# Lezione 12 - 27/10/2022



## Definzione - Spazio vettoriale

Uno spazio vettoriale su $\mathbb{K}$ (campo) è un **insieme non vuoto** $V$ dotato di un'**operazione binaria** $+$ rispetto alla quale $V$ è un **gruppo abeliano** e di un'applicazione

$$\begin{aligned}\mathbb{K} \times V &\to V \\ (\alpha,\ v) &\mapsto \alpha v\end{aligned}$$

tale che

$$\begin{aligned}(\alpha+\beta)v &= \alpha v + \beta v && \forall \alpha, \beta \in \mathbb{K},\ \forall v \in V \\ (\alpha\beta)v &= \alpha(\beta v) && \forall \alpha, \beta \in \mathbb{K},\ \forall v \in V \\ \alpha(v_1+v_2) &= \alpha v_1 + \alpha v_2 && \forall \alpha \in \mathbb{K},\ \forall v_1, v_2 \in V \\ 1v &= v && \forall v \in V\end{aligned}$$

Nomenclatura

- Gli elementi di $V$ si chiamano **vettori**
- Gli elementi di $\mathbb{K}$ si chiamano **scalari**

Esempi

1. Sia $\mathbb{K}$ un campo e $V = \mathbb{K}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{K}\}$

   Prendiamo come esempio $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$

   $$\begin{aligned}(x_1, ..., x_n) + (y_1, ..., y_n) &= (x_1 + y_1, ..., x_n + y_n) \\ \alpha(x_1, ..., x_n) &= (\alpha x_1, ..., \alpha x_n)\end{aligned}$$

   Esempio pratico

   $$\begin{aligned}&4(2,1,6) + 5(-1, 2, \frac{1}{4}) + \frac{3}{2}(0,1,3) = \\ =&(8,4,24) + (-5, 10, \frac{5}{4}) + (0, -\frac{3}{2}, -\frac{9}{2}) = (3, \frac{25}{2}, \frac{83}{4})\end{aligned}$$

2. Definzione: Una matrice a $m$ righe e $n$ colonne a **coefficienti nel campo** $\mathbb{K}$ è una tabella di elementi di $\mathbb{K}$ del tipo

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & a_{ij} & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Chiamiamo $M_{mn}(\mathbb{K})$ tale insieme.
Diciamo che una matrice è **quadrata** se $m = n$

Notazione:

Se $A \in M_{mn}(\mathbb{K})$ denoto con

- $(A)_{ij}$ l'elemento di posto $(i, j)$
- $A^i$ l'i-esima colonna
- $A_j$ la j-esima riga

Esempio

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 5 & 6 \end{pmatrix}$$
$$(A)_{11} = 1 \quad (A)_{12} = 2 \quad (A)_{13} = 3$$
$$(A)_{21} = 4 \quad (A)_{22} = 5 \quad (A)_{23} = 6$$
$$A^1 = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \quad A^2 = \begin{pmatrix} 2 \\ 5 \end{pmatrix} \quad A^3 = \begin{pmatrix} 3 \\ 6 \end{pmatrix}$$
$$A_1 = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \quad A_1 = \begin{pmatrix} 4 & 5 & 6 \end{pmatrix}$$

$M_{mn}(\mathbb{K})$ è uno **spazio vettoriale** rispetto a

$$\begin{aligned} (A + B)_{ij} = (A)_{ij} + (B)_{ij} \qquad & 1 \leq i \leq m \\ & 1 \leq j \leq n \\ \alpha \in \mathbb{K} \quad (\alpha A)_{ij} = \alpha (A)_{ij} \qquad & 1 \leq i \leq m \\ & 1 \leq j \leq n \end{aligned}$$

N.B.:

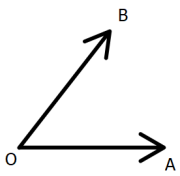
- se $m = n = 1,\ M_{11}(\mathbb{K}) = \mathbb{K}$, dunque ogni campo è uno **spazio vettoriale su se stesso**;
- se $m = 1,\ M_{1n}(\mathbb{K}) = \mathbb{K}^n$, chiamati **vettori riga**;
- se $n = 1,\ M_{m1}(\mathbb{K}) \leftrightarrow \mathbb{K}^m$, chiamati **vettori colonna**.

