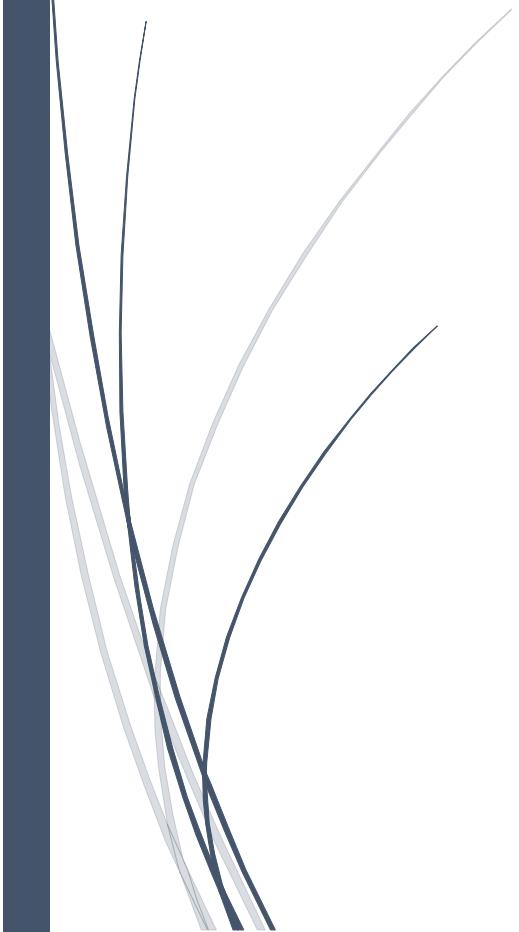




Appunti di algebra e matematica discreta



Rovesti Gabriel

Sommario

Numeri complessi	2
MCD ed MCM, Algoritmo di Euclide, Identità di Bezout, Congruenze	4
Classi di congruenza, Teorema cinese dei resti.....	12
Grafi orientati e non orientati, tipi, arcoconnettività, tagli, Kruskal, Dijkstra	25
Vettori e norme.....	51
Matrici e tipi	54
Operazioni tra matrici.....	61
Eliminazione di Gauss (MEG) e decomposizione LU.....	65
Determinanti e matrici inverse	75
Spazi e sottospazi vettoriali, tipi, combinazioni lineari.....	90
Sistemi di generatori, basi, applicazioni lineari	102
Basi ortogonali, ortonormali, autovalori, autovettori, diagonalizzazione	120
Metodi di conteggio, permutazioni, combinazioni, distribuzioni e relazioni di ricorrenza	132

Numeri complessi

L'equazione $x^2 + 1 = 0$ ha soluzione in un certo insieme numerico solo se esso contiene un numero il cui quadrato vale -1 . Chiamiamo questo "numero" **unità immaginaria** e lo denotiamo con i . Per definizione si ha quindi

$$i^2 = -1.$$

A partire dall'unità immaginaria si costruiscono i numeri complessi nel modo seguente.

Definizione 14.1 Si dice **numero complesso** ogni scrittura della forma $a + ib$, con a, b numeri reali e i unità immaginaria. L'insieme dei numeri complessi si denota con \mathbb{C} e si ha:

$$\mathbb{C} = \{a + ib \text{ tali che } a, b \in \mathbb{R} \text{ e } i^2 = -1\}.$$

Di solito, i numeri complessi si indicano con le ultime lettere dell'alfabeto: z, w, \dots

Dato il numero complesso $z = a + ib$, i numeri reali a e b si dicono rispettivamente **parte reale** e **parte immaginaria** di z e si scrive: $a = \operatorname{Re}(z)$, $b = \operatorname{Im}(z)$.

Esempi 14.2

- $z = 1 - 2i$ è un numero complesso con parte reale 1 e parte immaginaria -2 .
- $z = -\sqrt{2} + 0i = -\sqrt{2}$ è un numero complesso con parte reale $-\sqrt{2}$ e parte immaginaria 0.
- $z = 0 + 4i = 4i$ è un numero complesso con parte reale 0 e parte immaginaria 4.

Due numeri complessi $z = a + ib$ e $w = c + id$ si dicono **uguali** se hanno la stessa parte reale e la stessa parte immaginaria:

$$z = w \iff a = c \text{ e } b = d.$$

Nell'insieme \mathbb{C} dei numeri complessi si definiscono inoltre le seguenti operazioni:

► **Somma di due numeri complessi** $z = a + ib$ e $w = c + id$ è il numero complesso

$$z + w = (a + c) + i(b + d);$$

► **Prodotto di due numeri complessi** $z = a + ib$ e $w = c + id$ è il numero complesso

$$z \cdot w = (ac - bd) + i(ad + bc).$$

Per la somma e il prodotto appena definiti valgono le usuali proprietà delle operazioni (commutativa, associativa, distributiva). Inoltre:

- il numero complesso $0 = 0 + i0$ è tale che $z + 0 = z$ per ogni z ;
- il numero complesso $1 = 1 + i0$ è tale che $z \cdot 1 = z$ per ogni z ;
- il numero complesso $-z = -a - ib$ è l'**opposto** di $z = a + ib$;
- se $z \neq 0$, il numero complesso

$$\frac{1}{z} = \frac{a}{a^2 + b^2} - i \cdot \frac{b}{a^2 + b^2}$$

è il **reciproco** di $z = a + ib$. (Ovviamente si ha $z \cdot \frac{1}{z} = 1$ per ogni $z \neq 0$.)

È noto che numeri reali sono in corrispondenza biunivoca con i punti della retta euclidea.

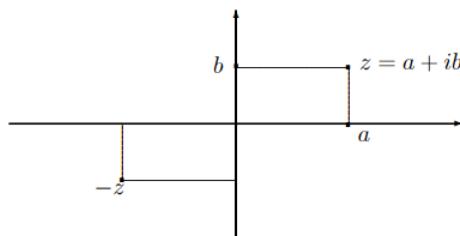
Analogamente, associando al numero della forma $z = a + ib$ il punto di coordinate (a, b) , si realizza una corrispondenza biunivoca tra i numeri complessi e i punti del piano cartesiano (detto in questo contesto **piano di Argand-Gauss**).

In tale corrispondenza: $a = \operatorname{Re}(z)$ è l'ascissa di (a, b) e $b = \operatorname{Im}(z)$ è l'ordinata di (a, b) .

I numeri della forma $a + 0i$, (che sono di fatto numeri reali) corrispondono ai punti dell'asse delle ascisse che verrà perciò detto **asse reale**, evidenziando che si ha $\mathbb{R} \subset \mathbb{C}$.

I numeri della forma $0 + ib = ib$, (detti **immaginari puri**) corrispondono ai punti dell'asse delle ordinate che verrà perciò detto **asse immaginario**.

L'opposto di z , ossia il numero $-z = -a - ib$ corrisponde al punto $(-a, -b)$ simmetrico di (a, b) rispetto all'origine.



Definizione 14.5 Dato il numero $z = a + ib$ si chiama

► **Coniugato** di z il numero complesso

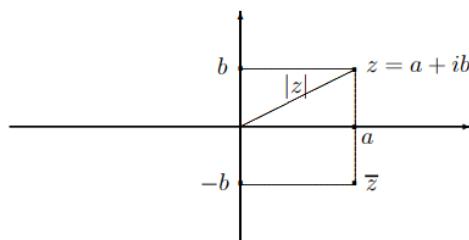
$$\bar{z} = a - ib.$$

Esso corrisponde al punto $(a, -b)$ simmetrico di (a, b) rispetto all'asse reale.

► **Modulo** di z il numero

$$|z| = \sqrt{a^2 + b^2}$$

che rappresenta la distanza del punto (a, b) dall'origine ed è quindi un numero reale maggiore o uguale a zero.



Teorema fondamentale dell'algebra Ogni polinomio (a coefficienti complessi) di grado n ha, nel campo complesso, esattamente n radici (pur di contarle con la loro molteplicità).

Da questo teorema si deduce che:

- Ogni polinomio a coefficienti complessi di grado n si può scrivere come prodotto di n polinomi a coefficienti complessi di primo grado.
- Ogni polinomio a coefficienti reali di grado dispari ha almeno una radice reale.
- Le eventuali radici complesse di un polinomio a coefficienti reali sono a due a due complesse coniugate e quindi un polinomio a coefficienti reali si può scrivere come prodotto di un opportuno numero di polinomi a coefficienti reali di grado non superiore a 2.

MCD ed MCM, Algoritmo di Euclide, Identità di Bezout, Congruenze

La divisione in N può essere descritta come:

- Siamo $a, b \in N$, con $b \neq 0$. Allora esistono e sono unici due numeri naturali q detto *quoziente* ed r detto *resto*.

Abbiamo quindi: $a = b * q + r$, $0 \leq r < b$

La divisione in Z può essere descritta come:

- Siamo $a, b \in Z$, con $b \neq 0$. Allora esistono e sono unici due numeri naturali q detto *quoziente* ed r detto *resto*.

Descriviamo quindi: $a = b * q + r$, $0 \leq r < b$

Analogamente possiamo descrivere:

- la divisibilità in N , descrivendo che b divide a se $a = bq$ per un opportuno $q \in N$.
 - Se b divide a , si scrive $b | a$
 - Se b non divide a , si scrive $b \nmid a$
- la divisibilità in Z , descrivendo che b divide a se $a = bq$ per un opportuno $q \in Z$.
 - Se b divide a , si scrive $b | a$
 - Se b non divide a , si scrive $b \nmid a$

Descriviamo inoltre il Massimo Comune Divisore (M.C.D.) è il più alto numero intero d divisore di due interi a e b diversi da zero. Si indica con $MCD(a, b)$ oppure semplicemente (a, b) .

Dati due interi a e b dell'insieme Z , un elemento d di Z si dice massimo comune divisore di a e b , se

- L'intero d è un divisore di a e b .
- Se esiste un altro intero c divisore di a e b , allora c divide anche d

$$\forall c \in Z : c | a \wedge c | b \rightarrow c | d$$

IN N Siano $a, b \in N$ NON ENTRAMBI NULLI.

Si dice che $d \in N$ è UN massimo comune divisore

d' a e b se

1) $d | a$ e $d | b$

$$\begin{array}{r} 12 \\ 6 \\ 3 \end{array} \mid \begin{array}{r} 2 \\ 2 \\ 3 \end{array} \quad \begin{array}{r} 18 \\ 9 \\ 3 \end{array} \mid \begin{array}{r} 2 \\ 3 \\ 3 \end{array}$$

2) se $z | a$ e $z | b$ allora $z | d$
(con $z \in N$)

$$12 = 2^2 \cdot 3 \quad 18 = 2 \cdot 3^2 \\ 2 \cdot 3 = 6$$

(ora se d è un divisore comune di a e b che è multiplo

d' ogni altro $\Rightarrow \exists z \in N$ tali che $d = z \cdot d'$)

ESEMPIO

$$6 = MCD(12, 18)$$

NB IN N d ESISTE ED È UNICO, dico IL massimo comune
divisore d' a e b

$$d = MCD(a, b)$$

IN \mathbb{Z} Sono $a, b \in \mathbb{Z}$ **NON ENTRA NEI NULLI**. Si dice

che $d \in \mathbb{Z}$ è UN massimo comune divisore d' a e b se

1) $d | a$ e $d | b$

2) se $z | a$ e $z | b$ allora $z | d$

se d è UN massimo comune divisore d' a e b ($\in \mathbb{Z}$)

si scrive $d = \text{MCD}(a, b)$

NB1 in \mathbb{Z} "il" massimo comune divisore è individuato

a meno del segno ($\because d = \text{MCD}(a, b)$ anche $-d = \text{MCD}(a, b)$)

NB2 se $a, b \in \mathbb{Z}$ con $b \neq 0$,

$$a = bq + r$$

$q, r \in \mathbb{Z}$ tali che $0 \leq r < |b|$

Allora $\text{MCD}(a, b) = \text{MCD}(b, r)$

L'algoritmo di Euclide è un metodo antico ed efficiente per trovare il massimo comune divisore (MCD) di due numeri interi positivi. L'algoritmo è stato introdotto da Euclide, un matematico greco, nel suo libro "Gli Elementi" intorno al 300 a.C. L'algoritmo di Euclide sfrutta la proprietà che il MCD di due numeri non cambia se sottraiamo il numero più piccolo dal numero più grande.

Ecco come funziona l'algoritmo di Euclide per trovare il MCD di due numeri a e b :

Inizio: Prendi i due numeri a e b .

Dividi: Dividi a per b e ottieni il quoziente q e il resto r , cioè $a = bq + r$.

Resto non nullo: Se r è uguale a zero, allora b è il MCD dei numeri originali a e b , quindi puoi terminare l'algoritmo.

Scambio: Se r non è zero, scambia a con b e b con r , quindi torna al passo 2.

L'algoritmo prosegue ripetendo i passaggi 2, 3 e 4 fino a quando il resto r diventa zero. A quel punto, il MCD si trova in b .

L'algoritmo di Euclide è noto per essere molto efficiente e richiede solo un numero limitato di passaggi per trovare il MCD. Questa proprietà lo rende adatto per essere implementato manualmente o in algoritmi informatici.

1^o PASSAGGIO si divide a per b : $\exists q_1, r_1 \in \mathbb{N}$ tali che

$$a = b \cdot q_1 + r_1 \quad \text{con} \quad 0 \leq r_1 < b$$

$$\text{MCD}(a, b) = \text{MCD}(b, r_1)$$

SE $r_1 = 0$

$$\text{allora } \text{MCD}(b, r_1) = \text{MCD}(b, 0) = b$$

L'ALGORITMO SI FERMA: $\text{MCD}(a, b) = b$

SE $r_1 \neq 0$

l'algoritmo continua ...

ESEMPIO

$$\text{MCD}(36, 12)$$

$a \uparrow$ $\uparrow b$

$$36 = 12 \cdot 3 + 0 \quad r_1 = 0 \Rightarrow b | a \Rightarrow \text{MCD}(a, b) = b$$

$\text{MCD}(36, 12) = 12$

ESEMPIO

$$\text{MCD}(42, 12)$$

$a \uparrow$ $\uparrow b$

$$42 = 12 \cdot 3 + 6 \quad r_1 \neq 0 \Rightarrow \text{CONTINUO}$$

$a \uparrow$ $\uparrow b$ $\uparrow q_1$ $\uparrow r_1$

2^o PASSAGGIO SE $r_1 \neq 0$ si divide b per r_1 : $\exists q_2, r_2 \in \mathbb{N}$

tali che $b = r_1 \cdot q_2 + r_2$ con $0 \leq r_2 < r_1$

$$\text{MCD}(b, r_1) = \text{MCD}(r_1, r_2)$$

SE $r_2 = 0$

$$\text{allora } \text{MCD}(r_1, r_2) = \text{MCD}(r_1, 0) = r_1$$

$$\text{MCD}(b, r_1) = \text{MCD}(a, b)$$

SE $r_2 \neq 0$

l'algoritmo continua

ESEMPIO

$$\text{MCD}(42, 12)$$

1^o PASSAGGIO

$$42 = 12 \cdot 3 + 6 \quad r_1 \neq 0 \Rightarrow \text{continuo}$$

$a \uparrow$ $\uparrow b$ $\uparrow q_1$ $\uparrow r_1$

2^o PASSAGGIO

$$12 = 6 \cdot 2 + 0 \quad \begin{cases} r_2 = 0 \\ r_1 \neq 0 \end{cases} \Rightarrow \text{MCD}(42, 12)$$

$b \uparrow$ $\uparrow r_1$ $\uparrow q_2$ $\uparrow r_2$

$6''$

Il massimo comun divisore sarà questo l'ultimo resto non nullo della sequenza di divisioni successive.

Parliamo quindi dei polinomi, descrivendo $S[x]$ come insieme dei polinomi nella indeterminata x ed a coefficienti in S ; tale $S \in \{Z, Q, R, C\}$.

$$f(x) \in S[x] \text{ se } f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m$$

dove $a_0, a_1, a_2, \dots, a_m \in S$

\nearrow
i coefficienti di $f(x)$

SE $a_n \neq 0$ allora il grado di $f(x)$ è $m = \deg f(x)$,
e $a_m =$ il coefficiente direttore di $f(x)$
e $a_0 =$ il termine noto di $f(x)$

SOMMA DI POLINOMI

$\forall f(x), g(x) \in S[x]$ definisco $f(x) + g(x) \in S[x]$

nel seguente modo:

$$f(x) = a_0 + a_1 x + \dots + a_m x^m \quad \sum_{i=0}^m a_i x^i \quad (a_n \neq 0)$$

$$g(x) = b_0 + b_1 x + \dots + b_m x^m \quad \sum_{i=0}^m b_i x^i \quad (b_m \neq 0)$$

$$\Rightarrow \sum_{i=0}^m a_i x^i + \sum_{i=0}^m b_i x^i$$

PRODOTTO DI POLINOMI

$\forall f(x), g(x) \in S[x]$ definisco $f(x) \cdot g(x) \in S[x]$

nel seguente modo:

$$\text{se } f(x) = \sum_{j=0}^n a_j x^j \quad e \quad g(x) = \sum_{j=0}^m b_j x^j$$

$a_n \neq 0 \quad b_m \neq 0$

allora

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n) \cdot (b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m) \\ &= a_0 \cdot b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \dots \\ &= \sum_{j=0}^{n+m} \left(\sum_{k=0}^j a_k b_{j-k} \right) x^j \end{aligned}$$

In generale, nell'insieme S (ed evidenti insiemi contenuti), vale la legge di cancellazione del prodotto.

La divisione tra polinomi è un'operazione che consente di dividere un polinomio (dividendo) per un altro polinomio (divisore). Il risultato è composto da due parti: il quoziente e il resto. Formalmente, la divisione tra polinomi può essere espressa come segue:

Dati due polinomi:

- Dividendo: $D(x)$ con coefficienti $d_n, d_{n-1}, \dots, d_1, d_0$, dove n è il grado di $D(x)$.
- Divisore: $d(x)$ con coefficienti $d_m, d_{m-1}, \dots, d_1, d_0$, dove m è il grado di $d(x)$ e $m \leq n$.

L'obiettivo è ottenere un quoziente $q(x)$ e un resto $r(x)$ tali che:

$$D(x) = q(x) \cdot d(x) + r(x)$$

dove il grado di $r(x)$ è minore del grado di $d(x)$.

L'algoritmo di divisione tra polinomi procede nel seguente modo:

1. **Inizializzazione:** Si parte con il polinomio dividendo $D(x)$ e si cerca di portare il termine di grado più alto di $D(x)$ allo stesso grado del termine di grado più alto di $d(x)$. Si ottiene un termine $q_1(x)$ che è il termine principale del quoziente.
2. **Moltiplicazione e Sottrazione:** Si moltiplica il polinomio divisor $d(x)$ per $q_1(x)$ e si sottrae il risultato ottenuto da $D(x)$. Questo genera un nuovo polinomio $D_1(x)$ di grado inferiore rispetto a $D(x)$.
3. **Ripeti:** Si ripete il processo con $D_1(x)$, cercando di portare il termine di grado più alto di $D_1(x)$ allo stesso grado del termine di grado più alto di $d(x)$. Si ottiene un nuovo termine $q_2(x)$ che si aggiunge al quoziente.
4. **Moltiplicazione e Sottrazione (di nuovo):** Si moltiplica $d(x)$ per $q_2(x)$ e si sottrae il risultato da $D_1(x)$, ottenendo un nuovo $D_2(x)$.
5. **Ripeti il processo:** Si ripete questo processo finché il grado del nuovo $D_i(x)$ è ancora maggiore o uguale al grado di $d(x)$.

Alla fine del processo, il polinomio $D_i(x)$ ottenuto è il resto $r(x)$, e i polinomi $q_1(x), q_2(x), \dots$ sono i vari termini del quoziente $q(x)$.

$$S \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$$

$\begin{array}{l} \text{N.B } S \neq \mathbb{Z} \\ \mathbb{Z}[x] \ni f(x) = x \\ \mathbb{Z}[x] \ni g(x) = 2x \\ \quad \quad \quad \text{sono e'} \\ \quad \quad \quad \text{nel } \mathbb{Z}[x] \end{array}$

$$\forall f(x), g(x) \in S[x] \quad \boxed{\text{con } g(x) \neq 0} \quad \text{esistono } \in$$

Sono UNICI $q(x) \in S[x]$ e $r(x) \in S[x]$ tali che

$\overset{\rightarrow}{\text{QUOTIENTE}} \quad \overset{\uparrow}{\text{RESTO}}$

$$f(x) = g(x) \cdot q(x) + r(x) \quad \boxed{\text{con } \deg r(x) < \deg g(x)}$$

Le radici di un polinomio sono i valori delle variabili che, quando sostituiti nelle equazioni del polinomio, rendono il polinomio uguale a zero. In altre parole, una radice r di un polinomio $P(x)$ è un valore tale che $P(r) = 0$. Le radici sono anche chiamate soluzioni dell'equazione polinomiale $P(x) = 0$.

Ad esempio, nel caso del polinomio $P(x) = x^2 - 3x + 2$, le sue radici sono $x = 1$ e $x = 2$, poiché sostituendo questi valori nel polinomio otteniamo $P(1) = 0$ e $P(2) = 0$.

TEOREMA DI RUFFINI

Sia $f(x) \in S[x]$ ed $x_0 \in S$

$$x_0 \text{ è una radice di } f(x) \Leftrightarrow \begin{array}{l} x-x_0 \mid f(x) \\ \uparrow \\ \text{divide} \end{array} \Leftrightarrow \exists q(x) \in S[x] \text{ tale che } f(x) = (x-x_0)q(x)$$

RADICI DI POLINOMI REALI DI 2° GRADO

$a, b, c \in \mathbb{R}$ le soluzioni dell'equazione di 2° grado
 $a \neq 0$

$$ax^2 + bx + c = 0 \quad \text{sono...}$$

$$\Delta = b^2 - 4ac \quad (\text{il discriminante})$$

- se $\Delta > 0$ ha 2 soluzioni reali distinte:

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad \text{e} \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a}$$

- se $\Delta = 0$ ha 1 soluzione reale "contata 2 volte"

$$x_1 = x_2 = -\frac{b}{2a}$$

- se $\Delta < 0$ l'equazione non ha soluzioni reali

$$x_1 = \frac{-b + i\sqrt{-\Delta}}{2a} \quad x_2 = \frac{-b - i\sqrt{-\Delta}}{2a}$$

ha le 2 soluzioni complesse coniugate

$$\text{NB} \quad x_2 = \overline{x_1} \quad , \quad x_1 = \overline{x_2} \quad \text{radici di } f(x)$$

$$\text{NB} \quad \left. \begin{aligned} f(x) &= ax^2 + bx + c \\ a, b, c &\in \mathbb{R} \\ a &\neq 0 \end{aligned} \right\} \Rightarrow \exists x_1, x_2 \in \mathbb{C} \quad \begin{cases} \text{tali che} \\ \begin{cases} f(x_1) = 0 \\ f(x_2) = 0 \end{cases} \end{cases}$$

L'algoritmo di Euclide ci permette, una volta individuato $d = \text{MCD}(a, b)$, di trovare due numeri interi s, t tali che

$$d = s * a + t * b$$

questa relazione si chiama **IDENTITA' DI BEZOUT**.

$$\forall a, b \in \mathbb{Z} \text{ t.c. } (a, b) \neq (0, 0)$$

posto $d = \text{MCD}(a, b)$, $\exists m, n \in \mathbb{Z}$

TALI CHE

$$d = ma + nb$$

Per trovarli:

1^o modo applico Euclide in \mathbb{Z} e lo ripercorro
all'inverso trovando m, n

2^o modo $|a|, |b| \in \mathbb{N}$ $d = \text{MCD}(|a|, |b|)$

applico Euclide in \mathbb{N} e ripercorrendolo
all'inverso trovo $m^*, n^* \in \mathbb{N}$ t.c.

$$d = m^* |a| + n^* |b|$$

E poi "EVENTUALMENTE" CAMBIO i segni a m^* e n^*

$$\begin{aligned} a &= -36 \\ b &= 28 \end{aligned}$$

TROVARE $m, n \in \mathbb{Z}$ tali che

$$4 = d = m \cdot (-36) + n \cdot 28$$

dove $d = \text{MCD}(-36, 28)$

1^o modo

$$\begin{aligned} -36 &= 28 \cdot (-2) + 20 \Rightarrow 20 = -36 + 2 \cdot 28 \\ a &\uparrow \quad b \uparrow \quad q_1 \quad r_1 \\ m &\uparrow \quad n \uparrow \quad q_2 \quad r_2 \\ 28 &= 20 \cdot 1 + 8 \Rightarrow 8 = 28 + 20 \cdot (-1) \\ b &\uparrow \quad r_1 \uparrow \quad q_2 \quad r_2 \\ 20 &= 8 \cdot 2 + 4 \Rightarrow 4 = 20 + 8 \cdot (-2) \\ r_2 \uparrow &\quad q_3 \uparrow \quad r_3 \\ 8 &= 4 \cdot 2 + 0 \end{aligned}$$

$\begin{array}{rcl} \Rightarrow 3 \cdot [-36 + 2 \cdot 28] + (-2) \cdot 28 &=& a \\ = 3 \cdot (-36) + 4 \cdot 28 &=& b \\ = 4 &=& d \end{array}$

$$\begin{array}{l} a = -36 \\ b = 28 \end{array}$$

20 minuti $|a| = |-36| = 36$
 $|b| = |28| = 28$

esso $m^*, n^* \in \mathbb{Z}$ t.c.

$$d = a \frac{(-36)}{3} m + b \frac{28}{4} n \quad \text{c.c.m.m.c.} \in \mathbb{Z}$$

$$d = \text{MCD}(|a|, |b|)$$

$$= \text{MCD}(a, b)$$

$$d = |a|m^* + |b|n^*$$

$$36 = 28 \cdot 1 + 8 \Rightarrow 8 = 36 + 28 \cdot (-1)$$

$$28 = 8 \cdot 3 + 4 \Rightarrow 4 = 28 + 8 \cdot (-3) =$$

$$8 = 4 \cdot 2 + 0 \quad 4 = 4 \cdot 28 + (-3) \cdot 36$$

$$= 28 + (-3)[36 + 28 \cdot (-1)] =$$

$$= 28 + (-3) \cdot 36 + 3 \cdot 28$$

Classi di congruenza, Teorema cinese dei resti

Definizione. Se a è un intero, la *classe di congruenza* di a modulo m è definita come

$$[a]_m = \{ x \in \mathbf{Z} / x \equiv a \pmod{m} \} = \{ x \in \mathbf{Z} / x = a + km, \text{ con } k \in \mathbf{Z} \},$$

cioè è l'insieme di tutti gli interi che sono congrui ad a modulo m .

NB 1

$$a \equiv b \pmod{m} \Leftrightarrow \begin{cases} \text{IL RESTO DELLA DIVISIONE} \\ \text{DI } a \text{ PER } m \\ // \\ \text{IL RESTO DELLA DIVISIONE} \\ \text{DI } b \text{ PER } m \end{cases}$$

NB 2 Fissato $m \in \mathbf{N}, m > 0$ gode delle seguenti proprietà:

1 È RIFLESSIVA: $a \equiv a \pmod{m}$ (perché $m | (a-a) = 0$)

2 È SIMMETRICA: $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (perché se $m | (a-b)$ allora $m | (b-a)$)

3 È TRANSITIVA:

$$\begin{aligned} m | a-b &\Leftrightarrow a \equiv b \pmod{m} \\ m | b-c &\Leftrightarrow b \equiv c \pmod{m} \end{aligned} \quad \left. \begin{array}{l} \Rightarrow a \equiv c \pmod{m} \\ m | a-c = (a-b) + (b-c) \end{array} \right.$$

4 Le congruenze mod m si possono sommare

$$\begin{cases} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{cases} \Rightarrow (a_1 + a_2) \equiv (b_1 + b_2) \pmod{m}$$

5 Le congruenze mod m si possono moltiplicare

$$\begin{cases} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{cases} \Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$$

Le relazioni che siano:

- Riflessive
- Simmetriche
- Transitive

sono definite relazioni di equivalenza.

Sia R una relazione binaria definita su un insieme A .

1. **Riflessività:** Ogni elemento a dell'insieme è in relazione con se stesso, cioè $(a, a) \in R$.
2. **Simmetria:** Se due elementi a e b sono in relazione, allora b è in relazione con a , cioè se $(a, b) \in R$, allora $(b, a) \in R$.
3. **Transitività:** Se due elementi a e b sono in relazione e b e c sono in relazione, allora a e c sono in relazione, cioè se $(a, b) \in R$ e $(b, c) \in R$, allora $(a, c) \in R$.

Una relazione di equivalenza sull'insieme degli interi divide gli interi in classi di equivalenza; nel nostro caso la congruenza modulo un intero strettamente positivo m dividerà \mathbb{Z} in classi di congruenza (modulo m).

Similmente, esistono, dati $a \in \mathbb{Z}, n \in \mathbb{N}, n > 0$ la classe di congruenza di a modulo n e si indica $[a]_n$ oppure $[a] \text{ mod } n$. Possiamo descrivere $[a]_n$ come l'insieme di tutti i numeri interi che sono congrui ad a modulo n .

$$[a]_m = \begin{array}{l} \text{insieme di tutti numeri interi che} \\ \text{sono congrui ad } a \text{ modulo } m \\ = \{ b \in \mathbb{Z} \mid b \equiv a \pmod{m} \} \end{array}$$

Possiamo quindi descrivere:

$$\mathbb{Z}_m = \{ [0]_m, [1]_m, [2]_m, \dots, [m-1]_m \} = \underline{\text{l'insieme}} \\ \underline{\text{degli interi modulo } m}$$

In essa definisco una somma e un prodotto; la definizione della somma in \mathbb{Z}_n non dipende dalla scelta dei rappresentanti delle classi (i rappresentanti sono elementi scelti all'interno di ciascuna classe per rappresentare l'intera classe. Ogni classe di equivalenza ha uno o più rappresentanti, che condividono la stessa proprietà che definisce l'equivalenza tra gli elementi della classe).

Nel contesto delle classi di congruenza modulo n , i rappresentanti sono spesso scelti tra gli interi nell'intervallo $[0, n-1]$ per semplificare i calcoli e l'analisi)-

Importante ricordare:

$$\mathbb{Z}_m, +, \cdot$$

$$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$$

TAVOLE DI ADDIZIONE E DI MULTIPLICAZIONE

+	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

\cdot	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

$$[1]_2 + [1]_2 = [1+1]_2 = [2]_2 = [0]_2$$

$$\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$$

+	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$$[5]_4 = [1]_4 \quad [6]_4 = [2]_4$$

$$\begin{aligned} [6]_4 &= [2]_4 \\ [8]_4 &= [0]_4 \end{aligned}$$

\cdot	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[1]_4$	$[2]_4$

$$\begin{aligned} [2]_4 \cdot [2]_4 &= [0]_4 \\ \text{NON VALE} \\ \text{LA LEGGE DI} \\ \text{CANCELLAZIONE} \end{aligned}$$

Definiamo quindi le congruenze, descrivendo:

- Le congruenze lineari modulo n , espressioni del tipo $ax \equiv b \pmod{n}$, con $a, b \in \mathbb{Z}$

$x_0 \in \mathbb{Z}$ è una soluzione d' (K) se $ax_0 \equiv b \pmod{n}$
oppure se $\exists k \in \mathbb{Z}$ tale che $ax_0 = b + nk$

Non tutte le congruenze hanno soluzioni:

Esempio $2x \equiv 3 \pmod{4}$ non ha soluzioni :

Se esistesse $x_0 \in \mathbb{Z}$ t.c. $2x_0 \equiv 3 \pmod{4}$

$$\begin{aligned} \text{esisterebbe } k \in \mathbb{Z} \text{ t.c. } 2x_0 &= 3 + 4k \\ &\Rightarrow 3 = \underbrace{2(x_0 - 2k)}_{\text{DISPARI}} \underbrace{+ 4k}_{\text{PAIR}} \end{aligned}$$

Risolvere una congruenza significa:

- dire se ha o non ha soluzioni
- nel caso le abbia, trovarle tutte.

Come numeri interi sono infinite. Non tutte le equazioni lineari in Z_n hanno soluzioni e non tutte le equazioni lineari in Z_n che hanno soluzioni ne hanno una sola.

PROPOSIZIONE *Sia (*) $ax \equiv b \pmod{m}$*
con $m \in \mathbb{N}, m > 0, a, b \in \mathbb{Z}$

Supponiamo che () abbia soluzioni. Sia x_0 una soluzione.*

Allora TUTTI i NUMERI INTERI IN

$[x_0]_m = \{x_0 + tn \mid t \in \mathbb{Z}\}$ sono soluzioni di (*)

Enunciamo due teoremi importanti:

TEOREMA 1 (ESISTENZA DI SOLUZIONI DI UNA CONGRUENZA)

Siano $m \in \mathbb{N}, m > 0, a, b \in \mathbb{Z}$ e $d = \text{MCD}(a, m)$. Allora

$$[ax \equiv b \pmod{m} \text{ HA SOLUZIONI}] \iff d \mid b$$

TEOREMA 2 *Si suppone che $ax \equiv b \pmod{m}$ abbia soluzioni*

Sia $d = \text{MCD}(a, m)$ (dunque $d \mid b$)

SIA x_0 UNA SOLUZIONE DI $ax \equiv b \pmod{m}$.

Allora LE SOLUZIONI DI $ax \equiv b \pmod{m}$

Sono TUTTI E SOLO I NUMERI INTERI DEL TIPO:

$$x_k = x_0 + k \cdot \frac{m}{d} \quad \text{al variare di } k \in \mathbb{Z}.$$

Ci sono infatti numeri interi soluzioni di $ax \equiv b \pmod{m}$

E si ripartiscono in esattamente d

CLASSI DI CONGRUENZA MODULO m :

$$[x_0]_m = \{x_0 + tn \mid t \in \mathbb{Z}\}$$

$$[x_1]_m = \{x_1 + tn \mid t \in \mathbb{Z}\}$$

$$[x_2]_m = \{x_2 + tn \mid t \in \mathbb{Z}\}$$

\vdots

$$[x_{d-1}]_m = \{x_{d-1} + tn \mid t \in \mathbb{Z}\}$$

$$\text{NB: } [x_d]_m = [x_0 + d \cdot \frac{m}{d}]_m =$$

$$= [x_0 + m]_m = [x_0]_m$$

$$\text{E così: } [x_{d+1}]_m =$$

$$= [x_0 + (d+1) \cdot \frac{m}{d}]_m =$$

$$= [x_0 + d \cdot \frac{m}{d} + \frac{m}{d}]_m = [x_0 + m + \frac{m}{d}]_m =$$

$$= [x_1 + m]_m = [x_1]_m \quad \text{ECETERA}$$

Un elemento a in Z_n è invertibile (o ha un inverso) se esiste un altro elemento b in Z_n tale che il prodotto di a e b sia congruente a 1 modulo n . In altre parole, a è invertibile se esiste un b tale che $ab \equiv 1 \pmod{n}$.

In un contesto numerico, due numeri interi a e b si dicono "coprimi" (o "relativamente primi" o "primo fra loro") se il loro massimo comune divisore (MCD) è uguale a 1. In altre parole, due numeri sono coprimi se non hanno fattori primi in comune, oltre al fattore primo 1.

Formalmente, dati due numeri interi a e b , essi sono coprimi se:

$$MCD(a, b) = 1$$

Ad esempio, i numeri 15 e 28 sono coprimi poiché il loro MCD è 1, mentre i numeri 12 e 18 non sono coprimi poiché il loro MCD è 6.

In matematica, un "anello" è una struttura algebraica che combina due operazioni binarie, di solito chiamate "addizione" e "moltiplicazione", soddisfacendo una serie di proprietà.

Z_p rappresenta l'anello dei numeri interi modulo p , dove p è un numero primo positivo. In Z_p , gli elementi sono le classi di congruenza modulo p , cioè insiemi di numeri interi che sono congruenti tra loro modulo p . In altre parole, due numeri interi a e b appartengono alla stessa classe di congruenza modulo p se la loro differenza $a - b$ è un multiplo intero di p .

In Z_p tutti gli elementi $\neq [0]_p$ e sono esattamente $p - 1$.

La funzione di Eulero (φ di Euler) è una funzione aritmetica che associa a un numero intero positivo n il numero di interi positivi inferiori a n che sono coprimi con n . In altre parole, $\varphi(n)$ conta quanti numeri interi positivi minori di n sono relativamente primi a n .

Ad esempio, se $n = 8$, i numeri interi positivi minori di 8 che sono coprimi con 8 sono 1, 3, 5, 7, quindi $\varphi(8) = 4$.

La FUNZIONE DI EULERO φ li "conta":

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$

è definita da $\varphi(n) = \begin{cases} \text{il numero dei} \\ \text{naturali } k \text{ tali che} \\ 0 \leq k < n \\ \text{MCD}(k, n) = 1 \end{cases}$

Se p è un numero primo diverso $\varphi(p) = p - 1$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

dove p_1, \dots, p_m
sono numeri primi
DISTINTI,
 $\alpha_i \in \mathbb{N}$ $\alpha_i > 0$

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right)$$

Un sistema di congruenze è un insieme di equazioni di congruenza che coinvolgono una o più variabili intere e un modulo dato. L'obiettivo è trovare i valori delle variabili che soddisfano tutte le equazioni di congruenza contemporaneamente.

Un sistema di congruenze è solitamente espresso nella seguente forma:

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\\vdots \\x &\equiv a_n \pmod{m_n}\end{aligned}$$

Dove x è la variabile incognita che vogliamo trovare, a_1, a_2, \dots, a_n sono i resti delle divisioni e m_1, m_2, \dots, m_n sono i moduli rispettivi.

Risolvere il sistema significa:

- dire se ha soluzioni oppure no
- nel caso le abbia, trovarle tutte

Un $x_0 \in \mathbb{Z}$ è una soluzione del sistema se è contemporaneamente soluzione di ogni congruenza del sistema.

Valgono inoltre:

NB1 Se una congruenza del sistema non ha soluzioni, allora il sistema non ha soluzioni

NB2 Anche se tutte le congruenze del sistema hanno soluzioni, non è detto che il sistema abbia soluzioni

Il Teorema Cinese del Resto (CRT) è un risultato importante della teoria dei numeri e dell'aritmetica modulare che fornisce una soluzione per un sistema di congruenze lineari con moduli coprimi tra loro. Il teorema afferma che, se dati resti e moduli coprimi, è possibile trovare una soluzione che soddisfi tutte le congruenze contemporaneamente.

Siano m_1, m_2, \dots, m_n interi positivi coprimi a due a due e a_1, a_2, \dots, a_n interi qualsiasi.

Allora il sistema di congruenze

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\\vdots \\x &\equiv a_n \pmod{m_n}\end{aligned}$$

ha una soluzione x che è unica modulo $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$.

Il metodo di Newton per risolvere le congruenze quadratiche è una tecnica che mira a trovare soluzioni per le equazioni di congruenza quadratiche modulo un numero intero positivo n . Questo metodo è particolarmente utile quando si cerca una radice quadrata modulo n , cioè un numero intero x tale che $x^2 \equiv a \pmod{n}$, dove a è un residuo dato.

