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) $* : X \times X \to X$, 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 $f \circ g : A \to A$ 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 $Id_A : A \to A$ (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 $f : A \to A$, 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 $f : A \to A$, essa è un elemento invertibile di $(A^A, \circ)$ se e solo se esiste una funzione $g : A \to A$ tale che:

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

Questo signfica 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 affinchè ciò sia possibile è che f sia una funzione *bigettiva*, ovvero sia ingettiva che surgettiva. La funzione $g : A \to A$ 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 $\cdot : \mathbb{R}^* \times \mathbb{R}^* \to \mathbb{R}^*$ 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* $f : A \to A$ 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 $F : A \to A$ 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 $\sigma : E \to E$ 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 semplicmente 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 mediate 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

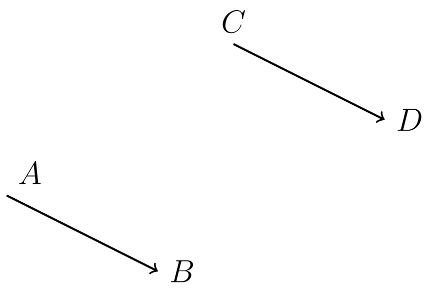
$$(x, y) + [(x', y') + (x'', y'')] = (x, y) + (x' + x'', y' + y'') = (x + x' + x'', y + y' + y'').$$

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.

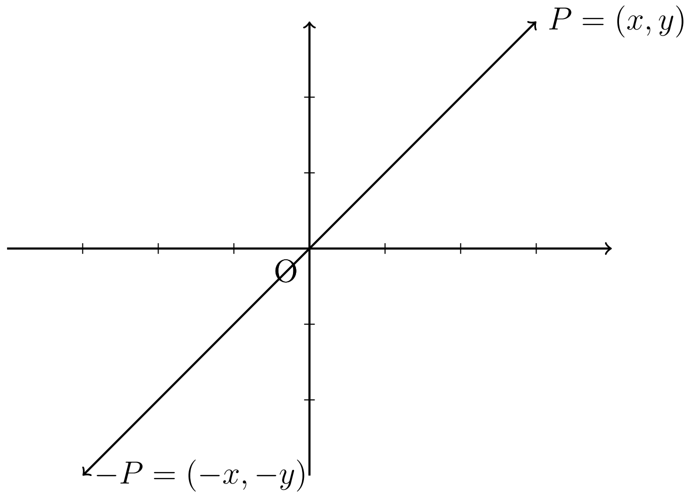
Dato un vettore $\overrightarrow{AB}$ e un punto C, esiste un unico vettore $\overrightarrow{CD}$ che ha lo stesse caratteristiche di $\overrightarrow{AB}$ (direzione, lunghezza e verso): esso si dice *equipollente ad* $\overrightarrow{AB}$. I vettori equipollenti $\overrightarrow{AB}$ e $\overrightarrow{CD}$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



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

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 $\overrightarrow{AB} + \overrightarrow{AC}$, 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*

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

è il punto

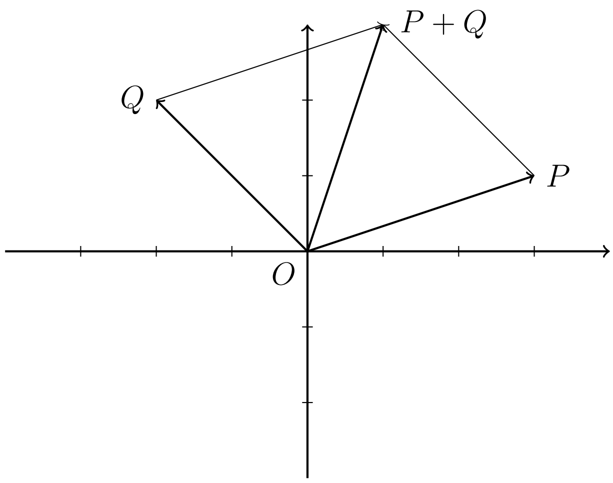
$$D = C + B - A.$$

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

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

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:

