ALGEBRA

(appunti delle lezioni del professor Pellarin - con note/osservazioni aggiunte)

https://open.spotify.com/playlist/3zMsGGKjUNlxx3DFJ133ex?si=rGWujY5LSLy7B1vKdUThnA&pi=e-SkW9gkIWTLG5

def ANELLO

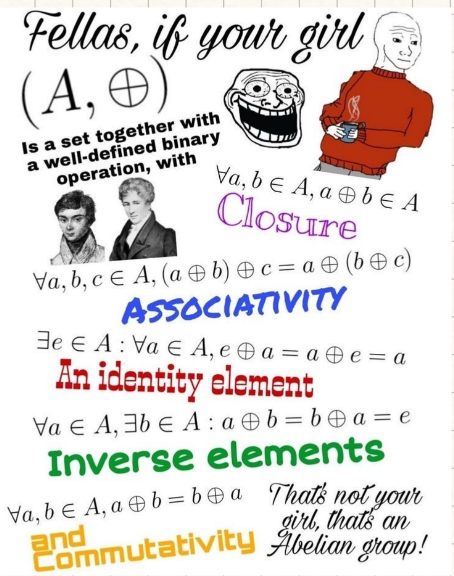
poi lo chiameremo solo A

Un anello (commutativo unitario) è il dato di una SESTUPLA $(A, +, -, \cdot, 0_A, 1_A)$

non tutti gli anelli lo sono, ma quelli studiati in questo corso sì

dove:

- $A \longrightarrow$ insieme non vuoto
- $+, \cdot \longrightarrow A \times A \longrightarrow A$ operazioni binarie
- $- \longrightarrow A \longrightarrow A$ opposto
- $0_A \longrightarrow 0_A \in A$ elemento neutro addizione
- $1_A \longrightarrow 1_A \in A$ elemento neutro moltiplicazione



questi dati devono soddisfare 8 proprietà

4 sull'addizione $(A, +, -, \cdot, 0_A, 1_A)$

① $\forall a, b \in A, \quad a + b = b + a$ COMMUTATIVITÀ

② $\forall a, b, c \in A, \quad (a+b)+c = a+(b+c)$ ASSOCIATIVITÀ della somma

③ $\forall a \in A, \quad a + 0_A = 0_A + a = a$ ELEMENTO NEUTRO della somma

④ $\forall a \in A, \quad a + (-a) = 0_A$ OPPOSTO

queste 4 proprietà indicano che $(A, +, -, 0_A)$ è un GRUPPO ABELIANO in notazione additiva

(gruppi, p.57)

4 sul prodotto $(A, +, -, \cdot, 0_A, 1_A)$:

⑤ $\forall a, b, c \in A, \quad a(b \cdot c) = (a \cdot b)c = abc$ ASSOCIATIVITÀ del prodotto

⑥ $\forall a, b, c \in A, \quad a(b+c) = ab + ac$ DISTRIBUTIVITÀ

$(a+b)c = ac + bc$

rende l'anello "unitario"

⑦ $\forall a \in A, \quad a \cdot 1_A = 1_A \cdot a = a$ EL. NEUTRO DEL PRODOTTO

⑧ $\forall a, b \in A, \quad ab = ba$ COMMUTATIVITÀ DEL PRODOTTO

rende l'anello "commutativo"

esempi: $\mathbb{Z} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ è un anello commutativo unitario

$\mathbb{N}$ non è un anello commutativo unitario perché non definisce un "opposto"

alcune proprietà

- $\forall a \in A, \quad a \cdot 0_A = 0_A$ dim: $a \cdot 0_A = a \cdot (0_A + (-0_A)) = a \cdot 0_A + a \cdot -0_A = a \cdot 0_A + (-(a \cdot 0_A)) = 0_A$

  ovvero $a + (-a)$

- Se $0_A = 1_A$, allora $\forall a \in A$, si ha $a = 0_A$ – ovvero $A = \{0_A\}$

  dim $a \in A: 1_A = 0_A \Longrightarrow a = a \cdot 1_A = a \cdot 0_A = 0_A$

def ELEMENTI INVERTIBILI

Dato A anello comm. un. con $1_A \neq 0_A$,

$a \in A$ t.c. $\exists b \in A$: $ab = ba = 1_A$ è detto elemento invertibile (a)

· b si dice inverso di a e si scrive $b = a^{-1}$

es: 1_A è invertibile di inverso $1_A^{-1} = 1_A$

Si pone $A^\times = \{ a \in A \text{ t.c. } a \text{ è invertibile} \}$ ($A^\times$ è un gruppo)

- $A^\times$ è non vuoto : 1_A è invertibile di inverso 1_A, e $1_A \in A$ per def. di anello comm. un. quindi, $A^\times$ contiene almeno 1_A
- se $a \in A^\times$, allora $a^{-1} \in A^\times$ (se $a \cdot a^{-1} = a^{-1} a = 1_A$, non solo a^{-1} è l'inverso di a ma a è l'inverso di a^{-1} $\Rightarrow$ a^{-1} invertibile)
- se $a, b \in A^\times$, allora $ab \in A^\times$ di inverso $(ab)^{-1} = b^{-1}a^{-1}$

  $ab \cdot (ab)^{-1} = 1_A \iff a \underbrace{\overbrace{b \cdot b^{-1}}^{1_A} a^{-1}}_{1_A} = 1_A \quad a \cdot 1_A \cdot a^{-1} = a \cdot a^{-1} = 1_A$

- $0_A \notin A^\times$ $\quad \forall a \in A,\ a \cdot 0_A = 0_A$

es. · $\mathbb{Z}^\times = \{-1, 1\}$ · dato $\mathbb{Q} = (\mathbb{Q}, +, -, \cdot, 0, 1)$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

ANELLO $A = \mathbb{Z}$ L'anello $\mathbb{Z}$ (interi) ha alcune proprietà particolari

buon ordinamento e ordine totale

esiste il sottoinsieme $\mathbb{N}^* = \mathbb{N} \setminus \{0\} \subset \mathbb{Z}$ che permette di definire una relazione su $\mathbb{Z}$:

si scrive $a < b \iff a - b \in \mathbb{N}^*$

$$\forall a \in \mathbb{Z}, \text{ si ha: } \begin{cases} a \in \mathbb{N}^* & \text{è positivo} \\ a = 0 & \text{è nullo} \\ -a \in \mathbb{N}^* & \text{è negativo} \end{cases} \quad \text{(proprietà di tricotomia)}$$

Ogni sottoinsieme $E \subset \mathbb{N}^*$ non vuoto possiede un più piccolo elemento, per il principio di buon ordinamento

$$\exists c \in E \text{ t.c., } \forall e \in E \setminus \{c\}, \text{ si ha } e > c$$

Le relazioni $<$ e $\leq$ sono compatibili con $+, \cdot, -$ in questo modo:

- $a < b \iff -b < -a$, $a \leq b \iff -b \leq -a$
- $a < b$ e $c \leq d \Rightarrow a + c < b + d$, $a \leq b$ e $c \leq d \Rightarrow a + c \leq b + d$
- $0 < a < b$ e $0 < c < d \Rightarrow ac < bd$, $0 \leq a \leq b$ e $0 \leq c \leq d \Rightarrow ac \leq bd$

legge di cancellazione in $\mathbb{Z}$

Se $ab = ac$ con $a \neq 0$, allora $b = c$.

dim per induzione su $a \geq 1$

- $a = 1$ chiaro (è l'elemento neutro)
- ipotesi induttiva: $a > 1$ e $(a-1)b = (a-1)c$

Supponiamo per assurdo $b \neq c$. Allora (tricotomia) o $b > c$ o $b < c$.

Supponiamo $b > c$. $\Longrightarrow (a-1)b + b > (a-1)c + c$
(simmetrico per $b<c$)

$ab - b + b > ac - c + c$

$ab > ac$ impossibile (premessa: $ab = ac$)

quindi necessariamente $b = c$

invertibili in $\mathbb{Z}$: $\mathbb{Z}^{\times} = \{-1, +1\}$

RELAZIONE DI DIVISIBILITÀ

Introduciamo la relazione: $a, b \in A : a \mid b \iff \exists c \in A$ t.c. $b = a \cdot c$

è una relazione: • riflessiva $\forall a \in A,\ a = a \cdot 1_A$

- transitiva dati $a, b, c \in A$, • $a \mid b \iff b = aa'$ $\exists a' \in A$ • $b \mid c \iff c = bb'$ $\exists b' \in A$

quindi $c = aa'b' = a\underbrace{(a'b')}_{a''} \Longrightarrow c = aa'' \iff a \mid c$

- non simmetrica né antisimmetrica (in generale)

es. $2 \mid 4$ ma $4 \nmid 2$

è "quasi antisimmetrica" in $\mathbb{Z}$:

è però falso in un anello qualsiasi

$a, b \in \mathbb{Z}$ t.c. $a \mid b$ e $b \mid a \Longrightarrow \exists\, \underset{\pm 1}{c} \in \mathbb{Z}^{\times}$ t.c. $a = bc$

(ovvero $a \in \{b, -b\}$ o $\{a, -a\} = \{b, -b\}$)

supponiamo $a, b \neq 0$: $b = aa'$ e $a = bb'$ $\exists a', b' \in \mathbb{Z}$.

quindi $\cancel{b} = \cancel{b}a'b' \Longrightarrow 1 = a'b' \Longrightarrow a', b' \in \{1, -1\}$

è però antisimmetrica su $\mathbb{N}^*$ $(xy = 1 \iff (x,y) = (1,1))$

La divisibilità è anche compatibile con la somma (e con il prodotto): $a \mid b,\ a \mid c \Longrightarrow a \mid b+c$

$a \mid b \Longrightarrow a \mid bc$

$a \mid b \iff \exists a'$ t.c. $b = aa'$ $\qquad a \mid c \iff \exists a''$ t.c. $c = aa''$

$b + c = aa' + aa'' = a\underbrace{(a' + a'')}_{a'''} \iff a \mid b+c$

più generalmente, se $\alpha, \beta \in A$, $a \mid b$ e $a \mid c \Longrightarrow a \mid \alpha b + \beta c$ (per compatibilità: $a \mid b \Longrightarrow a \mid \alpha b$, $a \mid c \Longrightarrow a \mid \beta c$ quindi $a \mid \alpha b + \beta c$)

ELEMENTI IRRIDUCIBILI E PRIMI

def elemento irriducibile

$a \in A \setminus A^\times$ è detto irriducibile se:

$\forall b, c \in A,\ a = bc \implies$ o $b \in A^\times$ o $c \in A^\times$

/ or esclusivo (se sono entrambi invertibili, a è invertibile (x chiusura invertibili) e viene meno la premessa)

es. $A = \mathbb{Z}$ $\quad 12 = 4 \cdot 3$ con $4, 3 \notin \mathbb{Z}^\times \implies 12$ non è irr.

$7 = 1 \cdot 7 = 7 \cdot 1 = -1 \cdot -7 = -7 \cdot -1$

$1, -1 \in \mathbb{Z}^\times \implies 7$ è irr.

def numero primo

$a \in A \setminus A^\times,\ a \neq 0$ è detto primo se:

$\forall b, c \in A$, se $a | bc$ allora $a | b$ o $a | c$

es. $6 | 2 \cdot 9$ ma $6 \nmid 2$ e $6 \nmid 9 \implies 6$ non è primo

Lemma: $p \in \mathbb{Z}$ primo $\iff$ irriducibile

dim. $\implies$ (l'altro verso dimostrato a p.12)

Dato p primo, siano $a, b \in \mathbb{Z}$ t.c. $p = ab$. Quindi $p | ab$. (sappiamo quindi che $p | a$ o $p | b$)

Supponiamo senza perdita di generalità $p | a$.

$$p | a \implies a = pa' \ \exists a' \in \mathbb{Z} \implies p = \overset{a}{pa'}b \ \overset{\text{legge di cancellazione}}{\ } \ \cancel{p} = \cancel{p}(a'b) \implies 1 = a'b \implies a', b \in \{+1, -1\} = \mathbb{Z}^\times$$

- se $a' = 1$, allora $a = p \implies p = pb \implies b = 1$.
- se $a' = -1$, allora $a = -p \implies p = -pb \implies b = -1$.

quindi, p è irriducibile ∎ (ogni modo di scriverlo come $p = ab$ porta ad a o $b \in \{-1, +1\}$)

La divisibilità è una relazione di inclusione insiemistica

Dati $a, b \in \mathbb{Z} \setminus \{0\}$, $\quad a | b \iff b\mathbb{Z} \subset a\mathbb{Z}$

dim: • $\implies$ supponiamo $a | b$

$\iff \exists k \in \mathbb{Z}$ t.c. $b = ka$.

multiplo di b

Sia $b' \in b\mathbb{Z}$. Allora $\exists l$ t.c. $b' = lb$. $\quad b = ka \implies b' = \underbrace{lk}_{l'}a = l'a \iff b' \in a\mathbb{Z}$

• $\impliedby$ supponiamo $b\mathbb{Z} \subset a\mathbb{Z}$.

Allora, $\forall b' \in b\mathbb{Z}$, $b' \in a\mathbb{Z}$. Per def., $b' \in a\mathbb{Z} \iff \exists k \in \mathbb{Z}$ t.c. $b' = ka$

Ma $b' = lb$. Quindi, $lb = ka \iff b = \underbrace{k/l}_{k'}a$, quindi $b = k'a$ (ovvero $a | b$) ∎

---

def valore assoluto

$\mathbb{Z} \xrightarrow[|\cdot|]{} \mathbb{N}$ $\quad$ dato $a \in \mathbb{Z}$: • se $a = 0$, $|a| = 0$

• se $a \neq 0$, $|a| =$ l'unico elemento di $\mathbb{N}$ contenuto nell'insieme $\{a, -a\}$

$(\{a, -a\} \cap \mathbb{N})$

DIVISIONE EUCLIDEA

Dati $a, n \in \mathbb{Z}$ con $n \neq 0$, allora esistono unicamente determinati

$$q \in \mathbb{Z}, \quad r \in \{0, \dots, |n|-1\} \quad \text{t.c.} \quad a = \underbrace{n}_{\text{divisore}}\underbrace{q}_{\text{quoziente}} + \underbrace{r}_{\text{resto}}$$

$0 \leq r < |n|$ (importante)

CONGRUENZA

$a \underset{\text{"congruente a"}}{\equiv} b \pmod{n} \iff n \mid a-b$ (quindi b è il resto di a/n)

si scrive anche $\equiv_n$

$\iff \exists\, q \in \mathbb{Z}$ t.c. $a-b = qn$ ovvero il resto della divisione euclidea di $a-b$ per n è 0

La congruenza modulo n è una relazione di equivalenza:

① riflessiva: $a \equiv a \bmod n$ $\quad n \mid a-a$ vero perché $\forall x \in \mathbb{Z} \setminus \{0\},\ x \mid 0$

② simmetrica: $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n \qquad n \mid a-b \Rightarrow n \mid b-a$

$$n \mid a-b \iff a-b = qn \iff -(a-b) = -(qn) \iff b-a = -qn \iff n \mid b-a$$

③ transitiva: $a \equiv b \bmod n$ e $b \equiv c \bmod n \iff n \mid b-a$ e $n \mid c-b$

(visto che $n \mid a,\ n \mid b \Rightarrow n \mid a+b$) $\Rightarrow n \mid c-b+b-a \Rightarrow n \mid c-a \iff c \equiv a \bmod n \iff a \equiv c \bmod n$

esempi

congruenza modulo 2: $\underbrace{2\mathbb{Z}}_{[0]}^{\text{pari}} \sqcup \underbrace{2\mathbb{Z}+1}_{[1]}^{\text{dispari}} \qquad \mathbb{Z}/_{\equiv_2} = \{2\mathbb{Z}, 2\mathbb{Z}+1\}$

congruenza modulo 3: $3\mathbb{Z} \sqcup 3\mathbb{Z}+1 \sqcup 3\mathbb{Z}+2 \qquad \mathbb{Z}/_{\equiv_3} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$

$\mathbb{Z}/n\mathbb{Z}$ (ANELLO)

$\mathbb{Z}/_{\equiv_n} = \mathbb{Z}/n\mathbb{Z}$ con $n > 0$ è l'insieme quoziente di $\mathbb{Z}$ sulla congruenza mod. n

$[a] \in \mathbb{Z}/n\mathbb{Z} = \{x : x \equiv a \bmod n\} = a + n\mathbb{Z}$ ovvero tutti gli el. che danno resto a divisi per n

gli el. di $\mathbb{Z}/n\mathbb{Z}$ sono le classi di equivalenza mod. n

si esprimono come x + multiplo di n

· si può scrivere $[a]_n$

es. $\mathbb{Z}/2\mathbb{Z} = \{\underset{\text{tutti i pari}}{[0]}, \underset{\text{dispari}}{[1]}\}$ $\qquad \mathbb{Z}/3\mathbb{Z} = \{\underset{[3]}{[0]}, \underset{[4]}{[1]}, \underset{[5] = [-1]}{[2]}\}$ $\qquad \mathbb{Z}/1\mathbb{Z} = \{\underset{\text{contiene tutto } \mathbb{Z}}{[0]}\}$

Si vede "a occhio" la classe di equivalenza sottraendo o sommando n.

($[a] = x + n\mathbb{Z}$ ↳ sto solo "scalando" n, rimango nella stessa classe)

per esempio $[7] \bmod 5 = [7-5]_5 = [2]_5 = [-3]_5$

Le operazioni $+ \cdot -$ di $\mathbb{Z}$ sono compatibili con $\equiv_n$

① $\forall a, a' \in \mathbb{Z}, \quad a \equiv_n a' \iff -a \equiv_n -a'$ compatibilità con opposto

② $\forall a, a', b, b' \in \mathbb{Z}, \quad a \equiv_n a', \ b \equiv_n b' \implies a+b \equiv_n a'+b'$ compatibilità con somma

③ $\forall a, a', b, b' \in \mathbb{Z}, \quad a \equiv_n a', \ b \equiv_n b' \implies ab \equiv_n a'b'$ compatibilità con prodotto

operatori:

- $-[a] := [-a]$ opposto

- $[a]+[b] = [a+b]$ somma

indipendentemente dalla scelta di rappresentanti (ben definita):

scegliamo $a' \in [a], \ b' \in [b] \quad [a'+b'] = \{m : n \mid m - a' - b'\} \overset{a \equiv_n a',\ b \equiv_n b',\ \text{quindi per ②}}{=} \{m : n \mid m - a - b\}$

$\iff [a+b] = [a'+b']$ quindi è ben definita

es. $[1]_3 + [2]_3 = [3]$
$\quad \| \qquad \| \qquad \|$
$[4] + [-4] = [0]$

- $[a] \cdot [b] = [ab]$

ben definito:

$a' \in [a], \ b' \in [b] \quad [a'b'] = \{m : n \mid a'b'\} \overset{a' = n a,\ b' = n b,\ \text{quindi per ③}}{=} \{m : n \mid ab\}$

Teorema

$\left(\mathbb{Z}/n\mathbb{Z}, +, -, \cdot, [0], [1]\right)$ è un anello commutativo unitario. (di cui calcoleremo a breve l'insieme degli invertibili)

Alcuni sottoinsiemi di $\mathbb{Z}$

- $n\mathbb{Z} = \{ m \in \mathbb{Z} \text{ t.c. } \exists k \in \mathbb{Z} \text{ con } m = kn \}$ multipli di n
- $\mathbb{Z} \setminus \{0\} = \mathbb{Z}^*$
- $a\mathbb{Z} + b\mathbb{Z} = \{ m \in \mathbb{Z} : \exists u, v \in \mathbb{Z} \text{ con } m = ua + vb \}$

$$2\mathbb{Z} + 3\mathbb{Z} = \{ \underbrace{0, 2, 4}_{\text{multipli } 2}, \underbrace{3, 6, 9}_{\text{mul. } 3}, \underbrace{5}_{2+3}, \underbrace{8}_{2+6}, \underbrace{7}_{3+4}, \underbrace{-1}_{3-4}, \underbrace{1}_{4-3}, \dots \} = \mathbb{Z}$$

2	-7	-4	-1	2	5
0	-9	-6	-3	0	3
-2	-11	-8	-5	-2	1
-4	-13	-10	-7	-4	-1
-6	-15	-12	-9	-6	-3
	-9	-6	-3	0	3

Lemma: dato $\mathcal{E} = a\mathbb{Z} + b\mathbb{Z}$:

1. $-\mathcal{E} = \mathcal{E}$ — $\alpha \in \mathcal{E} = ua + vb$, $-\alpha = (-u)a + (-v)b$
2. $\forall \alpha, \beta \in \mathcal{E}$, $\alpha + \beta \in \mathcal{E}$ — $\alpha = xa + yb$, $\beta = x'a + y'b$ $\quad \alpha + \beta = (x+x')a + (y+y')b$
3. $\forall \alpha \in \mathcal{E}$, $x \in \mathbb{Z}$, $\alpha x \in \mathcal{E}$

logicamente, se $\alpha = ka + yb$, $xa = (xk)a + (xy)b$

Lemma Supponiamo $(a,b) \neq (0,0)$. Allora $\exists! \, \delta \in \mathbb{N}^*$ t.c. $\mathcal{E} = a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$

(tutte le combinazioni sono multiple di un solo numero)

dim: Possiamo supporre senza perdita di generalità $a, b \neq 0$

Infatti, se per esempio $b = 0$, $a\mathbb{Z} + 0 = a\mathbb{Z}$ e $\delta = |a| \in \mathbb{N}^*$

Poniamo $\mathcal{E}^* := \mathcal{E} \cap \mathbb{N}^* \subset \mathbb{N}^*$

- osserviamo che $\mathcal{E} \neq \emptyset$ ($\mathcal{E} = (-\mathcal{E}^*) \sqcup \{0\} \sqcup \mathcal{E}^*$: se $\mathcal{E}^* = \emptyset$, si avrebbe $\mathcal{E} = \{0\}$, contraddicendo $(a,b) \neq (0,0)$)

per il principio del minimo, $\mathcal{E}$ contiene quindi un più piccolo elemento.

- poniamo $\delta = \min(\mathcal{E}^*)$

- osserviamo che $|\delta| \leq a$ e $|\delta| \leq b$

- per la divisione euclidea, $a = q\delta + r$ con $r \in \{0, \dots, \delta - 1\}$

notiamo che $r = a - q\delta$. in più, dato che $\delta \in \mathcal{E}$, $\delta = ua + vb$ con $u, v \in \mathbb{Z}$

quindi, $r = a - q(ua + vb) \iff r = a - qua - qvb \iff r = a(\underbrace{1 - qu}_{k}) + b(\underbrace{-qv}_{k'}) \iff r \in \mathcal{E}$

ci sono due possibilità: ① $r = 0$, ovvero $\delta | a$

② $r > 0$ e $r \in \mathcal{E}^*$. ma, se fosse vero, avremmo $r \geq \delta$ (min $\mathcal{E}^*$), il che è impossibile per $r \in \{0, \dots, \delta - 1\}$ (div. euclidea)

quindi necessariamente $r = 0$ e $\delta | a$. per la stessa ragione, $\delta | b$.

- $\forall \alpha, \beta \in \mathbb{Z}$, $\delta \,|\, \alpha a + \beta b$ (ovvero $\mathcal{E}$) $\implies \mathcal{E} \subset \delta\mathbb{Z}$ (per $a | b \iff b\mathbb{Z} \subset a\mathbb{Z}$)

- inoltre, $\delta \in \mathcal{E} \iff \delta = ka + k'b$. quindi, $\forall x \in \mathbb{Z}$, $x\delta = xka + xkb \implies x\delta \in \mathcal{E} \implies \delta\mathbb{Z} \subset \mathcal{E}$ (ogni multiplo di δ appartiene a $\mathcal{E}$)

quindi, $\mathcal{E} \subset \delta\mathbb{Z}$ e $\delta\mathbb{Z} \subset \mathcal{E} \implies \mathcal{E} = \delta\mathbb{Z}$

MASSIMO COMUN DIVISORE

def: dato $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ con $(a,b) \neq (0,0)$

$d \in \mathbb{N}$ è MCD di a e b se:

① $d|a$ e $d|b$

② se $\exists\, d' \in \mathbb{N}$ t.c. $d'|a$ e $d'|b$, allora $d'|d$ — ogni divisore di a e b divide anche d

Lemma: se d soddisfa ① e ②, allora è unico

dim. Supponiamo che d_1, d_2 soddisfino ① e ②. mostriamo che $d_1 = d_2$

si ha $d_2 | d_1$ e $d_1 | d_2 \Longrightarrow \{d_1, -d_1\} = \{d_2, -d_2\}$ ma $d_1, d_2 \in \mathbb{N}^* \Longrightarrow d_1 = d_2$

devono essere uguali o opposti (vedi non-antisimmetria divisibilità)

def COPRIMI

Se $MCD(a,b) = 1$, si dice che a e b sono coprimi o primi tra loro

Lemma

Dato $\delta = MCD(a,b)$, $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$ $\quad \delta > 0$, $(a,b) \neq (0,0)$

$$\begin{pmatrix} \cdot \text{ se } a = 0 \quad b \neq 0 \quad \text{allora} \quad \delta = |a| > 0 \\ \cdot \text{ se } a \neq 0, \quad b = 0 \quad \text{allora} \quad \delta = |b| > 0 \end{pmatrix}$$

dim: cond. ① $\delta | a$ vero per $a\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$ $\quad (\delta | a \Longleftrightarrow a\mathbb{Z} \subset \delta\mathbb{Z})$

stessa cosa per $\delta | b$

② sia $d' \in \mathbb{N}^*$ t.c. $d'|a$ e $d'|b$.

$d'|a \Longleftrightarrow a\mathbb{Z} \subset d'\mathbb{Z}$ e $d'|b \Longleftrightarrow b\mathbb{Z} \subset d'\mathbb{Z}$

quindi, $\underbrace{a\mathbb{Z} + b\mathbb{Z}}_{\delta\mathbb{Z}} \subset d'\mathbb{Z} + d'\mathbb{Z} = d'\mathbb{Z}$

$$\delta\mathbb{Z} \subset d'\mathbb{Z} \Longleftrightarrow d' | \delta \quad \blacksquare$$

minimo comune multiplo

dati $m_1, \ldots, m_k \in \mathbb{Z} \setminus \{0\}$, il minimo comune multiplo (mcm) di $m_1, \ldots, m_k$ è l'unico intero m t.c.

① $m_1, \ldots, m_k | m$

② se $\exists\, m'$ t.c. $m_1, \ldots, m_k | m'$, allora $m | m'$

- $m\mathbb{Z} = m_1\mathbb{Z} \cap m_2\mathbb{Z} \cap \ldots \cap m_k\mathbb{Z}$
- in più, $mcm(a,b) \overset{a,b \in \mathbb{N}^*}{=} \dfrac{ab}{MCD(a,b)}$

ALGORITMO DI EUCLIDE × MCD

dati $a, b > 0$, mi permette di trovare $d = MCD(a,b)$

comincio con la divisione euclidea a diviso b (funziona sia con $a \div b$ che con $b \div a$, ma conviene fare $a \div b$ con $a > b$)

$$a = q_0 b + r_0 \qquad (0 \le r_0 < b)$$

x def resto

poi continuo dividendo il divisore per il resto

$$b = q_1 r_0 + r_1 \qquad (0 \le r_1 < r_0)$$

$$r_0 = q_2 r_1 + r_2 \qquad (0 \le r_2 < r_1)$$

⋮ $r_0, r_1, r_2 \dots$ decrescono - arriveranno a 0

$$r_{n-2} = q_n r_{n-1} + r_n \qquad (0 \le r_n < r_{n-1})$$

l'ultimo resto diverso da 0 è l'MCD

$$r_{n-1} = q_n r_n + 0$$

esempio: $a = 3522$, $b = 321$

$3522 = 10 \cdot 321 + 312$

$321 = 1 \cdot 312 + 9$

$312 = 34 \cdot 9 + 6$

$9 = 1 \cdot 6 + 3$

$6 = 2 \cdot 3 + 0$

$3 = MCD(3522, 321)$

1. $3522 \div 321$ — $3522 = 10 \cdot 321 + 312$
2. $321 \div 312$ — $321 = 1 \cdot 312 + 9$
3. $312 \div 9$ — $312 = 34 \cdot 9 + 6$
4. $9 \div 6$ — $9 = 1 \cdot 6 + 3$
5. $6 \div 3$ — $6 = 2 \cdot 3 + 0$

IDENTITÀ DI BÉZOUT

Dati $a, b \in \mathbb{Z}$ con $(a,b) \neq (0,0)$ e con $\delta = MCD(a,b)$
allora esistono due interi u, v t.c. $au + bv = \delta$

come calcolare u, v?

NOTA BENE:
- u e v NON SONO unicamente determinati

prendiamo come esempio l'algoritmo di Euclide della pagina precedente.

stiamo cercando u, v t.c. $3 = u \cdot 3522 + v \cdot 321$

partendo da sotto (metodo Pellarin)

scriviamo il penultimo passo dell'algoritmo / quello con resto = MCD
in funzione del resto, e sostituiamo i resti "risalendo"

$3 = 9 - 1 \cdot 6$

$6 = 312 - 34 \cdot 9$

$3 = 9 - 1 \cdot (312 - 34 \cdot 9)$ (svolgo)

$3 = -312 + 35 \cdot 9$

$9 = 321 - 1 \cdot 312$

$3 = -312 + 35\,(321 - 312)$

$3 = 35 \cdot 321 + 36 \cdot -312$

$312 = 3522 - 10 \cdot 321$

$3 = 321 \cdot 35 + 36 \cdot -(3522 \cdot 10 \cdot 321)$

$3 = \underline{395} \cdot 321 \underline{- 36} \cdot 3522$

abbiamo trovato u e v!

partendo da sopra (metodo Tutor) (metodo migliore imo)

partendo dal PRIMO passo dell'algoritmo,
li riscrivo tutti in funzione del resto sostituendo dove possibile
- in più, per non confondermi, scrivo a e b al posto dei due numeri iniziali

$a = 3522$, $b = 321$

$312 = a - 10b$

$9 = 321\,(b) - 312$ (sostituisco)

$9 = b - a + 10b = -a + 11b$

$6 = 312$ (sostituisco) $- 34 \cdot 9$ (sostituisco)

$6 = a - 10b - 34 \cdot (-a + 11b) = a - 10b + 34a - 374b = 35a - 384b$

$3 = 9$ (sostituisco) $- 6$ (sostituisco)

$3 = -a + 11b - (35a - 384b) = -36a + 395b$

ovvero $3 = \underline{-36} \cdot 3522 + \underline{395} \cdot 321$

trovati!

Lemma di Gauss

se $a, b \in \mathbb{Z}^*$ e $MCD(a,b) = 1$, allora $a | bc \Rightarrow a | c$

dim:

$MCD(a,b) = 1 \iff a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, quindi $\exists\, u, v \in \mathbb{Z}$ t.c. $au + bv = 1$.

Moltiplicando per c, $acu + bcv = c$

per ipotesi, $a | bc$, quindi $bc = ka$

$$acu + kav = c \iff a\underbrace{(uc + kv)}_{k'} = c \quad \text{quindi } a | c \quad \blacksquare$$

---

altro verso dimostrato a p.5

dimostriamo p irriducibile $\Rightarrow$ p primo

ricordiamo: p irriducibile $\rightarrow$ se $p = ab$ allora o $a \in A^\times$ o $b \in A^\times$

p primo $\rightarrow$ se $p | ab$, allora $p | a$ o $p | b$

- claim: se p irriducibile e $p \nmid a$, allora $a\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$

  infatti, altrimenti $\exists\, \delta > 1$ t.c. $\delta | a$ e $\delta | p$. ma p irriducibile $\Rightarrow \delta = p$.

  (divisori di un irriducibile p in $\mathbb{Z}$ sono ± 1 e $\pm p$, e $\delta > 1$)

  Avremmo quindi $p | a$ (CONTRADDIZIONE)

  Quindi $\nexists\, \delta$ e $a\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$

- Supponiamo ora $p | ab$ con p irriducibile

  Se $p | a$ ho finito: supponiamo $p \nmid a$.

  Ma allora (x il claim) $a\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$. Moltiplicando per b: $\underbrace{ab\mathbb{Z}}_{\text{divisibile per } p} + \underbrace{pb\mathbb{Z}}_{\text{divisibile per } p} = b\mathbb{Z}$ quindi $\subset p\mathbb{Z}$

  $$b\mathbb{Z} \subset p\mathbb{Z} \Rightarrow p | b \quad \blacksquare$$

Elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{ [a] : \exists\, [b] \text{ con } [a]\cdot[b] = [1] \}$$

abbiamo visto che $[a]\cdot[b] = [ab]$

(mod. n) $[ab] = 1 \iff n | ab - 1 \iff \exists\, k \in \mathbb{Z}$ t.c. $ab - 1 = kn$

$\iff a\underline{b} - \underline{k}n = 1$ è un'identità di Bézout per a, n

quindi $MCD(a,b) = 1$

quindi $(\mathbb{Z}/n\mathbb{Z})^\times = \{ [a] : a \in \mathbb{Z},\ MCD(a,n) = 1 \}$

gli invertibili sono le classi dei coprimi a n

esiste quindi un'applicazione biiettiva:

$$\{ r \in \{0, \dots, n-1\} \text{ t.c. } MCD(r,n) = 1 \} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \quad \text{che porta } r \mapsto [r]$$

invertibili

esempio: $\mathbb{Z}/12\mathbb{Z} = \{ [0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11] \}$

Cosa si osserva quando n è primo?

$n = p$ primo. Sia $r \in \{1, \dots, p-1\}$. Allora, $MCD(p, r) = 1$

p primo e irr., se $\delta > 1 | p$, $\delta = p$

Altrimenti, se si avesse $\delta = MCD(p,r) > 1$, si avrebbe $\delta | p$, $\delta | r \implies \delta = p$ e quindi $p | r$.

Ma, per def. resto, $r < p \longrightarrow$ CONTRADDIZIONE.

Quindi $MCD(p,r) = 1$

0 mai invertibile

Si ottiene quindi $(\mathbb{Z}/p\mathbb{Z})^\times = \{ [r] : 1 \le r \le p-1 \}$ ovvero $\forall [r] \in \mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$, $[r]$ è invertibile

CAMPO

def: A anello commutativo unitario t.c. $\forall a \setminus \{0\}$, $a \in A^\times$ si dice campo

esempi: · $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ è quindi un campo.

· anche $\mathbb{Q}$ e $\mathbb{R}$ sono campi.

PICCOLO TEOREMA DI FERMAT

Dato p primo e $n \in \mathbb{Z}$, $n^p \equiv n \mod p$.

· in più: se $[n] \neq [0]$ (ovvero se $[n] \in \mathbb{F}_p^\times$), allora so che $[n]$ è invertibile di inverso $[x]$

So che $[n] = [n]^p$, e quindi che $[x][n]^p = 1$

Si ha $[x][n]^p = \underbrace{[x]\,[n]}_{\text{inversi}}\,[n]^{p-1} = [n]^{p-1}$ ($[n] = [n]^p$)

dim claim: in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ campo, si ha $([a]+[b])^p = [a]^p + [b]^p$

dimostriamo il claim. scegliamo a e b rappresentanti di $[a],[b]$

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{p-2} a^2 b^{p-2} + \binom{p}{p-1} a b^{p-1} + b^p$$ sviluppo di Newton

· con $0 < i < p$, abbiamo $\binom{p}{i} = \frac{p!}{i!\,(p-i)!}^{\,*} \in \mathbb{N}$ (perché è una cardinalità) e quindi $i!\,(p-i)! \mid p$ (per questo)

· supponiamo $1 \le i \le p-1$

Siccome $p > i$, si ha $p \nmid i!$ ($i!$ si scompone in $i\,(i-1) \dots 3 \cdot 2 \cdot 1$ tutti $< p$ e p non può essere un loro prodotto in quanto primo)

Similmente, $p > p-i$ e quindi $p \nmid (p-i)!$

quindi ho $p! = \underbrace{k}_{a} \cdot \underbrace{i!\,(p-i)!}_{b}$ $\exists k \in \mathbb{N}^*$ (per $*$)

(visto che $p \nmid i$ e $p \nmid (p-i)!$) ho anche $p \nmid b$.

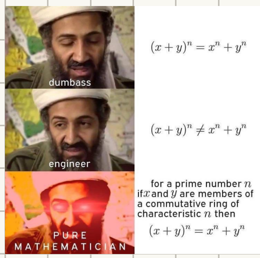
ma $p \mid p! = ab$. Quindi, visto che p primo e $p \nmid b$, allora $p | a$ per il lemma di Gauss.

Ma $a = k = \binom{p}{i}$ perché $p! = \overbrace{\frac{p!}{\cancel{i!\,(p-i)!}}}^{a} \cdot \overbrace{\cancel{i!\,(p-i)!}}^{b}$

Quindi, tutti i coefficienti "in mezzo" nello sviluppo di Newton (nella forma $\binom{p}{i}\cdot$ qualcosa) si riducono a $\emptyset$ e rimangono solo a^p e b^p

- ho dimostrato che se $1 \leq i \leq p-1$ e p primo, si ha $\binom{p}{i} = \binom{p}{p-i} \equiv_p \emptyset$

e, riducendo, ottengo $([a]+[b])^p = [a]^p + \binom{p}{1}[a]^{p-1}[b] + \ldots + [b]^p \equiv_p [a]^p + [b]^p$



torniamo alla dimostrazione principale

$[0]^p = [0]$, $[1]^p = [1]$, $[2]^p = ([1]+[1])^p = [1]^p + [1]^p = [1] + [1] = [2]$

$[3] = ([2]+[1])^p = [2]^p + [1]^p = [2] + [1] = [3]$

quindi, per induzione (con ipotesi: $[n-1]^p = [n-1]$)

$[n]^p = ([n-1]+[1])^p = [n-1]^p + [1]^p = [n-1] + [1] = [n]$

quindi, $\forall n \in \mathbb{Z}$, $n^p \equiv n$ con p primo

PRECISAZIONE

Se $[n] \neq [0]$, ovvero se $[n] \in \mathbb{F}_p$

allora $[n]$ invertibile di inverso $[n']$.

Per il PTF, so già che $[n] = [n]^p$ e $[n'] \underbrace{[n^p]}_{=} = [n'][n] \overset{\text{def. inverso}}{=} 1$

p primo $\Longrightarrow$ $p \geq 2$ si può decomporre in $p-1 \geq 1 + p$

$$[n'][n]^p = [n'][n] = [1]$$

$$\underbrace{[n'] \cdot [n]}_{\substack{\text{sono} \\ \text{inversi} \\ \text{quindi } = [1]}} [n]^{p-1} = [n'][n] = [1]$$

quindi $[1]\,[n]^{p-1} = [1]$ se $[n] \neq [0]$

(il PTF ha dei difetti:)

- se $[a] \in \mathbb{F}_p^{\times}$ (invertibili), calcolare $[a]^{-1}$ (inverso) usando il PTF

So che $[a]^{p-1} = [1]$ (PTF).