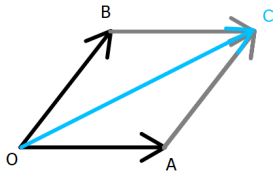
3. **Vettori geometrici**

   Consideriamo lo spazio **bidimensionale della geometria euclidea** e fissiamo un punto $o$. Chiamiamo **vettore** un segmento orientato $\overrightarrow{AB}$. Definiamo una struttura di **spazio vettoriale su** $\mathbb{R}$ sull'insieme $\nu_0$ dei vettori applicati in $o$.

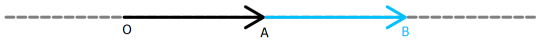
   $$\nu_0 = \{\overrightarrow{OA} : a \in \mathbb{E}^3\}$$

   - $\overrightarrow{OA} + \overrightarrow{OB} = \overrightarrow{OC}$



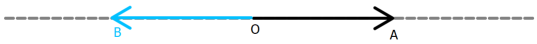




- $0 \cdot \overrightarrow{OA} = \overrightarrow{OO}$
  $\alpha \cdot \overrightarrow{OO} = \overrightarrow{OO}$
  - Se $\alpha > 0$



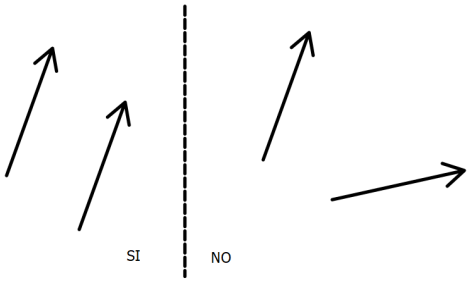

$$\overrightarrow{OB} = \alpha \cdot \overrightarrow{OA}$$

  - Se $\alpha < 0$




$$\overrightarrow{OB} = \alpha \cdot \overrightarrow{OA}$$

Si definiscono poi i **vettori liberi** come lo spazio di vettori applicati modulo la **relazione di equivalenza** che identifica due vettori applicati se esiste una **traslazione** che manda uno all'altro




le operazioni di $\nu_0$ passano al quoziente.

# Prodotto righe per colonne tra matrici

Per comodità scrivo $M_{mn}$ invece di $M_{mn}(\mathbb{K})$.

$$M_{ms} \times M_{sn} \to M_{mn}$$

$$(AB)_{ij} = \sum_{k=1}^{s} (A)_{ik} \cdot (B)_{ki}, \quad 1 \leq i \leq m,\ 1 \leq j \leq n$$

Esempio:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 0 & 1 & 4 & -1 \\ 2 & 3 & 0 & 4 \\ 3 & 6 & -1 & -1 \end{pmatrix} =$$
$$= \begin{pmatrix} 1\cdot 0+2\cdot 2+3\cdot 3 & 1\cdot 1+2\cdot 3+3\cdot 6 & 1\cdot 4+2\cdot 0+3\cdot(-1) & 1\cdot(-1)+2\cdot 4+3\cdot(-1) \\ 4\cdot 0+5\cdot 2+6\cdot 3 & 4\cdot 1+5\cdot 3+6\cdot 6 & 4\cdot 4+5\cdot 0+6\cdot(-1) & 4\cdot(-1)+5\cdot 4+6\cdot(-1) \end{pmatrix} =$$
$$= \begin{pmatrix} 13 & 25 & 1 & 4 \\ 28 & 55 & 10 & 10 \end{pmatrix}$$

## Proposizone

Se $A \in M_{ms},\ B \in M_{st},\ C \in M_{tn}$

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

## Osservazione

Nel caso delle matrici quadrate $M_n$, il prodotto righe per colonne è un'operazione binaria associativa per la proprietà precedente che, per elemento neutro ha la **matrice identità**

$$I_n = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & ... & 1 & 0 \\ 0 & ... & 0 & 1 \end{pmatrix}$$

$(I_n)_{ij} = \delta_{ij}$ dove $\delta_{ij}$ è detta la **delta di Krnoecker** ed è definita come segue

$$\delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

ovvero vale $1$ solamente nella **diagonale** e tutto il resto è $0$.

