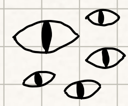
ALGEBRA

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

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

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



$\mathbb{Z} \xrightarrow{-(\ )} \mathbb{Z}$ opposto , $\mathbb{Z} \times \mathbb{Z} \xrightarrow[\cdot]{+} \mathbb{Z}$ somma e prodotto (binarie)

altro modo di esprimere l'addizione

ci sono diverse condizioni di compatibilità tra le operazioni:

$a(b+c) = ab + ac$, $a + b = b + a$, $a + (b+c) = (a+b) + c$

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

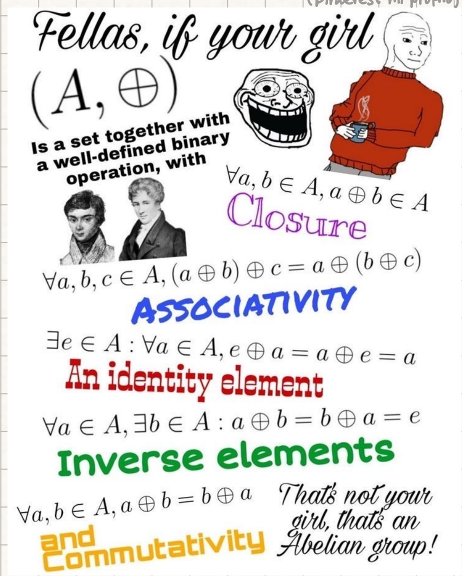
poi lo chiameremo solo A

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

dove:

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

(pinterest mi profila)



questi dati devono soddisfare 8 proprietà:

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

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

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

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 $\forall a, b, c \in A$, $a(b \cdot c) = (a \cdot b)c = abc$ ASSOCIATIVITÀ DEL PRODOTTO

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

rende l'anello "UNITARIO"

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

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

rende l'anello "COMMUTATIVO"

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

BUON ORDINAMENTO E ORDINE TOTALE

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

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

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

- Ogni sottoinsieme $E \subset \mathbb{N}^*$ non vuoto possiede un più piccolo elemento per

$<$ $\exists c \in E$ t.c. $\forall e \in E \setminus \{c\}$ si ha $e > c$ BUON ORDINAMENTO

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

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

legge di cancellazione in $\mathbb{Z}$

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

altrimenti basta molt. per -1 entrambe le parti

Infatti, supponendo $a > 0$

Induzione su $a \geq 1$

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

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

tricotomia

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

$a - b + b > a - c + c$

premessa $ab = ac$

$ab > ac$, 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 $b = a^{-1}$)

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

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

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

$\underbrace{a \cdot b = a \cdot b'}_{\text{devono essere }=} = 1$ con $b, b' \in A$

allora $(a \cdot b)\, b' = 1_A \cdot b' = b'$

quindi $\xrightarrow{③}$ uguali

2a uguali

$(a \cdot b')\, b = 1_A \cdot b = b$

2b uguali

$\underbrace{(a \cdot b)\, b' = a\,(b \cdot b') = a\,(b' \cdot b) = ab' \cdot b}_{① \text{ uguali}}$

si pone $A^\times = \{a \in A$ t.c. a 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 $\mathbb{Z}^\times = \{1, -1\}$

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

risposta: $\mathbb{Q}^\times = \{r \in \mathbb{Q} ; r \neq 0\}$ $\left[\frac{1}{1}\right] = [1_A]$

PICCOLI ESEMPI

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

$$a \cdot 0_A = a \cdot (\overbrace{0_A + (-0_A)}^{0_A \text{ (assioma)}}) = a \cdot 0_A + a \cdot (-0_A)$$

$$= a \cdot 0_A + (-a \cdot 0_A)$$

$$= \underbrace{a \cdot 0_A + (-(a \cdot 0_A))}_{= 0_A \text{ x assioma}}$$ elemento + il suo opposto quindi $a \cdot 0_A = 0_A$

② Supponiamo $0_A = 1_A$.
Mostriamo che $\forall a \in A,\ a = 0_A = 1_A$ $(A = \{0_A\})$

$a \in A : 1_A = 0_A \Longrightarrow \underbrace{a \cdot 1_A}_{= a} = \underbrace{a \cdot 0_A}_{0_A}$ quindi, $\forall a,\ a = 0_A$

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

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

gli assiomi implicano che 0_A non è mai invertibile si pone $A^\times = \{a \in A$ t.c. a 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 anello comm. un. (sestupla)
quindi, $1_A \in A \Rightarrow A \neq \emptyset$

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

visto 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 $b \notin A^\times$, $\nexists x \in A$ t.c. $bx = xb = 1_A$. ma questo è falso. esiste ed è a.
o $\forall x \in A$, $bx = xb \neq 1_A$ falso per a

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

$(ab^{-1}) = a^{-1} b^{-1} \iff a^{-1} b^{-1} \cdot ab = 1_A$ per definizione. (e, poiché unicamente determinato, se $a^{-1} b^{-1} \cdot ab = 1_A$ e $(a \cdot b)^{-1} \cdot ab = 1_A$ allora $(ab)^{-1} = a^{-1} b^{-1}$)

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

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

$a^{-1} \cdot b^{-1} \cdot a \cdot b$ commutatività e associatività $\underbrace{(a \cdot a^{-1})}_{1_A} \cdot \underbrace{(b \cdot b^{-1})}_{1_A} = 1_A$

$1_A \cdot 1_A = 1_A$ vero perché 1_A el. neutro della molt.
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 $-(1^{-1}) = -(1)$ moltiplico 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 $\mathbb{Q}^\times = \{x \in \mathbb{Q} : x \text{ è invertibile}\}$

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

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

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

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

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

$qx = 1 \Longleftrightarrow x = \frac{1}{q}$ e $\frac{1}{q} \in \mathbb{Q}$. trovato x t.c. $qx = 1$ (+ vediamo nuovamente che $\times$ 0 non va) perché $\frac{1}{0}$ impossibile

(non sono sicura che questo basti, ngl)

esercizio: c'è un unico elemento neutro

Siano u, u' due elementi neutri per la moltiplicazione

$\forall a \in A$ $\quad au = ua = a \quad$ con $a = u \quad uu' = u'u = u \quad$ quindi $u = u'$
$\quad au' = u'a = a \quad$ con $a = u' \quad u'u = uu' = u'$

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

9 ottobre

Relazione di divisibilità

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

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

- è una relazione riflessiva: $\forall a \in A$, $a = a \cdot 1_A$
- è una relazione transitiva: $a, b, c \in A$ supponiamo $a \mid b \iff b = aa'$ $\exists a' \in A$
- non è simmetrica né antisimmetrica, ma su $\mathbb{N}^*$ è antisimmetrica

$b \mid c \iff c = bb'$ $\exists b' \in A$

a divide c

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

- se $a \mid b$ e $a \mid c$ allora $a \mid b+c$ (compatibilità)

$a \mid b \iff \exists a'$ t.c. $b = aa'$ $\quad a \mid c \iff \exists a'' \in A$ t.c. $c = aa''$

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

dim. $\alpha, \beta \in A$
$a \mid b, a \mid c \Longrightarrow a \mid \alpha b + \beta c$
- $a \mid b \Longrightarrow a \mid \alpha b$ per def. di moltiplicazione
- $a \mid c \Longrightarrow a \mid \beta c$

per la dim. di compatibilità, $a \mid \alpha b + \beta c$

più generalmente, se $\alpha, \beta \in A$, $a \mid b$, $a \mid c \Longrightarrow a \mid \alpha b + \beta c$ (la dimostrazione è banale)

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

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

ignoriamo il caso 0

$a, b \in \mathbb{Z}$ $\quad a \mid b$ e $b \mid a \Longrightarrow \exists c \in \mathbb{Z}^*$ t.c. $a = bc$ (ovvero $a \in \{b, -b\}$ o $\{a, -a\} = \{b, -b\}$)

$0 \mid 1 \Longrightarrow 1 = 0 \cdot b$ $\quad 0$ non divide mai un el. non nullo $\quad$ quindi possiamo supporre $a, b \neq 0$

$a \mid b$, $b \mid a \Longrightarrow b = aa'$, $a = bb'$ $\exists a, b \in \mathbb{Z}$

$b = ba'b'$ $\quad$ con $b \neq 0$, legge di cancellazione $\cancel{b} = \cancel{b} a'b' \Longrightarrow 1 = a'b' \Longrightarrow a'b' \in \{1, -1\}$

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

- non è simmetrica $\longrightarrow$ supponiamo $a \mid b$ simmetrica. Allora $a \mid b$ ($\exists c$ t.c. $b = a \cdot c$) $\Longrightarrow b \mid a$ ($\exists c'$ t.c. $a = b \cdot c'$)

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

oppure, con esempio: $2 \mid 4$ ma $4 \nmid 2$

- non è antisimmetrica: se fosse antisimmetrica, $a \mid b \wedge b \mid a \Longrightarrow a = b$

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

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

def **elemento irriducibile**

$a \in A \setminus A^{\times}$ (invertibili) è detto irriducibile se

$\forall b, c \in A,\ a = bc$ allora o $b \in A^{\times}$ o $c \in A^{\times}$

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

$7 = 1 \cdot 7 = 7 \cdot 1 = -1 \cdot -7 = -7 \cdot -1$ $\quad$ 7 è irriducibile

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

def **numero primo**

$a \in A \setminus A^{\times}$ (invertibili), $a \neq 0$ è detto primo se

$\forall b, c \in A$, se $a \mid bc$ allora $a \mid b$ oppure $a \mid c$

Supponiamo $A = \mathbb{Z}$

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

dim p primo, siano $a, b \in \mathbb{Z}$ t.c. $p = ab \Longrightarrow p \mid a \cdot b$ ($ab = p \cdot 1$) $\Rightarrow$ o $p \mid a$ o $p \mid b$

Supponiamo senza perdita di generalità $p \mid a$

$p \mid a \Longrightarrow a = pa' \ \exists a' \in \mathbb{Z} \Longrightarrow p = pa'b$ (sost. $a = pa'$) legge di cancellazione $\quad p = p(a'b) \Longleftrightarrow 1 = a'b \Longrightarrow a', b \in \{+1, -1\} = \mathbb{Z}^{\times}$

se $a' = 1$ allora $a = p \Longrightarrow p = pb \Longrightarrow b = 1$

se $a' = -1$ allora $a = -p \Longrightarrow p = p \cdot -b \Longrightarrow -b = 1 \Longrightarrow b = -1 \Longrightarrow p$ è irriducibile

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

---

def **Valore assoluto**

$\mathbb{Z} \xrightarrow[|\cdot|]{} \mathbb{N}$ $\quad a \in \mathbb{Z}$ $\quad$ • 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

$a, n \in \mathbb{Z}$ $\quad n \neq 0$ $\quad$ 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 a/n — $n \mid a-b$ vuol dire che b è il resto (n divide a − il resto)

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

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

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

- la congruenza modulo n è di equivalenza

① transitiva : $a \equiv b \bmod n$ e $b \equiv c \bmod n \iff n \mid b-a$ e $n \mid c-b$

$n \mid \alpha$: $n \mid \beta \implies n \mid \alpha+\beta$ $\quad n \mid c-b+b-a \implies n \mid c-a \iff a \equiv c \pmod{n}$

scrivi rifl. e simm.

$$\mathbb{Z}/\equiv_{\bmod n} = \{ \underbrace{n\mathbb{Z}}_{[0]}, \underbrace{n\mathbb{Z}+1}_{[1]}, \dots, \underbrace{n\mathbb{Z}+n-1}_{[n-1]\ [-1]} \}$$

② riflessiva : $a \equiv a \bmod n \quad n \mid a-a$ vero perché $\forall x \in \mathbb{Z}, x \neq 0, x \mid 0$

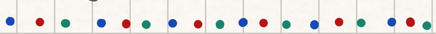
③ simmetrica : $a \equiv_n b \implies b \equiv_n a \quad n \mid a-b \implies n \mid b-a$

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

esempi: congruenza modulo 2

$$\mathbb{Z} = \underbrace{\overset{\text{pari}}{2\mathbb{Z}}}_{[0]} \sqcup \underbrace{\overset{\text{dispari}}{2\mathbb{Z}+1}}_{[1]} \qquad \mathbb{Z}/\equiv_{\bmod 2} = \{2\mathbb{Z}, 2\mathbb{Z}+1\}$$

congruenza mod. 3



$$\mathbb{Z}/\equiv_{\bmod 3} = \{ \underbrace{3\mathbb{Z}}_{[0]_3}, \underbrace{3\mathbb{Z}+1}_{[1]_3}, \underbrace{3\mathbb{Z}+2}_{[2]_3} \}$$

10 ottobre

$\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z}$ $n>0$ insieme quoziente di $\mathbb{Z}$ su congr. modulo n

$\equiv_n$: congruenza 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

$[2] = [5] = [-1]$

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

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

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

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

mod. n

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

dim ②

$2 \mid 5-1$ e $2 \mid 1-5$

$a \equiv_n a' \iff n \mid a-a'$ e $n \mid a'-a$

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

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

Devo ottenere $a+b \equiv_n a'+b'$

somma le due formule

$\implies a'+b' - (a+b) = n(k+k') \iff a'+b' \equiv_n a+b$

quindi $n \mid (a'+b') - a+b$

(perché $n \cdot$ qualcosa $=$ quello)

dim. ①

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

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

dim. ③

$\forall a, a', b, b' \in \mathbb{Z}$ $a \equiv_n a'$, $b \equiv_n b' \implies ab \equiv_n a'b'$ ovvero $ab - a'b' = kn$ o $ab = kn + a'b'$

$a = qn + a'$ e $b = q'n + b'$ quindi $a \cdot b = (a'+qn)(b'+q'n) = a'b' + n(\underbrace{qb' + a'q' + qq'n}_{k})$ $ab = a'b' + n(k)$

OPERATORI

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

$-[a] \overset{\text{definiamo}}{:=} [-a]$ questa funz. $\mathbb{Z}/_{n}\mathbb{Z} \longrightarrow \mathbb{Z}/_{n}\mathbb{Z}$ è ben definito: opposto in $\mathbb{Z}/_{n}\mathbb{Z}$

definiamo

- $[a] + [b] := [a+b]$ ben definito (ovvero indipendente dalla scelta di rapp. di $[a]$ e $[b]$

perché $[a] = [a']$ quindi $a \equiv_n a'$ e stessa cosa b

scegliamo $a' \in \underset{=[a']}{[a]}$ e $b' \in \underset{=[b']}{[b]}$ e calcoliamo $[a'+b'] = \{m : n \mid \underbrace{m - a' - b'}_{m-(a'+b')}\} \overset{\text{per } ②}{=} \{m : n \mid \underbrace{m - a - b}_{m-(a+b)}\}$

$\Longleftrightarrow$ $[a+b] = [a'+b']$ l'operazione + introdotta su $\mathbb{Z}/\mathbb{Z}_n$ è ben definita

esempi $[1]_3$ $[2]_3 \in \mathbb{Z}/_{3}\mathbb{Z}$ $[1] + [2] = [3] = [0]$

altri rapp. $[1] = [4]$ $[2] = [-4]$

quindi $[4 + -4] = [0]$

- definiamo inoltre $[a], [b] \in \mathbb{Z}/_{n}\mathbb{Z}$ $[a] \cdot [b] = [ab]$ ben definito

scegliamo $a' \in [a]$ e $b' \in [b]$, $[ab] = \{m : n \mid m - a'b'\}$ ma $a' \equiv_n a$ e $b' \equiv_n b$ – quindi, per ③ $= \{m : n \mid m - ab\}$

esempi $[1]_3$ $[2]_3 \in \mathbb{Z}/\mathbb{Z}_3$ $[1] \cdot [2] = [2]$

e $[4 \cdot -4] = [-16] = [2]$ – perché $\frac{2}{3} = 0$ resto 2 e $\frac{-16}{3} = -6$ resto 2

TEOREMA

$(\mathbb{Z}/\mathbb{Z}_n, \overbrace{+, -, \cdot}^{\text{definiti prima}}, [0], [1])$ è un ANELLO (comm. un.)

è grande la voglia di calcolare l'insieme degli elementi invertibili (ma lo faremo dopo)

alcuni sottoinsiemi di $\mathbb{Z}$

- $n\mathbb{Z} = \{m \in \mathbb{Z} \text{ t.c. } \exists\, k \in \mathbb{Z} \text{ con } m = kn\}$ multipli di n
- $\mathbb{Z} \setminus \{0\} = \mathbb{Z}^*$
- $a\mathbb{Z} + b\mathbb{Z} := \{m \in \mathbb{Z} : \exists\, k, k' \in \mathbb{Z} \text{ con } m = ka + k'b\}$ multipli di a + multipli di b

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

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

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

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

la divisibilità è una relazione di inclusione di sottoinsiemi

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

- supponiamo $a \mid b$

$\iff \exists\, k \in \mathbb{Z}$ t.c. $b = ka$ se $a|b$, allora ogni multiplo di b può essere riscritto come b·qualcosa. ma, per def di $|$, $b = a \cdot$ qualcosa. quindi, un multiplo di b è un multiplo di a

multiplo di b

sia $b' \in b\mathbb{Z} \iff \exists\, l$ t.c. $b' = lb$

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

dimostriamo $b\mathbb{Z} \subset a\mathbb{Z} \implies a \mid b$

- supponiamo $b\mathbb{Z} \subset a\mathbb{Z}$

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

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

lemma $\mathcal{E} = a\mathbb{Z} + b\mathbb{Z}$ con $a, b \neq 0$, allora $\exists!\ \delta \in \mathbb{N}^*$ t.c. $\mathcal{E} = \delta\mathbb{Z}$ — tutte le combinazioni sono multiple di un certo intero unico

dimostrazione

poniamo $\mathcal{E}^* := \underbrace{\mathcal{E} \cap \mathbb{N}^*}_{\text{el. di } \mathcal{E} > 0} \subset \mathbb{N}^*$

- osserviamo che $\mathcal{E}^* \neq \emptyset$

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

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

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

piccola parentesi esempio:

$$\mathcal{E} = \mathcal{E}^* \sqcup \{0\} \sqcup \{-\mathcal{E}\}$$

$$\forall x \in \mathcal{E},\ -x \in \mathcal{E}$$

perché

$$x = ka + k'b \quad e \quad -x = (-k)a + (-k)b$$

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

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

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

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

notiamo che $r = a - q\delta$

$a \in \mathcal{E}$, $\delta \in \mathcal{E}^* \subset \mathcal{E} \implies \delta = ua + vb$ con $u, v \in \mathbb{Z}$ (sempre per $\mathcal{E} = a\mathbb{Z} + b\mathbb{Z}$)

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

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

② altrimenti, $r > 0$ e $r \in \mathcal{E}^*$. se fosse vero, $r \geq \delta$ (per $\delta = \min(\mathcal{E}^*)$). ma questo è impossibile per $a = q\delta + r$ con $r = \{0, 1 \dots \delta - 1\}$ — r nec $< \delta$

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

- $\forall\ \alpha, \beta \in \mathbb{Z}$, $\delta \mid \underbrace{\alpha a + \beta b}_{=} \implies \mathcal{E} \subset \delta\mathbb{Z}$ per la dim sopra $(a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z})$

d'altronde, $\delta \in \mathcal{E} \iff \delta = ka + k'b$

$\forall l \in \mathbb{Z}$, $l\delta = lka + lk'b \implies l\delta \in \mathcal{E}$ — se i multipli di δ sono elementi di $\mathcal{E}$, allora $\delta\mathbb{Z}$ è contenuto in $\mathcal{E}$ (per def $\subset$) $\implies \delta\mathbb{Z} \subset \mathcal{E}$

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

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

notiamo che

- a (e b) si può riscrivere come $a = q\delta + r$. Questo implica che $r < \delta - 1$ (per questioni resto)
- e che $r \in \mathcal{E}$, 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 o > 0 o $= 0$. Ma se fosse > 0, dovrebbe essere anche $< \delta - 1$ per def resto e $\delta = \min$, il che è IMPOSSIBILE

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

ora: visto che $\delta \mid a$ e $\delta \mid b$, $\delta \mid a + b$ e $\delta \mid \alpha a + \beta b$ (δ divide i membri di $\mathcal{E}$ formato da $\alpha a + \beta b$). Questo implica $\delta\mathbb{Z} \supset \mathcal{E}$

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

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

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:

① $d \mid a$ e $d \mid b$

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

lemma:

se d soddisfa ① e ②, allora è unico.

dim.

