RIASSUNTO x me

- prodotto scalare

$\langle v,w\rangle = v_1w_1 + v_2w_2 + v_3w_3$

- prodotto vettoriale $v=(x_1,x_2,x_3)$ $w=(y_1,y_2,y_3)$

123 231 312

$v\wedge w = (x_2y_3 - x_3y_2,\ x_3y_1 - x_1y_3,\ x_1y_2 - x_2y_1)$

PROPRIETA'

1) $w\wedge v = -w\wedge v \Rightarrow v\wedge v = 0$
2) $v\wedge w =$ e' ORTOGONALE a v e w
3) $\|v\wedge w\| = \|v\|\,\|w\|\sin\Theta$

- NORMA (lunghezza del vettore)

$\|v\| = \sqrt{\langle v,v\rangle}$

+ DISTANZA $dist(v,w) = \|v-w\| = \sqrt{\langle v-w, v-w\rangle}$
+ Teorema di Pitagora

$\|v+w\|^2 = \|v\|^2 + \|w\|^2 + 2\langle v,w\rangle$

+ Disuguaglianza Cauchy Schwarz

$\langle v,w\rangle \leq \|v\|\,\|w\|$

- Angolo tra vettori $\cos\Theta = \dfrac{\langle v,w\rangle}{\|v\|\,\|w\|}$

- Proiezione ortogonale $pr_v(w) = \dfrac{\langle v,w\rangle}{\|v\|^2}\cdot v$

-$pr_v(w)$ e' un multiplo di v
-$w - pr_v(w)$ e' ORTOGONALE a v

- Teorema di Rouchè Capelli

SIS. RISOLUBILE $\longrightarrow$ $\forall$ ogni riga nulla dei coefficienti è nullo anche il termine noto

$\longrightarrow$ $rg(A|b) = rg(A)$

$\longrightarrow$ Allora il # di parametri da cui dipende e':

parametri = # variabili $- rg(A)$

RETTE

eq. retta $X = \underbrace{P}_{\text{PUNTO}} + t\underbrace{A}_{\text{VETTORE DIREZIONE}}$

→ **eq. CARTESIANA**

$$r: \begin{cases} ax_1 + bx_2 + cx_3 = d \\ a'x_1 + b'x_2 + c'x_3 = d' \end{cases}$$

→ **eq. PARAMETRICA**

$$X = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} + t \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

PARAMETRICA

Ricavo t ↓ ↑ Introduco t

CARTESIANA

Date due rette:

$r: X = P + tA$

$s: X = P' + tA'$

→ A non è multiplo di A'
$\Rightarrow$ s e r non sono la stessa retta

→ A è multiplo di A'
1) non hanno punti in comune
$\Rightarrow$ sono rette diverse
2) hanno un punto in comune
$\Rightarrow$ coincidono

PIANI

$$\alpha = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \middle| \ ax + by + cz + d = 0 \right\}$$

$x, y, z \rightarrow$ possibili soluzioni

$a, b, c \rightarrow$ numeri
+
COORDINATE del **VETTORE NORMALE AL PIANO**

→ **eq. CARTESIANA**

$\alpha: ax + by + cz = d$

$n_\alpha = (a, b, c)$

PARAMETRICA

$A_1 \wedge A_2$ ↓ ↑ Risolvo il sistema

CARTESIANA

→ **eq. PARAMETRICA**

$$\alpha: X = P + t\underbrace{A_1}_{\text{I grado di libertà}} + s\underbrace{A_2}_{\text{II grado di libertà}}$$

MUTUE POSIZIONI

1) RETTA e RETTA

METODO 1: Vettori Direzione

$r: \; X = P + tA$

$s: \; X = P' + tA'$

a) $A = kA'$
1) PARALLELE COINCIDENTI, se hanno un punto in comune
2) PARALLELE NON COINCIDENTI, se non hanno punti in comune

b) $A \neq kA'$
1) INCIDENTI, hanno un punto in comune
2) SGHEMBE, non hanno punti in comune

c) $A \perp A'$, allora le rette sono ORTOGONALI

METODO 2: sistemi lineari

$r: \begin{cases} ax + by + cz = d \\ a'x + b'y + c'z = d' \end{cases} \qquad s: \begin{cases} ex + fy + gz = h \\ e'x + f'y + g'z = h' \end{cases}$

$$\underbrace{\left(\begin{array}{ccc|c} a & b & c & d \\ a' & b' & c' & d' \\ e & f & g & h \\ e' & f' & g' & h' \end{array}\right)}_{(A|b)}$$

SIS. COMPATIBILE $\Updownarrow$ $rg\,A = rg(A|b)$ → se compatibile, # param = # var − rg(A)

3 − ?

$rg\,A = \cancel{0}, \cancel{1}, 2, 3, \cancel{4}$

PERCHÈ CIASCUNA RETTA HA 2 EQ.

GAUSS: $rgA \leq$ # colonne (3)

a) $rg\,A = 2$ RETTE PARALLELE
- $rg(A|b) = 2$: Sis. compatibile ⇒ rette PARALLELE COINCIDENTI
- $rg(A|b) = 3$: Sis. non è compatibile ⇒ rette PARALLELE NON COINCIDENTI

b) $rg\,A = 3$ RETTE NON PARALLELE
- $rg(A|b) = 3$: Sis. compatibile ⇒ INCIDENTI
- $rg(A|b) = 4$: Sis. non compatibile ⇒ SGHEMBE

2) PIANO e PIANO

METODO 1: vettori normali

$\alpha: ax + by + cz = d \qquad n_\alpha = (a, b, c)$

$\beta: a'x + b'y + c'z = d' \qquad n_\beta = (a', b', c')$

a) $n_\alpha = k\, n_\beta$
1) PARALLELI COINCIDENTI, se hanno un punto in comune
2) PARALLELI NON COINCIDENTI, non hanno punti in comune

b) $n_\alpha \neq k\, n_\beta$ PIANI INCIDENTI, si intersecano in una retta

c) CASO PARTICOLARE : $n_\alpha \perp n_\beta$, PIANI ORTOGONALI

METODO 2: sistemi lineari

$$\begin{array}{l} \alpha: \\ \beta: \end{array} \begin{cases} ax + by + cz = d \\ a'x + b'y + c'z = d' \end{cases} \qquad (A|b) = \left(\begin{array}{ccc|c} a & b & c & d \\ a' & b' & c' & d' \end{array}\right)$$

