

ALGEBRA

Monday, February 28, 2022 1:22 PM

"

I NOSTRI RAGIONAMENTI SONO DI NATURA TEORICA "

"

RELAZIONE

Monday, February 28, 2022 1:31 PM

Una RELAZIONE di A in B è un sottoinsieme del PRODOTTO CARTESIANO

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$$

$$A = \{1, 2, 5, -1, 7\} \quad B = \{4, 25, 1, 15, 6\}$$

$$a R b \text{ se } b = a^2$$

$$(1, 1) \begin{matrix} 1R1 \\ 2R4 \\ 5R25 \\ -1R1 \end{matrix} \quad R = \{(1, 1), (-1, 1), (2, 4), (5, 25)\} \subseteq A \times B$$

$A = B$ relazione su A

$$A = \{1, 3, -1, 7, -5\} \quad R = \{(1, 3), (1, -1), (1, 7), (7, -5)\}$$

FUNZIONI SONO RELAZIONI $f: A \rightarrow B \quad \forall a \in A \exists! b \in B \quad b = f(a)$

$$(a, b) \in A \times B$$

$$(a, b), (a, b') \in A \times B \Rightarrow b = b'$$

A = dominio

B = codominio

RELAZIONE DI EQUIVALENZA

Una relazione di equivalenza su un insieme A è una relazione che soddisfa le seguenti proprietà

RIFLESSIVA $\forall a \in A \quad a Ra$

SIMMETRICA $\forall a, b \in A \quad a R b \Leftrightarrow b R a$

TRANSITIVA $\forall a, b, c \in A \quad a R b \text{ e } b R c \Rightarrow a R c$

ESERCIZIO

(=)

$$\textcircled{1} \quad \forall a \in A \quad a = a$$

$$\textcircled{2} \quad \text{se } a = b \Rightarrow b = a$$

$$\textcircled{3} \quad \text{se } a = b \text{ e } b = c \Rightarrow a = c$$

$(\forall a, b \in \mathbb{Z} \quad a R b \Leftrightarrow a - b = 2k \quad k \in \mathbb{Z})$

$$\textcircled{1} \quad a R a \quad a - a = 0 = 2 \cdot 0$$

$$\textcircled{2} \quad a R b \quad \Rightarrow \quad a - b = 2k \quad \Rightarrow \quad b R a \\ b - a = 2(-k)$$

$$\textcircled{3} \quad a R b \text{ e } b R c \quad \Rightarrow \quad a R c$$

$$a R b \Rightarrow a - b = 2k \\ b R c \Rightarrow b - c = 2h \quad \Rightarrow \quad a - c = 2k + 2h = 2(k+h)$$

RELAZIONE DI EQUIVALENZA

Monday, February 28, 2022 1:55 PM

$A \quad R =$ relazione di equivalenza

$\forall a \in A$

DEFINIZIONE

In classe di equivalenza individuata da $a \in A$

$$[a] = \{ b \in A \mid b R a \}$$

OSSERVAZIONE

$$a \in [a]$$

PROPRIETÀ

- 1) $[a] = [b] \Leftrightarrow a R b$
- 2) $[a] \cap [b] = \emptyset \text{ se } a \not R b$

DIMOSTRAZIONE

$$\text{Se } [a] = [b] \Rightarrow b \in [b] \cdot [a] \Rightarrow b \in [a] \Rightarrow b R a \Rightarrow a R b$$

$$\text{Se } a R b, x \in [a] \Rightarrow x R a \Rightarrow x R b \Rightarrow x \in [b]$$

$$[a] \subseteq [b]$$

$$x \in [b] \Rightarrow x R b \Rightarrow x R a \Rightarrow x \in [a]$$

$$[b] \subseteq [a]$$

$$1) [a] = [b] \quad \forall b \in [a] \quad a \text{ è rappresentante di classe}$$

$$2) [a] \cap [b] = \begin{cases} [a] & \text{se } a R b \\ \emptyset & \text{se } a \not R b \end{cases}$$

$$\text{Se } x \in [a] \cap [b] \Rightarrow x \in [a] \quad x R a = a R x \Rightarrow a R b \\ x \in [b] \quad x R b = b R x$$

A, R

DEFINIZIONE

$$I' \quad \omega \sim \Omega'$$

DEFINIZIONE

L'insieme quoziente è l'insieme

$$A/R = \{[a] \mid a \in A\}$$

DEFINIZIONE

Sia A un insieme $\{A_i\}_{i \in I}$ famiglia di sottinsiemi è una partizione di A se $\bigcup A_i = A$

$$A_i \cap A_j = \emptyset \forall i, j \text{ DISGIUNTI}$$

PROPOSIZIONE

L'insieme quoziente è una partizione di A

A insieme $\{A_i\}_{i \in I}$ partizione \Rightarrow definire una relazione di equivalenza

aRb se $a, b \in A_i$ [per qualche i]

R è una relazione d. eq. $\forall a \in A \quad aRa \quad \exists i : a \in A_i$

Simm.

se $aRb = bRa$?

$a, b \in A_i \Rightarrow bRa \quad b, a \in A_i$

Trans.

$$\begin{array}{ll} aRb & a, b \in A_i \\ bRc & b, c \in A_j \end{array} \quad i=j \quad b \in A_i \cap A_j$$

$$a, b, c \in A_i \Rightarrow a, c \in A_i \Rightarrow aRc$$

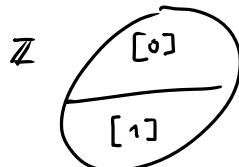
$$\mathbb{Z} \quad aRb \Leftrightarrow a-b = 2k$$

$$[0] = \{b \in \mathbb{Z} \mid bR0\} \quad b = 2k$$

$$= \{2k \mid k \in \mathbb{Z}\}$$

$$[1] = \{b \in \mathbb{Z} \mid bR1\} \quad \begin{aligned} b-1 &= 2h \\ b &= 2h+1 \end{aligned}$$

$$= \{b = 2h+1 \mid h \in \mathbb{Z}\}$$



$$\mathbb{Z} \sim m \sim n \Leftrightarrow |m| = |n|$$

$$|m| = \begin{cases} m \text{ se } m \geq 0 \\ -m \text{ se } m < 0 \end{cases}$$

RIFLESSIVA $\forall m \in \mathbb{Z} \quad m \sim m \Rightarrow |m| = |m|$

SIMMETRICA $\forall m_1, m_2 \in \mathbb{Z} \quad m_1 \sim m_2 \Rightarrow |m_1| = |m_2|$

$$\Rightarrow |m_1| = |m_2| \Rightarrow m_1 \sim m_2$$

TRANSITIVA

$$\forall m, n, p \in \mathbb{Z} \quad \begin{matrix} m \sim n, n \sim p \\ \Downarrow \quad \Downarrow \end{matrix} \Rightarrow m \sim p$$

$$|m| = |n| \quad |n| = |p| \Rightarrow |m| = |p| \Rightarrow m \sim p$$

$$[m] = \{n \in \mathbb{Z} \mid n \sim m\} \quad |m| = |m| \quad m = \pm m$$

$$= \{\pm m \mid m \in \mathbb{Z}\}$$

~~X CASA~~ 

$$\mathbb{Z} \nvdash a, b \in \mathbb{Z} \quad a \sim b \Leftrightarrow a^2 - a = b^2 - b$$

?

RELAZIONE D'ORDINE

Monday, February 28, 2022 1:55 PM

DEFINIZIONE

R è una relazione d'ordine su A se soddisfa

1) RIFLESSIVA $aRa \quad \forall a \in A$

2) ANTI-SIMMETRICA se $a \neq b \quad aRb \Rightarrow bR \neq a$
equivalentemente se $aRb \wedge bRa \Rightarrow a = b$

3) TRANSITIVA

Se A possiede una relazione d'ordine si dice parzialmente ordinato

Se $\forall a, b \in A \quad aRb \Rightarrow bRd \Rightarrow A$ totalmente ordinato

(\leq)

1) $\forall a \in \mathbb{Z} \quad a \leq a$

2) se $a \leq b \wedge b \leq a \Rightarrow a = b$

3) se $a \leq b \wedge b \leq c \Rightarrow a \leq c$

$$A = \{2, 5, 4, 6, 3, 8\}$$

È UNA RELAZIONE D'ORDINE

MA A NON È TOTALMENTE ORDINATO

1)

aRb se a divide b

2) se $a \neq b \quad aRb \Rightarrow bR \neq a$

3) $aRb, bRc \Rightarrow aRc$

OPERAZIONE

venerdì 4 marzo 2022 08:17

DEFINIZIONE

Un'operazione su un insieme A è una funzione

$$*: A \times A \rightarrow A$$

$$(a_1, a_2) \mapsto a_1 * a_2$$

ESEMPI

$$+ \text{ IN, } \mathbb{Z}, \mathbb{R}, \mathbb{Q}$$

$$- \text{ } \mathbb{Z}, \mathbb{R}, \mathbb{Q}$$

PROPRIETÀ

$$\text{ASSOCIAZIONE} \quad \forall a, b, c \in A \quad (a * b) * c = a * (b * c)$$

$$\text{COMMUTATIVITÀ} \quad \forall a, b \in A \quad a * b = b * a$$

$$\begin{array}{ll} \text{ESISTENZA} & \forall a \in A \quad \exists e \in A \mid a * e = e * a = a \\ \text{DEL ELEMENTO NEUTRO} & \end{array}$$

$$\begin{array}{ll} \text{ESISTENZA} & \forall a \in A \quad \exists a' \in A \mid a * a' = a' * a = a \\ \text{DEL SIMMETRIO} & \end{array}$$

$$\mathbb{N} = \{0, 1, 2, \dots\} \subseteq \mathbb{Z} = \{0, \pm 1, \pm 2\}$$

$$(\mathbb{Z}, +)$$

- ASSOCIAZIONE
- \exists ELEMENTO NEUTRO
- \exists SIMMETRIO
- COMMUTATIVITÀ

$\left. \begin{array}{l} \text{ASSOCIAZIONE} \\ \exists \text{ ELEMENTO NEUTRO} \\ \exists \text{ SIMMETRIO} \\ \text{COMMUTATIVITÀ} \end{array} \right\}$

GRUPPO

GRUPPO ABELIANO

$$(\mathbb{Z}, +) \text{ ABELIANO}$$

+ DISTRIBUTIVA

ANELLO

$$(\mathbb{Z}, *)$$

- ASSOCIAZIONE
- \exists ELEMENTO NEUTRO
- $\cancel{\exists}$ SIMMETRIO
- COMMUTATIVITÀ

$(\mathbb{Z}, \oplus, \odot)$

$a \oplus b = a+b-1$

$a \odot b = a+b-ab$

 (\mathbb{Z}, \oplus)

$\textcircled{1} \quad \forall a, b, c \in \mathbb{Z} \quad (a \oplus b) \oplus c = a \oplus (b \oplus c)$

$$(a+b-1) \oplus c = (a+b-1) + c - 1 = a+b+c-2 = \\ a-1 + (b+c-1) = a-1 + (b \oplus c) = a \oplus (b \oplus c)$$

$\textcircled{2} \quad \forall a, b \in \mathbb{Z} \quad a \oplus b = b \oplus a$

$a+b-1 = b+a-1$

$\textcircled{3} \quad \forall a \in \mathbb{Z} \quad \exists e \in \mathbb{Z} \mid a \oplus e = a$

$a+e-1 = a \quad [e=1] \text{ SOTTO}$

$\textcircled{4} \quad \forall a \in \mathbb{Z} \quad \exists a' \in \mathbb{Z} \mid a \oplus a' = e = 1$

$a+a'-1 = 1 \quad [a'=2-a] \text{ NEUTRO}$

 (\mathbb{Z}, \odot)

$\textcircled{1} \quad \forall a, b, c \in \mathbb{Z} \quad (a \odot b) \odot c = a \odot (b \odot c)$

$$(a \odot b) \odot c = (a+b-a \cdot b) \odot c = a+b-ab+c-(a+b-ab)c = a+b-ab+c-2c-bc+abc = \\ = a-ab-2c+abc+(b+c-bc) = a-ab-a+c+abc+(b \oplus c) = \text{X}$$

 $\textcircled{2} \quad \text{OK}$

$\textcircled{3} \quad \forall a \in \mathbb{Z} \quad \exists e \in \mathbb{Z} \quad a \odot e = a$

$a+e-a \cdot e = a \Rightarrow e=0$

$$3) \quad \forall a \in \mathbb{Z} \quad \exists a' \in \mathbb{Z} \mid a + a' = 0$$

$$a + a' - aa' = 0 \quad a + a'(1-a) = 0 \quad \not\models \text{SMTLIB}$$

$$a' = \frac{-a}{1-a} \notin \mathbb{Z}$$

DISTRIBUTIVA

$$\forall a, b, c \in \mathbb{Z} \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

PRINCIPIO DEL BUON ORDINAMENTO E DI INDUZIONE

venerdì 4 marzo 2022 08:39

PRINCIPIO DEL BUON ORDINAMENTO (o del minimo)

OGNI SOTTOinsieme NON vuoto DI \mathbb{N} AMMETTE MINIMO

$$\forall S \subseteq \mathbb{N}, \quad S \neq \emptyset \quad \exists s \in S \mid \forall x \in S \quad s \leq x$$

PRINCIPIO DI INDUZIONE

Sia $P(n)$ una proprietà riguardante i numeri naturali. Se

- 1) $P(0)$ è vera
- 2) $P(k)$ è vera $\Rightarrow P(k+1)$ è vera

Allora $P(m)$ è vera $\forall m \in \mathbb{N}$

DIMOSTRAZIONE

Supponiamo che $\exists m \in \mathbb{N} \mid P(m)$ è falsa

$$S = \{m \in \mathbb{N} \mid P(m) \text{ è falsa}\} \subseteq \mathbb{N}$$

$S \neq \emptyset \Rightarrow S$ ammette minimo sia $s \in S$

$$s \neq 0 \quad s \geq 1, \quad s-1 \geq 0 \quad s-1 \in \mathbb{N}$$

$\Rightarrow P(s-1)$ è vera $\Rightarrow P(j)$ è vera **Contraddizione**

ESEMPPIO

$$1+2+\dots+m = \frac{m(m+1)}{2}$$

$$m=1 \quad \text{BASE INDUZIONE}$$

$$P(1) \text{ è vero} \quad \underline{1(1+1)} = 1$$

$$P(1) \text{ è vero} \quad \frac{1(1+1)}{2} = 1$$

Supposto vero $P(k) \Rightarrow P(k+1)$ è vero?

$$1+2+\dots+m+(m+1) = \frac{(m+1)(m+2)}{2}$$

$$\frac{m(m+1)}{2} + (m+1) = \frac{m(m+1) + 2(m+1)}{2} = \frac{m(m+1)(m+2)}{2} \quad \checkmark$$

$$1^3 + 2^3 + \dots + m^3 = \frac{m^2(m+1)^2}{4}$$

$$P(1) \quad 1^3 = \frac{1^2(1+1)^2}{4} = 1 \quad P(1) \text{ è vero}$$

Supposto vero $P(m)$ dimostra $P(m+1)$

$$1^3 + 2^3 + \dots + m^3 = \frac{(m+1)^2(m+2)^2}{4}$$

$$\begin{aligned} \frac{m^2(m+1)^2}{4} + (m+1)^3 &= \underbrace{m^2(m+1)^2 + 4(m+1)^3}_{4} = \frac{(m+1)^2(m^2 + 4m + 4)}{4} \\ &= \frac{(m+1)^2(m+2)^2}{4} \quad \checkmark \end{aligned}$$

PER CASA

$$1) \quad 1^2 + 3^2 + (2m-1)^2 = \frac{m(2m-1)(2m+1)}{3}$$

$$2) \quad 1+3+\dots+(2m-1) = m^2$$

$$3) \quad 1^2 + 2^2 + \dots + m^2 = \frac{m(m+1)(2m+1)}{6}$$

PRINCIPIO DI INDUZIONE (II forma)

Sia $P(m)$ una proprietà riguardante i numeri naturali ($m \geq m_0$). Se

- 1) $P(0)$ è vero ($P(m_0)$ è vero)
- 2) $P(k)$ è vero $\forall k < m \Rightarrow P(m)$ è vero

