

Appunti Geometria 1

Biagio Altruda Mastrorilli

October 17, 2024

Definizione (Campo o Corpo commutativo): Sia \mathbb{F} un insieme munito di due operazioni:

$$+ : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$$

$$\cdot : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$$

La terna $(\mathbb{F}, +, \cdot)$ si dice campo se valgono le seguenti proprietà:

1. $\forall a, b, c \in \mathbb{F}$, $(a + b) + c = a + (b + c)$ e anche $a(b \cdot c) = a(b \cdot c)$.
2. $\forall a, b \in \mathbb{F}$, $a + b = b + a$ e anche $a \cdot b = b \cdot a$.
3. $\exists 0_{\mathbb{F}}$ e $1_{\mathbb{F}}$ tali che: $\forall a \in \mathbb{F} \ a + 0_{\mathbb{F}} = a$ e $a \cdot 1_{\mathbb{F}} = a$.
4. $\forall a \in \mathbb{F}$, $\exists b \in \mathbb{F}$ tale che $a + b = 0_{\mathbb{F}}$ (e l'opposto è unico).
5. $\exists b \in \mathbb{F}$ tale che $a \cdot b = 1_{\mathbb{F}}$ ($b = a^{-1} = \frac{1}{a}$).
6. $\forall a, b, c \in \mathbb{F}$, $a \cdot (b + c) = a \cdot b + a \cdot c$. *Osservazioni:*
7. l'opposto di $0_{\mathbb{F}}$ è $0_{\mathbb{F}}$ infatti se cerco $b \in \mathbb{F}$ tale che $0_{\mathbb{F}} + b = 0_{\mathbb{F}}$ ma quindi $0_{\mathbb{F}} + b = b$ ma allora $b = 0_{\mathbb{F}} + b = 0_{\mathbb{F}}$.
8. l'inverso di $1_{\mathbb{F}}$ è $1_{\mathbb{F}}$.
9. $-(-a) = a$.
10. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
11. Se $a \neq 0$, $(a^{-1})^{-1} = a$. *Esempi:*
12. \mathbb{R} i numeri reali.
13. $\mathbb{Q} = \left\{ \frac{p}{q} \text{ tali che } p, q \in \mathbb{Z} \right\}$ i numeri razionali.
14. $\mathbb{C} = \{a + b \in \mathbb{R} \text{ tali che } a, b \in \mathbb{R}, i^2 = -1\}$ i numeri complessi. Definiamo somma e prodotto su \mathbb{C} : $(a + ib) = (c + id) = (a + c) + i(b + d)$. $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$

15. Sia p un numero primo, \mathbb{F}_p è il campo di p elementi. $\mathbb{F}_p = \{0, 1, 2, \dots, p-1, p\}$. Notare che $\forall a \in \mathbb{Z}, \exists m, r \in \mathbb{Z}$ tale che $a = mp + r$ (Contiamo *modulo* p). $+: \mathbb{F}_p \times \mathbb{F}_p \rightarrow \mathbb{F}_p, (a+b)$ è il resto della divisione euclidea $\frac{a+b}{p}$. $\cdot: \mathbb{F}_p \times \mathbb{F}_p \rightarrow \mathbb{F}_p, a \cdot b$ è il resto della divisione euclidea $\frac{ab}{p}$.
16. \mathbb{N} e \mathbb{Z} non sono campi. *Esercizi:*
17. Dimostrare che \mathbb{F}_3 è un campo.
18. Dimostrare che \mathbb{F}_4 non è un campo.

Spazi Vettoriali *Definizione:* Sia \mathbb{F} un campo, definiamo \mathbb{F}^n , con $n \in \mathbb{N}$ tranne 0, come

$$\mathbb{F}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \text{ tale che } x_1, x_2, \dots, x_n \in \mathbb{F} \right\}$$

Definiamo due operazioni:

$+: \mathbb{F}^n \times \mathbb{F}^n \rightarrow \mathbb{F}^n$, tale che

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

$\cdot: \mathbb{F} \times \mathbb{F}^n \rightarrow \mathbb{F}^n$ tale che

$$\lambda \in \mathbb{F}, \lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

Definizione: Sia \mathbb{F} un campo e V un insieme su cui sono definite due operazioni:

$+: V \times V \rightarrow V$ (Somma)

$\cdot: \mathbb{F} \times V \rightarrow V$ (Prodotto per scalari).

La terna $(V, +, \cdot)$ si dice spazio vettoriale sul campo \mathbb{F} se valgono le seguenti proprietà:

1. $\forall u, v, w \in V, (u + v) + w = u + (v + w)$ (Associatività della somma)
2. $\forall u, v \in V, u + v = v + u$ (Commutatività della somma)

3. $\exists \underline{0} \in V : \forall v \in V, v + \underline{0} = v$ ed è detto vettore nullo (Elemento neutro della somma)
4. $\forall v \in V, \exists v' \in V : v + v' = \underline{0}$ e si scrive $-v$ (Opposto per la somma)
5. $\forall a, b \in F, \forall \underline{v}, a(b\underline{v}) = (ab)\underline{v}$ (Compatibilità di \cdot)
6. $\forall v \in V \mathbf{1}_{\mathbb{F}} \underline{v} = \underline{v}$
7. $\forall a \in \mathbb{F}, \forall u, v \in V : a(u + v) = au + av$ (Distributiva 1)
8. $\forall a, b \in \mathbb{F}, \forall v \in V : (a + b)v = av + bv$. (Distributiva 2).

Esempi: Sono spazi vettoriali

1. I vettori geometrici
2. \mathbb{F}^n , infatti: Vale l'associativa della somma perché se

$$u, v, w \in \mathbb{F}^n \implies u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

$$u + (v + w) = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} + \left(\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \right) = \begin{pmatrix} u_1 + (v_1 + w_1) \\ \vdots \\ u_n + (v_n + w_n) \end{pmatrix} = \begin{pmatrix} (u_1 + v_1) + w_1 \\ \vdots \\ (u_n + v_n) + w_n \end{pmatrix}$$

$$\underline{0} \in \mathbb{F}^n = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \text{ infatti: } \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ Siano } a \in \mathbb{F}, u, v \in \mathbb{F}^n \text{ allora}$$

$$a(u+v) = a \left(\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} + \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right) = a \left(\begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix} \right) = \begin{pmatrix} a(u_1 + v_1) \\ \vdots \\ a(u_n + v_n) \end{pmatrix} = \begin{pmatrix} au_1 + av_1 \\ \vdots \\ au_n + av_n \end{pmatrix} = a \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} + a \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = au + av$$

1. Verificare il resto delle proprietà

Osservazione:

1. Se $v, w \in V$, con $v - w$ indicherò $v + (-w)$. Valgono le seguenti proprietà:
2. $\forall v \in V, \mathbf{0}_{\mathbb{F}} v = \underline{0}$
3. $\forall s \in \mathbb{F}, s \mathbf{0}_V = \mathbf{0}_V$

4. $\forall v \in V, (-1_{\mathbb{F}})v = -v$

5. Siano $s \in \mathbb{F}, v \in V$, se $sv = 0_V \implies s = 0$ oppure $v = 0_V$

Esercizio: Dimostrare le proprietà da 1) a 4)

Sia V uno spazio vettoriale su \mathbb{F} e $v_1, \dots, v_n \in V$ e $\alpha_1, \dots, \alpha_n \in \mathbb{F}$, posso sommare i vettori e moltiplicarli per α_i e quindi

Definizione: Sia V spazio vettoriale su \mathbb{F} , siano $v_1, \dots, v_n \in V$ e $\alpha_1, \dots, \alpha_n \in \mathbb{F}$, il vettore

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n = v$$

v si dice combinazione lineare di v_1, \dots, v_n a coefficienti $\alpha_1, \dots, \alpha_n$.

