Fondamenti di algebra lineare e geometria

Corso di Laurea in Ingegneria Meccanica (Canale 2)

Lorenzo Martini

Università degli Studi di Padova

A.A. 2023-2024

Lezione 8

Richiamo della lezione precedente

- Matrici elementari.
- La forma a scala di una matrice si ottiene premoltiplicando quest'ultima per un prodotto di matrici elementari.
- Applicazioni alle matrici invertibili.

L'oggetto fondamentale del corso

Siamo pronti ad entrare nel vivo del corso. Sintetizziamo quanto detto nelle precedenti lezioni: le matrici sono "contenitori" di tuple ordinate di numeri reali: $M_{m,n}(\mathbb{R}) = \mathbb{R}^{mn}$; dunque, sono una generalizzazione ad un'arbitraria dimensione del piano reale $\mathbb{R}^2$ e dello spazio reale $\mathbb{R}^3$.

Questi ultimi insiemi, muniti della somma coordinata per coordinata, sono un modello algebrico per il piano e lo spazio dei vettori geometrici.

Ciò premesso, l'idea fondamentale del corso è quella di astrarre e generalizzare ulteriormente gli insiemi $M_{m,n}(\mathbb{R})$ visti come modelli algebrici per studiare lo spazio geometrico.

La nozione che ci serve è quella di spazio vettoriale sopra un campo, che ora introdurremo e discuteremo.

Dicendo che gli spazi vettoriali sopra un campo generalizzano $M_{m,n}(\mathbb{R})$ intendiamo dire che $M_{m,n}(\mathbb{R})$ è uno spazio vettoriale sopra un campo, e che tutto ciò che abbiamo visto sulle matrici avrà una precisa traduzione nel contesto degli spazi vettoriali.

L'esempio di $M_{m,n}(\mathbb{R})$

Per motivare le definizioni che ora daremo, ricordiamo che

- In $M_{m,n}(\mathbb{R})$ è definita una operazione di somma (quella entrata per entrata); cioè per ogni coppia di matrici $A_1, A_2 \in \mathbb{R}^n$ rimane definita una matrice $A_1 + A_2$, pure di tipo $m \times n$. Inoltre, per questa somma si verifica la seguente identità:

$$(A_1 + A_2) + A_3 = A_1 + (A_2 + A_3),$$

  per ogni $A_1, A_2, A_3 \in M_{m,n}(\mathbb{R})$. Ogni tale matrice potrà in effetti indicarsi come $A_1 + A_2 + A_3$. In particolare, in $M_{m,n}(\mathbb{R})$ possiamo formare somme finite di suoi elementi.
- Rispetto a tale somma, la matrice $m \times n$ ad entrate nulle, indicata semplicemente con 0, è tale che $A + 0 = 0 + A = A$, per ogni $A \in M_{m,n}(\mathbb{R})$.
- In $M_{m,n}(\mathbb{R})$ possiamo scalare gli elementi: dati una matrice A ed un numero reale $\lambda \in \mathbb{R}$, rimane definita la matrice $\lambda \cdot A$ (o λA), anch'essa di tipo $m \times n$, definita scalando ogni entrata di A per il fattore λ (quindi usando la moltiplicazione di $\mathbb{R}$).

L'esempio di $M_{m,n}(\mathbb{R})$

Osserviamo nuovamente che l'addizione e l'azione di scalare gli elementi di $M_{m,n}(\mathbb{R})$ consistono di operazioni che sono possibili in $\mathbb{R}$; cioè, la somma di matrici è definita tramite la somma di $\mathbb{R}$, mentre scalare una matrice si fa con mn moltiplicazioni in $\mathbb{R}$. In particolare, possiamo riscalare a piacimento: vale infatti

$$\lambda_1(\lambda_2 A) = \lambda_1\lambda_2 \cdot A,$$

per ogni $A \in M_{m,n}(\mathbb{R})$ e $\lambda_1, \lambda_2 \in \mathbb{R}$. Si osservi che tutti i prodotti denotano un riscalamento, ma il terzo, cioè $\lambda_1\lambda_2$, è l'usuale prodotto in $\mathbb{R}$.