$rg\, A = \cancel{0}\ 1\ 2$

a) $rg\, A = 1$ PIANI PARALLELI

$rg(A|b) = 1$
sis. compatibile $\Longrightarrow$ COINCIDENTI

$rg(A|b) = 2$ $\Longrightarrow$ NON COINCIDENTI
sis. non compatibile

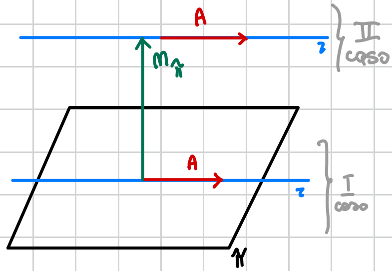
b) $rg\, A = 2$ $\quad rg(A|b) = 2 \Longrightarrow$ INCIDENTI
sis. compatibile, si intersecano in una retta
(# parametri $= 3 - 2 = 1$) ✓

c) Per trovare l'ortogonalità confrontiamo i vettori normali

3) **RETTA e PIANO**

$r: X = P + tA$ $\qquad$ $\pi: ax+by+cz=d$

$\qquad\qquad\qquad\qquad n_\pi = (a,b,c)$



METODO 1:

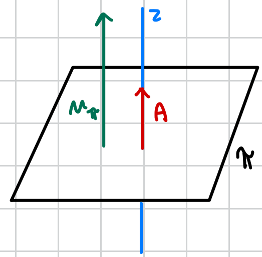
a) $n_\pi \perp A$ $\quad$ 1) $r \cap \pi \neq \emptyset \Rightarrow r$ giace in π

r è contenuta in π

PARALLELI COINCIDENTI

2) $r \cap \pi = \emptyset \Rightarrow r$ non giace in π

PARALLELI NON COINCIDENTI



b) n_π non è ortogonale ad A $\Rightarrow$ INCIDENTI

si intersecano in un punto

METODO 2: Sistemi lineari (guardiamo l'intersezione)

$$r: \begin{cases} ax+by+cz=d \\ a'x+b'y+c'z=d' \end{cases}$$

$$\alpha: \quad ex+fy+gz=h$$

$$(A|b) = \left(\begin{array}{ccc|c} a & b & c & d \\ a' & b' & c' & d' \\ e & f & g & h \end{array}\right)$$

$$rg\,A = \cancel{0}, \cancel{1}, 2, 3$$

a) $rg\,A = 2$ $\quad$ PARALLELI $\quad$ 1) $rg(A|b) = 2$

sis. compatibile $\Rightarrow$ PARALLELI COINCIDENTI

($\#par = 3-2 = 1$)

2) $rg(A|b) = 3$

sis. non compatibile $\Rightarrow$ PARALLELI NON COINCIDENTI

b) $rg\,A = 3$ $\quad$ $rg(A|b) = 3$ $\Rightarrow$ INCIDENTI

sis. compatibile

c) Per vedere l'ORTOGONALITÀ devo tornare ai vettori

MATRICI

- **quadrate** # righe = # colonne
- **nulle** formata solo da zeri.
- **PRODOTTO RIGHE PER COLONNE** $A \times B = AB$ — prodotto scalare riga i della prima matrice, colonna j della seconda

$A \in M_{m \times n}$ $\quad AB \in M_{m \times p}$

$B \in M_{n \times p}$

- **triangolari**
  - SUPERIORE se $A_{ij} = 0$ per $i > j$ (tutti i coeff. sotto la diagonale sono nulli)
  - INFERIORE se $A_{ij} = 0$ per $i < j$ (tutti i coeff. sopra la diagonale sono nulli)
- **identità** I_n $\quad I_{ij} = 1$ se $i = j$, $= 0$ se $i \neq j$ (ha tutti 1 sulla diagonale principale)

es. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$\boxed{\forall A \in M_{n \times n} \quad AI = IA}$$

- **traccia**

$\operatorname{tr} A$ = somma degli elementi sulla diagonale $\quad$ es. I_n $\quad \operatorname{tr} I_n = n$

PROPRIETÀ:
- $\operatorname{tr}(A+B) = \operatorname{tr} A + \operatorname{tr} B$
- $\operatorname{tr}(cA) = c \operatorname{tr} A$
- $\operatorname{tr}(AB) = \operatorname{tr}(BA)$
- $\operatorname{tr}(A^T) = \operatorname{tr}(A)$

- **diagonali** $D_{ij} = 0$ per $i \neq j$ (gli elementi sono nulli se non si trovano sulla diagonale)

$$D = \begin{pmatrix} a_{11} & 0 & \dots & \\ 0 & a_{22} & \dots & \\ & & \ddots & \\ 0 & \dots & & a_{nn} \end{pmatrix}$$

- somma/prodotto di due mat. diagonali è diagonale
- due mat. diagonali commutano sempre

- **Invertibili** (quadrate)

$A \in M_{n \times n}$ è INVERTIBILE se $\exists$ un'altra mat. $n \times n$ detta A^{-1}, t.c.

$$\boxed{A \cdot (A^{-1}) = (A^{-1}) \cdot A = I_n}$$

- $(AB)^{-1} = B^{-1} A^{-1}$

es. (perché non ho capito)

$A = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}$ è invertibile: $A^{-1} = \begin{pmatrix} 1/3 & 0 \\ 0 & 1/5 \end{pmatrix}$

Infatti: $AA^{-1} = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1/3 & 0 \\ 0 & 1/5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ NON è invertibile $\Rightarrow$ se la matrice contiene una RIGA/COLONNA di $\emptyset$ allora NON è INVERTIBILE