COMINCIAMO A STUDIARE IL CASO $K=2$

METODO DI
NEWTON

$$\begin{array}{l} A \rightarrow \left\{ \begin{array}{l} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{array} \right. \\ B \end{array} \quad \text{MCD}(m_1, m_2) = 1$$

I Chiamo $x_1 = b_1$ (è una particolare sol. di A)

II cerco $t_2 \in \mathbb{Z}$ tale che $x_1 + t_2 m_2 \stackrel{x_2}{=} \text{soluzione}$
fa soluzione di B

$$\text{cioè cerco } t_2 \in \mathbb{Z} \text{ t.c. } \begin{aligned} b_1 + t_2 m_2 &\equiv b_2 \pmod{m_2} \\ t_2 m_1 &\equiv (b_2 - b_1) \pmod{m_2} \end{aligned}$$

faccio i conti in \mathbb{Z}_{m_2}

III $x_2 \in$ UNA SOLUZIONE DI {A B}

IV Per il teorema cinese dei resti, le soluzioni del sistema sono esattamente tutti i numeri interi nelle classi

$$[x_2]_m = \{x_2 + km \mid k \in \mathbb{Z}\}$$

$$\text{dove } m = m_1 \cdot m_2$$

ESEMPIO

$$\left\{ \begin{array}{l} x \equiv 4 \pmod{6} \\ x \equiv 3 \pmod{5} \end{array} \right. \quad \begin{array}{l} b_1 = 4 \\ b_2 = 3 \end{array} \quad \begin{array}{l} m_1 = 6 \\ m_2 = 5 \end{array}$$

$\text{MCD}(m_1, m_2) = \text{MCD}(6, 5) = 1$ posso applicare il teorema cinese dei resti e concludere che il sistema ha infinite

soluzioni: tutti i numeri in $[x_2]_{30} = \{x_2 + 30k \mid k \in \mathbb{Z}\}$

$$m = m_1 \cdot m_2 = 6 \cdot 5 = 30 \quad \text{dove } x_2 \text{ è una particolare soluzione}$$

I $x_1 = 4$

II cerco $t_2 \in \mathbb{Z} \mid 4 + t_2 \cdot 6 \equiv 3 \pmod{5}$

$$[6]_5 = [1]_5 \quad 1 \rightarrow 6t_2 \equiv 3 - 4 \pmod{5} \quad [4]_5 = [-1]_5$$

$$t_2 \equiv 4 \pmod{5}$$

III ad esempio prendo $t_2 = 4$

$$\begin{aligned} x_2 &= x_1 + t_2 m_1 \\ &= 4 + 4 \cdot 6 \\ &= 4 + 24 \\ &= 28 \end{aligned}$$

IV le soluzioni del sistema sono:

$$[28]_{30} = \{ 28 + 30k \mid k \in \mathbb{Z} \}$$

IL CASO $k=3$

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ x \equiv b_3 \pmod{m_3} \end{cases}$$

CON L'IPOTESI:

$$\begin{array}{l} \text{MCD}(n_1, n_2) = 1 \\ \text{MCD}(n_1, n_3) = 1 \\ \text{MCD}(n_2, n_3) = 1 \end{array}$$

Trovate una soluzione x_3 del sistema, tutte le soluzioni

del sistema sono: $[x_3]_m = \{ x_3 + mk \mid k \in \mathbb{Z} \}$

$$M = M_1 \cdot M_2 \cdot M_3$$

PER TROVARE x_3 :

$$\begin{array}{l} A \rightarrow \left\{ \begin{array}{l} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{array} \right. \\ B \rightarrow \left\{ \begin{array}{l} x \equiv b_1 \pmod{n_1} \\ x \equiv b_3 \pmod{n_3} \end{array} \right. \\ C \rightarrow \left\{ \begin{array}{l} x \equiv b_2 \pmod{n_2} \\ x \equiv b_3 \pmod{n_3} \end{array} \right. \end{array}$$

I chiamo $x_1 = b_2$, ma sol. di A

II cerco $t_2 \in \mathbb{Z}$ tale che $x_1 + t_2 m_1 \stackrel{\text{def}}{=} x_2$ sia sol. di B
dunque

III x_2 è sol. d'  

IV cerco $t_3 \in \mathbb{Z}$ tale che $x_2 + t_3 (M_1 \cdot M_2) \stackrel{\text{def}}{=} x_3$
Sia soluzione d' C

V x_3 è UNA SOL. DEL SISTEMA



$$m = M_1 M_2 M_3$$

VI Le soluzioni del sistema sono $[x_3]_m = \{ x_3 + mk \mid k \in \mathbb{Z} \}$

Esempio

$$\begin{cases} A \rightarrow x \equiv 10 \pmod{11} \\ B \rightarrow x \equiv 5 \pmod{6} \\ C \rightarrow x \equiv 5 \pmod{7} \end{cases}$$

$$\text{MCD}(11,6)=1, \text{ MCD}(11,7)=1, \text{ MCD}(6,7)=1$$

$$\Rightarrow \exists \infty \text{ sol: tutti i numeri interi in } [x_3]_{462} = \{x_3 + 462k \mid k \in \mathbb{Z}\}$$

$$m = m_1 \cdot m_2 \cdot m_3 = 11 \cdot 6 \cdot 7 = 66 \cdot 7 = 462$$

I) $x_1 = 10$ una sol. di A

II) cerca $t_2 \in \mathbb{Z}$ | $x_1 + t_2 \cdot m_2 = x_2$ sia sol. di B
 $10 + t_2 \cdot 11 \equiv 5 \pmod{6}$

$$10 + t_2 \cdot 11 \equiv 5 \pmod{6}$$

$$11t_2 \equiv (5 - 10) \pmod{6}$$

$$11t_2 \equiv -5 \pmod{6}$$

$$5t_2 \equiv 1 \pmod{6}$$

$$6 = 5 \cdot 1 + 1 \Rightarrow 1 = 6 + 5(-1)$$

$$\begin{aligned} t_2 &= \alpha \cdot q \\ 1 = b = qd &\stackrel{q=1}{=} \frac{q}{d=1} \end{aligned} \quad \Rightarrow \quad t_2 = \alpha = -1$$

$$[11]_6 = [5]_6$$

$$[-5]_6 = [1]_6$$

$$d = \text{MCD}(a, n) = \text{MCD}(5, 6) = 1$$

$$1 = \alpha 5 + \beta 6$$

$$\begin{matrix} 1 \\ \downarrow \alpha \quad \uparrow \beta \\ 6 = 5 \cdot 1 + 1 \end{matrix}$$

$$\begin{aligned} t_2 &= 5 \\ x_2 &= x_1 + t_2 \cdot m_2 = 10 + 5 \cdot 11 = 10 + 55 = 65 \\ x_2 &= 65 \end{aligned}$$

III) cerca $t_3 \in \mathbb{Z}$ tale che

$$x_3 = x_2 + t_3(m_1 \cdot m_2) \text{ ha s.d. C: } x \equiv 5 \pmod{7}$$

$$x_2 + t_3(m_1 \cdot m_2) \equiv 5 \pmod{7}$$

$$65 + t_3(11 \cdot 6) \equiv 5 \pmod{7}$$

$$\begin{aligned} [66]_7 &= [3]_7 \\ [-60]_7 &= [3]_7 \end{aligned} \quad \begin{aligned} 3 \rightarrow 66t_3 &\equiv -60 \pmod{7} \\ 3t_3 &\equiv 3 \pmod{7} \end{aligned} \quad \begin{aligned} &\text{ad esempio} \\ &t_3 = 1 \end{aligned}$$

$$\begin{aligned}x_3 &= x_2 + t_3 \cdot m_1 \circ m_2 \\&= 65 + 1 \cdot 11 \cdot 6 \\&= 65 + 66 = 131\end{aligned}$$

IV $x_3 = 131$ è una soluzione sf. d' $\left\{ \begin{array}{l} A \quad 131 \equiv 10 \pmod{11} \\ B \quad 131 \equiv 5 \pmod{6} \\ C \quad 131 \equiv 5 \pmod{7} \end{array} \right.$

V Il insieme delle sf. del sistema è

$$\{ 131 + 462k \mid k \in \mathbb{Z} \}$$

Continuando con questo:

In generale se $k \geq 4$ e

$$\begin{cases} \textcircled{1} \rightarrow x \equiv b_1 \pmod{n_1} \\ \textcircled{2} \rightarrow x \equiv b_2 \pmod{n_2} \\ \vdots \\ \textcircled{k} \rightarrow x \equiv b_k \pmod{n_k} \end{cases} \text{ con } \text{MCD}(m_i, m_j) = 1 \quad \forall i \neq j$$

ITERO IL PROCEDIMENTO :

- $x_1 = b_1$ è una sf. d' $\textcircled{1}$
- suppongo che $x_1 + m_1 t_2 = x_2$ sia sf. d' $\textcircled{2}$
(c'è $t_2 \in \mathbb{Z}$ tale che ...) allora x_2 è sf. d' $\textcircled{1,2}$

◦ suppongo che $x_2 + m_1 m_2 t_3 = x_3$ sia soluz. d' $\textcircled{3}$
(c'è $t_3 \in \mathbb{Z}$ tale che ...) allora x_3 è sf. d' $\textcircled{1,2,3}$

◦ suppongo che $x_3 + m_1 m_2 m_3 t_4 = x_4$ sia soluz. d' $\textcircled{4}$
(c'è $t_4 \in \mathbb{Z}$ tale che ...) allora x_4 è sf. d' $\textcircled{1,2,3,4}$

al paragrafo K-tesimo ho x_K soluzione del sistema e tutte le sf. del sistema sono in $[x_K]_n$ dove $n = n_1 n_2 \dots n_K$

Il metodo di Lagrange per risolvere i sistemi di congruenze è una tecnica utilizzata per trovare soluzioni intere di un sistema di equazioni di congruenza lineari. Questo metodo sfrutta il Teorema Cinese del Resto (CRT) e consente di semplificare la risoluzione di un sistema complesso di congruenze suddividendolo in sistemi più semplici.

Supponiamo di avere il seguente sistema di congruenze:

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\&\vdots \\x &\equiv a_n \pmod{m_n}\end{aligned}$$

Dove m_1, m_2, \dots, m_n sono interi positivi coprimi a due a due e a_1, a_2, \dots, a_n sono gli resti corrispondenti. Il metodo di Lagrange procede nel seguente modo:

1. Calcolo dei Prodotti Parziali:

Calcola il prodotto $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$.

2. Calcolo delle Equazioni di Lagrange:

Per ciascun i , calcola il prodotto parziale $M_i = \frac{M}{m_i}$ e trova l'inverso moltiplicativo M_i^{-1} di M_i modulo m_i . Quindi, calcola $y_i = M_i \cdot M_i^{-1} \pmod{m_i}$.

3. Calcolo della Soluzione:

La soluzione x del sistema di congruenze è data da:

$$x = a_1 \cdot y_1 + a_2 \cdot y_2 + \dots + a_n \cdot y_n \pmod{M}$$

Il metodo di Lagrange sfrutta il fatto che y_i annulla tutti i termini tranne $a_i \cdot y_i$ nella formula di x . Pertanto, la somma $a_1 \cdot y_1 + a_2 \cdot y_2 + \dots + a_n \cdot y_n$ rappresenta una soluzione valida del sistema di congruenze.

INFATTI:

$$z = \boxed{\alpha_1 n_1} b_2 + \boxed{\alpha_2 n_2} b_1$$

$$z \equiv b_2 \pmod{n_1}$$

$$\alpha_1 n_1 + \alpha_2 u_2 = 1 \Rightarrow$$

$$\Rightarrow \boxed{\alpha_2 u_2 = 1 - \alpha_1 n_1}$$

$$\begin{aligned}z &= \alpha_1 n_1 b_2 + (1 - \alpha_1 n_1) b_1 \\&= \alpha_1 n_1 b_2 + b_1 - \alpha_1 n_1 b_1 \equiv b_1 \pmod{n_1}\end{aligned}$$

$$z \equiv b_2 \pmod{n_2}$$

$$\alpha_1 n_1 + \alpha_2 u_2 = 1 \Rightarrow$$

$$\Rightarrow \boxed{\alpha_1 n_1 = 1 - \alpha_2 u_2}$$

$$\begin{aligned}z &= (1 - \alpha_2 u_2) b_2 + \alpha_2 u_2 b_1 \\&= b_2 - \alpha_2 u_2 b_2 + \alpha_2 u_2 b_1 \equiv b_2 \pmod{n_2}\end{aligned}$$

Ad es.: $\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 3 \pmod{5} \end{cases}$

PER IL TEOREMA CINQUE DEI RESTI TUTTE LE SOLUZIONI SONO IN \mathbb{Z}_M DOVE $M = M_1 \cdot M_2 = 6 \cdot 5 = 30$

$$\text{MCD}(6, 5) = 1 \quad \text{cioè } d_1, d_2 \in \mathbb{Z} \mid \begin{array}{l} d_1 M_1 + d_2 M_2 = 1 \\ d_1 6 + d_2 5 = 1 \end{array}$$

$$6 = 5 \cdot 1 + 1$$

$$1 = 6 + 5 \cdot (-1)$$

$$\begin{aligned} z &= d_1 n_1 b_2 + d_2 n_2 b_1 \\ &= 1 \cdot 6 \cdot 3 + (-1) \cdot 5 \cdot 4 \\ &= 18 - 20 = -2 \\ &[-2]_{30} = [-2 + 30]_{30} = [28]_{30} \end{aligned}$$

Come "ridurre" (SE SI PUÒ) un generico sistema di congruenze

$$(*) \quad \begin{cases} a_1 x \equiv c_1 \pmod{m_1} \\ a_2 x \equiv c_2 \pmod{m_2} \\ \vdots \\ a_k x \equiv c_k \pmod{m_k} \end{cases} \quad \text{ad un sistema nella forma} \quad \begin{cases} x \equiv b_1 \pmod{M_1} \\ x \equiv b_2 \pmod{M_2} \\ \vdots \\ x \equiv b_k \pmod{M_k} \end{cases}$$

$a_i, c_i \in \mathbb{Z}, m_i \in \mathbb{N}, m_i > 0$ $b_i \in \mathbb{Z}, M_i \in \mathbb{N}, M_i > 0$

PASSAGGIO 1 Calcolo $d_i = \text{MCD}(a_i, m_i) \quad \forall i=1, \dots, k$

- Esiste d_i tale che $d_i | c_i$ allora $a_i x \equiv c_i \pmod{m_i}$ non ha soluzioni, altrimenti (k) non ha soluzioni.
 - se $d_i | c_i \quad \forall i=1, \dots, k$ allora ogni congruenza $d_i \mid (k)$ ha soluzioni e
 - se $d_i = 1$ MANTENGO la congruenza $a_i x \equiv c_i \pmod{m_i}$
 - se $d_i \neq 1$ SOSTITUISCO // //
- con la congruenza :

$$\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \pmod{\frac{m_i}{d_i}}$$

Alla fine del PASSAGGIO 1 otengo che (*)
non ha soluzioni oppure che (*) è equivalente a

$$(*) \quad \left\{ \begin{array}{l} \frac{a_1}{d_1} x \equiv \frac{c_1}{d_1} \pmod{\frac{m_1}{d_1}} \\ \vdots \\ \frac{a_k}{d_k} x \equiv \frac{c_k}{d_k} \pmod{\frac{m_k}{d_k}} \end{array} \right.$$

PASSAGGIO 2 Risvolto c'è scuna congruenza di (**)

$$\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \pmod{\frac{m_i}{d_i}} \quad \text{VA sostituendo} \quad x \equiv b_i \pmod{\frac{m_i}{d_i}}$$

DOVE $[b_i]_{m_i/d_i} = \{b_i + \frac{m_i t}{d_i} | t \in \mathbb{Z}\}$ E' L'INSIEME DELLE SOLUZIONI DELLA CONGRUENZA

Posto $m'_i = \frac{m_i}{d_i}$ ottengo un sistema

$$(***) \quad \left\{ \begin{array}{l} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{array} \right.$$

Se $\text{MCD}(m_i, m_j) = 1 \quad \forall i \neq j$ posso

applicare il Teorema c'è soluz di mst . In tal caso:

PASSAGGIO 3 Con Newton trovo x_K nelle particolari

soluzione di (*) e per il teorema c'è soluz

l'insieme di tutte le soluzioni (***). **EQUINDI**

ANCHE DI (*) è $[x_K]_m = \{x_K + mt | t \in \mathbb{Z}\}$

dove $m = m_1 \cdot m_2 \cdot \dots \cdot m_k$

Grafi orientati e non orientati, tipi, arcoconnettività, tagli, Kruskal, Dijkstra

In teoria dei grafi, un "grafo non orientato" è una struttura matematica composta da due elementi principali: un insieme finito di vertici o nodi e un insieme finito di archi.

- Vertici (V): I vertici sono punti o nodi nel grafo. Ogni vertice rappresenta un'entità o un oggetto. Ad esempio, in un grafo che rappresenta le amicizie tra persone, i vertici rappresenterebbero le persone stesse. I vertici possono avere nomi, etichette o numeri per identificarli.
- Archi (E): Gli archi sono linee o connessioni tra i vertici. Gli archi rappresentano le relazioni tra i vertici. Se in un grafo rappresentante le amicizie, un arco collega due vertici, ciò indica che le due persone sono amiche. Gli archi possono essere bidirezionali, cioè non hanno direzione, il che significa che la relazione è reciproca. In alcuni casi, gli archi possono avere un peso associato per indicare una misura o una distanza tra i vertici.
 - o I nodi collegati da un arco sono vertici e l'arco vi è incidente
 - o I vertici sono adiacenti se esiste un arco di cui sono estremi

Un grafo non orientato può essere rappresentato in forma visuale tramite un diagramma in cui i vertici sono rappresentati come punti e gli archi come linee che collegano i vertici corrispondenti.

Enunciamo:

$$\text{TEOREMA 1} \quad \sum_{v \in V} d(v) = 2 \cdot |E|$$

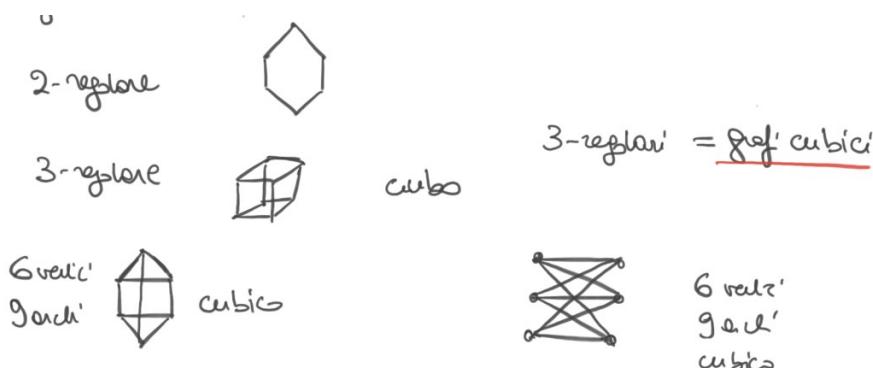
Inoltre:

- Il numero dei vertici di grado dispari è un numero pari

Descriviamo inoltre il grado di un vertice come il numero di volte in cui v è estremo di un arco.

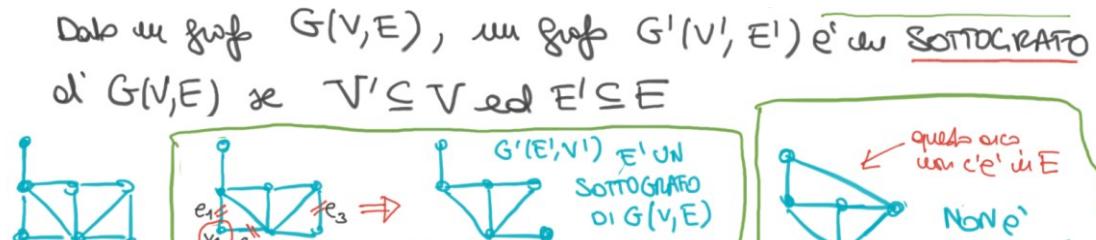
Possiamo definire:

- Un grafo viene definito k – regolare se ogni vertice ha grado k .



- Un grafo si dice completo se tutti i vertici sono adiacenti; questo si indica con K_n

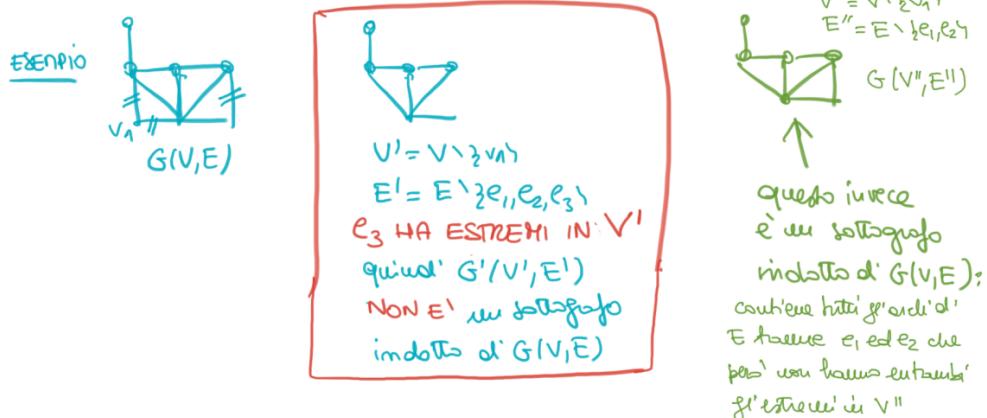
Un "sottografo" è una parte di un grafo più grande che conserva alcune o tutte le sue caratteristiche strutturali. In altre parole, un sottografo è ottenuto selezionando un sottoinsieme dei vertici e degli archi dal grafo originale in modo tale che le connessioni tra i vertici rimangano intatte. Un sottografo può essere una porzione del grafo originale oppure può avere alcuni vertici e archi rimossi.



Un sottografo indotto di un grafo G è ottenuto selezionando un sottoinsieme dei vertici di G e tutti gli archi che connettono quei vertici. In altre parole, un sottografo indotto contiene tutte le connessioni tra i vertici selezionati.

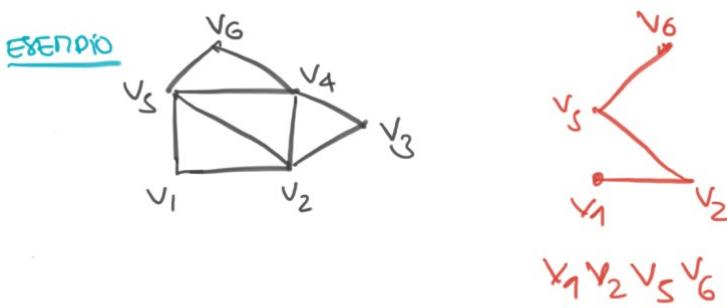
Un SOTTOGRAFO $G'(V', E')$ del grafo $G(V, E)$ si dice INDOTTO

se E' contiene tutti gli archi di E che abbiano estremi in V'



Per attraversare un grafo descriviamo:

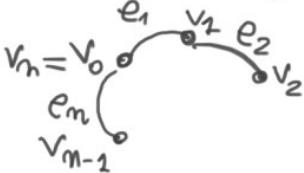
- un cammino, cioè una sequenza di vertici distinti dove ogni coppia di vertici consecutivi del cammino è collegata da un arco



- un ciclo/circuito, cammino in cui i due estremi sono coincidenti
- la lunghezza del cammino (o del circuito) è il numero di archi del cammino
 - o un cammino è detto dispari se ha lunghezza dispari, pari altrimenti

Abbiamo inoltre che:

NB Se un grafo è un ciclo, la lunghezza del ciclo è uguale al numero dei vertici'



Poi possiamo dire che:

- un percorso è una sequenza di vertici non necessariamente distinti dove ogni coppia di vertici consecutivi del percorso è collegata da un arco
 - o viene detto chiuso se i suoi estremi coincidono
 - o la lunghezza del percorso è il numero di archi attraversati

TEOREMA 2 Dato un percorso con estremi v_1 e v_n

($v_1 \neq v_n$: non chiuso) esiste un cammino con estremi

v_1 e v_n

TEOREMA 3 Un PERCORSO CHIUSO di lunghezza

DISPARI contiene almeno un ciclo di lunghezza

dispari

Dato inoltre un $G(V, E)$, con $u, v \in V$, diremo che u è connesso a v se esiste un cammino di estremi u e v . La relazione di connessione è una relazione di equivalenza (come tale: riflessiva, simmetrica e transitiva).

$$u \in V \quad [u] = \{v \in V \mid u \sim v\}$$

LA COMPONENTE CONNESSA DEL GRAFO CHE CONTIENE u è la classe d'equivalenza rispetto alla relazione "essere connessi"

Le classi di equivalenza rispetto alla relazione

"essere connessi" si chiamano LE COMPONENTI CONNESSE DEL GRAFO



1 COMPONENTE CONNESSA



2 COMPONENTI CONNESSE

Il grafo è detto connesso se ha un'unica componente连通的.

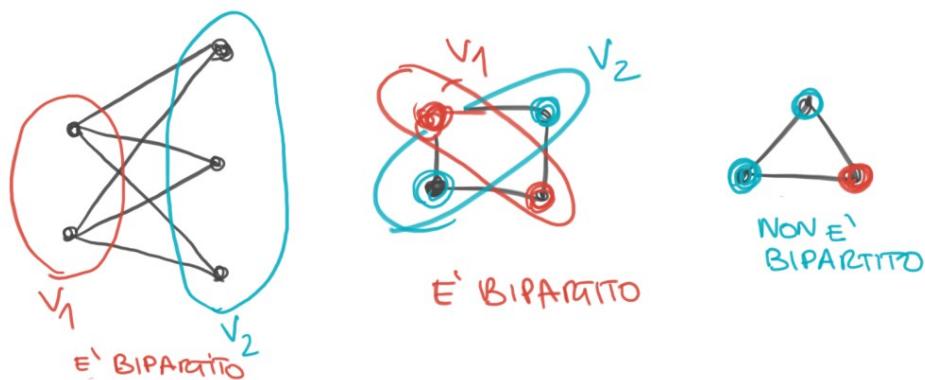
Un grafo bipartito è un tipo specifico di grafo non orientato in cui i vertici possono essere suddivisi in due insiemi disgiunti in modo tale che tutti gli archi collegano vertici appartenenti a insiemi diversi. In altre parole, un grafo è bipartito se i suoi vertici possono essere divisi in due gruppi in modo che non ci siano archi all'interno dello stesso gruppo e tutti gli archi collegano vertici dei due gruppi differenti.

Formalmente:

Un GRAFO $G(V, E)$ si dice BIPARTITO se

$$\begin{cases} V = V_1 \cup V_2 \text{ con } V_1 \cap V_2 = \emptyset \\ \text{ogni arco ha un estremo in } V_1 \text{ ed un estremo in } V_2 \end{cases}$$

Po iudicarlo: $G(V_1, V_2, E)$



Un grafo bipartito completo è un tipo particolare di grafo bipartito in cui ogni vertice del primo insieme è collegato a ogni vertice del secondo insieme. In altre parole, tutti i possibili archi che possono collegare i vertici dei due insiemi sono presenti nel grafo bipartito completo.

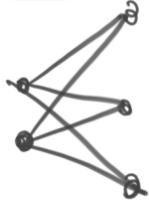
IL GRAFO BIPARTITO COMPLETO è un grafo $G(V_1, V_2, E)$

(quindi è bipartito) in cui OGNI VERTICE DI V_1 È A DIACENTE AD OGNI VERTICE DI V_2 (ad es. i 2 graf bipartiti in queste pagine sono entrambi bipartiti completi) SI INDICA: K_{m_1, m_2} DOVE $m_1 = |V_1|$ E $m_2 = |V_2|$

ESEMPI DI BIPARTITI COMPLETI



$K_{2,3}$



$K_{2,3}$



$K_{2,4}$

In K_{m_1, n_2} si ha che $|E| = |V_1| \cdot |V_2| = m_1 \cdot n_2$

Inoltre:

se $v \in V_1$



gli archi che hanno un vertice $v \in V_1$ come estremo sono in numero di $|V_2|$

Allora $|E| = |V_1| + |V_2| + \dots + |V_n| = |V_1| \cdot |V_2|$

tutti quelli quanti sono i $v \in V_1$

Proseguendo:

TEOREMA 4

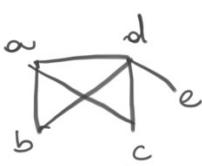
Un grafo è bipartito se e solo se non contiene cicli d'impari

Poi:

NB UN CICLO È BIPARTITO
SE E SOLO SE È PARI

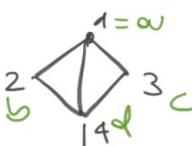
Due grafi si dicono isomorfi se possono essere disegnati nello stesso modo, cioè se esiste una corrispondenza biunivoca tra i loro vertici tale che gli archi vengono conservati. In altre parole, due grafi sono isomorfi se hanno la stessa struttura di base, anche se i nomi dei vertici e gli etichette degli archi possono essere diversi.

Uno stesso grafo può essere disegnato in modi diversi



$$\begin{array}{l} f: \\ \begin{array}{l} a \mapsto 1 \\ b \mapsto 2 \\ c \mapsto 3 \\ d \mapsto 4 \\ e \mapsto 5 \end{array} \end{array}$$

E' ISOMORFO A



Df $G(V, E)$ È ISOMORFO A $G'(V', E')$

Se esiste una biiezione $f: V \rightarrow V'$
che conserva le adiacenze;

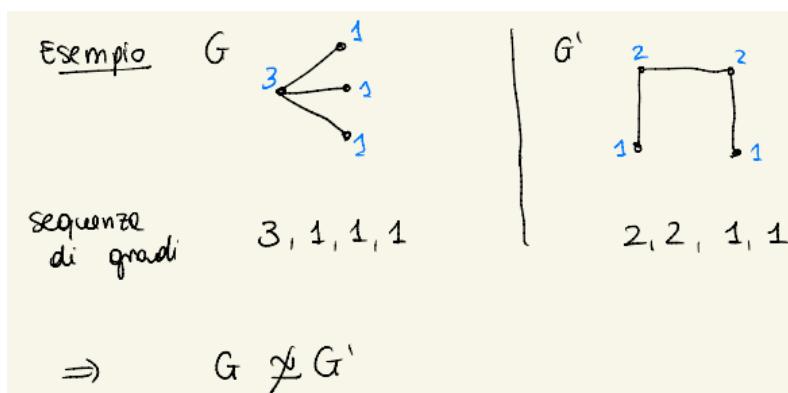
$$u, v \in V, (u, v) \in E \Rightarrow (f(u), f(v)) \in E'$$

Inoltre, possiamo descrivere:

Il "grafo complementare" di un grafo G è un grafo che ha gli stessi vertici di G , ma gli archi sono presenti solo quando non sono presenti in G , e viceversa. In altre parole, due vertici nel grafo complementare sono collegati da un arco se e solo se non sono collegati da un arco nel grafo originale G .

Formalmente, se G ha un insieme di vertici V e insieme di archi E , allora il grafo complementare G' avrà gli stessi vertici V e un insieme di archi E' tali che uv è un arco in G' se e solo se uv non è un arco in G .

Poi, vi è la "sequenza di gradi" di un grafo, cioè una sequenza ordinata che elenca i gradi dei vertici del grafo. In altre parole, per ogni vertice nel grafo, la sequenza di gradi elenca quanti archi sono adiacenti a quel vertice.



Un corollario possibile, aggiunto a livello logico, è il seguente:

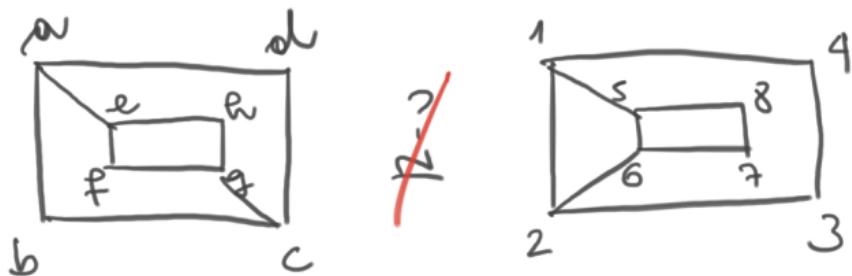
TEOREMA : $\left\{ \begin{array}{l} \text{Due grafi } G(V, E) \text{ e } G'(V', E') \text{ sono isomorfi} \\ \text{se e solo se i loro complementari} \\ \overline{G}(V, E) \text{ e } \overline{G}'(V', E') \text{ sono isomorfi.} \end{array} \right.$

Possiamo inoltre descrivere una partizione in un grafo come suddivisione dei suoi vertici in sottoinsiemi disgiunti chiamati "classi" o "parti". In altre parole, una partizione rappresenta una divisione dei vertici del grafo in gruppi tali che ogni vertice appartenga esclusivamente a una delle classi e non vi sia sovrapposizione tra le classi.

Formalmente, data una partizione di un grafo G con n vertici, ciò significa che esistono k classi disgiunte $\{V_1, V_2, \dots, V_k\}$ tali che:

1. Ogni vertice di G appartiene a una sola classe, cioè $V_i \cap V_j = \emptyset$ per $i \neq j$.
2. L'unione di tutte le classi è uguale all'insieme completo dei vertici, cioè $V_1 \cup V_2 \cup \dots \cup V_k = V$.

Di fatto, dei grafi per essere isomorfi, hanno anche bisogno di avere gli stessi sottografi indotti. Ciò è visibile anche dal seguente esempio:



Riassumendo qui:

- hanno lo stesso numero di vertici: 8
- = = = = = di archi: 15
- = la stessa sequenza di gradi: 3,3,3,3,2,2,2,2
- sono entrambi bipartiti:

STUDIO I SOTTOGRAFI INDOTTI DAI VERTICI DI GRADO MASSIMO:

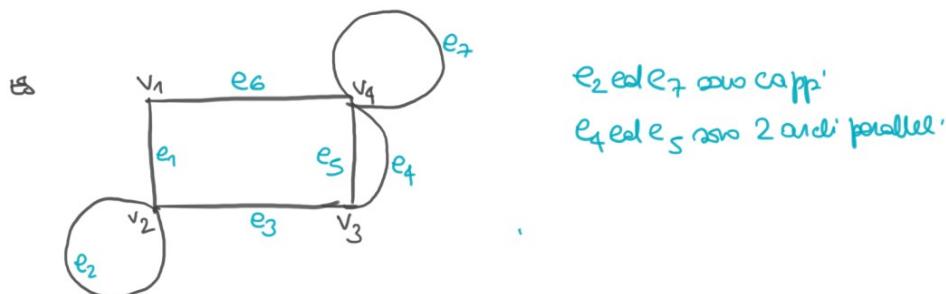


Nei grafi visti fino ad ora, cosiddetti grafi semplici, abbiamo che:

- vi è una coppia di vertici con al massimo un arco
- ogni arco ha due estremi distinti

Possiamo parlare di multigrafo come un grafo dove le due condizioni precedenti non sono richieste, ma:

- ci possono essere archi paralleli
- ci possono essere archi che sono cappi
 - Nel contesto dei grafi, un cappio è un arco che collega un vertice a se stesso. In altre parole, un cappio è un'autoconnessione di un vertice attraverso un arco.
 - Un cappio è rappresentato come una sorta di loop



I CAPPI CONTRIBUISCONO 2 AL GRADO DELL'ESTREMITÀ

$$d(v_2) = 2 + 1 + 1 = 4$$

$$d(v_4) = 2 + 1 + 1 + 1 = 5$$

NB: ne' multigrafi gli archi devono essere indicati nel 'pecos'

$v_3 \leftarrow v_4 \leftarrow v_7 \leftarrow v_4 \leftarrow v_6 \leftarrow v_1$

Ora un concetto molto importante, cioè l'arcoconnettività, spesso indicata come " k -arcoconnettività" o "arcoconnettività minima", misura che descrive la robustezza di un grafo orientato rispetto alla rimozione di archi. Indica il numero minimo di archi che devono essere rimossi affinché il grafo risulti sconnesso o non più fortemente connesso.

Formalmente, l'arcoconnettività di un grafo orientato è definita come il valore minimo k tale che il grafo rimanga fortemente connesso dopo la rimozione di k archi. In altre parole, un grafo è k -arcoconnesso se, anche dopo aver rimosso fino a k archi, rimane ancora fortemente connesso.

Dati $u, v \in V$

se esiste un cammino d'estremi u e v , u e v sono CONNESSI

se u e v non sono connessi, dico che sono DISCONNESSI

$G(V, E)$ è CONNESSO se $\forall u, v \in V$ u e v sono connessi

se $G(V, E)$ non è connesso, dico che $G(V, E)$ è DISCONNESSO

In teoria dei grafi, un taglio rappresenta una divisione di un grafo in due insiemi disgiunti di vertici, insieme ai loro archi associati, in modo tale che la rimozione di questi archi dividerebbe il grafo in due componenti separate.

Formalmente, dato un grafo G e due insiemi disgiunti di vertici S e T tali che $S \cup T = V$ (dove V è l'insieme dei vertici del grafo), il taglio C è costituito da tutti gli archi che collegano un vertice in S a un vertice in T . In altre parole, C è l'insieme di archi che attraversa la divisione tra S e T .

Possiamo quindi distinguere:

Dato $S \subseteq V$

$G(V, E)$ GRAFO O MULTIGRAFO

si chiama TAGLIO ASSOCIATO AD S

l'insieme degli archi

NB qui un taglio può contenere un cappio

$\delta(S) = \{ \text{gl'archi che hanno ESATTAMENTE UNA ESTREMITÀ in } S \} =$

$$= \{ uv \in E \mid |S \cap \{u, v\}| = 1 \}$$

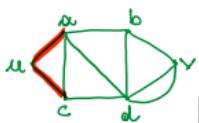
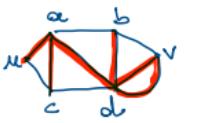
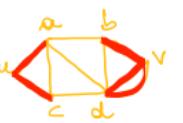
Quindi, un taglio associato è un taglio che rappresenta il numero minimo di archi da rimuovere per disconnettere due vertici specifici nel grafo. Più formalmente, dato un grafo e due vertici u e v , il taglio associato tra u e v è un taglio in cui u è in un insieme e v è nell'altro insieme, e l'insieme di archi del taglio rappresenta il numero minimo di archi da rimuovere per isolare u da v .

Fissati $w, z \in V$ si dice IL TAGLIO $\delta(S)$ SEPARA $w \in z$

SE S CONTIENE ESATTAMENTE 1 TRA $w \in z$

Invece, un taglio connesso è un taglio che separa il grafo in due componenti connesse. Ciò significa che se si rimuovessero gli archi nel taglio connesso, il grafo sarebbe diviso in due parti, e non ci sarebbero percorsi che collegano i vertici di S ai vertici di T .

Seguono specifici esempi di tagli:

 $S = \{u\}$ $\delta(S) = \{ua, uc\}$ $\delta(S)$ SEPARA u DA TUTTI GLI ALTRI VERTICI. IN PARTICOLARE, $\delta(S)$ SEPARA $u \in v$	 $S = \{u, c, d\}$ $\delta(S) = \{ua, ca, da, db, e_1, e_2\}$ $\delta(S)$ SEPARA u DAI VERTICI CHE NON SONO NE' c , NE' d . IN PARTICOLARE, $\delta(S)$ SEPARA $u \in v$	 $S = \{u, v\}$ $\delta(S) = \{ua, uc, vb, e_1, e_2\}$ $\delta(S)$ SEPARA u DA CIASCUN VERTICE CHE SIA DIVERSO DA v . MA $\delta(S)$ NON SEPARA $u \in v$
$G(V, E \setminus \delta(S))$ 	$G(V, E \setminus \delta(S))$ 	$G(V, E \setminus \delta(S))$ 

In tutti e 3 i casi di $G(V, E \setminus \delta(S))$ $u \in v$ sono disconnessi, ma nel 3° caso $\delta(S)$ non separa $u \in v$

Attenzione però che:



Possiamo quindi dare la seguente definizione definitiva di arcoconnettività:

$$K_{uv}^E(G) = \text{ARCOCONNETTIVITÀ FRA } u \in V =$$

$\min \left\{ |\delta(S)| \mid S \text{ taglio che separa } u \text{ e } v \right\}$

NB Per i multigrafi i cappi non influiscono su $K_{uv}^E(G)$
(nessun taglio contiene un cappo)

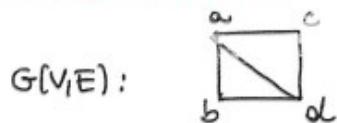
O in altri termini, per quanto riguarda un grafo:

$$K^E(G) = \text{ARCOCONNETTIVITÀ DI } G$$

$= \min_{u,v \in V} K_{uv}^E(G)$

Quindi se G è连通的, $K^E(G)$ è il minimo
numero di archi da togliere da G per "disconnetterlo"

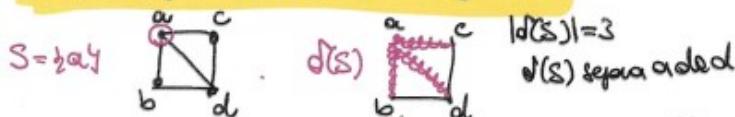
ESEMPIO ARCOCONNETTIVITÀ



$$K^E(G) = ?$$

$$K^E(G) = \min \{ K_{ad}^E(G), K_{ac}^E(G), K_{dc}^E(G), K_{bc}^E(G), K_{bd}^E(G), K_{ab}^E(G) \}$$

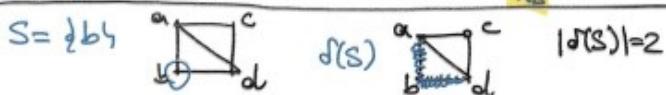
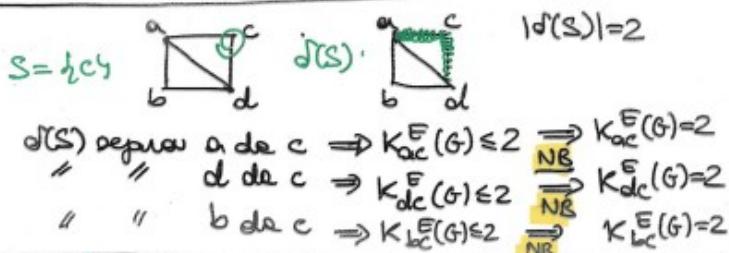
N.B. $\forall x, y \in V, x \neq y$ è $K_{xy}^E(G) > 1$



$\Rightarrow K_{ad}^E(G) \leq 3$, siccome ci sono 3 cammini disgiunti

singolo archi da e a d:

$$K_{ad}^E(G) = 3$$



$d(S)$ separa b da d $\Rightarrow K_{bd}^E(G) \leq 2 \xrightarrow{\text{N.B.}} K_{bd}^E(G) = 2$

$\parallel \quad \parallel \quad a \text{ da } b \Rightarrow K_{ab}^E(G) \leq 2 \xrightarrow{\text{N.B.}} K_{ab}^E(G) = 2$

concludendo: $K^E(G) = \min \{ 2, 3 \} = 2$

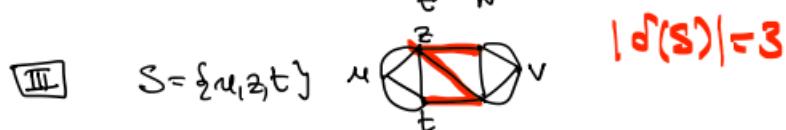
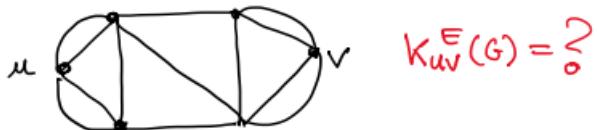
N.B., avrebbe fatto sufficiente fermarsi al calcolo di $K_{ac}^E(G)$

Sarebbe possibile provare che:

[1] $K_{uv}^E(G)$ è il minimo numero d'archi da togliere da $G(V, E)$ affinché u e v diventino disconnessi

[2] $K_{uv}^E(G)$ è il massimo numero d'cammini con estremità u e v CHE NON HANNO ARCHI IN COMUNE (CAMMINI DISGIUNTI SUGLI ARCHI)

E completando ciò:

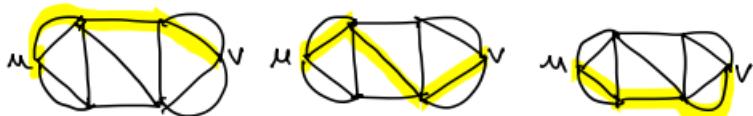


IN TUTTI I 3 I CASI, $\delta(S)$ SEPARA $u \in V$

QUINDI $K_{uv}^E(G) \leq 3$

SICCOME CI SONO ALMENO 3 CAMMINI DA u AV

DISGIUNTI SUGLI ARCHI:



Allora ogni taglio che separa $u \in V$

DEVE CONTENERE ALMENO 3 ARCHI

PER CIÒ $K_{uv}^E(G) \geq 3$

Parliamo poi di separatore, che all'interno di un grafo rappresenta un insieme di vertici che, se rimosso dal grafo insieme ai suoi archi associati, divide il grafo in due o più componenti connesse più piccole. In altre parole, il separatore è un insieme di vertici la cui rimozione spezza il grafo in parti distinte.