Allora $P(m)$ è vero $\forall m \in \mathbb{N}$

PROPOSIZIONE

Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora esistono e sono unici $p, r \in \mathbb{Z}$ tali che $a = bq + r$ con $0 \leq r < |b|$

DIMOSTRAZIONE

$$\text{Sia } b > 0 \quad b = |b| \quad |b| \geq |a|$$

$$\text{Ges:} \text{cerca l'insieme } S = \{ z = a - bx \geq 0 \mid x \in \mathbb{Z} \}$$

$$z = a - b(-|a|) = a + b|a| \geq a + |a| \geq 0$$

$S \neq \emptyset \Rightarrow$ per l'assunzione del minimo che S ammette minimo.

$$\text{Sia } r = a - bq \text{ con } q \in \mathbb{Z} \Rightarrow a = bq + r$$

$$r \geq 0 \quad r < |b| = b$$

Supponiamo per assurdo che $r \geq b \Rightarrow 0 \leq r - b = a - bq - b = a - b(q+1) < r$

$$\Rightarrow r - b \in S \quad r - b < r \xrightarrow{\text{Assurdo}}$$

$$\text{Se } b < 0, -b > 0$$

$$\text{per la prima parte } \Rightarrow a = (-b)q + z \text{ con } r < |b| \quad 0 \leq r < |b|$$

$$= b(-q) + r = bq' + r$$

Dimostriamo che q e r sono unici

$$\begin{aligned} \text{Supponiamo che} \quad a &= bq + r \quad 0 \leq r < |b| \\ a &= b'q' + r' \quad 0 \leq r' < |b| \end{aligned}$$

Voglio dimostrare che $q = q'$ e $r = r'$

$$\text{Sia } r' > r$$

$$0 < r' - r = (a - bq') - (a - bq) = bq - bq' = b(q - q') < r'$$

$$|b(q - q')| = |b| |q - q'| < r' < |b|$$

$$0 < r - 1 = (d - bq) - (d - bq') = bq - bq' > b(q - q') < r$$

$$|b(q - q')| = |b| |q - q'| < r < |b|$$

$$\Rightarrow |b| |q - q'| < |b|$$

$$\Rightarrow |q - q'| < 1 \quad \Rightarrow \boxed{q = q'}$$

Yellow box

$$\Rightarrow r = a - bq$$

$$\Rightarrow r = r'$$

$$r' > a - bq' = a - bq$$

DIVIDE

venerdì 4 marzo 2022 10:30

DEFINIZIONE

Dat. $a, b \in \mathbb{Z}$ diremo che b divide a

($b|a$) se esiste $c \in \mathbb{Z} \mid a = bc$

PROPRIETÀ

1) $a | 0 \quad \forall a \in \mathbb{Z}$

DIMOSTRAZIONE

$$0 = a \cdot 0$$

2) $0 | a \Rightarrow a = 0$

DIMOSTRAZIONE

$$a = 0 \cdot c = 0$$

3) Se $a | b$ e $b | c$ allora $a | c$

DIMOSTRAZIONE

$$a|b \Rightarrow \exists x \in \mathbb{Z} \mid b = ax$$

$$b|c \Rightarrow \exists y \in \mathbb{Z} \mid c = by = axy$$

$$\Rightarrow a|c$$

4) Se $a|b$ e $b|a$ allora $a = \pm b$

Dimostrazione

$$a|b \Leftrightarrow b = ax \quad x \in \mathbb{Z}$$

$$b|a \Leftrightarrow a = by \quad y \in \mathbb{Z}$$

$$a = axy \Rightarrow xy = 1 \Rightarrow x = y = 1 \Rightarrow a = b$$
$$x = y = -1$$

5)

Se $a|b$ e $a|c \Rightarrow a|bx+cy \quad \forall x, y \in \mathbb{Z}$

Dimostrazione

$$a|b \Leftrightarrow b = az \quad z, t \in \mathbb{Z}$$

$$a|c \Leftrightarrow c = at$$

$$bx + cy = azx + aty = a(zx + ty) \Rightarrow a|bx + cy$$

$$bx+cy = azx+aty = a(zx+ty) \Rightarrow a \mid bx+cy$$

6) $\pm 1, \pm 2$ divides a (divisor: buralı)

DEFINIZIONE

Dati $a, b \in \mathbb{Z}$ ($a, b \neq (0, 0)$) si dice: massimo comun divisore tra a e b , un numero intero d tale che

- 1) $d | a$ e $d | b$
- 2) $d' | a$ e $d' | b \Rightarrow d' | d$

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

PROPOSIZIONE

Siano $a, b \in \mathbb{Z}$, ($a, b \neq (0, 0)$). Allora esiste un $\text{MCD}(a, b)$.

Se d e d' sono MCD $d = \pm d'$

DIMOSTRAZIONE

$$\text{Sia } S = \{ z = ax + by > 0 \mid x, y \in \mathbb{Z} \}$$

$$z = a^2 + b^2 > 0 \quad z \in S \Rightarrow S \neq \emptyset$$

$$\text{Sia } d : \text{l minimo di } S \Rightarrow d = ax_0 + by_0 \quad x_0, y_0 \in \mathbb{Z}$$

$d = ax_0 + by_0$ Dimostro che d è un $\text{MCD}(a, b)$

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

Supponiamo che $d \nmid a \Rightarrow a = dq + r \quad 0 < r < |d|$

$$0 < r = a - dq = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q) \in S < d$$

$r \in S$ con $r < d$ \Rightarrow

- 2) $d' | a$ e $d' | b \Rightarrow d' | d$

$$\begin{aligned} d' | a &\Rightarrow a = d' \cdot \alpha \quad \alpha \in \mathbb{Z} \\ d' | b &\Rightarrow b = d' \cdot \beta \quad \beta \in \mathbb{Z} \end{aligned}$$

$$d = ax_0 + by_0 = d' \alpha x_0 + d' \beta y_0 = d'(ax_0 + \beta y_0) \Rightarrow d' | d$$

3) d, d' sono MCD $\Rightarrow d' = \pm d$

$$\begin{array}{l} d \mid d' \quad \left\{ \begin{array}{l} d' = d \cdot x \\ d' \mid d \quad \left\{ \begin{array}{l} d = d' \cdot y = dxy \Rightarrow d \mid dxy \Rightarrow xy = 1 \Rightarrow x, y = \pm 1 \end{array} \right. \end{array} \right. \end{array}$$

$$\begin{array}{l} d = \text{MCD}(a, b) = (a, b) \\ d = ax_0 + by_0 \quad x_0, y_0 \in \mathbb{Z} \end{array} \quad \left. \begin{array}{l} \text{IDENTITÀ DI BEZOUT} \end{array} \right\}$$

$$2 = 2(-3) + 4(2)$$

$$2 = 2(-1) + 4(1)$$

METODO DELLE DIVISIONI SUCCESSIVE

lunedì 7 marzo 2022 14:45

$$\text{Se } a = bq + r \Rightarrow \text{MCD}(a, b) = b$$

$$a = bq_1 + r_1 \quad 0 < r_1 < b$$

$$b = r_1 q_2 + r_2 \quad 0 \leq r_2 \leq r_1$$

$$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 \leq r_2$$

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

....

$$r_{m-2} = r_{m-1} q_m + r_m \quad 0 < r_m < r_{m-1}$$

$$r_{m-1} = r_m q_{m+1} + 0$$

OSSERVAZIONE

$$a = bq_1 + r_1$$

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

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

$$d_1 = \text{MCD}(b, r_1)$$

$d \mid a \text{ e } d \mid b$ poiché $r = a - bq_1 \Rightarrow d \mid r$

$$d \mid b \Rightarrow d \mid \text{MCD}(b, r_1) = d_1$$

$d_1 \mid b$ e $d_1 \mid r_1$ ma $a = bq_1 + r_1 \Rightarrow d_1 \mid a$ ma $d_1 \mid b$

$$\Rightarrow d_1 \mid \text{MCD}(a, b) = d \Rightarrow d \cdot d'$$

ESEMPIO

$$(1804, 328) = 164$$

$$1804 = 328 \cdot 5 + 164$$

$$328 = \underline{164 \cdot 2 + 0}$$

$$(1547, 560) = 7$$

$$1547 = 560 \cdot 2 + 427$$

$$560 = 427 \cdot 1 + 133$$

$$427 = 133 \cdot 3 + 28$$

$$133 = 28 \cdot 4 + 21$$

$$28 = 21 \cdot 1 + 7$$

$$21 = \underline{7 \cdot 3 + 0}$$

$$(-44880, 5292) = 12$$

$$44880 = 5292 \cdot 8 + 2544$$

$$5292 = 2544 \cdot 2 + 204$$

$$2544 = 204 \cdot 12 + 96$$

$$204 = 96 \cdot 2 + 12$$

$$96 = \underline{12 \cdot 8}$$

DEFINIZIONE

$a, b \in \mathbb{Z}$ sono coprimi se $\text{MCD}(a, b) = 1$

DEFINIZIONE

Un numero $p \in \mathbb{Z}$, $p \neq 0$ e $p \neq \pm 1$ è primo se i suoi divisori sono ± 1 e $\pm p$

PROPRIETÀ

1) Se $a|bc$ e $\text{MCD}(a, c) = 1 \Rightarrow a|b$

2) p primo $p|ab$ allora $p|a$ o $p|b$

$$10 \mid 2 \cdot 5 \quad 10 \nmid 2 \quad 10 \nmid 5$$

DIMOSTRAZIONE

1) $a|bc$ e $\text{MCD}(a, b) = 1 \Rightarrow \exists x_0, y_0 \in \mathbb{Z}$ tali che $1 = ax_0 + by_0 \Rightarrow$

$$\begin{aligned} a|bc &\Rightarrow b \cdot c = a \cdot t \\ &\Rightarrow b = abx_0 + bcy_0 = \\ &= abx_0 + aby_0 = a(bx_0 + ty_0) \\ &\Rightarrow a|b \end{aligned}$$

2) p primo $p|ab \Rightarrow p|a$ o $p|b$

Supponiamo $p \nmid a \quad (\varphi, a) = 1 \Rightarrow p \nmid b$

TEOREMA FONDAMENTALE DELL'ARITMETICA

Se $m > 1$, $m \in \mathbb{N}$. Allora m si decomponga in prodotto di primi:

$Sia m = p_1, p_2, \dots, p_m = q_1, q_2, \dots, q_m \Rightarrow m = m$ e $p_i \in p_j$ per qualche i, j

DIMOSTRAZIONE

Induzione su m

Se $m=2$ è primo OK!

Supponiamo la proprietà vera $\forall k \in \mathbb{N}$ con $k < m$ e proviamolo per m

Se m è primo OK

Se m non è primo m ammette divisioni non banali:

$$\Rightarrow m = h \cdot k \text{ con } h, k < m \quad h, k \neq \pm 1, \pm m$$

Per ipotesi induttiva $\Rightarrow h = p_1 p_2 \dots p_t$
 $k = q_1 q_2 \dots q_s$

$\Rightarrow m = p_1 \cdot p_2 \dots p_t \cdot q_1 \dots q_s$ prodotto di primi

$$m = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$$

$$p_1 \mid m = q_1 q_2 \dots q_m \text{ riordinando i } q_i \quad p_1 \mid q_1 \Rightarrow p_1 = q_1$$

PROPRIETÀ

Esistono infiniti numeri primi

DIMOSTRAZIONI

Supponiamo che \exists un numero finito di numeri primi

$$\text{Sia } \{p_1, p_2, \dots, p_m\}$$

$$z = p_1 p_2 \dots p_m + 1 \quad \text{Sia } p_i \text{ un primo che divide } z$$

$$p_i \mid z \quad p_i \mid p_1, \dots, p_m \Rightarrow p_i \mid z - p_1 \dots p_m = 1 \quad \left. \right\}$$

NUMERI DI FERMAT

venerdì 11 marzo 2022 07:54

$$2^k + 1 \quad k \in \mathbb{Z} \quad \text{per quali valori di } k \text{ sono primi?}$$

$$(a^m + b^m) = (a+b)(a^{m-1} - a^{m-2}b + a^{m-3}b^2 - \dots + 1)$$

m dispari

$$2^k + 1 \quad \text{se } k = d \cdot r \quad d = 2t + 1$$

$$\begin{aligned} 2^k + 1 &= 2^{d \cdot r} + 1 = (2^r)^d + 1 = (2^r)^d + 1^d = \\ &= (2^r + 1)((2^r)^{d-1} - (2^r)^{d-2} + \dots + 1) \end{aligned}$$

$$\text{Affinché } 2^k + 1 \text{ sia primo} \Rightarrow k = 2^m$$

$$2^{2^m} + 1 = F_m$$

CONGETTURA DI FERMAT

$$\forall 2^{2^m} + 1 \text{ sono primi: } F_m$$

EULERO

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

$f_5 : 6416700417 \Rightarrow \text{NON E PRIMO}$

NUMERI DI MERSENNE

venerdì 11 marzo 2022 08:37

$$M_k = 2^k - 1 \quad k \geq 2$$

$$M_2 = 2^2 - 1 = 3 \quad M_3 = 2^3 - 1 = 7 \quad M_4 = 15 \quad M_5 = 31 \quad M_6 = 63 \quad M_7 = 127$$

$$M_k \text{ primo} \Rightarrow k \text{ è primo}$$

$$\text{Se } k \text{ non fosse primo} \quad k = a \cdot b$$

$$2^k - 1 = 2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots + 1)$$

TEOREMA

$$\text{Se } p > 2$$

$$M_p = 2^{p-1} \text{ è primo} \Leftrightarrow M_p \text{ divide } S_p \text{ dove } S_h \text{ è definito ricorsivamente}$$

$$S_2 = 4 \quad S_h = S_{h-1}^2 - 2$$

MINIMO COMUNE MULTIPLO

venerdì 11 marzo 2022 08:49

DEFINIZIONE

Sono $a, b \in \mathbb{Z}$. Il minimo comune mult. plo di a e b è un intero $m \in \mathbb{Z}$ tale che

- 1) m è mult. plo di a e di b
- 2) Se m' è mult. plo di a e di b $\Rightarrow m'$ è mult. plo di m

PROPOSIZIONE

Dati $a, b \in \mathbb{Z}$ esiste il loro minimo comune multiplo $\text{mcm}(a, b) = [a, b]$

$$[a, b] = \frac{|ab|}{(a, b)}$$

$f: A \rightarrow B$ funzione se $\forall a \in A \quad \exists! b \in B$ tale che $b = f(a)$

$f: A \rightarrow B$ funzione se $\forall a \in A \quad \exists ! b \in B$ tale che $b = f(a)$

$\text{Se } a_1 = a_2 \Rightarrow f(a_1) = f(a_2)$

$f: \mathbb{Q} \rightarrow \mathbb{R}$

$$\frac{m}{n} \rightarrow m \cdot n$$

$$|A| = m \quad |B| = n$$

Quante funzioni

$f: A \rightarrow B$ esistono?

$f: A \rightarrow B$

$$A = \{a_1, a_2, \dots, a_m\}$$

$$a_1 \rightarrow (B)$$

$$a_2 \rightarrow (B)$$

:

$$a_m \rightarrow (B)$$

FUNZIONI $|A|^{|B|} = m^n$

$$A = \{1, 2\} \quad B = \{a, b\}$$

$f_1: A \rightarrow B$

$f_2: A \rightarrow B$

$f_3: A \rightarrow B$

$f_4: A \rightarrow B$

$$1 \rightarrow a$$

$$1 \rightarrow a$$

$$1 \rightarrow b$$

$$1 \rightarrow b$$

$$2 \rightarrow 5$$

$$2 \rightarrow 5$$

$$2 \rightarrow 5$$

$$2 \rightarrow 2$$

$$|A|=m$$

$f: A \rightarrow B$, f è iniettiva

ad elementi distinti di A hanno immagini distinte

$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

$$A \Rightarrow B \Rightarrow \sim B \Rightarrow \sim A$$

$$\text{Se } f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

$f: A \rightarrow B$ è suriettiva

se $\forall b \in B \exists a \in A$ tale che $f(a) = b$

$f: \mathbb{Z} \rightarrow \mathbb{N}$

$$a \rightarrow a^2$$

$$\text{Se } a_1 = a_2 \Rightarrow f(a_1) = f(a_2)$$

È iniettiva? Se $f(a_1) = f(a_2) \Rightarrow ? a_1 = a_2$

$$f(a_1) = f(a_2) \quad a_1^2 = a_2^2 \Rightarrow a_1 = \pm a_2$$

È suriettiva?

$$\forall b \in \mathbb{N} \quad \exists a \in \mathbb{Z} ? \quad f(a) = b \Rightarrow a = \pm \sqrt{b} \notin \mathbb{N}$$

$$\nexists b \in \mathbb{N} \quad \exists a \in \mathbb{Z} ? \quad f(a) = b \Rightarrow a = \pm \sqrt{b} \notin \mathbb{N}$$
$$\downarrow$$
$$a^2$$

$|A|=m$ Quante sono le funzioni $f: A \rightarrow A$ bivie?

