Indice

Capitolo 1

Lezione 1 - 24/09

1.1 Operazione Binaria

Definizione (Operazioni su Insiemi)
Siano A, B, C insiemi. Diremo **operazione binaria** ogni applicazione

$$\varphi : A \times B \to C.$$

- Se in particolare $A = B = C$, allora diremo che $\varphi : A \times A \to A$ è un operazione binaria interna su A.
- Se $B = C$, allora diremo che φ si dice esterna con operatori in A.

1.2 Strutture Algebriche

Ricorda: Strutture Algebriche

- $(S, \perp)$ si dice **semigruppo** se $\perp$ è associativa;
- $(S, \perp)$ si dice **semigruppo commutativo** se $\perp$ è semigruppo con commutatività;
- $(S, \perp)$ si dice **monoide** se $\perp$ è semigruppo dotato di neutro;
- $(S, \perp)$ si dice **monoide commutativo** se $\perp$ è monoide con commutatività;
- $(S, \perp)$ si dice **gruppo** se $\perp$ è monoide dove ogni elemento è simmetrizzabile;
- $(S, \perp)$ si dice **gruppo abeliano** se $\perp$ è gruppo con commutatività.

Definizione (Struttura Algebrica)
Per **struttura algebrica** si intende una n-upla costituita da insiemi e operazioni su di essi. La più semplice struttura algebrica, spesso detta *gruppoide*, è una coppia $(X, \perp)$, dove X è un insieme e $\perp$ è un operazione binaria interna su X.

1.2.1 Gruppo

Definizione (Gruppo)

Un **gruppo** è una struttura algebrica $(G, \perp)$ formata da un insieme G e da un'operazione binaria interna $\perp: G \times G \to G$, che soddisfa le seguenti proprietà:

1. **Associatività:** $\forall\, a, b, c \in G,\ (a \perp b) \perp c = a \perp (b \perp c)$;
2. **Elemento neutro:** esiste un elemento $e \in G$ tale che $\forall\, a \in G,\ a \perp e = e \perp a = a$;
3. **Elemento inverso:** per ogni $a \in G$ esiste un elemento $\bar{a} \in G$ tale che $a \perp \bar{a} = \bar{a} \perp a = e$.

Se inoltre vale la **proprietà commutativa**

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

allora il gruppo si dice **abeliano**.

Proposizione: Proprietà elementari in un gruppo

Sia $(X, \perp)$ un gruppoide (cioè X insieme non vuoto con un'operazione binaria $\perp$ su X). Valgono le seguenti proprietà.

1. Se $(X, \perp)$ ammette un elemento neutro, questo è unico.
2. Se $(X, \perp)$ ammette un elemento neutro e e $\perp$ è associativa, allora per ogni $x \in X$ invertibile l'inverso di x è unico.
3. Inoltre, se $\perp$ è associativa e ha elemento neutro $u \in A$ e abbiamo $x, y \in A$ che hanno i loro inversi $\bar{x}, \bar{y}$, allora $x \perp y$ è invertibile e il suo inverso è $\bar{y} \perp \bar{x}$.

Dimostrazioni:

Dimostrazione della proprietà 1 (unicità dell'elemento neutro). Supponiamo che e ed e' siano due elementi neutri in $(X, \perp)$. Per definizione di elemento neutro:

$$\forall x \in X: \quad e \perp x = x \quad \text{e} \quad e' \perp x = x.$$

In particolare, considerando $x = e'$ nella prima uguaglianza e $x = e$ nella seconda otteniamo

$$e \perp e' = e' \quad \text{e} \quad e' \perp e = e.$$

Se non assumiamo necessariamente commutatività, bperpa usare una delle due uguaglianze applicata all'altro neutro: usando $e \perp e' = e'$ e insieme $e' \perp e = e$ otteniamo

$$e = e' \quad (\text{poiché } e = e' \perp e = e').$$

Quindi $e = e'$ e l'elemento neutro è unico. □

Dimostrazione della proprietà 2 (unicità dell'inverso e formula dell'inverso del prodotto). Sia $(X, \perp)$ associativo e con elemento neutro e.

Unicità dell'inverso. Sia $x \in X$ e supponiamo che y e y' siano due inversi di x, cioè

$$x \perp y = e = y \perp x, \qquad x \perp y' = e = y' \perp x.$$

Allora, usando l'associatività,

$$y = y \perp e = y \perp (x \perp y') = (y \perp x) \perp y' = e \perp y' = y'.$$

Quindi $y = y'$ e l'inverso è unico. □

Dimostrazione della proprietà 3. Siano $(A, \perp)$ un insieme con operazione binaria $\perp$, associativa, e dotato di elemento neutro $u \in A$. Supponiamo $x, y \in A$ invertibili e indichiamo con $\overline{x}$ e $\overline{y}$ i loro inversi, cioè

$$x \perp \overline{x} = \overline{x} \perp x = u, \qquad y \perp \overline{y} = \overline{y} \perp y = u.$$

Consideriamo il candidato $\overline{y} \perp \overline{x}$ come possibile inverso di $x \perp y$. Calcoliamo il prodotto a destra:

$$\begin{aligned}(x \perp y) \perp (\overline{y} \perp \overline{x}) &\overset{\text{(assoc.)}}{=} x \perp \big(y \perp (\overline{y} \perp \overline{x})\big)\\ &= x \perp \big((y \perp \overline{y}) \perp \overline{x}\big)\\ &= x \perp (u \perp \overline{x})\\ &= x \perp \overline{x}\\ &= u.\end{aligned}$$

Analogamente, il prodotto a sinistra:

$$\begin{aligned}(\overline{y} \perp \overline{x}) \perp (x \perp y) &\overset{\text{(assoc.)}}{=} \overline{y} \perp \big(\overline{x} \perp (x \perp y)\big)\\ &= \overline{y} \perp \big((\overline{x} \perp x) \perp y\big)\\ &= \overline{y} \perp (u \perp y)\\ &= \overline{y} \perp y\\ &= u.\end{aligned}$$

Quindi $\overline{y} \perp \overline{x}$ è sia inverso a destra sia inverso a sinistra di $x \perp y$. Poiché in una struttura con elemento neutro e operazione associativa l'inverso (se esiste) è unico, segue che

$$\overline{(x \perp y)} = \overline{y} \perp \overline{x},$$

come volevamo dimostrare. □

1.2.2 Anello

Definizione (Anello)
Un **anello** è una struttura algebrica $(A, +, \cdot)$ formata da un insieme A e da due operazioni binarie interne:

$$+ : A \times A \to A, \qquad \cdot : A \times A \to A,$$

tali che valgono le seguenti proprietà:

1. $(A, +)$ è un **gruppo abeliano**
2. L'operazione $\cdot$ (detta *moltiplicazione*) è associativa
3. La moltiplicazione è distributiva rispetto all'addizione:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c, \quad \forall\, a, b, c \in A.$$

Se esiste un elemento $1 \in A$ tale che $1 \cdot a = a \cdot 1 = a$ per ogni $a \in A$, l'anello si dice **unitario** o **con elemento neutro moltiplicativo**.
Se inoltre la moltiplicazione è commutativa, l'anello si dice **commutativo**.

1.2.3 Campo

Definizione (Campo)
Un **campo** è una struttura algebrica $(K, +, \cdot)$ formata da un insieme K e da due operazioni binarie interne:

$$+ : K \times K \to K, \qquad \cdot : K \times K \to K,$$

che soddisfano le seguenti proprietà:

1. $(K, +)$ è un **gruppo abeliano**:
2. $(K \setminus \{0\}, \cdot)$ è un **gruppo abeliano** rispetto alla moltiplicazione:
3. Le due operazioni sono collegate dalle proprietà distributive:

In altre parole, un campo è un **anello commutativo con elemento unità** in cui **ogni elemento non nullo è invertibile**.