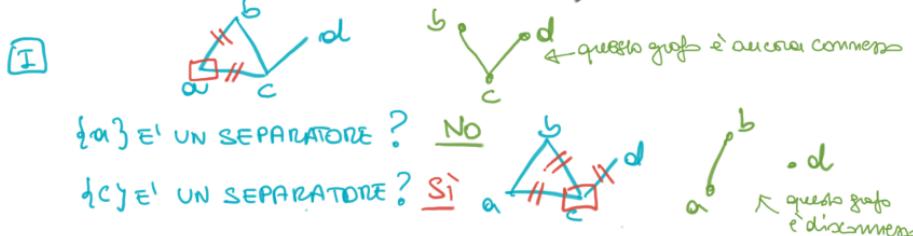
Formalmente, dato un grafo G e un insieme di vertici S , S è un separatore se la rimozione di S e degli archi adiacenti ai vertici di S aumenta il numero di componenti connesse nel grafo. In altre parole, se $G-S$ (il grafo ottenuto dalla rimozione di S e dei suoi archi) ha più componenti connesse di G , allora S è un separatore.

Un $S \subseteq V$ si dice un SEPARATORE DI $G(V, E)$

se il grafo che si ottiene da $G(V, E)$

- togliendo S da V e
- togliendo da E tutti gli archi che abbiano almeno un estremo in S

è disconnected (i.e. non è连通的)



Descriviamo poi la connettività di un grafo come il numero minimo di vertici la cui rimozione dal grafo trasforma G in un grafo sconnesso.

\Rightarrow $[G$ contiene una coppia di vertici non adiacenti $\Rightarrow \exists$ un separatore in G]

segue: $[\nexists$ un separatore in $G \Rightarrow G$ è completo]
 $G = K_n$

Più matematicamente:

$$K_{uv}(G) = \text{CONNEDTIVITÀ TRA } u \in V \underset{\text{def}}{=} \\ = \text{minimale dimensione di un separatore } S \text{ tale che} \\ u \in V \text{ risulti in due componenti connesse} \\ \text{distinte in } G \setminus S$$

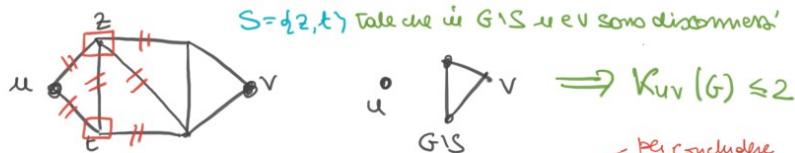
Quindi $K(G) = \min_{\substack{u, v \in V \\ u, v \text{ NON ADIACENTI}}} K_{uv}(G)$

Indichiamo con $G \setminus S$ il grafo che si ottiene da G togliendo S da V e togliendo gli archi che abbiano almeno un estremo in S

Dati quindi i vertici non adiacenti, il concetto di connettività definisce dei cammini interamente disgiunti, come segue anche:

$K_{uv}(G) =$ il massimo numero di cammini con estremi u, v che non hanno vertici intermedi in comune
 (cammini INTERNAMENTE DISGIUNTI)

ESEMPIO

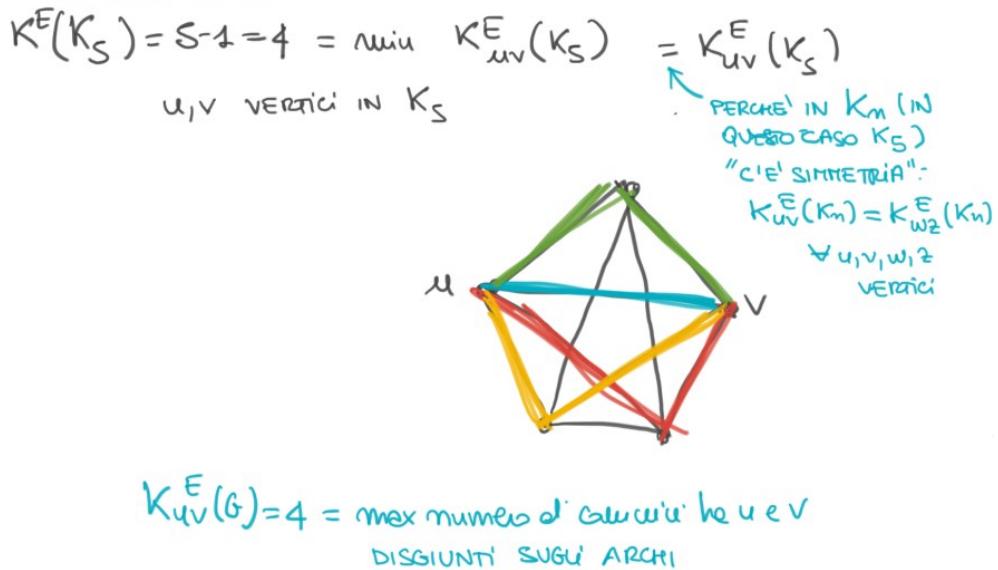


Dato poi un grafo con almeno 2 vertici, il grado minimo di G è $d_g^{\min} = \min\{d(v) \mid v \in V\}$.

Inoltre, per teorema, dato un grafo sempre con almeno due vertici, avremo che:

$$K(G) \leq K^E(G) \leq d^{\min}(G)$$

AD ESEMPIO, se $m=5$ otteriamo:



Possiamo inoltre definire:

- una foresta come grafo senza cicli (aciclico)
- un albero come foresta connessa

Per gli alberi (con un numero di vertici ≥ 2) definiamo come proprietà:

- ci sono almeno 2 vertici di grado 1
- $|E| = V - 1$

Definiamo quindi l'algoritmo di Kruskal, utilizzato per trovare un albero di copertura minima in un grafo con pesi sugli archi. In altre parole, cerca di trovare un sottoinsieme di archi che connettano tutti i vertici del grafo in modo tale che la somma dei pesi degli archi sia la più piccola possibile.

Ecco come funziona l'algoritmo di Kruskal:

1. **Inizializzazione:** Si inizia con un insieme vuoto di archi A che costituiranno l'albero di copertura minima. Si ordina tutti gli archi del grafo in ordine crescente di peso.
2. **Scansione degli Archi:** Si considerano gli archi uno per uno nell'ordine crescente dei pesi.
3. **Aggiunta degli Archi:** Per ciascun arco considerato, si verifica se l'aggiunta di quell'arco a A creerebbe un ciclo nell'insieme degli archi finora selezionato. Se l'aggiunta dell'arco non forma un ciclo, viene aggiunto a A .
4. **Terminazione:** L'algoritmo termina quando sono stati considerati tutti gli archi o quando A contiene $n - 1$ archi, dove n è il numero di vertici del grafo.

Quindi, dato un grafo connesso, ad ogni arco è associato un peso e si vuole trovare il peso minimo, come albero.

INPUT $G(V, E)$ connesso, pesi $w(e)$, $e \in E$

OUTPUT $T(V, E')$ albero di peso minimo

- ordina gli archi $\{1, 2, 3, \dots, m\}$ in ordine
non decrescente di peso: $w(1) \leq w(2) \leq \dots \leq w(m)$

al passaggio i -esimo: trovare arco i -esimo:

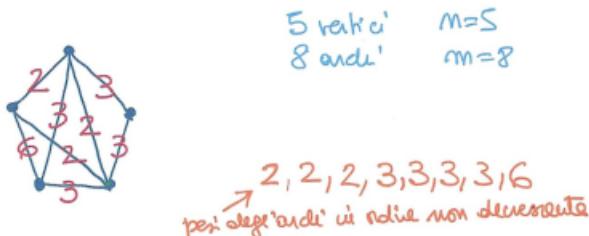
Lo inserisco se non forma alcun ciclo con
gli archi precedentemente inseriti

Lo rifiuto altrimenti

STOP quando arriva un albero con $m = |V|$ vertici
(quindi $|E'| = m-1$)

[VEDERE ESEMPIO SU
FOGLIO AGGIUNTO]

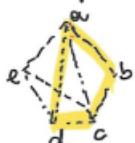
L'esempio in questione è il seguente:



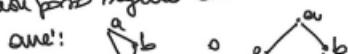
Possibili scelte delle prime due archi:



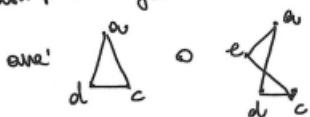
Non posso negare tutti e tre gli archi di peso 2

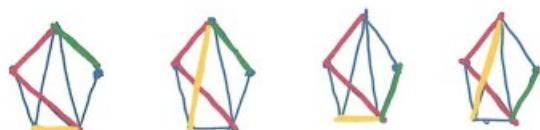
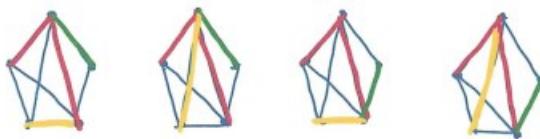
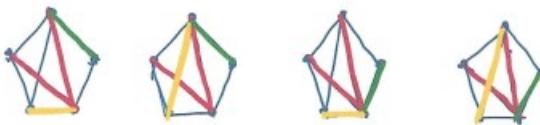


- non posso negare entrambi ab e bc :



- non posso negare entrambi ad e dc :





N.B. L'arco d'peso 6 non puo' essere effettuato.
Questi sono tutti i possibili archi d'peso minimo.

Hanno tutti peso $2+2+3+3=10$
N.B. $m=5 \Rightarrow$ tutti gli archi hanno $m-1=5-1=4$ archi!

Similmente, abbiamo l'algoritmo di Dijkstra, utilizzato per trovare il percorso più breve da un nodo di partenza a tutti gli altri nodi in un grafo con pesi sugli archi non negativi. L'algoritmo assegna una distanza minima stimata da un nodo di partenza a tutti gli altri nodi del grafo, aggiornando queste distanze man mano che esplora il grafo.

Ecco l'algoritmo di Dijkstra formalmente:

- Inizializzazione: Si assegna al nodo di partenza una distanza di 0 e a tutti gli altri nodi una distanza infinita. Si crea un insieme di nodi non visitati.
- Esplorazione: Finché ci sono nodi non visitati:
 - o Si seleziona il nodo con la distanza minima tra quelli non visitati.
 - o Si marca il nodo come visitato e si aggiornano le distanze dei nodi adiacenti attraverso gli archi non ancora visitati. Se la distanza calcolata è inferiore alla distanza attuale, si aggiorna la distanza.
- Terminazione: L'algoritmo termina quando tutti i nodi sono stati visitati o quando il nodo di destinazione è stato visitato (se si cerca il percorso più breve verso un nodo specifico).

INPUT $G(V, E)$ connesso, le lunghezze $l(e) > 0, e \in E$
Sia u il vertice "DI PARTENZA"

OUTPUT DISTANZA E CAMMINI MINIMI TRA u E $w, \forall w \in V$

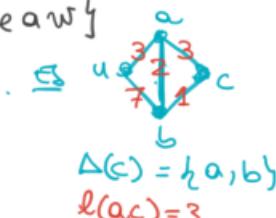
$$\forall w \in V, \Delta(w) = \{x \in V \mid x \text{ adiacente a } w\}$$

$$\forall x \in \Delta(w), l(xw) = \text{LA LUNGHEZZA DELL'ARCO } xw$$

Se $i \in N$ sia

$d_i(w) = \text{LA DISTANZA DI } w \text{ DA } u \text{ AL PASSAGGIO}$

$$d_{i-1}(w) = \min \{d_{i-2}(w), d_{i-2}(x) + l(xw) \mid x \in \Delta(w)\}$$



$$\Delta(c) = \{a, b\}$$

$$l(ac) = 3$$

$$l(bc) = 1$$

INIZIALIZZAZIONE

Se $i=0$: $d_0(u)=0, d_0(w)=\infty \quad \forall w \neq u$
 $S_0 := \{u\}$

ITERAZIONE :

se $i > 0$ STUDIO SOLO I VERTICI CHE NON STANNO IN S_{i-1}

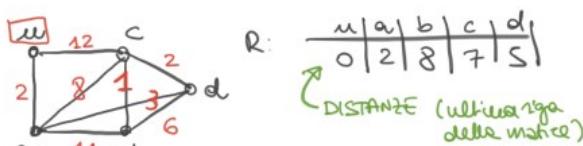
Preso u_i = vertice CHE NON SIA IN S_{i-1}

$$d_i(u_i) \leq d_{i-1}(w) \quad \forall w \notin S_{i-1}$$

$$\text{Poi} \quad S_i = S_{i-1} \cup \{u_i\}$$

STOP quando $i = |V|-1$

ESERCIZIO
TROVARE DISTANZE E CAMMINI MINIMI DA u A TUTTI GLI ALTRI VERTICI



	u	a	b	c	d
$i=0$	$S_0 = \{u\}$	0	∞	∞	∞
$i=1$	$S_1 = S_0 \cup \{a\}$	0	2	∞	12
$i=2$	$S_2 = S_1 \cup \{b\}$	0	2	13	10
$i=3$	$S_3 = S_2 \cup \{c\}$	0	2	11	7
$i=4$	$S_4 = S_3 \cup \{d\}$	0	2	8	5

$|V|=5$ dà 4 iterazioni (tavola matrice 5×5)

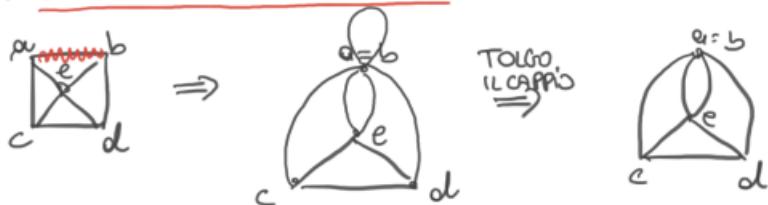
	u	a	b	c	d
$i=0$	$S_0 = \{u\}$	0	∞	∞	∞
$i=1$	$S_1 = S_0 \cup \{a\}$	0	2	∞	12
$i=2$	$S_2 = S_1 \cup \{b\}$	0	2	13	10
$i=3$	$S_3 = S_2 \cup \{c\}$	0	2	11	7
$i=4$	$S_4 = S_3 \cup \{d\}$	0	2	8	5

Sugli alberi, possiamo fare alcune caratterizzazioni (intanto la prima):

1. Dato $T(V, E)$ grafo, sono equivalenti:
 - a. $T(V, E)$ è un albero
 - b. $T(V, E)$ è arcoconnesso
 - c. $\forall x, y \in V, x \neq y, \exists! \alpha$ cammino di estremi x, y

Possiamo inoltre descrivere un grafo come planare quando può essere disegnato sul piano senza intersecare gli archi. Prima di enunciare il successivo teorema, occorre descrivere il minore di un grafo, ottenibile attraverso:

1 Una CONTRAZIONE DI UN ARCO:



2 RITRAZIONE DI UN ARCO

3 RITRAZIONE DI UN VERTICE ISOLATO



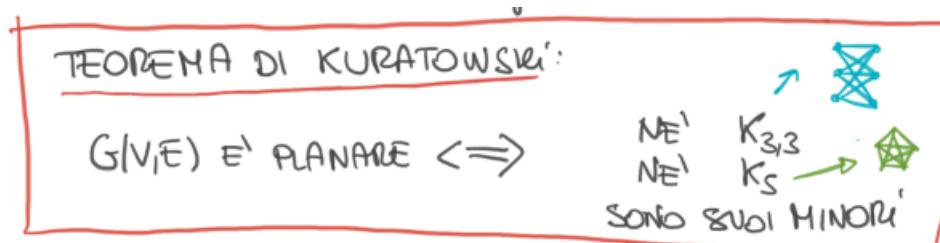
non adiacente
ad altri vertici?

Un grafo $G'(V', E')$ è un MINORE del grafo $G(V, E)$

se G' si ottiene da G con le 3 operazioni descritte.



Sulla base di queste osservazioni, determiniamo il teorema di Kuratowski.



Per rappresentare grafi planari visualmente, descriviamo il metodo dei cerchi e delle corde, tecnica utilizzata per rappresentare grafi planari in modo visuale, sfruttando cerchi e segmenti di retta (chiamati "corde") per rappresentare vertici e archi rispettivamente. Questo metodo consente di disegnare grafi planari in modo ordinato e chiaro, evitando sovrapposizioni e incroci tra archi.

Esso può essere usato solo se il grafo ha un circuito hamiltoniano (cioè, attraversa tutti i vertici del grafo):

- 1 trovare (se esiste) un circuito hamiltoniano
- 2 disegnalo come un cerchio
- 3 scrivere l'elenco degli archi che non sono nel circuito
(chiamiamoli CORDE)
- 4 inserirli dentro o fuori dal cerchio cercando di evitare gli archi (SCEGLIENDO AD OGNI PASSAGGIO Archi che siano)

Concretamente:

- Ogni vertice del grafo è rappresentato da un cerchio. I centri dei cerchi sono posizionati in modo da rispettare la struttura del grafo, garantendo che gli archi possano essere collegati senza sovrapposizioni.
- Gli archi del grafo sono rappresentati da segmenti di retta (corde) che collegano i cerchi corrispondenti ai vertici collegati dall'arco. Le corde vengono disegnate all'esterno dei cerchi in modo da non attraversarli.
- L'obiettivo è posizionare i cerchi (vertici) e le corde (archi) in modo che non si sovrappongano e che gli archi siano chiari e facilmente tracciabili. Questo può richiedere un po' di pianificazione e regolazione per evitare incroci indesiderati.

A livello di vantaggi:

- Chiarezza: I cerchi e le corde forniscono una rappresentazione chiara dei vertici e degli archi.
- Evita Incroci: Quando utilizzato correttamente, il metodo evita sovrapposizioni e incroci tra archi.

A livello di svantaggi:

- Spazio: In alcuni casi, potrebbe richiedere molto spazio per rappresentare grafici complessi.
- Complessità: La rappresentazione dei grafi più grandi può diventare complessa e disordinata.
- Estetica: La disposizione dei cerchi e delle corde richiede attenzione per garantire che l'aspetto visuale sia gradevole e comprensibile.

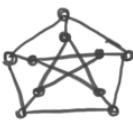
FORZATI DALLE SCELTE PRECEDENTI - SE ESISTONO)

Se si riesce ad inserirli tutti, UNO AD UNO, senza fare incroci, il grafo è plattico.

Altrimenti no.

Un grafo notoriamente non planare è il grafo di Petersen.

IL GRAFO DI PETERSEN :



10 VERTICI
15 ARCHI

Il grafo di Petersen non è planare: contragendo gli

archi in rosso:

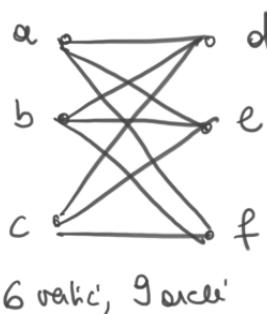


si ottiene il sottografo K5



Altrimenti, possiamo anche aggiungere:

K_{3,3} NON È PLANARE



Un circuito hamiltoniano:

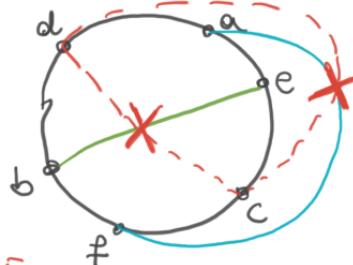
adcfbda PRENDE 6 ARCHI

AVANZANO 9-6 = 3 CORDE

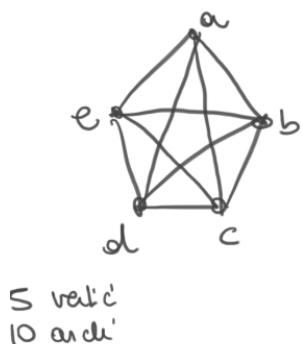
1° gf
2° be
3° cd

CREA INCROCI
CON LE CORDE
GIÀ INSERITE

⇒ K_{3,3} NON È PLANARE



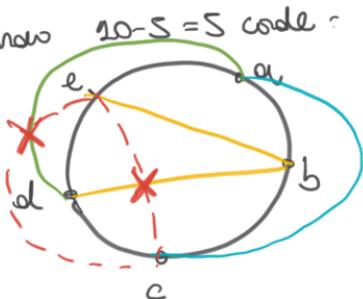
K₅ NON È PLANARE



abcde è un circuito hamiltoniano
prende 5 archi

mi avanzano 10-5 = 5 corde:

1° ac
4° ad
2° ba
3° be
ce



Dato inoltre un grafo planare, ogni rappresentazione piana divide il piano in facce (o regioni). Il numero delle facce dipende solo dal grafo e non dalla particolare rappresentazione piana disegnata.

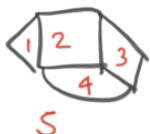
La formula di Eulero è una relazione matematica che coinvolge i vertici, gli archi e le facce di un poliedro convesso. Questa formula è spesso utilizzata nella teoria dei poliedri e nella geometria per collegare queste tre quantità fondamentali in un poliedro.

La formula di Eulero per i poliedri è data da:

$$V - E + F = 2$$

Dove:

- V rappresenta il numero di vertici del poliedro.
- E rappresenta il numero di archi del poliedro.
- F rappresenta il numero di facce del poliedro.



FORMULA DI EULERO

Se G è un grafo, $G(V, E)$

- ① semplice (NON UN MULTIGRAFO)
- ② connesso
- ③ planare

$$\begin{aligned} R &= \text{numero delle regioni} \\ e &= |E| \\ v &= |V| \end{aligned}$$

si ha:

$$R = e - v + 2$$

numero delle regioni numero degli archi numero dei vertici

A livello di teorema, possiamo quindi determinare:

TEOREMA Se $G(V, E)$ è un grafo semplice, connesso e planare e con ALMENO 3 VERTICI

$$\begin{aligned} |V| &= v \geq 3 \\ |E| &= e \quad \text{si ha: } e \leq 3v - 6 \end{aligned}$$

In un grafo, il concetto di faccia è tipicamente associato ai grafi planari. Un grafo planare è un grafo che può essere disegnato su un piano in modo che i suoi archi non si incrocino. In questo contesto, le facce rappresentano regioni del piano delimitate dagli archi del grafo.

Formalmente, in un grafo planare:

- Una "faccia esterna" è la regione del piano che è delimitata da tutti i vertici e gli archi del grafo. È la regione esterna in cui il grafo è disegnato.
- Le "facce interne" sono le regioni del piano delimitate dagli archi del grafo, escludendo l'esterno. Ogni volta che un arco attraversa il piano, esso delimita due facce interne.

Possiamo quindi definire:

- Una frontiera, definibile come l'insieme degli archi che delimitano f
- Il perimetro di f , percorso chiuso che mi porta da un vertice attraversando tutta la frontiera

$$\underline{l_f = \text{LUNGHEZZA DEL PERIMETRO DI } f = \text{LA LUNGHEZZA DI QUEL PERCORSO}}$$

in $\sum_f l_f$ OGNI ARCO DEL GRAFO VIENE CONTATO 2 VOLTE

QUINDI $\sum_f l_f = 2|E| = 2e$

NB. $\forall f \quad l_f \geq 3$

EULERIO
 $r = e - v + 2$

Un circuito hamiltoniano di un grafo $G(V, E)$ è un circuito che attraverso tutti gli vertici $v \in V$.

Un grafo è hamiltoniano se possiede un circuito hamiltoniano.

ESEMPI DI GRAFI HAMILTONIANI

K_n

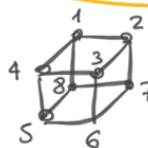


K_n È HAMILTONIANO $\forall n \geq 3$

K_2 NON LO È K_2

aba

NON È UN CICLO DA È UN ARCO PERCORSO 2 VOLTE



È HAMILTONIANO:

1 2 3 4 5 6 7 8 1 è un circuito hamiltoniano

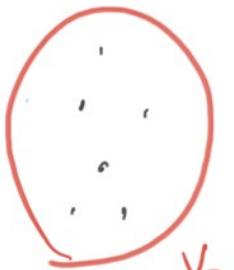
Proviamo che

$$K_{\pi, s} \text{ E' HAMILTONIANO} \iff \pi = s \geq 2$$

" \Rightarrow "



$$V_1 \\ |V_1| = \pi$$



$$V_2 \\ |V_2| = s$$

$$\begin{aligned} V &= \text{insieme dei vertici} \\ &= V_1 \cup V_2 \end{aligned}$$

QUINDI
 x_1, x_2, \dots, x_m
SONO ESATTAMENTE
TUTTI I VERTICI
DI $K_{\pi, s}$

$K_{\pi, s}$ è hamiltoniano x ipotesi $\Rightarrow \exists \gamma = x_1 x_2 x_3 \dots x_m x_1$ circuito hamiltoniano
w.l.o.g. $x_1 \in V_1 \Rightarrow x_2 \in V_2 \Rightarrow x_3 \in V_1 \dots x_i \in V_2 \Leftrightarrow i \text{ E' PARI}$
 $\Rightarrow |V_1| = |V_2| = \frac{|V|}{2}$ $x_i \in V_1 \Leftrightarrow i \text{ E' DISPARI}$

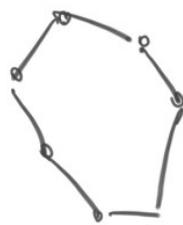
CONDIZIONI NECESSARIE PER ESSERE HAMILTONIANO

Sia $G(V, E)$ hamiltoniano. Allora $\exists \gamma$ circuito hamiltoniano. Fa
 $H(V, E')$ il grafo costituito dai vertici di G e gli archi di γ

- ① SICCOME IN $H(V, E')$ IL GRADO DI OGNI VERTICE E' 2
ALLORA IN $G(V, E)$ DEVE ESSERE: $d(v) \geq 2 \quad \forall v \in V$
- ② SICCOME $K(H) = 2$ ALLORA DEVE ESSERE $K(G) \geq 2$



$G(V, E)$



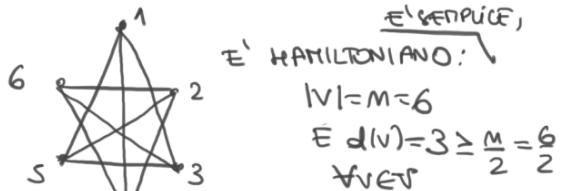
$H(V, E')$

Il teorema di Dirac è un risultato nella teoria dei grafi che fornisce una condizione sufficiente per l'esistenza di un ciclo hamiltoniano in un grafo non orientato. Un ciclo hamiltoniano è un ciclo che passa per ogni vertice del grafo esattamente una volta.

Teorema di Dirac: Se G è un grafo non orientato con almeno 3 vertici in cui il grado di ogni vertice è almeno la metà del numero totale dei vertici (ovvero $d(v) \geq \frac{n}{2}$ per ogni vertice v in G), allora G contiene un ciclo hamiltoniano.

AD ESEMPIO

IL GRAFO



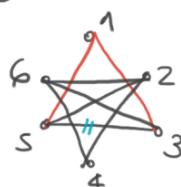
E' SEMPLICE,
E' HAMILTONIANO:

$$|V|=M=6 \\ E d(V)=3 \geq \frac{M}{2} = \frac{6}{2}$$

PER TROVARE UN CIRCUITO HAMILTONIANO...

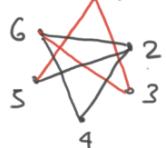


partendo, salvo eccezione, da 1, tolgo un arco.
ad es. 14



partendo a 3
dalo togliere uno
fra 35 e 36
NON POSSONO TENERE 35
anche chiuso in ciclo

Tolgo 36



dalo togliere uno
fra 62 e 64



Attenzione che il teorema di Dirac dà una condizione sufficiente ma non necessaria per essere hamiltoniano. Un percorso è una sequenza di vertici non necessariamente distinti in cui ogni vertice è collegato a quello precedente.

Un percorso è euleriano se:

- È chiuso
- Attraversa esattamente una volta tutti gli archi del grafo (ma i vertici possono comparire più di una volta)

Invece, un grafo è euleriano se contiene un percorso euleriano.

TEOREMA DI EUERIO

$G(V, E)$ è euleriano \Leftrightarrow

$\begin{cases} \text{1} G(V, E) \text{ è connesso} \\ \text{2 OGNI VERTICE HA GRADO PARI} \end{cases}$

Sugli alberi, la seconda caratterizzazione

1. Dato $T(V, E)$ grafo, sono equivalenti:
 - a. $T(V, E)$ è un albero
 - b. $T(V, E)$ è un grafo aciclico e $|E| = |V| - 1$
 - c. $T(V, E)$ è un grafo connesso e $|E| = |V| - 1$

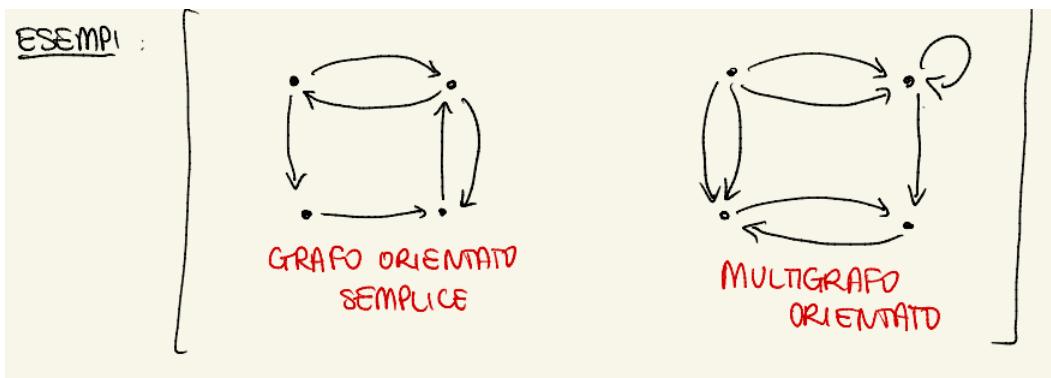
Un grafo orientato è un tipo di grafo in cui gli archi hanno una direzione associata. In altre parole, ogni arco nel grafo orientato collega un "nodo di partenza" a un "nodo di arrivo" e ha una direzione che va dal nodo di partenza al nodo di arrivo. Questa direzione rappresenta un flusso o una relazione unidirezionale tra i nodi.

Nel contesto di un grafo orientato:

- I "nodi" (o "vertici") sono gli elementi fondamentali del grafo, rappresentando entità o punti di interesse.
- Gli "archi orientati" (o "frecce") collegano un nodo di partenza a un nodo di arrivo. Gli archi sono direzionati e indicano una relazione da un nodo all'altro.
- La "direzione" di un arco indica il senso in cui si muove dal nodo di partenza al nodo di arrivo.
- Il "grado di entrata" di un nodo è il numero di archi che entrano nel nodo.
- Il "grado di uscita" di un nodo è il numero di archi che escono dal nodo.
- Una coppia ordinata di vertici è quella con un senso di percorrenza

Inoltre:

- In un multigrafo orientato posso avere archi paralleli (stessa coda e stessa testa) e cappi paralleli
- In un grafo orientato non posso avere cappi o archi paralleli

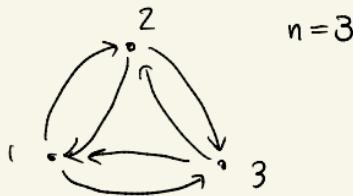


Descriviamo inoltre:

- un cammino orientato come sequenza di vertici distinti dove ogni coppia di vertici consecutivi nel cammino è collegato da un arco orientato;
- la lunghezza del cammino come numero di archi del cammino orientato.
- la nozione di fortemente connesso se per ogni coppia di vertici u e v esiste un cammino orientato da u a v e viceversa

Il numero massimo di archi in un grafo orientato semplice con n vertici è $\frac{n \cdot (n-1)}{2}$

numero
di vertici



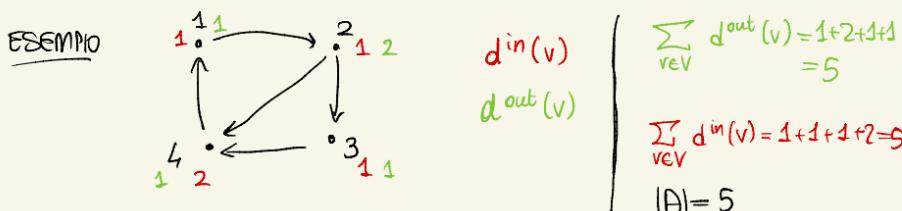
per ogni vertice v ho al massimo $n-1$ archi che "escono" da v (uno verso ognuno degli altri vertici)

$$\xrightarrow{3} \text{massimo } 3 \cdot 2 = 6 \text{ archi}$$

- caso non orientato: $G(V, E)$ con n vertici ha al massimo $\frac{n \cdot (n-1)}{2}$ archi

Inoltre, descriviamo in questo modo i gradi:

- $D(V, A)$ grafo orientato e $v \in V$
- $d^{in}(v) = \text{grado entrante di } v = \frac{\text{numero di archi in } A}{\text{"entranti in } v\text{"}}$
(= con v come testo)
- $d^{out}(v) = \text{grado uscente di } v = \frac{\text{numero di archi}}{\text{"uscenti da } v\text{"}}$
(= con v come codice)



Da questo delineiamo il seguente:

Teorema : $\left\{ \begin{array}{l} \text{Per ogni grafo orientato } D(V, A), \text{ si ha} \\ |A| = \sum_{v \in V} d^{in}(v) = \sum_{v \in V} d^{out}(v) \end{array} \right.$

↑
• ogni arco (u, v) contribuisce 1 a $d^{out}(u)$ e 1 a $d^{in}(v)$

= coppia : $u \underset{\text{arco}}{\sim} v \quad d^{in}(u) = 1 = d^{out}(u)$

Vettori e norme

Dati m numeri reali $a_1, \dots, a_i, \dots, a_m$, si definisce **vettore** (reale) a m componenti (o di ordine m) l'insieme ordinata di tali numeri reali. Un vettore si indica elencando i numeri reali ordinati all'interno di una coppia di parentesi tonde oppure quadre, eventualmente separati da una virgola.

Un vettore può essere scritto come **vettore riga**:

$$(a_1, \dots, a_i, \dots, a_m)$$

oppure come **vettore colonna**:

$$\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix}$$

Possiamo 'dare un nome' al vettore, ad esempio:

$$a_m = (a_1 \dots a_i \dots a_m)$$

L'indice m a pedice indica la **dimensione del vettore**.
Quando non è necessario, tale indice può essere omesso.

Definizione (operazione di trasposizione)

Dato un **vettore riga** a, si definisce **trasposizione di a** l'operazione che trasforma a in **vettore colonna**.

Dato un **vettore colonna** a, si definisce **trasposizione di a** l'operazione che trasforma a in **vettore riga**.

ESEMPIO $a = (1 \ 2 \ 3) \rightarrow a^T = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$

Proprietà

Il risultato di due trasposizioni successive di un vettore a è il vettore a stesso:

$$(a^T)^T = a$$

Definizione (vettore nullo)

Prende il nome di **vettore nullo di ordine m** il vettore di m componenti tutte uguali a 0:

$$(0 \ 0 \ 0 \ \dots \ 0 \ \dots \ 0)$$

Definizione (scalare)

Prende il nome di **scalare** il vettore composto da una singola componente (cioè un vettore di ordine 1).

Definizione (vettore fondamentale)

Prende il nome di **i-mo vettore fondamentale di ordine m** il vettore

$$e^i = (0 \ 0 \ 0 \ \dots \ 0 \underset{\substack{\uparrow \\ \text{componente } i-\text{ma}}}{1} \ 0 \ \dots \ 0)$$

Naturalmente con ciascun vettore possiamo fare una serie di operazioni:

Somma di due vettori

Dati due vettori a m componenti a e b, si definisce il vettore 'somma di a e b':

$$a+b = (a_1+b_1 \ a_2+b_2 \ \dots \ a_i+b_i \ \dots \ a_m+b_m)$$

Prodotto di un vettore per uno scalare

Dato un vettore a con m componenti e uno scalare (numero reale) λ, si definisce il **prodotto dello scalare λ per il vettore a** il vettore seguente:

$$\lambda a = (\lambda a_1 \ \lambda a_2 \ \dots \ \lambda a_i \ \dots \ \lambda a_m)$$

Modulo o norma euclidea di un vettore

Dato il vettore a m componenti a, si definisce **modulo o norma (euclidea) di a** il numero reale:

$$\|a\| = \sqrt{\langle a, a \rangle} \quad \begin{array}{l} \text{Radice quadrata del prodotto scalare} \\ (\text{sempre } \geq 0 \text{ per la proprietà appena vista}) \end{array}$$

ESEMPIO Per il vettore a=(2 5 4 6) si ha:

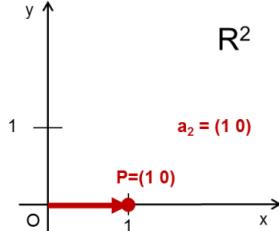
$$\|a\| = \sqrt{\langle a, a \rangle} = \sqrt{2^2 + 5^2 + 4^2 + 6^2} = \sqrt{81} = 9$$

ESEMPIO Per il vettore a=(1 1 1) si ha:

$$\|a\| = \sqrt{\langle a, a \rangle} = \sqrt{1^2 + 1^2 + 1^2} = \sqrt{3}$$

ESEMPIO Per il vettore **fondamentale** a=(1 0) si ha:

$$\|a\| = \sqrt{\langle a, a \rangle} = \sqrt{1^2 + 0^2} = \sqrt{1} = 1$$



La **norma di un vettore** $\vec{u} = (u_1, u_2, \dots, u_n) \in \mathbb{R}^n$ è una applicazione che a un vettore associa un numero reale

$$\|\cdot\| : \mathbb{R}^n \rightarrow \mathbb{R}$$

$$\vec{u} \mapsto \|\vec{u}\|$$

così definito:

$$\|\vec{u}\| = \sqrt{u_1^2 + u_2^2 + \dots + u_n^2}$$

In sostanza, la norma di un vettore si calcola estraendo la **radice quadrata** della somma dei quadrati delle componenti del vettore.

In modo equivalente possiamo esprimere la norma di un vettore in termini di prodotto scalare

$$\|\vec{u}\| = \sqrt{\vec{u} \cdot \vec{u}}$$

infatti

$$\|\vec{u}\| = \sqrt{\vec{u} \cdot \vec{u}} = \sqrt{u_1 u_1 + u_2 u_2 + \dots + u_n u_n} = \sqrt{u_1^2 + u_2^2 + \dots + u_n^2}$$

Distanza euclidea

Consideriamo due vettori a m componenti a e b, e i due punti A e B con coordinate date rispettivamente dalle componenti dei vettori a e b.

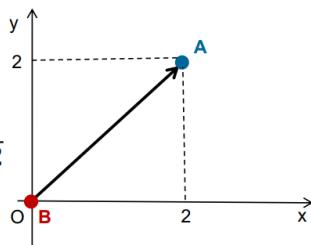
La **distanza euclidea tra i punti A e B** corrisponde alla **norma euclidea del vettore (a-b)**:

$$\|(a - b)\| = \sqrt{\sum_{i=1}^m (a_i - b_i)^2}$$

ESEMPIO 1

Consideriamo a=(2 2) e b=(0 0)

$$\|(a - b)\| = \sqrt{(2 - 0)^2 + (2 - 0)^2} = \sqrt{8} = 2\sqrt{2}$$



Per ogni $\vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^n$ e per ogni $\lambda \in \mathbb{R}$ si può dimostrare che valgono le seguenti proprietà:

1) la norma è definita positiva, cioè restituisce un numero reale non negativo; in formule

$$\|\vec{u}\| \geq 0$$

In particolare, la norma di \vec{u} è zero se e solo se \vec{u} è il vettore nullo

$$\|\vec{u}\| = 0 \iff \vec{u} = \vec{0}$$

2) Proprietà di omogeneità: la norma del prodotto di un vettore per uno scalare è uguale al **valore assoluto** dello scalare per la norma del vettore

$$\|\lambda \vec{u}\| = |\lambda| \|\vec{u}\|$$

3) Disegualanza di Cauchy-Schwarz: il valore assoluto del prodotto scalare tra vettori è minore, o al più uguale, del prodotto delle rispettive norme

$$|\vec{u} \cdot \vec{v}| \leq \|\vec{u}\| \|\vec{v}\|$$

4) Disegualanza triangolare: la norma della somma tra due vettori è minore o uguale della somma delle norme

$$\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$$

5) Disegualanza triangolare inversa: la norma della differenza di due vettori è maggiore o uguale del valore assoluto della differenza delle rispettive norme

$$\|\vec{u} - \vec{v}\| \geq |\|\vec{u}\| - \|\vec{v}\||$$

Grazie al prodotto scalare e alla norma, possiamo quindi definire la nozione di *angolo tra vettori*.

