n)$ si ha $(L_u)e_i = u_i$ e usare questo fatto per ogni riga di A :

$$Ae_i = \begin{pmatrix} A^{(1)}e_i \\ \vdots \\ A^{(m)}e_i \end{pmatrix} = \begin{pmatrix} L_{A^{(1)}}e_i \\ \vdots \\ L_{A^{(m)}}e_i \end{pmatrix} = \begin{pmatrix} a_i^1 \\ \vdots \\ a_i^m \end{pmatrix} = A_{(i)}.$$

Analogamente per ogni vettore colonna $\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$ si ha:

$$e_i \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = u_i.$$

Quindi

$$e_i A = (e_i A_{(1)} \cdots e_i A_{(n)}) = (a_1^i \cdots a_n^i) = A^{(i)}.$$

In particolare, abbiamo ottenuto, con riferimento all'applicazione lineare L_A , che

$$(11) \quad L_A(e_i) = A^{(i)}.$$

Riassumiamo quanto detto sin qui: data una generica applicazione lineare

$$F = (F_1, \dots, F_m) = L_A : \mathbb{K}^n \rightarrow \mathbb{K}^m,$$

la matrice A contiene le seguenti informazioni:

- Le righe corrispondono alle funzioni lineari componenti F_1, \dots, F_m , nel senso che ciascuna F_i è ricostruibile dalla corrispondente riga come $L_{A^{(i)}}$.
- Le colonne corrispondono alle immagini $F(e_i)$ dei vettori della base canonica dello spazio di partenza \mathbb{K}^n .

Inoltre, data $F = L_A$, è possibile calcolare $F(x)$ direttamente a partire dalle colonne di A , mediante la seguente relazione:

$$(12) \quad L_A(x) = x_1 A_{(1)} + x_2 A_{(2)} + \cdots + x_n A_{(n)},$$

che esprime ogni immagine $F(x)$ come combinazione lineare delle colonne della matrice.

Questa relazione è di dimostrazione immediata, sfruttando la (14.2) e tenendo conto della (11):

$$L_A(x) = L_A(x_1 e_1 + \cdots + x_n e_n) = x_1 F(e_1) + \cdots + x_n F(e_n) = x_1 A_{(1)} + \cdots + x_n A_{(n)}.$$

Proposizione 15.9. *Siano $A, B \in M_{m,n}(\mathbb{K})$ e $\lambda \in \mathbb{K}$. Allora:*

- 1) $A = B \iff L_A = L_B$.
- 2) $L_{A+B} = L_A + L_B$.
- 3) $L_{\lambda A} = \lambda L_A$.

DIMOSTRAZIONE: 1) L'implicazione \Rightarrow è ovvia. Supponiamo che $L_A = L_B$. Allora in particolare

$$Ae_i = Be_i$$

che si può riscrivere

$$A_{(i)} = B_{(i)}$$

e ciò comporta che $A = B$.

2) Si tratta di un'uguaglianza tra applicazioni lineari da \mathbb{K}^n in \mathbb{K}^m ; quindi basta verificare che esse assumano gli stessi valori quando applicate ai vettori della base canonica di \mathbb{K}^n ; risulta in effetti:

$$L_{A+B}(e_i) = (A+B)e_i = (A+B)_{(i)} = A_{(i)} + B_{(i)} = L_A(e_i) + L_B(e_i) = (L_A + L_B)(e_i).$$

La verifica di 3) è simile e si lascia per esercizio. \square

Proposizione 15.10. *Siano $A \in M_{m,n}(\mathbb{K})$ e $B \in M_{n,q}(\mathbb{K})$. Allora*

$$L_{AB} = L_A \circ L_B.$$

DIMOSTRAZIONE: Notiamo che $L_{AB} : \mathbb{K}^q \rightarrow \mathbb{K}^m$ e anche $L_A \circ L_B : \mathbb{K}^q \rightarrow \mathbb{K}^m$; anche in questo caso confrontiamo i valori assunti dalle due applicazioni lineari sui vettori della base canonica di \mathbb{K}^q ; tenendo conto della (15.8) si ha:

$$L_{AB}(e_i) = (AB)_{(i)} = AB_{(i)} = L_A(L_B(e_i)) = (L_A \circ L_B)(e_i).$$

\square

Come applicazione delle Proposizioni appena stabilite, siamo in grado di ricavare le seguenti proprietà basilari delle operazioni tra matrici:

Corollario 15.11. *Le operazioni di somma e prodotto tra matrici soddisfano:*

1) *Siano $A, B \in M_{m,n}(\mathbb{K})$, $C \in M_{n,q}(\mathbb{K})$ e $D \in M_{s,m}(\mathbb{K})$. Allora*

$$(A+B)C = AC + BC,$$

$$D(A+B) = DA + DB.$$

2) *Siano $A \in M_{m,n}(\mathbb{K})$, $B \in M_{n,q}(\mathbb{K})$ e $C \in M_{q,s}(\mathbb{K})$. Allora*

$$A(BC) = (AB)C.$$

DIMOSTRAZIONE: Tutte queste uguaglianze tra matrici si possono provare utilizzando il criterio fornito dalla 1) della Prop. 15.9, mostrando l'uguaglianza delle corrispondenti applicazioni lineari. Nel caso 1) si ha, ad esempio:

$$L_{(A+B)C} = L_{A+B} \circ L_C = (L_A + L_B) \circ L_C = L_A \circ L_C + L_B \circ L_C = L_{AC} + L_{BC} = L_{AC+BC}.$$

Quanto a 2):

$$L_{A(BC)} = L_A \circ L_{BC} = L_A \circ (L_B \circ L_C) = (L_A \circ L_B) \circ L_C = L_{AB} \circ L_C = L_{(AB)C}.$$

□

16. CLASSIFICAZIONE DEGLI SPAZI \mathbb{K}^n A MENO DI ISOMORFISMO

In questo paragrafo proviamo alcuni risultati significativi, su cui verrà basata la nozione di dimensione di uno spazio vettoriale. Cominciamo col provare che se $n > m$, lo spazio \mathbb{K}^n è “più grande” dello spazio \mathbb{K}^m ; cioè che non è possibile trovare una copia isomorfa del primo nel secondo.

Ricordiamo che due spazi vettoriali V e V' sono isomorfi se esiste almeno un isomorfismo tra essi; in tal caso scriviamo $V \cong V'$.

Proposizione 16.1. *Siano V, V' e V'' spazi vettoriali sullo stesso campo \mathbb{K} . Allora*

- a) $V \cong V$.
- b) $V \cong V' \Rightarrow V' \cong V$.
- c) $V \cong V' \wedge V' \cong V'' \Rightarrow V \cong V''$.

La prima affermazione si ottiene considerando l'applicazione identica $Id_V : V \rightarrow V$. È immediato che si tratta di un isomorfismo. Le c) e b) sono immediate conseguenze del fatto che la composizione di isomorfismi è un isomorfismo, e del fatto che l'inverso di un isomorfismo è anch'esso un isomorfismo.

Assegnato dunque un campo \mathbb{K} , la “relazione di isomorfismo” è una *relazione di equivalenza* sull'insieme di tutti i \mathbb{K} -spazi vettoriali. Ciò permette di “classificare” gli spazi vettoriali su \mathbb{K} disponendoli nelle classi di equivalenza corrispondenti. Dato uno spazio, la classe cui appartiene contiene tutti e soli gli spazi ad esso isomorfi, che potranno essere opportunamente identificati con esso. Nel seguito ci occuperemo di tale classificazione nel caso di spazi vettoriali di dimensione finita, dando un preciso significato matematico all'attributo “dimensione”.

Cominciamo dunque dalla classificazione, a meno di isomorfismo degli spazi \mathbb{K}^n .

Osserviamo che, intuitivamente ci aspettiamo che per m e n diversi, \mathbb{K}^m e \mathbb{K}^n siano spazi sostanzialmente diversi, dato il numero diverso di parametri scalari liberi che occorrono per individuarne univocamente i vettori. Anzi, pensando al caso $\mathbb{K} = \mathbb{R}$ e all'interpretazione geometrica di \mathbb{R}^2 e \mathbb{R}^3 come piano Euclideo e spazio Euclideo tridimensionale, è lecito ritenere che lo spazio di “dimensione più grande” contenga al suo interno qualche copia di quello “di dimensione più piccola”. In effetti non è difficile convincersi che, se $n \leq m$, tali copie esistono, ovvero più precisamente che \mathbb{K}^m contiene sempre qualche *sottospazio* vettoriale W isomorfo a \mathbb{K}^n , se $n \leq m$.

Ad esempio, un sottospazio vettoriale di \mathbb{R}^3 isomorfo a \mathbb{R}^2 è

$$W = \{(x, y, 0) : x, y \in \mathbb{R}\},$$

un isomorfismo essendo:

$$(x, y) \in \mathbb{R}^2 \mapsto (x, y, 0) \in W.$$

Si noti che questa applicazione è manifestamente una funzione lineare da \mathbb{R}^2 in \mathbb{R}^3 , che possiamo considerare a valori in W , conservando il carattere di linearità.

Per costruire un tale W in generale, assumendo $n \leq m$ è sufficiente considerare l'applicazione lineare

$$F : \mathbb{K}^n \rightarrow \mathbb{K}^m$$

definita da

$$F(x_1, \dots, x_n) := (x_1, \dots, x_n, 0, \dots, 0).$$

È chiaro che le funzioni componenti di F sono lineari (si tratta di $(p_1, \dots, p_n, 0, \dots, 0)$, dove le p_i sono proiezioni e le restanti funzioni nulle), per cui F è lineare. Tale funzione è ingettiva perchè se $(x_1, \dots, x_n) \in \text{Ker}(F)$, allora

$$(x_1, \dots, x_n, 0, \dots, 0) = (0, \dots, 0)$$

e quindi $x_1 = \dots = x_n = 0$. Dunque il $\text{Ker}(F)$ è banale.