$f: A \rightarrow A$

$$\begin{array}{l} a_1 \mapsto m \\ a_2 \mapsto m-1 \\ \vdots \\ a_m \mapsto 1 \end{array}$$
$$m! = m(m-1)\dots 1$$

$S_A = \{ f: A \rightarrow A \mid f \text{ bivie} \}$

$|S_A| = m!$ Se $A = \{1, 2, \dots, m\}$

$S_A = S_m = \text{Insieme delle permutazioni di } m \text{ elementi}$

In quanti modi si può programmare

2753

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$|A|=m$ $|B|=n$ Quante sono le $f: A \rightarrow B$ iniettive?

$m \leq n$

$f: A \rightarrow B$

$$\begin{array}{l} a_1 \mapsto m \\ a_2 \mapsto m-1 \\ \vdots \\ a_m \mapsto m-n+1 \end{array}$$

Il numero delle applicazioni iniettive $f: A \rightarrow B$

$|A|=m > n$ $|B|=n$ è

DISPOSIZIONI

$$D_{m,k} = \frac{m!}{(m-k)!}$$

DISPOSIZIONI DI m ELEMENTI A k A k

Sono: sottosinsiemi di k elementi scelti tra gli m att. che differiscono solo per gli elementi che per l'ordine

$$D_{m,k} = \frac{m!}{(m-k)!}$$

COMBINAZIONI

$$C_{m,k} \quad \text{COMBINAZIONI DI } m \text{ ELEMENTI A } k \text{ A } k \quad \text{CHE DIFFERISCONO SOLO PER GLI ELEMENTI}$$

$$\frac{D_{m,k}}{k!} = \frac{m(m-1) \dots (m-k+1)}{k!} = \frac{m!}{k!(m-k)!} = \binom{m}{k}$$

$P(A)$ = insieme delle part. di A = insieme costituito da tutti i sottainsiemi di A

$$A = \{1, 2\}$$

$$P(A) = \{\emptyset, A, \{1\}, \{2\}\}$$

$$\text{Se } |A| = m \Rightarrow |P(A)| = 2^m$$

INDUZIONE SU m

$$\text{Se } m=0 \quad A = \emptyset \quad P(A) = \{\emptyset\} \quad |P(A)| = 2^0 = 1$$

Supponiamo la proprietà vera per m è proviamo per $m+1$

$$|A| = m+1 \Rightarrow |P(A)| = 2^{m+1}$$

$$A = \{a_1, \dots, a_m, a_{m+1}\} = \{a_1, \dots, a_m\} \cup \{a_{m+1}\}$$

$$P(A_{m+1}) = P(A_m) \cup (P(A_m) \cdot a_{m+1})$$

$$|P(A)| = 2^m + 2^m = 2^m(1+1) = 2 \cdot 2^m = 2^{m+1}$$

Esercizio

Per induzione dimostrare che per $m \geq 1$

$$2^{2m} (m!)^2 > (2m)!$$

Per $m=1$

$$2^2 > 2! \rightarrow 4 > 2$$

Supponiamo P_m è vero

$$2^{2(m+1)} ((m+1)!)^2 > (2m+2)!$$

$$2^{2m+2} \cdot 2^2 \cdot (m! \cdot (m+1))^2$$

$$2^{2m+2} \cdot 2^2 \cdot (m!)^2 \cdot (m+1)^2 > 2^2 \cdot (mm!)^2 \cdot (2m)!$$

$$< < (m \cdot (m+1))$$

$$2^{2m} \cdot 2^2 \cdot (m!)^2 (m+1)^2 > 2^2 (mm!)^2 (2m)!$$

$$2 \cdot 2(m+1)(m+1) (2m)!$$

$$2(m+1) \cdot (2m+2) \cdot (2m)!$$

$$(2m+2)(2m+2)(2m)! > (2m+1)(2m+2)(2m)! = (2m+2)! = (2(m+1))!$$

ESERCIZIO

Dimostrare che 3 divide $(4^n - 1)$ $\forall n \geq 1$

$$\text{Per } m=1 \quad (4^1 - 1) = 3 \Rightarrow 3 | 3$$

Supponiamo che per $m \geq n$ vera dimostrazione per $m+1$

$$3 | 4^{m+1} + 1$$

$$4^{m+1} - 4 + 4 - 1 = 4(4^m - 1) + (4 - 1) = 4(4^m - 1) + 3$$

Per ipotesi induttiva

$$3 | 4^m - 1 \Rightarrow 4^m - 1 = 3 \cdot x \quad x \in \mathbb{Z}$$

$$4^{m+1} - 1 = 4 \cdot 3x + 3 = 3(4x + 1) \Rightarrow 3 | 4^{m+1} - 1$$

X CASA

$$1) \quad 6 | m^3 + 5m$$

$$2) \quad 6 | 5^{2m+1} + 1 \quad \forall m \in \mathbb{N} \quad m \geq 1$$

1)

Per $m=1$

$$6 | 1+5 \Rightarrow 6 | 6 \quad \text{VERA}$$

Supponiamo che $P(m)$ è vera

$$6 | (m+1)^3 + 5(m+1)$$

$$6 \mid m^3 + 3m^2 + 3m + 1 + 5m + 5$$

Sappiamo che $m^3 + 5m = 6x$

$$6x + 3m^2 + 3m + 6 \Rightarrow$$

$$6x + 3m(m+1) + 6 \Rightarrow$$

$$6(x + \frac{1}{2}m^2 + \frac{1}{2}m + 1)$$

$$\Rightarrow 6 \mid (m+1)^3 + 5(m+1)$$

2) $6 \mid 5^{2m+1} + 1$

Per $m=1$

$$6 \mid 5^3 + 1 = 6 \mid 126 \quad \text{VERA}$$

Sappiamo che $P(m)$ vero

$$6 \mid 5^{2(m+1)+1} + 1 = 6 \mid 5^{2m+1+2} + 1$$

$$6 \mid 5^{2m+1} \cdot 5^2 + 1 \cdot$$

$$5^{2m+1} + 1 = 6x \quad 5^{2m+1} = 6x - 1$$

$$6 \mid (6x-1)5^2 + 1$$

$$6 \mid 6 \cdot 5^2 - 25 + 1$$

$$6 \mid 6 \cdot 5^2 - 24$$

$$6 \mid 6(5^2 - 4)$$

$$\Rightarrow 6 \mid 5^{2(m+1)+1} + 1 \quad \text{VERA}$$

$$\mathbb{Z} \ni x, y \in \mathbb{Z} \quad x \sim y \Leftrightarrow \frac{x-y}{2} \in \mathbb{Z} \text{ e } 3 \mid \frac{x-y}{2}$$

Dimostrare che è una relazione di equivalenza

1) Riflessiva $x \sim x \quad \frac{x-x}{2} = 0 \in \mathbb{Z} \text{ e } 3 \mid 0$

2) Simmetrica $x \sim y \Rightarrow y \sim x$

$$x \sim y \Rightarrow \frac{x-y}{2} \in \mathbb{Z} \text{ e } 3 \mid \frac{x-y}{2} = z$$

$$\Rightarrow y \sim x \quad \text{per ch} \quad \frac{y-x}{2} = -z \in \mathbb{Z} \text{ e } 3 \mid -z$$

3) Transitiva

$$\text{se } x \sim y \text{ e } y \sim z \Rightarrow x \sim z$$

$$x \sim y \Rightarrow \frac{x-y}{2} \in \mathbb{Z} \text{ e } 3 \mid \frac{x-y}{2}$$

$$y \sim z \Rightarrow \frac{y-z}{2} \in \mathbb{Z} \text{ e } 3 \mid \frac{y-z}{2}$$

$$x \sim z \Rightarrow \frac{x-z}{2} \in \mathbb{Z} \text{ e } 3 \mid \frac{x-z}{2}$$

SORRANNO LE DUE QUANTITA

$$\frac{x-y}{2} + \frac{y-z}{2} = \frac{x-z}{2}$$

CLASSE DI EQUIVALENZA

$$[1]_{\sim} = \{ a \in \mathbb{Z} \mid a \sim 1 \}$$

$$a \sim 1 \Rightarrow \frac{a-1}{2} \in \mathbb{Z} \quad e \quad 3 \mid \frac{a-1}{2}$$

$$\begin{aligned} \frac{a-1}{2} &= z & a-1 &= 2z & 3 \mid z & z = 3t \\ &&&= 2z+1 && \\ &&&= 2(3t)+1 && \\ &&&= 6t+1 && \end{aligned}$$

$$\{ 6t+1 \mid t \in \mathbb{Z} \}$$

X CASA

$$[2]_{\sim} = \{ b \in \mathbb{Z} \mid b \sim 2 \}$$

$$b \sim 2 \Rightarrow \frac{b-2}{2} \in \mathbb{Z} \quad e \quad 3 \mid \frac{b-2}{2}$$

$$\begin{aligned} \frac{b-2}{2} &= z \Rightarrow b-2 = 2z & 3 \mid z & z = 3t \\ &&= 2z+2 & \\ &&= 2(3t)+2 & \\ &&= 6t+2 & \end{aligned}$$

$$\{ 6t+2 \mid t \in \mathbb{Z} \}$$

COEFFICIENTE BINOMIALE

lunedì 14 marzo 2022 14:14

$$\binom{m}{k} = \frac{m!}{k!(m-k)!}$$

1) $\binom{m}{0} = \binom{m}{m} = 1$

$$\binom{m}{0} = \frac{m!}{0!m!} = 1$$

$$\binom{m}{m} = \frac{m!}{m!0!} = 1$$

2) $\binom{m}{k} = \binom{m}{m-k}$

3) $\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}$

2) $\binom{m}{m-k} = \frac{m!}{(m-k)!(m-(m-k))!} = \frac{m!}{(m-k)!m!} = \binom{m}{k}$

3) $\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}$

$$\binom{m}{k} + \binom{m}{k-1} = \frac{m!}{k!(m-k)!} + \frac{m!}{(k-1)!(m+1-k)!}$$

$$= \frac{m!(m+1-k)+m!k}{k!(m+1-k)!} = \frac{m!(m+1-k+k)}{k!(m+1-k)!} = \frac{(m+1)!}{k!(m+1-k)!} = \binom{m+1}{k}$$

$\forall m \geq 1$

$$(x+y)^m = \sum_{k=0}^m \binom{m}{k} x^{m-k} y^k$$

Dimostrazione per induzione su m

$$\text{Se } m=1 \quad (x+y) = \sum_{k=0}^1 \binom{1}{k} x^{1-k} y^k = \binom{1}{0}x + \binom{1}{1}y = x+y \quad \text{VERO}$$

Dimostrazione per induzione su m

$$\text{Se } m=1 \quad (x+y) = \sum_{k=0}^1 \binom{1}{k} x^{m-k} y^k = \binom{1}{0} x + \binom{1}{1} y = x+y \quad \text{VERO}$$

Supponiamo vero per m e proviamo per $m+1$

$$(x+y)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} x^{m+1-k} y^k$$

$$(x+y)^m \cdot (x+y) = \sum_{k=0}^m \binom{m}{k} x^{m-k} y^k \quad (x+y)$$

$$= \left[\binom{m}{0} x^m + \binom{m}{1} x^{m-1} y + \binom{m}{2} x^{m-2} y^2 + \dots + \binom{m}{n} y^m \right] (x+y) =$$

$$= \binom{m}{0} x^{m+1} + \binom{m}{1} x^m y + \binom{m}{2} x^{m-1} y^2 + \dots + \binom{m}{n} x y^m +$$

$$+ \binom{m}{0} x^m y + \binom{m}{1} x^{m-1} y^2 + \binom{m}{2} x^{m-2} y^3 + \dots + \binom{m}{n} y^{m+1} =$$

$$= \binom{m+1}{0} x^{m+1} + \left[\binom{m}{1} + \binom{m}{0} \right] x^m y + \left[\binom{m}{2} + \binom{m}{1} \right] x^{m-1} y^2 + \dots +$$

$$+ \binom{m+1}{m+1} y^{m+1}$$

$$= \sum_{k=0}^m \binom{m+1}{k} x^{m+1-k} y^k$$

TRIANGOLI DI TARTAGLIA

$\begin{array}{ccccccccc} & & & & & & \binom{0}{0} \\ & & & & & & \binom{1}{0} & \binom{1}{1} \\ & & & & & & \binom{2}{0} & \binom{2}{1} & \binom{2}{2} \\ & & & & & & \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} \\ & & & & & & \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} \end{array}$	$\begin{array}{ccccccccc} 1 & & & & & & \binom{0}{0} \\ 1 & 1 & & & & & \binom{1}{0} & \binom{1}{1} \\ 1 & 2 & 1 & & & & \binom{2}{0} & \binom{2}{1} & \binom{2}{2} \\ 1 & 3 & 3 & 1 & & & \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} \\ 1 & 4 & 6 & 4 & 1 & & \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} \end{array}$
---	---

SUCCESSIONE DI FIBONACCI

$$\{F_n\}_{n \geq 1}$$

$$F_m = F_{m-1} + F_{m-2} \quad F_0 = 0 \quad F_1 = 1$$

$$F_1 = 1$$

$$F_2 = F_1 + F_0 = 1 + 0 = 1$$

$$F_3 = F_2 + F_1 = 1 + 1 = 2$$

1 1 2 3 5 8 13 21

RAPPORTO AUREO

lunedì 14 marzo 2022 15:17

DEFINIZIONE

Due grandezze $a, b \quad a > b$ si dicono in rapporto aureo se è medra proporzionale a b ed a $a+b$

$$b : a = a : (b+a)$$

$$b(b+a) = a^2$$

$$\frac{a}{b} = \frac{a+b}{a}$$

Rapporto Aureo

ESERCIZI INDUZIONE

lunedì 14 marzo 2022 15:40

$$m \geq 3 \quad \binom{3m}{2m} \geq 4^m$$

per $m=3$

$$\binom{9}{6} = \frac{9!}{6!3!} = \frac{9 \cdot 8 \cdot 7}{3 \cdot 2} = 84 \geq 4^3 = 64$$

$$\binom{3(m+1)}{2(m+1)} \geq 4^{m+1}$$

$$\binom{3m+3}{2m+2} \geq 4^{m+1}$$

$$= \binom{3m+3}{2m+2} = \frac{(3m+3)!}{(2m+2)!(m+1)!} = \frac{(3m)!(3m+1)(3m+2)(3m+3)}{(2m)!(2m+1)(2m+2)m!(m+1)}$$

$$= \frac{3m!}{2m!m!} \left[\frac{3(3m+1)(3m+2)(3m+3)}{(2m+1)(2m+2)(m+1)} \right] \geq 4^m$$

$$\frac{3(3m+1)(3m+2)}{(2m+1)(2m+2)} \geq 4$$

$$27m^2 + 18m + 9m + 6 \geq 4(4m^2 + 4m + 2m + 2)$$

$$11m^2 + 3m - 2 \geq 0$$

$$m = \frac{-3 \pm \sqrt{9+88}}{22}$$

ESERCIZI INDUZIONE 2

venerdì 18 marzo 2022 08:11

$$3526 = 3 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10 + 6$$

PROPOSIZIONE

$$\forall b > 1, \forall a > 0 \quad a, b \in \mathbb{Z}$$

allora

$$a = r_k b^k + r_{k-1} b^{k-1} + \dots + r_1 b + r_0$$

DIMOSTRAZIONE

INDUZIONE

$$\text{Se } a=1 \quad a = b \cdot 0 + a \quad a = r_0$$

Supponiamo che la proprietà sia vera per tutti $c \in \mathbb{Z}$ con $c < a$ e proviamo per a