Scrivendo $[a]^{p-1} = [a]^{p-2} \cdot [a]$

(quindi $[1] = \underbrace{[a]^{p-2} \cdot [a]}_{\text{inversi}}$)

Dunque $[a]^{-1} = [a]^{p-2}$

es. $p = 691$ (primo)

Voglio calcolare $[2]^{-1}$. "Basta" calcolare $[2]^{p-2}$, ovvero $[2]^{689}$.

```
1[2, 4, 8, 16, 32, 64, 128, 256, 512, 333, 666, 641, 591, 491, 291, 582, 473, 255, 510, 329, 658, 625, 5
59, 427, 163, 326, 652, 613, 535, 379, 67, 134, 268, 536, 381, 71, 142, 284, 568, 445, 199, 398, 105, 2
10, 420, 149, 298, 596, 501, 311, 622, 553, 415, 139, 278, 556, 421, 151, 302, 604, 517, 343, 686, 681,
 671, 651, 611, 531, 371, 51, 102, 204, 408, 125, 250, 500, 309, 618, 545, 399, 107, 214, 428, 165, 330
, 660, 629, 567, 443, 195, 390, 89, 178, 356, 21, 42, 84, 168, 336, 672, 653, 615, 539, 387, 83, 166, 3
32, 664, 637, 583, 475, 259, 518, 345, 690, 689, 687, 683, 675, 659, 627, 563, 435, 179, 358, 25, 50, 1
00, 200, 400, 109, 218, 436, 181, 362, 33, 66, 132, 264, 528, 365, 39, 78, 156, 312, 624, 557, 423, 155
, 310, 620, 549, 407, 123, 246, 492, 293, 586, 481, 271, 542, 393, 95, 190, 380, 69, 138, 276, 552, 413
, 135, 270, 540, 389, 87, 174, 348, 5, 10, 20, 40, 80, 160, 320, 640, 589, 487, 283, 566, 441, 191, 382
, 73, 146, 292, 584, 477, 263, 526, 361, 31, 62, 124, 248, 496, 301, 602, 513, 335, 670, 649, 607, 523,
 355, 19, 38, 76, 152, 304, 608, 525, 359, 27, 54, 108, 216, 432, 173, 346, 1, 2, 4, 8, 16, 32, 64, 128
, 256, 512, 333, 666, 641, 591, 491, 291, 582, 473, 255, 510, 329, 658, 625, 559, 427, 163, 326, 652, 6
13, 535, 379, 67, 134, 268, 536, 381, 71, 142, 284, 568, 445, 199, 398, 105, 210, 420, 149, 298, 596, 5
01, 311, 622, 553, 415, 139, 278, 556, 421, 151, 302, 604, 517, 343, 686, 681, 671, 651, 611, 531, 371,
 51, 102, 204, 408, 125, 250, 500, 309, 618, 545, 399, 107, 214, 428, 165, 330, 660, 629, 567, 443, 195
, 390, 89, 178, 356, 21, 42, 84, 168, 336, 672, 653, 615, 539, 387, 83, 166, 332, 664, 637, 583, 475, 2
59, 518, 345, 690, 689, 687, 683, 675, 659, 627, 563, 435, 179, 358, 25, 50, 100, 200, 400, 109, 218, 4
36, 181, 362, 33, 66, 132, 264, 528, 365, 39, 78, 156, 312, 624, 557, 423, 155, 310, 620, 549, 407, 123
, 246, 492, 293, 586, 481, 271, 542, 393, 95, 190, 380, 69, 138, 276, 552, 413, 135, 270, 540, 389, 87,
 174, 348, 5, 10, 20, 40, 80, 160, 320, 640, 589, 487, 283, 566, 441, 191, 382, 73, 146, 292, 584, 477,
 263, 526, 361, 31, 62, 124, 248, 496, 301, 602, 513, 335, 670, 649, 607, 523, 355, 19, 38, 76, 152, 30
4, 608, 525, 359, 27, 54, 108, 216, 432, 173, 346, 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 333, 666, 641
, 591, 491, 291, 582, 473, 255, 510, 329, 658, 625, 559, 427, 163, 326, 652, 613, 535, 379, 67, 134, 26
8, 536, 381, 71, 142, 284, 568, 445, 199, 398, 105, 210, 420, 149, 298, 596, 501, 311, 622, 553, 415, 1
39, 278, 556, 421, 151, 302, 604, 517, 343, 686, 681, 671, 651, 611, 531, 371, 51, 102, 204, 408, 125,
250, 500, 309, 618, 545, 399, 107, 214, 428, 165, 330, 660, 629, 567, 443, 195, 390, 89, 178, 356, 21,
42, 84, 168, 336, 672, 653, 615, 539, 387, 83, 166, 332, 664, 637, 583, 475, 259, 518, 345, 690, 689, 6
87, 683, 675, 659, 627, 563, 435, 179, 358, 25, 50, 100, 200, 400, 109, 218, 436, 181, 362, 33, 66, 132
, 264, 528, 365, 39, 78, 156, 312, 624, 557, 423, 155, 310, 620, 549, 407, 123, 246, 492, 293, 586, 481
, 271, 542, 393, 95, 190, 380, 69, 138, 276, 552, 413, 135, 270, 540, 389, 87, 174, 348, 5, 10, 20, 40,
 80, 160, 320, 640, 589, 487, 283, 566, 441, 191, 382, 73, 146, 292, 584, 477, 263, 526, 361, 31, 62, 1
24, 248, 496, 301, 602, 513, 335, 670, 649, 607, 523, 355, 19, 38, 76, 152, 304, 608, 525, 359, 27, 54,
 108, 216, 432, 173, 346, 1]
```

689' (690)

ma notiamo che le classi sono cicliche – possiamo trovare l'inverso molto prima di 689 – è quello precedente all'1, perché sappiamo che $[n]^{p-1} = [1]$ (e cerchiamo $[n]^{p-2}$)

questo funziona bene con 2, ma, per esempio, non con 3

⑤ per ogni intero n, $2n^{17} + 2n^{15} + 3n^3 + 3n$ è divisibile per 5 — esercizio

- la classe mod 5 ($\mathbb{Z}/5\mathbb{Z}$) ha le stesse operazioni di $\mathbb{Z}$

$$\left[2n^{17} + 2n^{15} + 3n^3 + 3n\right]_5 \quad \text{deve essere } [0]$$

oper. in $\mathbb{Z}/5\mathbb{Z}$

$$= [2]\cdot[n]^{17} + [2]\cdot[n]^{15} + [3]\cdot[n]^3 + [3]\cdot[n] = [0]$$

un intero n (mod 5) ha resto da 1 a 4 (quindi mi basta verificare queste classi)

- se $n \equiv_5 0 \Longleftrightarrow [n] = [0]$ allora è chiaramente verificato

altri casi:

$[1]^3 = [1\cdot1\cdot1] = [1]$ stessa cosa 15, 17

	$\bar{n}$	$[n]^3$	$[n]^{15}$	$[n]^{17}$	$3[n]$	$3[n]^3$	$2[n]^{15}$	$2[n]^{17}$	$3[n] + 3[n]^3 + 2[n]^{15} + 2[n]^{17}$
$n\equiv1$	[1]	[1]	[1]	[1]	[3] +	[3] +	[2] +	[2] =	[0]
					$3\cdot2=6$	$3\cdot3=9$	$2\cdot3=6$	$2\cdot2$	
$n\equiv2$	[2]	[3]	[3]	[2]	[1] +	[4] +	[1] +	[4] =	[0]
					$3\cdot3=9$	ecc.			
$n\equiv3$	[3]	[2]	[2]	[3]	[4] +	[1] +	[4] +	[1] =	[0]
$n\equiv4$	[4]	[4]	[4]	[4]	[2]	[2]	[3]	[3] =	[0]

divisibile per 5 in tutti i casi

studiamo le potenze 2 mod. 5

$[2]^0 = [1] \quad [2]^1 = [2] \quad [2]^2 = [4] \quad [2]^3 = [3] \; (= [8]) \quad [2]^4 = [1]$

è ciclico:

$[2]^5 = [2]\cdot[2]^4 = [2]\cdot[1] = [2]$

$[2]^6 = [2]\cdot[2]^5 = [4]$

il ciclo è lungo 4, quindi $[2]^m = [2]^{q\cdot4+r} = [2]^{q\cdot4}\cdot[2]^r = [2]^r$ (dove $[2]^{4^q} = 1^q = 1$)

quindi per calcolare $[2]^n$ basta calcolare $[2]^r$ ← resto div. per 4

potenze 3 mod 5:

$[3]^0 = [1] \quad [3]^1 = [3] \quad [3]^2 = [4] \quad [3]^3 = [2] \quad [3]^4 = [1]$

potenze 4 mod 5

$[4]^0 = [1] \quad [4]^1 = [4] \quad [4]^2 = [1] \quad [4]^3 = [4] \quad [4]^4 = [1]$

③ Nessun intero in $4\mathbb{Z}+3$

calcoliamo le classi resto modulo 4 dei quadrati

$\bar{n}$	$\bar{n}^2$
$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$
$\bar{2}$	$\bar{0}$
$\bar{3}$	$\bar{1}$

la somma di quadrati mod 4 può essere soltanto

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{2}$

in particolare, non è mai $\bar{3}$

no (si può vedere con la riduzione mod 8 e una tabella 3d)

Variante: è vero che ogni intero > 0 è somma di 3 quadrati? Si può dimostrare che ogni intero > 0 è somma di 4 quadrati (Lagrange)

FIBONACCI

(F_n) $n \geq 0$ definita induttivamente: $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$

proprietà

$MCD(F_m, F_n) = F_{MCD(m,n)}$

in particolare, $MCD(F_m, F_{m+1}) = F_1 = 1$

dim. × induzione con algo euclideo

$F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n+1}$

$MCD(F_n, F_{n+1}) = \delta_n$

$\mathbb{Z}F_n + \mathbb{Z}F_{n+1} = \mathbb{Z}\delta_n$ devo dimostrare $= 1\mathbb{Z}$

$$\begin{gathered} \| \\ \{ aF_n + bF_{n+1} : a,b \in \mathbb{Z} \} \\ \| \end{gathered}$$

def. fibonacci

$\{ aF_n + b(F_n + F_{n-1}) : a,b \in \mathbb{Z} \}$

ci serve dimostrare $= \mathbb{Z}F_{n-1} + \mathbb{Z}F_n$ così $\longrightarrow$ ipotesi induttiva: $\mathbb{Z}F_{n-1} + \mathbb{Z}F_n = \mathbb{Z}$

(claim)

17/10

claim: $=$ (serve che la funzione sia suriettiva)

$\{ (a+b)F_n + bF_{n-1} : a,b \in \mathbb{Z} \} \subseteq \mathbb{Z}F_{n-1} + \mathbb{Z}F_n = \{ uF_{n-1} + vF_n ; u,v \in \mathbb{Z} \}$

mi serve dim applicazione biiettiva:

$f: \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$

$\overset{a\ \ b}{(a,b)} \longmapsto (\overset{u}{a+b}, \overset{v}{b})$ sia $f(\mathbb{Z}^2)$ l'immagine $= \{ uF_n, vF_{n-1} : (u,v) \in f(\mathbb{Z}^2) \}$

se lo dimostro, dimostro che ogni volta che prendo a,b posso trovare u e v t.c. $u = a+b$, $v = b$ e viceversa (basta che sia suriettiva, ma dimostriamo biiettiva)

Mostriamo f suriettiva - questo basta per giustificare il claim

Possiamo mostrare che f biiettiva (+ forte)

richiamo: $A \xrightarrow{f} B$ f biiettiva $\Longleftrightarrow \forall b \in B,\ f^{-1}(\{b\})$ singleton

prop del corso $\Rightarrow f$ biiett. $\Longleftrightarrow \exists\, g : B \to A$ t.c. $f \circ g = Id_B$ $(\forall b \in B,\ f(g(b)) = b,\ \forall a \in A,\ g \circ f(a) = a)$

$f(a,b) = (a+b,\ b) =: (u,v)$

$$\begin{cases} a+b = u \\ b = v \end{cases} \qquad \begin{cases} a = u-v \\ b = v \end{cases}$$

unica soluzione (biiettività) (singleton f^{-1})

pongo $g : \mathbb{Z}^2 \to \mathbb{Z}^2$, $\quad g(u,v) \overset{\text{inversa}}{\longmapsto} (u-v,\ v)$

$$(f \circ g)(u,v) = f(g(u,v)) = f(\underbrace{u-v}_{a},\ \underbrace{v}_{b}) = \overset{a+b}{u-\cancel{v}+\cancel{v}},\ \overset{b}{v} = (u,v)$$

$$(g \circ f)(a,b) = g(f(a,b)) = g(a+b,\ b) = (a+b-b,\ b) = (a,b)$$

sono identità: f e g biiettive

Abbiamo dimostrato $\forall n > 0$ (× fibonacci indice ≥ 0) $\quad F_{n+1}\mathbb{Z} + F_n\mathbb{Z} = F_n\mathbb{Z} + F_{n-1}\mathbb{Z} = F_{n-1}\mathbb{Z} + F_{n-2}\mathbb{Z} = \dots = F_1\mathbb{Z} + F_0\mathbb{Z} =$

$= F_1\mathbb{Z} + \{0\} = \mathbb{Z}$

ho dim. che $\forall n > 0$ $\quad F_n\mathbb{Z} + F_{n-1}\mathbb{Z} = \mathbb{Z} \Longleftrightarrow MCD(F_n, F_{n-1}) = 1$ ∎

TEOREMA FONDAMENTALE DELL'ARITMETICA

$\forall a \in \mathbb{Z}^*$

① l'insieme $I = \{ p \text{ primo} : p | a \}$ è finito (il numero di primi che dividono a è finito)

② $a = (\pm 1) \cdot \prod_{\substack{p \\ \text{primo}}} p^{V_p(a)}$ dove $V_p(a) \in \mathbb{N}$ unicamente determinati

(ogni numero $\neq 0$ è il prodotto di una certa combinazione di numeri primi elevati a un certo esponente – quelli che non vogliamo saranno elevati a 0 –)

OSS

si sa che $\mathbb{P} = \{ p \in \mathbb{N}, p \text{ primo} \}$ è infinito.

Siccome

$\forall a \in \mathbb{Z}$, I_a è finito, $\prod_p p^{V_p(a)} = \prod_{p \in I_a} p^{V_p(a)} \cdot \underbrace{\prod_{p \notin I_a} p^{V_p(a)}}_{\text{sarà } 0 \text{ ("non ci servono")}}$

posso dividere i primi in divisori di a e non-divisori di a e splittare la produttoria

esempio:

$a = 7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2$
$= 7 \cdot 2 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 2$
$= 7 \cdot 5 \cdot 3^2 \cdot 2^4$

quindi $V_p(a) = \begin{cases} 1 & p = 7 \\ 1 & p = 5 \\ 2 & p = 3 \\ 4 & p = 2 \\ 0 & p > 7 \end{cases}$

OSS: dati $a = \prod_p p^{V_p(a)}$ e $b = \prod_p p^{V_p(b)}$

- $a \cdot b = \prod_p p^{V_p(a)} \prod_p p^{V_p(b)} = \prod_p p^{V_p(a) + V_p(b)}$
- $p^{V_p(a)} \, p^{V_p(b)} = p^{V_p(a) + V_p(b)}$
- $V_p(ab) = V_p(a) + V_p(b)$

$a = 12 = 2^2 \cdot 3$
$b = 15 = 5 \cdot 3$ $\Longrightarrow$

$V_2(a) = 2$ $\quad V_2(b) = 0$

$V_3(a) = 1$ $\quad V_3(b) = 1$

$V_5(a) = 0$ $\quad V_5(b) = 1$

$V_p(a \cdot b) = V_p(12 \cdot 15) = V_p(a) + V_p(b)$

$V_2(ab) = 2$ $\quad V_3(ab) = 2$ $\quad V_5(ab) = 1$ $\quad V_p(ab) = 0 \quad p > 5$

(enunciato) $\forall a > 0$, $\exists$ un numero finito di primi distinti $p_1, \dots p_r$ t.c. $a = p_1^{\alpha} \cdot \ldots \cdot p_r^{\alpha_r}$ e questa fattorizzazione è unicamente determinata.

dimostrazione teorema $a = (\pm 1) \prod_p p^{v_p(a)}$

- posso supporre $a > 0$ senza perdita di generalità

① Supponiamo per assurdo I_a infinito - vuol dire che esiste una collezione infinita di primi t.c. $p \mid a$

ma $p \mid a \implies p \leq a$ e impossibile infiniti INTERI $\leq a$ CONTR.

② Procediamo per induzione:

- $a = 1$ $\quad V_p(1) = 0 \ \forall p$ $\quad 1 = \prod_p p^0 = 1 \cdot 1 \cdot 1 \cdot \ldots \cdot 1 = 1$

- Supponiamo $a > 1$.

due casi ① a primo $\longrightarrow$ allora $a = \prod_p p^{v_p(a)}$ $\quad V_p(a) = \begin{cases} 0 & p \neq a \\ 1 & p = a \end{cases}$

② a non primo, a non è irriducibile

si può scrivere in fattori diversi da 1 e a

$\implies a = U \cdot V$ con $1 < U < a$ e $1 < V < a$

per ipotesi induttiva, visto che $U, V < a$ posso usare la formula del prodotto

posso scrivere $U = \prod_p p^{v_p(U)}$, $V = \prod_p p^{v_p(V)}$

$$a = UV = \prod_p p^{v_p(U) + v_p(V)} \ \blacksquare$$

altre proprietà (in teoria esercizi ma mi sembrano più proprietà)

① $a|b \iff \forall p,\ V_p(a) \leq V_p(b)$

dim • supponiamo $V_p(a) \leq V_p(b)$

$\iff V_p(b) - V_p(a) \geq 0 \in \mathbb{N}$

poniamo $k = \prod_p p^{V_p(b) - V_p(a)}$ è quindi un intero

osserviamo che $V_p(b) - V_p(a) = 0$ per p abbastanza grande

$$k \cdot a = \prod_p p^{V_p(b) - V_p(a)} \prod_p p^{V_p(a)} = \prod_p p^{V_p(b) - \cancel{V_p(a)} + \cancel{V_p(a)}} = \prod_p p^{V_p(b)} = b$$

quindi $b = k \cdot a$ $\exists k \in \mathbb{N}$ e quindi $a|b$

• supponiamo $a|b$

$\implies b = ka \quad \exists k \in \mathbb{N}^*$

per il teorema fondamentale:

$$\prod_p p^{V_p(b)} = \prod_p p^{V_p(k)} \cdot \prod_p p^{V_p(a)}$$

osservo che ≥ 0 perché k intero

quindi $\prod_p p^{V_p(b)} = \prod_p p^{V_p(k) + V_p(a)}$

per unicità della fattorizzazione: $V_p(b) = \underbrace{V_p(k)}_{\geq 0} + V_p(a) \iff V_p(a) = V_p(b) - V_p(k)$

$\forall p,\ V_p(b) \geq V_p(a)$ ■

② $a, b \in \mathbb{N}^*$, $MCD(a,b) = \prod_p p^{\min(V_p(a), V_p(b))}$

dim. $\delta = MCD(a,b)$ è l'unico intero di $\mathbb{N}^*$ t.c.

① $\delta | a$ e $\delta | b$

② $\forall d' \in \mathbb{N}$ $d'|a$ e $d'|b \implies d'|\delta$

considerando che $a|b \iff \forall p,\ V_p(a) \leq V_p(b)$

① $\forall p,\ V_p(\delta) \leq V_p(a)$ e $V_p(\delta) \leq V_p(b)$

② se $\exists\, d'$ t.c. $\forall p$ $\quad v_p(d') \leq v_p(a)$ e $v_p(d') \leq v_p(b)$

allora $\forall p,\ v_p(d') \leq v_p(\delta)$:

① $\Longleftrightarrow v_p(\delta) \leq \min(v_p(a), v_p(b))$

② $\Longleftrightarrow$ se d' è tale che $v_p(d') \leq \min(v_p(a), v_p(b))$
allora $v_p(d') \leq v_p(\delta)$

$\forall p,\ v_p(\delta)$ è il più grande degli interi n t.c. $n \leq \min(v_p(a), v_p(b))$

quindi $v_p(\delta) = \min(v_p(a), v_p(b))$ (se è il massimo tra i $\leq$, è l'$=$)

esercizio

$a, b, c \in \mathbb{N}^* \qquad MCD(a,b,c) \mid MCD(a,c) \cdot MCD(b,c)$

pongo $x, y, z = v_p(a), v_p(b), v_p(c)$ (per comodità)

$MCD(a,b,c) \mid MCD(a,c) \cdot MCD(b,c) \iff \exists\, n$ t.c. $MCD(a,c) \cdot MCD(b,c) = n \cdot MCD(a,b,c)$

Come dimostrato a lezione:

- $MCD(a,b,c) = \prod_p p^{\min(x,y,z)}$
- $MCD(a,c) = \prod_p p^{\min(x,z)}$
- $MCD(b,c) = \prod_p p^{\min(y,z)}$

- $MCD(a,c) \cdot MCD(b,c) = \prod_p p^{\min(x,z) + \min(y,z)}$

quindi $MCD(a,b,c) \mid MCD(a,c) \cdot MCD(b,c) \iff \prod_p p^{\min(x,z)+\min(y,z)} = \prod_p p^{\min(x,y,z)} \cdot \prod_p p^{k}$

$\iff \min(x,z) + \min(y,z) = \min(x,y,z) + k$

3 casi:

① $\min = z$

qui $\min(x,z) = z$ e $\min(y,z) = z$
e $\min(x,y,z) = z$

quindi $z + z = z + k$
ovvero $k = z$

② $\min = x$

qui $\min(x,z) = x$
e $\min(y,z) = z \circ y$

z: $x + z = x + k$, ovvero $k = z$

y: $x + y = x + k$, ovvero $k = y$

③ $\min = y$

qui $\min(y,z) = y$
e $\min(x,z) = x \circ z$

x: $x + y = y + k$, $k = x$

z: $z + y = y + k$, $k = z$

quindi $n = \prod_p p^{k}$ con k definito sopra

DIVISORI DI ZERO

dato A anello

in $\mathbb{Z}/_{6\mathbb{Z}}$, $\{[0], [1], [2], [3], [4], [5]\}$

$[2] \cdot [3] = [0]$ con $[2], [3] \neq [0]$

ma in $\mathbb{Z}$ non succede

def $a \in A$ è divisore di zero

se $\exists b \in A \setminus \{0\}$ t.c. $ab = 0_A$

in A qualsiasi (tranne se $1_A = 0_A$, $A = \{0\}$) 0_A è divisore di 0

- se $A = K$ CAMPO (es. $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$)

cioè $\forall a \in K \setminus \{0\}$, a invertibile $\quad K^* = K \setminus \{0\}$

L'unico divisore di zero in K è 0_K

dim • Supponiamo a divisore di zero:

da qui in poi usiamo 0 per 0_K

$\exists b \neq 0$ t. c. $ab = 0$

però b è invertibile $\longrightarrow \exists b^{-1} \in K^*$ t.c. $b \cdot b^{-1} = 1_K$

quindi posso moltiplicare termine a termine per b^{-1}

$$a\underbrace{bb^{-1}}_{1} = \underbrace{0\,b^{-1}}_{0}$$

$$a = 0$$

in $\mathbb{Z}$

in $\mathbb{Z}$, se a è divisore di 0, allora $a = 0$ (anche se $\mathbb{Z}$ non è un campo)

dim • sia a divisore di zero $\Longleftrightarrow \exists b \in \mathbb{Z}^*$ t.c. $ab = 0 \qquad (-a)(-b) = ab = 0$

Senza perdita di generalità, supponiamo $a \geq 0$

$\exists b$ t.c. $ab = 0 \Longleftrightarrow 0 = ab = \underbrace{b+b+b \ldots +b}_{a \text{ volte}} \geq b > 0$

questo è impossibile se $a > 0$.

quindi $a = 0$ ∎

def dominio

Dato A anello, $A \neq \{0\}$, si dice che A è un dominio se l'unico divisore di zero in A è 0_A.

- ogni campo è un dominio, e $\mathbb{Z}$ è un dominio (es) mostrare che $\mathbb{Z}/_{N\mathbb{Z}}$ è un dominio $\iff N$ primo ($\iff$ campo) (ngl non ho capito se basta dimostrare dominio $\iff N$ primo visto che abbiamo già visto in classe che $\mathbb{Z}/_{p\mathbb{Z}}$ campo)

- dimostriamo $\mathbb{Z}/_{N\mathbb{Z}}$ dominio $\longrightarrow N$ primo

Supponiamo $\mathbb{Z}/_{N\mathbb{Z}}$ dominio. Allora, l'unico divisore di 0_{K_N} è 0_{K_N}

Supponiamo per assurdo N non primo $\longrightarrow \exists\ a, b$, $1<a<n$, $1<b<n$ t.c. $N = ab$

quindi, $[a]\cdot[b] = [ab] = [0]$. K_n non è dominio. CONTRADD.

- dimostriamo che N primo $\longrightarrow \mathbb{Z}/_{N\mathbb{Z}}$ dominio

$\left(\mathbb{Z}/_{N\mathbb{Z}} \text{ dominio} \iff \forall\ [a], [b] \text{ t.c. } [a]\cdot[b] = [0], \text{ o } [a] = [0] \text{ o } [b] = [0]\right)$

Supponiamo $\exists\ [a], [b] \in \mathbb{Z}/_{N\mathbb{Z}}$ t.c. $[a]\cdot[b] = [0]$

$[a]\cdot[b] = [ab] = [0]$, significa $N \mid ab$ (il resto è 0)

Ma, se $N \mid ab$, poiché N primo, o $N \mid a$ o $N \mid b$. (per def. primo)

Ma, se $N \mid a$, $[a] = [0]$ e se $N \mid b$, $[b] = [0]$

Quindi, uno dei due divisori è zero

22/10

- Se $a \in A$ non è divisore di zero $(\forall b \in A \setminus \{0\},\ ab \neq 0)$ e $ax = 0_A \implies x = 0_A$

lemma <u>legge di cancellazione</u> (in A anello)

Se $a \in A$ non divisore di zero, allora $ab = ac \implies b = c$

dim:

$ab = ac \iff a(b-c) = 0$ visto che a non è divisore di 0 e $a(b-c) = 0$ $\implies b-c = 0 \iff b = c$

OSSERVAZIONE: Questo implica la legge di cancellazione in $\mathbb{Z}$ (dominio) ($a \neq 0$ perché 0 unico divisore di 0 in $\mathbb{Z}$)

risoluzione di equazioni in A (in particolare $A = \mathbb{Z}$, $A = \mathbb{Z}/_{n\mathbb{Z}}$)

$aX = b \qquad a, b \in A$

- X indeterminata (può essere un valore o un insieme) mentre x (minuscolo) è un valore

- in $A = \mathbb{Z}$ una soluzione di $aX = b$ esiste $\iff a|b$
  - infatti, se l'insieme delle soluzioni $\neq \emptyset$ e se x soluzione, si ha $ax = b \iff a|b$ (def. $|$)
  - Se, invece, $a|b \implies \exists k \in \mathbb{Z}$ t.c. $b = ak$ e prendo $k = x$

esempio: $2x = 3$ insieme delle soluzioni $= \{x \in \mathbb{Z} : 2x = 3\} = \emptyset$ vorrebbe dire $2|3$ – impossibile

$2x = 6 \quad \{x \in \mathbb{Z} : 2x = 6\} = \{3\}$ osserviamo $6 = 2 \cdot 3$ quindi $2x = 2 \cdot 3 \implies x = 3$

- $A = \mathbb{Z}/_{n\mathbb{Z}}$, $n \in \mathbb{N}^*$

$aX = b$

- Nel caso in cui A è un anello qualsiasi e $a \in A^\times$ di inverso a^{-1}, posso moltiplicare termine a termine per a^{-1}

$$\underbrace{a^{-1}a}_{1_A} X = a^{-1} b$$

quindi l'eq. ha l'unica soluzione $x = a^{-1} b$

- Se per esempio $A = K$ campo (es $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$)

$aX = b$ con $a \neq 0$ ammette sempre l'unica soluzione $x = a^{-1} b$

Proposizione $aX = b \quad a, b \in A = \mathbb{Z}/n\mathbb{Z}$

ammette soluzioni $\iff \mathrm{MCD}(\alpha, n) \mid \beta$ con $a = [\alpha]$, $b = [\beta]$, $\alpha, \beta \in \mathbb{Z}$

dim:

- Dimostro ammette soluzioni $\implies \mathrm{MCD}(\alpha, n) \mid \beta$

$[\alpha][x] - [\beta] = [0]$ quindi $\equiv_n 0$ quindi multiplo di n

Sia $[x]$ soluzione: $a[x] = b$ quindi $[\alpha][x] = [\beta] \iff \alpha x - \beta \in n\mathbb{Z}$

Bézout; $\mathrm{MCD}(\alpha, n)$; $\beta \in$ ai multipli di δ

$\iff \alpha x - \beta = nk \ \exists k \in \mathbb{Z} \iff \alpha x - nk = \beta \implies \beta \in \alpha\mathbb{Z} + n\mathbb{Z} = \delta\mathbb{Z} \iff \delta \mid \beta$

- Ora dimostro $\mathrm{MCD}(\alpha, n) \mid \beta \implies$ ammette soluzioni

Sappiamo $\delta = \mathrm{MCD}(\alpha, n) \mid \beta \iff \beta = \delta x \implies \beta \in \underbrace{\alpha\mathbb{Z} + n\mathbb{Z}}_{\delta\mathbb{Z}}$

$\overset{\text{Bézout}}{\iff} \exists\, u, z$ t.c. $\beta = u\alpha + vn \iff \beta - u\alpha = vn$

x def congr. mod

$\iff \beta \equiv_n u\alpha \iff \underset{b}{[\beta]} = \underset{x}{[u]}\,\underset{=a}{[\alpha]} \qquad b = xa$

esempio: $[3]X = 0$ in $A = \mathbb{Z}/6\mathbb{Z}$

$\alpha = 3, \ \beta = 0, \ n = 6 \qquad \mathrm{MCD}(\alpha, 6) = 3 \mid 0 = \beta$

ci sono soluzioni.

$X = [2]$ è soluzione $\left([3]\cdot[2] = [6] = [0] \text{ in } \mathbb{Z}/6\mathbb{Z}\right)$

$X = [4]$ è soluzione $\left([3]\cdot[4] = [12] = [0]\right.$ o anche $\left.[3]\cdot[2]\cdot[2] = [0][2] = [0]\right)$

$X = [0]$ è soluzione $([3][0] = [0])$

l'insieme delle soluzioni è $\{[0], [2], [4]\} \subset A$

parentesi tutoraggio: equazioni diofantee

risolvere la seguente equazione diofantea: $\underset{a}{858}x + \underset{b}{253}y = \underset{c}{33}$

① calcolo l'MCD (a,b)

$858 = 3 \cdot 253 + 99$

$253 = 2 \cdot 99 + 55$

$99 = 1 \cdot 55 + 44$

$55 = 1 \cdot 44 + 11$

$44 = 4 \cdot 11 + 0$

$d = MCD(858, 253) = 11$

② mi assicuro che l'MCD divida c

(altrimenti, l'eq. non ha soluzioni)

$11 \mid 33$? sì

③ calcolo l'identità di Bézout

(la tutor lo fa da sopra e usando a, b invece dei numeri corrispondenti)

$99 = 858 - 3 \cdot 253 = a - 3b$

$55 = 253 - 2 \cdot 99 = b - 2(a-3b) = -2a + 7b$

$44 = 99 - 55 = a - 3b - (-2a + 7b) = 3a - 10b$

$11 = 55 - 44 = -2a + 7b - (3a - 10b) = -5a + 17b$

quindi $11 = -5a + 17b$

④ devo trovare $33 = xa + yb$: moltiplico a dx e sx per arrivare al numero che cerco

$11 = -5a + 17b$

x3

$33 = 3(-5a + 17b) = -15a + 51b = \underbrace{-15}_{x_0} \cdot 858 + \underbrace{51}_{y_0} \cdot 253$

ho trovato x_0 e y_0 soluzioni particolari dell'equazione

⑤ trovo le soluzioni generali

(soluzioni intere dell'omogenea associata)

(termine non moltiplicato da x_0)

$$x = x_0 + \frac{b}{MCD(a,b)} k \qquad k \in \mathbb{Z}$$

$$y = y_0 - \frac{a}{MCD(a,b)} k$$

quindi

$$x = -15 + \frac{253}{11} k = -15 + 23k \qquad k \in \mathbb{Z}$$

$$y = 51 - \frac{858}{11} k = 51 - 78k$$

lemma

$a, b, c \in \mathbb{Z}$ $\quad a, b \mid c$ e $MCD(a,b) = 1$ allora $ab \mid c$

dim:

c multiplo di a e b

$a, b \mid c \iff c = ak = bh \quad (\exists h, k \in \mathbb{Z})$

$\implies a \mid bh$ (o anche $b \mid ak$, ma scegliamo $a \mid bh$)

• Devo dimostrare $MCD(a,b) = 1 \implies a \mid h$ * $\implies ab \mid c$ moltiplicando per b da entrambi i lati ($c = bh$)

• $MCD(a,b) = 1 \iff b$ è invertibile modulo a (b invertibile se $by \equiv_a 1$ ovvero $by - 1 = ka$ $\iff by - ka = 1$ $\quad MCD(a,b) = 1 \iff ax + by = 1$ prendo $x = -k$ e queste cose sono uguali)

$\iff \exists b' \in \mathbb{Z}$ t.c. $bb' \in 1 + a\mathbb{Z}$ multiplo a con resto 1

• Dicendo $a \mid bh \implies ab' \mid b'bh = (1 + ak)h \iff ab' \overset{def\,|}{=} h + ahk$

$\iff ab' - ahk = h \iff a(b' - hk) = h$ quindi $a \mid h$ ∎

III secolo dal matematico Sun Tsu! ($\neq$ the art of war Sun Tsu)

TEOREMA CINESE DEI RESTI

Poniamo $r_1 \dots r_s \in \mathbb{N}^*$ e supponiamo $MCD(r_i, r_j) = 1 \quad \forall r_i \neq r_j$ a due a due coprimi

Consideriamo inoltre $c_1 \dots c_s \in \mathbb{Z}$

Allora il sistema

$$(*) \begin{cases} x \equiv c_1 \mod r_1 \\ x \equiv c_2 \mod r_2 \\ \vdots \\ x \equiv c_s \mod r_s \end{cases}$$

ha un'unica soluzione modulo $R := r_1 \cdot r_2 \cdot \ldots \cdot r_s$

ovvero l'insieme $\mathcal{E}_* = \{ x \text{ soluzione in } \mathbb{Z} \text{ di } (*) \}$ è $x_0 + R\mathbb{Z}$

come calcolare una soluzione particolare x_0 di $(*)$?

• $R = r_1 \cdot r_2 \cdot \ldots r_s$ • poniamo $R_i = \dfrac{R}{r_i} = r_1 \cdot r_2 \ldots \cdot \check{r_i} \cdot \ldots \cdot r_s = r_1 \cdot r_2 \cdot \ldots r_{i-1} \cdot r_{i+1} \cdot \ldots \cdot r_s$ "non c'è"

e notiamo che $MCD(R_i, r_i) = 1$ (perché $r_1 r_2$ ecc primi tra loro e in R_i "manca" proprio r_i)

Visto che sono primi tra loro, questa proprietà può essere riformulata dicendo che $[R_i] = r_i\mathbb{Z} + R_i$ (multipli di r_i con resto R_i) classe di R_i in $\mathbb{Z}/r_i\mathbb{Z}$

è invertibile di inverso $[S_i] \in \mathbb{Z}/r_i\mathbb{Z}$ $\quad [R_i][S_i] = [1]$

Quindi, $\underbrace{[R_i][S_i]}_{[1]}[c_i] = [c_i]$, $\underbrace{[S_i][c_i]}_{[y_i] \in \mathbb{Z}/r_i\mathbb{Z}}$ quindi abbiamo costruito elementi $[y_1], \ldots, [y_s] \in \mathbb{Z}/r_i\mathbb{Z}$ formati dall'inverso di R_i e c

• Ora, dimostriamo che $x_0 = \sum_{i=1}^{s} y_i R_i \in \mathbb{Z}$ è soluzione di $(*)$

$x_0 = \sum_{i=1}^{s} y_i R_i \in \mathbb{Z}$ è soluzione di $(*)$

infatti, se $i \neq j$, $r_i \mid R_j$ perché R_j è il prodotto di tutti "gli r" tranne r_j, quindi l'unico che non lo divide è r_j

Quindi $x_0 = \sum_{j=1}^{s} y_j R_j = \boxed{\underbrace{\sum_{\substack{j=1 \\ j \neq i}}^{s} y_j R_j}_{\equiv_{r_i} 0}} + y_i R_i$ isoliamo il termine non divisibile per r_i (quindi il resto)

(divisibile per r_i)

il tutto è quindi $\equiv_{r_i} y_i R_i$

(definito come)

$\equiv_{r_i} c_i$ quindi abbiamo trovato x_0 congruente a c_i mod r_i

Questo è valido $\forall i = 1, \dots, s$ dunque $x_0 = \sum_j y_j R_j$ è una sol. particolare di $(*)$

sistema omogeneo associato

$$*_{(H)} \begin{cases} x \equiv 0 & \text{mod } r_1 \\ x \equiv 0 & \text{mod } r_2 \\ \vdots \\ x \equiv 0 & \text{mod } r_s \end{cases} \qquad x \equiv_{r_i} 0, \quad i = 1 \dots s$$

Soluzioni? $x \equiv_{r_1} 0 \iff r_1 \mid x$
$x \equiv_{r_2} 0 \iff r_2 \mid x$

ma r_1, r_2 sono primi fra loro, quindi (x lemma) $r_1 r_2 \mid x$ (Si può andare avanti fino a r_s: $x \equiv_{r_3} 0 \iff r_3 \mid x$, $MCD(r_1, r_2, r_3) = 1 \implies r_1 r_2 r_3 \mid x$ ecc..)

Iterando, ottengo che $R := r_1 \dots r_s \mid x$

Quindi, l'insieme delle soluzioni di $(*_H)$ è $\mathcal{E}_H = R\mathbb{Z}$ (i multipli di R)

proposizione

L'insieme delle soluzioni di $(*)$, $\mathcal{E}_*$ è dato da $x_0 + R\mathbb{Z}$

dim: • $\mathcal{E}_* \supset x_0 + R\mathbb{Z}$ è chiaro. Infatti, se $x \in x_0 + R\mathbb{Z}$, allora $x = x_0 + Rk$ $\exists k \in \mathbb{Z}$

ma $Rk \equiv_{r_i} 0$ $\forall i = 1 \dots, s$ ($r_i \mid Rk$, perché $r_i \mid R$ – R è il prodotto di tutti gli r_i)

Addizionando con x_0, che è soluzione particolare, ottengo $x \equiv \underbrace{c_i}_{\equiv_{r_i} x_0} + \overset{Rk}{0} \equiv c_i \mod r_i$

• Dimostriamo $\mathcal{E}_* \subset x_0 + R\mathbb{Z}$

$x \equiv_{r_i} c_i \iff x - c_i \equiv_{r_i} 0$
(dal sistema)

Sia x soluzione di $(*)$. Allora, $x - x_0 \equiv_{r_i} 0$ $\forall i = 1 \dots s$

$\implies x - x_0 \in R\mathbb{Z}$ x Lemma ($r_i \mid x - x_0$, quindi $\overset{\text{coprimi}}{r_1 \cdot r_2 \dots r_s} \mid x - x_0$, quindi $x - x_0$ multiplo di R)

$\implies x \in x_0 + R\mathbb{Z} \implies \mathcal{E}_* \subset x_0 + R\mathbb{Z}$

piccola parentesi pratica: quello che ci hanno detto al TUTORAGGIO sul teorema cinese del resto (consiglio metodo Pellarin) prossima pagina

$$\begin{cases} x \equiv 1^{c} \mod 11 \\ x \equiv 2 \mod 5 \\ x \equiv 1 \mod 2 \end{cases}$$

$\cdot\ r_1 = 11, \quad r_2 = 5, \quad r_3 = 2$

Se sono coprimi, ammette un'unica soluzione modulo R

$$\bar{X} = R_1 \bar{x}_1 + R_2 \bar{x}_2 + R_3 \bar{x}_3 + Rk \qquad k \in \mathbb{Z}$$

con $R = r_1 \cdot r_2 \cdot r_3$ e $R_i = \frac{R}{r_i}$ e $\bar{X}_i$ t.c. $R_i x \equiv c \mod r_i$

① $r_1 = 11 \quad r_2 = 5 \quad r_3 = 2$ sono coprimi? sì.

② $R = r_1 \cdot r_2 \cdot r_3 = 11 \cdot 5 \cdot 2 = 110$ ricordiamo $c_1 = 1 \quad c_2 = 2 \quad c_3 = 1$

$$R_1 = \frac{11 \cdot 5 \cdot 2}{11} = 10 \qquad R_2 = \frac{11 \cdot 5 \cdot 2}{5} = 22 \qquad R_3 = \frac{11 \cdot 5 \cdot 2}{2} = 55$$

③ $\bar{X}_i = R_i x \equiv_r c$

- $\bar{X}_1 = 10x \equiv 1 \mod 11$

è un'equazione diofantea di tipo

$10x - 11h = 1$ che posso scrivere (per non avere il $-$)

con $y = -h$ $\quad 10x + 11y = 1$ (cerco solo x)

risolvo l'eq.: $\bullet\ MCD(\overset{a}{10}, \overset{b}{11}) = 1$

Bézout $\quad 1 = 10 \cdot \underline{-1} + 11 \cdot 1$ ho trovato x_0 particolare

- metto l'x particolare nella formula $\quad x = x_0 + \frac{b}{MCD(a,b)} k$

$$x = -1 + \frac{11}{1} k$$

k deve essere $\quad 0 \le k \le d-1$ (MCD)

- quindi $k \in \{0\} \longrightarrow x = -1 + 0 = -1$

quindi $[x_1] \equiv [-1] \equiv [10]$ siamo in mod 11

- $\bar{X}_2 = 22x \equiv 2 \mod 5$

$22x - 5h = 2 \Longleftrightarrow 22x + 5y = 2$ *

$\cdot\ MCD(22,5) = 1$

$22 = 4 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

quindi (Bézout)

$1 = 5 - 2 \cdot 2$

$1 = 5 - 2 \cdot (22 - 4 \cdot 5)$

$1 = \underline{-2} \cdot 22 + 9 \cdot 5$

ma qui cerchiamo $= 2$ * quindi moltiplico per 2

$2 = -4 \cdot 22 + 18 \cdot 5$

$x = -4 + \frac{5}{1} k$

$k \in \{0\} \quad [x_2] \equiv [4] \equiv [1]$

- $\bar{X}_3 = 55x \equiv 1 \mod 2$

55 è dispari, quindi $\equiv 1 \mod 2$

$1x \equiv 1 \mod 2$

$[x_3] \equiv [1] \mod 2$

④ metto tutto nella formula finale $(\bar{X} = R_1 \bar{x}_1 + R_2 \bar{x}_2 + R_3 \bar{x}_3 + Rk)$

$$[X] = 10 \cdot 10 + 22 \cdot 1 + 55 \cdot 1 + 110k = 177 + 110k = \overset{177-110}{67} + 110k$$

esercizio 8 (foglio 3)

Esercizio 8. Trovare tutti gli interi $x \in \mathbb{Z}$ che soddisfino
(i) $4x \equiv 7 (\bmod 15)$
(ii) $6x \equiv 8 (\bmod 9)$
(iii) $\begin{cases} 1025x \equiv 5312065 & (\bmod 8) \\ 36x \equiv 322 & (\bmod 5) \\ 4x \equiv 7 & (\bmod 3) \end{cases}$
(iv) $4x \equiv 3 (\bmod 385)$.

