

ALGEBRA

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

[https://open.spotify.com/playlist/3zMsGGKjUNlx3DFJ133ex?
si=rGWujY5LSLy7B1vKdUTHnA&pi=e-SkW9gkIWTLG5](https://open.spotify.com/playlist/3zMsGGKjUNlx3DFJ133ex?si=rGWujY5LSLy7B1vKdUTHnA&pi=e-SkW9gkIWTLG5)



Si vuole creare una teoria generale che contenga come esempio \mathbb{Z} e le sue operazioni

$$\mathbb{Z} \xrightarrow{-} \mathbb{Z} \quad \text{opposto}, \quad \mathbb{Z} \times \mathbb{Z} \xrightarrow{+} \mathbb{Z} \quad \text{somma e prodotto (binarie)}$$

l'altro modo di esprimere l'addizione



Ci sono diverse condizioni di compatibilità tra le operazioni:

$$\circ(b+c) = ab+ac, \quad a+b = b+a, \quad a+(b+c) = (a+b)+c$$

def ANELLO es. $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$

poi lo chiameremo solo A

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

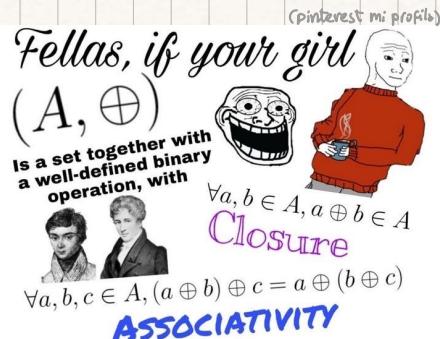
dove:

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

questi dati devono soddisfare 8 proprietà:

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

- ① $\forall a, b \in A, a+b = b+a$ COMMUTATIVITÀ
- ② $\forall a, b, c \in A, (a+b)+c = a+(b+c)$ ASSOCIAZIATIVITÀ DELLA SOMMA
- ③ $\forall a \in A, a+0_A = 0_A+a = a$ EL. NEUTRO SOMMA
- ④ $\forall a \in A, a+(-a) = 0_A$ (OPPOSTO)



$\exists e \in A : \forall a \in A, e+a = a+e = a$
An identity element
 $\forall a \in A, \exists b \in A : a+b = b+a = e$
Inverse elements
 $\forall a, b \in A, a+b = b+a$ That's not your girl, that's an Abelian group!
and Commutativity

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 $\forall a, b, c \in A, a(b \cdot c) = (a \cdot b)c = abc$ ASSOCIAZIATIVITÀ DEL PRODOTTO
- ⑥ $\forall a, b, c \in A, a(b+c) = ab+ac$ DISTRIBUTIVITÀ
 $(a+b)c = ac+bc$
- ⑦ $\forall a \in A, a \cdot 1_A = 1_A \cdot a = a$ EL. NEUTRO DEL PRODOTTO
rende l'anello "UNITARIO"
- ⑧ $\forall a, b \in A, a \cdot b = b \cdot a$ COMMUTATIVITÀ DEL PRODOTTO
rende l'anello "COMMUTATIVO"

l'anello $A = \mathbb{Z}$ ha proprietà più specifiche:

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

$\langle \exists c \in E \text{ tc. } \forall e \in E \setminus \{c\} \text{ si ha } e > c \rangle \text{ BUON ORDINAMENTO}$

un anello commutativo e unitario che soddisfa le proprietà di tricotomia e buon ordinamento "è essenzialmente" \mathbb{Z}

- se $a < b \quad c < d$ allora $a+c < b+d$ e $-a > -b$ allora l'operazione + e > sono compatibili in modo simile, c'è compatibilità tra \circ e $>$

legge di cancellazione in \mathbb{Z}

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

altrimenti basta mult per -1 entrambi le parti

Infatti, supponendo $a > 0$

Induzione su $a \geq 1$

$\cdot a=1$ è chiaro perché 1 è l'el. neutro

\cdot Supponiamo per ip. induttiva che $a > 1$ e $(a-1)b = (a-1)c$

Supponiamo x ass. che $b \neq c$. Allora $\circ b > c \circ b < c$. Supponiamo $b > c \implies (a-1)b + b > (a-1)c + c$

tricotomia

$\circ -b + b > -c + c$ premessa $ab = ac$

$\circ ab > ac$, che è impossibile quindi necessariamente $b=c$

def ELEMENTI INVERTIBILI dato A anello $1_A \neq 0_A$

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

(si dice che b è inverso di a e si scrive $b = a^{-1}$)

es. se a è invertibile allora a^{-1} è unicamente determinato

inverso di a : el che, moltiplicato per a , dà 1_A

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

$$a \cdot b = a \cdot b' = 1 \text{ con } b, b' \in A$$

deve essere =

$$\begin{aligned} \text{allora } (a \cdot b) b' &= 1_A \cdot b' = b' \\ \text{quindi } (2) &\xrightarrow{(3)} \text{uguali} \\ (a \cdot b') b &= 1_A \cdot b = b \\ \text{allora } (a \cdot b) b' &= a(b \cdot b') = a(b' \cdot b) = ab' \cdot b \\ \text{quindi } (2) &\xrightarrow{(1)} \text{uguali} \end{aligned}$$

Si pone $A^x = \{ \alpha \in A \text{ t.c. } \alpha \text{ è invertibile} \}$ A^x è un gruppo

verificare ① A^x è non vuoto ② se $\alpha \in A^x$ allora $\alpha^{-1} \in A^x$

③ se $a, b \in A^x$ sono invertibili, allora $(ab)^{-1} = a^{-1}b^{-1}$

④ $\mathbb{Z}^x = \{1, -1\}$

esercizio $(\mathbb{Q}, +, -, \cdot, 0, 1)$ è un anello (cu). Calcolare l'insieme degli elementi invertibili

risposta: $\mathbb{Q}^x = \{r \in \mathbb{Q}; r \neq 0\}$ $[1] = [1_A]$

PICCOLI ESEMPI

① $\forall \alpha \in A, \alpha \cdot 0_A = 0_A$

$$\begin{aligned} \alpha \cdot 0_A &= \underbrace{\alpha \cdot (0_A + (-0_A))}_{0_A \text{ (assioma)}} = \alpha \cdot 0_A + \alpha \cdot (-0_A) \\ &= \alpha \cdot 0_A + (-(\alpha \cdot 0_A)) \text{ elemento} + \text{il suo opposto quindi } \alpha \cdot 0_A = 0_A \\ &= 0_A \times \text{assioma} \end{aligned}$$

② Supponiamo $0_A = 1_A$.

Mostriamo che $\forall \alpha \in A, \alpha = 0_A = 1_A$ ($A = \{0_A\}$)

$$\alpha \in A : 1_A = 0_A \implies \underbrace{\alpha \cdot 1_A}_{=\alpha} = \underbrace{\alpha \cdot 0_A}_{0_A} \text{ quindi, } \forall \alpha, \alpha = 0_A$$

③ se $1_A \neq 0_A$ allora $0_A \notin A^x$.

Supponiamo per assurdo $\exists x \in A^x$ t.c. $1_A = x \cdot 0_A = 0_A$ contraddizione

gli assiomi implicano che 0_A non è mai invertibile

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

verificare ① A^\times è non vuoto ② se $a \in A^\times$ allora $a^{-1} \in A^\times$

③ se $a, b \in A^\times$ sono invertibili, allora $(ab)^{-1} = a^{-1}b^{-1}$

④ $\mathbb{Z}^\times = \{1, -1\}$

① A^\times non è vuoto.

Abbiamo visto che 1_A è sempre invertibile e $1_A \in A$ per def. di omessa comm. un. (semplice)

quindi, $1_A \in A \Rightarrow A \neq \emptyset$

② se $a \in A^\times$ allora $a^{-1} \in A^\times$

vista in classe
se $a \in A^\times$, vuol dire che \exists unicamente determinato $b \in A : ab = ba = 1_A$.

Supponiamo per assurdo che $b \notin A^\times$.

se $b \notin A^\times$, $\nexists x \in A \text{ t.c. } bx = xb = 1_A$. ma questo è falso. esiste ed è a .

$\forall x \in A, bx = xb \neq 1_A$ falso per a

③ se $a, b \in A^\times$, allora $(ab)^{-1} = a^{-1}b^{-1}$

$$(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow a^{-1}b^{-1} \cdot ab = 1_A \quad (\text{per definizione})$$

$$\Leftrightarrow a^{-1} \cdot b^{-1} \cdot a \cdot b = 1_A \quad (\text{e, poiché unicamente determinato})$$

se $a^{-1}b^{-1} \cdot ab = 1_A$

e $(a \cdot b)^{-1} \cdot ab = 1_A$ allora $(ab)^{-1} = a^{-1}b^{-1}$

visto che $a^{-1} \cdot a = 1_A$ e $b^{-1} \cdot b = 1_A$

$$a^{-1} \cdot b^{-1} \cdot a \cdot b \quad \begin{matrix} \text{commutatività} \\ \text{e associtività} \end{matrix} \quad (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) = 1_A$$

$1_A \cdot 1_A = 1_A$ vero perché 1_A il.

neutro della mult.

quindi $x \cdot 1_A = 1_A$

④ $\mathbb{Z}^\times = \{1, -1\}$

• dimostriamo $1, -1 \in \mathbb{Z}^\times$

① su \mathbb{Z} , $1_A = 1$. Visto che 1_A è sempre invertibile, $1 \in \mathbb{Z}^\times$

② $-1 = -(-1)$ se $-1^{-1} = 1$, allora $-(-1)^{-1} = -(-1)$ moltiplica per -1 da entrambe le parti
quindi $-1 \in \mathbb{Z}^\times$ e $-1^{-1} = -1$

③ dimostriamo che $\forall x \in \mathbb{Z}, x \notin \{1, -1\} \Rightarrow x \notin \mathbb{Z}^\times$

Supponiamo per assurdo $x \in \mathbb{Z}, x \notin \{1, -1\}, x \in \mathbb{Z}^\times$

Allora $x \cdot y = 1_A$. su \mathbb{Z} , $1_A = 1$, quindi $x \cdot y = 1$

Ma, su \mathbb{Z} , le uniche coppie che moltiplicate danno 1 sono $(-1, -1)$ e $(1, 1)$

Per ipotesi, $x \notin \{1, -1\}$, quindi CONTRADDIZIONE

esercizio $(\mathbb{Q}, +, -, \cdot, 0, 1)$ è un anello (cu). Calcolare $\mathbb{Q}^{\times} = \{x \in \mathbb{Q} : x \text{ è invertibile}\}$

- invertibili: $\exists x \in \mathbb{Q} \text{ t.c. } \exists y \in \mathbb{Q} \text{ t.c. } xy = 1$

- in \mathbb{Q}^{\times} , $1_A = 1$.

quindi $\exists x \in \mathbb{Q} \text{ t.c. } \exists y \in \mathbb{Q} \text{ t.c. } xy = 1$

① dimostriamo che $0 \notin \mathbb{Q}^{\times} \rightarrow 0 = 0_A \in \mathbb{Q}_A \text{ e } 0_A \text{ non è invertibile per definizione}$
(ma, comunque, basta fare: $0 \cdot y = 1$ impossibile perché $0 \cdot y = 0$)

② dimostriamo che $\forall q \in \mathbb{Q}, q \neq 0, q \in \mathbb{Q}^{\times}$

$qx = 1 \iff x = \frac{1}{q} \text{ e } \frac{1}{q} \in \mathbb{Q}$. Trovato x t.c. $qx = 1$ (per vedere inviamente che $x \neq 0$ non va)
perché $\frac{1}{0}$ impossibile
(non sono sicura che questo basti, ngl.)

esercizio: c'è un unico elemento neutro

Siamo v, v' due elementi neutri per la moltiplicazione

$$\begin{array}{lll} \forall a \in A \quad av = ua = a & \text{con } a = v & vv' = v'u = v \\ \quad av' = u'a = a & \text{con } a = v' & v'u \cancel{=} vv' = v' \end{array} \quad \text{quindi } v = v'$$

Dedurre che anche l'elemento neutro per l'addizione è unicamente determinato

Relazione di divisibilità

Introduciamo la relazione: $a, b \in A : a|b \iff \exists c \in A \text{ t.c. } b = a \cdot c$.

$$2|6 : 6 = 2 \cdot 3$$

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

• è una relazione **transitiva**: $a, b, c \in A$ supponiamo $a|b \iff b = a \cdot a' \exists a' \in A$

• Non è simmetrica né antisimmetrica
ma su N^* è antisimmetrica

$$b|c \iff c = b \cdot b' \exists b' \in A$$

$$\Rightarrow c = a \cdot a' \cdot b' = a(\underbrace{a' \cdot b'}_{a''}) \Rightarrow c = a \cdot a'' \iff a|c$$

• se $a|b \wedge a|c$ allora $a|b+c$ (compatibilità)

$$a|b \iff \exists a' \text{ t.c. } b = a \cdot a' \quad a|c \iff \exists a'' \in A \text{ t.c. } c = a \cdot a''$$

$$b+c = a \cdot a' + a \cdot a'' = a(\underbrace{a' + a''}_{a'''}) \iff a|b+c$$

più generalmente, se $\alpha, \beta \in A$, $\alpha|b, \alpha|c \Rightarrow \alpha|b+\beta c$ (la dimostrazione è banale)

$$\alpha b + \beta c = \alpha \cdot a \cdot a' + \beta \cdot a \cdot a'' = a(\underbrace{\alpha a' + \beta a''}_{a'''})$$

dim. $\alpha, \beta \in A$

$$a|b, a|c \Rightarrow a|\alpha b + \beta c$$

$\cdot \alpha|b \Rightarrow \alpha|\alpha b$ per def. di moltiplicazione

$\cdot \alpha|c \Rightarrow \alpha|\beta c$

per la dim. d. compatibilità, $\alpha|\alpha b + \beta c$

In \mathbb{Z} la relazione di divisibilità è quasi antisimmetrica:

ignoriamo il caso 0

$$a, b \in \mathbb{Z} \quad a|b \wedge b|a \Rightarrow \exists c \in \mathbb{Z}^* \text{ t.c. } a = bc \quad (\text{ovvero } a \in \{b, -b\} \circ \{a, -a\} = \{b, -b\})$$

$$\textcircled{1} \mid 1 \Rightarrow 1 = \textcircled{0} \cdot b \quad \textcircled{0} \text{ non divide mai un el. non nullo} \quad \text{quindi possiamo supporre } a, b \neq \textcircled{0}$$

$$a|b, b|a \Rightarrow b = a \cdot a', a = b \cdot b' \exists a, b \in \mathbb{Z}$$

$$b = b \cdot a' \cdot b' \quad \text{con } b \neq \textcircled{0}, \text{ legge di cancellazione} \quad b' = b \cdot a' \cdot b' \Rightarrow 1 = a' \cdot b' \Rightarrow a' \cdot b' \in \{1, -1\}$$

$$\Rightarrow \{a, -a\} = \{b, -b\}$$

• non è simmetrica \rightarrow supponiamo $a|b$ simmetrica. Allora $a|b$ ($\exists c \text{ t.c. } b = a \cdot c$) $\Rightarrow b|a$ ($\exists c' \text{ t.c. } a = b \cdot c'$)

$$\text{quindi, } b = b \cdot c' \cdot c \quad \text{con } b \neq \textcircled{0} \quad b = b \cdot c' \cdot c \iff 1 = c \cdot c' \iff (c, c') \in \{(1, 1), (-1, -1)\}$$

oppure, con esempio: $2|4$ ma $4 \not| 2$

• non è antisimmetrica: se fosse antisimmetrica, $a|b \wedge b|a \Rightarrow a = b$

ma (ragionamento di prima) $1 = c \cdot c \iff (c, c) \in \{(1, 1), (-1, -1)\}$

$$\begin{cases} (c', c) = (1, 1) \Rightarrow b = a \\ (c', c) = (-1, -1) \Rightarrow b = -a \end{cases}$$

def elemento irriducibile

invertibili

$\alpha \in A \setminus A^\times$ è detto irriducibile se

$\forall b, c \in A, \alpha = bc \Rightarrow b \in A^\times \text{ o } c \in A^\times$

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

$$7 = 1 \cdot 7 = 7 \cdot 1 = -1 \cdot -7 = -7 \cdot -1 \quad 7 \text{ è irriducibile}$$

$1 \in \mathbb{Z}$ non è irriducibile perché abbiamo definito $\alpha \in A \setminus A^\times$

def numero primo

invertibili

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

$\forall b, c \in A, \text{ se } \alpha | bc \Rightarrow \alpha | b \text{ oppure } \alpha | c$

Supponiamo $A = \mathbb{Z}$

lemma $p \in \mathbb{Z}$ primo $\Rightarrow p$ è irriducibile

dim p primo, siano $a, b \in \mathbb{Z}$ t.c. $p = ab \Rightarrow p | a \cdot b$

$$ab = p \cdot 1$$

Supponiamo senza perdita di generalità $p | a$

$$\text{sost. } a = p a'$$

$$p | a \Rightarrow a = p a' \exists a' \in \mathbb{Z} \Rightarrow p = p a' b \quad \begin{matrix} \text{legge di} \\ \text{concessione} \end{matrix} \quad p = p(a'b) \Leftrightarrow 1 = a'b \Rightarrow a', b \in \{+1, -1\} = \mathbb{Z}^\times$$

Se $a' = 1$ allora $a = p \Rightarrow p = pb \Rightarrow b = 1$

Se $a' = -1$ allora $a = -p \Rightarrow p = p \cdot -b \Rightarrow -b = 1 \Rightarrow b = -1 \Rightarrow p$ è irriducibile

!! ogni modo di scriverlo come
 $p = ab$ porta ad $a, b \in \{-1, 1\}$
 $A^\times \text{ in } \mathbb{Z}$

def valore assoluto

$$\mathbb{Z} \xrightarrow{\text{1.1}} \mathbb{N} \quad a \in \mathbb{Z} \quad \bullet \text{ se } a = 0 \quad |a| = 0$$

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

ALGORITMO DELLA DIVISIONE EUCLIDEA

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

$q \in \mathbb{Z}, r \in \{0, \dots, |n|-1\}$ t.c. $a = nq + r$

resto
quoziente

è una riformulazione
del principio del minimo su \mathbb{N}

def CONGRUENZA

b è il resto di $\frac{a}{n}$

$$a \equiv b \pmod{n} \iff n \mid a - b$$

$$\iff \exists q \in \mathbb{Z} \text{ t.c. } d-b = qn$$

ovvero, il resto della divisione escluse di $a - b$ per n è 0

- La congruenza modulo n è di equivalenza

④ transitivs : $a \equiv b \pmod{n}$ & $b \equiv c \pmod{n} \iff n \mid b-a$ & $n \mid c-b$

$$n|\alpha: n|\beta \Rightarrow n|\alpha+\beta \quad n|c-b+b-\delta \Rightarrow n|c-\delta \Leftrightarrow \delta \equiv c \pmod{n}$$

Scw. rifl. e simm.

$$\mathbb{Z}_{/\equiv_{\text{mod } n}} = \left\{ \begin{smallmatrix} n\mathbb{Z} \\ [0] \end{smallmatrix}, \begin{smallmatrix} n\mathbb{Z}+1 \\ [-1] \end{smallmatrix}, \dots, \begin{smallmatrix} n\mathbb{Z}+n-1 \\ [n-1] \end{smallmatrix} \right\}$$

② riflessiva : $\delta = \delta \bmod n$ $n | \delta - \delta$ vero perché $\forall x \in \mathbb{Z}, x \neq 0, x | 0$

$$\textcircled{3} \text{ simmetria: } a \equiv_n b \implies b \equiv_n a \quad n | a - b \implies n | b - a$$

$$n|a-b \iff a-b = qn \iff -(a-b) = -(qn) \iff b-a = -qn \quad \text{quindi } n|b-a$$

Esempi: congruenze modulo 2

$$\mathbb{Z} = \underbrace{2\mathbb{Z}}_{[0]} \sqcup \underbrace{2\mathbb{Z} + 1}_{[1]} \quad \mathbb{Z}/\equiv_{\text{mod}_2} = \{2\mathbb{Z}, 2\mathbb{Z} + 1\}$$

convergente mod. 3

$$\mathbb{Z} \equiv_{\text{mod } 3} = \{ 3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2 \}$$

$$\mathbb{Z}/\equiv_n = \mathbb{Z}_{n\mathbb{Z}} \quad n > 0 \quad \text{insieme quoziente}$$

di \mathbb{Z} su congr. modulo n

l'componente
mod. n

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

tutti gli interi

$[2]_3 = \{m \in \mathbb{Z} : m \equiv 2 \pmod{3}\} = \{m \in \mathbb{Z} : 3 | m-2\}$

Le operazioni: + - di \mathbb{Z} sono compatibili con \equiv_n ($n > 0$)

① $\forall \alpha, \alpha' \in \mathbb{Z}, \alpha \equiv \alpha' \pmod{n} \iff -\alpha \equiv -\alpha' \pmod{n}$ compatibilità con opposto

② $\forall \alpha, \alpha', b, b' \in \mathbb{Z}, \alpha \equiv_n \alpha', b \equiv_n b' \Rightarrow \alpha + b \equiv_n \alpha' + b'$ comp. con somma

③ $\forall \alpha, \alpha', b, b' \in \mathbb{Z}, \alpha \equiv_n \alpha', b \equiv_n b' \Rightarrow \alpha b \equiv_n \alpha' b'$ comp. con prodotto

dim ②

$$2 \mid 5-1 \quad \text{e} \quad 2 \mid 1-5$$

$$\alpha \equiv_n \alpha' \iff n \mid \alpha - \alpha' \quad \text{e} \quad n \mid \alpha' - \alpha$$

$$n \mid b' - b \iff \exists k \in \mathbb{Z} \text{ t.c. } \underline{\alpha'} - \underline{\alpha} = nk$$

$$n \mid b' - b \iff \exists k' \in \mathbb{Z} \text{ t.c. } \underline{b'} - \underline{b} = nk'$$

Dove ottenere $\alpha + b \equiv_n \alpha' + b'$

sommare le due formule

$$\Rightarrow \underline{\alpha'} + \underline{b'} - (\underline{\alpha} + \underline{b}) = n(k+k') \iff \alpha' + b' \equiv_n \alpha + b$$

quindi $n(\alpha' + b') - \alpha + b$
(perché $n \cdot \text{qualcosa} = \text{quello}$)

dim. ①

$$\forall \alpha, \alpha' \in \mathbb{Z}, \alpha \equiv_n \alpha' \iff -\alpha \equiv_n -\alpha'$$

$$\alpha \equiv_n \alpha' \iff n \mid \alpha - \alpha' \iff \alpha - \alpha' = qn \iff -\alpha + \alpha' = -qn$$

dim. ③

$$\forall \alpha, \alpha', b, b' \in \mathbb{Z}, \alpha \equiv_n \alpha', b \equiv_n b' \Rightarrow \alpha b \equiv_n \alpha' b'$$

ovvero $\alpha b - \alpha' b' = kn \quad \text{o} \quad \alpha b = kn + \alpha' b'$

$$\alpha = qn + \alpha' \quad \text{e} \quad b = q'n + b' \quad \text{quindi } \alpha b = (\alpha + qn)(b + q'n) = \alpha b' + n(q'b' + \alpha'q' + qq'n)$$

$\alpha b = \alpha' b' + n(k)$

OPERATORI

$\mathbb{Z}/n\mathbb{Z}$ definiamo $[\alpha] \in \mathbb{Z}/n\mathbb{Z}$ $[\alpha] = \alpha + n\mathbb{Z}$ insieme degli interi che si esprimono come $\alpha +$ multiplo di n (interi che hanno come resto α)

- $[\alpha] := [-\alpha]$ questa funz. $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ è ben definita: opposto in $\mathbb{Z}/n\mathbb{Z}$

definiamo

• $[\alpha] + [b] := [\alpha + b]$ ben definito (ovvero indipendente dalla scelta di rapp. di $[\alpha] \in [b]$)

$$\text{scelgiamo } \alpha' \in [\alpha] \quad \text{e } b' \in [b] \quad \text{e calcoliamo } [\alpha' + b'] = \left\{ m : n \mid m - \alpha' - b' \right\} = \left\{ m : n \mid m - (\alpha' + b') \right\}$$

per (2), perché $[\alpha] = [\alpha']$
quindi $\alpha \equiv \alpha' \pmod{n}$
e stessa cosa per b

$\Leftrightarrow [\alpha + b] = [\alpha' + b']$ l'operazione + introdotta su $\mathbb{Z}/n\mathbb{Z}$ è ben definita

$$\text{esempi: } [1]_3, [2]_3 \in \mathbb{Z}/3\mathbb{Z} \quad [1] + [2] = [3] = [0]$$

$$\text{altri rapp. } [1] = [4] \quad [2] = [-4]$$

$$\text{quindi } [4 + -4] = [0]$$

• definiamo inoltre $[\alpha], [b] \in \mathbb{Z}/n\mathbb{Z}$ $[\alpha] \cdot [b] = [\alpha b]$ ben definito

$$\text{scelgiamo } \alpha' \in [\alpha] \quad \text{e } b' \in [b], \quad [\alpha b] = \left\{ m : n \mid m - \alpha' b' \right\} \xrightarrow{\text{ma } \alpha' = n\alpha \text{ e } b' = nb} = \left\{ m : n \mid m - nb\alpha \right\}$$

e quindi, per (3)

$$\text{esempi: } [1]_3, [2]_3 \in \mathbb{Z}/3\mathbb{Z} \quad [1] \cdot [2] = [2]$$

$$\text{e } [4 \cdot -4] = [-16] = [2] \quad \begin{aligned} &\text{- perché } \frac{2}{3} = 0 \text{ resto } 2 \\ &\text{e } \frac{-16}{3} = -6 \text{ resto } 2 \end{aligned}$$

TEOREMA

$(\mathbb{Z}/n\mathbb{Z}, +, -, \cdot, [0], [1])$ è un ANELLO (comm. un.)

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

• $\mathbb{Z} \setminus \{0\} = \mathbb{Z}^*$

• $\alpha\mathbb{Z} + b\mathbb{Z} := \{m \in \mathbb{Z} : \exists k, k' \in \mathbb{Z} \text{ con } m = \alpha k + b k'\}$ multipli di $\alpha +$ multipli di b

$$2\mathbb{Z} + 3\mathbb{Z} = \left\{ \begin{array}{c} 0, 2, 4, \\ \text{mod. 2} \end{array}, \begin{array}{c} 3, 6, 9, \\ \text{mod. 3} \end{array}, \begin{array}{c} 5, 8, \\ 2+3 \end{array}, \begin{array}{c} 7, -1, 1, \dots \\ 2+6 \end{array} \right\} = \mathbb{Z}$$

vedremo $\alpha\mathbb{Z} + b\mathbb{Z} = \text{MCD}(\alpha, b)\mathbb{Z}$

in particolare $\text{MCD}(2, 3) = 1 \quad 2\mathbb{Z} + 3\mathbb{Z} = 1\mathbb{Z}$

• (visto dopo ma utile) invertibili in $\mathbb{Z}/n\mathbb{Z}$

con $n \in \mathbb{N}$,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ [\alpha] : \alpha \in \mathbb{Z} \text{ e } \text{MCD}(\alpha, n) = 1 \right\}$$

le classi dei coprimi di n

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
-8	-17	-14	-11	-8	-5
-10	-19	-16	-13	-10	-7
-12	-21	-18	-15	-12	-9
-14	-23	-20	-17	-14	-11
-16	-25	-22	-19	-16	-13
-18	-27	-24	-21	-18	-15
-20	-29	-26	-23	-20	-17
-22	-31	-28	-25	-22	-19
-24	-33	-30	-27	-24	-21
-26	-35	-32	-29	-26	-23
-28	-37	-34	-31	-28	-25
-30	-39	-36	-33	-30	-27
-32	-41	-38	-35	-32	-29
-34	-43	-40	-37	-34	-31
-36	-45	-42	-39	-36	-33
-38	-47	-44	-41	-38	-35
-40	-49	-46	-43	-40	-37
-42	-51	-48	-45	-42	-39
-44	-53	-50	-47	-44	-41
-46	-55	-52	-49	-46	-43
-48	-57	-54	-51	-48	-45
-50	-59	-56	-53	-50	-47
-52	-61	-58	-55	-52	-49
-54	-63	-60	-57	-54	-51
-56	-65	-62	-59	-56	-53
-58	-67	-64	-61	-58	-55
-60	-69	-66	-63	-60	-57
-62	-71	-68	-65	-62	-59
-64	-73	-70	-67	-64	-61
-66	-75	-72	-69	-66	-63
-68	-77	-74	-71	-68	-65
-70	-79	-76	-73	-70	-67
-72	-81	-78	-75	-72	-69
-74	-83	-80	-77	-74	-71
-76	-85	-77	-74	-71	-68
-78	-87	-74	-71	-68	-65
-80	-89	-71	-68	-65	-62
-82	-91	-68	-65	-62	-59
-84	-93	-65	-62	-60	-57
-86	-95	-62	-59	-56	-53
-88	-97	-59	-56	-53	-50
-90	-99	-56	-53	-50	-47
-92	-101	-53	-50	-47	-44
-94	-103	-50	-47	-44	-41
-96	-105	-47	-44	-41	-38
-98	-107	-44	-41	-38	-35
-100	-109	-41	-38	-35	-32
-102	-111	-38	-35	-32	-29
-104	-113	-35	-32	-29	-26
-106	-115	-32	-29	-26	-23
-108	-117	-29	-26	-23	-20
-110	-119	-26	-23	-20	-17
-112	-121	-23	-20	-17	-14
-114	-123	-20	-17	-14	-11
-116	-125	-17	-14	-11	-8
-118	-127	-14	-11	-8	-5
-120	-129	-11	-8	-5	-2
-122	-131	-8	-5	-2	-1
-124	-133	-5	-2	-1	-4
-126	-135	-2	-1	-4	-7
-128	-137	-1	-4	-7	-10
-130	-139	-4	-7	-10	-13
-132	-141	-7	-10	-13	-16
-134	-143	-10	-13	-16	-19
-136	-145	-13	-16	-19	-22
-138	-147	-16	-19	-22	-25
-140	-149	-19	-16	-22	-28
-142	-151	-16	-19	-22	-31
-144	-153	-19	-16	-22	-34
-146	-155	-16	-19	-22	-37
-148	-157	-19	-16	-22	-40
-150	-159	-16	-19	-22	-43
-152	-161	-19	-16	-22	-46
-154	-163	-16	-19	-22	-49
-156	-165	-19	-16	-22	-52
-158	-167	-16	-19	-22	-55
-160	-169	-19	-16	-22	-58
-162	-171	-16	-19	-22	-61
-164	-173	-19	-16	-22	-64
-166	-175	-16	-19	-22	-67
-168	-177	-19	-16	-22	-70
-170	-179	-16	-19	-22	-73
-172	-181	-19	-16	-22	-76
-174	-183	-16	-19	-22	-79
-176	-185	-19	-16	-22	-82
-178	-187	-16	-19	-22	-85
-180	-189	-19	-16	-22	-88
-182	-191	-16	-19	-22	-91
-184	-193	-19	-16	-22	-94
-186	-195	-16	-19	-22	-97
-188	-197	-19	-16	-22	-100
-190	-199	-16	-19	-22	-103
-192	-201	-19	-16	-22	-106
-194	-203	-16	-19	-22	-109
-196	-205	-19	-16	-22	-112
-198	-207	-16	-19	-22	-115
-200	-209	-19	-16	-22	-118
-202	-211	-16	-19	-22	-121
-204	-213	-19	-16	-22	-124
-206	-215	-16	-19	-22	-127
-208	-217	-19	-16	-22	-130
-210	-219	-16	-19	-22	-133
-212	-221	-19	-16	-22	-136
-214	-223	-16	-19	-22	-139
-216	-225	-19	-16	-22	-142
-218	-227	-16	-19	-22	-145
-220	-229	-19	-16	-22	-148
-222	-231	-16	-19	-22	-151
-224	-233	-19	-16	-22	-154
-226	-235	-16	-19	-22	-157
-228	-237	-19	-16	-22	-160
-230	-239	-16	-19	-22	-163
-232	-241	-19	-16	-22	-166
-234	-243	-16	-19	-22	-169
-236	-245	-19	-16	-22	-172
-238	-247	-16	-19	-22	-175
-240	-249	-19	-16	-22	-178
-242	-251	-16	-19	-22	-181
-244	-253	-19	-16	-22	-184
-246	-255	-16	-19	-22	-187
-248	-257	-19	-16	-22	-190
-250	-259	-16	-19	-22	-193
-252	-261	-19	-16	-22	-196
-254	-263	-16	-19	-22	-199
-256	-265	-19	-16	-22	-202
-258	-267	-16	-19	-22	-205
-260	-269	-19	-16	-22	-208
-262	-271	-16	-19	-22	-211
-264	-273	-19	-16	-22	-214
-266	-275	-16	-19	-22	-217
-268	-277	-19	-16	-22	-220
-270	-279	-16	-19	-22	-223
-272	-281	-19	-16	-22	-226
-274	-283	-16	-19	-22	-229
-276	-285	-19	-16	-22	-232
-278	-287	-16	-19	-22	-235
-280	-289	-19	-16	-22	-238
-282	-291	-16	-19	-22	-241
-284	-293	-19	-16	-22	-244
-286	-295	-16	-19	-22	-247
-288	-297	-19	-16	-22	-250
-290	-299	-16	-19	-22	-253
-292	-301	-19	-16	-22	-256
-294	-303	-16	-19	-22	-259
-296	-305	-19	-16	-22	-262
-298	-307	-16	-19	-22	-265
-300	-309	-19	-16	-22	-268
-302	-311	-16	-19	-22	-271
-304	-313	-19	-16	-22	-274
-306	-315	-16	-19	-22	-277
-308	-317	-19	-16	-22	-280
-310	-319	-16	-19	-22	-283
-312	-321	-19	-16	-22	-286
-314	-323	-16	-19	-22	-289
-316	-325	-19	-16	-22	-292
-318	-327	-16	-19	-22	-295
-320	-329	-19	-16	-22	-298
-322	-331	-16	-19	-22	-301
-324	-333	-19	-16	-22	-304
-326	-335	-16	-19	-22	-307
-328	-337	-19	-16	-22	-310
-330	-339	-16	-19	-22	-313
-332	-341	-19	-16	-22	-316
-334	-343	-16	-19	-22	-319
-336	-345	-19	-16	-22	-322
-338	-347	-16	-19	-22	-325
-340	-349	-19	-16	-22	-328
-342	-351	-16	-19	-22	-331
-344	-353	-19	-16	-22	-334
-346	-355	-16	-19	-22	-337
-348	-357	-19	-16	-22	-340
-350	-359	-16	-19	-22	-343
-352	-361	-19	-16	-22	-346
-354	-363	-16	-19	-22	-349
-356	-365	-19	-16	-22	-352
-358	-367	-16	-19	-22	-355
-360	-369	-19	-16	-22	-358
-362	-371	-16	-19	-22	-361
-364	-373	-19	-16		