Infine, l'addizione di $M_{m,n}(\mathbb{R})$ è compatibile con la somma e il prodotto di $\mathbb{R}$: valgono

$$\lambda(A_1 + A_2) = \lambda A_1 + \lambda A_2$$
$$(\lambda_1 + \lambda_2)A = \lambda_1 A + \lambda_2 A,$$

per tutte le $A_1, A_2, A \in M_{m,n}(\mathbb{R})$ ed i $\lambda, \lambda_1, \lambda_2 \in \mathbb{R}$.

Sugli spazi vettoriali sopra un campo

In definitiva, per generalizzare l'esempio di $M_{m,n}(\mathbb{R})$ abbiamo bisogno:

- di un insieme con una operazione di somma, diciamo $(V, +)$, e
- di un insieme $\mathbb{K}$ con cui scalare gli elementi di V; tale $\mathbb{K}$ dovrà dunque avere una propria moltiplicazione (per riscalare a piacimento) ed una propria addizione (per avere compatibilità con la somma di V).

In questo senso, V sarà lo spazio vettoriale e $\mathbb{K}$ il campo su cui V è definito.

Con queste premesse, possiamo dare le definizioni formali di campo e di spazio vettoriale su di esso.

Notazione

Ricordiamo che un'operazione ω su un insieme S è una qualsiasi funzione $S \times S \to S$, la cui immagine su un generico elemento $(x_1, x_2) \in S \times S$ si scrive, in luogo di $\omega(x_1, x_2)$, come $x_1 \, \omega \, x_2$. Più precisamente, indicheremo ω come

$$\begin{aligned} \omega\colon S \times S &\longrightarrow S \\ (x_1, x_2) &\longmapsto x_1 \, \omega \, x_2 \,. \end{aligned}$$

Definizione di campo

Iniziamo con la definizione di campo. Come detto, vogliamo un insieme con due operazioni, che potremo chiamare rispettivamente addizione e moltiplicazione, come si fa in $\mathbb{R}$.

Definizione

Un campo è un insieme $\mathbb{K}$ munito di due operazioni

$$\begin{aligned} +\colon \mathbb{K}\times\mathbb{K} &\longrightarrow \mathbb{K} \\ (\lambda_1,\lambda_2) &\longmapsto \lambda_1+\lambda_2 \end{aligned} \quad \text{e} \quad \begin{aligned} *\colon \mathbb{K}\times\mathbb{K} &\longrightarrow \mathbb{K} \\ (\lambda_1,\lambda_2) &\longmapsto \lambda_1\lambda_2 \end{aligned}$$

soddisfacenti rispettivamente alle seguenti proprietà:

- A1 $(\lambda_1+\lambda_2)+\lambda_3=\lambda_1+(\lambda_2+\lambda_3)$ per ogni $\lambda_1,\lambda_2,\lambda_3\in\mathbb{K}$;
- A2 $\lambda_1+\lambda_2=\lambda_2+\lambda_1$ per ogni $\lambda_1,\lambda_2\in\mathbb{K}$;
- A3 esiste un elemento $0\in\mathbb{K}$ tale che $\lambda+0\,(=0+\lambda)=\lambda$ per ogni $\lambda\in\mathbb{K}$;
- A4 per ogni $\lambda\in\mathbb{K}$ esiste $\lambda^+\in\mathbb{K}$ tale che $\lambda+\lambda^+=0$.

Definizione di campo

- M1 $(\lambda_1 * \lambda_2) * \lambda_3 = \lambda_1 * (\lambda_2 * \lambda_3)$ per ogni $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K}$;
- M2 $\lambda_1 * \lambda_2 = \lambda_2 * \lambda_1$ per ogni $\lambda_1, \lambda_2 \in \mathbb{K}$;
- M3 esiste un elemento $1 \in \mathbb{K}$ tale che $\lambda * 1 \,(= 1 * \lambda) = \lambda$ per ogni $\lambda \in \mathbb{K}$;
- M4 per ogni $\lambda \in \mathbb{K}$, $\lambda \neq 0$, esiste $\lambda^* \in \mathbb{K}$ tale che $\lambda * \lambda^* = 1$.
- AM Valgono

$$(\lambda_1 + \lambda_2) * \lambda = \lambda_1\lambda + \lambda_2\lambda$$
$$\lambda * (\lambda_1 + \lambda_2) = \lambda\lambda_1 + \lambda\lambda_2,$$

per ogni $\lambda, \lambda_1, \lambda_2 \in \mathbb{K}$.