Effettuo la divisione di a per b

$$a = bq + r_0 \quad q < a$$

$$\text{per induzione} \quad q = r_k b^{k-1} + r_{k-1} b^{k-2} + \dots + r_1$$

$$a = b(r_k b^{k-1} + r_{k-1} b^{k-2} + \dots + r_1) + r_0 = r_k b^k + r_{k-1} b^{k-1} + \dots + r_1 b + r_0$$

$$(2476)_{10}$$

$$2476 = 1238 \cdot 2 + 0$$

$$1238 = 619 \cdot 2 + 0$$

$$619 = 309 \cdot 2 + 1$$

$$309 = 154 \cdot 2 + 1$$

$$154 = 77 \cdot 2 + 0$$

$$77 = 38 \cdot 2 + 1$$

$$38 = 19 \cdot 2 + 0$$

$$19 = 9 \cdot 2 + 1$$

$$9 = 4 \cdot 2 + 1$$

$$4 = 2 \cdot 2 + 0$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 0 \cdot 2 + 1$$

$$(100110101100)_2$$

$$(b)_b = 10$$

$$b = b \cdot 1 + 0$$

$$1 = b \cdot 0 + 1$$

EQUAZIONI DIOFANTEE

Un'equazione diofantea è un'equazione del tipo

$$ax + by = c \quad a, b, c \in \mathbb{Z}$$

ESEMPIO

$$5x + 7y = 1 \quad (3, -2) \quad (-4, 3)$$

$$\forall a, b \in \mathbb{Z} \quad d \mid a \text{ e } d \mid b \Rightarrow d \mid ax + by \quad \forall x, y \in \mathbb{Z}$$

$$(a, b) = d = ax_0 + by_0$$

PROPOSIZIONE

L'equazione $ax + by = c$ ha soluzione se e solo se $d = (a, b)$ divide c

hcd
↓

DIMOSTRAZIONE

Supponiamo che $ax + by = c$ ammette soluzione

$$\Rightarrow \exists x_0, y_0 \in \mathbb{Z} \mid ax_0 + by_0 = c$$

$$\text{Se } d = (a, b) \Rightarrow d \mid ax_0 + by_0 = c \Rightarrow d \mid c$$

Viceversa se $d = (a, b)$ e supponiamo che $d \mid c$

$$c = ax + by \quad d \mid a \text{ e } d \mid b \Rightarrow d \mid ax + by$$

$$c = d \cdot t \quad t \in \mathbb{Z} \Rightarrow c \cdot (ax_0 + by_0)t = a(x_0t) + b(y_0t) \Rightarrow (x_0t, y_0t) \text{ è soluzione}$$

$$35x + 6y = 2 \quad (35, 6) = 1$$

$$1 = 35 \cdot x_0 + 6 \cdot y_0$$

$$1 = 35(-1) + 6(6)$$

$$2 = 35(-2) + 6(12)$$

$$123x + 6y = 30$$

$$41x + 2y = 10$$

$$\begin{aligned} 1 &= 41(1) + 2(-20) \\ 10 &= 41(10) + 2(-200) \quad (10, 200) \end{aligned}$$

PROPOSIZIONE

$S \ni (\bar{x}, \bar{y})$ una soluzione intera di $ax+by=c$

Tutte le soluzioni sono del tipo

$$(x', y') \text{ con } x' = \bar{x} + \frac{b}{d}t, \quad y' = \bar{y} - \frac{a}{d}t \quad \text{con } d(a, b) \quad \forall t \in \mathbb{Z}$$

$$a\bar{x} + b\bar{y} = c$$

$$a(\bar{x} + \frac{b}{d}t) + b(\bar{y} - \frac{a}{d}t)$$

$$153x + 45y = 18$$

$$17x + 5y = 2 \quad 2 = 17(-4) + 5(14)$$

$$17 = 5 \cdot 3 + 2$$

$$2 = 17 - 5 \cdot 3$$

$$5 = 2 \cdot 2 + 1$$

$$1 = 5 - 2 \cdot 2 = 5 - 2(17 - 5 \cdot 3)$$

$$2 = 2 \cdot 1 + 0$$

$$= 5 + 17(-2) + 5 \cdot 6$$

$$= 17(-2) + 5(7)$$

OSSERVAZIONE

$$\text{MCD}(a_1, a_2, \dots, a_m) =$$

$$= \text{MCD}((a_1, \dots, a_{m-1}), a_m) =$$

In generale l'egazione

$$a_1x_1 + a_2x_2 + \dots + a_mx_m = c \quad \text{con } a_i, c \in \mathbb{Z}$$

ammette soluzione se

$$\text{NCD}(a_1, a_2, \dots, a_n) | c$$

CONGRUENZE MODULO N

venerdì 18 marzo 2022 09:47

CONGRUENZE MODULO m

Sono $a, b, m \in \mathbb{Z}$. Diremo che a è congruo a b modulo m

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

$m \mid a-b$ o equivalentemente se $a-b = m \cdot t \quad t \in \mathbb{Z}$

ESEMPIO

$$\begin{array}{ll} 3 \equiv 1 \pmod{2} & 2 \mid 3-1=2 \\ 7 \equiv 1 \pmod{2} & 2 \mid 7-1=6 \end{array}$$

$a \equiv b \pmod{m}$ se $m \mid a-b$

se $m=0 \quad a-b = 0 \cdot t = 0 \Rightarrow a=b$

se $m=1 \quad a \equiv b \pmod{1} \quad 1 \mid a-b \quad$ È sempre vero

$$\begin{array}{ccc} \text{Se } a \equiv b \pmod{m} & \Rightarrow & a \equiv b \pmod{(-m)} \\ \Downarrow & & \Downarrow \\ m \mid a-b & & -m \mid a-b \end{array}$$

Possiamo supporre $m \geq 2$

\pmod{m}

RELAZIONE DI EQUIVALENZA

REFLESSIVA $a \equiv a \pmod{m} \Rightarrow a-a=0=m \cdot 0$

SIMMETRICA Se $a \equiv b \pmod{m} \Rightarrow m \mid a-b \quad a-b=m \cdot t$

$$\Rightarrow b-a = m(-t) \Rightarrow m \mid b-a \Rightarrow b \equiv a \pmod{m}$$

TRANSITIVA

Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

$$a \equiv b \pmod{m} \Rightarrow a-b=m \cdot h \quad h \in \mathbb{Z}$$

$$b \equiv c \pmod{m} \Rightarrow b - c = m \cdot k \quad k \in \mathbb{Z}$$

$$\begin{aligned} a - b + b - c &= m \cdot h + m \cdot k \\ a - c &= m(h+k) \Rightarrow a \equiv c \pmod{m} \end{aligned}$$

$\equiv \pmod{2}$

$$\begin{aligned} [a] &= \left\{ b \in \mathbb{Z} \mid b \equiv a \pmod{2} \right\} \quad b - a = 2t \\ &\quad \cdot \left\{ b = a + 2t \mid t \in \mathbb{Z} \right\} \end{aligned}$$

$$[0] = \{ 2t \mid t \in \mathbb{Z} \} = [2]$$

$$[1] = \{ 1+2t \mid t \in \mathbb{Z} \}$$

$\equiv \pmod{3}$

$$[a] = \{ b \in \mathbb{Z} \mid b \equiv a \pmod{3} \} = \{ a + 3t \mid t \in \mathbb{Z} \}$$

$$b - a = 3t \quad b = a + 3t$$

$$[0] = \{ 3t \mid t \in \mathbb{Z} \}$$

$$[1] = \{ 1+3t \mid t \in \mathbb{Z} \}$$

$$[2] = \{ 2+3t \mid t \in \mathbb{Z} \}$$

$$\mathbb{Z} \quad a \equiv b \pmod{m} \Leftrightarrow m \mid a - b \quad a - b = m \cdot t$$

$\forall a \in \mathbb{Z} \quad [a] = [r] \quad$ dove r è il resto della divisione di a per m

PROPOSIZIONE

$\forall a \in \mathbb{Z} \quad [a] = [r] \quad$ dove r è il resto della divisione di a per m

DIMOSTRAZIONE

$\forall a \in \mathbb{Z}$, dividendo per $m \Rightarrow a = mq + r$ con $0 \leq r \leq m$

$$\Rightarrow a - r = mq \Rightarrow m | a - r \Rightarrow a \equiv r \pmod{m} \Rightarrow [a] = [r]$$

Definiamo l'insieme quoziente indicando con \mathbb{Z}_m

$$\mathbb{Z}_m = \mathbb{Z}/_{\equiv_m} = \{[0], [1], \dots, [m-1]\}$$

$$\forall a \in \mathbb{Z}, [a] = [r] \quad r = 0, \dots, m-1$$

$$[i] + [j] = [i+j] \quad \text{if } i+j < m \\ [i] + [j] = [i+j-m] \quad \text{if } i+j \geq m$$

\mathbb{Z}_m = insieme delle classi: resto modulo m

$$|\mathbb{Z}_m| = m \text{ elementi} = \left\{ \frac{[0]}{\overline{0}}, \frac{[1]}{\overline{1}}, \dots, \frac{[m]}{\overline{m}} \right\}$$

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

$$7 \equiv_4 \bar{3}$$

$$36 \equiv_7 \bar{1}$$

$$\overline{120} \equiv_9 \overline{30} \equiv_9 \overline{3}$$

$$\mathbb{Z}_m = \mathbb{Z}/_{\equiv_m} = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$$

PROPRIETÀ

Se $a \equiv_m a'$ e $b \equiv_m b'$

- Allora
- 1) $a+b \equiv_m a'+b'$
 - 2) $ab \equiv_m a'b'$

DIMOSTRAZIONE

$$\begin{array}{ll} a \equiv_m a' & \Rightarrow a - a' = mt \\ b \equiv_m b' & \Rightarrow b - b' = mh \end{array} \quad \begin{array}{l} \text{sommando} \\ \text{messo a termine} \end{array} \quad (a - a') + (b - b') = mt + mh$$

$$(a - a') + (b - b') = m(t + h)$$

$$(a+b) - (a'+b') = m(t+h) \Rightarrow (a+a') \equiv_m b+b'$$

$$\begin{array}{ll} 2) \quad a - a' = mt & ab - a'b' = mbt \\ b - b' = mh & \cancel{a'b' - a'b'} = m'a't \\ & \cancel{a'b' - a'b'} = m'a't \end{array} \quad \begin{array}{l} \text{sommando} \\ \text{messo a termine} \end{array}$$

$$ab - a'b' = m(bt + at) \Rightarrow ab \equiv_m a'b'$$

$$\mathbb{Z}_m = \{ \bar{0}, \bar{1}, \dots, \bar{m-1} \}$$

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

$(\mathbb{Z}_m, +)$ GRUPPO ABELIANO

$$(\mathbb{Z}_m, \cdot)$$

$$\forall \bar{a}, \bar{b} \in \mathbb{Z}_m \quad \bar{a} + \bar{b} = \bar{a+b}$$

$$\bar{a} \cdot \bar{b} = \bar{ab}$$

$$\begin{array}{l} \bar{a} = \bar{a}' \\ \bar{b} = \bar{b}' \end{array}$$

$$\begin{array}{l} \bar{a} + \bar{b} = \bar{a}' + \bar{b}' \\ \bar{a} \cdot \bar{b} = \bar{a}' \cdot \bar{b}' \end{array}$$

$$\begin{array}{l} a \equiv_m a' \\ b \equiv_m b' \end{array}$$

$$\begin{array}{l} a+b \equiv_m a'+b' \\ ab \equiv_m a'b' \end{array}$$

Z CON P PRIMO E' UN CAMPO

lunedì 21 marzo 2022 10:23

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

\mathbb{Z}_p con p primo è un campo!

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

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

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

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

*	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$$\mathbb{Z}_m = \mathbb{Z}_{\frac{m}{\gcd(m)}} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{m-1}\}$$

$$(\mathbb{Z}_m, +, \cdot) \quad (\mathbb{Z}_m, +) \quad \text{GRUPPO ABELIANO}$$

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

$$\forall \bar{a}, \bar{b}, \bar{c} \quad (\bar{a} + \bar{b}) + \bar{c} = (\overline{a+b}) + \bar{c} = \overline{(a+b)+c} = \overline{\bar{a} + (b+c)} = \bar{a} + (\overline{b+c}) = \bar{a} + (\bar{b} + \bar{c})$$

$$(\mathbb{Z}_m - \bar{0}, \cdot)$$

ASSOCIAZIONE
ESISTENZA ELEMENTO NEUTRO $\bar{1}$
COMMUTATIVITÀ
DISTRIBUTIVITÀ

$$(\mathbb{Z}_m, +, \cdot) \quad \text{ANELLO COMMUTATIVO CON 1}$$

PROPOSIZIONE

$\bar{a} \in \mathbb{Z}_m$ è invertibile se $\gcd(a, m) = 1$

DIMOSTRAZIONE

$$\begin{aligned} \bar{a} \text{ è invertibile} \Rightarrow & \exists \bar{x} \in \mathbb{Z}_m \mid \bar{ax} = \bar{a}\bar{x} = \bar{1} \Rightarrow ax \equiv 1 \pmod{m} \Rightarrow \\ & \Rightarrow ax - 1 = tm \Rightarrow ax \cdot t_m = 1 \end{aligned}$$

$$\text{Sia } d = \gcd(a, m) \Rightarrow d \mid ax - tm \Rightarrow d \mid 1 \Rightarrow d = 1$$

PROPOSIZIONE

\mathbb{Z}_m è un campo $\Leftrightarrow m = p$

DIMOSTRAZIONE

$$\text{Se } m = p \text{ è primo} \quad \mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \bar{p-1}\}$$

$$p \text{ primo} \Rightarrow (p, i) = 1 \quad \forall i \in \{1, \dots, p-1\}$$

$$\Rightarrow \forall i \in \{1, \dots, p-1\}$$

Viceversa sia \mathbb{Z}_m un campo deve dimostrare che m è primo

$$\Rightarrow m = a \cdot b \quad \bar{m} = \bar{a} \cdot \bar{b} = \bar{0} \quad 0 < a, b \leq m-1 \Rightarrow \bar{a} \text{ NON È INVERTIBILE}$$

PROPOSIZIONE

Sia $a \equiv b \pmod{m}$ $\forall c \in \mathbb{Z}$ s. t.:

- 1) $a+c \equiv_m b+c$
- 2) $ac \equiv_m bc$
- 3) $a^i \equiv_m b^i \quad \forall i \in \mathbb{N}$

DIMOSTRAZIONE

$$1) a \equiv_m b \Rightarrow a-b = tm$$

$$a-b+c-c = tm$$

$$(a+c) - (b+c) = tm$$

$$a+c \equiv_m b+c$$

$$2) a-b = tm$$

$$ac - bc = tmc$$

$$ac \equiv_m bc$$

$$3) \begin{array}{ll} a \equiv_m b & a \equiv_m b \\ a \equiv_m b^m & \Rightarrow ac \equiv_m bd \\ c \equiv_m d & \end{array}$$

$$\Rightarrow a^2 \equiv_m b^2 \Rightarrow a^i \equiv_m b^i$$

PROPOSIZIONE

Se $ac \equiv_m bc$ e $(c, m) = 1 \Rightarrow a \equiv_m b$

Se $ac \equiv_m bc$ allora $a \equiv b \pmod{m/d}$ con $d = (m, c)$

DIMOSTRAZIONE

1) $ac \equiv_m bc \quad (c, m) = 1$

$$ac - bc = mt \Rightarrow (a-b)c = mt \Rightarrow m \mid (a-b)c$$

$$\text{poiché } (m, c) = 1 \Rightarrow m \mid a-b \Rightarrow a \equiv_m b$$

2) $ac \equiv_m bc \Rightarrow ac - bc = mt \quad d = (c, m)$

$$= (a-b) \frac{c}{d} = \frac{m}{d} t \quad \frac{m}{d} \mid (a-b) \frac{c}{d} \quad \left(\frac{m}{d}, \frac{c}{d} \right) = 1$$
$$\Rightarrow \frac{m}{d} \mid a-b \Rightarrow a \equiv b \pmod{\frac{m}{d}}$$

ESEMPIO

$$3 \cdot 5 \equiv_9 3 \cdot 8 \quad 5 \equiv_9 8 \quad \text{NO!}$$

$$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{d}}$$

EQUAZIONI CONGRUENZIALI

giovedì 24 marzo 2022 09:27

È un'equazione del tipo $ax \equiv_m b$ $a, b \in \mathbb{Z}$, x indeterminata

PROBLEMA : Amaette soluzioni intere?