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

$d_2 = k \cdot d_1$ e $d_1 = k \cdot d_2$ quindi d_1 e d_2 devono essere uguali o opposti

si ha $d_2 \mid d_1$ e $d_1 \mid d_2 \implies \{d_1, -d_1\} = \{d_2, -d_2\} \implies d_1 = d_2$

- Si scrive $d = MCD(a,b)$

def COPRIMI $\longrightarrow$ se $MCD(a,b) = 1$, si dice che a e b sono primi tra loro o coprimi

lemma

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

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

dim.

$\delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ $\quad$ ① $\supset a\mathbb{Z} \implies \delta \mid a$ $\quad$ condizione ①

$\supset b\mathbb{Z} \implies \delta \mid b$ $\quad$ verificata

② (mostro $d' \mid \delta \iff \delta\mathbb{Z} \subset d'\mathbb{Z}$)

ogni divisore di a e b divide il MCD

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

$d' \mid a \iff a\mathbb{Z} \subset d'\mathbb{Z}$ e $d' \mid b \iff b\mathbb{Z} \subset d'\mathbb{Z}$

quindi $\underbrace{a\mathbb{Z} + b\mathbb{Z}}_{\overset{!}{=} \delta\mathbb{Z}} \subset \overbrace{d'\mathbb{Z} + d'\mathbb{Z}}^{= d'\mathbb{Z}}$ $\quad \neq 2d'\mathbb{Z}$

$\delta\mathbb{Z} \subset d'\mathbb{Z} \iff d' \mid \delta$ $\quad$ cond. ② verificata

ALGORITMO DI EUCLIDE × MCD

dati $a, b > 0$ $\quad \delta = MCD(a,b)$

comincio con la divisione euclidea a, b (o b, a - è uguale)

$$a = q_0 b + r_0 \qquad (0 \le r_0 < b) \text{ — x def. resto}$$

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

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

$\vdots$ $\quad r_0, r_1, r_2 \ldots$ decrescono - arriveranno a 0

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

δ !! (MCD)

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

esercizio d'esempio

$a = 3522$, $b = 321$

$3522 = 10 \cdot 321 + 312$

$321 = 1 \cdot 312 + 9$

$312 = 34 \cdot 9 + 6$

$9 = 1 \cdot 6 + 3$

$6 = 2 \cdot 3 + 0$

$3 = MCD(3522, 321)$

$3522 = 10 \cdot 321 + 312$

321/312

$321 = 1 \cdot 312 + 9$

312/9

$312 = 34 \cdot 9 + 6$

9/6

$9 = 1 \cdot 6 + 3$

6/3

$6 = 2 \cdot 3 + 0$

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

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

Come calcolare u e v? IDENTITÀ DI BÉZOUT

Saliamo tra le iterazioni di euclide e prendiamo il resto

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

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

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

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

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

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

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

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

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

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

abbiamo trovato v e u !! (bravi tutti)

15/10

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

dim.

sono primi tra loro (MCD = 1)

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

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

$$au+bv=1$$

$a \mid bc$ per ipotesi, quindi $bc = ka$

moltiplico tutto per c $\quad acu+bcv=c$

$acu+akv=c \iff a\underbrace{(uc+kv)}_{l}=c$ quindi $a \mid c$ ■

$\exists\, l$ t.c. $c=al$

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

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

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

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

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

Se $p \mid a$, ho finito → suppongo $p \nmid a$.

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

fun fact del collega di Pellarin.

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

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

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

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

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

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 $\mathbb{Z}$

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

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

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

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

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

altri casi:

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

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

$\left.\right\}$ divisibile per 5 in tutti i casi

studiamo le potenze 2 mod 5

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

è ciclico:

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

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

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

$[2]^{4^q} = 1^q = 1$

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

potenze 3 mod 5:

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

potenze 4 mod 5

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

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

- $A = \mathbb{Z}/_{N\mathbb{Z}} = \mathbb{Z}/_{\equiv_n}$

- $[a] + [b] = [a+b]$ e $[a] \cdot [b] = [a \cdot b]$ (premesse)

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

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

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

$[ab] = [1] \iff N \mid ab - 1$ è invertibile $\iff$ scelto un qualsiasi rapp. quando faccio $ab-1$, è div per N

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

porto 1 e kn dall'altra parte

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

$\iff a$ e N sono primi fra loro!

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

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

$r \longrightarrow [r]$

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

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

Che cosa si osserva quando N è primo?

- $N = p$ primo : Sia $r \in \{ \bar{1}, \dots, \overline{p-1} \}$ — $p-1$ classi

$MCD(p,r) = 1$. Altrimenti, qualora si avesse $\delta = MCD(p,r) > 1$ avrei: $\delta \mid p$, $\delta \mid r \implies \delta = p$ — p primo, quindi se $\delta \mid p$, $\delta = p$

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

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

def CAMPO

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

17/10

PICCOLO TEOREMA DI FERMAT

ricordiamo:

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

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

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

non vero in $\mathbb{Z}$

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

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

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

- $0 < i < p$ (non $\le \ge$ perché so che la rid. mod. p di $\emptyset$ e p è $\emptyset$)

perché è una cardinalità

Scriviamo $\binom{p}{i} = \frac{p!}{i!\,(p-i)!}^{*} \in \mathbb{N}$, quindi si ha che $i!\,(p-i)! \mid p$ (appunto perché la frazione $\in \mathbb{N}$)

- Supponiamo $1 \le i \le p-1$ e inoltre $i! = i\,(i-1) \dots 3 \cdot 2 \cdot 1$

quindi, siccome $p > i$, si ha $p \nmid i$ (perché i si scompone 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 $p \nmid (p-i)!$

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

(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.

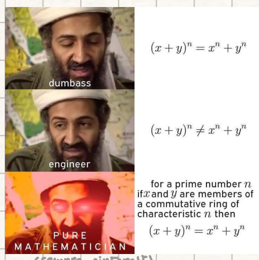
per def. fattoriale

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

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

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

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



(sempre pinterest)

TORNIAMO ALLA DIM. PRINCIPALE (PTF)

appena dim.

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

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

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)

PRECISAZIONE

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

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

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

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

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

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

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

(il PTF ha dei difetti:)

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

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

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

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

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

es. $p = 691$ (primo)

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

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

689' (690)

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

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

③ Nessun intero in $4\mathbb{Z}+3$

calcoliamo le classi resto modulo 4 dei quadrati

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

la somma di quadrati mod 4 può essere soltanto

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

in particolare, non è mai $\bar{3}$

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

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

FIBONACCI

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

proprietà

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

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

dim. × induzione con algo euclideo

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

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

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

$\| $

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

$\|$ def. fibonacci

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

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

17/10

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

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

mi serve dim applicazione biiettiva:

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

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

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

Mostriamo f suriettiva - questo basta per giustificare il claim

Possiamo mostrare che f biiettiva (+ forte)

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

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

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

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

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

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

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

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

sono identità: f e g biiettive

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

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

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

Esercizio 5 Dimostrare che $2^n \not\equiv 1 \mod n \quad \forall n > 1$ $\qquad$ X CASA

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

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

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

2 casi:

1. n primo $\to$ Fermat: $[2^{n-1}]_n = [1]_n$

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

2. n non primo $\longrightarrow$ $n = a \cdot b$ con $1 < a < n$, $1 < b < n$

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

TEOREMA FONDAMENTALE DELL'ARITMETICA

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

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

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

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

OSS

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

Siccome

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

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

esempio:

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

$= 7 \cdot 2 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 2$

$= 7 \cdot 5 \cdot 3^2 \cdot 2^4$

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

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

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

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

$v_2(a) = 2$ $\quad v_2(b) = 0$

$v_3(a) = 1$ $\quad v_3(b) = 1$

$v_5(a) = 0$ $\quad v_5(b) = 1$

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

$v_2(ab) = 2$ $\quad v_3(ab) = 2$ $\quad v_5(ab) = 1$ $\quad v_p(ab) = 0 \quad p > 5$

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

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

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

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

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

② Procediamo per induzione:

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

- Supponiamo $a > 1$.

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

② a non primo, a non è irriducibile

si può scrivere in fattori diversi da 1 e a

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

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

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

$a = UV = \prod_p p^{V_p(U) + V_p(V)}$ ∎

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

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

dim • supponiamo $V_p(a) \le V_p(b)$

$\iff V_p(b) - V_p(a) \ge \emptyset \in \mathbb{N}$

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

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

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

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

• supponiamo $a|b$

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

per il teorema fondamentale:

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

osservo che $\ge \emptyset$ perché k intero

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

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

$\forall p,\ V_p(b) \ge V_p(a)$ ∎

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

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

① $\delta | a$ e $\delta | b$

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

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

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

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

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

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

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

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

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

esercizio

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

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

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

Come dimostrato a lezione:

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

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

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

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

3 casi:

① $\min = z$

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

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

② $\min = x$

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

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

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

③ $\min = y$

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

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

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

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

DIVISORI DI ZERO

dato A anello

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

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

ma in $\mathbb{Z}$ non succede

def $a\in A$ è <u>divisore di zero</u>

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

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

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

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

<u>L'unico divisore di zero in K è 0_K</u>

dim • Supponiamo a divisore di zero:

da qui in poi usiamo 0 per 0_K

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

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

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

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

$$a=0$$

in $\mathbb{Z}$

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

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

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

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

questo è impossibile se $a>0$.
quindi $a=0$ ■

def <u>dominio</u>

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

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

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

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

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

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

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

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

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

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

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

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

Quindi, uno dei due divisori è zero

22/10

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

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

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

dim:

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

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

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

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

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

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

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

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

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

$aX = b$

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

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

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

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

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

proposizione $aX = b \quad a, b \in A = \mathbb{Z}/_n\mathbb{Z}$

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

dim:

- Dimostro ammette soluzioni $\Longrightarrow MCD(\alpha, n) \mid \beta$

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

quindi $\equiv_n 0$ quindi multiplo di n

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

$\beta \in$ ai multipli di δ

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

$\delta = MCD(\alpha, n)$

- Ora dimostro $MCD(\alpha, n) \mid \beta \Longrightarrow$ ammette soluzioni

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

Bézout

$\iff \exists\, u, z$ t.c. $\beta = u\alpha + vn \iff \beta - u\alpha = vn$

x def congr. mod

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

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

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

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

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

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

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

parentesi tutoraggio: equazioni diofantee

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

① calcolo l'MCD (a,b)

$858 = 3 \cdot 253 + 99$
$253 = 2 \cdot 99 + 55$
$99 = 1 \cdot 55 + 44$
$55 = 1 \cdot 44 + 11$
$44 = 4 \cdot 11 + 0$
$d = MCD(858, 253) = 11$

② mi assicuro che l'MCD divida c
(altrimenti, l'eq. non ha soluzioni)

$11 | 33$? sì

③ calcolo l'identità di Bézout
(la tutor lo fa da sopra e usando a, b invece dei numeri corrispondenti)

$99 = 858 - 3 \cdot 253 = a - 3b$
$55 = 253 - 2 \cdot 99 = b - 2(a - 3b) = -2a + 7b$
$44 = 99 - 55 = a - 3b - (-2a + 7b) = 3a - 10b$
$11 = 55 - 44 = -2a + 7b - (3a - 10b) = -5a + 17b$

quindi $11 = -5a + 17b$

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

$11 = -5a + 17b$
$\times 3$
$33 = 3(-5a + 17b) = -15a + 51b = \underbrace{-15}_{x_0} \cdot 858 + \underbrace{51}_{y_0} \cdot 253$

ho trovato x_0 e y_0 soluzioni particolari dell'equazione

⑤ trovo le soluzioni generali
(soluzioni intere dell'omogenea associata)

(termine non moltiplicato da x_0)

$$x = x_0 + \frac{b}{MCD(a,b)} k \qquad k \in \mathbb{Z}$$
$$y = y_0 - \frac{a}{MCD(a,b)}$$

quindi
$$x = -15 + \frac{253}{11} k = -15 + 23k$$
$$y = 51 - \frac{858}{11} k = 51 - 78k \qquad k \in \mathbb{Z}$$

lemma

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

** credo che "basti" il lemma di Gauss? Sapendo $a \mid bh$ e $MCD(a,b)=1$ allora $a \mid h$ (cambiano i vincoli, per Gauss $a, b \in \mathbb{Z}^*$ e non $\mathbb{Z}$, ma non credo ci sarebbe perdita di generalità chiederò al prof)* — $a, b \in \mathbb{Z}^*$ e $c \in \mathbb{Z}$ e $MCD(a,b)=1$ allora $a \mid bc \implies a \mid c$

dim:

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

$$\implies a \mid bh \quad \text{(o anche } b \mid ak\text{, ma scegliamo } a \mid bh\text{)}$$

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

  - $MCD(a,b) = 1 \iff b$ è invertibile modulo a

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

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

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

$$\iff ab' - ahk = h \iff a(b' - hk) = h \quad \text{quindi } a \mid h \ \blacksquare$$

TEOREMA CINESE DEI RESTI

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

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

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

Allora il sistema
$$(*) \begin{cases} x \equiv c_1 \mod r_1 \\ x \equiv c_2 \mod r_2 \\ \vdots \\ x \equiv c_s \mod r_s \end{cases}$$
ha un'unica soluzione modulo $R := r_1 \cdot r_2 \cdot \ldots \cdot r_s$

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

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

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

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

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

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

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

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

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

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

Quindi $x_0 = \sum_{j=1}^{s} y_j R_j = \boxed{\underbrace{\sum_{\substack{j=1 \\ j\neq i}}^{s} y_j R_j}_{\equiv_{r_i} 0 \text{ (divisibile per } r_i)}} + y_i R_i$ 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 $c_i \mod r_i$

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

sistema omogeneo associato

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

soluzioni? $x \equiv_{r_1} 0 \iff r_1 \mid x$

$x \equiv_{r_2} 0 \iff r_2 \mid x$

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

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

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

proposizione

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

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

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

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

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

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

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

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

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

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

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

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

Se sono coprimi, ammette un'unica soluzione modulo R

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

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

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

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

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

③ $\bar{X}_i = R_i x \equiv_r c$

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

è un'equazione diofantea di tipo

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

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

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

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

ho trovato x_0 particolare

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

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

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

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

quindi $[X_1] \equiv [-1] \equiv [10]$ siamo in mod 11

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

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

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

$22 = 4 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

quindi (Bézout)

$1 = 5 - 2 \cdot 2$

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

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

ma qui cerchiamo $= 2$ *

quindi moltiplico per 2

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

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

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

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

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

$1x \equiv 1 \mod 2$

1

$[X_3] \equiv [1] \mod 2$

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

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

esercizio 8 (foglio 3)

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

METODO PELLARIN CRT

① $4x \equiv 7 \mod 15$

① calcolo l'MCD tra 4 e 15

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

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

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

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

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

$x \equiv_{15} 13$

(multipli con resto 13)

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

② $6x \equiv 8 \mod 9$

noto che 6 e 9 non sono coprimi

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

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

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

mentre 8 non lo è

$\mathcal{E} = \emptyset$

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

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

② semplifichiamo le congruenze

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

$\cdot$ 5312065

① $8 | 40$ quindi $8 | 40 \cdot 10\mathbb{Z}$

notiamo che $5312065 = 4000000 + 1312065$

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

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

$8 | 8000 \equiv_8 65 \equiv_8 1$

② $\cdot\ 36 \equiv_5 1$

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

③ $\cdot\ 4 \equiv_3 1$

$\cdot\ 7 \equiv_3 1$

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

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

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

④ troviamo gli inversi S_i

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

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

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

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

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

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

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

POLINOMI in una indeterminata a coeff in un campo

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

Un polinomio in X a coefficienti in K è definito come

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

esempio

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

→ insieme 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:

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

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

prodotto di Cauchy

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

→ grado di un polinomio

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

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

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

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

Lemma

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

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

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

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

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

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

operazioni:

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

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

proprietà

① $|a| = 0 \iff a = 0$

② $|ab| = |a| \cdot |b|$

③ $|a+b| \leq |a| + |b|$ diseg. triangolare

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

① $\deg(a) = -\infty \iff a = 0$

② $\deg(ab) = \deg(a) + \deg(b)$

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

ci sono delle corrispondenze, ma serve qualcosa di più vicino

def c-valore assoluto di un polinomio

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

Scegliamo $c > 1$

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

invece, se $P = 0$

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

Allora proprietà

① $|a|_c = 0 \iff a = 0$

② $|ab|_c = |a|_c \cdot |b|_c$

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

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

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

ALGORITMO DELLA DIVISIONE EUCLIDEA SUI POLINOMI

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

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

divisione in colonna

$a = x^4 + x + 1$

$b = x^3 - 2$

$$\begin{array}{ccc|cc}
x^4 + & & x+1 & x^3 & -2 \\ \hline
x^4 & & -2x & x & \\
0 & & 3x+1 & &
\end{array}$$

① x^4 / x^3

② moltiplico per $(x^3 - 2)$

③ scrivo qui

④ sottraggo

grado < quindi fine

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

TABELLA ANALOGIE TRA $\mathbb{Z}$ e $K[X]$

(il grande ripasso delle proprietà di $\mathbb{Z}$)

$\mathbb{Z}$	$A = K[X]$
interi divisione euclidea valore assoluto	polinomi divisione euclidea $\lvert\cdot\rvert_c$ o deg
$\mathbb{N}^*$ ("positivi")	$A^+ = \{\text{polinomi monici}\}$ in forma $P = a_0 + a_1 X + \ldots + a_n X^n$ con $a_n = 1$ (coeff. grado massimo) · il prodotto di monici è monico (ma la somma non necessariamente)
$\mathbb{Z}^\times = \{\pm 1\}$	inversi sui polinomi $A^\times = K^\times$ sia $a \in A^\times$ $\exists b \in A^\times$ t.c. $ab = 1$ $\Longrightarrow \deg(a) + \deg(b) = \emptyset$ ($\deg(ab) = \emptyset = \deg(a) + \deg(b)$) $\Longrightarrow \deg(a), \deg(b) \in \mathbb{N}$ (o avrei $-\infty$) $\Longrightarrow \deg(a) = \deg(b) = \emptyset$ $\Longrightarrow a, b \in K^\times$ ("costanti" diverse da $\emptyset$)
divisibilità in $\mathbb{Z}$ $a \mid b \iff$ $\exists k \in \mathbb{Z}$ t.c. $b = ak$ $\iff b \in a\mathbb{Z}$ $\iff b\mathbb{Z} \subset a\mathbb{Z}$	$a \mid b \iff$ $\exists H \in A$ t.c. $b = aH$ $\iff b \in aA$ $\{al : l \in A\}$ $\iff bA \subset aA$

proprietà di $\mid$ su A

① riflessiva

② transitiva

$a \mid b,\ b \mid c \iff cA \subset bA \subset aA$

$\iff cA \subset aA \iff a \mid c$

③ quasi riflessiva ma non:

$a, b \in A$. Supponiamo $a \mid b \wedge b \mid a$

$\iff \exists u \in A$ t.c. $b = au$, $\exists v \in A$ t.c. $a = bv$

quindi $a = uva \iff \deg(a) = \deg(u) + \deg(v) + \deg(a)$

possiamo supporre $a, b \neq \emptyset$

$\cancel{\deg(a)} = \cancel{\deg(a)} + \deg(u) + \deg(v) \iff \emptyset = \deg(u) + \deg(v)$

$\iff \deg(u) = \deg(v) = \emptyset$

$\iff u = \lambda \in K^\times$, $v = \mu \in K^\times$ (sempre per la questione $\deg(0) =$ "costante" $!= \emptyset$)

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

$\mathbb{Z}$ è un dominio d'integrità

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

dim Sia $P \in A$ divisore di zero

$\exists Q \in A \setminus \{0\}$ t.c. $PQ = 0$

$\deg(PQ) = \deg(0) = \underbrace{\deg(P) + \deg(Q)}_{\text{impossibile somma due numeri} \in \mathbb{N} = -\infty} = -\infty$

Quindi $\deg(P) = -\infty \iff P = 0$ ■

$a \equiv b \mod n$

$\iff n \mid a-b$

$a, b \in A$, $H \in A \setminus \{0\}$

$a \equiv b \mod H$ rel di eq.