1.2.4 Spazio Vettoriale

Definizione (Spazio vettoriale)
Diremo che $(V, \boxplus, \boxdot)$ è **spazio vettoriale** sul campo $\mathbb{R}$ se:

1. $V \neq \emptyset$
   Operazione interna: $\boxplus : V \times V \to V$, $(u, v) \mapsto u + v$
   Operazione esterna: $\boxdot : K \times V \to V$, $(\lambda, v) \mapsto \lambda v$
2. $(V, \boxplus)$ è gruppo abeliano, $\forall \underline{v}, \underline{w}, \underline{z} \in V$
   (a) Proprietà associativa: $(\underline{v} \boxplus \underline{w}) \boxplus \underline{z} = \underline{v} \boxplus (\underline{w} \boxplus \underline{z})$
   (b) Proprietà commutativa: $\underline{v} \boxplus \underline{w} = \underline{w} \boxplus \underline{v}$
   (c) Esiste opposto: $\underline{v} \boxplus (-\underline{v}) = \underline{0}$
   (d) Esiste elemento neutro: $\underline{v} \boxplus \underline{0} = \underline{0} \boxplus \underline{v} = \underline{v}$
3. Esiste elemento neutro rispetto a $\boxdot$: $1 \boxdot \underline{v} = \underline{v} = \underline{v} \boxdot 1$
4. **Per tutti** $h, k \in \mathbb{R}, \underline{v}, \underline{w} \in V$ valgono le seguenti proprietà:
   (a) Compatibilità della moltiplicazione scalare: $(h \cdot k) \boxdot \underline{v} = h \boxdot (k \boxdot \underline{v})$
   (b) Distributività rispetto alla somma scalare: $(h + k) \boxdot \underline{v} = (h \boxdot \underline{v}) \boxplus (k \boxdot \underline{v})$
   (c) Distributività rispetto alla somma vettoriale: $h \boxdot (\underline{v} \boxplus \underline{w}) = (h \boxdot \underline{v}) \boxplus (h \boxdot \underline{w})$

Proposizione: Proprietà aritmetiche degli Spazi Vettoriali

Sia V uno spazio vettoriale sul campo $\mathbb{K}. \forall \alpha, \beta \in \mathbb{K}, \forall v \in V$ si ha:

1. $\alpha \boxdot v = 0 \iff \alpha = 0$ oppure $v = 0$
2. $(-\alpha) \boxdot v = \alpha \boxdot (-v) = -(\alpha \boxdot v)$
3. se $\alpha \boxdot v = \beta \boxdot v$ e $v \neq \varnothing$, allora $\alpha = \beta$
4. se $\alpha \boxdot u = \alpha \boxdot v$ e $\alpha \neq \varnothing$, allora $u = v$

Dimostrazione delle proprietà. **(i)** Dimostriamo che

$$av = 0 \iff a = 0 \text{ oppure } v = 0.$$

Direzione "⇒": se $a = 0$ oppure $v = 0$, allora chiaramente $av = 0$. Infatti:

- se $a = 0$, per le proprietà dello spazio vettoriale abbiamo $0 \cdot v = 0$;
- se $v = 0$, allora $a \cdot 0 = 0$.

Direzione "$\Leftarrow$": supponiamo che $av = 0$ e $a \neq 0$. Poiché $a \neq 0$, esiste l'inverso $a^{-1} \in K$. Moltiplicando entrambi i membri per a^{-1} otteniamo:

$$a^{-1}(av) = a^{-1} \cdot 0 = 0.$$

Usando l'associatività della moltiplicazione scalare:

$$(a^{-1}a)v = 1 \cdot v = v = 0.$$

Quindi, se $a \neq 0$ e $av = 0$, necessariamente $v = 0$. Pertanto, la proprietà (i) è dimostrata.

(ii) Dimostriamo ora che

$$(-a)v = a(-v) = -(av).$$

Si ha immediatamente:

$$av + (-a)v = (a + (-a))v = 0v = 0,$$

e anche

$$av + a(-v) = a(v + (-v)) = a0 = 0.$$

Poiché in entrambi i casi la somma è nulla, segue che

$$(-a)v = -(av) = a(-v).$$

(iii) Se $av = \beta v$, allora

$$(a + (-\beta))v = av + (-\beta)v = \beta v + (-\beta)v = 0.$$

Poiché $v \neq 0$ per ipotesi, per la proprietà (i) segue che $a + (-\beta) = 0$, e quindi $a = \beta$.

(iv) Se $au = av$ e $a \neq 0$, allora

$$a(u + (-v)) = au + a(-v) = au - av = 0.$$

Poiché $a \neq 0$, per la proprietà (i) si ha $u + (-v) = 0$, cioè $u = v$.

□

Capitolo 2

Lezione 2 - 26/09

2.1 Polinomi

Definizione (Polinomi)
Sia $(K, +, \cdot)$ un campo e x una variabile (detta anche *incognita*).

- Per ogni $n \in \mathbb{N} \cup \{0\}$ si definisce $x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ volte}}$, con la convenzione $x^0 = 1$.
- Un **polinomio** nella variabile x a coefficienti in K è una somma finita di potenze di x moltiplicate per scalari in K:
$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d = \sum_{i=0}^{d} a_i x^i,$$
dove $a_0, a_1, \ldots, a_d \in K$ e $a_d \neq 0$.

Il numero naturale d è detto **grado** del polinomio, e si indica con
$$\mathrm{gr}(p) = \max\{i \mid a_i \neq 0\}.$$
L'insieme di tutti i polinomi in una variabile x a coefficienti in K si indica con
$$K[x] = \{p(x) \mid p(x) \text{ è un polinomio in } x \text{ con coefficienti in } K\}.$$

—

Osservazione: Operazioni in $K[x]$
In $K[x]$ sono definite naturalmente le seguenti operazioni:

- **Somma di polinomi:**
$$(p+q)(x) = \sum_{i=0}^{\max(d_p,d_q)} (a_i + b_i)x^i, \quad p(x) = \sum a_i x^i,\ q(x) = \sum b_i x^i.$$
Esempio:
$$(2x^2 + 3x + 1) + (x^2 - x + 4) = 3x^2 + 2x + 5.$$

- **Moltiplicazione per scalare:**
$$(\lambda p)(x) = \sum_{i=0}^{d} (\lambda a_i)x^i, \quad \lambda \in K.$$
Esempio:
$$3(2x^2 + x + 1) = 6x^2 + 3x + 3.$$

- **Prodotto di polinomi:**
$$(p \cdot q)(x) = \left(\sum_{i=0}^{d} a_i x^i\right)\left(\sum_{\alpha=0}^{e} b_\alpha x^\alpha\right) = \sum_{k=0}^{d+e}\left(\sum_{i+\alpha=k} a_i b_\alpha\right) x^k.$$
Esempio:
$$(x+1)(x^2 + x + 1) = x^3 + 2x^2 + 2x + 1.$$

Con queste operazioni $(K[x], +, \cdot)$ è un **anello commutativo con identità** e, rispetto alla sola somma, uno **spazio vettoriale** su K.

—

Definizione (Polinomi in più variabili)
Siano $x_1, x_2, \dots, x_n$ variabili e K un campo.
Un **monomio** nelle variabili $x_1, \dots, x_n$ è un prodotto del tipo
$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$
dove $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$.
Un **polinomio in n variabili** a coefficienti in K è una somma finita di monomi moltiplicati per scalari:
$$p(x_1, \dots, x_n) = \sum_{\alpha \in A} a_\alpha x^\alpha, \quad a_\alpha \in K,$$
dove $A \subset \mathbb{N}^n$ è un insieme finito.
L'insieme di tutti i polinomi in n variabili a coefficienti in K si indica con
$$K[x_1, \dots, x_n].$$

—

Definizione (Grado di un polinomio in più variabili)
Sia $p(x_1, \dots, x_n) = \sum_\alpha a_\alpha x^\alpha$, con $a_\alpha \neq 0$ per un certo numero finito di α.

- Il **grado del monomio** $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ è
$$\operatorname{gr}(x^\alpha) = \sum_{i=1}^n \alpha_i.$$

- Il **grado del polinomio** è
$$\operatorname{gr}(p) = \max\{\operatorname{gr}(x^\alpha) \mid a_\alpha \neq 0\}.$$

Esempio:
$$p(x, y, z) = 2x^2y + 3xyz^3 - 5z^2 \quad \Rightarrow \quad \operatorname{gr}(p) = \max\{3, 5, 2\} = 5.$$

Definizione (Polinomio lineare)
Un **polinomio lineare** in una variabile x su un campo K è un polinomio del tipo
$$p(x) = a_1 x + a_0,$$
dove $a_1, a_0 \in K$ e $a_1 \neq 0$.