ESEMPIO

$$4x \equiv 7 \pmod{6} \Rightarrow 4x - 7 = 6h \Rightarrow 4x - 6h = 7$$

Non ha soluzioni intere $\leftarrow (4, 6) = 2 \nmid 7$

$$3x \equiv 1 \pmod{4}$$
$$\begin{array}{ll} x = -1 & x = 7 \\ x = 3 & x = 11 \end{array}$$

PROPOSIZIONE

L'equazione $ax \equiv_m b$ ha soluzione $\Leftrightarrow (a, m) \mid b$

DIMOSTRAZIONE

Sia x_0 soluzione di $ax \equiv_m b \Rightarrow ax_0 \equiv_m b$

$$\Rightarrow ax_0 - b = tm \Rightarrow ax_0 + tm = b \quad \text{Se } d = (a, m)$$

$$\Rightarrow d \mid ax_0 + tm = b$$

$$\text{Viceversa } d = (a, m) \mid b \Rightarrow d \mid ax_0 + my_0 \mid b$$

$$\Rightarrow b = dt = (ax_0 + my_0)t = a(x_0t) + m(y_0t)$$

$$\Rightarrow 2(x_0 + t) - b = m(-y_0) \Rightarrow x_0 + t \text{ è soluzione di } 2x \equiv_m b$$

PROPOSIZIONE

Sono \bar{x} ed x_0 soluzioni. Allora $\bar{x} \equiv x_0 \pmod{\frac{m}{d}}$

DIMOSTRAZIONE

$$2\bar{x} \equiv_m b \Rightarrow 2\bar{x} \equiv_m 2x_0 \Rightarrow 2\bar{x} - 2x_0 = tm \Rightarrow 2x_0 \equiv_m b$$

$$\Rightarrow 2(\bar{x} - x_0) = tm \Rightarrow \frac{2}{d}(\bar{x} - x_0) = \frac{tm}{d}$$

$$\Rightarrow \frac{m}{d} \mid (\bar{x} - x_0) \frac{2}{d} \quad \left(\frac{m}{d}, \frac{2}{d} \right) = 1$$

$$\Rightarrow \frac{m}{d} \mid \bar{x} - x_0 \quad \bar{x} \equiv x_0 \pmod{\frac{m}{d}}$$

$$\bar{x} = x_0 + t \frac{m}{d} \quad t \in \mathbb{Z}$$

Quelle distinte $\pmod{\frac{m}{d}}$ si ottengono per $t = 0, 1, \dots, d-1$

$$7x \equiv 3 \pmod{5} \quad (7, 5) = 1$$

$$1 = 7 \cdot x_0 + 5 \cdot y_0$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) =$$

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

$$7(-2) \equiv 1 \pmod{5}$$

$$7(-6) \equiv 3 \pmod{5}$$

$$x_0 = -6$$

Tutte le soluzioni

$$\bar{x} = x_0 + tm$$

$$= -6 + 5t$$

EQUAZIONI CONGRUENZIALI 2

venerdì 25 marzo 2022 08:16

PROPOSIZIONE

$ax \equiv_m b$ ha soluzione $\Leftrightarrow (a, m) = d | b$

Se x_0 e \bar{x} sono soluzioni: $\bar{x} = x_0 + t \frac{m}{d} \quad t \in \mathbb{Z}$

Le soluzioni distinte mod m sono d es: ottengono $t = 0, \dots, t-1$

TEOREMA

$ax \equiv_m b$ se $(a, m) = 1$

ammette una sola soluzione mod m

ESERCIZIO

$$327x \equiv 11 \pmod{52} = 1$$

$$\begin{aligned} 327 &= 52 \cdot 6 + 15 & 1 &= 15 - 7 \cdot 2 = 15 - (52 - 15 \cdot 3) \cdot 2 = \\ 52 &= 15 \cdot 3 + 7 & &= 52 \cdot (-2) + 15 \cdot 7 \\ 15 &= 7 \cdot 2 + 1 & &= 52 \cdot (-2) + (327 - 52 \cdot 6) \cdot 7 = \\ 7 &= 1 \cdot 7 & &= 327 \cdot 7 + 52 \cdot (-44) \end{aligned}$$

$$1 = 327 \cdot 7 + 52 \cdot (-44)$$

$$\bar{x} = 25 + t \cdot 52 \quad t \in \mathbb{Z}$$

$$327 \cdot 7 \equiv 1 \pmod{52}$$

$$327 \cdot 77 \equiv 11 \pmod{52}$$

$$x_0 = 77 \equiv 25 \pmod{52}$$

$$220x \equiv 12 \pmod{16}$$

$$d = (220, 16) = 4$$

$$4 | 12$$

$$220 = 16 \cdot 13 + 12$$

$$4 = 16 \cdot 12 = 16 - (220 - 16 \cdot 13) =$$

$$16 = 12 \cdot 1 + 4$$

$$= 220 \cdot (-1) + 16 \cdot 14$$

$$12 = 4 \cdot 3$$

$$220 \cdot (-1) \equiv 4 \pmod{16}$$

$$220 \cdot (-3) \equiv 12 \pmod{16}$$

$$x = -3 + t \frac{m}{d}$$

$$x = -3 + 4t \quad t \in \mathbb{Z}$$

Le soluzioni distinte mod 16 sono

$$x = -3$$

$$[-3]_{16} + [1]_{16} + [5]_{16} + [9]_{16}$$

$$x = 1$$

$$x = 5$$

$x = 9$

TEOREMA CINESE DEL RESTO

venerdì 25 marzo 2022 09:00

Un sistema di congruenze è

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1} \\ a_2x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_tx \equiv b_t \pmod{m_t} \end{cases}$$

Una soluzione è $x_0 \in \mathbb{Z}$ che soddisfa le singole congruenze

$$(a_i, m_i) \mid b_i \quad \forall i = 1, \dots, t$$

* è equivalente ad un sistema del tipo

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \vdots \\ x \equiv c_t \pmod{m_t} \end{cases}$$

TEOREMA CINESE DEL RESTO

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_t \pmod{m_t} \end{cases} \quad \text{con la condizione } (m_i, m_j) = 1$$

Allora il sistema è compatibile (ammette soluzioni)

Se x_0 ed \bar{x} sono soluzioni allora $\bar{x} \equiv x_0 + h(m_1 \cdot m_2 \cdot m_3 \cdots m_t)$

È una condizione sufficiente

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{4} \end{cases} \quad (2, 4) = 2$$

$$x = 1 + 4t \quad t \in \mathbb{Z}$$

DIMOSTRAZIONE

$$(m_i, m_j) = 1 \quad \forall i \neq j$$

$$N = m_1, m_2, \dots, m_t \quad N_i = \frac{N}{m_i}$$

$$(N_i, m_i) = 1$$

$$N_1 x \equiv a_1 \pmod{m_1} \Rightarrow x_1 \text{ soluzione}$$

$$N_2 x \equiv a_2 \pmod{m_2} \Rightarrow x_2 \text{ soluzione}$$

:

$$N_t x \equiv a_t \pmod{m_t} \Rightarrow x_t \text{ soluzione}$$

$\bar{x} = N_1 x_1 + N_2 x_2 + \dots + N_t x_t$ è soluzione del nostro sistema

$$N_1 x_1 + N_2 x_2 + \dots + N_t x_t \equiv a_1, \quad a_1 + 0 + \dots + 0 \equiv a_1$$

$m_r \mid N_i \quad \forall r \neq i \Rightarrow \bar{x}$ è soluzione del sistema

Sia y un'altra soluzione $\Rightarrow y \equiv \bar{x} \pmod{(m_1, m_2, \dots, m_t)}$

$$y \equiv a_i \pmod{m_i} \quad \forall i = 1, \dots, t$$

$$\bar{x} \equiv a_i \pmod{m_i} \quad \forall i = 1, \dots, t \quad \Rightarrow y \equiv \bar{x} \pmod{m_i} \quad \forall i$$

$\Rightarrow y - \bar{x}$ è multiplo del $\text{MCM}(m_1, m_2, \dots, m_t) = m_1 \cdot m_2 \cdot \dots \cdot m_t$

$$\Rightarrow y \equiv \bar{x} \pmod{m_1 \cdot m_2 \cdot \dots \cdot m_t}$$

$$y - \bar{x} = h_1 m_1$$

$$y - \bar{x} = h_2 m_2$$

:

$$y - \bar{x} = h m t$$

ESERCIZI EQUAZIONI CONGRUENZIALI

venerdì 25 marzo 2022 09:27

$$\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 5 \pmod{8} \end{cases} \quad (7,8) = 1$$

$$N = m_1 m_2 = 7 \cdot 8 = 56$$

$$N_1 = \frac{N}{m_1} = \frac{56}{7} = 8$$

$$N_2 = \frac{N}{m_2} = \frac{56}{8} = 7$$

$$\begin{cases} 8x \equiv 4 \pmod{7} \\ 7x \equiv 5 \pmod{8} \end{cases}$$

$$1) 8x \equiv 4 \pmod{7} \quad (8,7) = 1$$

$$2) 7x \equiv 5 \pmod{8} \quad (7,8) = 1$$

$$1) \quad 1 = 8(1) + 7(-1)$$

$x_1 = 4$ è soluzione

$$8(1) \equiv 1 \pmod{7}$$

$$1 = 8(1) + 7(-1)$$

$$2) \quad 7(-1) \equiv 1 \pmod{8}$$

$$\bar{x} = N_1 x_1 + N_2 x_2$$

$$\bar{x} = 8 \cdot 4 + 7 \cdot (-5) = -3$$

VERIFICARE CON IL SISTEMA DI PARTENZA

$$\begin{cases} x \equiv 5 \pmod{3} \\ x \equiv 7 \pmod{8} \\ x \equiv 2 \pmod{5} \end{cases}$$

$$N = 3 \cdot 8 \cdot 5 = 120$$

$$N_1 = \frac{N}{3} = 40$$

$$1) 40x \equiv 5 \pmod{3}$$

$$N_2 = \frac{N}{8} = 15$$

$$2) 15x \equiv 7 \pmod{8}$$

$$N_3 = \frac{N}{5} = 24$$

$$3) 24x \equiv 2 \pmod{5}$$

$$x = 2 \text{ è soluzione}$$

$$(40, 3) = 1 \quad 40 = 3 \cdot 13 + 1$$

$$1 = 40(1) + 3(-13) \quad 40(1) = 1 \bmod 3 \Rightarrow x=5 \Rightarrow x \equiv 2$$

2) $x=1$ è soluzione

3) $(24, 5) = 1 \quad 1 = 5(5) + 24(-1) \quad x = -2$ è soluzione

$$\bar{x} = N_1 x_1 + N_2 x_2 + N_3 x_3$$

$$= 40 \cdot 2 + 15 \cdot 1 + 24 \cdot (-2) =$$

$$= 80 + 15 - 48 \bmod 120$$

$$= 47 \bmod 120$$

ESERCIZI EQUAZIONI CONGRUENZIALI 2

domenica 27 marzo 2022 17:37

$$\left\{ \begin{array}{l} a_1 x_1 \equiv b_1 \pmod{m_1} \\ a_2 x_2 \equiv b_2 \pmod{m_2} \\ \vdots \\ a_t x_t \equiv b_t \pmod{m_t} \end{array} \right. \quad \begin{array}{l} (a_i, m_i) = d \mid b_i \quad \forall i = 1, \dots, t \\ (m_i, m_j) = 1 \end{array}$$

$$\frac{a_1}{d_1} x_1 \equiv \frac{b_1}{d_1} \pmod{\frac{m_1}{d_1}}$$

$$\frac{a_2}{d_2} x_2 \equiv \frac{b_2}{d_2} \pmod{\frac{m_2}{d_2}}$$

$$\left\{ \begin{array}{l} a'_1 x_1 \equiv b'_1 \pmod{m'_1} \\ a'_2 x_2 \equiv b'_2 \pmod{m'_2} \\ \vdots \\ a'_t x_t \equiv b'_t \pmod{m'_t} \end{array} \right.$$

$$a'_i = \frac{a_i}{d_i} \quad b'_i = \frac{b_i}{d_i} \quad m'_i = \frac{m_i}{d_i}$$

$(a'_i, m'_i) = 1$ ogni equazione ammette soluzione unica modulo m'_i sia che

$$\left\{ \begin{array}{l} x_1 \equiv c_1 \pmod{m'_1} \\ x_2 \equiv c_2 \pmod{m'_2} \\ \vdots \\ x_t \equiv c_t \pmod{m'_t} \end{array} \right.$$

$$\left\{ \begin{array}{l} 7x \equiv 1 \pmod{6} \\ 5x \equiv 3 \pmod{7} \end{array} \right.$$

$$\left\{ \begin{array}{l} x \equiv 1 \pmod{6} \\ x \equiv 2 \pmod{7} \end{array} \right.$$

$$N = 6 \cdot 7 \quad N_1 = 7 \quad N_2 = 6$$

$$7x \equiv 1 \pmod{6} \quad x_1 \equiv 1$$

$$6x \equiv 2 \pmod{7}$$

$$(6, 7) = 1 \quad 1 = 7(1) + 6(-1) \quad x_2 = -2$$

$$\bar{x} = N_1 x_1 + N_2 x_2$$

$$7(1) + 6(-2) = 7 - 12 = -5 \bmod 42$$

PICCOLO TEOREMA DI FERMAT

lunedì 28 marzo 2022 13:10

PROPOSIZIONE

$\forall x, y \in \mathbb{Z}, \forall p \text{ primo}$

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

DIMOSTRAZIONE

$$\binom{p}{i} i! (p-i)! = p! \Rightarrow p \mid \binom{p}{i} i! (p-i)!$$

$$i, p-i < p \quad i \neq p \Rightarrow p \mid \binom{p}{i}$$

$$(x+y)^p = \sum_{i=0}^p \binom{p}{i} x^{p-i} y^i = x^p + \binom{p}{1} x^{p-1} y + \binom{p}{2} x^{p-2} y^2 + \dots + \binom{p}{p} y^p$$

↳ a $p-1$ ↓
z $\equiv 0 \pmod{p}$

$$\equiv_p x^p + y^p$$

PICCOLO TEOREMA DI FERMAT

Se $a \in \mathbb{Z}, p \text{ primo}$

$$\text{Allora } a^p \equiv a \pmod{p}$$

DIMENSIONE

Induzione su a , 230

$$\text{Se } a \neq 0 \quad a^p \equiv 0 \pmod{p}$$

Supponiamo la proprietà sia vera per a e dimostriamolo per $a+1$

Dimostriamo che

$$(a+1)^p \equiv a+1 \pmod{p}$$

$$(a+1)^p \geq a^p + 1 \pmod{p} \geq a+1 \pmod{p}$$

Sia $a < 0 \Rightarrow -a > 0$

$$0 = a + (-a)$$

$$0^p = [a + (-a)]^p \equiv a^p + (-a)^p \pmod{p} \equiv a^p + (-a)$$

$$\begin{aligned} a^p + (-a) &\equiv 0 \pmod{p} \\ a^p &\equiv a \pmod{p} \end{aligned}$$

Dalché $-a > 0$ per la 1^a parte della dimostrazione $(-a)^p \equiv (-a) \pmod{p}$

COROLARIO

\forall primo, $\forall a \in \mathbb{Z}$, $(a,p) = 1$ allora $a^{p-1} \equiv 1 \pmod{p}$