La divisibilità è una relazione di inclusione di sottoinsiemi

$$a, b \in \mathbb{Z}^* \quad a|b \iff b \mathbb{Z} \subset a\mathbb{Z} \quad \text{solo se i multipli di } b \text{ sono un sott. dei multipli di } a$$

• Supponiamo $a|b$

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

se $a|b$, allora
ogni multiplo di b può essere riscritto
come $b \cdot$ qualcosa. Ma, per def di $|$, $b = a \cdot$ qualcosa.
quindi, un multiplo di b è un multiplo di a

per definizione, $b = ka \Rightarrow b' = \underbrace{l}_{l'} \underbrace{ka}_{= l'a} = l'a \iff b' \in a\mathbb{Z}$

$$\text{dimostriamo } b\mathbb{Z} \subset a\mathbb{Z} \Rightarrow a|b$$

• Supponiamo $b\mathbb{Z} \subset a\mathbb{Z}$

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

$$\text{ma } b' = lb. \text{ Quindi, } lb = ka \iff b = \underbrace{k}_{k'} \underbrace{l}_{= a} a \quad \text{quindi } b = ka \quad \blacksquare$$

Lemma: $E = a\mathbb{Z} + b\mathbb{Z}$ con $a, b \neq 0$, allora $\exists! \delta \in \mathbb{N}^*$ t.c. $E = \delta\mathbb{Z}$

tutte le
combinazioni sono
multiple di un certo
numero unico

dimostrazione

el. d: $E > 0$

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

• osserviamo che $E^* \neq \emptyset$

- infatti, se $a, b > 0$, esiste una coppia $(k, k') \in \mathbb{N}^2$ t.c. $k_a + k'b > 0$

$\in E^*$

- se invece $a > 0$ e $b < 0$, $\exists (k, k') \in \mathbb{N} \times \mathbb{N}$ t.c. $k_a + k'b > 0$

(e, per $a < 0$, $b > 0$ $\exists (k, k') \in -\mathbb{N} \times \mathbb{N}$ e per $a < 0$, $b < 0$ $\exists (k, k') \in -\mathbb{N} \times -\mathbb{N}$)

• poniamo $\delta = \min(E^*)$ ben definito in \mathbb{N}^* (principio del minimo)

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

infatti $|a| \in E^*$ (perché $E = a\mathbb{Z} + b\mathbb{Z}$) $\subset \delta = \min(E^*)$

• per la DIVISIONE EUCLIDEA $a = q\delta + r$, $r \in \{0, 1, \dots, \delta-1\}$

notiamo che $r = a - q\delta$

$a \in E$, $\delta \in E^* \subset E \implies \delta = ua + vb$ con $u, v \in \mathbb{Z}$

sempre per
 $E = a\mathbb{Z} + b\mathbb{Z}$

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

Ci sono 2 opzioni: ① $r = 0$, $\delta | a$ ($a = q\delta + r$) e abbiamo finito

per $\delta = \min(E^*)$

② altrimenti, $r > 0$ e $r \in E^*$. Se fosse vero, $r \geq \delta$. Ma questo è impossibile per $a = q\delta + r$ con $r \in \{0, 1, \dots, \delta-1\}$

$r \neq \delta$

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

• $\forall \alpha, \beta \in \mathbb{Z}$, $\delta | \alpha a + \beta b \implies E \subset \delta\mathbb{Z}$ per la dim sopra ($a | b \iff b\mathbb{Z} \subset a\mathbb{Z}$)

d'altronde, $\delta \in E \iff \delta = ka + kb$

$\forall l \in \mathbb{Z}$, $l\delta = lk a + lk' b \implies l\delta \in E$

se i multipli di δ sono

elementi di E , allora $\Rightarrow \delta\mathbb{Z} \subset E$

$\delta\mathbb{Z}$ è contenuto in E

(per def $=$)

QUINDI, visto che $E \subset \delta\mathbb{Z}$ e $E \supset \delta\mathbb{Z}$, $E = \delta\mathbb{Z}$

cosa abbiamo fatto? POSTI: $E = a\mathbb{Z} + b\mathbb{Z}$ con $a, b \neq 0$ • $E^* = E \cap \mathbb{N}^*$ (dimostrato $E \neq \emptyset$) • $\delta = \min(E^*)$

notiamo che

• a e b si può riscrivere come $a = q\delta + r$. Questo implica che $r < \delta-1$ (per questioni resto)

• e che $r \in E$, perché $\delta = ua + vb$ e $r = a - q\delta \iff r = a - (ua + vb)$ che porta a $r = a(1-qu) + b(-qv)$

• r può essere $0 > 0 = 0$. Ma se fosse > 0 , dovrebbe essere anche $< \delta-1$ per def resto e $\delta = \min$, il che è IMPOSSIBILE

quindi, $r = 0 \Rightarrow$ abbiamo dimostrato che $\delta | a$ (e $\delta | b$)

δ divide i numeri di E \iff formati da $\alpha a + \beta b$

ora: visto che $\delta | a$ e $\delta | b$, $\delta | a+b$ e $\delta | \alpha a + \beta b$. Questo implica $\delta\mathbb{Z} \supset E$

e, visto che $\delta \in E$ allora i suoi multipli $\in E$. Questo implica $\delta\mathbb{Z} \subset E$

quindi, $\delta\mathbb{Z} \subset E$ e $\delta\mathbb{Z} \supset E \iff \delta\mathbb{Z} = E$

MASSIMO COMUN DIVISORE

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

def $d \in \mathbb{N}$ è MCD di a e b se:

$$\textcircled{1} \quad d | a \text{ e } d | b$$

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

lemma:

se d soddisfa \textcircled{1} e \textcircled{2}, allora è unico.

dim.

Supponiamo che d_1, d_2 soddisfano \textcircled{1} e \textcircled{2}. Mostriamo che $d_1 = d_2$.

$d_2 = k \cdot d_1 \text{ e } d_1 = l \cdot d_2$ quindi d_1 e d_2 devono essere uguali o opposti

$$\text{Si ha } d_2 | d_1 \text{ e } d_1 | d_2 \Rightarrow \{d_1, -d_1\} = \{d_2, -d_2\} \Rightarrow d_1 = d_2$$

• Si scrive $d = \text{MCD}(a, b)$

def COPRIMI \rightarrow Se $\text{MCD}(a, b) = 1$, si dice che a e b sono primi tra loro o coprimi

lemma

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

$$\left(\begin{array}{l} \cdot \text{ se } a=0, b \neq 0 \text{ allora } d = |b| > 0 \\ \cdot \text{ se } a \neq 0, b=0 \text{ allora } d = |a| > 0 \end{array} \right)$$

dim.

$$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \quad \begin{array}{l} \textcircled{1} \supset a\mathbb{Z} \rightarrow d | a \\ \supset b\mathbb{Z} \rightarrow d | b \end{array} \quad \begin{array}{l} \text{condizione } \textcircled{1} \\ \text{verificata} \end{array}$$

$$\textcircled{2} \quad (\text{mostro } d' | d \Leftrightarrow d\mathbb{Z} \subset d'\mathbb{Z})$$

Ogni divisore di
 a e b divide il MCD

per la cond. \textcircled{2}: sia $d' \in \mathbb{N}$ t.c. $d' | a \text{ e } d' | b$

$$d' | a \Leftrightarrow a\mathbb{Z} \subset d'\mathbb{Z} \quad \text{e} \quad d' | b \Leftrightarrow b\mathbb{Z} \subset d'\mathbb{Z}$$

$$\text{quindi } \underbrace{a\mathbb{Z} + b\mathbb{Z}}_{= d\mathbb{Z}} \subset \underbrace{d'\mathbb{Z} + d'\mathbb{Z}}_{\neq 2d'\mathbb{Z}} = d'\mathbb{Z}$$

$$d\mathbb{Z} \subset d'\mathbb{Z} \Leftrightarrow d' | d \quad \text{cond. } \textcircled{2} \text{ verificata}$$

note: se $a \neq 0$, $\text{MCD}(a, 0) = a$

ALGORITMO DI EUCLIDE x MCD

dati: $a, b > 0$ $\delta = \text{MCD}(a, b)$

comincia con la divisione euclidea a, b (\circ $b, a - \text{è uguale}$)

$$a = q_0 b + r_0 \quad (0 \leq r_0 < b) - x \text{ def. resto}$$

$$b = q_1 r_0 + r_1 \quad (0 \leq r_1 < r_0)$$

$$r_0 = q_2 r_1 + r_2 \quad (0 \leq r_2 < r_1)$$

$\therefore r_0, r_1, r_2 \dots$ decrescono - arriveranno ≥ 0

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

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

$\delta !!$ (MCD)

esercizio d'esempio

$$a = 3522, b = 321$$

$$3522 = 10 \cdot 321 + 312$$

$$321 = 1 \cdot 312 + 9$$

$$312 = 34 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

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

$$3522 = 10 \cdot 321 + 312$$

$$321 = 1 \cdot 312 + 9$$

$$312 = 34 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

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

$$3 = \text{MCD}(3522, 321)$$

ma, da qui, sappiamo che vale $\delta \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

$$\Rightarrow \exists u, v \in \mathbb{Z} \text{ t.c. } 3 = 3522u + 321v$$

Come calcolare u e v ? IDENTITÀ DI BÉZOUT

se $a, b \in \mathbb{Z}$ e $d = \text{MCD}(a, b)$ allora $\exists u, v \in \mathbb{Z}$
t.c. $au + bv = d$

Solviamo tra le $\longrightarrow 3 = 9 - 1 \cdot 6$

iterazioni di euclide

e prendiamo

il resto

$$6 = 312 - 34 \cdot 9$$

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

$$3 = -312 + 35 \cdot 9$$

$$9 = 321 - 1 \cdot 312$$

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

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

$$312 = 3522 - 10 \cdot 321$$

$$3 = 35 \cdot 321 - (3522 - 10 \cdot 321) \cdot 36 = 35 \cdot 321 - 3522 \cdot 36 + 321 \cdot 36 \cdot 10 \\ = 321(35 + 360) - 3522 \cdot 36$$

$$3 = 321 \cdot 395 - 36 \cdot 3522$$

abbiamo trovato v e u !! (bravi tutti)

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

dim.

$$\text{MCD}(a, b) = 1 \iff a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$$

Sono primi tra loro ($\text{MCD}=1$)

$$\text{quindi } \exists u, v \in \mathbb{Z} \text{ t.c. } au + bv = 1$$

$$au + bv = 1$$

$$\text{moltiplico tutto per } c \quad acu + bcv = c$$

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

$$acu + bcv = c \iff a(\underbrace{uc + bv}_{\exists 1 \text{ t.c. } c=1}) = c \quad \text{quindi } a|c \quad \blacksquare$$

Lemma $p \in \mathbb{N}, p > 1$, allora p irriducibile $\Rightarrow p$ primo

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

infatti, altrimenti $\exists \delta > 1$ t.c. $\delta | a$, $\delta | p$

ma visto che p irr., $\delta = p \Rightarrow p | a$ CONTRADDIZIONE

Supponiamo $p | ab$ con p irriducibile. (Devo dim. che $p | a$ o $p | b$)

Se $p \nmid a$, ho finito \rightarrow suppongo $p \nmid b$.

Ma allora $a\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}$. Moltiplico tutto per b $\rightarrow \underbrace{ab\mathbb{Z}}_{\text{div per } p} + \underbrace{pb\mathbb{Z}}_{\text{div per } p} = b\mathbb{Z}$ quindi $b\mathbb{Z} \subset p\mathbb{Z} \Rightarrow p | b$ (perché \subset è una rel. di \subset)

fun fact del collega di Pellorin.

James P Jones, Daishachiro Sato, Hideo Wada, Douglas Wiens

$f(a, b, c, \dots, z)$ sostituendo le lettere (variabili) con elementi di \mathbb{N} ottengo elementi di \mathbb{Z}

$$\mathbb{N}^{26} \xrightarrow{f} \mathbb{Z}$$

$$f(\mathbb{N}^{26}) \subset \mathbb{Z} \quad \text{il teorema dice che } f(\mathbb{N}^{26}) \cap \mathbb{N}^* = \{x : x \text{ primo}\} = \{2, 3, 5, 7, \dots\} = \mathbb{P}$$

$$\text{per esempio } f^{-1}(\{13\}) = \emptyset$$

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

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

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

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 $n \pmod{5}$ ha resto da 1 a 4 (quindi mi basta verificare queste classi)

• se $n \equiv_5 0 \iff [n] = [0]$ allora è chiaramente verificato

altr: così:

\bar{n}	$[n]^3$	$[n]^{15}$	$[n]^{17}$	$3[n]$	$3[n]^3$	$2[n]^{15}$	$2[n]^{17}$	$3[n] + 3[n]^3 + 2[n]^{15} + 2[n]^{17}$
$n \equiv 1$	$[1]$	$[1]$	$[1]$	$3[1]$	$3[1]^3$	$2[1]^{15}$	$2[1]^{17}$	$3[1] + 3[1]^3 + 2[1]^{15} + 2[1]^{17}$
	$[1] = [1 \cdot 1 \cdot 1] = [1]$	$[1] = [1 \cdot 1 \cdot 1]$	$[1] = [1]$	$3 \cdot 1$	$3 \cdot 1$	$2 \cdot 1$	$2 \cdot 1$	$3 \cdot 1 + 3 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 = 10 = 0$
$n \equiv 2$	$[2]$	$[3]$	$[2]$	$[1]$	$[3] + [3]$	$[2] + [2]$	$[2] + [2]$	$[1] + [3] + [2] + [2] = 0$
	$[2] = [2 \cdot 2 \cdot 2]$	$[3] = [3 \cdot 3 \cdot 3]$	$[2] = [2]$	$3 \cdot 2 = 6$	$3 \cdot 3 = 9$	$2 \cdot 2 = 4$	$2 \cdot 2 = 4$	$6 + 9 + 4 + 4 = 23 = 0$
$n \equiv 3$	$[3]$	$[2]$	$[2]$	$[3]$	$[4]$	$[1]$	$[4]$	$[3] + [2] + [1] + [4] = 0$
	$[3] = [3 \cdot 3 \cdot 3]$	$[2] = [2 \cdot 2 \cdot 2]$	$[2] = [2]$	$3 \cdot 3 = 9$	$4 \cdot 4 = 16$	$1 \cdot 1 = 1$	$4 \cdot 1 = 4$	$9 + 16 + 1 + 4 = 30 = 0$
$n \equiv 4$	$[4]$	$[4]$	$[4]$	$[4]$	$[2]$	$[2]$	$[3]$	$[4] + [4] + [2] + [3] = 0$
	$[4] = [4 \cdot 4 \cdot 4]$	$[4] = [4 \cdot 4 \cdot 4]$	$[4] = [4]$	$4 \cdot 4 = 16$	$4 \cdot 4 = 16$	$4 \cdot 4 = 16$	$3 \cdot 4 = 12$	$16 + 16 + 16 + 12 = 64 = 0$

studiando le potenze 2 mod 5

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

è ciclico:

$$[2]^5 = [2] \cdot [2]^4 = [2] \cdot [1] = [2] \quad \text{il ciclo è lungo 4, quindi } [2]^m = [2]^{\frac{m}{4} \cdot 4 + r} = [2]^{\frac{m}{4} \cdot 4} \cdot [2]^r = [2]^r$$

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

quindi per calcolare $[2]^n$ basta calcolare $[2]^r$ e 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

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

④ Calcolare $(\mathbb{Z}/N\mathbb{Z})^\times$ con $N \in \mathbb{N}$

$$\cdot A = \mathbb{Z}/N\mathbb{Z} = \mathbb{Z}_{\equiv_N}$$

$$\cdot [a] + [b] = [a+b] \quad e \quad [a] \cdot [b] = [ab] \quad (\text{premesse})$$

• con l'elemento $[0]$ ($= N\mathbb{Z}$) per l'elemento neutro per + e con l'elemento $[1]$ ($= N\mathbb{Z}+1$) per il neutro di \cdot , si ottiene che A è un anello unitario commutativo.

Si cerca

$$A^\times = \{[n] \text{ t.c. } \exists [m] \text{ con } [m] \cdot [n] = [1]\} \quad ("insieme delle unità")$$

③ Si $\exists [a] \in (\mathbb{Z}/N\mathbb{Z})^\times$: esiste $b \in \mathbb{Z}/N\mathbb{Z}$ t.c. $[a] \cdot [b] = [1]$

$$[ab] = [1] \iff N \mid ab - 1 \quad \text{è invertibile} \iff \text{esiste un qualsiasi rapp. quando faccio } ab-1, \text{ è div per } N$$

$$\iff \exists k \in \mathbb{Z} \text{ t.c. } kN = ab - 1$$

porta 1 e kn dall'altra parte

$$\iff ab - kN = 1 \quad \text{è un'identità di Bézout per } a, N$$

$\iff a \text{ e } N$ sono primi fra loro!

$$\text{quindi } (\mathbb{Z}/N\mathbb{Z})^\times = \{[a] : a \in \mathbb{Z} \text{ e } \text{MCD}(a, N) = 1\} \quad \begin{matrix} \text{invertibili in } \mathbb{Z}/N\mathbb{Z} \\ \text{classi dei coprimi a } N \end{matrix}$$

Esiste quindi un'applicazione biiettiva $\{r \in \{0, \dots, N-1\} \text{ t.c. } \text{MCD}(r, N) = 1\} \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times$

$$r \mapsto [r]$$

$$N=24=2^3 \cdot 3 \quad \text{verificare che } (\mathbb{Z}/24\mathbb{Z})^\times = \{r : z \mid r, 3 \nmid r\} \quad \text{tengo i coprimi}$$

$$\text{esempio } (\mathbb{Z}/24\mathbb{Z})^\times = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}, \bar{15}, \bar{16}, \bar{17}, \bar{18}, \bar{19}, \bar{20}, \bar{21}, \bar{22}, \bar{23}\}$$

che cosa si osserva quando N è primo?

$$\cdot N=p \text{ primo} : \quad \text{Si } r \in \{\bar{1}, \dots, \bar{p-1}\}$$

$$\text{MCD}(p, r) = 1 \quad . \quad \text{Altrimenti, qualora si avesse } d = \text{MCD}(p, r) > 1 \quad \text{avrà: } d \mid p, d \mid r \Rightarrow d = p$$

e si avrebbe $p \mid r$. Ma $r < p$ (perché è resto) \rightarrow CONTRADDIZIONE \quad Quindi r coprimo p

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

def CAMP

A anello commutativo unitario t.c. $\forall a \in A \setminus \{0\}$ invertibile
si dice campo

in particolare, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ è un campo

PICCOLO TEOREMA DI FERMAT

es. 5 dato p primo e $n \in \mathbb{Z}$, $n^p \equiv_p n$

Ricordiamo:

$$\bullet \binom{n}{m} = \frac{n!}{m!(n-m)!} = \#\{U \subset \{1, \dots, n\} : \#U = m\} \quad 0 \leq m \leq n$$

in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ campo, ovvero $\mathbb{F}_p^\times = \{[1], [2], \dots, [p-1]\}$
non vero in \mathbb{Z}

$$\bullet \binom{n}{0} = \binom{n}{n} = 1$$

$$\bullet \binom{n}{m} = \binom{n}{n-m}$$

$$\bullet ([a] + [b])^p = [a]^p + [b]^p \text{ con } [a], [b] \in \mathbb{F}_p$$

Sceglieremo rapp. a, b per le classi $[a], [b]$

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{p-2} a^2 b^{p-2} + \binom{p}{p-1} a b^{p-1} + b^p \quad (\text{NEWTON})$$

$\bullet 0 < i < p$ (non $\leq \geq$ perché so che la rid. mod. p di 0 è 0)

SCRIVIAMO $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ * perché è una cardinalità

\bullet SUPPONIAMO $1 \leq i \leq p-1$ e inoltre $i! = i(i-1) \dots 3 \cdot 2 \cdot 1$

quindi, siccome $p > i$, si ha $p \nmid i$ (perché i si scomponono in fattori tutti $< p$ (quindi nessuno di questi è p) e p non può essere il prodotto tra alcuni di questi perché è primo)

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

$$\text{quindi, ho } p! = \underbrace{k}_{\geq} \cdot \underbrace{i!(p-i)!}_{b} \quad (\text{da qui } *) \quad \exists k \in \mathbb{N}^*$$

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

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

$$\text{ma } a = k = \binom{p}{i} \quad \text{perché } p! = \underbrace{\frac{p!}{i!(p-i)!}}_{\text{per def. fattoriale}} \cdot \underbrace{i!(p-i)!}_{b}$$

$(\in [0] \text{ mod } p)$

quindi, tutti i coeff. "in mezzo" nello sv. di Newton (nello forma $\binom{p}{i} \cdot \text{qualcosa}$) si riducono a 0 e rimangono solo a^p e b^p .

\bullet ho dim. che se $1 \leq i \leq p-1$ e p primo, si ha: $\binom{p}{i} = \binom{p}{p-i} \equiv_p 0$

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

TORNIAMO ALLA DIM. PRINCIPALE (PTF)

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

$$[1]^p = [1] \quad [\bar{2}]^p = ([\bar{2}] + [1])^p = [\bar{2}]^p + [1]^p = [\bar{2}] + [1] = [\bar{2}]$$

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

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

which is very cool

if you ask me!!

quindi, $\forall n \in \mathbb{Z}, n^p \equiv_p n$ (con p primo)



$$(x+y)^n = x^n + y^n$$



$$(x+y)^n \neq x^n + y^n$$



for a prime number n , if x and y are members of a commutative ring of characteristic n then
 $(x+y)^n = x^n + y^n$

PRECISAZIONE

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

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

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

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

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

$$\begin{array}{c} \text{Il } [n]^p \\ \text{è } \\ [n'] \cdot \underbrace{[n] [n]^{p-1}}_{\substack{\text{sono} \\ \text{inversi} \\ \text{quindi} = [1]}} = [n'] [n] = [1] \end{array}$$

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

(il PTF ha dei difetti.)

- se $[\alpha] \in \mathbb{F}_p^\times$, calcolare $[\alpha]^{-1}$ usando il PTF

$$\text{So che } [\alpha]^{p-1} = [1] \quad (\text{PTF}).$$

$$\begin{array}{c} \text{Scrivendo } [\alpha]^{p-1} = [\alpha]^{p-2} \cdot [\alpha] \\ \text{(quindi } [1] = \underbrace{[\alpha]^{p-2} \cdot [\alpha]}_{\text{inversi}}) \end{array}$$

$$\text{Dunque } [\alpha]^{-1} = [\alpha]^{p-2}$$

$$\text{es. } p = 689 \quad (\text{primo})$$

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, 442, 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
 08, 216, 432, 173, 346, 1, 689' (689)

ma notiamo che le classi

sono cicliche - possiamo trovare

l'inverso molto prima di 689

- è quello precedente all'1,

perciò sappiamo che $[n]^{p-1} = [1]$
(e cerchiamo $[n]^{p-2}$)

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

③ Nessun intero in $4\mathbb{Z} + 3$

calcoliamo le classi resto modulo 4 dei quadrati

\bar{n}	\bar{n}^2	la somma dei quadrati mod 4 può essere soltanto
0	0	
1	1	
2	0	
3	1	

	+	$\bar{0} \quad \bar{1}$	in particolare, non è mai $\bar{3}$
		$\bar{0} \quad \bar{0} \quad \bar{1}$	
		$\bar{1} \quad \bar{1}$	

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

proprietà

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

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

dim. x induzione con algoritmo di Euclideo

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

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

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

||

$$\left\{ \exists F_n + b F_{n+1} : a, b \in \mathbb{Z} \right\}$$

|| def. Fibonacci

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

ci serve



$$\mathbb{Z} F_{n-1} + \mathbb{Z} F_n$$

così → ipotesi induttiva: $\mathbb{Z} F_{n-1} + \mathbb{Z} F_n = \mathbb{Z}$

(claim)

17/10

claim: = (serve che la funzione sia suriettiva)

$$\left\{ (\alpha+b) F_n + b F_{n-1} : \alpha, b \in \mathbb{Z} \right\} \subseteq \mathbb{Z} F_{n-1} + \mathbb{Z} F_n = \left\{ u F_{n-1} + v F_n : u, v \in \mathbb{Z} \right\}$$

mi serve dim applicazione biiettiva:

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

$$(\alpha, b) \mapsto (\alpha+b, b) \quad \text{sia } f(\mathbb{Z}^2) \text{ l'immagine} = \{ u F_n, v F_{n-1} : (u, v) \in f(\mathbb{Z}^2) \}$$

se lo dimostro, dimostro che

ogni volta che prendo α, b posso trovare u e v t.c. $u = \alpha + b$, $v = b$ e viceversa

(basta che sia suriettiva)
ma dimostriamo biiettiva

Mostriamo f suriettiva - questo basta per giustificare il claim

Possiamo mostrare che f biiettiva (+ forse)

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

prop del corso $\Rightarrow f$ biiett. $\iff \exists g: B \rightarrow A$ t.c. $f \circ g = \text{Id}_B$ ($\forall b \in B, f(g(b)) = b, \forall a \in A, g(f(a)) = a$)

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

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

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

inverso

$$\text{pongo } g: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2, \quad g(u, v) \mapsto (u-v, v)$$

$$\begin{aligned} (f \circ g)(u, v) &= f(g(u, v)) = f(u-v, v) = u-v+v, v = (u, v) \\ (g \circ f)(a, b) &= g(f(a, b)) = g(a+b, b) = (a+b-b, b) = (a, b) \end{aligned} \quad \left. \begin{array}{l} \text{x fibonacchi indice } \geq 0 \\ \text{sono identità:} \\ f \text{ e } g \text{ biiettive} \end{array} \right\}$$

$$\begin{aligned} \text{Abbiamo dimostrato } \forall n > 0 \quad F_{n+1} \mathbb{Z} + F_n \mathbb{Z} &= F_n \mathbb{Z} + F_{n-1} \mathbb{Z} = F_{n-1} \mathbb{Z} + F_{n-2} \mathbb{Z} = \dots = F_1 \mathbb{Z} + F_0 \mathbb{Z} = \\ &= F_1 \mathbb{Z} + \{0\} = \mathbb{Z} \end{aligned}$$

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

Esercizio 5 Dimostrare che $2^n \not\equiv 1 \pmod{n}$ $\forall n > 1$ x CASA

$$2^n \not\equiv_n 1 \quad \forall n > 1$$

$$n^p \equiv_p n \quad \text{e } n^{p-2} \text{ inverso } n^p$$

$$n^{p-1} \equiv_p 1$$

2 casi:

$$\textcircled{1} \quad n \text{ primo} \rightarrow \text{Fermat: } [2^{n-1}]_n = [1]_n$$

$$[2^n] = [2^{n-1}] \cdot [2] = [1] \cdot [2] = [2]$$

$$\textcircled{2} \quad n \text{ non primo} \rightarrow n = a, b \text{ con } 1 < a < n, \quad 1 < b < n$$

$$\text{sicuramente } n = p \cdot k \text{ con } p \text{ primo e } 2^n = 2^{pk} = (2^p)^k$$

TEOREMA FONDAMENTALE DELL'ARITMETICA

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

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

② $\alpha = (\pm 1) \cdot \prod_{\substack{p \\ \text{primo}}} p^{v_p(\alpha)}$ dove $v_p(\alpha) \in \mathbb{N}$ unicamente determinato.

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

OSS

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

Siccome

$$\forall \alpha \in \mathbb{Z}, I_\alpha \text{ è finito, } \prod_{\substack{p \\ \text{primo}}} p^{v_p(\alpha)} = \prod_{p \in I_\alpha} p^{v_p(\alpha)} \cdot \prod_{p \notin I_\alpha} p^{v_p(\alpha)}$$

sarà 0 ("non ci servono")

posso dividere i primi in divisori di α e non-divisori di α e suddividere la produttoria

ESEMPIO:

$$\begin{aligned} \alpha = 7! &= 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \\ &= 7 \cdot 2 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 2 \\ &= 7 \cdot 5 \cdot 3^2 \cdot 2^4 \end{aligned}$$

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

OSS: dato $\alpha = \prod_p p^{v_p(\alpha)}$ e $b = \prod_p p^{v_p(b)}$

$$\begin{aligned} \alpha = 12 &= 2^2 \cdot 3 \\ b = 15 &= 5 \cdot 3 \implies v_2(\alpha) = 2 & v_2(b) = 0 \\ & & v_3(\alpha) = 1 & v_3(b) = 1 \end{aligned}$$

$$\bullet \alpha \cdot b = \prod_p p^{v_p(\alpha)} \prod_p p^{v_p(b)} = \prod_p p^{v_p(\alpha) + v_p(b)}$$

$$v_5(\alpha \cdot b) = 0 \quad v_5(b) = 1$$

$$\bullet p^{v_p(\alpha)} p^{v_p(b)} = p^{v_p(\alpha) + v_p(b)}$$

$$v_p(\alpha \cdot b) = v_p(12 \cdot 15) = v_p(\alpha) + v_p(b)$$

(enunciato) $\forall \alpha > 0, \exists$ un numero finito di primi distinti p_1, \dots, p_r t.c. $\alpha = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$
e questa fattorizzazione è unicamente determinata.

$$v_2(\alpha \cdot b) = 2 \quad v_3(\alpha \cdot b) = 2 \quad v_5(\alpha \cdot b) = 1 \quad v_p(\alpha \cdot b) = 0 \quad p \geq 7$$

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

• posso supporre $\Delta > 0$ senza perdita di generalità

① Supponiamo per assurdo \mathbb{P}_{Δ} infinito - vuol dire che esiste una collezione infinita di primi t.c. $p \mid \Delta$

ma $p \mid \Delta \Rightarrow p \leq \Delta$ e impossibile infiniti interi $\leq \Delta$ contr.