Esempio: Considero in \mathbb{R}^3 i vettori: $v_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}, v_3 = \begin{pmatrix} 0 \\ \frac{1}{2} \\ 0 \end{pmatrix}, v_4 =$

$\begin{pmatrix} 0 \\ 0 \\ -2 \end{pmatrix}$ e $\alpha_1 = -1, \alpha_2 = 0, \alpha_3 = 4, \alpha_4 = 2$, allora:

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_4 v_4 = -1 \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix} + 4 \begin{pmatrix} 0 \\ \frac{1}{2} \\ 0 \end{pmatrix} + 2 \begin{pmatrix} 0 \\ 0 \\ -2 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix} = v$$

Definizione: Fissato un campo \mathbb{F} , una matrice con m righe e n colonne a coefficienti in \mathbb{F} è una tabella A

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix}$$

$\forall i = 1, \dots, m, j = 1, \dots, n, \alpha_{ij} \in \mathbb{F}$ Oppure si scrive $A = (\alpha_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$ Indicheremo con $M_{m,n}(\mathbb{F})$ l'insieme di tutte le matrici $m \times n$ a coefficienti in \mathbb{F} .

è possibile definire le seguenti operazioni:

$$+ : M_{m,n}(\mathbb{F}) \times M_{m,n}(\mathbb{F}) \rightarrow M_{m,n}(\mathbb{F})$$

$$\cdot : \mathbb{F} \times M_{m,n}(\mathbb{F}) \rightarrow M_{m,n}(\mathbb{F})$$

Se $A = (a_{ij}), B = (b_{ij}) \in M_{m,n}(\mathbb{F})$, se $\lambda \in \mathbb{F}$ allora $A + B = (a_{ij} + b_{ij}) =$

$$\begin{pmatrix} a_{11} + b_{11} & \dots & a_{1m} + b_{1m} \\ \dots & \dots & \dots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

$$\lambda A = (\lambda a_{ij}) = \begin{pmatrix} \lambda a_{11} & \dots & \lambda a_{1m} \\ \dots & \dots & \dots \\ \lambda a_{m1} & \dots & \lambda a_{mn} \end{pmatrix}$$

Se $A = \begin{pmatrix} 1 & -7 & 0 \\ 2 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 4 & 2 \\ 1 & 1 & 3 \end{pmatrix}$, $\lambda = \frac{1}{3}$
 $A+B = \begin{pmatrix} 1 & -3 & 2 \\ 3 & 1 & 2 \end{pmatrix}$ $\lambda A = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & 0 \\ \frac{2}{3} & 0 & -\frac{1}{3} \end{pmatrix}$ *Esercizio:* Dimostrare che $(M_{m,n}(\mathbb{F}), +, \cdot)$
 è uno spazio vettoriale

Esempio: Sia X un insieme e \mathbb{F} un campo. Definiamo $\mathbb{F}^X = \{f : X \rightarrow \mathbb{F} \mid f \text{ è una funzione}\}$.
 Definiamo

$$+ : \mathbb{F}^X \times \mathbb{F}^X \rightarrow \mathbb{F}^X$$

$$\cdot : \mathbb{F}^X \times \mathbb{F}^X \rightarrow \mathbb{F}^X$$

Se $f, g \in \mathbb{F}^X$, $\lambda \in \mathbb{F}$ allora $f+g : X \rightarrow \mathbb{F}$ tale che $(f+g)(x) = f(x) + g(x)$. E anche
 $\lambda f : X \rightarrow \mathbb{F}$ tale che $(\lambda f)(x) = \lambda f(x)$.

Esempio: Polinomi a coefficienti in \mathbb{F} di incognita t .
 $\mathbb{F}[t] = \{a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0 \mid a_i \in \mathbb{F}, \forall i = 1, \dots, n, n > 0\}$.

$$+ : \mathbb{F}[t] \times \mathbb{F}[t] \rightarrow \mathbb{F}[t]$$

$$\cdot : \mathbb{F}[t] \times \mathbb{F}[t] \rightarrow \mathbb{F}[t]$$

Se $p, q \in \mathbb{F}[t]$, $\lambda \in \mathbb{F}$, $p = a_n t^n + \dots + a_0$, $q = b_n t^n + \dots + b_0$. Allora $\lambda \cdot p = \lambda a_n t^n + \dots + \lambda a_0$. $p + q = (a_n + b_n) t^n + \dots + (a_0 + b_0)$. Posso interpretare p e q come funzioni da $\mathbb{R} \rightarrow \mathbb{R}$, la somma appena definita coincide con la somma di funzioni, quella definita sopra. E lo stesso per il prodotto per scalari.

Definizione: Se $p = a_n t^n + \dots + a_0 \in \mathbb{F}[t]$, si dice grado di p , indicato con $\deg(p)$, quel numero $n \geq 0$ tale che $a_n \neq 0$ e $a_j = 0, \forall j > n$.

I polinomi si possono anche scrivere come:

$$p = \sum_{i=1}^n a_i t^i$$

Sottospazi vettoriali

Definizione: Sia V uno spazio vettoriale sul campo \mathbb{F} . $W \subset V$ si dice sottospazio vettoriale di V se soddisfa:

1. $W \neq \emptyset$
2. $\forall u, v \in W, \forall \lambda, \mu \in \mathbb{F}$ si ha che $\lambda u + \mu v \in W$

Osservazione:

1. Se W è sottospazio di V allora W è spazio vettoriale sullo stesso campo di V
2. Le condizioni 1) e 2), della definizione di sopra, sono equivalenti alla 2) e alla 1') cioè $0_V \in W$. Infatti se $W \neq \emptyset \implies \exists v \in W \implies \forall \lambda \in \mathbb{F} : \lambda v \in W$. Quindi se $\lambda = 0_F \implies 0v \in W \implies 0_V \in W$. Viceversa se $0_V \in W \implies W \neq \emptyset$.

3. $\{0_V\}$ è un sottospazio vettoriale.
4. V è sottospazio vettoriale di V .
5. $\{\underline{0}\}$ è l'unico sottospazio vettoriale di V con un numero finito di elementi se \mathbb{F} ha infiniti elementi.

Osservazione: Quali sono tutti i sottospazi vettoriali di \mathbb{R}^2 e \mathbb{R}^3 ?. Chiaramente \mathbb{R}^n è sottospazio di \mathbb{R}^n e $\{\underline{0}\}$ è sottospazio.