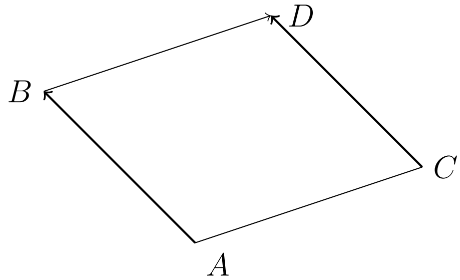
$$\overrightarrow{OP}+\overrightarrow{OQ}=\overrightarrow{O(P+Q)}.$$



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:

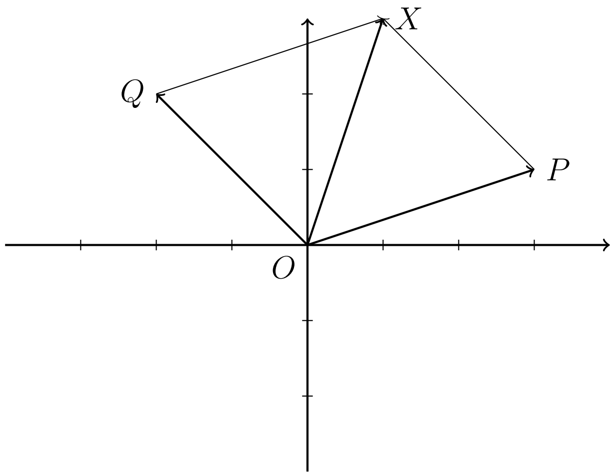


Affermiamo che tale punto è $X := C + B - A$. Per far ciò, posto $A(a_1, a_2)$, $B(b_1, b_2)$ e $C(c_1, c_2)$, basta controllare che la retta $r_{A,B}$ è parallela alla retta $r_{C,X}$ e che la retta $r_{B,X}$ è parallela alla retta $r_{A,C}$. Infatti, abbiamo che il punto X ha coordinate $(b_1 + c_1 - a_1, b_2 + c_2 - a_2)$ 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*:*

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

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:

$$a \neq 0 \ e \ b \neq 0 \ \Rightarrow a \cdot b \neq 0.$$

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

$$+ : V \times V \to V, \qquad \cdot : \mathbb{K} \times V \to V$$

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 moltplicazione esterna $\cdot : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}$ 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 $\overrightarrow{OQ}$, 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 $\overrightarrow{OQ}$ è concorde con quello di $\overrightarrow{OP}$ se $\lambda > 0$, mentre è il verso opposto a quello di $\overrightarrow{OP}$ 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

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

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

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

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 separamente 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 $(x, y) \in \mathbb{K}$, 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

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

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

$$+ : (V_1 \times V_2) \times (V_1 \times V_2) \to V_1 \times V_2, \qquad \cdot : \mathbb{K} \times (V_1 \times V_2) \to V_1 \times V_2$$

nel modo seguente

$$(v_1, v_2) + (w_1, w_2) := (v_1 + v_2, w_1 + w_2), \;\; \lambda(v_1, v_2) := (\lambda v_1, \lambda v_2). \tag{1}$$

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

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

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

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

Si scrive anche in modo compatto $A = (a_j^i)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ 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 $1 \times n$

$$A^{(i)} := \begin{pmatrix} a_1^i & a_2^i & \cdots & a_n^i \end{pmatrix}$$

mentre, fissato $j \in \{1, \dots, m\}$, 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:

$$A = \begin{pmatrix} A_{(1)} & A_{(2)} & \cdots & A_{(n)} \end{pmatrix}$$

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 $A = (a^i_j)$, $B = (b^i_j)$ e $\lambda \in \mathbb{K}$ si pone:*

$$A + B := (a^i_j + b^i_j), \quad \lambda A := (\lambda a^i_j).$$

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 $A = (a^i_j) \in M_{m,n}(\mathbb{K})$, il vettore opposto di A in $M_{m,n}(\mathbb{K})$ è la matrice

$$-A = (-a^i_j).$$

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) $\forall u, v \in W: \quad u + v \in W.$

b) $\forall u \in W\, \forall \lambda \in \mathbb{K}: \quad \lambda u \in W.$

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

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

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. □

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 innazitutto 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 $A = (a^i_j)$ di ordine n a coefficienti in un campo assegnato $\mathbb{K}$ si dice *simmetrica* se:

$$a^i_j = a^j_i, \text{ per ogni } i, j \in \{1, \ldots, n\}.$$

Ciò significa che gli elementi della matrice sono disposti in modo simmetrico rispetto alla cosiddetta *diagonale principale*, formata dagli ingressi del tipo $a^1_1, \ldots, a^n_n$, 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

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

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 $u + v$ 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 $u = u + 0_V$ 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

$$\lambda_1 v_1 + \cdots + \lambda_k v_k$$

dove $\lambda_1, \dots, \lambda_r$ 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 $\sin : \mathbb{R} \to \mathbb{R}$, $\cos : \mathbb{R} \to \mathbb{R}$, 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 $v_1, \ldots, v_m$, $m \geq 1$, una successione finita di vettori.