② Procediamo per induzione:

$$\cdot \Delta = 1 \quad V_p(1) = \emptyset \quad \forall p \quad 1 = \prod_p p^0 = 1 \cdot 1 \cdot 1 \cdots 1 = 1$$

• Supponiamo $\Delta > 1$.

dove così ① Δ primo \rightarrow allora $\Delta = \prod_p p^{v_p(\Delta)} \quad V_p(\Delta) = \begin{cases} \emptyset & p \neq \Delta \\ 1 & p = \Delta \end{cases}$

② Δ non primo, Δ non è irriducibile

si può scrivere in fattori diversi da 1 e Δ

$$\Rightarrow \Delta = U \cdot V \quad \text{con} \quad 1 < U < \Delta \quad \& \quad 1 < V < \Delta$$

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

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

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

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 $V_p(a) < V_p(b)$

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

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

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

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

• supponiamo $a|b$

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

per il teorema fondamentale:

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

osservo che
 ≥ 0 perché
k intero

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

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

$$\forall p, V_p(b) \geq V_p(a) \blacksquare$$

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

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

③ $\forall p, V_p(\delta) \leq V_p(a) \quad e \quad V_p(\delta) \leq V_p(b)$

② Se $\exists d' \text{ t.c. } \forall p \quad v_p(d') \leq v_p(a) \leftarrow v_p(d') \leq v_p(b)$

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

③ $\iff v_p(\delta) \leq \min(v_p(a), v_p(b))$

④ \iff se d' è tale che $v_p(d') \leq \min(v_p(a), v_p(b))$

Allora $v_p(d') \leq v_p(\delta)$

$\forall p, \quad v_p(\delta)$ 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 $i \leq, i \neq$)

Esercizio

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

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

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

Come dimostrare la lezione:

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

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

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

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

3 casi:

$$\textcircled{1} \min = z$$

$$\textcircled{2} \min = x$$

$$\textcircled{3} \min = y$$

$$\begin{aligned} \text{qui } \min(x, z) &= z \text{ e } \min(y, z) = z \\ \text{e } \min(x, y, z) &= z \end{aligned}$$

$$\begin{aligned} \text{qui } \min(x, z) &= x \\ \text{e } \min(y, z) &= z \circ y \end{aligned}$$

$$\begin{aligned} \text{qui } \min(y, z) &= y \\ \text{e } \min(x, z) &= x \circ z \end{aligned}$$

$$\begin{aligned} \text{quindi } z+z &= z+k \\ \text{ovvero } k &= z \end{aligned}$$

$$\begin{aligned} x+z &= x+k \\ \text{ovvero } k &= z \end{aligned}$$

$$\begin{aligned} x+y &= x+k \\ \text{ovvero } k &= y \end{aligned}$$

$$\begin{aligned} x+y &= y+k \\ k &= x \\ k &= z \end{aligned}$$

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

DIVISORI DI ZERO

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

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

ma in \mathbb{Z} non succededef $\alpha \in A$ è divisore di zerose $\exists b \in A \setminus \{0\}$ t.c. $\alpha b = 0_A$ in A qualiasi (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 $\forall \alpha \in K \setminus \{0\}$, α invertibile $K^\times = K \setminus \{0\}$ L'unico divisore di zero in K è 0_K dim • Supponiamo α divisore di zero:da qui in poi usiamo 0 per 0_K

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

però b è invertibile $\rightarrow \exists b^{-1} \in K^\times$ t.c. $b \cdot b^{-1} = 1_K$ quindi posso moltiplicare termine α termine per b^{-1}

$$\underbrace{\alpha b b^{-1}}_1 = \underbrace{0}_0 b^{-1}$$

$$\alpha = 0$$

in \mathbb{Z} in \mathbb{Z} , se α è divisore di 0 , allora $\alpha = 0$ (anche se \mathbb{Z} non è un campo)dim • sia α divisore di zero $\iff \exists b \in \mathbb{Z}^* \text{ t.c. } \alpha b = 0 \quad (-\alpha)(-\alpha) = \alpha b = 0$ Senza perdita di generalità, supponiamo $\alpha \geq 0$

$$\exists b \text{ t.c. } \alpha b = 0 \iff 0 = \alpha b = \underbrace{b + b + b + \dots + b}_{\alpha \text{ volte}} \geq b > 0$$

questo è impossibile se $\alpha > 0$.quindi, $\alpha = 0$ ■def dominiodato A snello, $A \neq \{0\}$, 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) (noi 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 $\rightarrow N$ 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 $\rightarrow \exists a, b, 1 < a < n, 1 < b < n$ t.c. $N = ab$

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

dimostriamo che N primo $\rightarrow \mathbb{Z}/N\mathbb{Z}$ dominio

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

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

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

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

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

Quindi, uno dei due divisori è zero

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

Lemma legge di cancellazione (in A snello)

Se $\alpha \in A$ non divisore di zero, allora $\alpha b = \alpha c \implies b = c$

dim:

$$\alpha b = \alpha c \iff \alpha(b-c) = 0 \quad \text{visto che } \alpha \text{ non è divisore di } 0 \implies b-c = 0 \iff b = c$$

$\alpha \neq 0$

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

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

$$\alpha X = b \quad \alpha, b \in A$$

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

- in $A = \mathbb{Z}$ una soluzione di $\alpha X = b$ esiste $\iff \alpha | b$

infatti, se l'insieme delle soluzioni $\neq \emptyset$ e se
 x soluzione, si ha $\alpha x = b \iff \alpha | b$ (def. |)

Se, invece, $\alpha | b \implies \exists k \in \mathbb{Z}$ t.c. $b = \alpha k$ e prendo $k = x$

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

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

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

$$\alpha X = b$$

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

$$\underbrace{\alpha^{-1} \alpha}_1 X = \alpha^{-1} b \quad \text{quindi l'eq. ha l'unica soluzione } X = \alpha^{-1} b$$

(es $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$)

- Se per esempio $A = K$ campo

$$\alpha X = b \quad \text{con } \alpha \neq 0 \quad \text{ammette sempre l'unica soluzione } X = \alpha^{-1} b$$

proposizione $\exists X = b \quad \exists, b \in A = \mathbb{Z}/n\mathbb{Z}$

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

dim:

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

$$[\alpha][x] - [\beta] = [0]$$

quindi $\exists n \in \mathbb{Z}$ quindi multiplo
di n

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

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

$\beta \in \text{multiplo}$
 $\text{di } \delta$

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

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

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

\times def congr. mod

$$\iff \beta \equiv_n u\alpha \iff [\beta] = [u][\alpha]^{=\delta} \quad b = x\delta$$

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

$$\alpha = 3, \beta = \emptyset, n = 6 \quad \text{MCD}(\alpha, n) = 3 \mid \emptyset = \beta$$

ci sono soluzioni. $X = [2]$ è soluzione ($[3] \cdot [2] = [6] = [0] \text{ in } \mathbb{Z}/6\mathbb{Z}$)

$X = [4]$ è soluzione ($[3] \cdot [4] = [12] = [0]$)

o anche $[3] \cdot [2] \cdot [2] = [0] \cdot [2] = [0]$)

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

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

parentesi tutoraggio: equazioni diofantee

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

① Calcolo l'MCD (a, b)

$$858 = 3 \cdot 253 + 99$$

$$253 = 2 \cdot 99 + 55$$

$$99 = 1 \cdot 55 + 44$$

$$55 = 1 \cdot 44 + 11$$

$$44 = 4 \cdot 11 + 0$$

$$d = \text{MCD}(858, 253) = 11$$

② Mi assicuro che l'MCD divide c

(altrimenti, l'eq. non ha soluzioni)

$$11 \mid 33 ? \text{ sì}$$

③ Calcolo l'identità di Bézout

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

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

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

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

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

$$\text{quindi } 11 = -5a + 17b$$

④ Devo trovare $\underline{\underline{33}} = x\underline{a} + yb$: moltiplico a dx e sx per arrivare al numero che cerco

$$11 = -5a + 17b$$

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

ho trovato x_0 e y_0 soluzioni particolari dell'equazione

⑤ Trovo le soluzioni generali

(Soluzioni intere dell'omogeneo associato)

(termine non moltiplicato da x_0)

$$x = x_0 + \frac{b}{\text{MCD}(a, b)} K \quad K \in \mathbb{Z}$$

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

$$\text{quindi } x = -15 + \frac{253}{11} K = -15 + 23K$$

$$K \in \mathbb{Z}$$

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

Lemma

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

dim:

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

$$\implies a | bh \quad (\text{o anche } b | ah, \text{ ma sceglieremo } a | bh)$$

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

• $\text{MCD}(a, b) = 1 \iff b$ è invertibile modulo a

$$\iff \exists b' \in \mathbb{Z} \text{ t.c. } bb' \equiv 1 + a\mathbb{Z}$$

(b invertibile se $by \equiv 1$ ovvero $by - 1 \equiv 0$
 $\iff by - k \equiv 1 \quad \text{MCD}(a, b) = 1 \iff ax + by = 1$
 prendo $x = -k$ e queste cose sono uguali)

$$\begin{aligned} \bullet \text{ Dicendo } a | bh &\implies a | b' | b'b h = (1 + ak)h \iff a | b' = h + ahk \\ &\iff ab' - ahk = h \iff a(b' - hk) = h \quad \text{quindi } a | h \blacksquare \end{aligned}$$

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 $\text{MCD}(r_i, r_j) = 1 \quad \forall i \neq j$ \Rightarrow due coprimi

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

Allora il sistema

$$(*) \left\{ \begin{array}{l} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ \vdots \\ x \equiv c_s \pmod{r_s} \end{array} \right. \text{ ha un'unica soluzione modulo } R := r_1 \cdot r_2 \cdot \dots \cdot r_s$$

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

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

$$\bullet R = r_1 \cdot r_2 \cdot \dots \cdot r_s \quad \bullet \text{ poniamo } R_i = \frac{R}{r_i} = r_1 \cdot r_2 \cdot \dots \overset{\text{"non } c_i \text{ in "}}{r_i} \cdot \dots \cdot r_s = r_1 \cdot r_2 \cdot \dots \cdot r_{i-1} \cdot r_{i+1} \cdot \dots \cdot r_s$$

e notiamo che $\text{MCD}(R_i, r_i) = 1$ (perché r_i, r_j ecc primi fra loro e in R_i "manca" proprio r_i)

Visto che sono primi fra loro, questa proprietà può essere riformulata dicendo che $[R_i]$ classe di R_i in $\mathbb{Z}/r_i\mathbb{Z}$

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

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

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

* credo che "basti" il lemma di Gauss? Sospendo e $\text{MCD}(a, b) = 1$
 $a | bh$ e $\text{MCD}(a, b) = 1$ allora $a | bc \Rightarrow a | c$
 allora $a | h$
 (combinano i vincoli, per Gauss $a, b \in \mathbb{Z}^*$
 e non \mathbb{Z} , ma non credo ci sarebbe
 perdita di generalità chiedere
 al prof.)

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

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

Quindi $x_0 = \sum_{j=1}^s y_j R_j = \sum_{\substack{j=1 \\ j \neq i}}^s y_j R_j + y_i R_i$ isoliamo il termine non divisibile per r_i (quindi il resto)
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 $c_i \text{ mod } r_i$

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

$$\begin{aligned} *_{(H)} & \left\{ \begin{array}{l} x \equiv 0 \pmod{r_1} \\ x \equiv 0 \pmod{r_2} \\ \vdots \\ x \equiv 0 \pmod{r_s} \end{array} \right. & x \equiv_{r_i} 0, \quad i=1 \dots s \end{aligned}$$

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

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

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

Quindi, l'insieme delle soluzioni di $(*_{(H)})$ è $E_H = R\mathbb{Z}$ (i multipli di R)

proposizione

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

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

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

• Addizionando con x_0 , che è soluzione particolare, ottengo $x \equiv_{r_i} c_i + 0 \equiv c_i \pmod{r_i}$

• Dimostriamo $E_* \subset x_0 + R\mathbb{Z}$

$$x \equiv_{r_i} c_i \iff x - c_i \equiv_{r_i} 0$$

(old sistema)

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

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

$\implies x \in x_0 + R\mathbb{Z} \implies E_* \subset x_0 + R\mathbb{Z}$

piccola parentesi pratico: quello che ci hanno detto al TUTORAGGIO sul teorema cinese del resto

$$\left\{ \begin{array}{l} x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{2} \end{array} \right. \quad \begin{array}{l} \cdot r_1 = 11, \quad r_2 = 5, \quad r_3 = 2 \\ \text{se sono coprimi, ammette un'unica soluzione modulo R} \end{array}$$

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

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

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 $c_1 = 1 \quad c_2 = 2 \quad c_3 = 1$

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

③ $\bar{x}_i = R_i x \equiv_r c$

• $\bar{x}_1 = 10x \equiv 1 \pmod{11}$

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.: • $\text{MCD}(10, 11) = 1$

Bézout $1 = 10 \cdot \underline{-1} + 11 \cdot 1$

(ho trovato)

x_0 particolare

$22 = 4 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

quindi (Bézout)

$1 = 5 - 2 \cdot 2$

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

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

• $\bar{x}_3 = 55x \equiv 1 \pmod{2}$

55 è dispari, quindi

$\equiv 1 \pmod{2}$

$1x \equiv 1 \pmod{2}$

$[x_3] \equiv [1] \pmod{2}$

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

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

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

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

ma qui cerchiamo $= 2^*$

quindi moltiplico per 2

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

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

Siamo in
 $\pmod{11}$

quindi $[x_1] \equiv [-1] \equiv [10]$

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

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

$177 - 110$

$$[x] = 10 \cdot 10 + 22 \cdot 1 + 55 \cdot 1 + 110k = 177 + 110k = 67 + 110k$$

Esercizio 8 (foglio 3)

Esercizio 8. Trovare tutti gli interi $x \in \mathbb{Z}$ che soddisfino

- (i) $4x \equiv 7 \pmod{15}$
- (ii) $6x \equiv 8 \pmod{9}$
- (iii) $\begin{cases} 1025x \equiv 5312065 \pmod{8} \\ 36x \equiv 322 \pmod{5} \\ 4x \equiv 7 \pmod{3} \end{cases}$
- (iv) $4x \equiv 3 \pmod{385}$.

METODO PELLARIN CRT

$$\textcircled{1} \quad 4x \equiv 7 \pmod{15}$$

① calcolo l'MCD tra 4 e 15

$$\text{MCD}(4, 15) = 1 \iff [4] \text{ invertibile mod. 15}$$

$$\exists n \in \mathbb{Z} \text{ t.c. } 4 \cdot n \equiv_1 1 \quad (\text{es. } n=4)$$

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

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

$$4 \cdot 4x \equiv_{15} 28$$

$$x \equiv_{15} 13$$

(moltiplichi con resto 13)

$$\text{quindi, le sol. sono } \mathcal{E} = 15\mathbb{Z} + 13$$

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

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

② semplifichiamo le congruenze

$$\textcircled{4} \pmod{8} \quad 1025 = 1024 + 1 = 2^{10} + 1 = \underbrace{(2^3)^2 \cdot 2}_{\equiv_8 0 \text{ perciò}} + 1 \equiv 1 \pmod{8}$$

$$\cdot 5312065$$

$$\textcircled{5} \quad 8 \mid 40 \quad \text{quindi } 8 \mid 40 \cdot 10\mathbb{Z}$$

$$\text{notiamo che } 5312065 = 4000000 + 1312065$$

$$\text{visto che } 8 \mid 4 \cdot 10^6 \quad 5312065 \equiv_8 1312065$$

$$8 \mid 1200000 \equiv_8 112065 \quad 8 \mid 120000 \equiv_8 -7935$$

$$8 \mid 8000 \equiv_8 65 \equiv_8 1$$

il sistema diventa quindi

$$\begin{cases} x \equiv_8 1 \\ x \equiv_5 2 \\ x \equiv_3 1 \end{cases}$$

$$\textcircled{6} \quad \text{calcoliamo le altre cose: } R = 3 \cdot 5 \cdot 8 = 120$$

$$R_1 = r_2 r_3 = 15$$

$$R_2 = r_1 r_3 = 24$$

$$R_3 = r_1 r_2 = 40$$

$$\textcircled{2} \quad 6x \equiv 8 \pmod{9}$$

notiamo che 6 e 9 non sono coprimi.

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

$$\iff 8 = \underbrace{6x - 9k}_{\text{ma questo è impossibile}}$$

notiamo che questi sono divisibili per 3 (MCD 3, 9)

mentre 8 non lo è

$$\mathcal{E} = \emptyset$$

$$\textcircled{2} \cdot 36 \equiv_5 1$$

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

$$\textcircled{3} \cdot 4 \equiv_3 1$$

$$\cdot 7 \equiv_3 1$$

④ troviamo gli inversi S_i :

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

$$R_2 = 24 \quad 24 \cdot 4 \stackrel{-1}{\equiv} 1 \quad S_2 = 4$$

$$R_3 = 40 \quad 40 \cdot 1 \stackrel{-1}{\equiv} 1 \quad S_3 = 1$$

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	$8 \stackrel{-1}{\equiv} 3$
3	1	1	1

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

$$\text{Soltuzione generale: } E = 217 + 120Z$$

POLINOMI in una indeterminata \Rightarrow 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

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

$\alpha_i = 0 \quad \forall i > 0$ (abbastanza grande)

esempio

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

→ insieme di 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:

$$\text{con } P = \sum_{i \geq 0} \alpha_i X^i \quad \alpha_i = 0 \quad \forall i > 0 \quad Q = \sum_{i \geq 0} b_i X^i \quad b_i = 0 \quad \forall i > 0$$

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

prodotto di Cauchy

- $P \cdot Q := \sum_{k \geq 0} c_k X^k \quad \text{con } c_k = \sum_{i+j=k} \alpha_i b_j \quad \begin{array}{l} \text{(qui si nota che } c_k = 0 \quad \forall k > 0 \\ \text{- per numeri abbastanza grandi,} \\ \alpha_i e b_j saranno 0 \end{array}$

→ grado di un polinomio

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

$$\deg(P) = \max \{i \in \mathbb{N}, \alpha_i \neq 0\} \quad \text{grado massimo} \quad \bullet \text{ Si pone } \deg(0) := -\infty$$

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

- 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")

Lemmas

$$\textcircled{1} \quad \deg(\alpha) = -\infty \iff \alpha = 0$$

$$\textcircled{2} \quad \deg(\alpha b) = \deg(\alpha) + \deg(b)$$

$$\textcircled{3} \quad \deg(\alpha + b) \leq \max(\deg(\alpha), \deg(b))$$

$$\text{e } \deg(\alpha + b) = \max(\deg(\alpha), \deg(b)) \text{ se } \deg(\alpha) \neq \deg(b)$$

se i gradi sono uguali gli el. di grado maggiore si potrebbero annullare e il grado sarebbe < (es. $(x^3+x) + (-x^3+2)$)

$$\text{es. } \alpha = x^2 + x + 1 \quad \deg = 2 \quad b = x + 1 \quad \deg = 1 \quad \alpha + b = x^2 + 2x + 2 \quad \deg = 2$$

ANALOGIE TRA I POLINOMI E \mathbb{Z}

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

anello di polinomi
Compone

operazioni:

$$\cdot \mathbb{Z} \xrightarrow{1:1} \mathbb{N} \quad \text{val assoluto}$$

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

proprietà

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

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

$$\textcircled{1} \deg(a) = -\infty \iff a = 0$$

$$\textcircled{2} \deg(ab) = \deg(a) + \deg(b)$$

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

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 $c > 1$

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

Allora proprietà

$$\textcircled{1} |a|_c = 0 \iff a = 0$$

$$\textcircled{2} |ab|_c = |a|_c \cdot |b|_c$$

$$\textcircled{3} |a+b|_c \leq \max(|a|_c, |b|_c) \leq |a|_c + |b|_c$$

invece, se $P = 0$

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

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

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

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 colonne

$$\begin{array}{l} a = x^4 + x + 1 \\ b = x^3 - 2 \end{array} \quad \begin{array}{r} x^4 + \\ x^3 - 2 \\ \hline x^4 \end{array} \quad \begin{array}{r} x+1 \\ -2x \\ \hline 0 \end{array} \quad \begin{array}{r} x^3 \quad -2 \\ \hline x \end{array} \quad \begin{array}{r} x^4/x^3 \\ \textcircled{1} \\ \textcircled{2} \end{array} \quad \begin{array}{l} \textcircled{1} x^4/x^3 \\ \textcircled{2} \text{ moltiplico per } (x^3 - 2) \end{array}$$

grado <
quindi fine

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

\mathbb{Z} $A = K[x]$

inter:	polinomi	TABELLA ANALOGIE TRA \mathbb{Z} e $K[x]$
divisione euclides	divisione euclides	(il grande ripasso delle proprietà di \mathbb{Z})
valore assoluto	$ \cdot _c \circ \deg$	

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

$A^+ = \{ \text{polinomi monici} \}$
 in forma $P = a_0 + a_1 x + \dots + a_n x^n$
 con $a_n \neq 0$ (coeff. grado massimo)
 il prodotto di monici è monico
 (ma la somma non necessariamente)

 $\mathbb{Z}^\times = \{ \pm 1 \}$

inversi sui polinomi:

$$\begin{aligned} A^\times &= K^\times \\ \text{sia } a \in A^\times \exists b \in A^\times \text{ t.c. } ab &= 1 \\ \implies \deg(a) + \deg(b) &= 0 \quad (\deg(ab) = 0 = \deg(a) + \deg(b)) \\ \implies \deg(a) = \deg(b) &\in \mathbb{N} \text{ (o avrei } -\infty) \\ \implies \deg(a) = \deg(b) &= 0 \\ \implies a, b \in K^\times &(\text{"costanti" diverse da } 0) \end{aligned}$$

divisibilità in \mathbb{Z}

$$\begin{aligned} a|b &\iff \exists H \in \mathbb{Z} \text{ t.c. } b = ah \\ a|b &\iff b \in a\mathbb{Z} \\ \exists k \in \mathbb{Z} \text{ t.c. } b &= ak \\ \iff b &\in a\mathbb{Z} \\ \iff b\mathbb{Z} &\subset a\mathbb{Z} \\ \iff ba &\subset aA \end{aligned}$$

proprietà di $|$ su A

$$\begin{aligned} \textcircled{1} \text{ riflessiva} \\ \textcircled{2} \text{ transitiva} \\ a|b, b|c \iff c \in aA &\iff aA \subset bA \subset cA \\ \iff cA &\subset aA \iff a|c \\ \textcircled{3} \text{ quasi riflessiva ma non:} \end{aligned}$$

$$\begin{aligned} a, b \in A. \text{ Supponiamo } a|b \wedge b|a \\ \iff \exists u \in A \text{ t.c. } b = au, \exists v \in A \text{ t.c. } a = bv \\ \text{quindi } a = uv \iff \deg(a) = \deg(u) + \deg(v) + \deg(a) \\ \text{possiamo supporre } a, b \neq 0 \\ \deg(a) = \deg(a) + \deg(u) + \deg(v) \iff 0 = \deg(u) + \deg(v) \\ \iff \deg(u) = \deg(v) = 0 \\ \iff u = \lambda \in K^\times, v = \mu \in K^\times \quad (\text{sempre per la questione } \deg(0) = \text{"costante" } \neq 0) \end{aligned}$$

Quindi $\exists \lambda \in K^\times = A^\times \text{ t.c. } b = \lambda a$

Lemmas $A = K[X]$ è un dominio d'integrità

\mathbb{Z} è un dominio d'integrità

dim Sia $P \in A$ divisore di zero

$$\exists Q \in A \setminus \{\emptyset\} \text{ t.c. } PQ = \emptyset$$

$$\deg(PQ) = \deg(\emptyset) = \deg(P) + \deg(Q) = -\infty$$

impossibile somma due numeri $\in \mathbb{N} = -\infty$

$$\text{Quindi } \deg(P) = -\infty \iff P = \emptyset$$

$$a \equiv b \pmod{n}$$

$$\iff n | a - b$$

$$a, b \in A, H \in A \setminus \{\emptyset\}$$

$$a \equiv b \pmod{H} \text{ rel d'eq.}$$

es. transitività $a \equiv_H b, b \equiv_H c$

$$\iff H | a - b \wedge H | b - c$$

$$\iff a - b = Hv \quad \exists v \in A, b - c = Hw \quad \exists w \in A$$

$$a - b + b - c = H(v + w)$$

$$\iff H | a - c \iff a \equiv_H c$$

$$A/H \text{ snello}$$

commutativo unitario

$$A/H = \{[x] : x \in A\} = \{x + HA : \deg(x) < \deg(H)\}$$

$$a \in A, [a] = a + HA \subset A$$

$$\text{Sistema compl. Rapp. mod } H = \{a \in A : \deg(a) < \deg(H)\}$$

de: MCD in \mathbb{Z}

de: MCD in A

Bézout in \mathbb{Z} :

$$a, b \in A, \text{ poniamo } aA + bA = \{m \in A \text{ t.c. } \exists u, v \in A \text{ con } m = ua + vb\}$$

Lemmas Bézout in $A = K[X]$

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

$$\text{allora } aA + bA = \Delta A \quad \exists! \delta \in A^+$$

dimostri che \mathcal{E}^+ contiene un el. di grado minimo unico (δ)

(mostrare non vuoto $(a, b) \neq \emptyset$, principio Minimo)

$$\mathcal{E} = aA + bA, \quad \mathcal{E}^+ = \{m \in \mathcal{E} \text{ t.c. } m \in A^+\}$$

monico
(notiamo che infatti è l'insieme "analogo" a \mathbb{N}^* in A)

MCD

$$(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$$

prop. $\exists! d \in \mathbb{N}^* \text{ t.c.}$

$$\textcircled{1} \quad d | a \wedge d | b$$

\textcircled{2} se $d' \in A$ t.c.

$$d' | a \wedge d' | b \Rightarrow d' | d$$

MCD

$$(a, b) \in A^2 \setminus \{(0, 0)\}$$

prop. $\exists! d \in A^+ \text{ t.c.}$

$$\textcircled{1} \quad d | a \wedge d | b$$

\textcircled{2} se $d' \in A$ t.c.

$$d' | a \wedge d' | b \Rightarrow d' | d$$

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

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

$$\text{coprimi } a, b \in \mathbb{Z} \text{ t.c. } \text{MCD}(a, b) = 1$$

$$\text{coprimi } a, b \in A \text{ t.c. } \text{MCD}(a, b) = 1$$

irriducibile $a \in A \setminus A^\times$

a irriducibile se $\forall b, c \in A : a = bc$

allora $\circ b \in A^\times \circ c \in A^\times$

primo $a \in A \setminus A^\times, a \neq \emptyset$

primo se $a | bc \Rightarrow a | b \circ a | c$

Lemmas: primo \iff irriducibile

irriducibile $P \in A \setminus A^\times \quad (\deg(P) > 0)$

P è irriducibile se, scrivendo $P = QR$

allora si ha $\circ Q \in A^\times \circ R \in A^\times (= K^\times)$

osservazione:

$X - x$ è irriducibile $\forall x \in K$

$$X - x = U \cdot V$$

$$\deg(X - x) = \deg(U) + \deg(V)$$

$$\Rightarrow \{\deg(U), \deg(V)\} = \{0, 1\} \text{ almeno uno è invertibile (di grado 0)}$$

Lemmas: P irriducibile $\iff P$ primo

Teorema Fondamentale Aritmetica

$\forall a \in \mathbb{Z}^*$ a si decomponga
in modo unico come:

$$d = (\pm 1) \cdot \prod_{p \text{ primo}} p^{v_p(a)}$$

$v_p(a) \in \mathbb{N}$, $\{p : v_p(a) \neq 0\}$ finito

Teorema della Fattorizzazione Unica

Ogni $H \in A - \{\emptyset\}$ si decomponga
in modo unico come prodotto:

$$H = \lambda \cdot \prod_{\substack{P \text{ irr.} \\ P \in A^+}} P^{v_P(H)} \quad v_P(H) \in \mathbb{N} \text{ e} \\ \{P : v_P(H) \neq 0\} \text{ finito}$$

FATTORIZZAZIONE

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 $\deg(P) = 2$

$$(P = X^2 + \alpha X + b) \text{ allora } \Delta = \alpha^2 - 4b < 0$$

def VALUTAZIONE

dati $k \in K$, $F \in K[X] = F_0 + F_1X + \dots + F_nX^n$

la valutazione di F in x

è $ev_x(F) = F_0 + F_1x + \dots + F_nx^n$ (è la "sostituzione" di X)

$$ev: K[X] \longrightarrow K$$

OSSERViamo:

$$\textcircled{1} ev_x(F+G) = ev_x(F) + ev_x(G)$$

$$\textcircled{2} ev_x(F \cdot G) = ev_x(F) \cdot ev_x(G)$$

$$\textcircled{3} \lambda \in k, ev_x(\lambda) = \lambda \text{ (costanti) e non invertibili perché vale per 0}$$

• Si dice che $ev_x: K[X] \longrightarrow K$ è un ^{OMO}MORFISMO DI ANELLI

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

Lemma Sia $x \in K$

allora $ev_x^{-1}(\{0\}) = (X-x)A$ $\curvearrowleft K[X]$ $(x \in K \text{ tali che sostituire danno 0})$
polinomi che si annullano in X

dim:

• dimostra $ev_x^{-1}(\{0\}) \supset (X-x)A$ \curvearrowleft

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

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

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

per l'algoritmo di divisione euclidea per $X-x$ $\exists! (q, r) \in A \times A$ t.c. $P = q(X-x) + r$ $\deg(r) < \deg(X-x)$ $\deg(r) \in \{-\infty, 0\} \iff r \in K$
 $r = 0, r \text{ const} \neq 0$

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

P ha una radice in x

$$\implies ev_x(r) = 0 \text{ e, per ③ } r = ev_x(r) = 0 \text{ quindi } X-x | P \iff P \in (X-x)A \blacksquare$$

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

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

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

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

· $\exists v_0$ no ($c'è -6$)

$$\exists v_1 (x^3 - 6x^2 + 11x - 6) = 12 - 6 - 6 = 0$$

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

calcolo il quoziente:

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

poi uso la formula quadratica:

$$\Delta = 25 - 24 = 1 > 0 \quad z \\ \text{quindi } x_i = \frac{5 \pm \sqrt{1}}{2} \quad \begin{array}{c} z \\ \diagdown \\ 3 \end{array}$$

$$x^2 - 5x + 6 = (x-2)(x-3) \quad (\text{entrambi dividono } x-1 \text{ e sono coprimi, quindi il loro prodotto divide } (x-1)^2)$$

$$\text{quindi: } P = (x-1)(x^2 - 5x + 6)$$

Avrei anche potuto provare $\exists v_1, \exists v_2, \exists v_3$ e vedere che avrebbe funzionato

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

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

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

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

$$x_1 = \frac{2+2i}{2} = i+1 \quad x_2 = \frac{2-2i}{2} = i-1$$

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

■ $F = x^3 - 1$ si ha $\text{ev}_1(F) = 0$ per qualunque campo

$F = (x-1) G$ div.
escludes
FALCA $= (x-1)(x^2+x+1)$ ha $\Delta < \emptyset$, 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 $x_1 = \frac{-1 - \sqrt{-3}}{2}$ $x_2 = \frac{-1 + \sqrt{-3}}{2}$

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

\mathbb{C}

NUMERI COMPLESSI

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

$$i := \sqrt{-1} \quad \text{Caratterizzato dalla condizione } i^2 = -1$$

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

realizzazione cartesiana di \mathbb{C}

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

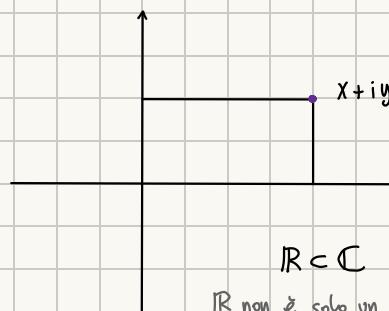
$$\bullet -z := -x + i(-y) \in \mathbb{C} \quad \text{opposto}$$

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

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

• NUOVA operazione: CONIUGAZIONE COMPLESSA su \mathbb{C}

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



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

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

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

→ esponenziale di Euler

$$e^{iy} := \cos(y) + i \sin(y) \in \mathbb{C} \quad \mathbb{R} \rightarrow \mathbb{C} \quad y \mapsto e^{iy}$$

Euler ha notato che, se $\theta, \eta \in \mathbb{R}$

$$e^{i\theta} \cdot e^{i\eta} \xrightarrow{\text{prop. potenze}} e^{i(\theta+\eta)}$$

$$\begin{aligned} & [\cos(\theta) + i \sin(\theta)] \cdot [\cos(\eta) + i \sin(\eta)] \\ & \quad || \\ & \cos(\theta)\cos(\eta) + \cos(\theta)i\sin(\eta) + i\sin(\theta)\cos(\eta) + i^2\sin(\theta)\sin(\eta) \\ & \quad (i^2 = -1) - \sin(\theta)\sin(\eta) \end{aligned}$$

$$e^{i\theta} = \cos(\theta) + i \sin(\theta) \quad \text{con } \theta = \theta + \eta$$

raggruppo parte reale e immaginaria

$$\begin{aligned} & \cos(\theta)\cos(\eta) - \sin(\theta)\sin(\eta) \xrightarrow{\quad} \cos(\theta+\eta) + i \sin(\theta+\eta) \\ & + i (\cos(\theta)\sin(\eta) + \cos(\eta)\sin(\theta)) \quad \cdot \cos(\theta)\cos(\eta) - \sin(\theta)\sin(\eta) = \cos(\theta+\eta) \\ & \quad \cdot \cos(\theta)\sin(\eta) + \cos(\eta)\sin(\theta) = \sin(\theta+\eta) \end{aligned}$$

$$\bullet \text{in modo simile si trova } (e^{iy})^n = e^{iny} \quad \forall n \in \mathbb{N}$$

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

Esempi numeri complessi (Eulero, De Moivre)

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

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

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

$x^3 = 1$ quindi x è radice di $x^3 - 1$ $\operatorname{ev}_x(x^3 - 1) = 0$

• 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 $x^3 - 1$

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

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

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

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

$$\forall y \in R, \operatorname{ev}_y(x^3 - 1) = 0 \implies x^3 - 1 = (x - x^0)(x - x^1)(x - x^2)$$

$$\text{in (4)} \quad e^{\frac{2\pi i}{3}} = \frac{-1 + i\sqrt{3}}{2} \quad e^{\frac{4\pi i}{3}} = \frac{-1 - i\sqrt{3}}{2}$$

CONIUGAZIONE COMPLESSA nuova operazione di \mathbb{C}

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

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

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

proprietà

$$\textcircled{1} \quad \overline{z+z'} = \bar{z} + \bar{z'} \quad (h(z+z') = h(z) + h(z'))$$

$$\textcircled{2} \quad \overline{zz'} = \bar{z} \cdot \bar{z'} \quad (h(zz') = h(z)h(z'))$$

$$\textcircled{3} \quad \overline{-z} = -\bar{z} \quad (h(-z) = -h(z))$$

$$\textcircled{4} \quad h \text{ è una biiezione} \quad h^{-1} = h$$

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

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

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

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

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

$$\textcircled{3} \quad \overline{-z} = -\bar{z}$$

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

reali e \bar{z}

$$z \in \mathbb{R} \iff z = \bar{z}$$

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

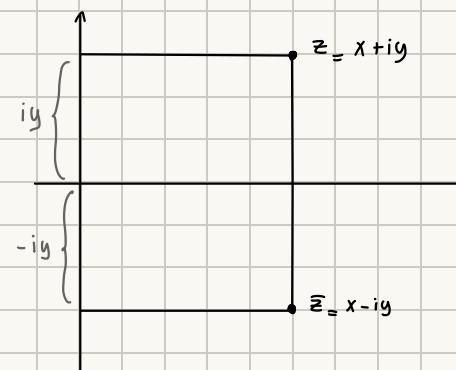
$$z = x + i0 \iff z = x - i0$$

come isomorfismo
gruppi, ma con anelli vedi p.57

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

isomorfismo: omomorfismo biiettivo

h è un
isomorfismo
di anelli



graficamente, $(-)$ corrisponde alla riflessione rispetto all'asse \mathbb{R}
 $h: \mathbb{C} \rightarrow \mathbb{C}$
 $z \mapsto \bar{z}$

Formule fondamentali

$$z\bar{z} = (x+iy)(x-iy) = x^2 - ixy + ixy + y^2 = x^2 + y^2$$

$= 0 \iff x = y = 0$
 $> 0 \iff z \in \mathbb{C} \setminus \{0\}$

$$|z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$$

valore assoluto complesso

- \mathbb{C} è un campo

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

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

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

"Sui libri si trova:"

$$z \cdot \frac{\bar{z}}{(x^2 + y^2)} = 1$$

esempi:

$$\cdot z = 2 = 2+i0 \in \mathbb{R} \quad \bar{z} = 2, \quad x^2 + y^2 = 4, \quad z^{-1} = \frac{\bar{z}}{x^2 + y^2} = \frac{2}{4} = \frac{1}{2}$$

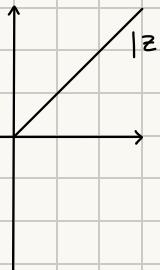
$$\cdot z = i = 0+1 \cdot i \quad \bar{z} = -i \quad x^2 + y^2 = 1 \quad z^{-1} = \frac{-i}{1} = -i$$

$$\cdot z = 1+i \quad \bar{z} = 1-i \quad z\bar{z} = 2 \quad z^{-1} = \frac{1-i}{2} \quad (1+i) \frac{1-i}{2} = \frac{2}{2} = 1$$

Valore assoluto complesso

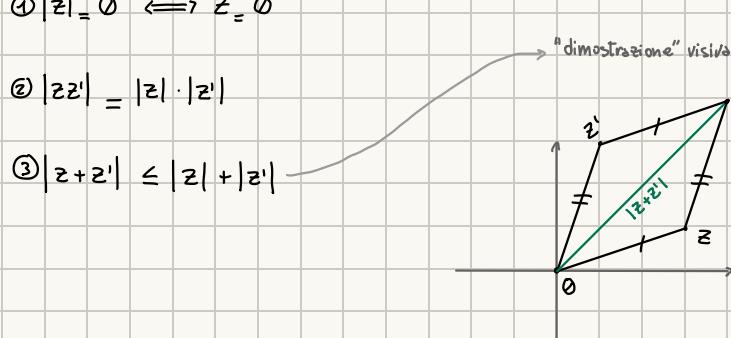
proprietà

$$\textcircled{1} |z| = 0 \iff z = 0$$



$$\textcircled{2} |zz'| = |z| \cdot |z'|$$

$$\textcircled{3} |z+z'| \leq |z| + |z'|$$



per le proprietà dei triangoli:
lunghezza lato < somma 1. altri lati

Proprietà / esercizio

$$\forall g \in \mathbb{R} \quad \textcircled{1} |e^{ig}| = 1 \quad \textcircled{2} (e^{ig})^{-1} = \overline{e^{ig}} = e^{-ig}$$

dim:

$$\textcircled{1} e^{ig} = \cos(g) + i \sin(g) \quad \left| e^{ig} \right| = \sqrt{\underbrace{\cos(g)^2 + \sin(g)^2}_{=1 \text{ (prop sin, cos)}}} = \sqrt{1} = 1$$

• $e^{ig} \neq 0$, quindi è invertibile

$$e^{ig} \cdot e^{-ig} = e^{ig} e^{-ig} \quad \text{con } \eta = -g = e^{i(g-\eta)} = e^{i0} = 1 \quad \text{quindi } e^{-ig} = (e^{ig})^{-1} \text{ (inverso)}$$

$$\overline{e^{ig}} = \overline{\cos(g) + i \sin(g)} = \frac{\overline{e^{ig}}}{\cos(g)^2 + \sin(g)^2} = \frac{\overline{e^{ig}}}{1} \quad \text{ma anche } \frac{\overline{e^{ig}}}{|\overline{e^{ig}}|^2} \quad \text{quindi } \frac{1}{\overline{e^{ig}}} \quad \text{quindi } \overline{e^{ig}} = (e^{ig})^{-1}$$

RAPPRESENTAZIONE POLARE

i numeri complessi possono essere rappresentati in due modi: • rappresentazione complesso ($z = x+iy$) - utile per la somma

• rappresentazione polare (trigonometrica) - utile per il prodotto

dati $z \in \mathbb{C}^*$ $z = x+iy$, $\rho = \sqrt{z\bar{z}} = \sqrt{x^2+y^2} \in \mathbb{R}_{>0}$
 $z \neq 0$ è un unicum ($z=0 \rightarrow \rho=0$; $\exists g'$)

distanza euclidea

(dall'origine)

Lemma

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

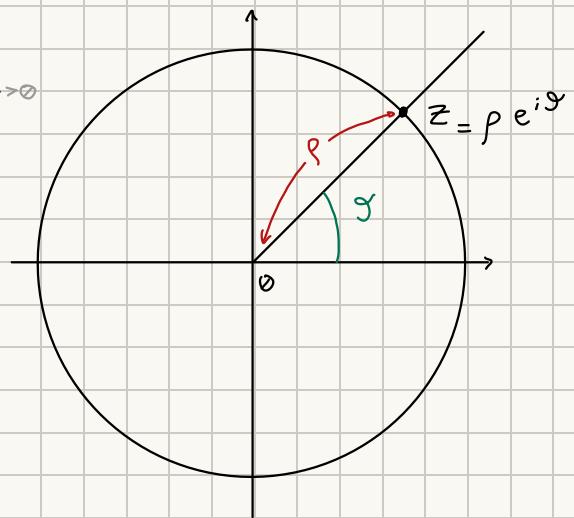
dim (di g...)