1. In \mathbb{R}^2 , sia $v \in \mathbb{R}^2$ e $v \neq \underline{0}$, se W è un sottospazio e $v \in W$. Allora per 2), $\forall \lambda \in \mathbb{R}, \lambda v \in W$. Cioè W contiene tutta la retta passante per l'origine e v . Se W contiene w che non è multiplo di v , allora W contiene anche tutta la retta tra $\underline{0}$ e w . Ma allora ottengo tutto \mathbb{R}^2 , dato che v e w non sono allineati. Quindi tutti i sottospazi vettoriali di \mathbb{R}^2 sono: il vettore nullo, le rette per l'origine ed \mathbb{R}^2 stesso.
2. In \mathbb{R}^3 tutti e soli i sottospazi vettoriali sono: il vettore nullo, le rette e i piani passanti per l'origine e tutto \mathbb{R}^3 .

Numeri complessi Nascono come estensione dei numeri reali.

Osservazione: Considero l'equazione $x^2 + 1 = 0$, e ne cerco le soluzioni reali cioè

$$\{x \in \mathbb{R} \mid x^2 + 1 = 0\} = \emptyset$$

Perché $\forall x \in \mathbb{R}, x^2 \geq 0 \implies x^2 + 1 > 0$ Si introduce allora un nuovo "numero" che chiamiamo i , tale che $i^2 = -1$. i è detto unità immaginaria.

Definizione: Si dice numero complesso ogni scrittura della forma: $a+ib$, $a, b \in \mathbb{R}$. E si definisce l'insieme dei numeri complessi come $\mathbb{C} = \{a+ib \mid a, b \in \mathbb{R}\}$

Definizione: $\forall z \in \mathbb{C}, z = a+ib$, a è detto parte reale, $\text{Re}(z)$, e b è detto parte immaginaria, $\text{Im}(z)$. Ad esempio se $z = \sqrt{3} - 5i$. $\text{Re}(z) = \sqrt{3}$, $\text{Im}(z) = -5$.

Due numeri complessi $z = a+ib$ e $z' = a'+b'i$ sono uguali se e solo se $a = a'$ e $b = b'$.

Osservazione: Per assegnare un numero complesso $z = a+ib$ diamo una coppia ordinata (a, b) di numeri reali. Perciò possiamo rappresentare il numero complesso z come il punto $(a, b) \in \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. Infatti la funzione

$$f: \mathbb{R}^2 \rightarrow \mathbb{C} \text{ tale che } (a, b) \rightarrow a+ib$$

Definizione: Su \mathbb{C} sono definite delle operazioni di somma e prodotto. Siano $z = x+iy$ e $z' = x'+iy'$, due numeri complessi allora:

$$+ : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$$

$$(z, z') = (x+iy, x'+iy') \rightarrow x+x' + i(y+y')$$

$$\cdot : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$$

$$(z, z') = (x+iy, x'+iy') \rightarrow xx' - yy' + i(x'y + xy')$$

Proposizione: Proprietà della somma e del prodotto:

1. $\forall z, z' \in \mathbb{C}, z + z' = z' + z$ (Proprietà commutativa della somma)
2. $\forall z, z', z'' \in \mathbb{C} z + (z' + z'') = (z + z') + z''$ (Proprietà associativa della somma)
3. $\forall z \in \mathbb{C} : z + 0 = z$ (Esistenza dell'elemento neutro della somma)
4. $\forall z \in \mathbb{C} : z + (-z) = 0$ (Esistenza degli opposti)
5. $\forall z, z' \in \mathbb{C} : z \cdot z' = z' \cdot z$ (Proprietà commutativa del prodotto)
6. $\forall z, z', z'' \in \mathbb{C} : z \cdot (z' \cdot z'') = (z \cdot z') \cdot z''$ (Proprietà associativa del prodotto)
7. $\forall z, z', z'' \in \mathbb{C} : z \cdot (z' + z'') = z \cdot z' + z \cdot z''$ (Proprietà distributiva)
8. $\forall z \in \mathbb{C} : z \cdot 1 = z$ (Esistenza dell'elemento neutro del prodotto)
9. $\forall z \in \mathbb{C} \setminus \{0\}, \exists w \in \mathbb{C} : z \cdot w = 1$

Dimostrazione:

1.

$$\begin{aligned} z \cdot (z' + z'') &= (x + iy)(x' + iy' + x'' + iy'') = (x + iy)(x' + x'' + i(y' + y'')) = \\ &= x(x' + x'') - y(y' + y'') + i(y(x' + x'') + x(y' + y'')) = xx' + xx'' - yy' - yy'' + i(yx' + yx'' + xy' + xy'') = \\ &= xx' - yy' + i(yx' + xy') + xx'' - yy'' + i(yx'' + xy'') = z \cdot z' + z \cdot z'' \quad \blacksquare. \end{aligned}$$

1. Cerco $w \in \mathbb{C}$ tale che $z \cdot w = 1$. Pongo $z = x + iy$ e $w = u + iv$

$$\begin{aligned} (x + iy)(u + iv) &= 1 \implies (x - iy)(x + iy)(u + iv) = x - iy \\ (x^2 + y^2)(u + iv) &= x - iy \implies u + iv = \frac{x - iy}{x^2 + y^2} \implies w = \frac{x}{x^2 + y^2} - i \frac{y}{x^2 + y^2} \Leftrightarrow (x, y) \neq (0, 0) \quad \blacksquare. \end{aligned}$$

Osservazione: Dalle proprietà viste $(\mathbb{C}, +, \cdot)$ è un campo.

Definizione: Sia $z \in \mathbb{C}, z = x + iy$, si chiama coniugato di z il numero complesso $\bar{z} = x - iy$.

Proprietà del coniugio: $\forall z, w \in \mathbb{C}$ valgono

1. $\bar{\bar{z}} = z$
2. $\overline{z + w} = \bar{z} + \bar{w}$
3. $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
4. $z = \bar{z} \Leftrightarrow z \in \mathbb{R}$ dimostrazione di 4): (\implies) Sia $z = x + iy$ tale che $x + iy = x - iy \implies x = x$ e anche $y = -y \Leftrightarrow y = 0 \implies z \in \mathbb{R}$ (\Leftarrow) $z \in \mathbb{R}, x = x + i0 \implies \bar{z} = \overline{x + i0} = x - i0 = x = z$

Definizione: Sia $z = x + iy \in \mathbb{C}$ si chiama modulo di z il numero reale, indicato con $|z| = \sqrt{x^2 + y^2}$.

Valgono le seguenti proprietà:

1. $z \in \mathbb{C}, |z| \geq 0$ e $|z| = 0 \Leftrightarrow z = 0$

2. $\forall z \in \mathbb{C}, |\bar{z}| = |z|$
3. $\forall z \in \mathbb{C}, z \cdot \bar{z} = |z|^2$
4. $\forall z, w \in \mathbb{C}, |z \cdot w| = |z| \cdot |w|$
5. $\forall z \in \mathbb{C}, z \neq 0, z^{-1} = \frac{\bar{z}}{|z|^2}$

Esempi sottospazi vettoriali: Sia $V = \mathbb{R}^3$, $W = \{(x, y, z) \in \mathbb{R}^3 \mid 3x - y + z = 0\}$.
 è un sottospazio vettoriale. Dimostriamolo:

1. $W \neq \emptyset$, infatti $\underline{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \in W$.
2. Mostriamo adesso che W è chiuso per combinazioni lineari. Siano $u = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$, $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \in W$, e siano $\lambda, \mu \in \mathbb{R}$. $3u_1 - u_2 + u_3 = 0$ ma anche $3v_1 - v_2 + v_3 = 0$. Consideriamo $\lambda u + \mu v$:

$$\lambda u + \mu v = \begin{pmatrix} \lambda u_1 \\ \lambda u_2 \\ \lambda u_3 \end{pmatrix} + \begin{pmatrix} \mu v_1 \\ \mu v_2 \\ \mu v_3 \end{pmatrix} = \begin{pmatrix} \lambda u_1 + \mu v_1 \\ \lambda u_2 + \mu v_2 \\ \lambda u_3 + \mu v_3 \end{pmatrix} \implies$$

$$3(\lambda u_1 + \mu v_1) - \lambda u_2 - \mu v_2 + \lambda u_3 + \mu v_3 =$$

$$\lambda(3u_1 - u_2 + u_3) + \mu(3v_1 - v_2 + v_3) = \lambda(0) + \mu(0) = 0 \blacksquare.$$

Osservazione: Se $\underline{0} \notin W$ allora, W non è sottospazio vettoriale.