METODO PELLARIN CRT (3)

1 $4x \equiv 7 \mod 15$

1 calcolo l'MCD tra 4 e 15

$MCD(4,15) = 1 \iff [4]$ invertible mod. 15

$\exists n \in \mathbb{Z}$ t.c. $4 \cdot n \equiv_{15} 1$ (es. $n=4$)

lo faccio perché voglio che quel $4x$ diventi un $(1)x$

2 trasformo $4x$ in $x \to$ moltiplico entrambi i lati per 4

$\underbrace{4 \cdot 4}_{[1]} x \equiv_{15} 28$

$x \equiv_{15} 13$

quindi, le sol. sono $\mathcal{E} = 15\mathbb{Z} + 13$ (multipli con resto 13)

2 $6x \equiv 8 \mod 9$

noto che 6 e 9 non sono coprimi

$6x \equiv_9 8 \iff 6x - 8 = 9 \cdot k$

$\iff 8 = 6x - 9k$ ma questo è impossibile

notiamo che questi sono divisibili per 3 (MCD 3,9)
mentre 8 non lo è

$\mathcal{E} = \emptyset$

3 $\begin{cases} 1025x \equiv 5312065 \mod 8 \\ 36x \equiv 322 \mod 5 \\ 4x \equiv 7 \mod 3 \end{cases}$

1 notiamo che r_1, r_2, r_3 sono primi tra loro ✓

2 semplifichiamo le congruenze

1 (mod 8) $\cdot\ 1025 = 1024 + 1 = 2^{10} + 1 = \underbrace{(2^3)^3}_{\equiv_8 \emptyset \text{ perché } 2^3 \equiv_8 \emptyset} \cdot 2 + 1 \equiv 1 \mod 8$

$\cdot\ 5312065$

1 $8 | 40$ quindi $8 | 40 \cdot 10\mathbb{Z}$
notiamo che $5312065 = 4000000 + 1312065$

visto che $8 | 4 \cdot 10^6$ $\quad 5312065 \equiv_8 1312065$

$8 | 1200000 \quad \equiv_8 112065 \qquad 8 | 120000 \equiv_8 -7935$

$8 | 8000 \quad \equiv_8 65 \quad \equiv_8 1$

2 $\cdot\ 36 \equiv_5 1$

$\cdot\ 322 \quad 5|320 \quad \equiv_5 2$

3 $\cdot\ 4 \equiv_3 1$

$\cdot\ 7 \equiv_3 1$

il sistema diventa quindi $\begin{cases} x \equiv_8 1 \\ x \equiv_5 2 \\ x \equiv_3 1 \end{cases}$

3 calcoliamo le altre cose: $R = 3 \cdot 5 \cdot 8 = 120$

$R_1 = r_2 r_3 = 15 \qquad R_2 = r_1 r_3 = 24 \qquad R_3 = r_1 r_2 = 40$

④ troviamo gli inversi S_i

$R_1 = 15$ è invertibile modulo $r_1 = 8$ $\quad 7^{-1} \cdot 15^{-1} \equiv_8 1$ di inverso $S_1 = 7$

$R_2 = 24 \qquad 24 \cdot 4 \equiv_5 1 \qquad S_1 = 4$

$R_3 = 40 \qquad 40 \cdot 1 \equiv_3 1 \qquad S_1 = 1$

⑤ calcoliamo $y_i = S_i c_i$ e li inseriamo nella formula finale

i	S_i	c_i	y_i
1	7	1	7
2	4	2	8 $\equiv_5 3$
3	1	1	1

$$X_0 = \sum_{i=1}^{3} y_i R_i = 7 \cdot 15 + 3 \cdot 24 + 1 \cdot 40 = 217 \quad \text{soluzione particolare}$$

soluzione generale: $\mathcal{E} = 217 + 120\mathbb{Z} \overset{R}{=} 97 + 120\mathbb{Z}$

POLINOMI in una indeterminata a coeff in un campo

K campo $= \mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Un polinomio in X a coefficienti in K è definito come

$$P = \sum_{i=0}^{n} a_i X^i \qquad \text{con } a_i \in K \text{ coefficienti}, \; n \in \mathbb{Z} \text{ (dipende dal polinomio)}$$

$a_i = 0 \;\; \forall i >> 0$ (abbastanza grande)

esempio

$K = \mathbb{R}$, 0, $a_i = 0 \;\forall i$ $\quad K = \mathbb{F}_2 \quad [1]x^5 + [0]x^4 + [2]x^3 + [6]x^3 + [1]x + [1] = x^5 + x + [1]$

Insieme dei polinomi

(OSSERVAZIONE: è quindi possibile che un insieme finito es. $K = \mathbb{F}_p$ ne "generi" uno infinito - $K[X]$)

$A = K[X]$ è l'insieme dei polinomi (ogni $P \in A$)

L'insieme di polinomi ha una struttura ad anello (comm. un.) $(A, -, +, \cdot, 0, 1)$

Definiamo infatti le operazioni di somma e prodotto:

con $P = \sum_{i \geq 0} a_i X^i \quad a_i = 0 \;\forall i >> 0 \qquad Q = \sum_{i \geq 0} b_i X^i \quad b_i = 0 \;\forall i >> 0$

- $P + Q := \sum_{i \geq 0} (a_i + b_i) X^i$

prodotto di Cauchy

- $P \cdot Q := \sum_{k \geq 0} c_k X^k \quad$ con $c_k = \sum_{i+j=k} a_i b_j$ (qui si nota che $c_k = 0 \;\forall k >> 0$ - per numeri abbastanza grandi, a_i e/o b_j saranno 0)

$\longrightarrow$ grado di un polinomio

$P \in A[X] \qquad P = \sum_{i \geq 0} a^i X^i \quad a_i = 0 \;\forall i >> 0 \quad$ con $P \neq 0$ (ovvero $\{ i \in \mathbb{N} \text{ t.c. } a_i \neq 0 \}$ finito non vuoto)

$\deg(P) = \max \{ i \in \mathbb{N}, \; a_i \neq 0 \}$ grado massimo $\qquad$ • Si pone $\deg(0) := -\infty$

Quindi, l'insieme dei gradi è $\mathbb{N} \sqcup \{-\infty\} \qquad \deg : K[X] \longrightarrow \mathbb{N} \sqcup \{-\infty\}$

- elementi di grado zero $\{ P \in K[X] : \deg(P) = 0 \} = K^\times$ sono gli invertibili del campo, ovvero (per def campo) tutti gli el del campo tranne 0 (quindi sono le "costanti") associato al polinomio

Lemma

① $\deg(a) = -\infty \iff a = 0$ $\qquad$ ② $\deg(ab) = \deg(a) + \deg(b)$

③ $\deg(a+b) \leq \max(\deg(a), \deg(b))$

e $\deg(a+b) = \max(\deg(a), \deg(b))$ se $\deg(a) \neq \deg(b)$ $\quad$ se i gradi sono uguali gli el di grado maggiore si potrebbero annullare e il grado sarebbe $<$ (es. $(x^3+x) + (-x^3+2)$)

es. $a = x^2 + x + 1 \quad \deg = 2 \qquad b = x + 1 \quad \deg = 1 \qquad a+b = x^2 + 2x + 2 \quad \deg = 2$

ANALOGIE TRA I POLINOMI E $\mathbb{Z}$

$\mathbb{Z}$ $\quad$ $A = K[X]$ (anello di polinomi; K campo)

operazioni:

- $\mathbb{Z} \xrightarrow{|\cdot|} \mathbb{N}$ val assoluto

$a \longrightarrow \begin{cases} a & a \geq 0 \\ -a & a \leq 0 \end{cases}$

proprietà

1. $|a| = 0 \iff a = 0$
2. $|ab| = |a| \cdot |b|$
3. $|a+b| \leq |a| + |b|$ diseg. triangolare

- $A \xrightarrow{\deg} \mathbb{N} \sqcup \{-\infty\}$ grado polinomio

1. $\deg(a) = -\infty \iff a = 0$
2. $\deg(ab) = \deg(a) + \deg(b)$
3. $\deg(a+b) \leq \max(\deg(a), \deg(b))$

ci sono delle corrispondenze, ma serve qualcosa di più vicino

def c-valore assoluto di un polinomio

Dato un polinomio $P \in A \setminus \{0\}$

Scegliamo $c > 1$

$$|P|_c := c^{\deg(P)}$$ (dipende da c)

invece, se $P = 0$

$$|0|_c := 0 = c^{-\infty}$$

Allora proprietà

1. $|a|_c = 0 \iff a = 0$
2. $|ab|_c = |a|_c \cdot |b|_c$
3. $|a+b|_c \leq \max(|a|_c, |b|_c) \leq |a|_c + |b|_c$

Per ② $|ab|_c = c^{\deg(ab)} = c^{\deg(a)} \cdot c^{\deg(b)} = |a|_c \cdot |b|_c$

Per ③ $|a+b|_c = c^{\deg(a+b)} \leq c^{\max(\deg(a), \deg(b))} \leq c^{\deg(a)} + c^{\deg(b)}$

ALGORITMO DELLA DIVISIONE EUCLIDEA SUI POLINOMI

Teorema $a, b \in A = K[X]$ $\quad (a,b) \neq (0,0)$

Esiste unica $(q, r) \in A \times A$ t.c. $a = qb + r$ dove $\deg(r) < \deg(b)$ ovvero $|r|_c < |b|_c$

divisione in colonna

$a = x^4 + x + 1$

$b = x^3 - 2$

$x^4 +$	$x + 1$	x^3	-2
x^4	$-2x$	x	
0	$3x + 1$		

① x^4 / x^3

② moltiplico per $(x^3 - 2)$

③ scrivo qui

④ sottraggo

grado < quindi fine

$q = x$, $\quad r = 3x + 1$

CARATTERISTICHE DI $A = K[X]$

in analogia con $\mathbb{Z}$

$\mathbb{Z}$ | $A = K[X]$

$\mathbb{N}^*$ ("positivi")

POLINOMI MONICI (insieme A^+)

polinomi nella forma $P = a_0 + a_1 x + \ldots + a_n x^n$

con $a_n = 1$ (coefficiente di grado massimo $= 1$)

$\mathbb{Z}^\times = \{+1, -1\}$

INVERTIBILI

$A^\times = K^\times$ gli invertibili sono gli invertibili del campo associato

Sia $a \in A^\times$. $\exists\, b^\times$ con $ab = 1$

$\deg(ab) = \deg(a) + \deg(b) = \deg(1)$

$\Longrightarrow \deg(a) + \deg(b) = 0$ — non può dare 0 in una somma

$\deg(a)$ e $\deg(b) \in \mathbb{N}$ $(\deg(\cdot) \in \mathbb{N} \sqcup \{-\infty\})$

$\Longrightarrow \deg(a) = \deg(b) = 0$

$\Longrightarrow a, b \in K^\times$

"costanti" diverse da 0

---

divisibilità:

$a | b \iff \exists\, k \in \mathbb{Z}$ t.c. $b = ak$

- $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$

è una relazione:
- riflessiva
- transitiva
- "quasi antisimmetrica"

divisibilità per i polinomi

$P | Q \iff \exists\, H \in A$ t.c. $Q = HP$

- $P|Q \iff QA \subset PA$

è una relazione:
- riflessiva
- transitiva

- "quasi antisimmetrica":

dati $P, Q \in A$ t.c. $P|Q \wedge Q|P$

$\iff Q = HP \;\; \exists H \in A, \quad P = KQ \;\; \exists K \in A$

$\iff Q = HKQ \iff \deg(Q) = \deg(H) + \deg(K) + \deg(Q)$

$\cancel{\deg(Q)} = \deg(H) + \deg(K) + \cancel{\deg(Q)}$

$0 = \deg(H) + \deg(K)$

$\iff \deg(H) = \deg(K) = 0$

$\iff H \in K^\times, \; K \in K^\times$

$\mathbb{Z}$ è un dominio di integrità

$A = K[X]$ è un dominio d'integrità.

dim: sia $P \in A$ divisore di zero.
Allora $\exists Q \in A \setminus \{0\}$ t.c. $PQ = 0$
ovvero $\deg(PQ) = \deg(0)$
$\iff \underbrace{\deg(P) + \deg(Q)}_{\text{entrambi } \in \mathbb{N}\text{, la loro somma non può essere } -\infty} = -\infty$

quindi $\deg(P) = -\infty$ e $P = 0$ ∎

congruenza:
$a \equiv b \mod n \iff n \mid a - b$

anche i polinomi hanno la relazione di congruenza
$P, Q \in A$, $H \in A \setminus \{0\}$
$P \equiv Q \mod H$ è una relazione di equivalenza

$\mathbb{Z}/n\mathbb{Z}$ è un anello commutativo unitario

A/HA (funny) è un anello commutativo unitario

dato $a \in \mathbb{Z}$, $[a] = a + n\mathbb{Z}$

dato $P \in K[X]$, $[P] = P + HK[X]$ $(\deg(P) < \deg(H))$

Massimo Comun Divisore per i polinomi

dati $P, Q \in A$, poniamo $PA + QA = \{M \in A \text{ t.c. } \exists U, V \in A \text{ con } M = AU + BV\}$

- se $(P,Q) \neq (0,0)$, allora $PA + QA = DK[X]$ $\exists! D \in A^+$ quindi monico — se con l'algoritmo di Euclide si ottiene un polinomio non monico, basta renderlo monico (moltiplicando per l'inverso del termine con grado maggiore)

MCD:
- $D \mid P \wedge D \mid Q$
- se $\exists D' \in A$ t.c. $D' \mid P$ e $D' \mid Q$, allora $D' \mid D$

polinomi irriducibili
$P \in A \setminus A^\times$ con $\deg(P) > 0$ t.c. se $P = QR$ allora o $Q \in A^\times$ oppure $R \in A^\times$

osservazione
$X - x$ è irriducibile $\forall x \in K$.
poniamo $X - x = U \cdot V$
abbiamo $\underbrace{\deg(X - x)}_{1} = \deg(U) + \deg(V)$
$\implies \{\deg(U), \deg(V)\} = \{0, 1\}$

polinomi primi
$P \in A \setminus A^\times$ t.c. $P \mid QR \implies P \mid Q$ o $P \mid R$

anche in questo caso, P irriducibile $\iff$ P primo

Teorema della fattorizzazione unica

Ogni $H \in A \setminus \{0\}$ si decompone in modo unico come prodotto:

$$H = \underbrace{\lambda}_{\in A^\times} \cdot \prod_{\substack{P \text{ irr.} \\ \text{e monico}}} P^{V_P(H)} \qquad \text{con } V_P(H) \in \mathbb{N} \quad \text{e} \quad \{P : V_P(H) \neq 0\} \text{ finito}$$

FATTORIZZARE POLINOMI

in $K = \mathbb{R}, \mathbb{C}$ la fattorizzazione è "facile" (è facile caratterizzare i polinomi irriducibili), invece in $K = \mathbb{F}_p, \mathbb{Q}$ la fattorizzazione è difficile

teorema

- in $\mathbb{C}[x]$ i monici irriducibili sono tutti i polinomi nella forma $X - \alpha : \alpha \in \mathbb{C}$ (polinomi di primo grado)
- in $\mathbb{R}[x]$, se P monico irriducibile, allora o: ① $\deg(P) = 1$ $(X - \alpha : \alpha \in \mathbb{R})$
  ② se $\deg(P) = 2$
  $(P = X^2 + ax + b)$ allora $\Delta = a^2 - 4b < 0$

def VALUTAZIONE

dati $x \in X$, $F \in K[X] = F_0 + F_1 X + \ldots + F_n X^n$

la valutazione di F in x

è $ev_x(F) = F_0 + F_1 x + \ldots + F_n x^n$ (è la "sostituzione" di X)

$ev : K[X] \longrightarrow K$

osserviamo:

① $ev_x(F + G) = ev_x(F) + ev_x(G)$

② $ev_x(F \cdot G) = ev_x(F) \cdot ev_x(G)$

③ $\lambda \in K$, $ev_x(\lambda) = \lambda$ (costanti) e non invertibili perché vale per 0

- Si dice che $ev_x : K[X] \longrightarrow K$ è un OMOMORFISMO DI ANELLI (come gruppi ma con gli anelli)

omomorfismo gruppi p. 57

esempio: $F = X^2 + 1 \in \mathbb{R}[X]$, $x = 1$, $ev_x(F) = x^2 + 1 = 2$

Lemma

Sia $x \in K$

allora $ev_x^{-1}(\{0\}) = (X - x)A$ ($A \to K[X]$) $(x \in K$ tali che sostituite diano $0)$

($X - x$: polinomi che si annullano in X)

dim:

- dimostro $ev_x^{-1}(\{0\}) \supset (X - x)A$

  Sia $Q = (X - x)H$. Allora $ev_x(Q) = \overbrace{ev_x(X - x)}^{x - x = 0} \cdot ev_x(H) = 0$
  $\Longrightarrow Q \in ev_x^{-1}(\{0\})$

- dimostro $ev_x^{-1}(\{0\}) \subset (X - x)A$

  Sia $P \in A$ t.c. $ev_x(P) = 0$.

  per l'algoritmo di divisione euclidea per $X - x$ $\quad \exists!\, (q, r) \in A \times A$ t.c. $P = q\overbrace{(X - x)}^{b} + r \quad \deg(b) = 1$, $\deg(r) \in \{-\infty, 0\} \Longrightarrow r \in K$ (deve essere $< \deg(b)$; $r = 0$, r const $\neq 0$)

  $\underbrace{ev_x(P)}_{0 \text{ per ipotesi}} = ev_x(q(X - x) + r) = ev_x(q)\overbrace{ev_x(X - x)}^{0\ (x - x)} + ev_x(r)$

  $\Longrightarrow ev_x(r) = 0$ $(0 = 0 + ev_x(r))$ e, per ③ $r = ev_x(r) = 0$ quindi $X - x \mid P \Longleftrightarrow P \in (X - x)A$ ■ (P ha una radice in x)

$(P$ ha una radice in $x \Longleftrightarrow X - x \mid P$, $ev_x(P) = 0)$

29/10

es. 1 scheda Fattorizzare (non c'è una tecnica universale)

- $X^2 + X + 6$ in $\mathbb{R}[X]$ — un polinomio di grado 1 in $K[X]$ è sempre irriducibile. In $\mathbb{R}[X]$ anche i polinomi di grado 2 (SOLO) con $\Delta < 0$ sono irriducibili

nessuna radice reale

① $\Delta(ax^2+bx+c) = b^2 - 4ac = 1-24 = -23 < 0$ è irriducibile $\quad \forall x \in \mathbb{R},\ ev_x(X^2+X+6) \neq 0$

essendo irriducibile, la sua fattorizzazione è uguale a se stesso: "X^2+X+6"

- $X^3 - 6X^2 + 11X - 6$ in $\mathbb{R}[X]$

per i polinomi grado 3 si può andare a tentativi

· ev_0 no (c'è -6)

$ev_1(x^3-6x^2+11x-6) = 12-6-6=0$

1 è radice, quindi il pol. irriducibile $X-1$ divide il polinomio $\Longleftrightarrow X-1 \mid x^3-6x^2+11x-6$

calcolo il quoziente:

$$
\begin{array}{r|l}
X^3 - 6x^2 + 11x - 6 & x-1 \\ \cline{2-2}
X^3 - x^2 \quad\quad\quad\quad & X^2 - 5x^2 + 6 \\ \cline{1-1}
-5x^2 + 11x - 6 & \\
-5x^2 + 5x \quad\ \ & \\ \cline{1-1}
6x - 6 & \\
6x - 6 & \\ \cline{1-1}
0 &
\end{array}
$$

poi uso la formula quadratica:

$\Delta = 25-24 = 1 > 0$

quindi $x_i = \dfrac{5 \pm \sqrt{1}}{2}$ $\begin{cases} 2 \\ 3 \end{cases}$

$x^2 - 5x + 6 = (x-2)(x-3)$ (entrambi dividono e sono coprimi, quindi il loro prodotto divide) (lemma)

quindi $P = (x-1)(x^2-5x+6)$

avrei anche potuto provare ev_1, ev_2, ev_3 e vedere che avrebbe funzionato

- $X^2 - 2X + 2$ in $\mathbb{C}[X]$ $\qquad \mathbb{C} = \{x+iy \quad x,y \in \mathbb{R},\ i = \sqrt{-1} \text{ ovvero } i^2 = -1\}$

pensiamo prima in $\mathbb{R}[X]$ — un'eventuale fattorizzazione rimarrebbe in $\mathbb{C}[X]$ (al massimo da affinare)

$\Delta = 4 - 8 = -4 < 0$ è irriducibile in $\mathbb{R}[X]$

ma si fattorizza in $\mathbb{C}[X]$ perché ammette le radici

$x_1 = \dfrac{2+2i}{2} = i+1 \qquad x_2 = \dfrac{2-2i}{2} = i-1$

$F = (X-(i+1))(X-(i-1))$

- $F = X^3 - 1$ si ha $ev_1(F) = 0$ per qualunque campo

$F = (X-1)\,G$ div. euclidea FALLA $= (X-1)(X^2+X+1)$ ha $\Delta < 0$, irriducibile (anche in $\mathbb{Q}$ - se lo è in $\mathbb{R}$)

la fattorizzazione in $\mathbb{R}[X]$ è $(X-1)(X^2+X+1)$ (idem in $\mathbb{Q}[\mathbb{R}]$)

in $\mathbb{C}$: radici $x_1 = \dfrac{-1-\sqrt{-3}}{2}$ $x_2 = \dfrac{-1\ \sqrt{-3}}{2}$

la fatt. in $\mathbb{C}[X]$ è $F = (X-1)(X-x_1)(X-x_2)$

$\mathbb{C}$ NUMERI COMPLESSI

$\mathbb{C} := \{ x + iy : x, y \in \mathbb{R} \}$

$i := \sqrt{-1}$ caratterizzato dalla condizione $i^2 = -1$

possiamo anche scrivere $\mathbb{C} = \mathbb{R} + i\mathbb{R}$

Operazioni: posti $z = x + iy$ $\quad z' = x' + iy'$

- $-z := -x + i(-y) \in \mathbb{C}$ opposto

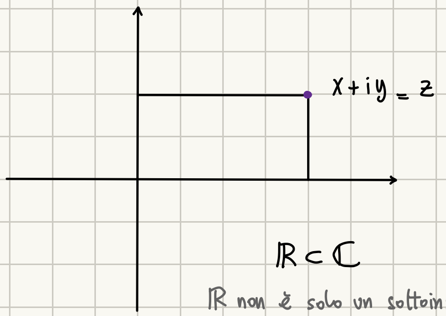
  $z + z' := (x + x') + i(y + y') \in \mathbb{C}$ somma

- $zz' := (x + iy)(x' + iy') = xx' + ix'y + ixy' + i^2 yy' =$
  $= xx' - yy' + i(x'y + xy') \in \mathbb{C}$ prodotto

- nuova operazione: CONIUGAZIONE COMPLESSA qui

$\cdot (\mathbb{C}, -, +, \cdot, 0, 1)$ è anello commutativo unitario

realizzazione cartesiana di $\mathbb{C}$



la parte reale $\mathrm{Re}(z) = x$
la parte immaginaria $\mathrm{Im}(z) = y$

$\mathbb{R} \subset \mathbb{C}$

$\mathbb{R}$ non è solo un sottoinsieme,
ma un SOTTOCAMPO (sottoinsieme campo di un campo)

$\longrightarrow$ esponenziale di Eulero

$e^{i\vartheta} := \cos(\vartheta) + i\sin(\vartheta) \in \mathbb{C}$ $\qquad \mathbb{R} \to \mathbb{C} \quad \vartheta \mapsto e^{i\vartheta}$

Eulero ha notato che, se $\vartheta, \eta \in \mathbb{R}$

$$e^{i\vartheta} \cdot e^{i\eta} \overset{\text{prop. potenze}}{=\!=\!=} e^{i(\vartheta+\eta)}$$

$$\|$$

$$[\cos(\vartheta) + i\sin(\vartheta)] \cdot [\cos(\eta) + i\sin(\eta)]$$

$$\|$$

$$\cos(\vartheta)\cos(\eta) + \cos(\vartheta) i \sin(\eta) + i\sin(\vartheta)\cos(\eta) + i^2 \sin(\vartheta)\sin(\eta)$$

$(i^2 = -1)$ $\quad i^2 \sin(\vartheta)\sin(\eta) = -\sin(\vartheta)\sin(\eta)$

$e^{i\vartheta} = \cos(\vartheta) + i\sin(\vartheta)$
con $\vartheta = \vartheta + \eta$

$$\|$$

raggruppo parte reale e immaginaria

$$\cos(\vartheta)\cos(\eta) - \sin(\vartheta)\sin(\eta) + i\left(\cos(\vartheta)\sin(\eta) + \cos(\eta)\sin(\vartheta)\right) =\!=\!= \cos(\vartheta+\eta) + i\sin(\vartheta+\eta)$$

- $\cos(\vartheta)\cos(\eta) - \sin(\vartheta)\sin(\eta) = \cos(\vartheta+\eta)$
- $\cos(\vartheta)\sin(\eta) + \cos(\eta)\sin(\vartheta) = \sin(\vartheta+\eta)$

- in modo simile si trova $(e^{i\vartheta})^n = e^{i\vartheta n}$ $\quad \forall n \in \mathbb{N}$

non l'ha fatto ma l'ho trovata su internet
(+ formula di De Moivre: $(\cos(\vartheta) + i\sin(\vartheta))^n = \cos(n\vartheta) + i\sin(\vartheta))$

esempi numeri complessi (Eulero, De Moivre)

$e^{i2\pi} = \cos(2\pi) + i\sin(2\pi) = 1 + i0 = 1$

$e^{i\cdot 0} = \cos(0) + i\sin(0) = 1 + i0 = 1$

$1 = e^{i2\pi} = e^{\frac{2\pi i}{3}\cdot 3} = \left(e^{\frac{2\pi i}{3}}\right)^3$ poniamo $x = e^{\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$

$x^3 = 1$ quindi x è radice di $x^3 - 1$ $ev_x(x^3-1) = 0$

- Osserviamo $1 = 1^2 = \left(e^{\frac{2\pi i}{3}}\right)^{3\cdot 2} = \left(e^{\frac{2\pi i}{3}\cdot 2}\right)^3 = \left(e^{\frac{4\pi i}{3}}\right)^3$ quindi anche x^2 è radice di x^3-1

- $x^0 = e^{\frac{0\pi i}{3}} = \cos\left(\frac{0\pi}{3}\right) + i\sin\left(\frac{0\pi}{3}\right) = 1$
- $x^1 = e^{\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$
- $x^2 = e^{\frac{4\pi i}{3}} = \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) = \cos\left(\frac{2\pi}{3}\right) - i\sin\left(\frac{2\pi}{3}\right)$

L'insieme $\{x^0, x^1, x^2\} = R$ ha 3 elementi distinti e

$\forall y \in R,\ ev_y(x^3-1) = 0 \implies x^3 - 1 = (x-x^0)(x-x^1)(x-x^2)$

in 4 $\quad e^{\frac{2\pi i}{3}} = \dfrac{-1+i\sqrt{3}}{2} \qquad e^{\frac{4\pi i}{3}} = \dfrac{-1-i\sqrt{3}}{2}$

CONIUGAZIONE COMPLESSA   nuova operazione di $\mathbb{C}$

Per $z = x+iy \in \mathbb{C}$

$$\bar{z} = x - iy$$ cambio segno alla parte immaginaria

poniamo anche $h: \mathbb{C} \to \mathbb{C}$, $h(z) = \bar{z}$

proprietà

1. $\overline{z+z'} = \bar{z} + \bar{z'}$ $(h(z+z') = h(z) + h(z'))$
2. $\overline{zz'} = \bar{z} \cdot \bar{z'}$ $(h(zz') = h(z)\,h(z'))$
3. $\overline{-z} = -\bar{z}$ $(h(-z) = -h(z))$
4. h è una biiezione $h^{-1} = h$

h è un **isomorfismo di anelli** → come isomorfismo gruppi, ma con anelli vedi p.57

omomorfismo: dati $(G, \cdot)$, $(H, \odot)$ strutture algebriche dello stesso tipo
un omomorfismo è $f: G \to H$
tale che $f(g \cdot h) = f(g \odot h)$ $\forall g, h \in G$

isomorfismo: omomorfismo biiettivo

es. mostrare ①, ②, ③, ④: $z = x+iy$ $z' = x'+iy'$

① $\overline{z+z'} = \bar{z} + \bar{z'}$

$\overline{x+iy} = x - iy$

$$\overline{z+z'} = \overline{(x+x') + i(y+y')} = x+x' - i(y+y') \qquad \bar{z} + \bar{z'} = x - iy + x' - iy' = \text{(raccogliendo) } x+x'+i(y+y')$$

② $\overline{zz'} = \bar{z} \cdot \bar{z'}$

$$\overline{zz'} = \overline{xx' - yy' + i(x'y + xy')} = xx' - yy' - i(x'y + xy') \qquad \bar{z} \cdot \bar{z'} = x - iy\,(x' - iy') = xx' - ixy' - ix'y + i^2 yy' = xx' - yy' - i(x'y + xy')$$

(i^2: -1)

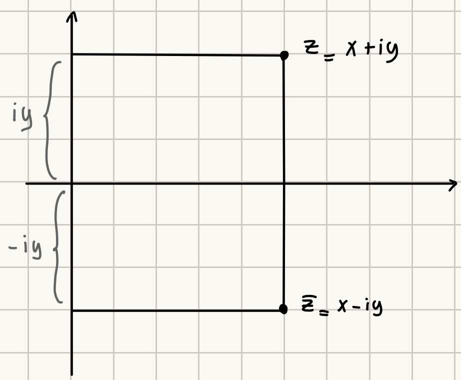
③ $\overline{-z} = -\bar{z}$

$$\overline{-z} = \overline{-x + i(-y)} = -x - i(-y) \qquad -\bar{z} = -(x - iy) = -x - i(-y)$$

reali e $\bar{z}$

$$\begin{array}{ccc} z \in \mathbb{R} & \Longleftrightarrow & z = \bar{z} \\ \Updownarrow & & \Updownarrow \\ z = x + i0 & \Longleftrightarrow & z = x - i0 \end{array}$$

nei reali, $z = \bar{z}$
(i numeri reali non hanno parte immaginaria)



graficamente, $(\bar{\cdot})$ corrisponde alla riflessione rispetto all'asse $\mathbb{R}$

$$h: \mathbb{C} \to \mathbb{C}, \quad z \mapsto \bar{z}$$

formule fondamentali

$$z\overline{z} = (x+iy)(x-iy) = x^2 - ixy + ixy + y^2 = x^2+y^2 \quad \begin{cases} = 0 \iff x = y = 0 \\ > 0 \iff z \in \mathbb{C} \setminus \{0\} \end{cases}$$

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2+y^2}$$ valore assoluto complesso

---

- $\mathbb{C}$ è un campo

(uso l'inverso di $z\overline{z}$ per trovare quello di z)

dim: dato $z \in \mathbb{C} \setminus \{0\}$, prendo $z\overline{z} = \underbrace{x^2+y^2}_{>0 \ (z \in \mathbb{C} \setminus \{0\})}$ e lo moltiplico per il suo inverso: $(x^2+y^2)^{-1}$

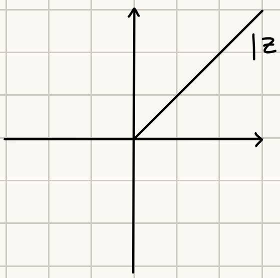
$$z \underbrace{\overline{z}(x^2+y^2)^{-1}}_{\text{inverso di } z} = 1$$ quindi ogni elemento non nullo di $\mathbb{C}$ è invertibile ∎

$$\boxed{\text{"sui libri si trova:"} \quad z \cdot \frac{\overline{z}}{(x^2+y^2)} = 1}$$

esempi:

- $z = 2 = 2+i0 \in \mathbb{R}$ $\quad \overline{z} = 2$, $\quad x^2+y^2 = 4$, $\quad z^{-1} = \frac{\overline{z}}{x^2+y^2} = \frac{2}{4} = \frac{1}{2}$
- $z = i = 0+1\cdot i$ $\quad \overline{z} = -i$ $\quad x^2+y^2 = 1$ $\quad z^{-1} = \frac{-i}{1} = -i$
- $z = 1+i$ $\quad \overline{z} = 1-i$ $\quad z\overline{z} = 2$ $\quad z^{-1} = \frac{1-i}{2}$ $\quad (i+1)\frac{1-i}{2} = \frac{2}{2} = 1$

valore assoluto complesso



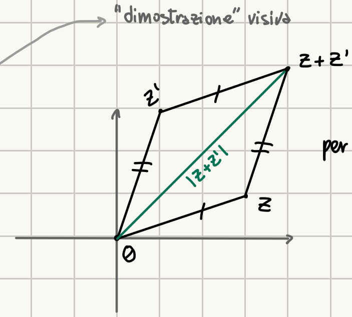
proprietà

① $|z| = 0 \iff z = 0$

② $|zz'| = |z| \cdot |z'|$

③ $|z+z'| \leq |z| + |z'|$

"dimostrazione" visiva



per le proprietà dei triangoli:
lunghezza lato < somma l. altri lati

proprietà / esercizio

$$\forall \vartheta \in \mathbb{R} \quad ① \ |e^{i\vartheta}| = 1 \qquad ② \ (e^{i\vartheta})^{-1} = \overline{e^{i\vartheta}} = e^{-i\vartheta}$$

dim:

① $e^{i\vartheta} = \cos(\vartheta) + i\sin(\vartheta)$ $\qquad |e^{i\vartheta}| \underset{\text{def } ||}{=} \sqrt{\underbrace{\cos(\vartheta)^2 + \sin(\vartheta)^2}_{=1 \ (\text{prop sin, cos})}}^{\,*} = \sqrt{1} = 1$

② • $e^{i\vartheta} \neq 0$, quindi è invertibile

$$e^{i\vartheta} \cdot e^{-i\vartheta} = e^{i\vartheta}e^{i\eta} \text{ con } \eta = -\vartheta = e^{i(\vartheta+\eta)} = e^{i0} = 1$$ quindi $e^{-i\vartheta} = (e^{i\vartheta})^{-1}$ (inverso)

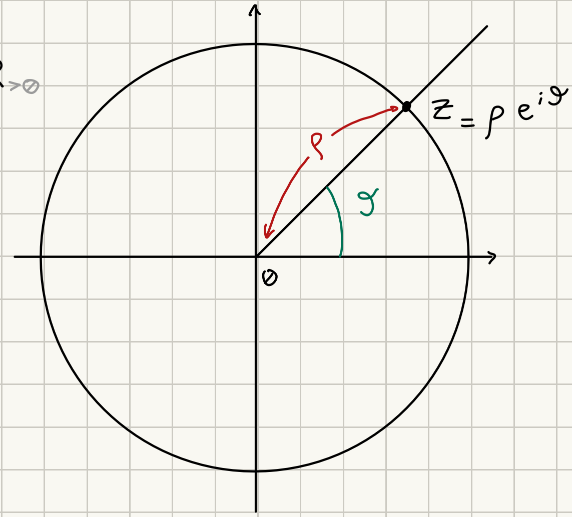
$$\overline{e^{i\vartheta}} = \cos(\vartheta) - i\sin(\vartheta) \qquad \frac{\overline{e^{i\vartheta}}}{\cos(\vartheta)^2+\sin(\vartheta)^2} \text{ è } \frac{\overline{e^{i\vartheta}}}{\underbrace{1}_{\sin(\vartheta)^2+\cos(\vartheta)^2=1}} = \overline{e^{i\vartheta}} \text{ ma anche } \frac{\overline{e^{i\vartheta}}}{\underbrace{|e^{i\vartheta}|^2}_{*}} \text{ quindi } \frac{1}{e^{i\vartheta}} \text{ quindi } \overline{e^{i\vartheta}} = (e^{i\vartheta})^{-1}$$

RAPPRESENTAZIONE POLARE

i numeri complessi possono essere rappresentati in due modi: • rappresentazione complessa ($z = x+iy$) – utile per la somma
• rappresentazione polare (trigonometrica) – utile per il prodotto

dati $z \in \mathbb{C}^{\times}$, $z = x+iy$, $\rho = \sqrt{z\bar{z}} = \sqrt{x^2+y^2}$ distanza euclidea (dall'origine) $\in \mathbb{R}_{>0}$

$z = 0$ è un unicum ($z=0 \to \rho = 0$; $\nexists(\vartheta)$)



Lemma

- $\exists\ \vartheta \in \mathbb{R}$ t.c. $z = \rho e^{i\vartheta}$
- inoltre, $\vartheta + 2\pi\mathbb{Z}$ è unicamente determinato

dim ($\exists\ \vartheta$...)

$\rho = \sqrt{z\bar{z}} = \sqrt{x^2+y^2}$, $z' := \rho^{-1}\cdot z$ — "componente angolare" $z' = \rho^{-1} z$, $z' = \rho^{-1}\rho e^{i\vartheta} = e^{i\vartheta}$

• $z' = x'+iy'$

$\exists\ \vartheta$ t.c. $x' = \cos(\vartheta)$ $y' = \sin(\vartheta)$ ①

$\Longrightarrow$ (sostituisco in $z' = x'+iy'$) $z' = \cos(\vartheta) + i\sin\vartheta = e^{i\vartheta}$ quindi (per $z' = \rho^{-1}z$) $z = \rho e^{i\vartheta}$ quindi esiste ϑ.

Le soluzioni di ① sono esattamente gli elementi di $\vartheta + 2\pi\mathbb{Z}$ per un certo $\vartheta \in [0, 2\pi)$

• Su $\mathbb{R}$ c'è la relazione di congruenza mod. 2π

$\alpha, \beta \in \mathbb{R}$ $\quad \alpha \equiv \beta \pmod{2\pi} \iff \alpha - \beta \in 2\pi\mathbb{Z}$ (che è una rel. di equivalenza)

da cui $\vartheta + 2\pi\mathbb{Z}$ è una classe di equivalenza e si identifica con un elemento di $\mathbb{R}/_{2\pi\mathbb{Z}}$ (anche se non è un anello)

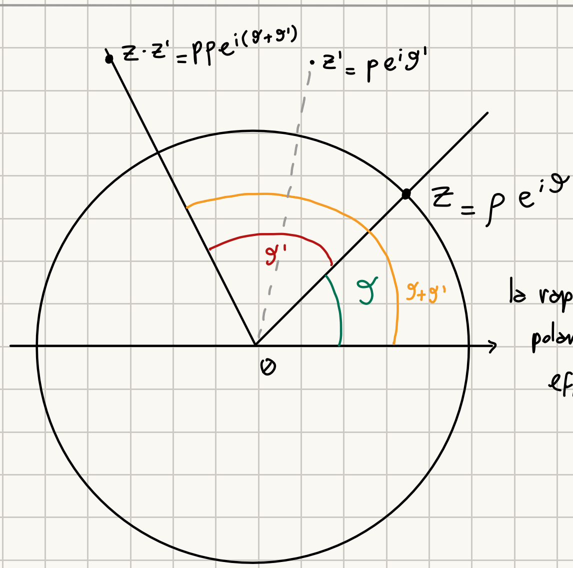
OSS: $z \in \mathbb{C}$ è della forma $e^{i\vartheta} \iff |z| = 1$. Viceversa, se $|z=1|$, la sua distanza dall'origine è 1
Quindi giace sul cerchio delle unità. $(\rho = 1)$

OSS: il coniugato di z è il suo inverso se $\rho = 1$ ($z \in$ cerchio unità)

dim (fatto al QnA)

$\bar{z} = \overline{\rho e^{i\vartheta}} = \bar{\rho}\,\overline{e^{i\vartheta}} = \rho(\cos(\vartheta) - i\sin(\vartheta)) = \rho(\cos(-\vartheta) + i\sin(-\vartheta)) = \rho e^{-i\vartheta}$ $\quad \bar{\rho} = \rho\ (\in\mathbb{R})$

$z^{-1} = (\rho e^{i\vartheta})^{-1} = \rho^{-1}e^{-i\vartheta}$ $\qquad$ Quindi, $z^{-1} = \bar{z} \iff \rho e^{-i\vartheta} = \rho^{-1}e^{-i\vartheta} \iff \rho = 1$



la rappresentazione polare è utile per effettuare moltiplicazioni di numeri complessi

in aula, visto così: • $z'\bar{z}' = \rho^{-1}z\,\overline{\rho^{-1}\bar{z}} = \rho^{-2}z\bar{z} = \rho^{-2}\cdot\rho^2 = 1$

$z\bar{z} = 1$, quindi $\sqrt{z\bar{z}} = 1$

OSS (al QnA): si ha che

$\bar{z} = -z \iff z \in i\mathbb{R}$ $\quad (y = 0)$

$\bar{z} = -z \iff x - iy = -x - iy \iff x = 0$

def ALGEBRICAMENTE CHIUSO

K campo è detto algebricamente chiuso se: $\forall F \in K[X] \setminus K$ — no el. del campo ("costanti")

$$\exists x \in K \text{ t.c. } x \text{ è radice di } F \iff \exists x \in K : X-x \mid F$$

(se ha almeno una radice in K)

Lemma

K è algebricamente chiuso se e solo se i soli polinomi irriducibili e monici sono i polinomi $X-x$, $x \in K$ (grado 1)

dimostrazione

- ($\Longrightarrow$ lemma) Sia $P \in K[X]$ irriducibile e monico.

  Siccome K è chiuso algebricamente (per ipotesi) $\exists x \in K$ t.c. $X-x \mid P$

  $P = (X-x)Q$ con $Q \in K[X] \setminus \{0\}$

  $\deg(P) = 1 + \deg(Q)$ · se P è di grado 1, ho già dimostrato.

- se $\deg(P) \geq 2$ allora $\deg(Q) \geq 1$. Quindi, $Q \notin K[X]^\times = K^\times$ ($= K \setminus \{0\}$)

  ma anche $(X-x) \notin K[X]^\times$. Questo contraddice P irriducibile $\Longrightarrow \deg(P) = 1$
  $\Longrightarrow P = X-x$

- ($\Longleftarrow$ lemma) Supponiamo $\{P \in K[X] \text{ monico irriducibile}\} = \{X-x : x \in K\}$

  Sia P monico $\deg \geq 1$. Allora $P = \prod_{\substack{Q \text{ irr.} \\ \text{e monico}}} Q^{V_Q(P)}$ (i soli irr. e monici hanno $\deg = 1$) Q è di grado 1 $\prod_{x \in K} (X-x)^{V_{X-x}(P)}$

  Sia $x \in K$ t.c. $V_{X-x}(P) \neq 0$. Allora $X-x \mid P \iff ev_x(P) = 0$
  $\iff x$ è radice di P ■

Corollario: MOLTEPLICITÀ

K algebricamente chiuso $\Longrightarrow \forall F \in K[X] \setminus \{0\}$ si scrive in modo unico come

$$F = \underset{\in K^\times}{\lambda} \prod_{x \in K} (X-x)^{V_x(F)}$$

$V_x(F)$ è la MOLTEPLICITÀ di F in x

Si ha che $\{x : V_x(F) \neq 0\} = \underbrace{\{x : ev_x(F) = 0\}}_{\text{chiaramente un pol. si decompone solo con le sue radici}} = \{x \text{ radice di } F\} = R$

Questo insieme ha cardinalità $\leq \deg(F) := n$

$$\deg(F) = \sum_{x \in K} V_x(F) = \sum_{x \in R} V_x(F) \geq \sum_{x \in R} 1 = \text{cardinalità di } R$$

(esp. dei polinomi in cui si scompone) (ovvero, perché un pol. di grado n ha $\leq n$ soluzioni)

Teorema (fondamentale dell'algebra)

$\mathbb{C}$ è algebricamente chiuso (dim. omessa perché usa element. dell'analisi)

Teorema

$\forall K$ campo esiste sempre un altro campo algebricamente chiuso che lo contiene

esempio $\mathbb{R}$ non è algebricamente chiuso ma $\mathbb{R} \subset \mathbb{C}$

(x^2+1 $\Delta < 0$ è irr. e non ha grado 1)

31/10

FATTORIZZAZIONE DI VARI POLINOMI

- $X^n - 1$ $(n \leq 5)$

il polinomio $X^n - 1$ ha sempre radice 1 (e $X-1 \mid X^n - 1$)

$$X^n - 1 = (X-1)\underbrace{Q}_{\text{unicamente determinato}}^{\deg(Q) = n-1}$$

più precisamente $Q = X^{n-1} + X^{n-2} + \ldots + X + 1$

$\downarrow$

infatti $(X-1)(X^{n-1} + X^{n-2} + \ldots + X + 1) = X^n + X^{n-1} + \ldots X^2 + X - (X^{n-1} + X^{n-2} + \ldots + X + 1) = X^n - 1$

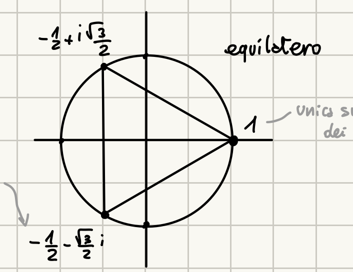
- $n = 3$ $\quad X^3 - 1 = (X-1)\underbrace{(X^2+X+1)}_{\Delta<0 \text{ irriducibile}}$ fattorizzazione in $\mathbb{R}[X]$

in $\mathbb{C}[X]$ $\quad X^2+X+1 = \left(X + \frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(X + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$

queste sono $X - X_0$ con $X_0 \in \mathbb{C}$

quindi $X_0 = x + iy$

quindi $x = -\frac{1}{2}$ e $y = -\frac{\sqrt{3}}{2}$ sul piano



(io che ragiono:)

per la rapp. polare, $\exists\, \vartheta$ t.c. $z = \rho e^{i\vartheta}$

nel cerchio delle unità, $\rho = 1$, $z = e^{i\vartheta} = \cos(\vartheta) + i \sin(\vartheta)$

quindi $-\frac{1}{2}$ e $\frac{\sqrt{3}}{2}$ sono cos e sin di un ϑ - quale?