- Il **grado** di un polinomio lineare è 1, poiché il termine di grado più alto è $a_1 x$.
- Il termine a_1 si chiama **coefficiente angolare** o **coefficiente direttore**.
- Il termine a_0 si chiama **termine noto**.

Nel caso di più variabili, un **polinomio lineare** in $x_1, x_2, \dots, x_n$ è della forma
$$p(x_1, x_2, \dots, x_n) = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n + a_0,$$
con $a_0, a_1, \dots, a_n \in K$ e almeno uno tra $a_1, \dots, a_n$ non nullo.

2.2 Matrici

Definizione (Matrice)
Siano $m, n \in \mathbb{N}$ e sia X un insieme non vuoto. Una **matrice di tipo** $m \times n$ a valori in X è una applicazione
$$A : \{1, 2, \dots, m\} \times \{1, 2, \dots, n\} \longrightarrow X$$
che associa a ogni coppia (i, j) un elemento $a_{ij} \in X$.
Scriviamo
$$A = (a_{ij})_{m \times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$
L'insieme di tutte le matrici $m \times n$ a valori in X si indica con $M_{m,n}(X)$.

Esempio

Matrice 3×2 su un insieme X Siano

$$m = 3, \quad n = 2, \quad X = \{\pi, \sqrt{2}, \square, \star, y\}.$$

Definiamo

$$A : \{1,2,3\} \times \{1,2\} \longrightarrow X$$

tale che:

$$\begin{aligned} A(1,1) &= \pi, & A(1,2) &= \sqrt{2}, \\ A(2,1) &= \square, & A(2,2) &= \star, \\ A(3,1) &= y, & A(3,2) &= \pi. \end{aligned}$$

Allora la matrice A è:

$$A = \begin{pmatrix} \pi & \sqrt{2} \\ \square & \star \\ y & \pi \end{pmatrix}.$$

Osservazioni: Operazioni sulle matrici

Siano $A, B \in M_{m,n}(K)$.

- La loro somma è la matrice $C = A + B$ definita da:

$$c_{ij} = a_{ij} + b_{ij}, \quad \forall i = 1, \ldots, m, \ j = 1, \ldots, n.$$

Esempio

Somma di matrici

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} \Rightarrow A + B = \begin{pmatrix} 6 & 8 \\ 10 & 12 \end{pmatrix}.$$

- Sia $A = (a_{ij}) \in M_{m,n}(K)$ e $\lambda \in K$. Definiamo la matrice $\lambda A = (\lambda a_{ij})$, cioè:

$$(\lambda A)_{ij} = \lambda \cdot a_{ij}.$$

Esempio

Moltiplicazione per uno scalare

$$\lambda = 3, \quad A = \begin{pmatrix} 1 & -2 \\ 0 & 4 \end{pmatrix} \Rightarrow 3A = \begin{pmatrix} 3 & -6 \\ 0 & 12 \end{pmatrix}.$$

Capitolo 3

Lezione 3 - 01/10

3.1 Matrice Trasposta

Definizione (Matrice Trasposta)
Sia $A \in M_{m,n}(K)$. La trasposta di A, denotata ${}^tA$, è la matrice del tipo $[n, m]$ che come righe ha le colonne di A.

$${}^tA = \begin{bmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{bmatrix} \in M_{n,m}(K), \text{ ottenuta scambiando righe e colonne di } A.$$

3.2 Prodotto Scalare

Definizione (Prodotto scalare)
Sia $K = \mathbb{R}$ e siano due vettori $\mathbf{a} = (a_1, a_2, \dots, a_n), \mathbf{b} = (b_1, b_2, \dots, b_n) \in K^n$.
Il **prodotto scalare** è la funzione

$$K^n \times K^n \longrightarrow K, \quad (\mathbf{a}, \mathbf{b}) \longmapsto a_1b_1 + a_2b_2 + \cdots + a_nb_n = \langle \mathbf{a}, \mathbf{b} \rangle \,,$$

che associa la coppia di vettori ad uno scalare, dato dalla somma delle componenti omonime dei due vettori.

3.3 Matrice Conformabile

Definizione (Matrice Conformabile)
Due matrici $A \in M_{m,n}(K)$ e $B \in M_{p,q}(K)$ si dicono **conformabili** per il prodotto se e solo se il numero di colonne di A è uguale al numero di righe di B, cioè $n = p$. In tal caso, il prodotto AB è definito ed è una matrice di dimensione $m \times q$.
Esempio: Siano

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix} \in M_{3,2}(K), \quad B = \begin{bmatrix} 7 & 8 & 9 \\ 10 & 11 & 12 \end{bmatrix} \in M_{2,3}(K).$$

Allora A e B sono conformabili e

$$AB = \begin{bmatrix} 1 \cdot 7 + 2 \cdot 10 & 1 \cdot 8 + 2 \cdot 11 & 1 \cdot 9 + 2 \cdot 12 \\ 3 \cdot 7 + 4 \cdot 10 & 3 \cdot 8 + 4 \cdot 11 & 3 \cdot 9 + 4 \cdot 12 \\ 5 \cdot 7 + 6 \cdot 10 & 5 \cdot 8 + 6 \cdot 11 & 5 \cdot 9 + 6 \cdot 12 \end{bmatrix} \in M_{3,3}(K).$$

3.4 Prodotto Riga per Colonna

Definizione (Prodotto Riga Per Colonna)
Siano $A \in M_{m,n}(K)$ e $B \in M_{n,p}(K)$. Il prodotto di una riga i-esima di A per una colonna j-esima di B è definito come la somma dei prodotti delle componenti corrispondenti:

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}.$$

In altre parole, per ottenere l'elemento in posizione (i, j) del prodotto AB, si moltiplicano elemento per elemento la riga i di A con la colonna j di B e si sommano i risultati.
Esempio: Siano

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}, \quad B = \begin{bmatrix} 7 & 8 \\ 9 & 10 \\ 11 & 12 \end{bmatrix}.$$

Allora

$$(AB)_{11} = 1 \cdot 7 + 2 \cdot 9 + 3 \cdot 11 = 58, \quad (AB)_{12} = 1 \cdot 8 + 2 \cdot 10 + 3 \cdot 12 = 68,$$

e così via per gli altri elementi del prodotto.

Osservazione: Proprietà Prodotto riga per colonna

- Non è commutativa.
- Distributività destra e sinistra.
- È associativa.
- Ha elemento neutro formato dalla matrice identica $I_n =$.

3.5 Sistema Lineare

Definizione (Sistema Lineare)
Siano $m, n \in \mathbb{N}$, e sia K un campo. Un **sistema lineare** di m equazioni in n incognite $x_1, x_2, \ldots, x_n$ su un campo K è un insieme di m equazioni del tipo:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n - b_1 = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n - b_2 = 0 \\ \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n - b_m = 0 \end{cases}$$

In forma compatta, un sistema lineare può essere scritto come:

$$A\mathbf{x} = \mathbf{b},$$

dove:

- $A \in M_{m,n}(K)$ è la **matrice dei coefficienti**;
- $\mathbf{x} \in K^n$ è il **vettore incognite**;
- $\mathbf{b} \in K^m$ è il **vettore dei termini noti**.

Osservazione: Soluzioni di un sistema lineare
L'insieme delle soluzioni di un sistema lineare è dato da

$$S_1 \text{ soluzioni della prima equazione } E_1(x)$$

$$S_2 \text{ soluzioni della seconda equazione } E_2(x)$$

$$\dots$$

$$S_m \text{ soluzioni della m-esima equazione } E_m(x)$$

Noi siamo interessati a

$$S = \bigcap_{i=1}^{m} S_i,$$

ovvero l'intersezione di tutte le soluzioni del sistema.

Definizione (Compatibilità di un sistema lineare)
Un sistema lineare Σ si dice **compatibile** se ammette almeno una soluzione, ossia se l'insieme delle soluzioni è diverso dal vuoto.