Sia $V = \mathbb{R}^4$, $W = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid 2x_1 - x_3 = 1\}$. $W \neq \emptyset$, infatti $\begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ 0 \end{pmatrix} \in W$

Ma non è un sottospazio vettoriale dato che $\underline{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ non rispetta la condizione di

W . Alternativamente si può fare il seguente controllo: Siano $\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix}$, $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} \in$

W , e siano $\lambda, \mu \in \mathbb{R}$. Con gli stessi conti di prima otteniamo:

$$\lambda(2u_1 - u_3) + \mu(2v_1 - v_3) = \lambda(1) + \mu(1) = \lambda + \mu \neq 1 \quad \forall \lambda, \mu \in \mathbb{R}$$

Allora W non è chiuso per combinazioni lineari, quindi non è un sottospazio vettoriale.

Dire se $U \subset \mathbb{R}^3$ è sottospazio.

$$U = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid x^2 - y + 2z = 0 \right\}.$$

1. $U \neq \emptyset$ dato che $\underline{0} \in U$.
2. Siano $u, v \in U$, $\lambda, \mu \in \mathbb{R}$, considero $\lambda u + \mu v$.

$$\lambda u + \mu v = \begin{pmatrix} \lambda u_1 + \mu v_1 \\ \lambda u_2 + \mu v_2 \\ \lambda u_3 + \mu v_3 \end{pmatrix}$$

$$\begin{aligned} & (\lambda u_1 + \mu v_1)^2 - (\lambda u_2 + \mu v_2) + 2(\lambda u_3 + \mu v_3) = \\ & \lambda^2 u_1^2 + 2\lambda\mu u_1 v_1 + \mu^2 v_1^2 - \lambda u_2 - \mu v_2 + 2\lambda u_3 + 2\mu v_3 = \\ & \lambda^2 u_1^2 + 2\lambda\mu u_1 v_1 + \mu^2 v_1^2 + \lambda(-v_1)^2 + \mu(-v_1)^2 = (\lambda^2 - \lambda)v_1^2 + 2\lambda\mu u_1 v_3 + (\mu^2 + \mu)v_1^2 \end{aligned}$$

Che non fa 0, $\forall \lambda, \mu \in \mathbb{R}$, ad esempio se $u_1 = v_1 = 1$ $\lambda = \mu = 2$ non funziona.

Sia $V = \mathbb{R}[t]$, e sia $W = \{2at^2 + 3b \mid a, b \in \mathbb{R}\}$.

1. Mi chiedo se $\underline{0} \in W$, cioè $\underline{0} = 0 + 0t + 0t^2 + \dots$. Sì, mi basta considerare $a = b = 0$ allora $2 \cdot 0t^2 + 3 \cdot 0 \in W$.
2. Siano $p, q \in W$, $\lambda, \mu \in \mathbb{R}$, allora $p = 2a_1t^2 + 3b_1$, e $q = 2a_2t^2 + 3b_2$, Con $a_1, a_2, b_1, b_2 \in \mathbb{R}$.

$$\begin{aligned} \lambda p + \mu q &= \lambda(2a_1t^2 + 3b_1) + \mu(2a_2t^2 + 3b_2) \\ 2\lambda a_1t^2 + 2\mu a_2t^2 + 3\lambda b_1 + 3\mu b_2 &= 2(\lambda a_1 + \mu a_2)t^2 + 3(\lambda b_1 + \mu b_2). \end{aligned}$$

Che è della forma che cercavo. Quindi W è un sottospazio vettoriale.

Definizione: Un sistema di equazioni della forma:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ \dots \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}$$

Con $a_{ij} \in \mathbb{F}$, $b_i \in \mathbb{F}$, $i = 1, \dots, m$, $j = 1, \dots, n$. è detto sistema lineare con m equazioni ed n incognite. Gli a_{ij} si dicono coefficienti del sistema, le x_j incognite del sistema e i b_i termini noti. Se $b_i = 0$, $\forall i$, il sistema è detto sistema lineare omogeneo.

La matrice $A = (a_{ij}) \in M_{m,n}(\mathbb{F})$, è detta matrice associata al sistema. Il

vettore $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$ si dice vettore dei termini noti, e $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ vettore delle

incognite. Si scrive $Ax = b$ per indicare il sistema precedente. Inoltre indico con $A' = (A|b)$, la matrice ottenuta da A "aggiungendo" la colonna b , e si chiama matrice completa associata al sistema.

Esempi: 1.

$$\begin{cases} 2x_1 - 3x_2 + 4x_3 - x_4 = 2 \\ -x_1 + x_2 + \frac{1}{2}x_4 = \pi \end{cases}$$

$$A = \begin{pmatrix} 2 & -3 & 4 & -1 \\ -1 & 1 & 0 & \frac{1}{2} \end{pmatrix}$$

$$b = \begin{pmatrix} 2 \\ \pi \end{pmatrix}$$

$$A' = \begin{pmatrix} 2 & -3 & 4 & -1 & 2 \\ -1 & 1 & 0 & \frac{1}{2} & \pi \end{pmatrix}$$

1.

$$\begin{cases} 2x_1 - x_2 = 0 \\ x_1 + x_2 = 0 \\ 3x_1 = 0 \end{cases}$$

è un sistema omogeneo $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \\ 3 & 0 \end{pmatrix}$, $b = \underline{0}$, $A' = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 0 \\ 3 & 0 & 0 \end{pmatrix}$.

1.

$$\{3x = 2\}$$

$A = (3)$, $A' = (3|2)$.

Teorema: Sia $W \subset \mathbb{F}^n$, l'insieme delle soluzioni del sistema lineare omogeneo $Ax = \underline{0}$, con $A \in M_{m,n}(\mathbb{F})$ e $\underline{0} \in \mathbb{F}^n$. $W = \text{Sol}(Ax = \underline{0})$. Allora W è sottospazio vettoriale di \mathbb{F}^n .

Dimostrazione: Devo dimostrare che $\underline{0} \in \mathbb{F}^n$ appartiene a W e che $\forall z, t \in$

W , $\forall \alpha, \beta \in \mathbb{F}$, $\alpha z + \beta t \in W$. $\underline{0} \in W$, infatti: $\underline{0} = \begin{pmatrix} 0 \\ 0 \\ . \\ . \\ 0 \end{pmatrix} \in \mathbb{F}^n$,

$$Ax = \underline{0} : \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ . \\ . \\ a_{m1}x_1 + \dots + a_{mn}x_n = 0 \end{cases}$$

Ogni sistema lineare omogeneo ammetta la soluzione nulla.