$\cos(\vartheta) = -\frac{1}{2}$ se $\vartheta = \begin{cases} \frac{2\pi}{3} + 2k\pi \\ \frac{4\pi}{3} + 2k\pi \end{cases}$ $\qquad \sin(\vartheta) = \frac{\sqrt{3}}{2}$ se $\vartheta = \begin{cases} \frac{\pi}{3} + 2k\pi \\ \frac{2\pi}{3} + 2k\pi \end{cases}$

$\vartheta = \frac{2\pi}{3}$ - quindi $z = e^{\frac{2\pi i}{3}}$ $\quad$ (per $-\frac{1}{2}, -\frac{\sqrt{3}}{2}$ è $\frac{4\pi}{3}$)

$$-\frac{1}{2} + i\frac{\sqrt{3}}{2} = x = e^{\frac{2\pi i}{3}} \qquad -\frac{1}{2} - \frac{\sqrt{3}}{2}i = \underbrace{x^2 = \left(e^{\frac{2\pi i}{3}}\right)^2}_{①} = \underbrace{\left(e^{\frac{2\pi i}{3}}\right)^{-1}}_{②} = \overline{\left(e^{\frac{2\pi i}{3}}\right)}$$

① $-\frac{1}{2} - \frac{\sqrt{3}i}{2} = e^{\frac{4\pi}{3}} = e^{\frac{2\pi}{3} \cdot 2} = \left(e^{\frac{2\pi}{3}}\right)^2$

② abbiamo già dimostrato p.49 che $(e^{i\vartheta})^{-1} = \overline{(e^{i\vartheta})} = e^{-i\vartheta}$

quindi basta che $e^{\frac{4\pi i}{3}} = e^{\frac{-2\pi i}{3}}$ $\rightarrow$ questo è vero per periodicità:

$\frac{4\pi i}{3} = \frac{-2\pi i}{3} + 2\pi$

OSSERVAZIONE: n pari ha anche la radice -1 (perché $(-1)^n = 1$)

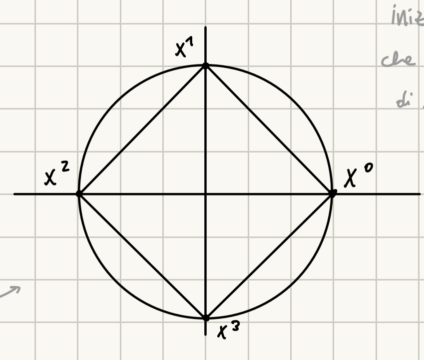
- $n = 4$ $\quad X^4 - 1 = (X-1)(X+1)(X^2+1)$ in $\mathbb{R}[X]$

$(x-1)(x+1)(x-i)(x+i)$ in $\mathbb{C}[X]$

$X^4 = (X - x^0)(X - x^1)(X - x^2)(X - x^3)$

con $x = e^{\frac{2\pi i}{4}} = e^{\frac{\pi i}{2}} = \cos\underbrace{\left(\frac{\pi}{2}\right)}_{0} + i \sin\underbrace{\left(\frac{\pi}{2}\right)}_{1} = i$

$= (x - i^0)(x - i^1)(x - i^2)(x - i^3) = (x-1)(x-i)(x+1)(x+i)$



iniziamo ad osservare che se α radice di $X^4 - 1$, allora

- o $\alpha \in \mathbb{R}$
- o anche $\overline{\alpha}$ è radice

- $n=5$ $\quad X^5-1=(X-1)\underbrace{(X^4+X^3+X^2+X+1)}_{\text{prodotto di due quadratici irriducibili monici}}$ in $\mathbb{R}[X]$

(e non quattro di primo grado perché c'è un fattore di grado 1 $\Longleftrightarrow$ c'è una radice reale e in X^5-1 c'è solo 1)

i due quadratici irriducibili (in $\mathbb{R}$) monici:

$P_1=(X-x)(X-x^4)\in\mathbb{R}[X]$

$P_2=(X-x^2)(X-x^3)\in\mathbb{R}[X]$

infatti, $P_1=(X-x)(X-\overset{x^4}{\overset{\shortparallel}{\bar{x}}})=X^2-(x+\bar{x})X+x\bar{x}$

$P_2=(X-x^2)(X-\overset{x^3}{\overset{\shortparallel}{\overline{x^2}}})=X^2-(x^2+\bar{x}^2)+|x^2|^2$

con:

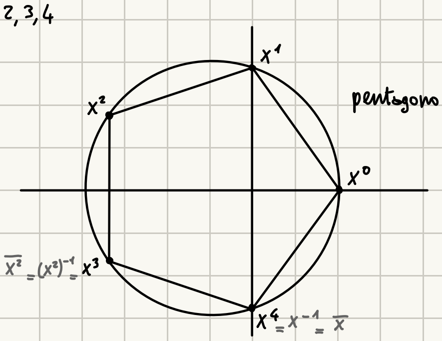
- $x=\alpha+i\beta$ $\quad$ - $\bar{x}=\alpha-i\beta$ $\quad$ - $x+\bar{x}=2\alpha\in\mathbb{R}=2\,\mathrm{Re}(x^2)=2\cos\left(\frac{2\pi}{5}\right)$

- $x\bar{x}=\alpha^2+\beta^2\geq 0=1$ (ricorda $z'\bar{z}'=1$) $\quad$ - $x^2+\overline{x^2}=2\,\mathrm{Re}(x^2)=2\cos\left(\frac{4\pi}{5}\right)$ $\quad$ - $|x^2|^2=1$

$P_1=X^2-2\cos\left(\frac{2\pi}{5}\right)X+1$, $\quad P_2=X^2-2\cos\left(\frac{4\pi}{5}\right)X+1$ $\qquad$ fatt in $\mathbb{R}[X]=(X-x^0)P_1P_2$

- in $\mathbb{C}[X]$, X^5-1 ha le radici distinte $\left(e^{\frac{2\pi i}{5}}\right)^k$ con $k=0,1,2,3,4$

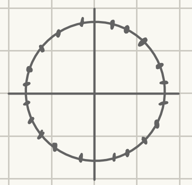
$$\left(\left(e^{\frac{2\pi i}{5}}\right)^k\right)^5=\left(e^{\frac{2\pi i}{5}\cdot 5}\right)^k=\left(\underbrace{e^{2\pi i}}_{=1}\right)^k=1$$



sono distinte perché $\left(e^{\frac{2\pi i}{5}}\right)^k\underset{\text{x De Moivre}}{=}\cos\left(\frac{2\pi k}{5}\right)+i\sin\left(\frac{2\pi k}{5}\right)$

quindi $X^5-1=\prod_{i=0}^{4}(X-x^i)=(X-x^0)\left[(X-x)(X-\underset{\bar{x}}{\underset{\shortparallel}{x^4}})\right]\left[(X-x^2)(X-\underset{\overline{x^2}}{\underset{\shortparallel}{x^3}})\right]$

OSSERVAZIONE: con $n\geq 1$, $X^n-1=\prod_{i=0}^{n-1}(X-x^i)$ con $x=e^{\frac{2\pi i}{n}}$



fatt. in $\mathbb{C}[X]$

def POLINOMIO CONIUGATO

Dato $F = f_0 + f_1 X + \ldots + f_n X^n \in \mathbb{C}[X]$, poniamo $\overline{F} = \overline{f_0} + \overline{f_1} X + \ldots + \overline{f_n} X^n$

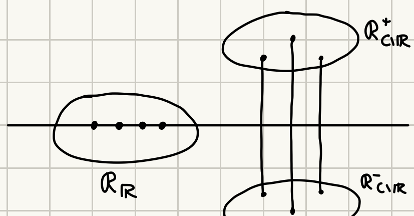
OSSERVAZIONE: $F \in \mathbb{R} \iff F = \overline{F}$ in $\mathbb{R}$, $x = \overline{x}$

inoltre, se $F \in \mathbb{R}[X]$ e $ev_z(F) = 0$, allora $ev_{\overline{z}}(F) = 0$ dim: $ev_{\overline{z}}[F] = ev_{\overline{z}}[\overline{F}]$ e, siccome la coniug. complessa è compatibile con $+, -, \cdot$ $= \overline{ev_z(F)} = \overline{0} = 0$

Lemma Dato $F \in \mathbb{R}[X]$

detto $\mathcal{R}$ l'insieme delle sue radici, allora $\mathcal{R} = \mathcal{R}_{\mathbb{R}} \sqcup \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} \sqcup \mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}}$ dove $\mathcal{R}_{\mathbb{R}} = \mathcal{R} \cap \mathbb{R}$

$\mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} = \{ z \in \mathcal{R}$ t.c. $z \in \mathbb{C}\setminus\mathbb{R}$, $\Im(z) > 0$ e scrivendo $z = \underset{\in\mathbb{R}}{x} + i\underset{\in\mathbb{R}}{y}$, $y > 0 \}$, $\mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}} = \{ z \in \mathcal{R}\setminus\mathbb{R}$ t.c. $\Im(z) < 0 \}$



inoltre $\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}} = \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} \sqcup \mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}}$ e $\overline{\mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}}} = \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}}$

Lemma già ampiamente utilizzato

$X^2 + \beta X + \gamma \in \mathbb{R}[X]$ è irriducibile $\iff \Delta = \beta^2 - 4\gamma < 0$

dim

Supponiamo P irriducibile.

$\mathcal{R}_{\mathbb{R}} = \emptyset$, quindi $\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}} = \{z, \overline{z}\}$ $\mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} = \{z\}$, $\mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}} = \{\overline{z}\}$

$$P = (X - z)(X - \overline{z}) = X^2 - \underset{2\,\mathrm{Re}(z)}{\underset{\parallel}{(z + \overline{z})}} + \underset{|z|^2}{\underset{\parallel}{z\overline{z}}}$$

$$\Delta = (z + \overline{z})^2 - 4z\overline{z} = z^2 + 2z\overline{z} + \overline{z}^2 - 4z\overline{z} = (z - \overline{z})^2$$

scrivo $z = x + iy$ $z - \overline{z} = 2iy$, quindi $(z - \overline{z})^2 = (2i\underset{\in\mathbb{R}}{y})^2 = 4i^2y^2 = 4y^2 \cdot -1 = -4y^2 < 0$ y è di parte imm > 0 quindi $y^2 \neq 0$

Lemma

Ogni $F \in \mathbb{R}[X]$ si spezza in $\mathbb{R}[X]$ in prodotto $F = \underset{\in\mathbb{R}^\times}{\lambda} \prod_{x \in \mathcal{R}_{\mathbb{R}}} (X - x)^{v_x(F)} \prod_{z \in \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}}} [(X - z)(X - \overline{z})]^{v_z(F)}$ polinomio grado 2 in $\mathbb{R}[X]$ irriducibile

presa dalle slide

dim: Siccome $\mathbb{C}$ è algebricamente chiuso,

$$F = \underset{\in\mathbb{R}^\times}{\lambda} \prod_{z \in \mathcal{R}} (X - z)^{v_z(F)} = \lambda \prod_{z \in \mathcal{R}_{\mathbb{R}}} (X - z)^{v_z(F)} \prod_{z \in \mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}} (X - z)^{v_z(F)}$$

se $z \in \mathcal{R}\setminus\mathbb{R}$ si ha $\overline{z} \in \mathcal{R}\setminus\mathbb{R}$. Quindi, posso scegliere, senza perdita di generalità, $z = x + iy$ con $y > 0$ e $\overline{z}$ apparterrà a $\mathcal{R}$

Si conclude osservando che $\mathcal{R} = \mathcal{R}_{\mathbb{R}} \sqcup \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} \sqcup \mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}}$

Lemma (in teoria esercizio ma mi sembra più un lemma)

Sia $P \in \mathbb{R}[X]$ di grado dispari. Allora P ammette almeno una radice reale.

questo implica $\deg(P) = \overset{\text{card}}{\#} R_{\mathbb{R}} + \# R_{\mathbb{C} \setminus \mathbb{R}} = \underbrace{\# R_{\mathbb{R}}}_{r} + \underbrace{2 R^+_{\mathbb{C} \setminus \mathbb{R}}}_{s}$ i coniugati

Siccome P è di grado dispari, $\deg(P) = 2n+1 = \# R_{\mathbb{R}} + 2s$ ma allora $2n+1 = r + 2s \iff r = \underbrace{2n - 2s}_{\text{pari}} + 1$ $+1 =$ dispari $\implies r \equiv 1 \mod 2 \implies r \neq 0$

ci serve il teorema dei valori intermedi (dell'Analisi)

se $h: \mathbb{R} \to \mathbb{R}$ è continua t.c. $\lim_{x \to +\infty} h(x) = +\infty$, $\lim_{x \to -\infty} h(x) = -\infty$

allora $\exists\, x_0 \in \mathbb{R}$ t.c. $h(x_0) = 0$

$P = X^{2n+1} + \alpha_{2n} X^{2n} + \ldots + \alpha_0 \in \mathbb{R}[X]$ dispari

sia $f: \mathbb{R} \to \mathbb{R}$ la funzione $f(x) = ev_x(P)$: è continua e soddisfa $\lim_{x \to -\infty} f(x) = -\infty$, $\lim_{x \to +\infty} f(x) = +\infty$

da cui $\exists\, x_0 \in \mathbb{R}$ t.c. $f(x) = 0 \iff x_0$ radice di f

esercizio 1

$P = X^4 - 10X^2 + 1$ in $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$

- in $\mathbb{C}$

tentiamo le radici. pongo $Y = X^2$ $P = Y^2 - 10Y + 1$

$\Delta > 0$, radici $y_1 = 5 - 2\sqrt{6} > 0$, $y_2 = 5 + 2\sqrt{6} > 0$ $5 > 2\sqrt{6} \iff 25 > 4 \cdot 6$

$Y^2 - 10Y + 1 = \underset{\text{in } \mathbb{Q}}{(X^2 - 5 + 2\sqrt{6})(X^2 - 5 - 2\sqrt{6})} = (X + \underbrace{\sqrt{5+2\sqrt{6}}}_{\alpha_1})(X + \underbrace{\sqrt{5-2\sqrt{6}}}_{\alpha_2})(X - \underbrace{\sqrt{5-2\sqrt{6}}}_{\alpha_3})(X - \underbrace{\sqrt{5+2\sqrt{6}}}_{\alpha_4})$ è la fatt. in $\mathbb{R}[X]$ e anche in $\mathbb{C}[X]$

POSSIBILI FATTORIZZAZIONI IN IRR. DI POLINOMI IN $\mathbb{Q}[X]$ UN CAMPO QUALSIASI

$Q \in \mathbb{Q}[X]$ (uguale per un campo qualsiasi)

- $\deg(Q) = 1$ è irriducibile
- $\deg(Q) = 2$ ① Q irriducibile
  ② $Q = P_1 P_2$ con $P_1 P_2$ irr grado 1
- $\deg(Q) = 3$ ① Q irriducibile
  ② $Q = P_1 P_2$ dove $\deg(P_1) = 1$, P_2 deg 2 irriducibile
- $\deg(Q) = 4$ ① Q irriducibile
  ② $Q = P_1 P_2$ $\deg(P_1) = 1$ $\deg(P_2) = 3$ irriducibili c'è radice
  ③ $Q = P_1 P_2$ $\deg(P_1) = \deg(P_2) = 2$ irriducibili non c'è radice
  ④ $Q = P_1 P_2 P_3$ $\deg(P_1) = 2$ $\deg(P_2) = \deg(P_3) = 1$ c'è radice

TEORIA DEI GRUPPI

GRUPPI

Dato G insieme $\neq \emptyset$ con $*$ operazione binaria su G, ovvero: $\begin{array}{l} G \times G \longrightarrow G \\ (a,b) \longrightarrow a*b \end{array}$, seleziono un elemento distinto e.

La terna $G = (G, *, e)$ è un **gruppo** se: (el. neutro)

(non per forza distinti)

① $\forall a,b,c \in G \quad (a*b)*c = a*(b*c) = a*b*c$ associatività

② $\forall a \in G \quad a*e = e*a = a$ elemento neutro per l'operazione binaria

③ $\forall a \in G \ \exists a' \in G$ t.c. $a*a' = a'*a = e$ inverso per l'op. binaria

Inoltre, se

④ $\forall a,b \in G$, $a*b = b*a$, allora G è un **gruppo abeliano** (o **commutativo**)

quindi – come avevamo visto – le prime 4 condizioni di un anello descrivono un gruppo abeliano

> add-on: **INVERSIONE NEI GRUPPI**
> $\forall a,b,c \in G \quad \cdot (ab)^{-1} = b^{-1}a^{-1}$
> $\cdot (abc)^{-1} = c^{-1}b^{-1}a^{-1}$ ecc
> (inversi dei singoli, in ordine inverso)

gruppi in notazione additiva

$(G, +, \emptyset)$ si scrive $+$ per l'operazione e $\emptyset$ o $\emptyset_G$ per l'el. neutro

si dice in notazione additiva

oss: di solito i gruppi in notazione additiva sono commutativi

In notazione additiva, l'inverso di $a \in G$ si chiama OPPOSTO e si scrive $-a$

ESEMPI $(A, +, \cdot, 0_A, 1_A)$ Anello

Allora $(A, +, 0_A)$ gruppo abeliano in not. additiva

$\mathbb{Z} = (\mathbb{Z}, +, 0)$ $\mathbb{R} = (\mathbb{R}, +, \emptyset)$, $\mathbb{C} = (\mathbb{C}, +, \emptyset)$

o anche $K = (K, +, \emptyset)$ con K qualunque campo

gruppi in notazione moltiplicativa

$(G, \cdot, \emptyset)$ si scrive $\cdot$ per l'operazione e 1 o 1_G per l'el. neutro

si dice in notazione moltiplicativa

oss: Per questi gruppi, non è garantita la commutatività.

In notazione moltiplicativa, l'inverso di $a \in G$ si scrive a^{-1}

ESEMPI $(A, +, \cdot, 0_A, 1_A)$ Anello

Allora $A^\times = (A^\times, \cdot, 1_A)$ gruppo in not. moltiplicativa

infatti abbiamo visto

⓪ il prodotto di el. invertibili è invertibile

① il prodotto è associativo

② se $a, b \in A^\times$ allora $ab \in A^\times$ e $(ab)^{-1} = b^{-1}a^{-1}$

inoltre, $A^\times$ è abeliano (se A è commutativo?)

def SOTTOGRUPPO

Dato un gruppo G e un sottoinsieme $H \subset G$ non vuoto

Si dice che H è un **Sottogruppo** di G se:

not. moltiplicativa $\quad \forall a,b \in H$, si ha $a \cdot b^{-1} \in H$ so che $\in G$, ma se $\in H$, è sottogruppo

$\forall a,b \in H$, si ha $a - b \in H$ not. additiva

Si scrive $H < G$

OSSERVAZIONE H è stabilizzato (rispetto al prodotto)

- Se $a \in H$, $\underbrace{aa^{-1}}_{a \cdot b^{-1} \text{ con } b=a} = 1_G \in H$
- Ma allora, $\forall b \in H$ $\underbrace{1_G \cdot b^{-1}}_{a \cdot b^{-1} \text{ con } a = 1_G} \in H$ quindi $b^{-1} \in H$ e $1_G = 1_H$
- Infine, se $a,b \in H$, $b^{-1} \in H$, $a(b^{-1})^{-1} = ab \in H$

(quindi un sottogruppo H contiene anche gli inversi e i prodotti dei suoi el.)
e anche l'el. neutro del gruppo di cui è sottogruppo

def OMOMORFISMI DI GRUPPI

Dati G_1, G_2 gruppi (in notazione moltiplicativa)

Sia $f: G_1 \longrightarrow G_2$ un'applicazione:

f è un omomorfismo di gruppi se

① $f(1_{G_1}) = 1_{G_2}$

② $\forall a \in G_1$, $f(\underbrace{a^{-1}}_{\text{inversione in } G_1}) = f(a)^{\overbrace{-1}^{\text{inversione in } G_2}}$ (ma basta solo la ③ - che implica le altre)

③ $\forall a, b \in G_1$, $f(a \underbrace{\,}_{\text{operazione di } G_1} b) = f(a) \underbrace{\,}_{\text{operazione di } G_2} f(b)$ (in modo più chiaro: $\cdot$ op. G_1, $\circ$ op. G_2)

$f(a \cdot b) = f(a) \circ f(b)$

(l'ordine conta! non si sa se è abeliano)

esercizio: mostrare che $f: G_1 \longrightarrow G_2$ è un omomorfismo $\Longleftrightarrow$ $\forall a, b \in G_1$, $f(ab^{-1}) = f(a) f(b)^{-1}$

- $\Longrightarrow$ supponiamo f omomorfismo.

  Allora $f(ab) = f(a) f(b)$ (③) quindi $f(ab^{-1}) = f(a) f(b^{-1})$.

  Ma (per ②) $f(b^{-1}) = f(b)^{-1}$

  Quindi $f(ab^{-1}) = f(a) f(b)^{-1}$

- $\Longleftarrow$ supponiamo $f(ab^{-1}) = f(a) f(b)^{-1}$

- $f(1_{G_1}) = 1_{G_2}$ dim: pongo $a = b$ $f(b b^{-1}) = f(b) f(b)^{-1} = 1_{G_2}$

- $f(a^{-1}) = f(a)^{-1}$ dim: pongo $a = 1_{G_1}$ $f(1_{G_1} b^{-1}) = f(1_{G_1}) f(b)^{-1} \underset{\text{per ①}}{=} 1_{G_2} f(b)^{-1} = f(b)^{-1}$

- $f(ab) = f(a) f(b)$ dim: pongo $b = b^{-1}$ $f(a(b^{-1})^{-1}) = f(a) f(b^{-1})^{-1} \underset{\text{per ②}}{=} f(a) f((b)^{-1})^{-1} = f(a) f(b)$

def ISOMORFISMO

Sia $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi

Se f è biiettiva, allora si dice che f è un isomorfismo

- il simbolo $\cong$ significa "è isomorfo a"

  ($G_1 \cong G_1$ esiste un isomorfismo tra G_1 e G_2)

esercizio

$f: G_1 \longrightarrow G_2$ isomorfismo. sappiamo che f biiettiva $\Longleftrightarrow \exists f^{-1}: G_2 \longrightarrow G_1$ biiettiva t.c. $f \circ f^{-1} = Id_{G_2}$ $f^{-1} \circ f = Id_{G_1}$

DIMOSTRARE CHE f^{-1} è un isomorfismo

Inoltre, $G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3$ con f, g omom. di gr

allora anche $g \circ f: G_1 \longrightarrow G_3$ omom. di gr.

e in più f, g sono isomorfismi e anche $g \circ f$, di inverso $f^{-1} \circ g^{-1}$

ESEMPI

$\mathbb{Z} \xrightarrow{f} m\mathbb{Z} < \mathbb{Z}$ notazione additiva

$m\mathbb{Z} < \mathbb{Z}$: $\forall a,b \in m\mathbb{Z}$, $a-b \in m\mathbb{Z}$

$\exists\ \alpha, \beta$ t.c. $a = \alpha m$, $b = \beta m$

quindi $a-b = (\alpha-\beta)m \in m\mathbb{Z}$

Con $f(n) := mn$ applicazione

è un isomorfismo di gruppi

Infatti ① $f(n-n') = m(n-n') = mn - mn' = f(n) - f(n')$ è omomorfismo di gruppi

② iniettiva $f(p) = f(q) \iff pm = qm \iff m(p-q) = 0 \iff p = q$

③ suriettiva $y \in m\mathbb{Z}$. $\exists\ k \in \mathbb{Z}$ t.c. $y = mk$. Ponendo $x = k$ si ha $f(x) = mk = y$

(esempio che mischia le notazioni $+, \cdot$)

$G_1 = \mathbb{R}$ con $+$, $G_2 = \mathbb{R}_{>0}$ con $\cdot$ notare che $\mathbb{R}_{>0} < \mathbb{R}^\times$: $a,b \in \mathbb{R}_{>0}$ $a>0, b>0, b^{-1}>0$ $ab^{-1}>0$ quindi $ab^{-1} \in \mathbb{R}^\times$

poniamo:

$f: \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ $f(x) := e^x$

$f: \mathbb{R}_{>0} \longrightarrow \mathbb{R}$ $g(x) := \underset{\ln}{\log}(x)$ $e^{\log(\cdot)} = \mathrm{Id}_{\mathbb{R}}$ $\log(e^{(\cdot)}) = \mathrm{Id}_{\mathbb{R}}$

Sono due isomorfismi di gruppi, uno l'inverso dell'altro $f^{-1} = g$ $g^{-1} = f$

$f(0) = e^0 = 1 = 1_{G_2} \in G_2$	$g(1) = 0$
$f(-x) = e^{-x} = (e^x)^{-1}$ inverso	$g(y^{-1}) = \log(y^{-1}) = -g(y)$
$f(x-x') = e^{x-x'} = e^x e^{-x}$ $= f(x) f(x')^{-1}$	$g(y' y^{-1}) = g(y') - g(y)$ $\log\left(\frac{y'}{y}\right)$

appunti del 6/11 spostati in su per comodità logica

es. 2 foglio sett. 4

(iii) $P = X^3 + X^2 - 6x + 1$ $\quad Q = X^4 - 2x^3 - 2x - 1$ $\qquad$ MCD e Bézout

con $K = \mathbb{Z}/_{7\mathbb{Z}}$ campo ($\mathbb{F}_7$)

$\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ dove questi simboli rappresentano le classi corrispondenti in $\mathbb{Z}/_{7\mathbb{Z}}$

posso anche usare altri interi per rappresentare elementi di $\mathbb{F}_7$, estraendoli dalle classi (es. $8 = 1$)

• abbiamo visto che $\mathbb{F}_7^\times$ è un gruppo (abeliano) in notazione •

tavola di moltiplicazione in $\mathbb{F}_7^\times$ (la usiamo per trovare facilmente gli inversi)

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

ogni volta che c'è un 1, i due numeri sono inversi

• ogni riga contiene uno e un solo 1 $\longrightarrow$ ogni el del gruppo è invertibile di inverso unic. det.

quindi $P = X^3 + X^2 \underbrace{-6}_{-6=1} x + 1$ $\quad Q = X^4 - 2x^3 - 2x - 1$

ALGO EUCLIDE

$$
\begin{array}{l|l}
X^4 - 2x^3 \qquad - 2x - 1 & X^3 + X^2 + X + 1 \\
\hline
X^4 + X^3 + X^2 + X & X + 4 \\
\hline
4x^3 - X^2 + 4x - 1 \quad (-3 = 4) & \\
4x^3 + 4x^2 + 4x + 4 & \\
\hline
2x^2 \qquad + 2 &
\end{array}
$$

$\underbrace{X^4 - 2x^3 - 2x - 1}_{Q} = \underbrace{(X+4)}_{\text{quoziente}} \underbrace{(X^3 + X^2 + X + 1)}_{P} + \underbrace{2(X^2+1)}_{\text{resto}}$

$\deg(2(x^2+1)) = 2 < \deg(P) = 3$

mentre $\deg(2(x^2+1)) > \deg(\text{quoziente})$ (non sono intersc.)

continuiamo: divisione di P per il resto

$$
\begin{array}{l|l}
X^3 + X^2 + X + 1 & 2x^2 + 2 \\
\hline
X^3 \qquad + X & 4x + 4 \\
\hline
X^2 \qquad + 1 & \\
X^2 \qquad + 1 & \\
\hline
0 &
\end{array}
$$

devo dividere $X^2 + 1$ per $2x^2 + 2$
ho quindi x^2 e $2x^2 \rightarrow$ basta molt. per $2^{-1} = 4$ (calcolato nella tavola)

l'ultimo resto non nullo è quindi $2x^2 + 2$
ma l'MCD deve essere monico $\rightarrow$ moltiplico per un invertibile: 4
4 inverso di 2, quindi $X^2 + 1$ è MCD

• IDENTITÀ DI BÉZOUT

abbiamo $\underbrace{X^4 - 2x^3 - 2x - 1}_{Q} = \underbrace{(X+4)}_{\text{quoziente}} \underbrace{(X^3 + X^2 + X + 1)}_{P} + \underbrace{2(X^2+1)}_{\text{resto}}$

trovare α, β in $\mathbb{F}_7$ t.c. $\alpha P + \beta Q = \delta = X^2 + 1$

$2(X^2+1) = Q - (X+4)P$ $\quad$ l'identità che abbiamo è buona, ma serve eliminare il 2 prima dell'MCD (2 è inv, moltiplichiamo per l'inverso)

$4 \cdot 2(X^2+1) = 4Q - 4(X+4)P$

$X^2 + 1 = 4Q + (3x+5)P$

COSTRUZIONI CANONICHE DI UN SOTTOGRUPPO

nota: un gruppo qualsiasi ha due sottogruppi evidenti:

- $\{1_G\}$
- sé stesso

0_G not. additiva

Lemma costruzione del kernel / nucleo

Sia $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi

$$H = \{g \in G_1 : f(g) = 1_{G_2}\} = f^{-1}(\{1_{G_2}\}) \subset G_1$$

elementi di G_1 che puntano all'el neutro di G_2

è un sottogruppo: $H < G_1$ si chiama NUCLEO di f e si scrive $H = Ker(f)$

dim: $a, b \in H$ con $f(a) = f(b) = 1_{G_2}$

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1_{G_2}\underbrace{1_{G_2}^{-1}}_{1_{G_2}} = 1_{G_2}$$ quindi $ab^{-1} \in H$ (in H ci sono gli el. che puntano a 1_{G_2})

Lemma

Sia $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi

"kernel banale" è banale perché, per def. omomorfismo di gruppi, $f(1_{G_1}) = 1_{G_2}$

si ha che $Ker(f) = \{1_{G_1}\} \Longleftrightarrow f$ è iniettiva

è il più piccolo sottogruppo di G_1

dim

$\Longrightarrow$ Supponiamo $Ker(f) = 1_G$ ($= \{x \in G_1 : f(x) = 1_{G_2}\}$)

Siano $x, x' \in G_1$ t.c. $f(x) = f(x') \underset{\text{divido}}{\Longleftrightarrow} f(x)f(x')^{-1} = 1_{G_2}$

$= f(x x'^{-1})$ (x omomorfismo)

$\Longleftrightarrow x(x')^{-1} \in Ker(f) = \{1_{G_1}\}$ quindi $\Longleftrightarrow x(x')^{-1} = 1_{G_1}$

molt. per x' $\quad x\underbrace{(x')^{-1}x'}_{1} = 1_{G_1}x' \Longleftrightarrow x' = x \quad f$ iniettiva

$\Longleftarrow$ Supponiamo f iniettiva

Sia $x \in Ker(f)$. Allora $f(x) = 1_{G_2}$

Ma f è un omomorfismo di gruppi, da cui deduco $f(1_{G_1}) = 1_{G_2}$

Siccome $f(x) = f(1_{G_1}) = 1_{G_2}$ e f iniettiva, si deve avere $x = 1_{G_1} \Longrightarrow Ker(f) = \{1_{G_1}\}$

· costruzione del SOTTOGRUPPO IMMAGINE

$f: G_1 \longrightarrow G_2$ e f omomorfismo, $f(G_1) \subset G_2$

$$f(G_1) < G_2 = \{ y \in G_2 : \exists x \in G_1 \text{ con } f(x) = y \}$$ è il sottogruppo immagine.

dim (sottogruppo)

devo dimostrare che se $y, y' \in f(G_1)$, allora $y(y')^{-1} \in f(G_1)$

$\exists\, x, x' \in G_1$ t.c. $f(x) = y$, $f(x') = y'$

$$y(y')^{-1} = f(x) f(x')^{-1} \underset{\text{omomorfismo}}{=} f(x x'^{-1}) = f(z)$$

$$\exists\, z \in G_1 \text{ t.c. } f(z) = y(y')^{-1} \Longleftrightarrow y(y')^{-1} \in f(G_1)$$

· costruzione dei SOTTOGRUPPI CONIUGATI

G gruppo. Scegliamo $H < G$ e $g \in G$

definisco $H^g := \{ g' \in G \text{ t.c. } \exists\, h \in H \text{ t.c. } g' = g^{-1} h g \} = g^{-1} H g$ — notazione semplificata

OSSERVAZIONE. se G abeliano $H^g = H \ \forall g$ $\left(g' = g^{-1} h g \Longleftrightarrow g' = \underbrace{g^{-1} g}_{1} h \Longleftrightarrow g' = h \right)$

Lemma: $H^g < G$

$\boxed{\text{In generale, } gH,\ Hg,\ Hg^{-1},\ g^{-1}H \not< G}$

dim dati $a, b \in H^g$

$a = g^{-1} a' g \quad \exists\, a' \in H$, $b = g^{-1} b' g \quad \exists\, b' \in H$

$\cdot\ b^{-1} = (g^{-1} b' g)^{-1} = g^{-1} b'^{-1} g$ — inversione in G: $(abc)^{-1} = c^{-1} b^{-1} a^{-1}$

$$a b^{-1} = g^{-1} a' \cancel{g} \cdot \cancel{g^{-1}} (b')^{-1} g = g^{-1} \underbrace{a' (b')^{-1}}_{\in H \text{ perché } H < G} g \implies ab^{-1} \in H^g \ \forall a, b \in H^g \implies H^g < G$$

dim alternativa

Definiamo, dato $g \in G$, un'applicazione $G \xrightarrow{f_g} G$, $x \longmapsto f_g(x) = g^{-1} x g$

osserviamo che $\forall g$, f_g è un omom di gruppi (si parla di endomorfismo $(G \to G)$)

per verificarlo devo mostrare che $\forall a, b \in G$, $f(ab^{-1}) = f_g(a) f_g(b^{-1})$

$$f_g(a) f_g(b^{-1}) = g^{-1} a g (g^{-1} b g)^{-1} = g^{-1} a \cancel{g} \cdot \cancel{g^{-1}} b^{-1} (g^{-1})^{-1} = g^{-1} a b^{-1} g = f_g(ab^{-1})$$

Questo dimostra perché: $H < G_1$ e se $G_1 \xrightarrow{f} G_2$ omomorfismo allora $f(G_1) < G_2$

Se $G_1 = G_2 = G$ e $f = f_g$ ottengo $\forall\, H < G$, $f_g(H) < G$, $f_g(H) = g^{-1} H g = H^g$ $\implies H^g < G$ ∎

PERMUTAZIONI

GRUPPI DI PERMUTAZIONI

elementi chiamati permutazioni

dato $\mathcal{E}$ insieme finito, sia $S(\mathcal{E}) = \{ f : \mathcal{E} \to \mathcal{E} \ : \ f \text{ biiettiva} \}$

- Su $S(\mathcal{E})$ esiste l'operazione di composizione di applicazioni: $\mathcal{E} \xrightarrow{f} \mathcal{E} \xrightarrow{g} \mathcal{E}$, $g \circ f$, e se $f, g \in S(\mathcal{E})$ (biiett.), allora $g \circ f \in S(\mathcal{E})$

Inoltre, $(g \circ f)^{-1} = f^{-1} \circ g^{-1} \implies (S(\mathcal{E}), \circ, Id_{\mathcal{E}})$ è un gruppo.

perché ① $f \circ (g \circ h) = (f \circ g) \circ h$ — $\circ$ è associativo

② $f \circ Id = Id \circ f = f \quad \forall f \in S(\mathcal{E})$ — el neutro $\circ$

③ $\forall f \in S(\mathcal{E})$ invertibile e $f \circ f^{-1} = f^{-1} \circ f \in S(\mathcal{E})$ — inverso per $\circ$

- Sia $\mathcal{E} = \{1, \dots, n\} =: I_n \quad n \geq 1$ allora si scrive $S_n = S(I_n) = S(\mathcal{E})$

  - ogni elemento di S_n, $f \in S_n$ può essere identificato con un diagramma:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow \\ f(1) & f(2) & f(3) & f(4) & \cdots & f(n) \end{pmatrix}$$
    che si può anche rappresentare non "in ordine" con frecce:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ f(2) & f(3) & f(4) & f(1) & & f(n) \end{pmatrix}$$

def n-ciclo

Una permutazione del tipo $\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{s-1} & a_s \\ a_2 & a_3 & a_4 & \dots & a_s & a_1 \end{pmatrix}$ con $a_1, a_2 \dots a_s \in I_n \ (s \leq n)$ distinti, che fissa (manda a sé stessi) tutti gli elementi che non appartengono a $\{a_1 \dots a_s\}$ (e manda quelli di $\{a_1 \dots a_s\}$ in maniera ciclica es: $a_1 \to a_2$, $a_2 \to a_3$, $a_3 \to a_1$)

il ciclo si vede meglio così imo
$$\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{s-1} & a_s \\ a_1 & a_2 & a_3 & a_4 & \dots & a_s \end{pmatrix}$$

$\notin \{a_1 \dots a_s\}$ e sono fissati
$$\begin{pmatrix} a_1 & a_2 & \dots & a_{s-1} & a_s & a_{s+1} & a_{s+2} \\ a_1 & a_2 & a_3 & \dots & a_s & a_{s+1} & a_{s+2} \end{pmatrix}$$
$\in \{a_1 \dots a_s\}$ e sono "ciclici"

si chiama s-ciclo e si scrive $(a_1 \ a_2 \dots a_s)$

term: dato un ciclo $(a_1 \ a_2 \dots a_s)$, la sua orbita è $\{a_1, a_2, \dots, a_s\}$ (insieme di el. permutati tra loro)

N.B rispetto alla notazione: è $(a_1 \ a_2 \ a_3 \dots a_s)$ e rispetta l'"ordine" del ciclo

si può shiftare: $(a_s \ a_1 \ a_2 \dots a_{s-1})$ ma non rimescolare: $\neq (a_1 \ a_3 \ a_2 \dots a_s)$

esempi: in S_2: $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1 \ 2)$ è un 2-ciclo   in S_3: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3)$ 3-ciclo   in S_5: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = (1 \ 3 \ 5)$ 3-ciclo

TERMINOLOGIA: tutti i 2-cicli si chiamano trasposizioni

OSS: l'identità è uno $\emptyset$-ciclo

- tutti i cicli sono permutazioni, ma esistono permutazioni che non sono cicli

es. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix}$ non è un ciclo seguendo le $\to$,

vedo $1 \to 2$, $2 \to 5$, $5 \to 1$ sono "cicliche", ma le altre non sono fissate: $3 \to 6$, $6 \to 3$ ...

(anche guardando $3 \to 6$, $6 \to 3$ stesso discorso: $1 \to 2$, $2 \to 5$, $5 \to 1$ non fissate)

INVERSIONE

qualsiasi di questi va bene

$$\begin{pmatrix}1&2&3&4&5&6&7\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 4&6&7&5&1&3&2\end{pmatrix}^{-1} = \begin{pmatrix}1&2&3&4&5&6&7\\ \uparrow&\uparrow&\uparrow&\uparrow&\uparrow&\uparrow&\uparrow\\ 4&6&7&5&1&3&2\end{pmatrix} = \begin{pmatrix}4&6&7&5&1&3&2\\ 1&2&3&4&5&6&7\end{pmatrix} = \begin{pmatrix}1&2&3&4&5&6&7\\ 5&7&6&1&4&2&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6&7\\ 1&2&3&4&5&6&7\end{pmatrix}^{-1} = \begin{pmatrix}1&2&3&4&5&6&7\\ 1&2&3&4&5&6&7\end{pmatrix}$$

oss: nella notazione semplificata di un ciclo $(a_1\, a_2 \dots a_s)$, l'inverso si ottiene leggendo da destra a sinistra:

$$(a_1\, a_2 \dots a_s)^{-1} = (a_s \dots a_3\, a_2\, a_1)$$

COMPOSIZIONE (possiamo chiamarla anche "prodotto")

$$\sigma = \begin{pmatrix}1&2&3&4&5\\ 3&1&4&2&5\end{pmatrix} = (1\,3\,4\,2) \in S_5 \,, \quad \tau = \begin{pmatrix}1&2&3&4&5\\ 5&4&2&1&3\end{pmatrix} = (1\,5\,3\,2\,4) \in S_5$$

$\sigma \circ \tau = \sigma \cdot \tau = \sigma\tau$ composizione → agisce prima τ

$$\sigma\circ\tau = \begin{array}{c} \\ \tau \\ \\ \sigma \\ \\ \end{array}\begin{pmatrix}1&2&3&4&5\\ |&|&|&|&|\\ 5&4&2&1&3\\ |&|&|&|&|\\ 5&2&1&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\ 5&2&1&3&4\end{pmatrix} = (5\,4\,3)$$

$\neq \implies S_5$ non è commutativo!

$$\tau\circ\sigma = \begin{pmatrix}1&2&3&4&5\\ 3&1&4&2&5\\ 2&5&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\ 2&5&1&4&3\end{pmatrix} = (1\,2\,5\,3)$$

> oss: il prodotto di cicli non è necessariamente un ciclo

Descrizione di S_3

$\# S_3 = 6 = 3\cdot 2\cdot 1$ (fattoriale)

$$\left\{ \begin{pmatrix}\boxed{1}&2&3\\ \boxed{1}&2&3\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{1}&3&2\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{2}&1&3\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{2}&3&1\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{3}&1&2\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{3}&2&1\end{pmatrix} \right\} =$$

$$= \{ Id,\ (2\,3),\ (1\,2),\ (1\,2\,3),\ (1\,3\,2),\ (1\,3) \}$$

in S_3, ogni permutazione è un s-ciclo con $s = 0, 2, 3$

- Qual è il più piccolo n t.c. in S_n esiste una permutazione che non è un ciclo?

$n = 4$. infatti, $(12)(34) =$ elemento per elemento

notazione funzioni: come $(f\circ g)(x)$

$((12)(34))(1) = (12)\,((34)(1)) = (12)(1) = 2$
$((12)(34))(2) = (12)(2) = 1$
$((12)(34))(3) = (12)(4) = 4$
$((12)(34))(4) = (12)(3) = 3$

quindi $(12)(34) = \begin{pmatrix}1&2&3&4\\ 2&1&4&3\end{pmatrix}$ non è un ciclo

es mostrare che $(123)^{-1} = (132)$ $(=(321)\dots)$ ⟶ $(123) = \begin{pmatrix}1&2&3\\ 2&3&1\end{pmatrix}$ $\quad (123)^{-1} = \begin{pmatrix}1&2&3\\ \uparrow&\uparrow&\uparrow\\ 2&3&1\end{pmatrix} = (1\,3\,2)$

def CICLI A SUPPORTI DISGIUNTI

Dati due cicli $(a_1 \dots a_s)$ e $(b_1 \dots b_s)$ di S_n,
si dice che sono a supporti disgiunti se $\{a_1, \dots, a_s\} \cap \{b_1, \dots, b_s\} = \emptyset$

Più generalmente, dati r cicli, $c_1, \dots, c_r$ di S_n sono a supporti disgiunti

es. $(1\,2)$, $(3\,4)$ sono a supp. disg. in S_4

TEOREMA (decomposizione di permutazioni)

Ogni $\sigma \in S_n$ può essere decomposto in prodotto di cicli a supporti disgiunti.

Inoltre, tali cicli sono unicamente determinati e commutano tra di loro.