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

$$\cdot z' = x' + iy' \quad \exists g \text{ t.c. } x' = \cos(g) \quad y' = \sin(g) \quad \textcircled{1}$$



$$\Rightarrow (\text{sostituendo in } z' = x' + iy') \quad z' = \cos(g) + i \sin(g) = e^{ig} \quad \text{quindi (per } z' = \rho^{-1} z) \quad z = \rho e^{ig} \quad \text{quindi esiste } g.$$



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

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

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

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

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

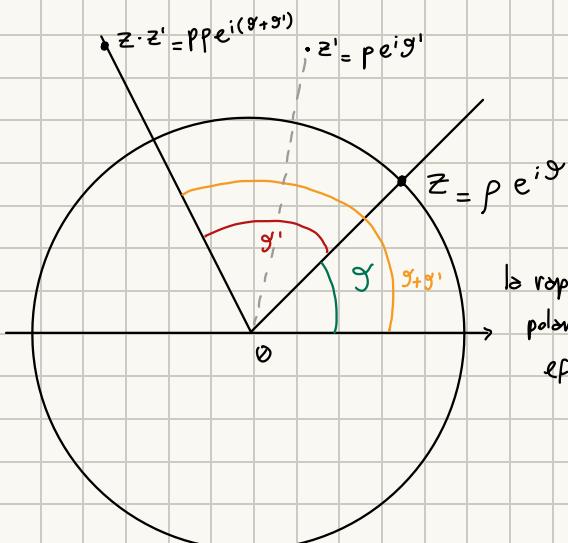
OSS: il coniugato di z è il suo inverso se $\rho = 1$ ($z \in$ cerchio unità)

dim (fatto al QnA)

$$\bar{z} = \overline{\rho e^{ig}} = \overline{\rho} \overline{e^{ig}} = \rho (\cos(g) - i \sin(g)) = \rho (\cos(-g) + i \sin(-g)) = \rho e^{-ig}$$

$$z^{-1} = (\rho e^{ig})^{-1} = \rho^{-1} e^{-ig}$$

$$\text{Quindi, } z^{-1} = \bar{z} \iff \rho e^{-ig} = \rho^{-1} e^{-ig} \iff \rho = 1$$



la rappresentazione
polare è utile per
effettuare moltiplicazioni
di numeri complessi

in cui,
visto che: $z' \bar{z}' = \rho^{-1} z \bar{\rho^{-1} z} = \rho^{-2} z \bar{z} = \rho^{-2} \cdot \rho^2 = 1$

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

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: $\forall F \in K[X] \setminus K$ non 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)

Lemme

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

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

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

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

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

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

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

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

Sia P monico $\deg \geq 1$. Allora $P = \prod_{\substack{Q \text{ irr.} \\ \in K \\ \text{monico}}} Q^{v_Q(P)}$ i soli irr. e monici hanno $\deg = 1$

$\prod_{x \in K} (X-x)$

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

Corollario: MOLTEPLICITÀ

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

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

$v_x(F)$ è la MOLTEPLICITÀ di F in x

$$\text{Si ha che } \{x : v_x(F) \neq 0\} = \{x : v_x(F) = 0\} = \{x \text{ radice di } F\} = R$$

chiaramente un pol.
Si decomponga solo con
le sue radici

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

$$\deg(F) = \sum_{x \in K} v_x(F) = \sum_{x \in R} v_x(F) \geq \sum_{x \in R} 1 = \text{cardinalità di } R \quad (\text{ovvero, perché un pol. di grado } n \text{ ha } \leq n \text{ soluzioni})$$

esp. dei polinomi
in cui si scomponete

Teorema (fondamentale dell'algebra)

\mathbb{C} è algebricamente chiuso

(dim. omessa perché usa elementi dell'analisi)

Teorema

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

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

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

31/10

FATTORIZZAZIONE DI VARI POLINOMI

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

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

$$X^n - 1 = (X-1)Q \quad \begin{matrix} \deg(Q) = n-1 \\ \text{unicamente determinata} \end{matrix}$$

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

↓

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

- $n=3 \quad X^3 - 1 = (X-1)(X^2 + X + 1) \quad \text{fattorizzazione in } \mathbb{R}[X]$

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

(io che ragiona...)

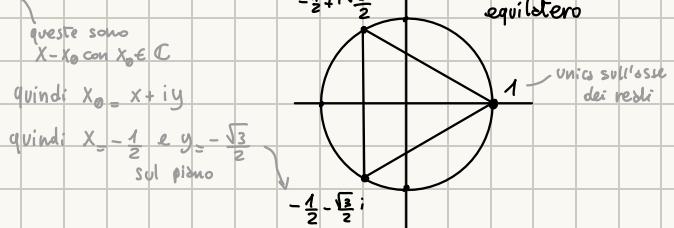
per la rapp. polare, $\exists \vartheta$ t.c. $z = \rho e^{i\vartheta}$

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

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

$$\cos(\vartheta) = -\frac{1}{2} \quad \text{se } \vartheta = \begin{cases} \frac{2\pi}{3} + 2k\pi \\ \frac{4\pi}{3} + 2k\pi \end{cases} \quad \sin(\vartheta) = \frac{\sqrt{3}}{2} \quad \text{se } \vartheta = \begin{cases} \frac{\pi}{3} + 2k\pi \\ \frac{7\pi}{3} + 2k\pi \end{cases}$$

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



$$-\frac{1}{2} + \frac{i\sqrt{3}}{2} = x = e^{\frac{2\pi i}{3}} \quad \text{①} \quad -\frac{1}{2} - \frac{i\sqrt{3}}{2} = x^2 = (e^{\frac{2\pi i}{3}})^2 = (e^{\frac{2\pi i}{3}})^{-1} \cdot (e^{\frac{2\pi i}{3}})^{-1} \quad \text{②}$$

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

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

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

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

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

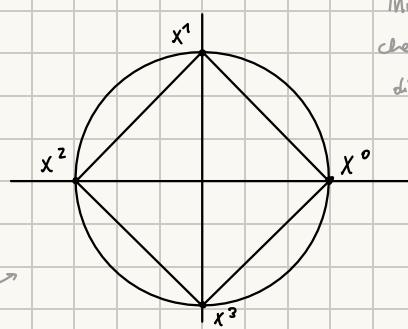
- $n=4 \quad X^4 - 1 = (X-1)(X+1)(X^2 + 1) \quad \text{in } \mathbb{R}[X]$

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

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

$$\text{con } x = e^{\frac{2\pi i}{4}} = e^{\frac{\pi i}{2}} = \underbrace{\cos\left(\frac{\pi}{2}\right)}_0 + i\underbrace{\sin\left(\frac{\pi}{2}\right)}_1 = i$$

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



Iniziamo ad osservare

che se α è radice

di $X^4 - 1$, allora

$\alpha \in \mathbb{R}$

o anche $\bar{\alpha}$ è radice

$$\blacksquare \quad n=5 \quad X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1) \quad \text{in } \mathbb{R}[X]$$

prodotto di due quadratici irriducibili monici

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

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

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

(e non quattro di primo grado perché c'è un fattore di grado 1 \iff c'è una radice reale)

e in $X^5 - 1$ c'è solo 1)

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

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

con:

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

$$\bullet \quad x\bar{x} = x^2 + \beta^2 \geq 0 = 1 \quad (\text{ricorda } z\bar{z} = 1) \quad \cdot \quad x^2 + \bar{x}^2 = 2 \operatorname{Re}(x^2) = 2 \cos\left(\frac{4\pi}{5}\right) \quad \cdot \quad |x^2|^2 = 1$$

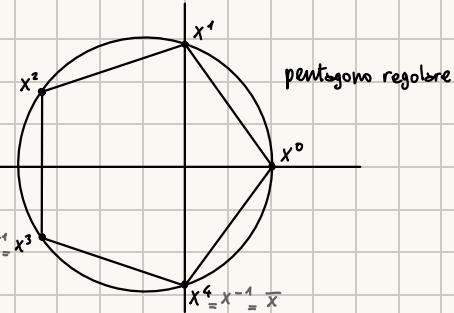
$$P_1 = X^2 - 2 \cos\left(\frac{2\pi}{5}\right)X + 1 \quad , \quad P_2 = X^2 - 2 \cos\left(\frac{4\pi}{5}\right)X + 1 \quad \text{fatt. in } \mathbb{R}[X] = (X-x^0)P_1P_2$$

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

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

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

x De Moivre



$$\text{quindi } X^5 - 1 = \prod_{i=0}^4 (X-x^i) = (X-x^0) \left[(X-x) \left(\frac{X-x^4}{X-x^2} \right) \right] \left[(X-x^2) \left(\frac{X-x^4}{X-x^3} \right) \right]$$

$$\text{osservazione: con } n \geq 1, \quad X^n - 1 = \prod_{i=0}^{n-1} (X-x^i) \quad \text{con } x = e^{\frac{2\pi i}{n}}$$



def POLINOMIO CONIUGATO

Dato $F = f_0 + f_1 X + \dots + f_n X^n \in \mathbb{C}[X]$, poniamo $\bar{F} = \bar{f}_0 + \bar{f}_1 X + \dots + \bar{f}_n X^n$

OSSERVAZIONE: $F \in \mathbb{R} \iff F = \bar{F}$ in \mathbb{R} , $x = \bar{x}$

Inoltre, se $F \in \mathbb{R}[X]$ e $\text{ev}_z(F) = 0$, allora $\text{ev}_{\bar{z}}(\bar{F}) = 0$

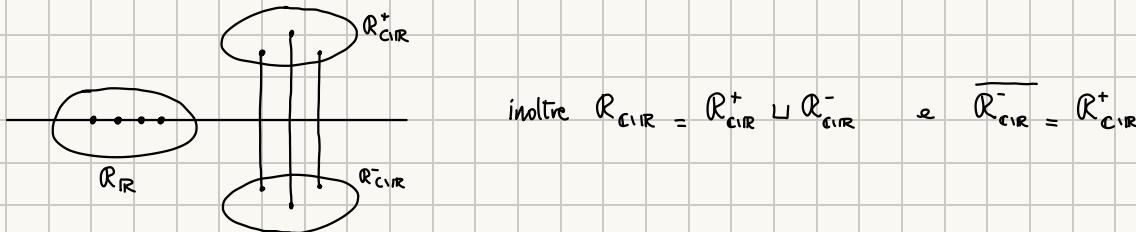
dim: $\text{ev}_z(F) = \text{ev}_{\bar{z}}(\bar{F})$ e, siccome la somma complessa è compatibile con $+$, $-$.

$$= \overline{\text{ev}_z(F)} = \bar{0} = 0$$

Lemma Dato $F \in \mathbb{R}[X]$

detto R l'insieme delle sue radici, allora $R = R_{\mathbb{R}} \cup R_{\mathbb{C} \setminus \mathbb{R}}^+ \cup R_{\mathbb{C} \setminus \mathbb{R}}^-$ dove $R_{\mathbb{R}} = R \cap \mathbb{R}$

$R_{\mathbb{C} \setminus \mathbb{R}}^+ = \{z \in \mathbb{C} \setminus \mathbb{R} \text{ t.c. } z \in \mathbb{C} \setminus \mathbb{R}, \operatorname{Im}(z) > 0 \text{ e scrivendo } z = \sum_{i \in \mathbb{R}} x_i + iy, y > 0\}$, $R_{\mathbb{C} \setminus \mathbb{R}}^- = \{z \in \mathbb{C} \setminus \mathbb{R} \text{ t.c. } \operatorname{Im}(z) < 0\}$



Lemma già dimostrato utilizzato

$X^2 + \beta X + \gamma \in \mathbb{R}[X]$ è irriducibile $\iff \Delta = \beta^2 - 4\gamma < 0$

dim

Supponiamo P irriducibile.

$R_{\mathbb{R}} = \emptyset$, quindi $R_{\mathbb{C} \setminus \mathbb{R}} = \{z, \bar{z}\}$, $R_{\mathbb{C} \setminus \mathbb{R}}^+ = \{z\}$, $R_{\mathbb{C} \setminus \mathbb{R}}^- = \{\bar{z}\}$

$$P = (X-z)(X-\bar{z}) = X^2 - (z+\bar{z})X + z\bar{z} \\ \stackrel{z \in \mathbb{R}}{=} z^2 - 2zX + |z|^2$$

$$\Delta = (z+\bar{z})^2 - 4z\bar{z} = z^2 + 2z\bar{z} + \bar{z}^2 - 4z\bar{z} = (z-\bar{z})^2$$

$$\text{scrivo } z = x+iy \quad z-\bar{z} = 2iy, \quad \text{quindi } (z-\bar{z})^2 = (2iy)^2 = 4i^2y^2 = 4y^2 \cdot -1 = -4y^2 < 0$$

Lemma

Ogni $F \in \mathbb{R}[X]$ si spezza in $\mathbb{R}[X]$ in prodotto $F = \lambda \prod_{x \in R_{\mathbb{R}}} (X-x)^{v_x(F)} \prod_{z \in R_{\mathbb{C} \setminus \mathbb{R}}} \underbrace{[(X-z)(X-\bar{z})]}_{v_z(F)}$

dim: siccome C è algebricamente chiuso,

$$F = \lambda \prod_{z \in C} (X-z)^{v_z(F)} = \lambda \prod_{z \in R_{\mathbb{R}}} (X-z)^{v_z(F)} \prod_{z \in R_{\mathbb{C} \setminus \mathbb{R}}} (X-z)^{v_z(F)}$$

se $z \in \mathbb{C} \setminus \mathbb{R}$ si ha $\bar{z} \in \mathbb{C} \setminus \mathbb{R}$. Quindi, possiamo scegliere, senza perdita di generalità, $z = x+iy$ con $y > 0$ e \bar{z} appartenente a \mathbb{R}

Sì conclude osservando che $R = R_{\mathbb{R}} \cup R_{\mathbb{C} \setminus \mathbb{R}}^+ \cup R_{\mathbb{C} \setminus \mathbb{R}}^-$

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.

$$\text{questo implica } \deg(P) = \# \underset{\substack{\text{card.} \\ P}}{R_{\mathbb{R}}} + \# \underset{\substack{\text{i coniugati} \\ S}}{R_{C \setminus \mathbb{R}}} = \# \underset{\substack{\text{pari} \\ P}}{R_{\mathbb{R}}} + 2 \# \underset{\substack{\text{dispari} \\ S}}{R_{C \setminus \mathbb{R}}}$$

Si come P è di grado dispari, $\deg(P) = 2n+1 = \# R_{\mathbb{R}} + 2S$ Ma allora $2n+1 = r + 2s \iff r = 2n - 2s + 1 \iff r \equiv 1 \pmod{2} \implies r \neq 0$

c'è servito il teorema dei valori intermedi (dell'Analisi)

se $h: \mathbb{R} \rightarrow \mathbb{R}$ è continua t.c. $\lim_{x \rightarrow +\infty} h(x) = +\infty, \lim_{x \rightarrow -\infty} h(x) = -\infty$

allora $\exists x_0 \in \mathbb{R}$ t.c. $h(x_0) = 0$

$$P = X^{2n+1} + \alpha_{2n} X^{2n} + \dots + \alpha_0 \in \mathbb{R}[x] \text{ dispari}$$

sia $f: \mathbb{R} \rightarrow \mathbb{R}$ la funzione $f(x) = ev_x(P)$: è continua e soddisfa $\lim_{x \rightarrow -\infty} f(x) = -\infty, \lim_{x \rightarrow +\infty} f(x) = +\infty$
da cui $\exists x_0 \in \mathbb{R}$ t.c. $f(x_0) = 0 \iff x_0$ radice di f

esercizio 1

$$P = X^4 - 10X^2 + 1 \quad \text{in } (\mathbb{Q}, \mathbb{R}, \mathbb{C})$$

• in \mathbb{C}

$$\text{tentiamo le radici. pongo } Y = X^2 \quad P = Y^2 - 10Y + 1$$

$$\Delta > 0, \text{ radici } y_1 = 5 - 2\sqrt{6} > 0, \quad y_2 = 5 + 2\sqrt{6} > 0$$

$$5 > 2\sqrt{6} \iff 25 > 4 \cdot 6$$

$$y^2 - 10y + 1 = (x^2 - 5 + 2\sqrt{6})(x^2 - 5 - 2\sqrt{6}) = \underset{\substack{\text{in } \mathbb{Q}}}{(x + \sqrt{5+2\sqrt{6}})} \underset{\alpha_1}{(x + \sqrt{5-2\sqrt{6}})} \underset{\alpha_2}{(x - \sqrt{5-2\sqrt{6}})} \underset{\alpha_3}{(x - \sqrt{5+2\sqrt{6}})} \underset{\alpha_4}{\text{è la fatt. in } \mathbb{R}[x] \text{ e anche in } \mathbb{C}[x]}$$

POSSIBILI FATTORIZZAZIONI IN IRR. DI POLINOMI IN $\mathbb{Q}[x]$

$Q \in \mathbb{Q}[x]$ (uguale per un campo qualsiasi)

• $\deg(Q) = 1$ è irriducibile

• $\deg(Q) = 3$ ② \mathbb{Q} irriducibile

• $\deg(Q) = 4$ ③ \mathbb{Q} irriducibile

② $Q = P_1 P_2$ $\deg(P_1) = 1, \deg(P_2) = 3$ irriducibili c'è radice

• $\deg(Q) = 2$ ④ \mathbb{Q} irriducibile

② $Q = P_1 P_2$ dove $\deg(P_1) = 1, \deg(P_2) = 2$ irriducibile

③ $Q = P_1 P_2$ $\deg(P_1) = \deg(P_2) = 2$ irriducibili non c'è radice

② $Q = P_1 P_2$ con P_1, P_2 irriducibili di grado 1

④ $Q = P_1 P_2 P_3$ $\deg(P_1) = \deg(P_2) = 2, \deg(P_3) = 1$ c'è radice

TEORIA DEI GRUPPI

GRUPPI

Dato G insieme $\neq \emptyset$ con $*$ operazione binaria su G , ovvero: $G \times G \rightarrow G$
 $(a, b) \rightarrow a * b$, seleziono un elemento distinto e .
 el. neutro

La terna $G = (G, *, e)$ è un gruppo se:

- non per forza distinti

$$\textcircled{1} \forall a, b, c \in G \quad (a * b) * c = a * (b * c) \quad \text{associatività}$$

$$\textcircled{2} \forall a \in G \quad a * e = e * a = a \quad \text{elemento neutro per l'operazione binaria}$$

$$\textcircled{3} \forall a \in G \quad \exists a' \in G \text{ t.c. } a * a' = a' * a = e \quad \text{inverso per l'op. binaria}$$

add-on: INVERSIONE NEI GRUPPI

$$\begin{aligned} \forall a, b, c \in G \quad & (ab)^{-1} = b^{-1}a^{-1} \\ & (abc)^{-1} = c^{-1}b^{-1}a^{-1} \text{ ecc} \\ & (\text{inversi dei singoli, in ordine inverso}) \end{aligned}$$

Inoltre, se

$$\textcircled{4} \forall a, b \in G, \quad a * b = b * a, \text{ allora } G \text{ è un gruppo abeliano (o commutativo)}$$

quindi - come avevamo visto - le prime 4 condizioni di un anello descrivono un gruppo abeliano.

gruppi in notazione additiva

$(G, +, 0)$ si scrive $+$ per l'operazione
 e 0_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 $-a$

gruppi in notazione moltiplicativa

$(G, \cdot, 1)$ si scrive \cdot per l'operazione
 e 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 $(A, -, +, 0_A, 1_A)$ Anello

Allora $(A, +, 0_A)$ gruppo abeliano in nat. additivo

$\mathbb{Z} = (\mathbb{Z}, +, 0) \quad \mathbb{R} = (\mathbb{R}, +, 0), \quad \mathbb{C} = (\mathbb{C}, +, 0)$

o anche $K = (K, +, 0)$ con K qualunque campo

ESEMPI $(A, -, +, 0_A, 1_A)$ Anello

Allora $A^{\times} = (A^{\times}, \cdot, 1_A)$ gruppo in nat. moltiplicativa
 infatti abbia visto

① il prodotto di el. invertibili è invertibile

② il prodotto è associativo

③ 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.
multiplicativa $\forall a, b \in H, \text{ si ha } a \cdot b^{-1} \in H$ so che $\in G$, ma se $\in H$, è sottogruppo

$\forall a, b \in H, \text{ si ha } a \cdot b \in H$ not.
additivo

Si scrive $H < G$

OSSERVAZIONE H è stabilizzato (rispetto al prodotto)

$$a \cdot b^{-1} \text{ con } b = a$$

$$\bullet \text{ Se } a \in H, \quad a \cdot a^{-1} = 1_G \in H$$

$$a \cdot a^{-1} \text{ con } a = 1_G$$

$$\bullet \text{ Ma allora, } \forall b \in H \quad 1_G \cdot b^{-1} \in H \text{ quindi } b^{-1} \in H \text{ e } 1_G = 1_H$$

$$\bullet \text{ Infine, se } a, b \in H, \quad b^{-1} \in H, \quad a \cdot (b^{-1})^{-1} = a \cdot b \in H$$

(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 $f: G_1 \rightarrow G_2$ un'applicazione:

f è un omomorfismo di gruppi se

$$\textcircled{1} f(1_{G_1}) = 1_{G_2}$$

$$\textcircled{2} \forall a \in G_1, f(a^{-1}) = f(a)^{-1} \quad \begin{matrix} \text{inversione} \\ \text{in } G_1 \end{matrix} \quad \begin{matrix} \text{inversione} \\ \text{in } G_2 \end{matrix} \quad (\text{ma basta solo la } \textcircled{3} - \text{che implica le altre})$$

$$\textcircled{3} \forall a, b \in G_1, f(a \cdot b) = f(a) f(b) \quad \begin{matrix} \text{operazione} \\ \text{di } G_1 \end{matrix} \quad \begin{matrix} \text{operazione} \\ \text{di } G_2 \end{matrix} \quad (\text{in modo più chiaro: } \circ \text{ op. } G_1, \circ \text{ op. } G_2)$$

(l'ordine conta! non si sa se è abeliano)

esercizio: mostrare che $f: G_1 \rightarrow G_2$ è un omomorfismo $\iff \forall a, b \in G_1, f(a \cdot b^{-1}) = f(a) f(b)^{-1}$

\Rightarrow supponiamo f omomorfismo.

$$\text{Allora } f(ab) = f(a)f(b) \quad (\textcircled{3}) \quad \text{quindi } f(ab^{-1}) = f(a)f(b)^{-1}.$$

$$\text{Ma (per } \textcircled{2} \text{)} f(b^{-1}) = f(b)^{-1}$$

$$\text{Quindi } f(ab^{-1}) = f(a)f(b)^{-1}$$

\Leftarrow supponiamo $f(ab^{-1}) = f(a)f(b)^{-1}$

$$\cdot f(1_{G_1}) = 1_{G_2} \quad \text{dim: pongo } a = b \quad f(b \cdot b^{-1}) = f(b)f(b)^{-1} = 1_{G_2}$$

$$\cdot f(a^{-1}) = f(a)^{-1} \quad \text{dim: pongo } a = 1_{G_1} \quad f(1_{G_1} \cdot b^{-1}) = f(1_{G_1})f(b)^{-1} = 1_{G_2} f(b)^{-1} = f(b)^{-1} \quad \text{per } \textcircled{1}$$

$$\cdot f(a \cdot b) = f(a)f(b) \quad \text{dim: pongo } b = b^{-1} \quad f(a \cdot (b^{-1})^{-1}) = f(a)f(b^{-1})^{-1} = f(a)f((b)^{-1})^{-1} = f(a)f(b) \quad \text{per } \textcircled{2}$$

def ISOMORFISMO

Sia $f: G_1 \rightarrow G_2$ omomorfismo di gruppi

Se f è biiettiva, allora si dice che f è un isomorfismo

esercizio

$f: G_1 \rightarrow G_2$ isomorfismo. Supponiamo che f biiettiva $\iff \exists f^{-1}: G_2 \rightarrow G_1$ biiettiva t.c. $f \circ f^{-1} = \text{Id}_{G_2}, f^{-1} \circ f = \text{Id}_{G_1}$

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 $g \circ f: G_1 \rightarrow G_3$ omom. di gr.

e in più f, g sono isomorfismi e anche $g \circ f$, di inverso $f^{-1} \circ g^{-1}$

ESEMPI

$$m\mathbb{Z} \subset \mathbb{Z} : \forall a, b \in m\mathbb{Z}, a-b \in m\mathbb{Z}$$

$$\exists x, \beta \text{ t.c. } a = xm, b = \beta m$$

$$\text{quindi } a-b = (\alpha-\beta)m \in m\mathbb{Z}$$

$$\mathbb{Z} \xrightarrow{f} m\mathbb{Z} \subset \mathbb{Z} \quad \text{notazione additiva}$$

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 iniettivo $f(p) = f(q) \iff pm = qm \iff m(p-q) = 0 \iff p=q$

③ suriettivo $y \in m\mathbb{Z}$. $\exists k \in \mathbb{Z}$ t.c. $y = mk$. Ponendo $x=k$ si ha $f(x) = mk = y$

(Esempio che mischia le notazioni +, ·)

$G_1 = \mathbb{R}$ con +, $G_2 = \mathbb{R}_{>0}$ con · notare che $\mathbb{R}_{>0} \subset \mathbb{R}^{\times}$: $a, b \in \mathbb{R}_{>0}$ $a > 0, b > 0, b^{-1} > 0$ $ab^{-1} > 0$ quindi $ab^{-1} \in \mathbb{R}^{\times}$

poniamo:

$$f: \mathbb{R} \rightarrow \mathbb{R}_{>0} \quad f(x) := e^x$$

$$f: \mathbb{R}_{>0} \rightarrow \mathbb{R} \quad g(x) := \underset{\ln}{\log}(x) \quad e^{\log(\cdot)} = \text{Id}_{\mathbb{R}} \quad \log(e^{\cdot}) = \text{Id}_{\mathbb{R}}$$

Sono due isomorfismi di gruppi, uno l'inverso dell'altro $f^{-1} = g, g^{-1} = f$

$$f(0) = e^0 = 1 = 1_{G_2} \in G_2$$

$$g(1) = 0$$

$$f(-x) = e^{-x} = (e^x)^{-1} \text{ inverso}$$

$$g(y^{-1}) = \log(y^{-1}) = -g(y)$$

$$f(x-x') = e^{x-x'} = e^x e^{-x} \\ = f(x) f(x')^{-1}$$

$$g(y' y^{-1}) = g(y') - g(y) \\ \log\left(\frac{y'}{y}\right)$$

es. 2 foglio sett. 4

(iii) $P = X^3 + X^2 - 6x + 1 \quad Q = X^4 - 2x^3 - 2x - 1$ MCD e Bézout
con $K = \mathbb{Z}/2\mathbb{Z}$ campo (\mathbb{F}_2)

$\mathbb{F}_2 = \{0, 1, 2, 3, 4, 5, 6\}$ dove questi simboli rappresentano le classi corrispondenti in $\mathbb{Z}/2\mathbb{Z}$
posso anche usare altri interi per rappresentare elementi di \mathbb{F}_2 , estraiendoli dalle classi (cls. 8=1)

abbiamo visto che \mathbb{F}_2^\times è un gruppo (abeliano) in notazione.