Siano ora $z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ e $t = \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \in W$, allora z_1, \dots, z_n e t_1, \dots, t_n sono soluzioni del sistema di sopra. Cioè $\forall i = 1, \dots, m, a_{i1}z_1 + \dots + a_{in}z_n = 0$ e $a_{i1}t_1 + \dots + a_{in}t_n = 0$.

Allora considero $\alpha z + \beta t = \begin{pmatrix} \alpha z_1 + \beta t_1 \\ \vdots \\ \alpha z_n + \beta t_n \end{pmatrix}$, è vero che questo nuovo vettore soddisfa tutte le equazioni del sistema? Sia $i \in \{1, \dots, n\}$, allora $a_{i1}x_1 + \dots + a_{in}x_n = 0$, sostituisco il vettore di sopra:

$$a_{i1}(\alpha z_1 + \beta t_1) + \dots + a_{in}(\alpha z_n + \beta t_n) = \alpha(a_{i1}z_1 + \dots + a_{in}z_n) + \beta(a_{i1}t_1 + \dots + a_{in}t_n)$$

Ma $a_{i1}z_1 + \dots + a_{in}z_n = 0$ così come $a_{i1}t_1 + \dots + a_{in}t_n = 0$

$$\implies \alpha(0) + \beta(0) = 0$$

Allora $\alpha z + \beta t \in W$ ■.

Osservazione: In particolare se $z \in \text{Sol}(Ax = \underline{0}) \implies \forall \lambda \in \mathbb{F} : \lambda z \in \text{Sol}(Ax = \underline{0})$.

Esercizio: Sia $Ax = b, b \neq \underline{0}$ un sistema lineare. Dimostrare che $\text{Sol}(Ax = b)$ non è un sottospazio vettoriale.

Definizione: Sia V uno spazio vettoriale su \mathbb{F} , e siano $v_1, v_2, \dots, v_k \in V$. Definiamo l'insieme $\text{Span}(v_1, \dots, v_k)$ oppure $\langle v_1, \dots, v_k \rangle = \{v \in V \mid \exists \alpha_1, \dots, \alpha_k \in \mathbb{F} : v = \alpha_1 v_1 + \dots + \alpha_k v_k\}$. Viene detto spazio generato dai vettori v_1, \dots, v_k o insieme delle combinazioni lineari di v_1, \dots, v_k .

Osservazione: Se almeno uno tra v_1, \dots, v_k non è il vettore nullo, allora $\text{Span}(v_1, \dots, v_k)$ ha infiniti elementi.

Un altro modo per scrivere $\text{Span}(v_1, \dots, v_k) = \{\alpha_1 v_1 + \dots + \alpha_k v_k \mid \alpha_i \in \mathbb{F}\}$. E $\text{Span}(v) = \{\alpha v \mid \alpha \in \mathbb{F}\}$.

Teorema: Sia V spazio vettoriale su \mathbb{F} , $v_1, \dots, v_k \in V$. Allora valgono le seguenti proprietà:

1. $\forall i = 1, \dots, k, v_i \in \text{Span}(v_1, \dots, v_k)$.
2. $\text{Span}(v_1, \dots, v_k)$ è sottospazio vettoriale.
3. Se W è sottospazio di V e $v_1, \dots, v_k \in W$ allora $\text{Span}(v_1, \dots, v_k) \subset W$
Oppure anche: $\text{Span}(v_1, \dots, v_k)$ è il più piccolo sottospazio vettoriale di V che contiene v_1, \dots, v_k . *Dimostrazione:*
4. Dobbiamo mostrare che $\forall i = 1, \dots, k, v_i \in \text{Span}(v_1, \dots, v_k)$. Mi chiedo se $\exists \alpha_1, \dots, \alpha_k \in \mathbb{F} : v_i = \alpha_1 v_1 + \dots + \alpha_k v_k$. Sì, infatti, $v_i = 1v_1 + 0v_2 + \dots + 0v_n$ ovvero $\forall i = 1, \dots, k, v_i = 0v_1 + \dots + 0v_{i-1} + 1v_i + 0v_{i+1} + \dots + 0v_k$. Cioè basta prendere $\alpha_i = 1$ e $\alpha_j = 0, \forall j = 1, \dots, k, j \neq i$. Allora, in particolare, $\text{Span}(v_1, \dots, v_k) \neq \emptyset$.

5. Essendo $\text{Span}(v_1, \dots, v_k) \neq \emptyset$, basta dimostrare che $\forall u, w \in \text{Span}(v_1, \dots, v_k), \forall \lambda, \mu \in \mathbb{F}: \lambda u + \mu w \in \text{Span}(v_1, \dots, v_k)$. Dato che $u, w \in \text{Span}(v_1, \dots, v_k): \exists \alpha_1, \dots, \alpha_k$, e $\beta_1, \dots, \beta_k \in \mathbb{F}$ tali che $u = \alpha_1 v_1 + \dots + \alpha_k v_k$ e $w = \beta_1 v_1 + \dots + \beta_k v_k$. Considero $\lambda u + \mu w \implies \lambda(\alpha_1 v_1 + \dots + \alpha_k v_k) + \mu(\beta_1 v_1 + \dots + \beta_k v_k) = (\lambda \alpha_1 + \mu \beta_1) v_1 + \dots + (\lambda \alpha_k + \mu \beta_k) v_k$, che è una combinazione lineare di v_1, \dots, v_k .
6. Sia $w \in \text{Span}(v_1, \dots, v_k)$. Allora $\exists \gamma_1, \gamma_k \in \mathbb{F}$ tali che $w = \gamma_1 v_1 + \dots + \gamma_k v_k$. Ma W è sottospazio vettoriale di V e contiene v_1, \dots, v_k . Ma allora $\forall x_1, \dots, x_k \in \mathbb{F}, x_1 v_1 + \dots + x_k v_k \in W \implies w \in W$ ■.

$$\begin{aligned} \text{Esempi: In } \mathbb{R}^3 \text{ } v_1 &= \begin{pmatrix} 1 \\ -2 \\ 4 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 3 \\ 1 \end{pmatrix}. \text{Span}(v_1, v_2) = \{ \alpha_1 v_1 + \alpha_2 v_2 \mid \alpha_1, \alpha_2 \in \mathbb{R} \} = \\ &= \left\{ \alpha_1 \begin{pmatrix} 1 \\ -2 \\ 4 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 3 \\ 1 \end{pmatrix} \mid \alpha_1, \alpha_2 \in \mathbb{R} \right\} = \\ &= \left\{ \begin{pmatrix} \alpha_1 \\ -2\alpha_1 + 3\alpha_2 \\ 4\alpha_1 + \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in \mathbb{R} \right\} \end{aligned}$$

$$\text{In } M_{2,3}(\mathbb{R}) \text{ } A_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} \text{Span}(A_1, A_2, A_3) &= \{ \gamma_1 A_1 + \gamma_2 A_2 + \gamma_3 A_3 \mid \gamma_1, \gamma_2, \gamma_3 \in \mathbb{R} \} = \\ &= \left\{ \begin{pmatrix} \gamma_1 & \gamma_1 & \gamma_1 \\ \gamma_2 & \gamma_1 + \gamma_2 & \gamma_3 \end{pmatrix} \mid \gamma_1, \gamma_2, \gamma_3 \in \mathbb{R} \right\} \end{aligned}$$

Lemma: $\forall n \geq 0$, l'insieme $\mathbb{F}[t; n] = \{a_n t^n + \dots + a_0 \mid a_0, \dots, a_n \in \mathbb{F}\}$, i polinomi di grado al massimo n è un sottospazio vettoriale di $\mathbb{F}[t]$.