C'è analogia con il TFA.

esempio

x "estrarre" cicli:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 7 & 3 & 8 & 1 & 5 \end{pmatrix}$$

parto da un el

$1 \to 2 \to 4 \to 7 \to 1$

(1247)

non ha senso prendere un el da qui → si parte da un altro

prendo il 3

$3 \to 6 \to 8 \to 5 \to 3$

(3685)

i due cicli sono disgiunti

$\sigma = (1247)(3685) =$

$= (3685)(1247)$

$$A = \{1, 2, 3\}$$

$R_1 = \{(1,1), (2,2), (1,2)\}$

$R_2 = \{(3,3), (1,2)\}$

$R_1 \cup R_2 = \{(1,1), (2,2), (3,3), (1,2)\}$

$R_1 \cap R_2 = \{(1,2)\}$

$R_1 = \{(1,1), (2,2)\}$

$R_2 = \{(3,3)\}$

$R_1 \cup R_2 = \{(1,1), (2,2), (3,3)\}$

$R_1 \cap R_2 = \emptyset$

 [verso il teorema di struttura delle applicazioni, ma con i gruppi]

Sia G gruppo (in not. moltiplicativa) e $H < G$.
Introduciamo una relazione $\sim$ su G:

dati $x, x' \in G$ $\quad x \sim x' \iff x(x')^{-1} \in H$

Lemma: $\sim$ è di equivalenza

dim: ① RIFLESSIVITÀ: $\quad x \sim x \quad \forall x \in G$

$H < G \implies \underset{(1_H = 1_G)}{1_G \in H}$. Ma $1_G = xx^{-1} \; \forall x \in G$, quindi $x \sim x \quad \forall x \in G$

② SIMMETRIA: $\quad x \sim x' \implies x' \sim x \quad \forall x \in G$

$x \sim x' \iff x(x')^{-1} \in H$
Ma $\forall h \in H$, $h^{-1} \in H$ (propr. sottogr.). Quindi $(x(x')^{-1})^{-1} = x'x^{-1} \in H$

③ TRANSITIVITÀ: $\quad x \sim x', \; x' \sim x'' \implies x \sim x'' \quad \forall x, x', x'' \in G$

Supponiamo $x \sim x'$ e $x' \sim x''$. Allora $x(x')^{-1}$, $x'(x'')^{-1} \in H$

Se $a, b \in$ sottogruppo: anche il loro prodotto $\in$ sottogruppo: $\quad x \underbrace{(x')^{-1} x'}_{1_G} (x'')^{-1} = x(x'')^{-1} \in H$

quoziente su $\sim$ dove: due el. x e x' sono nella stessa classe se $x(x')^{-1} \in H$

Domanda: È possibile costruire su $G/_\sim$ un'operazione binaria in modo tale che $G/_\sim$ acquisisca una struttura di gruppo?
Talvolta sì, talvolta no. Servono delle condizioni:

- Vorremmo che questa identità fosse valida per la nuova operazione:

$$[x] \overset{\text{nuova op.}}{*} [x'] = [\underset{\text{vecchia op. di } G}{x \cdot x'}] \qquad \text{indipendentemente dai rappresentanti}$$

Supponiamo $x \sim y$ e $x' \sim y'$.
$x \sim y \iff [x] = [y] \iff x(y)^{-1} \in H$
$x' \sim y' \iff [x'] = [y'] \iff x'(y')^{-1} \in H$

è necessario innanzitutto che $[xx'] = [yy']$ ovvero $xx'(yy')^{-1} \in H$

$$xx'(yy')^{-1} = x\underbrace{x'(y')^{-1}}_{\text{per ipotesi, } \in H} y^{-1}$$

sappiamo quindi che un pezzo del prodotto $\in H$,
ci serve una condizione per cui tutto il prodotto $\in H$

def SOTTOGRUPPO NORMALE

H è un sottogruppo normale di G se, $\forall x \in G$, $xH = Hx$

- Si scrive $H \triangleleft G$

quindi, per la formula di prima: $xHy^{-1} = \underbrace{xy^{-1}}H$ $\in H$ per ipotesi, quindi tutto $\in H$
(quindi $[xx'] = [yy']$)

Condizioni equivalenti (per H sottogr. normale)

ricordiamo: $g^{-1}Hg$

① $\underset{(gH = Hg)}{H \triangleleft G}$ ② $\forall g \in G$ e $\forall h \in H$, $\exists h' \in H$ t.c. $gh = h'g$ ③ $\forall g \in G$, $H^g = H$

OSS: G abeliano e $H < G \implies H \triangleleft G$ (tutti i sottogruppi di un gruppo abeliano sono normali)

ESEMPI (notevoli):

- $\mathbb{Z}$ gruppo abeliano in not. add. e $\forall n \in \mathbb{N}^*$, $n\mathbb{Z}$ è un sottogr. di $\mathbb{Z}$. $n\mathbb{Z} \triangleleft \mathbb{Z}$ e posso costruire, sempre in not. add., $\mathbb{Z}/_{n\mathbb{Z}}$ (coincide con la costruzione già vista in aritmetica modulare)
- dato G qualsiasi, ho $G \triangleleft G$ $\quad (\forall x \in G, \; xG = Gx$ e $G/_G = \{G\})$
- anche $\{1_G\} \triangleleft G$ $\quad (\forall x \in G, \; x1_G = 1_G x = x$ e $G/_{1_G} = \{\{g\} : g \in G\}$ rel. di uguaglianza$)$

dim condiz. equivalenti: basta mostrare che $(3) \Longrightarrow (1) \Longrightarrow (2) \Longrightarrow (3)$ (ordine scelto per facilità di dimostrazione)

- $(3) \Longrightarrow (1)$ ipotesi: $H^g = H$
  devo dim: $gH = Hg$

  se $H^g = H$, $g^{-1}Hg = H \overset{\text{molt. per } g \text{ a sx}}{\Longleftrightarrow} \underbrace{gg^{-1}}_{1_G}Hg = gH \Longleftrightarrow Hg = gH$

- $(1) \Longrightarrow (2)$ ipotesi: $gH = Hg$
  devo dim: $gh = h'g$

  se $\forall g$, $gH = \{x \in G : \exists h \in H \text{ con } x = gh\} = Hg = \{y \in G : \exists h' \in H \text{ con } y = h'g\}$
  allora $\exists h, h' \in H$ t.c. $x = gh = h'g$

- $(2) \Longrightarrow (3)$ ipotesi: $gh = h'g$
  devo dim: $H^g = H$

  se $\forall g \in G$, $\forall h \in H$ si ha $gh = h'g$ $\exists h' \in H$, allora $\overset{\text{molt. per } g^{-1} \text{ a sx}}{\Longrightarrow} \underbrace{g^{-1}g}_{1_G}h = g^{-1}h'g \Longleftrightarrow h = g^{-1}h'g$ quindi, $\forall g$, $H^g = H$ ∎

  $\forall h$ — se ogni el. h si può scrivere così (come def. coniugato), vuol dire che l'insieme dei coniugati è H stesso

Teorema

Dati $H \triangleleft G$, $\sim$ di eq.

Allora l'operazione su $G/\sim$ $[x][x'] = [xx']$ (ben posta) definisce una struttura di gruppo su $G/\sim$.

(mia spiegazione, non Pellarin)
$[g]$ contiene tutti gli el. x t.c. $gx^{-1} \in H$.
quindi, $gx^{-1} = h \Longleftrightarrow g = hx \Longleftrightarrow h^{-1}g = x$
Ma H è chiuso rispetto all'inverso, quindi $h^{-1} \in H$.
Quindi tutti gli el. $x \in [g]$ si possono scrivere come gh, $h \in H$ (quindi gH)

- si scrive $G/\sim = G/H$ gruppo quoziente di G per H
- osserviamo inoltre $[g] = gH = Hg$ — non è vero che $gh = hg$ ma $\forall h$ $\exists h'$ t.c. $gh = h'g$ quindi $gH = Hg$
- l'elemento neutro è $1_{G/H} = H$
- gli elementi di G/H (sottoinsiemi di G) sono le classi laterali di H
  quindi: $\{gh : h \in H\}$

Lemma:

L'applicazione $G \xrightarrow{\pi_H} G/H$, $g \longmapsto [g]$ è un omomorfismo di gruppi suriettivo

dim:

- la suriettività di π_H è chiara, perché ogni classe contiene un rappresentante
- inoltre, $\pi_H(xy) = [xy] = [x][y] = \pi(x)\pi(y)$ ∎

Lemma

Dato $G_1 \xrightarrow{f} G_2$ omomorfismo di gruppi

Allora, $\underbrace{Ker(f)}_{=\text{"}H\text{"}} \triangleleft G_1$. Inoltre, se $H \triangleleft G$, allora $H = Ker(\pi_H)$

el. di G_1 che puntano a 1_{G_2}

$[H]$ el. neutro di $G/\sim$, quindi $H = Ker(\pi_H)$

dim:

- $Ker(f) \triangleleft G_1$ (so già che $< G_1$) mostriamo che $Ker(f)^g = Ker(f)$ (def. equivalente ③ di $\triangleleft$)

  prendiamo $h \in G_1$ t.c. $f(h) = 1_{G_2}$ ($\Longleftrightarrow h \in Ker(f)$)

  allora si ha che $\forall x \in G_1$, $f(x^{-1}hx) \overset{\text{omom.}}{=} f(x^{-1})\overbrace{f(h)}^{=1_{G_2}}f(x) \overset{\text{omom.}}{=} f(x)^{-1}f(x) = 1_{G_2}$

  $$\Longleftrightarrow x^{-1}hx \in Ker(f) \ \forall h \in Ker(f), \forall x \in G \Longleftrightarrow Ker(f)^x = Ker(f)$$

- se $H \triangleleft G_1$, allora $H = Ker(\pi_H)$

  Abbiamo $H \triangleleft G_1$ e poniamo $f = \pi_H$. Mostriamo che $H = Ker(\pi_H)$. Ma se $g \in G_1$ soddisfa $\pi_H(g) = 1_{G/H} = H \Longleftrightarrow gH = H \Longleftrightarrow g \in H$ ∎

(spiegazione mia):
- $g \in H \Longrightarrow g \in Ker(\pi_H)$ — se $g \in H$, $gH = H$. Quindi, $\pi_H(g) = H$ ($[g] = gH$). Quindi (visto $H = 1_{G/H}$) $g \in Ker(\pi_H)$
- $g \in Ker(\pi_H) \Longrightarrow g \in H$ — se $g \in Ker(\pi_H)$, $\pi_H(g) = 1_{G/H} = H$. Quindi, $gH = H$. $gH = H \Longleftrightarrow g \in H$

Consideriamo un omomorfismo di gruppi: $G_1 \longrightarrow G_2$. Per il teorema di struttura delle applicazioni,
(di kernel $H \triangleleft G_1$)

$$\begin{tikzcd}
G_1 \arrow[rr, "f"] \arrow[d, "\pi"'] & & G_2 \\
G_1/\mathrm{Ker}(f) \arrow[rr, hook, two heads, "\varphi"'] & & f(G_1) \arrow[u, hook, "i"']
\end{tikzcd}$$

$g \mapsto [g]$ (π)

i (inclusione)

abbiamo $f = i \circ \varphi \circ \pi$

$G_1/\sim \;=\; G_1/\mathrm{Ker}(f) \;=\; G_1/R$, $\mathrm{Ker}(f) = H$

$[g] \longrightarrow f(g)$ biiettiva: se $[g] = [g']$ allora $f(g) = f(g')$

ha anche senso: stiamo quozientando sul Kernel di f, le classi avranno la stessa $f(\cdot)$

- Introduciamo la relazione R: dati $g, g' \in G$, $g R g' \iff f(g) = f(g')$

mostriamo che R e $\sim$ sono la stessa relazione. dati $a, b \in G_1$, $f(a) = f(b) \iff f(a)f(b)^{-1} = 1_{G_2}$

poiché f è un omomorfismo, $f(a)f(b)^{-1} = f(ab^{-1}) = 1_{G_2}$

il che equivale a dire $ab^{-1} \in \mathrm{Ker}(f) = H$, ovvero $a \sim b$.

- Si ha quindi $G_1/R = G_1/H$ (che abbiamo visto essere un gruppo), e π omomorfismo di gruppi. (lemma p.61)

- mostriamo che anche $\varphi: G_1/R \longrightarrow f(G_1)$ t.c. $\varphi(gH) = f(g)$ è un omomorfismo di gruppi

Voglio mostrare che $\forall a, b \in G_1$, si ha $\varphi(\underset{[a]}{aH})\,\varphi((bH)^{-1}) = \varphi(ab^{-1}H)$

si ha $\varphi(aH)\,\varphi(bH)^{-1} = f(a)f(b)^{-1} \underset{\text{omom.}}{=} f(ab^{-1}) = \varphi(ab^{-1}H)$

abbiamo così dimostrato il primo TEOREMA DI ISOMORFISMO PER I GRUPPI:

dato $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi, esso si decompone in composizione $f = \underbrace{i \circ \varphi \circ \pi}_{\text{tutti omomorfismi di gruppi}}$

Altre proprietà dei gruppi:

Lemma l'intersezione di sottogruppi è un sottogruppo: dati $H_1, \dots, H_n < G$, $\bigcap_{i=0}^{n} H_i < G$

dim: Siano $x, y \in \bigcap_{i=0}^{n} H_i$ (ovvero $x, y \in H_i \ \forall i$)

Allora, $\forall i$, $x y^{-1} \in H_i$, perché $H_i < G \ \forall i$

Ma allora $x y^{-1} \in \bigcap_{i=0}^{n} H_i$, ovvero $\bigcap_{i=0}^{n} H_i < G$

Lemma l'unione di sottogruppi non è un sottogruppo ($\longrightarrow$ lo è se uno dei due sottogruppi è contenuto nell'altro)

esempio $H_1 = \{1_G, (12)\}$, $H_2 = \{1_G, (13)\} < G = S_3$

$H_1 \cup H_2 = \{1_G, (12), (13)\} \subset G$, ma non $< G$.

Infatti $(12), (13) \in G$ e $\in H$ ma $(12)(13) = (1,3,2) \notin H_1 \cup H_2$ (non è chiuso rispetto alla sua operazione, $\circ$) quindi non è un sottogruppo

SOTTOGRUPPO GENERATO

Consideriamo $I \subset G$ ($I \neq \emptyset$). Il sottogruppo di G generato da I è:

$$\langle I \rangle := \bigcap_{\substack{H < G: \\ I \subset H}} H$$

(quindi si prendono tutti i sottogruppi di G che contengono I e si intersecano) è "il più piccolo sottogruppo di G che contiene I"

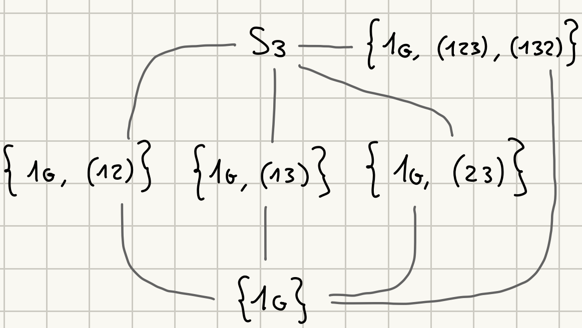
Si ha $I < G$ per il lemma per cui l'intersezione di sottogruppi è un sottogruppo.

per un singolo elemento:

- dato G gruppo (not. moltiplicativa) e $g \in G$, $\langle g \rangle = \langle \{g\} \rangle = \bigcap_{\substack{H < G \\ g \in H}} H$

esempio

i sottogruppi di S_3 sono:



Quindi $\langle (1\,2) \rangle = \{1_G, (12)\} = H_3$

$\langle (13) \rangle = \{1_G, (13)\} = H_2$

$\langle (23) \rangle = \{1_G, (23)\} = H_1$

$\langle (123) \rangle = \{1_G, (123), (132)\}$

$\langle H_1 \cup H_2 \rangle = S_3$

$= \{1_G, (13), (23), \underbrace{(132)}_{(23)(13)}, \underbrace{(123)}_{(13)(23)}, \underbrace{(12)}_{(23)(13)(23)}\} = S_3$ (i prodotti ci sono per chiusura rispetto a $\circ$)

(questo è un diagramma di Hasse - mostra i sottogruppi di un determinato gruppo)

SOTTOGRUPPO $g^{\mathbb{Z}}$ / $g\mathbb{Z}$

• Consideriamo l'insieme $\{1, g, g^2, \dots, g^{-1}, g^{-2}, \dots\} = \{g^n : n \in \mathbb{Z}\} = g^{\mathbb{Z}} \subset G$ con G gruppo moltiplicativo

Allora si ha che $g^{\mathbb{Z}} < G$. Infatti, $\forall x, x' \in g^{\mathbb{Z}}$, $\exists\, n, n' \in \mathbb{Z}$ t.c. $x = g^n$, $x' = g^{n'}$ e $x(x')^{-1} = g^{\overbrace{n-n'}^{n''}} \in g^{\mathbb{Z}}$

Si ha che $\langle g \rangle \subset g^{\mathbb{Z}}$. ($\langle g \rangle$ è un sottogruppo: è chiuso rispetto a inverso e prodotto – visto che contiene g, conterrà g^{-1} e tutte le potenze generate come prodotto)

Dato che $\langle g \rangle < G$, e $g \in \langle g \rangle$, $1 = g^0 \in \langle g \rangle$, $g^{-1} \in \langle g \rangle$ e gli altri sono generati dal prodotto di questi ... si ha anche $g^{\mathbb{Z}} \subset \langle g \rangle$

Lemma $\underline{\langle g \rangle = g^{\mathbb{Z}}}$. (per un gruppo additivo, $\langle g \rangle = g\mathbb{Z}$)

es., dato $\mathbb{Z}/_{5\mathbb{Z}}$, $\langle [2] \rangle = \{[0], [2], [4]\}$

Lemma SOTTOGRUPPI DI $\mathbb{Z}$

Sia G un sottogruppo di $\mathbb{Z}$ (in not. additiva), se $G \neq \{0\}$, allora $\exists\, n \in \mathbb{N}^*$ t.c. $G = n\mathbb{Z}$

(tutti i sottogruppi di $\mathbb{Z}$ sono o $\{0\}$ o $n\mathbb{Z}$)

FATTO: L'elemento neutro di un gruppo $\{e\}$ è sempre un suo sottogruppo (il più piccolo sottogruppo)

dim:

Supponiamo $G \neq \{0\}$. Allora esiste un più piccolo $n \in G \cap \mathbb{N}^*$ (principio del minimo) (per i negativi, G è stabile per l'inverso $x \longmapsto -x$)
tale che, preso $d \in G$ (per div. euclidea) $d = qn + r$ con $0 \le r < n$.

Quindi $r = \underbrace{d}_{\in G} - \underbrace{qn}_{\in G \text{ perché } n \in G}$. Se $r \neq 0$, si avrebbe $r < n$ e $r \in G \cap \mathbb{N}^*$ (impossibile perché n è il minimo su $G \cap \mathbb{N}^*$, ma allo stesso tempo $r < n$ e $r \neq 0$)
contraddizione con la minimalità di n.
Quindi $r = 0$, e $d \in n\mathbb{Z}$.
Quindi, $G \subset n\mathbb{Z}$. Ma $G \supset n\mathbb{Z}$, perciò $G = n\mathbb{Z}$
perché G è chiuso rispetto alla somma, quindi contiene tutti gli $n\mathbb{Z}$ (?)

Lemma

Se G è un gruppo finito (moltiplicativo)
allora $\forall g \in G$, $\exists\, n > 0$ t.c. $\langle g \rangle = g^{\mathbb{Z}} \cong \mathbb{Z}/_{n\mathbb{Z}}$. n è chiamato ordine di g.

dim

$f : \mathbb{Z} \longrightarrow G$ (non iniettiva perché $\mathbb{Z}$ infinito e G finito)
$\quad n \longrightarrow g^n \in g^{\mathbb{Z}} = \langle g \rangle$

f è un omomorfismo perché $f(n - n') = g^{n-n'} = g^n g^{-n'} = f(n) f(n')^{-1}$
per il primo teorema di isomorfismo:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "f"] \arrow[d, "\pi"'] & G \\ \mathbb{Z}/_{Ker(f)} \arrow[r, hook, "\varphi"] & f(\mathbb{Z}) \arrow[u, "i"'] \end{tikzcd} \quad f(\mathbb{Z}) = g^{\mathbb{Z}} = \langle g \rangle$$

$Ker(f) < \mathbb{Z}$ quindi, per il Lemma sopra, o è $\{0\}$ o è $n\mathbb{Z}$
Ma se fosse $\{0\}$, allora $\mathbb{Z}/_{0} \overset{1:1}{=} \mathbb{Z}$ e f sarebbe iniettiva (e $g^{\mathbb{Z}}$ infinito)
(perché φ è iso e andrebbe da $\mathbb{Z}/_{0}$ infinito a $g^{\mathbb{Z}}$)
Quindi $\exists\, n \in \mathbb{N}^*$ t.c. $Ker(f) = n\mathbb{Z}$

def ORDINE DI UN ELEMENTO

Sia G gruppo finito e $g \in G$.

Allora $\{ d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G \} \neq \emptyset$

(infatti si ha l'omomorfismo $f: \mathbb{Z} \to G$ visto sopra, non iniettivo)

in notazione additiva:

Si pone $\operatorname{ord}(g) = \min \{ d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G \}$ minimo numero di volte per cui bisogna moltiplicare g per se stesso per ottenere 1_G

$\operatorname{ord}(g) = \min \{ d \in \mathbb{N}^* \text{ t.c. } g\mathbb{Z} = 1_G \}$

es. $g = (123) \in S_3$

$\mathbb{Z} \to S_3$

$n \to (123)^n$

n	$(123)^n$
0	1_{S_3}
1	(123)
2	(132)
3	$\boxed{1_{S_3}}$
4	(123)

quindi $\operatorname{ord}((123)) = 3$

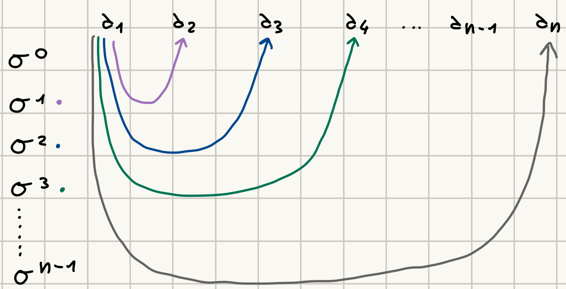
$\langle (123) \rangle \cong \mathbb{Z}/_{3\mathbb{Z}}$

$\{ (123), (132), 1_{S_3} \}$

ORDINE DI UN CICLO

Più generalmente, dato un n-ciclo di S_r $\sigma := (a_1\ a_2 \dots a_n)$

$\operatorname{ord}(\sigma) = n$ e $\langle \sigma \rangle \cong \mathbb{Z}/_{n\mathbb{Z}}$



(non l'ha detto, trovato su internet)

$\sigma = (a_1 a_2 \dots a_k)$ allora, $\forall k$ $\sigma^k(a_i) = a_{(i+k-1) \bmod n+1}$

quindi $\sigma^i \neq 1_{S_r}$ $\forall i = 1, \dots, n-1$

Inoltre $\sigma^n(a_1) = a_1$. Ma noi possiamo scrivere σ "scalando", e trasformare a_2 in a_1 : $(a_2\ a_3 \dots a_n\ a_1)$

Quindi $\sigma^n(a_2) = a_2$. Più generalmente, $\sigma^n(a_i) = a_i$ $\forall i = 1 \dots n$

Siccome σ è un ciclo, esso fissa tutti gli el. $b \in \{1, \dots, r\} \setminus \{a_1 \dots a_n\}$.

Quindi, $\sigma^n = 1_{S_r}$ da cui $n = \operatorname{ord}(\sigma)$.

Abbiamo dimostrato

Lemma ORDINE DI UN CICLO

Se σ è un n-ciclo, allora

$\operatorname{ord}(\sigma) = n$ e $\langle \sigma \rangle \cong \mathbb{Z}/_{n\mathbb{Z}}$

14/11

CALCOLARE ORD(σ)

Come si calcola $n = \text{ord}(\sigma)$? Lo sappiamo se σ è un m-ciclo: $\text{ord}(\sigma) = m$

ricordiamo: Ogni $\sigma \in S_n$ si decompone in modo unico in un prodotto di cicli disgiunti $c_1, \dots, c_s$ che commutano tra loro.

Quindi: sia $\sigma \in S_n$ - lo decomponiamo in prodotto di cicli disgiunti: $\sigma = c_1 \dots c_s$

Lemma: $\text{ord}(\sigma) = \text{mcm}\left(\text{ord}(c_1), \dots, \text{ord}(c_s)\right)$

esempio

Calcolare $\text{ord}(\sigma)$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} \in S_n \quad n \geq 7$$ — (se $\in S_n > 7$, gli altri el. sono fissati)

① Decomponiamo σ in prodotto di cicli disgiunti

$$1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 = \underset{\text{ord } 2}{(17)} \ \underset{\text{ord } 2}{(24)} \ \underset{\text{ord } 2}{(56)}$$ ((3) si può omettere)

② $\text{ord}(\sigma) = \text{mcm}(2, 2, 2) = 2$

metodo alternativo: sfrutto il fatto che $\text{ord}(\sigma) = $ min. esponente$^{>0}$ a cui elevare σ per avere l'identità

(3 omesso perché fissato)

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 4 & 5 & 6 & 7 \\ 7 & 4 & 2 & 6 & 5 & 1 \\ 1 & 2 & 4 & 5 & 6 & 7 \end{pmatrix} = 1_{S_n} \quad (n \geq 7)$$

l'inverso di una trasposizione è essa stessa — sia perché $\text{ord} = 2$ (quindi $\sigma^2 = 1$) e sia per il "trucco" di leggerla al contrario: $(17) = (71)$

del tipo $abcc^{-1}b^{-1}a^{-1} = 1$

Si può vedere anche così $\sigma^2 = (17)(24)(56)(17)(24)(56) \overset{\text{commut.}}{=} (17)(24)(56)(56)(24)(17) = 1_{S_n} \quad (n \geq 7)$

(uno alla volta "collassano" nell'identità: $(56)(56) = 1_S$ $(17)(24)(24)(17)$ ecc.)

esercizi:

- trovare α, β t.c. $(147)(132)\,\alpha\,\beta = 1_G$

  $\alpha = (132)^2 = (132)(132) = (123)$ oppure $\alpha = (132) = (231) = (123)$

  $\beta = (147)^2 = (174)$

- trovare α, β in S_8 t.c. $(1234)(137)\,\alpha\beta = 1_{S_8}$ $\quad \alpha = (137)^2, \ \beta = (1234)^3$

- $\text{ord}\left((12)(345)\right) = 6$

- $\text{ord}\left((12)(245)\right) = \,?$ non sono a supporto disgiunto

  rendiamoli a supp. disg. $= \text{ord}(1245) = 4$

- $\text{ord}\left((12)(13)(14)\right) = \text{ord}\left((1432)\right) = 4$

Teorema (decomp. di permutazione in trasposizioni)

Ogni permutazione si decompone in prodotto di trasposizioni non necessariamente a supporto disgiunto.

- in generale, una tale fattorizzazione non è unica

esempio $(a_1\, a_2)\,(a_1\, a_3)\,(a_1\, a_4) = (a_1\, a_4\, a_3\, a_2)$

$\# \{a_1, a_2, a_3, a_4\} = 4$

FORMULA per un n-ciclo

$\sigma = (a_1\, a_2 \dots a_n) = (a_n\, a_{n-1})\,(a_n\, a_{n-2}) \dots (a_n\, a_1)$ (ovvero n-1 fattori)*

in realtà $2\mathbb{Z} + n-1$, perché posso aggiungere quante identità voglio

esempio: $(12345) = (54)\,(53)\,(52)\,(51)$

Teorema "rinforzato" - SEGNATURA/SEGNO DI UNA PERMUTAZIONE

visto che $(a_1\, a_2)\,(a_1\, a_2) = 1_S$, aggiungere una coppia di trasposizioni (uguali) dà lo stesso risultato

Sia s il numero di trasposizioni in una fattorizzazione di $\sigma \in S_r$ in prodotto di trasposizioni.
Allora s mod 2 è unicamente determinato (anche se s non è unico)

non l'ha detto a lezione

Poniamo $\varepsilon_\sigma = (-1)^s \in \mathbb{Z}^\times$ è la segnatura di una permutazione. il segno

σ si dice pari se $\varepsilon = +1$, dispari se $\varepsilon = -1$

se ne deduce:

per *

$\boxed{\text{nota: se } \sigma \text{ n-ciclo, } \varepsilon(\sigma) = (-1)^{n-1}}$

PROPRIETÀ: $S_n \xrightarrow{\varepsilon} \mathbb{Z}^\times$ è un omomorfismo di gruppi

(funzione che manda una permutazione al suo segno - ovvero uno dei due invertibili di $\mathbb{Z}$: $1, -1$)

c'è quindi un diagramma:

$$\begin{array}{ccc} S & \xrightarrow{\varepsilon} & \mathbb{Z}^\times \\ \pi \downarrow & \nearrow \cong & \\ S_r/\mathrm{Ker}(\varepsilon) & & \end{array}$$

perché $\varepsilon(S_r) = \mathbb{Z}^\times$

Ker(ε) contiene tutte le permutazioni che hanno segno pari (elementi di S_r che puntano a 1) per la funzione ε

Quindi, questo quoziente divide le permutazioni in due classi: pari e dispari

COME CALCOLARE $\varepsilon(\sigma)$

metodo meno divertente

① Si calcola la fattorizzazione di σ in prod. di cicli disgiunti

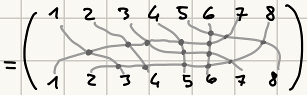
$\sigma = c_1 \dots c_m$

② $\varepsilon(\sigma) = \varepsilon(c_1) \cdot \ldots \cdot \varepsilon(c_m)$

③ Si usa la formula per cui se φ r-ciclo, allora $\varepsilon(\varphi) = (-1)^{r-1}$

metodo "adatto ad un venerdì sera" (era giovedì)

senza decomporre in prodotto di cicli disgiunti, calcoliamo la segnatura di σ con un procedimento grafico

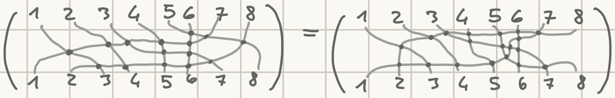
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 7 & 5 & 8 & 6 & 1 & 2 \end{pmatrix} =$ 

15 intersezioni

Si dispongono i numeri in ordine e si tracciano le frecce che li uniscono (non ci devono essere incroci a 3)
Si contano le intersezioni

$\varepsilon(\sigma) = (-1)^{15} = -1$

nota: quando conto le intersezioni, in base a come le disegno, avrò risultati diversi.
ma la classe mod 2 (parità) sarà sempre la stessa, quindi $\varepsilon(\sigma)$ non sarà inficiato.

es. 

15 = 19

$\varepsilon(\sigma) = (-1)^{15} = (-1)^{19} = -1$

- questo stesso esempio, ma con l'altra tecnica:

$\sigma = (137)\,(2458)$

$\varepsilon(\sigma) = \varepsilon(137) \cdot \varepsilon(2458) = (-1)^2 \cdot (-1)^3 = -1$

19/11

PRODOTTO CARTESIANO DI GRUPPI — o PRODOTTO DIRETTO

dati G_1, G_2 in not. additiva.

$$G_1 \times G_2 = \{ (g_1, g_2) : g_1 \in G_1,\ g_2 \in G_2 \}$$

Definiamo su $G_1 \times G_2$ una struttura di gruppo come segue:

$(g_1, g_2), (g_1', g_2') \in G_1 \times G_2$ operazione $+$: $(g_1, g_2) + (g_1', g_2') := (g_1 + g_1', g_2 + g_2')$

- associatività: $((g_1, g_2) + (g_1', g_2')) + (g_1'', g_2'') = (g_1 + g_1', g_2 + g_2') + (g_1'', g_2'') = (g_1 + g_1' + g_1'', g_2 + g_2' + g_2'') = (g_1, g_2) + ((g_1', g_2') + (g_1'', g_2''))$
- el neutro: $0_{G_1 \times G_2} = (0_{G_1}, 0_{G_2})$
  - $G_1 \times G_2$ è abeliano se G_1 e G_2 lo sono.

Questa operazione si estende a n gruppi $G_1, \dots, G_n$

Si può costruire $G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n)\}$ dotato di struttura di gruppo prodotto cartesiano di $G_1, \dots, G_n$ (e se $G_1, \dots, G_n$ abeliano allora $G_1 \times \dots \times G_n$ abeliano)

esempio $(\mathbb{R}, +)$

- posso costruire il gruppo $\mathbb{R}^n = \overbrace{\mathbb{R} \times \dots \times \mathbb{R}}^{n \text{ volte}}$ i cui elementi sono $(x_1, x_2, \dots, x_n)$ con $x_i \in \mathbb{R}$ $\forall i = 1, 2, \dots, n$

l'elemento neutro è $0 = (0, \dots, 0)$

"esercizio 19"

Teorema di Lagrange

Sia G gruppo finito.

Sia $H < G$ ($\#H < \#G$ perché $< \implies \subset$)

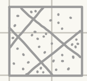
Allora:

$$\#H \mid \#G$$

dim.

Abbiamo, su G, una relazione di equivalenza associata ad H:

$$x \sim y \iff xy^{-1} \in H$$



se partiziono qualcosa di finito, ho un numero finito di porzioni finite a loro volta

Possiamo considerare l'insieme quoziente $G/\sim$ con $\#G/\sim \, < \infty$ (finito)

Poniamo $[G:H] = \#G/\sim$ $(= G/H)$

$[G:H]$: indice di H in G

Siccome $G/\sim$ è una partizione di G, $G = \bigsqcup_{c \in G/\sim} c$ $\longrightarrow$ quindi, $\#G = \sum_{c \in G/\sim} \#c$

Claim ①: $\#c = \#H$

[Se il claim è vero, abbiamo il teorema di Lagrange:
infatti, $\#G = \sum_{c \in G/\sim} \#c = \sum_{c \in G/\sim} \#H = \#H \underbrace{\sum_{c \in G/\sim} 1}_{\text{cardinalità di } G/\sim} = \#H \cdot [G:H]$ quindi $\#H \mid \#G$]

quindi $\#G = \#H \cdot$ un intero

Quindi, dobbiamo dimostrare che $\forall c \in G/\sim$, $\#c = \#H$

Claim ②

$\forall g \in G$, poniamo $\varphi_g : G \longrightarrow G$, $\varphi_g(x) = x \cdot g$ (ben definita perché G chiuso rispetto al prodotto)

allora, φ_g è una biiezione

N.B. $\varphi_g(1_G) = g$ $\forall g \neq 1_G$ quindi φ_g non è un omomorfismo (endo)

- Sappiamo che φ_g è invertibile di inverso $\varphi_{g^{-1}}$
  Infatti, se $x \in G$, $\varphi_g(\varphi_{g^{-1}}(x)) = \varphi_g(xg^{-1}) = xg^{-1}g = x$ quindi $\varphi_g \circ \varphi_{g^{-1}} = Id_G$
  Analogamente, $\varphi_{g^{-1}}(\varphi_g(x)) = \varphi_{g^{-1}}(xg) = xgg^{-1} = x$ quindi $\varphi_{g^{-1}} \circ \varphi_g = Id_G$

notiamo che, generalmente $\varphi_g \circ \varphi_{g'} = \varphi_{gg'}$ ma questo non ci serve per Lagrange (stiamo riscrivendo il gr. G in modo diverso) e $\varphi_{1_G} = Id_G$

In particolare, se $I \subset G$, allora $\#\varphi_g(I) = \#I$ (perché φ_g è una biiezione)

Quindi, se riusciamo a mostrare che una classe è l'immagine di H per un g ben scelto, abbiamo finito.
($\varphi_g(H) = c \implies \#H = \#c$, che è quello che cerchiamo)

Descriviamo una classe c:

Sia $x \in c$. Allora, $c = \{y : xy^{-1} \in H\}$ — visto che $H < G$, H è chiuso per l'inverso, quindi $h^{-1} = h'$ $\exists h' \in H$ quindi $y = h'x$

Se $y \in c$, $xy^{-1} \in H$.

Ma $xy^{-1} \in H \iff \underset{\exists h \in H}{x = hy} \iff \underset{\exists h \in H}{y = h^{-1}x} \iff y \in Hx \iff c = \varphi_x(H)$

ogni el "y" di c si può scrivere come $y = hx$ $\exists h \in H$, quindi $\varphi_x(H)$

Abbiamo quindi trovato il g per cui $\varphi_g(H) = c$. Quindi, $\#H = \#c$, e quindi $\#G = \sum_c \#c = \#H \, [G:H]$ ovvero $\#H \mid \#G$.

QUINDI IL TAKEAWAY È: TUTTI I SOTTOGRUPPI DI G DEVONO AVERE CARDINALITÀ CHE DIVIDE #G.

Quindi, per esempio

prendiamo S_{12}. $\# S_{12} = 12!$

Grazie al teorema di Lagrange, so che non esiste $H < S_{12}$ con $\# H = 13$, perché $13 \nmid 12!$

quindi, se p primo e $p \mid \# S_{12}$, allora esiste $H < S_{12}$ t.c. $\# H = p$

in particolare, $p = 2, 3, 5, 7, 11$

Basta prendere un p-ciclo: se σ è un p-ciclo, $\langle \sigma \rangle \cong \mathbb{Z}/_{p\mathbb{Z}} \implies \# \langle \sigma \rangle = p$

Più generalmente, $\forall n \leq 12$, $\exists H < G : \# H = n$ (si prende σ n-ciclo)

ma

• Sia $H < S_{12}$. È vero che $\# H \leq 12$? No! (esistono altri divisori di $12!$)

prendiamo $S \xrightarrow{\varepsilon} \mathbb{Z}^{\times}$, e $H = Ker(\varepsilon)$

$\{\pm 1\}$

per il 1o teorema iso:

$S_{12}/_H \cong \mathbb{Z}^{\times} \implies \# S_{12}/H = 2 \iff [S_{12} : H] = 2$

$12! = \# S_{12} = \# H \cdot 2 \implies \# H = \frac{12!}{2} \in \mathbb{N}^*$

(anche logicamente, metà delle perm. saranno dispari e metà pari, quindi $\# Ker(\varepsilon) = \frac{1}{2} \# S_{12}$)

• altro esempio

se $m \leq n$, c'è (almeno) un omomorfismo iniettivo $S_m \xhookrightarrow{f} S_n$

· $f(S_m) < S_n$ (perché $m \leq n$)

$\# f(S_m) = \# S_m = m!$ (perché è iniettiva)

Infatti f iniettiva $\implies S_m \cong f(S_m)$

Dal 1o teorema iso:

$$\begin{tikzcd} S_m \arrow[r, hook, "f"] \arrow[d, two heads] & S_n \\ S_m/_{\{1_{S_m}\}} \arrow[r, hook, two heads, "\cong"] & f(S_m) \arrow[u, bend right] \end{tikzcd}$$

$\cong S_m$

$Ker(f) = 1_{S_m}$ (l'unico el. di S_m che punta all'el. neutro di S_n è 1_{S_m})

"S maiuscola gotica"

Sia $\mathfrak{S}_m = \left\{ \sigma \in S_n \text{ t.c. } \begin{array}{l} \sigma(m+1) = m+1 \\ \sigma(m+2) = m+2 \\ \vdots \\ \sigma(n) = n \end{array} \right\} = \{$permutazioni in S_n che fissano gli elementi da $m+1$ a n (ce ne sono $n-m$)$\}$

con $m \leq n$, $f : S_m \hookrightarrow S_n$

$$\sigma \longmapsto \left(\begin{array}{c|c} 1 \dots m & m+1 \dots n \\ \downarrow \sigma & \downarrow \text{id.} \\ 1 \dots m & m+1 \dots n \end{array} \right)$$

Manda gli el. $1 \dots m$ seguendo σ, e fissa gli altri

è un omomorfismo di gruppi che soddisfa quanto richiesto e $f(S_m) = \mathfrak{S}_m$

def GRUPPI CICLICI

Sia G un gruppo, e $g \in G$ di ordine $n \geq 1$

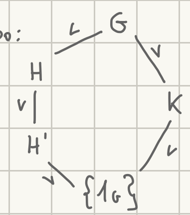
Allora, $\underset{\overset{\parallel}{H < G}}{<g>} \cong \mathbb{Z}/n\mathbb{Z}$ in not. additiva — quindi possiamo trovare i sottogruppi attraverso $\mathbb{Z}/n\mathbb{Z}$

sottogruppo del sottogruppo

PROP:

- $\forall\, d \mid n$, $\exists!$ sottogruppo $H_d < H$ t.c. $\# H_d = d$

Quindi il diagramma di Hasse di un gruppo G è del tipo: (per $<$)



($<$ è una relazione di equivalenza)

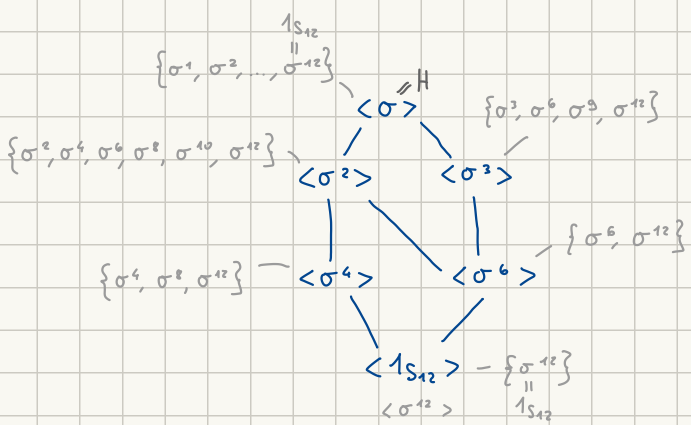
esempio

$G = S_{12}$, $\sigma = (1\ 2\ 3 \dots 12)$

$\text{ord}(\sigma) = 12$, quindi $\underset{\overset{\parallel}{H}}{<\sigma>} \cong \mathbb{Z}/12\mathbb{Z}$ di isomorfismo $\sigma^K \longrightarrow [K]$

e $\forall$ divisore di 12 c'è un unico $H_d < H$ con $\# H_d = d$ quindi: 1, 2, 3, 4, 6, 12

e il diagramma di Hasse è:



$\mathbb{Z}/12\mathbb{Z} = <\bar{1}>$

$<\bar{2}> = 2\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$

$<\bar{3}> = 3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$

$<\bar{4}> = 4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$

$<\bar{6}> = 6\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$

$2\mathbb{Z}/12\mathbb{Z} = \{[2]\ [4]\ [6]\ [8]\ [10]\ [12]\}$

$\cong$

$\mathbb{Z}/6\mathbb{Z} = \{[1]\ [2]\ [3]\ [4]\ [5]\ [6]\}$

perché? Abbiamo σ, una perm. di ordine 12 (quindi $\sigma^{12} = 1_{S_{12}}$)

Sappiamo che $<g>$ è ciclico isomorfo a $\mathbb{Z}/12\mathbb{Z}$ (in not. additiva)

Quindi esiste un sottogruppo $H_d < <g>$ con cardinalità d per ogni divisore di 12.

Per trovarli, possiamo "aiutarci" con $\mathbb{Z}/12\mathbb{Z}$. Visto che $\mathbb{Z}/12\mathbb{Z}$ è a sua volta ciclico 12, sappiamo che i sottogruppi di $\mathbb{Z}/12\mathbb{Z}$ sono generati dalle classi dei divisori di 12, ovvero:

$[1], [2], [3], [4], [6], [12]$.

$<[1]> = \{\bar{0}, \dots, \overline{11}\}$ corrisponde a $<\sigma>$ (sottogr. di ordine 12)

$<[2]> = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$ corrisponde a $<\sigma^2>$ (ordine 6)

$<[3]> = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ corr. a $<\sigma^3>$ (ordine 4)

$<[4]> = \{\bar{0}, \bar{4}, \bar{8}\}$ corr. a $<\sigma^4>$ (ord. 3)

$<[6]> = \{\bar{0}, \bar{6}\}$ corr. a $<\sigma^6>$ (ord. 2)

$<[12]> = \{\bar{0}\}$ corr. a $<\sigma^{12}> = 1_{S_{12}}$ (ord. 1)

ALGEBRA LINEARE: SPAZI VETTORIALI

SPAZI VETTORIALI

Dato K campo,

sia V un insieme $\neq \emptyset$ munito di

- operazione binaria: $V \times V \longrightarrow V$, $(a, b) \longmapsto (a+b)$
- un'operazione $\underset{\text{scalari}}{K} \times \underset{\text{vettori}}{V} \longrightarrow V$, $(\lambda, v) \longmapsto \lambda \cdot v$ — è commutativa

(V ha somma e prodotto scalare)

si dice che V è uno spazio vettoriale se: — su K (si può scrivere $/K$)

① $(V, +)$ è un gruppo abeliano (di el. neutro 0_V o 0)

② $\alpha \cdot (v+w) = \alpha v + \alpha w \qquad \forall \alpha \in K, \ \forall v, w \in V$ — distribuzione a sx (distr. di scalare su somma di vettori)

③ $(\alpha + \beta) \cdot v = \alpha v + \beta v \qquad \forall \alpha, \beta \in K, \ \forall v \in V$ — distribuzione a dx (distr. di vettore su somma di scalari)

④ $(\alpha \overset{\text{op. }K}{\cdot} \beta) \underset{\text{op. }V}{\cdot} v = \alpha \underset{\text{op }V}{\cdot} (\beta \overset{\text{op. }V}{\cdot} v) \qquad \forall \alpha, \beta \in K, \ \forall v \in V$ — non-proprio-associatività

⑤ $1_K \cdot v = v \qquad \forall v \in V$ — elemento neutro molt.

ma in V non esiste un el. neutro per la molt., quindi quello di K funge da neutro per questa operazione

da queste proprietà discende: • $0_K \cdot v = 0_V \quad \forall v$

infatti, $0_v = \underbrace{0_K \cdot v}_{\in V} - \underbrace{0_K \cdot v}_{\text{opposto}} = \underbrace{(0_K + 0_K) v}_{\text{per ③}} = 0_K \cdot v$ ($0 = -0$)

OSS:

la molt. di $v \in V$ per $-1 \in K$ (opposto dell'el. neutro per l'add in K),

$(-1) \cdot v = -v$

è l'opposto per la struttura di gruppo

infatti, dato $v \in V$,

$v + (-1) v = (1 + (-1)) v$

$= 0 \cdot v = 0$

- per esempio, $V = K$ è uno spazio vettoriale su K

(perché K campo quindi K anello quindi distr., assoc., el. neutro)

spazio vett. K^n

- Poniamo $V = K \times \ldots \times K = K^n$ con l'operazione $+$ di prodotto cartesiano di gruppi

(con 0 el. neutro di K, $0_{K^n} = (0, \ldots, 0)$ el. neutro di K^n)

Definiamo $K \times V \longrightarrow V$:

$$K \times \overbrace{K \times \ldots \times K}^{n \text{ volte}} \longrightarrow \overbrace{K \times \ldots \times K}^{n \text{ volte}}$$

$$(\lambda, (v_1, \ldots, v_n)) \longmapsto (\lambda v_1, \ldots, \lambda v_n) = \lambda(v_1, \ldots, v_n)$$

questa operazione soddisfa

tutti gli assiomi di spazio vettoriale

distr. a sx:

② $\lambda \cdot ((v_1, \ldots, v_n) + (w_1, \ldots, w_n)) = \lambda((v_1 + w_1, \ldots, v_n + w_n)) =$

$= (\lambda(v_1 + w_1), \ldots, \lambda(v_n + w_n)) = (\lambda v_1 + \lambda w_1, \ldots, \lambda v_n + \lambda w_n) =$

$= (\lambda v_1, \ldots, \lambda v_n) + (\lambda w_1, \ldots, \lambda w_n) =$

$= \lambda(v_1, \ldots, v_n) + \lambda(w_1, \ldots, w_n) = \qquad v = (v_1, \ldots, v_n) \qquad w = (w_1, \ldots, w_n)$

$= \lambda(v + w) = \lambda v + \lambda w$

V, con queste operazioni, è uno spazio vettoriale.