Il sottospazio $W := \text{Im}(F)$ di \mathbb{K}^m è allora isomorfo a \mathbb{K}^n mediante la ridotta di questa funzione:

$$F : \mathbb{K}^n \rightarrow \text{Im}(F),$$

che è automaticamente anche surgettiva, oltre che ingettiva.

L'intuizione suggerisce invece che questo tipo di costruzione non sia possibile se $n > m$. Proveremo ciò rigorosamente. Prima di procedere, è opportuno includere nella famiglia degli spazi vettoriali \mathbb{K}^n anche lo spazio \mathbb{K}^0 :

Definizione 16.2. Dato un campo \mathbb{K} , denoteremo con \mathbb{K}^0 il sottospazio banale $\{0_{\mathbb{K}}\}$ di \mathbb{K} , detto anch'esso spazio vettoriale banale o 0-dimensionale canonico sul campo \mathbb{K} .

Ciò premesso, sussiste il seguente:

Teorema 16.3. *Siano n, m interi con $n > m \geq 0$. Allora non esistono applicazioni lineari ingettive $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$.*

Prima di procedere con la dimostrazione, cominciamo con qualche osservazione preliminare. Data un'applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}$, $n \geq 2$,

$$F(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$$

tale che $a_1 = 0$ allora F è del tipo:

$$F(x) = a_2x_2 + \dots + a_nx_n.$$

e diremo quindi che F non dipende da x_1 ; in tal caso F si può trattare come una funzione lineare $\bar{F} : \mathbb{K}^{n-1} \rightarrow \mathbb{K}$; più precisamente denotiamo con $\bar{F} : \mathbb{K}^{n-1} \rightarrow \mathbb{K}$ l'applicazione lineare definita da:

$$\bar{F}(y_1, \dots, y_n) = a_2y_1 + \dots + a_ny_n.$$

Allora per ogni $x \in \mathbb{K}^n$, posto $\bar{x} = (x_2, \dots, x_n)$ abbiamo che:

$$F(x) = \bar{F}(\bar{x}).$$

Notiamo anche che la condizione che F non dipenda da x_1 è equivalente a $F(e_1) = 0$ perchè a priori si ha sempre, come sappiamo, $a_1 = F(e_1)$.

Lemma 16.4. *Siano $F : \mathbb{K}^n \rightarrow \mathbb{K}^n$ e $G : \mathbb{K}^n \rightarrow \mathbb{K}$ due applicazioni lineari, $n \geq 2$. Allora l'applicazione lineare $F(e_1)G - G(e_1)F : \mathbb{K}^n \rightarrow \mathbb{K}$ non dipende da x_1 .*

La dimostrazione di questo Lemma è immediata: si ha infatti

$$(F(e_1)G - G(e_1)F)(e_1) = F(e_1)G(e_1) - G(e_1)F(e_1) = 0.$$

Nel seguito, per ogni vettore $\bar{x} \in \mathbb{K}^{n-1}$, $\bar{x} = (\bar{x}_1, \dots, \bar{x}_{n-1})$, denotiamo per ogni $x_1 \in \mathbb{K}$ con (x, \bar{x}) il vettore $(x_1, \bar{x}_1, \dots, \bar{x}_{n-1})$ di \mathbb{K}^n .

Lemma 16.5. *Data un'applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}$, con $n \geq 2$, che dipende da x_1 , cioè tale che $F(e_1) \neq 0$ e un vettore $\bar{x} \in \mathbb{K}^{n-1}$, esiste sempre $x_1 \in \mathbb{K}$ tale che:*

$$F(x_1, \bar{x}) = 0.$$

DIMOSTRAZIONE: Infatti, abbiamo:

$$F(x_1, \bar{x}) = a_1 x_1 + a_2 \bar{x}_1 + \dots + a_n \bar{x}_{n-1},$$

e quindi affinché si abbia $F(x_1, \bar{x}) = 0$, si tratta di risolvere l'equazione:

$$a_1 x_1 + a_2 \bar{x}_1 + \dots + a_n \bar{x}_{n-1} = 0,$$

che, essendo per ipotesi $a_1 \neq 0$, ammette l'unica soluzione:

$$x_1 := -\frac{1}{a_1} (a_2 \bar{x}_1 + \dots + a_n \bar{x}_{n-1}).$$

□

Ciò premesso, discutiamo la dimostrazione del Teorema 16.3. Ragionando per induzione su $n \geq 1$, proviamo che ogni applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$ con $0 \leq m < n$ non è iniettiva. Ciò si può riformulare come segue: per ogni $n \geq 1$, ogni applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$ con $0 \leq m < n$ ha nucleo non banale. Il passo base ($n = 1$) consiste nell'esaminare un'applicazione lineare

$$F : \mathbb{K} \rightarrow \mathbb{K}^0$$

cioè

$$F : \mathbb{K} \rightarrow \{0_{\mathbb{K}}\}.$$

Tale applicazione è necessariamente costante, ovvero è la funzione nulla $F = 0$. Essa non è certamente iniettiva, in quanto il campo \mathbb{K} contiene, oltre lo 0, almeno l'elemento $1 \neq 0$, per cui $F(1) = 0$.

Sia $n > 1$ e proviamo l'asserto, assumendolo vero per $n - 1$. Anche in questo caso, se $m = 0$, non c'è nulla da provare in quanto l'unica applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}^0$ è la funzione nulla $F = 0$, che non è iniettiva. Supponiamo quindi $m > 0$. Sappiamo dal Teorema 14.4 che F è della forma

$$F(x) := (F_1(x), \dots, F_m(x)), \quad \forall x = (x_1, \dots, x_n) \in \mathbb{K}^n,$$

dove le $F_i : \mathbb{K}^n \rightarrow \mathbb{K}$ sono lineari. Se $m = 1$, si tratta ancora di un'applicazione lineare $F : \mathbb{K}^n \rightarrow \mathbb{K}$, e la prova che il nucleo di F è non banale è immediata; infatti, se $F(e_1) = 0$ non c'è nulla da provare, altrimenti basta applicare il Lemma 16.5 a partire da un qualsiasi vettore non nullo $\bar{x} \in \mathbb{K}^{n-1}$.

Trattiamo quindi il caso $m > 1$. Se $F(e_1) = 0$, si ha la tesi; altrimenti deve esistere una funzione componente F_i per cui $F_i(e_1) \neq 0$. A meno di scambiare due delle funzioni componenti F_1, \dots, F_m , senza con questo alterare il nucleo di F , possiamo supporre che $F_1(e_1) \neq 0$. Allora, posto $\alpha = F_1(e_1)$ abbiamo che tutte le funzioni:

$$\alpha F_i - F_i(e_1) F_1, \quad i = 2, \dots, m$$

non dipendono da x_1 (Lemma 16.4). Denotate con $G_i : \mathbb{K}^n \rightarrow \mathbb{K}$ queste funzioni, possiamo applicare l'ipotesi induttiva all'applicazione lineare:

$$G = (\bar{G}_2, \dots, \bar{G}_m) : \mathbb{K}^{n-1} \rightarrow \mathbb{K}^{m-1}.$$

Ciò è possibile perchè $0 \leq m-1 < n-1$. Quindi esiste un vettore $\bar{x} = (\bar{x}_2, \dots, \bar{x}_n) \in \mathbb{K}^{n-1}$, $\bar{x} \neq 0$, tale che $G(\bar{x}) = 0$. Sfrutteremo questo vettore per determinare un vettore non nullo nel nucleo di F . Scegliamo a tal scopo $x_1 \in \mathbb{K}$ in modo che

$$F_1(x_1, \bar{x}) = 0,$$

il che è sempre possibile applicando il Lemma 16.5. Con questa scelta risulta che il vettore non nullo $(x_1, \bar{x}) \in \mathbb{K}^n$ appartiene al nucleo di F ; infatti, poichè \bar{x} appartiene a $\text{Ker}(G)$ risulta, per ogni $i = 2, \dots, m$:

$$0 = \bar{G}_i(\bar{x}) = G_i(x_1, \bar{x}) = \alpha F_i(x_1, \bar{x}) - F_i(e_1) F_1(x_1, \bar{x}) = \alpha F_i(x_1, \bar{x}).$$

Pertanto possiamo concludere che $F_i(x_1, \bar{x}) = 0$ per ogni $i = 2, \dots, m$, ancora tenendo conto del fatto che $\alpha \neq 0$. \square .

Corollario 16.6. *(Teorema di classificazione) Siano \mathbb{K} un campo e $n, m \in \mathbb{N}$. Allora*

$$\mathbb{K}^n \cong \mathbb{K}^m \text{ se e solo se } n = m.$$

La dimostrazione è un'immediata applicazione del risultato precedente: infatti, se $\mathbb{K}^n \cong \mathbb{K}^m$, allora dev'essere $n = m$ perchè, fissato un isomorfismo $F : \mathbb{K}^n \rightarrow \mathbb{K}^m$, è impossibile che si abbia $n > m$, ma considerando l'isomorfismo inverso $F^{-1} : \mathbb{K}^m \rightarrow \mathbb{K}^n$, è anche impossibile che $m > n$.

