Corso di Algebra Lineare e Geometria
Strutture Algebriche

Docente **Marino Lucia**

Università di Catania

email: lucia.marino@unict.it
Sito web: https://www.dmi.unict.it/lmarino/

Testi consigliati

Libri **esercizi**:
P. Bonacini, M.G. Cinquegrani, L. Marino, *Algebra Lineare: Esercizi svolti*, Ed. Cavallotto, Catania 2012
P. Bonacini, M.G. Cinquegrani, L. Marino, *Geometria Analitica: Esercizi svolti*, Ed. Cavallotto, Catania 2012

Concetto di funzione tra due insiemi A e B

Dati due insiemi A e B, si dice *funzione* da A in B una legge che associa a **ogni elemento di A uno e un solo elemento di B**.

Notazione formale:

$$f : A \to B, \quad x \in A \mapsto f(x) \in B$$

Esempio: $A =$ figli, $B =$ madri.
Viceversa:

$$f : B \to A$$

non è una funzione, poiché a una madre possono corrispondere più figli.

Immagine di f

- A si chiama **dominio**.
- B si chiama **codominio**.
- Diremo *immagine* di f, indicata con $\operatorname{Im} f$, il sottoinsieme di B costituito dalle immagini di tutti gli elementi di A:

$$\operatorname{Im} f = \{\, b \in B \mid \exists a \in A \text{ con } f(a) = b \,\}$$

Operazione binaria interna

Generalizziamo il concetto di operazione elementare su cui abbiamo imparato a fare i calcoli.

Si chiama *operazione binaria interna* su un insieme A una funzione

$$\phi : A \times A \to A$$

Esempi:

1. Sia A l'insieme dei vettori. La somma tra due vettori è un'operazione binaria interna su A.
2. Il prodotto scalare tra due vettori **non** è un'operazione binaria interna su A.

Proprietà di un'operazione binaria

Un'operazione binaria su un insieme G può avere le seguenti proprietà:

- **Associativa:**

$$\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$$

- **Commutativa:**

$$\forall a, b \in G, \quad a * b = b * a$$

- **Elemento neutro:** esiste $e \in G$ tale che

$$\forall a \in G, \quad a * e = e * a = a$$

  Se esiste, è unico.

- **Invertibilità:** Se G ammette l'elemento neutro e, un elemento $a \in G$ si dice *invertibile* se esiste $a' \in G$ tale che

$$a * a' = a' * a = e$$

  In questo caso, a' si dice **elemento inverso** di a.

Gruppo

- Un insieme G su cui è definita un'operazione $*$, $(G, *)$, è un **gruppo** se valgono le seguenti proprietà rispetto all'operazione assegnata:
  1. Associativa: $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$
  2. Esistenza dell'elemento neutro $e \in G$, tale che $\forall a \in G,\ a * e = e * a = a$
  3. Ogni elemento di G è invertibile, cioè per ogni $a \in G$ esiste $a' \in G$ tale che $a * a' = a' * a = e$
- Se l'operazione è anche commutativa, il gruppo si dice **Abeliano o commutativo**.

Anello

- Dato un insieme A con due operazioni $(A, +, *)$, si dice **anello** se valgono le seguenti proprietà:
  1. $(A, +)$ è un **gruppo abeliano**.
  2. L'operazione $*$ è **associativa**:
  $$\forall a, b, c \in A, \quad (a * b) * c = a * (b * c)$$
  3. **Proprietà distributive** di $*$ rispetto a $+$:
  $$\forall a, b, c \in A, \quad a * (b + c) = a * b + a * c, \quad (a + b) * c = a * c + b * c$$
  4. Se $*$ è anche **commutativa**, l'anello si dice **commutativo**.

Esempi di Anelli

- Esempi di anelli commutativi sono:

$$(\mathbb{Z}, +, *), \quad (\mathbb{Q}, +, *), \quad (\mathbb{R}, +, *)$$

- Non è necessario che esista l'elemento neutro 1 della seconda operazione. Se invece esiste, l'anello si dice **unitario**.
- Lo **zero** di un anello non può essere mai invertibile.

Campo $\mathbb{K}$

- Si dice **campo** $(\mathbb{K}, +, \cdot)$ un **anello commutativo** in cui ogni elemento diverso da zero è *invertibile* rispetto al prodotto.