Esempi di spazi vettoriali: (dato K campo)

① K^n, con $n=1$, $K^n = K$ (e $V=K$ visto sopra), con $n=0$ $K^0 = (0)$ (spazio vettoriale banale)

② matrici con m linee e n colonne a coefficienti in K

$$M_{m,n}(K) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} : a_{ij} \in K \ \forall i,j \right\} = \left\{ (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} : a_{ij} \in K \ \forall i,j \right\}$$

con operazioni di addizione coefficiente per coefficiente $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$

e moltiplicazione esterna per λ separatamente per ogni coefficiente $\lambda = 2 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}$

nota: essenzialmente, $M_{m,n}(K)$ è una riscrittura di $K^{m \cdot n}$ sotto forma di matrice. (come vettori assembly)

per esempio, $M_{2,3}(K) = K^{2\times 3}$ è ~~uguale~~ (formalmente si dice) isomorfo a K^6

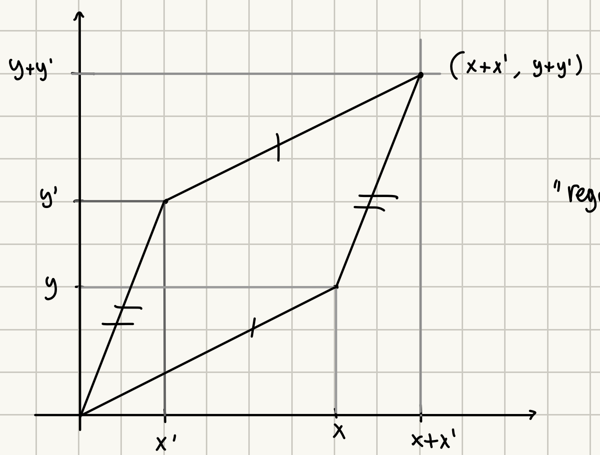
$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \in M_{2,3}(K) \xmapsto{1:1} (a,b,c,d,e,f) \in K^6$$

esempio operazioni:

$A = (a_{ij})$ $B = (b_{ij})$ $\in M_{m,n}(K) = K^{m\times n}$

- $A + B = (a_{ij} + b_{ij}) \in M_{m,n}(K)$
- $\lambda \in K$: $\lambda A = (\lambda A_{ij}) \in M_{m,n}(K)$

RAPPRESENTAZIONE GRAFICA DELLA SOMMA IN $\mathbb{R}^2$



"regola del parallelogramma"

③ Polinomi a coefficienti in K campo

$V = K[X]$ $\quad f = f_0 + f_1 x + f_2 x^2 \ldots$, $g = g_0 + g_1 x + g_2 x^2 \ldots$, $\lambda \in K$

$f + g = f_0 + g_0 + (f_1 + g_1)x + \ldots$

$\lambda \cdot f = \lambda f_0 + (\lambda f_1)x + (\lambda f_2)x^2 + \ldots$

Osservazione: K finito (es $K = \mathbb{F}_p$) ma $K[X]$ infinito

④ lo ho skippato per ora

⑤ $\mathbb{C}$ è uno spazio vettoriale su $\mathbb{C}$

ma si ha anche che $\mathbb{C}$ è uno spazio vettoriale su $\mathbb{R}$

$\mathbb{C} = \{ x+iy : x,y \in \mathbb{R} \}$ la struttura di gruppo abeliano è nota

· $\lambda \in \mathbb{R}$, $z \in \mathbb{C}$, $z = x+iy$ $\lambda \cdot z = \lambda(x+iy) = (\lambda x) + i(\lambda y)$

def **APPLICAZIONE LINEARE** (come omom. gruppi)

Dati due spazi vettoriali V, V' su K, un'applicazione $V \xrightarrow{f} V'$ è detta lineare se:

infatti notiamo che se $\lambda = 1$, è l'assioma dell'omomorfismo

$$\forall x,y \in V,\ \forall \lambda \in K, \quad f(x+\lambda y) = f(x) + \lambda f(y)$$

Se f è biiettiva, si dice isomorfismo.

Se $f: V \to V'$ isomorfismo esiste, allora si dice che V e V' sono isomorfi e si scrive $V \cong V'$.

def SOTTOSPAZIO VETTORIALE (è un sottoinsieme di uno sp. vett. che è a sua volta sp. vett.)

dato V spazio vettoriale su K,

$W \subset V$, $W \neq \emptyset$ è un sottospazio vettoriale se: (varie definizioni alternative)

1. è uno spazio vettoriale per le operazioni indotte da V
   ovvero se, come gruppi abeliani, si ha: (quindi anche W abeliano)
   - $W < V$
   - $\forall w \in W, \forall \lambda \in K, \quad \lambda \cdot w \in W$

2. - $\forall w, w' \in W$, si ha $w + w' \in W$ (stabilizzato rispetto alla somma)
   - $\forall w \in W, \forall \lambda \in K, \quad \lambda \cdot w \in W$

3. se è stabile per combinazioni lineari nel modo seguente:
   - $\forall w, w' \in W$, $\forall \lambda, \lambda' \in K$, si ha $\lambda w + \lambda' w' \in W$

4. $\forall w_1, \dots, w_n$ e $\forall \lambda_1, \dots, \lambda_n$, $\lambda_1 w_1 + \dots + \lambda_n w_n \in W$

5. $\forall w, w' \in W$ e $\forall \lambda \in K$, $w + \lambda w' \in W$

def COMBINAZIONE LINEARE

Dati $v, \dots, v_n \in V$, e $\lambda_1, \dots, \lambda_n \in K$ allora $\lambda_1 v_1 + \dots + \lambda_n v_n$ è una combinazione lineare di $v_1 \dots v_n$ (a coeff. $\lambda_1, \dots, \lambda_n$)

- si dice "Span" o "Sottospazio Generato da $v_1, \dots, v_n$" il sottospazio vettoriale ottenuto dall'insieme di tutte le possibili combinazioni lineari di un insieme di vettori.
  - si scrive "$\text{Span}_K(\{v_1, \dots, v_n\})$" o "$\text{Vett}_K(\{v_1, \dots, v_n\})$"

esempi

① Mostrare che $S = \{(x,y,z) \in \mathbb{R}^3 \text{ t.c. } x^2+y^2+z^2 = 1\}$ non è un sottospazio vettoriale di $\mathbb{R}^3$.

prendiamo $w = (1,0,0)$, $w' = (0\,1\,0)$, $\lambda = 1$

$w + \lambda w' = \overset{x\ y\ z}{(1\,1\,0)}$ e $x^2+y^2+z^2 = 1+1+0 = 2 \neq 1 \implies w + w' \notin S$

metodo alternativo: ogni sottosp. vettoriale di $\mathbb{R}^3$ deve contenere $\underbrace{0}_{\text{el. neutro somma (op. spazi vettoriali)}} = (0,0,0)$. Qui $(0,0,0) \notin S$

def SPAN / SOTTOSPAZIO GENERATO

Prendiamo V sp. vett. su K. Siano $v_1, \dots, v_n \in V$.

Poniamo $W = \text{Span}_K(\{v_1, \dots, v_n\}) = \{\text{comb. lineari di } v_1, \dots v_n\} = \{\lambda_1 v_1, \dots, \lambda_n v_n : \forall \lambda_1, \dots \lambda_n \in K\}$
o Vett_K

è un sottospazio vettoriale.

Per vederlo, consideriamo $w, w' \in W$, $\lambda \in K$, e calcoliamo $w + \lambda w'$

Ma $w = \sum_{i=1}^n \lambda_i v_i$, $w' = \sum_{i=1}^n \lambda'_i v_i$, quindi $w + \lambda w' = \sum_{i=1}^n \underbrace{\lambda_i v_i}_{w} + \underbrace{\lambda \lambda'_i v_i}_{\lambda w'} \underset{\text{distr.}}{=} \sum_{i=1}^n (\lambda_i + \underbrace{\lambda\lambda'_i}_{\lambda'' \text{ quindi si può scrivere come } \lambda v}) v_i \implies w + \lambda w' \in W$

quindi Span_K è un sottosp. vett.! per ⑤

OSSERVIAMO che $\text{Span}(\{v_1, \dots, v_n\}) = \bigcap_{\substack{W \subset V \\ \text{sottosp. vett.}, \\ W \supset \{v_1, \dots, v_n\}}} W$ intersez. dei sott. vett che contengono $v_1, \dots, v_n$

quindi è il più piccolo sottospazio vett. di W che contiene $\{v_1, \dots, v_n\}$. (analogo a sottogruppi generati)

Si chiama anche il sottospazio vettoriale generato da $\{v_1, \dots, v_n\}$. Talvolta si scrive $< \{v_1, \dots, v_n\} >$ ma non spesso per non confondersi con i sottogruppi oss: L'intersezione tra sottospazi vettoriali è un sottospazio vettoriale

dim:

dati W_1, W_2 sott. vett., $W_1 \cap W_2 < V$ (perché $W_1, W_2 < V$ per def. sottosp. vett., e $\cap$ sottogr. è un sottogr.)

Sia $v \in W_1 \cap W_2$, e $\lambda \in K$.

Allora, $\lambda v \in W_i$ perché W_i è sottosp. vett. di V (con $i = 1, 2$)

Quindi, $\lambda v \in W_1 \cap W_2$

oss: Se W è sottosp. vett. di V, allora $\emptyset \in W$.

def VETTORI LINEARMENTE INDIPENDENTI

Dato V sp. vett./K, $v_1, \dots, v_n$ sono linearmente indipendenti se, — o l.i. o lin. ind.

dati $\lambda_1, \dots, \lambda_n \in K$ t.c. $\lambda_1 v_1 + \dots + \lambda_n v_n = \emptyset_V$

allora $\lambda_1 = \dots = \lambda_n = \emptyset_K$

Ovvero, se l'unica combinazione lineare di $v_1, \dots, v_n$ che è nulla è quella banale (ovvero quella con tutti i $\lambda = \emptyset$) — $\sum_i 0 \cdot v_i$ ($\sum_i \lambda_i v_i$ con $\lambda_i = \emptyset \ \forall i$)

Al contrario, si dicono linearmente dipendenti se esiste almeno una combinazione lineare nulla non banale.

quindi, due vett. sono l.d. se uno si può scrivere in funzione dell'altro (come multiplo scalare)

es $v_1 = 2v_2$

$\iff v_1 - 2v_2 = \emptyset$

come vederlo? esempio.

- in $\mathbb{R}^2$, $v_1 = \begin{pmatrix}1\\2\end{pmatrix}$, $v_2 = \begin{pmatrix}2\\2\end{pmatrix}$ sono l.i.

Consideriamo una comb. lin. $\lambda_1 v_1 + \lambda_2 v_2 = \emptyset$

$$\text{ovvero} \quad \lambda_1 \begin{pmatrix}1\\2\end{pmatrix} + \lambda_2 \begin{pmatrix}2\\2\end{pmatrix} = \emptyset \overset{\text{molt. scalare}}{\iff} \begin{pmatrix}\lambda_1\\2\lambda_1\end{pmatrix} + \begin{pmatrix}2\lambda_2\\2\lambda_2\end{pmatrix} = \emptyset \overset{\text{somma vett.}}{\iff} \begin{pmatrix}\lambda_1 + 2\lambda_2\\2\lambda_1 + 2\lambda_2\end{pmatrix} = \emptyset$$

Costruiamo il sistema lineare che ha $\begin{pmatrix}\lambda_1\\\lambda_2\end{pmatrix}$ come soluzioni (si può direttamente mettere i vettori a sistema)

$$\begin{cases} \lambda_1 + 2\lambda_2 = \emptyset \ ① \\ 2\lambda_1 + 2\lambda_2 = \emptyset \end{cases} \underset{\text{si sottrae termine a termine}}{\Longrightarrow} 2\lambda_1 - \lambda_1 + 2\lambda_2 - \cancel{2\lambda_2} = \emptyset - \emptyset \iff \lambda_1 = \emptyset \quad \text{sostituiamo nell'eq. 1}$$

($\lambda_1 = x_1$ e $\lambda_2 = x_2$)

$\Longrightarrow 0 + 2\lambda_2 = \emptyset \iff \lambda_2 = \emptyset$ quindi $\lambda_1 = \lambda_2 = \emptyset$

oss: se ho m vettori $v_1, \dots, v_m \in K^n$ e se $m > n$, allora $v_1, \dots, v_m$ sono sempre l. d.

es. $\begin{pmatrix}1\\0\end{pmatrix} \begin{pmatrix}2\\1\end{pmatrix} \begin{pmatrix}3\\2\end{pmatrix}$ sono $3 > 2$ vettori in $\mathbb{R}^2$, e sono quindi l.d.

oss: Data $f: V \xrightarrow{\cong} V'$, $v_1, \dots, v_n$ sono l.i. se $f(v_1), \dots, f(v_n)$ sono l.i.

per esempio, $M_{m,n}(K) \cong K^{m \cdot n}$ può essere utile

esercizi

① notare che $v_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}$, $v_2 = \begin{pmatrix}2\\2\\0\end{pmatrix}$, $v_3 = \begin{pmatrix}1\\2\\1\end{pmatrix}$

$$\begin{cases} \lambda_1 + 2\lambda_2 + \lambda_3 = \emptyset \\ 2\lambda_2 + 2\lambda_3 = \emptyset \\ \lambda_3 = \emptyset \end{cases} \quad \begin{cases} \lambda_1 + 2\lambda_2 = \emptyset \\ 2\lambda_2 = \emptyset \\ \lambda_3 = \emptyset \end{cases} \quad \begin{cases} \lambda_1 = \emptyset \\ \lambda_2 = \emptyset \\ \lambda_3 = \emptyset \end{cases}$$

$\lambda_1 = \lambda_2 = \lambda_3 = \emptyset \Longrightarrow v_1, v_2, v_3$ l.i.

② Consideriamo $\underbrace{v_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, v_2 = \begin{pmatrix}2\\0\\0\end{pmatrix}}_{\text{uno multiplo dell'altro}}$, $v_3 = \begin{pmatrix}1\\2\\1\end{pmatrix}$

si vede che $2v_1 - v_2 + \emptyset v_3 = \emptyset$

def MATRICE TRIANGOLARE

$=\mathcal{M}_n$ - un pedice solo indica #righe = #colonne

una matrice $M \in \mathcal{M}_{n,n}(\mathbb{R})$

è detta triangolare superiore se si può scrivere come

(invece, una triangolare inferiore sarebbe così: $\begin{pmatrix} m & 0 & 0 & 0 \\ m & m & 0 & 0 \\ m & m & m & 0 \\ m & m & m & m \end{pmatrix}$)

(con gli zeri in alto)

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} & \dots & m_{1\,n-1} & m_{1n} \\ 0 & m_{22} & m_{23} & \dots & m_{2\,n-1} & m_{2n} \\ 0 & 0 & m_{33} & \dots & m_{3\,n-1} & m_{3n} \\ 0 & 0 & 0 & \dots & m_{4\,n-1} & m_{n-1,n} \\ & & & \vdots & & \\ 0 & 0 & 0 & \dots & m_{n-1,n-1} & m_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 & m_{n,n} \end{pmatrix}$$

diagonale della matrice ($m_{i,j}$ con $i=j$)

esempio: $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}$

- le colonne e le righe di M, viste come vettori di $\mathbb{R}^n$, sono l.i. $\iff m_{11}, m_{22}, \dots, m_{nn}$ (coeff. diag.) sono tutti non nulli

esempio:

- le colonne della matrice $\begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ sono l. d. $\iff \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ sono l. d.

(gli zeri non influenzano)

$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ l. d. perché

$$\begin{cases} \lambda_1 + 2\lambda_2 + 3\lambda_3 \\ \lambda_2 + 2\lambda_3 \end{cases} \iff \lambda_2 = -2\lambda_3 \qquad \begin{cases} \lambda_1 = \lambda_3 \\ \lambda_2 = -2\lambda_3 \end{cases}$$

se pongo $\lambda_3 = 1$ allora

$(\lambda_1, \lambda_2, \lambda_3) = (-1, -2, 1) \neq (0,0,0)$

e si ottiene la comb. nulla, ma non banale

$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} - 2\begin{pmatrix} 2 \\ 1 \end{pmatrix} + \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

esercizi (x casa)

1. $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$

   in $\mathbb{R}^3$, $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

Dimostrare che $e_1, \dots, e_n$ sono l.i. e che, considerando inoltre $e_{n+1} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$, allora $e_1, \dots, e_n, e_{n+1}$ sono l. d.
e caratterizzare tutte le comb. lin. nulle

2. a) $V = \mathcal{M}_n(K)$, mostrare che le matrici

   $e_{ij} = \begin{pmatrix} & \vdots & \\ \cdots & 1 & \\ & & \end{pmatrix}$ (tutti zeri) $1 \le i, j \le n$ (ce ne sono n^2) (matr. $n \times n$)

   sono l.i.

   b) Mostrare che $(e_{ij})_{1 \le i,j \le n}$ e $f: \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ (tutti uni) sono l. d.

DIVERSI MODI DI RAPPRESENTARE UNA MATRICE

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

- $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$
- $A = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}$ con A_i i-esima riga di A
- $A = (A^1 \dots A^n)$ con A^j j-esima colonna di A

$A = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} = M_{2,3}(\mathbb{R})$ $\quad A_1 = (abc) \quad A_2 = (def), \quad A^1 = \begin{pmatrix} a \\ d \end{pmatrix}, \ A^2 = \begin{pmatrix} b \\ e \end{pmatrix}, \ A^3 = \begin{pmatrix} c \\ f \end{pmatrix}$

PRODOTTO TRA MATRICI

prodotto scalare di una matrice linea e una matrice colonna

$U = (u_1 \dots u_n) \in M_{1,n}(K)$, $\quad V = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in M_{n,1}(K)$

$$\langle U, V \rangle = \sum_{i=1}^{n} u_i v_i = u_1 v_1 + \dots + u_n v_n$$

con questo prodotto scalare definiamo un'operazione: $M_{m,\underbrace{k}_{}}(K) \times M_{\underbrace{k}_{=},n}(K) \longrightarrow M_{m,n}(K)$

dove $(A, B) \longmapsto A \cdot B = (\langle A_i, B^j \rangle)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$

$A = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}$, $A_1 \in M_{1,k}(K)$ $\quad B = (B^1 \dots B^n)$, $B^1 \in M_{k,1}(K)$

è un'operazione associativa e distributiva

esempio

$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in M_{2,3}$, $\quad B = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \in M_{3,2}$

$A \cdot B = \begin{pmatrix} \text{linea 1 A} \cdot \text{colonna 1 B} & \text{linea 1 A} \cdot \text{colonna 2 B} \\ \text{linea 2 A} \cdot \text{col. 1 B} & \text{linea 2 A} \cdot \text{col. 2 B} \end{pmatrix}$

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

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

$$A \cdot B = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 & 1 \cdot 4 + 2 \cdot 5 + 3 \cdot 6 \\ 4 \cdot 1 + 5 \cdot 2 + 6 \cdot 3 & 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 6 \end{pmatrix} = \begin{pmatrix} 14 & 32 \\ 32 & 77 \end{pmatrix} \in M_{2,2}(\mathbb{R})$$

esercizio

- calcolare $B \cdot A \in M_{3,3}(\mathbb{R})$

$B = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$

$$B \cdot A = \begin{pmatrix} 1 \cdot 1 + 4 \cdot 4 & 1 \cdot 2 + 4 \cdot 5 & 1 \cdot 3 + 4 \cdot 6 \\ 2 \cdot 1 + 5 \cdot 4 & 2 \cdot 2 + 5 \cdot 5 & 2 \cdot 3 + 5 \cdot 6 \\ 3 \cdot 1 + 6 \cdot 4 & 3 \cdot 2 + 6 \cdot 5 & 3 \cdot 3 + 6 \cdot 6 \end{pmatrix} = \begin{pmatrix} 17 & 22 & 27 \\ 23 & 29 & 36 \\ 27 & 36 & 45 \end{pmatrix}$$

26/11 (un po' riordinati)

MATRICE IDENTITÀ 1_n, $Id_n \in M_n(K)$
in $M_n(K)$, la matrice

$$1_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$ svolge il ruolo di elemento neutro per il prodotto righe-colonne tra matrici

tutti zeri e diagonale di uni

es. in M_2, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

o in M_3, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

def MATRICI INVERTIBILI
Una matrice $A \in M_n(K)$ è invertibile se $\exists A' \in M_n$ t.c. $A \cdot A' = A' \cdot A = 1_n$

$$GL_n(K) := \{A \in M_n(K) : A \text{ invertibile}\}$$ GRUPPO LINEARE GENERALE

da Wikipedia: è un gruppo moltiplicativo (prodotto matriciale)

MATRICI 2×2

Notiamo che $M_2(K)$, dotato delle operazioni di $+, \cdot$, con el. neutri $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ e $1_2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
è un anello unitario (non commutativo)

$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

def determinante di una matrice 2×2

data $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K)$, $\det(A) := ad - bc \in K$

matrici 2×2 invertibili (Lemma)
$A \in M_2(K)$ è invertibile per la moltiplicazione linee per colonne
$\iff \det(A) \neq 0$ ($\iff \det(A) \in K^\times$)

di inverso

si scrive anche: $A \in GL_2(K)$, $A \in (M_2(K))^\times$

(A invertibile $\iff \exists A' \in M_2$ t.c. $A \cdot A' = A' \cdot A = 1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$)

dim:
① $\det(A) \neq 0 \implies A \in GL_2(K)$

Poniamo $A' = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2$ ($\neq 0$ per ip.)

Calcoliamo $AA' = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id_2$

e $A'A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \underset{\text{prod. scalare comm.}}{=} \frac{1}{ad-bc}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = Id_2$

Sappiamo quindi che $A' = A^{-1}$

Lemma: dati $A, B \in M_2(K)$ allora $\det(AB) = \det(A) \cdot \det(B)$ — non lo dimostriamo

② $A \in GL_2(K) \Longrightarrow \det(A) \neq 0$

$A \in M_2(K)^\times \Longleftrightarrow \exists\, A' \in M_2(K)^\times$ t.c. $AA' = A'A = 1_2$

Calcoliamo i determinanti: $\det(AA') = \det(A'A) = 1 \neq 0$

$$\underbrace{\det(AA')}_{\overset{\text{lemma}}{=}\ \det(A)\det(A')} \qquad \underbrace{\det(A'A)}_{=\ \det(A')\det(A)}$$

$\Longrightarrow \det(A), \det(A') \neq 0$ (K non ha divisori di 0) ∎

notiamo che $\det(A') = \det(A^{-1}) = \det(A)^{-1}$

in particolare, $\det : M_2(K)^\times \longrightarrow K^\times$ è un omomorfismo di gruppi

nota: $GL_2(\mathbb{R})$ non è abeliano: $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$ e $AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$

SISTEMI LINEARI

Dato un campo K, un sistema lineare di m equazioni e n indeterminate a coeff. in K è un sistema di equazioni del tipo:

$$(*)\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = \underbrace{b_1}_{\text{termini noti / costanti } \in K} \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \qquad\qquad\qquad\qquad \vdots \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + \underbrace{a_{mn}}_{\text{coefficienti } \in K}x_n = b_m \end{cases}$$

risolvere un sistema significa descrivere l'insieme di tutti i vettori

$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ tali che tutte le equazioni sono soddisfatte simultaneamente

- Un sistema lineare $(*)$ si dice compatibile se il sottoinsieme $Sol(*)$ di K^n delle sue soluzioni è non vuoto. Altrimenti, si dice incompatibile.

es. $\begin{cases} x_1 = 0 \\ x_1 = 1 \end{cases}$ è incompatibile ($1 \neq 0$ in ogni campo) $\qquad$ $\{x_1 = 0$ è compatibile, con $Sol = \{(0)\} \subset K^1$

Per quanto riguarda i sistemi lineari, i seguenti problemi sono importanti:

1. Decidere se un sistema è compatibile
2. Descrivere tutte le soluzioni nel caso compatibile
3. Nel caso compatibile, descrivere l'insieme delle soluzioni attraverso un insieme di "parametri minimali"

ESPRESSIONE MATRICIALE DI UN SISTEMA LINEARE SU K

Il sistema $(*)$ si può riscrivere alternativamente nel modo seguente

matrice dei coeff.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} \in M_{m,n}(K), \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in M_{m,1}(K), \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K)$$

$$A \cdot X = \begin{pmatrix} \langle A_1, X \rangle \\ \langle A_2, X \rangle \\ \vdots \\ \langle A_m, X \rangle \end{pmatrix} \in M_{m,1}(K)$$

prodotto matriciale linea · colonna di ogni linea di A (coeff. $a_1 \dots a_n$) per l'unica colonna di X

quindi il sistema lineare $(*)$ può essere riformulato in modo compatto attraverso l'equazione in matrici:

$$A \cdot X = b$$

esempio

dati $A \in GL_m(K)$, $b \in M_{m,1}(K)$,

il sistema $(\star)\ AX = b$ è sempre compatibile e ammette un'unica soluzione x.

Infatti, sia A^{-1} l'inverso di A. Allora, $x \in M_{m,1}(K)$ è soluzione di $(\star) \iff A^{-1}Ax = A^{-1}b \iff x = b$

Quindi, $Sol(\star) = \{(b)\}$.

MATRICE COMPLETA ASSOCIATA A UN SISTEMA LINEARE

Consideriamo un sistema lineare:

$$(*) = AX = b$$

tutti i suoi dati sono contenuti nella matrice: $\underbrace{(A|b)}_{\text{matrice completa del sistema}} \in M_{m,n+1}(K)$

giustapposizione di b ad A

- se $b = \emptyset$ il sistema è omogeneo
  altrimenti, è non omogeneo

OSS: $AX = b \iff x_1A^1 + x_2A^2 + \ldots + x_nA^n = b$

$\iff b$ è combinazione lineare di $A^1, \ldots, A^n$

$\iff b \in Span_K(A^1, \ldots, A^n)$

esempi

① $\begin{cases} 2x_1 + x_2 - 3x_3 + x_4 = 1 \\ x_3 + x_4 = 5 \\ x_1 - x_2 - x_3 - 2x_4 = \emptyset \end{cases}$ $(K = \mathbb{R})$

$A = \begin{pmatrix} 2 & 1 & -3 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & -1 & -2 \end{pmatrix}$, $b = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$, $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$

$(A|b) = \left(\begin{array}{cccc|c} 2 & 1 & -3 & 1 & 1 \\ 0 & 0 & 1 & 1 & 5 \\ 1 & -1 & -1 & -2 & 0 \end{array}\right)$

quindi $x_1 \underbrace{\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}}_{A^1} + x_2 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} -3 \\ 1 \\ -1 \end{pmatrix} + x_4 \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}}_{b}$

dire che $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ è soluzione di $(*)$ significa

che $x_1A^1 + x_2A^2 + x_3A^3 + x_4A^4 = b$

ovvero $(*)$ è compatibile $\iff b \in Span_{\mathbb{R}}(A^1, A^2, A^3, A^4)$

② $\begin{cases} 2x_1 - x_2 - x_3 = 1 \\ x_1 + x_3 = 5 \end{cases} \iff x_1\begin{pmatrix} 2 \\ 1 \end{pmatrix} + x_2\begin{pmatrix} -1 \\ 0 \end{pmatrix} + x_3\begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix}$

$A = \begin{pmatrix} 2 & -1 & -1 \\ 1 & 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 \\ 5 \end{pmatrix}$

questo sistema è compatibile $\iff \begin{pmatrix} 1 \\ 5 \end{pmatrix} \in Span_{\mathbb{R}}\left(\begin{pmatrix} 2 \\ 1 \end{pmatrix}\begin{pmatrix} -1 \\ 0 \end{pmatrix}\begin{pmatrix} -1 \\ 1 \end{pmatrix}\right)$

il che è vero, infatti $\begin{cases} 2x_1 - x_2 - x_3 = 1 \\ x_1 + x_3 = 5 \end{cases} \iff x_1 = 5 - x_3$ $\begin{cases} 10 - x_2 - 3x_3 = 1 \\ x_1 = 5 - x_3 \end{cases}$ $\begin{cases} x_2 = 9 - x_3 \\ x_1 = 5 - x_3 \end{cases}$

ammette soluzioni, es. $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \\ 0 \end{pmatrix}$

STRUTTURA DELL'INSIEME DI SOLUZIONI DI UN SISTEMA LINEARE

Consideriamo il sistema $AX = b$ $(*)$ con $A \in M_{m,n}(K)$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K)$, $b \in M_{n,1}(K)$

NOTAZIONE

Se $(*)$ è incompatibile, poniamo $Sol(A|b) = \emptyset$

Se $(*)$ è compatibile, poniamo $Sol(A|b) = \left\{ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n \text{ t.c. } X \text{ è sol. di } (*) \right\}$

Proposizione

$Sol(A|b)$ è un sottospazio vettoriale di $K^n \iff b = 0$

(sappiamo che sott. vett. $\implies$ sp. vett. $\implies$ gruppo, e non può essere un gruppo se non ha l'elemento neutro $0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$)
e non può avere l'el. neutro $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ se $b \neq 0$, perché $a_1 0 + a_2 0 + \dots a_n 0$ non può essere $\neq 0$
(se 0 è tra le sol, $b = 0$ per forza)

dim

- Se $b \neq 0$, visto che $Sol(A|b) = \left\{ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ t.c. } A^1 x_1 + A^2 x_2 + \dots + A^n x_n = b \right\} \not\ni \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, e $Sol(A|b)$ non è s.v. di K^n.

- Supponiamo quindi che $b = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = 0$.

Mostriamo che $Sol(A|0)$ è un s.v. di K^n.
Prendiamo $X, X' \in Sol(A|0)$ e $\alpha, \alpha' \in K$. Devo mostrare che $\alpha X + \alpha' X' \in Sol(A|0)$

p.80
def ③ sottosp. vett. : stabilità per comb. lineari

$X \in Sol(A|0) \iff AX = 0$ e $X' \in Sol(A|0) \iff AX' = 0$

$A(\alpha X + \alpha' X') = \alpha A x + \alpha' A x' = \alpha \cdot 0 + \alpha' \cdot 0 = 0 \implies \alpha X + \alpha X' \in Sol(A|0)$

prodotto scalare è commutativo

Teorema

Supponiamo di avere un sistema

$$(*)\ AX = b\ ,\quad A \in M_{m,n}(K)\ ,\quad b \in M_{m,1}(K)\ ,\quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K)$$

Supponiamo inoltre che $(*)$ sia compatibile $(Sol(A|b) \neq \emptyset)$ o K^m

($\text{ciò è equivalente a } b \in Span_K(A^1, \dots, A^n) \subset M_{m,1}(K)$)

Sia $x_0 \in Sol(A|b)$. Allora,

$$Sol(A|b) = x_0 + Sol(A|0)$$

struttura simile al CRT

dim

Sia $X \in Sol(A|b)$. Allora, $X = X - X_0 + X_0$ ovvero $X = X_0 + \underbrace{X - X_0}$

così ho $X_0 + Sol(A|0)$

① Per mostrare che $Sol(A|b) \subset X_0 + Sol(A|0)$, basta verificare che $X - X_0 \in Sol(A|0)$, ovvero che $A(X-X_0) = 0$

Noi sappiamo che $AX = b$ e che $AX_0 = b \implies \underbrace{AX - AX_0}_{A(X-X_0)} = \overset{b-b}{0} \implies X - X_0 \in Sol(A|0)$ mostrato $\subset$

② Mostriamo adesso che $\forall y \in Sol(A|0),\ X_0 + Y \in Sol(A|b)$

e deve darmi b.

Devo calcolare $A(X_0 + Y) = \underbrace{AX_0}_{b} + \underbrace{AY}_{0} = b + 0 = b \implies X_0 + Sol(A|0) \subset Sol(A|b)$ mostrato $\supset$

perché $X_0 \in Sol(A|b)$ perché $Y \in Sol(A|0)$

Quindi, $Sol(A|b) = X_0 + Sol(A|0)$ ■

esempio

$$\begin{cases} x_1 + 2x_2 + 3x_3 = 1 \\ \phantom{x_1 + {}} x_2 - x_3 = 4 \\ \phantom{x_1 + x_2 - {}} x_3 = 5 \end{cases} \qquad A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix},\quad b = \begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix}$$

• noto che $x_3 = 5$ - sostituisco "a cascata"

$x_3 = 5,\quad x_2 = 9,\quad x_1 = -32$

$$Sol(*) = \left\{ \begin{pmatrix} -32 \\ 9 \\ 5 \end{pmatrix} \right\}$$

equivalentemente, grazie al teorema precedente, posso scrivere

$$Sol(A|b) = X_0 + Sol(A|0) = \begin{pmatrix} -32 \\ 9 \\ 5 \end{pmatrix} + \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\} \subset M_{3,1}(\mathbb{R})$$

ALGORITMO DI GAUSS

Introduciamo una relazione sulle matrici complete di $M_{m,n+1}(K)$
$\llcorner$ n indet. e b giustapposto

$$M, M' \in M_{m,n+1}(K) \qquad M \sim M' \iff Sol(M) = Sol(M')$$

è una relazione di equivalenza — abbastanza ovvio (l'uguaglianza è di equiv)

$$AX = b \rightsquigarrow M(A|b)$$

Idea di Gauss: usare un insieme "semplice" di trasformazioni su $M_{m,n+1}(K)$ che lasciano invarianti le classi $\sim$ di equivalenza
(ogni classe ha un rapp. unico matrice "a gradini", le cui soluzioni si vedono subito)

operazioni elementari:

① PERMUTARE LE RIGHE

② MOLTIPLICARE UN'EQ (una riga qualsiasi) DEL SISTEMA PER UNO SCALARE $\lambda \in K^\times$ (non nullo)

③ SOSTITUIRE UNA RIGA CON SE STESSA + (somma vett) UN MULTIPLO SCALARE DI UN'ALTRA RIGA (es. 3a riga += 2· 2a riga)

Gauss ha mostrato che, operando con un numero finito
di operazioni del tipo ①, ②, ③, se ne ottiene un'altra, M', con $M \sim M'$

più sinteticamente
Date due matrici $M, M' \in M_{m,n+1}(K)$, scriviamo

— simbolo scelto da Pellarin (\lessgtr su LaTeX)

$M \stackrel{\cup}{\cap} M' \iff$ M' si può ottenere da M attraverso un numero finito di operazioni ①, ②, ③
$\llcorner$ è una rel. di equiv.

Teorema

$M \stackrel{\cup}{\cap} M' \implies M \sim M'$ (non vale il contrario - è possibile che due matrici unrelated abbiano le stesse soluzioni)

esempio:
I sistemi lineari associati alle seguenti matrici ammettono lo stesso insieme di soluzioni:

$$\left(\begin{array}{ccc|c} 1&1&1&2\\ 1&2&0&3\\ 2&2&2&4 \end{array}\right) \underset{R_3 \xmapsto[2]{} \frac{1}{2}R_3}{\stackrel{\cup}{\cap}} \left(\begin{array}{ccc|c} 1&1&1&2\\ 1&2&0&3\\ 1&1&1&2 \end{array}\right) \underset{R_2 \xmapsto[3]{} R_2 - R_1}{\stackrel{\cup}{\cap}} \begin{pmatrix} 1&1&1\\ 0&1&-1\\ 1&1&1 \end{pmatrix} \underset{R_3 \xmapsto[3]{} R_3 - R_1}{\stackrel{\cup}{\cap}} \left(\begin{array}{ccc|c} 1&1&1&2\\ 0&1&-1&1\\ 0&0&0&0 \end{array}\right) \underset{R_1 \xmapsto[3]{} R_1 - R_2}{\stackrel{\cup}{\cap}} \left(\begin{array}{ccc|c} 1&0&2&1\\ 0&1&-1&1\\ 0&0&0&0 \end{array}\right)$$

$-1 \cdot R_1$

questa riga è una tautologia (0=0) ma non la tolgo perché siamo in $M_{3,4}(\mathbb{R})$

a gradini ridotta (definita dopo)

e per il teorema, $Sol\left(\begin{cases} x+2z=1 \\ y-z=1 \end{cases}\right) = Sol(M) = \mathcal{E}$

soluzione sistema om. associato a $Span_{\mathbb{R}}\left(\begin{pmatrix} 2\\-1\\1 \end{pmatrix}\right)$
(sottosp. vett. generato dalle sol. dell'omogenea associata)

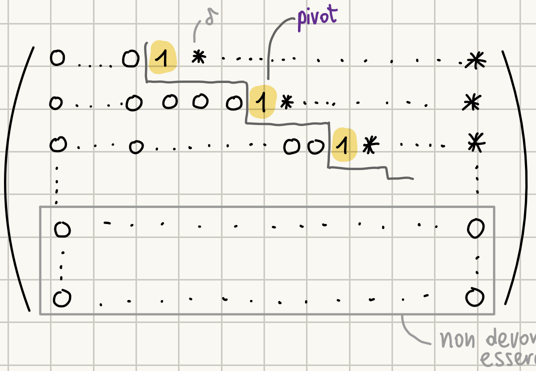
$$\mathcal{E} = \left\{ \begin{pmatrix} x\\y\\z \end{pmatrix} \in M_{3,1}(\mathbb{R}) \text{ t.c. } \begin{pmatrix} x\\y\\z \end{pmatrix} = \begin{pmatrix} 1\\1\\0 \end{pmatrix} + z\begin{pmatrix} -2\\1\\1 \end{pmatrix},\ z \in \mathbb{R} \right\}$$

$\llcorner$ riscritto il sistema

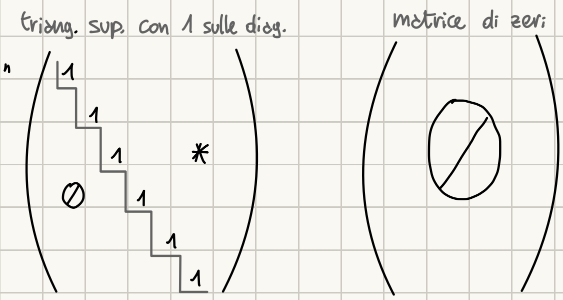
$$\begin{cases} x+2z=1 \\ y-z=1 \end{cases} \qquad \begin{cases} x = 1-2z \\ y = 1+z \end{cases}$$

qui (al posto di z=...) c'è $\emptyset = \emptyset$, quindi la sostituiamo con un'altra tautologia $(z=z)$ $\begin{pmatrix} \vdots\\z \end{pmatrix} = \begin{pmatrix} \vdots\\0 \end{pmatrix} + z\begin{pmatrix} \vdots\\1 \end{pmatrix}$

def MATRICE A GRADINI



casi "estremi"



- tra una riga e l'altra, l'uno deve essere almeno sulla colonna successiva al precedente

(cioè, $\begin{matrix}0&1&0\\0&1&0\end{matrix}$ No, $\begin{matrix}0&1&*\\0&0&1\end{matrix}$ sì, $\begin{matrix}0&1&*&*\\0&0&0&1\end{matrix}$ sì)

Più formalmente, A è a gradini se:

① $A_i = \emptyset \implies A_j = \emptyset \quad \forall j > i$

② Se $A_i \neq \emptyset$, allora il primo coeff. non nullo (pivot) è un 1

③ Se il pivot della riga i appare nella colonna j, allora il pivot della riga $i+1$ appare nella colonna $h > j$

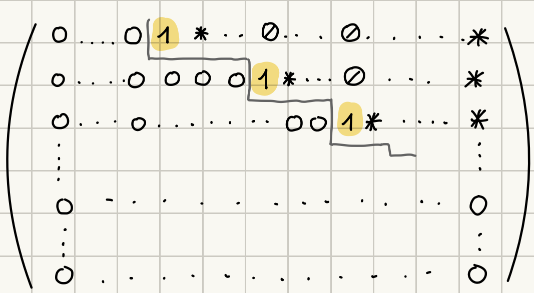
Teorema ALGORITMO DI GAUSS

$\forall M \in M_{m,n+1}(K)$, $\exists \Gamma \in M_{m,n+1}(K)$ t.c. $M \sim \Gamma$

$$(A|b) = \left(\begin{array}{cccc|c}1&1&-1&-2&4\\1&0&-1&0&0\\0&1&0&1&-2\end{array}\right) \underset{R_2 \mapsto R_2-R_1}{\sim} \begin{pmatrix}1&1&-1&-2&4\\0&-1&0&2&-4\\0&1&0&1&-2\end{pmatrix} \underset{R_2 \mapsto -R_2}{\sim} \begin{pmatrix}1&1&-1&-2&4\\0&1&0&-2&4\\0&1&0&1&2\end{pmatrix} \underset{R_3 \mapsto R_3-R_2}{\sim} \begin{pmatrix}1&1&-1&-2&4\\0&1&0&-2&4\\0&0&0&3&-6\end{pmatrix} \underset{R_3 \mapsto \frac{1}{3}R_3}{\sim} \begin{pmatrix}1&1&-1&-2&4\\0&1&0&-2&4\\0&0&0&1&-2\end{pmatrix}$$

a gradini

def MATRICE A GRADINI RIDOTTA



è una matrice a gradini t.c.