Corollario 16.7. *Fissato un campo \mathbb{K} e due interi $n > m$, non esiste alcun sottospazio vettoriale W di \mathbb{K}^m isomorfo a \mathbb{K}^n .*

Infatti, supponiamo che un tale sottospazio W esista e sia $F : \mathbb{K}^n \rightarrow W$ un isomorfismo. Allora la funzione composta

$$i \circ F : \mathbb{K}^n \rightarrow \mathbb{K}^m$$

con $i : W \rightarrow \mathbb{K}^m$ l'inclusione canonica di W in \mathbb{K}^m , ovvero $i = Id|_W : W \rightarrow \mathbb{K}^m$, con Id applicazione identica di \mathbb{K}^m , sarebbe un'applicazione lineare iniettiva, il che è impossibile essendo $n > m$.

17. SPAZI VETTORIALI FINITAMENTE GENERATI

Definizione 17.1. Sia V un \mathbb{K} -spazio vettoriale. Una sequenza finita v_1, \dots, v_m di vettori di V , $m \geq 1$, è detta **sistema di generatori** di V se ogni vettore v di V si può esprimere come combinazione lineare dei vettori della sequenza, ovvero se per ogni $v \in V$ esistono scalari $\lambda_1, \dots, \lambda_m \in \mathbb{K}$ tali che

$$v = \lambda_1 v_1 + \dots + \lambda_m v_m.$$

Osserviamo che la condizione in esame si può sintetizzare come segue; una sequenza $A = \{v_1, \dots, v_m\}$ è un sistema di generatori di V se e solo se:

$$V = L(v_1, \dots, v_m).$$

Mediante questa nozione introduciamo la classe di spazi vettoriali che saranno studiati sistematicamente nel seguito.

Definizione 17.2. Uno spazio vettoriale V sul campo \mathbb{K} si dice **finitamente generato** oppure **di dimensione finita** se ammette un sistema di generatori (finito) v_1, \dots, v_m .

ESEMPIO 17.3. Ogni spazio \mathbb{K}^n è finitamente generato: ciò è ovvio se $n = 0$; se $n > 0$, sappiamo dalla (5) che ogni vettore è combinazione lineare dei vettori della base canonica $\{e_1, \dots, e_n\}$ introdotta nel §14.

ESEMPIO 17.4. Consideriamo lo spazio vettoriale reale V costituito da *tutti* i polinomi di una variabile reale:

$$V = \{p : \mathbb{R} \rightarrow \mathbb{R} \mid p = p(x) \text{ è un polinomio}\}.$$

e il sottoinsieme:

$$W = \{p : \mathbb{R} \rightarrow \mathbb{R} \mid p = p(x) \text{ è un polinomio di grado } \leq 3\}.$$

Certamente W non è vuoto, e poichè la somma $p + q$ di due polinomi di grado al massimo 3 è anch'esso un polinomio dello stesso tipo, e analogamente per λp , con λ costante, risulta che W è un sottospazio vettoriale di V . In particolare, anche W è un \mathbb{R} -spazio vettoriale.

Risulta che

$$W = L(1, x, x^2, x^3)$$

per cui W è finitamente generato. Infatti ogni polinomio $p \in W$ è una funzione del tipo

$$p(x) = a_0 \cdot 1 + a_1x + a_2x^2 + a_3x^3,$$

dove gli $a_i \in \mathbb{R}$ sono costanti.

Invece lo spazio V *non* è finitamente generato. Infatti, ammettiamo per assurdo che esista un sistema di generatori p_1, \dots, p_m di W : allora ogni polinomio $p : \mathbb{R} \rightarrow \mathbb{R}$ sarebbe della forma

$$p = \lambda_1 p_1 + \dots + \lambda_m p_m$$

per opportune costanti λ_i . Detto M il grado massimo dei polinomi p_1, \dots, p_m seguirebbe da ciò che il grado di *ogni* polinomio p è al massimo M . Ciò è evidentemente impossibile, ad esempio il polinomio x^{M+1} ha grado $M+1$.

Vediamo ora che c'è uno stretto legame tra la nozione di sistema di generatori e quella di epimorfismo.

In corrispondenza di una successione finita $A = \{v_1, \dots, v_m\}$ di vettori qualsiasi di un \mathbb{K} -spazio vettoriale V possiamo definire un'applicazione

$$\varphi_A : \mathbb{K}^m \rightarrow V$$

nel modo seguente:

$$(13) \quad \varphi_A(\lambda_1, \dots, \lambda_m) := \lambda_1 v_1 + \dots + \lambda_m v_m.$$

Risulta che φ_A è un'applicazione lineare: la verifica è sostanzialmente la stessa che è stata discussa per giustificare che $L(v_1, \dots, v_m)$ è un sottospazio: infatti, dati i vettori $(\lambda_1, \dots, \lambda_m)$ e (μ_1, \dots, μ_m) di \mathbb{K}^m , allora:

$$\begin{aligned} \varphi_A((\lambda_1, \dots, \lambda_m) + (\mu_1, \dots, \mu_m)) &= \varphi_A((\lambda_1 + \mu_1, \dots, \lambda_m + \mu_m)) = \\ &= (\lambda_1 + \mu_1)v_1 + \dots + (\lambda_m + \mu_m)v_m = \\ &= (\lambda_1 v_1 + \dots + \lambda_m v_m) + (\mu_1 v_1 + \dots + \mu_m v_m) = \\ &= \varphi_A(\lambda_1, \dots, \lambda_m) + \varphi_A(\mu_1, \dots, \mu_m). \end{aligned}$$

Il lettore può agevolmente completare la verifica della linearità di φ_A tenendo conto della (3).

Notiamo anche che, per costruzione:

$$Im(\varphi_A) = L(v_1, \dots, v_m).$$

Consegue che sussiste la seguente utile caratterizzazione dei sistemi di generatori:

Proposizione 17.5. *Data una sequenza $A = \{v_1, \dots, v_m\}$ di vettori di uno spazio vettoriale V , allora:*

$$v_1, \dots, v_m \text{ è un sistema di generatori di } V \iff \varphi_A \text{ è surgettiva.}$$

DIMOSTRAZIONE: Infatti, dire che v_1, \dots, v_m è un sistema di generatori di V significa, per definizione, che $V = L(v_1, \dots, v_m) = \text{Im}(\varphi_A)$ il che è vero se e solo se φ_A è surgettiva. \square

18. VETTORI LINEARMENTE DIPENDENTI E LINEARMENTE INDIPENDENTI

Sia V uno spazio vettoriale sul campo \mathbb{K} .

Definizione 18.1. Si dice che i vettori v_1, \dots, v_m di V sono *linearmente dipendenti* se esistono m scalari **non tutti nulli** tali che:

$$\lambda_1 v_1 + \dots + \lambda_m v_m = 0_V.$$

Si introduce a questo proposito la seguente terminologia:

Definizione 18.2. Una combinazione lineare

$$\lambda_1 v_1 + \dots + \lambda_m v_m$$

di vettori di V verrà detta:

- nulla* se coincide con il vettore nullo, cioè se $\lambda_1 v_1 + \dots + \lambda_m v_m = 0_V$.
- banale* se tutti i coefficienti λ_i sono uguali a 0.

Con questa terminologia, i vettori v_1, \dots, v_m sono linearmente dipendenti se esiste una loro combinazione lineare nulla ma **non banale**.

Osserviamo esplicitamente che ogni combinazione lineare banale è sempre nulla, ma il viceversa può non essere vero: ad esempio, la seguente combinazione lineare

$$(1, 1) - \frac{1}{3}(3, 3)$$

dei vettori $(1, 1)$ e $(3, 3)$ di \mathbb{R}^2 è nulla, ma non è banale. Pertanto i vettori in questione sono linearmente dipendenti.

ESEMPIO 18.3. I vettori $(1, 0, -1)$, $(0, 2, 3)$, $(2, 2, 1)$ di \mathbb{R}^3 sono linearmente dipendenti.

Per stabilire ciò cerchiamo di determinarne una combinazione lineare nulla non banale, imponendo

$$\lambda_1(1, 0, -1) + \lambda_2(0, 2, 3) + \lambda_3(2, 2, 1) = 0.$$

Si tratta di stabilire se il seguente sistema di equazioni lineari ammette una soluzione non banale $(\lambda_1, \lambda_2, \lambda_3)$:

$$\begin{cases} \lambda_1 + 2\lambda_3 = 0 \\ 2\lambda_2 + 2\lambda_3 = 0 \\ -\lambda_1 + 3\lambda_2 + \lambda_3 = 0 \end{cases}.$$

Risolviendo con il metodo di sostituzione, otteniamo

$$\begin{cases} \lambda_1 = -2\lambda_3 \\ \lambda_2 = -\lambda_3 \\ 0 = 0 \end{cases} .$$

Quindi tutte le soluzioni sono le terne $(-2\lambda_3, -\lambda_3, \lambda_3)$ al variare della variabile libera λ_3 . Ponendo ad es. $\lambda_3 = 1$ otteniamo una soluzione non banale, corrispondente alla seguente combinazione lineare nulla non banale dei tre vettori:

$$-2(1, 0, -1) - (0, 2, 3) + (2, 2, 1) = 0.$$

Analogamente a quanto fatto in merito ai sistemi di generatori, possiamo utilizzare ancora la funzione φ_A per caratterizzare la nozione di dipendenza lineare tra vettori:

Proposizione 18.4. *Si consideri una successione finita $A = \{v_1, \dots, v_m\}$, $m \geq 1$ di vettori dello spazio V . Allora:*

$$v_1, \dots, v_m \text{ sono linearmente dipendenti} \iff \varphi_A \text{ non è iniettiva.}$$

DIMOSTRAZIONE: Per definizione, v_1, \dots, v_m sono linearmente dipendenti se e solo se esiste un vettore $(\lambda_1, \dots, \lambda_m) \in \mathbb{K}^m$, $(\lambda_1, \dots, \lambda_m) \neq (0, \dots, 0)$, tale che:

$$\lambda_1 v_1 + \dots + \lambda_m v_m = 0_V,$$

cioè

$$\varphi_A(\lambda_1, \dots, \lambda_m) = 0_V,$$

ovvero tale che

$$(\lambda_1, \dots, \lambda_m) \in \text{Ker}(\varphi_A).$$

In conclusione, abbiamo provato che v_1, \dots, v_m sono linearmente dipendenti se e solo se $\text{Ker}(\varphi_A) \neq \{0_{\mathbb{K}^m}\}$, da cui l'asserto. \square

Definizione 18.5. Diremo che i vettori v_1, \dots, v_m sono **linearmente indipendenti** se non sono linearmente dipendenti.