- **Algoritmo per calcolare A^{-1}** (variante di Gauss)

$$\left(A \mid I \right) \xrightarrow{\text{op. tra righe}} \left(I \mid A^{-1} \right)$$

• SIMMETRICA e ANTISIMMETRICA

Definisco la **TRASPOSTA** di una matrice come la matrice in cui si scambiano le righe con le colonne.

$$(A^T)_{ij} = A_{ji}$$

scambio indici di riga con indici di colonna

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix} \qquad A^T = \begin{pmatrix} 1 & 5 \\ 2 & 6 \\ 3 & 7 \\ 4 & 8 \end{pmatrix}$$

Def. [matrici quadrate]

$A \in M_{m \times m}$

- **SIMMETRICA** se $A = A^T$ $\qquad A_{ij} = (A^T)_{ij} = A_{ji}$
- **ANTISIMMETRICA** se $A = -A^T$ $\qquad A_{ij} = (A^T)_{ij} = -A_{ji}$

es.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix} \quad A^T = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix} \quad \text{SIMMETRICA} \checkmark$$

$$B = \begin{pmatrix} 0 & 2 & 3 \\ -2 & 0 & 4 \\ -3 & -4 & 0 \end{pmatrix} \quad B^T = \begin{pmatrix} 0 & -2 & -3 \\ 2 & 0 & -4 \\ 3 & 4 & 0 \end{pmatrix} \quad \text{ANTISIMMETRICA} \checkmark$$

• MATRICI ORTOGONALI

matrice ortogonale se $A^{-1} = A^T$ ovvero $A^TA = AA^T = I$

PROPRIETÀ:
- I vettori che formano le righe/colonne di A sono **mutualmente ortogonali** e hanno **norma = 1**
- Dato $w \in \mathbb{R}^m$, se $v_1 \text{ — } v_m$ sono le colonne di $A \Rightarrow \exists!\, c_1, \dots, c_m \in \mathbb{R}$ t.c.

$$w = c_1v_1 + \dots + c_mv_m$$

preservano gli angoli

• DETERMINANTE

Associa un numero a una matrice quadrata (ok rispetto al prodotto)

def. Ricorsiva sull'ordine della matrice. Sia $A \in M_{m \times m}$

se $m = 1 \Rightarrow A = a \qquad \det A = a$

se $m > 1 \Rightarrow A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & \dots & & \\ \dots & \dots & & \\ a_{m1} & \dots & & \end{pmatrix}$

SVILUPPO DI LAPLACE rispetto alla prima colonna

$$\det A = +a_{11}\det A_{11} - a_{21}\det(A_{21}) + \dots (-1)^{n+1} a_{n1}\det A_{n1}$$

A_{ij}: minori (sottomatrici) che si ottengono cancellando la riga i e la colonna j

$$A_{ij} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & a_{ij} & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

es. $\det(5) = 5$

$$\det\begin{pmatrix} -2 & 3 \\ 7 & 5 \end{pmatrix} = -2\cdot 5 - 7\cdot 3 = -31$$

$$\det\begin{pmatrix} 2 & 0 & 3 \\ 1 & 7 & -5 \\ 0 & 1 & 2 \end{pmatrix} = 2\cdot\begin{vmatrix} 7 & -5 \\ 1 & 2 \end{vmatrix} - (-1)\begin{vmatrix} 0 & 3 \\ 1 & 2 \end{vmatrix} + 0\begin{vmatrix} 0 & 3 \\ 7 & -5 \end{vmatrix} =$$

$$= 2\cdot(7(2) - 1(-5)) + 1(0(2) - 1(3)) + 0(0(3) - 7(3))$$

$$= 2\cdot(14+5) - 3 + 0 = 2\cdot 19 - 3 = 35 \checkmark$$

- posso sviluppare il determinante rispetto a qualsiasi riga/colonna

es. $\begin{pmatrix} 1 & 4 & 6 \\ 2 & 0 & 0 \\ 3 & 5 & 7 \end{pmatrix}$ → conviene sviluppare il det rispetto a questa

$$\det = 2\begin{vmatrix} 4 & 6 \\ 5 & 7 \end{vmatrix} - 0\begin{vmatrix} 1 & 6 \\ 3 & 7 \end{vmatrix} + 0\begin{vmatrix} 1 & 4 \\ 3 & 5 \end{vmatrix} =$$

$$= 2\cdot(4\cdot 7 - 5\cdot 6) = 2\cdot(28-30) = 2\cdot -2 = -4 \checkmark$$

- Se ho una riga/colonna di zeri, il determinante è sempre uguale a 0.

es. $\det\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} = 0$

Algoritmo di Gauss

- Scambiare due righe
- moltiplico una riga per $k \neq 0$
- $R_i \longrightarrow R_i + \alpha R_j$

Determinante

- det. viene moltiplicato per -1
- det. viene moltiplicato per k
- det non cambia

Proprietà Determinante

① $\det A = \det A^T$

② $\det \begin{pmatrix} | & | & | \\ A^1 & tA^j & A^n \\ | & | & | \end{pmatrix} = t \det \begin{pmatrix} | & | & | \\ A^1 & A^j & A^n \\ | & | & | \end{pmatrix} = t \det A$

moltiplico una colonna per t

$\det(tA) = \det(tA^1 \dots tA^n) = t^n \det A$

③ Se scambio due colonne il determinante cambia segno

③' Se A ha due colonne uguali, $\det A = 0$.