Commentiamo la definizione di campo:

- Le proprietà A1 e A2 (M1 ed M2), sono dette rispettivamente proprietà associativa e commutativa di $+$ (di $*$).
- La proprietà A3 (M3) assicura l'esistenza di un elemento neutro per $+$, detto lo zero di $\mathbb{K}$ (di un elemento neutro per $*$, detto l'uno di $\mathbb{K}$).

Definizione di campo

- La proprietà A4 (M4) garantisce l'esistenza di un inverso additivo, detto anche opposto, per ogni $\lambda \in \mathbb{K}$ (di un inverso moltiplicativo, per ogni $\lambda \neq 0$).
- Le identità in AM sono le proprietà distributive di $+$ con $*$.
- Gli elementi 0 ed 1 sono unici rispetto alle proprietà descritte sopra.
- L'inverso additivo di λ e l'inverso moltiplicativo di $\lambda \neq 0$ sono unici. Saranno indicati rispettivamente come $-\lambda$ e $\lambda^{-1} = 1/\lambda$. In particolare, scriveremo $\lambda_1 - \lambda_2$ in luogo di $\lambda_1 + (-\lambda_2)$, per ogni $\lambda_1, \lambda_2 \in \mathbb{K}$.

In definitiva, un campo è un insieme con due operazioni per le quali abbiamo la massimà libertà aritmetica (possiamo formare gli inversi). Ad esempio, gli insiemi $\mathbb{N}$ e $\mathbb{Z}$ con le usuali addizione e moltiplicazione <u>non</u> formano un campo.

Esempi di campo

Esempio

(1) $\mathbb{Q} := \{p/q \mid p, q \in \mathbb{Z},\ q \neq 0\}$, $\mathbb{R}$ e $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R},\ i^2 = -1\}$ sono campi, i cui zero ed uno sono quelli usuali. Ricordiamo che l'inverso moltiplicativo di $p/q \in \mathbb{Q}$ è q/p (è $p/q \neq 0$ se $p \neq 0$), mentre l'inverso di $z = a + bi \neq 0 + 0i$ in $\mathbb{C}$ è

$$z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\, i = \frac{a - ib}{a^2 + b^2}\ .$$

(2) Esistono campi finiti, cioè con un numero finito di elementi. Ad esempio, $\mathbb{F} := \{0, 1, a\}$ con le seguenti due operazioni

$$\begin{array}{c|ccc} + & 0 & 1 & a \\ \hline 0 & 0 & 1 & a \\ 1 & 1 & a & 0 \\ a & a & 0 & 1 \end{array} \qquad \text{e} \qquad \begin{array}{c|ccc} * & 0 & 1 & a \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & a \\ a & 0 & a & 1 \end{array}$$

è un campo con tre elementi.

Esempi di campo

(3) In generale, per ogni numero primo p possiamo formare un campo finito con p elementi come segue. Per ogni $a \in \mathbb{Z}$, sia $\bar{a}$ il resto della divisione euclidea di a per p. Al variare di a, ci sono quindi p possibili resti, cioè

$$\{\bar{a} \mid a \in \mathbb{Z}\} = \{\,\bar{0}, \bar{1}, \ldots, \overline{p-1}\,\}\,.$$

Su questo insieme, indicato $\mathbb{Z}_p$, definiamo addizione e moltiplicazione ponendo

$$\bar{a} + \bar{b} := \overline{a+b}$$
$$\bar{a}\ \cdot\ \bar{b} := \overline{a\ \cdot\ b},$$

per ogni $a, b \in \mathbb{Z}$. Si dimostra che $\mathbb{Z}_p$ è un campo; ad esempio, $\bar{a} \neq \bar{0}$ se p non divide a, e in questo caso $1/\bar{a} = \bar{a}^{\,\phi(a)-1}$, $\phi(a)$ essendo la funzione di Eulero di a.
(Ricordiamo che $\phi(a) = |\{n \in \mathbb{N} \mid 1 \leq n < a,\ \mathrm{MCD}(a, n) = 1\}|$. Ad ogni modo, per p piccolo, gli inversi si possono trovare semplicemente facendo dei tentativi.)

Definizione di spazio vettoriale

Passiamo ora a definire gli spazi vettoriali.