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

$$L(v_1, \ldots, v_m) := \{\lambda_1 v_1 + \cdots + \lambda_m v_m | \ \lambda_1, \ldots, \lambda_m \in \mathbb{K}\}$$

costituito da tutte le combinazione lineari dei vettori $v_1, \ldots, v_m$.

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

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

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

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

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

$$\lambda u = \lambda(\lambda_1 v_1 + \cdots + \lambda_m v_m) = (\lambda\lambda_1) v_1 + \cdots + (\lambda\lambda_m) v_m \tag{3}$$

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

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

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

Sussiste anzi la seguente proprietà:

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

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

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

Dimostrazione: Basta osservare che ogni vettore del tipo $\lambda_1 v_1 + \cdots + \lambda_m v_m$ 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. □

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 $F : V \to V'$ si dice $\mathbb{K}$-*lineare* o semplicemente *lineare* se ha le proprietà seguenti:

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

Ogni applicazione lineare deve soddisfare il seguente vincolo:

Proposizione 11.2. *Sia $F : V \to V'$ 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 $0_{V'} = F(0_V)$. □

Esempio 11.3. Sono lineari tutte le funzioni $\mathbb{R} \to \mathbb{R}$ 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 $F : \mathbb{R}^2 \to \mathbb{R}$ 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:

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

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 $F : V \to V'$ soddisfa anche:

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

per ogni $u, v \in V$.

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

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

Il seguente risultato è basilare:

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

1) $Ker(F)$ è un sottospazio vettoriale di V.

2) F è ingettiva $\iff$ $Ker(F) = \{0_V\}$.

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

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

e ciò mostra che $u + v \in \mathrm{Ker}(F)$. 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 $\{0_V\} \subset Ker(F)$ è sempre vera. Supponiamo dapprima che F sia ingettiva. Sia $u \in Ker(F)$; allora $F(u) = 0_{V'}$, ovvero stante la Prop. 11.2:

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

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

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

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

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

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

e quindi

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

pertanto $u - v \in Ker(F)$ 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 $F : \mathbb{R}^2 \to \mathbb{R}$ 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 $F : V \to V'$ 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 particolarizzare b) nel caso $\lambda = \mu = 1$ e nel caso $\mu = 0$.

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

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

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 $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ e due scalari λ, μ allora:

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

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 $F : V \to V'$ tra due $\mathbb{K}$-spazi vettoriali.

Se F è ingettiva, 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'avere nucleo banale; gli epimorfismi si caratterizzano, stante la definizione, mediante un altro sottospazio notevole:

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

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

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

Proposizione 12.3. *Per ogni applicazione lineare $F : V \to V'$, $Im(F)$ 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 $F : V \to V'$. 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 $F : V \to V'$ un isomorfismo. Allora anche l'applicazione inversa $F^{-1} : V' \to V$ è lineare, e quindi è anch'essa un isomorfismo.*

Concludiamo questo paragrafo con la seguente osservazione:

Proposizione 12.5. *Sia $F : V \to V'$ 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:*

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

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

a) la restrizione $F|_U : U \to V'$ 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:

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

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

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

□

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 $F : V \to V'$, $G : V' \to V''$ applicazioni lineari. Allora anche $G \circ F : V \to V''$ 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 $F : V \to W$ e $G : V \to W$ sono due applicazioni lineari, allora anche $F + G : V \to W$ è lineare.