④ $\det(AB) = \det A \cdot \det B \Longrightarrow$ Formula di Binet

conseguenza

A ortogonale $\Longrightarrow \det A = \pm 1$

⑤ A è invertibile $\Longleftrightarrow \det A \neq 0$ e $\det(A^{-1}) = \dfrac{1}{\det A}$

INVERSA 2x2 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow A^{-1} = \dfrac{1}{\det A} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

• Rango per minori (mat. rettangolari)

def. $A \in M_{m \times n}$,
Un minore di ordine p è una matrice quadrata $p \times p$ ottenuta da A cancellando $m-p$ righe e $n-p$ colonne

ho m righe, cancello $m-p$ righe $\longrightarrow$ restano $m-(m-p) = m-m+p$ righe $\Longrightarrow$ P RIGHE

ho n colonne, cancello $n-p$ colonne $\longrightarrow$ restano $n-(n-p) = n-n+p$ colonne $\Longrightarrow$ R COLONNE

es. $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$

• minori di ordine 3

- eliminiamo la 1° riga $\begin{pmatrix} 2 & 3 & 4 \\ 6 & 7 & 8 \\ 10 & 11 & 12 \end{pmatrix}$
- eliminiamo la 3° riga $\begin{pmatrix} 1 & 2 & 4 \\ 5 & 6 & 8 \\ 9 & 10 & 12 \end{pmatrix}$
- eliminiamo la 2° riga $\begin{pmatrix} 1 & 3 & 4 \\ 5 & 7 & 8 \\ 9 & 11 & 12 \end{pmatrix}$
- eliminiamo la 4° riga

• minori di ordine 2 [ho $\underbrace{3}_{\text{scelte riga}} \times \underbrace{4}_{\text{scelta 1° colonna da togliere}} \times \underbrace{3}_{\text{scelta 2° colonna da togliere}} = 36$ scelte]

- $\begin{pmatrix} 1 & 2 \\ 9 & 10 \end{pmatrix}, \begin{pmatrix} 6 & 7 \\ 10 & 11 \end{pmatrix}, \begin{pmatrix} 7 & 8 \\ 11 & 12 \end{pmatrix}$

def. rango per minori di A è il massimo ordine (dimensione) dei minori di A con det $\neq 0$.
Ovvero, guardo tutti i minori di A, scelgo il più grande con det $\neq 0$, la sua dim. è il rg A.

es.
$A = \begin{pmatrix} 1^{+} & 0 & 1 \\ -1^{-} & 1 & 0 \\ 0^{+} & 1 & 1 \end{pmatrix}$

mat. non nulla $\Longrightarrow$ rg è almeno 1
3 righe e 3 colonne $\Longrightarrow$ rg al max 3
$\Downarrow$
trovo un minore di rg 2, con det $\neq 0$
det $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$

$rg\,A = 2$ o 3 ? Controllo il det A

$$\det A = 1\begin{vmatrix}1 & 0\\1 & 1\end{vmatrix} - (-1)\begin{vmatrix}0 & 1\\1 & 1\end{vmatrix} + 0\begin{vmatrix}0 & 1\\1 & 0\end{vmatrix}$$

$$= 1[(1\cdot1)-(1\cdot0)]+1[(0\cdot1)-(1\cdot1)]+0 = 1-1+0=0 \Rightarrow$$ l'unico minore di ordine 3 ha det $=0$

$\Rightarrow rg\,A = 2$

- Gauss non fa diventare 0 il det di nessun minore e non crea minori nuovi con det $\neq 0$
  - $A \xrightarrow[\text{Gauss}]{} S \quad \Rightarrow rg$ per minori di $A = rg$ per minori di S

OSS. Se una matrice A ha m righe e n colonne, $rg\,A \leq \min(m,n)$

- Una matrice $A \in M_{n\times n}$ è invertibile se il $\det A \neq 0$ e $rg\,A = n$ (rango massimo)
- teo Rouché Capelli per matrici dei coeff. invertibili

  $A \in M_{n\times n}$, $\det A \neq 0 \Rightarrow$
  - Il sistema $Ax=b$ è compatibile $\forall b \in \mathbb{R}^n$
  - la soluzione è unica

• STRUTTURA DI GRUPPO

def. Un gruppo è un insieme S con
- una operazione $*$ t.c. $s_1 * s_2 = s \in S$
- $\exists\ e \in S$ elemento neutro t.c. $s*e = e*s = s\ \forall s \in S$
- $\exists$ inversi: $\forall s \in S\ \exists\ s^{-1} \in S$ t.c. $s * s^{-1} = e$

Gruppi di matrici rispetto alla somma

$S = M_{m\times n}, +, e = 0$ [mat. nulla]

- ok perché la somma di matrici è una matrice della stessa dimensione
- ok perché $A+0 = 0+A = A$
- $(-A)$, $(-A)+A = A+(-A) = 0$

Gruppi di matrici rispetto alla moltiplicazione

Devo considerare le mat $n\times n$, non tutte le moltiplicazioni sono possibili

$S = M_{n\times n}$ invertibili ($\det \neq 0$)

- ok: $s_1\cdot s_2 = s \in M_{n\times n}$
- $\exists e$: I: $I\cdot A = A\cdot I = A \quad \forall A$
- $\exists A^{-1}$ t.c. $A\cdot A^{-1} = A^{-1}A = I$

tanti sottogruppi:
simm., antisimm., traccia nulla ...

Sottogruppi:
matrici ortogonali, simm., det =1,
diagonali ...

08.04.24

Numeri

- numeri naturali (e numeri primi) $\mathbb{N} = \{0,1,2,\dots\}$
- numeri interi $\mathbb{Z} = \{\dots -2,-1,0,1\dots\}$
- numeri razionali $\mathbb{Q} = \{\frac{p}{q},\ p,q \in \mathbb{Z},\ q \neq 0\}$
- numeri reali $\mathbb{R}$
- numeri complessi $\mathbb{C} = \{a+ib,\ a,b \in \mathbb{R}\}$
  $i^2 = -1$

Studiamo la loro struttura:
- Proprietà dell'insieme
- Operazioni lecite

NUMERI NATURALI

Due proprietà fondamentali

1. Assioma del buon ordinamento

"Ogni sottoinsieme non vuoto di $\mathbb{N}$ ha un elemento minimo"

$\downarrow$

Se $S \subset \mathbb{N},\ S \neq \emptyset \Rightarrow \exists\, m \in S$ t.c. $m \leq n\ \ \forall n \in S$

OSS. • S potrebbe essere infinito $\Longrightarrow$ non avere un elemento massimo

• Peculiarità di $\mathbb{N}$: – in $\mathbb{Z}$, $S = \{$negativi multipli di $3\}$ non ha un elemento minimo

– in $\mathbb{R}$, $S = (0,1]$ non c'è elemento minimo perché dovrebbe essere 0, ma $0 \notin S$.

aperto

2. Principio di Induzione

Associamo a ogni n una asserzione $A(n)$. Allora, se

* $A(0)$ è vera

* $\forall n$, $A(n)$ implica $A(n+1) \Longrightarrow A(n)$ è vero $\forall n$.