Dunque v_1, \dots, v_m sono linearmente indipendenti se e solo se ogni relazione del tipo

$$\lambda_1 v_1 + \dots + \lambda_m v_m = 0_V$$

implica sempre che $\lambda_1 = \dots = \lambda_m = 0$, ovvero:

$$\forall (\lambda_1, \dots, \lambda_m) \in \mathbb{K}^m : \lambda_1 v_1 + \dots + \lambda_m v_m = 0 \Rightarrow \lambda_1 = \dots = \lambda_m = 0.$$

Ovviamente, data una sequenza $A = \{v_1, \dots, v_m\}$, sussiste la caratterizzazione:

$$v_1, \dots, v_m \text{ sono linearmente indipendenti} \iff \varphi_A \text{ è un monomorfismo.}$$

Osservazione 18.6. Una terminologia molto in uso in algebra lineare è la seguente: se v_1, \dots, v_m sono vettori linearmente indipendenti, allora l'insieme $A = \{v_1, \dots, v_m\}$ è detto *libero*.

19. BASI

Introduciamo ora una nozione cruciale per lo studio degli spazi vettoriali finitamente generati.

Definizione 19.1. Sia V uno spazio vettoriale sul campo \mathbb{K} . Una sequenza finita di vettori $\{v_1, \dots, v_n\}$ si dice **base** di V se:

- 1) v_1, \dots, v_n costituiscono un sistema di generatori di V .
- 2) v_1, \dots, v_n sono linearmente indipendenti.

ESEMPIO 19.2. La base canonica $\{e_1, \dots, e_n\}$ di \mathbb{K}^n è effettivamente una base nel senso della definizione precedente; osserviamo che l'indipendenza dei vettori e_1, \dots, e_n è ancora conseguenza immediata dell'identità fondamentale (5): infatti, data una combinazione lineare nulla

$$\lambda_1 e_1 + \dots + \lambda_n e_n = 0_{\mathbb{K}^n}$$

il vettore al primo membro si riscrive:

$$(\lambda_1, \dots, \lambda_n) = 0_{\mathbb{K}^n},$$

e quindi necessariamente tutti i coefficienti λ_i sono nulli.

ESEMPIO 19.3. Una base dello spazio vettoriale $M_2(\mathbb{K})$ è costituita dalla sequenza di matrici:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Ragionando in modo simile al caso della base canonica di \mathbb{K}^4 , ciò si giustifica tenendo conto del fatto che per ogni matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{K})$ si ha:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

In base a quanto stabilito nei paragrafi precedenti, considerata una sequenza di vettori $\mathfrak{B} = \{v_1, \dots, v_n\}$, abbiamo:

$$\mathfrak{B} \text{ è base di } V \iff \varphi_{\mathfrak{B}} : \mathbb{K}^n \rightarrow V \text{ è un isomorfismo.}$$

Un'applicazione molto importante di ciò e del Teorema di classificazione 16.6 è il risultato seguente, che stabilisce che due basi sono sempre necessariamente costituite dallo stesso numero di vettori:

Teorema 19.4. *Siano $\mathfrak{B} = \{v_1, \dots, v_n\}$ e $\mathfrak{C} = \{w_1, \dots, w_m\}$ due basi di un \mathbb{K} -spazio vettoriale V . Allora:*

$$n = m.$$

DIMOSTRAZIONE: Infatti, in corrispondenza della base \mathfrak{B} abbiamo l'isomorfismo $\varphi_{\mathfrak{B}} : \mathbb{K}^n \rightarrow V$, mentre in corrispondenza dell'altra base \mathfrak{C} abbiamo l'isomorfismo $\varphi_{\mathfrak{C}} : \mathbb{K}^m \rightarrow V$. Ne segue che $\mathbb{K}^n \cong \mathbb{K}^m$, e quindi necessariamente $n = m$. \square

20. PROPRIETÀ DEI VETTORI LINEARMENTE INDIPENDENTI

In questo paragrafo approfondiamo alcune proprietà utili relative al concetto di (in)dipendenza lineare tra vettori. Cominciamo con l'osservare che, se una sequenza di vettori v_1, \dots, v_n contiene il vettore nullo, allora sicuramente i vettori sono linearmente dipendenti.

Infatti, se $v_j = 0$, allora

$$0v_1 + \dots + 0v_{j-1} + v_j + 0v_{j+1} + \dots + 0v_n = 0.$$

Lo stesso dicasi se due dei vettori della sequenza concidono; se ad es. $v_i = v_j$ con $i < j$ due indici fissati, allora

$$v_i - v_j = 0$$

e quindi $v_i - v_j$ è una combinazione lineare nulla non banale di v_1, \dots, v_n (si sottintende qui che i coefficienti che moltiplicano i vettori della sequenza di indice diverso da i e j sono tutti uguali a 0).

Si osserva anche che ogni sottosequenza v_{i_1}, \dots, v_{i_k} di una sequenza di vettori linearmente indipendenti v_1, \dots, v_n conserva il carattere di lineare indipendenza. Ciò perchè ogni combinazione lineare $\lambda_1 v_{i_1} + \dots + \lambda_k v_{i_k}$ dei vettori della sottosequenza è anche una combinazione lineare dei vettori della sequenza originale v_1, \dots, v_n . In altri termini, ogni sottoinsieme di un insieme libero di vettori è libero.

Sussiste la seguente caratterizzazione:

Proposizione 20.1. *Siano assegnati i vettori v_1, \dots, v_m dello spazio vettoriale V . Le seguenti proprietà sono equivalenti:*

- a) v_1, \dots, v_m sono linearmente dipendenti.
- b) Almeno uno dei vettori v_1, \dots, v_m è combinazione lineare degli altri.

DIMOSTRAZIONE: $a) \Rightarrow b)$. Si assuma che v_1, \dots, v_m siano linearmente dipendenti; allora esiste una combinazione lineare nulla:

$$\lambda_1 v_1 + \dots + \lambda_m v_m = 0_V$$

non banale; supponiamo che $\lambda_j \neq 0$; allora utilizzando l'inverso di λ_j possiamo ricavare v_j dalla relazione precedente ottenendo

$$v_j = -\lambda_j^{-1} \lambda_1 v_1 - \dots - \lambda_j^{-1} \lambda_{j-1} v_{j-1} - \lambda_j^{-1} \lambda_{j+1} v_{j+1} - \dots - \lambda_j^{-1} \lambda_m v_m.$$

e ciò prova b).

b) \Rightarrow a). Per ipotesi esiste $j \in \{1, \dots, m\}$ tale che

$$v_j = \alpha_1 v_1 + \dots + \alpha_{j-1} v_{j-1} + \alpha_{j+1} v_{j+1} + \dots + \alpha_m v_m$$

per opportuni scalari α_i . Si ottiene pertanto:

$$0_V = \alpha_1 v_1 + \dots + \alpha_{j-1} v_{j-1} - v_j + \alpha_{j+1} v_{j+1} + \dots + \alpha_m v_m$$

il che mostra l'esistenza di una combinazione lineare nulla non banale dei vettori v_1, \dots, v_m , dandosi che $-1 \neq 0$. \square

Il risultato seguente è molto utilizzato; fornisce una condizione sufficiente affinché si possa "allungare" una sequenza libera, aggiungendo un altro vettore, conservando la lineare indipendenza:

Proposizione 20.2. *Siano v_1, \dots, v_s vettori linearmente indipendenti. Allora, se $v \notin L(v_1, \dots, v_s)$, anche i vettori v_1, \dots, v_s, v sono linearmente indipendenti.*

DIMOSTRAZIONE: Siano $\lambda_1, \dots, \lambda_{s+1} \in \mathbb{K}$ tali che

$$\lambda_1 v_1 + \dots + \lambda_s v_s + \lambda_{s+1} v = 0.$$

Cominciamo con l'osservare che non può essere $\lambda_{s+1} \neq 0$ perchè altrimenti si ricaverebbe

$$v = -\lambda_{s+1}^{-1} \lambda_1 v_1 - \dots - \lambda_{s+1}^{-1} \lambda_s v_s$$

contro il fatto che $v \notin L(v_1, \dots, v_s)$. Dunque $\lambda_{s+1} = 0$ e si ottiene:

$$\lambda_1 v_1 + \dots + \lambda_s v_s = 0,$$

da cui $\lambda_1 = \dots = \lambda_s = 0$ perchè i vettori v_1, \dots, v_s sono linearmente indipendenti. \square

21. ESISTENZA DI BASI

In questo paragrafo proviamo che ogni spazio vettoriale finitamente generato è sempre dotato di basi.

Vi è un caso particolare che merita un'osservazione preliminare.

Definizione 21.1. Uno spazio vettoriale V è detto **banale** se $V = \{0_V\}$.