Altrimenti se $S = \varnothing$, allora il sistema si dice **incompatibile**.

Definizione (Matrice completa e incompleta)
Dato un sistema lineare Σ si distinguono due matrici:

- La **matrice incompleta** (o matrice dei coefficienti) di un sistema lineare contiene solo i coefficienti delle incognite.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

- La **matrice completa** (o matrice dei coefficienti estesa) si ottiene aggiungendo a quella incompleta una colonna aggiuntiva con i termini noti del sistema.

$$C = (A \,|\, \mathbf{b}) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{bmatrix}$$

Esempi di matrici complete e incomplete

Consideriamo due sistemi lineari in due incognite x_1, x_2.

- **Sistema omogeneo** Σ (con termini noti nulli):

$$\Sigma_0 : \begin{cases} 3x_2 - x_2 + 2x_4 = 0 \\ x_1 + x_2 + 2x_3 = 0 \end{cases}$$

  - Matrice incompleta:

$$A = \begin{bmatrix} 0 & 3 & -1 & 2 \\ 1 & 1 & 2 & 0 \end{bmatrix}$$

- **Sistema non omogeneo** Σ (con termini noti $\neq 0$):

$$\Sigma : \begin{cases} 3x_2 - x_2 + 2x_4 - 3 = 0 \\ x_1 + x_2 + 2x_3 + 5 = 0 \end{cases}$$

  - Matrice completa:

$$A = \begin{bmatrix} 0 & 3 & -1 & 2 & | & -3 \\ 1 & 1 & 2 & 0 & | & 5 \end{bmatrix}$$

3.6 Operazioni o Trasformazioni Elementari sulle Righe di una Matrice

Definizione (Operazioni elementari sulle righe)

Sia $A \in M_{m,n}(K)$ una matrice. Si chiamano **operazioni elementari sulle righe** le seguenti trasformazioni che possono essere applicate alle righe di A:

1. **Scambio di due righe:** per ogni $h, k \in \{1, \ldots, m\}$,

$$\mathbf{b}^{(h)} \longleftrightarrow \mathbf{b}^{(k)}.$$

2. **Moltiplicazione di una riga per uno scalare non nullo:** per ogni $h \in \{1, \ldots, m\}$ e per ogni $\lambda \in K \setminus \{0\}$,

$$\mathbf{b}^{(h)} \longrightarrow \lambda \mathbf{b}^{(h)}.$$

3. **Somma di una riga con un multiplo di un'altra:** per ogni $h, k \in \{1, \ldots, m\}$ e per ogni $\beta \in K$,

$$\mathbf{b}^{(h)} \longrightarrow \mathbf{b}^{(h)} + \beta \mathbf{b}^{(k)}.$$

Osservazione: Invarianza dell'insieme delle soluzioni

Le operazioni elementari sulle righe di una matrice (e quindi sul sistema lineare associato) **modificano la forma del sistema**, ma **non alterano il suo insieme delle soluzioni**.

Capitolo 4

Lezione 4 - 3/10 (Teams)

4.1 Matrice a Gradini e Completamente a Gradini

Definizione (Matrice ridotta a gradini)
Una matrice si dice a gradini se ha le seguenti proprietà:

- Se una riga è nulla, tutte le righe successive sono nulle:

$$\exists\, h \in \{1, \dots, m\} \mid a^h = 0 \;\Rightarrow\; a^i = 0 \;\; \forall i > h$$

- Il primo elemento diverso da zero di una riga non nulla, detto *pivot*, è più a sinistra del primo elemento non nullo delle righe successive:

$$\text{Se } a_{ij} \neq 0 \text{ e } a_{ih} = 0,\ \forall\, h < j,\ \text{allora } a_{i+1,h} = 0,\ \forall\, h \leq j.$$

Definizione (Matrice completamente ridotta a gradini)
Una matrice si dice completamente ridotta a gradini se oltre le precedenti due proprietà verifica anche le seguenti:

- il pivot di una qualunque riga non nulla è 1;
- ogni colonna che contiene il pivot di una riga ha tutti gli altri elementi nulli.

4.2 Algoritmo di Gauss

Teorema (Algoritmo di Gauss)
Ogni matrice su un campo K può essere ridotta o completamente ridotta a gradini mediante un numero finito di operazioni elementari.

Dimostrazione (per induzione)

Procediamo per induzione sul numero di righe m:

- **Per** $m = 1$**:**

$$A = (a_{11}, a_{12}, \dots, a_{1n})$$

Se a_{1j} è il pivot, basta eseguire la seguente operazione di normalizzazione (ridurre a 1):

$$a^{(1)} \;\to\; \frac{1}{a_{1j}}\, a^{(1)}.$$

- **Per** $m > 1$**:** Dimostriamo che, se vale per $m-1$, allora vale anche per m. Prima di tutto, individuiamo la prima riga non nulla:

$$A = \begin{bmatrix} a_{11} & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{mj} & \dots & a_{mn} \end{bmatrix}.$$

Sia

$$j = \min\{\, l \in \{1, \dots, n\} \mid a_{1l} \neq 0 \,\}$$

la posizione del primo elemento non nullo nella prima riga.

Analogamente, poniamo

$$k = \min\{\, i \in \{1, \dots, m\} \mid a_{ij} \neq 0 \,\},$$

cioè l'indice della prima riga (a partire dall'alto) che contiene un elemento non nullo nella colonna j.

Una volta individuati tali indici, scambiamo la riga a_k con la prima riga a_1:

$$a_k \longleftrightarrow a_1.$$

Dopo lo scambio, otteniamo:

$$A' = \begin{bmatrix} a'_{11} & a'_{1j} & \dots & a'_{1n} \\ a'_{21} & a'_{2j} & \dots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{m1} & a'_{mj} & \dots & a'_{mn} \end{bmatrix}.$$

Dato a'_{1j} (pivot della prima riga, diverso da 0), dobbiamo annullare tutti gli elementi sottostanti:

Per la riga 2, basta prendere $B = -\dfrac{a'_{2j}}{a'_{1j}}$ in modo che

$$a'_{2j} + Ba'_{1j} = 0.$$

Procediamo quindi in questo modo per tutte le righe sottostanti, ottenendo:

$$\begin{aligned} a^{(2)} &\to a^{(2)} - \frac{a'_{2j}}{a'_{1j}}\, a^{(1)}, \\ a^{(3)} &\to a^{(3)} - \frac{a'_{3j}}{a'_{1j}}\, a^{(1)}, \\ &\vdots \\ a^{(m)} &\to a^{(m)} - \frac{a'_{mj}}{a'_{1j}}\, a^{(1)}. \end{aligned}$$

Se si vuole la matrice completamente ridotta, bisogna normalizzare il pivot a''_{kj} di ogni riga e annullare gli elementi della stessa colonna che si trovano sopra ai pivot delle righe successive.

Osservazione: Derivata dal Teorema di Rouché-Capelli
Un sistema lineare $\Sigma : Ax = b$ è compatibile $\Leftrightarrow$ la matrice completa, una volta ridotta a gradini tramite operazioni elementari, non presenta una riga in cui tutti gli elementi della matrice dei coefficienti sono 0 ma l'elemento nella colonna dei termini noti è diverso da 0.

$$\Sigma : \begin{cases} x_1 + x_2 = 1 \\ 2x_1 + 2x_2 = 3 \end{cases}$$

$$\text{Matrice completa:} \quad C = \begin{bmatrix} 1 & 1 & | & 1 \\ 2 & 2 & | & 3 \end{bmatrix}$$

$$\text{Applichiamo } R_2 \to R_2 - 2R_1 :$$

$$C = \begin{bmatrix} 1 & 1 & | & 1 \\ 0 & 0 & | & 1 \end{bmatrix}$$

Il sistema è impossibile.