④ dato un pivot di modo che $a_{ij} = 1$, allora $\forall k \in \{1, \dots, i-1\}$, $a_{kj} = \emptyset$

(sopra ogni pivot ci sono solo zeri)

ALGORITMO "RINFORZATO"

$\forall M \in M_{m,n+1}(K)$, $\exists! \Gamma \in M_{m,n+1}(K)$ a gradini ridotta t.c. $M \sim \Gamma$

continuiamo l'esempio di prima

$$\begin{pmatrix}1&1&-1&-2&4\\0&1&0&-2&4\\0&0&0&1&-2\end{pmatrix} \underset{R_1 \mapsto R_1-R_2}{\sim} \begin{pmatrix}1&0&-1&0&0\\0&1&0&-2&4\\0&0&0&1&-2\end{pmatrix} \underset{R_2 \mapsto R_2+2R_3}{\sim} \begin{pmatrix}1&0&-1&0&0\\0&1&0&0&0\\0&0&0&1&-2\end{pmatrix}$$

a gradini ridotta

$$Sol(M) = Sol\left(\begin{cases}x-z=\emptyset\\y=0\\t=-2\end{cases}\right) = \left\{\begin{pmatrix}x\\y\\z\\t\end{pmatrix} \in M_{4,1}(\mathbb{R}) \text{ t.c. } \begin{pmatrix}x\\y\\z\\t\end{pmatrix} = \begin{pmatrix}0\\0\\0\\-2\end{pmatrix} + z\begin{pmatrix}1\\0\\1\\0\end{pmatrix}\right\} = \begin{pmatrix}0\\0\\0\\-2\end{pmatrix} + Span_{\mathbb{R}}\left(\begin{pmatrix}1\\0\\1\\0\end{pmatrix}\right)$$

domanda: $Sol(M) = \begin{pmatrix}-1\\0\\-1\\-2\end{pmatrix} + Span_{\mathbb{R}}\left(\begin{pmatrix}1\\0\\1\\0\end{pmatrix}\right)$? Sì, perché X_0 soluzione particolare non è unica

↳ è sol part.: $\begin{pmatrix}0\\0\\0\\-2\end{pmatrix} + \begin{pmatrix}-1\\0\\-1\\0\end{pmatrix}$ $\quad X - X_0 \in Sol(A|b)$

esercizio

$\in M_{3,5+1}$

$$\begin{pmatrix} 0&0&0&1&0&0\\ 0&0&1&2&-1&-1\\ 0&0&0&0&2&3 \end{pmatrix} \underset{\substack{R_3 \mapsto \frac{1}{2}R_3 \\ \text{switch tra } R_1 \text{ e } R_2}}{\sim} \begin{pmatrix} 0&0&1&2&-1&-1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&3/2 \end{pmatrix} \underset{R_1 \mapsto R_1 - 2R_2}{\sim} \begin{pmatrix} 0&0&1&0&-1&-1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&3/2 \end{pmatrix} \underset{R_1 \mapsto R_1 + R_3}{\sim} \begin{pmatrix} 0&0&1&0&0&1/2\\ 0&0&0&1&0&0\\ 0&0&0&0&1&3/2 \end{pmatrix}$$ a gradini ridotta

$$Sol(M) = \left\{ \begin{pmatrix} 0\\0\\1/2\\0\\3/2 \end{pmatrix} + \mathrm{Span}_{\mathbb{R}}\left(\begin{pmatrix} 1\\0\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\0\\0 \end{pmatrix} \right) \right\}$$

perché?

$$\begin{array}{cccccc} 1&2&3&4&5&b \end{array}$$
$$\left(\begin{array}{ccccc|c} 0&0&1&0&0&1/2\\ 0&0&0&1&0&0\\ 0&0&0&0&1&3/2 \end{array}\right)$$

vediamo da qui che quelle tre righe "rappresentano" x_3, x_4, x_5

(in un sistema avremmo)
$$\begin{cases} x_3 = \frac{1}{2} \\ x_4 = 0 \\ x_5 = \frac{3}{2} \end{cases}$$

quindi i valori

invece, $\mathrm{Span}_{\mathbb{R}}$ viene dall'omogenea associata,

$$\left(\begin{array}{ccccc|c} 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0 \end{array}\right)$$ in cui x_3, x_4, x_5 sono invece "vincolati" a $\emptyset$

– le uniche "libere" (tutte le cui combinazioni formano le soluzioni dell'omogenea) sono x_1, x_2

per questo, $\mathrm{Span}_{\mathbb{R}}\left(\begin{pmatrix} 1\\0\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\0\\0 \end{pmatrix} \right)$ qui sono "1"

4/12

esercizio

ⓐ dire se il seguente sistema è compatibile e trovare tutte le soluzioni ($K = \mathbb{R}$)

soluzioni: matrici colonna $\begin{pmatrix} x\\y\\z \end{pmatrix} \in \mathbb{R}^3$ t.c. le equazioni in (*) siano simultaneamente soddisfatte

$$(*)\begin{cases} 2x + 3y - 2z = 1 \\ y - z = 2 \\ x + y + z = -2 \end{cases}$$

① trascriviamo in matrici complete

$$(A|b) = \left(\begin{array}{ccc|c} 2&3&-2&1\\ 0&1&-1&2\\ 1&1&1&-2 \end{array}\right)$$

② la trasformiamo in forma a gradini (+ ridotta) con l'algoritmo di Gauss

posso anche fare una m. a gradini "al contrario" e poi permutare le righe

$$(A|b) = \left(\begin{array}{ccc|c} 2&3&-2&1\\ 0&1&-1&2\\ 1&1&1&-2 \end{array}\right) \underset{R_1 \mapsto R_1 - 2R_3}{\sim} \left(\begin{array}{ccc|c} 0&1&-4&5\\ 0&1&-1&2\\ 1&1&1&-2 \end{array}\right) \underset{R_1 \mapsto R_1 - R_2}{\sim} \left(\begin{array}{ccc|c} 0&0&-3&3\\ 0&1&-1&2\\ 1&1&1&-2 \end{array}\right) \underset{R_1 \mapsto -\frac{1}{3}R_1}{\sim} \left(\begin{array}{ccc|c} 0&0&1&-1\\ 0&1&-1&2\\ 1&1&1&-2 \end{array}\right)$$

$$\underset{R_1 \longleftrightarrow R_3}{\sim} \left(\begin{array}{ccc|c} 1&1&1&2\\ 0&1&-1&2\\ 0&0&1&-1 \end{array}\right)$$ è a gradini. ora va ridotta.

$$\underset{\substack{R_2 \mapsto R_2 + R_3 \\ R_1 \mapsto R_1 - R_3}}{\sim} \left(\begin{array}{ccc|c} 1&1&0&-1\\ 0&1&0&1\\ 0&0&1&-1 \end{array}\right) \underset{R_1 \mapsto R_1 - R_2}{\sim} \left(\begin{array}{ccc|c} 1&0&0&-2\\ 0&1&0&1\\ 0&0&1&-1 \end{array}\right) \Longleftrightarrow Sol(*) = \left\{ \begin{pmatrix} -2\\1\\-1 \end{pmatrix} \right\}$$

Si possono fare due passaggi insieme, ma occhio a non operare sulle stesse righe

vediamo che è unica perché la sol. dell'omogenea è $\begin{pmatrix} 0\\0\\0 \end{pmatrix}$ (tutte le comb. sono $\emptyset$)

ⓑ interpretiamo z come un parametro invece che un'indeterminata

decido io il valore

$$(**)\begin{cases} 2x + 3y - 2z = 1 \\ y - z = 2 \\ x + y + z = -2 \end{cases}$$

determinare l'insieme E dei valori del parametro $z \in \mathbb{R}$ t.c. (**) sia compatibile

- z è un parametro, quindi il sistema è da considerarsi a indeterminate x,y ovvero a soluzioni in $\mathbb{R}^2$

$$A = \begin{pmatrix} 2&3\\ 0&1\\ 1&1 \end{pmatrix}, \quad b = \begin{pmatrix} 1+2z\\ 2+z\\ -2-z \end{pmatrix}$$

Gauss

$$(A|b) = \left(\begin{array}{cc|c} 2 & 3 & 1+2z \\ 0 & 1 & 2+z \\ 1 & 1 & -2-z \end{array}\right) \underset{R_1 \mapsto R_1 - R_3}{\sim} \left(\begin{array}{cc|c} 0 & 1 & 5+4z \\ 0 & 1 & 2+z \\ 1 & 1 & -2-z \end{array}\right) \underset{R_1 \mapsto R_1 - R_2}{\sim} \left(\begin{array}{cc|c} 0 & 0 & 3+3z \\ 0 & 1 & 2+z \\ 1 & 1 & -2-z \end{array}\right) \underset{R_1 \longleftrightarrow R_3}{\sim} \left(\begin{array}{cc|c} 1 & 1 & -2-z \\ 0 & 1 & 2+z \\ 0 & 0 & 3+3z \end{array}\right)$$

Il sistema associato è $\begin{cases} x+y = -2-z \\ y = 2+z \\ 0 = 3+3z \end{cases}$ che è compatibile $\iff z = -1$ $(0 = 3+3z)$

notiamo che $z = -1$ era anche nella sol. precedente $\begin{pmatrix} -2 \\ 1 \\ -1 \end{pmatrix}$

Quindi $\mathcal{Z} = \{-1\}$. Il sistema diventa quindi $\begin{cases} x+y = -1 \\ y = 1 \\ 0 = 0 \end{cases}$ in forma triangolare superiore, di soluzione $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ anche questa combacia

nota: praticamente ho portato di là
un po' inutile

$$\left(\begin{array}{ccc|c} 2 & 3 & -2 & 1 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array}\right)$$

• dim. del sottospazio di K^m generato dalle colonne di A
K^n generato dalle righe di A

def RANGO DI UNA MATRICE

Dato $A \in M_{m,n}(K)$, il **rango** è il numero di pivot di una sua forma a gradini (ridotta o non ridotta)
ridurre non cambia il nr. di pivot
(ovvero il numero di righe non nulle)

è il massimo numero di righe (o colonne) l.i. della matrice (non l'ha detto) (infatti, se riduco la matrice, le righe l.d. diventeranno nulle)

es. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}$

$\begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$

quindi, è anche
• dim del sottosp. di K^m generato dalle colonne
• " " K^n " righe

Notazione: $rg(A) \in \mathbb{N}$: $A \in M_{m,n}(K)$ • $rg(A) = 0 \iff A = (0)$
è impossibile che una matrice non nulla lo diventi con le operazioni date.

OSS: per definizione, se la matrice A' è ottenuta a partire dalla matrice A applicando operazioni elementari, allora $rg(A') = rg(A)$

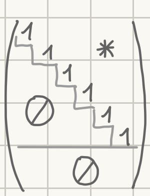
$$A = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 2 & 1 & 0 & 2 \\ 1 & 0 & -1 & 2 \end{pmatrix} \quad rg(A) \underset{\substack{A_2 \to A_2 - 2A_1 \\ A_3 \to A_3 - A_1}}{=} rg \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & -3 & -2 & -4 \\ 0 & -2 & -2 & -1 \end{pmatrix} \underset{A_3 \to 3A_3 - 2A_2}{=} rg \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & -3 & -2 & -4 \\ 0 & 0 & -2 & 5 \end{pmatrix} = 3$$

3 pivot
(non mi serve trasformarli in 1 per vederlo)

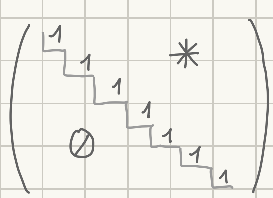
OSSERVAZIONI

① Una matrice $A \in M_{m,n}(K)$ può avere al massimo $\text{rango}(A) = \min(m,n)$

esempi "limite"



se c'è un pivot per colonna, rango $= n$ (colonne), che è $< m$ (righe)

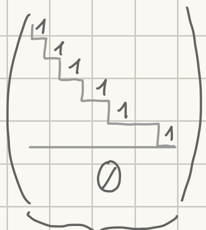


se c'è un pivot per riga, rango $= m$ e $m < n$

(se la matrice è quadrata con diagonale di pivot, $m = n$ quindi $\min(m,n) = m = n$ chiaramente)

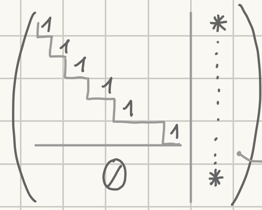
② $rg(A) \leq rg(A|b)$ qualunque sia data una colonna $b \in M_{m,1}(K)$

("aumentando" la matrice, il rango non può diminuire)



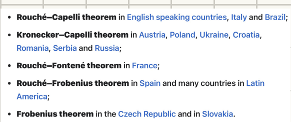
$\underbrace{\hphantom{xxxxxx}}_{A \text{ ridotta}}$

attraverso le operazioni elementari, trasformo A in questa matrice a gradini ridotta



qui può esserci al massimo un pivot in più

faccio le stesse operazioni su $(A|b)$ - visto che si mescolano le righe ma mai le colonne, la parte a sinistra sarà uguale - (A)



- **Rouché–Capelli theorem** in English speaking countries, Italy and Brazil;
- **Kronecker–Capelli theorem** in Austria, Poland, Ukraine, Croatia, Romania, Serbia and Russia;
- **Rouché–Fontené theorem** in France;
- **Rouché–Frobenius theorem** in Spain and many countries in Latin America;
- **Frobenius theorem** in the Czech Republic and in Slovakia.

OK.

se ne deduce che $rg(A) \leq rg(A|b)$

Teorema ROUCHÉ-CAPELLI vedi anche p.98

Si consideri il sistema $(*)\ AX = b$ con $A \in M_{m,n}(K)$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in M_{m,1}(K)$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K)$

① Il sistema $(*)$ è compatibile $\Longleftrightarrow rg(A) = rg(A|b)$

② Se $(*)$ è compatibile, poniamo $s := \overset{\text{colonne (= indeterminate)}}{n} - rg(A) \geq 0$ "grado di libertà" del sistema

Esistono allora $\overset{s}{}$ vettori $v_1, \dots, v_s \in Sol(A|0)$ linearmente indipendenti t.c. $Sol(A|0) = Span_K(v_1, \dots, v_s)$

Quindi, dato $v_0 \in Sol(A|b)$, si ha $Sol(A|b) = v_0 + \sum_{i=1}^{s} \overset{\text{costante}}{K}\, v_i$

parentesi mia x capire meglio:

esempi grado 1

$$\begin{array}{c} \\ \left(\begin{array}{ccc|c} 1 & 2 & 3 & \cdot \\ 0 & 0 & -1 & \cdot \\ 0 & 0 & 0 & \cdot \end{array}\right) \end{array} \qquad \left(\begin{array}{cccc|c} 1 & 0 & 0 & 2 & \cdot \\ 0 & 1 & 3 & 3 & \cdot \\ 0 & 0 & 1 & 5 & \cdot \end{array}\right)$$

ho 3 incognite ma 1 è "libera" (2 sono vincolate)

ho 4 incognite ma 1 è "libera"

(sono le colonne non pivot)

grado 3:
$$\left(\begin{array}{cccccc|c} 1 & * & * & * & * & * & \cdot \\ 0 & 1 & * & * & * & * & \cdot \\ 0 & 0 & 1 & \underbrace{*}_{} & \underbrace{*}_{3} & \underbrace{*}_{} & \cdot \end{array}\right)$$

infatti (esempi di prima)

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & -2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -1 \end{array}\right)$$

(visivamente vedo subito 0 colonne "libere")

$s = n - rg(A)$

$s = 3 - 3$

quindi $Sol(A|0) = Span_K \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \right\} = (0)$

la sol è unica:

$\left\{ \begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix} + \underset{= (0)}{Sol(A|0)} \right\} = \left\{ \begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix} \right\}$

$$\left(\begin{array}{cc|c} 1 & 1 & -2-z \\ 0 & 1 & 2+z \\ 0 & 0 & 3+3z \end{array}\right)$$

se qui c'è 0 va bene perché non ci sono altri pivot e $rg(A) = rg(A|b)$

(quindi se $z = -1$, è compatibile)

se invece $z \neq -1$,

$rg(A) = 2 < 3 = rg(A|b)$ e il sistema è incompatibile

esercizio

studiare le soluzioni del seguente sistema lineare

$$\begin{cases} x_2 - 2x_3 + x_4 - x_5 = 6 \\ x_3 - x_4 = -2 \\ x_1 - x_2 - x_3 - x_4 = 5 \\ x_2 + x_5 = 0 \end{cases}$$

$$\left(\begin{array}{ccccc|c} 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right) \underset{R_1 \longleftrightarrow R_3}{\sim} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right)$$

$$\underset{\substack{R_2 \longleftrightarrow R_3 \\ R_3 \longleftrightarrow R_4}}{\sim} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & -2 \end{array}\right) \underset{R_3 \mapsto R_3 - R_2}{\sim} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 2 & -1 & 2 & -6 \\ 0 & 0 & 1 & -1 & 0 & -2 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 2 & -1 & 2 & -6 \\ 0 & 0 & 1 & -1 & 0 & -2 \end{array}\right)$$

$R_2 = R_3$ di prima
$R_3 = R_4$ " "
$R_4 = R_2$ " "

$$\underset{R_3 \longleftrightarrow R_4}{\sim} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 0 & 0 & 2 & -1 & 2 & -6 \end{array}\right) \underset{R_4 \to R_4 - 2R_3}{\sim} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 2 & -2 \end{array}\right)$$

4 pivot

qui si vede che $rg(A) = rg(A|b) = 4$
quindi, per Rouché-Capelli, il sistema d'origine è compatibile

dopo qualche calcolo $\longrightarrow$ $$\left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 5 & -1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & -4 \\ 0 & 0 & 0 & 1 & 2 & -2 \end{array}\right)$$ a gradini ridotta

il sistema associato è quindi
$$\begin{cases} x_1 + 5x_5 = -1 \\ x_2 + x_5 = 0 \\ x_3 + 2x_5 = -4 \\ x_4 + 2x_5 = -2 \end{cases} \qquad \begin{cases} x_1 = -5x_5 - 1 \\ x_2 = -x_5 \\ x_3 = -2x_5 - 4 \\ x_4 = -2x_5 - 2 \end{cases}$$

da cui
$$Sol(A|b) = \left\{ \begin{pmatrix} -1 \\ 0 \\ -4 \\ -2 \end{pmatrix} + \underbrace{x_5 \begin{pmatrix} -5 \\ -1 \\ -2 \\ -2 \end{pmatrix}}_{\text{soluzioni dell'omogenea associata}} \right\}$$

Abbiamo visto che $\mathrm{Span}_K(v_1, \dots, v_k) \overset{\text{Vett}}{=} \{\alpha_1 v_1 + \dots + \alpha_k v_k : \alpha_1, \dots, \alpha_k \in K\}$ p.80

Più generalmente, se $\emptyset \neq S \subset V$ qualsiasi, si pone $\mathrm{Span}_K(S) = \{$"combinazioni lineari finite di vettori in S"$\}$, ovvero $\mathrm{Span}_K(S) = \bigcap_{\substack{W \text{ sottosp. di } V \\ S \subset W}} W$

- FATTO: $\mathrm{Span}_K(S)$ è un sottospazio vettoriale di V.

  es. $W \subset V$ sottospazio. Allora, $W = \mathrm{Span}_K(W)$

def SISTEMA DI GENERATORI, sottospazio FINITAMENTE GENERATO

- Se $W = \mathrm{Span}_K(S)$, allora S è un sistema di generatori per W.

- Se $\exists$ S finito con $W = \mathrm{Span}_K(S)$, allora W è finitamente generato (f.g.)

  può essere generato ANCHE da un insieme infinito (non ci interessa)

  - quello che conta è che possa essere generato da uno finito

es. $V = \mathbb{R}^2$, $K = \mathbb{R}$, $v = \begin{pmatrix}1\\1\end{pmatrix} \in V$, $S = \{v\}$

$W = \mathrm{Span}_{\mathbb{R}}(\overset{\#S=1}{S}) = \mathrm{Span}_{\mathbb{R}}(v)$ W è f.g.

def sistema di generatori LIBERO

$\emptyset \neq S \subset V$ è libero o linearmente indipendente se, comunque scelto un sottoinsieme finito $F = \{v_1, \dots, v_n\} \subset S$, allora $v_1, \dots, v_n$ sono l.i. (ogni combinazione lineare finita di vettori di S nulla è banale)

def BASE

Dato W sottospazio vett., $S \subset W$ è una base di W se

① S è un sistema di generatori di W, ovvero $W = \mathrm{Span}_K(S)$

② S è libero

Proposizione 1: Per ogni spazio vettoriale V/K ("su K"), esiste una base $\mathcal{B} \subset V$.

Inoltre, date due basi $\mathcal{B}, \mathcal{B}'$ di V, allora esiste una funzione biiettiva $f: \mathcal{B} \to \mathcal{B}'$

quindi in particolare, se esiste una base finita di cardinalità n, allora ogni base è finita, di cardinalità n.

def DIMENSIONE di uno sp. vett.

Dato uno spazio vettoriale V/K f.g., la dimensione $\dim_K(V)$ è l'intero $n \in \mathbb{N}$ tale che ogni base $\mathcal{B}$ di V ha cardinalità n.

N.B. $\dim_V(K) = 0 \iff V$ è banale - $V = (0)$

Proposizione 2: se W è un sottospazio vettoriale di V f.g. di dimensione n, allora anche W è f.g. e, data l la sua dimensione $l := \dim_K(W)$, si ha $l \leq n$

un sottospazio vett. ha sempre dim ≤ dim spazio (che è logico, perché è ⊆)

Applicazione alla notazione di rango di una matrice

Lemma Data una matrice $A \in \mathcal{M}_{m,n}(K)$, $\underset{\#pivot}{rg(A)} = \dim_K(\underbrace{Span_K(A_1, \dots, A_m)}_{\text{sottosp. vett. di } \mathcal{M}_{1,n}(K)})$

(ogni riga è una matrice riga con n colonne)

$Span_K(A_1, \dots, A_n)$ è l'insieme delle comb. lin. delle righe di A,
una base di $Span_K(\dots)$ è un insieme di vettori l.i. che generano $Span_K(\dots)$,
quindi la dim dello span (cardinalità delle basi) è il numero massimo di righe l.i. ⟶ ovvero il rango (se trasformo una matrice in forma a gradini ridotta, le righe l.d. diventeranno nulle)

dim

Sia A' la matrice a gradini ridotta tale che $A \underset{R}{\sim} A'$. Allora, ogni riga di A' è combinazione lineare delle righe di A.
Quindi,

$$Span_K(A'_1, \dots, A'_m) \subset Span_K(A_1, \dots, A_m)$$

ogni el. appartiene a

per la prop. 2, $\dim_K(Span_K(A'_1, \dots, A'_m)) \leq \dim_K(Span(A_1, \dots, A_m))$

Ma ogni trasformazione elementare di Gauss è invertibile ($\underset{R}{\sim}$ è una rel. di equivalenza)
Quindi, $\dim_K(Span_K(A'_1, \dots, A'_m)) = \dim_K(Span_K(A_1, \dots, A_m))$.

Si vede che $\dim_K(Span_K(A'_1, \dots, A'_m)) = rg(A')$ perché le righe contenenti i pivot sono l.i. (lo sp. vett. le ha come base) ∎

Applicazioni alle soluzioni di un sistema lineare (ROUCHÉ-CAPELLI)

Dato un sistema lineare $(*)$ $AX = b$, $M := (A|b)$, $A \in \mathcal{M}_{m,n}(K)$,
il teorema di Rouché-Capelli p.95 si riformula.

① $(*)$ è compatibile $\iff \dim_K(M^1, \dots, M^{n+1}) = \dim_K(A^1, \dots, A^n)$ $(rg(A) = rg(A|b))$

② $\dim_K(\underbrace{Sol(A|0)}_{\text{spazio vett. delle sol. del sistema omogeneo}}) = \underbrace{n - rg(A)}_{s}$ (da teorema: esistono s vettori $v_1, \dots, v_s \in Sol(A|0)$ l.i. t.c. $Sol(A|0) = Span_K(v_1, \dots, v_s)$) quindi $s = $ dim. base)

③ N.B. $rg(A) = \dim_K(Span_K(A_1, \dots, A_m)) = \dim_K(Span_K(A^1, \dots, A^n))$

Esercizi

t sulle slide, ma preferisco X — abbiamo visto che è uno sp. vett. (p.78)

Sia $W = K_d[X]$ il sottoinsieme di polinomi di $V = K[X]$ di grado $\leq d$.

W è un sottosp. vett. di $K[X]$.

1 ⓐ Mostrare che $K_d[X]$ è f.g. e ⓑ calcolarne una base.

f.g.

perché $K_d[X]$ polinomi $\deg \leq d$

ⓐ dato $P \in K_d[X] =: W$, $P = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$ con $a_0, \dots, a_n \in K$ e, se $a_n \neq 0$ allora $n \leq d$

è una comb. lineare di

quindi, $P \in \mathrm{Span}_K(1, x, x^2, \dots, x^d)$ - ovvero, $S = \{1, x, x^2, \dots, x^d\}$ è un sistema di generatori di $K_d[X]$

Siccome S è finito, $K_d[X]$ è f.g.

base

ⓑ bisogna trovare un sistema di generatori l. i.

Un polinomio è nullo $\iff$ i suoi coeff. sono tutti nulli.

Ma un polinomio $\in K_d[X]$ è una comb. lin. di $1, x, x^2, \dots, x^d$, quindi l'unica comb. lineare nulla di $1, x, x^2, \dots, x^d$ è quella banale.

$\Longrightarrow \{1, x, x^2, \dots, x^d\}$ è una base $\Longrightarrow \dim_K(K_d[X]) = d+1$ da $x^0 = 1$ a x^d

- Ma non è l'unica base:

  dato $d = 1$, $S = \{1, x\}$.

  Se sostituisco x con $x+1$ e costruisco $S' = \{1, x+1\}$, S' è un sistema di generatori

$$P = a_0 + a_1 X = a_0 + a_1 \underline{(x+1) - a_1} = \underbrace{(a_0 - a_1)}_{\text{"}a_2\text{"}} \cdot 1 + a_1 (x+1)$$ comb. lineare di 1, $x+1$

$\Longrightarrow \forall P \in K_1[X]$, si ha che $P \in \mathrm{Span}_K(1, x+1) \Longrightarrow K_1[X] \subset \mathrm{Span}_K(1, x+1)$

Sia adesso $Q \in \mathrm{Span}_K(1, x+1) \Longrightarrow Q = b_0 + b_1(x+1) = \underbrace{b_0 + b_1}_{\text{"}b_2\text{"} \cdot 1} + b_1 x \in K_1[X]$ comb. di $(1, x)$

$$\Longrightarrow K_1[X] = \mathrm{Span}_K(1, x+1) = \mathrm{Span}_K(1, x)$$

le comb. di $(1, x+1)$ sono anche comb. di $(1, x)$

1, $x+1$ sono l.i., quindi anche $\{1, x+1\}$ è una base di $K_1[X]$

GENERALIZZANDO

Dato un qualsiasi $\{1, x, x^2, \dots, x^d\}$ base di $K_d[X]$,

se si sostituisce un elemento di questa base con un polinomio di $K_d[X]$ ottenuto:

① permutando ② moltiplicando per uno scalare ③ sostituendo con se stesso più una combinazione lineare degli altri

(operazioni di Gauss)

uscirà un'altra base.

[trovare in $K_3[X]$ un sistema di generatori che non è una base]

per esempio, $\{1, 1, x, x^2, x^3\}$ è un sistema di generatori ($\forall P = a_0 + a_1 x + a_2 x^2 + a_3 x^3$, $P \in Span_K(\{1, x, x^2, x^3\}) \subset Span_K(\{1, 1, x, x^2, x^3\})$)

in generale, se $S \subset S'$, $Span_K(S) \subseteq Span_K(S')$

la comb. lin. $\lambda_1 \cdot 1 + \lambda_2 \cdot 1 + \lambda_3 \cdot x + \lambda_4 \cdot x^2 + \lambda_5 \cdot x^3$

con $\lambda_1 = -\lambda_2 = 1$ e $\lambda_3 = \lambda_4 = \lambda_5 = 0$ è non banale e nulla $\Rightarrow$ $\{1, 1, x, x^2, x^3\}$ non è libero.

$1 \cdot 1 - 1 \cdot 1 + 0 + 0 + 0 = 0$

② Mostrare che $V = K[X]$ non è f.g. e calcolarne una base

Supponiamo per assurdo che V sia f.g.

vorrebbe dire che esiste una base finita di cardinalità n tale che

$V = Span_K(P_0, P_1, \dots, P_n)$, $P_i \in V = K[X]$. (quindi ogni polinomio è comb. lineare di $P_0, \dots, P_n$)

Sia $d = \max(\deg(P_i), i = 0, \dots, n)$ (quindi esisterebbe un grado massimo)

Sia $P \in V$. Allora $P = \sum_{i=0}^{n} \underset{\in K}{\lambda_i} P_i$

il grado massimo che P può avere, visto che λ_i sono costanti (e non possono far aumentare di grado), è

$$\deg(P) \leq \max\{\deg(P_0), \dots, \deg(P_n)\} = d \quad \text{(definito sopra)}$$

Introduciamo un elemento $Q \in V$ con grado $n+1$ (che chiaramente esiste in $K[X]$)

Sia $Q \in V$ di grado $n+1$

Se $Q \in V$, vuol dire che può essere scritto come comb. lin. dei generatori

$Q \in Span_K(P_0, \dots, P_n)$ contraddizione

ma questo è impossibile, perché abbiamo visto sopra che quelle combinazioni hanno grado massimo n.

Quindi, $K[X]$ non è f.g. e ha base $\{1, x, x^2, \dots, x^n, \dots\}$ infinita.

FATTI generalizzati dall'es.

- se $\mathcal{B} = \{b_1, \dots, b_n\}$ è base di V, allora un sottoinsieme $\mathcal{B}' \subset V$ ottenuto attraverso ①, ②, ③ è un'altra base.

- Se $S \subset S'$, $Span_K(S) \subset Span_K(S')$

- $V = K[X]$ non è f.g.

ma fatto l'11/12 (matrice con rango non massimale) ($< \min(n,m)$)

Esercizio 1

$$M = \begin{pmatrix} -2 & 1 & 4 & -3 & -2 \\ 3 & -1 & -1 & 3 & 1 \\ 1 & 0 & 3 & 0 & -1 \\ 4 & 5 & 5 & -6 & 0 \end{pmatrix} \underset{R_4 \to R_4 + 2R_1}{\cup\!\!\!\cap} \begin{pmatrix} -2 & 1 & 4 & -3 & -2 \\ 3 & -1 & -1 & 3 & 1 \\ 1 & 0 & 3 & 0 & -1 \\ 0 & 7 & 13 & -12 & -4 \end{pmatrix} \underset{\substack{R_1 \to R_1 + 2R_3 \\ R_2 \to R_2 - 3R_3 \\ R_1 \leftrightarrow R_3}}{\cup\!\!\!\cap} \begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & -1 & -10 & 3 & 4 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 7 & 13 & -12 & -4 \end{pmatrix} \underset{\substack{R_2 \to R_2 + R_3 \\ R_4 \to R_4 - 7R_3}}{\cup\!\!\!\cap}$$

$$\begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 0 & -57 & * & * \end{pmatrix} \underset{R_3 \to R_2 \to R_4 \to R_3}{\cup\!\!\!\cap} \begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 0 & -57 & * & * \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

quindi rango$(M) = 3$

$=$ dimensione di $W = \mathrm{Span}_{\mathbb{R}}$(righe di M)

e le righe della matrice (l.i.) costituiscono una base di W

Come è stato generato l'esercizio?

scelti 3 vettori l.i a caso

$a = (1\ 2\ 4\ -3\ -1)$, $b = (3\ 1\ 0\ 0\ 1)$, $c = (0\ 2\ 1\ -3\ 0)$ $\in M_{1,5}(\mathbb{R})$

la matrice $\begin{pmatrix} a \\ b \\ c \end{pmatrix} \in M_{3,5}(\mathbb{R})$ ha rango 3 e

$M = \begin{pmatrix} a-b \\ b-c \\ a-c \\ a+b+c \end{pmatrix}$ $a-b$, $b-c$, $a-c$, $a+b+c \in \mathrm{Span}_{\mathbb{R}}(a,b,c) \in M_{1,5}(\mathbb{R})$

Esercizio 2

① In funzione del parametro $\lambda \in \mathbb{R}$, determinare il rango della matrice

$$M_\lambda = \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 2 & 1 & 1 & -2 & \lambda & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{4,7}(\mathbb{R})$$

② Supponiamo che M_λ sia la matrice completa associata ad un sistema lineare $Ax \overset{(*)}{=} b$.
Determinare in funzione di λ se il sistema è compatibile, e la dimensione di $Sol(A|0)$

$$M_\lambda = \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 2 & 1 & 1 & -2 & \lambda & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \underset{R_2 \to R_2 - 2R_4}{\cong} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \underset{R_4 \leftrightarrow R_2}{\cong} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix}$$

dobbiamo capire come trattarlo: è già 0 o deve diventarlo?

ci sono ora due casi: ① $\lambda \neq 0$ ② $\lambda = 0$

① $\lambda \neq 0$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix} \underset{R_3 \to \lambda^{-1} R_3}{\cong}$$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 1 & \frac{4}{\lambda} & \frac{3}{\lambda} & -2 & \frac{6}{\lambda} & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix} \underset{R_3 \to R_3 - R_2}{\cong}$$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & \frac{4}{\lambda}-2 & \frac{3}{\lambda}+1 & -2 & \frac{6}{\lambda}-1 & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix}$$

se $\lambda = 2$, è 0, altrimenti no

abbiamo ancora due casi:
- (1a) $\lambda \neq 2, 0$
- (1b) $\lambda = 2$

② $\lambda = 0$

$$M_0 \underset{\substack{\text{sostituiamo} \\ \lambda = 0}}{\cong} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 3 & 0 & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & -2 & 4 \end{pmatrix} \underset{R_4 \to -\frac{1}{3} R_4}{\cong}$$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 3 & 0 & 6 & 4 \\ 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} & -\frac{4}{3} \end{pmatrix} \underset{R_3 \to R_3 - 4R_4}{\cong}$$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 7 & * & * & * \\ 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} & -\frac{4}{3} \end{pmatrix} \underset{\substack{R_3 \to \frac{1}{7} R_3 \\ R_3 \leftrightarrow R_4}}{\cong}$$

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

rango 4

① a) $\lambda \neq 0, \ \lambda \neq 2$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & \frac{4}{\lambda}-2 & \frac{3}{\lambda}-1 & -2 & \frac{6}{\lambda}-1 & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix} \sim \quad R_3 \to R_3 \cdot \frac{1}{\frac{4}{\lambda}-2}$$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3+\lambda}{4-2\lambda} & \frac{-2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix} \sim \quad R_4 \to R_4 + 3R_3$$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3+\lambda}{4-2\lambda} & \frac{-2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & 0 & \frac{21-3\lambda}{4-2\lambda} & \frac{-4-\lambda}{2-\lambda} & * & * \end{pmatrix}$$

↳ se questi due si annullano contemporaneamente (e anche gli *) allora il rango è 3 - sennò, è 4

$\frac{21-3\lambda}{4-2\lambda}$ si annulla $\iff \lambda = 7$, e $\frac{-4-\lambda}{2-\lambda}$ non si annulla per $\lambda = 7$

quindi non possono essere cont nulli $\implies$ rango$(M_\lambda) = 4$

① b) $\lambda = 2$

$$M_2 \sim \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{5}{2} & -2 & * & * \\ 0 & 0 & -3 & * & * & * & * \end{pmatrix} \sim \quad \begin{array}{l} R_3 \to \frac{2}{5} R_3 \\ R_4 \to -\frac{1}{3} R_4 \\ R_3 \leftrightarrow R_4 \end{array}$$

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

rango$(M_2) = 4$

in ogni caso, rango$(M_\lambda) = 4$

② In ogni caso rg(M) è 4. Scriviamo

$$M_\lambda = \left.\left(\underbrace{A_\lambda}_{6} \ \middle| \ \underbrace{B_\lambda}_{1} \right)\right\} 4$$

il sistema (*) è compatibile $\iff$ rg$(A) = $ rg(M)

devo verificare per ogni caso che i gradini "finiscano" prima di B

① a) → può essere o così:

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3+\lambda}{4-2\lambda} & \frac{-2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & 0 & \frac{21-3\lambda}{4-2\lambda} & \frac{-4-\lambda}{2-\lambda} & * & * \end{pmatrix} \quad \text{se } \lambda = 7$$

o così:

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3+\lambda}{4-2\lambda} & \frac{-2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & 0 & \frac{21-3\lambda}{4-2\lambda} & \frac{-4-\lambda}{2-\lambda} & * & * \end{pmatrix} \quad \text{se } \lambda = 7$$

① b)

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

②

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

rg$(A) = $ rg(M) si verifica in tutti i casi

• Per Rouché-Capelli, $\dim(\mathrm{Sol}(A|0)) = \underbrace{n}_{\substack{\text{(di A)} \\ \text{\# indeterminate}}} - \overset{M_\lambda}{\mathrm{rg}(A)} = 6 - 4 = 2$

Si verifica che prop 1, prop 2 $\Longrightarrow$

se W sott. vett. di V f.g. di dim n, allora anche W è f.g. di dim $l \leq n$

per ogni V/K $\exists$ base $\mathcal{B} \subset V$ (e se una base è finita di card. n, ogni base lo è)

versione alternativa a p. 109

Proposizione 3: Dato V sp. vett. di dim. n su K, sia $S \subset V$.

ricordo: ha basi con card. n

Allora:

① S è libero $\Longrightarrow \#S < \infty$ e $\#S \leq n$ se le basi hanno card. n, non può avere card $k > n$

② S generatore $\Longrightarrow$ o S è infinito
oppure $\#S \geq n$

③ in particolare, S base $\Longleftrightarrow S$ finito, $\#S = n$ e S libero $\Longleftrightarrow \#S < \infty$, $\#S = n$ e S è generatore

Proposizione 4: Dato V spazio vettoriale f.g. su K,
$\{v_1, \dots, v_n\}$ è una base di V $\Longleftrightarrow$ ogni vettore di V si scrive in modo unico come combinazione lineare di $v_1, \dots, v_n$

dim

- $\Longrightarrow$ Se $\{v_1, \dots, v_n\}$ è base di V, allora è anche insieme di generatori. $\forall v \in V$, $v \in \mathrm{Span}_K(v_1, \dots, v_n)$

  Quindi $\exists\, \alpha_1, \dots, \alpha_n \in K$ t.c. $v = \alpha_1 v_1 + \dots + \alpha_n v_n$

  Inoltre, $v_1, \dots, v_n$ sono l.i.

  Mostriamo che $(\alpha_1, \dots, \alpha_n) \in K^n$ è unicamente determinato

  Supponiamo di avere $(\beta_1 \dots \beta_n) \in K^n$ t.c. $v = \beta_1 v_1 + \dots + \beta_n v_n$

  Si ha quindi: $v = \beta_1 v_1 + \dots + \beta_n v_n$, $v = \alpha_1 v_1 + \dots + \alpha_n v_n$

  Sottraiamo: $0 = (\beta_1 - \alpha_1) v_1 + \dots + (\beta_n - \alpha_n)$

  l'unica comb. nulla è quella banale

  Ma $v_1 \dots v_n$ sono l.i $\Longleftrightarrow \beta_1 = \alpha_1, \dots, \beta_n = \alpha_n$ da cui l'unicità

- $\Longleftarrow$ Supponiamo che $\forall v \in V$, si possa scrivere in modo unico $v = \alpha_1 v_1 + \dots + \alpha_n v_n$

  Allora $\{v_1, \dots, v_n\}$ genera V: $V = \mathrm{Span}_K(v_1, \dots, v_n)$

  Inoltre, per unicità $0 = \alpha_1 v_1 + \dots + \alpha_n v_n$
  $$0 = 0 v_1 + \dots + 0 v_n \Longrightarrow v_1, \dots, v_n \text{ l.i.} \quad \blacksquare$$

def VETTORE DELLE COORDINATE

- Dato V spazio vettoriale su K di dim. n, e data una base $\mathcal{B} = \{b_1, \dots, b_n\}$, ogni vettore $v \in V$ si scrive in modo unico:

$$v = v_1 b_1 + \dots + v_n b_n \qquad \text{con} \quad \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n$$

Tale vettore si chiama il vettore delle coordinate di v nella base $\mathcal{B}$, e si scrive $[v]_{\mathcal{B}}$

esempi di basi:

① $V = K = \mathbb{C}$ ogni singleton non nullo è una base - $\dim_{\mathbb{C}}(\mathbb{C}) = 1$

es. $\{1\}$ è una base

② $V = \mathbb{C}$, $K = \mathbb{R}$ sappiamo che ogni numero complesso $z \in \mathbb{C}$ si scrive in modo unico come $z = x \cdot 1 + y \cdot i$

$1, i$ vettori di $\mathbb{C}$, $x, y \in \mathbb{R}$ (quindi comb. lineare)

quindi $B = \{1, i\}$ è base - $\dim_{\mathbb{R}}(\mathbb{C}) = 2$

③ in modo simile,

$\dim_{\mathbb{C}}(M_2(\mathbb{C})) = 4$ con base $\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}\right\}$

dim: · chiaro che A B C D sono l.i.

· $\forall M \in M_2$, $M = \begin{pmatrix}a&b\\c&d\end{pmatrix} = a\begin{pmatrix}1&0\\0&0\end{pmatrix} + b\begin{pmatrix}0&1\\0&0\end{pmatrix} + c\begin{pmatrix}0&0\\1&0\end{pmatrix} + d\begin{pmatrix}0&0\\0&1\end{pmatrix}$

$\dim_{\mathbb{R}}(M_2(\mathbb{C})) = 8$ con base $\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}i&0\\0&0\end{pmatrix}\begin{pmatrix}0&i\\0&0\end{pmatrix}\begin{pmatrix}0&0\\i&0\end{pmatrix}\begin{pmatrix}0&0\\0&i\end{pmatrix}\right\}$

dim · sempre chiaro l.i.

· $\forall M \in M_2$, $M = \begin{pmatrix}a_1&a_2\\a_3&a_4\end{pmatrix} = x_1\begin{pmatrix}1&0\\0&0\end{pmatrix} + y_1\begin{pmatrix}i&0\\0&0\end{pmatrix} + \ldots$ uguale per a_2, a_3, a_4

$a_j = x_j \cdot 1 + y_j \cdot i$; quindi:

Esercizio 3 / base canonica

dato $V = K^n$, allora $B = (e_1, \ldots, e_n)$ è una base di V

dove $e_1 = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$, $e_2 = \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}$, $\ldots$, $e_i = \begin{pmatrix}0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix}$ i-esima posizione, $e_n = \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}$

dim

Scriviamo la matrice M che ha per righe i coefficienti dei vettori $e_1, \ldots, e_n$.