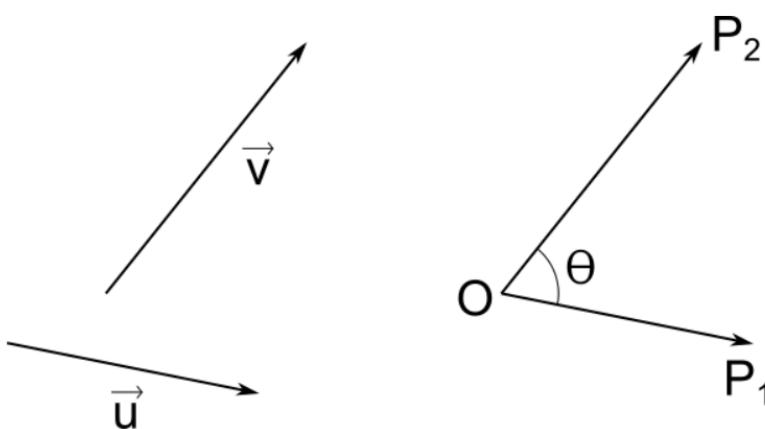
Siano \vec{u} e \vec{v} due vettori non nulli del piano o dello spazio euclideo. Sussiste la relazione

$$\vec{u} \cdot \vec{v} = \|\vec{u}\| \|\vec{v}\| \cos(\theta) \quad \text{con } \theta \in [0, \pi]$$

Da cui

$$\cos(\theta) = \frac{\vec{u} \cdot \vec{v}}{\|\vec{u}\| \|\vec{v}\|}$$

dove θ è l'**angolo convesso** formato dai vettori \vec{u} e \vec{v} .



Angolo tra due vettori

Matrici e tipi

Tabella ordinata di elementi appartenenti allo stesso insieme, i cui elementi sono numeri reali. Le righe orizzontali sono le righe, quelle verticali le colonne.

Generalmente una matrice si indica con una lettera maiuscola e viene scritta nel modo seguente:

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

Ecco spiegato il motivo per cui, poco fa, parlavamo di *tabella ordinata*. Ogni elemento ha una posizione ben precisa e, in generale, con la notazione

$$a_{ij}$$

si indica l'elemento della matrice A che corrisponde all'incrocio tra la riga i -esima e la colonna j -esima.

Il prodotto tra numero di righe e di colonne viene detto dimensione di una matrice.

Inoltre, una matrice di dimensione $m \times n$ viene detta **matrice di tipo (m,n)** , e se i suoi elementi sono numeri reali, si dice che essa appartiene a $\mathbb{R}^{m \times n}$, spesso indicato come $\mathbb{R}^{m,n}$ oppure come $Mat(m, n, \mathbb{R})$.

Più in generale, se gli elementi di una matrice appartengono al campo \mathbb{K} , si scrive $A \in \mathbb{K}^{m,n}$, oppure $A \in \mathbb{K}^{m \times n}$ o, ancora, $A \in Mat(m, n, \mathbb{K})$.

Esistono alcuni tipi di matrici:

Matrice riga: è una matrice di tipo $(1, n)$, ossia è formata da una sola riga, indipendentemente dal numero delle colonne. Le matrici riga vengono usate per riportare le componenti di un **vettore**, motivo per cui vengono anche dette *vettore riga*. Ne sono degli esempi:

$$\begin{pmatrix} -1 & 0 & 2 & 3 \end{pmatrix} \in \mathbb{R}^{1,4} \quad \begin{pmatrix} \frac{1}{3} & 2 \end{pmatrix} \in \mathbb{R}^{1,2}$$

Matrice colonna: è una matrice formata da una sola colonna, ossia del tipo $(m, 1)$ e viene anche detta *vettore colonna*.

$$\begin{pmatrix} -3 \\ 5 \\ 3 \\ 0 \\ 7 \end{pmatrix} \in \mathbb{R}^{5,1} \quad \begin{pmatrix} 6 \\ 2 \\ -5 \end{pmatrix} \in \mathbb{R}^{3,1}$$

Matrice rettangolare: è una matrice in cui il numero delle righe è diverso dal numero delle colonne, cioè con $m \neq n$. Non importa quante esse siano, l'importante è che non siano in ugual numero. Eccone due esempi:

$$\begin{pmatrix} -1 & 0 & 7 \\ 4 & 6 & -2 \end{pmatrix} \in \mathbb{R}^{2,3} \quad \begin{pmatrix} 5 & 8 \\ 3 & -5 \\ 0 & 1 \\ -1 & 3 \end{pmatrix} \in \mathbb{R}^{4,2}$$

Matrice quadrata: è una matrice che ha il numero di righe uguale al numero di colonne ($m = n$), e questo numero prende il nome di *ordine della matrice*.

Ad esempio

$$\begin{pmatrix} -2 & 3 \\ 1 & 1 \end{pmatrix} \in \mathbb{R}^{2,2} \quad \begin{pmatrix} 4 & -1 & 2 \\ 0 & 5 & 0 \\ 1 & 2 & -3 \end{pmatrix} \in \mathbb{R}^{3,3}$$

sono due matrici quadrate, la prima di ordine 2 e la seconda di ordine 3.

In una matrice quadrata, si dice:

- *diagonale principale*, la diagonale che va dall'angolo in alto a sinistra all'angolo in basso a destra;

- *diagonale secondaria* (o *antidiagonale*), la diagonale che va dall'angolo in alto a destra all'angolo in basso a sinistra.

Nella seguente matrice abbiamo indicato in rosso gli elementi della diagonale principale e in blu quelli della diagonale secondaria:

$$\begin{pmatrix} -4 & 9 & 1 \\ 15 & -81 & 7 \\ 5 & 12 & 44 \end{pmatrix} \quad \begin{pmatrix} -4 & 9 & 1 \\ 15 & -81 & 7 \\ 5 & 12 & 44 \end{pmatrix}$$

Matrice antidiagonale: è una matrice quadrata in cui i soli termini della diagonale secondaria possono essere diversi da zero.

$$\begin{pmatrix} 0 & 0 & 7 \\ 0 & 15 & 0 \\ -3 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 & -2 \\ 0 & 0 & 3 & 0 \\ 0 & -4 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Matrice identità: si indica generalmente con Id , Id_n , I o con I_n ed è una matrice diagonale avente tutti 1 sulla diagonale principale e tutti 0 altrove. In simboli:

$$\text{Id}_n \in \mathbb{R}^{n,n}, \forall i, j \in \{1, 2, \dots, n\} : a_{ij} = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$$

Ovviamente non importa quanto valga n , cioè il numero di righe o di colonne di una matrice identità può essere qualsiasi numero naturale non nullo. Eccone alcuni esempi:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Matrice nulla: è una matrice (rettangolare o quadrata) di dimensione qualsiasi, costituita da soli 0 e indicata col simbolo O .

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (0 \ 0 \ 0 \ 0) \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

sono tutte matrici nulle.

Matrice triangolare superiore: è una matrice quadrata avente tutti gli elementi al di sotto della diagonale principale uguali a zero. In formule:

$$A \in \mathbb{R}^{n,n} \text{ triangolare superiore} \iff \forall i, j \in \{1, 2, \dots, n\}, i > j : a_{ij} = 0$$

Per capirne la definizione e avere un esempio di matrice triangolare superiore, scriviamo una matrice 3x3 nella forma generale:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Gli elementi evidenziati in rosso sono quelli in cui l'indice di riga i è maggiore dell'indice di colonna j . Affinché la matrice sia triangolare superiore tali elementi devono essere uguali a zero, quindi, ad esempio, la seguente è una matrice triangolare superiore:

$$\begin{pmatrix} 5 & 7 & 0 \\ 0 & -2 & 11 \\ 0 & 0 & -3 \end{pmatrix}$$

Matrice triangolare inferiore: è una matrice quadrata avente tutti gli elementi al di sopra della diagonale principale uguali a 0. A voi il compito di scrivere la definizione rigorosa e di fare un esempio.
Suggerimento: seguite passo passo quanto visto per la matrice triangolare superiore.

Matrice a scalini: una qualsiasi matrice (quadrata o rettangolare) è detta matrice a scalini o matrice a gradini se il primo elemento diverso da zero della i -esima riga, con $i > 1$, è più a destra del primo elemento diverso da zero della riga precedente. Ad esempio, le matrici:

$$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

sono matrici a scalini, mentre non lo è la matrice

$$\begin{pmatrix} 5 & 0 & 3 & 8 \\ 0 & 2 & 0 & 0 \\ 0 & 9 & 2 & 6 \end{pmatrix}$$

Il primo elemento diverso da zero su ogni riga (quando c'è) è detto **pivot**.

Tramite il [metodo di eliminazione di Gauss](#) (argomento che tratteremo in una delle successive lezioni) è possibile ridurre qualsiasi matrice in una matrice a scalini.

Tramite il [metodo di eliminazione di Gauss](#) (argomento che tratteremo in una delle successive lezioni) è possibile ridurre qualsiasi matrice in una matrice a scalini.

Matrice simmetrica e matrice antisimmetrica: una matrice quadrata di ordine $n > 1$ si dice simmetrica se i suoi elementi sono simmetrici rispetto alla diagonale principale, ossia se per ogni $i, j \in \{1, 2, \dots, n\}$, con $i \neq j$: $a_{ij} = a_{ji}$.

$$\begin{pmatrix} 5 & 0 & 3 \\ 0 & 2 & 9 \\ 3 & 9 & 1 \end{pmatrix}$$

è una matrice simmetrica. Di contro, una matrice quadrata è detta antisimmetrica se $a_{ij} = -a_{ji}$ e ne è un esempio la seguente matrice

$$\begin{pmatrix} 0 & 4 & 1 \\ -4 & 0 & 7 \\ -1 & -7 & 0 \end{pmatrix}$$

Una **matrice hermitiana** è una [matrice](#) che coincide con la trasposta della complessa coniugata a essa associata, mentre una **matrice antihermitiana** è tale che la sua opposta coincide con la trasposta coniugata.

Sia A una matrice quadrata a coefficienti in campo complesso. A si dice **matrice hermitiana** o **matrice autoaggiunta** se coincide con la sua trasposta coniugata.

In altri termini, indicate con \bar{A} la matrice complessa coniugata associata ad A , e con $(\bar{A})^T$ la trasposta della matrice coniugata, abbiamo che

$$A \text{ matrice hermitiana} \iff A = (\bar{A})^T$$

Dunque, per stabilire se una matrice è autoaggiunta basta calcolare sua complessa coniugata, trasporla, e vedere se la matrice così ottenuta coincide con quella iniziale.

Esempio

$$A = \begin{pmatrix} 1 & 3+i \\ 3-i & 2 \end{pmatrix}$$

è una matrice hermitiana, infatti la matrice coniugata è

$$\bar{A} = \begin{pmatrix} 1 & 3-i \\ 3+i & 2 \end{pmatrix}$$

Una matrice quadrata A a coefficienti complessi si dice antihermitiana se la sua opposta $-A$ coincide con la trasposta coniugata, ossia

$$A \text{ matrice antihermitiana} \iff (\bar{A})^T = -A$$

Esempio

$$A = \begin{pmatrix} 3i & 4 \\ -4 & -5i \end{pmatrix}$$

è una matrice antihermitiana, infatti:

la sua opposta è

$$-A = \begin{pmatrix} -3i & -4 \\ 4 & 5i \end{pmatrix}$$

la complessa coniugata di A è

$$\bar{A} = \begin{pmatrix} -3i & 4 \\ -4 & 5i \end{pmatrix}$$

e la sua trasposta

$$(\bar{A})^T = \begin{pmatrix} -3i & 4 \\ -4 & 5i \end{pmatrix}^T = \begin{pmatrix} -3i & -4 \\ 4 & 5i \end{pmatrix}$$

coincide con l'opposta $-A$.

Possiamo inoltre determinare:

1) La matrice A si dice **definita positiva** se il prodotto $\mathbf{x}A\mathbf{x}^T$ è un numero positivo per ogni \mathbf{x} diverso dal vettore nullo.

$$\mathbf{x}A\mathbf{x}^T > 0 \quad \forall \mathbf{x} \in \mathbb{R}^n, \mathbf{x} \neq \mathbf{0}$$

2) Si dice che A è **definita negativa** se il prodotto $\mathbf{x}A\mathbf{x}^T$ è un numero negativo per ogni \mathbf{x} diverso dal vettore nullo.

$$\mathbf{x}A\mathbf{x}^T < 0 \quad \forall \mathbf{x} \in \mathbb{R}^n, \mathbf{x} \neq \mathbf{0}$$

3) Se le precedenti diseguaglianze non sono strette diremo rispettivamente che A è **semidefinita positiva**

$$\mathbf{x}A\mathbf{x}^T \geq 0 \quad \forall \mathbf{x} \in \mathbb{R}^n$$

4) e che A è **semidefinita negativa**

$$\mathbf{x}A\mathbf{x}^T \leq 0 \quad \forall \mathbf{x} \in \mathbb{R}^n$$

5) Infine, se esistono due vettori $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{R}^n$ tali che

$$\mathbf{x}_1 A \mathbf{x}_1^T > 0 \quad \text{e} \quad \mathbf{x}_2 A \mathbf{x}_2^T < 0$$

allora la matrice A è **indefinita**.

La **matrice trasposta** di una matrice assegnata si ottiene scambiandone le righe con le colonne. In altri termini, la trasposta di una matrice è una nuova **matrice** in cui le righe diventano colonne e le colonne diventano righe.

Sia A una generica matrice ad elementi in un campo \mathbb{K} , cioè A può essere una matrice di qualsiasi tipo: rettangolare o quadrata, matrice riga o matrice colonna.

In tutti i casi è sempre possibile trovarne la matrice trasposta. Essa si indica generalmente con A^T e si ottiene scambiando le righe di A con le sue colonne. Ad esempio, la trasposta di

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

è

$$A^T = \begin{pmatrix} 1 & 0 \\ 2 & -1 \\ 3 & 2 \end{pmatrix}$$

Def. 3. Data una matrice $A = [a_{ij}]$, $m \times n$, si chiama **H-trasposta** di A la matrice $n \times m$ $B = [b_{ij}]$ definita da:

$$b_{ij} = \bar{a}_{ji} \quad \text{per ogni } 1 \leq i \leq m, 1 \leq j \leq n.$$

La matrice B si indica con il simbolo A^H .

si indica $B = A^H$

$$\text{ESEMPIO } A = \begin{bmatrix} 1 & 2+3i & 1-i \\ -7i & 0 & 4 \end{bmatrix} \Rightarrow A^H = \overline{A^T} = \begin{bmatrix} \bar{1} & \bar{2+3i} & \bar{1-i} \\ \bar{-7i} & \bar{0} & \bar{4} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -7i & 1+i \\ 2-3i & 0 & 4 \end{bmatrix} =$$

$$(\overline{A})^T = \begin{bmatrix} 1 & 2-3i & 1+i \\ -7i & 0 & 4 \end{bmatrix}^T = \begin{bmatrix} 1 & -7i & 1+i \\ 2-3i & 0 & 4 \end{bmatrix}$$

Normalmente quest'ultima è nota come matrice aggiunta (o trasposta coniugata).

Dato un sistema lineare di n equazioni ed n incognite, del tipo:

$$(*) \left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \dots + a_{mn}x_n = b_m \end{array} \right.$$

la matrice $A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$ si chiama LA MATRICE
DEI COEFFICIENTI
DEL (*)

il vettore $\underline{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} \in \mathbb{C}^m$ si chiama:
IL VETTORE
DEI TERMINI
NON DI (*)

il vettore $\underline{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ si chiama:
IL VETTORE DELLE
INCognITE DI (*)

Denominato anche come scrittura $Ax = b$, detta scrittura matriciale.

Operazioni tra matrici

- Somma di matrici, effettuabile tra matrici dello stesso tipo

Consideriamo due matrici A e B e per fissare le idee supponiamo che i loro elementi siano **numeri reali**. Le due matrici sono sommabili se e solo se sono dello stesso tipo, cioè se hanno lo stesso numero di righe e di colonne. Tale somma si indica con

$$A+B$$

e restituisce una nuova matrice, detta *matrice somma*, avente lo stesso numero di righe e di colonne delle matrici sommate.

2) Svolgere la somma tra

$$A = [-1 \ 8 \ 4 ; 3 \ -2 \ 6 ; 9 \ -5 \ -3] \quad B = [10 \ -2 \ 3 ; 2 \ 1 \ 1 ; -5 \ 2 \ 3]$$

Svolgimento: abbiamo due **matrici quadrate** di ordine 3, quindi possiamo sommarle

$$\begin{aligned} A + B &= \begin{pmatrix} -1 & 8 & 4 \\ 3 & -2 & 6 \\ 9 & -5 & -3 \end{pmatrix} + \begin{pmatrix} 10 & -2 & 3 \\ 2 & 1 & 1 \\ -5 & 2 & 3 \end{pmatrix} = \\ &= \begin{pmatrix} -1 + 10 & 8 + (-2) & 4 + 3 \\ 3 + 2 & -2 + 1 & 6 + 1 \\ 9 + (-5) & -5 + 2 & -3 + 3 \end{pmatrix} = \begin{pmatrix} 9 & 6 & 7 \\ 5 & -1 & 7 \\ 4 & -3 & 0 \end{pmatrix} \end{aligned}$$

Sulla somma valgono:

- La proprietà commutativa
- La proprietà associativa
- L'elemento neutro (somma con matrice nulla)
- Esistenza dell'opposto (matrice opposta)

- Prodotto di una matrice per uno scalare, omonimo il significato, ottenendo come risultato un'altra matrice con la stessa dimensione di quella iniziale, i cui elementi sono ottenuti moltiplicando i termini della matrice per lo scalare presente

Un esempio pratico. In questo esempio moltiplico lo scalare $\alpha=3$ per una matrice A. Il risultato finale è la matrice A con tutti gli elementi moltiplicati per tre.

$$\alpha \cdot A = 3 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 3 \cdot 1 & 3 \cdot 2 \\ 3 \cdot 3 & 3 \cdot 1 \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 6 \\ 9 & 3 \end{pmatrix}$$

WWW.ANDREAMININI.ORG

- Prodotto tra matrici, detto anche moltiplicazione di matrici o riga per colonna, è un prodotto che avviene solo attraverso particolari condizioni. Restituisce una matrice avente tante righe quante quelle della prima matrice e tante colonne quante quelle della seconda

Siano A e B due matrici a elementi in un generico campo \mathbb{K} , quale potrebbe essere il campo \mathbb{R} dei numeri reali o il campo \mathbb{C} dei numeri complessi.

Possiamo eseguire il prodotto tra A e B a patto che il numero delle colonne della matrice A (prima matrice) sia uguale al numero delle righe di B (seconda matrice).

Il prodotto tra le matrici A e B è una nuova matrice, generalmente indicata con AB e detta **matrice prodotto**, avente tante righe quante sono le righe di A e tante colonne quante sono le colonne di B .

Come calcolare il prodotto tra matrici

Prendiamo due matrici

$$A = \underbrace{\begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & -1 \end{pmatrix}}_{(2,3)} \quad B = \underbrace{\begin{pmatrix} 4 & 1 \\ -2 & 2 \\ 0 & 3 \end{pmatrix}}_{(3,2)}$$

e proponiamoci di eseguire il prodotto AB . Possiamo farlo? Certo! Qual è la dimensione della matrice prodotto? In base a quanto scritto in precedenza, essa avrà 2 righe e 2 colonne.

Vediamo ora come si esegue praticamente.

1) Consideriamo la prima riga della matrice A

$$R_1(A) = (1 \ 0 \ 2)$$

e la prima colonna della matrice B

$$C_1(B) = \begin{pmatrix} 4 \\ -2 \\ 0 \end{pmatrix}$$

2) Moltiplichiamo il primo elemento di $R_1(A)$ col primo elemento di $C_1(B)$, il secondo elemento di $R_1(A)$ col secondo elemento di $C_1(B)$, e così via, fino ad esaurire tutti gli elementi della riga di A . Dopodiché sommiamo tra loro i vari prodotti

$$1 \cdot 4 + 0 \cdot (-2) + 2 \cdot 0 = 4 + 0 + 0 = 4$$

Osservate che, allo stesso tempo, si sono esauriti anche gli elementi della colonna di B , e ciò non è un caso. Per poter eseguire il prodotto tra matrici, il numero delle colonne della prima matrice deve coincidere col numero di righe della seconda e ora dovrebbe essere chiaro il motivo per cui è necessaria questa impostazione.

3) L'elemento ottenuto al punto 2) occupa il posto $(1, 1)$ (prima riga, prima colonna) della matrice prodotto.

4) Si ripete il procedimento visto al punto 2) considerando la sempre la prima riga di A

$$R_1(A) = \begin{pmatrix} 1 & 0 & 2 \end{pmatrix}$$

con, questa volta, la seconda colonna di B

$$C_2(B) = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

ottenendo

$$1 \cdot 1 + 0 \cdot 2 + 2 \cdot 3 = 1 + 0 + 6 = 7$$

quello ottenuto è l'elemento di posto $(1, 2)$ (prima riga, seconda colonna) della matrice prodotto.

$$\begin{aligned} B &= \begin{pmatrix} 4 & 1 \\ -2 & 2 \\ 0 & 3 \end{pmatrix} \\ A &= \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & -1 \end{pmatrix} \quad \underbrace{\begin{pmatrix} 4 & 7 \end{pmatrix}}_{AB} \end{aligned}$$

$$AB = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & -1 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ -2 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ p_{21} & p_{22} \end{pmatrix}$$

Ci mancano ancora due elementi della matrice prodotto: p_{21} (seconda riga, prima colonna) e p_{22} (seconda riga, seconda colonna).

L'elemento p_{21} si ottiene dal prodotto tra la seconda riga di A e la prima colonna di B

$$p_{21} = 0 \cdot 4 + 3 \cdot -2 + (-1) \cdot 0 = 0 - 6 + 0 = -6$$

Allo stesso modo, l'elemento p_{22} si calcola svolgendo il prodotto tra la seconda riga di A e la seconda colonna di B

$$p_{22} = 0 \cdot 1 + 3 \cdot 2 + (-1) \cdot 3 = 0 + 6 - 3 = 3$$

Possiamo così concludere che

$$AB = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & -1 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ -2 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ -6 & 3 \end{pmatrix}$$

Esempio di prodotto tra matrici

Calcolare, se possibile, il prodotto tra le matrici

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 5 & -1 \\ 3 & 2 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 7 & 1 \\ 1 & 0 \\ 0 & 4 \end{pmatrix}$$

Svolgimento: la dimensione di A è $(3, 3)$ e quella di B è $(3, 2)$, quindi possiamo calcolare la moltiplicazione tra le due matrici, e la dimensione della matrice prodotto è $(3, 2)$.

$$\begin{aligned} AB &= \begin{pmatrix} 1 & 0 & 1 \\ 1 & 5 & -1 \\ 3 & 2 & 0 \end{pmatrix} \begin{pmatrix} 7 & 1 \\ 1 & 0 \\ 0 & 4 \end{pmatrix} = \\ &= \begin{pmatrix} 1 \cdot 7 + 0 \cdot 1 + 1 \cdot 0 & 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 4 \\ 1 \cdot 7 + 5 \cdot 1 + (-1) \cdot 0 & 1 \cdot 1 + 5 \cdot 0 + (-1) \cdot 4 \\ 3 \cdot 7 + 2 \cdot 1 + 0 \cdot 0 & 3 \cdot 1 + 2 \cdot 0 + 0 \cdot 4 \end{pmatrix} = \begin{pmatrix} 7 & 5 \\ 12 & -3 \\ 23 & 3 \end{pmatrix} \end{aligned}$$

Come detto, per il prodotto:

- Non vale la proprietà commutativa

Tuttavia valgono:

- La proprietà associativa
- La proprietà distributiva
- Elemento neutro
- Moltiplicazione per matrice nulla

Invece:

- Non vale la legge di annullamento del prodotto

Eliminazione di Gauss (MEG) e decomposizione LU

Data una matrice A , l'obiettivo è prenderla e trasformarla in una matrice della forma a gradini (in cui sotto i gradini tutti i numeri sono uguali a 0, ciascun gradino inizia con il numero 1 ed ognuno è alto una riga).

Una **matrice a gradini**, detta anche *matrice a scalini* o *matrice a scala*, è una matrice quadrata o rettangolare in cui il primo elemento non nullo di ogni riga è più a destra del primo elemento non nullo della riga precedente.

In altri termini, $A = (a_{ij}) \in Mat(m, n, \mathbb{K})$ è una **matrice a scala** se nella i -esima riga, con $i > 1$, il primo elemento non nullo si trova in una delle colonne successive alla colonna corrispondente al primo elemento non nullo della riga precedente.

Inoltre, il primo elemento non nullo di ogni riga di una matrice a gradini prende il nome di **pivot**.

Esempi

$$\begin{pmatrix} 2 & 2 \\ 0 & 6 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 2 & 3 & 5 \\ 0 & 0 & 0 & 7 & 4 \\ 0 & 0 & 0 & 0 & 6 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 5 & 7 \\ 0 & 0 & 0 & 8 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 9 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 4 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

sono tutte matrici a scalini, mentre *non* lo sono

$$\begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 & 3 & 5 \\ 0 & 2 & 0 & 7 & 4 \\ 0 & 0 & 0 & 0 & 6 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 5 & 7 \\ 0 & 0 & 6 & 8 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 \\ 9 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 4 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 7 \end{pmatrix}$$

Le colonne che contengono gli inizi di gradini sono le colonne dominanti, invece le altre sono dette colonne libere. L'algoritmo è di natura iterativa e consiste nel:

- Sommare alla i -esima riga di A la j -esima riga di A moltiplicato per uno scalare C
- Moltiplicare la i -esima riga di A per uno scalare $C \neq 0$
- Scambiare la i -esima riga con la j -esima riga di A (sostituire una riga della matrice con quella ottenuta sommando ad essa un multiplo di un'altra riga)

Nello specifico, l'algoritmo si compone di questi passi:

1. Riduzione a forma triangolare superiore: L'obiettivo principale dell'algoritmo di Gauss è trasformare la matrice dei coefficienti in una forma detta "triangolare superiore", in cui tutti gli elementi sotto la diagonale principale sono zero.
2. Sostituzione all'indietro: Dopo aver ottenuto la forma triangolare superiore, si risolvono le variabili partendo dall'ultima equazione e risalendo, sostituendo i valori delle variabili già trovati nelle equazioni precedenti.

ESEMPIO Trovare una forma ridotta di Gauss per

$$A = \begin{bmatrix} 2 & -4 & 14 \\ 1 & 3 & 2 \\ -1 & 0 & -5 \end{bmatrix} \xrightarrow{E_1(\frac{1}{2})} \begin{bmatrix} 1 & -2 & 7 \\ 1 & 3 & 2 \\ -1 & 0 & -5 \end{bmatrix}$$

$$\xrightarrow{} \begin{bmatrix} 1 & -2 & 7 \\ 1 & 3 & 2 \\ -1 & 0 & -5 \end{bmatrix} \xrightarrow{E_{21}(-1)} \begin{bmatrix} 1 & -2 & 7 \\ 0 & 5 & -5 \\ -1 & 0 & -5 \end{bmatrix} \xrightarrow{E_{31}(1)}$$

$$\xrightarrow{} \begin{bmatrix} 1 & -2 & 7 \\ 0 & 5 & -5 \\ 0 & -2 & 2 \end{bmatrix} \xrightarrow{E_2(\frac{1}{5})} \begin{bmatrix} 1 & -2 & 7 \\ 0 & 1 & -1 \\ 0 & -2 & 2 \end{bmatrix}$$

$$\xrightarrow{} \begin{bmatrix} 1 & -2 & 7 \\ 0 & 1 & -1 \\ 0 & -2 & 2 \end{bmatrix} \xrightarrow{E_{32}(2)} \begin{bmatrix} 1 & -2 & 7 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix} = U$$

↑
↑
colonne
dominanti d'U

le 3^a colone
e' libere

U è una forma ridotta di Gauss per A

“Riassumendo” raggruppa le operazioni necessarie

“a sistemare” ogni colonna dominante

$$A = \begin{bmatrix} 2 & -4 & 14 \\ 1 & 3 & 2 \\ -1 & 0 & -5 \end{bmatrix} \xrightarrow{E_{31}(1) E_{21}(-1) E_1(\frac{1}{2})} \begin{bmatrix} 1 & -2 & 7 \\ 0 & 5 & -5 \\ 0 & -2 & 2 \end{bmatrix}$$

$$\xrightarrow{E_{32}(2) E_2(\frac{1}{5})} \begin{bmatrix} 1 & -2 & 7 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix} = U$$

Risolvere il sistema lineare $\mathbf{Ax} = \mathbf{b}$ nei tre seguenti casi:

$$(a) : \mathbf{A} = \begin{pmatrix} 2 & 2 & 4 \\ 1 & 1 & 3 \\ 3 & 3 & 7 \end{pmatrix} \text{ e } \mathbf{b} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix};$$

$$(b) : \mathbf{A} = \begin{pmatrix} 1 & 3 & -2 & 1 \\ 0 & 0 & 2 & 4 \\ 2 & 6 & -3 & 4 \end{pmatrix} \text{ e } \mathbf{b} = \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix};$$

$$(c) : \mathbf{A} = \begin{pmatrix} 4 & 8 & 4 \\ 0 & 0 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 1 \end{pmatrix} \text{ e } \mathbf{b} = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}.$$

(a) Troviamo una forma ridotta di Gauss della matrice aumentata del sistema:

$$\begin{aligned} (\mathbf{A} \quad | \quad \mathbf{b}) &= \left(\begin{array}{ccc|c} 2 & 2 & 4 & 0 \\ 1 & 1 & 3 & -1 \\ 3 & 3 & 7 & 0 \end{array} \right) \xrightarrow{E_{31}(-3)E_{21}(-1)E_1(\frac{1}{2})} \left(\begin{array}{ccc|c} 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{array} \right) \rightarrow \\ &\xrightarrow{E_{32}(-1)} \left(\begin{array}{ccc|c} 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{array} \right) = (\mathbf{U} \quad | \quad \mathbf{d}) \end{aligned}$$

Poichè \mathbf{d} è dominante, allora $\mathbf{Ux} = \mathbf{d}$, e quindi anche $\mathbf{Ax} = \mathbf{b}$, non ha soluzioni.

(Infatti: il sistema $\mathbf{Ax} = \mathbf{b}$ è equivalente al sistema $\mathbf{Ux} = \mathbf{d}$, che è una scrittura compatta per

$$(*) \quad \begin{cases} x_1 + x_2 + 2x_3 = 0 \\ x_3 = -1, \\ 0 = 1 \end{cases}$$

e poichè l'ultima equazione di (*) non ha soluzioni, (*) non ha soluzioni).

(b) Troviamo una forma ridotta di Gauss della matrice aumentata del sistema:

$$(\mathbf{A} \mid \mathbf{b}) = \left(\begin{array}{cccc|c} 1 & 3 & -2 & 1 & -1 \\ 0 & 0 & 2 & 4 & 2 \\ 2 & 6 & -3 & 4 & -1 \end{array} \right) \xrightarrow{E_{31}(-2)} \left(\begin{array}{cccc|c} 1 & 3 & -2 & 1 & -1 \\ 0 & 0 & 2 & 4 & 2 \\ 0 & 0 & 1 & 2 & 1 \end{array} \right) \rightarrow$$

$$\xrightarrow{E_{32}(-1)E_2(\frac{1}{2})} \left(\begin{array}{cccc|c} 1 & 3 & -2 & 1 & -1 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) = (\mathbf{U} \mid \mathbf{d}).$$

Il sistema $\mathbf{Ax} = \mathbf{b}$ è equivalente al sistema $\mathbf{Ux} = \mathbf{d}$, che è una scrittura compatta per

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

Poichè \mathbf{d} è libera, $\mathbf{Ux} = \mathbf{d}$ ammette soluzioni.

Poichè \mathbf{U} ha esattamente due colonne libere (la 2^a e la 4^a), $\mathbf{Ux} = \mathbf{d}$ ha ∞^2 soluzioni.

Scegliamo come parametri le variabili corrispondenti alle colonne libere di \mathbf{U} e con la sostituzione all'indietro otteniamo:

$$\begin{cases} x_2 = h \\ x_4 = k \\ x_3 = -2x_4 + 1 = -2k + 1 \\ x_1 = -3x_2 + 2x_3 - x_4 - 1 = -3h + 2 \times (-2k + 1) - k - 1 = -3h - 5k + 1 \end{cases}$$

Dunque l'insieme delle soluzioni di $\mathbf{Ux} = \mathbf{d}$, e quindi anche $\mathbf{Ax} = \mathbf{b}$ è

$$\left\{ \begin{pmatrix} -3h - 5k + 1 \\ h \\ -2k + 1 \\ k \end{pmatrix} \mid h, k \in \mathbb{C} \right\}.$$

(c) Troviamo una forma ridotta di Gauss della matrice aumentata del sistema:

$$(\mathbf{A} \mid \mathbf{b}) = \left(\begin{array}{ccc|c} 4 & 8 & 4 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 3 & 2 & 0 \\ 1 & 2 & 1 & 0 \end{array} \right) \xrightarrow{E_{41}(-1)E_{31}(-1)E_1(\frac{1}{4})} \left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right) \rightarrow$$

$$\xrightarrow{E_{23}} \left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{array} \right) = (\mathbf{U} \mid \mathbf{d})$$

Il sistema $\mathbf{Ax} = \mathbf{b}$ è equivalente al sistema $\mathbf{Ux} = \mathbf{d}$, che è una scrittura compatta per

$$\begin{cases} x_1 + 2x_2 + x_3 = 0 \\ x_2 + x_3 = 0 \\ x_3 = 2 \end{cases}$$

Poichè \mathbf{d} è libera, $\mathbf{Ux} = \mathbf{d}$ ammette soluzioni.

Poichè \mathbf{U} non ha colonne libere, $\mathbf{Ux} = \mathbf{d}$ ha esattamente una soluzione.

Con la sostituzione all'indietro otteniamo:

$$\begin{cases} x_3 = 2 \\ x_2 = -x_3 = -2 \\ x_1 = -2x_2 - x_3 = -2 \times (-2) - 2 = 4 - 2 = 2 \end{cases}$$

Dunque l'unica soluzione di $\mathbf{Ux} = \mathbf{d}$, e quindi anche di $\mathbf{Ax} = \mathbf{b}$, è il vettore

$$\mathbf{v} = \begin{pmatrix} 2 \\ -2 \\ 2 \end{pmatrix}.$$

Il risultato è sempre una matrice aumentata è un concetto utilizzato in algebra lineare per rappresentare sistemi di equazioni lineari. È una combinazione di una matrice dei coefficienti e un vettore colonna dei termini noti di un sistema di equazioni lineari.

Esiste una forma estesa dell'algoritmo presentato definita algoritmo di Gauss-Jordan, la quale Dopo aver ridotto la matrice a scalini, si applica in senso inverso, cioè dal basso verso l'alto, per ottenere una matrice che in ogni colonna contenente un pivot abbia solo il pivot come numero non nullo, (questa matrice risultante è anche detta matrice a scalini in forma ridotta): basta usare ogni riga, partendo dall'ultima, per eliminare tutte le cifre diverse da zero che stanno sopra al pivot di questa riga. Infine, sempre con mosse di Gauss (moltiplicando righe), si può ottenere che ogni pivot abbia valore 1.

Concretamente si compone di questi passi:

1. Riduzione a forma diagonale: L'obiettivo dell'algoritmo di Gauss-Jordan è trasformare la matrice dei coefficienti in una forma detta "diagonale", in cui gli elementi sia sopra che sotto la diagonale principale sono zero.
2. Operazioni aggiuntive: Dopo aver ottenuto la forma diagonale, si continua ulteriormente applicando operazioni di riga per ottenere la matrice identità sulla parte sinistra (matrice dei coefficienti) della matrice aumentata.

Algoritmo di Gauss-Jordan

Passo 1

Si esegue l'**algoritmo di Gauss** per trasformare la matrice A in una matrice a scala equivalente per righe.

Passo 2

Si moltiplica ogni riga per un opportuno scalare tale da rendere ogni pivot uguale ad 1.

Passo 3

Si considerano le righe non nulle e, a partire dall'ultima, si annullano gli elementi di ogni colonna contenente un pivot e che sono al di sopra del pivot stesso. Questo risultato si ottiene sommando alle varie righe opportuni multipli della riga in esame contenete il pivot.

Esempio

Si vuole ridurre a scala con l'algoritmo di Gauss-Jordan la seguente matrice:

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

La matrice è non nulla e per il passo 1 dell'**algoritmo di Gauss** quindi si può proseguire. La matrice ha più di una riga e dunque si considera il procedimento esposto nel passo 2. La colonna non nulla con indice più basso è la prima ed il suo pivot è 2. L'indice di riga corrispondente è 1. Bisogna allora moltiplicare la riga per 1/2, ottenendo:

$$\begin{pmatrix} 1 & \frac{1}{2} & 0 & 2 \\ 1 & -1 & 1 & 0 \\ 2 & 1 & -1 & 1 \end{pmatrix}$$

A questo punto vanno annullati tutti gli elementi nella prima colonna, sommando multipli della prima ottenendo:

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

Va ora considerata la matrice schermata:

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

La matrice schermata possiede due righe non nulle e la colonna non nulla con indice più basso è la seconda ed il pivot è $-3/2$. Ancora una volta non occorrono scambi, poiché il pivot è nella prima riga. Tale riga va moltiplicata per $-2/3$ e si ottiene:

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

Moltiplicando la terza riga per -1 si ottiene:

$$(0 \ 0 \ 1 \ 3)$$

Partendo dal basso, si annullano ora tutti gli elementi sovrastanti il pivot di ogni riga nella propria colonna. Va dunque considerata la matrice:

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

Alla seconda riga va sommata la terza moltiplicata per $2/3$, ottenendo:

$$\begin{pmatrix} 1 & 0 & 0 & \frac{1}{3} \\ 0 & 1 & 0 & \frac{10}{3} \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

Infine, la prima riga va sommata alla seconda moltiplicata per $-1/2$:

$$\boxed{\begin{pmatrix} 1 & 0 & 0 & \frac{1}{3} \\ 0 & 1 & 0 & \frac{10}{3} \\ 0 & 0 & 1 & 3 \end{pmatrix}}$$

Per parlare della decomposizione LU, necessario introdurre il concetto di matrice di permutazione.

Definizione (Matrice di permutazione)

*Una matrice P si dice di **permutazione** se si ottiene permutando le righe della matrice identica I .*

Esempio

In questo esempio, P è ottenuta da I scambiando la prima riga con la seconda.

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Rinfrescando inoltre i concetti di matrici triangolari:

Definizione (Matrici triangolari)

Una matrice $A = (a_{ij})$ si dice

- **triangolare superiore**, se $a_{ij} = 0$ per $i > j$;
- **triangolare inferiore**, se $a_{ij} = 0$ per $i < j$.

```
>> A=[1 2 3; 4 5 6; 7 8 9]
A =
    1      2      3
    4      5      6
    7      8      9
>> L=tril(A) % TRIANGOLARE INFERIORE
L =
    1      0      0
    4      5      0
    7      8      9
>> U=triu(A) % TRIANGOLARE SUPERIORE
U =
    1      2      3
    0      5      6
    0      0      9
>>
```

La decomposizione LU (Lower-Upper) è una tecnica comune nell'ambito dell'algebra lineare e delle matrici, utilizzata per scomporre una matrice quadrata in due matrici: una matrice triangolare inferiore (L) e una matrice triangolare superiore (U). Questa scomposizione è particolarmente utile per risolvere sistemi di equazioni lineari e calcolare l'inversa di una matrice.

Sia $A \in \mathbb{R}^{n \times n}$. Determinare, se esistono,

- $L = l_{i,j}$ triangolare inferiore con elementi diagonali uguali a 1, cioè $l_{i,i} = 1$,
- U triangolare superiore,

cosicché

$$A = LU.$$

Questa scomposizione ha numerose applicazioni pratiche:

1. **Risoluzione di sistemi di equazioni lineari:** Una volta ottenute le matrici L e U dalla decomposizione, è più semplice risolvere un sistema di equazioni lineari $Ax = b$ suddividendo il processo in due parti: risolvere $Ly = b$ per y , e quindi risolvere $Ux = y$ per x .
2. **Calcolo dell'inversa di una matrice:** Se hai la decomposizione LU di una matrice A , puoi utilizzare questa scomposizione per calcolare l'inversa di A in modo più efficiente risolvendo sistemi di equazioni lineari associati.
3. **Determinante di una matrice:** Il determinante di una matrice può essere calcolato come il prodotto dei termini diagonali di U , poiché L ha 1 sulla diagonale.
4. **Risolvere equazioni differenziali e analisi numerica:** La decomposizione LU è anche utile in diversi contesti avanzati, come la soluzione numerica di equazioni differenziali e la risoluzione di problemi di analisi numerica.

Teorema (Fattorizzazione LU e submatrici principali)

- Sia $A \in \mathbb{R}^{n \times n}$.
- Si supponga che tutte le sottomatrici principali di testa $A^{(k)} = (a_{i,j})_{i,j=1,\dots,k}$, $k = 1, \dots, n-1$ siano non singolari.