Tavola di moltiplicazione in \mathbb{F}_2^\times

•	1	2	3	4	5	6	(lo usiamo per trovare facilmente gli inversi)
1	1	2	3	4	5	6	
2	2	4	6	1	3	5	
3	3	6	2	5	1	4	ogni volta che c'è un 1, i due numeri sono inversi
4	4	1	5	2	6	3	
5	5	3	1	6	4	2	• Ogni riga contiene uno e un solo 1 → ogni el. del gruppo è invertibile di inverso unic. det.
6	6	5	4	3	2	1	

quindi $P = X^3 + X^2 - 6x + 1 \quad Q = X^4 - 2x^3 - 2x - 1$

ALGO EUCLIDE

$$\begin{array}{r|rrr}
X^4 - 2x^3 & -2x & -1 & X^3 + X^2 + X + 1 \\
X^4 + X^3 + X^2 + X & & & X + 4 \\
\hline
-3x^3 - X^2 + 4x - 1 & & & \\
4x^3 + 4x^2 + 4x + 4 & & & \\
\hline
2x^2 & + 2 & &
\end{array} \quad \begin{aligned} X^4 - 2x^3 - 2x - 1 &= \underbrace{(X+4)}_{Q} \underbrace{(X^3 + X^2 + X + 1)}_{\text{quoziente}} + \underbrace{2(X^2 + 1)}_{\text{resto}} \\ \deg(2(X^2 + 1)) &= 2 < \deg(P) = 3 \\ \text{mentre } \deg(2(X^2 + 1)) &> \deg(\text{quoziente}) \quad (\text{non sono interi}) \end{aligned}$$

continuiamo: divisione di P per il resto

$$\begin{array}{r|rr}
X^3 + X^2 + X + 1 & 2x^2 + 2 \\
X^3 + X & 4x + 4 \\
\hline
X^2 + 1 & \\
X^2 + 1 & \\
\hline
0 &
\end{array} \quad \begin{aligned} &\text{devo dividere } X^2 + 1 \text{ per } 2x^2 + 2 \\ &\text{ho quindi: } X^2 \text{ e } 2x^2 \rightarrow \text{basta mult.} \\ &\text{per } 2^{-1} = 4 \quad (\text{calcolato nella tavola}) \end{aligned} \quad \begin{aligned} &\text{l'ultimo resto non nullo è quindi: } 2x^2 + 2 \\ &\text{ma l'MCD deve essere monico} \rightarrow \text{moltiplico per un invertibile: } 4 \\ &4 \text{ inverso di } 2, \text{ quindi: } X^2 + 1 \text{ è MCD} \end{aligned}$$

• IDENTITÀ DI BÉZOUT

abbiamo $X^4 - 2x^3 - 2x - 1 = \underbrace{(X+4)}_Q \underbrace{(X^3 + X^2 + X + 1)}_P + \underbrace{2(X^2 + 1)}_{\text{resto}}$

trovare α, β in \mathbb{F}_2 t.c. $\alpha P + \beta Q = \delta = X^2 + 1$

$$2(X^2 + 1) = Q - (X+4)P \quad \text{l'identità che abbiamo è buona, ma serve eliminare il 2 prima dell'MCD (2 è inv. moltiplichiamo per l'inverso)}$$

$$4 \cdot 2(X^2 + 1) = 4Q - 4(X+4)P$$

$$X^2 + 1 = 4Q + (3x + 5)P$$

COSTRUZIONI CANONICHE DI UN SOTTOGRUPPO

Note: un gruppo qualsiasi ha due sottogruppi evidenti:

$$\cdot \{1_G\} \quad \cdot \text{se stesso}$$

\otimes not. additivo

Lemme costruzione del kernel / nucleo

Sia $f: G_1 \rightarrow G_2$ omomorfismo di gruppi

$$H = \left\{ g \in G_1 : f(g) = 1_{G_2} \right\} = f^{-1}(\{1_{G_2}\}) \subset G_1$$

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 $H = \text{Ker}(f)$

dim: $a, b \in H$ con $f(a) = f(b) = 1_{G_2}$

$$f(ab^{-1}) = f(a)f(b^{-1}) \stackrel{\text{def}}{=} f(a)f(b)^{-1} = 1_{G_2} 1_{G_2}^{-1} = 1_{G_2} \text{ quindi } ab^{-1} \in H$$

(in H ci sono gli el. che puntano a 1_{G_2})

Lemme

Sia $f: G_1 \rightarrow G_2$ omomorfismo di gruppi

"kernel banale" è banale perché, per def. omomorfismo di gruppi, $f(1_{G_1}) = 1_{G_2}$

si ha che $\text{Ker}(f) = \{1_{G_1}\} \iff f$ è iniettiva

\curvearrowleft è il più piccolo sottogruppo di G_1

dim

\implies Supponiamo $\text{Ker}(f) = 1_G$ ($= \{x \in G_1 : f(x) = 1_{G_2}\}$)

$$\text{siano } x, x' \in G_1 \text{ t.c. } f(x) = f(x') \iff \underbrace{f(x)}_{\text{diviso}} \underbrace{f(x')^{-1}}_{= f(x^{-1})} = 1_{G_2}$$

(\times omomorfismo)

$$\iff x(x')^{-1} \in \text{Ker}(f) = \{1_{G_1}\} \text{ quindi } \iff x(x')^{-1} = 1_{G_1}$$

$$\text{ma per } x' \quad \underbrace{x(x')^{-1} x'}_1 = 1_{G_1} x' \iff x' = x \quad f \text{ iniettiva}$$

\iff Supponiamo f iniettiva

Sia $x \in \text{Ker}(f)$. 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 $x = 1_{G_1} \implies \text{Ker}(f) = \{1_{G_1}\}$

• costruzione del SOTTOGRUPPO IMMAGINE

$f: G_1 \rightarrow G_2$ 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. $f(x) = y, f(x') = y'$

$$y(y')^{-1} = f(x)f(x')^{-1} \stackrel{\text{OMOMORFISMO}}{=} f(xx'^{-1}) = f(z)$$

$$\exists z \in G_1 \text{ t.c. } f(z) = y(y')^{-1} \iff y(y')^{-1} \in f(G_1)$$

• costruzione dei SOTTOGRUPPI CONIUGATI

G gruppo. Scegliamo $H < G$ e $g \in G$

$$\text{definisco } H^g := \{g' \in G \text{ t.c. } \exists h \in H \text{ t.c. } g' = g^{-1}hg\} = g^{-1}Hg \quad \begin{array}{l} \text{notazione} \\ \text{semplificata} \end{array}$$

OSSERVAZIONE. se G abeliano, $H^g = H \forall g$ ($g^1 = g^{-1}hg \iff g' = \underbrace{g^{-1}g}_{1}h \iff g' = h$)

Lemma: $H^g < G$

In generale $gH, Hg, Hg^{-1}, g^{-1}H \notin G$

dim dati $a, b \in H^g$

$$a = g^{-1}a'g \quad \exists a' \in H, \quad b = g^{-1}b'g \quad \exists b' \in H$$

$$\cdot b^{-1} = (g^{-1}b'g)^{-1} = g^{-1}b'^{-1}g \quad \begin{array}{l} \text{inversione in } G: (abc)^{-1} = c^{-1}b^{-1}a^{-1} \\ \text{perciò } H^g \end{array}$$

$$ab^{-1} = g^{-1}a'g \cdot g^{-1}(b')^{-1}g = g^{-1}\underbrace{a'(b')^{-1}}_{\in H}g \Rightarrow ab^{-1} \in H^g \quad \forall a, b \in H^g \Rightarrow H^g < G$$

dim alternativa

Definiamo, dato $g \in G$, un'applicazione $G \xrightarrow{f_g} G$

osserviamo che Hg, f_g è un omom di gruppi: (si parla di endomorfismo)

per verificarlo devo mostrare che $\forall a, b \in G, f(ab^{-1}) = f_g(a) f_g(b^{-1})$

$$f_g(a) f_g(b^{-1}) = g^{-1}a g (g^{-1}b g)^{-1} = g^{-1}a g \cdot g^{-1}b^{-1}(g^{-1})^{-1} = g^{-1}a b^{-1}g = f_g(ab^{-1})$$

Questo dimostra perciò: $H < G_1$ e se $G_1 \xrightarrow{f} G_2$ omomorfismo, allora $f(H) < G_2$

Se $G_1 = G_2 = G$ e $f = f_g$ otteniamo $\forall H < G, f_g(H) < G \quad \begin{array}{l} \text{perciò} \\ f_g(H) = H^g \end{array} \Rightarrow H^g < G$ •

PERMUTAZIONI

GRUPPI DI PERMUTAZIONI

elementi chiamati permutazioni

dato E insieme finito, sia $S(E) = \{ f: E \rightarrow E : f \text{ biiettiva} \}$

• Su $S(E)$ esiste l'operazione di composizione di applicazioni: $E \xrightarrow[f]{\circ} E$, e se $f, g \in S(E)$, allora $g \circ f \in S(E)$

Inoltre, $(g \circ f)^{-1} = f^{-1} \circ g^{-1} \implies (S(E), \circ, \text{Id}_E)$ è un gruppo.

perché ① $f \circ (g \circ h) = (f \circ g) \circ h$ \circ è associativo

② $f \circ \text{Id} = \text{Id} \circ f = f \quad \forall f \in S(E)$ è neutro

③ $\forall f \in S(E)$ invertibile e $f \circ f^{-1} = f^{-1} \circ f \in S(E)$ inverso per \circ

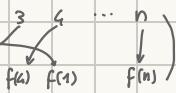
• Sia $E = \{1, \dots, n\} =: I_n \quad n \geq 1$ allora si scrive $S_n = S(I_n) = S(E)$

• ogni elemento di S_n , $f \in S_n$ può essere

identificato con un diagramma:



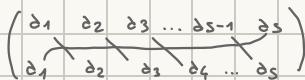
che si può anche rappresentare non "in ordine" con frecce:



def n-ciclo

Una permutazione del tipo $(\alpha_1 \alpha_2 \alpha_3 \dots \alpha_{s-1} \alpha_s \alpha_1 \alpha_2 \dots \alpha_s \dots \alpha_1)$ con $\alpha_1, \alpha_2, \dots, \alpha_s \in I_n$ ($s \leq n$) distinti,

il ciclo si vede meglio così immo



che fissa (mette a sé stessi) tutti gli

elementi che non appartengono a $\{\alpha_1, \dots, \alpha_s\}$

(e mette quelli di $\{\alpha_1, \dots, \alpha_s\}$ in maniera ciclica)

es: $\alpha_1 \rightarrow \alpha_2, \alpha_2 \rightarrow \alpha_3, \alpha_3 \rightarrow \alpha_1$

Si chiama **s-ciclo** e si scrive $(\alpha_1 \alpha_2 \dots \alpha_s)$

Term: dato un ciclo

$(\alpha_1 \alpha_2 \dots \alpha_s)$, la sua orbita

N.B rispetta alla notazione: è $(\alpha_1 \alpha_2 \alpha_3 \dots \alpha_s)$ e rispetta l'ordine del ciclo

è $\{\alpha_1, \alpha_2, \dots, \alpha_s\}$

(insieme di el. permutati da loro)

si può shiftare: $(\alpha_s \alpha_1 \alpha_2 \dots \alpha_{s-1})$ ma non rimescolare: $\neq (\alpha_1 \alpha_3 \alpha_2 \dots \alpha_s)$

Esempi: in S_2 : $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (12)$ è un 2-ciclo in S_3 : $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$ 3-ciclo in S_5 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = (135)$ 3-ciclo

TERMINOLOGIA: tutti i 2-cicli si chiamano **trasposizioni**.

OSS: l'identità è uno 0-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

vedo $1 \rightarrow 2, 2 \rightarrow 5, 5 \rightarrow 1$ sono "cicliche", ma

le altre non sono fissate: $3 \rightarrow 6, 6 \rightarrow 3 \dots$

(anche guardando $3 \rightarrow 6, 6 \rightarrow 3$ stesso discorso: $1 \rightarrow 2, 2 \rightarrow 5, 5 \rightarrow 1$ non fissate)

INVERSIONE

$$\left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 6 & 7 & 5 & 1 & 3 & 2 \end{array} \right)^{-1} = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 4 & 6 & 7 & 5 & 1 & 3 & 2 \end{array} \right) = \left(\begin{array}{cccccc} 4 & 6 & 7 & 5 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \right) = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 1 & 4 & 2 & 3 \end{array} \right)$$

$$= \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \diagdown & \diagdown & \diagdown & \diagdown & \diagdown & \diagdown & \diagdown \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \right)^{-1} = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \diagup & \diagup & \diagup & \diagup & \diagup & \diagup & \diagup \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \right)$$

OSS: nella notazione semplificata di un ciclo $(\alpha_1 \alpha_2 \dots \alpha_s)$, l'inverso si ottiene leggendo da destra a sinistra:
 $(\alpha_1 \alpha_2 \dots \alpha_s)^{-1} = (\alpha_s \dots \alpha_3 \alpha_2 \alpha_1)$

COMPOSIZIONE (possiamo chiamarla anche "prodotto")

$$\sigma = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{array} \right) = (1342) \in S_5, \quad \tau = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{array} \right) = (15324) \in S_5$$

$$\sigma \circ \tau = \sigma \cdot \tau = \sigma \tau \quad \text{composizione \(\rightarrow\) legge prima } \tau$$

$$\sigma \circ \tau = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \tau | & 1 & 1 & 1 & 1 \\ 5 & 4 & 2 & 1 & 3 \\ \sigma | & 1 & 1 & 1 & 1 \\ 5 & 2 & 1 & 3 & 4 \end{array} \right) = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{array} \right) = (543) \neq \Rightarrow S_5 \text{ non è commutativo!}$$

$$\tau \circ \sigma = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{array} \right) = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{array} \right) = (1253)$$

OSS: il prodotto di cicli non è necessariamente un ciclo

Descrizione di S_3 $\# S_3 = 6 = 3 \cdot 2 \cdot 1$ (fattoriale)

$$\left\{ \left(\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 2 & 3 \end{array} \right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array} \right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \end{array} \right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array} \right) \right\} =$$

$$= \{ \text{Id}, (23), (12), (123), (132), (13) \} \quad \text{in } S_3, \text{ ogni permutazione è un s-ciclo con } s = 0, 2, 3$$

- Quel 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

$$\begin{aligned} ((12)(34))(1) &= (12)((34)(1)) = (12)(1) = 2 \\ ((12)(34))(2) &= (12)(2) = 1 \\ ((12)(34))(3) &= (12)(4) = 4 \\ ((12)(34))(4) &= (12)(3) = 3 \end{aligned}$$

notazione funzioni: come $(f \circ g)(x)$

$$\text{quindi: } (12)(34) = \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{array} \right) \text{ non è un ciclo}$$

$$\text{es mostrare che } (123)^{-1} = (132) (= 321\dots) \longrightarrow (123) = (123) \quad (123)^{-1} = \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right) = (132)$$

def CICLI A SUPPORTI DISGIUNTI

Dati due cicli $(\alpha_1 \dots \alpha_s)$ e $(\beta_1 \dots \beta_t)$ di S_n ,

si dice che sono a supporti disgiunti se $\{\alpha_1, \dots, \alpha_s\} \cap \{\beta_1, \dots, \beta_t\} = \emptyset$

Più generalmente, dati r cicli, C_1, \dots, C_r di S_n sono a supporti disgiunti

es. $(12), (34)$ sono a supp. disgi. 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 fra di loro.

C'è analogia con il TFA.

esempio

x "estrae" 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 8

$1 \rightarrow 2 \rightarrow 4 \rightarrow 7 \rightarrow 1$

(1247)

Non ha senso
prendere un el.
da qui - si parte
da un altro

prendo il 3

$3 \rightarrow 6 \rightarrow 8 \rightarrow 5 \rightarrow 3$

(3685)

i due cicli sono disgiunti

$\sigma = (1247)(3685) =$

$= (3685)(1247)$

Sia G gruppo (in not. moltiplicativa) e $H \subset G$.

Introduciamo una relazione \sim su G :

$$\text{dati } X, X' \in G \quad X \sim X' \iff X(X')^{-1} \in H$$

Lemma: \sim è di equivalenza

dim: ① RIFLESSIVITÀ:

$$x \sim x \quad \forall x \in G$$

$$H \subset G \implies 1_G \in H. \text{ Ma } 1_G = xx^{-1} \quad \forall x \in G, \text{ quindi } x \sim x \quad \forall x \in G$$

($1_H = 1_G$)

② SIMMETRIA:

$$x \sim x' \implies x'(x')^{-1} \in H$$

$$\text{Ma } \forall h \in H, h^{-1} \in H \quad \begin{array}{l} (\text{prop.}) \\ (\text{sottogr.}) \end{array} \text{ Quindi } (x(x')^{-1})^{-1} = x'x^{-1} \in H$$

③ TRANSITIVITÀ:

$$x \sim x', x' \sim x'' \implies x \sim x'' \quad \forall x, x', x'' \in G$$

Supponiamo $x \sim x'$ e $x' \sim x''$. Allora $x(x')^{-1}, x'(x'')^{-1} \in H$

$$\text{Se } a, b \in \text{sottogruppo: } x(x')^{-1}x'(x'')^{-1} = x(x'')^{-1} \in H$$

anche il loro prodotto

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:

$$[x] * [x'] = [x \cdot x'] \quad \begin{array}{l} \text{nuova op.} \\ \text{indipendentemente dai rappresentanti} \\ \text{vecchio op. di } G \end{array}$$

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 $[x \cdot x'] = [y \cdot y']$ ovvero $xx'(yy)^{-1} \in H$

$$xx'(yy)^{-1} = x\underbrace{x'(y)}_{\text{per ipotesi, } \in H} y^{-1} \quad \begin{array}{l} \text{sappiamo quindi che un pezzo del prodotto } \in H, \\ \text{ci serve una condizione per cui tutto il prodotto } \in H \end{array}$$

def SOTTOGRUPPO NORMALE

H è un sottogruppo normale di G se, $\forall x \in G, xH = Hx$

• si scrive $H \triangleleft G$

$$\text{quindi, per la formula di prima: } xHy^{-1} = \underbrace{xy^{-1}H}_{\text{per ipotesi, } \in H} \quad \text{e } H \text{ per ipotesi, quindi tutto } \in H$$

(quindi $[x \cdot x'] = [y \cdot y']$)

Condizioni equivalenti (per H sottogr. normale)

$$\begin{array}{ll} \textcircled{1} H \triangleleft G & \textcircled{2} \forall g \in G \quad \forall h \in H, \exists h' \in H \text{ t.c. } gh = h'g \\ (\text{gh} = Hg) & \textcircled{3} \forall g \in G, H^g = H \end{array}$$

ricordiamo: $g^{-1}Hg$

OSS: G abeliano e $H \subset G \implies H \triangleleft G$ (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 sottgr. 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 $G \triangleleft G$ ($\forall x \in G, xG = Gx$ e $G/G = \{G\}$)
- anche $\{1_G\} \triangleleft G$ ($\forall x \in G, x1_G = 1_Gx = x$ e $G/\{1_G\} = \{ \{gg\} : g \in G \}$ rel. di ugualanza)

dim condiz. equivalenti: basta mostrare che $(3) \Rightarrow (1) \Rightarrow (2) \Rightarrow (3)$ (ordine scelto per facilità di dimostrazione)

- $(3) \Rightarrow (1)$ ipotesi: $H^g = H$ se $H^g = H$, $g^{-1}Hg = H \Leftrightarrow \underbrace{gg^{-1}Hg}_{1_H} = gH \Leftrightarrow Hg = gH$
devo dim: $gH = Hg$
- $(1) \Rightarrow (2)$ ipotesi: $gH = Hg$ se $\forall g$, $gH = \{x \in G : \exists h \in H \text{ con } x = gh\} = Hg = \{y \in G : \exists h' \in H \text{ con } y = h'g\}$
devo dim: $gh = h'g$. allora $\exists h, h' \in H$ t.c. $x = gh = h'g$
- $(2) \Rightarrow (3)$ ipotesi: $gh = h'g$ se $\forall g \in G, \forall h \in H$ si ha $gh = h'g \exists h' \in H$, allora $\underset{1_G}{\cancel{g^{-1} \Rightarrow}} g^{-1}gh = g^{-1}h'g \Leftrightarrow h = g^{-1}h'g$ quindi, $\forall g, H^g = H$ ■
devo dim: $H^g = H$

Teorema

Dato $H \triangleleft G$, \sim di eq.

Allora l'operazione su G/\sim $[x][x'] = [xx']$ (ben posta)

definisce una struttura di gruppo su G/\sim .

$[g]$ contiene tutti gli el. x t.c. $gx^{-1} \in H$

quindi, $gx^{-1} = h \Leftrightarrow g = hx \Leftrightarrow h^{-1}g = x$

Ma H è chiuso rispetto all'inverso, quindi $h^{-1} \in H$.

Quindi tutti gli el. $x \in [g]$ si possono scrivere come gh , $h \in H$

mino ragionamento

che poi, per simmetria,

visto che $x \in [g]$,

$g = x \Rightarrow x \in [g]$

quindi $x^{-1} = h'$

$\Leftrightarrow x = gh'$

e, sostituendo,

$g = h(g^{-1})$

$\Leftrightarrow 1 = gh^{-1}$

$h^{-1} = h^{-1}$

ppr credo

è potuto fare!

ip so, cool!

• si scrive $G/\sim = G/H$ gruppo quoziante di G per H

• osserviamo inoltre $[g] = gH = Hg$

non è vero che $gh = hg$

ma $\forall h \exists h' \text{ t.c. } gh = h'g$ 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

Lemma:

L'applicazione $\begin{array}{ccc} G & \xrightarrow{\Pi_H} & G/H \\ g & \mapsto & [g] \end{array}$ è un omomorfismo di gruppi suriettivo

dim:

• la suriettività di Π_H è chiara, perché ogni classe contiene un rappresentante

• inoltre, $\Pi_H(g(g)^{-1}) = [g(g)^{-1}] = [g][g^{-1}] = \Pi_H(g)\Pi_H(g^{-1})$ ■

Lemma

Dato $G_1 \xrightarrow{f} G_2$ omomorfismo di gruppi:

el. di G_1 che puntano a 1_{G_2}

$\mapsto [H]$ el. neutro di G/\sim ,

Allora, $\underbrace{\text{Ker}(f)}_{=H} \triangleleft G_1$. Inoltre, se $H \triangleleft G$, allora $H = \text{Ker}(\Pi_H)$ quindi $H = \text{Ker}(\Pi_H)$

dim:

• $\text{Ker}(f) \triangleleft G_1$ (so già che $\triangleleft G_1$) Mostriamo che $\text{Ker}(f)^g = \text{Ker}(f)$ (def. equivalente ③ di \triangleleft)

prendiamo $h \in G_1$ t.c. $f(h) = 1_{G_2}$ ($\Leftrightarrow h \in \text{Ker}(f)$)

$$\begin{aligned} \text{Allora si ha che } \forall x \in G_1, f(x^{-1}hx) &= f(x^{-1}) \overset{\text{OMOM.}}{=} f(h) \overset{\text{OMOM.}}{=} f(x) \\ &= f(x)^{-1}f(x) = 1_{G_2} \end{aligned}$$

$$\Leftrightarrow x^{-1}hx \in \text{Ker}(f) \quad \forall h \in \text{Ker}(f), \forall x \in G \Leftrightarrow \text{Ker}(f)^x = \text{Ker}(f)$$

• se $H \triangleleft G_1$, allora $H = \text{Ker}(\Pi_H)$

Abbiamo $H \triangleleft G_1$ e poniamo $f = \Pi_H$. Mostriamo che $H = \text{Ker}(\Pi_H)$. Ma se $g \in G_1$ soddisfa $\Pi_H(g) = 1_{G_2} = H \Leftrightarrow gH = H \Leftrightarrow g \in H$ ■

(Spiegazione mia):

• $g \in H \Rightarrow g \in \text{Ker}(\Pi_H)$ se $g \in H$, $gH = H$. Quindi, $\Pi_H(g) = H$ ($[g] = gH$). Quindi (visto $H = 1_{G_2}$) $g \in \text{Ker}(\Pi_H)$

• $g \notin \text{Ker}(\Pi_H) \Rightarrow g \notin H$ se $g \notin \text{Ker}(\Pi_H)$, $\Pi_H(g) = 1_{G_2} = H$. Quindi, $gH = H$. $gH = H \Leftrightarrow g \in H$

Consideriamo un omomorfismo di gruppi: $G_1 \rightarrow G_2$. Per il Teorema di struttura delle applicazioni,

$$\begin{array}{ccc}
 G_1 & \xrightarrow{f} & G_2 \\
 \downarrow \pi & & \downarrow i \\
 G_1/R & \xrightarrow{\psi} & f(G_1) \\
 [g] & \longmapsto & f(g) \\
 \text{(è biettiva: se } [g] = [g'] \text{ allora } f(g) = f(g')\text{)}
 \end{array}$$

$f = i \circ \psi \circ \pi$

dove R è la relazione:
 dati $g, g' \in G_1$, $g R g' \iff f(g) = f(g')$

In più, f è un omomorfismo di gruppi.

OSSERVIAMO: dati $g, g' \in G_1$, allora $f(g) = f(g') \iff f(g) f(g')^{-1} = 1_{G_2}$

\Downarrow

\Downarrow (dividere per $f(g)$)

\Downarrow (def.)

ma $f(g) f(g')^{-1} = f(g(g')^{-1})$ (\times omom.
gruppi)

(ricordiamo: el. che partono a 1_{G_2})

quindi $f(g(g')^{-1}) = 1_{G_2} \iff g(g')^{-1} \in \text{Ker}(f)$

(π omomorfismo, \sim è R stessa
relazione)

$\iff g \sim g'$ (\sim è definito come, dati G gr., $H \leq G$
e $x, x' \in G$: $x \sim x' \iff x(x')^{-1} \in H$)

quindi abbiamo dimostrato che R e \sim sono la stessa relazione.

Come abbiamo visto nel Lemma qui

Si ha quindi $G/R = G/\sim$ che è un gruppo, quindi G/R gruppo e π omomorfismo di gruppi.

(sappiamo chiaramente che l'identità è un omomorfismo di gruppi).

$\bullet H = \text{Ker}(f)$. Mostriamo che $\psi: G_1/H \rightarrow f(G_1)$: $\psi(gH) = f(g)$ è un omomorfismo di gruppi.

Vogliamo mostrare che, $\forall g, g' \in G_1$, si ha: $\psi(gH) \psi((g'H)^{-1}) = \psi(g(g')^{-1}H)$

\Downarrow

\Downarrow (def.)

ma $\psi(gH(g'H)^{-1}) = \psi(gHH(g')^{-1}) = \psi(gH(g')^{-1}) = \psi(g(g')^{-1}H) = f(g(g')^{-1}) = f(g) f(g')^{-1} = \psi(gH) \psi(g'H)^{-1}$

ovvero quello che cercavamo

• Si può vedere anche come
 $gH = [g]$ quindi $(g'H)^{-1} = [g']^{-1}$

Abbiamo dimostrato il PRIMO TEOREMA DI ISOMORFISMO PER I GRUPPI:

dato $f: G_1 \rightarrow G_2$ omomorfismo di gruppi, esso si decompona

in composizione: $f = \underbrace{i \circ \psi \circ \pi}_{\substack{\text{tutti omomorfismi} \\ \text{di gruppi}}}$

Altre proprietà dei gruppi:

Lemme l'intersezione di sottogruppi è un sottogruppo

Dati $H_1, \dots, H_n < G$, allora $\bigcap_{i=1}^n H_i < G$

dim: Siano $x, x' \in \bigcap_{i=1}^n H_i$:

Allora, $\forall i = 1, \dots, n \quad x(x')^{-1} \in H_i$, perché $H_i < G \forall i$

Ma allora $x(x')^{-1} \in \bigcap_{i=1}^n H_i$. Quindi si ha $\bigcap_{i=1}^n H_i < G$

(se appartiene a tutti i sottogruppi, allora appartiene all'intersezione)

Lemme l'unione di sottogruppi non è un sottogruppo

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 $(12), (13) \in G \text{ e } \in H$ ma $(12)(13) = (1, 3, 2) \notin H_1 \cup H_2$ (non è chiuso rispetto alla sua operazione, o)
quindi non è un sottogruppo

def SOTTOGRUPPO GENERATO

/

Consideriamo $I \subset G$. Il sottogruppo di G generato da I è:

$$\langle I \rangle := \bigcap_{\substack{H \leq G: \\ I \subset H}} H \quad (\text{quindi si prendono tutti i sottogruppi di } G \text{ che contengono } I \text{ e si intersecano})$$

Si chiama anche il "più piccolo sottogruppo di G che contiene I "

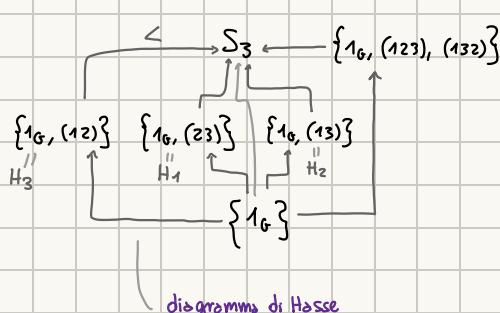
$\langle I \rangle$ è $< G$ per il lemma per cui l'intersezione di sottogruppi è un sottogruppo.

per un singolo elemento:

• dato G gruppo (nat. moltiplicativa) e $g \in G$, $\langle g \rangle = \bigcap_{\substack{H \leq G \\ g \in H}} H$

esempio

i sottogruppi di S_3 sono:



$$\text{Quindi, } \langle (12) \rangle = \{1_G, (12)\} = H_3$$

$$\langle (13) \rangle = \{1_G, (13)\} = H_2$$

$$\langle (23) \rangle = \{1_G, (23)\} = H_1$$

$$\langle (123) \rangle = \{1_G, (123), (132)\} \cap S_3 = \{1_G, (123), (132)\}$$

$$\langle H_1 \cup H_2 \rangle = S_3$$

$$H_1 \cup H_2 = \{1_G, (13), (23), (132), (123), (12)\} = S_3 \quad (\text{i prodotti ci sono per chiusura rispetto a } \circ)$$

$$(23)(13)(23)$$

Sottogruppo $g^{\mathbb{Z}}$

- Consideriamo l'insieme $\{1, g, g^2, \dots, g^{-1}, g^0, \dots\} = \{g^n : n \in \mathbb{Z}\} = g^{\mathbb{Z}} \subset G$

Allora si ha che $g^{\mathbb{Z}} \leq G$. Infatti, $\forall x, x' \in g^{\mathbb{Z}}, \exists n, n' \in \mathbb{Z}$ t.c. $x = g^n, x' = g^{n'}$ e $x(x')^{-1} = g^{n-n'} \in g^{\mathbb{Z}}$

Si ha che $\langle g \rangle \subset g^{\mathbb{Z}}$. (perché $\langle g \rangle$ è un sottogr. quindi è chiuso rispetto a inverso e prodotto, quindi visto che contiene g , contiene anche g^{-1} e tutte le potenze generali ($g^{\mathbb{Z}}$))

Dato che $\langle g \rangle \leq G$, 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 $g^{\mathbb{Z}} \subset \langle g \rangle$

Lemme $\langle g \rangle = g^{\mathbb{Z}}$.

Lemme 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 $n\mathbb{Z}$)

l'el. neutro è sempre un sottogruppo

dim:

Supponiamo $G \neq \{0\}$. Allora esiste un più piccolo $n \in G \cap \mathbb{N}^*$ (principio del minimo)

tale che, preso $d \in G$ (per div. euclideo) $d = qn + r$ con $0 \leq r < n$.

(impossibile perché n è il minimo su $G \cap \mathbb{N}^*$, ma allo stesso tempo $r < n$ e $r \neq 0$)

Quindi $r = d - qn$. Se $r \neq 0$, si avrebbe $r < n$ e $r \in G \cap \mathbb{N}^*$

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
rispetta alla somma,
quindi contiene tutti gli $n\mathbb{Z}$ (?)

Lemme

Se G è un gruppo finito (in notazione moltiplicativa),

allora, $\forall g \in G, \exists n > 0$ t.c. $\langle g \rangle = g^{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$

isomorfo a

not. additiva

dim:

$f: \mathbb{Z} \rightarrow G$
 $n \mapsto g^n \in g^{\mathbb{Z}} = \langle g \rangle$ non può essere iniettivo, perché \mathbb{Z} è infinito e G è finito

f è omomorfismo perché $f(n-n') = g^{n-n'} = g^n g^{-n'} = f(n) f(n)^{-1}$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & G \\ \pi \downarrow & & \uparrow i \\ \mathbb{Z}/\text{Ker}(f) & \xrightarrow{\cong} & f(\mathbb{Z}) = g^{\mathbb{Z}} = \langle g \rangle \end{array} \quad (\text{x teor. iso: } f = i \circ \psi \circ \pi)$$

$\langle \mathbb{Z}, \text{quindi: } 0 \in \{0\}, 0 \in n\mathbb{Z}$.

Ma se fosse $\{0\}$, allora $\mathbb{Z}/0 \stackrel{1:1}{\cong} \mathbb{Z}$ e f sarebbe iniettiva (non può esserlo)

-vedi sopra-

Quindi, $\text{Ker}(f) = n\mathbb{Z} \quad \exists n \in \mathbb{N}^*$

def ORDINE DI UN ELEMENTO

Sia G gruppo finito (not. mult.), e $g \in G$.

Allora $\{d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G\} \neq \emptyset$ (perché è contenuto in $\text{Ker}(f)$)

Si pone $\text{ord}(g) = \min \{d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G\}$ il minimo numero di volte per cui bisogna moltiplicare g per se stesso per ottenere 1_G

in not. additiva, $\text{ord}(g) = \min \{d \in \mathbb{N}^* \text{ t.c. } g \cdot d = 0_G\}$

Si ha allora $\langle g \rangle \cong \mathbb{Z}/\text{ord}(g)\mathbb{Z}$

esempio: $g = (123) \in S_3 =: G$

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & S_3 \\ n & \longmapsto & (123)^n \end{array}$$

n	$(123)^n$
0	1_{S_3}
1	(123)
2	(132)
3	1_{S_3}
4	(123)

$\text{ord}(123) = 3$
(si eleva al cubo per arrivare a 1_G)

$$\langle (123) \rangle \cong \mathbb{Z}/3\mathbb{Z}$$

ORDINE DI UN CICLO

Più generalmente, dato un n-ciclo di S_n $\sigma := (\alpha_1 \alpha_2 \dots \alpha_n)$

$$\text{ord}(\sigma) = n \quad e \quad \langle \sigma \rangle \cong \mathbb{Z}/n\mathbb{Z}$$



$$\text{quindi } \sigma^i \neq 1_{S_n} \quad \forall i = 1, \dots, n-1$$

Inoltre $\sigma^n(\alpha_1) = \alpha_1$. Ma noi possiamo scrivere σ "scalandolo", e trasformare α_2 in α_1 : $(\alpha_2 \alpha_3 \dots \alpha_n \alpha_1)$

Quindi, $\sigma^n(\alpha_2) = \alpha_2$. Più generalmente, $\sigma^n(\alpha_i) = \alpha_i \quad \forall i = 1 \dots n$

Siccome σ è un ciclo, esso fissa tutti gli el. $b \in \{1, \dots, n\} \setminus \{\alpha_1, \dots, \alpha_n\}$.

Quindi, $\sigma^n = 1_{S_n}$, da cui $n = \text{ord}(\sigma)$.

Abbiamo dimostrato

Lemma ORDINE DI UN CICLO

Se σ è un n-ciclo, allora

$$\text{ord}(\sigma) = n \quad e \quad \langle \sigma \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

[qui > lezione ha fatto un breve recap - omesso]

def MINIMO COMUNE MULTIPLOdati $m_1, \dots, m_l \in \mathbb{Z} \setminus \{0\}$ il minimo comune multiplo m di m_1, \dots, m_l è l'unico intero $m \in \mathbb{N}^*$ t.c.

$$\textcircled{1} \quad m_1, \dots, m_l \mid m$$

$$\textcircled{2} \quad \text{se } m \text{ è t.c. } m_1, \dots, m_l \mid m', \text{ allora } m \mid m'$$

Si scrive $m = \text{MCM}(m_1, \dots, m_l)$ e, per calcolarlo:

$$m_1\mathbb{Z} \cap m_2\mathbb{Z} \cap m_3\mathbb{Z} \cap \dots \cap m_l\mathbb{Z} = m\mathbb{Z}$$

ricordiamo che per l'MCD era lo stesso
cosa ma con il + ($m_1\mathbb{Z} + m_2\mathbb{Z} + \dots + m_l\mathbb{Z} = d\mathbb{Z}$)

$$\bullet \text{ in più, } \text{MCM}(a, b) = \frac{ab}{\text{MCD}(a, b)}$$

$$\bullet \text{ utilizzando il teorema fond. aritmetico: } a = \prod_p p^{v_p(a)}, \quad b = \prod_p p^{v_p(b)}$$

$$\text{allora } \text{MCM}(a, b) = \prod_p p^{\max(v_p(a), v_p(b))} \quad \text{per l'MCD era min}$$

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 decomponga 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: $\text{ord}(\sigma) = \text{MCM}(\text{ord}(c_1), \dots, \text{ord}(c_s))$

esempio

calcolare $\text{ord}(\sigma)$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} \in S_7 \quad n=7 \rightarrow (\text{se } \in S_n > 7, \text{ gli altri el. sono fissati})$$

① Decomponiamo σ in prodotto di cicli disgiunti

$$= \underbrace{(1 7)}_{\text{ord } 2} \underbrace{(2 4)}_{\text{ord } 2} \underbrace{(5 6 7)}_{\text{ord } 3} \quad ((3) \text{ si può omettere})$$

$$\textcircled{2} \quad \text{ord}(\sigma) = \text{MCM}(2, 2, 3) = 2$$

Metodo alternativo: sfrutta il fatto che $\text{ord}(\sigma) = \text{min. esponente}^{\textcircled{1}} \text{ a cui elevare } \sigma \text{ per avere l'identità}$

(3 omesso perché fissato)

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 4 & 5 & 6 & 7 \\ 7 & 4 & 2 & 6 & 5 & 1 \\ 1 & 2 & 4 & 5 & 6 & 7 \end{pmatrix} = 1_{S_7} \quad (n=7)$$

Si può vedere anche così $\sigma^2 = (17)(24)(56)(17)(24)(56) = (17)(24)(56)(56)(24)(17) = 1_{S_7} \quad (n=7)$ commuti, del tipo $a b c c^{-1} b^{-1} a^{-1} = 1$

l'inverso di una trasposizione è essa stessa

Sia perciò $\sigma = 2$ (quindi $\sigma^2 = 1$)
e sic per il "trucco" di leggerlo
al contrario: $(17) = (71)$

(uno delle volte "collusione"
nell'identità): $(56)(56) = 1_S$
 $(17)(24)(24)(17)$ ecc.)

esercizi:

- trovare α, β t.c. $(147)(132) \times \beta = 1_G$

$$\alpha = (132)^2 = (132)(132) = (123) \quad \text{oppure} \quad \alpha = \overleftarrow{(132)} = (231) = (123)$$

$$\beta = (147)^2 = (174)$$

- trovare α, β in S_7 t.c. $(1234)(137) \times \beta = 1_{S_8}$ $\alpha = (137)^2, \beta = (1234)^3$

- $\text{ord}((12)(345)) = 6$ • $\text{Ord}((12)(245)) = ?$ Non sono a supporto disgiunto.

Rendendosene di supp. disgi. = $\text{ord}(1245) = 4$

- $\text{ord}((12)(13)(14)) = \text{ord}((1432)) = 4$

Teorema (decomp. di permutazione in trasposizioni)

Ogni permutazione si decomponga in prodotto di trasposizioni non necessariamente a supporto disgiunto.