Dimostrazione: Infatti $\mathbb{F}[t; n] = \text{Span}(t^n, t^{n-1}, \dots, t, 1)$ ■.

Esempio: In $\mathbb{R}[t, 5]$. Considero $p_1(t) = t^5 - 3t^4 + 2t$, $p_2(t) = 2t^3 + 2$, $p_3(t) = t^4 + t^2$.

$$\begin{aligned} \text{Span}(p_1(t), p_2(t), p_3(t)) &= \{ \beta_1 p_1(t) + \beta_2 p_2(t) + \beta_3 p_3(t) \mid \beta_1, \beta_2, \beta_3 \in \mathbb{R} \} = \\ &= \{ \beta_1 (t^5 - 3t^4 + 2t) + \beta_2 (2t^3 + 2) + \beta_3 (t^4 + t^2) \mid \beta_1, \beta_2, \beta_3 \in \mathbb{R} \} = \end{aligned}$$

Basi

Definizione: Sia V spazio vettoriale sul campo \mathbb{F} . I vettori $v_1, \dots, v_k \in V$ si dicono linearmente indipendenti se $\forall \alpha_1, \dots, \alpha_k \in \mathbb{F}$, tali che $\alpha_1 v_1 + \dots + \alpha_k v_k = \underline{0} \implies \alpha_1 = \alpha_2 = \dots = \alpha_k = 0$. Viceversa si dicono linearmente dipendenti se $\exists \alpha_1, \dots, \alpha_k \in \mathbb{F}$, non tutti nulli, tali che $\alpha_1 v_1 + \dots + \alpha_k v_k = \underline{0}$.

Osservazione: v_1, \dots, v_k sono linearmente indipendenti se l'unica soluzione dell'equazione:

$$\alpha_1 v_1 + \dots + \alpha_k v_k = \underline{0}$$

nelle incognite α_i , l'unica soluzione è quella nulla ($\alpha_1 = \dots = \alpha_k$).

Esempio: In \mathbb{R}^4 Sia $v_1 = \begin{pmatrix} 1 \\ 0 \\ 2 \\ 3 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ -1 \\ 0 \\ -1 \end{pmatrix}, v_3 = \begin{pmatrix} 1 \\ -1 \\ 2 \\ 2 \end{pmatrix}$. Mi chiedo se sono

indipendenti.

$$\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = \underline{0} \\ \implies \alpha_1 \begin{pmatrix} 1 \\ 0 \\ 2 \\ 3 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ -1 \\ 0 \\ -1 \end{pmatrix} + \alpha_3 \begin{pmatrix} 1 \\ -1 \\ 2 \\ 2 \end{pmatrix} = \underline{0} \implies \begin{pmatrix} \alpha_1 + \alpha_3 \\ -\alpha_2 - \alpha_3 \\ 2\alpha_1 + 2\alpha_3 \\ 3\alpha_1 - \alpha_2 + 2\alpha_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Allora, vedendola come un sistema lineare otteniamo:

$$\begin{cases} \alpha_1 = -\alpha_3 \\ \alpha_2 = -\alpha_3 \\ 2(-\alpha_3) + 2\alpha_3 = 0 \\ 3(-\alpha_3) - (-\alpha_3) + 2\alpha_3 = 0 \end{cases}$$

$\forall \alpha_3 \in \mathbb{R}$ la terna: $\begin{pmatrix} -\alpha_3 \\ -\alpha_3 \\ -\alpha_3 \end{pmatrix}$ è una soluzione del sistema. Infatti $v_3 = v_1 + v_2$.

In \mathbb{R}^3 $w_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, w_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, w_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. $\alpha_1 w_1 + \alpha_2 w_2 + \alpha_3 w_3 = \underline{0}$ Allora:

$$\begin{cases} \alpha_1 + \alpha_2 = 0 \\ \alpha_1 + \alpha_3 = 0 \\ \alpha_2 + \alpha_3 = 0 \end{cases} \implies \begin{cases} \alpha_2 = -\alpha_1 \\ \alpha_3 = -\alpha_1 \\ -\alpha_1 - \alpha_1 = 0 \end{cases} \implies \alpha_1 = 0 \implies \begin{cases} \alpha_1 = 0 \\ \alpha_2 = 0 \\ \alpha_3 = 0 \end{cases}$$

Allora sono linearmente indipendenti.

Proposizione: Sia $Ax = \underline{0}$, un sistema lineare, omogeneo, con $A \in M_{m,n}(\mathbb{F})$. Il sistema $Ax = \underline{0}$ ha un'unica soluzione $x = \underline{0} \Leftrightarrow$ le colonne di A , A_1, \dots, A_n sono linearmente indipendenti.

Dimostrazione: Infatti il sistema $Ax = \underline{0}$, lo posso scrivere come:

$$A_1 x_1 + \dots + A_n x_n = \underline{0}$$

Quest'equazione ha come soluzione, o solo quella nulla con $x = \underline{0}$ e allora le colonne di A sono indipendenti oppure ne esiste una non nulla, $z \neq \underline{0}$ tale che $A_1 z_1 + \dots + A_n z_n = 0$. Allora le colonne di A sono linearmente dipendenti.

Proposizione: Valgono le seguenti proprietà:

1. Sia $v \in V$ allora v è indipendente $\Leftrightarrow v \neq \underline{0}$.
2. Se fra i vettori v_1, \dots, v_k , c'è il vettore nullo. Allora v_1, \dots, v_k sono linearmente dipendenti.

3. Se $\exists i, j, i \neq j$, tali che $v_i = v_j$. Allora i vettore v_1, \dots, v_k sono dipendenti.

Proposizione: Sia V spazio vettoriale su \mathbb{F} e $v_1, \dots, v_k \in V$. v_1, \dots, v_k sono linearmente dipendenti se e solo se: $\exists i = 1, \dots, k$, tale che v_i è combinazione lineare degli altri.