Un tale spazio è ovviamente finitamente generato. Ma in esso non esistono vettori linearmente indipendenti. Si converrà pertanto che ogni spazio banale *ha dimensione 0 e che l'insieme vuoto \emptyset è la sua unica base.*

Veniamo al caso di spazi vettoriali finitamente generati non banali. Descriveremo un algoritmo mediante il quale è sempre possibile estrarre da un sistema di generatori assegnato v_1, \dots, v_m , $m \geq 1$, una base $\{v_{i_1}, \dots, v_{i_n}\}$ con $1 \leq i_1 < \dots < i_n \leq m$ e $n \geq 1$. A tale scopo, introduciamo la seguente terminologia:

Definizione 21.2. Sia V uno spazio vettoriale sul campo \mathbb{K} e sia v_1, \dots, v_m un sistema di generatori di V . Sia $i \in \{1, \dots, m\}$. Il vettore v_i si dirà **eliminabile** se esso è combinazione lineare dei vettori che lo precedono, ovvero se

$$v_i \in L(v_1, \dots, v_{i-1}).$$

Altrimenti v_i si dirà **non eliminabile**.

Per $i = 1$, il sottospazio $L(v_1, \dots, v_{i-1})$ va inteso $\{0_V\}$, e quindi per definizione v_1 è eliminabile se e solo se è il vettore nullo.

Teorema 21.3. Sia V un \mathbb{K} -spazio vettoriale finitamente generato non banale. Dato un sistema di generatori v_1, \dots, v_m , siano

$$v_{i_1}, \dots, v_{i_n}, \quad 1 \leq i_1 < \dots < i_n \leq m$$

i vettori non eliminabili da esso. Allora $\mathfrak{B} = \{v_{i_1}, \dots, v_{i_n}\}$ è una base di V .

La base \mathfrak{B} così costruita si dice estratta dal sistema di generatori v_1, \dots, v_m mediante l'algoritmo di eliminazione o algoritmo degli scarti successivi.

DIMOSTRAZIONE: Mostriamo innanzitutto che se V è uno spazio vettoriale non banale, ogni sistema di generatori v_1, \dots, v_m contiene qualche vettore non eliminabile. Infatti, se tali vettori fossero tutti eliminabili, avremmo

$$V = L(v_1, \dots, v_m) \subset L(v_1, \dots, v_{m-1})$$

perchè tutti i vettori v_i appartengono al sottospazio $L(v_1, \dots, v_{m-1})$, stante l'eliminabilità di v_m ; da qui l'inclusione (si applichi la Prop. 10.2). Per lo stesso motivo, essendo anche v_{m-1} eliminabile, si ha:

$$V = L(v_1, \dots, v_m) \subset L(v_1, \dots, v_{m-1}) \subset L(v_1, \dots, v_{m-2}).$$

Ripetendo questo argomento più volte si ottiene in definitiva

$$V \subset L(v_1);$$

ma $v_1 = 0_V$ essendo eliminabile, per cui si avrebbe

$$V = L(0_V) = \{0_V\}$$

contro l'ipotesi.

Ciò premesso, proviamo che \mathfrak{B} è una base ragionando per induzione sulla lunghezza m della lista di vettori assegnata.

Nel caso $m = 1$, abbiamo per ipotesi

$$V = L(v_1)$$

e l'unico vettore v_1 della sequenza dev'essere necessariamente non eliminabile, perchè altrimenti si avrebbe $v_1 = 0$ e quindi $V = \{0_V\}$. Ora, $\mathfrak{B} = \{v_1\}$ è una base in quanto $\{v_1\}$ è un insieme libero avendosi, per ogni scalare λ :

$$\lambda v_1 = 0 \Rightarrow \lambda = 0$$

perchè $v_1 \neq 0$.

Supponiamo ora $m > 1$ e l'asserto vero per $m - 1$. Consideriamo il sottospazio $W = L(v_1, \dots, v_{m-1})$ di V e la sequenza v_1, \dots, v_{m-1} che ne costituisce un sistema di generatori.

Osserviamo che, se W è banale, allora $v_1 = \dots = v_{m-1} = 0_V$ e quindi

$$V = L(v_1, \dots, v_{m-1}, v_m) = L(0_V, \dots, 0_V, v_m) = L(v_m)$$

e, ragionando come sopra, v_m dev'essere non eliminabile e $\mathfrak{B} = \{v_m\}$ è una sua base.

Consideriamo quindi il caso in cui W non è banale. Per l'ipotesi induttiva applicata a W e al suo sistema di generatori v_1, \dots, v_{m-1} , la sequenza:

$$\mathfrak{C} = \{v_{i_1}, \dots, v_{i_k}\}$$

è una base di W , dove v_{i_1}, \dots, v_{i_k} sono i vettori non eliminabili della sequenza v_1, \dots, v_{m-1} . In particolare, i vettori di \mathfrak{C} sono linearmente indipendenti. A questo punto vi sono due possibilità:

- 1) v_m è eliminabile
- 2) v_m non è eliminabile.

Nel primo caso i vettori non eliminabili della sequenza v_1, \dots, v_m sono tutti e soli quelli non eliminabili della sottosequenza v_1, \dots, v_{m-1} , ovvero si ha $\mathfrak{B} = \mathfrak{C}$. Risulta che \mathfrak{B} è di fatto una base di V perchè in tal caso risulta che $W = V$; infatti, stante l'eliminabilità di v_m abbiamo:

$$V = L(v_1, \dots, v_m) \subset L(v_1, \dots, v_{m-1}) = W.$$

Nel caso 2), abbiamo $\mathfrak{B} = \{v_{i_1}, \dots, v_{i_k}, v_m\}$. Applicando la Prop. 20.2, i vettori di \mathfrak{B} risultano linearmente indipendenti, perchè v_{i_1}, \dots, v_{i_k} lo sono e inoltre $v_m \notin L(v_{i_1}, \dots, v_{i_k})$, essendo v_m non eliminabile. Infine

$$V = L(v_1, \dots, v_m) \subset L(v_{i_1}, \dots, v_{i_k}, v_m)$$

perchè tutti i vettori v_1, \dots, v_{m-1}, v_m appartengono al sottospazio $L(v_{i_1}, \dots, v_{i_k}, v_m)$, in quanto v_1, \dots, v_{m-1} sono tutti combinazioni lineari di v_{i_1}, \dots, v_{i_k} essendo \mathfrak{C} base di W . Quindi resta provato che i vettori di \mathfrak{B} costituiscono un sistema di generatori di V e con ciò che \mathfrak{B} è una base di V . \square

22. DIMENSIONE DI UNO SPAZIO VETTORIALE

I Teoremi 19.4 e 21.3 permettono di introdurre la seguente nozione fondamentale:

Definizione 22.1. Si chiama **dimensione** di un \mathbb{K} -spazio vettoriale V finitamente generato il numero $n \in \mathbb{N}$ di elementi di una sua qualsiasi base, dove $n = 0$ nel caso in cui V sia banale. La dimensione di uno spazio V si denota con

$$\dim_{\mathbb{K}}(V)$$

o semplicemente con $\dim(V)$.

Il seguente risultato fornisce una interpretazione alternativa dello stesso concetto:

Teorema 22.2. *La dimensione di un \mathbb{K} -spazio vettoriale V finitamente generato è l'unico intero $n \in \mathbb{N}$ tale che*

$$V \cong \mathbb{K}^n.$$

DIMOSTRAZIONE: Poniamo $n = \dim_{\mathbb{K}}(V)$. Se V è banale, allora $n = 0$ e si ha $V \cong \mathbb{K}^0$. Infatti, l'applicazione nulla

$$0 : V = \{0_V\} \rightarrow \{0_{\mathbb{K}}\}$$

è un isomorfismo. Se V non è banale, il Teorema 21.3 garantisce che $n > 0$ ed esiste almeno una base $\mathfrak{B} = \{v_1, \dots, v_n\}$, $n \geq 1$, necessariamente costituita da n vettori, per definizione di dimensione. In corrispondenza di tale base vi è l'isomorfismo $\varphi_{\mathfrak{B}} : \mathbb{K}^n \rightarrow V$ discusso nel §19.

Infine, n è l'unico numero intero con questa proprietà in forza del teorema di classificazione 16.6 degli spazi \mathbb{K}^n : se esistesse un altro intero m per cui $V \cong \mathbb{K}^m$, avremmo di conseguenza $\mathbb{K}^m \cong \mathbb{K}^n$, il che comporta $m = n$. \square

Dunque si può decidere qual è la dimensione di uno spazio vettoriale finitamente generato individuandone una base (per esempio mediante l'algoritmo di eliminazione) e contandone il numero di elementi, oppure individuando un isomorfismo con un opportuno spazio del tipo \mathbb{K}^n .

Ad esempio, abbiamo ovviamente $\dim_{\mathbb{K}}(\mathbb{K}^n) = n$, perchè la sua base canonica $\mathfrak{B} = \{e_1, \dots, e_n\}$ consta esattamente di n vettori. D'altra parte, il fatto che \mathbb{K}^n è isomorfo a sè stesso dà un'altra giustificazione della stessa cosa.

ESEMPIO 22.3. Lo spazio vettoriale $M_2(\mathbb{K})$ delle matrici di tipo 2x2 a coefficienti in \mathbb{K} ha dimensione 4, in quanto, come si è già osservato, esso ammette la base costituita dalle 4 matrici:

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, E_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Osservazione 22.4. Osserviamo che, se è assegnato un isomorfismo $F : \mathbb{K}^n \rightarrow V$, $n > 0$, allora esso determina in modo naturale una base di V , ottenuta "trasportando in V " la base canonica: infatti i vettori

$$F(e_1), \dots, F(e_n)$$

costituiscono automaticamente una base di V . Si lascia la verifica come esercizio. Nel caso ad esempio dello spazio $M_2(\mathbb{K})$, utilizzando l'isomorfismo

$$F(a, b, c, d) := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

si ottiene in tal modo la base E_1, E_2, E_3, E_4 discussa sopra.