- in generale, una tale fattorizzazione non è unica

Esempio: $(\alpha_1 \alpha_2)(\alpha_1 \alpha_3)(\alpha_1 \alpha_4) = (\alpha_1 \alpha_4 \alpha_3 \alpha_2)$

$\#\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = 4$

FORMULA per un n-ciclo

$$\sigma = (\alpha_1 \alpha_2 \dots \alpha_n) = (\alpha_n \alpha_{n-1})(\alpha_n \alpha_{n-2}) \dots (\alpha_n \alpha_1) \quad (\text{ovvero } n-1 \text{ fattori})$$

In realtà $2 \leq n-1$, perché posso aggiungere quante identità voglio

Esempio: $(12345) = (54)(53)(52)(51)$

Teorema "rinforzato" - SEGNATURA/SEGNO DI UNA PERMUTAZIONE

Sia s il numero di trasposizioni in una fattorizzazione di $\sigma \in S_r$ in prodotto di trasposizioni.

Allora $s \bmod 2$ è unicamente determinato (anche se s non è unico)

Visto che $(\alpha_1 \alpha_2)(\alpha_1 \alpha_2) = 1_S$, aggiungere una coppia di trasposizioni (uguali) dà lo stesso risultato

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 $\varepsilon = -1$

per *

Nota: se σ n-ciclo, $\varepsilon(\sigma) = (-1)^{n-1}$

Se ne deduce:

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: $S \xrightarrow{\varepsilon} \mathbb{Z}^\times$

$$\begin{array}{ccc} S & \xrightarrow{\varepsilon} & \mathbb{Z}^\times \\ \pi \downarrow & \nearrow \cong & \\ S_r & & \ker(\varepsilon) \\ & & \text{Ker}(\varepsilon) \text{ contiene tutte le permutazioni che hanno segno pari} \\ & & \text{elementi di } S_r \text{ che puntano a 1} \\ & & \text{per la funzione } \varepsilon \\ & & \text{Quindi, questo quoziente divide le permutazioni in due classi: pari e dispari} \end{array}$$

COME CALCOLARE $\varepsilon(\sigma)$

Metodo meno divertente

- ① Si calcola la fattorizzazione di σ in prod. di cicli disgiunti

$$\sigma = c_1 \dots c_m$$

$$② \varepsilon(\sigma) = \varepsilon(c_1) \cdot \dots \cdot \varepsilon(c_m)$$

- ③ Si usa la formula per cui se φ r-ciclo, allora $\varepsilon(\varphi) = (-1)^{r-1}$

Metodo "adatto ad un venerdì sera"

senza decomporre in prodotto di cicli disgiunti,

calcoliamo la segnatura di σ con un procedimento grafico

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 7 & 5 & 8 & 6 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

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: 15 intersezioni.

$$\varepsilon(\sigma) = (-1)^{15} = -1$$



notò: quando conto le intersezioni, in base a come le disegno, avrò risultati diversi.

Ma la classe mod 2 (parità) sarà sempre la stessa, quindi è (o) non sarò inficiato.

es. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$ $E(\sigma) = (-1)^{15} = (-1)^{13} = -1$

• questo stesso esempio, ma con l'altra tecnica:

$$\sigma = (137)(2458)$$

$$E(\sigma) = E(137) \cdot E(2458) = (-1)^2 \cdot (-1)^3 = -1$$

19/11

○ PRODOTTO DIRETTO

PRODOTTO CARTESIANO DI GRUPPI

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:

$$(g_1, g_2), (g'_1, g'_2) \in G_1 \times G_2 \quad \text{operazione + : } (g_1, g_2) + (g'_1, g'_2) := (g_1 + g'_1, g_2 + g'_2)$$

• 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: $O_{G_1 \times G_2} = (O_{G_1}, O_{G_2})$

• $G_1 \times G_2$ 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 abeliani allora $G_1 \times \dots \times G_n$ abeliano)

esempio $(\mathbb{R}, +)$

• posso costruire il gruppo $\mathbb{R}^n = \underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_{n \text{ volte}}$ 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 $O = (0, \dots, 0)$

"esercizio 19"

Teorema di Lagrange

Sia G gruppo finito.

Sia $H < G$ ($\#H < \#G$ perché $< \Rightarrow \subset$)

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
partizioni finite a loro volta

Possiamo considerare l'insieme quoziente G/\sim con $\#G/\sim < \infty$

Poniamo $[G:H] = \#G/\sim (= G/H)$

indice di H in G

Siccome G/\sim è una partizione di G , $G = \bigsqcup_{c \in G/\sim} c \rightarrow$ quindi, $\#G = \sum_{c \in G/\sim} \#c$

Claim ①: $\#c = \#H$

[Se il claim è vero, abbiamo il teorema di Lagrange:

$$\text{infatti, } \#G = \sum_{c \in G/\sim} \#c = \sum_{c \in G/\sim} \#H = \#H \sum_{c \in G/\sim} 1 = \#H \cdot [G:H] \text{ quindi } \#H \mid \#G]$$

quindi $\#G = \#H \cdot \text{un intero}$
cardinalità di G/\sim

Quindi, dobbiamo dimostrare che $\forall c \in G/\sim, \#c = \#H$

Claim ②

$\forall g \in G$, poniamo $\psi_g: G \rightarrow G, \psi_g(x) = x \cdot g$ (ben definito perché G chiuso rispetto al prodotto)

Allora, ψ_g è una biiezione

N.B. $\psi_g(1g) = g \quad \forall g \neq 1g$ quindi ψ_g non è un endomorfismo

• Sappiamo che ψ_g è invertibile di inverso $\psi_{g^{-1}}$

Infatti, se $x \in G, \psi_{g^{-1}}(\psi_g(x)) = \psi_{g^{-1}}(xg^{-1}) = xg^{-1}g = x$ quindi $\psi_g \circ \psi_{g^{-1}} = \text{Id}_G$

Analogamente, $\psi_{g^{-1}}(\psi_g(x)) = \psi_{g^{-1}}(xg) = xgg^{-1} = x$ quindi $\psi_{g^{-1}} \circ \psi_g = \text{Id}_G$

notiamo che, generalmente

In particolare, se $I \subset G$, allora $\#\psi_g(I) = \#I$

(perché ψ_g è una biiezione)

$\psi_g \circ \psi_{g^{-1}} = \text{Id}_G$ ma questo non ci serve per Lagrange
(stiamo riservando il gr. G in modo diverso)

$$\text{e } \psi_{1_G} = \text{Id}_G$$

Quindi, se riusciamo a mostrare che una classe è l'immagine di H per un g ben scelto, abbiamo finito.

$(\psi_g(H)) = c \Rightarrow \#H = \#c$, 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 $y = hx$

Se $y \in c, xy^{-1} \in H$.

$\exists h \in H \quad \exists h \in H \quad \text{ogni el "y" di } c \text{ si può scrivere}$

$$xy^{-1} \in H \iff x = hy \iff y = h^{-1}x \iff y \in Hx \iff c = \psi_x(H) \quad \text{come } y = hx \exists h \in H, \text{ quindi } \psi_x(H)$$

Abbiamo quindi trovato il g per cui $\psi_g(H) = c$. Quindi, $\#H = \#c$, e quindi $\#G = \sum_c \#c = \#H \cdot [G:H]$ 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, $\langle \sigma \rangle \cong \mathbb{Z}/p\mathbb{Z} \Rightarrow \#\langle \sigma \rangle = p$

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 $S \xrightarrow{\epsilon} \mathbb{Z}^\times$, e $H = \text{Ker}(\epsilon)$

per il 1^o teorema iso:

$$S_{12}/H \cong \mathbb{Z}^\times \Rightarrow \# S_{12}/H = 2 \iff [S_{12} : H] = 2$$

$$12! = \# S_{12} = \# H \cdot 2 \Rightarrow \# H = \frac{12!}{2} \in \mathbb{N}^*$$

(anche logicamente, metà delle perm. saranno dispari e metà pari, quindi $\# \text{Ker}(\epsilon) = \frac{1}{2} \# S_{12}$)

• altro esempio

Se $m \leq n$, c'è (almeno) un omomorfismo iniettivo $S_m \xrightarrow{f} S_n$

• $f(S_m) \subset S_n$ (perché $m \leq n$)

$$\# f(S_m) = \# S_m = m! \quad (\text{perché è iniettivo})$$

Infatti f iniettiva $\Rightarrow S_m \cong f(S_m)$

Dal 1^o teorema iso:

$$\begin{array}{ccc} S_m & \xrightarrow{f} & S_n \\ \downarrow & & \uparrow \\ S_m / \{1_{S_m}\} & \xrightarrow{\cong} & f(S_m) \\ & \cong S_m & \end{array}$$

$\text{Ker}(f) = 1_{S_m}$ (l'unico el. di S_m che punto all'el. neutro di $S_n \ni 1_{S_m}$)

Sia $\tilde{G}_m = \left\{ \sigma \in S_n \text{ t.c. } \begin{array}{l} \sigma(m+1) = m+1 \\ \sigma(m+2) = m+2 \\ \vdots \\ \sigma(n) = n \end{array} \right\} = \left\{ \text{perm. in } S_n \text{ che fissano gli elementi da } m+1 \text{ a } n \text{ (ce ne sono } n-m\text{)} \right\}$

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 $f(S_m) = \tilde{G}_m$

def GRUPPI CICLICI

Sia G un gruppo, e $g \in G$ di ordine $n \geq 1$

Allora, $\langle g \rangle \cong \mathbb{Z}_{n\mathbb{Z}}$ (in not. additiva)

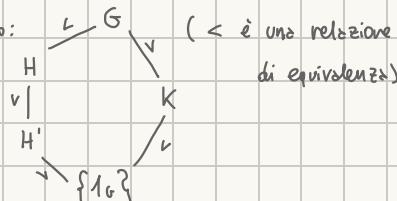
$$H \triangleleft G$$

quindi possiamo trovare i sottogruppi attraverso $\mathbb{Z}_{n\mathbb{Z}}$

prop:

- $\forall d \mid n, \exists$ sottogruppo $H_d \triangleleft H$ t.c. $\#H_d = d$

Quindi, il diagramma di Hasse di un gruppo G è del tipo:



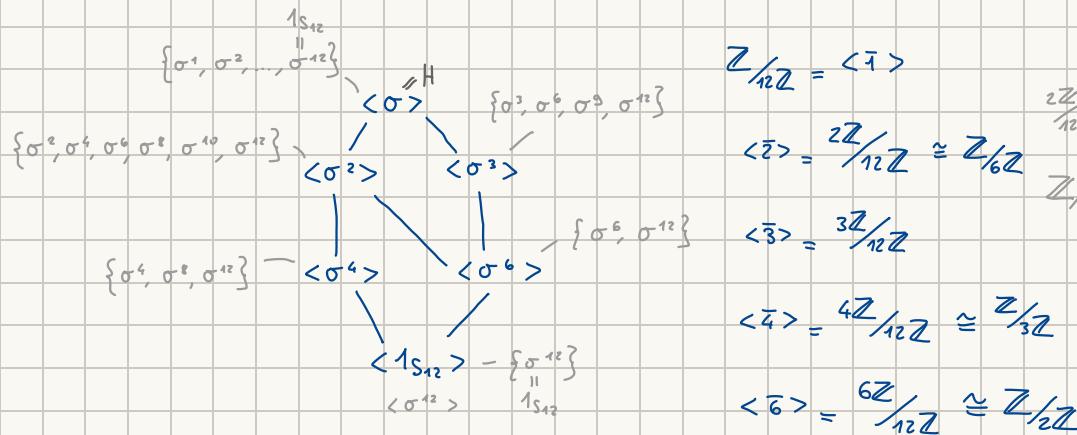
esempio

$$G = S_{12}, \sigma = (1 \ 2 \ 3 \dots 12)$$

$$\text{ord}(\sigma) = 12, \text{ quindi } \langle \sigma \rangle \cong \mathbb{Z}_{12\mathbb{Z}}$$

e \forall divisore di 12 c'è un unico $H_d \triangleleft H$ con $\#H_d = d$ quindi: 1, 2, 3, 4, 6, 12

e il diagramma di Hasse è:



perché? Abbiamo σ , una perm. di ordine 12 (quindi $\sigma^{12} = 1_{S_{12}}$)

Sappiamo che $\langle g \rangle$ è ciclico isomorfo a $\mathbb{Z}_{n\mathbb{Z}}$ (in not. additiva)

Quindi, esiste un sottogruppo $H_d \triangleleft \langle g \rangle$ con cardinalità d per ogni divisore di 12.

Per trovarli, possiamo "sviluppare" con $\mathbb{Z}_{12\mathbb{Z}}$. Visto che $\mathbb{Z}_{12\mathbb{Z}}$ è a sua volta ciclico di 12,

sappiamo che i sottogruppi di $\mathbb{Z}_{12\mathbb{Z}}$ sono generati dalle classi dei divisori di 12, ovvero:

$$[1], [2], [3], [4], [6], [12].$$

$$[1] = \{0, \dots, 11\} \text{ corrisponde a } \langle \sigma \rangle \quad (\text{sottogr. di ordine 12})$$

$$[2] = \{0, 2, 4, 6, 8, 10\} \text{ corrisponde a } \langle \sigma^2 \rangle \quad (\text{ordine 6})$$

$$[3] = \{0, 3, 6, 9\} \text{ corr. a } \langle \sigma^3 \rangle \quad (\text{ordine 4})$$

$$[4] = \{0, 4, 8\} \text{ corr. a } \langle \sigma^4 \rangle \quad (\text{ord. 3})$$

$$[6] = \{0, 6\} \text{ corr. a } \langle \sigma^6 \rangle \quad (\text{ord. 2})$$

$$[12] = \{0\} \text{ corr. a } \langle \sigma^{12} \rangle = 1_{S_{12}} \quad (\text{ord. 1})$$

SPAZI VETTORIALI

Data K campo,sia V un insieme $\neq \emptyset$ munito di:

$$\text{operazione binaria: } V \times V \longrightarrow V$$

$$(a, b) \longmapsto (a+b)$$

su K (si può scrivere)
/K

scalari vettori:

$$\text{un'operazione } K \times V \longrightarrow V$$

$$(\lambda, v) \longmapsto \lambda \cdot v$$

V ha
(somma e prodotto scalare)

è commutativa

Si dice che V è uno spazio vettoriale se:① $(V, +)$ è un gruppo abeliano (di el. neutro 0_V , $\circ \circ$)

$$\text{② } \alpha \cdot (v+w) = \alpha v + \alpha w \quad \forall \alpha \in K, \forall v, w \in V \quad \begin{matrix} \text{(distr. di scalare} \\ \text{su somma di vettori)} \end{matrix}$$

$$\text{③ } (\alpha + \beta) \cdot v = \alpha v + \beta v \quad \forall \alpha, \beta \in K, \forall v \in V \quad \begin{matrix} \text{(distr. di vettore} \\ \text{su somma di scalari)} \end{matrix}$$

$$\text{④ } (\alpha \cdot \beta) \cdot v = \alpha \cdot (\beta \cdot v) \quad \forall \alpha, \beta \in K, \forall v \in V \quad \text{Non-proprio-associatività}$$

$$\text{⑤ } 1_K \cdot v = v \quad \forall v \in V \quad \text{elemento neutro molt.}$$

Ma in V non esiste un
el. neutro per la molt., quindi
quello di K funge da neutro per
questa operazione

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 $v \in V$,

$$\begin{aligned} v + (-1)v &= (1 + (-1))v \\ &= 0 \cdot v = 0 \end{aligned}$$

• per esempio, $V = K$ è uno spazio vettoriale su K (perché K campo quindi K anche quindi distr., assoc., el. neutro)spazio vett. K^n • Poniamo $V = K \times \dots \times K = K^n$ con l'operazione $+$ di prodotto cartesiano di gruppi(con \emptyset el. neutro di K , $0_{K^n} = (0, \dots, 0)$ el. neutro di K^n)Definiamo $K \times V \rightarrow V$:

$$\begin{array}{ccc} n \text{ volte} & & n \text{ volte} \\ K \times \underbrace{K \times \dots \times K}_{n \text{ volte}} & \longrightarrow & \underbrace{K \times \dots \times K}_{n \text{ volte}} \\ (\lambda, (v_1, \dots, v_n)) & \longmapsto & (\lambda v_1, \dots, \lambda v_n) \\ & & \lambda(v_1, \dots, v_n) \end{array}$$

questa operazione soddisfa

tutti gli assiomi di spazio vettoriale

distr. a sx:

$$\begin{aligned} \text{② } \lambda \cdot ((v_1, \dots, v_n) + (w_1, \dots, w_n)) &= \lambda((v_1 + w_1, \dots, v_n + w_n)) = \\ &= (\lambda(v_1 + w_1), \dots, \lambda(v_n + w_n)) = (\lambda v_1 + \lambda w_1, \dots, \lambda v_n + \lambda w_n) = \\ &= (\lambda v_1, \dots, \lambda v_n) + (\lambda w_1, \dots, \lambda w_n) = \\ &= \lambda(v_1, \dots, v_n) + \lambda(w_1, \dots, w_n) = \lambda v + \lambda w \\ &= \lambda(v + w) \end{aligned}$$

 V , con queste operazioni, è uno spazio vettoriale.

Esempi di spazi vettoriali: (dato K campo)

$$\textcircled{1} \quad K^n, \quad \text{con } n=1, K^1 = K, \quad \text{con } n=0, K^0 = \{\emptyset\}$$

\textcircled{2} matrici con m linee e n colonne a coefficienti in K

$$M_{m,n}(K) = \left\{ \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} : a_{ij} \in K \forall i,j \right\} = \left\{ (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} : a_{ij} \in K \forall i,j \right\}$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$$

con operazioni di addizione coefficiente per coefficiente

e moltiplicazione esterna per λ separatamente per ogni coefficiente

$$\lambda = 2 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}$$

Note: essenzialmente, $M_{m,n}(K)$ è una riscrittura di $K^{m \times n}$ 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

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \in M_{2,3}(K) \xrightarrow{1:1} (a, b, c, d, e, f) \in K^6$$

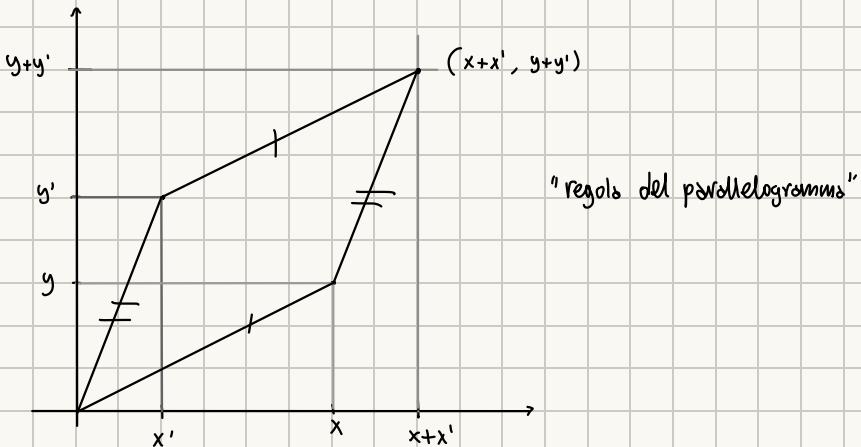
esempio operazioni:

$$A = (a_{ij}) \quad B = (b_{ij}) \quad \in M_{m,n}(K) = K^{m \times n}$$

$$\cdot A + B = (a_{ij} + b_{ij}) \in M_{m,n}(K)$$

$$\cdot \lambda \in K : \lambda A = (\lambda a_{ij}) \in M_{m,n}(K)$$

RAPPRESENTAZIONE GRAFICA DELLA SOMMA IN \mathbb{R}^2



\textcircled{3} Polinomi a coefficienti in K campo

$$V = K[x] \quad f = f_0 + f_1 x + f_2 x^2 \dots, \quad g = g_0 + g_1 x + g_2 x^2 \dots, \quad \lambda \in K$$

$$f+g = f_0 + g_0 + (f_1 + g_1)x + \dots$$

Osservazione: K finito (es. $K = \mathbb{F}_p$)

$$\lambda \cdot f = \lambda f_0 + (\lambda f_1)x + (\lambda f_2)x^2 + \dots$$

ma $K[x]$ infinito

④ lo ha skipato 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}

$$\mathbb{C} = \{x+iy : x, y \in \mathbb{R}\} \quad \text{la struttura di gruppo abelliano è nota}$$

$$\begin{aligned} \cdot \lambda \in \mathbb{R}, z \in \mathbb{C} \\ z = x+iy \end{aligned} \quad \begin{aligned} \lambda \cdot z &= \lambda(x+iy) = (\lambda x) + i(\lambda y) \\ &= \lambda z \end{aligned}$$

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 $f: V \rightarrow V'$ isomorfismo esiste, allora si dice che V e V' sono isomorfi e si scrive $V \cong V'$.

def SOTTOSPAZIO VETTORIALE

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 abelliani, si ha:

$$\cdot W \leq V$$

$$\cdot \forall w \in W, \forall \lambda \in K, \lambda \cdot w \in W$$

2 - $\cdot \forall w, w' \in W$, si ha $w + w' \in W$ (stabilità rispetto alla somma)

$$\cdot \forall w \in W, \forall \lambda \in K, \lambda \cdot w \in W$$

3 - Se è stabile per combinazioni lineari nel modo seguente:

$$\cdot \forall w, w' \in W, \forall \lambda, \lambda' \in K, \text{ si ha}$$

$$\lambda w + \lambda' w' \in W$$

4 - $\forall w_1, \dots, w_n \in V$ e $\forall \lambda_1, \dots, \lambda_n \in K$, $\lambda_1 w_1 + \dots + \lambda_n w_n \in W$

5 - $\forall w, w' \in W$ e $\forall \lambda \in K$, $w + \lambda w' \in W$

def COMBINAZIONE LINEARE

Dati $v_1, \dots, v_n \in V$, 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 "Span_K({v₁, ..., v_n})"
- "Vett_K({v₁, ..., 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 $w = (1, 0, 0)$, $w' = (0, 1, 0)$, $\lambda = 1$

$$w + \lambda w' = (1, 0, 0) + (0, 1, 0) = (1, 1, 0) \quad \text{e} \quad 1^2 + 1^2 + 0^2 = 1 + 1 + 0 = 2 \neq 1 \Rightarrow w + w' \notin S$$

metodo alternativo: ogni sottosp. vettoriale di \mathbb{R}^3 deve contenere $0 = (0, 0, 0)$. Qui $(0, 0, 0) \notin S$

el. neutro
somma (op. spaz. vett.)

def SPAN / SOTTOSPAZIO GENERATO

Prendiamo V sp.vett. su K . Sono $v_1, \dots, v_n \in V$.

Poniamo $W = \text{Span}_K(\{v_1, \dots, v_n\}) = \{\text{comb. lineari di } v_1, \dots, v_n\} = \{\lambda_1 v_1 + \dots + \lambda_n v_n : \lambda_1, \dots, \lambda_n \in K\}$

o Vett_K

è un sottospazio vettoriale.

Per vederlo, consideriamo $w, w' \in W$, $\lambda \in K$, e calcoliamo $w + \lambda w'$

$$\text{Mo} w = \sum_{i=1}^n \lambda_i v_i, w' = \sum_{i=1}^n \lambda'_i v_i, \text{ quindi } w + \lambda w' = \sum_{i=1}^n \underbrace{\lambda_i v_i}_{w} + \lambda \sum_{i=1}^n \lambda'_i v_i = \sum_{i=1}^n (\lambda_i + \lambda \lambda'_i) v_i \Rightarrow w + \lambda w' \in W$$

1° dist. 2° quindi si può scrivere quindi Span_K è un sottosp. vett.! per ⑤
come λv

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

analogo a sottogruppi generati

quindi è il più piccolo sottospazio vett. di W che contiene $\{v_1, \dots, v_n\}$.

Si chiama anche il sottospazio vettoriale generato da $\{v_1, \dots, v_n\}$. Talvolta si scrive $\langle \{v_1, \dots, v_n\} \rangle$

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., $W_1 \cap W_2 \subset V$ (perché $W_1, W_2 \subset V$ per def. sottosp.vett., e l'intersezione è un sottosp.vett.)

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 INDEPENDENTI

o l.i. o lin. ind.

Dato V sp.vett./K, v_1, \dots, v_n sono linearmente indipendenti se,

dati $\lambda_1, \dots, \lambda_n \in K$ t.c. $\lambda_1 v_1 + \dots + \lambda_n v_n = \emptyset$

Allora $\lambda_1 = \dots = \lambda_n = 0_K$

$$\sum_i \lambda_i v_i \quad (\sum_i \lambda_i v_i \text{ con } \lambda_i = 0 \text{ per } v_i)$$

Ovvero, se l'unica combinazione lineare di v_1, \dots, v_n che è nulla è quella banale (ovvero quella con tutti $\lambda_i = 0$)

Al contrario, si dicono linearmente dipendenti se esiste almeno una combinazione lineare nulla non banale.

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.

quindi, due vett. sono l.d. se uno si può scrivere in funzione dell'altro (come multiplo scalare)

$$\text{es } v_1 = 2v_2$$

$$\Leftrightarrow v_1 - 2v_2 = \emptyset$$

Consideriamo una comb. lin. $\lambda_1 v_1 + \lambda_2 v_2 = \emptyset$

$$\text{ovvero } \lambda_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \emptyset \iff \begin{pmatrix} \lambda_1 \\ 2\lambda_2 \end{pmatrix} + \begin{pmatrix} 2\lambda_1 \\ 2\lambda_2 \end{pmatrix} = \emptyset \iff \begin{pmatrix} \lambda_1 + 2\lambda_2 \\ 2\lambda_1 + 2\lambda_2 \end{pmatrix} = \emptyset$$

molt. scalare

somma
(vett.)

costruiamo il sistema lineare che ha $\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix}$ come soluzioni (si può direttamente mettere i vettori a sistema)

$$\begin{cases} \lambda_1 + 2\lambda_2 = 0 \\ 2\lambda_1 + 2\lambda_2 = 0 \end{cases} \iff \begin{cases} \lambda_1 + 2\lambda_2 = 0 \\ 2\lambda_1 + 2\lambda_2 = 0 \end{cases} \iff \begin{cases} \lambda_1 + 2\lambda_2 = 0 \\ 2(\lambda_1 + 2\lambda_2) = 0 \end{cases} \iff \begin{cases} \lambda_1 + 2\lambda_2 = 0 \\ 0 = 0 \end{cases} \iff \lambda_1 + 2\lambda_2 = 0 \iff \lambda_1 = -2\lambda_2 \quad \text{quindi: } \lambda_1 = \lambda_2 = 0$$

si
sottrae termine
a termine

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: Dato $f: V \xrightarrow{\cong} V'$, v_1, \dots, v_n sono l.i. se $f(v_1), \dots, f(v_n)$ sono l.i.
per esempio, $M_{m,n}(K) \cong K^{m \times n}$ può essere utile

esercizi

① notare che $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $v_2 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$$\begin{cases} \lambda_1 + 2\lambda_2 + \lambda_3 = 0 \\ 2\lambda_2 + 2\lambda_3 = 0 \\ \lambda_3 = 0 \end{cases}$$

$$\begin{cases} \lambda_1 + 2\lambda_2 = 0 \\ 2\lambda_2 = 0 \\ \lambda_3 = 0 \end{cases}$$

$$\begin{cases} \lambda_1 = 0 \\ \lambda_2 = 0 \\ \lambda_3 = 0 \end{cases}$$

② Consideriamo $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $v_2 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$
uno multiplo dell'altro

$$\lambda_1 = \lambda_2 = \lambda_3 = 0 \Rightarrow v_1, v_2, v_3 \text{ l.i.}$$

$$\text{si vede che } 2v_1 - v_2 + 0v_3 = \emptyset$$

def MATRICE TRIANGOLARE = M_n - un pedice solo indica righe = # colonne

una matrice $M \in M_{n,n}(\mathbb{R})$

è detta triangolare superiore se si può scrivere come

$$M = \begin{pmatrix} M_{11} & M_{12} & M_{13} & \dots & M_{1n-1} & M_{1n} \\ 0 & M_{22} & M_{23} & \dots & M_{2n-1} & M_{2n} \\ 0 & 0 & M_{33} & \dots & M_{3n-1} & M_{3n} \\ 0 & 0 & 0 & \dots & M_{4n-1} & M_{4n} \\ \vdots & & & & & \\ 0 & 0 & 0 & \dots & M_{n-1,n-1} & M_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 & M_{nn} \end{pmatrix}$$

(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)

diagonale della

matrice (m_{ij}) 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. $\iff \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 0 \\ 0 \end{pmatrix}$ sono l.d.

(gli zeri non influenzano)

$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix}$ l.d. perché

$$\begin{cases} \lambda_1 + 2\lambda_2 + 3\lambda_3 \\ \lambda_2 + 2\lambda_3 \end{cases} \iff \lambda_2 = -2\lambda_3 \quad \begin{cases} \lambda_1 = \lambda_3 \\ \lambda_2 = -2\lambda_3 \end{cases} \quad \text{se pongo } \lambda_3 = 1 \text{ allora} \\ (\lambda_1, \lambda_2, \lambda_3) = (-1, -2, 1) \neq (0, 0, 0)$$

e si ottiene la comb. nulla, ma non banale

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - 2 \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

esercizi (x casi)

$$\textcircled{1} \quad e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

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

\textcircled{2} \textcircled{3} $V = M_n(K)$, mostrare che le matrici

$$e_{ij} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{pmatrix} \quad 1 \leq i, j \leq n \quad \text{tutti zeroi} \quad \text{Matr. } n \times n$$

sono l.i.

$$\textcircled{4} \quad \text{Mostrare che } (e_{ij})_{1 \leq i, j \leq n} \text{ e } f: \begin{pmatrix} 1 & & 1 \\ & \ddots & \\ & & 1 \\ & & & 1 \end{pmatrix} \text{ sono l.d.} \quad \text{tutti uno}$$

DIVERSI MODI DI RAPPRESENTARE UNA MATRICE

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

$$\cdot A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

$$\cdot A = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} \text{ con } A_i: i\text{-esima riga di } A$$

$$\cdot A = (A^1 \dots A^n) \text{ con } A^j: j\text{-esima colonna di } A$$

$$A = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \in M_{2,3}(\mathbb{R}) \quad A_1 = (\text{dot}) \quad A_2 = (\text{def}), \quad A^1 = \begin{pmatrix} a \\ d \end{pmatrix}, \quad A^2 = \begin{pmatrix} b \\ e \end{pmatrix}, \quad A^3 = \begin{pmatrix} c \\ f \end{pmatrix}$$

PRODOTTO TRA MATRICI

prodotto scalare di una matrice linea e una matrice colonna

$$U = (v_1, \dots, v_n) \in M_{1,n}(K), \quad V = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in M_{n,1}(K)$$

$$\langle U, V \rangle = \sum_{i=1}^n U_i V_i = U_1 V_1 + \dots + U_n V_n$$

con questo prodotto scalare definiamo un'operazione: $M_{m,K}(K) \times \underbrace{M_{K,n}(K)}_{= \rightarrow} \rightarrow M_{m,n}(K)$

$$\text{dove } (A, B) \mapsto A \cdot B = \langle A_i, B^j \rangle_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

$$\overbrace{M_{1,K}(K)}^{A_1} \overbrace{\begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}}^B \overbrace{(B^1 \dots B^n)}_{M_{K,1}(K)} \quad \text{è un'operazione associativa e distributiva}$$

esempio

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in M_{2,3}, \quad B = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \in M_{3,2}$$

$$A \cdot B = \begin{pmatrix} \text{linea 1 A, colonna 1 B} & \text{linea 1 A, colonna 2 B} \\ \text{linea 2 A, col. 1 B} & \text{linea 2 A, col. 2 B} \end{pmatrix} \quad \text{ovvero} \quad B = \begin{pmatrix} 1 & 4 \\ -2 & 2 \\ 0 & 3 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 & 1 \cdot 4 + 2 \cdot 5 + 3 \cdot 6 \\ 4 \cdot 1 + 5 \cdot 2 + 6 \cdot 3 & 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 6 \end{pmatrix} = \begin{pmatrix} 14 & 32 \\ 32 & 77 \end{pmatrix} \in M_{2,2}(\mathbb{R})$$

esercizio

• calcolare $B \cdot A \in M_{3,3}(\mathbb{R})$

$$B = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

$$B \cdot A = \begin{pmatrix} 1 \cdot 1 + 4 \cdot 4 & 1 \cdot 2 + 4 \cdot 5 & 1 \cdot 3 + 4 \cdot 6 \\ 2 \cdot 1 + 5 \cdot 4 & 2 \cdot 2 + 5 \cdot 5 & 2 \cdot 3 + 5 \cdot 6 \\ 3 \cdot 1 + 6 \cdot 4 & 3 \cdot 2 + 6 \cdot 5 & 3 \cdot 3 + 6 \cdot 6 \end{pmatrix} = \begin{pmatrix} 17 & 22 & 27 \\ 23 & 29 & 36 \\ 27 & 36 & 45 \end{pmatrix}$$

MATRICE IDENTITÀ $1_n, \text{Id}_n \in M_n(K)$ in $M_n(K)$, la matrice

$$1_n = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

tutti zeri e
diagonale di uno

svolge il ruolo di elemento neutro per il prodotto righe-colonne tra matrici

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 INVERTIBILIUna 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)

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

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)

si scrive anche:

 $A \in M_2(K)$ è invertibile per la moltiplicazione linee per colonne

$$\iff \det(A) \neq 0 \quad (\iff \det(A) \in K^\times)$$

$$A \in GL_2(K), \quad A \in (M_2(K))^\times$$

di inverso *

$$(A \text{ invertibile} \iff \exists A' \in M_2 \text{ t.c. } A \cdot A' = A' \cdot A = 1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$$

dim:

$$\textcircled{1} \quad \det(A) \neq 0 \implies A \in GL_2(K)$$

Poniamo $A' = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2$
 $\neq 0$ per ip.

$$\text{Calcoliamo } AA' = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{Id}_2$$

$$\text{e } A'A = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{Id}_2$$

prod.
scolare colonna.