4.3 Teorema di struttura

Teorema (Teorema di struttura dell'insieme delle soluzioni di un sistema lineare)
Sia $\Sigma : A\mathbf{x} = \mathbf{b}$ un sistema lineare di equazioni in n incognite e sia $\Sigma_0 : A\mathbf{x} = \mathbf{0}$ il sistema lineare omogeneo associato.
Sia

$$\mathbf{S} = \{(y_1, \dots, y_n) \in K^n \mid A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \mathbf{b}\}$$

l'insieme delle soluzioni di Σ, e sia

$$\mathbf{S}_0 = \{(z_1, \dots, z_n) \in K^n \mid A \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \mathbf{0}\}$$

l'insieme delle soluzioni di Σ_0.
Allora, se $(\bar{y}_1, \dots, \bar{y}_n) \in \mathbf{S}$, si ha

$$\mathbf{S} = \{(\bar{y}_1, \dots, \bar{y}_n) + (z_1, \dots, z_n) \mid (z_1, \dots, z_n) \in \mathbf{S}_0\} = \mathbf{X}.$$

Dimostrazione:

Mostriamo che $\mathbf{S} \subseteq \mathbf{X}$ verificando le due inclusioni:

1. $\mathbf{S} \subseteq \mathbf{X}$: Sia $(y_1, \dots, y_n) \in \mathbf{S}$. Consideriamo $(z_1, \dots, z_n) = (y_1, \dots, y_n) - (\bar{y}_1, \dots, \bar{y}_n)$. Poiché
$$A\mathbf{z} = A(\mathbf{y} - \bar{\mathbf{y}}) = A\mathbf{y} - A\bar{\mathbf{y}} = \mathbf{b} - \mathbf{b} = \mathbf{0},$$
si ha $\mathbf{z} \in \mathbf{S}_0$. Quindi $\mathbf{y} = \bar{\mathbf{y}} + \mathbf{z} \in \mathbf{X}$.
2. $\mathbf{X} \subseteq \mathbf{S}$: Sia $\mathbf{x} \in \mathbf{X}$. Allora $\mathbf{x} = \bar{\mathbf{y}} + \mathbf{z}$ con $\mathbf{z} \in \mathbf{S}_0$. Allora
$$A\mathbf{x} = A(\bar{\mathbf{y}} + \mathbf{z}) = A\bar{\mathbf{y}} + A\mathbf{z} = \mathbf{b} + \mathbf{0} = \mathbf{b},$$
quindi $\mathbf{x} \in \mathbf{S}$.

Da queste due inclusioni segue che $\mathbf{S} = \mathbf{X}$. $\square$

4.4 Proprietà dell'insieme S_0 come sottospazio vettoriale

Proposizione: Proprietà dell'insieme delle soluzioni di un sistema lineare omogeneo

Sia $\Sigma_0 : A\mathbf{x} = \mathbf{0}$ un sistema lineare omogeneo in n incognite, e sia

$$\mathbf{S}_0 = \{\, \mathbf{z} \in K^n \mid A\mathbf{z} = \mathbf{0} \,\}$$

l'insieme delle sue soluzioni. Allora valgono le seguenti proprietà:

1. Il vettore nullo $\mathbf{0}$ appartiene a $\mathbf{S}_0$.
2. Se $\mathbf{z}, \mathbf{z}' \in \mathbf{S}_0$, allora $\mathbf{z} + \mathbf{z}' \in \mathbf{S}_0$.
3. Se $\alpha \in K$ e $\mathbf{z} \in \mathbf{S}_0$, allora $\alpha\mathbf{z} \in \mathbf{S}_0$.

In conclusione, $\mathbf{S}_0$ è chiuso rispetto alla somma e alla moltiplicazione per scalari, e quindi costituisce un sottospazio vettoriale di K^n.

Definizione (Sottospazio vettoriale)
Un sottoinsieme V si dice *linearmente chiuso* se:

1. $V \neq \emptyset$;
2. $\forall\, \mathbf{u}, \mathbf{v} \in V \Rightarrow \mathbf{u} + \mathbf{v} \in V$;
3. $\forall\, \alpha \in K,\ \mathbf{u} \in V \Rightarrow \alpha\mathbf{u} \in V$.

Poiché $\mathbf{S}_0$ soddisfa esattamente queste proprietà, segue che l'insieme delle soluzioni di un sistema lineare omogeneo è un sottospazio vettoriale di K^n.

Proposizione: Sottoinsiemi linearmente chiusi come sottospazi vettoriali

Sia V uno spazio vettoriale su un campo K e sia

$$W \subseteq V$$

un sottoinsieme non vuoto tale che:

1. $\forall \mathbf{u}, \mathbf{v} \in W \Rightarrow \mathbf{u} + \mathbf{v} \in W$;
2. $\forall \alpha \in K, \mathbf{u} \in W \Rightarrow \alpha\mathbf{u} \in W$.

Allora W è un sottospazio vettoriale di V.

Osservazione: Operazioni interne
Le proprietà di chiusura rispetto alla somma e al prodotto per scalare garantiscono che le operazioni siano interne anche se considerate come:

$$+ : W \times W \to W, \qquad \cdot : K \times W \to W.$$

In altre parole, la somma di due elementi di W appartiene ancora a W e il prodotto di uno scalare con un elemento di W appartiene sempre a W.

Capitolo 5

Lezione 5 - 08/10

5.1 Sistemi di Generatori

Definizione (Combinazione Lineare)
Consideriamo $(V, +, \cdot)$ uno spazio vettoriale su K. Sia $(u_1, ..., u_n)$ una n-upla di vettori di V. Un vettore u si dice **combinazione lineare** di questa n-upla se esiste una n-upla di scalari $(\alpha_1, ..., \alpha_n) \in K$ tali che

$$\mathbf{u} = \alpha_1 u_1 + ... + \alpha_n u_n$$

.
Se vogliamo permettere che ci siano ripetizioni tra i vettori e gli scalari, allora consideriamo t-uple $(u_1, ..., u_t) \in V^t$, $(\alpha_1, ..., \alpha_t) \in K^t$.

Definizione (Sistema di Generatori)
Sia V uno spazio vettoriale su un campo K. Un insieme $S \subseteq V$ si dice **sistema di generatori** di V se ogni vettore di V può essere espresso come combinazione lineare di un numero finito di vettori di S. In simboli:

$$V = L(S) = \left\{ \sum_{i=1}^{n} \lambda_i v_i \;\middle|\; v_i \in S,\ \lambda_i \in K,\ n \in \mathbb{N} \right\}.$$

In altre parole, i vettori di S *generano* lo spazio V. Se esiste un insieme finito S che genera V, allora si dice che V è **finitamente generato**.

Definizione (Chiusura Lineare)
Dato un sottinsieme $X \neq \emptyset$ di V, diremo **chiusura lineare** di X il sottoinsieme $L(X)$ di V, costituito da tutti e soli i vettori che sono combinazioni lineari di vettori di X. Se:

- $X = \emptyset$, porremo convenzionalmente $L(\emptyset) = 0$
- $X = x_1, ..., x_t$ è un insieme finito, scriveremo $L(x_1, .., x_t)$.

Esempio: $L((2, 3), (1, 1)) = \{\alpha_1(2, 3) + \alpha_2(1, 1) | \alpha_1, \alpha_2 \in \mathbb{R}\}$.

Proposizione: Importante sulla chiusura lineare

Sia $X \subseteq V$. Allora valgono le seguenti proprietà:

- $X \subseteq L(X)$;
- $L(X)$ è un sottospazio vettoriale di V;
- Se $W \subseteq V$ è un sottospazio vettoriale di V tale che $X \subseteq W$, allora $L(X) \subseteq W$.