La dimensione di uno spazio vettoriale si caratterizza ulteriormente mediante le nozioni di indipendenza lineare e di sistema di generatori, come segue:

Teorema 22.5. *Sia V uno spazio vettoriale finitamente generato di dimensione $n \geq 1$.*

- (1) *La dimensione n è il massimo numero di vettori linearmente indipendenti; ciò significa che esistono n vettori indipendenti e inoltre se w_1, \dots, w_m sono vettori linearmente indipendenti, allora $m \leq n$.*
- (2) *La dimensione n è il numero minimo di vettori che occorrono per generare V ; cioè esistono n vettori che generano V e inoltre se w_1, \dots, w_m è un sistema di generatori qualsiasi, allora $m \geq n$.*

DIMOSTRAZIONE: Proviamo (1). Fissiamo una base $\mathfrak{B} = \{v_1, \dots, v_n\}$ di V . Essa è costituita da n vettori, che sono linearmente indipendenti. Sia poi $A = \{w_1, \dots, w_m\}$ un insieme libero. Allora l'applicazione lineare $\varphi_A : \mathbb{K}^m \rightarrow V$ studiata nel paragrafo 19 è iniettiva. Componendola con un assegnato isomorfismo $F : V \rightarrow \mathbb{K}^n$ si ottiene un'applicazione lineare iniettiva

$$F \circ \varphi_A : \mathbb{K}^m \rightarrow \mathbb{K}^n.$$

In base al Teorema 16.3 dev'essere $m \leq n$.

Per quanto riguarda (2), i vettori di \mathfrak{B} sono n e generano V . Consideriamo un altro sistema di generatori w_1, \dots, w_m . Il Teorema 21.3 garantisce che da tale sistema si può estrarre una base w_{i_1}, \dots, w_{i_k} , $k \leq m$. Poichè qualunque base è costituita da n vettori dev'essere $k = n$, e pertanto $m \geq n$. \square

Corollario 22.6. *Sia V uno spazio vettoriale finitamente generato di dimensione $n \geq 1$. Si consideri una sequenza di n vettori v_1, \dots, v_n .*

- (1) *Se v_1, \dots, v_n sono indipendenti, allora $\{v_1, \dots, v_n\}$ è base di V .*
- (2) *Se v_1, \dots, v_n costituiscono un sistema di generatori, allora $\{v_1, \dots, v_n\}$ è base di V .*

DIMOSTRAZIONE: (1) Per assurdo, si assuma che v_1, \dots, v_n siano indipendenti e che $V \neq L(v_1, \dots, v_n)$. Allora esisterebbe almeno un vettore v_{n+1} di V tale che $v_{n+1} \notin L(v_1, \dots, v_n)$. Per la Proposizione 20.2, seguirebbe che v_1, \dots, v_n, v_{n+1} sono linearmente indipendenti, contro la (1) del Teorema precedente.

(2) Supponiamo per assurdo che v_1, \dots, v_n generino V e siano linearmente dipendenti. Allora uno di tali vettori v_j sarebbe combinazione lineare degli altri; avremmo quindi

$$V = L(v_1, \dots, v_n) \subset L(v_1, \dots, v_{j-1}, v_{j+1}, \dots, v_n)$$

contro la (2) del Teorema precedente. \square

ESEMPIO 22.7. Il lettore verifichi ad esempio che $\mathfrak{B} = \{(1, 2, 0), (1, -1, 0), (0, 0, 1)\}$ è una base di \mathbb{R}^3 . Poichè tale spazio ha dimensione 3, basta controllare che i vettori

in questione sono linearmente indipendenti (oppure che costituiscono un sistema di generatori).

Osservazione 22.8. Dati due \mathbb{K} -spazi vettoriali finitamente generati, allora essi hanno la stessa dimensione se e solo se isomorfi.

La dimostrazione è un semplice esercizio.

Un'altra applicazione del Teorema 22.5 è la seguente, che caratterizza gli spazi vettoriali che non hanno dimensione finita, mediante la possibilità di poter costruire sequenze libere di vettori di lunghezza arbitraria:

Proposizione 22.9. *Sia V un \mathbb{K} -spazio vettoriali. Le seguenti proprietà sono equivalenti:*

- a) V non è finitamente generato.
- b) Per ogni intero $n \geq 1$, esistono n vettori linearmente indipendenti v_1, \dots, v_n in V .

DIMOSTRAZIONE: a) \Rightarrow b) Assumendo che V non sia finitamente generato, proviamo la proprietà b) per induzione su n . Poichè in V esiste almeno un vettore $v_1 \neq 0$ (altrimenti si avrebbe $V = \{0_V\} = L(0_V)$, contro l'ipotesi), la b) è vera per $n = 1$. Supposta ora la b) vera per $n \geq 1$, abbiamo che in V esistono n vettori v_1, \dots, v_n linearmente indipendenti. Ora, siccome V non è finitamente generato, dev'essere $V \neq L(v_1, \dots, v_n)$. Scelto un vettore v_{n+1} di V tale che $v_{n+1} \notin L(v_1, \dots, v_n)$, abbiamo che v_1, \dots, v_n, v_{n+1} sono indipendenti, in forza sempre della Proposizione 20.2. Pertanto la proprietà b) è vera anche per $n + 1$.

b) \Rightarrow a). Assumendo b), certamente $V \neq \{0_V\}$. Ammettiamo che V sia finitamente generato. Posto $n = \dim(V)$, stante l'ipotesi esisterebbe almeno una sequenza v_1, \dots, v_{n+1} costituita da $n + 1$ vettori linearmente indipendenti, in contraddizione con la 1) del Teorema 22.5. \square

23. SOTTOSPAZI DI SPAZI DI DIMENSIONE FINITA

Teorema 23.1. *Sia V uno spazio vettoriale finitamente generato sul campo \mathbb{K} e sia W un sottospazio di V . Allora:*

- 1) W è finitamente generato.
- 2) Si ha $\dim_{\mathbb{K}}(W) \leq \dim_{\mathbb{K}}(V)$ ed inoltre

$$\dim_{\mathbb{K}}(W) = \dim_{\mathbb{K}}(V) \iff W = V.$$

DIMOSTRAZIONE: 1) Ragioniamo per assurdo, assumendo che W non sia finitamente generato. Allora, applicando a W la Prop. 22.9, per ogni $n \geq 1$ sarebbe

possibile individuare una sequenza w_1, \dots, w_n di n vettori di W linearmente indipendenti, che è anche una sequenza di vettori indipendenti di V ; dunque per la stessa Prop. 22.9, anche V non sarebbe finitamente generato, contro l'ipotesi.

2) Supponiamo che W abbia dimensione k . Possiamo supporre $k > 0$. Fissata una base $\mathfrak{B}' = \{w_1, \dots, w_k\}$ di W , i vettori che la costituiscono sono linearmente indipendenti. Quindi $k \leq \dim_{\mathbb{K}}(V)$ per il Teorema 22.5. Se $k = \dim_{\mathbb{K}}(V)$, i vettori di \mathfrak{B}' sono n formano necessariamente anche una base di V in virtù del Corollario 22.6; pertanto:

$$W = L(w_1, \dots, w_n) = V.$$

□

24. IL TEOREMA DI COMPLETAMENTO

Il risultato seguente mostra come si possano costruire basi di uno spazio vettoriale finitamente generato, a partire da un insieme libero qualsiasi.

Teorema 24.1. (*Completamento di un insieme libero*)

Sia V uno spazio vettoriale sul campo \mathbb{K} , di dimensione $n > 0$. Siano assegnati dei vettori linearmente indipendenti

$$u_1, \dots, u_k, \quad k \geq 1.$$

Sia inoltre $\mathfrak{B} = \{v_1, \dots, v_n\}$ una base di V . Allora esistono $n-k$ vettori $v_{j_1}, \dots, v_{j_{n-k}}$ della base \mathfrak{B} tali che

$$\mathfrak{B}' = \{u_1, \dots, u_k, v_{j_1}, \dots, v_{j_{n-k}}\}$$

è una base di V .

DIMOSTRAZIONE: Consideriamo la sequenza costituita da tutti i vettori

$$u_1, \dots, u_k, v_1, \dots, v_n.$$

Tale sequenza è ancora un sistema di generatori, da cui si può estrarre una base \mathfrak{B}' mediante l'algoritmo di eliminazione. Poichè u_1, \dots, u_k sono indipendenti, ciascuno di essi non è eliminabile. Dunque la base \mathfrak{B}' è del tipo richiesto. □

25. SOMME DIRETTE

Definizione 25.1. Dati due sottospazi vettoriali U e W di uno spazio vettoriale V , la somma $U + W$ verrà detta *diretta* se

$$(14) \quad U \cap W = \{0_V\}.$$

In tal caso, in luogo di $U + W$ si scrive $U \oplus W$.

Sussiste la seguente caratterizzazione della condizione (14).

Proposizione 25.2. *Dati i sottospazi U e W di V , le seguenti proprietà sono equivalenti:*

- a) La somma $U + W$ è diretta.
 b) Ogni vettore $v \in U + W$ si scrive in modo unico nella forma $v = u + w$ con $u \in U$ e $w \in W$.