Sappiamo quindi che $A' = A^{-1}$

Lemmo: dati $A, B \in M_2(K)$ non lo dimostriamo
allora $\det(AB) = \det(A) \cdot \det(B)$

② $A \in GL_2(K) \implies \det(A) \neq 0$

$$A \in M_2(K)^{\times} \iff \exists A' \in M_2(K)^{\times} \text{ t.c. } AA' = A'A = I_2$$

Calcoliamo i determinanti: $\det(AA') = \det(A'A) = 1 \neq 0$
 $\det(A) \det(A')$ || lemma || $\det(A') \det(A)$
 $\implies \det(A), \det(A') \neq 0$ (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

note: $GL_2(\mathbb{R})$ 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 $AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$

Esercizio

$$M_2(\mathbb{F}_2) \cong \mathbb{F}_2^4 = \mathbb{F} \times \mathbb{F} \times \mathbb{F} \times \mathbb{F}$$

di cardinalità $2^4 = 16$

liste completa degli el. di $M_2(\mathbb{F}_2)$ (con $1 = [1], 2 = [2]$)

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

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

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

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

Mostrare che
 $GL_2(\mathbb{F}_2) \cong S_3$

$$\square \in GL_2(\mathbb{F})$$

SPAZIO

SVOLGIMENTO

FUTURO

SISTEMI LINEARI

Dato un campo K , un sistema lineare di m equazioni e n indeterminati a coeff. in K

è un sistema di equazioni del tipo:

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

Coeffienti $\in K$

Termini noti / costanti $\in K$

Risolvere un sistema significa descrivere l'insieme di tutti i vettori

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n \text{ tali che tutte le equazioni sono soddisfatte simultaneamente}$$

• Un sistema lineare $(*)$ si dice compatibile se il sottoinsieme $\text{Sol}(*)$ 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 $\begin{cases} x_1 = 0 \end{cases}$ è compatibile, con $\text{Sol} = \{(0)\} \subset K^1$
 $(1 \neq 0 \text{ in ogni campo})$

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 minimi"

ESPRESSIONE MATRICIALE DI UN SISTEMA LINEARE SU K

Il sistema $(*)$ si può riscrivere alternativamente nel modo seguente

matrice dei coeff.
 $A = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{pmatrix} = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} \in M_{m,n}(K) , \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in M_{m,1}(K) , \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in M_{n,1}(K)$

$$A \cdot X = \begin{pmatrix} \langle A_1, X \rangle \\ \langle A_2, X \rangle \\ \vdots \\ \langle A_m, X \rangle \end{pmatrix} \in M_{m,1}(K)$$

prodotto matriciale linea · colonna
 da ogni linea di A (coeff. $\alpha_{11}, \dots, \alpha_{1n}$)
 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 $(*) A\mathbf{x} = b$ è sempre compatibile e ammette un'unica soluzione \mathbf{x} .

Infatti, sia A^{-1} l'inverso di A . Allora, $\mathbf{x} \in M_{m,1}(K)$ è soluzione di $(*) \iff A^{-1}A\mathbf{x} = A^{-1}b \iff \mathbf{x} = b$

Quindi, $\text{Sol}(\star) = \{(b)\}$.

MATRICE COMPLETA ASSOCIATA A UN SISTEMA LINEARE

Consideriamo un sistema lineare:

$$(*) = A\mathbf{x} = b$$

giustapposizione di b ad A

tutti i suoi dati sono contenuti nella matrice: $(A|b) \in M_{m,n+1}(K)$

matrice completa del sistema

• se $b = \emptyset$ il sistema è omogeneo

altrimenti, è non omogeneo

OSS: $A\mathbf{x} = b \iff x_1 A^1 + x_2 A^2 + \dots + x_n A^n = b$

esemp.

$\iff b$ è combinazione lineare di A^1, \dots, A^n

$$\textcircled{1} \quad \begin{cases} 2x_1 + x_2 - 3x_3 + x_4 = 1 \\ x_3 + x_4 = 5 \\ x_1 - x_2 - x_3 - 2x_4 = 0 \end{cases} \quad (K = \mathbb{R})$$

$\iff b \in \text{Span}_K(A^1, \dots, A^n)$

$$A = \begin{pmatrix} 2 & 1 & -3 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & -1 & -2 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$\text{quindi } x_1 \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} -3 \\ 1 \\ -1 \end{pmatrix} + x_4 \begin{pmatrix} 1 \\ -1 \\ -2 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$$

$$(A|b) = \begin{pmatrix} 2 & 1 & -3 & 1 & 1 \\ 0 & 0 & 1 & 1 & 5 \\ 1 & -1 & -1 & -2 & 0 \end{pmatrix}$$

dire che $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ è soluzione di $(*)$ significa

che $x_1 A^1 + x_2 A^2 + x_3 A^3 + x_4 A^4 = b$

ovvero $(*)$ è compatibile $\iff b \in \text{Span}_{\mathbb{R}}(A^1, A^2, A^3, A^4)$

$$\textcircled{2} \quad \begin{cases} 2x_1 - x_2 - x_3 = 1 \\ x_1 + x_3 = 5 \end{cases} \iff x_1 \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 2 & -1 & -1 \\ 1 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix}$$

questo sistema è compatibile $\iff \begin{pmatrix} 1 \\ 5 \\ 0 \end{pmatrix} \in \text{Span}_{\mathbb{R}}\left(\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}\right)$

$$\text{il che è vero, infatti } \begin{cases} 2x_1 - x_2 - x_3 = 1 \\ x_1 + x_3 = 5 \end{cases} \iff x_1 = 5 - x_3 \quad \begin{cases} 10 - x_2 - 3x_3 = 1 \\ x_1 = 5 - x_3 \end{cases} \quad \begin{cases} x_2 = 9 - x_3 \\ x_1 = 5 - x_3 \end{cases}$$

ammette soluzioni, e.s. $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \\ 0 \end{pmatrix}$

STRUTTURA DELL'INSIEME DI SOLUZIONI DI UN SISTEMA LINEARE

Consideriamo il sistema $Ax = b$ (*) con $A \in M_{m,n}(K)$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K)$, $b \in M_{m,1}(K)$

NOTAZIONE

Se (*) è incompatibile, poniamo $\text{Sol}(A|b) = \emptyset$

Se (*) è compatibile, poniamo $\text{Sol}(A|b) = \left\{ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n \text{ t.c. } x \text{ è sol. di } (*) \right\}$

Proposizione

$\text{Sol}(A|b)$ 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 $\alpha_1 0 + \alpha_2 0 + \dots + \alpha_n 0$ non può essere $\neq 0$

(se 0 è tra le sol, $b = 0$ per forza)

dim

- Se $b \neq 0$, visto che $\text{Sol}(A|b) = \left\{ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ t.c. } A^1 x_1 + A^2 x_2 + \dots + A^n x_n = b \right\} \not\ni \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, e $\text{Sol}(A|b)$ non è s.v. di K^n .
- Supponiamo quindi che $b = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = 0$.

Mostriamo che $\text{Sol}(A|0)$ è un s.v. di K^n .

Prendiamo $X, X' \in \text{Sol}(A|0)$ e $\alpha, \alpha' \in K$. Devo mostrare che $\alpha X + \alpha' X' \in \text{Sol}(A|0)$

p.80
def ③ sottosp. vett. :
stabilità per comb. lineari

$$X \in \text{Sol}(A|0) \iff AX = 0 \quad \& \quad X' \in \text{Sol}(A|0) \iff AX' = 0$$

$$A(\alpha X + \alpha' X') = \alpha A X + \alpha' A X' = \alpha \cdot 0 + \alpha' \cdot 0 = 0 \implies \alpha X + \alpha' X' \in \text{Sol}(A|0)$$

prodotto scalare
è commutativo

Teorema

Supponiamo di avere un sistema

$$(*) \quad AX = b, \quad A \in M_{m,n}(K), \quad b \in M_{m,1}(K), \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K)$$

Supponiamo inoltre che $(*)$ sia compatibile ($\text{Sol}(A|b) \neq \emptyset$) $\hookrightarrow K^m$
 (cioè è equivalente a $b \in \text{Span}_K(A^1, \dots, A^n) \subset M_{m,1}(K)$)

Sia $x_0 \in \text{Sol}(A|b)$. Allora,

$$\text{Sol}(A|b) = x_0 + \text{Sol}(A|\emptyset)$$

struttura simile al CRT

dim

Sia $X \in \text{Sol}(A|b)$. Allora, $X = X - x_0 + x_0$ ovvero $X = \underbrace{x_0}_{\substack{\text{così ho} \\ x_0 + \text{Sol}(A|\emptyset)}} + \underbrace{X - x_0}_{\substack{\text{ovvero} \\ X - x_0 \in \text{Sol}(A|\emptyset)}}$

① Per mostrare che $\text{Sol}(A|b) \subset x_0 + \text{Sol}(A|\emptyset)$, basta verificare che $X - x_0 \in \text{Sol}(A|\emptyset)$, ovvero che $A(X - x_0) = \emptyset$

Noi sappiamo che $AX = b$ e che $AX_0 = b \Rightarrow \underbrace{AX - AX_0}_{\substack{b-b \\ A(X - x_0)}} = \emptyset \Rightarrow X - x_0 \in \text{Sol}(A|\emptyset)$ mostrato \subset

② Mostriamo adesso che $\forall y \in \text{Sol}(A|\emptyset)$, $x_0 + y \in \text{Sol}(A|b)$

Dico deve dormire b.
 Dico calcolare $A(x_0 + y) = \underbrace{Ax_0}_b + \underbrace{Ay}_\emptyset = b + \emptyset = b \Rightarrow x_0 + \text{Sol}(A|\emptyset) \subset \text{Sol}(A|b)$ mostrato \subset
 perché $x_0 \in \text{Sol}(A|b)$ perché $y \in \text{Sol}(A|\emptyset)$

Quindi, $\text{Sol}(A|b) = x_0 + \text{Sol}(A|\emptyset)$ ■

esempio

$$\left\{ \begin{array}{l} x_1 + 2x_2 + 3x_3 = 1 \\ x_2 - x_3 = 4 \\ x_3 = 5 \end{array} \right. \quad A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix}$$

noto che $x_3 = 5$ - sostituisco "a cascata"

$x_3 = 5, \quad x_2 = 9, \quad x_1 = -32$

$$\text{Sol}(*) = \left\{ \begin{pmatrix} -32 \\ 9 \\ 5 \end{pmatrix} \right\}$$

equivalentemente, grazie al teorema precedente, posso scrivere

$$\text{Sol}(A|b) = x_0 + \text{Sol}(A|\emptyset) = \begin{pmatrix} -32 \\ 9 \\ 5 \end{pmatrix} + \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\} \subset M_{3,1}(\mathbb{R})$$

ALGORITMO DI GAUSS

Introduciamo una relazione sulle matrici complete di $M_{m,n+1}(K)$
 ↴
 n indet. e b giù l'opposto

$M, M' \in M_{m,n+1}(K) \quad M \sim M' \iff \text{Sol}(M) = \text{Sol}(M')$
 ↴
 abbastanza ovvio (l'ugualanza è di equiv)
 è una relazione di equivalenza

$$AX = b \rightsquigarrow M(A|b)$$

Ideas di Gauss: usare un insieme "semplice" di trasformazioni su $M_{m,n+1}(K)$ che lasciano invarienti 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 ↴ non nullo
- ② MOLTIPLICARE UN'EQ DEL SISTEMA PER UNO SCALARE $\lambda \in K^*$ ↴ una riga qualsiasi
- ③ SOSTITUIRE UNA RIGA CON SE STESSA + UN MULTIPLO SCALARE DI UN'ALTRA RIGA ↴ somma vett.
 ↴ es. 3a riga $\leftarrow 2 \cdot 2a$ 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 Perron (lasymp su LateX)

$M \asymp M' \iff M' \text{ si può ottenere da } M \text{ attraverso un numero finito di operazioni } ①, ②, ③$
 ↴ è una rel. di equiv.

Teorema

$M \asymp M' \implies M \sim M'$ (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:

$$\begin{array}{c} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 2 & 2 & 2 & 4 \end{array} \right) \xrightarrow{\substack{R_3 \xrightarrow{2} \frac{1}{2}R_3 \\ R_2 \xrightarrow{3} R_2 - R_1}} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & 1 & -1 & 3 \\ 0 & 0 & 0 & 4 \end{array} \right) \xrightarrow{\substack{R_3 \xrightarrow{3} R_3 - R_1 \\ -1 \cdot R_1}} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & 1 & -1 & 3 \\ 0 & 0 & 0 & 0 \end{array} \right) \xrightarrow{\substack{\text{questa riga è una tautologia } (0=0) \\ \text{ma non la tolgo} \\ \text{perché siamo in } M_{3,4}(\mathbb{R})}} \left(\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right) \\ \xrightarrow{\substack{R_1 \xrightarrow{3} R_1 - R_2}} \xrightarrow{\substack{\text{gradiini ridotto} \\ (\text{definito dopo})}} \end{array}$$

e per il teorema, $\text{Sol}\left(\begin{array}{l} x+2z=1 \\ y-z=1 \end{array}\right) = \text{Sol}(M) = \mathcal{E}$ ↴ soluzione sistema om. associata a $\text{Span}_{\mathbb{R}}\left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}\right)$
 (sottosp. vett. generato dalle sol. dell'omogeneo associato)

$$\mathcal{E} = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in M_{3,1}(\mathbb{R}) \text{ t.c. } \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + z \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}, z \in \mathbb{R} \right\}$$

↳ riscritto il sistema

$$\begin{cases} x+2z=1 \\ y-z=1 \end{cases} \quad \begin{cases} x=1-2z \\ y=1+z \end{cases}$$

qui (al posto di $z = \dots$) c'è $z = 0$, quindi la sostituiamo con un'altra tautologia ($z=z$) $\left(\begin{array}{c} \vdots \\ z \\ \vdots \end{array} \right) = \left(\begin{array}{c} \vdots \\ 0 \\ \vdots \end{array} \right) + z \left(\begin{array}{c} \vdots \\ 1 \\ \vdots \end{array} \right)$

def MATRICE A GRADINI

$$\left(\begin{array}{cccc|ccccc} 0 & \dots & 0 & 1 & * & \dots & \dots & \dots & * \\ 0 & \dots & 0 & 0 & 0 & 1 & * & \dots & * \\ 0 & \dots & 0 & \dots & 0 & 0 & 1 & * & * \\ \vdots & & & & & & & \vdots & \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & \dots & \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & \dots & \\ \end{array} \right)$$

pivot

caso "estremi"

Non devono per forza esserci tutti zeri in fondo

triang. sup. con 1 sulle diag.

$$\left(\begin{array}{ccccc} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \\ & 0 & & & & \\ \end{array} \right)$$

matrice di zeri:

$$\left(\begin{array}{c} \text{circle with diagonal line} \end{array} \right)$$

- tra una riga e l'altra, l'uno deve essere almeno sulla colonna successiva al precedente

(cioè, $\begin{matrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$ No, $\begin{matrix} 0 & 1 & * \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{matrix}$ Sì, $\begin{matrix} 0 & 1 & ** \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{matrix}$ Sì)

Più formalmente, A è a gradini se:

- ① $A_{ij} = 0 \Rightarrow A_{jh} = 0 \quad \forall j > i$
- ② Se $A_{ii} \neq 0$, 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. $M \xrightarrow{\sim} \Gamma$

$$(A|b) = \left(\begin{array}{ccccc|c} 1 & 1 & -1 & -2 & 4 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & -2 \end{array} \right) \xrightarrow{R_2 \leftarrow R_2 - R_1} \left(\begin{array}{ccccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & -1 & 0 & 2 & -4 \\ 0 & 1 & 0 & 1 & -2 \end{array} \right) \xrightarrow{R_2 \leftarrow -R_2} \left(\begin{array}{ccccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 1 & 0 & 1 & -2 \end{array} \right) \xrightarrow{R_3 \leftarrow R_3 - R_2} \left(\begin{array}{ccccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 3 & -6 \end{array} \right) \xrightarrow{R_3 \leftarrow \frac{1}{3}R_3} \left(\begin{array}{ccccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 1 & -2 \end{array} \right) \xrightarrow{\text{a gradini}}$$

def MATRICE A GRADINI RIDOTTA

$$\left(\begin{array}{cccc|ccccc} 0 & \dots & 0 & 1 & * & \dots & 0 & \dots & 0 & \dots & * \\ 0 & \dots & 0 & 0 & 0 & 1 & * & \dots & 0 & \dots & * \\ 0 & \dots & 0 & \dots & \dots & 0 & 0 & 1 & * & \dots & * \\ \vdots & & & & & & & \vdots & & & \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \dots & \dots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & \dots & \dots & 0 \\ \end{array} \right)$$

è una matrice a gradini t.c.

- ④ dato un pivot di modo che

$$a_{ij} = 1, \text{ allora } \forall k \in \{1, \dots, i-1\}, a_{kj} = 0$$

(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. $M \xrightarrow{\sim} \Gamma$

continuiamo l'esempio di prima

$$\left(\begin{array}{ccccc|c} 1 & 1 & -1 & -2 & 4 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 1 & -2 \end{array} \right) \xrightarrow{R_1 \leftarrow R_1 - R_2} \left(\begin{array}{ccccc|c} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -2 & 4 \\ 0 & 0 & 0 & 1 & -2 \end{array} \right) \xrightarrow{R_2 \leftarrow R_2 + 2R_3} \left(\begin{array}{ccccc|c} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{array} \right) \xrightarrow{\text{a gradini ridotta}}$$

$$\text{Sol}(M) = \text{Sol} \left(\begin{pmatrix} x-z=0 \\ y=0 \\ z=t=-2 \end{pmatrix} \right) = \left\{ \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \in M_{4,1}(\mathbb{R}) \text{ t.c. } \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + z \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + \text{Span}_{\mathbb{R}} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right)$$

domanda: $\text{Sol}(M) = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 2 \end{pmatrix} + \text{Span}_{\mathbb{R}} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right)$? Si, perché x_0 soluzione particolare non è unico
 è sol part.: $\begin{pmatrix} 0 \\ 0 \\ 0 \\ -2 \end{pmatrix} + \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad X - x_0 \in \text{Sol}(A|b)$

esercizio

$$\in M_{3,5+1} \quad \cup \quad \left(\begin{array}{cccc|c} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 2 \end{array} \right) \quad \cup \quad \left(\begin{array}{cccc|c} 0 & 0 & 1 & 2 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 3/2 \end{array} \right) \quad \cup \quad \left(\begin{array}{cccc|c} 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1/2 \end{array} \right) \quad \cup \quad \left(\begin{array}{cccc|c} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3/2 \end{array} \right) \rightarrow \text{gradini ridotti}$$

$R_3 \mapsto \frac{1}{2}R_3$
Switch tra $R_1 \leftrightarrow R_2$

$$\left(\begin{array}{ccccc|c} 1 & 2 & 3 & 4 & 5 & b \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3/2 \end{array} \right)$$

Vediamo da qui che quelle tre righe "rappresentano" x_3, x_4, x_5 quindi i valori

(in un sistema avremmo)

$$\left\{ \begin{array}{l} x_3 = \frac{1}{2} \\ x_4 = 0 \\ x_5 = \frac{3}{2} \end{array} \right.$$

$$\text{Sol}(M) = \left\{ \begin{pmatrix} 0 \\ 0 \\ 1/2 \\ 0 \\ 3/2 \end{pmatrix} + \text{Span}_{\mathbb{R}} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right) \right\}$$

perché? invece, $\text{Span}_{\mathbb{R}}$ viene dall'omogeneo associato, in cui X_3, X_4, X_5 sono invece "vincolati" a 0

- le uniche "libere" (tutte le cui combinazioni formano le soluzioni dell'omogeneo) sono X_1, X_2 per questo, $\text{Span}_{\mathbb{R}} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right)$ qui sono "1"

4/12

esercizio

② dire se il seguente sistema è compatibile e trovare tutte le soluzioni ($K = \mathbb{R}$)

Soluzioni: matrice colonna $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ t.c. le equazioni in (*) siano simultaneamente soddisfatte

$$(*) \left\{ \begin{array}{l} 2x + 3y - 2z = 1 \\ y - z = 2 \\ x + y + z = -2 \end{array} \right.$$

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 lo trasformiamo in forma a gradini (+ ridotta) con l'algoritmo di Gauss

$$(A|b) = \left(\begin{array}{ccc|c} 2 & 3 & -2 & 1 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array} \right) \quad \cup \quad \left(\begin{array}{ccc|c} 0 & 1 & -4 & 5 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array} \right) \quad \cup \quad \left(\begin{array}{ccc|c} 0 & 0 & -3 & 3 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array} \right) \quad \cup \quad \left(\begin{array}{ccc|c} 0 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array} \right)$$

$R_1 \mapsto R_1 - 2R_3$ $R_1 \mapsto R_1 - R_2$ $R_1 \mapsto -\frac{1}{3}R_1$

posso anche fare una m. a gradini: "al contrario" e poi permutare le righe

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -1 \end{array} \right)$$

$R_1 \leftrightarrow R_3$

è a gradini, ora va ridotta.

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right)$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right)$$

$$\Leftrightarrow \text{Sol}(\ast) = \left\{ \begin{pmatrix} -2 \\ 1 \\ -1 \end{pmatrix} \right\}$$

Si possono fare due

passaggi insieme, ma occhio

a non operare sulle stesse righe

perché le sol. dell'omogeneo

$$\text{è } \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Tutte le comb. sono 0)

③ interpretiamo z come un parametro invece che un'indeterminata
(decido io il valore)

$$(\ast\ast) \left\{ \begin{array}{l} 2x + 3y - 2z = 1 \\ y - z = 2 \\ x + y + z = -2 \end{array} \right.$$

determinare l'insieme E dei valori del parametro $z \in \mathbb{R}$ t.c. $(\ast\ast)$ 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

$$(A|b) = \left(\begin{array}{ccc|c} 2 & 3 & 1+2z & \\ 0 & 1 & 2+z & \\ 1 & 1 & -2-z & \end{array} \right) \xrightarrow{\text{R}_1 \leftrightarrow R_1 - R_3} \left(\begin{array}{ccc|c} 0 & 1 & 5+4z & \\ 0 & 1 & 2+z & \\ 1 & 1 & -2-z & \end{array} \right) \xrightarrow{\text{R}_2 \leftrightarrow R_2 - R_1} \left(\begin{array}{ccc|c} 0 & 0 & 3+3z & \\ 0 & 1 & 2+z & \\ 1 & 1 & -2-z & \end{array} \right) \xrightarrow{\text{R}_3 \leftrightarrow R_3} \left(\begin{array}{ccc|c} 1 & 1 & -2-z & \\ 0 & 1 & 2+z & \\ 0 & 0 & 3+3z & \end{array} \right)$$

Il sistema associato è $\begin{cases} x+y = -2-z \\ y = 2+z \\ 0 = 3+3z \end{cases}$ che è compatibile $\iff z = -1$

notiamo che $z = -1$
era anche nella sol. precedente $\begin{pmatrix} -2 \\ 1 \\ -1 \end{pmatrix}$

Quindi $E = \{-1\}$. 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 questo combacia

Note: praticamente ho portato di lì
una po' inutile

$$\left(\begin{array}{ccc|c} 2 & 3 & -2 & 1 \\ 0 & 1 & -1 & 2 \\ 1 & 1 & 1 & -2 \end{array} \right)$$

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)

(ovvero il numero di righe non nulle.)

Notazione: $\text{rg}(A) \in \mathbb{N} : A \in M_{m,n}(K)$ • $\text{rg}(A) = 0 \iff A = (\emptyset)$
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 $\text{rg}(A') = \text{rg}(A)$

ridurre non cambia il
nr. di pivot

(non l'ha detto)

è il massimo numero di righe (o colonne) l.i. della matrice (infatti, se riduco la matrice, le righe l.d. diventeranno nulle.)

es. $\left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 1 & 1 & 1 \end{array} \right) \xrightarrow{\text{riduzione}} \left(\begin{array}{ccc} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 1 & 2 \end{array} \right)$

$$\left(\begin{array}{c} 2 \\ 4 \\ 6 \end{array} \right) = 2 \cdot \left(\begin{array}{c} 1 \\ 2 \\ 3 \end{array} \right)$$

$$A = \left(\begin{array}{cccc} 1 & 2 & 1 & 3 \\ 2 & 1 & 0 & 2 \\ 1 & 0 & -1 & 2 \end{array} \right) \quad \text{rg}(A) = \text{rg} \left(\begin{array}{cccc} 1 & 2 & 1 & 3 \\ 0 & -3 & -2 & -4 \\ 0 & -2 & -2 & -1 \end{array} \right) = \text{rg} \left(\begin{array}{cccc} 1 & 2 & 1 & 3 \\ 0 & -3 & -2 & -4 \\ 0 & 0 & -2 & 5 \end{array} \right) = 3$$

3 pivot
(non mi serve trasformarli in 1 per vederlo)

OSSERVAZIONI

① Una matrice $A \in M_{m,n}(K)$ può avere al massimo rango $\text{rg}(A) = \min(m, n)$

e esempi "limite"

$$\left(\begin{array}{ccccc} 1 & & & & * \\ 1 & 1 & & & \\ 1 & 1 & 1 & & \\ 1 & 1 & 1 & 1 & \\ 0 & 0 & 0 & 0 & \end{array} \right)$$

se c'è un pivot per colonna,
 $\text{rg}(A) = n$ (colonne), che $i < m$ (righe)

$$\left(\begin{array}{ccccc} 1 & & & & * \\ 1 & 1 & & & \\ 1 & 1 & 1 & & \\ 1 & 1 & 1 & 1 & \\ 0 & 0 & 0 & 0 & \end{array} \right)$$

se c'è un pivot per riga,
 $\text{rg}(A) = m$ e $m < n$

(se la matrice è quadrata con diagonale di pivot, $m = n$
quindi $\min(m, n) = m = n$
chiaramente)

② $\text{rg}(A) \leq \text{rg}(A|b)$ qualunque sia data una colonna $b \in M_{m,1}(K)$
("aumentando" la matrice, il range non può diminuire)

A ridotto attraverso le operazioni elementari, trasformo A in questo matrice
→ gradini ridotta

faccio le stesse operazioni su (A|b)
- visto che si mescolano le righe ma non le colonne,
la parte a sinistra sarà uguale -
(A)

qui può esserci al massimo un pivot in più

se ne deduce che $\text{rg}(A) \leq \text{rg}(A|b)$

OK.

- Rouché-Capelli theorem in English speaking countries, Italy and Brazil;
- Kronecker-Capelli theorem in Austria, Poland, Ukraine, Croatia, Romania, Serbia and Russia;
- Rouché-Foncqd theorem in France;
- Rouché-Frobenius theorem in Spain and many countries in Latin America;
- Frobenius theorem in the Czech Republic and in Slovakia.

Theorema ROUCHE-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 $\iff \text{rg}(A) = \text{rg}(A|b)$

colonne (= indeterminate)

② Se $(*)$ è compatibile, poniamo $s := n - \text{rg}(A) \geq 0$ "grado di libertà" del sistema

Esistono allora vettori $v_1, \dots, v_s \in \text{Sol}(A|0)$ linearmente indipendenti t.c. $\text{Sol}(A|0) = \text{Span}_K(v_1, \dots, v_s)$

Quindi, dato $v_0 \in \text{Sol}(A|b)$, si ha $\text{Sol}(A|b) = v_0 + \sum_{i=1}^s K v_i$

x parentesi mia
x copiare meglio:

esempio grado 1

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & b \\ 0 & 0 & -1 & \vdots \\ 0 & 0 & 0 & \cdot \end{array} \right) \quad \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 3 & 3 \\ 0 & 0 & 1 & 5 \end{array} \right) \quad \begin{matrix} \text{(sono le colonne)} \\ \text{non pivot} \end{matrix}$$

ho 3 incognite
ma 1 è "libera"
(2 sono vincolate)

grado 3:

$$\left(\begin{array}{cccc|c} 1 & * & * & * & * & b \\ 0 & 1 & * & * & * & \vdots \\ 0 & 0 & 1 & * & * & \end{array} \right)$$

$\underbrace{\quad}_{3}$

infatti (esempi di prima)

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & -2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -1 \end{array} \right) \quad s = n - \text{rg}(A)$$

$\underbrace{\quad}_{(0)}$

$$s = 3 - 3$$

(visivamente vedo
subito 0
colonne "libere")

quindi $\text{Sol}(A|0) = \text{Span}_K \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \right\}$

la sol è unica:

$$\left\{ \begin{pmatrix} -z \\ z \\ 1 \end{pmatrix} + \text{Sol}(A|0) \right\} = \left\{ \begin{pmatrix} -z \\ z \\ 1 \end{pmatrix} \right\}$$

$\underbrace{\quad}_{(0)}$

$$\left(\begin{array}{ccc|c} 1 & 1 & -2-z & \\ 0 & 1 & 2+z & \\ 0 & 0 & 3+3z & \end{array} \right)$$

se qui c'è 0 va bene perché non ci sono altri pivot

e $\text{rg}(A) = \text{rg}(A|b)$

(quindi se $z = -1$, è compatibile)

se invece $z \neq -1$,

$\text{rg}(A) = 2 < 3 = \text{rg}(A|b)$ e il sistema
è incompatibile

esercizio

studiare le soluzioni del seguente sistema lineare

$$\left\{ \begin{array}{l} x_2 - 2x_3 + x_4 - x_5 = 6 \\ x_3 - x_4 = -2 \\ x_1 - x_2 - x_3 - x_4 = 5 \\ x_2 + x_5 = 0 \end{array} \right.$$

$$\left(\begin{array}{ccccc|c} 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array} \right) \xrightarrow{\substack{R_1 \leftrightarrow R_3 \\ R_4 \leftrightarrow R_3}} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array} \right)$$

$$\xrightarrow{\substack{R_2 \leftarrow R_3 \\ R_3 \leftarrow R_4}} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & -2 \end{array} \right) \xrightarrow{R_3 \leftarrow R_3 - R_2} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 2 & -1 & 2 & -6 \\ 0 & 0 & 1 & -1 & 0 & -2 \end{array} \right) \xrightarrow{\substack{R_4 \leftarrow R_4 - R_3}} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 2 & -1 & 2 & -6 \\ 0 & 0 & 1 & -1 & 0 & -2 \end{array} \right)$$

$$R_2 = R_3 \text{ di prima}$$

$$R_3 = R_4 \text{ " "}$$

$$R_4 = R_2 \text{ " "}$$

$$\xrightarrow{\substack{R_3 \leftarrow R_4}} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 0 & 0 & 2 & -1 & 2 & -6 \end{array} \right) \xrightarrow{R_4 \rightarrow R_4 - 2R_3} \left(\begin{array}{ccccc|c} 1 & -1 & -1 & -1 & 0 & 5 \\ 0 & 1 & -2 & 1 & -1 & 6 \\ 0 & 0 & 1 & -1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 2 & -2 \end{array} \right)$$

4 pivot

qui si vede che $\text{rg}(A) = \text{rg}(A|b) = 4$

quindi, per Rouché-Capelli, il sistema d'origine è compatibile

dopo qualche calcolo →

$$\left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 5 & -1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & -4 \\ 0 & 0 & 0 & 1 & 2 & -2 \end{array} \right) \text{ è gradini ridotti}$$

Vett p.80
 Abbiamo visto che $\text{Span}_K(V_1, \dots, V_k) = \{ \alpha_1 V_1 + \dots + \alpha_k V_k : \alpha_1, \dots, \alpha_k \in K \}$
 Più generalmente, se $\emptyset \neq S \subset V$ qualsiasi, si pone $\text{Span}_K(S) = \{ \text{"combinazioni lineari finite di vettori in } S \}$, ovvero $\text{Span}_K(S) = \bigcap_{\substack{W \text{ sottosp. di } V \\ S \subset W}} W$

- **FATTO:** $\text{Span}_K(S)$ è un sottospazio vettoriale di V .

es. $W \subset V$ sottospazio. Allora, $W = \text{Span}_K(W)$

def SISTEMA DI GENERATORI, SOTTOSPazio FINITAMENTE GENERATO

- Se $W = \text{Span}_K(S)$, allora S è un sistema di generatori per W .
- Se $\exists S$ finito con $W = \text{Span}_K(S)$, 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. $V = \mathbb{R}^2$, $K = \mathbb{R}$, $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in V$, $S = \{v\}$

$$W = \text{Span}_{\mathbb{R}}(S) = \text{Span}_{\mathbb{R}}(v) \quad W \text{ è f.g.}$$

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 $W = \text{Span}_K(S)$
- ② S è libero

"su K "

Proposizione 1: Per ogni spazio vettoriale V/K , esiste una base $B \subset V$.

Inoltre, date due basi (B, B') di V , allora esiste una funzione biiettiva $f: B \rightarrow B'$

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 (B) di V ha cardinalità n .

N.B. $\dim_K(K) = 0 \iff V \text{ è banale} - V = \{0\}$

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 \subseteq)

Applicazione alla notazione di rango di una matrice

Lemme Dato una matrice $A \in M_{m,n}(K)$, $\text{rg}(A) = \dim_K(\underbrace{\text{Span}_K(A_1, \dots, A_m)}_{\# \text{pivot}})$

sottosp. vett. di $M_{1,n}(K)$

(ogni riga è una matrice riga con n colonne)

$\text{Span}_K(A_1, \dots, A_m)$ è l'insieme delle comb. lin. delle righe di A ,

una base di $\text{Span}_K(\dots)$ è un insieme di vettori l.i. che generano $\text{Span}_K(\dots)$,

quindi la dim della span (cardinalità delle basi) è il numero massimo di righe l.i. \rightarrow ovvero il rango (se trasformo una matrice in forma a gradini ridotti, le righe l.i. diventeranno nulle)

dim

Sia A' la matrice a gradini ridotti tale che $A \leq A'$. Allora, ogni riga di A' è combinazione lineare delle righe di A .

Quindi,

$$\text{Span}_K(A'_1, \dots, A'_m) \subset \text{Span}_K(A_1, \dots, A_m)$$

ogni el. appartiene

per la prop. 2, $\dim_K(\text{Span}_K(A'_1, \dots, A'_m)) \leq \dim_K(\text{Span}_K(A_1, \dots, A_m))$

Ma ogni trasformazione elementare di Gauss è invertibile (\cup è una rel. di equivalenze)

Quindi, $\dim_K(\text{Span}_K(A'_1, \dots, A'_m)) = \dim_K(\text{Span}_K(A_1, \dots, A_m))$.

Si vede che $\dim_K(\text{Span}_K(A'_1, \dots, A'_m)) = \text{rg}(A')$ perché le righe contenenti i pivot sono l.i. (lo sp. vett. le ha come base) ■

Applicazioni alle soluzioni di un sistema lineare (ROUCHÉ-CAPPELLI)

Dato un sistema lineare (*) $AX = b$, $M := (A|b)$, $A \in M_{m,n}(K)$,

il teorema di Rouché-Capelli p.95 Si riformula.