Allora esiste ed è unica la fattorizzazione LU di A.

Nota. (Controesempio)

Non tutte le matrici posseggono la fattorizzazione LU. Un esempio in cui non esistono tali L, U per cui $A = LU$ è la matrice

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

Teorema (Fattorizzazione PA=LU)

Sia $A \in \mathbb{R}^{n \times n}$. Allora esiste una matrice di permutazione P tale che $PA = LU$.

Di conseguenza

- La fattorizzazione $A = LU$ non è sempre possibile.
- La fattorizzazione $PA = LU$ è sempre possibile.

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 8 & 6 \\ 6 & 7 & 10 \end{bmatrix}$$

Calcolo della Matrice L e Matrice U:

Applichiamo l'algoritmo di decomposizione LU per ottenere le matrici L e U. Iniziamo con la matrice A e cerchiamo di ottenere una forma triangolare superiore per U e una forma triangolare inferiore con 1 sulla diagonale per L.

Per ottenere una forma triangolare superiore da una matrice, devi eseguire una serie di operazioni di riga chiamate "eliminazione gaussiana". L'obiettivo dell'eliminazione gaussiana è trasformare la matrice in una forma in cui tutti gli elementi sotto la diagonale principale sono zero, creando così una forma triangolare superiore.

Ecco i passaggi generali per ottenere una forma triangolare superiore:

1. **Scegli una riga pivot:** Inizia scegliendo una riga (o colonna) pivot. L'elemento pivot è l'elemento principale sulla diagonale che userai come base per eliminare gli elementi sotto di esso.
2. **Riduci gli elementi sotto il pivot a zero:** Utilizza operazioni di riga per rendere zero gli elementi sotto il pivot. Per fare ciò, moltiplica la riga pivot per un opportuno coefficiente e sottrai questa riga dalle altre righe in modo da ottenere zeri sotto l'elemento pivot.
3. **Scegli un nuovo pivot:** Una volta completata l'eliminazione nella colonna corrente, passa alla colonna successiva e ripeti i passaggi 1 e 2 per ottenere zeri sotto il nuovo pivot.
4. **Ripeti:** Continua questo processo finché non hai ottenuto zeri sotto tutti gli elementi della diagonale principale.

A seguire un esempio semplificato per mostrarti come ottenere una forma triangolare superiore da una matrice:

Considera la matrice:

$$A = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 3 \\ 3 & 5 & 6 \end{bmatrix}$$

1. Scegliamo la prima riga come pivot. Dividiamo la prima riga per 2 (il pivot) per semplificare i calcoli:

$$A = \begin{bmatrix} 1 & \frac{3}{2} & 2 \\ 1 & 2 & 3 \\ 3 & 5 & 6 \end{bmatrix}$$

1. Sottraiamo la prima riga dalla seconda riga e 3 volte la prima riga dalla terza riga per ottenere zeri sotto il pivot:

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

1. Scegliamo la seconda riga come nuovo pivot. Moltiplichiamo la seconda riga per 2 (il pivot) per semplificare i calcoli:

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

1. Sottraiamo la seconda riga dalla terza riga per ottenere uno zero sotto il pivot:

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

Ora abbiamo ottenuto una forma triangolare superiore dalla matrice iniziale.

Determinanti e matrici inverse

Il **determinante di una matrice** è un numero associato a ciascuna matrice quadrata avente ordine (numero di righe o colonne) $n \geq 1$, indicato con $\det |A|$.

Il **determinante di una matrice quadrata di ordine 2** è dato dal prodotto degli elementi della diagonale principale meno il prodotto degli elementi dell'antidiagonale.

Dunque, se abbiamo una matrice 2×2 possiamo calcolarne il determinante con la formula

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a \cdot d) - (b \cdot c)$$

Esempi sul determinante di una matrice di ordine 2

Calcolare il determinante delle matrici

$$A = \begin{pmatrix} 1 & 3 \\ 4 & 5 \end{pmatrix} \quad B = \begin{pmatrix} 6 & 12 \\ 3 & 6 \end{pmatrix} \quad C = \begin{pmatrix} -2 & 5 \\ 0 & -1 \end{pmatrix}$$

Svolgimento: applichiamo la formula per il calcolo del determinante a ciascuna matrice

$$\det(A) = \det \begin{pmatrix} 1 & 3 \\ 4 & 5 \end{pmatrix} = (1 \cdot 5) - (3 \cdot 4) = 5 - 12 = -7$$

$$\det(B) = \det \begin{pmatrix} 6 & 12 \\ 3 & 6 \end{pmatrix} = (6 \cdot 6) - (12 \cdot 3) = 36 - 36 = 0$$

$$\det(C) = \det \begin{pmatrix} -2 & 5 \\ 0 & -1 \end{pmatrix} = (-2 \cdot (-1)) - (5 \cdot 0) = 2 - 0 = 2$$

A $m \times m$

$$m=2: \quad \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = [a_{11} \ a_{12}] \begin{bmatrix} A_{11} \\ A_{12} \end{bmatrix} = a_{11} A_{11} + a_{12} A_{12}$$

$$a_{11} a_{22} - a_{12} a_{21}$$

$$A_{ij} = (-1)^{i+j} \det C_{ij}$$

A_{ij} = COFATTORE DI POSIZIONE (i,j) DELLA MATRICE

Determinante di matrici 3x3 - regola di Sarrus

Per calcolare il determinante di una matrice quadrata di ordine 3 possiamo applicare la **regola di Sarrus**, secondo cui:

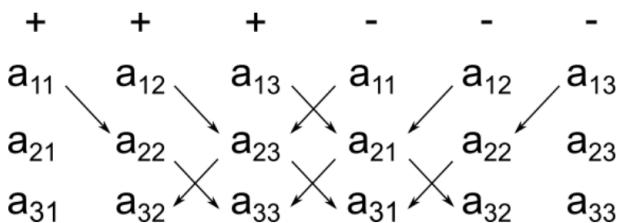
$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - (a_{13} \cdot a_{22} \cdot a_{31} + a_{12} \cdot a_{21} \cdot a_{33} + a_{11} \cdot a_{23} \cdot a_{32})$$

Ricordarla a memoria sarebbe quasi impossibile. Per fortuna c'è un modo comodo che permette di ricavarla: basta riscrivere la matrice accostando la matrice stessa sulla sua destra

$$\begin{array}{cccccc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} & a_{33} \end{array}$$

per poi:

- 1) sommare i prodotti lungo le prime tre diagonali complete da sinistra verso destra;
- 2) sommare i prodotti lungo le ultime tre antidiagonali complete percorse da destra verso sinistra;
- 3) calcolare la differenza tra i risultati ottenuti ai punti 1) e 2).



Determinante di matrici 3x3 con la regola di Sarrus

$$\text{Det } \begin{pmatrix} 3 & -2 & 1 \\ 0 & 1 & 4 \\ 2 & 6 & 3 \end{pmatrix} = [3 \quad -2 \quad 1] \begin{bmatrix} A_{11} \\ A_{12} \\ A_{13} \end{bmatrix} = 3A_{11} - 2A_{12} + A_{13}$$

$$A_{11} = (-1)^{1+1} \det \begin{pmatrix} 1 & 4 \\ 6 & 3 \end{pmatrix} = 1 \cdot 3 - 4 \cdot 6 = 3 - 24 = -21$$

$$A_{12} = (-1)^{1+2} \det \begin{pmatrix} 0 & 4 \\ 2 & 3 \end{pmatrix} = -[0 \cdot 3 - 4 \cdot 2] = -(-8) = 8$$

$$A_{13} = (-1)^{1+3} \det \begin{pmatrix} 0 & 1 \\ 2 & 6 \end{pmatrix} = 0 \cdot 6 - 1 \cdot 2 = -2$$

$$\Rightarrow = 3 \cdot (-21) - 2 \cdot 8 - 2 = -63 - 16 - 2 = -81$$

Applicando la regola di Sarrus calcolare il determinante della matrice

$$A = \begin{pmatrix} 2 & -1 & 4 \\ 1 & 2 & 0 \\ 3 & 5 & 1 \end{pmatrix}$$

Svolgimento: scriviamo due matrici l'una accanto all'altra e senza parentesi e tracciamo le tre diagonali complete procedendo da sinistra verso destra e le tre antidiagonali procedendo da destra verso sinistra.

$$\begin{matrix} 2 & -1 & 4 & 2 & -1 & 4 \\ 1 & 2 & 0 & 1 & 2 & 0 \\ 3 & 5 & 1 & 3 & 5 & 1 \end{matrix}$$

Sommiamo i prodotti lungo le prime tre diagonali principali

$$(2 \cdot 2 \cdot 1) + (-1 \cdot 0 \cdot 3) + (4 \cdot 1 \cdot 5) = 4 + 0 + 20 = 24$$

e quelli lungo le ultime tre antidiagonali

$$(4 \cdot 2 \cdot 3) + (-1 \cdot 1 \cdot 1) + (2 \cdot 0 \cdot 5) = 24 - 1 + 0 = 23$$

Sottraendo, nell'ordine, i due risultati otteniamo

$$\det(A) = 24 - 23 = 1$$

Dopo aver fatto un po' di pratica possiamo svolgere i calcoli in un'unica formula:

$$\begin{aligned} \det(A) &= (2 \cdot 2 \cdot 1) + (-1 \cdot 0 \cdot 3) + (4 \cdot 1 \cdot 5) - [(4 \cdot 2 \cdot 3) + (-1 \cdot 1 \cdot 1) + (2 \cdot 0 \cdot 5)] = \\ &= 4 + 0 + 20 - (24 - 1 + 0) = 24 - 23 = 1 \end{aligned}$$

Più generale e più utile è il teorema di Laplace.

Il **teorema di Laplace** permette di calcolare il determinante di una matrice quadrata attraverso formule ricorsive, dette *sviluppi di Laplace*, che possono essere applicate per righe o per colonne, e che si possono applicare a matrici quadrate di ordine qualsiasi (anche a matrici 2x2 o 3x3).

Consideriamo una matrice quadrata di ordine n

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

e denotiamo con A_{ij} la matrice che si ottiene eliminando la riga i e la colonna j della matrice A , e con $\det(A_{ij})$ il suo determinante.

Fissato un qualsiasi elemento $a_{ij} \in A$, chiamiamo **complemento algebrico** (o cofattore) di a_{ij} il numero:

$$(-1)^{i+j} \cdot \det(A_{ij})$$

FORMULA DEL DETERMINANTE (Sviluppo di LAPLACE)

RISPECTO ALLA 1^a RIGA:

se $A = (a_{ij})$ $m \times n$ alline

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{bmatrix}$$

$$\det A = [a_{11} \ a_{12} \ \dots \ a_{1m}] \begin{bmatrix} A_{11} \\ A_{12} \\ \vdots \\ A_{1m} \end{bmatrix} = a_{11} A_{11} + a_{12} A_{12} + \dots + a_{1m} A_{1m}$$

$$\text{per } m=4 \quad \det \begin{pmatrix} 1 & -5 & 0 & 3 \\ 6 & 2 & 0 & 4 \\ -2 & 0 & 0 & 2 \\ -1 & 7 & 5 & 1 \end{pmatrix} = (1 \ -5 \ 0 \ 3) \begin{bmatrix} A_{11} \\ A_{12} \\ A_{13} \\ A_{14} \end{bmatrix}$$

$$= A_{11} - 5A_{12} + 0 \cdot \cancel{A_{13}} + 3A_{14}$$

$$\det \begin{pmatrix} 1 & -5 & 0 & 3 \\ 6 & 2 & 0 & 4 \\ -2 & 0 & 0 & 2 \\ -1 & 7 & 5 & 1 \end{pmatrix} = A_{11} - 5A_{12} + 3A_{14}$$

$$= -20 - 5 \cdot 100 + 3 \cdot (-20)$$

$$= -20 - 500 - 60 = -580$$

$$A_{11} = (-1)^{1+1} \det \begin{pmatrix} 2 & 0 & 4 \\ 0 & 0 & 2 \\ 7 & 5 & 1 \end{pmatrix} = [2 \ 0 \ 4] \begin{bmatrix} B_{11} \\ B_{12} \\ B_{13} \end{bmatrix} =$$

$$= 2B_{11} + 0 \cdot \cancel{B_{12}} + 4B_{13} = 2 \cdot (-1)^{1+1} \det \begin{pmatrix} 0 & 2 \\ 5 & 1 \end{pmatrix} +$$

$$+ 4 \cdot (-1)^{1+3} \det \begin{pmatrix} 0 & 0 \\ 7 & 5 \end{pmatrix} = 2(0 \cdot 1 - 2 \cdot 5) + 4(0 \cdot 5 - 0 \cdot 7)$$

$$= 2 \cdot (-10) = -20$$

$$A = \begin{pmatrix} 1 & -5 & 0 & 3 \\ 6 & 2 & 0 & 4 \\ -2 & 0 & 0 & 2 \\ -1 & 7 & 5 & 1 \end{pmatrix}$$

$$A_{12} = (-1)^{1+2} \det \begin{pmatrix} 6 & 0 & 4 \\ -2 & 0 & 2 \\ -1 & 5 & 1 \end{pmatrix} = - \left[6B_{11} + 0 \cdot \cancel{B_{12}} + 4B_{13} \right]$$

$$= - \left[6(-1)^{1+1} \det \begin{pmatrix} 0 & 2 \\ 5 & 1 \end{pmatrix} + 4(-1)^{1+3} \det \begin{pmatrix} -2 & 0 \\ -1 & 5 \end{pmatrix} \right]$$

$$= - \left[6(0 \cdot 1 - 2 \cdot 5) + 4(-2 \cdot 5 - 0 \cdot (-1)) \right]$$

$$= - \left[6 \cdot (-10) + 4 \cdot (-10) \right] = -20 \cdot (-10) = 200$$

$$A = \begin{pmatrix} 1 & -5 & 0 & 3 \\ 6 & 2 & 0 & 4 \\ -2 & 0 & 0 & 2 \\ -1 & 7 & 5 & 1 \end{pmatrix}$$

$$\begin{aligned}
 A_{14} &= (-1)^{1+4} \det \begin{pmatrix} 6 & 2 & 0 \\ -2 & 0 & 0 \\ -1 & 7 & 5 \end{pmatrix} = \\
 &= - \left[6B_{11} + 2B_{12} + 0 \cancel{B_{13}} \right] = - \left[6(-1)^{1+1} \det \begin{pmatrix} 0 & 0 \\ 7 & 5 \end{pmatrix} + \right. \\
 &\quad \left. + 2(-1)^{1+2} \det \begin{pmatrix} -2 & 0 \\ -1 & 5 \end{pmatrix} \right] = - \left[6(0 \cdot 5 - 0 \cdot 7) + 2 \cdot (-1) \right. \\
 &\quad \left. \cdot (-2 \cdot 5 - 0 \cdot (-1)) \right] = - \left[-2 \cdot (-10) \right] = -20
 \end{aligned}$$

Sviluppo di Laplace per righe

Fissata una qualsiasi riga della matrice A , il determinante di A è pari alla somma dei prodotti degli elementi della riga scelta per i rispettivi complementi algebrici. In formule:

$$\det(A) = \sum_{j=1}^n [a_{ij} \cdot (-1)^{i+j} \cdot \det(A_{ij})]$$

(ci si muove lungo la i -esima riga).

Sviluppo di Laplace per colonne

Fissata una qualsiasi colonna di A , il suo determinante è uguale alla somma dei prodotti degli elementi della colonna fissata per i rispettivi complementi algebrici. In formule:

$$\det(A) = \sum_{i=1}^n [a_{ij} \cdot (-1)^{i+j} \cdot \det(A_{ij})]$$

(ci si muove lungo la j -esima colonna).

In base a cosa possiamo scegliere lo sviluppo per righe o per colonne? La regola è semplice e si basa su un principio di convenienza: usiamo il metodo che ci permette di risparmiare calcoli. Si tratta quindi di **scegliere la riga o la colonna della matrice contenente più zeri**, perché così facendo avremo il minor numero possibile di addendi nella formula scelta tra le precedenti. Risparmiare un addendo, d'altra parte, non è cosa da poco: ognuno di essi contiene a sua volta un determinante.

Proponiamoci di calcolare il determinante della seguente matrice con Laplace

$$A = \begin{pmatrix} 1 & 0 & 5 \\ 2 & -1 & 0 \\ 7 & -2 & 0 \end{pmatrix}$$

Svolgimento: tra tutte le colonne e tutte le righe di A vediamo subito che la terza colonna contiene due zeri, quindi decidiamo di calcolare il determinante con uno sviluppo per colonna, scegliendone la terza. Procediamo!

Dobbiamo sommare i prodotti degli elementi della terza colonna per i rispettivi complementi algebrici. Se un elemento è 0, il prodotto per il suo complemento algebrico dà 0, quindi basta considerare solo gli elementi non nulli cioè

$$a_{13} = 5$$

il cui complemento algebrico è

$$\begin{aligned} (-1)^{1+3} \cdot \det(A_{13}) &= (-1)^4 \cdot \det \begin{pmatrix} 2 & -1 \\ 7 & -2 \end{pmatrix} = \\ &= 1 \cdot [(2 \cdot (-2)) - (-1 \cdot 7)] = 1 \cdot (-4 + 7) = 1 \cdot 3 = 3 \end{aligned}$$

Dunque

$$\det(A) = a_{13} \cdot (-1)^{1+3} \cdot \det(A_{13}) = 5 \cdot 3 = 15$$

TEOREMA

Se A è una matrice $n \times n$. Finché $i \in \{1, \dots, n\}$ si ha

che:

(Sviluppo di Laplace rispetto alla i -esima riga)

$$\underbrace{a_{11} A_{11} + a_{12} A_{12} + \dots + a_{1n} A_{1n}}_{\det A} = a_{i1} A_{i1} + a_{i2} A_{i2} + \dots + a_{im} A_{im}$$

$$\det A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = [a_{i1} \ a_{i2} \ \dots \ a_{in}] \begin{bmatrix} A_{i1} \\ A_{i2} \\ \vdots \\ A_{in} \end{bmatrix}$$

$$\det A = \begin{pmatrix} 1 & -5 & 0 & 3 \\ 6 & 2 & 0 & 4 \\ -2 & 0 & 0 & 2 \\ -1 & 7 & 5 & 1 \end{pmatrix} = (-1)^{3+4} \begin{pmatrix} -2 & 0 & 0 & 2 \\ 1 & 3,1 & 3,2 & 3,3 \\ 1 & -2A_{31} + 0A_{32} + 0A_{33} + 2A_{34} \\ 1 & -260 - 320 = -580 \end{pmatrix} =$$

$$A_{31} = (-1)^{2+1} \det \begin{pmatrix} -5 & 0 & 3 \\ 2 & 0 & 4 \\ 7 & 5 & 1 \end{pmatrix} = 2(-1)^{2+1} \det \begin{pmatrix} 0 & 3 \\ 5 & 1 \end{pmatrix} +$$

$$+ 4(-1)^{2+3} \det \begin{pmatrix} -5 & 0 \\ 7 & 5 \end{pmatrix} = 2 \cdot (-1) (0 \cancel{1} - 3 \cdot 5) + 4 \cdot (-1) (-25)$$

$$= -2 \cdot (-15) + 100 = +30 + 100 = 130$$

$$A = \begin{pmatrix} 1 & -5 & 0 & 3 \\ 6 & 2 & 0 & 4 \\ -2 & 0 & 0 & 2 \\ -1 & 7 & 5 & 1 \end{pmatrix}$$

$$A_{34} = (-1)^{3+4} \det \begin{pmatrix} 1 & -5 & 0 \\ 6 & 2 & 0 \\ -1 & 7 & 5 \end{pmatrix} = - \left[6(-1)^{2+1} \det \begin{pmatrix} -5 & 0 \\ 7 & 5 \end{pmatrix} + \right.$$

$$+ 2(-1)^{2+2} \det \begin{pmatrix} 1 & 0 \\ -1 & 5 \end{pmatrix} \left. \right] = - \left[6 \cdot (-1) (-5 \cdot 5 - 0 \cdot 7) \right.$$

$$+ 2(1 \cdot 5 - 0 \cdot (-1)) \left. \right] = -[-6(-25) + 2 \cdot 5] =$$

$$= -[150 + 10] = -160$$

TEOREMA Ha $A = (a_{ij})_{m \times n}$. Per $j \in \{1, \dots, m\}$, si ha:

$$\det A = a_{1j} A_{1j} + a_{2j} A_{2j} + \dots + a_{nj} A_{nj}$$

(Sviluppo di Laplace rispetto alla
j-esima colonna di A)

$$\det A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{pmatrix} = [a_{1j} \ a_{2j} \ \dots \ a_{nj}] \begin{pmatrix} A_{1j} \\ A_{2j} \\ \vdots \\ A_{nj} \end{pmatrix}$$

j-esima colonna di A

$$A = \begin{pmatrix} 1 & -5 & 0 & 3 \\ 6 & 2 & 0 & 4 \\ -2 & 0 & 0 & 2 \\ -1 & 7 & 5 & 1 \end{pmatrix} = [0 \underset{1,3}{\uparrow} \ 0 \underset{2,3}{\uparrow} \ 0 \underset{3,3}{\uparrow} \ 5 \underset{4,3}{\uparrow}] \begin{pmatrix} A_{13} \\ A_{23} \\ A_{33} \\ A_{43} \end{pmatrix} =$$

$$= 0 \cdot \cancel{A_{13}} + 0 \cdot \cancel{A_{23}} + 0 \cdot \cancel{A_{33}} + 5 \cdot \cancel{A_{43}} = -116$$

$$A_{43} = (-1)^{4+3} \det \begin{pmatrix} 1 & -5 & 3 \\ 6 & 2 & 4 \\ -2 & 0 & 2 \end{pmatrix} = - \left[-5 (-1)^{1+2} \det \begin{pmatrix} 6 & 4 \\ -2 & 2 \end{pmatrix} \right]$$

$$+ 2 \cancel{(-1)^{2+2}} \det \begin{pmatrix} 1 & 3 \\ -2 & 2 \end{pmatrix} = - \left[-5 \cdot (-1) \cdot (6 \cdot 2 - 4 \cdot (-2)) \right]$$

$$+ 2 \left[1 \cdot 2 - 3 \cdot (-2) \right] = - \left[5 \cdot (12 + 8) + 2 \cdot (2 + 6) \right] =$$

$$= - [100 + 16] = -116$$

Una matrice quadrata A si dice invertibile o inversa (non singolare) se esiste una matrice B tale che:

$$AB = b_{in} = BA$$

La matrice B si indica con $B = A^{-1}$

Data una matrice A , voglio capire se è una matrice invertibile ed eventualmente qual è la sua matrice inversa A^{-1} .

$$A = \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$$

Se A è una matrice invertibile allora vale l'equazione $A \cdot A^{-1} = I$

$$A \cdot A^{-1} = A^{-1} \cdot A = I_{(n)}$$

Quindi, moltiplico A per una matrice B dello stesso ordine composta da variabili incognite.

Poi eguallo il prodotto a una matrice identità I .

$$A \cdot B = I_{(n)}$$

$$A \cdot B = \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

WWW.ANDREAMININI.ORG

Svolgo la moltiplicazione riga per colonna delle due matrici.

$$A \cdot B = \begin{pmatrix} 2a+c & 2b+d \\ -a+c & -b+d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

WWW.ANDREAMININI.ORG

A questo punto scrivo il sistema lineare equivalente all'uguaglianza delle due matrici

$$\begin{cases} 2a+c=1 \\ 2b+d=0 \\ -a+c=0 \\ -b+d=1 \end{cases}$$

WWW.ANDREAMININI.ORG

Se il sistema lineare ha una soluzione, allora la matrice è invertibile.

Se il sistema lineare ha una soluzione, allora la matrice è invertibile.

In questo caso il sistema lineare ha una soluzione.

$$\begin{cases} 2a+c=1 \\ 2b+d=0 \\ -a+c=0 \\ -b+d=1 \end{cases} \quad \begin{cases} 2a+c=1 \\ 2b+d=0 \\ a=c \\ b=d-1 \end{cases} \quad \begin{cases} 2(c)+c=1 \\ 2(d-1)+d=0 \\ a=c \\ b=d-1 \end{cases}$$

$$\begin{cases} 3c=1 \\ 2d-2+d=0 \\ a=c \\ b=d-1 \end{cases} \quad \begin{cases} c=\frac{1}{3} \\ 3d-2=0 \\ a=c \\ b=d-1 \end{cases} \quad \begin{cases} c=\frac{1}{3} \\ d=\frac{2}{3} \\ a=c \\ b=d-1 \end{cases}$$

$$\begin{cases} c=\frac{1}{3} \\ d=\frac{2}{3} \\ a=c \\ b=(\frac{2}{3})-1 \end{cases} \quad \begin{cases} c=\frac{1}{3} \\ d=\frac{2}{3} \\ a=c \\ b=-\frac{1}{3} \end{cases} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

Vediamo ora le principali **proprietà del determinante** che, oltre a rivestire un importante ruolo teorico, ci permettono di risparmiare un bel po' di tempo quando dobbiamo fare i calcoli. Per favorire chi è qui in fase di ripasso, elencheremo anche proprietà che richiedono nozioni che tratteremo nel prosieguo delle lezioni; nel caso stiate seguendo l'ordinamento delle lezioni, non preoccupatevene per il momento. ;)

Determinante nullo: il determinante di una matrice quadrata è uguale a 0 se e solo se

- ha una riga (o una colonna) tutta di elementi nulli, oppure
- due righe (o due colonne) sono proporzionali, oppure
- una riga (o una colonna) è **combinazione lineare** di due o più righe (o colonne).

Determinante di matrici triangolari: se la matrice quadrata di cui vogliamo calcolare il determinante è una **matrice triangolare** (superiore o inferiore), allora il determinante è dato dal prodotto degli elementi della diagonale principale.

Determinante del prodotto: se siamo di fronte a due matrici quadrate dello stesso ordine, tra le quali è quindi possibile eseguire il **prodotto riga per colonna**, il determinante del prodotto è uguale al prodotto dei determinanti

$$\det(AB) = \det(A) \det(B)$$

Tale proprietà è in realtà un vero e proprio teorema conosciuto con il nome di **teorema di Binet**.

Determinante dell'inversa: data una matrice invertibile, il determinante della **matrice inversa** è il reciproco del determinante della matrice di partenza

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

Determinante della trasposta: una matrice quadrata e la sua **matrice trasposta** hanno lo stesso determinante

$$\det(A^T) = \det(A)$$

Determinante del prodotto per uno scalare: il determinante del **prodotto di una matrice per uno scalare** è dato dal prodotto tra lo scalare elevato all'ordine della matrice e il determinante della matrice; dunque se A è una matrice quadrata di ordine n e λ è lo scalare abbiamo che

$$\det(\lambda A) = \lambda^n \cdot \det(A)$$

Determinante di matrici simili: due **matrici simili** hanno lo stesso determinante.

Dati i determinanti, abbiamo le sottomatrici, ottenute eliminando alcune righe e/o alcune colonne della matrice in esame, mentre si dicono minori associati a una matrice i determinanti delle sottomatrici quadrate da essa estratte (i rispettivi ordini sono *ordini dei minori*).

Esempi di sottomatrici

Consideriamo la seguente matrice

$$A = [1 \ 0 \ 2 \ 4 ; 5 \ 7 \ 6 \ 8 ; -2 \ 3 \ -1 \ 9]$$

Sono sottomatrici di A:

$$A' = [1 \ 0 \ 2 ; 5 \ 7 \ 6 ; -2 \ 3 \ -1]$$

ottenuta eliminando l'ultima colonna di A o, equivalentemente, pensata come l'intersezione tra le sue prime tre righe e tre colonne.

$$A'' = [0 \ 2 ; 3 \ -1]$$

costruita eliminando prima e quarta colonna e seconda riga di A o, equivalentemente, ricavata come intersezione tra prima e terza riga e seconda e terza colonna di A.

$$A''' = [7 \ 8]$$

estratta eliminando prima e terza riga e prima e terza colonna di A.

Esempi sui minori di una matrice

Prendiamo in esame la matrice

$$A = [2 \ 1 \ 4 ; -1 \ 0 \ -2 ; 3 \ 6 \ 5 ; -4 \ 7 \ -3]$$

I suoi minori di ordine 3 sono

$$\det \begin{pmatrix} -1 & 0 & 2 \\ 3 & 6 & 5 \\ -4 & 7 & -3 \end{pmatrix} = -37 \quad ; \quad \det \begin{pmatrix} 2 & 1 & 4 \\ 3 & 6 & 5 \\ -4 & 7 & -3 \end{pmatrix} = 63$$

$$\det \begin{pmatrix} 2 & 1 & 4 \\ -1 & 0 & 2 \\ -4 & 7 & -3 \end{pmatrix} = 5 \quad ; \quad \det \begin{pmatrix} 2 & 1 & 4 \\ -1 & 0 & 2 \\ 3 & 6 & 5 \end{pmatrix} = -1$$

ottenuti calcolando i determinanti delle sottomatrici ricavate eliminando, rispettivamente, prima, seconda, terza e quarta riga di A.

Alcuni dei suoi minori di ordine 2 sono, invece

$$\det \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} = 1 \quad ; \quad \det \begin{pmatrix} 2 & 4 \\ -1 & -2 \end{pmatrix} = 0$$

$$\det \begin{pmatrix} 0 & -2 \\ 6 & 5 \end{pmatrix} = 12 \quad ; \quad \det \begin{pmatrix} -1 & 0 \\ -4 & 7 \end{pmatrix} = -7$$

$$\det \begin{pmatrix} 1 & 4 \\ 7 & -3 \end{pmatrix} = -31$$

Esistono altri tipi di minori:

- Minori orlati, determinanti di ogni sottomatrice quadrata di ordine $p+1$, ottenuto dalla sottomatrice A' aggiungendo una riga e una colonna di A
- Minori complementari, determinante di una sottomatrice estratta da A eliminando una sola riga e una sola colonna

In particolare, fissato un elemento $a_{(ij)} \in A$, è detto **minore complementare relativo ad a_{ij}** , e si indica con $C_{(ij)}$, il minore complementare calcolato sulla base della sottomatrice $A_{(ij)}$ ottenuta dall'eliminazione dell' i -esima riga e della j -esima colonna di A .

Partendo dalla definizione di minore complementare relativo a un elemento $a_{(ij)}$ si introduce il concetto di **complemento algebrico** relativo a un elemento $a_{(ij)}$ (o cofattore relativo a un elemento $a_{(ij)}$).

Se $a_{(ij)} \in A$ si definisce **complemento algebrico (o cofattore) relativo all'elemento $a_{(ij)}$** , e si indica con $\text{Cof}(a_{(ij)})$, il minore complementare relativo all'elemento ad $a_{(ij)}$, a cui si antepone il segno + se $i+j$ è pari e il segno - se $i+j$ è dispari.

In formule:

$$\text{Cof}(a_{(ij)}) = (-1)^{i+j} \cdot C_{(ij)} = (-1)^{i+j} \cdot \det(A_{(ij)})$$

Il **complemento algebrico $\text{Cof}(a_{ij})$** si ottiene infatti anteponendo a C_{ij} :

- il segno più se $i + j$ è pari;
- il segno meno se $i + j$ è dispari.

In formule:

$$\text{Cof}(a_{ij}) = (-1)^{i+j} \cdot C_{ij}$$

dove la scrittura $\text{Cof}(a_{ij})$ indica il cofattore (o complemento algebrico) relativo all'elemento a_{ij} .

Dalla successiva alcuni minori complementari tagliati per sintesi:

Esempi di minori complementari

Sia

$$A = [2 \ 1 \ 0 \ ; -1 \ 3 \ 4 \ ; 5 \ -2 \ 6]$$

una matrice quadrata di ordine 3. I minori complementari relativi ai suoi nove elementi sono

$$C_{11} = \det(A_{11}) = \det \begin{pmatrix} 3 & 4 \\ -2 & 6 \end{pmatrix} = 26; \quad C_{12} = \det(A_{12}) = \det \begin{pmatrix} -1 & 4 \\ 5 & 6 \end{pmatrix} = -26;$$

$$C_{13} = \det(A_{13}) = \det \begin{pmatrix} -1 & 3 \\ 5 & -2 \end{pmatrix} = -13; \quad C_{21} = \det(A_{21}) = \det \begin{pmatrix} 1 & 0 \\ -2 & 6 \end{pmatrix} = 6;$$

Detto tutto ciò, per calcolare la matrice inversa di una matrice invertibile:

La prima cosa da fare è stabilire se si tratta di una matrice invertibile, ossia stabilire se il determinante di A è diverso da zero.

Dunque, per calcolare la matrice inversa dobbiamo:

1) calcolare il determinante di A :

1a) Se $\det(A) = 0$: fine! La matrice **non è invertibile** e quindi non si può calcolare l'inversa.

1b) Se $\det(A) \neq 0$ allora l'inversa esiste e possiamo proseguire.

2) Calcolare la **matrice dei cofattori**, (o *matrice dei complementi algebrici*) cioè sostituire ogni elemento della matrice di partenza con il relativo cofattore.

3) Determinare la **matrice trasposta** della matrice dei cofattori ottenuta al punto 2), cioè scambiarne le righe con le colonne. A titolo di cronaca è bene sapere che alcuni libri di testo chiamano la trasposta della matrice dei cofattori **matrice aggiunta**.

4) Moltiplicare la matrice ottenuta al punto 3) per lo scalare: $\frac{1}{\det(A)}$.

5) Quella del punto 4) è la matrice inversa della matrice di partenza.

A titolo di esempio calcoliamo, se esiste, l'inversa della matrice

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

$$\det(A) = -5 \neq 0$$

dunque la matrice è invertibile.

Calcoliamo ora i cofattori dei suoi elementi:

$$\text{Cof}(a_{11}) = (-1)^{1+1} \cdot C_{11} = (-1)^2 \cdot \det \begin{pmatrix} -1 & 3 \\ 4 & 2 \end{pmatrix} = 1 \cdot (-2 - 12) = -14$$

$$\text{Cof}(a_{12}) = (-1)^{1+2} \cdot C_{12} = (-1)^3 \cdot \det \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = -1 \cdot (4 - 3) = -1$$

$$\text{Cof}(a_{13}) = (-1)^{1+3} \cdot C_{13} = (-1)^4 \cdot \det \begin{pmatrix} 2 & -1 \\ 1 & 4 \end{pmatrix} = 1 \cdot (8 + 1) = 9$$

$$\text{Cof}(a_{21}) = (-1)^{2+1} \cdot C_{21} = (-1)^3 \cdot \det \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix} = -1 \cdot (0 - 4) = 4$$

$$\text{Cof}(a_{22}) = (-1)^{2+2} \cdot C_{22} = (-1)^4 \cdot \det \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = 1 \cdot (2 - 1) = 1$$

$$\text{Cof}(a_{23}) = (-1)^{2+3} \cdot C_{23} = (-1)^5 \cdot \det \begin{pmatrix} 1 & 0 \\ 1 & 4 \end{pmatrix} = -1 \cdot (4 - 0) = -4$$

$$\text{Cof}(a_{31}) = (-1)^{3+1} \cdot C_{31} = (-1)^4 \cdot \det \begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix} = 1 \cdot (0 + 1) = 1$$

$$\text{Cof}(a_{32}) = (-1)^{3+2} \cdot C_{32} = (-1)^5 \cdot \det \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = -1 \cdot (3 - 2) = -1$$

$$\text{Cof}(a_{33}) = (-1)^{3+3} \cdot C_{33} = (-1)^6 \cdot \det \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} = 1 \cdot (-1 - 0) = -1$$

Formiamo la matrice dei complementi algebrici sostituendo ogni elemento di \mathcal{A} col relativo cofattore

$$\begin{pmatrix} -14 & -1 & 9 \\ 4 & 1 & -4 \\ 1 & -1 & -1 \end{pmatrix}$$

Scriviamone la trasposta

$$\begin{pmatrix} -14 & -1 & 9 \\ 4 & 1 & -4 \\ 1 & -1 & -1 \end{pmatrix}^T = \begin{pmatrix} -14 & 4 & 1 \\ -1 & 1 & -1 \\ 9 & -4 & -1 \end{pmatrix}$$

Moltiplicandola per il reciproco del determinante di \mathcal{A} otteniamo la matrice inversa cercata

$$A^{-1} = \frac{1}{-5} \cdot \begin{pmatrix} -14 & 4 & 1 \\ -1 & 1 & -1 \\ 9 & -4 & -1 \end{pmatrix} = \begin{pmatrix} \frac{14}{5} & -\frac{4}{5} & -\frac{1}{5} \\ \frac{1}{5} & -\frac{1}{5} & \frac{1}{5} \\ -\frac{9}{5} & \frac{4}{5} & \frac{1}{5} \end{pmatrix}$$

Spazi e sottospazi vettoriali, tipi, combinazioni lineari

Uno spazio vettoriale è una struttura algebrica definita a partire da un insieme di vettori, da un campo di scalari e da due operazioni binarie, dette somma tra vettori e prodotto di un vettore per uno scalare, che devono soddisfare delle specifiche proprietà.

Def UNO SPAZIO VETTORIALE SU K

- se $K = \mathbb{C}$ dico un sp. vett. (complesso)
- se $K = \mathbb{R}$ dico un sp. vett. reale

è un insieme NON Vuoto V su cui sono definite 2 operazioni:

$$+: V \times V \rightarrow V \quad \text{e} \quad \cdot : K \times V \rightarrow V$$

\nwarrow addizione \nearrow prodotto d'elementi di V per K

che nev'fanno le seguenti condizioni:

$$\forall u, v, w \in V \quad (\text{gl' elementi di } V \text{ si chiamano} \quad \underline{\text{VETTORI}})$$

$$\forall \alpha, \beta \in K \quad (\text{gl' elementi di } K \text{ si chiamano} \quad \underline{\text{SCALARI}})$$

Per fornire la **definizione di spazio vettoriale** ci servono quattro ingredienti:

- un campo, solitamente indicato con K e detto *campo di scalari*. Per fissare le idee, nella maggior parte delle applicazioni pratiche il campo K coincide col campo \mathbb{R} dei **numeri reali** o col campo \mathbb{C} dei **numeri complessi**.

- Un insieme V , chiamato *spazio di vettori*, e i cui elementi sono generalmente indicati in grassetto per non generare confusione con gli elementi del campo K .

- Un'operazione binaria interna, indicata con $+$ e detta *somma di vettori*:

$$+: V \times V \rightarrow V ; (v, w) \mapsto v + w$$

- Un'operazione binaria esterna, indicata con \cdot e detta *prodotto di un vettore per uno scalare*:

$$\cdot : K \times V \rightarrow V ; (\lambda, v) \mapsto \lambda \cdot v$$

Un sottospazio vettoriale è un sottoinsieme di uno spazio vettoriale tale da essere, a sua volta, uno spazio vettoriale rispetto alle operazioni di somma tra vettori e di prodotto di un vettore per uno scalare definite nello spazio di partenza.

Def Un sottoinsieme U di V si dice un SOTTOSPAZIO VETTORIALE (o semplicemente un SOTTOSPAZIO) di V se sono soddisfatte le seguenti condizioni:

$$\boxed{1} \quad \underline{0} \in U$$

$$\boxed{2} \quad \underline{u}_1 + \underline{u}_2 \in U, \quad \forall \underline{u}_1, \underline{u}_2 \in U \quad (U \text{ È CHIUSO AUF+})$$

$$\boxed{3} \quad \alpha \underline{u} \in U, \quad \forall \underline{u} \in U, \forall \alpha \in K \quad (U \text{ È CHIUSO AL PRODOTTO PER SCALARI})$$

Si dice che un sottoinsieme non vuoto S di V ($S \subseteq V$) è un sottospazio vettoriale se S è uno spazio vettoriale su K rispetto alle stesse operazioni di somma tra vettori e di prodotto di un vettore per uno scalare definite in V .

I QUATTRO SOTTOSPAZI FONDAMENTALI DI UNA MATRICE

$$A \in M_{m \times m}(\mathbb{C})$$

$$A = [\underline{a}_1 \ \underline{a}_2 \ \dots \ \underline{a}_m] = \begin{bmatrix} \underline{r}_1^T \\ \underline{r}_2^T \\ \vdots \\ \underline{r}_m^T \end{bmatrix} \quad \underline{a}_i \in \mathbb{C}^m$$

$$A = \begin{bmatrix} & & \dots & \\ \underline{r}_1 & \underline{r}_2 & \dots & \underline{r}_m \end{bmatrix} = \begin{bmatrix} \vdots \\ \underline{r}_1 \\ \vdots \\ \underline{r}_m \end{bmatrix}$$

↑ questo mette in evidenza le colonne da parso come "UNA RIGA DI COLONNE!"

↑ questo mette in evidenza le righe la parso come "UNA COLONNA DI RIGHE!"