• è equivalente all'assioma di buon ordinamento

Operazioni sui naturali

- somma $n+m \in \mathbb{N}$ con $n,m \in \mathbb{N}$

  oss $0+n=n \quad \forall n \in \mathbb{N}$

  0 è l'elemento neutro della somma

- moltiplicazione $n \cdot m \in \mathbb{N}$ con $n,m \in \mathbb{N}$

  oss $1 \cdot n = n \quad \forall n \in \mathbb{N}$

  1 è l'elemento neutro della moltiplicazione

- divisione con resto

Non possiamo fare:
- sottrazione $\leadsto \mathbb{Z}$
- divisione "normale" $\leadsto \mathbb{Q}$ $(1:2=0.5 \notin \mathbb{N})$
- radici/risolvere equazioni $(x^n=5\,?)$ $\leadsto \mathbb{R}$

  $\leadsto \mathbb{C}$

NUMERI INTERI

operazioni: somma, moltiplicazione, divisione con resto, sottrazione

illecite: divisione normale, soluzioni di eq.

I numeri primi sono naturali, ma la def. si basa su concetti che valgono anche per gli interi

DIVISIONE CON RESTO

- naturali: $55:9=6$ resto 1

  Abbiamo cercato il più grande x tale che $9 \cdot x < 55$; $x=6$

  $55 - 9 \cdot 6 = 1$ (resto)

- interi: Convenzione: il resto deve essere positivo

  oss. Se il numero per cui divido è negativo, moltiplico entrambi per -1 in modo da farlo diventare positivo

  $55:(-9) \longrightarrow -55:9=-7$ resto 8

Divisione con resto: $\mathbb{N}$ $\quad a:b=q$ resto r

$\equiv a = q \cdot b + r$

Ci sono ∞ soluzioni, 1 sola se chiedo $r<b$

$\mathbb{Z}$ $\quad$ 1 sola se chiedo $0 \leq r < b$

convenzione

def. (divisore) Siano $a, b \in \mathbb{Z}$ diciamo che b divide a (b è un divisore di a) se $\exists\, c$ t.c. $a = b \cdot c$

- (la divisione di a per b dà resto 0)
- a è multiplo di b
- $b | a$

Attenzione! Anche i negativi sono divisori

$12 = 3 \cdot 4 = -3 \cdot -4$

- Esempio i divisori di 12: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6; \pm 12$
  di 7: $\pm 1, \pm 7$
- tutti i numeri sono divisori di 0, perchè $\forall\, b \in \mathbb{Z}$ $0 = b \cdot 0$
  (posso prendere $c = 0$)
- 0 non è divisore di nessun b, perchè $\forall\, b \in \mathbb{Z}$, $b \neq 0 \cdot c \quad \forall\, c \in \mathbb{Z}$

<u>OSS.</u> (1) Ogni intero a ha almeno 4 divisori: $\pm 1, \pm a$

(2) Se d divide a e $b \Rightarrow d$ divide $a \pm b$

dim: $d | a \equiv \exists\, c_1$ t.c. $a = d \cdot c_1$
$d | b \equiv \exists\, c_2$ t.c. $b = d \cdot c_2$

$$\Rightarrow a + b = \underbrace{d \cdot c_1}_{a} + \underbrace{d \cdot c_2}_{b} = d \underbrace{(c_1 + c_2)}_{c}$$

$a - b = \ldots$

(3) Se d divide $a \neq 0 \Rightarrow |d| \leq |a|$

($a \neq 0$ perchè tutti i d sono divisori di 0 ma 0 è il più piccolo)

dim. $d | a$, $\exists\, c$ t.c. $a = d \cdot c \rightarrow |a| = |d| \cdot |c|$
se $a \neq 0$, $c \neq 0$
$\Rightarrow |c| \geq 1 \Rightarrow$
$|a| \geq |d|\, 1 = |d|$

$-5 | -10$, ma $-5 > -10$
$\Rightarrow$ devo usare il modulo
$|-10| \geq |-5|$

Teorema (divisione con resto)

Siano $a, b \in \mathbb{Z}$, $b>0$. Allora $\exists$ unici due interi q, r (quoziente e resto) tali che

$a = qb + r$, $0 \leq r < b$

Scriviamo $a : b = q$ resto r

Divisori, congruenze e numeri primi

Vale per $\mathbb{Z}$ e $\mathbb{N}$

Studia i casi in cui la divisione di un numero "a" per un numero b dà resto 0.

def. <u>DIVISORE</u> Siano $a, b \in \mathbb{Z}$ diciamo che b divide a (b è un divisore di a) se $\exists\, c$ t.c. $a = b \cdot c$

- (la divisione di a per b da resto 0)
- a è multiplo di b
- $b | a$

! Anche i negativi sono DIVISORI !