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

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

$\iff a-b = Hu \ \exists u \in A$, $b-c = Hv \ \exists v \in A$

$a - \cancel{b} + \cancel{b} - c = H(u+v)$

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

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

$A/_{HA}$ anello commutativo unitario

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

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

$A/_{HA} = \{[a] : a \in A\} = \{a + Ha : a \in A \text{ t.c. } \deg(a) < \deg(H)\}$

non alteriamo il grado di a rispetto a H

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

---

de: MCD in $\mathbb{Z}$

de: MCD in A

Bézout in $\mathbb{Z}$:

$\mathcal{E} = a\mathbb{Z} + b\mathbb{Z}$ $a, b \neq 0$

allora $\exists! \delta \in \mathbb{N}^*$ t.c.

$\mathcal{E} = \delta\mathbb{Z}$

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

Lemma Bézout in $A = K[X]$

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

allora $aA + bA = \delta A$ $\exists! \delta \in A^+$ monico (notiamo che infatti è l'insieme "analogo" a $\mathbb{N}^*$ in A)

$\mathcal{E} = aA + bA$ (polinomi), $\mathcal{E}^+ = \{m \in \mathcal{E} \text{ t.c. } m \in A^+\}$ polinomi monici

dimostro che $\mathcal{E}^+$ contiene un el. di grado minimale unico (δ)

(mostrare non vuoto $(a,b) \neq 0$, principio minimo)

MCD

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

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

① $d \mid a \wedge d \mid b$

③ se $d' \in A$ t.c.

$d' \mid a \wedge d' \mid b \implies d' \mid d$

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

MCD

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

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

① $d \mid a \wedge d \mid b$

③ se $d' \in A$ t.c.

$d' \mid a \wedge d' \mid b \implies d' \mid d$

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

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

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

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

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

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

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

P è irriducibile se, scrivendo $P = QR$

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

Osservazione:

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

$X - x = U \cdot V$

$\underset{\substack{\| \\ 1}}{\deg(X-x)} = \deg(U) + \deg(V)$

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

primo $a \in A \setminus A^\times$, $a \neq 0$

primo se $a \mid bc \implies a \mid b$ o $a \mid c$

primo $P \in A \setminus A^\times$ è primo se

$P \mid QR \implies P \mid Q$ o $P \mid R$

Lemma: primo $\iff$ irriducibile

Lemma: P irriducibile $\iff P$ primo

Teorema Fondamentale Aritmetica

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

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

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

Teorema della Fattorizzazione Unica

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

$$H = \underset{\in A^\times}{\lambda} \cdot \prod_{\substack{P \text{ irr.} \\ P \in A^+}} P^{v_p(H)}$$

$v_p(H) \in \mathbb{N}$ e $\{P : v_p(H) \neq 0\}$ 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 $\deg(P) = 2$

  $(P = X^2 + aX + b)$ allora $\Delta = a^2 - 4b < 0$

def VALUTAZIONE

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

la valutazione di F in x

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

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

osserviamo:

① $ev_x(F+G) = ev_x(F) + ev_x(G)$

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

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

- Si dice che $ev_x : K[X] \longrightarrow K$ è un OMO MORFISMO DI ANELLI

DA APPUNTI EXYSS

(non l'ho fatto, è solo curiosità)

Omomorfismo: dati $(G, \cdot)$, $(H, \odot)$ strutture algebriche dello stesso tipo

un omomorfismo è $f : G \to H$

tale che $f(g \cdot h) = f(g \odot h)$ $\forall g, h \in G$

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

Lemma Sia $x \in K$

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

polinomi che si annullano in X

($x \in K$ tali che sostituite diano 0)

dim:

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

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

  $\Longrightarrow Q \in ev_x^{-1}(\{0\})$

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

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

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

$r = 0$, r const $\neq 0$

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

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

P ha una radice in x

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

29/10

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

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

nessuna radice reale

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

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

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

  per i polinomi grado 3 si può andare a tentativi
  · ev_0 no (c'è -6)

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

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

calcolo il quoziente:

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

poi uso la formula quadratica:
$\Delta = 25-24 = 1 > 0$
quindi $x_i = \dfrac{5 \pm \sqrt{1}}{2}$ → 2, 3

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$\mathbb{C}$ NUMERI COMPLESSI

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

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

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

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

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

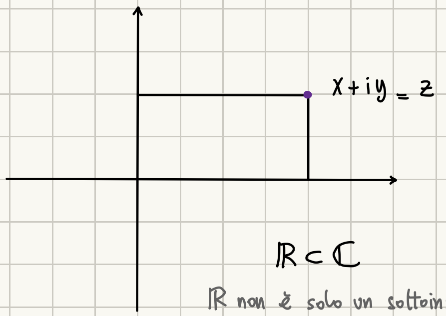
  $z + z' := (x + x') + i(y + y') \in \mathbb{C}$ somma

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

- nuova operazione: CONIUGAZIONE COMPLESSA qui

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

realizzazione cartesiana di $\mathbb{C}$



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

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

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

esponenziale di Eulero

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

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

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

$$\| $$

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

$$\|$$

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

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

$$\|$$

raggruppo parte reale e immaginaria

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

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

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

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

non l'ha fatto ma l'ho trovato su internet

(+ formula di De Moivre: $(\cos(\vartheta) + i\sin(\vartheta))^n = \cos(n\vartheta) + i\sin(\vartheta)$)

esempi numeri complessi (Eulero, De Moivre)

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

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

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

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

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

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

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

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

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

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

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

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

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

proprietà

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

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

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

④ h è una biiezione $h^{-1} = h$

h è un isomorfismo di anelli

→ DA APPUNTI EXYSS (non l'ho fatto a lezione non serve saperlo) era solo curiosità mia

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

isomorfismo: $f: G \to H$
se è OMOMORFISMO ed è BIIETTIVA

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

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

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

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

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

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

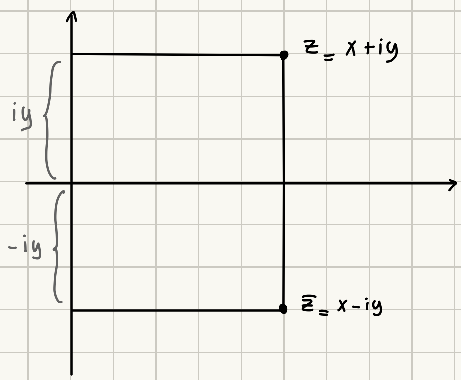
③ $\overline{-z} = -\bar{z}$

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

reali e $\bar{z}$

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

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



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

$$h: \mathbb{C} \to \mathbb{C}$$
$$z \longmapsto \bar{z}$$

formule fondamentali

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

$|z| = \sqrt{z\bar{z}} = \sqrt{x^2+y^2}$ 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 $z\bar{z} = \underbrace{x^2+y^2}_{>0 \ (z \in \mathbb{C}\setminus\{0\})}$ e lo moltiplico per il suo inverso: $(x^2+y^2)^{-1}$

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

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

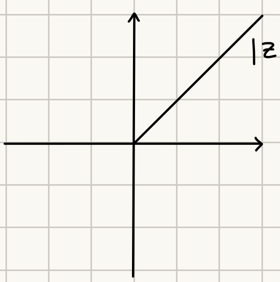
esempi:

• $z = 2 = 2+i0 \in \mathbb{R}$ $\quad \bar{z} = 2$, $\quad x^2+y^2 = 4$, $\quad z^{-1} = \frac{\bar{z}}{x^2+y^2} = \frac{2}{4} = \frac{1}{2}$

• $z = i = 0 + 1 \cdot i$ $\quad \bar{z} = -i$ $\quad x^2+y^2 = 1$ $\quad z^{-1} = \frac{-i}{1} = -i$

• $z = 1+i$ $\quad \bar{z} = 1-i$ $\quad z\bar{z} = 2$ $\quad z^{-1} = \frac{1-i}{2}$ $\quad (i+1)\frac{1-i}{2} = \frac{2}{2} = 1$

valore assoluto complesso



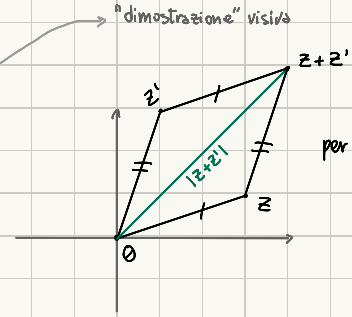
proprietà

① $|z| = 0 \iff z = 0$

② $|zz'| = |z| \cdot |z'|$

③ $|z+z'| \leq |z| + |z'|$

"dimostrazione" visiva



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

proprietà / esercizio

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

dim:

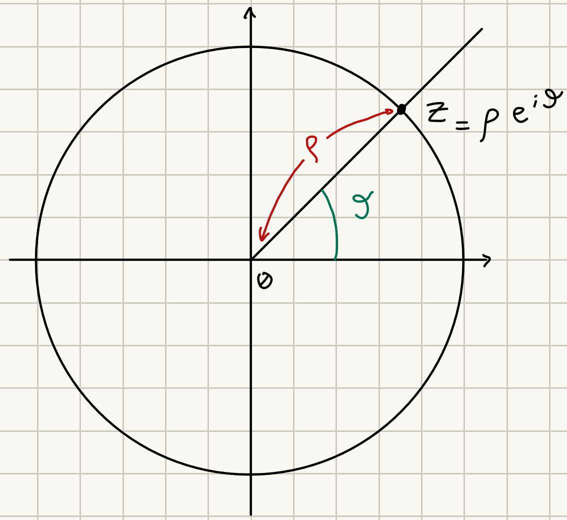
① $e^{i\vartheta} = \cos(\vartheta) + i\sin(\vartheta)$ $\quad |e^{i\vartheta}| \underset{\text{def }||}{=} \sqrt{\underbrace{\cos(\vartheta)^2 + \sin(\vartheta)^2}_{=1 \text{ (prop sin, cos)}}}^{\,*} = \sqrt{1} = 1$

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

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

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

RAPPRESENTAZIONE POLARE



dati $\quad z \in \mathbb{C} \qquad z = x + iy \quad , \; \rho = \sqrt{x^2+y^2}$

Lemma

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

z' è la "componente angolare" $\quad z' = \rho^{-1} z$

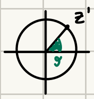
$z' = \rho^{-1} \rho e^{i\vartheta} = e^{i\vartheta}$

dim $(\exists\, \vartheta \ldots)$

$\rho = \sqrt{z\bar{z}} \quad , \quad z' := \rho^{-1} \cdot z$

il coniugato di un reale è il reale stesso

- $\underbrace{z'\overline{z'}}_{\text{ora so che è l'inverso}} = \rho^{-1} z \; \overline{\rho^{-1}}\, \bar{z} = \rho^{-2} z\bar{z} = \rho^{-2} \cdot \rho^2 = 1$ — val. ass $= 1 \quad \sqrt{z\bar{z}} = |z| \quad \sqrt{1} = 1$ quindi siamo nel cerchio delle unità

- $z' = x' + iy'$  $\quad \exists\, \vartheta$ t.c. $x' = \cos(\vartheta) \quad y' = \sin(\vartheta)$ ①

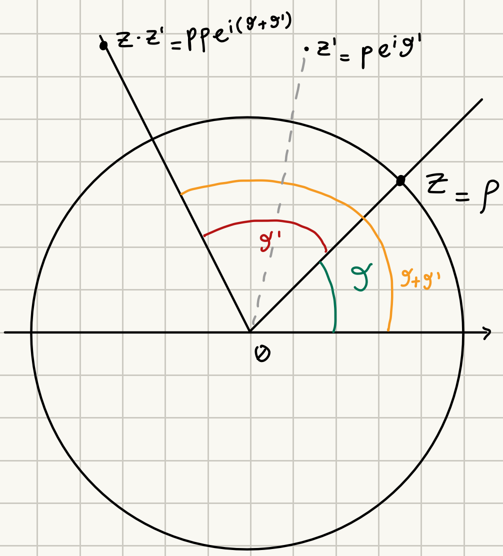
$\Longrightarrow$ (sostituisco in $z' = x' + iy'$) $\; z' = \cos(\vartheta) + i\sin\vartheta = e^{i\vartheta}$ quindi (per $z' = \rho^{-1} z$) $\; z = \rho e^{i\vartheta}$

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

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

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

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



la rappresentazione polare è utile per effettuare moltiplicazioni di numeri complessi

OSSERVAZIONE

$z \in \mathbb{C}$ è della forma $e^{i\vartheta} \iff |z| = 1$ — $\sqrt{\cos(\vartheta)^2 + \sin(\vartheta)^2}$

viceversa se $|z| = 1$ allora la sua distanza dall'origine è 1. Quindi giace sul cerchio delle unità di $\mathbb{C}$

$\Longrightarrow \exists\, \vartheta$ t.c $z = \cos(\vartheta) + i\sin(\vartheta)$

def ALGEBRICAMENTE CHIUSO

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

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

(se ha almeno una radice in K)

Lemma

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

dimostrazione

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

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

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

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

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

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

  $\Longrightarrow P = X - x$

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

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

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

  $\iff x$ è radice di P ∎

Corollario: MOLTEPLICITÀ

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

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

$V_x(F)$ è la MOLTEPLICITÀ di F in x

Si ha che $\{x : V_x(F) \neq 0\} = \{x : ev_x(F) = 0\} = \{x \text{ radice di } F\} = R$

(chiaramente un pol. si decompone solo con le sue radici)

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

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

(ovvero, perché un pol. di grado n ha $\leq n$ soluzioni)

↑ esp. dei polinomi in cui si scompone

Teorema (fondamentale dell'algebra)

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

Teorema

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

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

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

31/10

FATTORIZZAZIONE DI VARI POLINOMI

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

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

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

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

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

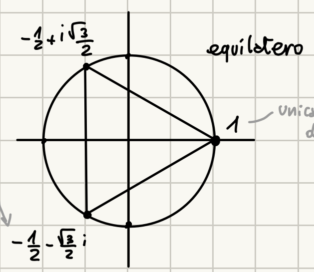
- $n=3$ $X^3 - 1 = (X-1)(\underbrace{X^2+X+1}_{\Delta<0 \text{ irriducibile}})$ fattorizzazione in $\mathbb{R}[X]$

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

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

quindi $X_0 = x + iy$

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



(io che ragiono:)

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

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

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

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

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

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

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

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

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

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

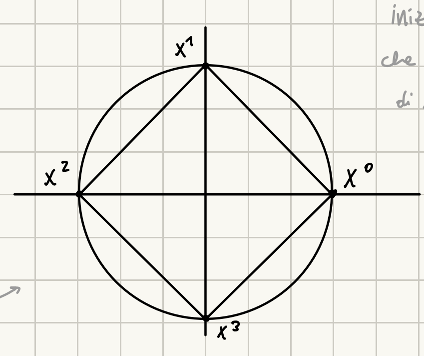
- $n=4$ $X^4 - 1 = (X-1)(X+1)(X^2+1)$ in $\mathbb{R}[X]$

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

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

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

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



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

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

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

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

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

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

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

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

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

con:

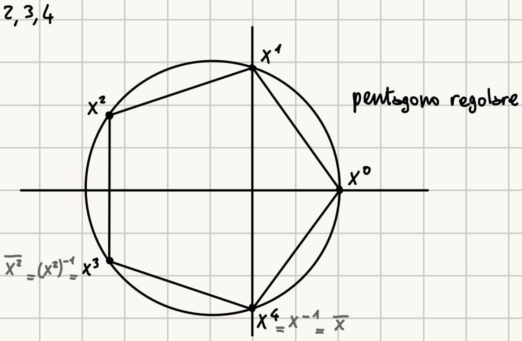
• $x = \alpha + i\beta$ $\qquad$ • $\bar{x} = \alpha - i\beta$ $\qquad$ • $x + \bar{x} = 2\alpha \in \mathbb{R} = 2\,\mathrm{Re}(x^2) = 2\cos\left(\frac{2\pi}{5}\right)$

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

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

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

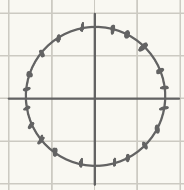
$$\left(\left(e^{\frac{2\pi i}{5}}\right)^k\right)^5 = \left(e^{\frac{2\pi i}{5}\cdot 5}\right)^k = \Big(\underbrace{e^{2\pi i}}_{=1}\Big)^k = 1$$



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

quindi $X^5 - 1 = \prod_{i=0}^{4}(X - x^i) = (X - x^0)\left[(X-x)(X-\underset{\bar{x}}{x^4})\right]\left[(X-x^2)(X-\underset{\overline{x^2}}{x^3})\right]$

OSSERVAZIONE: con $n \geq 1$, $\quad X^n - 1 = \prod_{i=0}^{n-1}(X - x^i)$ $\quad$ con $x = e^{\frac{2\pi i}{n}}$



fatt. in $\mathbb{C}[X]$

def <u>POLINOMIO CONIUGATO</u>

Dato $F = f_0 + f_1 X + \ldots + f_n X^n \in \mathbb{C}[X]$, poniamo $\overline{F} = \overline{f_0} + \overline{f_1} X + \ldots + \overline{f_n} X^n$

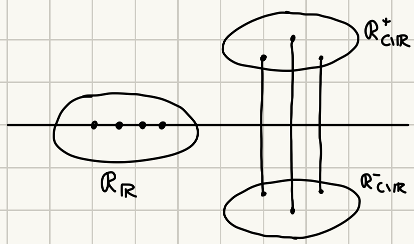
OSSERVAZIONE: $F \in \mathbb{R} \iff F = \overline{F}$ in $\mathbb{R}$, $x = \overline{x}$

inoltre, se $F \in \mathbb{R}[X]$ e $ev_z(F) = \emptyset$, allora $ev_{\overline{z}}(F) = \emptyset$ dim: $ev_{\overline{z}}[F] = ev_{\overline{z}}[\overline{F}]$ e, siccome la coniug. complessa è compatibile con $+, -, \cdot$ $= \overline{ev_z(F)} = \overline{\emptyset} = \emptyset$

Lemma Dato $F \in \mathbb{R}[X]$

detto $\mathcal{R}$ l'insieme delle sue radici, allora $\mathcal{R} = \mathcal{R}_{\mathbb{R}} \sqcup \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} \sqcup \mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}}$ dove $\mathcal{R}_{\mathbb{R}} = \mathcal{R} \cap \mathbb{R}$

$\mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} = \{ z \in \mathcal{R}$ t.c. $z \in \mathbb{C} \setminus \mathbb{R}$, $\Im(z) > 0$ e scrivendo $z = \underset{\in\mathbb{R}}{x} + i\underset{\in\mathbb{R}}{y}$, $y > 0 \}$, $\mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}} = \{ z \in \mathcal{R} \setminus \mathbb{R}$ t.c. $\Im(z) < 0 \}$



inoltre $\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}} = \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} \sqcup \mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}}$ e $\overline{\mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}}} = \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}}$

Lemma già ampiamente utilizzato

$X^2 + \beta X + \gamma \in \mathbb{R}[X]$ è irriducibile $\iff \Delta = \beta^2 - 4\gamma < 0$

dim

Supponiamo P irriducibile.