Dimostrazione: (\Rightarrow) Per ipotesi v_1, \dots, v_k sono dipendenti. Allora $\exists \alpha_1, \dots, \alpha_k$ non tutti nulli, ad esempio $\alpha_i \neq 0$, tali che $\alpha_1 v_1 + \dots + \alpha_k v_k = 0$. Se e solo se

$$\alpha_i v_i = -(\alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \dots + \alpha_k v_k) \implies$$

$$v_i = -\left(\frac{-\alpha_1}{\alpha_i}\right)v_1 + \dots + \left(\frac{-\alpha_k}{\alpha_i}\right)v_k$$

(\Leftarrow) Per ipotesi $v_i = \beta_1 v_1 + \dots + \beta_{i-1} v_{i-1} + \beta_{i+1} v_{i+1} + \dots + \beta_k v_k$. Che è vero se e solo se:

$$\beta_1 v_1 + \dots + \beta_{i-1} v_{i-1} + (-1)v_i + \beta_{i+1} v_{i+1} + \dots + \beta_k v_k = \underline{0} \blacksquare.$$

Esempio:

$$\text{Siano } v_1 = \begin{pmatrix} 1 \\ 0 \\ 2 \\ 3 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ -1 \\ 0 \\ -1 \end{pmatrix}, v_3 = \begin{pmatrix} 1 \\ -1 \\ 2 \\ 2 \end{pmatrix}. \quad v_3 = v_1 + v_2 \implies v_1 + v_2 - v_3 = \underline{0}.$$

Proposizione: Sia V spazio vettoriale su \mathbb{F} . $v_1, \dots, v_k \in V$ tali che $\exists \alpha_1, \dots, \alpha_{k-1}$: $v_k = \alpha_1 v_1 + \dots + \alpha_{k-1} v_{k-1}$. Allora $\text{Span}(v_1, \dots, v_k) = \text{Span}(v_1, \dots, v_{k-1})$.

Dimostrazione: L'inclusione verso sinistra è ovvia, perché se $v \in \text{Span}(v_1, \dots, v_{k-1})$ allora $\exists \gamma_1, \dots, \gamma_{k-1} \in \mathbb{F}$ tali che $v = \gamma_1 v_1 + \dots + \gamma_{k-1} v_{k-1} = \gamma_1 v_1 + \dots + \gamma_{k-1} v_{k-1} + 0v_k \in \text{Span}(v_1, \dots, v_k)$. Per l'altra inclusione invece, sia $w \in \text{Span}(v_1, \dots, v_k) \implies \exists \delta_1, \dots, \delta_k$ tali che $w = \delta_1 v_1 + \dots + \delta_k v_k$. Essendo v_k combinazione lineare degli altri, otteniamo:

$$w = \delta_1 v_1 + \dots + \delta_k (\alpha_1 v_1 + \dots + \alpha_{k-1} v_{k-1}).$$

$$w = (\delta_1 + \delta_k \alpha_1) v_1 + \dots + (\delta_{k-1} + \delta_k \alpha_{k-1}) v_{k-1} \in \text{Span}(v_1, \dots, v_{k-1}) \blacksquare.$$

Definizione: Sia V spazio vettoriale su \mathbb{F} , $v_1, \dots, v_k \in V$, si dicono generatori di V se $\forall v \in V, \exists \alpha_1, \dots, \alpha_k \in \mathbb{F}$ tali che $v = \alpha_1 v_1 + \dots + \alpha_k v_k$. Ovvero $V = \text{Span}(v_1, \dots, v_k)$.

Definizione: Sia V uno spazio vettoriale su \mathbb{F} , $\mathcal{B} = (v_1, \dots, v_n)$ si dice base di V se:

1. v_1, \dots, v_n sono linearmente indipendenti
2. v_1, \dots, v_n sono generatori di V .

Teorema(Caratterizzazione delle basi): Sia V spazio vettoriale su un campo \mathbb{F} . Sono fatti equivalenti:

1. $\mathcal{B} = (v_1, \dots, v_n)$ è una base
2. v_1, \dots, v_n sono tali che $\forall v \in V, \exists! \alpha_1, \dots, \alpha_n \in \mathbb{F}$ tali che $v = \alpha_1 v_1 + \dots + \alpha_n v_n$.

Dimostrazione: 1) \implies 2). Sia \mathcal{B} una base di V . Devo dimostrare che $\forall v \in V, \exists! \alpha_1, \dots, \alpha_n \in \mathbb{F}$ tali che $v = \alpha_1 v_1 + \dots + \alpha_n v_n$. L'esistenza di $\alpha_1, \dots, \alpha_n$ è garantita dal fatto che v_1, \dots, v_n sono generatori. Resta da dimostrare l'unicità. Per assurdo $\exists v \in V$ tale che $v = \alpha_1 v_1 + \dots + \alpha_n v_n = \beta_1 v_1 + \dots + \beta_n v_n$. Se e solo se $\alpha v_1 + \dots + \alpha_n v_n - (\beta_1 v_1 + \dots + \beta_n v_n) = \underline{0}$. Allora $(\alpha_1 - \beta_1)v_1 + \dots + (\alpha_n - \beta_n)v_n = \underline{0}$. Essendo \mathcal{B} base, v_1, \dots, v_n sono linearmente indipendenti, l'unica combinazione lineare che dà il vettore nullo è quella tale che $\alpha_1 = \beta_1, \dots, \alpha_n = \beta_n$. Che dimostra l'unicità. 2) \implies 1). I vettori v_1, \dots, v_n sono generatori perché $\forall v \in V, \exists \alpha_1, \dots, \alpha_n \in \mathbb{F}$ tali che $v = \alpha_1 v_1 + \dots + \alpha_n v_n$, per ipotesi. Dimostriamo che sono linearmente indipendenti. Imponiamo che $\alpha_1 v_1 + \dots + \alpha_n v_n = \underline{0}$. Ma so che $\underline{0} = 0v_1 + \dots + 0v_n$, però per ipotesi ho unicità della combinazione lineare. Allora $\alpha_1 = \dots = \alpha_n = 0$ ■.

Esempi: 1. In \mathbb{F}^n è definita la base canonica. $\mathcal{B}(e_1, \dots, e_n)$. $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 =$

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

1.

Sia $d \in \mathbb{N}$. $\mathbb{F}_d[t] = \{a_d t^d + \dots + a_1 t + a_0 \mid a_i \in \mathbb{F}\}$. Allora $\mathcal{B} = (t^d, t^{d-1}, \dots, t, 1)$ è una base.

Definizione: Sia V spazio vettoriale sul campo \mathbb{F} . $\mathcal{B} = (v_1, \dots, v_n)$ una base di V . Allora dato $v \in V$ definiamo coordinate di v rispetto alla base \mathcal{B} , indicato

$$\text{con } F_{\mathcal{B}}(v) = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{F}^n, \text{ tali che } v = \alpha_1 v_1 + \dots + \alpha_n v_n.$$

Osservazione: Se cambio base le coordinate cambiano. Se $\mathcal{B} = (v_1, v_2, \dots, v_n)$

è base, $\mathcal{B}' = (v_2, v_1, \dots, v_n)$ è una base diversa. Infatti se $F_{\mathcal{B}}(v) = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \neq$

$$F_{\mathcal{B}'}(v) = \begin{pmatrix} \alpha_2 \\ \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Esempi: In \mathbb{F}^n , $\mathcal{B} = (e_1, \dots, e_n)$. Sia $v \in \mathbb{F}^n, v = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, x_i \in \mathbb{F}$. $F_{\mathcal{B}}(v) =$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = v.$$

Definizione: Sia V spazio vettoriale sul campo \mathbb{F} . Sia $\mathcal{A} \subset V$, $\mathcal{B} \subset \mathcal{A}$ si dice sottoinsieme massimale di vettori indipendenti in \mathcal{A} se gli elementi di \mathcal{B} sono indipendenti e se $\forall v \in \mathcal{A}$, $\mathcal{B} \cup \{v\}$ non sono più indipendenti.