Definizione

Sia $(\mathbb{K}, +, *)$ un campo fissato. Uno spazio vettoriale sopra il campo $\mathbb{K}$ è un insieme V munito di una operazione $+$ e di un'applicazione di scala, indicate

$$\begin{aligned} +\colon V \times V &\longrightarrow V \\ (v_1, v_2) &\longmapsto v_1 + v_2 \end{aligned} \qquad \text{e} \qquad \begin{aligned} \mathbb{K} \times V &\longrightarrow V \\ (\lambda, v) &\longmapsto \lambda v, \end{aligned}$$

soddisfacenti rispettivamente alle seguenti proprietà:

- A1 $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$ per ogni $v_1, v_2, v_3 \in V$;
- A2 $v_1 + v_2 = v_2 + v_1$ per ogni $v_1, v_2 \in V$;
- A3 esiste un elemento $0 \in V$ tale che $v + 0\,(= 0 + v) = v$ per ogni $v \in V$;
- A4 per ogni $v \in V$ esiste $-v \in V$ tale che $v + (-v) = 0$.

Definizione di spazio vettoriale

V1 $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$ per ogni $v_1, v_2 \in V$ e $\lambda \in \mathbb{K}$;

V2 $(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$ per ogni $v \in V$ e $\lambda_1, \lambda_2 \in \mathbb{K}$;

V3 $\lambda_1(\lambda_2 v) = (\lambda_1\lambda_2)v$ per ogni $v \in V$ e $\lambda_1, \lambda_2 \in \mathbb{K}$;

V4 $1_{\mathbb{K}} v = v$ per ogni $v \in V$.

- Gli assiomi An sono gli stessi che valgono per l'addizione in un campo;
- gli assiomi Vn danno la compatibilità delle operazioni di V con quelle del campo soggiacente $\mathbb{K}$. Si noti nuovamente in V3 il ruolo dei singoli prodotti, cioè se questi sono riscalamenti in V oppure prodotti in $\mathbb{K}$.
- Lo zero di V è diverso dallo zero di $\mathbb{K}$; tuttavia, si conviene di denotarli con lo stesso simbolo 0 (del resto, entrambe le addizioni vengono indicate con lo stesso simbolo $+$). A volte, per distinguere tali elementi neutri potremo indicare lo zero di V come $\vec{0}$.
- Nel contesto degli spazi vettoriali, gli elementi di V vengono chiamati vettori, mentre gli elementi del suo campo base $\mathbb{K}$ si chiamano scalari.

Esempi di spazio vettoriale

Esempio

(1) Fissati $m, n \in \mathbb{N}$, l'insieme $M_{m,n}(\mathbb{R})$ è uno spazio vettoriale sopra il campo $\mathbb{R}$, con le operazioni introdotte precedentemente. (Il suo $\vec{0}$ è la matrice $m \times n$ ad entrate nulle, che avevamo indicato con 0.) In particolare, $\mathbb{R}^n$ è spazio vettoriale reale.

(2) Tutto ciò che abbiamo detto precedentemente su $M_{m,n}(\mathbb{R})$ può essere riformulato sostituendo $\mathbb{R}$ con un campo arbitrario $\mathbb{K}$. Rimane così definito l'insieme $M_{m,n}(\mathbb{K})$ delle matrici $m \times n$ ad entrate nel campo $\mathbb{K}$, con la propria struttura di $\mathbb{K}$-spazio vettoriale. In particolare, $\mathbb{K}^n$ è spazio vettoriale su $\mathbb{K}$.
(Possiamo pure risolvere sistemi lineari a coefficienti in $\mathbb{K}$ con il metodo di eliminazione di Gauss risultante.)

(3) Ogni campo $\mathbb{K}$ è spazio vettoriale sopra se stesso.

(4) Se $F \subseteq K$ è una inclusione tra campi, allora ogni K-spazio vettoriale V diventa automaticamente un F-spazio vettoriale, in cui l'azione scalare è quella usuale su K ma ristretta ad F.
Ad esempio, $M_{m,n}(\mathbb{C})$ è spazio vettoriale su $\mathbb{C}, \mathbb{R}, \mathbb{Q}$.