Dimostrazione del primo punto. Consideriamo un qualunque $u \in X$. Poiché $u = 1 \cdot u$, ed $1 \in K$, si ha che u è combinazione lineare di un elemento di X. Dunque $u \in L(X)$, e quindi:

$$X \subseteq L(X).$$

□

Dimostrazione del secondo punto. Dimostriamo che $L(X)$ è un sottospazio vettoriale di V.
(1) Non vuoto. Poiché $L(X) \supseteq X$ e $X \neq \emptyset$, segue immediatamente che $L(X) \neq \emptyset$.
(2) Chiusura rispetto all'addizione. Siano $u, u' \in L(X)$. Allora, per definizione di chiusura lineare, esistono $t, t' \in \mathbb{N}$, vettori $u_1, \dots, u_t, u'_1, \dots, u'_{t'} \in X$ e scalari $\alpha_1, \dots, \alpha_t, \alpha'_1, \dots, \alpha'_{t'} \in K$ tali che:

$$u = \alpha_1 u_1 + \cdots + \alpha_t u_t, \qquad u' = \alpha'_1 u'_1 + \cdots + \alpha'_{t'} u'_{t'}.$$

Sommando membro a membro otteniamo:

$$u + u' = \alpha_1 u_1 + \cdots + \alpha_t u_t + \alpha'_1 u'_1 + \cdots + \alpha'_{t'} u'_{t'} \in L(X),$$

poiché è ancora una combinazione lineare di vettori di X.
(3) Chiusura rispetto alla moltiplicazione per scalare. Sia $\lambda \in K$. Allora:

$$\lambda u = \lambda(\alpha_1 u_1 + \cdots + \alpha_t u_t) = (\lambda\alpha_1)u_1 + \cdots + (\lambda\alpha_t)u_t \in L(X),$$

poiché anche in questo caso otteniamo una combinazione lineare di elementi di X.
Pertanto, $L(X)$ è chiuso rispetto alla somma e alla moltiplicazione per scalare, quindi è un sottospazio vettoriale di V. □

Dimostrazione del terzo punto. Ipotizziamo che W sia un sottospazio vettoriale di V tale che $X \subseteq W$.
Vogliamo mostrare che $L(X) \subseteq W$; cioè, per ogni $u \in L(X)$, si ha $u \in W$.
Sia dunque $u \in L(X)$. Per definizione di chiusura lineare, esistono $u_1, \dots, u_t \in X$ e $\alpha_1, \dots, \alpha_t \in K$ tali che:

$$u = \alpha_1 u_1 + \cdots + \alpha_t u_t.$$

Poiché $X \subseteq W$, ciascun $u_i \in W$. Poiché W è sottospazio vettoriale, è chiuso rispetto alla moltiplicazione per scalare:

$$\alpha_i u_i \in W \quad \forall i.$$

Inoltre, W è chiuso rispetto all'addizione, dunque:

$$\alpha_1 u_1 + \cdots + \alpha_t u_t \in W.$$

Quindi $u \in W$, e pertanto $L(X) \subseteq W$. □

5.2 Dipendenza e indipendenza lineare

Definizione (Linearmente dipendente e indipendente)
Una $n - pla(v_1, ..., v_n)$ di vettori di V spazio vettoriale su K sarà detta **linearmente dipendente** se esiste una $n - pla(\alpha_1, ..., \alpha_n) \in K$ di scalari non tutti nulli, tale che

$$\alpha_1 v_1 + ... + \alpha_n v_n = 0.$$

In caso contrario, e cioè se gli scalari sono tutti nulli

$$(\alpha_1 v_1 + ... + \alpha_n v_n) \Rightarrow (a_i = 0, \forall i \in \mathbb{N}_n)$$

la $n - pla(v_1, ..., v_n)$ sarà detta **linearmente indipendente**.

Osservazione:
Se $X \subseteq T \subseteq V$, con X linearmente **dipendente** $\Rightarrow T$ è linearmente **dipendente**.
Se $Y \subseteq X \subseteq V$, con X linearmente **indipendente** $\Rightarrow Y$ è linearmente **indipendente**.

Teorema (Caratterizzazione della dipendenza lineare)
Un sottoinsieme X di V è **linearmente dipendente** se e solo se

$$\exists\, u \in X \text{ tale che } L(X) = L(X \setminus \{u\}).$$

Non consideriamo il caso $X = \emptyset$, poiché l'insieme vuoto è per definizione linearmente indipendente. Quindi supponiamo $X \neq \emptyset$.

Dimostrazione.
(Direzione "⇒"): Sia X linearmente dipendente. Per definizione, esistono $u_1, \dots, u_t \in X$ e scalari $\alpha_1, \dots, \alpha_t \in K$, non tutti nulli, tali che:

$$\vec{0} = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_t u_t.$$

Sia $\alpha_t \neq 0$. Allora esiste $\alpha_t^{-1} \in K$. Moltiplicando entrambi i membri per α_t^{-1}, otteniamo:

$$\vec{0} = (\alpha_t^{-1}\alpha_1)u_1 + \cdots + (\alpha_t^{-1}\alpha_{t-1})u_{t-1} + (\alpha_t^{-1}\alpha_t)u_t.$$

Ma $\alpha_t^{-1}\alpha_t = 1$, quindi:

$$u_t = -(\alpha_t^{-1}\alpha_1)u_1 - \cdots - (\alpha_t^{-1}\alpha_{t-1})u_{t-1}.$$

Da cui segue che u_t è combinazione lineare degli altri vettori $u_1, \dots, u_{t-1}$, cioè:

$$u_t \in L(\{u_1, \dots, u_{t-1}\}) \subseteq L(X \setminus \{u_t\}).$$

Quindi:

$$L(X) = L(X \setminus \{u_t\}),$$

perché rimuovere u_t non cambia la chiusura lineare dell'insieme. Ciò dimostra la direzione "⇒".

(Direzione "⇐"): Supponiamo ora che esista $u \in X$ tale che $L(X) = L(X \setminus \{u\})$. Allora $u \in L(X \setminus \{u\})$, cioè:

$$u = \alpha_1 u_1 + \cdots + \alpha_t u_t,$$

con $u_1, \dots, u_t \in X \setminus \{u\}$ e $\alpha_i \in K$.
Portando tutto a primo membro otteniamo:

$$\vec{0} = (-1)u + \alpha_1 u_1 + \cdots + \alpha_t u_t.$$

Questa è una combinazione lineare non banale (poiché il coefficiente di u è $-1 \neq 0$) che dà il vettore nullo. Quindi X è linearmente dipendente.

□

Capitolo 6

Lezione 6 - 10/10

6.1 Basi

Definizione (Base)
Una **base** B di uno spazio vettoriale V è un insieme di vettori tale che:

- B è **linearmente indipendente**;
- B è un **sistema di generatori** di V, cioè $L(B) = V$.

In altre parole, ogni vettore di V può essere scritto in modo unico come combinazione lineare dei vettori di B.

6.1.1 Teorema di estrazione di una base

Teorema (di estrazione di una base)
Sia V uno spazio vettoriale finitamente generato sul campo K. Sia $S = \{v_1, \dots, v_t\}$ un sistema finito di generatori di V. Allora esiste una base B di V tale che $B \subseteq S$.

Dimostrazione. Consideriamo due casi.

Caso 1: $S = \emptyset$. In questo caso, $V = L(\emptyset) = \{\bar{0}\}$, ossia V è lo spazio vettoriale nullo. La base di V è per definizione l'insieme vuoto stesso, quindi $B = S = \emptyset$.

Caso 2: $S \neq \emptyset$. Verifichiamo se S è linearmente indipendente.

- Se S è linearmente indipendente, allora essendo anche un sistema di generatori, è già una base di V; dunque $B = S$.
- Se invece S è linearmente dipendente, allora per il teorema della dipendenza lineare esiste un vettore $u \in S$ tale che
$$L(S) = L(S \setminus \{u\}).$$
Ciò significa che possiamo eliminare u dall'insieme dei generatori senza modificare lo spazio generato. Poniamo quindi $S_1 = S \setminus \{u\}$.

Ora applichiamo lo stesso ragionamento a S_1:

- se S_1 è linearmente indipendente, allora $B = S_1$ è una base di V;
- se S_1 è ancora dipendente, allora esiste $v \in S_1$ tale che $L(S_1) = L(S_1 \setminus \{v\})$, e possiamo quindi togliere anche v.

Procedendo in questo modo, ad ogni passo eliminiamo un vettore "superfluo" mantenendo lo stesso spazio generato. Poiché S è finito, dopo un numero finito di eliminazioni otterremo un sottoinsieme $B \subseteq S$ che:

$$L(B) = V \quad \text{e} \quad B \text{ è linearmente indipendente.}$$

Pertanto B è una base di V contenuta in S. $\square$

Proposizione:

Sia V uno spazio vettoriale su un campo K, e sia $S = \{u_1, \dots, u_h\} \subseteq V$ un insieme linearmente indipendente. Se $u \in V \setminus L(S)$, allora anche l'insieme $S \cup \{u\}$ è linearmente indipendente.