## Proposizione

$M_n(\mathbb{K})$ è un **anello con unità**.
N.B.: se $n \geq 2$, $M_n(\mathbb{K})$ **non è commutativo**

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} \quad = \quad \begin{pmatrix} -2 & 8 \\ -3 & 18 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad = \quad \begin{pmatrix} 6 & 8 \\ 8 & 10 \end{pmatrix}$$

# Esempi di gruppi

1. $(\mathbb{Z}, +),\ (\mathbb{Z}_n, +)$
2. $(\nu, +),\ \nu$ spazio vettoriale $(\nu = \mathbb{R},\ \mathbb{Q})$
3. $S_n$
4. $\mathbb{U}_n$ elementi invertibili in $\mathbb{Z}_n$
5. $(\mathbb{K} \setminus \{0\}, \cdot)$

# Domanda

Abbiamo visto che $M_n$ sono **un anello**; possiamo chiederci se $M_n \setminus \{0\}$ è un **gruppo** rispetto il **prodotto righe per colonne**. Questo è vero se per ogni $A \in M_n,\ A \neq 0\ \exists B \in M_n$ tale che

$$AB = BA = I_n \quad (*)$$

Questo in generale è **falso**. Dimostreremo che esiste una funzione detta **determinante**

$$\det : M_n(\mathbb{K}) \to \mathbb{K}$$

tale che

$$A \text{ è invertibile } \iff \det A \neq 0$$

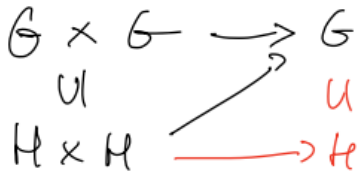
cioè vale $(*)$. Quindi $\{A \in M_n(\mathbb{K}) : \det A \neq 0\}$ è un gruppo **infinito** (se $\mathbb{K}$ è infinito) **non abeliano** se $n \geq 2$.

Esempio:

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

# Definizione - Sottogruppo

Sia $G$ un **gruppo**. Diciamo che $\emptyset \neq H \subseteq G$ è un **sottogruppo** di $G$ (notazione: $H \leq G$) se $H$ è un **gruppo rispetto all'operazione indotta da $G$.**




Osservazione: $H \leq G$ se e solo se

1. $\forall h_1, h_2 \in H \qquad h_1 \cdot h_2 \in H$
2. $e \in H$
3. $\forall h \in H,\ h^{-1} \in H$

## Proposizione

$$H \leq G \iff ab^{-1} \in H, \quad \forall a, b \in H\ (*)$$

con questa scrittura sono state compattate le tre proprietà sopra.

Nota: in notazione additiva:

$$ab^{-1} \in H \text{ diventa } a - b \in H$$

Dimostrazione: Supponiamo che valgano *1. 2.* e *3.* e vediamo che vale $(*)$.

Dati $a, b \in H$, per la proprietà *3.* si ha $b^{-1} \in H$ e per la *1.* $ab^{-1} \in H$, quindi vale $(*)$.

Supponiamo che valga $(*)$, dobbiamo dimostrare *1. 2.* e *3.*

Prendiamo in $(*)$ $a = b$

$$ab^{-1} = aa^{-1} = e \in H$$

quindi vale *2.* Prendiamo in $(*)$ $a = e,\ b = h$. Abbiamo

$$e \cdot h^{-1} = h^{-1} \in H$$

quindi vale *3.* Infine prendiamo in $(*)$ $a = h_1,\ b = h_2^{-1}$

$$ab^{-1} = h_1(h_2^{-1})^{-1} = h_1 \cdot h_2 \in H$$

quindi vale *1.*

Esempio: **il centro di un gruppo**. Sia $G$ un gruppo. Definiamo

$$Z(G) = \{x \in G : xy = yx\ \forall y \in G\}$$

osserviamo che $G$ è **abeliano** se e solo se $Z(G) = G$ (tutti gli elmenti in $G$ commutano). In generale si ha $Z(G) \leq G$.