Esempi di spazio vettoriale

(5) Sia $\mathbb{K}$ un campo ed x un'indeterminata. Ricordiamo che si chiama polinomio in x di grado n a coefficienti in $\mathbb{K}$ una espressione formale del tipo

$$p(x) := a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

dove $n \in \mathbb{N}$ ed $a_0, \ldots, a_n \in \mathbb{K}$, con $a_n \neq 0$. Dati polinomi $p(x) = \sum_{k=0} a_k x^k$ e $q(x) = \sum_{k=0}^{m} b_k x^k$, in x, di grado n ed m rispettivamente, definiamo:

$$p(x) + q(x) := \sum_{k=0}^{n+m} (a_k + b_k) x^k \qquad \begin{aligned} a_k &= 0 \quad \text{se } k > n, \\ b_k &= 0 \quad \text{se } k > m. \end{aligned}$$

È facile verificare che l'insieme $\mathbb{K}[x]$ dei polinomi in x a coefficienti in $\mathbb{K}$ è uno spazio vettoriale su $\mathbb{K}$ rispetto alla somma appena definita, il suo $\vec{0}$ essendo il polinomio nullo $0(x) = 0$.

Ricordiamo inoltre che in $\mathbb{K}[x]$ è definito un prodotto come segue:

$$p(x) \cdot q(x) := \sum_{k=0}^{t} \Big(\sum_{i+j=k} a_i b_j \Big) x^k, \qquad t := \max\{n, m\}.$$

Esempi di spazio vettoriale

L'insieme $\mathbb{K}[x]$, munito delle operazioni di somma e prodotto appena definite, non ammette mai una struttura di campo (solamente le costanti non nulle sono polinomi invertibili). Idem per $M_n(\mathbb{K})$, $n \geq 2$.

(6) Dato un campo $\mathbb{K}$, l'insieme $\mathcal{F} = \{f : \mathbb{K} \to \mathbb{K}\}$ di tutte le funzioni di $\mathbb{K}$ in se stesso è uno spazio vettoriale su $\mathbb{K}$, rispetto all'addizione e all'azione di scala definite rispettivamente come

$$\begin{aligned} +\colon \mathcal{F} \times \mathcal{F} &\longrightarrow \mathcal{F} \\ (f, g) &\longmapsto f + g\colon \mathbb{K} \longrightarrow \mathbb{K} \\ &\qquad\qquad\qquad x \longmapsto f(x) + g(x) \end{aligned}$$

e

$$\begin{aligned} \mathbb{K} \times \mathcal{F} &\longrightarrow \mathcal{F} \\ (\lambda, f) &\longmapsto \lambda f\colon \mathbb{K} \longrightarrow \mathbb{K} \\ &\qquad\qquad\quad x \longmapsto \lambda \cdot f(x) \end{aligned}$$

cioè "punto a punto": $(f+g)(x) = f(x) + g(x)$ e $(\lambda f)(x) = \lambda f(x)$, per ogni $x \in \mathbb{K}$. (Lo zero è la funzione costante 0.)

Concludiamo dimostrando alcune proprietà generali.

Proprietà in uno spazio vettoriale

Lemma

Sia V un $\mathbb{K}$-spazio vettoriale. Allora

(i) $0v = \vec{0}$ per ogni $v \in V$;

(ii) $\lambda\vec{0} = \vec{0}$ per ogni $\lambda \in \mathbb{K}$;

(iii) $1(-v) = -v$ per ogni $v \in V$;

(iv) se $\lambda v = \vec{0}$, allora $\lambda = 0$ oppure $v = \vec{0}$.

Dimostrazione.

(i) Abbiamo $0v = (0+0)v \overset{\text{V2}}{=} 0v + 0v$, quindi cancellando $0v$ dai membri esterni di queste uguaglianze otteniamo quanto voluto.

(ii) Analoga ad (i), usando V1.

(iii) Abbiamo $v + 1(-v) \overset{\text{V4}}{=} v + (-v) = v - v = \vec{0}$, quindi si conclude per unicità dell'inverso.

(iv) Sia $\lambda v = \vec{0}$, con $\lambda \neq 0$. Allora $\vec{0} = \lambda^{-1}\vec{0} = \lambda^{-1}(\lambda v) \overset{\text{V3}}{=} (\lambda^{-1}\lambda)v \overset{\text{V4}}{=} v$, da cui $v = 0$. Da ciò segue anche che, per ogni $\lambda \neq 0$, l'applicazione $\dot{\lambda}\colon V \to V$, $v \mapsto \lambda v$ è iniettiva. Quindi, se $\lambda v = \vec{0}$ e $v \neq \vec{0}$, allora necessariamente $\lambda = 0$. $\square$