DIMOSTRAZIONE: $a) \Rightarrow b)$. Stante la definizione di $U + W$, assumendo a) è chiaro che ogni $v \in U + W$ si può scrivere come enunciato in b); supponiamo che ciò possa farsi in due modi diversi: $v = u + w = u' + w'$, con ovvio significato dei simboli. Allora $u - u' = w' - w$ ed il vettore con cui coincidono ambo i membri appartiene sia ad U che a W in virtù delle proprietà dei sottospazi. Pertanto, per la a), si ha $u - u' = 0_V = w' - w$ e di qui la b).

$b) \Rightarrow a)$. Sia $v \in U \cap W$; poichè

$$v = v + 0_V = 0_V + v,$$

applicando la b), dal confronto di tali rappresentazioni di v si ottiene che necessariamente $v = 0_V$. \square

Un'utile proprietà in merito al completamento di un insieme libero ad una base è la seguente:

Corollario 25.3. *Siano assegnata una sequenza di vettori linearmente indipendenti*

$$u_1, \dots, u_k, \quad k \geq 1.$$

dello spazio vettoriale V e siano u_{k+1}, \dots, u_n altri $n - k$ vettori che completano tale sequenza ad una base $\mathfrak{B} = \{u_1, \dots, u_k, u_{k+1}, \dots, u_n\}$. Allora risulta:

$$V = L(u_1, \dots, u_k) \oplus L(u_{k+1}, \dots, u_n).$$

DIMOSTRAZIONE: Occorre provare che la somma di tali sottospazi è diretta. Sia $v \in L(u_1, \dots, u_k) \cap L(u_{k+1}, \dots, u_n)$. Allora v si può scrivere in due modi:

$$v = \lambda_1 u_1 + \dots + \lambda_k u_k, \quad v = \lambda_{k+1} u_{k+1} + \dots + \lambda_n u_n,$$

per opportuni scalari λ_i , da cui:

$$\lambda_1 u_1 + \dots + \lambda_k u_k - \lambda_{k+1} u_{k+1} + \dots - \lambda_n u_n = 0$$

e quindi $\lambda_1 = \dots = \lambda_n = 0$ stante la lineare indipendenza dei vettori della base; in particolare $v = 0$. Infine, è chiaro che

$$V \subset L(u_1, \dots, u_k) + L(u_{k+1}, \dots, u_n)$$

perchè $V = L(u_1, \dots, u_k, u_{k+1}, \dots, u_n)$ e tutti i vettori u_i appartengono al sottospazio somma di $L(u_1, \dots, u_k)$ e $L(u_{k+1}, \dots, u_n)$.

\square

Osservazione 25.4. Applicando questa Proposizione, otteniamo che, data una base qualsiasi $\mathfrak{B} = \{v_1, \dots, v_n\}$ di uno spazio vettoriale V e un indice $1 \leq k \leq n$, allora si ha sempre:

$$V = L(v_1, \dots, v_k) \oplus L(v_{k+1}, \dots, v_n).$$

26. CALCOLO DELLA DIMENSIONE DI ALCUNI SPAZI NOTEVOLI

Nel seguito calcoliamo la dimensione ed una base di alcuni spazi vettoriali interessanti.

ESEMPIO 26.1. Fissato $n \geq 0$, l'insieme

$$\mathbb{R}_n[x] = \{p : \mathbb{R} \rightarrow \mathbb{R} \mid p = p(x) \text{ è un polinomio di grado } \leq n\},$$

è un sottospazio vettoriale dello spazio $\mathbb{R}^{\mathbb{R}}$ di tutte le funzioni $p : \mathbb{R} \rightarrow \mathbb{R}$.

Risulta che tale spazio è finitamente generato e ha dimensione $n + 1$. Infatti ogni polinomio p di grado al massimo n è del tipo

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

dove gli a_i sono costanti. Ciò significa che p è combinazione lineare dei polinomi

$$1, x, x^2, \dots, x^n \quad (*)$$

con coefficienti esattamente a_0, \dots, a_n ; tali polinomi costituiscono quindi un sistema generatori di $\mathbb{R}_n[x]$. I polinomi (*) costituiscono di fatto una base di $\mathbb{R}_n[x]$; infatti data una loro combinazione lineare nulla:

$$a_0 + a_1x + \cdots + a_nx^n = 0,$$

dove 0 è il polinomio nullo (la funzione costante di valore 0), allora il principio di identità dei polinomi garantisce che necessariamente tutti i coefficienti a_i devono essere uguali a zero. Dunque gli $n + 1$ vettori (*) formano una base del nostro spazio $\mathbb{R}_n[x]$, che pertanto ha dimensione $n + 1$.

ESEMPIO 26.2. Lo spazio vettoriale $M_{m,n}(\mathbb{K})$ delle matrici di tipo $m \times n$ a coefficienti in un campo \mathbb{K} è isomorfo a \mathbb{K}^{mn} e quindi ha dimensione mn . Un isomorfismo naturale si ottiene associando a ogni matrice A un vettore con mn elementi, costituito da tutti gli ingressi a_j^i della matrice, scritti in ordine lessicografico, ovvero scansionando le righe dalla prima all'ultima e disponendo gli elementi per ordine crescente rispetto alla colonna di appartenenza; si definisce così la bigezione:

$$F : M_{m,n}(\mathbb{K}) \rightarrow \mathbb{K}^{mn}$$

definita da:

$$F(A) = (a_1^1, \dots, a_n^1, a_1^2, \dots, a_n^2, \dots, a_1^m, \dots, a_n^m).$$

Possiamo anche scrivere (con piccolo abuso di notazione):

$$F(A) = (A^{(1)}, \dots, A^{(m)}).$$

Date due matrici $A, B \in M_{m,n}(\mathbb{K})$ e scalari λ, μ , poichè la riga i -ma della matrice $\lambda A + \mu B$ è $\lambda A^{(i)} + \mu B^{(i)}$, si ottiene:

$$F(\lambda A + \mu B) = (\lambda A^{(1)} + \mu B^{(1)}, \dots, \lambda A^{(m)} + \mu B^{(m)}) = \lambda(A^{(1)}, \dots, A^{(m)}) + \mu(B^{(1)}, \dots, B^{(m)})$$

il che mostra che F è lineare.

Una base di tale spazio è

$$\mathfrak{B} = \{E_{ij} : 1 \leq i, j \leq n\}$$

dove denotiamo con E_{ij} la matrice con m righe e n colonne, i cui elementi sono tutti nulli, eccetto l'elemento di posto (i, j) che è uguale a 1. Tale base si ottiene applicando ai vettori della base canonica $\{e_i\}$ di \mathbb{K}^{mn} l'inverso $F^{-1} : \mathbb{K}^{mn} \rightarrow M_{mn}(\mathbb{K})$ dell'isomorfismo F , trasformando in modo naturale ogni vettore e_i in una matrice. Così, ad esempio:

$$E_{11} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, E_{12} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, E_{13} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

$$E_{21} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, E_{22} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, E_{23} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

è una base di $M_{2,3}(\mathbb{K})$.

ESEMPIO 26.3. Dato un campo \mathbb{K} , calcoliamo la dimensione di $Hom(\mathbb{K}^n, \mathbb{K})$, ovvero lo spazio di tutte le applicazioni lineari $F : \mathbb{K}^n \rightarrow \mathbb{K}$.

Sappiamo che ogni tale F è del tipo:

$$F(x) = a_1x_1 + \cdots + a_nx_n \quad (*)$$

dove gli scalari a_1, \dots, a_n sono univocamente determinati, essendo $a_i = F(e_i)$, dove come al solito $\{e_1, \dots, e_n\}$ è la base canonica di \mathbb{K}^n . Notiamo ora che (*) si può interpretare in termini di combinazione lineare, come segue:

$$F = a_1p_1 + \cdots + a_np_n$$

dove per ogni i , $p_i : \mathbb{K}^n \rightarrow \mathbb{K}$ è la proiezione

$$p_i(x) := x_i,$$

che è anch'essa un vettore di $Hom(\mathbb{K}^n, \mathbb{K})$. Ciò mostra che tali proiezioni p_1, \dots, p_n formano un sistema di generatori di $Hom(\mathbb{K}^n, \mathbb{K})$.

Risulta poi che p_1, \dots, p_n sono linearmente indipendenti; infatti, data una combinazione lineare nulla:

$$a_1p_1 + \cdots + a_np_n = 0,$$

allora la funzione lineare al primo membro è quella costante di valore 0, ma ciò implica direttamente che $a_i = 0$ per ogni i . Conclusione: $\mathfrak{B} = \{p_1, \dots, p_n\}$ è una base di $Hom(\mathbb{K}^n, \mathbb{K})$ e dunque:

$$\dim_{\mathbb{K}} Hom(\mathbb{K}^n, \mathbb{K}) = n.$$

Ad esempio, una base di $Hom(\mathbb{R}^3, \mathbb{R})$ è costituita dalle 3 proiezioni:

$$p_1(x_1, x_2, x_3) = x_1, p_2(x_1, x_2, x_3) = x_2, p_3(x_1, x_2, x_3) = x_3.$$

ESEMPIO 26.4. Più in generale, risulta che lo spazio $\text{Hom}(\mathbb{K}^n, \mathbb{K}^m)$ ha dimensione mn . Risulta che esso è isomorfo a $M_{m,n}(\mathbb{K})$ mediante l'applicazione

$$\Phi : A \in M_{m,n}(\mathbb{K}) \mapsto L_A \in \text{Hom}(\mathbb{K}^n, \mathbb{K}^m).$$

Sappiamo infatti che questa funzione è bigettiva in virtù del Teorema 15.6; essa è lineare grazie alla Prop. 15.9; infatti:

$$\Phi(A + B) = L_{A+B} = L_A + L_B = \Phi(A) + \Phi(B),$$

mentre è immediato che

$$\Phi(\lambda A) = L_{\lambda A} = \lambda L_A = \lambda \Phi(A).$$

Concludiamo questo paragrafo trattando il caso del prodotto diretto di due spazi vettoriali.