$\mathcal{R}_{\mathbb{R}} = \emptyset$, quindi $\mathcal{R}_{\mathbb{C}\setminus\mathbb{R}} = \{z, \overline{z}\}$ $\mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} = \{z\}$, $\mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}} = \{\overline{z}\}$

$$P = (X - z)(X - \overline{z}) = X^2 - \underset{2\,\mathrm{Re}(z)}{\underset{\|}{(z + \overline{z})}} + \underset{|z|^2}{\underset{\|}{z\overline{z}}}$$

$$\Delta = (z + \overline{z})^2 - 4 z\overline{z} = z^2 + 2z\overline{z} + \overline{z}^2 - 4z\overline{z} = (z - \overline{z})^2$$

scrivo $z = x + iy$ $z - \overline{z} = 2iy$, quindi $(z - \overline{z})^2 = (2iy)^2 = 4i^2y^2 = 4y^2 \cdot -1 = -4y^2 < 0$ ($\in\mathbb{R}$; y è di parte imm > 0 quindi $y^2 \neq 0$)

Lemma

Ogni $F \in \mathbb{R}[X]$ si spezza in $\mathbb{R}[X]$ in prodotto $F = \underset{\in\mathbb{R}^\times}{\lambda} \prod_{x \in \mathcal{R}_{\mathbb{R}}} (X - x)^{v_x(F)} \prod_{z \in \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}}} \overbrace{[(X - z)(X - \overline{z})]}^{\text{polinomio grado 2 in } \mathbb{R}[X] \text{ irriducibile}}{}^{v_z(F)}$

presa dalle slide

dim: Siccome $\mathbb{C}$ è algebricamente chiuso,

$$F = \underset{\in\mathbb{R}^\times}{\lambda} \prod_{z \in \mathcal{R}} (X - z)^{v_z(F)} = \lambda \prod_{z \in \mathcal{R}_{\mathbb{R}}} (X - z)^{v_z(F)} \prod_{z \in \mathcal{R}_{\mathbb{C}\setminus\mathbb{R}}} (X - z)^{v_z(F)}$$

se $z \in \mathcal{R} \setminus \mathbb{R}$ si ha $\overline{z} \in \mathcal{R} \setminus \mathbb{R}$. Quindi, posso scegliere, senza perdita di generalità, $z = x + iy$ con $y > 0$ e $\overline{z}$ apparterrà a $\mathcal{R}$

Si conclude osservando che $\mathcal{R} = \mathcal{R}_{\mathbb{R}} \sqcup \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}} \sqcup \mathcal{R}^-_{\mathbb{C}\setminus\mathbb{R}}$

Lemma (in teoria esercizio ma mi sembra più un lemma)

Sia $P \in \mathbb{R}[X]$ di grado dispari. Allora P ammette almeno una radice reale.

questo implica $\deg(P) = \overset{\text{card}}{\#} R_{\mathbb{R}} + \# R_{\mathbb{C}\setminus\mathbb{R}} = \underbrace{\# R_{\mathbb{R}}}_{r} + \underbrace{\overset{\text{i coniugati}}{2}\, R^{+}_{\mathbb{C}\setminus\mathbb{R}}}_{s}$

Siccome P è di grado dispari, $\deg(P) = 2n+1 = \# R_{\mathbb{R}} + 2s$ ma allora $2n+1 = r + 2s \iff r = \underbrace{2n-2s}_{\text{pari}} + 1 = \text{dispari} \implies r \equiv 1 \bmod 2 \implies r \neq 0$

> ci serve il teorema dei valori intermedi (dell'Analisi)
>
> se $h: \mathbb{R} \to \mathbb{R}$ è continua t.c. $\lim_{x\to+\infty} h(x) = +\infty$, $\lim_{x\to-\infty} h(x) = -\infty$
>
> allora $\exists\, x_0 \in \mathbb{R}$ t.c. $h(x_0) = 0$

$P = X^{2n+1} + \alpha_{2n} X^{2n} + \dots + \alpha_0 \in \mathbb{R}[X]$ dispari

Sia $f: \mathbb{R} \to \mathbb{R}$ la funzione $f(x) = ev_x(P)$: è continua e soddisfa $\lim_{x\to-\infty} f(x) = -\infty$, $\lim_{x\to+\infty} f(x) = +\infty$

da cui $\exists\, x_0 \in \mathbb{R}$ t.c. $f(x) = 0 \iff x_0$ radice di f

esercizio 1

$P = X^4 - 10X^2 + 1$ in $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$

• in $\mathbb{C}$

tentiamo le radici. pongo $Y = X^2$ $\quad P = Y^2 - 10Y + 1$

$5 > 2\sqrt{6} \iff 25 > 4 \cdot 6$

$\Delta > 0$, radici $y_1 = 5 - 2\sqrt{6} > 0$, $y_2 = 5 + 2\sqrt{6} > 0$

$Y^2 - 10Y + 1 = (X^2 - 5 + 2\sqrt{6})(X^2 - 5 - 2\sqrt{6}) = (X + \underset{\alpha_1}{\sqrt{5+2\sqrt{6}}})(X + \underset{\alpha_2}{\sqrt{5-2\sqrt{6}}})(X - \underset{\alpha_3}{\sqrt{5-2\sqrt{6}}})(X - \underset{\alpha_4}{\sqrt{5+2\sqrt{6}}})$ è la fatt. in $\mathbb{R}[X]$ e anche in $\mathbb{C}[X]$

in $\mathbb{Q}$

POSSIBILI FATTORIZZAZIONI IN IRR. DI POLINOMI IN $\mathbb{Q}[X]$ UN CAMPO QUALSIASI

$Q \in \mathbb{Q}[X]$ (uguale per un campo qualsiasi)

- $\deg(Q) = 1$ è irriducibile
- $\deg(Q) = 2$
  ① Q irriducibile
  ② $Q = P_1 P_2$ con P_1, P_2 irr grado 1
- $\deg(Q) = 3$
  ① Q irriducibile
  ② $Q = P_1 P_2$ dove $\deg(P_1) = 1$, P_2 deg 2 irriducibile
- $\deg(Q) = 4$
  ① Q irriducibile
  ② $Q = P_1 P_2$ $\deg(P_1) = 1$ $\deg(P_2) = 3$ irriducibili c'è radice
  ③ $Q = P_1 P_2$ $\deg(P_1) = \deg(P_2) = 2$ irriducibili non c'è radice
  ④ $Q = P_1 P_2 P_3$ $\deg(P_1) = 2$ $\deg(P_2) = \deg(P_3) = 1$ c'è radice

TEORIA DEI GRUPPI

GRUPPI

Dato G insieme $\neq \emptyset$ con $*$ operazione binaria su G, ovvero: $G \times G \to G$, $(a,b) \to a*b$, seleziono un elemento distinto e.

La terna $G = (G, *, e)$ è un **gruppo** se: (el. neutro)

(non per forza distint.)

① $\forall a,b,c \in G \quad (a*b)*c = a*(b*c) = a*b*c$ associatività

② $\forall a \in G \quad a*e = e*a = a$ elemento neutro per l'operazione binaria

③ $\forall a \in G \ \exists a' \in G$ t.c. $a*a' = a'*a = e$ inverso per l'op. binaria

> add-on: INVERSIONE NEI GRUPPI
> $\forall a,b,c \in G \quad \cdot (ab)^{-1} = b^{-1}a^{-1}$
> $\cdot (abc)^{-1} = c^{-1}b^{-1}a^{-1}$ ecc
> (inversi dei singoli, in ordine inverso)

Inoltre, se

④ $\forall a,b \in G, \ a*b = b*a$, allora G è un **gruppo abeliano** (o **commutativo**)

quindi - come avevamo visto - le prime 4 condizioni di un anello descrivono un gruppo abeliano

gruppi in notazione additiva

$(G, +, 0)$ si scrive $+$ per l'operazione e 0 o 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 $-a$

ESEMPI $(A, +, \cdot, 0_A, 1_A)$ Anello

Allora $(A, +, 0_A)$ gruppo abeliano in not. additiva

$\mathbb{Z} = (\mathbb{Z}, +, 0) \quad \mathbb{R} = (\mathbb{R}, +, 0), \quad \mathbb{C} = (\mathbb{C}, +, 0)$

o anche $K = (K, +, 0)$ con K qualunque campo

gruppi in notazione moltiplicativa

$(G, \cdot, 0)$ si scrive $\cdot$ per l'operazione e 1 o 1_G per l'el. neutro

si dice in notazione moltiplicativa

oss: Per questi gruppi, non è garantita la commutatività.

In notazione moltiplicativa, l'inverso di $a \in G$ si scrive a^{-1}

ESEMPI $(A, +, \cdot, 0_A, 1_A)$ Anello

Allora $A^\times = (A^\times, \cdot, 1_A)$ gruppo in not. moltiplicativa

infatti abbiamo visto

⓪ il prodotto di el. invertibili è invertibile

① il prodotto è associativo

② se $a, b \in A^\times$ allora $ab \in A^\times$ e $(ab)^{-1} = b^{-1}a^{-1}$

inoltre, $A^\times$ è abeliano (se A è commutativo ?)

def SOTTOGRUPPO

Dato un gruppo G e un sottoinsieme $H \subset G$ non vuoto

Si dice che H è un **Sottogruppo** di G se:

not. moltiplicativa $\quad \forall a,b \in H$, si ha $a \cdot b^{-1} \in H$ so che $\in G$, ma se $\in H$, è sottogruppo

$\forall a,b \in H$, si ha $a - b \in H$ not. additiva

Si scrive $H < G$

OSSERVAZIONE H è stabilizzato (rispetto al prodotto)

- Se $a \in H$, $aa^{-1} = 1_G \in H$ ($a \cdot b^{-1}$ con $b = a$)
- Ma allora, $\forall b \in H \quad 1_G \cdot b^{-1} \in H$ quindi $b^{-1} \in H$ e $1_G = 1_H$ ($a \cdot b^{-1}$ con $a = 1_G$)
- Infine, se $a, b \in H$, $b^{-1} \in H$, $a(b^{-1})^{-1} = ab \in H$

(quindi un sottogruppo H contiene anche gli inversi e i prodotti dei suoi el.)
e anche l'el. neutro del gruppo di cui è sottogruppo

def OMOMORFISMI DI GRUPPI

Dati G_1, G_2 gruppi (in notazione moltiplicativa)

Sia $f: G_1 \longrightarrow G_2$ un'applicazione:

f è un omomorfismo di gruppi se

① $f(1_{G_1}) = 1_{G_2}$

(ma basta solo la ③ - che implica le altre)

② $\forall a \in G_1$, $f(a^{-1}) = f(a)^{-1}$ (inversione in G_1; inversione in G_2)

③ $\forall a,b \in G_1$, $f(a\,b) = f(a)\,f(b)$ (operazione di G_1; operazione di G_2)

(in modo più chiaro: $\cdot$ op. G_1, $\circ$ op. G_2)

$f(a \cdot b) = f(a) \circ f(b)$

(l'ordine conta! non si sa se è abeliano)

esercizio: mostrare che $f: G_1 \longrightarrow G_2$ è un omomorfismo $\iff \forall a,b \in G_1$, $f(a b^{-1}) = f(a) f(b)^{-1}$

- $\Longrightarrow$ supponiamo f omomorfismo.
  Allora $f(ab) = f(a) f(b)$ (③) quindi $f(ab^{-1}) = f(a) f(b^{-1})$.
  Ma (per ②) $f(b^{-1}) = f(b)^{-1}$
  Quindi $f(a b^{-1}) = f(a) f(b)^{-1}$

- $\Longleftarrow$ supponiamo $f(a b^{-1}) = f(a) f(b)^{-1}$

  - $f(1_{G_1}) = 1_{G_2}$ dim: pongo $a = b$ $f(b\,b^{-1}) = f(b)\,f(b)^{-1} = 1_{G_2}$
  - $f(a^{-1}) = f(a)^{-1}$ dim: pongo $a = 1_{G_1}$ $f(1_{G_1} b^{-1}) = f(1_{G_1})\,f(b)^{-1} \underset{\text{per ①}}{=} 1_{G_2}\,f(b)^{-1} = f(b)^{-1}$
  - $f(ab) = f(a) f(b)$ dim: pongo $b = b^{-1}$ $f(a(b^{-1})^{-1}) = f(a)\,f(b^{-1})^{-1} \underset{\text{per ②}}{=} f(a)\,f((b)^{-1})^{-1} = f(a)\,f(b)$

def ISOMORFISMO

Sia $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi

Se f è biiettiva, allora si dice che f è un isomorfismo

- il simbolo $\cong$ significa "è isomorfo a"
  ($G_1 \cong G_1$ esiste un isomorfismo tra G_1 e G_2)

esercizio

$f: G_1 \longrightarrow G_2$ isomorfismo. sappiamo che f biiettiva $\iff \exists\, f^{-1}: G_2 \longrightarrow G_1$ biiettiva t.c. $f \circ f^{-1} = Id_{G_2}$ $f^{-1} \circ f = Id_{G_1}$

DIMOSTRARE CHE f^{-1} è un isomorfismo

Inoltre, $G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3$ con f, g omom. di gr

allora anche $g \circ f: G_1 \longrightarrow G_3$ omom. di gr.

e in più f, g sono isomorfismi e anche $g \circ f$, di inverso $f^{-1} \circ g^{-1}$

ESEMPI

$m\mathbb{Z} < \mathbb{Z}$: $\forall a,b \in m\mathbb{Z}$, $a-b \in m\mathbb{Z}$

$\exists\, \alpha, \beta$ t.c. $a = \alpha m$, $b = \beta m$

quindi $a - b = (\alpha - \beta)m \in m\mathbb{Z}$

$\mathbb{Z} \xrightarrow{f} m\mathbb{Z} < \mathbb{Z}$ 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 iniettiva $f(p) = f(q) \iff pm = qm \iff m(p-q) = 0 \iff p = q$

③ suriettiva $y \in m\mathbb{Z}$. $\exists\, k \in \mathbb{Z}$ t.c. $y = mk$. Ponendo $x = k$ si ha $f(x) = mk = y$

(esempio che mischia le notazioni $+$, $\cdot$)

$G_1 = \mathbb{R}$ con $+$, $G_2 = \mathbb{R}_{>0}$ con $\cdot$ notare che $\mathbb{R}_{>0} < \mathbb{R}^\times$: $a,b \in \mathbb{R}_{>0}$ $a>0$, $b>0$, $b^{-1}>0$ $ab^{-1}>0$ quindi $ab^{-1} \in \mathbb{R}^\times$

poniamo:

$f: \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ $f(x) := e^x$

$f: \mathbb{R}_{>0} \longrightarrow \mathbb{R}$ $g(x) := \underset{\ln}{\log}(x)$ $e^{\log(\cdot)} = Id_{\mathbb{R}}$ $\log(e^{(\cdot)}) = Id_{\mathbb{R}}$

Sono due isomorfismi di gruppi, uno l'inverso dell'altro $f^{-1} = g$ $g^{-1} = f$

$f(0) = e^0 = 1 = 1_{G_2} \in G_2$	$g(1) = 0$
$f(-x) = e^{-x} = (e^x)^{-1}$ inverso	$g(y^{-1}) = \log(y^{-1}) = -g(y)$
$f(x-x') = e^{x-x'} = e^x e^{-x}$ $= f(x) f(x')^{-1}$	$g(y' y^{-1}) = g(y') - g(y)$ $\log\left(\frac{y'}{y}\right)$

appunti del 6/11 spostati in su per comodità logica

es. 2 foglio sett. 4

(iii) $P = X^3+X^2-6x+1 \quad Q = X^4-2x^3-2x-1$ MCD e Bézout

con $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$ campo ($\mathbb{F}_7$)

$\mathbb{F}_7 = \{0,1,2,3,4,5,6\}$ dove questi simboli rappresentano le classi corrispondenti in $\mathbb{Z}/7\mathbb{Z}$

posso anche usare altri interi per rappresentare elementi di $\mathbb{F}_7$, estraendoli dalle classi (es. $8=1$)

• abbiamo visto che $\mathbb{F}_7^\times$ è un gruppo (abeliano) in notazione •

tavola di moltiplicazione in $\mathbb{F}_7^\times$

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(la usiamo per trovare facilmente gli inversi)

ogni volta che c'è un 1, i due numeri sono inversi

• ogni riga contiene uno e un solo 1 $\longrightarrow$ ogni el del gruppo è invertibile di inverso unic. det.

quindi $P = X^3+X^2\underbrace{-6x}_{-6=1}+1 \quad Q = X^4-2x^3-2x-1$

ALGO EUCLIDE

$$\begin{array}{r|l} X^4-2x^3 \quad -2x-1 & X^3+X^2+X+1 \\ \hline X^4+X^3+X^2+X & X+4 \\ \hline 4x^3-X^2+4x-1 & \\ 4x^3+4x^2+4x+4 & \\ \hline 2x^2 \quad +2 & \end{array}$$

$-3=4$

$$\underbrace{X^4-2x^3-2x-1}_{Q} = \underbrace{(X+4)}_{\text{quoziente}}\underbrace{(X^3+X^2+X+1)}_{P} + \underbrace{2(X^2+1)}_{\text{resto}}$$

$\deg(2(x^2+1)) = 2 < \deg(P) = 3$

mentre $\deg(2(x^2+1)) > \deg(\text{quoziente})$ (non sono interss.)

continuiamo: divisione di P per il resto

$$\begin{array}{r|l} X^3+X^2+X+1 & 2x^2+2 \\ \hline X^3 \quad +X & 4x+4 \\ \hline X^2 \quad +1 & \\ X^2 \quad +1 & \\ \hline 0 & \end{array}$$

devo dividere X^2+1 per $2x^2+2$

ho quindi x^2 e $2x^2 \rightarrow$ basta molt. per $2^{-1} = 4$ (calcolato nella tavola)

l'ultimo resto non nullo è quindi $2x^2+2$

ma l'MCD deve essere monico $\rightarrow$ moltiplico per un invertibile: 4

4 inverso di 2, quindi X^2+1 è MCD

• IDENTITÀ DI BÉZOUT

abbiamo $\underbrace{X^4-2x^3-2x-1}_{Q} = \underbrace{(X+4)}_{\text{quoziente}}\underbrace{(X^3+X^2+X+1)}_{P} + \underbrace{2(X^2+1)}_{\text{resto}}$

trovare α, β in $\mathbb{F}_7$ t.c. $\alpha P + \beta Q = \delta = X^2+1$

$2(X^2+1) = Q-(X+4)P$ l'identità che abbiamo è buona, ma serve eliminare il 2 prima dell'MCD (2 è inv, moltiplichiamo per l'inverso)

$4\cdot 2(X^2+1) = 4Q-4(X+4)P$

$X^2+1 = 4Q+(3x+5)P$

COSTRUZIONI CANONICHE DI UN SOTTOGRUPPO

nota: un gruppo qualsiasi ha due sottogruppi evidenti:
- $\{1_G\}$
- sé stesso

0_G not. additiva

Lemma costruzione del kernel / nucleo

Sia $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi

$$H = \{ g \in G_1 : f(g) = 1_{G_2} \} = f^{-1}(\{1_{G_2}\}) \subset G_1$$

elementi di G_1 che puntano all'el. neutro di G_2

è un sottogruppo: $H < G_1$ si chiama NUCLEO di f e si scrive $H = Ker(f)$

dim: $a, b \in H$ con $f(a) = f(b) = 1_{G_2}$

$$f(ab^{-1}) = f(a) f(b^{-1}) = f(a) f(b)^{-1} = 1_{G_2} \overset{1_{G_2}}{\overset{\|}{1_{G_2}}}{}^{-1} = 1_{G_2} \quad \text{quindi } ab^{-1} \in H$$

(in H ci sono gli el. che puntano a 1_{G_2})

Lemma

Sia $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi

"kernel banale" è banale perché, per def. omomorfismo di gruppi, $f(1_{G_1}) = 1_{G_2}$

si ha che $Ker(f) = \{1_{G_1}\} \iff f$ è iniettiva

è il più piccolo sottogruppo di G_1 (HA DETTO CHE METTERÀ QUESTA DOMANDA NELLA PROVA IN ITINERE: L'INSIEME VUOTO NON PUÒ ESSERE UN GRUPPO)

dim

$\Longrightarrow$ Supponiamo $Ker(f) = 1_G$ $(= \{x \in G_1 : f(x) = 1_{G_2}\})$

Siano $x, x' \in G_1$ t.c. $f(x) = f(x') \underset{\text{divido}}{\iff} \underbrace{f(x) f(x')^{-1}}_{= f(x x'^{-1})} = 1_{G_2}$ (x omomorfismo)

$$\iff x(x')^{-1} \in Ker(f) = \{1_{G_1}\} \quad \text{quindi} \iff x(x')^{-1} = 1_{G_1}$$

molt. per x' $\quad x\underbrace{(x')^{-1} x'}_{1} = 1_{G_1} x' \iff x' = x \quad f$ iniettiva