1 LO SPAZIO DEI DUE COLONNE DI A:

$$C(A) = \langle \underline{a}_1, \underline{a}_2, \dots, \underline{a}_m \rangle = \{ d_1 \underline{a}_1 + d_2 \underline{a}_2 + \dots + d_m \underline{a}_m \mid d_i \in \mathbb{C} \} \leq \mathbb{C}^m$$

2 LO SPAZIO DEI DUE RIGHE DI A

$$R(A) = \langle \underline{r}_1, \underline{r}_2, \dots, \underline{r}_m \rangle \leq \mathbb{C}^m$$

$$= \{ d_1 \underline{r}_1 + d_2 \underline{r}_2 + \dots + d_m \underline{r}_m \mid d_i \in \mathbb{C} \}$$

NB $A_{m \times n}$

$$\left\| \begin{bmatrix} \underline{r}_1^T \\ \vdots \\ \underline{r}_m^T \end{bmatrix} \right\|$$

$A^H \quad m \times m$

$$\left\| \begin{bmatrix} \underline{r}_1 & \underline{r}_2 & \dots & \underline{r}_m \end{bmatrix} \right\|$$

$$R(A) = C(A^H)$$

3 Lo spazio nullo di A

$$N(A) = \left\{ \underline{x} \mid \begin{matrix} A \underline{x} = \underline{0} \\ m \times n \quad m \times 1 \end{matrix} \right\} \subseteq \mathbb{C}^n$$

4 Lo spazio nullo sinistro di A :

$$N(A^H) = \left\{ \underline{x} \mid \begin{matrix} A^H \underline{x} = \underline{0} \\ m \times m \quad m \times 1 \end{matrix} \right\} \subseteq \mathbb{C}^m$$

La somma e l'intersezione di due sottospazi di uno stesso spazio vettoriale sono due sottospazi dello spazio di partenza, per cui è possibile individuare una base per ciascuno di essi e calcolarne le dimensioni.

Consideriamo uno **spazio vettoriale** V su un campo K e due suoi **sottospazi vettoriali** S, T \subseteq V. Definiamo l'insieme **somma dei due sottospazi vettoriali**, e lo indichiamo con S+T, come

$$S+T := v \in V \text{ t.c. } v = s+t, \text{ con } s \in S, t \in T$$

Definiamo poi l'**intersezione dei due sottospazi vettoriali**, e la chiamiamo S \cap T, l'**intersezione** tra i due insiemi

$$S \cap T := v \in V \text{ t.c. } v \in S, v \in T$$

Sia V uno **spazio vettoriale** finitamente generato e definito su un campo K e siano S e T due **sottospazi vettoriali** di V tali che V sia somma diretta di S e T.

I sottospazi S e T si dicono **sottospazi supplementari** in V.

In altri termini, due sottospazi S e T di uno spazio vettoriale V sono supplementari se e solo se V = S oplus T.

$$S \text{ e } T \text{ sottospazi supplementari in } V \Leftrightarrow V = S \text{ oplus } T$$

Inoltre, se V = S oplus T allora si dice che S è il supplementare di T in V e che T è il supplementare di S in V.

Dalla definizione segue che per **verificare se due sottospazi sono supplementari** in V bisogna stabilire se sono in somma diretta rispetto a V.

Teorema di caratterizzazione degli spazi vettoriali

Fortunatamente esiste un *teorema di caratterizzazione* che ci evita di dover verificare le otto proprietà una a una, e che quindi viene molto usato negli esercizi. Tale teorema afferma che:

un sottoinsieme non vuoto S di uno spazio vettoriale V su un campo K è un sottospazio vettoriale di V se e solo se S è chiuso rispetto alle due operazioni definite in V , cioè:

- (a) per ogni $s_1, s_2 \in S$ risulta che $s_1 + s_2 \in S$
- (b) per ogni $s \in S$ e per ogni $\lambda \in K$ risulta che $\lambda \cdot s \in S$

Data una matrice A , inoltre, un sistema lineare del tipo $Ax = 0$ (vettore dei termini noti pari a 0), è definito sistema lineare omogeneo.

Similmente, abbiamo che $A0 = 0$ è detto spazio nullo della matrice A .

INSIEME DEI MULUPI DI UN VETTORE

Haia V uno sp. vett. su $K \in \{\mathbb{R}, \mathbb{C}\}$ e $v \in V$

$$\{ \alpha v \mid \alpha \in K \} = \text{insieme dei multipli di } v$$

S' indica $\langle v \rangle$ oppure Span (v)

① $\langle v \rangle$ è un sottospazio di V

① $\underline{0} \in \langle v \rangle : \underline{0} = 0 \cdot v \quad (\text{perché } 0=0)$

② $\alpha_1 v + \alpha_2 v = (\alpha_1 + \alpha_2)v \quad \text{la somma di due multipli di } v \text{ è un multiplo di } v$

③ $\beta(\alpha v) = (\beta\alpha)v \quad \text{il prodotto di } \beta \text{ per un multiplo di } v \text{ è un multiplo di } v$

② SE $v = \underline{0}$ ALLORA $\langle v \rangle = \langle \underline{0} \rangle = \{ \alpha \cdot \underline{0} \mid \alpha \in K \} = \{ \underline{0} \}$
E $\langle v \rangle$ HA UN UNICO ELEMENTO

SE $v \neq \underline{0}$ ALLORA $\langle v \rangle = \{ \alpha v \mid \alpha \in K \}$ quindi ha INFINITI ELEMENTI
ha tutt' elementi quanti sono gli elementi di K .

Dato quindi uno spazio vettoriale, una combinazione lineare degli n vettori, $v_1, v_2, \dots, v_n \in V$ con coefficienti (o pesi) $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n \in V$.

Definiamo **combinazione lineare** di questi vettori una qualsiasi espressione della forma

$$a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \dots + a_n \mathbf{v}_n$$

dove a_1, a_2, \dots, a_n sono n scalari qualsiasi del campo \mathbb{K} .

A volte, per comodità, si indica la precedente combinazione lineare nella notazione più compatta

$$\sum_{i=1}^n a_i \mathbf{v}_i$$

che fa uso del simbolo di sommatoria.

Quest'ultimo è il sottospazio generato da tutti i vettori.

Dati $\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n \in V$ (V sp. vett. su \mathbb{K}) e l'insieme

di tutte le loro combinazioni lineari è:

$$\left\{ a_1 \underline{v}_1 + a_2 \underline{v}_2 + \dots + a_n \underline{v}_n \mid a_1, a_2, \dots, a_n \in \mathbb{K} \right\} = \\ = \left\{ \sum_{i=1}^n a_i \underline{v}_i \mid a_1, a_2, \dots, a_n \in \mathbb{K} \right\}$$

SI INDICA: $\langle \underline{v}_1, \underline{v}_2, \dots, \underline{v}_n \rangle$

OPPURE: $\text{Span}(\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n)$

SI CHIAMA: IL SOTTOSPAZIO (DI V)

GENERATO DA $\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n$

N.B. La volta nostra

abbiamo visto '0'

così $n=1$: $\underline{v}=\underline{v}_1$

$\langle \underline{v} \rangle = \{d\underline{v} \mid d \in \mathbb{K}\}$

Dati gli insiemi dei vettori, definiamo due concetti chiave:

- I vettori linearmente indipendenti

Si dice che gli n vettori $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ sono **linearmente indipendenti tra loro** se, prendendo n scalari $a_1, a_2, \dots, a_n \in \mathbb{K}$ e imponendo

$$a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \dots + a_n \mathbf{v}_n = \mathbf{0}$$

risulta che la precedente uguaglianza è soddisfatta se e solo se

$$a_1 = a_2 = \dots = a_n = 0$$

cioè se e solo se l'**unica** n -upla di scalari che annulla la **combinazione lineare** $a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \dots + a_n \mathbf{v}_n$ è la n -upla di coefficienti nulli.

- I vettori linearmente dipendenti

Diciamo invece che i vettori $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ sono **linearmente dipendenti** se oltre alla n-upla di scalari tutti nulli esiste almeno una n-upla di scalari non tutti nulli che annulla la combinazione lineare.

In altri termini, un insieme di vettori si dice linearmente dipendente se almeno uno dei vettori può essere espresso come combinazione lineare degli altri vettori nell'insieme. In altre parole, esiste almeno un vettore nell'insieme che può essere ottenuto come una combinazione lineare dei restanti vettori.

Quando avete n vettori $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ e volete vedere se sono linearmente indipendenti o meno, se si considera $a_1 = a_2 = \dots = a_n = 0$ (tutti nulli) è sempre vero che

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n = \mathbf{0}$$

Ciò che distingue l'indipendenza lineare dalla dipendenza lineare è che nel primo caso la n-upla di coefficienti nulli è l'**unica** che annulla la combinazione lineare dei vettori, mentre nel secondo deve esistere almeno un'altra n-upla di scalari non tutti nulli che la annulla.

1) I vettori $\mathbf{v}_1 = (1, 0)$, $\mathbf{v}_2 = (0, 1) \in \mathbb{R}^2$ sono linearmente indipendenti.

Consideriamo due generici scalari $a, b \in \mathbb{R}$ e imponiamo che sia nulla la generica combinazione lineare

$$a\mathbf{v}_1 + b\mathbf{v}_2$$

$$a(1, 0) + b(0, 1) = (0, 0)$$

Svolgendo le [operazioni tra vettori](#) otteniamo

$$(a, 0) + (0, b) = (0, 0)$$

$$(a, b) = (0, 0)$$

La precedente uguaglianza è soddisfatta se e solo se $a = b = 0$, il che ci permette di concludere che i vettori sono linearmente indipendenti.

2) I vettori $\mathbf{v}_1 = (1, 1, 0)$, $\mathbf{v}_2 = (0, 0, 2)$, $\mathbf{v}_3 = (0, 0, -3) \in \mathbb{R}^3$ sono linearmente dipendenti.

Per vederlo basta considerare tre generici scalari $a, b, c \in \mathbb{R}$ e richiedere che

$$a\mathbf{v}_1 + b\mathbf{v}_2 + c\mathbf{v}_3 = \mathbf{0}$$

ossia

$$a(1, 1, 0) + b(0, 0, 2) + c(0, 0, -3) = (0, 0, 0)$$

Dopo qualche semplice calcolo si ottiene

$$(a, a, 2b - 3c) = (0, 0, 0)$$

che è soddisfatta per

$$a = b = c = 0$$

ma anche per

$$a = 0, 2b = 3c$$

Ad esempio $a = 0$, $b = \frac{3}{2}$, $c = 1$ sono tre scalari non tutti nulli che annullano la generica combinazione lineare, dunque i tre vettori sono linearmente dipendenti.

Per stabilire se un insieme di vettori è linearmente indipendente, puoi utilizzare la definizione di linearità indipendente e applicare il concetto di combinazioni lineari. Un insieme di vettori è linearmente indipendente se nessun vettore nell'insieme può essere espresso come una combinazione lineare degli altri vettori.

Ecco come puoi verificare se un insieme di vettori è linearmente indipendente:

1. Scrivi la relazione di combinazione lineare:

Supponiamo di avere un insieme di vettori $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$. Scrivi l'equazione di combinazione lineare:

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \dots + c_n\mathbf{v}_n = \mathbf{0}$$

Dove c_1, c_2, \dots, c_n sono coefficienti scalari e $\mathbf{0}$ è il vettore nullo dello spazio vettoriale.

1. Verifica i coefficienti:

Se l'unico modo per ottenere la combinazione lineare nulla è impostare tutti i coefficienti c_1, c_2, \dots, c_n a 0, allora gli vettori sono linearmente indipendenti. In altre parole, l'equazione $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \dots + c_n\mathbf{v}_n = \mathbf{0}$ ha solo la soluzione $c_1 = c_2 = \dots = c_n = 0$

2. Se esiste una combinazione non nulla:

Se puoi trovare una combinazione di coefficienti non tutti nulli che soddisfa l'equazione $c_1v_1 + c_2v_2 + \dots + c_nv_n = 0$, allora gli vettori sono linearmente dipendenti e non linearmente indipendenti.

In breve, se non esiste una combinazione non nulla che rende l'equazione di combinazione lineare uguale al vettore nullo, allora gli vettori sono linearmente indipendenti. Altrimenti, sono linearmente dipendenti.

Ad esempio, considera due vettori in \mathbb{R}^2 :

$$v_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \text{ e } v_2 = \begin{bmatrix} 3 \\ 4 \end{bmatrix}.$$

Se la combinazione lineare $c_1v_1 + c_2v_2 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ ha solo la soluzione $c_1 = c_2 = 0$, allora i vettori sono linearmente indipendenti. In questo caso, possiamo vedere che non esistono coefficienti diversi da zero che soddisfino l'equazione, quindi i due vettori sono linearmente indipendenti.

Per stabilire se un insieme è un sottospazio vettoriale, devi verificare se soddisfa le tre proprietà fondamentali di un sottospazio vettoriale: chiusura rispetto all'addizione vettoriale, chiusura rispetto alla moltiplicazione per uno scalare e contenimento del vettore nullo.

Supponiamo di avere uno spazio vettoriale V su un campo F (solitamente i numeri reali o complessi). Ecco come puoi verificare se un insieme S è un sottospazio vettoriale di V:

1. Chiusura rispetto all'addizione vettoriale

Per ogni coppia di vettori v_1 e v_2 in S, la loro somma $v_1 + v_2$ deve appartenere a S. In altre parole, l'operazione di addizione tra due vettori all'interno di S deve produrre un vettore che è ancora in S.

2. Chiusura rispetto alla moltiplicazione per uno scalare

Per ogni vettore v in S e per ogni scalare c in F, il prodotto $c * v$ deve appartenere a S. Ciò significa che moltiplicare un vettore in S per uno scalare deve ancora produrre un vettore in S.

3. Contenimento del vettore nullo

Il vettore nullo (il vettore che aggiunto a qualsiasi altro vettore non cambia il vettore stesso) deve appartenere a S.

Se l'insieme S soddisfa tutte e tre queste proprietà, allora è un sottospazio vettoriale di V. Altrimenti, se almeno una di queste proprietà non è verificata, l'insieme non è un sottospazio vettoriale.

Ecco un esempio concreto:

Supponiamo di avere lo spazio vettoriale \mathbb{R}^2 (tutti i vettori bidimensionali) e l'insieme S che contiene tutti i vettori di forma (x, y) dove x e y sono numeri interi positivi o nulli.

1. Chiusura rispetto all'addizione vettoriale: Se prendiamo due vettori (x_1, y_1) e (x_2, y_2) da S, la loro somma $(x_1 + x_2, y_1 + y_2)$ avrà ancora componenti intere o nulle. Quindi, la chiusura rispetto all'addizione è soddisfatta.

2. Chiusura rispetto alla moltiplicazione per uno scalare: Se prendiamo un vettore (x, y) da S e lo moltiplichiamo per uno scalare c , otteniamo $(c * x, c * y)$, che ha ancora componenti intere o nulle. Quindi, anche la chiusura rispetto alla moltiplicazione scalare è soddisfatta.

3. Contenimento del vettore nullo: Il vettore nullo $(0, 0)$ ha componenti intere o nulle, quindi fa parte di S .

Poiché tutte e tre le proprietà sono soddisfatte, l'insieme S è un sottospazio vettoriale di R^2 .

A questo punto, data una qualsiasi matrice, si può parlare di rango (o caratteristica), definibile come:

- Il massimo numero di righe linearmente indipendenti di A
- Il massimo numero di colonne linearmente indipendenti di A
- Spiegato in modo più semplice, data una matrice qualsiasi il rango è l'ordine massimo dei minori con determinante non nullo.

Data una matrice A di tipo $m \times n$ ha rango p se esiste almeno un minore di ordine p con determinante non nullo e tutti i minori di ordine $p+1$, se esistono, hanno un determinante nullo.

Il rango della matrice A è un numero reale ed è indicato con il simbolo $\text{rk}(A)$, $\text{rg}(A)$, $r(A)$, $p(A)$.

Se la matrice A appartiene $M_{m \times n}$ allora il rango della matrice $r(A)$ è compreso tra zero e il numero intero minore tra righe e colonne.

$$0 \leq \text{rk}A \leq \min(m, n)$$

Il numero di righe/colonne linearmente indipendente non può essere superiore al numero di righe e di colonne della matrice.

Quanti appena descritto è il cosiddetto teorema di Kronecker.

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 2 & 1 & 1 & 2 \\ 0 & 2 & 0 & 0 \end{pmatrix} \quad 0 \leq rg(A) \leq \min(3,4)$$

la matrice ha 12 minori di ordine 1

almeno un minore di ordine 1 è maggiore di 0 quindi il rango della matrice è compreso tra 1 a 3

$$\begin{array}{llll} \det(1)=1 & \det(0)=0 & \det(2)=2 & \det(1)=1 \\ \det(2)=2 & \det(1)=1 & \det(1)=1 & \det(2)=2 \\ \det(0)=0 & \det(2)=2 & \det(0)=0 & \det(0)=0 \end{array}$$

tra i minori di ordine 2, ce n'è almeno uno diverso da zero

quindi il rango della matrice è compreso tra 2 a 3

$$\begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} = 1 \quad , \quad \begin{vmatrix} 1 & 2 \\ 2 & 1 \end{vmatrix} = -3 \quad , \quad \dots$$

tra i minori di ordine 3, ce n'è almeno uno diverso da zero

quindi **il rango della matrice è 3**

$$\begin{vmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \\ 0 & 2 & 0 \end{vmatrix} = 6 \quad , \quad \begin{vmatrix} 0 & 2 & 1 \\ 1 & 1 & 2 \\ 2 & 0 & 0 \end{vmatrix} = 6 \quad , \quad \dots$$

WWW.ANDREAMININI.ORG

Nella risoluzione di sistemi lineari, si utilizza spesso il Teorema di Rouché-Capelli, che ci dice quando un sistema di equazioni ha soluzioni e quando non ne ha. In termini semplici, stabilisce una condizione per determinare se un sistema di equazioni lineari abbia una soluzione, non abbia alcuna soluzione o abbia infinite soluzioni.

In modo più specifico, il teorema afferma che:

1. Se il numero di equazioni (righe) in un sistema è uguale al numero di incognite (colonne) e il determinante della matrice dei coefficienti è diverso da zero, allora il sistema ha una sola soluzione unica.
2. Se il numero di equazioni è maggiore del numero di incognite e il determinante della matrice dei coefficienti è diverso da zero, allora il sistema non ha soluzioni.
3. Se il numero di equazioni è minore del numero di incognite, il sistema ha infinite soluzioni o nessuna, e ciò dipende dalla specifica configurazione delle equazioni.

Più formalmente:

Consideriamo un sistema lineare di m equazioni in n incognite e con coefficienti in un campo \mathbb{K}

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

Per enunciare il teorema di Rouché Capelli scriviamo il precedente sistema in forma matriciale

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

dove

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{K}^{m,n}$$

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^{n,1} \quad ; \quad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{K}^{m,1}$$

Chiamiamo A la **matrice incompleta** (o *matrice dei coefficienti*) associata al sistema e diciamo **matrice completa** la seguente **matrice**, ottenuta accostando ad A il vettore colonna \mathbf{b} dei termini noti

$$(A|\mathbf{b}) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array} \right)$$

Il teorema di Rouché-Capelli stabilisce che

1) Se $\text{rk}(A) < \text{rk}(A|\mathbf{b})$, cioè se il rango della matrice incompleta è minore del rango della matrice completa, allora il sistema è impossibile, cioè non ammette soluzioni.

2) Se $\text{rk}(A) = \text{rk}(A|\mathbf{b})$, cioè se il rango della matrice incompleta coincide con il rango della matrice completa, allora il sistema è compatibile (ammette cioè una o infinite soluzioni).

In particolare, ricordando che n è il numero di incognite, risulta che:

2.A) se $\text{rk}(A) = \text{rk}(A|\mathbf{b}) = n$, allora abbiamo una e una sola soluzione;

2.B) se $\text{rk}(A) = \text{rk}(A|\mathbf{b}) < n$, allora il sistema ammette $\infty^{n-\text{rk}(A)}$ soluzioni, quindi ammette infinite soluzioni che dipendono da $n - \text{rk}(A)$ parametri.

Sistemi di generatori, basi, applicazioni lineari

Un sistema di generatori di uno spazio o sottospazio vettoriale è un insieme di vettori che permette di ricostruire, mediante combinazioni lineari, *tutti* i vettori dello spazio.

Sia V uno spazio vettoriale su un campo \mathbb{K} . Diciamo che un insieme di vettori $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \subseteq V$ è un **sistema di generatori** (o *insieme di generatori*) di V se ogni elemento di V si può esprimere mediante una **combinazione lineare** di tali vettori.

In altri termini, $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \subseteq V$ è un sistema di generatori di V se e solo se (per definizione) per ogni $\mathbf{w} \in V$ esistono n scalari $a_1, a_2, \dots, a_n \in \mathbb{K}$ tali che

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n = \sum_{i=1}^n a_i\mathbf{v}_i = \mathbf{w}$$

Dunque, **cos'è un sistema di generatori?** È un insieme di vettori appartenenti allo spazio considerato che permette di ricostruire *tutti* i vettori dello spazio mediante opportune combinazioni lineari.

1) Consideriamo lo spazio vettoriale \mathbb{R}^2 dei vettori a due componenti **reali**, e consideriamo l'insieme

$$\{(0, 2), (1, 0), (1, 1)\} \subseteq \mathbb{R}^2$$

Esso costituisce un sistema di generatori di \mathbb{R}^2 , infatti per ogni $\mathbf{w} \in \mathbb{R}^2$, ossia per ogni $(w_1, w_2) \in \mathbb{R}^2$, possiamo trovare dei coefficienti $a_1, a_2, a_3 \in \mathbb{R}$ tali che

$$(w_1, w_2) = a_1(0, 2) + a_2(1, 0) + a_3(1, 1)$$

Per fissare le idee proviamo, ad esempio, col vettore

$$\mathbf{w} = (w_1, w_2) = (27, 4)$$

Se consideriamo i coefficienti

$$a_1 = 2, a_2 = 27, a_3 = 0$$

allora

$$\begin{aligned} a_1(0, 2) + a_2(1, 0) + a_3(1, 1) &= \\ &= 2 \cdot (0, 2) + 27 \cdot (1, 0) + 0 \cdot (1, 1) = \\ &= (0, 4) + (27, 0) + (0, 0) = (27, 4) \end{aligned}$$

Ci teniamo a farvi osservare che, *in generale*, la scelta degli scalari $a_1, a_2, a_3 \in \mathbb{R}$ non è unica. Anche considerando

$$a_1 = 1, a_2 = 25, a_3 = 2$$

si può costruire una combinazione lineare che genera il vettore $\mathbf{w} = (27, 4)$, infatti

$$\begin{aligned} a_1(0, 2) + a_2(1, 0) + a_3(1, 1) &= \\ &= 1 \cdot (0, 2) + 25 \cdot (1, 0) + 2 \cdot (1, 1) = \\ &= (0, 2) + (25, 0) + (2, 2) = (27, 4) \end{aligned}$$

Per stabilire se un insieme di vettori è un sistema di generatori (o spazio generato), devi verificare se ogni vettore nello spazio vettoriale può essere espresso come combinazione lineare dei vettori nell'insieme dato. In altre parole, devi verificare se ogni vettore nel tuo spazio vettoriale può essere creato utilizzando una combinazione dei vettori forniti.

Ecco come puoi farlo:

1. Scrivi l'equazione di combinazione lineare:

Considera l'insieme di vettori $\{v_1, v_2, \dots, v_n\}$. Scrivi l'equazione di combinazione lineare generale:

$$c_1v_1 + c_2v_2 + \dots + c_nv_n = v$$

Dove v è un vettore generico nello spazio vettoriale che stai considerando e c_1, c_2, \dots, c_n sono coefficienti scalari.

1. Risovi per i coefficienti:

L'obiettivo è trovare i valori dei coefficienti c_1, c_2, \dots, c_n che rendono vera l'equazione di combinazione lineare per il vettore v . In pratica, risovi il sistema di equazioni lineari ottenuto dalla tua equazione di combinazione lineare rispetto ai coefficienti c_1, c_2, \dots, c_n .

2. Verifica per ogni vettore nello spazio vettoriale:

Esegui il passaggio 2 per ciascun vettore v nello spazio vettoriale. Se puoi sempre trovare i valori dei coefficienti c_1, c_2, \dots, c_n che rendono vera l'equazione di combinazione lineare per ogni vettore v , allora l'insieme di vettori $\{v_1, v_2, \dots, v_n\}$ è un sistema di generatori dello spazio vettoriale.

In sostanza, se ogni vettore nel tuo spazio vettoriale può essere scritto come combinazione lineare dei vettori forniti, allora quei vettori costituiscono un sistema di generatori per lo spazio vettoriale.

Ad esempio, considera l'insieme di vettori $\{(1, 0), (0, 1)\}$ in \mathbb{R}^2 . Ogni vettore in \mathbb{R}^2 può essere scritto come una combinazione lineare di questi due vettori. Ad esempio, $(2, 3)$ può essere scritto come $2 \cdot (1, 0) + 3 \cdot (0, 1)$, quindi l'insieme di vettori $\{(1, 0), (0, 1)\}$ è un sistema di generatori per \mathbb{R}^2 .

Definizione 1.3.36. Uno spazio vettoriale V è detto *finitamente generato* se esiste un insieme finito di generatori di V .

A questo punto, introduciamo il concetto di base, cioè un insieme di vettori con i quali possiamo ricostruire in modo unico tutti i vettori dello spazio mediante combinazioni lineari.

Più precisamente, dato uno spazio vettoriale V su un campo \mathbb{K} , diciamo che un insieme di vettori $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \subseteq V$ è una base di V se:

(a) $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ è un sistema di generatori di V ;

(b) i vettori $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ sono vettori linearmente indipendenti.

Le condizioni espresse in (a) e in (b) possono essere formalmente riscritte nel modo seguente.

(a) Per ogni $\mathbf{w} \in V$ esistono n scalari $a_1, a_2, \dots, a_n \in \mathbb{K}$ tali che

$$\mathbf{w} = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \dots + a_n \mathbf{v}_n$$

I numeri a_1, a_2, \dots, a_n si dicono le *coordinate* o le *componenti* del vettore \mathbf{w} rispetto alla base $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$.

(b) L'unica n-upla di scalari che soddisfa l'uguaglianza

$$b_1 \mathbf{v}_1 + b_2 \mathbf{v}_2 + \dots + b_n \mathbf{v}_n = \mathbf{0}$$

è la n-upla di scalari tutti nulli, cioè $b_1 = b_2 = \dots = b_n = 0$.

In definitiva, per verificare che un insieme di vettori è una base per uno spazio vettoriale dobbiamo stabilire se è un sistema di generatori e se i vettori in esame sono linearmente indipendenti.

La base canonica è una base particolare che è spesso utilizzata negli spazi vettoriali standard. La base canonica rappresenta i vettori elementari, cioè i vettori con un solo componente diverso da zero, mentre tutti gli altri componenti sono zero.

Ecco la base canonica in \mathbb{R}^n :

- $e_1 = (1, 0, 0, \dots, 0)$
- $e_2 = (0, 1, 0, \dots, 0)$
- \vdots
- $e_n = (0, 0, 0, \dots, 1)$

Ogni vettore in \mathbb{R}^n può essere espresso come combinazione lineare di questi vettori elementari. Ad esempio, il vettore $v = (2, 3, 0, 1)$ può essere scritto come $v = 2e_1 + 3e_2 + 0e_3 + 1e_4$.

La base canonica è spesso utilizzata perché semplifica le operazioni vettoriali e rende più chiara la rappresentazione dei vettori.

Vediamo ora qualche importante risultato teorico sulla nozione di base di uno spazio vettoriale, grazie a cui potremo definire il concetto di dimensione di uno spazio vettoriale.

Teorema 1 (esistenza di una base)

Ogni spazio vettoriale $V \neq \{\mathbf{0}\}$ ammette almeno una base.

Teorema 2 (non unicità della base)

Ogni spazio vettoriale $V \neq \{\mathbf{0}\}$ definito su un campo \mathbb{K} ammette infinite basi.

Teorema 3 (cardinalità delle basi)

Due basi qualsiasi \mathcal{B} e \mathcal{B}' di uno stesso spazio vettoriale V hanno la stessa **cardinalità**, cioè lo stesso numero di elementi.

$$\forall \mathcal{B}, \mathcal{B}' \text{ basi di } V \Rightarrow |\mathcal{B}| = |\mathcal{B}'|$$

In virtù del precedente teorema ha senso dare la **definizione** di **dimensione** di uno spazio vettoriale: dato uno spazio vettoriale V su un campo \mathbb{K} definiamo la dimensione di V come il numero di elementi di una sua *qualsiasi* base, e la indichiamo con $\dim(V)$

$$\dim(V) := |\mathcal{B}| \text{ con } \mathcal{B} \text{ base qualsiasi di } V$$

Possiamo inoltre definire **coordinate** (o componenti) di un vettore rispetto a una base gli scalari mediante cui il vettore si esprime come combinazione lineare dei vettori della base.

Equivalentemente, fissata una base di uno spazio vettoriale, le coordinate di un vettore rispetto alla base scelta sono i coefficienti della combinazione lineare con cui si esprime il vettore in termini degli elementi della base.

Considera uno spazio vettoriale V e una base $\{v_1, v_2, \dots, v_n\}$ per questo spazio. Ogni vettore v in V può essere espresso in modo unico come una combinazione lineare dei vettori nella base:

$$v = c_1 v_1 + c_2 v_2 + \dots + c_n v_n$$

Le "coordinate di v rispetto alla base" sono gli scalari c_1, c_2, \dots, c_n che rappresentano la combinazione lineare di v rispetto a quella specifica base.

Ad esempio, supponiamo di avere la base canonica in \mathbb{R}^3 :

- $e_1 = (1, 0, 0)$
- $e_2 = (0, 1, 0)$
- $e_3 = (0, 0, 1)$

Se vogliamo rappresentare il vettore $v = (2, 3, 1)$ rispetto a questa base canonica, troviamo gli scalari c_1, c_2, c_3 che soddisfano l'equazione:

$$v = c_1 e_1 + c_2 e_2 + c_3 e_3$$

Sostituendo i vettori e risolvendo il sistema di equazioni, otteniamo $c_1 = 2, c_2 = 3$ e $c_3 = 1$. Questi sono i valori delle "coordinate di v rispetto alla base canonica", e rappresentano come v può essere scritto come combinazione lineare dei vettori elementari.

In generale, le coordinate di una base sono fondamentali per rappresentare e lavorare con vettori in uno spazio vettoriale. Forniscono un meccanismo per "misurare" la contribuzione di ciascun vettore nella base nella composizione del vettore desiderato.

Data quindi una matrice A , sapendo il suo rango k ed essendo stata ridotta ad U in forma ridotta di Gauss.

1 U ha k colonne dominanti ($\text{rk } A = k$)

$A = [\underline{a}_1 \ \underline{a}_2 \ \dots \ \underline{a}_m]$ $U = [\underline{u}_1 \ \underline{u}_2 \ \dots \ \underline{u}_m]$

sono esse: $\underline{u}_{i_1}, \underline{u}_{i_2}, \dots, \underline{u}_{i_k}$

Una base B di $C(A)$ è l'unione DEUE COLONNE
di A CORRISPONDENTI AUE COLONNE DOMINANTI DI U

$$B = \{\underline{a}_{i_1}, \underline{a}_{i_2}, \dots, \underline{a}_{i_k}\}$$

NB1 $\dim C(A) = |B| = k = \text{rk } A$

NB2 $\dim C(A) = \text{rk } A = \text{rk } U = \dim C(U)$

MA $C(A) \neq C(U)$ in generale, per es.

$\{\underline{u}_{i_1}, \underline{u}_{i_2}, \dots, \underline{u}_{i_k}\}$ è una base di $C(U)$ MA PUÒ NON

ESSERE UNA BASE DI $C(A)$

Esempio $A = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix} \xrightarrow{E_{2,1}(-1)} \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} = U$

Una base di $C(A)$ è $\left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$

una base di $C(U)$ è $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$

ATTENZIONE: $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$ NON È UNA BASE DI $C(A)$

addirittura $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\} \not\subseteq C(A) = \left\{ \begin{bmatrix} \alpha & 1 \\ \beta & 2 \end{bmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$
 $= \left\{ \delta \begin{bmatrix} 1 \\ 1 \end{bmatrix} \mid \delta \in \mathbb{C} \right\}$

2 $A = \begin{bmatrix} \underline{s}_1^T \\ \vdots \\ \underline{s}_m^T \end{bmatrix} \rightsquigarrow U = \begin{bmatrix} \underline{s}_1^T \\ \vdots \\ \underline{s}_k^T \\ 0^T \\ \vdots \\ 0^T \end{bmatrix}_{m-k} \left\{ \begin{array}{l} k = \text{rk } A \\ \underline{s}_i^T \neq 0^T \end{array} \right. \}$

U ha le prime k righe non nulle (e le altre $m-k$ nulle)

Si ha che $R(A) = R(U)$ e che una base D

d' $R(A) = R(U)$ è

$$D = \left\{ \bar{s}_1, \bar{s}_2, \dots, \bar{s}_k \right\}$$

$$\boxed{3} \quad N(A) = \{ \underline{x} \mid A\underline{x} = \underline{0} \} \subseteq \mathbb{C}^n \quad A_{m \times n}$$

$$[A|\underline{0}] \sim [U|\underline{0}]$$

$A\underline{x} = \underline{0}$ è equivalente a $U\underline{x} = \underline{0}$

quindi:

$$\boxed{\text{NB}} \quad \underline{N(A) = N(U)}$$

TEOREMA NULLITÀ + RANGO

$$\dim N(A) = (\underset{\text{colonne di } A}{\text{numero delle}}) - r_{\text{r}A} = m - k$$

$A_{m \times n}$
 $r_{\text{r}A} = k$

Il "teorema della nullità più il rango" è un importante risultato nell'ambito dell'algebra lineare che fornisce una relazione tra la dimensione dello spazio nullo di una matrice ($N(A)$) e la dimensione dello spazio delle colonne di quella matrice ($C(A)$). Questo teorema è spesso indicato come "teorema fondamentale delle matrici" ed è una conseguenza diretta dell'approccio algebrico al concetto di rango.

Il teorema afferma che per una qualsiasi matrice A , la somma della dimensione dello spazio nullo ($N(A)$) e della dimensione dello spazio delle colonne ($C(A)$) è uguale al numero di colonne della matrice A , ovvero il suo numero di variabili o dimensione. Formalmente:

$$\text{nullità}(A) + \text{rango}(A) = \text{numero di colonne di } A$$

Dove:

- $\text{nullità}(A)$ è la dimensione dello spazio nullo di A , cioè il numero di soluzioni del sistema omogeneo $A\underline{x} = \underline{0}$.
- $\text{rango}(A)$ è il rango di A , cioè il numero massimo di colonne linearmente indipendenti in A .

Questo teorema riflette la relazione tra le dimensioni dei diversi spazi che sono associati a una matrice. In altre parole, se il rango di una matrice è r , significa che ci sono r colonne linearmente indipendenti, quindi le restanti colonne sono dipendenti. La somma di r e del numero di variabili rimanenti (cioè il numero totale di colonne) rappresenta l'intera dimensione dello spazio vettoriale in cui operiamo.

Consideriamo un [sistema lineare omogeneo](#)

$$(*) \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

ossia un [sistema lineare](#) in cui i termini noti delle equazioni che lo compongono sono tutti nulli. Scriviamo la matrice incompleta A associata al sistema, vale a dire la matrice dei coefficienti delle incognite

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

La **dimensione dello spazio delle soluzioni di sistema lineare omogeneo** è data dalla differenza tra il numero delle incognite e il rango della matrice A .

All'atto pratico, dato un sistema lineare omogeneo $(*)$, per trovare la dimensione dello spazio delle soluzioni occorre:

- 1) scrivere la matrice dei coefficienti associata al sistema, quella che abbiamo indicato con A ;
- 2) determinare il [rango](#) di A ;
- 3) sottrarre dal numero n di incognite del sistema il rango della matrice.

Per trovare una base dello spazio delle soluzioni di un sistema lineare omogeneo $Ax = 0$, dove A è una matrice e x è un vettore di incognite, segui questi passaggi:

1. **Scrivi il sistema omogeneo:** Scrivi il sistema di equazioni lineari omogeneo nella sua forma matriciale $Ax = 0$, dove A è la matrice dei coefficienti e x è il vettore delle incognite.
2. **Riduci la matrice a forma ridotta:** Utilizzando l'eliminazione gaussiana o altri metodi, riduci la matrice A alla sua forma ridotta a scala (RREF). Questo ti aiuterà a trovare le soluzioni parametriche del sistema.
3. **Trova le soluzioni parametriche:** Dalla forma ridotta a scala, individua le variabili libere (quelle che corrispondono a colonne senza pivot) e scrivi le soluzioni in termini di queste variabili libere. Questo ti darà le soluzioni parametriche del sistema.
4. **Esprimi le soluzioni in forma vettoriale:** Scrivi le soluzioni parametriche in forma vettoriale, dove le variabili libere diventano componenti del vettore.
5. **Costruisci una base delle soluzioni:** I vettori che compongono la base dello spazio delle soluzioni sono le soluzioni parametriche ottenute nell'ultimo passo. Assicurati che ogni vettore della base sia espressione delle variabili libere in modo indipendente.

In generale, se il sistema ha n variabili, la dimensione dello spazio delle soluzioni (nullità) sarà $n - \text{rango}(A)$, dove $\text{rango}(A)$ è il numero di pivot nella forma ridotta a scala di A . Pertanto, dovrai trovare $n - \text{rango}(A)$ vettori indipendenti come base dello spazio delle soluzioni.

Ecco un esempio semplificato per illustrare il processo:

Supponiamo di avere il sistema:

$$\begin{aligned}x + 2y + z &= 0 \\2x + 3y - z &= 0\end{aligned}$$

1. Scriviamo la matrice dei coefficienti A e il vettore delle incognite x :

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 3 & -1 \end{bmatrix}, \quad x = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

1. Riduciamo A alla forma ridotta a scala:

$$RREF(A) = \begin{bmatrix} 1 & 0 & \frac{3}{5} \\ 0 & 1 & -\frac{7}{5} \end{bmatrix}$$

1. Troviamo le soluzioni parametriche:

$$x = -\frac{3}{5}z, \quad y = \frac{7}{5}z, \quad z = z$$

1. Esprimiamo le soluzioni in forma vettoriale:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} -\frac{3}{5}z \\ \frac{7}{5}z \\ z \end{bmatrix} = z \begin{bmatrix} -\frac{3}{5} \\ \frac{7}{5} \\ 1 \end{bmatrix}$$

1. Costruiamo una base dello spazio delle soluzioni:

Una base dello spazio delle soluzioni è $\left\{ \begin{bmatrix} -\frac{3}{5} \\ \frac{7}{5} \\ 1 \end{bmatrix} \right\}$.

Questo vettore rappresenta tutte le possibili soluzioni del sistema omogeneo $Ax = 0$, e quindi costituisce una base per lo spazio delle soluzioni.

Una "base ordinata" è una base per uno spazio vettoriale in cui gli elementi sono organizzati in un ordine specifico. Questo ordine è solitamente importante quando si lavora con le coordinate dei vettori rispetto alla base o quando si vogliono rappresentare le combinazioni lineari in modo strutturato. Una base ordinata segue la stessa definizione di una base regolare, ma gli elementi sono disposti in una sequenza specifica.

Ad esempio, considera lo spazio vettoriale \mathbb{R}^3 con la base canonica ordinata:

$$\{e_1, e_2, e_3\} = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$$

Questa è una base ordinata perché gli elementi sono organizzati nell'ordine e_1 (primo elemento), e_2 (secondo elemento) e e_3 (terzo elemento).

Def Siano V sp. vett. su $K \in \{\mathbb{R}, \mathbb{C}\}$ e
 $B = \{v_1, \dots, v_n\}$ una base ordinata di V .
Per $v \in V$,

S' dice VETTORE DUE COORDINATE DEL VETTORE $v \in V$
RISPETTO ALLA BASE ORDINATA B: il vettore $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} \in K^n$
tale che $v = \sum_{i=1}^n \alpha_i v_i$. Si scrive
 $C_B(v) = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$

I "vettori delle coordinate rispetto a una base" sono rappresentazioni numeriche dei vettori in uno spazio vettoriale in termini della base specificata. In altre parole, quando hai una base di uno spazio vettoriale, puoi esprimere qualsiasi vettore in quel sistema vettoriale come una combinazione lineare dei vettori della base, e le "coordinate" sono i coefficienti di questa combinazione lineare.

Considera uno spazio vettoriale V con una base $\{v_1, v_2, \dots, v_n\}$. Un vettore v in V può essere rappresentato come:

$$v = c_1 v_1 + c_2 v_2 + \dots + c_n v_n$$

Dove c_1, c_2, \dots, c_n sono i coefficienti che rappresentano le "coordinate" del vettore v rispetto alla base data.

Ad esempio, considera lo spazio \mathbb{R}^2 con la base ordinata $\{(1, 0), (0, 1)\}$. Se vogliamo rappresentare il vettore $v = (3, 4)$ rispetto a questa base, calcoliamo i coefficienti c_1 e c_2 in modo che:

$$(3, 4) = c_1 \cdot (1, 0) + c_2 \cdot (0, 1)$$

Semplicemente, otteniamo $c_1 = 3$ e $c_2 = 4$. Le "coordinate" di $v = (3, 4)$ rispetto alla base ordinata sono $c_1 = 3$ e $c_2 = 4$.

Per ricavare una base da un sistema di generatori:

- Verifica dell'Indipendenza Lineare: Verifica se i vettori del sistema di generatori sono linearmente indipendenti. Questo è un passaggio cruciale perché una base deve consistere di vettori linearmente indipendenti.
- Seleziona i Vettori Linearmente Indipendenti: Se i vettori del sistema di generatori sono già linearmente indipendenti, allora hai già una base. In tal caso, non c'è bisogno di ulteriori passaggi. Questi vettori costituiranno la tua base.
- Seleziona Subset Linearmente Indipendente: Se i vettori del sistema di generatori sono linearmente dipendenti, dovrai selezionare un subset di vettori che siano linearmente indipendenti e costituiscano ancora un sistema di generatori. Questo subset costituirà la tua base.
- Aggiungi Vettori Aggiuntivi se Necessario: Se il subset selezionato nel passaggio precedente non genera tutto lo spazio vettoriale, dovrai aggiungere ulteriori vettori dal sistema di generatori originale finché non ottieni una base che sia linearmente indipendente che generatrice.
- Opzionale: Ordina la Base: Se hai bisogno di una base ordinata, puoi organizzare i vettori selezionati in un ordine specifico. Questo può semplificare i calcoli successivi.