DIMOSTRAZIONE

$$a^p \equiv a \pmod{p} \Rightarrow p \mid a^p - a \equiv a(a^{p-1} - 1)$$

$$\Rightarrow p \mid a(a^{p-1} - 1) \text{ poiché } (p,a) = 1 \Rightarrow p \mid (a^{p-1} - 1) \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

ESEMPIO

Determinare il resto della divisione per 7 del numero 3526^{351}

$$\begin{array}{r} 3526 \\ 5 \mid \overline{503} \end{array}$$

$$3526 \equiv 7 \cdot 503 + 5$$

$$3526 \equiv 5 \pmod{7}$$

$$3526^{351} \equiv 5^{351} \pmod{7} \quad (5,7) = 1 \quad 5^{p-1} \equiv 1 \pmod{p}$$

$$5^6 \equiv 1 \pmod{p}$$

$$\begin{array}{r} 351 \\ 3 \mid \overline{58} \end{array}$$

$$351 = 58 \cdot 6 + 3$$

$$\begin{aligned} 5^{351} &\equiv 5^{6 \cdot 58 + 3} \equiv 5^{6 \cdot 58} \cdot 5^3 \equiv (5^6)^{58} \cdot 5^3 \equiv 1^{58} \cdot 5^3 \pmod{7} \\ &\equiv 5^3 \pmod{7} \end{aligned}$$

$$125 \overline{) 77}$$

$$3526^{351} \equiv 6 \pmod{7}$$

$$15^{1443} \equiv x \pmod{17}$$

$$(15, 17) = 1 \quad a^{p-1} \equiv 1 \pmod{p}$$

$$15^{16} \equiv 1 \pmod{16}$$

$$1443 \overline{) 16}$$

$$1443 = 16 \cdot 90 + 3$$

$$15^{1443} = (15^{16})^{90} \cdot 15^3 \equiv 15^3 \pmod{17}$$

$$\equiv 15^2 \cdot 15 \pmod{17} \equiv 4 \cdot 15 \pmod{17} \equiv \\ \equiv 60 \pmod{17} \equiv 9 \pmod{17}$$

$$15^{1443} \equiv 9 \pmod{17}$$

FUNZIONE DI EULERO

lunedì 28 marzo 2022 13:59

$$\varphi(n) = \{ m \mid m \leq n, \gcd(m, n) = 1 \}$$

DEFINIZIONE

Se $m \geq 1$ la funzione di Eulero è una funzione $\varphi: \mathbb{N} \rightarrow \mathbb{N}$

$$m \mapsto \varphi(m)$$

$\varphi(m)$ è il numero dei naturali $< m$ e coprimi con m

$$\varphi(1) = 1$$

ESEMPIO

$$\varphi(4) = 2$$

$$\varphi(5) = 4$$

$$\varphi(18) = 6$$

PROPRIETÀ

1) Se $(m, n) = 1$ $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

2) p primo $\varphi(p) = p - 1$

3) p primo $\forall k \quad \varphi(p^k) = p^k - p^{k-1}$

4) $\forall m = p_1^{t_1} \cdot p_2^{t_2} \cdots p_m^{t_m}$

$$\varphi(m) = \varphi(p_1^{t_1}) \cdot \varphi(p_2^{t_2}) \cdots \varphi(p_m^{t_m})$$

DIMOSTRAZIONE

2) $\varphi(p) = p - 1$ poiché tutti i naturali $< p$ sono coprimi con p

3) $\varphi(p^k)$ tutti i naturali $< p^k$ e non coprimi con p^k devono essere multipli di p e sono in numero p^{k-1}

TEOREMA DI EULERO

$s \in \mathbb{Z}, m \in \mathbb{N}$

$$(a, m) = 1 \text{ allora } a^{\varphi(m)} \equiv 1 \pmod{m}$$

$$\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3 \cdot 3) = \varphi(2^3) \cdot \varphi(3) = (2^3 - 2^2)(2) = 4 \cdot 2 = 8$$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = 2 \cdot 20 = 40$$

Calcolare le ultime due cifre di 421^{323}

$$z = a_m a_{m-1} \dots a_1 a_0 \equiv a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \dots + a_1 \cdot 10 + a_0$$

$$421^{323} \equiv 21^{323} \pmod{100} \quad (21, 100) = 1 \quad \varphi(100) = 40$$

Per il Teorema di EULERO $21^{\varphi(100)} \equiv 1 \pmod{100}$ $21^4 \equiv 1 \pmod{100}$

$$421^{323} \equiv_{100} 21^{323} \equiv_{100} (21^{40})^8 \cdot 21^3 \equiv_{100} 21^3 \equiv_{100} 21^2 \cdot 21 \equiv_{100} 41 \cdot 21 \equiv_{100} 61$$

$$21^{40} \equiv 1 \pmod{100}$$
$$323 \mid \frac{40}{8}$$
$$323 = 40 \cdot 8 + 3$$

Ultime due cifre di 112302^{42}

$$112302^{42} \equiv_{100} 2^{42}$$

CRITERI DI DIVISIBILITÀ

lunedì 28 marzo 2022 14:37



Un numero è divisibile per 3 (per 9) se la somma delle sue cifre è divisibile per 3

$$a_m a_{m-1} a_{m-2} \dots a_1 a_0 = a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0$$

$$10 \equiv 1 \pmod{3} \quad (\pmod{9})$$

$$10^i \equiv 1 \pmod{3} \quad (\pmod{9})$$



$$a_m a_{m-1} \dots a_1 a_0 = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \dots + a_1 \cdot 10 + a_0 \equiv a_0 \pmod{2}$$

$$10 \equiv 0 \pmod{2} \quad (\pmod{5})$$

Un numero intero è divisibile per 2 \Leftrightarrow a_0 è divisibile per 2
 (per 5) $\qquad\qquad\qquad$ (per 5)



$$10 \equiv -1 \pmod{11}$$

$$10^i \equiv_{11} \begin{cases} 1 & \text{se } i \text{ è pari} \\ -1 & \text{se } i \text{ è dispari} \end{cases}$$

$$\equiv_{11} a_0 - a_1 + a_2 - \dots + (-1)^m a_m$$

$$\varphi(p) = p - 1$$

$$\varphi(p^k) = p^k - p^{k-1}$$

$\varphi(p^k) = p^k - (\text{numero degli interi } x \text{ che non sono coprimi con } p^k \quad 1 \leq x \leq p^k)$

$$\Rightarrow x = p \cdot i \quad 1 \leq i \leq p^{k-1} \quad \varphi(p^k) = p^k - p^{k-1}$$

ESEMPIO

$$p = 3 \quad p^2 = 9$$

1 2 $\textcircled{3}$ 4 5 $\textcircled{6}$ 7 8 $\textcircled{9}$

$$p \cdot i \quad i=1, \quad p^1 = 1, 2, 3$$

3, 6, 9

G insieme non vuoto, dotato di un'operazione $*$ dicesi gruppo se

- 1) * ASSOCIAZIONE: $\forall a, b, c \in G \quad (a * b) * c = a * (b * c)$
- 2) * \exists ELEMENTO NEUTRO: $e \in G, \forall a \in G \quad (a * e) = (e * a) = a$
- 3) * SOTTRACCIONE: $\forall a \in G, \exists a' \text{ tale che } a * a' = a' * a = e$

Se $*$ è commutativa G si dice GRUPPO ABELIANO

$$(G, \cdot) \quad e = 1 \quad a' = a^{-1}$$

$$(G, +) \quad e = 0 \quad a' = -a \quad \forall a \in G$$

Esemp: di gruppo $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$

$$(\mathbb{Q}^*, \mathbb{Q} - \{0\}, \cdot) \quad (\mathbb{R}^*, \mathbb{R} - \{0\}, \cdot) \quad (\mathbb{C}^*, \cdot) \quad \text{GRUPPI ABELIANI}$$

Esempio d: gruppo non abeliano $GL_n(k) \leftarrow$ INSIEME OGNI MATEZI INVERTIBILI

$$A = \text{insieme} \quad S_A = \{ f: A \rightarrow A \mid f \text{ è biunivoco} \}$$

(S_A, \circ) è un gruppo

\circ è intorno

la composizione di 2 applicazioni biunivoco è biunivoco

$\exists id =$ elemento neutro

$\forall f: A \rightarrow A$ biunivoco $\exists f: A \rightarrow A$ biunivoco

Se $A = \{1, 2, \dots, n\}$

$$S_A = S_N \quad |S_N| > n!$$

$$S_N = \{ f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \mid f \text{ è biunivoca} \}$$

$$f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

$$\begin{array}{ccc} 1 & \rightarrow & f(1) \\ 2 & \rightarrow & f(2) \\ \vdots & & \\ n & \rightarrow & f(n) \end{array}$$

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \quad S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \text{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \delta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\delta_1 \circ \delta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\delta_1 \circ \delta_2(i) = \delta_1(\delta_2(i))$$

$$\delta_1 \circ \delta_2(1) = \delta_1(3) = 3$$

$$\delta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \delta_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\delta_3 \circ \delta_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \delta_3 \circ \delta_4 \neq \delta_4 \circ \delta_3$$

$$\delta_4 \circ \delta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad S_3 \text{ non è commutativo}$$

S_m per $m \geq 3$ non è commutativo

DEFINIZIONE

Un ciclo di lunghezza k è una permutazione che muove k elementi e fissa gli altri.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} \quad \text{3. ciclo} \\ = (1\ 5\ 3)(2)(4), (1\ 5\ 3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 7 & 1 & 6 & 4 \end{pmatrix} = (1\ 3\ 5)(4\ 7), \quad \text{CICLI DISGIUNTI}$$

PROPOSIZIONE

Ogni permutazione è prodotto di cicli disgiunti.

$$S_8 \quad \begin{matrix} \delta_2 & & \delta_1 \\ 1 \rightarrow 1 & \rightarrow 3 \end{matrix} \\ \begin{matrix} \delta_1 & & \delta_2 \\ (1\ 3\ 5) & (5\ 7\ 8\ 3) & = (1\ 3) \end{matrix}$$

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

DEFINIZIONE

Un ciclo di lunghezza 2 si dice trasposizione.

$$(1\ 3)$$

PROPOSIZIONE

Un ciclo di lunghezza k è prodotto di k-1 trasposizioni.

Dimostrazione

$$(i_1 i_2 \dots i_{k-1} i_k) = (i_1 i_k)(i_1 i_{k-1})(i_1 i_{k-2})$$



$$(2\ 3\ 5\ 7\ 9\ 11\ 6) = (2\ 6)(2\ 11)(2\ 9)(2\ 7)(2\ 5)(2\ 3) \cdot (1\ 2)(1\ 2)$$

$$(1\ 2)(1\ 2) = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \text{id}$$

$$f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$$

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

$$\begin{array}{rcl} 1 & \rightarrow & 2 \\ 2 & \rightarrow & 4 \\ 3 & \rightarrow & 1 \\ 4 & \rightarrow & 3 \end{array}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

$$f^{-1}: A \rightarrow A$$

$$a \rightarrow f^{-1}(a)$$

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

$$(1\ 2\ 3)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3\ 2) = (3\ 2\ 1)$$

PERMUTAZIONE

venerdì 22 aprile 2022 11:39

Ogni permutazione si scrive in prodotto di cicli disgiunti.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 6 & 3 \end{pmatrix} = (1\ 2\ 4)(3\ 5\ 6) = (3\ 5\ 6)(1\ 2\ 4)$$

Ogni ciclo di lunghezza k è prodotto di k-1 cicli di lunghezza 2 (trasposizioni)

$$(i_1, i_2, \dots, i_k) = (i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_2)$$

$$(3\ 4)(3\ 4) = \text{id}$$

$$(5\ 6\ 7\ 9\ 8) = (5\ 8)(5\ 9)(5\ 6)(5\ 7) \cdot \\ = (5\ 8)(5\ 9)(5\ 6)(5\ 7)(1\ 4)(1\ 4)$$

PROPOSIZIONE

Un ciclo è sempre prodotto o di un numero pari di trasposizioni o di un numero dispari.

DEFINIZIONE

Una permutazione si dice pari se è prodotto di un numero pari di trasposizioni, dispari in caso contrario.

CONSEGUENZA

Un ciclo di lunghezza k è pari se k è dispari
dispari se k è pari

$$(1\ 3\ 5\ 7\ 6) = (1\ 6)(1\ 7)(1\ 5)(1\ 3)$$

$$(1\ 5\ 7\ 6)(4\ 3\ 2) = (1\ 6)(1\ 7)(1\ 5)(4\ 2)(4\ 3)$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

$$(1) = \text{id} \quad (1\ 2) \quad (1\ 3) \quad (2\ 3) \quad (1\ 3\ 2) \quad (1\ 2\ 3)$$

$$\begin{array}{ll} \text{LUNGHEZZA PARI} & \left\{ \text{id}, (123), (132) \right\} \\ \text{DISPARI} & \left\{ (12), (13), (2,3) \right\} \end{array}$$

$$\det A = \sum_{\sigma \in S_n} (-1)^{\sigma} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

PROPRIETA' DEI GRUPPI (G, \cdot)

- 1) elemento neutro è unico
- 2) l' inverso è unico
- 3) $(ab)^{-1} = b^{-1}a^{-1}$
- 4) Se $ax = bx$

DIMOSTRAZIONE

- 1) Sono e_1, e_2 elementi neutri

$$e_1 = e_1 \cdot e_2 = e_2$$

- 2) $a \in G$ e supponiamo che a_1, a_2 sono inversi di a

$$aa_1 = a_1 a = e$$

$$aa_2 = a_2 a = e$$

$$a_1 = a_1 \cdot e = a_1 \cdot a \cdot a_2 = e \cdot a_2 = a_2$$

- 3) $(ab)(b^{-1}a^{-1}) = e$

$$(b^{-1}a^{-1})(ab) = e$$

$$(a \cdot b)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$$

- 4) Se $ax = bx$, moltiplico per x^{-1} a destra

$$a(x \cdot x^{-1}) = b(x \cdot x^{-1})$$

$$a = b$$

$$[(1356)(24)]^{-1} = (24)^{-1}(1356)^{-1} = (24)(6531)$$

$$(1356)(24)(24)(6531) = (1356)(6531) = (1)(3)(5)(6)$$

$(\{1, -1\}, \cdot)$ è un gruppo

$(\{1, -1, i, -i\}, \cdot)$ è un gruppo $(-i)^{-1} = i$ $i^2 = -1$

$(\mathbb{Z}, +)$

~~non è~~

$(\mathbb{Z}, +)$

~~#~~

$(\mathbb{Z}_m, +)$ è un gruppo

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

DEFINIZIONE

Se (G, \cdot) gruppo. Un sottoinsieme $H \subseteq G$ è sottogruppo di G se rispetto all'operazione definita in G è gruppo

(H, \cdot)

PROPOSIZIONE

$$H \subseteq G \text{ è sottogruppo} \Leftrightarrow \forall a, b \in H \Rightarrow a \cdot b^{-1} \in H$$

DIMOSTRAZIONE

$$\text{Se } H \text{ è sottogruppo} \Rightarrow a \cdot b^{-1} \in H \quad \forall a, b \in H$$

$$\text{Viceversa supponiamo che } \forall a, b \in H \Rightarrow a \cdot b^{-1} \in H$$

$$\forall a \in H \quad a \cdot a^{-1} = 1_G \in H$$

$$1 \in H, \forall b \in H \Rightarrow 1 \cdot b^{-1} \in H \quad \forall b \exists b^{-1} \in H$$

$$\forall a, b \in H \stackrel{?}{\Rightarrow} a \cdot b \in H$$

$$\begin{array}{ll} b^{-1} \in H & \\ \parallel & \\ a \cdot (b^{-1})^{-1} & \end{array}$$

OSSERVAZIONE

$$\text{Se } (G, +), \quad H \subseteq G \text{ è sottogruppo} \Leftrightarrow \forall a, b \in H, \quad a - b \in H$$