$\Longleftarrow$ Supponiamo f iniettiva

Sia $x \in Ker(f)$. Allora $f(x) = 1_{G_2}$

Ma f è un omomorfismo di gruppi, da cui deduco $f(1_{G_1}) = 1_{G_2}$

Siccome $f(x) = f(1_{G_1}) = 1_{G_2}$ e f iniettiva, si deve avere $x = 1_{G_1} \Longrightarrow Ker(f) = \{1_{G_1}\}$

· costruzione del SOTTOGRUPPO IMMAGINE

$f: G_1 \longrightarrow G_2$ e f omomorfismo, $f(G_1) \subset G_2$

$f(G_1) < G_2 = \{ y \in G_2 : \exists x \in G_1$ con $f(x) = y \}$ è il sottogruppo immagine.

dim (sottogruppo)

devo dimostrare che se $y, y' \in f(G_1)$, allora $y(y')^{-1} \in f(G_1)$

$\exists\, x, x' \in G_1$ t.c. $f(x) = y$, $f(x') = y'$

$$y(y')^{-1} = f(x)f(x')^{-1} \underset{\text{omomorfismo}}{=} f(x x'^{-1}) = f(z)$$

$$\exists\, z \in G_1 \text{ t.c. } f(z) = y(y')^{-1} \iff y(y')^{-1} \in f(G_1)$$

· costruzione dei SOTTOGRUPPI CONIUGATI

G gruppo. Scegliamo $H < G$ e $g \in G$

definisco $H^g := \{ g' \in G$ t.c. $\exists\, h \in H$ t.c. $g' = g^{-1}hg \} = g^{-1}Hg$ notazione semplificata

OSSERVAZIONE. se G abeliano $H^g = H$ $\forall g$ $\left(g' = g^{-1}hg \iff g' = \underbrace{g^{-1}g}_{1}h \iff g' = h \right)$

Lemma: $H^g < G$

$$\boxed{\text{In generale, } gH,\ Hg,\ Hg^{-1},\ g^{-1}H \not< G}$$

dim dati $a, b \in H^g$

$a = g^{-1}a'g$ $\exists a' \in H$, $b = g^{-1}b'g$ $\exists b' \in H$

$\cdot\, b^{-1} = (g^{-1}b'g)^{-1} = g^{-1}b'^{-1}g$ inversione in G: $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$

$ab^{-1} = g^{-1}a'\cancel{g} \cdot \cancel{g^{-1}}(b')^{-1}g = g^{-1}\underbrace{a'(b')^{-1}}_{\in H}g \implies ab^{-1} \in H^g\ \forall a, b \in H^g \implies H^g < G$

$\in H$ perché $H < G$

dim alternativa

Definiamo, dato $g \in G$, un'applicazione $G \xrightarrow{f_g} G$, $x \longrightarrow f_g(x) = g^{-1}xg$

osserviamo che $\forall g$, f_g è un omom di gruppi (si parla di endomorfismo ($G \to G$))

per verificarlo devo mostrare che $\forall a, b \in G$, $f(ab^{-1}) = f_g(a)f_g(b^{-1})$

$$f_g(a)f_g(b^{-1}) = g^{-1}ag(g^{-1}bg)^{-1} = g^{-1}a\cancel{g} \cdot \cancel{g^{-1}}b^{-1}(g^{-1})^{-1} = g^{-1}ab^{-1}g = f_g(ab^{-1})$$

Questo dimostra perché: $H < G_1$ e se $G_1 \xrightarrow{f} G_2$ omomorfismo allora $f(G_1) < G_2$

Se $G_1 = G_2 = G$ e $f = f_g$ ottengo $\forall H < G$, $f_g(H) < G$ $\quad (f_g(H) = g^{-1}Hg = H^g)$ $\implies H^g < G$ ■

PERMUTAZIONI

GRUPPI DI PERMUTAZIONI

dato $\mathcal{E}$ insieme finito, sia $S(\mathcal{E}) = \{ f : \mathcal{E} \to \mathcal{E} : f \text{ biiettiva} \}$ — elementi chiamati permutazioni

- Su $S(\mathcal{E})$ esiste l'operazione di composizione di applicazioni: $\mathcal{E} \xrightarrow{f} \mathcal{E} \xrightarrow{g} \mathcal{E}$, $g \circ f$, e se $f, g \in S(\mathcal{E})$ (biiett.), allora $g \circ f \in S(\mathcal{E})$

Inoltre, $(g \circ f)^{-1} = f^{-1} \circ g^{-1} \implies (S(\mathcal{E}), \circ, Id_{\mathcal{E}})$ è un gruppo.

perché
① $f \circ (g \circ h) = (f \circ g) \circ h$ — $\circ$ è associativo
② $f \circ Id = Id \circ f = f \quad \forall f \in S(\mathcal{E})$ — el neutro $\circ$
③ $\forall f \in S(\mathcal{E})$ invertibile e $f \circ f^{-1} = f^{-1} \circ f \in S(\mathcal{E})$ — inverso per $\circ$

- Sia $\mathcal{E} = \{1, \dots, n\} =: I_n \quad n \geq 1$ allora si scrive $S_n = S(I_n) = S(\mathcal{E})$

  - ogni elemento di S_n, $f \in S_n$ può essere identificato con un diagramma: $\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow \\ f(1) & f(2) & f(3) & f(4) & \dots & f(n) \end{pmatrix}$

    che si può anche rappresentare non "in ordine" con frecce: $\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ f(2) & f(3) & f(4) & f(1) & & f(n) \end{pmatrix}$

def n-ciclo

Una permutazione del tipo $\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{s-1} & a_s \\ | & | & | & & | & | \\ a_2 & a_3 & a_4 & \dots & a_s & a_1 \end{pmatrix}$ con $a_1, a_2 \dots a_s \in I_n \ (s \leq n)$ distinti, che fissa (manda a sé stessi) tutti gli elementi che non appartengono a $\{a_1 \dots a_s\}$ (e manda quelli di $\{a_1 \dots a_s\}$ in maniera ciclica es: $a_1 \to a_2$, $a_2 \to a_3$, $a_3 \to a_1$)

il ciclo si vede meglio così imo

$\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{s-1} & a_s \\ a_1 & a_2 & a_3 & a_4 & \dots & a_s \end{pmatrix}$

$\begin{pmatrix} a_1 & a_2 & \dots & a_{s-1} & a_s & a_{s+1} & a_{s+2} \\ a_1 & a_2 & a_3 & \dots & a_s & a_{s+1} & a_{s+2} \end{pmatrix}$

$\notin \{a_1 \dots a_s\}$ e sono fissati

$\in \{a_1 \dots a_s\}$ e sono "ciclici"

si chiama s-ciclo e si scrive $(a_1\, a_2 \dots a_s)$

term: dato un ciclo $(a_1\, a_2 \dots a_s)$, la sua orbita è $\{a_1, a_2, \dots, a_s\}$ (insieme di el. permutati tra loro)

N.B rispetto alla notazione: è $(a_1\, a_2\, a_3 \dots a_s)$ e rispetta l'"ordine" del ciclo

si può shiftare: $(a_s\, a_1\, a_2 \dots a_{s-1})$ ma non rimescolare: $\neq (a_1\, a_3\, a_2 \dots a_s)$

esempi: in S_2: $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\,2)$ è un 2-ciclo   in S_3: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$ 3-ciclo   in S_5: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = (1\,3\,5)$ 3-ciclo

TERMINOLOGIA: tutti i 2-cicli si chiamano trasposizioni

OSS: l'identità è uno $\emptyset$-ciclo

- tutti i cicli sono permutazioni, ma esistono permutazioni che non sono cicli

es. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix}$ non è un ciclo seguendo le $\to$, vedo $1 \to 2$, $2 \to 5$, $5 \to 1$ sono "cicliche", ma le altre non sono fissate: $3 \to 6$, $6 \to 3$ ...

(anche guardando $3 \to 6$, $6 \to 3$ stesso discorso: $1 \to 2$, $2 \to 5$, $5 \to 1$ non fissate)

INVERSIONE

qualsiasi di questi va bene

$$\begin{pmatrix}1&2&3&4&5&6&7\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 4&6&7&5&1&3&2\end{pmatrix}^{-1} = \begin{pmatrix}1&2&3&4&5&6&7\\ \uparrow&\uparrow&\uparrow&\uparrow&\uparrow&\uparrow&\uparrow\\ 4&6&7&5&1&3&2\end{pmatrix} = \begin{pmatrix}4&6&7&5&1&3&2\\ 1&2&3&4&5&6&7\end{pmatrix} = \begin{pmatrix}1&2&3&4&5&6&7\\ 5&7&6&1&4&2&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6&7\\ 1&2&3&4&5&6&7\end{pmatrix}^{-1} = \begin{pmatrix}1&2&3&4&5&6&7\\ 1&2&3&4&5&6&7\end{pmatrix}$$

OSS: nella notazione semplificata di un ciclo $(a_1\, a_2 \dots a_s)$, l'inverso si ottiene leggendo da destra a sinistra:
$$(a_1\, a_2 \dots a_s)^{-1} = (a_s \dots a_3\, a_2\, a_1)$$

COMPOSIZIONE (possiamo chiamarla anche "prodotto")

$$\sigma = \begin{pmatrix}1&2&3&4&5\\ 3&1&4&2&5\end{pmatrix} = (1\,3\,4\,2) \in S_5 \quad , \quad \tau = \begin{pmatrix}1&2&3&4&5\\ 5&4&2&1&3\end{pmatrix} = (1\,5\,3\,2\,4) \in S_5$$

$\sigma \circ \tau = \sigma \cdot \tau = \sigma\tau$ composizione $\to$ agisce prima τ

OSS: il prodotto di cicli non è necessariamente un ciclo

$$\sigma \circ \tau = \begin{pmatrix} & 1&2&3&4&5\\ \tau & \mid&\mid&\mid&\mid&\mid\\ & 5&4&2&1&3\\ \sigma & \mid&\mid&\mid&\mid&\mid\\ & 5&2&1&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\ 5&2&1&3&4\end{pmatrix} = (5\,4\,3)$$

$\neq \implies S_5$ non è commutativo!

$$\tau \circ \sigma = \begin{pmatrix}1&2&3&4&5\\ 3&1&4&2&5\\ 2&5&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\ 2&5&1&4&3\end{pmatrix} = (1\,2\,5\,3)$$

Descrizione di S_3

$\# S_3 = 6 = 3 \cdot 2 \cdot 1$ (fattoriale)

$$\left\{ \begin{pmatrix}\boxed{1}&2&3\\ \boxed{1}&2&3\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{1}&3&2\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{2}&1&3\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{2}&3&1\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{3}&1&2\end{pmatrix}, \begin{pmatrix}\boxed{1}&2&3\\ \boxed{3}&2&1\end{pmatrix} \right\} =$$

$$= \{ Id, (2\,3), (1\,2), (1\,2\,3), (1\,3\,2), (1\,3) \}$$ in S_3, ogni permutazione è un s-ciclo con $s = 0, 2, 3$

- Qual è il più piccolo n t.c. in S_n esiste una permutazione che non è un ciclo?

$n = 4$. infatti, $(12)(34) =$ elemento per elemento

notazione funzioni: come $(f \circ g)(x)$

$$((12)(34))(1) = (12)((34)(1)) = (12)(1) = 2$$
$$((12)(34))(2) = (12)(2) = 1$$
$$((12)(34))(3) = (12)(4) = 4$$
$$((12)(34))(4) = (12)(3) = 3$$

quindi $(12)(34) = \begin{pmatrix}1&2&3&4\\ 2&1&4&3\end{pmatrix}$ non è un ciclo

es mostrare che $(123)^{-1} = (132)$ $(=(321)\dots)$ $\longrightarrow$ $(123) = \begin{pmatrix}1&2&3\\ 2&3&1\end{pmatrix}$ $\quad (123)^{-1} = \begin{pmatrix}1&2&3\\ \uparrow&\uparrow&\uparrow\\ 2&3&1\end{pmatrix} = (1\,3\,2)$

def CICLI A SUPPORTI DISGIUNTI

Dati due cicli $(a_1 \dots a_s)$ e $(b_1 \dots b_s)$ di S_n, si dice che sono a supporti disgiunti se $\{a_1, \dots, a_s\} \cap \{b_1, \dots, b_s\} = \emptyset$

Più generalmente, dati r cicli, $c_1, \dots, c_r$ di S_n sono a supporti disgiunti

es. $(1\,2)$, $(3\,4)$ sono a supp. disg. in S_4

TEOREMA (decomposizione di permutazioni)

Ogni $\sigma \in S_n$ può essere decomposto in prodotto di cicli a supporti disgiunti.

Inoltre, tali cicli sono unicamente determinati e commutano tra di loro.

C'è analogia con il TFA.

esempio

x "estrarre" cicli:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 7 & 3 & 8 & 1 & 5 \end{pmatrix}$$

parto da un el

$1 \to 2 \to 4 \to 7 \to 1$

$(1\,2\,4\,7)$

non ha senso prendere un el da qui → si parte da un altro

prendo il 3

$3 \to 6 \to 8 \to 5 \to 3$

$(3\,6\,8\,5)$

i due cicli sono disgiunti

$\sigma = (1247)(3685) =$

$= (3685)(1247)$

Sia G gruppo (in not. moltiplicativa) e $H < G$.

Introduciamo una relazione $\sim$ su G:

dati $x, x' \in G$ $\quad x \sim x' \iff x(x')^{-1} \in H$

Lemma: $\sim$ è di equivalenza

dim: ① RIFLESSIVITÀ: $\qquad x \sim x \quad \forall x \in G$

$H < G \Longrightarrow \underset{(1_H = 1_G)}{1_G \in H}$. Ma $1_G = xx^{-1} \; \forall x \in G$, quindi $x \sim x \quad \forall x \in G$

② SIMMETRIA: $\qquad x \sim x' \Longrightarrow x' \sim x \quad \forall x \in G$

$x \sim x' \iff x(x')^{-1} \in H$

Ma $\forall h \in H$, $h^{-1} \in H$ (propr. sottogr.). Quindi $(x(x')^{-1})^{-1} = x'x^{-1} \in H$

③ TRANSITIVITÀ: $\qquad x \sim x', \; x' \sim x'' \Longrightarrow x \sim x'' \quad \forall x, x', x'' \in G$

Supponiamo $x \sim x'$ e $x' \sim x''$. Allora $x(x')^{-1}$, $x'(x'')^{-1} \in H$

Se $a, b \in$ sottogruppo: anche il loro prodotto $\in$ sottogruppo $\qquad x\underbrace{(x')^{-1}x'}_{1_G}(x'')^{-1} = x(x'')^{-1} \in H$

quoziente su $\sim$ dove: due el. x e x' sono nella stessa classe se $x(x')^{-1} \in H$

Domanda: È possibile costruire su $G/_\sim$ un'operazione binaria in modo tale che $G/_\sim$ acquisisca una struttura di gruppo?

Talvolta sì, talvolta no. Servono delle condizioni:

- Vorremmo che questa identità fosse valida per la nuova operazione:

$$[x] \overset{\text{nuova op.}}{*} [x'] = [\underset{\text{vecchia op. di } G}{x \cdot x'}] \qquad \text{indipendentemente dai rappresentanti}$$

Supponiamo $x \sim y$ e $x' \sim y'$.

$x \sim y \iff [x] = [y] \iff x(y)^{-1} \in H$

$x' \sim y' \iff [x'] = [y'] \iff x'(y')^{-1} \in H$

è necessario innanzitutto che $[xx'] = [yy']$ ovvero $xx'(yy')^{-1} \in H$

$$xx'(yy')^{-1} = x\underbrace{x'(y')^{-1}}_{\text{per ipotesi}, \in H} y^{-1}$$

sappiamo quindi che un pezzo del prodotto $\in H$, ci serve una condizione per cui tutto il prodotto $\in H$

def SOTTOGRUPPO NORMALE

H è un sottogruppo normale di G se, $\forall x \in G$, $xH = Hx$

- Si scrive $H \triangleleft G$

quindi, per la formula di prima: $xHy^{-1} = x\underbrace{y^{-1}H}$ $\in H$ per ipotesi, quindi tutto $\in H$ (quindi $[xx'] = [yy']$)

Condizioni equivalenti (per H sottogr. normale)

ricordiamo: $g^{-1}Hg$

① $H \triangleleft G$ $(gH = Hg)$ $\quad$ ② $\forall g \in G$ e $\forall h \in H$, $\exists h' \in H$ t.c. $gh = h'g$ $\quad$ ③ $\forall g \in G$, $H^g = H$

OSS: G abeliano e $H < G \Longrightarrow H \triangleleft G$ (tutti i sottogruppi di un gruppo abeliano sono normali)

ESEMPI (notevoli):

- $\mathbb{Z}$ gruppo abeliano in not. add. e $\forall n \in \mathbb{N}^*$, $n\mathbb{Z}$ è un sottogr. di $\mathbb{Z}$. $n\mathbb{Z} \triangleleft \mathbb{Z}$ e posso costruire, sempre in not. add., $\mathbb{Z}/_{n\mathbb{Z}}$ (coincide con la costruzione già vista in aritmetica modulare)
- dato G qualsiasi, ho $G \triangleleft G$ $\quad (\forall x \in G,\; xG = Gx$ e $G/_G = \{G\})$
- anche $\{1_G\} \triangleleft G$ $\quad (\forall x \in G,\; x1_G = 1_Gx = x$ e $G/_{1_G} = \{\{g\} : g \in G\}$ rel. di uguaglianza

dim condiz. equivalenti: basta mostrare che $(3) \Longrightarrow (1) \Longrightarrow (2) \Longrightarrow (3)$ (ordine scelto per facilità di dimostrazione)

- $(3) \Longrightarrow (1)$ ipotesi: $H^g = H$ devo dim: $gH = Hg$

se $H^g = H$, $g^{-1}Hg = H \overset{\text{molt. per } g \text{ a sx}}{\Longleftrightarrow} \underbrace{gg^{-1}}_{1_G}Hg = gH \Longleftrightarrow Hg = gH$

- $(1) \Longrightarrow (2)$ ipotesi: $gH = Hg$ devo dim: $gh = h'g$

se $\forall g$, $gH = \{x \in G : \exists h \in H \text{ con } x = gh\} = Hg = \{y \in G : \exists h' \in H \text{ con } y = h'g\}$
allora $\exists h, h' \in H$ t.c. $x = gh = h'g$

- $(2) \Longrightarrow (3)$ ipotesi: $gh = h'g$ devo dim: $H^g = H$

se $\forall g \in G$, $\forall h \in H$ si ha $gh = h'g$ $\exists h' \in H$, allora $\overset{\text{molt. per } g^{-1} \text{ a sx}}{\Longrightarrow} \underbrace{g^{-1}g}_{1_G}h = g^{-1}h'g \Longleftrightarrow h = g^{-1}h'g$ ($\forall h$) quindi, $\forall g$, $H^g = H$ ■

se ogni el. h si può scrivere così (come def. coniugato), vuol dire che l'insieme dei coniugati è H stesso

Teorema

Dati $H \triangleleft G$, $\sim$ di eq.

Allora l'operazione su $G/\sim$ $[x][x'] = [xx']$ (ben posta) definisce una struttura di gruppo su $G/\sim$.