Proposizione 26.5. *Siano U e W due \mathbb{K} -spazi vettoriali di dimensione finita. Allora*

$$\dim(U \times W) = \dim(U) + \dim(W).$$

DIMOSTRAZIONE: Possiamo limitarci a considerare il caso in cui i due spazi sono entrambi non banali: se ad es. $U = \{0_U\}$, allora è evidente che $U \times W \cong W$ tramite l'isomorfismo:

$$(0_U, w) \mapsto w.$$

Cominciamo con lo studiare il caso in cui $U = \mathbb{K}^n$ e $W = \mathbb{K}^m$ con m e n interi positivi. In tal caso risulta:

$$\mathbb{K}^n \times \mathbb{K}^m \cong \mathbb{K}^{n+m}.$$

Per giustificare ciò, è sufficiente considerare l'applicazione

$$((x_1, \dots, x_n), (y_1, \dots, y_m)) \in \mathbb{K}^n \times \mathbb{K}^m \mapsto (x_1, \dots, x_n, y_1, \dots, y_m) \in \mathbb{K}^{n+m}.$$

Si lascia al lettore la semplice verifica che si tratta di un isomorfismo.

Venendo ora al caso generale, posto $n = \dim(U)$ e $m = \dim(W)$, siano assegnati due isomorfismi $F : U \rightarrow \mathbb{K}^n$ e $G : W \rightarrow \mathbb{K}^m$. A partire da questi, possiamo definire in modo standard un'applicazione:

$$F \times G : U \times W \rightarrow \mathbb{K}^n \times \mathbb{K}^m,$$

ponendo

$$(F \times G)(u, w) := (F(u), G(w)) \quad \forall (u, w) \in U \times W.$$

È un semplice esercizio verificare che si tratta di una bigezione, stante la bigettività di entrambe le funzioni coinvolte. Tale applicazione è lineare; infatti, dati due vettori

(u, w) e (u', w') di $U \times W$, allora:

$$\begin{aligned}
 (F \times G)(\lambda(u, w) + \mu(u', w')) &= (F \times G)(\lambda u + \mu u', \lambda w + \mu w') \\
 &= (F(\lambda u + \mu u'), G(\lambda w + \mu w')) \\
 &= (\lambda F(u) + \mu F(u'), \lambda G(w) + \mu G(w')) \\
 &= \lambda(F(u), G(w)) + \mu(F(u'), G(w')) \\
 &= \lambda(F \times G)(u, w) + \mu(F \times G)(u', w').
 \end{aligned}$$

Resta quindi stabilito che:

$$U \times V \cong \mathbb{K}^n \times \mathbb{K}^m,$$

da cui la conclusione. \square

27. IL TEOREMA DEL RANGO

Proposizione 27.1. *Sia $F : V \rightarrow V'$ un'applicazione lineare tra \mathbb{K} -spazi vettoriali.*

a) *Data una sequenza qualsiasi di vettori v_1, \dots, v_n di V si ha:*

$$F(L(v_1, \dots, v_n)) = L(F(v_1), \dots, F(v_n)).$$

b) *Dati due sottospazi vettoriali U e W di V , si ha: $F(U + W) = F(U) + F(W)$.*

DIMOSTRAZIONE: a) Ciò è conseguenza immediata del fatto che F trasforma combinazioni lineari dei vettori v_i in combinazioni lineari delle loro immagini $F(v_i)$, cfr. Prop. 12.5:

$$\begin{aligned}
 F(L(v_1, \dots, v_n)) &= F(\{\lambda_1 v_1 + \dots + \lambda_n v_n : \lambda_1, \dots, \lambda_n \in \mathbb{K}\}) = \\
 &= \{F(\lambda_1 v_1 + \dots + \lambda_n v_n) : \lambda_1, \dots, \lambda_n \in \mathbb{K}\} = \\
 &= \{\lambda_1 F(v_1) + \dots + \lambda_n F(v_n) : \lambda_1, \dots, \lambda_n \in \mathbb{K}\} = \\
 &= L(F(v_1), \dots, F(v_n)).
 \end{aligned}$$

b) Basta applicare la definizione di spazio somma:

$$\begin{aligned}
 F(U + W) &= F(\{u + w \mid u \in U, w \in W\}) = \{F(u + w) \mid u \in U, w \in W\} = \\
 &= \{F(u) + F(w) \mid u \in U, w \in W\} = F(U) + F(W).
 \end{aligned}$$

\square

Mostriamo ora che le applicazioni lineari conservano la proprietà degli spazi a cui sono applicati di essere finitamente generati:

Proposizione 27.2. *Sia $F : V \rightarrow V'$ un'applicazione lineare tra \mathbb{K} -spazi vettoriali e sia W un sottospazio vettoriale di V . Allora, se W è finitamente generato, tale è $F(W)$ e si ha*

$$\dim_{\mathbb{K}} F(W) \leq \dim_{\mathbb{K}} W.$$

Se F è un monomorfismo, allora risulta:

$$\dim_{\mathbb{K}} F(W) = \dim_{\mathbb{K}} W.$$

DIMOSTRAZIONE: Assunto che W sia finitamente generato, se $W = \{0_V\}$, allora $F(W) = \{0_V\}$ e quindi la tesi. Supponiamo quindi $\dim_{\mathbb{K}} W = n > 0$ e fissiamo una base $\mathfrak{B} = \{w_1, \dots, w_n\}$ di W . Allora abbiamo:

$$F(W) = F(L(w_1, \dots, w_n)) = L(F(w_1), \dots, F(w_n))$$

per cui anche $F(W)$ è finitamente generato; siccome la dimensione di $F(W)$ è il numero minimo di vettori costituenti un sistema di generatori, deve aversi

$$\dim_{\mathbb{K}} F(W) \leq n.$$

Se F è un monomorfismo, consideriamo la funzione

$$F|_W : W \rightarrow F(W),$$

ridotta della restrizione di F a W . Essa è ancora lineare, e per costruzione surgettiva, ma anche iniettiva perchè lo è F . Dunque è un isomorfismo e pertanto W e $F(W)$ in tal caso hanno la stessa dimensione. \square

Il risultato seguente è di importanza basilare in tutte le applicazioni dell'algebra lineare.

Teorema 27.3. (*Teorema del rango, o della dimensione, o rango-nullità*).

Siano V e V' spazi vettoriali sullo stesso campo \mathbb{K} . Si assuma che V sia finitamente generato. Sia

$$F : V \rightarrow V'$$

un'applicazione lineare. Allora risulta:

$$(15) \quad \dim(V) = \dim(\text{Ker}(F)) + \dim(\text{Im}(F)).$$

DIMOSTRAZIONE: Esaminiamo dapprima il caso in cui F è iniettiva. Allora, in base alla Prop. 27.2 sappiamo che $\dim(F(V)) = \dim(V)$. D'altra parte per l'iniettività, $\text{Ker}(F) = \{0_V\}$ e quindi $\dim(\text{Ker}(F)) = 0$ e pertanto la (15) è vera in questo caso.

Supponiamo ora che F non sia iniettiva e poniamo $k := \dim(\text{Ker}(F))$; dunque $k > 0$. Fissiamo una base $\mathfrak{B} = \{u_1, \dots, u_k\}$ di $\text{Ker}(F)$. Posto $n = \dim(V)$, applicando il Teorema di completamento, sappiamo che esistono $n - k$ vettori u_{k+1}, \dots, u_n che completano \mathfrak{B} ad una base

$$\mathfrak{B}' = \{u_1, \dots, u_n\}$$

di V . Consideriamo quindi il sottospazio di V :

$$W = L(u_{k+1}, \dots, u_n).$$

Chiaramente, tale sottospazio ha dimensione $n - k$ perchè i vettori u_{k+1}, \dots, u_n ne costituiscono una base, in quanto sono linearmente indipendenti. Sappiamo inoltre dal Cor. 25.3 che

$$V = L(u_1, \dots, u_k) \oplus L(u_{k+1}, \dots, u_n)$$

cioè che:

$$V = \text{Ker}(F) \oplus W.$$

Consideriamo quindi la restrizione di F a W :

$$F|_W : W \rightarrow V'.$$

Questa funzione, che è ancora lineare, è iniettiva, perchè, se $w \in W$ è un vettore appartenente a $\text{Ker}(F|_W)$, si ha $F(w) = 0_{V'}$, ma allora $w \in W \cap \text{Ker}(F) = \{0_V\}$, da cui $w = 0$. Pertanto, sempre per la Prop. 27.2, $F(W)$ ha la stessa dimensione di W , ovvero ha dimensione $n - k$. Ma $F(W) = \text{Im}(F)$; infatti, applicando b) della Prop. 27.1:

$$\text{Im}(F) = F(V) = F(\text{Ker}(F) + W) = F(\text{Ker}(F)) + F(W) = \{0_{V'}\} + F(W) = F(W).$$

In conclusione

$$\dim(\text{Im}(F)) = \dim(F(W)) = n - k = n - \dim(\text{Ker}(F))$$

e la (15) è provata. \square

28. IL TEOREMA DI GRASSMANN

Discutiamo ora il caso della somma di due sottospazi, provando un altro risultato fondamentale:

Teorema 28.1. (*Formula di Grassmann*) *Sia V uno spazio vettoriale di dimensione finita. Siano U e W due sottospazi di V . Allora:*

$$(16) \quad \dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W).$$