Supponiamo che $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$ sia un sistema di generatori di V , che può eventualmente essere un [sottospazio](#) di un altro spazio vettoriale. Per quanto visto nella lezione sulle basi il discorso ha senso solamente se la [dimensione dello spazio vettoriale](#) V è minore della cardinalità dell'insieme di generatori, infatti in caso contrario:

- se $\dim(V) = n > m$, allora $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$ non può essere un sistema di generatori;
- se $\dim(V) = n = m$, allora $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$ è già una base di V . Questo perché la dimensione di uno spazio vettoriale è, per definizione, il numero di elementi di una sua qualsiasi base. L'unica possibilità per un sistema di n generatori di uno spazio vettoriale V di dimensione n è che essi costituiscano una base di V .

Che vuol dire *estrarre una base*? Significa sostanzialmente individuare un *sottoinsieme massimale di vettori linearmente indipendenti tra i generatori*, cioè individuare un sottoinsieme di generatori che siano:

- linearmente indipendenti e
- con il maggior numero possibile di vettori tra quelli dati (in questo senso *massimale*).

Estrarre una base col metodo degli scarti successivi

Sia $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$ un sistema di generatori per uno spazio vettoriale di dimensione $n < m$; per estrarne una base con il *metodo degli scarti successivi* dobbiamo attenerci ai seguenti passaggi.

- Consideriamo il primo vettore dell'insieme: \mathbf{v}_1 .

Se è uguale al vettore nullo ($\mathbf{v}_1 = \mathbf{0}$) lo scartiamo, se invece è diverso dal vettore nullo ($\mathbf{v}_1 \neq \mathbf{0}$) lo teniamo da parte.

- Consideriamo il secondo vettore \mathbf{v}_2 .

Lo teniamo da parte se $\mathbf{v}_2 \neq \mathbf{0}$ e se \mathbf{v}_1 è stato scartato, oppure se \mathbf{v}_1 è stato accettato e se \mathbf{v}_2 è indipendente da \mathbf{v}_1 . In caso contrario dobbiamo scartarlo.

- Consideriamo poi il terzo vettore \mathbf{v}_3 , che viene accettato solo se non è combinazione lineare dei vettori accettati in precedenza.

- Si continua in questo modo fino a esaurire tutti i vettori $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$.

I vettori che di volta in volta sono stati accettati formano una base estratta dal sistema di generatori.

L'altro metodo che presentiamo, che tra l'altro è il più usato, si basa sulla procedura di [eliminazione gaussiana](#).

Scriviamo i vettori del sistema di generatori $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m\}$ rendendone esplicite le coordinate rispetto a una qualsiasi base di V . Volendo fissare le idee, immaginiamo che sia $V = \mathbb{R}^n$ e che le coordinate dei vettori siano riferite alla base canonica.

$$\mathbf{v}_1 = (v_{11}, v_{21}, \dots, v_{n1})$$

$$\mathbf{v}_2 = (v_{12}, v_{22}, \dots, v_{n2})$$

⋮

$$\mathbf{v}_m = (v_{1m}, v_{2m}, \dots, v_{nm})$$

Nella precedente scrittura un generico elemento v_{ij} indica l' i -esima componente del vettore \mathbf{v}_j .

Disponiamo i vettori per colonne in una [matrice](#) che chiamiamo M e che è formata da n righe e m colonne.

$$M = \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1m} \\ v_{21} & v_{22} & \dots & v_{2m} \\ \vdots & \vdots & \dots & \vdots \\ v_{n1} & v_{n2} & \dots & v_{nm} \end{pmatrix}$$

Applichiamo il metodo di eliminazione gaussiana alla matrice M , e passiamo a una [matrice a scala](#) che indichiamo con M' . In questa nuova matrice c'è una serie di [pivot](#), dove con *pivot* si intende il primo elemento non nullo che si incontra leggendo ogni riga da sinistra verso destra.

Benissimo! Abbiamo praticamente finito:

- il numero di pivot rappresenta il [rango della matrice](#), cioè il massimo numero di vettori colonna linearmente indipendenti. In parole povere è la dimensione dello spazio generato dai vettori considerati inizialmente.

- I vettori colonna della matrice non ridotta M , che corrispondono ai vettori colonna della matrice ridotta M' che contengono i pivot, costituiscono una base dello spazio generato dal sistema di generatori.

Descriviamo ora il concetto di mappa delle coordinate:

Sia V uno spazio vettoriale su K , $K \in \{\mathbb{R}, \mathbb{C}\}$.

Finata una base ordinata $B = \{v_1, \dots, v_n\}$ di V , la funzione

$$c_B: V \longrightarrow K^n$$

$$v \longmapsto c_B(v)$$

si chiama LA MAPPA DELLE COORDINATE RISPETTO ALLA BASE ORDINATA B .

La "mappa delle coordinate" è un concetto che si riferisce alla trasformazione di un vettore rispetto a una base in uno spazio vettoriale in un vettore di coordinate rispetto alla stessa base. Questa mappa facilita il passaggio tra la rappresentazione geometrica e la rappresentazione algebrica dei vettori.

Supponiamo di avere uno spazio vettoriale V con una base $\{v_1, v_2, \dots, v_n\}$. La mappa delle coordinate, spesso denotata come $[\cdot]_B$, mappa ogni vettore v in V alle sue coordinate rispetto alla base B .

Se un vettore v può essere espresso come combinazione lineare dei vettori nella base B come:

$$v = c_1 v_1 + c_2 v_2 + \dots + c_n v_n$$

Allora le sue coordinate rispetto alla base B sono semplicemente i coefficienti c_1, c_2, \dots, c_n :

$$[v]_B = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$$

La mappa delle coordinate è utile perché permette di collegare gli aspetti geometrici e algebrici dei vettori. Con questa mappa, puoi rappresentare un vettore come una serie di numeri, i cui valori indicano quanto il vettore contribuisce lungo ciascun vettore della base.

Ad esempio, considera lo spazio vettoriale \mathbb{R}^2 con la base canonica $\{(1, 0), (0, 1)\}$. Se hai il vettore $v = (3, 4)$, le sue coordinate rispetto alla base canonica sono $[v]_{\text{canonica}} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$.

Ora il momento di introdurre una funzione nota come applicazione lineare:

Un'applicazione lineare, nota anche come trasformazione lineare o operatore lineare, è una corrispondenza tra due spazi vettoriali che preserva le operazioni di somma vettoriale e moltiplicazione per uno scalare. In altre parole, un'applicazione lineare mappa vettori da uno spazio vettoriale in un altro spazio vettoriale in modo che le proprietà delle operazioni vettoriali siano mantenute.

Formalmente, un'applicazione lineare T tra due spazi vettoriali V e W è una funzione che soddisfa le seguenti due proprietà:

1. **Preservazione della Somma:** Per ogni coppia di vettori u, v in V , l'applicazione lineare deve soddisfare:

$$T(u + v) = T(u) + T(v)$$

2. **Preservazione della Moltiplicazione Scalare:** Per ogni scalare c e ogni vettore v in V , l'applicazione lineare deve soddisfare:

$$T(c \cdot v) = c \cdot T(v)$$

Def Un' APPICAZIONE LINEARE è una funzione

$$f: V \rightarrow W$$

tale che

① V e W sono 'spaz' vettoriali sullo stesso K
(entrambi reali oppure entrambi complessi)

② $f(\underline{v}_1 + \underline{v}_2) = f(\underline{v}_1) + f(\underline{v}_2), \forall \underline{v}_1, \underline{v}_2 \in V$

③ $f(\alpha \underline{v}) = \alpha f(\underline{v}), \forall \underline{v} \in V, \forall \alpha \in K$

ESEMPI IMPORTANTI DI APPLICAZIONI LINEARI

1 V sp. vett. su $K \in \{\mathbb{R}, \mathbb{C}\}$

Fissato $\lambda \in K$

$$\begin{aligned} f_\lambda: V &\rightarrow V & \text{la moltiplicazione per lo scalare } \lambda \\ \underline{v} &\mapsto \lambda \underline{v} \end{aligned}$$

2 V sp. vett. su $K \in \{\mathbb{R}, \mathbb{C}\}$ con $\dim V = n$

B una base ordinata di V

$$\begin{aligned} C_B: V &\rightarrow K^n \\ \underline{v} &\mapsto C_B(\underline{v}) \end{aligned}$$

le esprese delle coordinate
rispetto alla base ordinata B

3) $A \in M_{m \times m}(\mathbb{C})$

$$f_A : \mathbb{C}^m \rightarrow \mathbb{C}^m$$
$$\underline{v} \mapsto A\underline{v}$$
$$\begin{matrix} m \times m & m \times 1 \\ m \times 1 & \end{matrix}$$

1) APPLICAZIONE LINEARE
INDOTTA DA (UNA
MATRICE) A

Un'applicazione lineare indotta, nota anche come mappa indotta o mappa derivata, è una trasformazione che avviene tra spazi vettoriali mediante una funzione. Questa funzione agisce sui vettori in uno spazio vettoriale di partenza e li mappa in un altro spazio vettoriale di arrivo. L'applicazione lineare indotta è specificamente definita per garantire che le proprietà di linearità siano rispettate.

Più formalmente, considera due spazi vettoriali V e W con le relative operazioni vettoriali e scalari. Supponiamo inoltre di avere un'applicazione (funzione) $f : V \rightarrow W$ che associa a ciascun vettore v in V un vettore w in W . Se f rispetta le proprietà di linearità, allora è un'applicazione lineare.

L'applicazione lineare indotta è una trasformazione che agisce sugli elementi di V e li mappa in W , mantenendo la struttura vettoriale di entrambi gli spazi. Ciò significa che l'applicazione lineare indotta preserva le operazioni di somma vettoriale e moltiplicazione per uno scalare in entrambi gli spazi.

La "matrice associata" a un'applicazione lineare rispetto a basi ordinate fisse sul dominio e sul codominio è una matrice che rappresenta l'effetto dell'applicazione lineare sulla base di partenza espressa in termini della base di arrivo. Questa matrice consente di collegare le coordinate dei vettori nei due spazi vettoriali attraverso l'applicazione lineare.

Consideriamo un'applicazione lineare $T : V \rightarrow W$ tra due spazi vettoriali V e W , e supponiamo di avere basi ordinate fisse:

- $\{v_1, v_2, \dots, v_n\}$ è la base ordinata di V .
- $\{w_1, w_2, \dots, w_m\}$ è la base ordinata di W .

La matrice associata A a T rispetto a queste basi è una matrice $m \times n$ in cui ogni colonna rappresenta le coordinate dei vettori di base di V rispetto alla base di W dopo aver subito la trasformazione lineare T .

Ogni colonna j della matrice A è ottenuta applicando l'applicazione lineare T al j -esimo vettore di base v_j di V e scrivendo il risultato come combinazione lineare dei vettori di base di W . Le coordinate di questa combinazione lineare costituiscono la colonna j della matrice A .

Formalmente, se $T(v_j) = c_{1j}w_1 + c_{2j}w_2 + \dots + c_{mj}w_m$, allora la colonna j della matrice A sarà $[c_{1j}, c_{2j}, \dots, c_{mj}]^T$.

La matrice associata A ci permette di calcolare l'azione dell'applicazione lineare T su qualsiasi vettore $v \in V$ rispetto alle basi date, usando la seguente relazione:

$$T(v) = A[v]_V$$

Dove $[v]_V$ rappresenta il vettore delle coordinate di v rispetto alla base di V .

La "matrice di passaggio" da una base ordinata a un'altra è una matrice che consente di trasformare le coordinate di un vettore da una base a un'altra base dello stesso spazio vettoriale. Questa matrice è utile quando si desidera calcolare le coordinate di un vettore rispetto a una nuova base, utilizzando le coordinate rispetto a una base di partenza.

Supponiamo di avere uno spazio vettoriale V e due basi ordinate:

- $\{v_1, v_2, \dots, v_n\}$ è la base di partenza.
- $\{w_1, w_2, \dots, w_n\}$ è la base di arrivo.

La matrice di passaggio P da $\{v_1, v_2, \dots, v_n\}$ a $\{w_1, w_2, \dots, w_n\}$ è una matrice $n \times n$ tale che la colonna j della matrice P rappresenta le coordinate del j -esimo vettore di base w_j rispetto alla base di partenza.

In altre parole, se $w_j = c_{1j}v_1 + c_{2j}v_2 + \dots + c_{nj}v_n$, allora la colonna j della matrice P sarà $[c_{1j}, c_{2j}, \dots, c_{nj}]^T$.

La matrice di passaggio P ha la proprietà che moltiplicando P per il vettore delle coordinate rispetto alla base di partenza, si ottengono le coordinate del vettore rispetto alla base di arrivo. Formalmente:

$$[v]_{\text{arrivo}} = P \cdot [v]_{\text{partenza}}$$

Dove:

- $[v]_{\text{partenza}}$ rappresenta il vettore delle coordinate di v rispetto alla base di partenza.
- $[v]_{\text{arrivo}}$ rappresenta il vettore delle coordinate di v rispetto alla base di arrivo.

La "regola del parallelogramma" è un concetto geometrico che è spesso utilizzato per verificare se una base è o meno ortogonale. In una base ortogonale, i vettori di base sono tutti mutuamente perpendicolari.

La regola del parallelogramma afferma che una base è ortogonale se e solo se per ogni coppia di vettori di base v_i e v_j , la seguente equazione è vera:

$$\langle v_i, v_j \rangle = 0 \quad \text{per ogni } i \neq j$$

Dove $\langle v_i, v_j \rangle$ rappresenta il prodotto scalare tra v_i e v_j .

In altre parole, in una base ortogonale, i vettori di base non hanno componenti in comune, e il prodotto scalare tra vettori diversi è zero. La base ortogonale semplifica molti calcoli e analisi geometriche in quanto riduce l'interazione tra i vettori di base.

Il completamento ad una base è un concetto utilizzato quando si ha uno spazio vettoriale generato da un insieme di vettori e si desidera trovare ulteriori vettori che, insieme agli originali, costituiscono una base completa per lo spazio vettoriale. In altre parole, il completamento ad una base estende l'insieme di vettori in modo da ottenere una base che copre tutto lo spazio.

Sia V uno spazio vettoriale di dimensione n definito su un campo \mathbb{K} e siano $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_p$, vettori linearmente indipendenti di V , con $p < n$.

Esistono allora $n - p$ vettori $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_{n-p}$ tali che l'insieme

$$\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_p, \mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_{n-p}\}$$

sia una base di V .

Esempio di completamento a base

Siano

$$\mathbf{v}_1 = (1, 1, 0), \mathbf{v}_2 = (1, 2, 0)$$

due vettori di $V = \mathbb{R}^3$. Verificare che sono linearmente indipendenti e completare l'insieme $\{\mathbf{v}_1, \mathbf{v}_2\}$ a una base di V .

Svolgimento: per verificare l'indipendenza lineare di \mathbf{v}_1 e \mathbf{v}_2 componiamo la matrice avente come colonne le coordinate dei vettori rispetto alla base canonica

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 0 & 0 \end{pmatrix}$$

Se ha rango massimo, cioè rango 2, i vettori sono linearmente indipendenti, in caso contrario non lo sono.

La sottomatrice di ordine 2 che si ottiene da A eliminando l'ultima riga ha determinante non nullo

$$\det \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = 1$$

dunque \mathbf{v}_1 e \mathbf{v}_2 sono linearmente indipendenti.

La dimensione dello spazio vettoriale $V = \mathbb{R}^3$ è $n = 3$, dunque per completare l'insieme $\{\mathbf{v}_1, \mathbf{v}_2\}$ (formato da $p = 2$ vettori) a una base di V è sufficiente scegliere

$$n - p = 3 - 2 = 1$$

ossia un vettore \mathbf{w} in modo tale che

$$\mathbf{v}_1, \mathbf{v}_2, \mathbf{w}$$

siano linearmente indipendenti tra loro.

Prendiamo, ad esempio, $\mathbf{w} = (1, 2, 3)$.

La matrice avente per colonne le componenti dei vettori $\mathbf{v}_1, \mathbf{v}_2, \mathbf{w}$ ha determinante non nullo

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 0 & 0 & 3 \end{pmatrix} = 3$$

I vettori sono allora linearmente indipendenti e quindi $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{w}\}$ è una base di $V = \mathbb{R}^3$.

L'**algoritmo di completamento a base** è un metodo meccanico ma efficace che consente di completare a base un qualsiasi insieme di vettori linearmente indipendenti di uno spazio vettoriale V .

Siano $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_p$ vettori linearmente indipendenti di V , con p minore della dimensione dello spazio vettoriale V e sia $\mathcal{B} = \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\}$ una base di V .

L'algoritmo di completamento a base prevede di considerare l'insieme

$$\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_p, \mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\}$$

che è evidentemente un sistema di generatori di V , e da esso estrarre una base con il metodo degli scarti successivi o con quello di eliminazione gaussiana, come spiegato nella lezione [come estrarre una base da un sistema di generatori](#).

Chi ha già affrontato la lezione precedente avrà anche letto a proposito dell'utilizzo del metodo dei minori, ma vi sconsigliamo di usarlo per risolvere questo genere di esercizi in quanto non garantisce che nella base estratta vi siano i vettori $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_p$, che invece vi devono appartenere necessariamente.

Basi ortogonali, ortonormali, autovalori, autovettori, diagonalizzazione

Per i tipi di base, distinguiamo:

- Le basi ortogonali, definite come tali se e solo se i vettori che le compongono sono a due a due ortogonali rispetto al prodotto scalare

In formule:

$$\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \text{ base ortogonale di } V \iff$$

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0 \text{ per ogni } i \neq j, \text{ con } i, j \in \{1, 2, \dots, n\}$$

In definitiva, data una base di uno spazio vettoriale su cui è definito un prodotto scalare, per **verificare se è una base ortogonale** è sufficiente stabilire se è formata da **vettori ortogonali** a due a due.

- Le basi ortonormali, cioè delle basi ortogonali in cui tutti i vettori hanno norma unitaria rispetto ad un fissato prodotto scalare

Una **base** $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ di V è una **base ortonormale** se e solo se:

- i vettori che la definiscono sono a due a due ortogonali rispetto al prodotto scalare $\langle \cdot, \cdot \rangle$;
- ciascun vettore della base ha norma 1.

In formule:

$$\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} \text{ base ortonormale di } V \iff$$

$$\begin{cases} \langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0 \text{ per ogni } i \neq j, \text{ con } i, j \in \{1, 2, \dots, n\} \\ \|\mathbf{v}_i\| := \sqrt{\langle \mathbf{v}_i, \mathbf{v}_i \rangle} = 1 \text{ per ogni } i \in \{1, 2, \dots, n\} \end{cases}$$

Un insieme di vettori $\{v_1, v_2, \dots, v_n\}$ in uno spazio vettoriale è ortogonale se $\langle v_i, v_j \rangle = 0$ per ogni coppia di vettori v_i e v_j nell'insieme, con $i \neq j$.

Ciò significa che se hai un insieme ortogonale, ogni coppia di vettori nell'insieme è perpendicolare e il loro prodotto scalare è nullo.

Normalizzare in questo contesto significa trasformare un insieme di vettori in un insieme ortonormale, cioè un insieme di vettori che sono sia ortogonali tra loro che di norma unitaria (lunghezza 1).

Quando normalizzi un insieme di vettori, stai dividendo ciascun vettore per la sua norma (lunghezza) in modo che diventi un vettore di lunghezza 1. In altre parole, stai proiettando ciascun vettore nell'insieme sulla sfera unitaria centrata nell'origine.

Supponiamo di avere un insieme di vettori ortogonali $\{v_1, v_2, \dots, v_n\}$ in uno spazio vettoriale. Per normalizzare questi vettori, calcoli il vettore normalizzato u_i associato a ciascun v_i dividendo v_i per la sua norma:

$$u_i = \frac{v_i}{\|v_i\|}$$

Dopo la normalizzazione, gli u_i saranno unitari (di lunghezza 1) e continueranno a essere mutuamente ortogonali (poiché il fattore di scala non influisce sulla loro ortogonalità).

Un "insieme ortonormale" è un insieme di vettori in uno spazio vettoriale in cui ogni vettore è di norma unitaria (lunghezza 1) e tutti i vettori sono mutuamente perpendicolari (ortogonali) tra loro. In altre parole, un insieme ortonormale è un insieme di vettori che soddisfa entrambe le condizioni di ortogonalità e normalizzazione.

Considera uno spazio vettoriale V dotato di un prodotto scalare (interno) $\langle \cdot, \cdot \rangle$. Un insieme $\{v_1, v_2, \dots, v_n\}$ di vettori in V è definito come:

Insieme Ortonormale: Se $\langle v_i, v_j \rangle = 0$ per ogni coppia di vettori v_i e v_j nell'insieme, con $i \neq j$, e $\|v_i\| = 1$ per ogni i .

In altre parole, in un insieme ortonormale, i vettori sono sia ortogonali che di norma unitaria.

Ciò significa che:

1. Ogni coppia di vettori nell'insieme è perpendicolare tra loro, quindi $\langle v_i, v_j \rangle = 0$ per $i \neq j$.
2. Ogni vettore nell'insieme ha una norma (lunghezza) di 1, quindi $\|v_i\| = 1$.

Una base ortogonale (rispettivamente ortonormale) è una base che è anche un insieme ortogonale.

Una "base ortogonale" è una base per uno spazio vettoriale in cui i vettori di base sono tra loro perpendicolari (ortogonali). In altre parole, una base ortogonale è un insieme di vettori di base che soddisfa la condizione di ortogonalità.

Più formalmente, una base $\{v_1, v_2, \dots, v_n\}$ per uno spazio vettoriale V è definita come una base ortogonale se $\langle v_i, v_j \rangle = 0$ per ogni coppia di vettori v_i e v_j nella base, con $i \neq j$.

In una base ortogonale, i vettori di base sono perpendicolari tra loro e non hanno componenti in comune, il che semplifica notevolmente i calcoli, specialmente quando si tratta di prodotti scalari, proiezioni, decomposizioni e altre operazioni.

Una "base ortonormale" è una base ortogonale in cui i vettori di base sono anche di norma unitaria (lunghezza 1). Quindi, una base ortonormale è sia un insieme ortogonale che un insieme di vettori di norma unitaria.

In sintesi:

- Una base ortogonale è un insieme di vettori di base che sono ortogonali tra loro, ma non necessariamente di norma unitaria.
- Una base ortonormale è un insieme di vettori di base che sono sia ortogonali che di norma unitaria.

Dato S un insieme di generatori di V , possiamo costruire S_0 come insieme di generatori ortogonale di V attraverso l'algoritmo di Gram-Schmidt.

Questo è un metodo utilizzato per trasformare una base lineare qualsiasi in una base ortogonale o ortonormale. Questo algoritmo è particolarmente utile nell'ambito dell'algebra lineare e ha applicazioni in diverse aree, come la risoluzione di sistemi lineari, la diagonalizzazione di matrici e altro ancora.

Al fine di costruire una base ortonormale di V , si normalizzano i vettori di una base ortogonale.

L'obiettivo dell'algoritmo di Gram-Schmidt è partire da una base lineare $\{v_1, v_2, \dots, v_n\}$ di uno spazio vettoriale e costruire una nuova base $\{u_1, u_2, \dots, u_n\}$ in cui ciascun vettore u_i sia ortogonale a tutti i vettori precedenti u_1, u_2, \dots, u_{i-1} .

Ecco come funziona l'algoritmo di Gram-Schmidt:

1. Inizializzazione: Parti con la base di partenza $\{v_1, v_2, \dots, v_n\}$.
2. Calcolo dei Vettori Ortogonali: Calcola il primo vettore u_1 come il vettore v_1 stesso.
3. Per $i = 2$ a n :
 - Proietta v_i sugli u_j precedenti, $j = 1, 2, \dots, i - 1$, per ottenere le componenti parallele ai vettori precedenti.
 - Sottrai queste componenti parallele da v_i per ottenere una componente ortogonale a tutti i vettori precedenti.
 - Normalizza il vettore ottenuto per ottenere u_i (se si desidera una base ortonormale).
4. Alla fine, avrai ottenuto una nuova base $\{u_1, u_2, \dots, u_n\}$ che è ortogonale (o ortonormale, se normalizzata) rispetto alla base di partenza.

In formule, il processo di proiezione e sottrazione per ottenere la componente ortogonale di v_i rispetto agli u_j precedenti può essere espresso come:

$$u_i = v_i - \sum_{j=1}^{i-1} \frac{\langle v_i, u_j \rangle}{\langle u_j, u_j \rangle} u_j$$

Dove $\langle \cdot, \cdot \rangle$ rappresenta il prodotto scalare e u_j sono i vettori ortogonali già calcolati.

L'algoritmo di Gram-Schmidt è un processo iterativo che costruisce una base ortogonale o ortonormale in uno spazio vettoriale, migliorando la proprietà di ortogonalità in ogni passaggio.

Ho $\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n$ e costruisco $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_n$

$$\underline{u}_1 = \underline{v}_1$$

$$\underline{u}_2 = \underline{v}_2 - \alpha_{12} \underline{u}_1$$

$$\alpha_{12} = \begin{cases} 0 & \text{se } \underline{u}_1 = \underline{0} \\ \frac{\langle \underline{u}_1, \underline{v}_2 \rangle}{\langle \underline{u}_1, \underline{u}_1 \rangle} & \text{se } \underline{u}_1 \neq \underline{0} \end{cases}$$

$$\underline{u}_3 = \underline{v}_3 - \alpha_{13} \underline{u}_1 - \alpha_{23} \underline{u}_2$$

$$\alpha_{13} = \begin{cases} 0 & \text{se } \underline{u}_1 = \underline{0} \\ \frac{\langle \underline{u}_1, \underline{v}_3 \rangle}{\langle \underline{u}_1, \underline{u}_1 \rangle} & \text{se } \underline{u}_1 \neq \underline{0} \end{cases}$$

$$\alpha_{23} = \begin{cases} 0 & \text{se } \underline{u}_2 = \underline{0} \\ \frac{\langle \underline{u}_2, \underline{v}_3 \rangle}{\langle \underline{u}_2, \underline{u}_2 \rangle} & \text{se } \underline{u}_2 \neq \underline{0} \end{cases}$$

$$\underline{u}_4 = \underline{v}_4 - \alpha_{14} \underline{u}_1 - \alpha_{24} \underline{u}_2 - \alpha_{34} \underline{u}_3 \text{ eccetera ...}$$

$$\underline{u}_j = \underline{v}_j - \sum_{i=1}^{j-1} \alpha_{ij} \underline{u}_i$$

dove

$$\alpha_{ij} = \begin{cases} 0 & \text{se } \underline{u}_i = \underline{0} \\ \frac{\langle \underline{u}_i | \underline{v}_j \rangle}{\langle \underline{u}_i | \underline{u}_i \rangle} & \text{se } \underline{u}_i \neq \underline{0} \end{cases}$$

Vediamo un semplice esempio applicativo considerando la seguente base:

$$v_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \quad v_2 = \begin{bmatrix} -1 \\ 2 \\ 1 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 3 \\ 0 \\ -1 \end{bmatrix}$$

Eseguiamo l'algoritmo di Gram-Schmidt passo dopo passo:

1. Inizializzazione:

$$u_1 = v_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

2. Calcolo dei Vettori Ortogonali:

$$u_2 = v_2 - \frac{\langle v_2, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 = \begin{bmatrix} -1 \\ 2 \\ 1 \end{bmatrix} - \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -\frac{3}{2} \\ \frac{3}{2} \\ 1 \end{bmatrix}$$

3. Calcolo dei Vettori Ortogonali:

$$u_3 = v_3 - \frac{\langle v_3, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 - \frac{\langle v_3, u_2 \rangle}{\langle u_2, u_2 \rangle} u_2 = \begin{bmatrix} 3 \\ 0 \\ -1 \end{bmatrix} - \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} - \frac{6}{14} \begin{bmatrix} -\frac{3}{2} \\ \frac{3}{2} \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{9}{14} \\ -\frac{9}{14} \\ -\frac{5}{7} \end{bmatrix}$$

Ora, normalizziamo i vettori per ottenere una base ortonormale:

$$e_1 = \frac{u_1}{\|u_1\|} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}, \quad e_2 = \frac{u_2}{\|u_2\|} = \begin{bmatrix} -\frac{\sqrt{14}}{6} \\ \frac{\sqrt{14}}{6} \\ \frac{\sqrt{14}}{3} \end{bmatrix}, \quad e_3 = \frac{u_3}{\|u_3\|} = \begin{bmatrix} \frac{3}{\sqrt{14}} \\ \frac{3}{\sqrt{14}} \\ -\frac{5}{\sqrt{14}} \end{bmatrix}$$

Ora abbiamo ottenuto una base ortonormale $\{e_1, e_2, e_3\}$ a partire dalla base di partenza $\{v_1, v_2, v_3\}$ utilizzando l'algoritmo di Gram-Schmidt.

Consideriamo ad esempio:

Si trovi una base ortonormale del sottospazio di \mathbb{C}^4

$$V = \left\langle \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix}; \begin{pmatrix} i \\ 1 \\ 0 \\ -1 \end{pmatrix}; \begin{pmatrix} 0 \\ -1 \\ -1 \\ 1 \end{pmatrix}; \begin{pmatrix} 0 \\ 0 \\ 0 \\ i \end{pmatrix} \right\rangle.$$

1^oMODO

- 1 Troviamo una base \mathcal{B}_1 di V .

Poniamo

$$\mathbf{w}_1 = \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix}, \quad \mathbf{w}_2 = \begin{pmatrix} i \\ 1 \\ 0 \\ -1 \end{pmatrix}, \quad \mathbf{w}_3 = \begin{pmatrix} 0 \\ -1 \\ -1 \\ 1 \end{pmatrix}, \quad \mathbf{w}_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ i \end{pmatrix}$$

e costruiamo la matrice $\mathbf{A} = (\mathbf{w}_1 \quad \mathbf{w}_2 \quad \mathbf{w}_3 \quad \mathbf{w}_4)$, ossia una matrice tale che $C(\mathbf{A}) = V$.

$$\begin{aligned} \mathbf{A} &= \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 1 & -1 & 0 \\ i & 0 & -1 & 0 \\ 0 & -1 & 1 & i \end{pmatrix} \xrightarrow{E_{31}(-i)} \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & i \end{pmatrix} \xrightarrow{E_{42}(1)E_{32}(-1)} \\ &\rightarrow \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} \xrightarrow{E_{34}} \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{E_3(-i)} \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \mathbf{U} \end{aligned}$$

Dunque $\mathcal{B}_1 = \{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4\}$ è una base di $C(\mathbf{A}) = V$.

- 2 Troviamo una base ortogonale \mathcal{B}_2 di V : poniamo $\mathbf{v}_1 = \mathbf{w}_1, \mathbf{v}_2 = \mathbf{w}_2$ e $\mathbf{v}_3 = \mathbf{w}_4$, e applichiamo l'algoritmo di Gram-Schmidt a $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$.

$$\mathbf{u}_1 = \mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix}$$

$$\mathbf{u}_2 = \mathbf{v}_2 - \alpha_{12}\mathbf{u}_1, \quad \mathbf{u}_1 \neq \mathbf{0} \implies \alpha_{12} = \frac{(\mathbf{u}_1 | \mathbf{v}_2)}{(\mathbf{u}_1 | \mathbf{u}_1)}$$

$$(\mathbf{u}_1 | \mathbf{v}_2) = \mathbf{u}_1^H \mathbf{v}_2 = (1 \quad 0 \quad -i \quad 0) \begin{pmatrix} i \\ 1 \\ 0 \\ -1 \end{pmatrix} = i$$

$$(\mathbf{u}_1 | \mathbf{u}_1) = \mathbf{u}_1^H \mathbf{u}_1 = (1 \quad 0 \quad -i \quad 0) \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix} = 2$$

$$\implies \alpha_{12} = i/2$$

$$\mathbf{u}_2 = \mathbf{v}_2 - \alpha_{12}\mathbf{u}_1 = \\ = \mathbf{v}_2 - \frac{i}{2}\mathbf{u}_1 =$$

$$= \begin{pmatrix} i \\ 1 \\ 0 \\ -1 \end{pmatrix} - \frac{i}{2} \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{i}{2} \\ 1 \\ \frac{1}{2} \\ -1 \end{pmatrix}$$

$$\mathbf{u}_3 = \mathbf{v}_3 - \alpha_{13}\mathbf{u}_1 - \alpha_{23}\mathbf{u}_2,$$

$$\mathbf{u}_1 \neq \mathbf{0} \implies \alpha_{13} = \frac{(\mathbf{u}_1 | \mathbf{v}_3)}{(\mathbf{u}_1 | \mathbf{u}_1)}$$

$$(\mathbf{u}_1 | \mathbf{v}_3) = \mathbf{u}_1^H \mathbf{v}_3 = (1 \ 0 \ -i \ 0) \begin{pmatrix} 0 \\ 0 \\ 0 \\ i \end{pmatrix} = 0$$

$$\implies \alpha_{13} = 0$$

$$\mathbf{u}_2 \neq \mathbf{0} \implies \alpha_{23} = \frac{(\mathbf{u}_2 | \mathbf{v}_3)}{(\mathbf{u}_2 | \mathbf{u}_2)}$$

$$(\mathbf{u}_2 | \mathbf{v}_3) = \mathbf{u}_2^H \mathbf{v}_3 = \left(-\frac{i}{2} \ 1 \ \frac{1}{2} \ -1 \right) \begin{pmatrix} 0 \\ 0 \\ 0 \\ i \end{pmatrix} = -i$$

$$(\mathbf{u}_2 | \mathbf{u}_2) = \mathbf{u}_2^H \mathbf{u}_2 = \left(-\frac{i}{2} \ 1 \ \frac{1}{2} \ -1 \right) \begin{pmatrix} \frac{i}{2} \\ 1 \\ \frac{1}{2} \\ -1 \end{pmatrix} = \frac{5}{2}$$

$$\implies \alpha_{23} = -\frac{2}{5}i$$

Introduciamo altri concetti chiave:

- Un autovalore di una matrice è un numero scalare che rappresenta come un'operazione lineare (rappresentata dalla matrice) allunga o comprime un vettore.
- Un autovettore è il vettore associato a un determinato autovalore.

Si dice che lo scalare $\lambda_0 \in \mathbb{K}$ è un **autovalore** della matrice quadrata A se esiste un vettore colonna non nullo $\mathbf{v} \in \mathbb{K}^n$ tale che

$$A\mathbf{v} = \lambda_0\mathbf{v}$$

Il vettore \mathbf{v} è detto **autovettore relativo all'autovalore** λ_0 .

Autovalore (o Valore Proprio):

Un autovalore di una matrice è un numero scalare che rappresenta come un'operazione lineare (rappresentata dalla matrice) allunga o comprime un vettore. In altre parole, è uno scalare λ tale che esiste un vettore non nullo v tale che $Av = \lambda v$, dove A è la matrice associata alla trasformazione lineare. L'autovalore rappresenta il fattore di scala per il quale il vettore v viene moltiplicato quando sottoposto alla trasformazione lineare rappresentata da A .

Autovettore:

Un autovettore è il vettore associato a un determinato autovalore. In altre parole, se v è un autovettore di A con autovalore λ , allora $Av = \lambda v$. L'autovettore è la direzione in cui l'operazione lineare rappresentata dalla matrice allunga o comprime il vettore, mantenendolo nella stessa direzione.

In termini più semplici, gli autovalori e gli autovettori forniscono informazioni su come una trasformazione lineare cambia o scala i vettori. Gli autovalori possono essere reali o complessi, e una matrice può avere più di un autovalore e più di un autovettore associato ad ogni autovalore. Gli autovettori associati allo stesso autovalore possono essere linearmente indipendenti, costituendo una base per lo spazio degli autovettori.

Gli autovettori relativi a uno stesso autovalore λ_0 di una matrice quadrata A di ordine n , insieme al vettore nullo, formano un **sottospazio vettoriale** di \mathbb{K}^n . Tale sottospazio prende il nome di **autospazio relativo all'autovalore** λ_0 , si indica con V_{λ_0} ed è definito nel modo seguente:

$$V_{\lambda_0} := \{\mathbf{v} \in \mathbb{K}^n \text{ tali che } A\mathbf{v} = \lambda_0 \mathbf{v}\}$$

Per completezza, dimostriamo che V_{λ_0} è un sottospazio vettoriale di \mathbb{K}^n .

Per **stabilire se un insieme è un sottospazio vettoriale** bisogna verificare se è chiuso rispetto alle operazioni di somma e di prodotto per uno scalare, cioè se per ogni $\mathbf{v}_1, \mathbf{v}_2 \in V_{\lambda_0}$ e per ogni $\alpha \in \mathbb{K}$ valgono le seguenti proprietà:

- 1) $\mathbf{v}_1 + \mathbf{v}_2 \in V_{\lambda_0}$
- 2) $\alpha \mathbf{v}_1 \in V_{\lambda_0}$

Introduciamo due precisazioni:

1. Autovalori di Matrici Triangolari

Una matrice triangolare è una matrice in cui tutti gli elementi al di sopra o al di sotto della diagonale principale sono nulli. Le matrici triangolari possono essere superiori (tutti gli elementi sotto la diagonale sono nulli) o inferiori (tutti gli elementi sopra la diagonale sono nulli).

Per le matrici triangolari, gli autovalori corrispondono agli elementi diagonali. In altre parole, gli autovalori di una matrice triangolare sono gli elementi che si trovano sulla diagonale principale. Questo perché gli autovettori associati a ciascun autovalore sono gli autovettori che hanno componenti non nulle solo nella colonna corrispondente all'autovalore (cioè, gli autovettori associati agli elementi diagonali). Poiché le matrici triangolari non cambiano la struttura della loro diagonale quando vengono moltiplicate per un vettore, è intuitivo che gli autovalori siano direttamente legati agli elementi diagonalmente.

2. Autovalori di Matrici Diagonali

Una matrice diagonale è una matrice triangolare sia superiore che inferiore, in cui tutti gli elementi al di sopra e al di sotto della diagonale principale sono nulli. In altre parole, tutti gli elementi non diagonali sono nulli.

Per le matrici diagonali, gli autovalori corrispondono direttamente agli elementi diagonali. Gli autovalori di una matrice diagonale sono gli elementi che si trovano sulla diagonale principale. Inoltre, gli autovettori associati agli autovalori sono gli autovettori che hanno componenti non nulle solo nella posizione corrispondente all'autovalore.

Nelle matrici diagonali, gli autovettori non cambiano direzione quando vengono moltiplicati per la matrice stessa, poiché ciascun componente dell'autovettore è scalato solo per l'autovalore corrispondente. Questo rende gli autovalori e gli autovettori delle matrici diagonali particolarmente semplici da calcolare e comprendere.

In sintesi, sia per le matrici triangolari che per le matrici diagonali, gli autovalori sono direttamente associati agli elementi diagonali, semplificando il calcolo e l'interpretazione delle proprietà degli autovalori e degli autovettori.

A proposito di autovalori, definiamo ora:

Molteplicità Algebrica:

La molteplicità algebrica di un autovalore è il numero di volte che l'autovalore appare come radice dell'equazione caratteristica della matrice. In altre parole, è la molteplicità delle radici dell'equazione polinomiale che si ottiene calcolando il determinante $|A - \lambda I|$, dove A è la matrice e λ è l'autovalore.

Ad esempio, se un autovalore λ appare con molteplicità algebrica 3, significa che l'equazione caratteristica ha tre radici uguali a λ .

Molteplicità Geometrica:

La molteplicità geometrica di un autovalore è il massimo numero di autovettori linearmente indipendenti associati a quell'autovalore. In altre parole, rappresenta la dimensione dello spazio degli autovettori associati all'autovalore.

Ad esempio, se un autovalore λ ha molteplicità geometrica 2, significa che esistono due autovettori linearmente indipendenti associati a λ .

Le molteplicità algebriche e geometriche possono essere uguali o diverse per un autovalore. Ecco alcuni scenari possibili:

1. Molteplicità Algebrica = Molteplicità Geometrica
 - a. In questo caso, ci sono abbastanza autovettori linearmente indipendenti per riempire tutto lo spazio degli autovettori associati all'autovalore.
2. Molteplicità Algebrica > Molteplicità Geometrica
 - a. Questo indica che l'autovalore ha più autovettori linearmente indipendenti di quanti ne siano necessari per formare lo spazio degli autovettori associati.
3. Molteplicità Algebrica < Molteplicità Geometrica
 - a. Questo indica che ci sono meno autovettori linearmente indipendenti di quanti ne sarebbero necessari.

Date due matrici $n \times n$ A e B , abbiamo che sono simili quando esiste S non singolare (invertibile) tale che

$$A = SBS^{-1}$$

Oppure anche:

Due matrici A e B si dicono "simili" se esiste una matrice invertibile P tale che $B = P^{-1}AP$. In altre parole, le matrici simili rappresentano la stessa trasformazione lineare espressa in sistemi di coordinate diversi, ciascuno definito dalla matrice P .