Es.
- i divisori di 12 sono
  $\pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 12$
- i divisori di 7 sono $\pm 1; \pm 7$
- tutti i numeri sono divisori di 0, perchè $\forall b \in \mathbb{Z}$, $0 = b \cdot 0$
- 0 non è divisore di alcun b, perchè $\forall b \in \mathbb{Z}$, $b \neq 0 \cdot c$ $\forall c \in \mathbb{Z}$

<u>oss.</u>
1. Ogni intero a ha almeno 4 divisori : ± 1, $\pm a$
2. Se d divide a e b $\Rightarrow$ d divide $a \pm b$

   dim. $d | a \equiv \exists\, c_1$ t.c. $a = d \cdot c_1$

   $d | b \equiv \exists\, c_2$ t.c. $b = d \cdot c_2$

   $\Rightarrow (a+b) = \underbrace{d \cdot c_1}_{a} + \underbrace{d \cdot c_2}_{b} = d(\underbrace{c_1 + c_2}_{c})$ ✓

   $(a-b) = \ldots$
3. Se d divide $a \neq 0 \Rightarrow |d| \leq |a|$

   $a \neq 0$ perchè tutti i d sono divisori di 0 ma 0 è il più piccolo

   dim. $d | a$, $\exists\, c$ t.c. $a = d \cdot c \rightarrow |a| = |d| \cdot |c|$

   Se $a \neq 0$, $c \neq 0$

   $\Rightarrow |c| \geq 1 \Rightarrow$

   $|a| \geq |d| \cdot 1 = |d|$

def. Massimo Comun Divisore GCD greatest common divisor

Siano $a, b \in \mathbb{Z}$, non entrambi 0. Il loro massimo comun divisore (MCD) è il più grande intero che divide sia a che b

Definiamo $MCD(0,0) = 0$

$MCD(0,a) = |a|$

Tutti i numeri dividono $\emptyset$, e il più grande divisore di a è $|a|$.

Es. $MCD(12, 52) = 4$

Div. di $12 = \dots$

Div. di $52 = 4 \cdot 13$

Come si trova? [Scomposizione fattori primi]

Algoritmo di Euclide

(vedere dopo)

Altre proprietà del MCD

- è sempre positivo (Il più grande tra i divisori)
- $MCD(a,a) = MCD(-a,-a) = |a|$
- $MCD(1,a) = 1$
- $MCD(b,a) = MCD(a,b) = MCD(a,-b) = MCD(-a,b)$
- Se $(a,b) \neq (0,0) \Rightarrow MCD(a,b) > 0$

a e b non sono entrambi nulli

Naturali! NON interi

def. Numeri primi $p \in \mathbb{N} \setminus \{0\}$ [p intero positivo]

p è un numero primo se ha esattamente due divisori positivi: 1 e p.

! 1 non è un numero primo

Prop. (Proprietà del MCD)

Se $a, b \in \mathbb{Z}$, $\forall q \in \mathbb{Z}$, $MCD(a, b+qa) = MCD(a,b)$

(Il MCD non cambia se aggiungo a un numero il multiplo di un altro.)

Es. • $a=3$ $b=7$ $q=5$ $\quad MCD(\overset{\overset{1}{\shortparallel}}{3,7}) = MCD(3, 7+5\cdot 3) =$
$= MCD(3, 22) = 1$

• $a=10$
$b=3$
$q=10^5$
$MCD(10, \underset{\underset{10\cdot 10^5+3}{\shortparallel}}{100003}) = \underset{\underset{1}{\shortparallel}}{MCD(10,3)}$

• dim. Sia $q \in \mathbb{Z}$ (a, b fissati) Dobbiamo dimostrare:
① Se d divisore di a e di b, $\Rightarrow$ è divisore di $b+qa$

② di a e di $b+qa$ $\Rightarrow$ è divisore di b

[≡ l'insieme dei divisori di a e b coincide con l'insieme dei div. di a e $b+qa$]

① $d|b$ e $d|a$ $\Rightarrow$
$a = m_1 d$
$b = m_2 d$
$\Rightarrow b + qa = m_2 d + q m_1 d = (m_2 + q m_1) d$
$\Rightarrow d | (b+qa)$

② $d|a$ e $d|b+qa$
$a = m_1 d$
$b+qa = m_2 d$
$\longrightarrow b = (b+qa) - qa =$
$= m_2 d - q m_1 d = (m_2 - q m_1) d$
$\Rightarrow d|b$

• Somma/sottrazione/moltiplicazione di n interi danno numeri interi

Abbiamo usato: • $d|a \iff \exists\, m, a = md$
Q: Cosa non si può fare sui naturali

10/04/24

Prop. Se $a,b \in \mathbb{Z}$, $\forall q \in \mathbb{Z}$ $MCD(a,b) = MCD(a, b+qa)$

resto quoz.

$d | a \iff \exists\, m \in \mathbb{Z}$ t.c. $a = md$

num che divide

Applicazione: Algoritmo di Euclide

es. $MCD(48,32) =$
$= MCD(32,16) =$

$48 = 32 \cdot 1 + 16 \to b$
$b + qa$ $\to a$ $\to q$
$32 = 16 \cdot 2 + 0$
$\Rightarrow$ Il MCD è l'ultimo resto prima di ottenere $\emptyset$.
$\Rightarrow 16$

MCD > 0

· Siano $a,b > 0$ definiamo $r_0, r_1, r_2 \dots$ come:
$r_0 = a$ $\quad r_1 = b$ $\quad r_{k+1} =$ resto di $r_{k-1} : r_k$
$(r_i) \to$ è una successione decrescente di interi positivi $\Rightarrow$ prima o poi arrivo a $\emptyset$,
resto < quoziente
l'ultimo resto non nullo è il MCD

es. $MCD(444,100) =$
$= MCD(100,44) =$
$= MCD(44,12) =$
$= MCD(12,8) =$
$= MCD(8,4)$

$444 = 100 \cdot 4 + 44$
$100 = 44 \cdot 2 + 12$
$44 = 12 \cdot 3 + 8$
$12 = 8 \cdot 1 + 4$
$8 = 4 \cdot 2 + 0$
$\Rightarrow MCD = 4$

Proprietà: Se $d = MCD(a,b) \Rightarrow \exists\, x,y \in \mathbb{Z}$ t.c. **Identità di Bezout**
$d = ax + by$ (x e y possono essere negativi)

es. $MCD(25,10) = 5$ $\quad 5 = 25 \cdot 1 - 10 \cdot 2$

Lemma di Bezout Sia $a,b \in \mathbb{Z}$, $(a,b) \neq (0,0)$ non entrambi nulli
$S = \{ax + by \mid x,y \in \mathbb{Z}\} \Rightarrow MCD(a,b) =$ più piccolo elemento positivo di S.

dim. $S \neq \emptyset$ infatti $a \in S$ Prendiamo solo gli elementi in S che sono positivi: S_+

$\Longrightarrow S_+ \neq \emptyset$ infatti a o $-a \in S_+$.