(mia spiegazione, non Pellarin)
$[g]$ contiene tutti gli el. x t.c. $gx^{-1} \in H$.
quindi, $gx^{-1} = h \Longleftrightarrow g = hx \Longleftrightarrow h^{-1}g = x$
Ma H è chiuso rispetto all'inverso, quindi $h^{-1} \in H$.
Quindi tutti gli el. $x \in [g]$ si possono scrivere come gh, $h \in H$ (quindi gH)

mio ragionamento: che poi, per simmetria, visto che $x \in [g]$, $g \sim x \Longrightarrow x \sim g$ quindi $xg^{-1} = h'$ $\Longleftrightarrow x = gh'$ e, sostituendo, $g = h(gh')$ $\Longleftrightarrow 1 = hh'$ $h' = h^{-1}$?? credo di poterlo fare! if so, cool!

- si scrive $G/\sim\ = G/H$ gruppo quoziente di G per H
- osserviamo inoltre $[g] = gH = Hg$ non è vero che $gh = hg$ ma $\forall h\ \exists h'$ t.c. $gh = h'g$ quindi $gH = Hg$
- l'elemento neutro è $1_{G/H} = H$
- gli elementi di G/H (sottoinsiemi di G) sono le classi laterali di H

Lemma:

L'applicazione $G \xrightarrow{\pi_H} G/H$, $g \longmapsto [g]$ è un omomorfismo di gruppi suriettivo

dim:

- la suriettività di π_H è chiara, perché ogni classe contiene un rappresentante
- inoltre, $\pi_H\left(g\,(g')^{-1}\right) = \left[g\,(g')^{-1}\right] = [g]\left[(g')^{-1}\right] = \pi_H(g)\,\pi_H(g^{-1})$ ■

Lemma

Dato $G_1 \xrightarrow{f} G_2$ omomorfismo di gruppi

Allora, $\underbrace{Ker(f)}_{=\text{"}H\text{"}} \triangleleft G_1$ (el. di G_1 che puntano a 1_{G_2}). Inoltre, se $H \triangleleft G$, allora $H = Ker(\pi_H)$

dim:

- $Ker(f) \triangleleft G_1$ (so già che $< G_1$) mostriamo che $Ker(f)^g = Ker(f)$ (def. equivalente ③ di $\triangleleft$)

prendiamo $h \in G_1$ t.c. $f(h) = 1_{G_2}$ ($\Longleftrightarrow h \in Ker(f)$)

allora si ha che $\forall x \in G_1$, $f(x^{-1}hx) \overset{\text{omom.}}{=} f(x^{-1})\overbrace{f(h)}^{=1_{G_2}}f(x)$
$\overset{\text{omom.}}{=} f(x)^{-1}f(x) = 1_{G_2}$

$$\Longleftrightarrow x^{-1}hx \in Ker(f)\ \forall h \in Ker(f), \forall x \in G \Longleftrightarrow Ker(f)^x = Ker(f)$$

- se $H \triangleleft G_1$, allora $H = Ker(\pi_H)$

Abbiamo $H \triangleleft G_1$ e poniamo $f = \pi_H$. Mostriamo che $H = Ker(\pi_H)$. Ma se $g \in G_1$ soddisfa $\pi_H(g) = 1_{G/H} = H \Longleftrightarrow gH = H \Longleftrightarrow g \in H$ ■

(spiegazione mia):
- $g \in H \Longrightarrow g \in Ker(\pi_H)$ se $g \in H$, $gH = H$. Quindi, $\pi_H(g) = H$ ($[g] = gH$). Quindi (visto $H = 1_{G/H}$) $g \in Ker(\pi_H)$
- $g \in Ker(\pi_H) \Longrightarrow g \in H$ se $g \in Ker(\pi_H)$, $\pi_H(g) = 1_{G/H} = H$. Quindi, $gH = H$. $gH = H \Longleftrightarrow g \in H$

Consideriamo un omomorfismo di gruppi: $G_1 \longrightarrow G_2$. Per il teorema di struttura delle applicazioni,

$$\begin{tikzcd} G_1 \arrow[r, "f"] \arrow[d, "\pi"'] & G_2 \\ G_1/R \arrow[r, "\varphi"] & f(G_1) \arrow[u, "i"'] \end{tikzcd}$$

$g \mapsto [g]$; i identità

$[g] \longmapsto f(g)$

(è biiettiva: se $[g]=[g']$ allora $f(g)=f(g')$)

$$f = i \circ \varphi \circ \pi$$

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 $\underbrace{f(g) = f(g')}_{g R g' \text{ (x def.)}} \overset{\text{(divido per } f(g')\text{)}}{\iff} f(g)f(g')^{-1} = 1_{G_2}$ (π omomorfismo di gruppi, $\sim$ e R stessa relazione)

ma $f(g)f(g')^{-1} = f(g(g')^{-1})$ (x omom. gruppi)

quindi $f(g(g')^{-1}) = 1_{G_2} \iff g(g')^{-1} \in Ker(f)$ (ricordiamo: el. che portano a 1_{G_2})

$\iff g \sim g'$ ($\sim$ è definita come, dati G gr., $H < G$ 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.

Si ha quindi $G/R = G/H$ – che è un gruppo, quindi G/R gruppo e π omomorfismo di gruppi. (come abbiamo visto nel Lemma qui)

(sappiamo chiaramente che l'identità è un omomorfismo di gruppi).

- $H = Ker(f)$. Mostriamo che $\varphi: G_1/H \longrightarrow f(G_1)$: $\varphi(gH) = f(g)$ è un omomorfismo di gruppi. ($G_1/H = G_1/R = G_1/\sim$; $[g] = gH$)

Vogliamo mostrare che, $\forall g, g' \in G_1$, si ha: $\varphi(\underset{=Hg}{gH})\,\varphi((g'H)^{-1}) = \varphi(g(g')^{-1}H)$

Ma $\varphi(gH(g'H)^{-1}) = \varphi(gHH(g')^{-1}) \overset{HH=H}{=} \varphi(gH(g')^{-1}) = \varphi(g(g')^{-1}H) = f(g(g')^{-1}) = f(g)f(g')^{-1} = \varphi(gH)\varphi(g'H)^{-1}$

ovvero quello che cercavamo

posso "commutare" H liberamente anche se l'op non è commutativa

$\varphi: [g] \longmapsto f(g)$; f omom.

$(g'H)^{-1} = (g')^{-1}H$ perché:

$\{(g'h)^{-1} : h \in H\}$

$= \{h^{-1}(g')^{-1} : h \in H\}$ ma l'inversione è una biiezione e, se poniamo $h^{-1} = h'$,

$= \{h'(g')^{-1} : h' \in H\}$ – stiamo "prendendo" tutte le h di H, solo in un ordine diverso

- Si può vedere anche come $g'H = [g']$ quindi $(g'H)^{-1} = [g']^{-1}$

Abbiamo dimostrato il PRIMO TEOREMA DI ISOMORFISMO PER I GRUPPI:

dato $f: G_1 \longrightarrow G_2$ omomorfismo di gruppi, esso si decompone

in composizione: $f = \underbrace{i \circ \varphi \circ \pi}_{\text{tutti omomorfismi di gruppi}}$

Altre proprietà dei gruppi:

Lemma l'intersezione di sottogruppi è un sottogruppo

Dati $H_1, \dots, H_n < G$, 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)

Lemma 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 $(12), (13) \in G$ e $\in H$ ma $(12)(13) = (1,3,2) \notin H_1 \cup H_2$ (non è chiuso rispetto alla sua operazione, $\circ$) quindi non è un sottogruppo

def SOTTOGRUPPO GENERATO

Consideriamo $\overset{\neq \emptyset}{I} \subset G$. Il sottogruppo di G generato da I è:

$$\langle I \rangle := \bigcap_{\substack{H < G: \\ I \subset H}} H$$

(quindi si prendono tutti i sottogruppi di G che contengono I e si intersecano)

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 (not. moltiplicativa) e $g \in G$, $\overset{\langle \{g\} \rangle}{\overset{\|}{\langle g \rangle}} = \bigcap_{\substack{H < G \\ g \in H}} H$

esempio

i sottogruppi di S_3 sono:

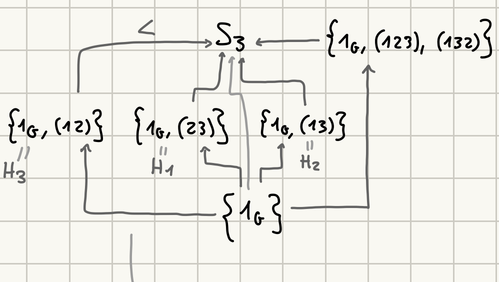


diagramma di Hasse

Quindi $\langle (1\ 2) \rangle = \{1_G, (12)\} = H_3$

$\langle (13) \rangle = \{1_G, (13)\} = H_2$

$\langle (23) \rangle = \{1_G, (23)\} = H_1$

$\langle (123) \rangle = \{1_G, (123), (132)\} \cap S_3 = \{1_G, (123), (132)\}$

$\langle H_1 \cup H_2 \rangle = S_3$

$H_1 \cup H_2 = \{1_G, (13), (23), \overset{(23)(13)}{(132)}, \overset{(13)(23)}{(123)}, \underset{(23)(13)(23)}{(12)}\} = S_3$ (i prodotti ci sono per chiusura rispetto a $\circ$)

Sottogruppo $g^{\mathbb{Z}}$

- Consideriamo l'insieme $\{1, g, g^2, \dots, g^{-1}, g^{-2}, \dots\} = \{g^n : n \in \mathbb{Z}\} = g^{\mathbb{Z}} \subset G$

Allora si ha che $g^{\mathbb{Z}} < G$. Infatti, $\forall x, x' \in g^{\mathbb{Z}}$, $\exists\, n, n' \in \mathbb{Z}$ t.c. $x = g^n$, $x' = g^{n'}$ e $x(x')^{-1} = g^{\overbrace{n-n'}^{n''}} \in g^{\mathbb{Z}}$

Si ha che $<g> \subset g^{\mathbb{Z}}$. (perché $<g>$ è un sottogr, quindi è chiuso rispetto a inverso e prodotto, quindi visto che contiene g, contiene anche g^{-1} e tutte le potenze generate ($g^{\mathbb{Z}}$))

Dato che $<g> < G$, e $g \in <g>$, $1 = g^0 \in <g>$, $g^{-1} \in <g>$ e gli altri sono generati dal prodotto di questi ... si ha anche $g^{\mathbb{Z}} \subset <g>$

Lemma $\underline{<g> = g^{\mathbb{Z}}}$.

Lemma SOTTOGRUPPI DI $\mathbb{Z}$

Sia G un sottogruppo di $\mathbb{Z}$ (in not. additiva),
se $G \neq \{0\}$, allora $\exists\, n \in \mathbb{N}^*$ t.c. $G = n\mathbb{Z}$

(tutti i sottogruppi di $\mathbb{Z}$ sono o $\{0\}$ o $n\mathbb{Z}$)
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) (per i negativi, G è stabile per l'inverso $x \longmapsto -x$)
tale che, preso $d \in G$ (per div. euclidea) $d = qn + r$ con $0 \leq r < n$.

Quindi $r = \underbrace{d}_{\in G} - \underbrace{qn}_{\in G \text{ perché } n \in G}$. Se $r \neq 0$, si avrebbe $r < n$ e $r \in G \cap \mathbb{N}^*$ (impossibile perché n è il minimo su $G \cap \mathbb{N}^*$, ma allo stesso tempo $r < n$ e $r \neq 0$)
contraddizione con la minimalità di n.
Quindi $r = 0$, e $d \in n\mathbb{Z}$.
Quindi, $G \subset n\mathbb{Z}$. Ma $G \supset n\mathbb{Z}$, perciò $G = n\mathbb{Z}$
perché G è chiuso rispetto alla somma, quindi contiene tutti gli $n\mathbb{Z}$ (?)

Lemma

Se G è un gruppo finito (in notazione moltiplicativa),
allora, $\forall g \in G$, $\exists\, n > 0$ t.c. $<g> = g^{\mathbb{Z}} \cong \mathbb{Z}/_{n}\mathbb{Z}$
isomorfo a — not. additiva

dim:

$f: \mathbb{Z} \longrightarrow G$
$n \longmapsto g^n \in g^{\mathbb{Z}} = <g>$

non può essere iniettiva, perché $\mathbb{Z}$ è infinito e G è finito

f è omomorfismo perché $f(n-n') = g^{n-n'} = g^n g^{-n'} = f(n)\, f(n)^{-1}$

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "f"] \arrow[d, "\pi"'] & G \\ \mathbb{Z}/\mathrm{Ker}(f) \arrow[r, "\varphi", "\cong"', leftrightarrow] & f(\mathbb{Z}) = g^{\mathbb{Z}} = g \arrow[u, "i"'] \end{tikzcd}$$

(x 1o teor. iso : $f = i \circ \varphi \circ \pi$)

$< \mathbb{Z}$, quindi: o è $\{0\}$, o è $n\mathbb{Z}$.
Ma se fosse $\{0\}$, allora $\mathbb{Z}/_0 \overset{1:1}{\cong} \mathbb{Z}$ e f sarebbe iniettiva (non può esserlo) - vedi sopra -
Quindi, $\mathrm{Ker}(f) = n\mathbb{Z}$ $\exists\, n \in \mathbb{N}^*$

def ORDINE DI UN ELEMENTO

Sia G gruppo finito (not. molt.), e $g \in G$.
Allora $\{d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G\} \neq \emptyset$ (perché è contenuto in $\mathrm{Ker}(f)$)

Si pone $\mathrm{ord}(g) = \min\{d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G\}$ il minimo numero di volte per cui bisogna moltiplicare g per se stesso per ottenere 1_G

Si ha allora $<g> \cong \mathbb{Z}/_{\mathrm{ord}(g)}\mathbb{Z}$

esempio: $g = (123) \in S_3 =: G$

$\mathbb{Z} \longrightarrow S_3$
$n \longrightarrow (123)^n$

n	$(123)^n$
0	1_{S_3}
1	(123)
2	(132)
3	1_{S_3}
4	(123)

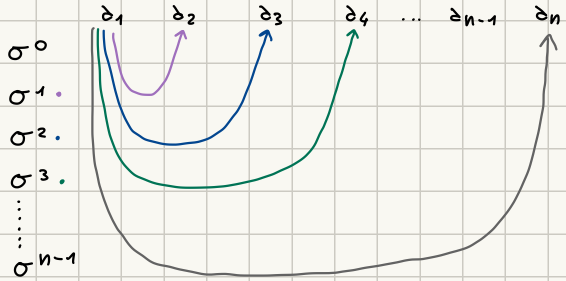
$\mathrm{ord}(123) = 3$ (va elevato al cubo per arrivare a 1_G)

$<(123)> \cong \mathbb{Z}/_{3}\mathbb{Z}$ $= \{1_{S_3}, (123), (132)\}$

ORDINE DI UN CICLO

Più generalmente, dato un n-ciclo di S_r $\sigma := (a_1\ a_2 \dots a_n)$

$$\mathrm{ord}(\sigma) = n \quad e \quad \langle\sigma\rangle \cong \mathbb{Z}/_{n\mathbb{Z}}$$



(non l'ha detto, trovato su internet)

$\sigma = (a_1 a_2 \dots a_k)$ allora, $\forall k$ $\sigma^k(a_i) = a_{(i+k-1) \bmod n+1}$

quindi $\sigma^i \neq 1_{S_r}$ $\forall i = 1, \dots, n-1$

Inoltre $\sigma^n(a_1) = a_1$. Ma noi possiamo scrivere σ "scalando", e trasformare a_2 in a_1 : $(a_2\ a_3 \dots a_n\ a_1)$

Quindi, $\sigma^n(a_2) = a_2$. Più generalmente, $\sigma^n(a_i) = a_i$ $\forall i = 1 \dots n$

Siccome σ è un ciclo, esso fissa tutti gli el. $b \in \{1, \dots, r\} \setminus \{a_1 \dots a_n\}$.

Quindi, $\sigma^n = 1_{S_r}$ da cui $n = \mathrm{ord}(\sigma)$.

Abbiamo dimostrato

Lemma ORDINE DI UN CICLO

Se σ è un n-ciclo, allora

$$\mathrm{ord}(\sigma) = n \quad e \quad \langle\sigma\rangle \cong \mathbb{Z}/_{n\mathbb{Z}}$$

14/11 [qui a lezione ha fatto un breve recap - omesso]

def MINIMO COMUNE MULTIPLO

dati $m_1, \dots, m_l \in \mathbb{Z} \setminus \{0\}$

il minimo comune multiplo m di $m_1, \dots m_l$ è l'unico intero $m \in \mathbb{N}^*$ t.c.

1. $m_1, \dots, m_l \mid m$
2. se m' è t.c. $m_1, \dots, m_l \mid m'$, 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 la stessa cosa ma con il $+$ $(m_1\mathbb{Z} + m_2\mathbb{Z} + \dots + m_l\mathbb{Z} = d\mathbb{Z})$

- in più, $\underset{a,b \in \mathbb{N}^*}{\text{mcm}(a,b)} = \dfrac{ab}{\text{MCD}(a,b)}$

- utilizzando il teorema fond. aritmetica: $a = \prod_p p^{v_p(a)}$, $b = \prod_p p^{v_p(b)}$

  allora $\text{mcm}(a,b) = \prod_p p^{\max(v_p(a), v_p(b))}$ 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 decompone in modo unico in un prodotto di cicli disgiunti $c_1, \dots, c_s$ che commutano tra loro.

Quindi: sia $\sigma \in S_n$ - lo decomponiamo in prodotto di cicli disgiunti: $\sigma = c_1 \dots c_s$

Lemma: $\text{ord}(\sigma) = \text{mcm}(\text{ord}(c_1), \dots, \text{ord}(c_s))$

esempio

Calcolare $\text{ord}(\sigma)$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} \in S_n \quad n \geq 7$$

(se $\in S_n > 7$, gli altri el. sono fissati)

1. Decomponiamo σ in prodotto di cicli disgiunti

$$1 \; 2 \; 3 \; 4 \; 5 \; 6 \; 7 = \underset{\text{ord } 2}{(17)} \; \underset{\text{ord } 2}{(24)} \; \underset{\text{ord } 2}{(56)}$$

((3) si può omettere)

2. $\text{ord}(\sigma) = \text{mcm}(2, 2, 2) = 2$

metodo alternativo: sfrutto il fatto che $\text{ord}(\sigma) = $ min. esponente >0 a cui elevare σ per avere l'identità

(3 omesso perché fissato)

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 4 & 5 & 6 & 7 \\ 7 & 4 & 2 & 6 & 5 & 1 \\ 1 & 2 & 4 & 5 & 6 & 7 \end{pmatrix} = 1_{S_n} \quad (n \geq 7)$$

sia perché $\text{ord} = 2$ (quindi $\sigma^2 = 1$) e sia per il "trucco" di leggerla al contrario: $(17) = (71)$

l'inverso di una trasposizione è essa stessa

del tipo $abcc^{-1}b^{-1}a^{-1} = 1$

Si può vedere anche così $\sigma^2 = (17)(24)(56)(17)(24)(56) \overset{\text{commut.}}{=} (17)(24)(56)(56)(24)(17) = 1_{S_n} \quad (n \geq 7)$

(uno alla volta "collassano" nell'identità: $(56)(56) = 1_S$, $(17)(24)(24)(17)$ ecc.)

esercizi:

- trovare α, β t.c. $(147)(132)\,\alpha\,\beta = 1_G$

  $\alpha = (132)^2 = (132)(132) = (123)$ oppure $\alpha = \overleftarrow{(132)} = (231) = (123)$

  $\beta = (147)^2 = (174)$

- trovare α, β in S_8 t.c. $(1234)(137)\,\alpha\beta = 1_{S_8}$ $\alpha = (137)^2$, $\beta = (1234)^3$

- $\text{ord}\big((12)(345)\big) = 6$

- $\text{ord}\big((12)(245)\big) = ?$ non sono a supporto disgiunto

  rendiamoli a supp. disg. $= \text{ord}\,(1245) = 4$

- $\text{ord}\big((12)(13)(14)\big) = \text{ord}\big((1432)\big) = 4$

Teorema (decomp. di permutazione in trasposizioni)

Ogni permutazione si decompone in prodotto di trasposizioni non necessariamente a supporto disgiunto.