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

DIMOSTRAZIONE: a) Date le applicazioni lineari $F : V \to W$ e $G : V \to W$, 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 definzione 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:

$$(\lambda F)(\alpha u + \beta v) = \lambda(F(\alpha u + \beta v)) = \lambda(\alpha F(u) + \beta F(v)) =$$
$$\lambda\alpha F(u) + \lambda\beta F(v) = \alpha\lambda F(u) + \beta\lambda F(v) = \alpha(\lambda F)(u) + \beta(\lambda F)(v).$$

□

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

$$Hom(V, W)$$

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

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

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

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

In particolare anche $Hom(V, W)$ 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 $0 : V \to W$.

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

Proposizione 13.5. *Siano $F : V \to V'$ e $G : V \to V'$ due applicazioni $\mathbb{K}$-lineari e $T : U \to V$, $L : V' \to W$ 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:

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

□

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

$$e_1, \ldots, e_n$$

così definiti:

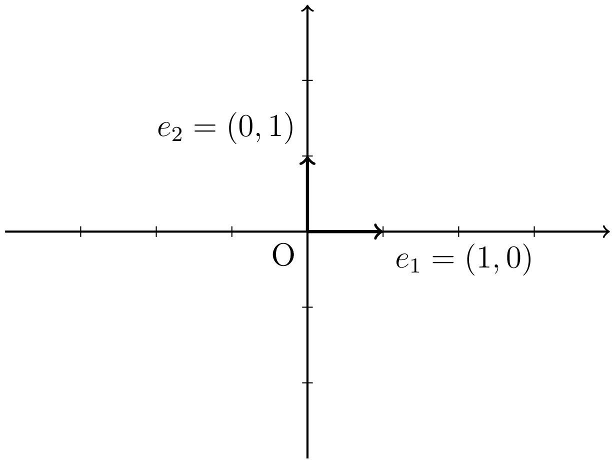
$$e_1 := (1, 0, \ldots, 0),\ e_2 := (0, 1, 0, \ldots, 0), \ldots, e_n := (0, 0, \ldots, 0, 1). \tag{4}$$

Dunque per ogni $j \in \{1, \ldots, n\}$, 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

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

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

$$x = x_1 e_1 + \cdots + x_n e_n = \sum_{i=1}^{n} x_i e_i, \tag{5}$$

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

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

$$\begin{aligned}
&x_1e_1 + \cdots + x_ne_n = \\
&x_1(1, 0, \ldots, 0) + x_2(0, 1, \ldots, 0) + \cdots + x_n(0, 0, \ldots, 0, 1) = \\
&(x_1, 0, \ldots, 0) + (0, x_2, \ldots, 0) + \cdots + (0, 0, \ldots, 0, x_n) = \\
&(x_1 + 0 + \cdots + 0, 0 + x_2 + 0 + \cdots + 0, \cdots, 0 + \cdots + 0 + x_n) = \\
&(x_1, x_2, \ldots, x_n).
\end{aligned}$$

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

$$x = \lambda_1e_1 + \cdots + \lambda_ne_n$$

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

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

e pertanto necessariamente $\lambda_i = x_i$ per ogni $i = 1, \ldots, n$. □

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

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

$$F(x_1, \ldots, x_n) := a_1x_1 + \cdots + a_nx_n \tag{6}$$

L dove $a_1, \ldots, a_n$ 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 $p_i : \mathbb{K}^n \to \mathbb{K}$, $i = 1, \ldots, n$ e osservare che

$$F = a_1p_1 + \cdots + a_np_n.$$

Infatti per ogni si ha $a_ip_i(x) = a_ip_i(x) = a_ix_i$ e quindi

$$F(x) = a_1x_1 + \cdots a_nx_n = a_1p_1(x) + \cdots a_np_n(x) = (a_1p_1 + \cdots a_np_n)(x).$$

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

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

$$x = x_1e_1 + \cdots + x_ne_n$$

otteniamo, applicando la Proposizione 12.5:

$$F(x) = x_1F(e_1) + \cdots + x_nF(e_n)$$

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 $F : \mathbb{K}^n \to \mathbb{K}$ 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 $F, G : \mathbb{K}^n \to \mathbb{K}$:

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

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

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

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

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

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

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

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 $\mathbb{R}^3 \to \mathbb{R}$ 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:

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

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

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

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 $i = 1, \ldots, m$, $p_i : \mathbb{K}^m \to \mathbb{K}$ è la i-ma proiezione

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

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

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

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

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

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

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

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 $A = (a_1 \ \ldots \ a_n)$ 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