$S_+ \subset \mathbb{N}$, $S_+ \neq \emptyset \Rightarrow$ principio del buon ordinamento

$\Rightarrow \exists\, d$ elemento minimo $\quad d = a\cdot s + b\cdot t$

Dobbiamo far vedere $d = MCD(a,b)$ ovvero:

- $d|a$, $d|b$ e
- se $c|a$, $c|b$ e $c \in S \Rightarrow c \leq d$

- usando divisione con resto $a = dq + r$ per $q, r \in \mathbb{Z}$, $0 \leq r < a$

$\longrightarrow r = a - dq = a - (as + bt)q = a\underbrace{(1-sq)}_{x} - b\underbrace{tq}_{-y} \Rightarrow r \in S_+$

- $r \geq d$ perché d era minimo
- $r < d$ perché è il resto

$\Rightarrow r = 0$

$\Rightarrow d|a$.

Stesso per $b \rightsquigarrow d|b \Rightarrow d$ divisore di a e di b

- Sia $c|a$, $c|b$ $\exists\, u, v$ t.c. $a = c\cdot u$ $b = c\cdot v$

$\Rightarrow$ poiché $d = as + bt = (cu)\cdot s + (cv)\cdot t = c(us + vt) \Rightarrow$

$c|d \Rightarrow c \leq d$.

Conseguenze di Bezout

(unici)

- $MCD(a,b) = d \Rightarrow d = ax + by$ per qualche $x, y \in \mathbb{Z}$
- Se $d|a$, $d|b \Rightarrow d \mid MCD(a,b)$
- Se $MCD(a,b) = 1$ Sono PRIMI tra loro

Dim*

$\Rightarrow$ se $a|bc$, abbiamo anche $a|c$

Es.
- $MCD(25, 10) = 5 = 25\cdot 1 - 10\cdot 2$
- $MCD(12, 18) = 6$ $\quad 2, 3$ dividono 12 e 18 e di conseguenza anche 6
- $a = 4$, $b = 7$ $\quad MCD(4,7) = 1$ (Euclide)

se $c = 8$, $\quad a \mid \underset{c\cdot b}{\underset{\parallel}{8\cdot 7}} \Rightarrow a|c$ (infatti $4|8$)

*Dim. $1 = MCD(a,b) \overset{\text{Bezout}}{=} ax + by$ per qualche $x, y \in \mathbb{Z} \Rightarrow$

$c = c\cdot 1 = c\cdot(ax + by)$

poiché $a|bc \Rightarrow bc = a\cdot m$ per qualche $m \in \mathbb{Z}$

$\Longrightarrow c = c\,ax + c\,by = c\cdot ax + a\,my =$

$= a(cx + my) \Rightarrow a|c$.

Prop. Siano $a, b \in \mathbb{Z}$ p primo
Se $p | ab \Rightarrow p | a$ o $p | b$

dim Supponiamo $p | ab$, $p \nmid a$. Voglio mostrare $p | b$.
MCD(a, p) divide sia p che a MA gli unici divisori di p sono $\pm p, \pm 1$
MCD $> 0 \Rightarrow$ MCD$(a, p) = 1$ o p.
Poiché $p \nmid a \Rightarrow$ MCD$(a, p) = 1$. $\Rightarrow$ poiché $p | ab$, $p | b$

Teo. Fondamentale dell'Aritmetica

(DECOMPOSIZIONE IN FATTORI PRIMI)

Sia $n \in \mathbb{N}$, $n \neq 0 \Rightarrow \exists$ k numeri primi (non necessariamente distinti)
Tali che $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$
p_1 —— p_k si chiamano fattori primi di n e sono unici a meno dell'ordine.

(Su $\mathbb{Z}$: 0 non va bene
$n \neq 0$, scrivo $n = -($decomposizione di $\underset{\in \mathbb{N}}{-n}$ $)$
1 teoricamente non c'è decomposizione)

dim Esistenza. {Suppongo non vero. $\Rightarrow \exists$ $n > 1$ minimo senza decomposizione.
n non è primo (altrimenti $n = p$)
n non primo $\Rightarrow n = ab$ per qualche $1 < a, b < n$
per minimalità di n, a e b si scompongono in fattori primi e quindi anche n. }

Percorso alternativo facile: Osservo che vale per tutti i primi,
$\Rightarrow \exists$ $n > 1$ minimo e non primo per cui il teo non vale.

Oss Abbiamo visto p primo, $a, b \in \mathbb{Z} \Rightarrow p | a \cdot b$, p divide a o b.
p non primo $\Rightarrow$ falso

Corollario: I numeri primi sono ∞
Supponiamo che siano finiti: p_1 —— p_k
Consideriamo il loro prodotto $a = p_1 \cdot \quad \cdot p_k$
$b = p_1 \cdot \quad \cdot p_k + 1 = a + 1$

MCD$(a, b) = 1$
- perché MCD$(a+1, a) = $ MCD$(1, a) = 1$
- perché $1 = b - a = 1 \cdot b - 1 \cdot a \in S^+$ del lemma di Bezout
  $\Rightarrow$ poiché MCD è il più piccolo intero > 0

Per la scomposizione in fattori primi,

b = prodotto di primi MA questo prodotto non può contenere nessuno dei primi p_1 —— p_n perchè $MCD(a,b)=1$

$\Rightarrow$ b è primo

def. <u>Ordine di un intero</u> Sia $a \in \mathbb{N}$, $a \neq 0, 1$. sia p primo

$\Rightarrow ord_p(a) = \#$ volte che p compare nei fattori primi di a

Se $a \in \mathbb{Z}$, a negativo

$\rightarrow ord_p(a) = ord_p(-a)$ >0

$\hat{0}$

$Ord_p(0)$ non def.