- in generale, una tale fattorizzazione non è unica

esempio $(a_1 a_2)(a_1 a_3)(a_1 a_4) = (a_1 a_4 a_3 a_2)$

$\#\{a_1, a_2, a_3, a_4\} = 4$

FORMULA per un n-ciclo

$\sigma = (a_1 a_2 \dots a_n) = (a_n a_{n-1})(a_n a_{n-2}) \dots (a_n a_1)$ (ovvero $n-1$ fattori)*

in realtà $2\mathbb{Z} + n-1$, perché posso aggiungere quante identità voglio

esempio: $(12345) = (54)(53)(52)(51)$

Teorema "rinforzato" - SEGNATURA/SEGNO DI UNA PERMUTAZIONE

visto che $(a_1 a_2)(a_1 a_2) = 1_S$, aggiungere una coppia di trasposizioni (uguali) dà lo stesso risultato

Sia s il numero di trasposizioni in una fattorizzazione di $\sigma \in S_r$ in prodotto di trasposizioni.

Allora $s \bmod 2$ è unicamente determinato (anche se s non è unico)

non l'ha detto a lezione

Poniamo $\varepsilon_\sigma = (-1)^s \in \mathbb{Z}^\times$ è la segnatura di una permutazione. il segno

σ si dice pari se $\varepsilon = +1$; dispari se $\varepsilon = -1$

per *

$\boxed{\text{noto: se } \sigma \text{ n-ciclo, } \varepsilon(\sigma) = (-1)^{n-1}}$

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:

$$\begin{tikzcd} S \arrow[r, two heads, "\varepsilon"] \arrow[d, "\pi"'] & \mathbb{Z}^\times \\ S_r/\ker(\varepsilon) \arrow[ur, "\cong"'] & \end{tikzcd}$$

$\cong$ perché $\varepsilon(S_r) = \mathbb{Z}^\times$

$\ker(\varepsilon)$ contiene tutte le permutazioni che hanno segno pari (elementi di S_r che puntano a 1 per la funzione ε)

Quindi, questo quoziente divide le permutazioni in due classi: pari e dispari

COME CALCOLARE $\varepsilon(\sigma)$

metodo meno divertente

① si calcola la fattorizzazione di σ in prod. di cicli disgiunti

$\sigma = c_1 \dots c_m$

② $\varepsilon(\sigma) = \varepsilon(c_1) \cdot \dots \cdot \varepsilon(c_m)$

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

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 7 & 5 & 8 & 6 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$

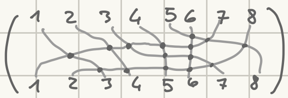
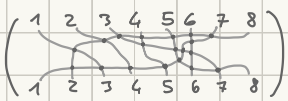
15 intersezioni

si dispongono i numeri in ordine e si tracciano le frecce che li uniscono (non ci devono essere incroci a 3)

si contano le intersezioni

$\varepsilon(\sigma) = (-1)^{15} = -1$

nota: quando conto le intersezioni, in base a come le disegno, avrò risultati diversi.
ma la classe mod 2 (parità) sarà sempre la stessa, quindi $\varepsilon(\sigma)$ non sarà inficiato.

es.  =  $\quad \varepsilon(\sigma) = (-1)^{15} = (-1)^{19} = -1$

15 $\qquad$ 19

- questo stesso esempio, ma con l'altra tecnica:

  $\sigma = (137)(2458)$

  $\varepsilon(\sigma) = \varepsilon(137) \cdot \varepsilon(2458) = (-1)^2 \cdot (-1)^3 = -1$

19/11

PRODOTTO CARTESIANO DI GRUPPI o PRODOTTO DIRETTO

dati G_1, G_2 in not. additiva.

$$G_1 \times G_2 = \{ (g_1, g_2) : g_1 \in G_1,\ g_2 \in G_2 \}$$

Definiamo su $G_1 \times G_2$ una struttura di gruppo come segue:

$(g_1, g_2), (g_1', g_2') \in G_1 \times G_2 \qquad$ operazione $+$: $(g_1, g_2) + (g_1', g_2') := (g_1 + g_1', g_2 + g_2')$

- associatività: $((g_1, g_2) + (g_1', g_2')) + (g_1'', g_2'') = (g_1 + g_1', g_2 + g_2') + (g_1'', g_2'') = (g_1 + g_1' + g_1'', g_2 + g_2' + g_2'') = (g_1, g_2) + ((g_1', g_2') + (g_1'', g_2''))$
- el neutro: $0_{G_1 \times G_2} = (0_{G_1}, 0_{G_2})$
  - $G_1 \times G_2$ è abeliano se G_1 e G_2 lo sono.

Questa operazione si estende a n gruppi $G_1, \dots, G_n$

Si può costruire $G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n)\}$ dotato di struttura di gruppo prodotto cartesiano di $G_1, \dots, G_n$ (e se $G_1, \dots, G_n$ abeliano allora $G_1 \times \dots \times G_n$ abeliano)

esempio $(\mathbb{R}, +)$

- posso costruire il gruppo $\mathbb{R}^n = \overbrace{\mathbb{R} \times \dots \times \mathbb{R}}^{n \text{ volte}}$ i cui elementi sono $(x_1, x_2, \dots, x_n)$ con $x_i \in \mathbb{R}$ $\forall i = 1, 2, \dots, n$

  l'elemento neutro è $0 = (0, \dots, 0)$

"esercizio 19"

Teorema di Lagrange

Sia G gruppo finito.

Sia $H < G$ ($\# H < \# G$ perché $< \implies \subset$)

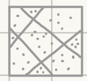
Allora:

$$\# H \mid \# G$$

dim.

Abbiamo, su G, una relazione di equivalenza associata ad H:

$$x \sim y \iff xy^{-1} \in H$$



se partiziono qualcosa di finito, ho un numero finito di porzioni finite a loro volta

Possiamo considerare l'insieme quoziente $G/\sim$ con $\# G/\sim \; < \infty$ (finito)

Poniamo $[G:H] = \# G/\sim$ $(= G/H)$

$[G:H]$: indice di H in G

Siccome $G/\sim$ è una partizione di G, $G = \bigsqcup_{c \in G/\sim} c$ $\longrightarrow$ quindi, $\# G = \sum_{c \in G/\sim} \# c$

Claim ①: $\# c = \# H$

[Se il claim è vero, abbiamo il teorema di Lagrange:

infatti, $\# G = \sum_{c \in G/\sim} \# c = \sum_{c \in G/\sim} \# H = \# H \underbrace{\sum_{c \in G/\sim} 1}_{\text{cardinalità di } G/\sim} = \# H \cdot [G:H]$ quindi $\# H \mid \# G$]

quindi $\# G = \# H \cdot$ un intero

Quindi, dobbiamo dimostrare che $\forall c \in G/\sim$, $\# c = \# H$

Claim ②

$\forall g \in G$, poniamo $\varphi_g : G \longrightarrow G$, $\varphi_g(x) = x \cdot g$ (ben definita perché G chiuso rispetto al prodotto)

allora, φ_g è una biiezione

N.B. $\varphi_g(1_G) = g$ $\forall g \neq 1_G$ quindi φ_g non è un omomorfismo (endo)

- Sappiamo che φ_g è invertibile di inverso $\varphi_{g^{-1}}$

Infatti, se $x \in G$, $\varphi_g(\varphi_{g^{-1}}(x)) = \varphi_g(xg^{-1}) = xg^{-1}g = x$ quindi $\varphi_g \circ \varphi_{g^{-1}} = Id_G$

Analogamente, $\varphi_{g^{-1}}(\varphi_g(x)) = \varphi_{g^{-1}}(xg) = xgg^{-1} = x$ quindi $\varphi_{g^{-1}} \circ \varphi_g = Id_G$

notiamo che, generalmente $\varphi_g \circ \varphi_{g'} = \varphi_{gg'}$ ma questo non ci serve per Lagrange (stiamo riscrivendo il gr. G in modo diverso) e $\varphi_{1_G} = Id_G$

In particolare, se $I \subset G$, allora $\# \varphi_g(I) = \# I$ (perché φ_g è una biiezione)

Quindi, se riusciamo a mostrare che una classe è l'immagine di H per un g ben scelto, abbiamo finito.

($\varphi_g(H) = c \implies \# H = \# c$, che è quello che cerchiamo)

Descriviamo una classe c:

Sia $x \in c$. Allora, $c = \{ y : xy^{-1} \in H \}$

Se $y \in c$, $xy^{-1} \in H$.

Ma $xy^{-1} \in H \iff \underset{\exists h \in H}{x = hy} \iff \underset{\exists h \in H}{y = h^{-1}x} \iff y \in Hx \iff c = \varphi_x(H)$

visto che $H < G$, H è chiuso per l'inverso, quindi $h^{-1} = h'$ $\exists h' \in H$ quindi $y = h'x$

ogni el "y" di c si può scrivere come $y = hx$ $\exists h \in H$, quindi $\varphi_x(H)$

Abbiamo quindi trovato il g per cui $\varphi_g(H) = c$. Quindi, $\# H = \# c$, e quindi $\# G = \sum_c \# c = \# H \; [G:H]$ ovvero $\# H \mid \# G$.

QUINDI IL TAKEAWAY È: TUTTI I SOTTOGRUPPI DI G DEVONO AVERE CARDINALITÀ CHE DIVIDE $\# G$.

Quindi, per esempio

prendiamo S_{12} $\quad \# S_{12} = 12!$

Grazie al teorema di Lagrange, so che non esiste $H < S_{12}$ con $\# H = 13$, perché $13 \nmid 12!$

quindi, se p primo e $p \mid \# S_{12}$, allora esiste $H < S_{12}$ t.c. $\# H = p$

in particolare, $p = 2, 3, 5, 7, 11$

Basta prendere un p-ciclo: se σ è un p-ciclo, $\langle \sigma \rangle \cong \mathbb{Z}/p\mathbb{Z} \implies \# \langle \sigma \rangle = p$

Più generalmente, $\forall n \leq 12$, $\exists H < G : \# H = n$ (si prende σ n-ciclo)

ma

- Sia $H < S_{12}$. È vero che $\# H \leq 12$? No! (esistono altri divisori di $12!$)

prendiamo $S \xrightarrow{\varepsilon} \mathbb{Z}^{\times} = \{\pm 1\}$, e $H = \operatorname{Ker}(\varepsilon)$

per il 1o teorema iso:

$$S_{12}/H \cong \mathbb{Z}^{\times} \implies \# S_{12}/H = 2 \iff [S_{12} : H] = 2$$

$$12! = \# S_{12} = \# H \cdot 2 \implies \# H = \frac{12!}{2} \in \mathbb{N}^*$$

(anche logicamente, metà delle perm. saranno dispari e metà pari, quindi $\# \operatorname{Ker}(\varepsilon) = \frac{1}{2} \# S_{12}$)

- altro esempio

se $m \leq n$, c'è (almeno) un omomorfismo iniettivo $S_m \overset{f}{\hookrightarrow} S_n$

- $f(S_m) < S_n$ (perché $m \leq n$)

$\# f(S_m) = \# S_m = m!$ (perché è iniettiva)

Infatti f iniettiva $\implies S_m \cong f(S_m)$

Dal 1o teorema iso:

$$\begin{tikzcd} S_m \arrow[r, hook, "f"] \arrow[d, two heads] & S_n \\ S_m/\{1_{S_m}\} \arrow[r, hook, two heads, "\cong"] & f(S_m) \arrow[u] \end{tikzcd}$$

$S_m/\{1_{S_m}\} \cong S_m$

$\operatorname{Ker}(f) = 1_{S_m}$ (l'unico el. di S_m che punta all'el. neutro di S_n è 1_{S_m})

"S maiuscola gotica"

Sia $\mathfrak{S}_m = \left\{ \sigma \in S_n \text{ t.c. } \begin{array}{l} \sigma(m+1) = m+1 \\ \sigma(m+2) = m+2 \\ \vdots \\ \sigma(n) = n \end{array} \right\} = \{$permutazioni in S_n che fissano gli elementi da $m+1$ a n (ce ne sono $n-m$)$\}$

con $m \leq n$, $f : S_m \hookrightarrow S_n$

$$\sigma \longmapsto \left(\begin{array}{c|c} 1 \ldots m & m+1 \ldots n \\ \downarrow \sigma & \downarrow \text{id.} \\ 1 \ldots m & m+1 \ldots n \end{array} \right)$$

Manda gli el. $1 \ldots m$ seguendo σ, e fissa gli altri

è un omomorfismo di gruppi che soddisfa quanto richiesto e $f(S_m) = \mathfrak{S}_m$

def GRUPPI CICLICI

Sia G un gruppo, e $g \in G$ di ordine $n \geq 1$

Allora, $\underset{\underset{H < G}{\parallel}}{\langle g \rangle} \cong \mathbb{Z}/n\mathbb{Z}$ in not. additiva

quindi possiamo trovare i sottogruppi attraverso $\mathbb{Z}/n\mathbb{Z}$

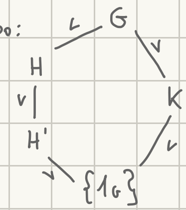
sottogruppo del sottogruppo

PROP:

- $\forall\, d \mid n$, $\exists!$ sottogruppo $H_d < H$ t.c. $\# H_d = d$

Quindi il diagramma di Hasse di un gruppo G è del tipo: ($<$ è una relazione di equivalenza)

per $<$



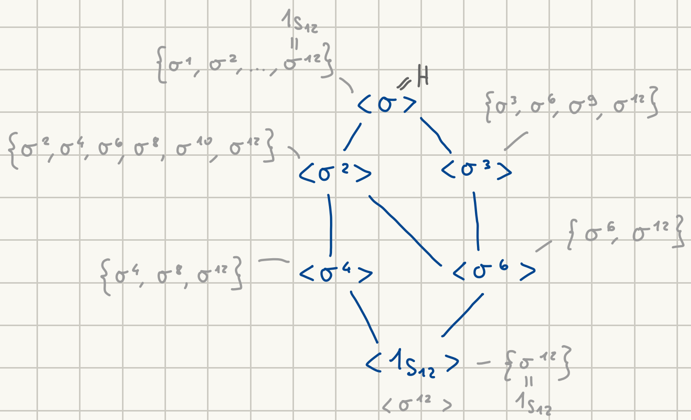
esempio

$G = S_{12}$, $\sigma = (1\ 2\ 3 \dots 12)$

$\text{ord}(\sigma) = 12$, quindi $\underset{\underset{H}{\parallel}}{\langle \sigma \rangle} \cong \mathbb{Z}/12\mathbb{Z}$

e $\forall$ divisore di 12 c'è un unico $H_d < H$ con $\# H_d = d$ quindi: 1, 2, 3, 4, 6, 12

e il diagramma di Hasse è:



$\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle$

$\langle \bar{2} \rangle = 2\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$

$\langle \bar{3} \rangle = 3\mathbb{Z}/12\mathbb{Z}$

$\langle \bar{4} \rangle = 4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$

$\langle \bar{6} \rangle = 6\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$

$2\mathbb{Z}/12\mathbb{Z} = \{[2]\ [4]\ [6]\ [8]\ [10]\ [12]\}$

$\cong$

$\mathbb{Z}/6\mathbb{Z} = \{[1]\ [2]\ [3]\ [4]\ [5]\ [6]\}$

perché? Abbiamo σ, una perm. di ordine 12 (quindi $\sigma^{12} = 1_{S_{12}}$)

Sappiamo che $\langle g \rangle$ è ciclico isomorfo a $\mathbb{Z}/12\mathbb{Z}$ (in not. additiva)

Quindi esiste un sottogruppo $H_d < \langle g \rangle$ con cardinalità d per ogni divisore di 12.

Per trovarli, possiamo "aiutarci" con $\mathbb{Z}/12\mathbb{Z}$. Visto che $\mathbb{Z}/12\mathbb{Z}$ è a sua volta ciclico 12, sappiamo che i sottogruppi di $\mathbb{Z}/12\mathbb{Z}$ sono generati dalle classi dei divisori di 12, ovvero:

$[1], [2], [3], [4], [6], [12]$.

$[1] = \{0, \dots, 11\}$ corrisponde a $\langle \sigma \rangle$ (sottogr. di ordine 12)

$[2] = \{0, 2, 4, 6, 8, 10\}$ corrisponde a $\langle \sigma^2 \rangle$ (ordine 6)

$[3] = \{0, 3, 6, 9\}$ corr. a $\langle \sigma^3 \rangle$ (ordine 4)

$[4] = \{0, 4, 8\}$ corr. a $\langle \sigma^4 \rangle$ (ord. 3)

$[6] = \{0, 6\}$ corr. a $\langle \sigma^6 \rangle$ (ord. 2)

$[12] = \{0\}$ corr. a $\langle \sigma^{12} \rangle = 1_{S_{12}}$ (ord. 1)

SPAZI VETTORIALI

Dato K campo,

sia V un insieme $\neq \emptyset$ munito di

- operazione binaria: $V \times V \longrightarrow V$

$(a, b) \longmapsto (a+b)$

- un'operazione $\underset{\text{scalari}}{K} \times \underset{\text{vettori}}{V} \longrightarrow V$

$(\lambda, v) \longmapsto \lambda \cdot v$

(V ha somma e prodotto scalare)

si dice che V è uno spazio vettoriale su K (si può scrivere $/K$) se:

① $(V, +)$ è un gruppo abeliano (di el. neutro 0_V o $\emptyset$)

② $\alpha \cdot (v+w) = \alpha v + \alpha w \quad \forall \alpha \in K, \ \forall v, w \in V$ distribuzione a sx (distr. di scalare su somma di vettori)

③ $(\alpha+\beta) \cdot v = \alpha v + \beta v \quad \forall \alpha, \beta \in K, \ \forall v \in V$ distribuzione a dx (distr. di vettore su somma di scalari)

④ $(\alpha \overset{\text{op. }K}{\cdot} \beta) \underset{\text{op. }V}{\cdot} v = \alpha \cdot (\beta \overset{\text{op. }V}{\cdot} v) \quad \forall \alpha, \beta \in K, \ \forall v \in V$ non-proprio-associatività

op. V? perché $\beta v \in V$ e $\alpha \in K$ CHIEDERÒ CONFERMA

⑤ $1_K \cdot v = v \quad \forall v \in V$ elemento neutro molt.

ma in V non esiste un el. neutro per la molt., quindi quello di K funge da neutro per questa operazione

da queste proprietà discende: • $0_K \cdot v = 0_V \quad \forall v$

infatti, $0_v = \underbrace{0_K \cdot v}_{\in V} - \underbrace{0_K \cdot v}_{\text{opposto}} = (0_K + 0_K) v = 0_K \cdot v$ ($0 = -0$, per ③)

OSS:

la molt. di $v \in V$ per $-1 \in K$ (opposto dell'el. neutro per l'add in K),

$(-1) \cdot v = -v$

è l'opposto per la struttura di gruppo

infatti, dato $v \in V$,

$v + (-1) v = (1 + (-1)) v$

$= 0 \cdot v = \emptyset$

- per esempio, $V = K$ è uno spazio vettoriale su K

(perché K campo quindi K anello quindi distr., assoc., el. neutro)

spazio vett. K^n

- Poniamo $V = K \times \ldots \times K = K^n$ con l'operazione $+$ di prodotto cartesiano di gruppi

(con $\emptyset$ el. neutro di K, $0_{K^n} = (0, \ldots, 0)$ el. neutro di K^n)

Definiamo $K \times V \longrightarrow V$:

$$K \times \overbrace{K \times \ldots \times K}^{n \text{ volte}} \longrightarrow \overbrace{K \times \ldots \times K}^{n \text{ volte}}$$

$$(\lambda, (v_1, \ldots, v_n)) \longmapsto (\lambda v_1, \ldots, \lambda v_n) = \lambda(v_1, \ldots, v_n)$$

questa operazione soddisfa

tutti gli assiomi di spazio vettoriale

distr. a sx:

② $\lambda \cdot ((v_1, \ldots, v_n) + (w_1, \ldots, w_n)) = \lambda((v_1 + w_1, \ldots, v_n + w_n)) =$

$= (\lambda (v_1 + w_1), \ldots, \lambda (v_n + w_n)) = (\lambda v_1 + \lambda w_1, \ldots, \lambda v_n + \lambda w_n) =$

$= (\lambda v_1, \ldots, \lambda v_n) + (\lambda w_1, \ldots, \lambda w_n) =$

$= \lambda (v_1, \ldots, v_n) + \lambda (w_1, \ldots, w_n) =$ $\qquad v = (v_1, \ldots, v_n) \quad w = (w_1, \ldots, w_n)$

$= \lambda (v + w) = \lambda v + \lambda w$

V, con queste operazioni, è uno spazio vettoriale.