ESEMPI

$$(\mathbb{Z}, +) \quad P = \{2h \mid h \in \mathbb{Z}\} \text{ è un sottogruppo di } \mathbb{Z}?$$

$$\forall p_1, p_2 \in P \quad p_1 - p_2 \in P$$

$$p_1 = 2h$$

$$p_2 = 2k$$

$$p_1 - p_2 = 2h - 2k = 2(h - k) \in \mathbb{Z}$$

$$D = \{2h+1 \mid h \in \mathbb{Z}\}$$

$$\begin{aligned} d_1 &= 2h+1 \\ d_2 &= 2k+1 \end{aligned} \quad d_1 \cdot d_2 = (2h+1) \cdot (2k+1) = 2h \cdot 2k + 2(h+k)$$

$$GL_m(K) = \{ A \in M_m(K) \mid A \text{ invertibile} \}$$

$U = \{ A \in GL_m(K) \mid \det A = 1 \}$ È un sottogruppo

$$\forall A, B \in U \Rightarrow A \cdot B^{-1} \in U$$

$$\det(A \cdot B^{-1}) = \det A \cdot \det(B^{-1}) = 1 \cdot 1 = 1$$

Ogn: gruppo ammette sottogruppi banali:

$$(G, \cdot) \quad \{1\} \subset G$$

$$(G, +) \quad \{0\} \subset G$$

DEFINIZIONE

$\langle a \rangle \subset (G, \cdot)$ Se $a \in G$. Dici si sottogruppo ciclico generato da a il sottogruppo di G

$$\langle a \rangle = \{a^h \mid h \in \mathbb{Z}\}$$

$$\langle a \rangle \subset (G, +) \quad \langle a \rangle = \{ha \mid h \in \mathbb{Z}\}$$

PROPOSIZIONE

$\langle a \rangle$ è un sottogruppo di G

DIMOSTRAZIONE

$$\forall a^h, a^k \in \langle a \rangle \Rightarrow a^h (a^k)^{-1} = a^h a^{-k} = a^{h-k} \in \langle a \rangle$$

$$(\mathbb{Z}, +)$$

$$\forall a \in \mathbb{Z} \quad \langle a \rangle = \{ha \mid h \in \mathbb{Z}\}$$

PROPOSIZIONE

\exists almeno un sottogruppo di $(\mathbb{Z}, +)$. Allora $H = \langle a \rangle$ con $a \in \mathbb{Z}$

DIMOSTRAZIONE

$\langle a \rangle$ è un sottogruppo di \mathbb{Z}

Se H un sottogruppo di $(\mathbb{Z}, +)$. Se $H = \{0\} = \langle 0 \rangle$

$Sa H \neq 0 \Rightarrow \exists a \in H, a \neq 0$ possiamo supporre

$a > 0$ (perché se $a < 0$ $-a > 0 \in H$)

$\exists a$ il più piccolo intero positivo $\in H$

Voglio dimostrare che $H = \langle a \rangle$

$$\langle a \rangle \subseteq H$$

$\forall h \in H$ dividendo per a $h = qa+r$ con $0 \leq r < a \Rightarrow h - qa = r \in H$

$\Rightarrow r \in H$ ma $r < a \Rightarrow r = 0$

$$h = qa \in \langle a \rangle$$

$$(G, +)$$

DEFINIZIONE

Dicesi periodo di $g \in G$, il più piccolo intero positivo t , tale che $g^{t+1} = g^t$ ($\omega(g) = t$) (se $\omega(g) = 0$)

Se non esiste tale t , diremo che $g \in G$ è un elemento aperiodico ($\omega(g) = \infty$)

ESEMPIO

$$(\mathbb{Z}_4, +) \quad \mathbb{Z}_4 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \} \quad \omega(\bar{1}) = 4 \quad 4 \cdot \bar{1} = \bar{0}$$

$$\omega(\bar{2}) = 2$$

$$\omega(\bar{3}) = 4$$

$$(\mathbb{Z}, +) \quad \forall a \in \mathbb{Z} \quad a \text{ è aperiodico}$$

$$ta = 0 \Rightarrow t = 0$$

$$\therefore (34)^2 = 1 \quad \omega(34) = 2$$

$$S_3 \quad (34)^2 = \text{id} \quad \text{o}((34)) = 2$$

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in U \quad A^2 = A \cdot A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\text{o}(A) = 4 \quad A^3 = A^2 \cdot A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$A^4 = A^3 \cdot A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

PROPOSIZIONE

$$\text{Se } (G, \cdot) \quad \text{Se } H = \langle a \rangle$$

- 1) Se a è aperiodico gli unici generatori di $H = \langle a \rangle$ sono a ed a^{-1} .
Inoltre $a^h = a^k \Leftrightarrow h = k$
- 2) Se a è periodico di periodo m ($\text{o}(a) = m$) allora i generatori di $H = \langle a \rangle$ sono a^h con $(h, m) = 1$
 $\langle a \rangle = \{1, a, a^2, \dots, a^{m-1}\}$
Inoltre $a^h = a^k \Leftrightarrow h \equiv k \pmod{m}$

DIMOSTRAZIONE

1) $H = \langle a \rangle$ Supponiamo che a^t sia un altro generatore

$$\Rightarrow H = \langle a^t \rangle, \quad a \in H = \langle a^t \rangle \Rightarrow a = a^{th} \Rightarrow$$

$$\Rightarrow a^{th-1} = 1 \quad \text{perché } a \text{ è aperiodico} \Rightarrow th-1 = 0 \Rightarrow th = 1$$

$$\Rightarrow t \cdot h = \pm 1 \Rightarrow a \text{ ed } a^{-1} \text{ sono i generatori}$$

$$a^h = a^k \Leftrightarrow a^{h-k} = 1 \Leftrightarrow h-k = 0 \Leftrightarrow h = k$$

$$2) \quad \text{o}(a) = m \quad H = \langle a \rangle = \{1, a, \dots, a^{m-1}\}$$

Se $a^h \in H, \quad h \in \mathbb{Z}$. Dobbiamo provare

$$h = mq + r \quad \text{con } 0 \leq r < m$$

$$a^h = a^{mq+r} = a^{mq} \cdot a^r = (a^m)^q \cdot a^r \quad \text{perché } \text{o}(a) = m \Rightarrow a^m = 1$$

$$= a^t$$

$$H = \langle a \rangle = \{ a^0, a^1, \dots, a^{m-1} \}$$

Dimostriamo che le potenze sono distinte

$$\begin{aligned} a^i &= a^j & 0 \leq i \leq m-1 \\ & & 0 \leq j \leq m-1 \end{aligned}$$

$$a^{i-j} = 1 \quad i-j < m \quad \text{perché } m \text{ è il periodo di } A$$

$$\Rightarrow i-j = 0 \Rightarrow i=j$$

$$S_{\alpha} a^h \cdot a^k \Rightarrow a^{h+k} = 1$$

$$\text{Dividiamo } h+k \text{ per } m \Rightarrow (h+k) = mq+r \quad 0 \leq r \leq m$$

$$a^{mq} \cdot a^r = 1 \Rightarrow a^r = 1 \Rightarrow r=0 \quad \text{perché } 0 \leq r \leq m$$

$$\Rightarrow h+k = mq \Rightarrow h \equiv k \pmod{m}$$

ESEMPI

$$(\mathbb{Z}, +) \quad \mathbb{Z} = \langle 1 \rangle = \{m \cdot 1 \mid m \in \mathbb{Z}\}$$

$$(\mathbb{Z}_m, +) \quad \mathbb{Z}_m = \langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \dots, \bar{m-1}\}$$

DEFINIZIONE

(G, \circ) , $H \triangleleft G$ H sottogruppo di G

$\forall a, b \in G$, a è congruo a destra a b modulo H

$$a \equiv_d b \pmod{H}$$

$$\text{se } ab^{-1} \in H$$

\equiv_d è una relazione d'equivalenza

1) RIPLESSIVA $a \equiv_d a \pmod{H}$

$$a \cdot a^{-1} = 1 \in H$$

2) SIMMETRICA se $a \equiv_d b \pmod{H} \Rightarrow b \equiv_d a \pmod{H}$

$$ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H$$

$$(ab^{-1})^{-1} = (b^{-1})^{-1} a^{-1} \cdot ba^{-1} \in H$$

$$\Rightarrow b \equiv_d a \pmod{H}$$

3) TRANSITIVA

$$a \equiv_d b \pmod{H} \text{ e } b \equiv_d c \pmod{H} \Rightarrow a \equiv_d c \pmod{H}$$

$$ab^{-1} \in H \quad bc^{-1} \in H \Rightarrow (ab^{-1})(bc^{-1}) \in H \Rightarrow$$

$$= a(b^{-1}c)c^{-1} \in H \Rightarrow a \equiv_d c \pmod{H}$$

DEFINIZIONE

Dicesi classe laterale destra di $a \in G$ mod H l'insieme

$$Ha = \{ hah^{-1} \mid h \in H \}$$

$$a \equiv_d b \text{ mod } H \Leftrightarrow ab^{-1} \in H$$

$$[a] = \{ b \in G \mid b \equiv_d a \text{ mod } H \}$$

Dimostriamo che $[a] = Ha$

$$\begin{aligned} b \in [a] &\Rightarrow b \equiv_d a \text{ mod } H \Rightarrow ba^{-1} \in H \Rightarrow ba^{-1} = h \\ &\Rightarrow b = ha \in Ha \Rightarrow [a] \subseteq Ha \end{aligned}$$

$$\text{Viceversa se } ha \in Ha \Rightarrow ha \equiv_d a \text{ mod } H$$

$$haa^{-1} = h \in H \Rightarrow ha \in [a]$$

$$\text{Analogamente } \forall a, b \in G \quad a \equiv_s b \text{ mod } H \Leftrightarrow a^{-1}b \in H$$

$$[a] = aH = \{ ah \mid h \in H \}$$

$$Ha = Hb \Leftrightarrow a \equiv_d b \text{ mod } H \Leftrightarrow ab^{-1} \in H$$

$$Ha = H \Leftrightarrow a \in H$$

$$G = \bigcup_{a \in G} Ha = \bigcup_{a \in G} aH$$

$$(G, +) \quad a \equiv_d b \text{ mod } H \Leftrightarrow a - b \in H$$

$$a + H = \{ a + h \mid h \in H \}$$

$$(\mathbb{Z}, +) \quad H = \langle m \rangle = \{ hm \mid h \in \mathbb{Z} \}$$

$$\forall a \in \mathbb{Z} \quad H+a = a+H$$

$$a, b \in \mathbb{Z} \quad a \equiv b \pmod{H} \Rightarrow a-b \in H \Rightarrow a-b = tm \\ \Rightarrow a \equiv b \pmod{m}$$

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

$$H = \langle (12) \rangle \cup \{\text{id}, (12)\} \quad o((12)) = 2$$

$$\equiv_d \pmod{H}$$

$$[(13)] = H(13), \{h(13) \mid h \in H\} \subset \{(13), (12)(13)\} \\ = \{\text{id}, (132)\}$$

$$H(13) = \{\text{id}, (132)\} \subset H(132)$$

$$(13)H = \{(13)\text{id}, (13)(12)\} = \{(13), (123)\} = (13)H$$

$$H(13) \neq (13)H$$

$$H = \langle (123) \rangle \quad (123)^2 = (123)(123) = (132)$$

$$(123)^3 = (123)^2(123) = (132)(123) = (1)(2)(3) = \text{id}$$

$$(2357)^3 = (2753)$$

$$\cup(i_1 i_2 \dots i_k) \in K$$

$$o[(i_1 i_2 \dots i_k)(j_1 j_2 \dots j_h)] = m < m(h, k)$$

$$\left[(12)(345) \right]^2 = (354)$$

$$a^3 = (354)(12)(345) = (12) \quad a^6 = (a^3)^2 = (12)^2 = \text{id}$$

$$S_3 \quad H = \langle (1\ 2\ 3) \rangle = \{ \text{id}, (1\ 2\ 3), (1\ 3\ 2) \}$$

$$\begin{aligned} H(1\ 3) &= \{ h(1\ 3) \mid h \in H \} = \{ (1\ 3), (1\ 2\ 3)(1\ 3), (1\ 3\ 2)(1\ 3) \} \\ &= \{ (1\ 3), (2\ 3), (1\ 2) \} \end{aligned}$$

$$\begin{aligned} (1\ 3)H &= \{ (1\ 3)h \mid h \in H \} = \\ &= \{ (1\ 3), (1\ 3)(1\ 2\ 3), (1\ 3)(1\ 3\ 2) \} = \{ (1\ 3), (1\ 2), (2\ 3) \} \end{aligned}$$

G gruppo finito, H sottogruppo di G

In generale $H_a \neq aH$

$$|H_a| = |aH|$$

PROPOSIZIONE

$$|H_a| = |H|$$

DIMOSTRAZIONE

Costruisco una corrispondenza biunivoca tra H ed H_a

$$\begin{aligned} f: H &\rightarrow H_a & \text{È un'applicazione} \\ h &\mapsto h_a \end{aligned}$$

È suriettiva $\forall h_1, a \in H_a \Rightarrow h_1 a = f(h_1) \Rightarrow \exists h_1 \in H \mid f(h_1) = h_1 a$

È inieettiva Se $f(h_1) = f(h_2) \Rightarrow h_1 = h_2$

$$f(h_1) = f(h_2) \Rightarrow h_1 a = h_2 a \Rightarrow h_1 = h_2 \Rightarrow |H| = |H_a|$$

Analogamente si dimostra che $|aH| = |H|$

$$|H_a| = |aH|$$

$G = \bigcup H_a = \bigcup aH \Rightarrow$ il numero delle classi laterali destre coincide con il numero delle classi laterali sinistre

DEFINIZIONE

Dico: indice di H in G e si indica con $[G : H]$

il numero delle classi laterali destre (o sinistre)

TEOREMA DI LAGRANGE

TEOREMA DI LAGRANGE

Sia G gruppo finito e sia H sottogruppo di G

Allora $|H|/|G|$ in particolare

$$|G| = |H| \cdot [G:H]$$

Dimostrazione

$$G = \bigcup H_a, |G| = \sum_a |H_a| \Rightarrow |H| \cdot |H_a|$$

$$\Rightarrow |H| \cdot (\text{numero delle classi left})$$

$$\Rightarrow |H| \cdot [G:H]$$

PROPOSIZIONE

Sia G un gruppo finito di ordine un numero p

1) I sottogruppi di G sono banali, $\{1_G\}, G$

2) G è ciclico

Dimostrazione

1) Segue dal fatto che p è primo \Rightarrow gli unici divisori sono $1 \cdot p \Rightarrow$

\Rightarrow i sottogruppi avranno ordine 1 e $p \Rightarrow \{1_G\}, G$

2) $G, a \in G, a \neq 1_G$ considero $\langle a \rangle \neq \{1_G\} \Rightarrow G = \langle a \rangle$

PROPOSIZIONE

G gruppo finito. $\forall a \in G, a^{|G|} = 1_G$

Dimostrazione

Sia $a \in G \Rightarrow o(a) = t \Rightarrow |a|_G = t$

per Lagrange $t \mid |G| \Rightarrow |G| = t \cdot h \Rightarrow a^t = a^{th} = (a^t)^h = 1_G^h = 1_G$

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

$\forall \bar{a} \in \mathbb{Z}_m$ è invertibile $\Leftrightarrow \exists \bar{x}$ tale che $\bar{a}\bar{x} = \bar{1}$

$\bar{a}\bar{x} = \bar{1} \Leftrightarrow ax \equiv 1 \pmod{m} \Leftrightarrow (a, m) = 1$

$$\begin{aligned} U(\mathbb{Z}_m) &= \{\bar{a} \in \mathbb{Z}_m \mid \bar{a} \text{ è invertibile}\} = \text{gruppo delle unità di } \mathbb{Z}_m \\ &= \{\bar{a} \in \mathbb{Z}_m \mid (a, m) = 1\} \Rightarrow |U(\mathbb{Z}_m)| = \varphi(m) \end{aligned}$$