Verifichiamolo usando la proposizione precedente: $x, y \in Z(G) \Rightarrow xy^{-1} \in Z(G)$

- **Ipotesi**:

$$\begin{array}{ll} xg = gx & \forall g \in G\ (2) \\ yg = gy & \forall g \in G \end{array}$$

- **Tesi**: $xy^{-1}g = gxy^{-1} \quad \forall g \in G$

  $yg = gy$ può essere riscritta come

$$\begin{array}{ll} y^{-1}ygy^{-1} = y^{-1}gyy^{-1} & \text{moltiplico } y^{-1} \text{ a sx e dx} \\ gy^{-1} = y^{-1}g\ (1) & \end{array}$$

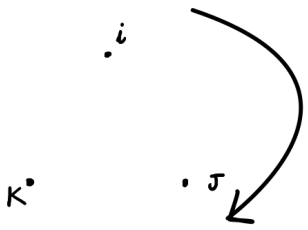
  Da cui si ricava

$$xy^{-1}g = x(y^{-1}g) \overset{(1)}{=} x(gy^{-1}) = (xg)y^{-1} \overset{(2)}{=} (gx)y^{-1} = gxy^{-1}$$

Esempio: $Q$ **:** unità dei **quaternioni**

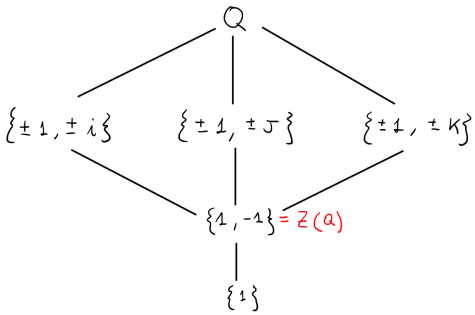
$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

Le regole moltiplicative seguono dal seguente disegno:




- $i^2 = j^2 = k^2 = -1$
- $ij = k \quad jk = i \quad ki = j$
- $ji = -k \quad kj = -i \quad ik = -j$

I **sottogruppi generati** sono i seguenti:




# Sottogruppi di Z

Proposizione: i sottogruppi di $\mathbb{Z}$ sono tutti e soli del tipo $n\mathbb{Z},\ n \in \mathbb{N}$.

Dimostrazione: vediamo prima di tutto che $n\mathbb{Z}$ è un sottogruppo. Per la proposizione dobbiamo vedere che se $x, y \in n\mathbb{Z}$, allora $x - y \in n\mathbb{Z}$ (ricordiamo che $\mathbb{Z}$ non + un gruppo rispetto alla moltiplicazione, quindi usiamo la notazione additiva).

Ma $x, y \in n\mathbb{Z}$ significa $x = na,\ y = nb$, per cui

$$x - y = na - nb = n(a - b) \in n\mathbb{Z}$$

Viceversa, sia $H \leq \mathbb{Z}$; se $H = \{0\}$ allora $H = n\mathbb{Z}$ con $n = 0$. Quindi possiamo supporre che esista $h \in H, n \neq 0$; poiché $H \leq \mathbb{Z}$, se $h \in H$, anche $-h \in H$, quindi posso supporre $h > 0$. Sia

$$\emptyset \neq H' = \{h \in H : h > 0\}$$

Quindi esiste $\overline{h} = \min H'$.

Dico che $H = \overline{h}\mathbb{Z}$. È chiaro che $\overline{h}\mathbb{Z} \subseteq H$, perchè $\overline{h} \in H$ e quindi tutti i multipli di $\overline{h}$ appartengono ad $H$ ($H \leq \mathbb{Z}$).

Viceversa, prendo $x \in H$ e scrivo

$$x = q\overline{h} + r \qquad 0 \leq r < h$$

quindi $r = x - q\overline{h}$ e sappiamo che $x \in H$ per ipotesi. Dunque $r \in H$, ma $\overline{h}$ è il **minimo intero positivo** che appartiene ad $H$, quindi $r = 0$ e quindi

$$x = q\overline{h} \in \overline{h}\mathbb{Z}$$

come volevamo.

# Omomorfismo

Siano $G_1,\ G_2$ gruppi. Un **omomorfismo** tra $G_1$ e $G_2$ è un'applicazione

$$f : G_1 \to G_2$$

tale che $f(gg') = f(g)f(g'),\ \forall g, g' \in G_1$.

Un **isomorfismo**

$$f : G_1 \to G_2$$

è un **omomorfismo biunivoco**.

Esempio:

$$f : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$$
$$x \mapsto e^x$$

è un **isomorfismo** in quanto

$$f(x+y) = f(x)f(y)$$
$$e^{x+y} = e^x e^y$$

La **biunivocità** segue dal grafico dell'esponenziale