Esempi di spazi vettoriali: (dato K campo)

① K^n, con $n=1$, $K^n = K$ (e $V=K$ visto sopra), con $n=0$ $K^0 = (0)$ (spazio vettoriale banale)

② matrici con m linee e n colonne a coefficienti in K

$$M_{m,n}(K) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} : a_{ij} \in K \ \forall i,j \right\} = \left\{ (a_{ij})_{\substack{1\le i \le m \\ 1 \le j \le n}} : a_{ij} \in K \ \forall i,j \right\}$$

con operazioni di addizione coefficiente per coefficiente $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$

e moltiplicazione esterna per λ separatamente per ogni coefficiente $\lambda = 2 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}$

nota: essenzialmente, $M_{m,n}(K)$ è una riscrittura di $K^{m \cdot n}$ sotto forma di matrice. (come vettori assembly)

per esempio, $M_{2,3}(K) = K^{2\times 3}$ è ~~uguale~~ (formalmente si dice) isomorfo a K^6

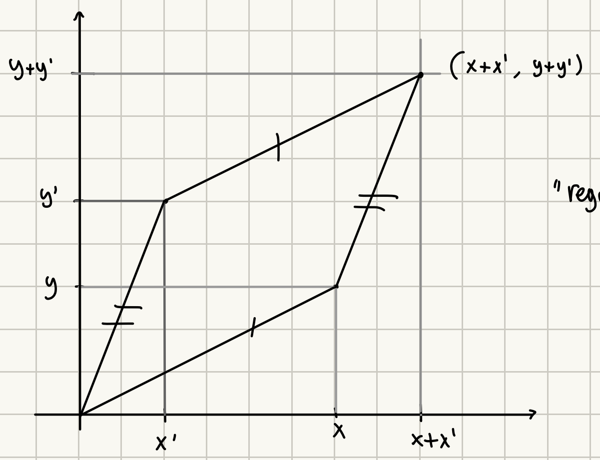
$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \in M_{2,3}(K) \xmapsto{1:1} (a,b,c,d,e,f) \in K^6$$

esempio operazioni:

$A = (a_{ij})$ $B = (b_{ij})$ $\in M_{m,n}(K) = K^{m\times n}$

- $A + B = (a_{ij} + b_{ij}) \in M_{m,n}(K)$
- $\lambda \in K$: $\lambda A = (\lambda A_{ij}) \in M_{m,n}(K)$

RAPPRESENTAZIONE GRAFICA DELLA SOMMA IN $\mathbb{R}^2$



"regola del parallelogramma"

③ Polinomi a coefficienti in K campo

$V = K[X]$ $\quad f = f_0 + f_1 x + f_2 x^2 \ldots$, $g = g_0 + g_1 x + g_2 x^2 \ldots$, $\lambda \in K$

$f + g = f_0 + g_0 + (f_1 + g_1)x + \ldots$

$\lambda \cdot f = \lambda f_0 + (\lambda f_1)x + (\lambda f_2)x^2 + \ldots$

osservazione: K finito (es $K = \mathbb{F}_p$) ma $K[X]$ infinito

④ lo ho skippato per ora

⑤ $\mathbb{C}$ è uno spazio vettoriale su $\mathbb{C}$

ma si ha anche che $\mathbb{C}$ è uno spazio vettoriale su $\mathbb{R}$

$\mathbb{C} = \{ x+iy : x,y \in \mathbb{R} \}$ la struttura di gruppo abeliano è nota

- $\lambda \in \mathbb{R}$, $z \in \mathbb{C}$, $z = x+iy$ $\quad \lambda \cdot z = \lambda(x+iy) = (\lambda x) + i(\lambda y)$

def APPLICAZIONE LINEARE (come omom. gruppi)

Dati due spazi vettoriali V, V' su K, un'applicazione $V \xrightarrow{f} V'$ è detta lineare se:

infatti notiamo che se $\lambda = 1$, è l'assioma dell'omomorfismo

$$\forall x,y \in V, \ \forall \lambda \in K, \quad f(x+\lambda y) = f(x) + \lambda f(y)$$

Se f è biiettiva, si dice isomorfismo.

Se $f: V \to V'$ isomorfismo esiste, allora si dice che V e V' sono isomorfi e si scrive $V \cong V'$.

def SOTTOSPAZIO VETTORIALE

dato V spazio vettoriale su K,

$W \subset V$, $W \neq \emptyset$ è un sottospazio vettoriale se: (varie definizioni alternative)

1. è uno spazio vettoriale per le operazioni indotte da V

   ovvero se, come gruppi abeliani, si ha: quindi anche W abeliano

   - $W < V$
   - $\forall w \in W, \forall \lambda \in K, \quad \lambda \cdot w \in W$

2. - $\forall w, w' \in W$, si ha $w + w' \in W$ (stabilizzato rispetto alla somma)
   - $\forall w \in W, \forall \lambda \in K, \quad \lambda \cdot w \in W$

3. se è stabile per combinazioni lineari nel modo seguente:

   - $\forall w, w' \in W, \ \forall \lambda, \lambda' \in K$, si ha $\lambda w + \lambda' w' \in W$

4. $\forall w_1, \dots, w_n$ e $\forall \lambda_1, \dots, \lambda_n$, $\quad \lambda_1 w_1 + \dots + \lambda_n w_n \in W$

5. $\forall w, w' \in W$ e $\forall \lambda \in K$, $\quad w + \lambda w' \in W$

def COMBINAZIONE LINEARE

Dati $v, \dots, v_n \in V$, e $\lambda_1, \dots, \lambda_n \in K$ allora $\lambda_1 v_1 + \dots + \lambda_n v_n$ è una combinazione lineare di $v_1 \dots v_n$ (a coeff. $\lambda_1, \dots, \lambda_n$)

- si dice "Span" o "Sottospazio Generato da $v_1, \dots, v_n$" il sottospazio vettoriale ottenuto dall'insieme di tutte le possibili combinazioni lineari di un insieme di vettori.
  - si scrive "$\mathrm{Span}_K(\{v_1, \dots, v_n\})$" o "$\mathrm{Vett}_K(\{v_1, \dots, v_n\})$"

esempi

① Mostrare che $S = \{(x,y,z) \in \mathbb{R}^3 \text{ t.c. } x^2+y^2+z^2 = 1\}$ non è un sottospazio vettoriale di $\mathbb{R}^3$.

prendiamo $w = (1,0,0)$, $w' = (0\,1\,0)$, $\lambda = 1$

$$w + \lambda w' = \overset{x\ y\ z}{(1\,1\,0)} \quad e \quad x^2+y^2+z^2 = 1+1+0 = 2 \neq 1 \implies w + w' \notin S$$

metodo alternativo: ogni sottosp. vettoriale di $\mathbb{R}^3$ deve contenere $0 = (0,0,0)$. Qui $(0,0,0) \notin S$

el. neutro somma (op. spazi vettoriali)

def SPAN / SOTTOSPAZIO GENERATO

Prendiamo V sp. vett. su K. Siano $v_1, \dots, v_n \in V$.

Poniamo $W = \mathrm{Span}_K(\{v_1, \dots, v_n\}) = \{\text{comb. lineari di } v_1, \dots v_n\} = \{\lambda_1 v_1 , \dots, \lambda_n v_n : \forall \lambda_1, \dots \lambda_n \in K\}$
o Vett_K

è un sottospazio vettoriale.

Per vederlo, consideriamo $w, w' \in W$, $\lambda \in K$, e calcoliamo $w + \lambda w'$

$$\text{Ma } w = \sum_{i=1}^n \lambda_i v_i, \quad w' = \sum_{i=1}^n \lambda'_i v_i, \quad \text{quindi } w + \lambda w' = \sum_{i=1}^n \underbrace{\lambda_i v_i}_{w} + \underbrace{\lambda \lambda'_i v_i}_{\lambda w'} \underset{\text{distr.}}{=} \sum_{i=1}^n (\lambda_i + \underbrace{\lambda\lambda'_i}_{\lambda''}) v_i \implies w + \lambda w' \in W$$

λ'' quindi si può scrivere come λv

quindi Span_K è un sottosp. vett.! per ⑤

OSSERVIAMO che $\mathrm{Span}(\{v_1, \dots, v_n\}) = \bigcap_{\substack{W \subset V \\ \text{sottosp. vett.}, \\ W \supset \{v_1, \dots, v_n\}}} W$ 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., $W_1 \cap W_2 < V$ (perché $W_1, W_2 < V$ per def. sottosp. vett., e $\cap$ sottogr. è un sottogr.)

Sia $v \in W_1 \cap W_2$, e $\lambda \in K$.

Allora, $\lambda v \in W_i$ perché W_i è sottosp. vett. di V (con $i = 1,2$)

Quindi, $\lambda v \in W_1 \cap W_2$

oss: Se W è sottosp. vett. di V, allora $\emptyset \in W$.

def VETTORI LINEARMENTE INDIPENDENTI

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. $\lambda_1 v_1 + \dots + \lambda_n v_n = \emptyset_V$

allora $\lambda_1 = \dots = \lambda_n = \emptyset_K$

$\sum_i 0 \cdot v_i$ $\left(\sum_i \lambda_i v_i \text{ con } \lambda_i = \emptyset \ \forall i\right)$

Ovvero, se l'unica combinazione lineare di $v_1, \dots, v_n$ che è nulla è quella banale (ovvero quella con tutti i $\lambda = \emptyset$)

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.

Consideriamo una comb. lin. $\lambda_1 v_1 + \lambda_2 v_2 = \emptyset$

$$\text{ovvero } \lambda_1 \begin{pmatrix}1\\2\end{pmatrix} + \lambda_2 \begin{pmatrix}2\\2\end{pmatrix} = \emptyset \overset{\text{molt. scalare}}{\iff} \begin{pmatrix}\lambda_1\\2\lambda_2\end{pmatrix} + \begin{pmatrix}2\lambda_2\\2\lambda_2\end{pmatrix} = \emptyset \overset{\text{somma vett.}}{\iff} \begin{pmatrix}\lambda_1 + 2\lambda_2\\2\lambda_2 + 2\lambda_2\end{pmatrix} = \emptyset$$

Costruiamo il sistema lineare che ha $\begin{pmatrix}\lambda_1\\\lambda_2\end{pmatrix}$ come soluzioni (si può direttamente mettere i vettori a sistema)

$$\begin{cases} \lambda_1 + 2\lambda_2 = \emptyset \quad (1) \\ 2\lambda_1 + 2\lambda_2 = \emptyset \end{cases} \underset{\text{si sottrae termine a termine}}{\Longrightarrow} 2\lambda_1 - \lambda_1 + 2\lambda_2 - \cancel{2\lambda_2} = \emptyset - \emptyset \iff \lambda_1 = \emptyset \text{ sostituiamo nell'eq. 1}$$

$(\lambda_1 = x_1 \text{ e } \lambda_2 = x_2)$

$$\Longrightarrow 0 + 2\lambda_2 = \emptyset \iff \lambda_2 = \emptyset \qquad \text{quindi } \lambda_1 = \lambda_2 = \emptyset$$

> oss: se ho m vettori $v_1, \dots, v_m \in K^n$ e se $m > n$, allora $v_1, \dots, v_m$ sono sempre l. d.
>
> es. $\begin{pmatrix}1\\0\end{pmatrix} \begin{pmatrix}2\\1\end{pmatrix} \begin{pmatrix}3\\2\end{pmatrix}$ sono $3 > 2$ vettori in $\mathbb{R}^2$, e sono quindi l.d.
>
> oss: Data $f: V \xrightarrow{\cong} V'$, $v_1, \dots, v_n$ sono l.i. se $f(v_1), \dots, f(v_n)$ sono l.i.
>
> per esempio, $M_{m,n}(K) \cong K^{m \cdot n}$ può essere utile

esercizi

(1) notare che $v_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}$, $v_2 = \begin{pmatrix}2\\2\\0\end{pmatrix}$, $v_3 = \begin{pmatrix}1\\2\\1\end{pmatrix}$

$$\begin{cases} \lambda_1 + 2\lambda_2 + \lambda_3 = \emptyset \\ 2\lambda_2 + 2\lambda_3 = \emptyset \\ \lambda_3 = \emptyset \end{cases} \quad \begin{cases} \lambda_1 + 2\lambda_2 = \emptyset \\ 2\lambda_2 = \emptyset \\ \lambda_3 = \emptyset \end{cases} \quad \begin{cases} \lambda_1 = \emptyset \\ \lambda_2 = \emptyset \\ \lambda_3 = \emptyset \end{cases}$$

$\lambda_1 = \lambda_2 = \lambda_3 = \emptyset \Longrightarrow v_1, v_2, v_3$ l.i.

(2) Consideriamo $\underbrace{v_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, v_2 = \begin{pmatrix}2\\0\\0\end{pmatrix}}_{\text{uno multiplo dell'altro}}$, $v_3 = \begin{pmatrix}1\\2\\1\end{pmatrix}$

si vede che $2v_1 - v_2 + \emptyset v_3 = \emptyset$

def MATRICE TRIANGOLARE $= M_n$ - un pedice solo indica #righe = #colonne

una matrice $M \in M_{n,n}(\mathbb{R})$

è detta triangolare superiore se si può scrivere come

(invece, una triangolare inferiore sarebbe così: $\begin{pmatrix} m & 0 & 0 & 0 \\ m & m & 0 & 0 \\ m & m & m & 0 \\ m & m & m & m \end{pmatrix}$

(con gli zeri in alto)

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} & \dots & m_{1\,n-1} & m_{1n} \\ 0 & m_{22} & m_{23} & \dots & m_{2\,n-1} & m_{2n} \\ 0 & 0 & m_{33} & \dots & m_{3n-1} & m_{3n} \\ 0 & 0 & 0 & \dots & m_{4\,n-1} & m_{n-1,n} \\ & & & \vdots & & \\ 0 & 0 & 0 & \dots & m_{n-1,n-1} & m_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 & m_{n,n} \end{pmatrix}$$

diagonale della matrice $(m_{i,j}$ con $i=j)$

esempio: $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}$

- le colonne e le righe di M, viste come vettori di $\mathbb{R}^n$, sono l.i. $\iff m_{11}, m_{22}, \dots, m_{nn}$ (coeff. diag.) sono tutti non nulli

esempio:

- le colonne della matrice $\begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ sono l. d. $\iff \binom{1}{0}\binom{2}{1}\binom{3}{2}$ sono l. d.

(gli zeri non influenzano)

$\binom{1}{0}, \binom{2}{1}, \binom{3}{2}$ l. d. perché

$$\begin{cases} \lambda_1 + 2\lambda_2 + 3\lambda_3 \\ \lambda_2 + 2\lambda_3 \end{cases} \iff \lambda_2 = -2\lambda_3 \quad \begin{cases} \lambda_1 = \lambda_3 \\ \lambda_2 = -2\lambda_3 \end{cases}$$

se pongo $\lambda_3 = 1$ allora

$(\lambda_1, \lambda_2, \lambda_3) = (-1, -2, 1) \neq (0,0,0)$

e si ottiene la comb. nulla, ma non banale

$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = \binom{1}{0} - 2\binom{2}{1} + \binom{3}{2} = \binom{0}{0}$

esercizi (x casa)

① $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$

in $\mathbb{R}^3$, $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

Dimostrare che $e_1, \dots, e_n$ sono l.i. e che, considerando inoltre $e_{n+1} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$, allora $e_1, \dots, e_n, e_{n+1}$ sono l. d.
e caratterizzare tutte le comb. lin. nulle

② ⓐ $V = M_n(K)$, mostrare che le matrici

$e_{ij} = \begin{pmatrix} & | & \\ — & 1 & — \\ & | & \end{pmatrix}$ $1 \leq i, j \leq n$ (ce ne sono n^2)

tutti zeri

matr. $n \times n$

sono l.i.

ⓑ Mostrare che $(e_{ij})_{1 \leq i,j \leq n}$ e $F: \begin{pmatrix} 1 & — & 1 \\ | & & | \\ 1 & — & 1 \end{pmatrix}$ sono l. d.

tutti uni

DIVERSI MODI DI RAPPRESENTARE UNA MATRICE

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

- $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$
- $A = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}$ con A_i i-esima riga di A
- $A = (A^1 \dots A^n)$ con A^j j-esima colonna di A

$A = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} = M_{2,3}(\mathbb{R})$ $\quad A_1 = (abc) \quad A_2 = (def), \quad A^1 = \begin{pmatrix} a \\ d \end{pmatrix}, \; A^2 = \begin{pmatrix} b \\ e \end{pmatrix}, \; A^3 = \begin{pmatrix} c \\ f \end{pmatrix}$

PRODOTTO TRA MATRICI

prodotto scalare di una matrice linea e una matrice colonna

$U = (u_1 \dots u_n) \in M_{1,n}(K), \quad V = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in M_{n,1}(K)$

$$\langle U, V \rangle = \sum_{i=1}^{n} u_i v_i = u_1 v_1 + \dots + u_n v_n$$

con questo prodotto scalare definiamo un'operazione: $M_{m,\underbrace{k}(K) \times M_{k},n}(K) \longrightarrow M_{m,n}(K)$

$$\text{dove } \big(\underset{\substack{\| \\ \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}}}{A}, \underset{\substack{\| \\ (B^1 \dots B^n)}}{B}\big) \longmapsto A \cdot B = \left(\langle A_i, B^j \rangle\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

$M_{1,k}(K)$ $\quad$ $M_{k,1}(K)$

è un'operazione associativa e distributiva

esempio

$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in M_{2,3}, \quad B = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \in M_{3,2}$

$A \cdot B = \begin{pmatrix} \text{linea 1 A} \cdot \text{colonna 1 B} & \text{linea 1 A} \cdot \text{colonna 2 B} \\ \text{linea 2 A} \cdot \text{col. 1 B} & \text{linea 2 A} \cdot \text{col. 2 B} \end{pmatrix}$

ovvero $B = \begin{pmatrix} 4 & 1 \\ -2 & 2 \\ 0 & 3 \end{pmatrix}$

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

$A \cdot B = \begin{pmatrix} 1\cdot 1 + 2\cdot 2 + 3\cdot 3 & 1\cdot 4 + 2\cdot 5 + 3\cdot 6 \\ 4\cdot 1 + 5\cdot 2 + 6\cdot 3 & 4\cdot 4 + 5\cdot 5 + 6\cdot 6 \end{pmatrix} = \begin{pmatrix} 14 & 32 \\ 32 & 77 \end{pmatrix} \in M_{2,2}(\mathbb{R})$

esercizio

- calcolare $B \cdot A \in M_{3,3}(\mathbb{R})$

$B = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$

$B \cdot A = \begin{pmatrix} 1\cdot 1 + 4\cdot 4 & 1\cdot 2 + 4\cdot 5 & 1\cdot 3 + 4\cdot 6 \\ 2\cdot 1 + 5\cdot 4 & 2\cdot 2 + 5\cdot 5 & 2\cdot 3 + 5\cdot 6 \\ 3\cdot 1 + 6\cdot 4 & 3\cdot 2 + 6\cdot 5 & 3\cdot 3 + 6\cdot 6 \end{pmatrix} = \begin{pmatrix} 17 & 22 & 27 \\ 23 & 29 & 36 \\ 27 & 36 & 45 \end{pmatrix}$