Si ha $M = \begin{pmatrix}1 & & & \emptyset\\ & 1 & & \\ & & \ddots & \\ \emptyset & & & 1\end{pmatrix} = 1_n \in M_n(K)$ a gradini ridotta con n pivot. $rg(M) = n$ da cui B libera (rango = cardinalità B)

e, siccome $W = \operatorname{Span}_K(B) \subset V$ ha dim. n, $W = V$ e B base di V ■

è $\dim(K^n) = n$

def BASE CANONICA

La base $B = (e_1, \ldots, e_n)$ si chiama la base canonica di K^n

· $\{e_{ij} : {1 \le i \le m \atop 1 \le j \le n}\}$ è la base canonica di $M_{m,n}(K)$

Esercizio 4

In $\mathcal{M}_{m,n}(K)$, ponendo $e_{ij} = \begin{array}{cc} & \text{colonna } j \\ \left(\begin{array}{c|c} \emptyset & \emptyset \\ & 1 \\ \hline \emptyset & \emptyset \end{array}\right) & \text{riga } i \end{array} \in \mathcal{M}_{m,n}$ con $\begin{smallmatrix} 1 \leq i \leq m \\ 1 \leq j \leq n \end{smallmatrix}$ [esempio: $m=2$, $n=3$ $e_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$]

mostrare che $\left\{ e_{ij} : \begin{smallmatrix} 1 \leq i \leq m \\ 1 \leq j \leq n \end{smallmatrix} \right\}$ è la base canonica di $\mathcal{M}_{m,n}(K)$ e che $\dim(\mathcal{M}_{m,n}(K)) = m \cdot n$

Esercizio 5

dato $V = \mathbb{R}^2$, mostrare che $B = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$ è una base di V.

ci sono 2 metodi: (sappiamo che $2 = \# B = \dim_{\mathbb{R}}(V)$)

① usando la prop. 3 (S base $\iff \# S = n$ e S libero $\iff \underbrace{\# S = n \text{ e } S \text{ è generatore}}_{\text{usiamo questo}}$)

Mostriamo che $\forall \begin{pmatrix} a \\ b \end{pmatrix} \in V$, si ha che $\begin{pmatrix} a \\ b \end{pmatrix}$ è combinazione dei vettori $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ (ovvero che $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathrm{Span}_{\mathbb{R}}(B)$)

$$x_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \quad \exists\, x_1, x_2 \in \mathbb{R} \iff \text{il sistema } \begin{cases} x_1 + x_2 = a \\ x_1 - x_2 = b \end{cases} \text{ è compatibile.}$$

Per Rouché - Capelli, il sistema è compatibile $\iff rg(A) = rg(A|\begin{smallmatrix} a \\ b \end{smallmatrix})$

$$\begin{pmatrix} 1 & 1 & a \\ 1 & -1 & b \end{pmatrix} \underset{L_2 \to L_2 - L_1}{\cong} \begin{pmatrix} 1 & 1 & a \\ 0 & -2 & b-a \end{pmatrix} \underset{L_2 \to -\frac{1}{2} L_2}{\cong} \underline{\begin{pmatrix} 1 & 1 & a \\ 0 & 1 & \frac{a-b}{2} \end{pmatrix}} \underset{L_1 \to L_1 - L_2}{\cong} \underset{\text{(ridotta)}}{\begin{pmatrix} 1 & 0 & \frac{a+b}{2} \\ 0 & 1 & \frac{a-b}{2} \end{pmatrix}}$$

$\hookrightarrow rg(A) = rg(A|b) \implies \mathbb{R}^2 = \mathrm{Span}_{\mathbb{R}}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right)$

inoltre, ho le soluzioni uniche del sistema $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{a+b}{2} \\ \frac{a-b}{2} \end{pmatrix}$

quindi, scrivendo $v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ si ha $\underset{\text{vett. coordinate}}{[v]_B} = \begin{pmatrix} \frac{a+b}{2} \\ \frac{a-b}{2} \end{pmatrix}$

② usando la prop. 3 (S base $\iff \underbrace{\# S = n \text{ e } S \text{ libero}}_{\text{usiamo questo}} \iff \# S = n$ e S è generatore)

Mostriamo che B è libero (metodo più facile)

$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cong \begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix} \cong \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, che ha rango 2. Le righe contenenti i pivot sono l.i., quindi B è libera.

Quindi sappiamo che è una base di V.

Trasposizione di matrici

Sia $A \in \mathcal{M}_{m,n}(K)$, la **trasposta** di A $({}^tA)$ è la matrice di $\mathcal{M}_{m,n}(K)$ ottenuta da A scambiando righe e colonne.

$$A = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} \quad , \quad {}^tA = (a_{ji})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

$$A = \begin{pmatrix} \boxed{1} & 2 \\ \boxed{3} & 4 \\ \boxed{5} & 6 \end{pmatrix} \in \mathcal{M}_{3,2}(\mathbb{R}) \quad , \quad {}^tA = \begin{pmatrix} \boxed{1 \; 3 \; 5} \\ 2 \; 4 \; 6 \end{pmatrix} \in \mathcal{M}_{3,2}(\mathbb{R})$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R}) \quad , \quad {}^tA = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

è una riflessione rispetto alla diagonale

(per le non-quadrate: $\begin{pmatrix} * & * \\ * & * \\ * & * \\ * & * \end{pmatrix}$)

oss (importante!) dato $A \in \mathcal{M}_{m,n}(K)$ $\quad rg(A) = rg({}^tA)$

quindi, se cerco il rango tramite Gauss, posso accelerare applicando l'algoritmo a righe e colonne simultaneamente

(ma se lo faccio, non posso trarre conclusioni sulle soluzioni del sistema associato - neanche se la riduco -)

proprietà:

① ${}^t({}^tA) = A$

② ${}^t(\alpha A + \beta B) = \alpha {}^tA + \beta {}^tB$ $\quad$ con $\alpha, \beta \in K$ e $A, B \in \mathcal{M}_{m,n}(K)$

③ ${}^t(AB) = {}^tB \, {}^tA$ $\quad$ (un po' come l'inversione nei gruppi)

ricordiamo le condizioni di compatibilità per il prodotto matriciale

$A \in \mathcal{M}_{m,n}(K)$, $B \in \mathcal{M}_{n,s}(K)$ - è ben definito anche per ${}^tB \in \mathcal{M}_{s,n}(K)$, ${}^tA \in \mathcal{M}_{n,m}(K)$

Inoltre, ${}^t(AB) \in \mathcal{M}_{s,m}(K)$.

def MATRICE SIMMETRICA/ASIMMETRICA

$A \in \mathcal{M}_n(K)$ (quindi quadrata) si dice **simmetrica** se $A = {}^tA$

antisimmetrica se $A = -{}^tA$

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 4 & 1 \\ 0 & 1 & 3 \end{pmatrix} \in \mathcal{M}_3 \text{ è simmetrica} \quad , \quad A = \begin{pmatrix} 0 & 4 \\ -4 & 0 \end{pmatrix} \text{ è antisimmetrica}$$

- In $\mathcal{M}_n(\mathbb{R})$, $A = -{}^tA \implies$ diagonale nulla

  falso in $\mathcal{M}_n(\mathbb{F}_2)$

Lemma /Esercizio 6/

Sia $\mathcal{M}_n^+(\mathbb{R})$ l'insieme delle matrici simmetriche di $\mathcal{M}_n(\mathbb{R})$ e $\mathcal{M}_n^-(\mathbb{R})$ l'insieme delle matrici antisimmetriche.
$\mathcal{M}_n^+(\mathbb{R})$ e $\mathcal{M}_n^-(\mathbb{R})$ sono sottospazi vettoriali di $\mathcal{M}_n(\mathbb{R})$

dim

Poniamo $M = \mathcal{M}_n^+(\mathbb{R})$ (e poi $M = \mathcal{M}_n^-(\mathbb{R})$)
Dobbiamo dimostrare che $\forall\, A, B \in M$ e $\alpha, \beta \in \mathbb{R}$,

$$\alpha A + \beta B \in M$$

per $\mathcal{M}^+$ A, B sono simmetriche : $A = {}^tA$, $B = {}^tB$
quindi ${}^t(\alpha A + \beta B) = \alpha\, {}^tA + \beta\, {}^tB = \alpha A + \beta B$

per $\mathcal{M}^-$ $A = {}^t{-A}$, $B = {}^t{-B}$
quindi ${}^t(\alpha A + \beta B) = \alpha(-A) + \beta(-B) = -(\alpha A + \beta B)$

Esercizio 7

Trovare basi per $\mathcal{M}_2^+(\mathbb{R})$ e $\mathcal{M}_2^-(\mathbb{R})$

① $\mathcal{M}_2^+(\mathbb{R})$

Sia $A \in \mathcal{M}_2^+(\mathbb{R})$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2^+(\mathbb{R})$ generica

$$V := \mathcal{M}_2^+(\mathbb{R}) = \operatorname{Span}_{\mathbb{R}}\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{= e_{11}} + b \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{= e_{22}} + c \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{= e_{21} + e_{12}}$$

② $\mathcal{M}_2^-(\mathbb{R})$

$A = {}^t{-A}$, $A = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} \in \mathcal{M}_2^-(\mathbb{R})$ generica

$$V = \mathcal{M}_2^-(\mathbb{R}) = \operatorname{Span}_{\mathbb{R}}\left(\underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{= e_{12} - e_{21}} \right)$$

Proposizione 3 versione alternativa - parte ③

Dato V/K s.v. f.g. e $B = \{v_1, \dots, v_n\} \subset V$

B è una base $\iff$ B è un insieme massimale di vettori l.i. $\iff$ B è un insieme minimale di generatori

↳ se aggiungo un altro vettore, non è più libero

dim ② $\implies$ ①

Prendiamo $B = \{v_1, \dots, v_n\}$ libero massimale

Sia $v \in V$. Allora $B' = \{\underbrace{v_1, \dots, v_n, v}_{\text{aggiungo } v}\}$ non è libero (perché B massimale)

$\exists\, \lambda, \lambda_1, \dots, \lambda_n \in K$ non tutti nulli t.c. $\lambda v + \lambda_1 v_1 + \dots + \lambda_n v_n = 0$

e quindi $\lambda v = \lambda_1 v_1 + \dots + \lambda_n v_n$

└ sarebbero $-\lambda_1, \dots, -\lambda_n$, ma è come scegliere un $\lambda' = -\lambda$

Claim: λ non nullo

Altrimenti, $\lambda = 0$ e ci sarebbero $\lambda_1 v_1, \dots, \lambda_n v_n$ non tutti nulli t.c. $0 = \lambda_1 v_1 + \dots + \lambda_n v_n$

(contraddizione con B libero)

Quindi (visto $\lambda \neq 0$) posso moltiplicare per λ^{-1}

$$v = \frac{\lambda_1}{\lambda} v_1 + \dots + \frac{\lambda_n}{\lambda} v_n = u_1 v_1 + \dots + u_n v_n$$

$\implies v \in \mathrm{Span}_K(B)\ \forall v \in V$

$\implies V \subset \mathrm{Span}_K(B) \subset V \implies V = \mathrm{Span}_K(B)$

$\implies B$ è un sistema di generatori per V

Teorema (concetto già visto prima)

Dato V/K f.g., due basi hanno lo stesso numero di elementi

dim

Prendiamo due basi $B = (b_1, \dots, b_r)$, $B' = (b'_1, \dots, b'_{r'})$ due basi.

Posso supporre che $r' \geq r$.

In particolare, $\mathrm{Span}_K(B) = \mathrm{Span}_K(B') = V$

quindi $\mathrm{Span}_K(B) \supset \mathrm{Span}_K(B')$

quindi posso scrivere, in modo unico, $\forall 1 \leq i \leq r'$ $\; b'_i = \sum_{j=1}^{r} \underset{\in K}{u_{ij}}\, b_j$ — sto scrivendo ogni el. di B' nella base B

Costruisco quindi una matrice in questo modo:

- nella parte sinistra, ogni riga i è formata dalle coord. di b'_i nella base B, $[b'_i]_B$
- la parte destra contiene la matrice identità di $\mathcal{M}_{r'}(K)$ → $\underbrace{\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}}_{r'} \Big\}\, r'$

$$M = \left(\begin{array}{c|c} \underbrace{(u_{ij})_{\substack{1 \leq i \leq r' \\ 1 \leq j \leq r}}}_{r} & \underbrace{\mathbb{1}_{r'}}_{r'} \end{array} \right) \Big\}\, r' \qquad M \in \mathcal{M}_{r', r+r'}$$

Applichiamo ora le operazioni elementari di Gauss per rendere solo la parte sinistra a gradini ridotta

che può essere un rettangolo così $\underset{r}{\square}^{r'}$ (se $r < r'$) o al massimo un quadrato ($r = r'$)

(non può essere così $\underset{r}{\square}^{r'}$ - avremmo $r > r'$)

Riducendo M otteniamo una cosa del genere

$$\left(\begin{array}{ccccccc|c} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & * \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ \hline & & & \emptyset & & & & \end{array}\right)$$

Ad ogni tappa, le matrici intermedie hanno il blocco di sx costituito da coordinate nella base B di vettori di una base di V con r' elem.

(applicando le op. fondamentali su delle basi si ottengono sempre basi)

Ma, se ci fosse questo blocco di zeri, staremmo dicendo che un blocco di vettori che contiene zeri è una base → CONTRADDIZIONE

$\hookrightarrow b'_x = \emptyset \cdot b_1 + 0 \cdot b_2 \cdots = \emptyset$

Una base non contiene mai $\emptyset$ (altrimenti non sarebbe libera)

$\hookrightarrow$ la combo $(\forall x \in K)\ \underset{\vee}{x \cdot \emptyset} + 0 \cdot v_1 + 0 \cdot v_2 + \ldots + 0 \cdot v_n$ non è nulla ma darebbe $\emptyset$

(tutti zeri e un numero qualunque al vettore $\emptyset$)

perché non ci siano righe nulle, la parte di sx deve essere quadrata

quindi, $r = r'$ ∎

(MATRICE INVERSA)

Analizziamo la situazione con $r = r'$

- matrice iniziale:

$$r \left\{ \left(\underbrace{A}_{r} \;\middle|\; \underbrace{1_r}_{r} \right) \right.$$

sempre coord. vettori di B' nella base B

ogni riga dà le coordinate di b'_i nella base B'

(nella base B', b'_1 ha coord. $1\ 0 \ldots 0$, $b'_1 = 1 \cdot b'_1 + 0 \cdot b'_2 + 0 \cdot b'_3 + \ldots$)

$b'_2 = 0 \cdot b'_1 + 1 \cdot b'_2 + 0 \cdot b'_3 \ldots$ ecc.

(sia C una base di V, $C = \{v_1, \ldots, v_n\}$

$[v_i]_C = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e_i$ perché $v_i = 0 \cdot v_1 + 0 \cdot v_2 + \ldots + 1 \cdot v_i + \ldots + 0 \cdot v_n$)

Alla fine dell'algoritmo (rendendo la parte di sx a gradini ridotta) si ottiene:

$$\left(1_r \;\middle|\; A' \right)$$

matrice quadrata a gradini ridotta diventa 1_r

il contrario di prima

dove le righe di A' sono le coordinate dei vettori della base B nella base B'

e si osserva che A è invertibile di inversa A'.

(quindi, per trovare l'inversa di una matrice: • si giustappone la matrice identità

• si applica l'algoritmo di Gauss per ridurre la matrice originale (a gradini ridotta) • la matrice giustapposta è l'inversa)

esercizio

$U = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 2 & 1 \\ 1 & 0 & -1 \end{pmatrix}$ calcolare l'inverso (se esiste)

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 \end{array}\right) \underset{\substack{R_2 \to R_2 - 3R_1 \\ R_3 \to R_3 - R_1}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -4 & -2 & -3 & 1 & 0 \\ 0 & -2 & -2 & -1 & 0 & 1 \end{array}\right) \underset{R_3 \to -\frac{1}{2} R_3}{\sim} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -4 & -2 & -3 & 1 & 0 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \end{array}\right) \underset{R_2 \to R_2 + 4R_3}{\sim} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & -1 & 1 & -2 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \end{array}\right) \underset{\substack{R_2 \leftrightarrow R_3 \\ R_3 \to \frac{1}{2} R_3}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array}\right)$$

$$\underset{\substack{R_1 \to R_1 - R_3 \\ R_2 \to R_2 - R_3}}{\sim} \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & \frac{3}{2} & -\frac{1}{2} & 1 \\ 0 & 1 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array}\right) \underset{R_1 \to R_1 - 2R_2}{\sim} \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & \boxed{\begin{matrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ 1 & -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & -1 \end{matrix}} \\ 0 & 0 & 1 & \end{array}\right)$$

inverso di U

Dalla discussione appena conclusa, traspare:

Teorema:

Data $A \in M_n(K)$, c'è equivalenza tra: importante! × calcolare basi o invertibili

① $A \in GL_n(K)$ (A invertibile)

② $\text{rango}(A) = n$ (se le righe sono l.i. e ce ne sono n, esse sono base di K^n - perché $\dim(K^n) = n$ e, per la prop. 3, S base $\iff$ $\#S = n$, S libero)

③ le righe di A sono una base di K^n

④ le colonne di A sono una base di K^n — da questo deduciamo:

OSS: data una matrice M invertibile, anche la sua trasposta ${}^tM$ è invertibile (di inversa ${}^t(M^{-1})$)

OSS: esiste una nozione di determinante

$$\det: M_n(K) \longrightarrow K$$ per ora descritta solo per $n=2$

- si dimostra ⑤ $A \in M_n(K)$ è invertibile $\iff \det(A) \in K^\times$

(c'è una formula universale — data $A = (a_{ij})_{1 \le i,j \le n} \in M_n(K)$

$$\det(A) = \sum_{\sigma \in S_n} \underbrace{\varepsilon(\sigma)}_{\in \pm 1} a_{1\sigma(1)} \dots a_{n\sigma(n)})$$

def APPLICAZIONE LINEARE

Dati V, V' due sp. vett. /K, un'applicazione $V \xrightarrow{f} V'$ è detta **lineare** se $\forall v, v' \in V$ e $\forall \alpha, \alpha' \in K$,

si ha $f(\alpha v + \alpha' v') = \alpha f(v) + \alpha' f(v')$ (come un omomorfismo)

prodotto scalare di V — addiz. in V — prodotto scalare di V' — addiz. in V'

(un'applicazione lineare di spazi vettoriali è un'omomorfismo di gruppi)

gli spazi vettoriali sono gruppi abeliani con op. di somma vettoriale

- Se inoltre f è biiettiva, si dice **isomorfismo**

(e se f è un isomorfismo, anche f^{-1} è un isomorfismo)

Proposizione

Dati V/K f.g., $B = \{b_1, \dots, b_n\}$ base di V, V' s.v. qualsiasi /K, e $f: B \longrightarrow V'$

allora $\exists !$ applicazione lineare $\tilde{f}: V \longrightarrow V'$ t.c. $\tilde{f}\big|_B = f$ (restrizione su B)

dim

Siccome B è base, $\forall v \in V$, $\exists ! \, (\alpha_1 \dots \alpha_n) \in K^n$ t.c. $v = \sum_{i=1}^n \alpha_i b_i$

vett. coordinate su B, $[v]_B$

Poniamo $\tilde{f}(v) = \sum_{i=1}^n \alpha_i f(b_i)$ — è un'applicazione $V \xrightarrow{\tilde{f}} V'$ (per unicità di $[v]_B$ → quindi il valore $\tilde{f}(v)$ dipende solo da v)

① Mostriamo che $\tilde{f}$ è lineare

dati $v, v' \in V$, $\beta, \beta' \in K$, calcolo $\tilde{f}(\beta v + \beta' v') \overset{?}{=} \beta \tilde{f}(v) + \beta' \tilde{f}(v')$

- Calcoliamo $[v]_B = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$, $[v']_B = \begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix}$

$v = \sum_{i=1}^n \alpha_i b_i$, $v' = \sum_{i=1}^n \alpha'_i b_i$, $\beta v + \beta' v' = \sum_{i=1}^n (\beta \alpha_i + \beta' \alpha'_i) b_i$

- $\tilde{f}(\beta v + \beta v') = \sum_{i=1}^n (\beta \alpha_i + \beta' \alpha'_i) f(b_i)$ =

- $\beta \tilde{f}(v) + \beta' \tilde{f}(v') = \beta \sum_{i=1}^n \alpha_i \tilde{f}(b_i) + \beta' \sum_{i=1}^n \alpha'_i \tilde{f}(b_i) = \sum_{i=1}^n (\beta \alpha_i + \beta' \alpha'_i) \tilde{f}(b_i)$ quindi $\tilde{f}$ lineare

② Mostriamo l'unicità

supponiamo che $\exists\, \hat{f}: V \to V'$ lineare t.c. $\hat{f}(b_i) = \tilde{f}(b_i) = f(b_i)$

e mostriamo che $\hat{f} = \tilde{f}$ ovvero che $\hat{f} - \tilde{f} = \emptyset$.

- Poniamo $g = \tilde{f} - \hat{f}$.

$$g(v) = g\left(\sum_{i=0}^{n} \alpha_i b_i\right) = \sum_{i=1}^{n} \alpha_i\, g(b_i) = \sum_{i=1}^{n} \alpha_i \big(\underbrace{\tilde{f}(b_i) - \hat{f}(b_i)}_{=\emptyset}\big) = \emptyset \implies g \equiv \emptyset$$

$$\implies \hat{f} = \tilde{f} \quad \blacksquare$$

esempio

dato $V/\mathbb{R}$ di base $B = (b_1 \ldots b_n)$, $V' = \mathbb{R}^n$, $\dim(V) = \dim(V') = n$

- dato $v \in V$, posso scrivere in modo unico $v = \sum_{i=1}^{n} \alpha_i b_i$.

poniamo $f(b_i) = e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ pos. i

$$\tilde{f}(v) = \sum_i \alpha_i\, f(b_i) = \sum_i \alpha_i\, e_i = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = [v]_B$$

OSS:

$\tilde{f}$ è un isomorfismo di spazi vettoriali di inverso $\tilde{f}^{-1}\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} := \sum_{i=1}^{n} \alpha_i b_i \in V$

ABUSO DI NOTAZIONE: se $\tilde{f}$ prolunga $f: B \to V$, allora scriviamo $f = \tilde{f}$

Corollario

Se $\dim_K(V) = n$, allora $f: V \to K^n$ è un isomorfismo

Immagine e nucleo (def)

data $f: V \to V'$ applicazione lineare, poniamo

- $\mathrm{Ker}(f) = \{ v \in V \text{ t.c. } f(v) = \emptyset \} = f^{-1}(\{\emptyset\})$ nucleo
- $\mathrm{Im}(f) = \{ v' \in V' : \exists\, v \in V \text{ t.c. } f(v) = v' \}$ immagine

Lemma

$\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ sono sottospazi vettoriali di V e V' rispettivamente

dim:

È chiaro che si tratta di sottogruppi visto che f è anche omom. di gruppi. V, V' sono gruppi abeliani con op. addizione vettoriale

Rimane da mostrare che $\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ sono stabili per il prodotto scalare

$\mathrm{Ker}(f)$:

- Siano $v \in V$, $\alpha \in K$: sappiamo che $f(v) = \emptyset$. $\alpha f(v) = \alpha\emptyset = \emptyset$ (è stabile)

$v \in \mathrm{Ker}(f) \implies \alpha v \in \mathrm{Ker}(f) \implies \mathrm{Ker}(f)$ è un sottosp. vett. (definizione 1 sottosp. vett.: $\mathrm{Ker}(f) < V$ e $\underset{\in K}{\lambda} v \in \mathrm{Ker}(f)$)

$Im(f)$:

- Siano $v' \in V'$, $\alpha \in K$: $\exists v \in V$ t.c. $f(v) = v' \implies \alpha f(v) = \alpha v'$.

  ma $\alpha f(v) = f(\alpha v) \implies$ il vettore $\alpha v \in V$ è tale che $f(\alpha v) = \alpha v' \implies \alpha v' \in Im(f) \implies Im(f)$ è un sottosp. vett. di V'.

OSS: Visto che un omomorfismo è iniettivo solo se il nucleo è banale, lemma p.60

$$Ker(f) = \{\emptyset\} \iff f \text{ iniettiva}$$

inoltre, $Im(f) = V' \iff f$ suriettiva

intersezione/unione di sottosp. vett.

- In modo simile, se V_1, V_2 sottosp. vett. di V, allora $V_1 \cap V_2$ sottosp. vett. di V
  (come per i sottogruppi)

- $V_1 \cup V_2$ non è un sottosp. vett.

def <u>SOMMA DI SOTTOSP. VETT.</u>

Dati V_1, V_2 sottospazi vettoriali di V.

Definiamo

$$V_1 + V_2 = \{ v \in V : \exists v_1 \in V_1, v_2 \in V_2 \text{ t.c. } v = v_1 + v_2 \}$$

Si ha che $V_1 + V_2$ è un sottospazio vettoriale.

dim: siano $v, v' \in V_1 + V_2$ e $\alpha, \alpha' \in K$.

voglio mostrare che $\alpha v + \alpha' v' \in V_1 + V_2$

- visto che $v \in V_1 + V_2$, $v = v_1 + v_2$ con $v_1 \in V_1$, $v_2 \in V_2$

  $v' \in V_1 + V_2$, $v' = v'_1 + v'_2$ con $v'_1 \in V_1$, $v'_2 \in V_2$

$$\alpha v + \alpha' v' = \alpha(v_1 + v_2) + \alpha'(v'_1 + v'_2) = \underbrace{(\alpha v_1 + \alpha' v'_1)}_{\in V_1} + \underbrace{(\alpha v_2 + \alpha' v'_2)}_{\in V_2} \in V_1 + V_2$$

Proprietà $V_1 + V_2 = \bigcap_{\substack{W \text{ s.v. di } V \\ W \supset V_1 \cup V_2}} W$ più piccolo sottospazio vettoriale di V che contiene V_1 e V_2

Teorema Formula di Grassmann

$$\dim(V_1) + \dim(V_2) = \dim(V_1 \cap V_2) + \dim(V_1 + V_2)$$

non l'ho fatto a lezione ma può essere utile

Teorema: dato un'appl. lineare $V \xrightarrow{f} V'$ con $\dim(V) = n$,

$$\dim(Ker(f)) + \dim(Im(f)) = n$$

Fine del programma

mancano solo scritto e orale ora! yay

(seguono esercizi sugli spazi vettoriali svolti durante le ultime lezioni)

Esercizio 2. Dati i seguenti insiemi di vettori, si dica in ciascun caso, motivando la risposta, se essi sono :

- linearmente indipendenti
- generatori di V
- una base di V.

(a) $V = \mathbb{R}^4$, $T = \left\{ \underset{v_1}{\begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}}, \underset{v_2}{\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}}, \underset{v_3}{\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}} \right\}$;

(b) $V = \{$ matrici simmetriche reali 2×2$\}$, $T = \left\{ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}$;

(c) $V = \mathbb{R}_2[t]$ (i polinomi di grado al più 2 a coefficienti reali), $T = \{1+t, 1-t, t^2, 1-t^2\}$.

(a)

(1) è libero? — per verificarlo, calcoliamo il rango della matrice associata, e usiamo Rouché-Capelli per trarre conclusioni su dim(Sol(A|0))

$$x\begin{pmatrix}1\\0\\1\\1\end{pmatrix} + y\begin{pmatrix}1\\1\\0\\1\end{pmatrix} + z\begin{pmatrix}0\\1\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

(dobbiamo vedere se l'unica comb. nulla è quella banale)

$$A = \begin{pmatrix}1&1&0\\0&1&1\\1&0&1\\1&1&1\end{pmatrix} \underset{\substack{R_3 \to R_3 - R_1 \\ R_4 \to R_4 - R_1}}{\cup\!\!\!\cap} \begin{pmatrix}1&1&0\\0&1&1\\0&-1&1\\0&0&1\end{pmatrix} \underset{R_3 \to R_3 + R_2}{\cup\!\!\!\cap} \begin{pmatrix}1&1&0\\0&1&1\\0&0&2\\0&0&1\end{pmatrix} \underset{\substack{R_3 \to R_3 - R_4 \\ R_4 \to R_4 - R_3}}{\cup\!\!\!\cap} \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\\0&0&0\end{pmatrix} \underset{\substack{R_2 \to R_2 - R_3 \\ R_1 \to R_1 - R_2}}{\cup\!\!\!\cap} \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\0&0&0\end{pmatrix}$$

$$rg(A) = 3 = rg(A|0)$$

per Rouché-Capelli, $Sol(A|0) \xleftrightarrow[\text{corr. biun.}]{1:1} \mathbb{R}^{\overset{\#\text{ indet.}}{n - rg(A)}} = \mathbb{R}^{3-3} = \mathbb{R}^0 \iff Sol(A|0) = \{(0)\}$ ovvero $\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$

noi avevamo detto $\dim_K(Sol(A|0)) = n - rg(A)$ (equivalente)

$\iff \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0 \implies \alpha_1 = \alpha_2 = \alpha_3 = 0$

$\iff v_1, v_2, v_3$ sono l.i.

[2,3] In realtà, ho finito. So che $\dim_{\mathbb{R}}(\mathbb{R}^4) = 4$ (fatto), e che v_1, v_2, v_3 sono l.i.

(3) So che la dimensione di uno sp. vett. è la cardinalità di tutte le sue basi e ho:

$$\dim_{\mathbb{R}}(\mathbb{R}^4) = 4 \quad , \quad \#T = 3 \implies T \text{ non può essere base di } \mathbb{R}^4$$

(2) So che S base $\iff$ S generatore libero.

Ho che T è libero $\implies$ T non può essere generatore, altrimenti sarebbe base. (e non può esserlo)

però, dimostriamo comunque che v_1, v_2, v_3 non generano $\mathbb{R}^4$, ovvero che $Span_K(v_1, v_2, v_3) \subsetneq \mathbb{R}^4$

Vogliamo quindi mostrare che $\exists\, v \in \mathbb{R}^4$ che non è combinazione lineare di v_1, v_2, v_3

quindi, che non può essere scritto come $v = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3$, $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$.

Per farlo, costruiamo la matrice completa associata $(T|v)$ con $v = \begin{pmatrix}a\\b\\c\\d\end{pmatrix}$, e vediamo se esiste almeno un valore di $v = \begin{pmatrix}a\\b\\c\\d\end{pmatrix}$ per cui esso è INCOMPATIBILE (ovvero $rg(A) \neq rg(A|b)$)

$$(A|b) = \left(\begin{array}{ccc|c}1&1&0&a\\0&1&1&b\\1&0&1&c\\1&1&1&d\end{array}\right) \underset{\substack{R_3 \to R_3 - R_1 \\ R_4 \to R_4 - R_1}}{\cup\!\!\!\cap} \begin{pmatrix}1&1&0&a\\0&1&1&b\\0&-1&1&c-a\\0&0&1&d-a\end{pmatrix} \underset{\substack{R_3 \to R_3 + R_2 \\ R_3 \leftrightarrow R_4}}{\cup\!\!\!\cap} \begin{pmatrix}1&1&0&a\\0&1&1&b\\0&0&1&c-a+b\\0&0&2&d-a\end{pmatrix} \underset{R_4 \to R_4 - 2R_3}{\cup\!\!\!\cap} \begin{pmatrix}1&1&0&a\\0&1&1&b\\0&0&1&d-a\\0&0&2&c+a+b-2d\end{pmatrix}$$

esiste (più di) un valore di $\begin{pmatrix}a\\b\\c\\d\end{pmatrix}$ per cui $rg(A) \neq rg(A|b)$ → per esempio, $\begin{pmatrix}a\\b\\c\\d\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$ $(rg(A|b) = 4 \neq 3 = rg(A))$

Sistema inc. $\iff \exists\, v \in \mathbb{R}^4$ t.c. $v \notin Span(v_1, v_2, v_3) \iff Span(v_1, v_2, v_3) \neq \mathbb{R}^4$

ⓑ $V = \{$ matrici simmetriche reali $2\times 2\}$ $\quad T = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \subset \mathcal{M}_2^+(\mathbb{R})$

$\dim_{\mathbb{R}}(V) = 3$ ⤳ sono tutte nella forma $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ - servono 3 parametri a, b, c - che possono avere qualunque valore (non sono vincolati, sono liberi) per descriverle
↳ grado di libertà $= 3$

• per verificare la libertà

studiamo il sistema: $x \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + y \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + z \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$$\Longleftrightarrow \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \underset{\substack{R_3 \to R_3 - R_2 \\ R_3 \leftrightarrow R_4}}{\sim} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \underset{\substack{R_2 \to R_2 - R_3 \\ R_3 \to R_3 - R_1 \\ R_3 \to R_3 - R_2}}{\sim} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad rg(A) = rg(A|\emptyset) = 3$$

inoltre $Sol(A|\emptyset) \overset{1:1}{\longleftrightarrow} \mathbb{R}^{3-3} = \mathbb{R}^{\emptyset} \Longrightarrow$ le matrici di T sono l.i.

Per la prop. 3, visto che $\dim_{\mathbb{R}}(V) = 3$ e $\#T = 3$ e T libero, T è base di $V = \mathcal{M}_2^+(\mathbb{R})$
(S base $\Longleftrightarrow \#S = n$ e S libero)

ⓒ $T = \{1+t, 1-t, t^2, 1-t^2\} \subset \mathbb{R}_2[t]$ (polinomi grado max 2 coeff. reali)

(Sappiamo che) $\mathbb{R}_2[t]$ è il sottosp. vett. di $\mathbb{R}[t]$ generato da $\{1, t, t^2\}$, che ne è una base.
Quindi, $\dim(\mathbb{R}_2[t]) = 3$

• Osserviamo che $T \subset \mathbb{R}_2[t]$, quindi $Span(T) \subset \mathbb{R}_2[t]$
$Span(T) \subset Span(\mathbb{R}_2[t]) = \mathbb{R}_2[t]$ stesso

ma, visto che $\#T = 4$, per la prop. 3, T non è libero - $\#T = 4 > \dim_{\mathbb{R}}(\mathbb{R}_2[t]) = 3$
(S è libero $\Longrightarrow \#S \leq n$) ↳ quindi non è base.

• è generatore?

Osserviamo che $\mathbb{R}_2[t] = Span_{\mathbb{R}}(1, t, t^2)$

ⓐ $t^2 \in T$

ⓑ $t = \frac{1}{2}(1+t-(1-t)) \in Span_{\mathbb{R}}(T)$

ⓒ $1 = \frac{1}{2}(1+t+1-t) \in Span_{\mathbb{R}}(T)$

$\Longrightarrow Span_{\mathbb{R}}(1, t, t^2) = \mathbb{R}_2[t] \subset Span_{\mathbb{R}}(T) \Longrightarrow T$ è sistema di generatori
(ogni elemento della base $\{1, t, t^2\}$ di $\mathbb{R}_2[t]$ può essere scritto come comb. lineare di T, quindi ogni el. di $\mathbb{R}_2$ con, too)

Esercizio 3. (a) Si determini una base per il sottospazio S di $\mathbb{R}^4$ generato dai vettori $v_1 = (1,1,0,1)$, $v_2 = (1,0,1,1)$, $v_3 = (1,-1,1,-1)$, $v_4 = (2,2,1,4)$.

(b) Si dica se il vettore $v = (0,3,-2,2)$ appartiene al sottospazio S.

(c) Si dica (motivando la risposta) se i vettori $\{v_1, v_2, v_3, v\}$ formano una base di $\mathbb{R}^4$.

(d) Dopo aver verificato che l'insieme $\mathcal{B} = \left\{ \begin{bmatrix} 1\\1\\0\\0 \end{bmatrix}, \begin{bmatrix} 1\\0\\0\\0 \end{bmatrix}, \begin{bmatrix} 0\\0\\1\\1 \end{bmatrix}, \begin{bmatrix} 0\\0\\1\\-1 \end{bmatrix} \right\}$

è una base di $\mathbb{R}^4$, si determinino le coordinate del vettore v nella base $\mathcal{B}$.

ⓐ Calcolare una base di $\mathrm{Span}_{\mathbb{R}}(v_1, v_2, v_3, v_4) = S$

Se effettuiamo trasformazioni lineari (op. di Gauss) su v_1, v_2, v_3, v_4, essi rimangono generatori di S – vogliamo vedere se sono anche l.i.

$$A = \begin{pmatrix} 1&1&0&1\\1&0&1&1\\1&-1&1&-1\\2&2&1&4 \end{pmatrix} \underset{\substack{R_2 \to -1(R_2-R_1)\\ R_3 \to R_3-R_1\\ R_4 \to R_4-2R_1}}{\cup\!\cap} \begin{pmatrix} 1&1&0&1\\0&1&-1&0\\0&-2&1&-2\\0&0&1&2 \end{pmatrix} \underset{R_3 \to R_3+2R_2}{\cup\!\cap} \begin{pmatrix} 1&1&0&1\\0&1&-1&0\\0&0&-1&-2\\0&0&1&2 \end{pmatrix} \underset{\substack{R_4 \to R_4+R_3\\ R_3 \to -R_3}}{\cup\!\cap} \begin{pmatrix} 1&1&0&1\\0&1&-1&0\\0&0&1&2\\0&0&0&0 \end{pmatrix}$$

quindi: $rg(A) = 3$

Abbiamo quindi $S = \mathrm{Span}_{\mathbb{R}}\begin{pmatrix} (1\ 1\ 0\ 1)\\(0\ 1\ -1\ 0)\\(0\ 0\ 1\ 2) \end{pmatrix}$

In più, le righe con pivot di una matrice a gradini sono l.i. $\Longrightarrow \begin{Bmatrix} (1\ 1\ 0\ 1),\\(0\ 1\ -1\ 0),\\(0\ 0\ 1\ 2) \end{Bmatrix}$ è generatore libero ed è quindi base di S. (e $\dim_{\mathbb{R}}(S) = 3$)

(non di $\mathbb{R}^4$ però)

(quindi, anche i vettori originali, v_1, v_2, v_3, sono una base)

ⓑ Per vedere se $v \in S$, bisogna vedere se è una comb. lineare dei vettori della base

bisogna quindi vedere se $\exists\, x, y, z \in \mathbb{R}$ t.c. $x\underbrace{\begin{pmatrix}1\\1\\0\\1\end{pmatrix}}_{v_1'} + y\underbrace{\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}}_{v_2'} + z\underbrace{\begin{pmatrix}0\\0\\1\\2\end{pmatrix}}_{v_3'} = \underbrace{\begin{pmatrix}0\\3\\-2\\2\end{pmatrix}}_{v}$, ovvero se il sistema è compatibile $(rg(A) = rg(A|v))$

La matrice completa associata al sistema è:

$$\left(\begin{array}{ccc|c} 1&0&0&0\\1&1&0&3\\0&-1&1&-2\\1&0&2&2 \end{array}\right) \underset{\substack{R_2 \to R_2-R_1\\ R_4 \to R_4-R_1}}{\cup\!\cap} \begin{pmatrix} 1&0&0&0\\0&1&0&3\\0&-1&1&-2\\0&0&2&2 \end{pmatrix} \underset{\substack{R_3 \to R_3+R_2\\ R_4 \to \frac{1}{2}R_4}}{\cup\!\cap} \begin{pmatrix} 1&0&0&0\\0&1&0&3\\0&0&1&1\\0&0&1&1 \end{pmatrix} \underset{R_4 \to R_4-R_3}{\cup\!\cap} \begin{pmatrix} 1&0&0&0\\0&1&0&3\\0&0&1&1\\0&0&0&0 \end{pmatrix}$$

$rg(A) = rg(A|v) = 3 \Longrightarrow v \in \mathrm{Span}_{\mathbb{R}}(v_1', v_2', v_3')$

ⓒ No, $\{v_1, v_2, v_3, v\}$ non può essere una base. Infatti, $S = \mathrm{Span}_{\mathbb{R}}(v_1, v_2, v_3) = \mathrm{Span}_{\mathbb{R}}(v_1', v_2', v_3')$, e: nella ⓑ abbiamo visto che $v \in \mathrm{Span}_{\mathbb{R}}(v_1', v_2', v_3')$

quindi esistono $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ t.c. $v = \lambda_1 v_1' + \lambda_2 v_2' + \lambda_3 v_3'$

e quindi $\emptyset = -v + \lambda_1 v_1' + \lambda_2 v_2' + \lambda_3 v_3' = \lambda_0 v + \lambda_1 v_1' + \lambda_2 v_2' + \lambda_3 v_3'$

$\lambda_0 = -1 \neq \emptyset$ quindi c'è almeno un coeff. non nullo per cui la combinazione $= \emptyset$

quindi i vettori non sono l.i.

quindi $\{v_1', v_2', v_3', v\}$ non è una base di $\mathbb{R}^4$ $\left(\mathrm{Span}_{\mathbb{R}}(v_1', v_2', v_3', v) = \mathrm{Span}_{\mathbb{R}}(v_1', v_2', v_3') = \mathrm{Span}_{\mathbb{R}}(v_1, v_2, v_3) \right)$

che ha dim $3 \neq \dim(\mathbb{R}^4) = 4$

ⓓ $B = \left(\begin{pmatrix}1\\1\\0\\0\end{pmatrix} \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \begin{pmatrix}0\\0\\1\\1\end{pmatrix} \begin{pmatrix}0\\0\\1\\-1\end{pmatrix} \right)$ base di $\mathbb{R}^4$?

matrice vettori di B

B è base di $\mathbb{R}^4 \iff rg(M) = 4$

$$M = \begin{pmatrix}1&1&0&0\\1&0&1&1\\0&0&1&-1\\0&0&0&0\end{pmatrix} \underset{\substack{R_3 \to R_2 \to \\ R_4 \to R_3}}{\cong} \begin{pmatrix}1&1&0&0\\0&0&1&1\\0&0&1&-1\\1&0&0&0\end{pmatrix} \underset{R_1 \leftrightarrow R_3}{\cong} \begin{pmatrix}0&0&1&-1\\0&0&1&1\\1&1&0&0\\1&0&0&0\end{pmatrix} \underset{R_2 \to R_2+R_1}{\cong} \begin{pmatrix}0&0&1&-1\\0&0&2&0\\1&1&0&0\\1&0&0&0\end{pmatrix}$$

Si vede $rg(M) = 4 \implies B$ base di $\mathbb{R}^4$

- troviamo $[v]_B = \begin{pmatrix}v_1\\v_2\\v_3\\v_4\end{pmatrix} \in \mathbb{R}$

abbiamo $v_1 b_1 + v_2 b_2 + v_3 b_3 = v = \begin{pmatrix}0\\3\\-2\\2\end{pmatrix}$

Dobbiamo quindi risolvere il sistema

$$v_1 \begin{pmatrix}1\\1\\0\\0\end{pmatrix} + v_2 \begin{pmatrix}1\\0\\0\\0\end{pmatrix} + v_3 \begin{pmatrix}0\\0\\1\\1\end{pmatrix} + v_4 \begin{pmatrix}0\\0\\1\\-1\end{pmatrix} = \begin{pmatrix}0\\3\\-2\\2\end{pmatrix}$$

La matrice completa associata è:

applichiamo le trasformazioni viste sopra anche sul vettore v

$$\left(\begin{array}{cccc|c}1&1&0&0&0\\1&0&1&1&3\\0&0&1&-1&-2\\0&0&0&0&2\end{array}\right) \cong \left(\begin{array}{cccc|c}0&0&1&-1&2\\0&0&2&0&0\\1&1&0&0&0\\1&0&0&0&3\end{array}\right) \qquad \begin{pmatrix}0\\3\\-2\\2\end{pmatrix} \underset{\substack{R_3 \to R_2 \to \\ R_4 \to R_3}}{\cong} \begin{pmatrix}0\\-2\\2\\3\end{pmatrix} \underset{R_1 \leftrightarrow R_3}{\cong} \begin{pmatrix}2\\-2\\0\\3\end{pmatrix} \underset{R_2 \to R_2+R_1}{\cong} \begin{pmatrix}2\\0\\0\\3\end{pmatrix}$$

a cui corrisponde il sistema

$$\begin{cases} v_3 - v_4 = 2 \\ 2v_3 = \emptyset \\ v_1 + v_2 = \emptyset \\ v_1 = 3 \end{cases} \implies v_1 = 3,\ v_2 = -3,\ v_3 = \emptyset,\ v_4 = -2$$

quindi $\begin{pmatrix}v_1\\v_2\\v_3\\v_4\end{pmatrix} = \begin{pmatrix}3\\-3\\0\\-2\end{pmatrix}$ è l'unica soluzione del sistema

(infatti B è una base di $\mathbb{R}^4$, quindi ogni vettore si scrive in modo unico come comb. lineare dei suoi vettori)