Dimostrazione (per assurdo). Procediamo per assurdo. Supponiamo che $S \cup \{u\}$ *non* sia linearmente indipendente. Allora, per definizione, esistono scalari $\alpha_1, \dots, \alpha_h, \beta \in K$, non tutti nulli, tali che:

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_h u_h + \beta u = \vec{0}.$$

Caso 1: $\beta = 0$. Allora la relazione diventa:

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_h u_h = \vec{0}.$$

Ma S è linearmente indipendente per ipotesi, quindi necessariamente:

$$\alpha_1 = \alpha_2 = \cdots = \alpha_h = 0.$$

Ciò implica che tutti gli scalari sono nulli, il che contraddice l'assunzione iniziale ("non tutti nulli"). Quindi $\beta \neq 0$.

Caso 2: $\beta \neq 0$. Possiamo allora isolare u:

$$\beta u = -(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_h u_h).$$

Moltiplicando ambo i membri per β^{-1} (che esiste, poiché $\beta \neq 0$):

$$u = (-\beta^{-1}\alpha_1)u_1 + (-\beta^{-1}\alpha_2)u_2 + \cdots + (-\beta^{-1}\alpha_h)u_h.$$

Ma questo significa precisamente che $u \in L(S)$.

Tuttavia, per ipotesi, $u \notin L(S)$. Questa è una contraddizione.

Pertanto, la nostra ipotesi iniziale è falsa, e $S \cup \{u\}$ deve essere linearmente indipendente.

$$\boxed{S \cup \{u\} \text{ è linearmente indipendente.}}$$

□

Teorema (Lemma di Steinitz)

Sia V uno spazio vettoriale finitamente generato su un campo K e sia $S = \{u_1, \dots, u_n\}$ un suo sistema di generatori finito, cioè $L(S) = V$.

Sia $X = \{v_1, \dots, v_m\}$ un insieme di vettori di V.

Se $m = |X| > n = |S|$, allora X è linearmente dipendente.

Proposizione: Corollario

Utilizzando le stesse notazioni del Lemma di Steinitz, se X è linearmente indipendente, allora:

$$|X| \leq |S|.$$

Dimostrazione

Iniziamo con un caso banale: se il vettore nullo $\mathbf{0} \in X$, allora X è linearmente dipendente (poiché contiene il sottoinsieme $\{\mathbf{0}\}$ che è L.D.), e la tesi è dimostrata.

Supponiamo quindi $\mathbf{0} \notin X$. Ciò implica che tutti i vettori $v_i \in X$ sono non nulli.

Passo 1: Scambio di v_1

Consideriamo il primo vettore $v_1 \in X$. Poiché $v_1 \in V$ e $L(S) = V$, v_1 è combinazione lineare dei vettori di S:

$$v_1 = \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_n u_n$$

Poiché abbiamo supposto $v_1 \neq \mathbf{0}$, almeno uno dei coefficienti $\lambda_1, \ldots, \lambda_n$ deve essere non nullo. A meno di riordinare i vettori u_i (operazione che non altera $L(S)$), possiamo supporre che $\lambda_1 \neq 0$. Esistendo $\lambda_1^{-1} \in K$, possiamo isolare u_1:

$$\lambda_1 u_1 = v_1 - \lambda_2 u_2 - \cdots - \lambda_n u_n$$

$$u_1 = \lambda_1^{-1} v_1 - (\lambda_1^{-1}\lambda_2) u_2 - \cdots - (\lambda_1^{-1}\lambda_n) u_n$$

Questa equazione mostra che $u_1 \in L(\{v_1, u_2, \ldots, u_n\})$.

Definiamo il nuovo insieme $S_1 = \{v_1, u_2, \ldots, u_n\}$. Dimostriamo che $L(S_1) = V$. Osserviamo che:

- $u_1 \in L(S_1)$ (come appena mostrato).
- $u_2, \ldots, u_n \in S_1 \subseteq L(S_1)$ (banalmente).

Dato che tutti i generatori originali $S = \{u_1, \ldots, u_n\}$ appartengono a $L(S_1)$, si ha che $S \subseteq L(S_1)$. Questo implica $V = L(S) \subseteq L(S_1) \subseteq V \Rightarrow L(S_1) = V$. Abbiamo quindi sostituito u_1 con v_1 ottenendo un nuovo sistema di n generatori.

Passo 2: Scambio di v_2

Consideriamo il secondo vettore $v_2 \in X$. Per la nostra ipotesi, $v_2 \neq \mathbf{0}$. Poiché $v_2 \in V$ e (dal passo precedente) $V = L(S_1)$, possiamo scrivere v_2 come combinazione lineare dei vettori di S_1:

$$v_2 = \beta_1 v_1 + \beta_2 u_2 + \beta_3 u_3 + \cdots + \beta_n u_n$$

Ora abbiamo due possibilità:

Caso A: Tutti i coefficienti dei vettori u_i sono nulli. Cioè, $\beta_2 = \beta_3 = \cdots = \beta_n = 0$. L'equazione diventa:

$$v_2 = \beta_1 v_1 \Rightarrow \beta_1 v_1 - v_2 = \mathbf{0}$$

Poiché $v_2 \neq \mathbf{0}$, questa è una combinazione lineare non banale (il coefficiente di v_2 è -1) di vettori di X. Dunque $\{v_1, v_2\} \subseteq X$ è linearmente dipendente, e di conseguenza X è linearmente dipendente. In questo caso, la tesi è dimostrata.

Caso B: Almeno uno dei coefficienti $\beta_2, \ldots, \beta_n$ è non nullo. A meno di riordinare i restanti u_i, supponiamo $\beta_2 \neq 0$. Possiamo allora isolare u_2:

$$\beta_2 u_2 = v_2 - \beta_1 v_1 - \beta_3 u_3 - \cdots - \beta_n u_n$$

$$u_2 = (-\beta_2^{-1}\beta_1) v_1 + \beta_2^{-1} v_2 - (\beta_2^{-1}\beta_3) u_3 - \cdots - (\beta_2^{-1}\beta_n) u_n$$

Questo mostra che $u_2 \in L(\{v_1, v_2, u_3, \ldots, u_n\})$.

Definiamo $S_2 = \{v_1, v_2, u_3, \ldots, u_n\}$. Come prima, dimostriamo che $L(S_2) = V$ osservando che $S_1 \subseteq L(S_2)$:

- $v_1 \in S_2 \subseteq L(S_2)$.
- $u_2 \in L(S_2)$ (come appena mostrato).
- $u_3, \ldots, u_n \in S_2 \subseteq L(S_2)$.

Dunque $V = L(S_1) \subseteq L(S_2)$, e concludiamo $L(S_2) = V$.

Iterazione e Conclusione

Si ripete questo procedimento ("così via"). Ad ogni passo $k \leq n$, si considera v_k e lo si scrive come C.L. dei generatori ottenuti al passo $k-1$: $S_{k-1} = \{v_1, \ldots, v_{k-1}, u_k, \ldots, u_n\}$.

O si incontra il **Caso A** (tutti i coefficienti dei restanti u_i sono nulli), il che dimostra che $\{v_1, \ldots, v_k\}$ è L.D. e quindi X è L.D. (e la dimostrazione termina).

Dimostrazione
Oppure si procede con il **Caso B** (almeno un coefficiente di un u_i è non nullo), e si "scambia" quel vettore (diciamo u_k) con v_k, ottenendo un nuovo sistema di generatori $S_k = \{v_1, \dots, v_k, u_{k+1}, \dots, u_n\}$.
Se non si incontra mai il Caso A, dopo n passi avremo sostituito tutti i vettori u_i, ottenendo il sistema di generatori:

$$S_n = \{v_1, \dots, v_n\}$$

(che hai chiamato S'').
Ora usiamo l'ipotesi fondamentale: $m > n$. Questo significa che in X esiste almeno un altro vettore, v_{n+1}. Poiché $v_{n+1} \in V$ e $V = L(S_n) = L(\{v_1, \dots, v_n\})$, v_{n+1} deve essere combinazione lineare di S_n:

$$v_{n+1} = \gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_n v_n$$

Riscrivendo l'equazione, otteniamo:

$$\gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_n v_n - v_{n+1} = \mathbf{0}$$

Questa è una combinazione lineare non banale (il coefficiente di v_{n+1} è $-1 \neq 0$) dei vettori $\{v_1, \dots, v_{n+1}\} \subseteq X$.
Pertanto, X è linearmente dipendente. In ogni possibile scenario, la tesi è dimostrata.