$Ord_p(1) = \cancel{0}$ non def.

Es. $Ord_2(12)=2$

$Ord_3(12)=1$

$Ord_7(12)=0$

$\Rightarrow$ Si può scrivere la decomposizione in fattori primi come

$a \in \mathbb{N}$, $a \neq 0, 1$

$$a = \prod_{p \text{ primi}} p^{ord_p(a)}$$

$$12 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \ldots$$

Oss. $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$

1. $\forall$ p primo, $ord_p(ab) = ord_p(a) \cdot ord_p(b)$
2. $d \in \mathbb{Z}$, $d \neq 0 \Rightarrow$

   $d | a \iff ord_p(a) \geq ord_p(d)$ $\forall$ p primo

   (i fattori primi di d devono apparire in a con ordini $\geq$)
3. $MCD(a,b) = \prod_p p^{\min(ord\, a,\ ord\, b)}$

   prendo tutti i fattori primi in comune con l'esponente + piccolo

def. Minimo Comune Multiplo dati $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$

$mcm(a,b)$ è il più piccolo $m>0$ t.c. $a|m$, $b|m$

(multiplo di entrambi)

es. $mcm(5,12)=60$

$mcm(4,6)=12$

$mcm(a,b)=a \cdot b$ se $MCD(a,b)=1$

$$\text{mcm}(a,b) = \prod_{p \text{ primo}} p^{\max(\text{ord}_p(a), \text{ord}_p(b))}$$

$$\text{mcm}(a,b) \cdot \text{MCD}(a,b) = |ab|$$ [faccio il conto usando la decom. in f. primi]

NUMERI RAZIONALI

Sono i numeri della forma $\frac{p}{q}$, con $p, q \in \mathbb{Z}$, $q \neq 0$

Ci sono ∞ modi per scrivere ogni razionale.
Formalmente si fa così:

$$\mathbb{Q} = \{(p,q) \in \mathbb{Z} \times \mathbb{Z}_*,\ (p,q) \sim (p', q') \iff p \cdot q' = q \cdot p'$$

$\mathbb{Z}_* = \mathbb{Z} / \{0\}$

Classe di equivalenza: ∞ modi di rappresentare la stessa cosa

$\frac{2}{3}$ è un rappresentante della classe $\{ , \frac{2}{3}, \frac{4}{6}, \frac{-2}{-3}, \frac{200}{300} \dots \}$

(posso scegliere qualunque altra frazione)

- le classi di equivalenza che contengono $(n,1)$ ovvero le coppie $(bn, b) \in \mathbb{Z} \times \mathbb{Z}^*$
si possono identificare con gli interi, $\Rightarrow$
$$\mathbb{Z} \subset \mathbb{Q}$$

Operazioni su $\mathbb{Q}$

- somma e sottrazione $\quad \frac{p}{q} + \frac{p'}{q'} = \frac{pq' \pm p'q}{qq'}$

  elem. neutro 0

  inverso di $\frac{p}{q}$ è $-\frac{p}{q}$

- moltiplicazione $\quad \frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}$

  elem. neutro 1

  inverso di $\frac{p}{q}$ è $\frac{q}{p}$ $\quad (p \neq 0)$

- divisione $\quad \frac{p}{q} : \frac{p'}{q'} = \frac{p}{q} \cdot \frac{q'}{p'}$ inverso moltiplicativo di $\frac{p'}{q'}$

• No radici! No equazioni! $\sqrt{\frac{2}{3}} \notin \mathbb{Q}$

Oss. Aggiungendo gli irrazionali da $\mathbb{Q}$ si ottiene $\mathbb{R}$.

$\hookrightarrow$ radici ..., π, ...

$\mathbb{Q}$ densi in $\mathbb{R}$ ($\forall z \in \mathbb{R}$ $\exists q \in \mathbb{Q}$ arbitrariamente vicino)

$\mathbb{Q}$ ha area $\emptyset$.

NUMERI COMPLESSI $\mathbb{C}$

$x^2 = -1$ su $\mathbb{R}$ ✗

$i^2 = -1$ ✓

$\mathbb{C} = \{$ numeri complessi $\}$

$= \{ z = a + ib \quad a, b \in \mathbb{R}, \; i^2 = -1 \}$

$\text{Re}\, z = a =$ Parte Reale

$\text{Im}\, z = b =$ Parte immaginaria

Operazioni $z_1 = a_1 + ib_1$

$z_2 = a_2 + ib_2$

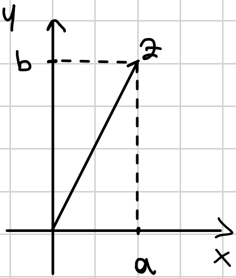
- $z_1 \pm z_2 = (a_1 \pm a_2) + i(b_1 \pm b_2)$

- $z_1 z_2 = (a_1 + ib_1)(a_2 + ib_2) = a_1 a_2 - b_1 b_2 + i a_1 b_2 + i a_2 b_1$

- $|z_1| = \sqrt{a_1^2 + b_1^2}$ (Modulo di un numero complesso)

- $\overline{z_1} = a_1 - ib_1$ Coniugio

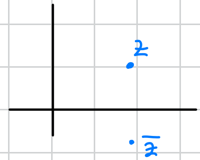
Interpretazione Geometrica dei numeri complessi



$z = a + ib$

z vettore $(a, b) = v$

- $|z| = \|v\| = \sqrt{a^2+b^2} \Rightarrow$ RAGGIO
- $\bar{z}$ è il riflesso di z rispetto all'asse x



- $z \cdot \bar{z} = (a+ib)(a-ib) = a^2 + iba - iba - (-b^2)$
  $= a^2 + b^2 = |z|^2$

- $z = a + ib$
  $$\frac{1}{z} = \frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{\bar{z}}{|z|^2}$$

- $\frac{1}{i} = -i$