  In altre parole:

  $$\forall a \in \mathbb{K} \setminus \{0\}, \quad \exists\, a^{-1} \in \mathbb{K} \text{ tale che } a \cdot a^{-1} = 1.$$

- Tutti i numeri razionali $\mathbb{Q}$, reali $\mathbb{R}$ e complessi $\mathbb{C}$ sono esempi di campi.

Esempi di campo

- Esempio di un insieme che **non è un campo**:

$$(\mathbb{Z}, +, *)$$

- Esempio di un insieme che **è un campo**:

$$(\mathbb{Q}, +, *)$$

Campo dei numeri reali $\mathbb{R}$

- L'insieme dei numeri reali con le operazioni di somma e prodotto, $(\mathbb{R}, +, \cdot)$, è un **campo**.
- In $\mathbb{R}$ ogni elemento diverso da zero è **invertibile** rispetto al prodotto:

$$\forall x \in \mathbb{R} \setminus \{0\}, \quad \exists\, x^{-1} \in \mathbb{R} \text{ tale che } x \cdot x^{-1} = 1.$$

Campo dei numeri complessi $\mathbb{C}$

- L'insieme dei numeri complessi con le operazioni di somma e prodotto, $(\mathbb{C}, +, \cdot)$, è un **campo** che contiene il campo dei numeri reali $\mathbb{R}$.
- In $\mathbb{C}$ ogni elemento diverso da zero è **invertibile** rispetto al prodotto. Sia $z = a + ib \neq 0$. Cerchiamo $w = c + id$ tale che:

$$(a + ib)(c + id) = 1.$$

Dalla condizione di invertibilità segue che:

$$w = \frac{a - ib}{a^2 + b^2}.$$

Quindi l'elemento $\frac{a - ib}{a^2 + b^2}$ è **l'inverso moltiplicativo** di $a + ib$ (verificabile con un semplice calcolo algebrico).

Operazione esterna

Definizione

Sia V un insieme e $\mathbb{K}$ un campo. Chiamiamo **operazione esterna** una funzione

$$f : \mathbb{K} \times V \longrightarrow V, \qquad (\alpha, v) \longmapsto \alpha * v,$$

dove $\alpha \in \mathbb{K}$ e $v \in V$.

Sottostrutture

Dato un gruppo $(G, +)$, sia $S \subseteq G$. Diremo che $(S, +)$ è un **sottogruppo** di $(G, +)$ se S è un gruppo rispetto alla stessa operazione di G.

In modo analogo si definiscono *sottoanello* e *sottocampo*.

Spazio Vettoriale

Sia $\mathbb{K}$ un campo e V un insieme qualsiasi.

Dicesi **spazio vettoriale** $(V, +, \cdot)$ su un campo $\mathbb{K}$, oppure $\mathbb{K}$-**spazio vettoriale**, una struttura dotata di due operazioni:

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

dette rispettivamente **somma vettoriale** e **prodotto scalare**, tali che valgono le seguenti proprietà:

1. $(V, +)$ è un **gruppo abeliano**.
2. **Compatibilità tra scalari:** $(ab) \cdot v = a \cdot (b \cdot v)$ per ogni $a, b \in \mathbb{K}$ e $v \in V$.
3. **Elemento neutro scalare:** $1 \cdot v = v$ per ogni $v \in V$.
4. **Distributività rispetto ai numeri:** $(a + b) \cdot v = a \cdot v + b \cdot v$ per ogni $a, b \in \mathbb{K}$ e $v \in V$.
5. **Distributività rispetto ai vettori:** $a \cdot (v + w) = a \cdot v + a \cdot w$ per ogni $a \in \mathbb{K}$ e $v, w \in V$.

Esempi di spazi vettoriali

Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo $\mathbb{K}$: gli elementi di V si chiamano **vettori**, quelli di $\mathbb{K}$ **scalari**.

Esempi principali:

- **Ogni campo** $\mathbb{K}$ è uno spazio vettoriale su sé stesso.
- $\mathbb{R}^3$ con le usuali operazioni di somma e prodotto per scalare è uno spazio vettoriale su $\mathbb{R}$.
- Più in generale, $\mathbb{K}^n$ con:

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1,\ x_2 + y_2,\ \ldots,\ x_n + y_n)$$

$$a \cdot (x_1, x_2, \ldots, x_n) = (ax_1,\ ax_2,\ \ldots,\ ax_n)$$

è uno spazio vettoriale su $\mathbb{K}$.