TEOREMA Siano A e B $(n \times n)$ simili. Allora

① $P_A(x) = P_B(x)$. Quindi:

- $\text{Spec } A = \text{Spec } B$
- $\forall \lambda \in \text{Spec } A$ si ha:

$$\left(\begin{array}{l} \text{le molteplicità} \\ \text{algebriche di } \lambda \\ \text{come autovetore di } A \end{array} \right) = \left(\begin{array}{l} \text{le molteplicità} \\ \text{algebriche di } \lambda \\ \text{come autovetore di } B \end{array} \right)$$

DUE MATRICI SIMILI
HANNO GLI STESSI
AUTOVALORI CON
LE STESSE MOLTE-
PLICITÀ ALGEBRICHES
E GEOMETRICHE

② $\forall \lambda \in \text{Spec } A$ $\dim E_A(\lambda) = \dim E_B(\lambda)$

mult. geometrica di λ come aut. di A \uparrow come autovetore di B

Possiamo definire inoltre la matrice diagonalizzabile, che è una matrice quadrata simile a una matrice diagonale. In altri termini una matrice A è diagonalizzabile se esiste una matrice invertibile P tale che $PD=AP$, dove D è una matrice diagonale dello stesso ordine di A .

Def A $n \times n$, A si dice DIAGONALIZZABILE

se è simile ad una matrice diagonale, cioè se

$\exists D$ diagonale
 $\exists S$ non singolare

tali che

$$A = SDS^{-1}$$

\uparrow non singolare \downarrow diagonale

oppure anche:

Sia A una matrice quadrata di ordine n a coefficienti in un campo \mathbb{K} . Si dice che A è una matrice diagonalizzabile se e solo se esiste una matrice invertibile P tale che $D = P^{-1}AP$, ossia

$$PD = AP$$

La matrice P è detta matrice diagonalizzante di A .

Il teorema di diagonalizzabilità stabilisce le condizioni sotto le quali una matrice può essere diagonalizzata. In particolare, il teorema afferma che una matrice quadrata A è diagonalizzabile se e solo se ha n autovettori linearmente indipendenti, dove n è la dimensione della matrice.

Eccone l'enunciato: una matrice quadrata A è diagonalizzabile in un campo \mathbb{K} se e solo se valgono le seguenti condizioni:

- 1) il numero degli autovalori di A appartenenti al campo \mathbb{K} e contati con la loro molteplicità è pari all'ordine della matrice;
- 2) la molteplicità geometrica di ciascun autovalore coincide con la relativa molteplicità algebrica.

Prima di vedere un esempio richiamiamo la vostra attenzione su alcuni casi particolari, utili a far risparmiare qualche passaggio negli esercizi.

- A) Se $A = (a_{ij})$ è una matrice simmetrica, cioè se $a_{ij} = a_{ji}$ per ogni $i \neq j$, allora A è diagonalizzabile.
- B) Se A è una matrice quadrata di ordine n che ammette esattamente n autovalori distinti in \mathbb{K} , allora A è diagonalizzabile nel campo \mathbb{K} .
- C) Se $\mathbb{K} = \mathbb{C}$ o, più in generale, \mathbb{K} è un campo algebricamente chiuso, il punto 1) del teorema di diagonalizzabilità è verificato in automatico, infatti il numero degli autovalori (contati con la loro molteplicità) è il numero delle radici del polinomio caratteristico associato ad A , che ha grado pari all'ordine della matrice. Come stabilito da un corollario del teorema fondamentale dell'Algebra, in un campo algebricamente chiuso il numero delle radici di un polinomio è pari al grado di quest'ultimo.

Infine, indicando con $m_a(\lambda_0)$ la molteplicità algebrica e con $m_g(\lambda_0)$ la molteplicità geometrica dell'autovalore λ_0 , è utile ricordare che

$$1 \leq m_g(\lambda_0) \leq m_a(\lambda_0) \leq n$$

Dalla precedente relazione si deduce che se un autovalore ha molteplicità algebrica pari a 1, allora è pari a 1 anche la sua molteplicità geometrica.

Prima di introdurre le matrici diagonalizzabili, occorre necessariamente parlare di:

Matrice Unitaria:

Una matrice U è detta "unitaria" se la sua trasposta coniugata (trasposta e coniugata di ciascun elemento) è uguale all'inversa della matrice stessa. In altre parole, una matrice U è unitaria se $U^*U = UU^* = I$, dove I è la matrice identità. Le matrici unitarie preservano la norma euclidea, il prodotto scalare e l'angolo tra vettori, rendendole particolarmente utili in diverse applicazioni, come la diagonalizzazione di matrici hermitian e la risoluzione di sistemi lineari.

Matrice Ortogonale:

Una matrice Q è detta "ortogonale" se la sua trasposta è uguale all'inversa della matrice stessa. In altre parole, una matrice Q è ortogonale se $Q^TQ = QQ^T = I$, dove I è la matrice identità. Le matrici ortogonal preservano le lunghezze dei vettori e gli angoli tra di essi, quindi sono spesso utilizzate per rappresentare trasformazioni lineari che preservano queste proprietà.

Matrice Normale:

Una matrice N è detta "normale" se commuta con la sua trasposta coniugata: $NN^* = N^*N$. Le matrici normali sono importanti perché possono essere diagonalizzate da una matrice unitaria. In altre parole, esiste una matrice unitaria U tale che U^*NU è una matrice diagonale.

Unitarily Diagonalizable (Unitariamente Diagonalizzabile):

Una matrice A è unitariamente diagonalizzabile se può essere diagonalizzata attraverso una matrice unitaria U . Questo significa che esiste una matrice unitaria U tale che U^*AU è una matrice diagonale. Le matrici unitariamente diagonalizzabili sono particolarmente interessanti perché le matrici unitarie preservano le proprietà geometriche importanti, come la norma euclidea e gli angoli tra vettori. Quindi, le matrici unitariamente diagonalizzabili possono semplificare notevolmente l'analisi delle trasformazioni lineari rappresentate da tali matrici.

Lo spettro di una matrice è un concetto importante nell'ambito della teoria delle matrici e dell'analisi lineare. Si riferisce all'insieme dei valori propri (autovalori) della matrice.

Gli autovalori di una matrice sono numeri scalari che, quando moltiplicati per un vettore, danno un vettore parallelo a quello iniziale, in altre parole, non cambiano la sua direzione, ma possono solo scalare il vettore. Lo spettro di una matrice può essere visto come una generalizzazione dei concetti di radici di un polinomio alle matrici.

Teorema Spettrale (Versione Additiva):

Il Teorema Spettrale, nella sua versione additiva, si applica alle matrici simmetriche. Afferma che ogni matrice simmetrica reale può essere diagonalizzata da una matrice di autovettori ortogonali. In altre parole, se A è una matrice simmetrica, allora esiste una matrice ortogonale P e una matrice diagonale D tali che:

$$A = PDP^{-1}$$

Dove D ha gli autovalori di A sulla diagonale. Questo teorema è di fondamentale importanza nella risoluzione di problemi legati a matrici simmetriche, come nella risoluzione di equazioni differenziali alle derivate parziali.

Il Teorema Spettrale versione additiva riguarda le matrici simmetriche e stabilisce che ogni matrice simmetrica reale può essere diagonalizzata da una matrice di autovettori ortogonali.

Teorema Spettrale (Versione Moltiplicativa):

Il Teorema Spettrale, nella sua versione moltiplicativa, si applica alle matrici normali, che includono sia le matrici simmetriche che le matrici hermitiane (complesse). Questo teorema generalizza il concetto di diagonalizzabilità per le matrici normali. Afferma che ogni matrice normale A può essere scritta come:

$$A = UDU^*$$

Dove U è una matrice unitaria (o hermitiana nel caso complesso) e D è una matrice diagonale contenente gli autovalori di A sulla diagonale. La matrice unitaria U rappresenta una base di autovettori ortonormali.

COSTRUZIONE DI D :

$$D = \begin{bmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & \lambda_2 & \\ & & & \ddots \\ & & & & \lambda_k \\ & & & & & \ddots \\ & & & & & & \lambda_k \end{bmatrix}$$

Le righe sono indicate da m_1 volte λ_1 , m_2 volte λ_2 , ..., m_k volte λ_k .
Le colonne sono indicate da $d_1 = m_1$, $d_2 = m_2$, ..., $d_k = m_k$.

$U = [Q_1 \ Q_2 \ \dots \ Q_k]$ è una matrice $n \times n$ con colonne orthonormali Q_i di dimensione m_i .

$$m_1 + m_2 + \dots + m_k = n$$

COSTRUZIONE DI U :

B_i^* è la base ortonormale di $E_A(\lambda_i)$, $i=1,\dots,k$
 Q_i è una matrice $n \times m_i$ che ha come colonne i vettori di B_i^* .

Metodi di conteggio, permutazioni, combinazioni, distribuzioni e relazioni di ricorrenza

I metodi di conteggio si basano sul contare oggetti di insiemi finiti.

Ci sono diversi principi fondamentali che stanno alla base dei metodi di conteggio:

- **Principio Fondamentale del Conteggio:** Questo principio afferma che se ci sono n modi di fare una prima operazione e m modi di fare una seconda operazione indipendentemente dalla prima, allora ci sono $n \times m$ modi di fare entrambe le operazioni in successione
 - **Principio di Somma:** Questo principio afferma che, se un evento può verificarsi in n modi diversi o in m modi diversi (senza sovrapposizione), allora ci sono $n + m$ modi in cui l'evento può verificarsi.

Dati: un insieme con n_1 effetti (è ordinabile d'istruzione)
" " n_2 effetti
" " n_m effetti

SE QUESTI' INSIEMI SONO A DUE A DUE DISGIUNTI'
 ALLORA il numero d' modi d' selezione su effetto da uno
 degli' m insiemmi è:

$$r_1 + r_2 + \dots + r_m$$

- **Principio di Moltiplicazione:** Questo principio è una generalizzazione del Principio Fondamentale del Conteggio e afferma che se ci sono n_1 modi di fare la prima operazione, n_2 modi di fare la seconda operazione dopo la prima, e così via fino a n_k modi di fare l'ultima operazione, allora ci sono $n_1 \times n_2 \times \dots \times n_k$ modi di fare tutte le operazioni in sequenza.

Dato una procedura che SI SPEZZA IN m FASI
SUCCESSIVE ORDINATE (IN RUOLO SEQUENZIALE)

SE

- a** IL NUMERO DI ESITI DI CIASCUNA FASE È INDEPENDENTE DAUE SCELTE FATTE NELE FASI PRECEDENTI

b Gli esiti finali della procedura (un "esito finale" è una composizione di m "esiti parziali") SONO TUTTI DISTINTI TRA loro

ANALISI: il numero dei differenti esiti finali della procedura è:

$\tau_1, \tau_2, \tau_3, \dots, \tau_m$

Ora tutti i modi di combinazione:

- Una "permutazione" di un insieme di elementi è un ordinamento diverso di quegli elementi. In altre parole, una permutazione rappresenta un modo di organizzare gli elementi in un ordine specifico.

Il numero di tutte le possibili permutazioni d'oggetti è:

$$P(m,m) = m \cdot (m-1) \cdot (m-2) \cdots 2 \cdot 1 = m!$$



 1º Poco 2º Poco 3º poco
 m-same poco
 m possibile anche d' un effetto nel 1º poco
 m-1 " " " " " " " "
 m-2 " " " " " " " "
 " 2º poco
 PENULTIMO POCO

m! m FATTORI DI

PER CONVENTIONE S' PONE $O! = 1$

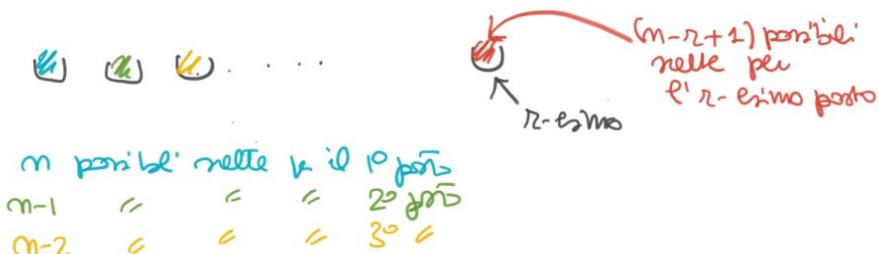
ESEMPIO quest'ora gli' autografi delle parla CIAO

$$m=4 \quad 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

- Una "r-permutazione" di un insieme di elementi è un ordinamento di r elementi presi dall'insieme, appunto presi con un ordine specifico.

Il numero di tutte le possibili r -permutazioni di m oggetti è:

$$P(m, r) = m \cdot (m-1) \cdot (m-2) \cdots (m-r+1)$$



N.B. $P(m, r) = m \cdot (m-1) \cdots (m-r+1) \cdot \frac{(m-r)!}{(m-r)!}$

Quindi

$$P(m, r) = \frac{m!}{(m-r)!}$$

N.B. $P(m, m) = \frac{m!}{(m-m)!} = \frac{m!}{0!} = \frac{m!}{1} = m!$

usando il precedente N.B. con $r=m$

PER CONVENZIONE $0!=1$

Possiamo inoltre descrivere:

- Una "combinazione" di un insieme di elementi è una selezione di elementi senza considerare l'ordine. In altre parole, una combinazione rappresenta un insieme di elementi scelti dall'insieme, ma l'ordine di scelta non è rilevante. Il numero di combinazioni possibili di un insieme di n elementi è 2^n , dove ogni elemento può essere incluso o escluso.
- Una "r-combinazione", descritta come selezione non ordinata di r degli n oggetti (un sottoinsieme di r oggetti dell'insieme degli n oggetti)

Il numero di tutte le possibili r -combinazioni

di m oggetti è indicato con il simbolo $C(m, r)$

Lo calcolo:

in una π -permutazione

- prima scegli r effetti tra n , e lo puoi fare in $C(n, r)$ modi
- poi ordini gli r effetti nell', e lo puoi fare in $r!$ modi

$$P(n, r) = C(n, r) \cdot r!$$

Da cui s'ricava:

$$\begin{aligned} C(n, r) &= \frac{P(n, r)}{r!} = \frac{n!}{(n-r)!} \cdot \frac{1}{r!} = \\ &= \frac{n!}{(n-r)! r!} = \binom{n}{r} \quad \begin{array}{l} \text{r' chiamer} \\ \text{COEFFICIENTE} \\ \text{BINOMIALE} \end{array} \\ &\quad \begin{array}{l} \text{r' indicav} \\ \text{e} \end{array} \end{aligned}$$

NB Per convenzione si pone

$$\binom{m}{k} = 0 \quad \text{se} \quad 0 \leq m < k$$

ESEMPIO Ci sono 7 donne e 4 uomini e tra loro dobbiamo scegliere un comitato formato da 3 donne e 2 uomini.

Quante possibilità abbiamo?

PRINCIPIO DI MOLTIPLICAZIONE

1^a fase: mette d' 3 donne he 7 : $r_1 = \binom{7}{3}$ possibilità

2^a fase: // " 2 uomini // 4 : $r_2 = \binom{4}{2}$ //

NB le scelte degli uomini è indipendente dalle scelte delle donne

Le possibilità d' mette del comitato sono:

$$\begin{aligned} r_1 \cdot r_2 &= \binom{7}{3} \cdot \binom{4}{2} = \frac{7!}{3!(7-3)!} \cdot \frac{4!}{2!(4-2)!} = \frac{7!}{3!4!} \cdot \frac{4!}{2!2!} = \frac{7!}{3! \cdot 2 \cdot 2} = \\ &= \frac{7 \cdot 6 \cdot 5 \cdot \cancel{4} \cdot \cancel{(3!)}}{\cancel{(3!) \cdot 2 \cdot 2}} = 7 \cdot 6 \cdot 5 = 7 \cdot 30 = 210 \end{aligned}$$

La "formula binomiale", nota anche come "teorema del binomio", è una formula matematica che esprime il risultato dell'elevamento a potenza di un binomio $a + b$ alla n -esima potenza. La formula è spesso utilizzata per espandere l'espressione $(a + b)^n$ senza dover scrivere esplicitamente tutti i termini nell'espansione.

La formula binomiale è data da:

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

Dove:

- a e b sono numeri reali o variabili.
- n è un numero intero non negativo.
- $\binom{n}{k}$ rappresenta il coefficiente binomiale, che rappresenta il numero di modi in cui è possibile scegliere k elementi da un insieme di n elementi. È calcolato come $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

La formula binomiale è utilizzata per calcolare espansioni di potenze del binomio, come $(a + b)^2$, $(a + b)^3$, ecc. Per esempio, l'espressione $(a + b)^2$ può essere espansa utilizzando la formula binomiale come:

$$(a + b)^2 = \binom{2}{0} a^2 + \binom{2}{1} ab + \binom{2}{2} b^2 = a^2 + 2ab + b^2$$

Per corollario, i successivi:

COROLLARIO (TEOREMA BINOMIALE)

$$(1+x)^m = \sum_{k=0}^m \binom{m}{k} x^k$$

IDENTITÀ BINOMIALI

$m, k \in \mathbb{N}$, $k \leq m$

1 $\binom{m}{k} = \binom{m}{m-k}$

IN modo COMBINATORIO: scegliere k oggetti
equivale a scegliere gli $m-k$ oggetti da togliere

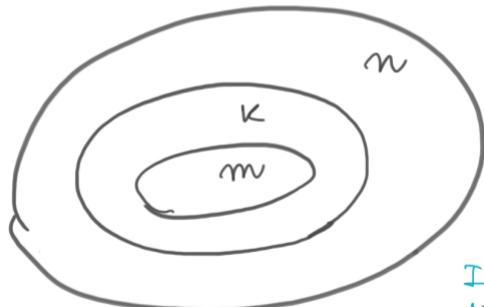
2 $\binom{m}{k} = \binom{m-1}{k} + \binom{m-1}{k-1}$ per $k \leq m-1$

IN modo COMBINATORIO: "ETICHETTO" uno degli n
oggetti. "Lo dipingo al giallo"

$$[3] \quad 0 \leq m \leq k \leq n$$

$$\binom{n}{k} \binom{k}{m} = \binom{n}{m} \binom{n-m}{k-m}$$

IN modo COMBINATORIO : selezione di comitati:



n = numero degli elettori

k = numero dei componenti della giunta comunale

m = numero degli assessori

In esercizio ci sono due modi diversi di contare le possibili scelte d'assessori per la giunta comunale:

1^o MODO:

(NB in entrambi i modi si applica il principio di moltiplicazione)

$$\binom{n}{k} \binom{k}{m} = \left(\begin{array}{l} \text{prima selezione} \\ k \text{ membri delle} \\ \text{funte tra gli} \\ n \text{ elettori} \end{array} \right) \cdot \left(\begin{array}{l} \text{poi selezione} \\ m \text{ assessori} \\ \text{tra i } k \text{ membri} \\ \text{delle funte} \end{array} \right)$$

\hookrightarrow $\binom{n}{k}$ scelte \hookrightarrow $\binom{k}{m}$ scelte

2^o MODO:

$$\binom{n}{m} \binom{n-m}{k-m} = \left(\begin{array}{l} \text{prima selezione} \\ \text{di } m \text{ assessori} \\ \text{tra gli } n \text{ elettori} \end{array} \right) \left(\begin{array}{l} \text{poi selezione} \\ \text{di } k-m \text{ membri} \\ \text{delle funte} \\ \text{che non sono} \\ \text{assessori} \end{array} \right)$$

\hookrightarrow $\binom{n}{m}$ scelte \hookrightarrow $\binom{n-m}{k-m}$ scelte

Dunque $\binom{n}{k} \binom{k}{m} = \binom{n}{m} \binom{n-m}{k-m}$

ESEMPPIO In un scaffale ci sono 7 libri distinti in inglese,

5 libri distinti in tedesco, 10 libri distinti in italiano.

In quanti modi posso scegliere delle libri scelti in due lingue diverse?

NB Una scelta è una coppia **NON ORDINATA** di libri

PRINCIPIO DI ADDIZIONE: sommo le possibili scelte da cui ho:

$$\left(\begin{array}{l} 1 \text{ libro in inglese} \\ 1 \text{ libro in tedesco} \end{array} \right) \cup \left(\begin{array}{l} 1 \text{ libro in inglese} \\ 1 \text{ libro in italiano} \end{array} \right) \cup \left(\begin{array}{l} 1 \text{ libro in tedesco} \\ 1 \text{ libro in italiano} \end{array} \right)$$

$\times \rightarrow \quad Y \rightarrow \quad Z \rightarrow$

PRINCIPIO DI MOLTIPLICAZIONE:

$$|X| = ? \quad r_1 = 7 \text{ ed } r_2 = 5 \Rightarrow |X| = 7 \cdot 5 = 35$$

$$|Y| = ? \quad r_1 = 7 \text{ ed } r_2 = 10 \Rightarrow |Y| = 7 \cdot 10 = 70$$

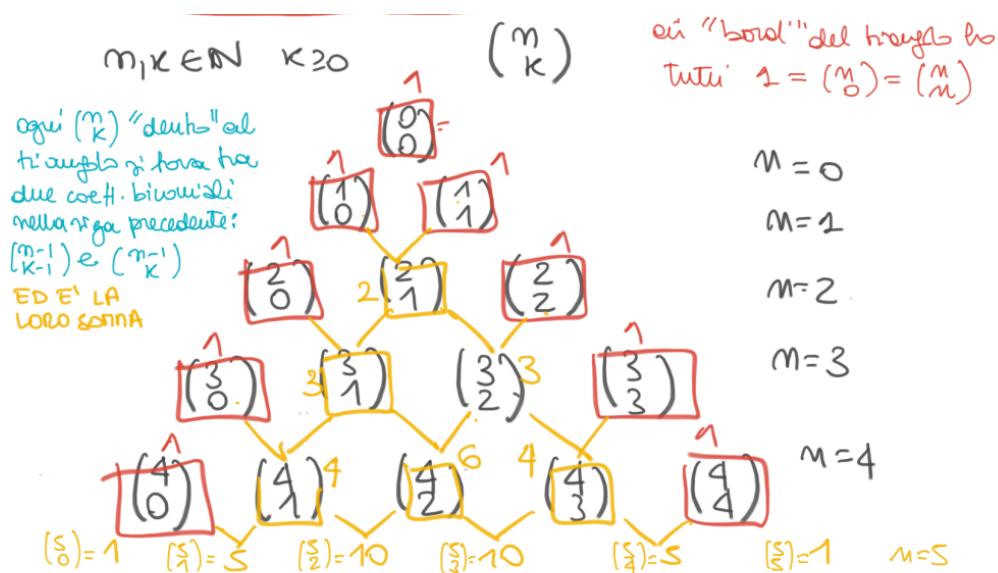
$$|Z| = ? \quad r_1 = 5 \text{ ed } r_2 = 10 \Rightarrow |Z| = 5 \cdot 10 = 50$$

Il numero delle possibili scelte è: $|X| + |Y| + |Z| = 35 + 70 + 50 = 155$

Un altro modo di disporre le combinazioni è usare il "triangolo di Pascal", noto anche come "triangolo di Tartaglia", è una disposizione di numeri in forma di triangolo che è utilizzata per calcolare rapidamente i coefficienti binomiali e altre proprietà combinatorie.

La costruzione del triangolo di Pascal avviene come segue:

1. La prima riga contiene il numero 1.
2. Ogni riga successiva inizia e termina con 1.
3. Gli altri numeri in ogni riga sono ottenuti sommando i due numeri immediatamente sopra di essi nella riga precedente.



Descriviamo inoltre:

- Una "permutazione con ripetizioni" come disposizione ordinata (un allineamento) di oggetti alcuni dei quali non distinguibili

Quanti sono? **TEOREMA** Dati m oggetti

$$\begin{matrix} r_1 & \text{del tipo } 1 \\ r_2 & = 2 \\ \vdots & \\ r_m & = m \end{matrix}$$

$$\text{con } r_1 + r_2 + \dots + r_m = m$$

il numero delle permutazioni di questi m oggetti è:

$$\begin{aligned} P(m; r_1, r_2, \dots, r_m) &= \\ &= \frac{m!}{r_1! r_2! r_3! \dots r_m!} \quad \left(\frac{r_m}{r_m} \right) = \\ &= \frac{m!}{r_1! r_2! r_3! \dots r_m!} \quad \text{Nell'ultimo esempio della nostra} \\ &\quad \text{lezione; quanti sono gli'arrangiamenti} \\ &\quad \text{delle parole BANANA} \\ &\quad m=6 \quad \begin{array}{l|l} B & r_1=1 \\ N & r_2=2 \\ A & r_3=3 \end{array} \quad \begin{array}{l} P(6; 1, 2, 3) = \\ = \binom{6}{1} \binom{5}{2} \binom{3}{3} \end{array} \end{aligned}$$

- Le "combinazioni con ripetizioni" sono un'estensione del concetto di combinazioni standard, in cui gli elementi possono essere selezionati più di una volta. Questo tipo di combinazioni si verificano quando si desidera contare il numero di modi in cui è possibile selezionare un certo numero di oggetti da un insieme, consentendo la possibilità di selezionare lo stesso oggetto più volte.

- In una combinazione con ripetizioni:

- Si ha un insieme di n elementi distinti.
 - Si vuole selezionare r elementi da questo insieme, permettendo la ripetizione degli elementi.
 - L'ordine di selezione non è rilevante, quindi due selezioni che differiscono solo per l'ordine vengono considerate la stessa selezione.

In quanti modi si possono scegliere r oggetti tra
oggetti di m tipi diversi?

NB 1 alcuni degli r oggetti nella posso avere uguali

NB 2 non c'è una limitazione superiore sul numero
degli oggetti tra cui avviene la mappa

Presentiamo il problema come se una scelta corrispondesse ad una suddivisione:
 In quanti modi 6 persone ad un tavolo possono ordinare un caffè nel modo che
 decaffenato, meccanico e normale? $n=3$ (i tipi di caffè ordinabili)
 $r=6$ (il numero di caffè ordinati)
 Un'ordinazione avrà la forma $\text{XX} | \text{XXX} | \text{X}$
 2 decaffenato 3 meccanici 1 normale

ovvero una stringa composta da X e da " $|$ " divise in
 (per distinguere i tipi di caffè ordinati)

Quindi una stringa di lunghezza

$$r + (n-1)$$

"il numero di caffè ordinati"
 $=$ "il numero degli oggetti da scegliere"

numero dei divisi

Il problema diventa: quante sono le stringhe
 di lunghezza $r + (n-1)$ composte da X in numero di r
 e da " $|$ " in numero di $n-1$?

Ormai siamo quasi arrivati alla soluzione:
 (le posizioni delle X nella stringa) cioè $r + (n-1)$ posti
 (le lunghezze delle stringhe)? RISPOSTA:
 in $C(r+n-1, r)$ modi

Le "distribuzioni di oggetti distinti" si riferiscono al modo in cui oggetti diversi vengono assegnati o distribuiti in un certo numero di "contenitori" o "slot". Questo concetto è spesso utilizzato per contare il numero di modi in cui è possibile organizzare oggetti diversi in gruppi o posizioni specifiche.

Ci sono diversi scenari di distribuzioni di oggetti distinti che possono essere considerati:

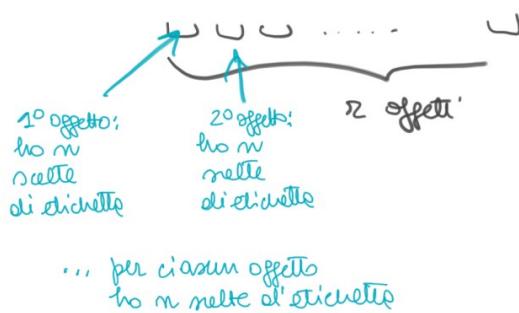
1. Distribuzioni in Posizioni Distinte: In questo caso, si tratta di distribuire n oggetti distinti in r posizioni, dove $n \geq r$. Ogni oggetto viene assegnato a una posizione e non ci sono duplicati. Il numero di modi per fare ciò è $n!$ (n fattoriale), poiché ci sono n modi di assegnare il primo oggetto, $n - 1$ modi per assegnare il secondo oggetto, e così via.
2. Distribuzioni con Restrizioni: A volte potrebbero esserci restrizioni su come gli oggetti distinti possono essere assegnati. Ad esempio, potremmo avere n oggetti distinti che devono essere distribuiti in r posizioni, ma alcune posizioni possono avere restrizioni specifiche. In questo caso, è possibile utilizzare il principio del prodotto o la formula del coefficiente multinomiale per calcolare il numero di modi.
3. Distribuzioni con Ripetizioni: Se consentiamo la possibilità di assegnare lo stesso oggetto a più di una posizione, allora ci troviamo in un caso di distribuzioni con ripetizioni. Questo è simile al concetto di combinazioni con ripetizioni, ma stavolta assegniamo oggetti distinti a posizioni distinte.

4. Distribuzioni in Contenitori Indistinti (o di oggetti identici): In alcuni casi, potremmo essere interessati a distribuire oggetti in gruppi o contenitori indistinti. Questo si riferisce al numero di modi in cui possiamo suddividere n oggetti in r gruppi indistinti. Il numero di modi in cui ciò può essere fatto è rappresentato dal coefficiente binomiale $\binom{n+r-1}{r-1}$

r oggetti distinti
 m scatole d'uscita

1) In quanti modi si possono distribuire gli r oggetti nelle scatole se ciascuna scatola può contenere un numero illimitato di oggetti?

- numero le scatole da 1 a m
- a ciascun oggetto metto una etichetta con il numero della scatola in cui lo metto



RISPOSTA: è
il numero delle stringhe
di lunghezza r
in cui in posizione i
metto l'etichetta
con il numero della
scatola che contiene
l'oggetto i esso

In totale:
in m^r modi

2) In quanti modi si possono distribuire gli r oggetti richiedendo che
nella matrice i-sima riga vengano posti r_i oggetti, $i=1, \dots, m$

$$r_1 + r_2 + \dots + r_m = r$$

RISPOSTA: è il numero delle permutazioni di r oggetti di cui r_1 del tipo 1,
 r_2 del tipo 2, ..., r_m del tipo m =

$$= \binom{r}{r_1} \binom{r-r_1}{r_2} \binom{r-r_1-r_2}{r_3} \dots \binom{r_m}{r_m}$$

selezio
ne
ma
n
que
ll
che
vanno
nelle
scatole 1

... poi quelli
che vanno
nelle scatole 2

... poi quelli
che vanno
nelle scatole 3

abbiamo visto
che è uguale a
 $\frac{r!}{r_1! r_2! \dots r_m!}$

Per concludere, le relazioni di ricorrenza, formule ricorsive che contano il numero di modi di eseguire una procedura con n oggetti in funzione del numero di modi di eseguirla con un numero minore di oggetti.

Descriviamo quindi a_k modi di eseguire la procedura con k oggetti, in funzione di alcuni degli a_k con $k < n$.

ESEMPIO 0

$$a_n = 2 a_{n-1}$$

Una possibile calcolo gli a_n se ha solo

un "punto di partenza": delle CONDIZIONI INIZIALI

$$a_0 = ?$$

$$\text{es. } a_0 = 1 \text{ altrimenti}$$

$$\begin{aligned} a_1 &= 2 \cdot a_0 = 2 \cdot 1 = 2 \\ a_2 &= 2 \cdot a_1 = 2 \cdot 2 = 4 \\ a_3 &= 2 \cdot a_2 = 2 \cdot 4 = 8 \dots \end{aligned}$$

$$\text{es. } a_0 = 6 \text{ altrimenti}$$

$$\begin{aligned} a_1 &= 2 \cdot a_0 = 2 \cdot 6 = 12 \\ a_2 &= 2 \cdot a_1 = 2 \cdot 12 = 24 \dots \end{aligned}$$

Descriviamo poi una soluzione di una relazione di ricorrenza come formula esplicita per a_n che dipende solo da n (e da non gli a_k precedenti).

ESEMPIO 1 Contare quanti sono i possibili allineamenti

d' m effetti (permutazioni d' m effetti)

a_m = numero delle permutazioni d' m effetti

↙ ↘ ↙ ⋯ ↘

FASE 1 Scegli l'effetto da mettere nel 1° posto ho m scelte

FASE 2 Per ciascuna di queste scelte completare l'allineamento

Si arrivederebbe in allineamenti d' $m-1$ effetti: ho a_{m-1} scelte

$$a_m = m \cdot a_{m-1} \quad \leftarrow \text{LA RELAZIONE DI RICORRENZA}$$

$$\text{LA CONDIZIONE INIZIALE} \rightarrow a_1 = 1 \quad \leftarrow \begin{matrix} \text{in quanti modi} \\ \text{posso allineare} \\ 1 \text{ effetto} \end{matrix}$$

LA SOLUZIONE

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 2 \cdot a_1 = 2 \cdot 1 = 2 \cdot 1 = 2! \\ a_3 &= 3 \cdot a_2 = 3 \cdot 2 \cdot 1 = 3! \\ a_4 &= 4 \cdot a_3 = 4! \\ &\vdots \end{aligned}$$

$$a_m = m!$$

ESEMPPIO 3

C'è una scala con m gradini.

Per salire a passi fare passi di 1 gradino

e/o passi di 2 gradini. Trovare una

relazione di ricorrenza che conti il numero

a_m dei diversi modi di salire la scala

$$m=1 \quad \begin{array}{c} \diagup \\ \diagdown \end{array} \quad a_1 = 1 \quad \begin{array}{l} \text{per una scala con 1 gradino ho 1 solo modo: 1 passo di 1 gradino} \end{array}$$

$$m=2 \quad \begin{array}{c} \diagup \\ \diagdown \end{array}^2 \quad \begin{array}{c} \diagup \\ \diagdown \end{array}^2 \quad a_2 = 2 \quad \begin{array}{l} \text{per una scala con 2 gradini ho 2 modi: o 2 passi di un gradino oppure} \\ \text{1 passo di 2 gradini!} \end{array}$$

per una scala con 3 gradini ho 3 modi:

$$m=3 \quad \begin{array}{c} \diagup \\ \diagdown \end{array}^3 \quad \begin{array}{c} \diagup \\ \diagdown \end{array}^3 \quad \begin{array}{c} \diagup \\ \diagdown \end{array}^3 \quad a_3 = 3 \\ [3 passi di 1] \circ [(1 de 1) + (1 de 2)] \circ [(1 de 2) + (1 de 1)]$$

Nella scala con m gradini faccio il 1° passo

se faccio il 1° passo

de 1 gradino

mi avvicino
di salire
 $m-1$ gradini
che posso
fare in

a_{m-1} modi

(come una scala di $m-1$ gradini)

Se faccio il 1° passo de 2 gradini ho
ancora da salire $m-2$ gradini: a_{m-2}
modo possibile.

IN TOTALE:

$$a_m = a_{m-1} + a_{m-2}$$



LA RELAZIONE DI RICORRENZA

Abbiamo infine:

Una "relazione di ricorrenza lineare omogenea" è un tipo di equazione di ricorrenza che coinvolge termini precedentemente calcolati nella definizione di nuovi termini. È "omogenea" perché il termine noto è zero o assente. Una relazione di ricorrenza lineare omogenea può essere espressa nella forma generale:

$$a_k f(k) + a_{k-1} f(k-1) + \dots + a_1 f(1) + a_0 f(0) = 0$$

dove a_k, a_{k-1}, \dots, a_0 sono costanti, e $f(k), f(k-1), \dots, f(1), f(0)$ sono termini precedentemente calcolati.

Esempio:

$$f(k) = 2f(k-1) - f(k-2)$$

Questa è una relazione di ricorrenza lineare omogenea di secondo ordine. I termini $f(k-1)$ e $f(k-2)$ sono usati per calcolare il termine $f(k)$.

Per poterle risolvere OCCORRONO R CONDIZIONI

INIZIALI che permettono di calcolare c_1, c_2, \dots, c_r

r = grado della relazione di ricorrenza.

PER RISOLVERLE:

① PORRE x^k AL POSTO DI a_k NELLA RELAZIONE:

$$x^m = c_1 x^{m-1} + c_2 x^{m-2} + \dots + c_r x^{m-r}$$

② DIVIDERE PER x^{m-r} :

$$x^r = c_1 x^{r-1} + c_2 x^{r-2} + \dots + c_{r-1} x + c_r$$

"EQUAZIONE CARATTERISTICA" OCUA RELAZIONE È:

③ $x^r - c_1 x^{r-1} - c_2 x^{r-2} - \dots - c_{r-1} x - c_r = 0$

④ LA SOLUZIONE GENERALE DELLA RELAZIONE DI RICORRENZA
E' L'INSIEME DELLE COMBINAZIONI LINEARI DELLE SEGUENTI
SOLUZIONI:

$$\left. \begin{array}{l} \text{in questo tipo} \\ \text{sono m} \rightarrow d_1^m, m d_1^m, m^2 d_1^m, \dots, m^{m_1-1} d_1^m, \\ \text{in questo tipo} \\ \text{sono m} \rightarrow d_2^m, m d_2^m, m^2 d_2^m, \dots, m^{m_2-1} d_2^m, \\ \vdots \\ \text{in questo tipo} \\ \text{sono m} \rightarrow d_K^m, m d_K^m, m^2 d_K^m, \dots, m^{m_K-1} d_K^m \end{array} \right\} \begin{array}{l} \text{qui ci sono} \\ \text{2 soluzioni} \\ \leftarrow \text{della} \\ \text{relazione} \\ \text{d'ricorrenza} \\ (\text{2 possibilan}) \end{array}$$

LA SOLUZIONE GENERALE E':

$$a_m = A_1 d_1^m + A_2 m d_1^m + \dots + A_{m_1} m^{m_1-1} d_1^m + A_{m_1+1} d_2^m + \dots + A_K m^{m_K-1} d_K^m$$

dove A_1, A_2, \dots, A_K sono costanti.

⑤ A questo punto determiniamo il valore delle costanti

A_1, A_2, \dots, A_K si trovano le 2 condizioni iniziali

Una "relazione di ricorrenza lineare non omogenea di grado 1" è simile a quella omogenea, ma include un termine noto non nullo. La forma generale di una relazione di ricorrenza lineare non omogenea di grado 1 è:

$$a_k f(k) + a_{k-1} f(k-1) + \dots + a_1 f(1) + a_0 f(0) = g(k)$$

dove $g(k)$ è il termine noto, e a_k, a_{k-1}, \dots, a_0 sono costanti.

Esempio:

$$f(k) = 2f(k-1) + 1$$

Questa è una relazione di ricorrenza lineare non omogenea di primo ordine. Il termine noto è 1, che è aggiunto al lato destro dell'equazione.

Procedimento:

- ① Si ha la soluzione generale delle relazioni d'ricorrenza omogenee associate (*), cioè:

$$(*) \quad a_n = c a_{n-1}$$

$$x^n = c x^{n-1}$$

$$x = c$$

sol. gen. d' (*) è $A c^n$

dove A è una costante
(che si determina SOL
ALLA FINE)

- ② Si assume altra soluzione generale
d' (**), cioè $A c^n$, una "soluzione particolare" $p(n)$
d' (*)

LA SOLUZIONE GENERALE DI (*) è:

$$A c^n + p(n)$$

Ci limitiamo ai seguenti casi:

$$f(n) = d \text{ (costante)}$$

PRENDERE $p(n) = B$

$$f(n) = d n$$

$$\approx p(n) = B_1 n + B_0$$

$$f(n) = d n^2$$

$$\approx p(n) = B_2 n^2 + B_1 n + B_0$$

- ③ LE COSTANTI VENGONO DETERMINATE ALLA FINE
IMPONDENDO LE CONDIZIONI INIZIALI

Le relazioni "Divide and Conquer" sono un tipo particolare di relazioni di ricorrenza utilizzate per analizzare algoritmi "divide and conquer" (dividi e conquista), che risolvono un problema suddividendolo in sottoproblemi più piccoli. Queste relazioni descrivono il tempo di esecuzione di un algoritmo ricorsivo in termini del tempo di esecuzione delle sue sottoparti.

Esempio:

$$T(n) = 2T(n/2) + n$$

Questa è una relazione "divide and conquer" che rappresenta il tempo di esecuzione di un algoritmo che suddivide il problema in due sottoproblemi di dimensione $n/2$ e poi combina le loro soluzioni. Il termine n rappresenta il tempo aggiuntivo richiesto per combinare le soluzioni dei sottoproblemi.

LE RELAZIONI "DIVIDE AND CONQUER" sono relazioni d' ricorrenza delle forme:

$$a_n = c \cdot a_{\frac{n}{2}} + f(n)$$

dove c è una costante ed $f(n)$ è una funzione di n .

LE SOLUZIONI DI ALCUNI CASI:

c	$f(n)$	a_n
$c=1$	d	$d[\log_2 n] + A$
$c=2$	d	$A_n - d$
$2 < c > 0$	$d n$	$A n^{\log_2 c} + \left(\frac{2d}{2-c}\right) \cdot n$
$c=2$	$d n$	$d n([\log_2 n] + A)$

LA COSTANTE A VIENE DETERMINATA IN BASE
ALLE CONDIZIONI INIZIALI

quindi nell'esempio 7 $\boxed{a_n = 2a_{\frac{n}{2}} + 1}$
 $(f(n)=d=1 \text{ e } c=2)$ $d=1$

la soluzione generale è $a_n = A_n - d \leftarrow A_n - 1$

la condizione iniziale è $\underset{n=1}{\bullet} \underset{n=2}{\circ} \quad 1 \text{ con } a_2 = 1$

$1 = a_2 = A \cdot 2 - 1 \Rightarrow 2A = 2 \Rightarrow A = 1 \Rightarrow \boxed{a_n = n - 1}$
 VERIFICA: $n - 1 = a_n = 2a_{\frac{n}{2}} + 1 = 2\left(\frac{n}{2} - 1\right) + 1 = n - 2 + 1 = n - 1 \text{ OK.}$