6.2 Teorema di equipotenza della base

Teorema (Teorema di equipotenza della base)
Sia V uno spazio vettoriale finitamente generato su un campo K. Allora tutte le basi di V hanno la stessa cardinalità.
Questa cardinalità comune alle basi di V viene detta **dimensione** di V e si indica con:

$$\dim V.$$

Dimostrazione
Poiché V è finitamente generato, esiste un sistema di generatori finito $S \subseteq V$. Sia B una base di V estratta da S. Allora:

$$|B| = n < +\infty.$$

Sia B' un'altra base di V.
1. Dimostriamo che $|B'| = h < +\infty$. Se così non fosse, esisterebbe un insieme $X \subseteq B'$ tale che $|X| = n + 1 > |B|$, ma questo è impossibile per il **Lemma di Steinitz**, poiché un insieme di vettori con più elementi di un sistema di generatori sarebbe linearmente dipendente.

2. Dimostriamo ora che $|B'| = |B|$.

- Poiché B' è linearmente indipendente in V e B è un sistema di generatori di V, per il Corollario del Lemma di Steinitz si ha:
$$|B'| \leq |B|.$$
- Analogamente, poiché B è linearmente indipendente in V e B' è un sistema di generatori di V, si ha:
$$|B| \leq |B'|.$$

Dalle due disuguaglianze segue che:

$$|B| = |B'|.$$

Quindi tutte le basi di V hanno la stessa cardinalità, che chiamiamo **dimensione** di V:

$$\dim V = |B|.$$

□

Proposizione: Caratterizzazione dei sistemi di generatori di dimensione n

Sia V uno spazio vettoriale su un campo K, con $\dim V = n$. Sia $S = \{u_1, \dots, u_n\} \subseteq V$ un insieme di n vettori.
Allora valgono le seguenti equivalenze:

$$S \text{ è un sistema di generatori di } V \iff S \text{ è linearmente indipendente.}$$

Dimostrazione

($\Rightarrow$) Supponiamo per assurdo che S sia linearmente dipendente. Allora esiste $v \in S$ tale che:

$$L(S) = L(S \setminus \{v\}).$$

Ma in tal caso $L(S \setminus \{v\})$ genererebbe ancora tutto V, pur avendo $|S \setminus \{v\}| = n - 1 < n = \dim V$, il che è impossibile per la definizione stessa di dimensione (nessun insieme di meno di n vettori può generare V). Dunque S deve essere linearmente indipendente.

($\Leftarrow$) Supponiamo ora per assurdo che S sia linearmente indipendente ma non generi V, cioè:

$$L(S) \subsetneq V.$$

Allora esiste $u \in V \setminus L(S)$. Consideriamo quindi l'insieme $S' = S \cup \{u\}$.
Poiché $u \notin L(S)$, il nuovo insieme S' risulta ancora linearmente indipendente. Tuttavia:

$$|S'| = n + 1,$$

il che è impossibile per il **Lemma di Steinitz**, che vieta l'esistenza di un insieme linearmente indipendente con più di n elementi in uno spazio vettoriale di dimensione n.

Quindi $L(S) = V$ e S è un sistema di generatori. $\square$

Teorema (Di completamento in una base)

Sia V uno spazio vettoriale su K con $\dim V = n$. Sia $X = \{v_1, \dots, v_t\} \subseteq V$ un insieme linearmente indipendente. Allora esiste un sottoinsieme $Y = \{v_{t+1}, \dots, v_n\} \subseteq V$ tale che $B := X \cup Y$ è una base di V.

Dimostrazione. Se $t = n$, allora X ha già n vettori linearmente indipendenti. Poiché la dimensione di V è n, ogni insieme di n vettori linearmente indipendenti è una base di V. Quindi in questo caso possiamo prendere $Y = \varnothing$ e $B = X$.

Supponiamo ora $t < n$. Allora X non può generare tutto V, cioè $L(X) \neq V$. Infatti se $L(X) = V$ avremmo che X è un sistema di generatori con t elementi e quindi $\dim V \leq t$, contraddicendo $t < n$. Quindi esiste almeno un vettore $v_{t+1} \in V \setminus L(X)$.

Per la proposizione già vista, poiché $v_{t+1} \notin L(X)$, l'insieme

$$X_1 := X \cup \{v_{t+1}\} = \{v_1, \dots, v_t, v_{t+1}\}$$

è ancora linearmente indipendente. Se $|X_1| = t+1 = n$ abbiamo finito: $B = X_1$ è una base. Altrimenti $t+1 < n$ e ripetiamo lo stesso ragionamento.

In generale, costruiamo per induzione una successione di insiemi linearmente indipendenti

$$X = X_0 \subset X_1 \subset X_2 \subset \cdots$$

in cui $X_{k+1} = X_k \cup \{v_{t+k+1}\}$ con $v_{t+k+1} \in V \setminus L(X_k)$. Ad ogni passo il numero di vettori aumenta di 1. Poiché $\dim V = n$, non è possibile continuare indefinitamente: non esistono insiemi di più di n vettori linearmente indipendenti in V. Quindi il processo termina dopo al più $n - t$ passaggi, producendo un insieme

$$B = X_m = \{v_1, \dots, v_t, v_{t+1}, \dots, v_{t+m}\}$$

con $|B| = n$ e B linearmente indipendente.

Un insieme di n vettori linearmente indipendenti in uno spazio di dimensione n genera V, dunque $L(B) = V$ e quindi B è una base di V. Ponendo $Y = \{v_{t+1}, \dots, v_n\}$ otteniamo la conclusione voluta. $\square$

Osservazioni:

- Sia V uno spazio vettoriale su K e siano $S, T \subseteq V$. Allora

$$L(S) = L(T) \iff S \subseteq L(T) \text{ e } T \subseteq L(S).$$

  (⇒) Poiché $S \subseteq L(S)$ e $L(S) = L(T)$, si ha $S \subseteq L(T)$; analogamente $T \subseteq L(S)$.
  (⇐) Se $S \subseteq L(T)$ allora $L(S) \subseteq L(T)$ (perché $L(T)$ è un sottospazio che contiene S); analogamente $T \subseteq L(S)$ implica $L(T) \subseteq L(S)$. Da entrambe le inclusioni segue $L(S) = L(T)$.

  Da questa osservazione segue la seguente proprietà sulle righe di matrici: se $A \in M_{m,n}(K)$ e B è ottenuta da A mediante un numero finito di operazioni elementari, allora indicando con $\bar{a^1}, \dots, \bar{a^m}$ le righe di A e con $\bar{b^1}, \dots, \bar{b^m}$ le righe di B, si ha

$$\{\bar{b^1}, \dots, \bar{b^m}\} \subseteq L(\bar{a^1}, \dots, \bar{a^m}) \quad \text{e} \quad \{\bar{a^1}, \dots, \bar{a^m}\} \subseteq L(\bar{b^1}, \dots, \bar{b^m}),$$

  da cui segue

$$L(\bar{b^1}, \dots, \bar{b^m}) = L(\bar{a^1}, \dots, \bar{a^m}).$$

- Per vettori $u, v, w \in V$ (con V uno spazio vettoriale) valgono le seguenti equivalenze geometriche:
  - u, v sono linearmente dipendenti $\iff$ u e v sono paralleli (cioè uno è multiplo scalare dell'altro);
  - u, v, w sono linearmente dipendenti $\iff$ u, v, w sono complanari (cioè esiste un piano che contiene i tre vettori).

Definizione (Rango di una matrice)
$A \in M_{mn}(K)$. Il rango di A è la dimensione dello spazio vettoriale generato dalle sue righe e dallo spazio vettoriale generato dalle sue colonne.