Proposizione: Sia V spazio vettoriale sul campo \mathbb{F} . Sia $\mathcal{B} = \{v_1, \dots, v_n\}$ base di V . Allora \mathcal{B} è un insieme massimale di vettori linearmente indipendenti in V .

Dimostrazione: Essendo \mathcal{B} base di V , tutti i suoi vettori sono indipendenti. Ora sia $v \in V$. \mathcal{B} è base di V quindi $\exists \alpha_1, \dots, \alpha_n \in \mathbb{F}$ tali che $v = \alpha_1 v_1 + \dots + \alpha_n v_n$. Allora $\{v_1, \dots, v_n, v\}$ è formato da vettori dipendenti ■.

Lemma: Sia $\mathcal{B} \subset V$ insieme finito. Se $\text{Span}(\mathcal{B})$ contiene un sistema di generatori per V allora $\text{Span}(\mathcal{B}) = V$.

Dimostrazione: Sia $\mathcal{A} \subset \text{Span}(\mathcal{B})$ un insieme di generatori per V . Ovvero, $\forall v \in V$ v è combinazione lineare di elementi di \mathcal{A} . $\mathcal{A} \subset \text{Span}(\mathcal{B}) \implies \text{Span}(\mathcal{A}) \subset \text{Span}(\mathcal{B}) \subset V$ ■.

Teorema: Sia $\mathcal{A} = (v_1, \dots, v_n)$ sistema di generatori di V e $\mathcal{B} \subset \mathcal{A}$ sottoinsieme massimale di vettori indipendenti in \mathcal{A} . Allora \mathcal{B} è base.

Dimostrazione: Per ipotesi gli elementi di \mathcal{B} sono indipendenti. Devo dimostrare che gli elementi di \mathcal{B} generano V . Vorremmo mostrare che $\mathcal{A} \subset \text{Span}(\mathcal{B})$, e concludere per il lemma precedente. Per ipotesi $\forall v \in \mathcal{A}$, $\mathcal{B} \cup \{v\}$ non è linearmente indipendente. Allora ogni elemento di \mathcal{A} lo posso scrivere come combinazione degli elementi di \mathcal{B} , quindi $\mathcal{A} \subset \text{Span}(\mathcal{B})$. Per il lemma precedente, ho concluso ■.

Corollario: Sia V spazio vettoriale finitamente generato, cioè contenente un sistema finito di generatori. Allora V ammette una base.

Osservazione: Esistono spazi vettoriali che non sono finitamente generati, ad esempio $\mathbb{R}[t]$: i polinomi a coefficienti reali nell'incognita t di grado arbitrario.

Teorema (Di completamento): Sia V uno spazio vettoriale sul campo \mathbb{F} . $\mathcal{B} = (v_1, \dots, v_n)$ base di V , e w_1, \dots, w_p vettori linearmente indipendenti in V , con $p \leq n$. Allora $\exists \#n - p$ vettori di \mathcal{B} che uniti a w_1, \dots, w_p formano una base.

Dimostrazione: Per induzione su p . Caso $p = 1$, sia w_1 è indipendente cioè w_1 è non nullo. Essendo \mathcal{B} una base, $\exists! \alpha_1, \dots, \alpha_n \in \mathbb{F}$ tali che $w_1 = \alpha_1 v_1 + \dots + \alpha_n v_n$. Poiché $w_1 \neq \underline{0}$, allora gli α_i non sono tutti nulli. A meno di riordinare, suppongo che $\alpha_1 \neq 0$. Ma allora $v_1 = \frac{1}{\alpha_1} (w_1 - \sum_{i=2}^n \alpha_i v_i) \in \text{Span}(w_1, v_2, \dots, v_n)$ e quindi sono generatori. Basta dimostrare che sono indipendenti. Siano $\beta_1, \dots, \beta_n \in \mathbb{F}$ tali che

$$\beta_1 w_1 + \beta_2 v_2 + \dots + \beta_n v_n = \underline{0} \implies \beta_1 (\alpha_1 v_1 + \dots + \alpha_n v_n) + \beta_2 v_2 + \dots + \beta_n v_n.$$

$$\beta_1 \alpha_1 v_1 + \sum_{i=2}^n (\beta_1 \alpha_i + \beta_i) v_i = \underline{0}$$

che è una combinazione lineare dei v_i che sono indipendenti perché sono una base. Quindi $\beta_1 \alpha_1 = 0$ ma essendo $\alpha_1 \neq 0 \implies \beta_1 = 0$. Allora $\beta_i = 0, \forall i$.

Supponiamo che il teorema sia vero per $p-1$ vettori e dimostriamolo per p vettori. w_1, \dots, w_{p-1} sono indipendenti per ipotesi. Allora, a meno di riordinare, posso supporre che $(w_1, \dots, w_{p-1}, v_p, \dots, v_n)$ sono base di V . Allora w_p è combinazione lineare di $(w_1, \dots, w_{p-1}, v_p, \dots, v_n)$ cioè $\exists! \alpha_1, \dots, \alpha_n \in \mathbb{F}$ tali che $w_p = \sum_{i=2}^{p-1} \alpha_i w_i + \sum_{j=p}^n \alpha_j v_j$. w_p non è il vettore nullo, allora gli α_i, α_j non sono tutti nulli. più precisamente almeno uno tra gli α_j è diverso da 0, altrimenti $w_p = \sum_{i=1}^{p-1} \alpha_i w_i$ contro l'indipendenza dei w_i . A meno di riordinare suppongo che $\alpha_p \neq 0$. Allora

$$v_p = \frac{1}{\alpha_p} \left(\sum_{i=1}^{p-1} \alpha_i w_i + w_p - \sum_{j=p}^n \alpha_j v_j \right).$$

Ma allora $v_p \in \text{Span}(w_1, \dots, w_p, v_{p+1}, \dots, v_n)$. Quindi $(w_1, \dots, w_p, v_{p+1}, \dots, v_n)$ generano. Basta dimostrare che sono linearmente indipendenti. Infatti

$$\begin{aligned} \sum_{i=1}^p \beta_i w_i + \sum_{i=p+1}^n \beta_i v_i &= \underline{0} \implies \\ \implies \sum_{i=1}^{p-1} \beta_i w_i + \beta_p \left(\sum_{i=1}^{p-1} \alpha_i w_i + \sum_{j=p}^n \alpha_j v_j \right) + \sum_{j=p+1}^n \beta_j v_j &= \underline{0} \end{aligned}$$

Ma quindi:

$$(\beta_1 + \beta_p \alpha_1) w_1 + (\beta_2 + \beta_p \alpha_2) w_2 + \dots + (\beta_{p-1} + \beta_p \alpha_{p-1}) w_{p-1} + (\beta_p \alpha_p) v_p + (\beta_p \alpha_{p+1} + \beta_{p+1}) v_{p+1} + \dots$$

Tutti i coefficienti di questa combinazione devono essere nulli, ma in particolare lo è $\beta_p \alpha_p$, ma $\alpha_p \neq 0$, quindi $\beta_p = 0 \implies \beta_i = 0, \forall i$ ■.

Corollario: Sia V spazio vettoriale sul campo \mathbb{F} . $\mathcal{B}, \mathcal{B}'$ basi. Allora \mathcal{B} e \mathcal{B}' hanno lo stesso numero di elementi.