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

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

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

D'altra parte il secondo membro è semplicemente il prodotto tra $(a_1 \ \cdots \ a_n)$ e il vettore colonnna $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. Questo fatto suggerisce di definire, per ogni vettore riga $A = (a_1 \ \cdots \ a_n)$ la seguente applicazione lineare

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

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

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

Così facendo ogni applicazione lineare $F : \mathbb{K}^n \to \mathbb{K}$ 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 concida 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:

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

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

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

definita come segue:

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

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

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

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 $F : \mathbb{K}^n \to \mathbb{K}^m$ 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 $F : \mathbb{K}^n \to \mathbb{K}^m$ lineare è del tipo $F = L_A$. Sappiamo che F è della forma

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

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

$$F_i = L_{u^i} \qquad i = 1, \ldots, m \tag{10}$$

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

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

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 $L_A : \mathbb{R}^3 \to \mathbb{R}^2$, data da

$$L_A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 + 2x_2 + 3x_3 \\ 4x_1 + 5x_2 + 6_3 \end{pmatrix}$$

ovvero

$$L_A(x_1, x_2, x_3) = (x_1 + 2x_2 + 3x_3, 4x_1 + 5x_2 + 6_3).$$

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 defինzione 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 di 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

$$L_A(e_i) = A_{(i)}. \tag{11}$$

Riassumiamo quanto detto sin qui: data una generica applicazione lineare

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

la matrice A contiene le seguenti informazioni:

• Le righe corrispondono alle funzioni lineari componenti $F_1, \ldots, F_m$, 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:

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

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 assumino 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. □

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 $L_{AB} : \mathbb{K}^q \to \mathbb{K}^m$ e anche $L_A \circ L_B : \mathbb{K}^q \to \mathbb{K}^m$; 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:

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

□

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 $Id_V : V \to V$. È immediato che si tratta di un isomorfismo. Le c) e b) sono immediate conseguenza 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

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

definita da

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

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

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

e quindi $x_1 = \cdots = x_n = 0$. Dunque il $Ker(F)$ è banale.

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

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

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 $F : \mathbb{K}^n \to \mathbb{K}^m$.*

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

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

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

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

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

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

Allora per ogni $x \in \mathbb{K}^n$, posto $\bar{x} = (x_2, \ldots, x_n)$ 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 $F : \mathbb{K}^n \to \mathbb{K}^n$ e $G : \mathbb{K}^n \to \mathbb{K}$ due applicazioni lineari, $n \geq 2$. Allora l'applicazione lineare $F(e_1)G - G(e_1)F : \mathbb{K}^n \to \mathbb{K}$ 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 $\bar{x} \in \mathbb{K}^{n-1}$, $\bar{x} = (\bar{x}_1, \cdots, \bar{x}_{n-1})$, denotiamo per ogni $x_1 \in \mathbb{K}$ con $(x, \bar{x})$ il vettore $(x_1, \bar{x}_1, \cdots, \bar{x}_{n-1})$ di $\mathbb{K}^n$.

Lemma 16.5. *Data un'applicazione lineare $F : \mathbb{K}^n \to \mathbb{K}$, 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:

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

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

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

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

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

□

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

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

cioè

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

Tale applicazione è necessariamente costante, ovvero è la funzione nulla $F = 0$. Essa non è certamente ingettiva, 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 $F : \mathbb{K}^n \to \mathbb{K}^0$ è la funzione nulla $F = 0$, che non è ingettiva. Supponiamo quindi $m > 0$. Sappiamo dal Teorema 14.4 che F è della forma

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

dove le $F_i : \mathbb{K}^n \to \mathbb{K}$ sono lineari. Se $m = 1$, si tratta ancora di un'applicazione lineare $F : \mathbb{K}^n \to \mathbb{K}$, 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 $G_i : \mathbb{K}^n \to \mathbb{K}$ queste funzioni, possiamo applicare l'ipotesi induttiva all'applicazione lineare:

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

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 $Ker(G)$ 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 $F : \mathbb{K}^n \to \mathbb{K}^m$, è impossibile che si abbia $n > m$, ma considerando l'isomorfismo inverso $F^{-1} : \mathbb{K}^m \to \mathbb{K}^m$, 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 $F : \mathbb{K}^n \to W$ un isomorfismo. Allora la funzione composta

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

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