① (*) è compatibile $\iff \dim_K(M^1, \dots, M^{n+1}) = \dim_K(A^1, \dots, A^n)$ ($\text{rg}(A) = \text{rg}(A|b)$)

② $\dim_K(\underbrace{\text{Sol}(A|b)}_{\substack{\text{spazio vett.} \\ \text{delle sol. del} \\ \text{sistema omogeneo}}}) = \underbrace{n - \text{rg}(A)}_S$ (da teorema: esistono S vettori $v_1, \dots, v_S \in \text{Sol}(A|b)$ l.i.
t.c. $\text{Sol}(A|b) = \text{Span}_K(v_1, \dots, v_S)$)
quindi $S = \dim$ base \uparrow)

③ N.B. $\text{rg}(A) = \dim_K(\text{Span}_K(A_1, \dots, A_m)) = \dim_K(\text{Span}_K(A^1, \dots, A^n))$

Esercizi

*f sulle slide, ma preferisco x
f 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 ② Mostrire che $K_d[X]$ è f.g. e ③ calcolarne una base.

f.g.

② dato $P \in K_d[X] =: W$, $P = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \dots + \alpha_n X^n$ con $\alpha_0, \dots, \alpha_n \in K$ e, se $\alpha_n \neq 0$ allora $n \leq d$

è una comb. lineare di

quindi, $P \in \text{Span}_K(1, X, X^2, \dots, X^d)$ - 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

③ 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'unico comb. lineare nullo di $1, X, X^2, \dots, X^d$ è quello banale.

$\Rightarrow \{1, X, X^2, \dots, X^d\}$ è una base $\Rightarrow \dim_K(K_d[X]) = d+1$

• 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:

$$P = \alpha_0 + \alpha_1 X = \alpha_0 + \alpha_1 (X+1) - \alpha_1 = \underbrace{(\alpha_0 - \alpha_1)}_{\in \text{comb. di } 1} \cdot 1 + \alpha_1 (X+1) \quad \text{comb. lineare di } 1, X+1$$

$\Rightarrow \forall P \in K_1[X]$, si ha che $P \in \text{Span}_K(1, X+1) \Rightarrow K_1[X] \subset \text{Span}_K(1, X+1)$

Sia adesso $Q \in \text{Span}_K(1, X+1) \Rightarrow Q = b_0 + b_1 (X+1) = \underbrace{b_0 + b_1}_{\in \text{comb. di } (1, X)} + b_1 X \in K_1[X]$

comb. di $(1, X)$

$$\Rightarrow K_1[X] = \text{Span}_K(1, X+1) = \text{Span}_K(1, X)$$

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 $K[x]$ un sistema di generatori che non è una base]

per esempio, $\{1, 1, x, x^2, x^3\}$ è un sistema di generatori ($\forall P = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3, P \in \text{Span}_K(\{1, x, x^2, x^3\}) \subset \text{Span}_K(\{1, 1, x, x^2, x^3\})$)
in generale, se $S \subseteq S'$, $\text{Span}_K(S) \subseteq \text{Span}_K(S')$

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.

$$\downarrow 1 \cdot 1 - 1 \cdot 1 + 0 \cdot 0 + 0 \cdot 0 = 0$$

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

$V = \text{Span}_K(P_0, P_1, \dots, P_n)$, $P_i \in V = K[x]$. (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 $P = \sum_{i=0}^n \lambda_i P_i$

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

$Q \in \text{Span}_K(P_0, \dots, P_n)$ \downarrow 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 $B = \{b_1, \dots, b_n\}$ è base di V , allora un sottoinsieme $B' \subset V$ ottenuto attraverso ①, ②, ③ è un'altra base.

- Se $S \subseteq S'$, $\text{Span}_K(S) \subseteq \text{Span}_K(S')$

- $V = K[x]$ non è f.g.

ma fatto 1' 11/12 (matrice con rango non massimale) ($< \min(n, m)$)

Esercizio 1

$$M = \begin{pmatrix} -2 & 1 & 4 & -3 & -2 \\ 3 & -1 & -1 & 3 & 1 \\ 1 & 0 & 3 & 0 & -1 \\ 4 & 5 & 5 & -6 & 0 \end{pmatrix} \quad \text{U} \quad \begin{pmatrix} -2 & 1 & 4 & -3 & -2 \\ 3 & -1 & -1 & 3 & 1 \\ 1 & 0 & 3 & 0 & -1 \\ 0 & 7 & 13 & -12 & -4 \end{pmatrix} \quad \text{U} \quad \begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & -1 & -10 & 3 & 4 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 7 & 13 & -12 & -4 \end{pmatrix}$$

$R_4 \rightarrow R_4 + 2R_1$

$R_2 \rightarrow R_2 - 3R_3$

$R_1 \leftrightarrow R_3$

\cap

$R_2 \rightarrow R_2 + R_3$

$R_4 \rightarrow R_4 - 7R_3$

$$\begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 0 & -57 & * & * \end{pmatrix} \quad \text{U} \quad \begin{pmatrix} 1 & 0 & 3 & 0 & -1 \\ 0 & 1 & 10 & -3 & -4 \\ 0 & 0 & -57 & * & * \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$R_3 \rightarrow R_2 \rightarrow R_4 \rightarrow R_3$

quindi $\text{range}(M) = 3$
 = dimensione di $W = \text{Span}_{\mathbb{R}}(\text{righe di } M)$
 e le righe dello matrice (l.i.) costituiscono
 una base di W

Come è stato generato l'esercizio?

scelti 3 vettori: l.i > caso

$$a = (1 \ 2 \ 4 \ -3 \ -1), \quad b = (3 \ 1 \ 0 \ 0 \ 1), \quad c = (0 \ 2 \ 1 \ -3 \ 0) \in M_{1,5}(\mathbb{R})$$

la matrice $\begin{pmatrix} a \\ b \\ c \end{pmatrix} \in M_{3,5}(\mathbb{R})$ ha rango 3 e

$$M = \begin{pmatrix} a-b \\ b-c \\ a-c \\ a+b+c \end{pmatrix} \quad a-b, b-c, a-c, a+b+c \in \text{Span}_{\mathbb{R}}(a, b, c) \in M_{1,5}(\mathbb{R})$$

Esercizio 2

① In funzione del parametro $\lambda \in \mathbb{R}$, determinare il rango della matrice

$$M_\lambda = \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 2 & 1 & 1 & -2 & \lambda & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \in M_{4,7}(\mathbb{R})$$

② Supponiamo che M_λ sia la matrice completa associata ad un sistema lineare $Ax \underset{(*)}{=} b$.

Determinare in funzione di λ se il sistema è compatibile, e la dimensione di $\text{Sol}(A|b)$

$$M_\lambda = \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 2 & 1 & 1 & -2 & \lambda & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{\text{U}} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{\text{U}} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix}$$

$R_2 \rightarrow R_2 - 2R_4$ $R_4 \leftrightarrow R_2$

dobbiamo capire come
trattarlo: è già $\textcircled{0}$ o deve diventarlo?

ci sono ora due casi: ① $\lambda \neq 0$ ② $\lambda = 0$

① $\lambda \neq 0$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & \lambda & 4 & 3 & -2\lambda & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix} \xrightarrow{\text{U}}$$

$R_3 \rightarrow \lambda^{-1}R_3$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 1 & \frac{4}{\lambda} & \frac{3}{\lambda} & -2 & \frac{6}{\lambda} & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix} \xrightarrow{\text{U}}$$

$R_3 \rightarrow R_3 - R_2$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & \frac{4}{\lambda}-2 & \frac{3}{\lambda}+1 & -2 & \frac{6}{\lambda}-1 & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{pmatrix}$$

se $\lambda = 2$, è $\textcircled{0}$, altrimenti no

dobbiamo ancora due casi:

①a) $\lambda \neq 2, 0$

①b) $\lambda = 0$

② $\lambda = 0$

$$M_0 \xrightarrow{\text{U}} \begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 3 & 0 & 6 & 4 \\ 0 & 0 & -3 & 3 & -2 & -2 & 4 \end{pmatrix} \xrightarrow{\text{U}}$$

$\lambda = 0$
sostituiamo

$R_4 \rightarrow -\frac{1}{3}R_4$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 4 & 3 & 0 & 6 & 4 \\ 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} & -\frac{4}{3} \end{pmatrix} \xrightarrow{\text{U}}$$

$R_3 \rightarrow R_3 - 4R_4$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 7 & * & * & * \\ 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} & -\frac{4}{3} \end{pmatrix} \xrightarrow{\text{U}}$$

$R_3 \rightarrow \frac{1}{7}R_3$
 $R_3 \leftrightarrow R_4$

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

rango 4

①b) $\lambda \neq 0, \lambda \neq 2$

$$\left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & \frac{4}{\lambda}-2 & \frac{3}{\lambda}-1 & -2 & \frac{6}{\lambda}-1 & \frac{4}{\lambda} \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{array} \right) \xrightarrow{\text{U}} R_3 \rightarrow R_3 \cdot \frac{1}{\frac{4}{\lambda}-2}$$

①b) $\lambda = 2$

$$M_2 \xrightarrow{\text{U}} \left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{5}{2} & -2 & * & * \\ 0 & 0 & -3 & * & * & * & * \end{array} \right) \xrightarrow{\text{U}} R_3 \rightarrow \frac{2}{5} R_3 \\ R_4 \rightarrow -\frac{1}{3} R_4 \\ R_3 \leftrightarrow R_4$$

$$\left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3+\lambda}{4-2\lambda} & \frac{-2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & -3 & 3 & -2 & \lambda-2 & 4 \end{array} \right) \xrightarrow{\text{U}} R_4 \rightarrow R_4 + 3R_3$$

$$\left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & * & * & * & * \\ 0 & 0 & 0 & 1 & * & * & * \end{array} \right)$$

$$\left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3+\lambda}{4-2\lambda} & \frac{-2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & 0 & \frac{21-3\lambda}{4-2\lambda} & \frac{-4-\lambda}{2-\lambda} & * & * \end{array} \right)$$

se questi due si annullano contemporaneamente (e anche gli *) allora il rango è 3 - scanno, è 4

$$\frac{21-3\lambda}{4-2\lambda} \text{ si annulla} \Leftrightarrow \lambda = 7, \text{ e } \frac{-4-\lambda}{2-\lambda} \text{ non si annulla per } \lambda = 7$$

quindi non possono essere cont. nulli $\Rightarrow \text{rango}(M_\lambda) = 4$

in ogni caso, $\text{rango}(M_\lambda) = 4$

② In ogni caso $\text{rg}(M) \geq 4$. Scriviamo

$$M_\lambda = \left(\begin{array}{c|c} A_\lambda & B_\lambda \end{array} \right) \left. \right\} 4 \quad \text{il sistema (*) è compatibile} \Leftrightarrow \text{rg}(A) = \text{rg}(M)$$

devo verificare per ogni caso che i gradini "finiscono" prima di B

①b) può essere o così:

$$\left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3+\lambda}{4-2\lambda} & \frac{-2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & 0 & \frac{21-3\lambda}{4-2\lambda} & \frac{-4-\lambda}{2-\lambda} & * & * \end{array} \right) \text{ se } \lambda = 7$$

$$\left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & * & * & * & * \\ 0 & 0 & 0 & 1 & * & * & * \end{array} \right)$$

$$\text{o così: } \left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3+\lambda}{4-2\lambda} & \frac{-2\lambda}{4-2\lambda} & * & * \\ 0 & 0 & 0 & \frac{21-3\lambda}{4-2\lambda} & \frac{-4-\lambda}{2-\lambda} & * & * \end{array} \right) \text{ se } \lambda = 7$$

$$\left(\begin{array}{cccccc} 1 & 2 & -1 & 3 & 2 & 0 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & \frac{2}{3} & \frac{2}{3} & -\frac{4}{3} \\ 0 & 0 & 0 & 1 & * & * & * \end{array} \right)$$

$\text{rg}(A) = \text{rg}(M)$ si verifica in tutti i casi

• Per Rouché-Capelli, $\dim(\text{Sol}(A|0)) = \frac{\text{M}_\lambda}{\text{rg}(A)} = n - \text{rg}(A) = 6 - 4 = 2$
indeterminate

Si verifica che **prop 1, prop 2** \Rightarrow

\hookrightarrow per ogni $V/K \exists$ base $(B \subset V)$
(e se una base è finita di card. n ,
ogni base lo è.)

versione alternativa a p.

Proposizione 3: Dato V sp.vett. di dim. n su K , sia $S \subset V$.

Allora:

① S è libero $\Rightarrow \#S < \infty$ e $\#S \leq n$ se le basi hanno card. n , non può avere card. $k > n$

② S generatore \Rightarrow o S è infinito
oppure $\#S \geq n$

③ in particolare, S base $\Leftrightarrow S$ finito, $\#S = n$ e S libero $\Leftrightarrow \#S < \infty$, $\#S = n$ e S è generatore

Proposizione 4: Dato V spazio vettoriale f.g. su K ,

$\{v_1, \dots, v_n\}$ è una base di $V \Leftrightarrow$ ogni vettore di V si scrive in modo unico come combinazione lineare di v_1, \dots, v_n

dim

• \Rightarrow Se $\{v_1, \dots, v_n\}$ è base di V , allora è anche insieme di generatori. $\hookrightarrow \forall v \in V, \exists \alpha_i \in K$ t.c. $v = \sum \alpha_i v_i$

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: $0 = (\beta_1 - \alpha_1) v_1 + \dots + (\beta_n - \alpha_n) v_n$

L'unica comb. nulla è quella banale

Ma v_1, \dots, v_n sono l.i. $\Leftrightarrow \beta_1 = \alpha_1, \dots, \beta_n = \alpha_n$ da cui l'unicità

• \Leftarrow 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 : $V = \text{Span}_K(v_1, \dots, v_n)$

Inoltre, per unicità $0 = \alpha_1 v_1 + \dots + \alpha_n v_n$

$$0 = \underbrace{\alpha_1}_{||} v_1 + \dots + \underbrace{\alpha_n}_{||} v_n \implies v_1, \dots, v_n \text{ l.i.} \blacksquare$$

def VETTORE DELLE COORDINATE

Dato V spazio vettoriale su K di dim. n , e dato una base $B = \{b_1, \dots, b_n\}$, ogni vettore $v \in V$ si scrive in modo unico:

$$v = v_1 b_1 + \dots + v_n b_n \quad \text{con} \quad \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n$$

Tale vettore si chiama il vettore delle coordinate di v nella base B , e si scrive $[v]_B$

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 $\{(10)(01)(00)(00)\}$ dim: . chiaro che A, B, C, D sono l.i.

$\cdot \forall M \in M_2, M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a(10) + b(01) + c(00) + d(00)$

$\dim_{\mathbb{R}}(M_2(\mathbb{C})) = 8$ con base $\{(10)(01)(00)(00), (00)(00)(10)(01), (00)(00)(01)(00)\}$ dim: sempre chiaro l.i. $\delta_j = x_j \cdot 1 + y_j \cdot i$: quindi: $\cdot \forall M \in M_2, M = \begin{pmatrix} \delta_1 \delta_2 \\ \delta_3 \delta_4 \end{pmatrix} = x_1(10) + y_1(01) + \dots -$ uguali per $\delta_2, \delta_3, \delta_4$

Esercizio 3 / base canonica

dato $V = K^n$, allora $B = (e_1, \dots, e_n)$ è una base di V

dove $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_i = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}_{i\text{-esima posizione}}, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

dim

Scriviamo la matrice M che ha per righe i coefficienti dei vettori e_1, \dots, e_n .

Si ha $M = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \end{pmatrix} = 1_n \in M_n(K)$ \Rightarrow gradi: ridotto con n pivot. $\text{rg}(M) = n$ da cui B libera (range = cardinalità B) e, siccome $W = \text{Span}_K(B) \subset V$ ha dim. n , $W = V$ e B base di V $\Leftrightarrow \dim(K^n) = n$

def BASE CANONICA

La base $B = (e_1, \dots, e_n)$ si chiama la base canonica di K^n

$\cdot \{e_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ è la base canonica di $M_{m,n}(K)$

Esercizio 4

In $M_{m,n}(K)$, ponendo $e_{ij} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$ colonna j rispetto a $\epsilon M_{m,n}$ con $1 \leq i \leq m$ e $1 \leq j \leq n$

mostrare che $\{e_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ è la base canonica di $M_{m,n}(K)$ e che $\dim(M_{m,n}(K)) = m \cdot n$

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 .

c'è 2 metodi: (sappiamo che $2 = \#B = \dim_{\mathbb{R}}(V)$)

① usando la prop. 3 (S base $\iff \#S = n$ e S libero $\iff \#S = n$ e S è generatore) 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 $\begin{pmatrix} a \\ b \end{pmatrix} \in \text{Span}_{\mathbb{R}}(B)$)

$$x_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \quad \exists x_1, x_2 \in \mathbb{R} \iff \text{il sistema } \begin{cases} x_1 + x_2 = a \\ x_1 - x_2 = b \end{cases} \text{ è compatibile.}$$

Per Rouché-Capelli, il sistema è compatibile $\iff \text{rg}(A) = \text{rg}(A|b)$

$$\begin{pmatrix} 1 & 1 & a \\ 1 & -1 & b \end{pmatrix} \xrightarrow[L_2 \rightarrow L_2 - L_1]{\cup} \begin{pmatrix} 1 & 1 & a \\ 0 & -2 & b-a \end{pmatrix} \xrightarrow{\cup} \begin{pmatrix} 1 & 1 & a \\ 0 & 1 & \frac{a-b}{2} \end{pmatrix} \xrightarrow[L_1 \rightarrow L_1 - L_2]{\cup} \begin{pmatrix} 1 & 0 & \frac{a+b}{2} \\ 0 & 1 & \frac{a-b}{2} \end{pmatrix}$$

(ridotto)

$$\Rightarrow \text{rg}(A) = \text{rg}(A|b) \Rightarrow \mathbb{R}^2 = \text{Span}_{\mathbb{R}}(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix})$$

$$\text{Inoltre, ho le soluzioni uniche del sistema } \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{a+b}{2} \\ \frac{a-b}{2} \end{pmatrix}$$

$$\text{quindi, scrivendo } v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \text{ si ha } [v]_B = \begin{pmatrix} \frac{a+b}{2} \\ \frac{a-b}{2} \end{pmatrix}$$

vett. coordinate

② usando la prop. 3 (S base $\iff \#S = n$ e S libero $\iff \#S = n$ e S è generatore) usiamo questo

Mostriamo che B è libero (metodo più facile)

$(1 \ 1) \cup (1 \ 1) \cup (1 \ 1)$, che ha rango 2. Le righe contenenti i pivot sono l.i., quindi B è libero.

Quindi sappiamo che è una base di V .

Trasposizione di matrici

Sia $A \in M_{m,n}(K)$, lo trasposto di A (${}^t A$) è la matrice di $M_{n,m}(K)$ ottenuta da A scambiando righe e colonne.

$$A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}, \quad {}^t A = (a_{ji})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \in M_{3,2}(\mathbb{R}), \quad {}^t A = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix} \in M_{3,2}(\mathbb{R})$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in M_3(\mathbb{R}), \quad {}^t A = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

↪ è una riflessione rispetto alla diagonale

(per le non-quadrati: 

oss (importante!) dato $A \in M_{m,n}(K)$ $\text{rg}(A) = \text{rg}({}^t A)$

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 lo riduco -)

proprietà:

- ① ${}^t({}^t A) = A$
- ② ${}^t(\alpha A + \beta B) = \alpha {}^t A + \beta {}^t B$ con $\alpha, \beta \in K$ e $A, B \in M_{m,n}(K)$
- ③ ${}^t(AB) = {}^t B {}^t A$ (un po' come l'inversione nei gruppi)

↪ ricordiamo le condizioni di compatibilità per il prodotto matriciale

$A \in M_{m,n}(K), B \in M_{n,s}(K)$ - è ben definito anche per ${}^t B \in M_{s,n}(K), {}^t A \in M_{n,m}(K)$

Inoltre, ${}^t(AB) \in M_{s,m}(K)$.

def MATRICE SIMMETRICA/ASIMMETRICA

$A \in M_n(K)$ (quindi quadrata) si dice simmetrica se $A = {}^t A$

antisimmetrica se $A = -{}^t A$

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 4 & 1 \\ 0 & 1 & 3 \end{pmatrix} \in M_3 \text{ è simmetrica}, \quad A = \begin{pmatrix} 0 & 4 \\ -4 & 0 \end{pmatrix} \text{ è antisimmetrica}$$

- In $M_n(\mathbb{R})$, $A = -{}^t A \Rightarrow$ diagonale nulla

↪ falso in $M_n(\mathbb{F}_2)$

Lemmo / Esercizio 6 /

Sia $M_n^+(\mathbb{R})$ l'insieme delle matrici simmetriche di $M_n(\mathbb{R})$ e $M_n^-(\mathbb{R})$ l'insieme delle matrici antisimmetriche.

$M_n^+(\mathbb{R})$ e $M_n^-(\mathbb{R})$ sono sottospazi vettoriali di $M_n(\mathbb{R})$

dim

Poniamo $M = M_n^+(\mathbb{R})$ (e poi $M = M_n^-(\mathbb{R})$)

Dobbiamo dimostrare che $\forall A, B \in M$ e $\alpha, \beta \in \mathbb{R}$,

$$\alpha A + \beta B \in M$$

per M^+ A, B sono simmetriche : $A = {}^t A$, $B = {}^t B$

$$\text{quindi } {}^t(\alpha A + \beta B) = \alpha {}^t A + \beta {}^t B = \alpha A + \beta B$$

per M^- $A = {}^t -A$, $B = {}^t -B$

$$\text{quindi } {}^t(\alpha A + \beta B) = \alpha (-A) + \beta (-B) = -(\alpha A + \beta B)$$

Esercizio 7

Trovare basi per $M_2^+(\mathbb{R})$ e $M_2^-(\mathbb{R})$

① $M_2^+(\mathbb{R})$

Sia $A \in M_2^+(\mathbb{R})$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbb{R})$ generica

$$V := M_2^+(\mathbb{R}) = \text{Span}_{\mathbb{R}} \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{e_{11}} + b \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{e_{22}} + c \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{e_{21} + e_{12}}$$

② $M_2^-(\mathbb{R})$

$A = {}^t -A$, $A = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} \in M_2^-(\mathbb{R})$ generica

$$V := M_2^-(\mathbb{R}) = \text{Span}_{\mathbb{R}} \left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right)$$

Proposizione 3 versione alternativa - parte ③

Data 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 minimo di generatori:

Se aggiungo un altro vettore, non è più libero

dim ② \implies ①Prendiamo $B = \{v_1, \dots, v_n\}$ libero massimaleSia $v \in V$. Allora $B' = \{v_1, \dots, v_n, v\}$ non è libero (perché B massimale)aggiungo v $\exists \lambda_1, \lambda_2, \dots, \lambda_n \in K$ non tutti nulli t.c. $\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n = 0$ e quindi $\lambda v = \lambda_1 v_1 + \dots + \lambda_n v_n$ (sarebbero $-\lambda_1, \dots, -\lambda_n$, ma è come scegliere un λ')Claim: λ non nulloAltrimenti, $\lambda = 0$ 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}

$$\begin{aligned} v &= \frac{\lambda_1}{\lambda} v_1 + \dots + \frac{\lambda_n}{\lambda} v_n = u_1 v_1 + \dots + u_n v_n \implies v \in \text{Span}_K(B) \quad \forall v \in V \\ &\implies V \subseteq \text{Span}_K(B) \subset V \implies V = \text{Span}_K(B) \\ &\implies B \text{ è un sistema di generatori per } V \end{aligned}$$

Teorema (concetto già visto prima)

Data 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, $\text{Span}_K(B) = \text{Span}_K(B') = V$ quindi $\text{Span}_K(B) \supseteq \text{Span}_K(B')$ quindi posso scrivere, in modo unico, $\forall 1 \leq i \leq r \quad b'_i = \sum_{j=1}^r \underbrace{u_{ij}}_{\in K} b_j$ 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 $M_{r'}(K)$

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}_{r' \times r'}$$

$$M \in M_{r \times r+r'}$$

$$M = \left(\begin{array}{c|cc} (u_{ij})_{1 \leq i \leq r, 1 \leq j \leq r} & & \\ \hline & 1_{r'} & \\ & \vdots & \\ & 1_{r'} & \end{array} \right)_{r \times r+r'}$$

Applichiamo ora le operazioni elementari di Gauss per rendere solo la parte sinistra a gradini ridotti

Che può essere un rettangolo così $\boxed{}_{r'}^{r}$ (se $r < r'$) o al massimo un quadrato $(r = r')$ (non può essere così $\boxed{}_r^{r'} \rightarrow r' > r'$)

Riducendo M otteniamo una cosa del genere

$$\left(\begin{array}{cccc|c} 1 & & & & * \\ 1 & 1 & & & \\ 1 & & 1 & & \\ 1 & & & 1 & \\ 1 & & & & 1 \\ 0 & & & & 0 \end{array} \right)$$

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, stremmo dicendo che un blocco di vettori che contiene zeri è una base \rightarrow CONTRADDIZIONE

Una base non contiene mai 0 (altrimenti non sarebbe libera)

$$\begin{aligned} & \hookrightarrow b'_x = 0 \cdot b_1 + 0 \cdot b_2 + \dots = 0 \\ & (\forall x \in K) x \cdot 0 + 0 \cdot v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n \text{ non è nulla ma dovrebbe } 0 \\ & (\text{tutti zeri è un numero qualunque al vettore } 0) \end{aligned}$$

perché non ci siano righe nulle, la parte di sx deve essere quadrata

$$\text{quindi, } r = r' \blacksquare$$

(MATRICE INVERSA)

Analizziamo la situazione con $r = r'$

• matrice iniziale:

$$r \left\{ \left(\begin{array}{c|cc} A & 1_r \\ \hline r & n \end{array} \right) \right.$$

ogni riga dà le coordinate di b_i nella base B'
(nella base B' , b_i ha coord. $1 \ 0 \dots 0$, $b'_1 = 1 \cdot b'_1 + 0 \cdot b'_2 + 0 \cdot b'_3 + \dots$)
 $b'_2 = 0 \cdot b'_1 + 1 \cdot b'_2 + 0 \cdot b'_3 \dots$ ecc.
(sia C una base di V , $C = \{v_1, \dots, v_n\}$)
 $[v_i]_C = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e_i$ perché $v_i = 0 \cdot v_1 + 0 \cdot v_2 + \dots + 1 \cdot v_i + \dots + 0 \cdot v_n$)

sempre coord. vettori di B' nella base B

Alla fine dell'algoritmo (rendendo la parte di sx a gradini ridotti) si ottiene:

$$\left(\begin{array}{c|cc} 1_r & A' \\ \hline \end{array} \right)$$

matrice quadrata
a gradini ridotti
diventa 1_r

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' .

\hookrightarrow il contrario di prima

(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 ridotti)
• la matrice giustapposta è l'inversa)

esercizio

$$U = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 2 & 1 \\ 1 & 0 & -1 \end{pmatrix} \text{ calcolare l'inverso (se esiste)}$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 \end{array} \right) \quad U \quad \cap \quad R_2 \rightarrow R_2 - 3R_1 \quad R_3 \rightarrow R_3 - R_1$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -4 & -2 & -3 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 \end{array} \right) \quad U \quad \cap \quad R_3 \rightarrow -\frac{1}{2}R_3$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -4 & -2 & -3 & 1 & 0 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \end{array} \right) \quad U \quad \cap \quad R_2 \rightarrow R_2 + 4R_3$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & -1 & 1 & -2 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \end{array} \right) \quad U \quad \cap \quad R_2 \leftrightarrow R_3 \quad R_3 \rightarrow \frac{1}{2}R_3$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & \frac{1}{2} & 1 & -1 \end{array} \right)$$

$$\begin{array}{l} U \\ \cap \\ R_1 \rightarrow R_1 - R_3 \\ R_2 \rightarrow R_2 - R_3 \end{array} \quad \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & \frac{1}{2} & -\frac{1}{2} & 1 \\ 0 & 1 & 0 & -\frac{1}{2} & \frac{1}{2} & -1 \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array} \right) \quad \begin{array}{l} U \\ \cap \\ R_1 \rightarrow R_1 - 2R_2 \end{array} \quad \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 1 & 0 & 1 & -\frac{1}{2} & -1 \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array} \right) \quad \text{l'inverso di } U$$

Dalla discussione appena conclusa, traspare:

Teorema:

Dato $A \in M_n(K)$, c'è equivalenza tra:

① $A \in GL_n(K)$ (A invertibile)

② $\text{range}(A) = K^n$

③ le righe di A sono una base di K^n

④ le colonne di A sono una base di K^n

OSS: dato una matrice M invertibile, anche la sua trasposta ${}^t M$ è invertibile (di inversa ${}^t(M^{-1})$)

OSS: esiste una nozione di determinante

$$\det: M_n(K) \rightarrow K \quad \text{per ora descritta solo per } n=2$$

• si dimostra ⑤ $A \in M_n(K)$ è invertibile $\Leftrightarrow \det(A) \in K^\times$

(c'è una formula universale - dato $A = (a_{ij})_{1 \leq i,j \leq n} \in M_n(K)$

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \alpha_{1\sigma(1)} \dots \alpha_{n\sigma(n)})$$

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 $\forall \alpha, \alpha' \in K$,

$$\text{si ha } f(\alpha v + \alpha' v') = \alpha f(v) + \alpha' f(v')$$

prodotto scalare di v
in V
addiz.

(come un **omomorfismo**)

prodotto scalare di v'
in V'

(un'applicazione lineare di spazi vettoriali è

un'omomorfismo di gruppi)

• Se inoltre f è biiettiva, si dice **isomorfismo**

(e se f è un isomorfismo, anche f^{-1} è un isomorfismo)

gli spazi vettoriali sono gruppi

abeliani con op. di somma vettoriale

Proposizione

Dati V/K f.g., $B = \{b_1, \dots, b_n\}$ base di V , V' s.v. qualsiasi /K, e $f: B \rightarrow V'$

Allora $\exists!$ applicazione lineare $\tilde{f}: V \rightarrow V'$ t.c. $\tilde{f}|_B = f$

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 (per unicità di \tilde{f} quindi il valore $f(v)$ dipende solo da v)
 $V \xrightarrow{\tilde{f}} V'$

① Mostriamo che \tilde{f} è lineare

$$\text{dati } v, v' \in V, \beta, \beta' \in K, \text{ calcolo } \tilde{f}(\beta v + \beta' v') = ? \quad \beta \tilde{f}(v) + \beta' \tilde{f}(v')$$

• Calcoliamo $[v]_B = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, [v']_B = \begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix}$

$$v = \sum_{i=1}^n \alpha_i b_i, v' = \sum_{i=1}^n \alpha'_i b_i, \beta v + \beta' v' = \sum_{i=1}^n (\beta \alpha_i + \beta' \alpha'_i) b_i$$

$$\tilde{f}(\beta v + \beta' v') = \sum_{i=1}^n (\beta \alpha_i + \beta' \alpha'_i) f(b_i) =$$

$$\beta \tilde{f}(v) + \beta' \tilde{f}(v') = \beta \sum_{i=1}^n \alpha_i \tilde{f}(b_i) + \beta' \sum_{i=1}^n \alpha'_i \tilde{f}(b_i) = \sum_{i=1}^n (\beta \alpha_i + \beta' \alpha'_i) \tilde{f}(b_i) \quad \text{quindi } \tilde{f} \text{ lineare}$$

② Mostriamo l'unicità

Supponiamo che $\exists \hat{f}: V \rightarrow V'$ 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 $g = \tilde{f} - \hat{f}$.

$$g(v) = g\left(\sum_{i=0}^n \alpha_i b_i\right) = \sum_{i=0}^n \alpha_i g(b_i) = \sum_{i=0}^n \alpha_i (\underbrace{\tilde{f}(b_i) - \hat{f}(b_i)}_{=0}) = 0 \Rightarrow g \equiv 0 \Rightarrow \hat{f} = \tilde{f} \blacksquare$$

Esempio

Dato V/\mathbb{R} di base $B = (b_1 \dots b_n)$, $V' = \mathbb{R}^n$, $\dim(V) = \dim(V') = n$

• 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.

$$\tilde{f}(v) = \sum_i \alpha_i f(b_i) = \sum_i \alpha_i e_i = \begin{pmatrix} \alpha_1 \\ \vdots \\ v \\ \vdots \\ \alpha_n \end{pmatrix} = [v]_B$$

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 $f: B \rightarrow V$, allora scriviamo $f = \tilde{f}$

Corollario

Se $\dim_K(V) = n$, allora $f: V \rightarrow K^n$ è un isomorfismo

Immagine e nucleo (def)

Dato $f: V \rightarrow V'$ applicazione lineare, poniamo

$$\cdot \text{Ker}(f) = \{v \in V \text{ t.c. } f(v) = \emptyset\} = f^{-1}(\{\emptyset\}) \quad \text{nucleo}$$

$$\cdot \text{Im}(f) = \{v' \in V' : \exists v \in V \text{ t.c. } f(v) = v'\} \quad \text{immagine}$$

Lemma

$\text{Ker}(f)$ e $\text{Im}(f)$ 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 $\text{Ker}(f)$ e $\text{Im}(f)$ sono stabili per il prodotto scalare

$\text{Ker}(f)$:

• Siano $v \in V, \alpha \in K$: Sappiamo che $f(v) = \emptyset \Rightarrow \alpha f(v) = \alpha \emptyset = \emptyset$ (è stabile)

$v \in \text{Ker}(f) \Rightarrow \alpha v \in \text{Ker}(f) \Rightarrow \text{Ker}(f)$ è un sottosp. vett. (definizione 1 sottosp.vett.: $\text{Ker}(f) \subset V$ e $\lambda v \in \text{Ker}(f)$)

$\in K$

$\text{Im}(f)$:

• Siano $v \in V'$, $\alpha \in K$: $\exists v \in V \text{ t.c. } f(v) = v' \implies \alpha f(v) = \alpha v'$.

ma $\alpha f(v) = f(\alpha v) \implies$ il vettore $\alpha v \in V$ è tale che $f(\alpha v) = \alpha v' \implies \alpha v' \in \text{Im}(f) \implies \text{Im}(f)$ è un sottosp. vett. di V' .

OSS: Visto che un omomorfismo è iniettivo solo se il nucleo è banale, lemma p.60

$\text{Ker}(f) = \{\emptyset\} \iff f \text{ iniettiva}$

inoltre, $\text{Im}(f) = V' \iff f \text{ suriettiva}$

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 SOMMA DI SOTTOSP. VETT.

Dati V_1, V_2 sottospazi vettoriali di V .

Definiamo

$$V_1 + V_2 = \{v \in V : \exists v_1 \in V_1, v_2 \in V_2 \text{ t.c. } v = v_1 + v_2\}$$