TEOREMA DI EULERO

Sia $a \in \mathbb{Z}$, $(a, m) = 1$ allora $a^{\varphi(m)} \equiv 1 \pmod{m}$

DIMOSTRAZIONE

$$|U(\mathbb{Z}_m)| = \varphi(m) \Rightarrow \forall \bar{a} \in U(\mathbb{Z}_m)$$

$$\bar{a}^{\varphi(m)} = \bar{1}$$

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

ESEMPIO

$$\mathbb{Z}_8 \quad |U(\mathbb{Z}_8)| = \varphi(8) = (2^3 - 2^2) = 8 - 4 = 4$$

$$U(\mathbb{Z}_8) = \{\bar{a} \in \mathbb{Z}_8 \mid (a, 8) = 1\}$$

$$1 \ 3 \ 5 \ 7 \quad = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$$

$$|U(\mathbb{Z}_{12})| = \varphi(12) = \varphi(3 \cdot 2^2) = (2^2 - 2) \cdot 2 = 4$$

$$U(\mathbb{Z}_{12}) = \{ \bar{1}, \bar{5}, \bar{7}, \bar{11} \}$$

DEFINIZIONE

H sottogruppo di G è normale se $\forall g \in G$

$$Hg = gH$$

ESEMPIO

$$\{1_G\}, \quad G \text{ sono normali:}$$

Se G è abeliano ogni sottogruppo è normale

PROPOSIZIONE

H sottogruppo di G . H è normale $\Leftrightarrow \forall g \in G \quad \forall h \in H$

$$g^{-1}hg \in H$$

DIMOSTRAZIONE

$$\text{Sia } H \text{ normale} \Rightarrow Hg = gH \quad \forall g \in G$$

$$\Rightarrow hg \in Hg \Rightarrow hg \in gH \Rightarrow hg = gh_1$$

$$\text{moltiplico per } g^{-1} \text{ a sinistra} \Rightarrow g^{-1}hg = g^{-1}gh_1 = h_1$$

$$\Rightarrow g^{-1}hg \in H$$

$$\text{Viceversa. Sia } g^{-1}hg \in H \quad \forall g \in G$$

voglio dimostrare che $Hg = gH$

$$\text{Sia } hg \in Hg \Rightarrow g^{-1}hg \in H \quad g^{-1}hg = h_1$$

$$\text{moltiplicando per } g \text{ a sinistra} \quad g^{-1}g^{-1}hg = g^{-1}h_1$$

$$Hg \subseteq gH$$

$$\boxed{hg = gh_1 \in gH}$$

Analogamente si dimostra che $gH \subseteq Hg \Rightarrow Hg = gH$

Analogamente si dimostra che $gH \subseteq Hg \Rightarrow Hg = gH$

H è sottogruppo normale di G . Bisogna dimostrare

D) H è sottogruppo $\forall a, b \in H \quad ab^{-1} \in H$

2) H è normale $\forall g \in G, \forall h \in H \Rightarrow g^{-1}hg \in H$

$$GL_2(\mathbb{R}) = \{ A \in M_2(\mathbb{R}) \mid A \text{ è invertibile} \}$$

$$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\} \subseteq GL_2(\mathbb{R})$$

$$\left(\begin{array}{cc} a & b \\ c & d \end{array} \right)^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \frac{1}{\det A} \operatorname{Agg}(A)$$

$$\begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix}$$

D) U sottogruppo

$\forall A_1, A_2 \in U \Rightarrow A_1 A_2^{-1} \in U$

$$A_1 = \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & a_2 \\ 0 & 1 \end{pmatrix} \quad A_1 \cdot A_2^{-1} = \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a_2 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & c \cdot a_2 + a_1 \\ 0 & 1 \end{pmatrix} \in U$$

2) $\forall A \in G^{\overset{GL_2(\mathbb{R})}{\longrightarrow}}, B \in U \Rightarrow A \cdot B \in U$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \det A \neq 0$$

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$A^{-1}BA = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} =$$

$$= \frac{1}{\det A} \begin{pmatrix} d & da-b \\ -c & -ca+d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{\det A} \begin{pmatrix} ad-bc+da & da-bc \\ -ca-c^2a+dc & -cb-ca+d+ad \end{pmatrix}$$

Non è normale

$$\mathbb{Z}_3 \text{ è un campo} \quad G = GL_2(\mathbb{Z}_3) = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \mid \bar{a}\bar{d} - \bar{b}\bar{c} = \bar{1} \right\}$$

$$H = \left\{ \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{b} & \bar{c} \end{pmatrix} \mid \bar{a}\bar{c} = \bar{1} \right\}$$

H è sottogruppo normale di G?

H è sottogruppo? $\forall A_1, A_2 \in H$

$$A_1 = \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{b} & \bar{c} \end{pmatrix} \quad A_2 = \begin{pmatrix} \bar{\alpha} & \bar{0} \\ \bar{\beta} & \bar{\gamma} \end{pmatrix} \quad A_1 A_2^{-1} = \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{b} & \bar{c} \end{pmatrix} \begin{pmatrix} \bar{\gamma} & \bar{0} \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} \bar{a}\bar{\gamma} & \bar{0} \\ \bar{b}\bar{\gamma} - \bar{b}\bar{\beta} & \bar{c}\bar{\alpha} \end{pmatrix}$$

$$(\bar{a}\bar{\gamma})(\bar{c}\bar{\alpha}) = (\bar{a}\bar{c})(\bar{\alpha}\bar{\gamma}) = \bar{1}$$

$$\begin{aligned} \text{E normale?} \quad & \forall A \in G \quad A = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \\ & \forall B \in H \quad B = \begin{pmatrix} \bar{\alpha} & \bar{0} \\ \bar{\beta} & \bar{\gamma} \end{pmatrix} \end{aligned}$$

$$\bar{\alpha}\bar{\gamma} = 1$$

$$A^{-1}BA \in H$$

$$\frac{1}{\det A} \begin{pmatrix} \bar{d} & -\bar{b} \\ -\bar{c} & \bar{a} \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{d} \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \frac{1}{\det A} \begin{pmatrix} \bar{d}\bar{a} - \bar{b}\bar{b} & -\bar{b}\bar{b} \\ -\bar{c}\bar{a} + \bar{a}\bar{b} & \bar{a}\bar{b} \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$$

$$= \frac{1}{\det A} \begin{pmatrix} (\bar{d}\bar{a} - \bar{b}\bar{b})\bar{a} - \bar{b}\bar{b}\bar{c} & (\bar{d}\bar{a} - \bar{b}\bar{b})(\bar{b}) - \bar{b}\bar{b}\bar{d} \\ (-\bar{c}\bar{a} + \bar{a}\bar{b})\bar{a} + \bar{a}\bar{b}\bar{c} & (-\bar{c}\bar{a} + \bar{a}\bar{b})\bar{b} + \bar{a}\bar{b}\bar{d} \end{pmatrix}$$

$$= \bar{b}(\bar{d}\bar{a} - \bar{b}\bar{b} - \bar{b}\bar{d})$$

G gruppo, H sottogruppo normale $H \trianglelefteq G$

DEFINIZIONE

Insieme quoziente $G/H = \{Hg \mid g \in G\}$

$$(G/H, \cdot) \quad Hg_1 \cdot Hg_2 \stackrel{\text{def}}{=} Hg_1g_2$$

$$\begin{aligned} Hg_1 &= H\bar{g}_1 \\ Hg_2 &= H\bar{g}_2 \end{aligned} \Rightarrow Hg_1g_2 = H\bar{g}_1\bar{g}_2$$

Se G è finito

$$|G/H| = [G:H]$$

PROPOSIZIONE

H è sottogruppo normale di $G \iff$

$$1) \bar{g}Hg \subseteq H$$

$$2) g^{-1}Hg = H$$

N SOTTOGRUPPO NORMALE

$$G/N = \{gN \mid g \in G\} \quad (G, \cdot)$$

$$(G/N, \cdot) \quad gN \cdot g'N = gg'N \quad gN = g'N \Leftrightarrow gg'N \in N$$

$$(G/N, +) \quad gN + g'N = (g+g')N \quad gN = g'N \Leftrightarrow g-g' \in N$$

DEFINIZIONE

Sono $(G, *)$, $(H, *)$ gruppi. Un'applicazione $f: G \rightarrow H$ è un omomorfismo se

$$\forall g_1, g_2 \in G \quad f(g_1 * g_2) = f(g_1) * f(g_2)$$

$$(G, \cdot), (H, \cdot) \quad f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2)$$

$$(G, \cdot), (H, +) \quad f(g_1 \cdot g_2) = f(g_1) + f(g_2)$$

$$(G, +), (H, +) \quad f(g_1 + g_2) = f(g_1) + f(g_2)$$

$$f: (\mathbb{Z}, +) \rightarrow (\mathbb{Q}^*, \cdot) \quad \text{È un omomorfismo?}$$

$$a \rightarrow 2^a$$

$$\forall a, b \in \mathbb{Z} \quad f(a+b) = f(a) \cdot f(b)$$

$$f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$$

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_7 \quad \forall a, b \in \mathbb{Z} \quad f(a+b) = f(a) + f(b)$$

$\frac{\parallel}{a+b} = \overline{a} + \overline{b}$

PROPRIETÀ (G, \cdot) $f: G \rightarrow H$

1) $f(1_G) = 1_H$

2) $f(g^{-1}) = f(g)^{-1}$

DIMOSTRAZIONE

1) $1_H \cdot f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot f(1_G) \Rightarrow 1_H = f(1_G)$

2) $f(g \cdot g^{-1}) \cdot f(1_G) = 1_H \Rightarrow 1_H = f(g) \cdot f(g^{-1}) \Rightarrow f(g^{-1}) = (f(g))^{-1}$

DEFINIZIONE

Il nucleo di $f: G \rightarrow H$ è l'insieme

$$\ker f = \{g \in G \mid f(g) = 1_H\} \subseteq G$$

L'immagine di f è $\text{Im } f = f(G) = \{f(g) \mid g \in G\} \subseteq H$

PROPOSIZIONE

1) $\ker f$ è un sottogruppo normale di G

2) $\text{Im } f$ è un sottogruppo di H

DIMOSTRAZIONE

1) $\ker f$ è sottogruppo normale

1) $\forall g_1, g_2 \in \ker f \Rightarrow$

2) $\forall h \in G, \forall g \in \ker f \Rightarrow$

1) $\forall g_1, g_2 \in \ker f \Rightarrow f(g_1) = f(g_2) = 1_H$

D) $\forall g_1, g_2 \in \ker f \Rightarrow f(g_1) = f(g_2) = 1_H$

$$g_1, g_2^{-1} \in \ker f? \quad f(g_1 g_2^{-1}) = f(g_1) \cdot f(g_2^{-1}) = f(g_1) \cdot f(g_2)^{-1} = 1_H$$

2) $\forall h \in G \quad \forall g \in \ker f \quad h^{-1}gh \in \ker f?$

$$f(h^{-1}gh) = f(h^{-1}) \underset{1_H}{\underset{n}{\dots}} f(g) f(h) = f(h^{-1}) \cdot f(h) = 1_H$$

3) $\text{Im } f$ è un sottogruppo di H

$$\forall h_1, h_2 \in \text{Im } f \Rightarrow h_1 h_2^{-1} \in \text{Im } f$$

$$h_1 = f(g_1)$$

$$h_1 h_2^{-1} = f(g_1) \cdot f(g_2)^{-1} = f(g_1) \cdot f(g_2^{-1}) = f(g_1 g_2^{-1})$$

$$h_2 = f(g_2)$$

OMOMORFISMO

mercoledì 4 maggio 2022 09:12

$$f: (\mathbb{Q}^*, \cdot) \rightarrow (\mathbb{Q}^*, \cdot)$$

$$a \mapsto a^{-1}$$

$$\text{Im } f = \mathbb{Q}^*$$

È un omomorfismo?

$$\forall a, b \in \mathbb{Q}^* \quad f(a \cdot b) = f(a) \cdot f(b)$$

$$f(a \cdot b) = (ab)^{-1} = a^{-1}b^{-1} = f(a) \cdot f(b)$$

$$\ker f = \{ a \in \mathbb{Q}^* \mid f(a) = 1 \} \quad f(a) = 1 \iff a^{-1} = 1 \iff a = 1$$

PROPOSIZIONE

$f: G \rightarrow H$ omomorfismo è iniettivo \Leftrightarrow

$$\ker f = \{ 1_G \}$$

DIMOSTRAZIONE

Supponiamo f iniettivo. Se $y \in \ker f \Rightarrow f(y) = 1_H = f(1_G) \Rightarrow$

\Rightarrow poiché f è iniettivo $\Rightarrow y = 1_G$

Viceversa supponiamo che $\ker f = \{ 1_G \}$. Dimostriamo che f è iniettivo.

Supponiamo $f(y) = f(g_1) \Rightarrow f(y) f(g_1)^{-1} = 1_H$

$\Rightarrow f(y) \cdot f(g_1^{-1}) = 1_H \Rightarrow f(y \cdot g_1^{-1}) = 1_H \Rightarrow$

$$gg^{-1} \in \ker f = \{1_G\} \quad gg^{-1} = 1_G \Rightarrow g = g$$

PROPOZIONE

$f: G \rightarrow H$ omomorfismo suriettivo = epimorfismo

$f: G \rightarrow H$ omomorfismo biettivo = isomorfismo

$f: G \rightarrow G$ isomorfismo = automorfismo

$$f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_7, +)$$

$$a \rightarrow \bar{a}_7 \quad \text{Im } f = \mathbb{Z}_7$$

$$\ker f = \{ a \in \mathbb{Z} \mid f(a) = \bar{0} \}$$

$$f(a) = \bar{a}_7 = \bar{0} \quad a \equiv 0 \pmod{7}$$

$$\Rightarrow a = 7 \cdot h \quad a \in \langle 7 \rangle$$

$$G \rightarrow H \quad \ker f \stackrel{\text{sottogruppo normale}}{\cong} G \quad G/\ker f = \{ g\ker f \mid g \in G \}$$

gruppo

PRIMO TEOREMA DEGLI ISOMORFISMI FRA GRUPPI

$f: G \rightarrow H$ un omomorfismo di gruppi

$$\text{Allora } G/\ker f \cong \text{Im } f = f(G)$$

DIMOSTRAZIONE

$$h: G/\ker f \rightarrow \text{Im } f$$

$$g\ker f \rightarrow f(g)$$

h è ben posta infatti se $g_1\ker f = g_2\ker f \Rightarrow h(g_1\ker f) = h(g_2\ker f)$

$$g_1 \ker f = g_2 \ker f \Rightarrow g_1, g_2^{-1} \in \ker f \Rightarrow f(g_1 g_2^{-1}) = 1_H$$

$$\Rightarrow f(g_1) \cdot f(g_2)^{-1} = 1_H \Rightarrow$$

$$\Rightarrow f(g_1) = f(g_2)$$

$$\Rightarrow h(g_1 \ker f) = h(g_2 \ker f)$$

h è un omomorfismo $\Leftrightarrow g_1 \ker f, g_2 \ker f$

$$\underbrace{h(g_1 \ker f) \cdot (g_2 \ker f)}_{//} = \underbrace{h(g_1 \ker f)}_{//} \cdot \underbrace{h(g_2 \ker f)}_{//}$$

$$h(g_1 g_2 \ker f) = f(g_1 g_2) = f(g_1) \cdot f(g_2)$$

È un omomorfismo

$$\ker h = \{g \ker f \mid h(g \ker f) = 1_H\}$$

$$h(g \ker f) = f(g) = 1_H$$

$$\Rightarrow g \in \ker f$$

$$\ker h = \{g \ker f \mid f(g) = 1_H\} = \ker f$$

$\Rightarrow \ker f$ è l'elemento neutro di $G/\ker f$ \Rightarrow

$\Rightarrow h$ è suriettivo

$$\begin{aligned} h: G/\ker f &\rightarrow \text{Im } f \\ &\text{è suriettivo} \\ g \ker f &\rightarrow f(g) \end{aligned}$$

$\Rightarrow h$ è isomorfismo $\Rightarrow G/\ker f \cong \text{Im } f$

COROLARIO

Se $f: G \rightarrow H$ è un omomorfismo è suriettivo

$$\Rightarrow G/\ker f \cong H = \text{Im } f$$

ESEMPIO

$$\begin{aligned} f: \mathbb{Z} &\rightarrow \mathbb{Z}_7 & \ker f = \langle 7 \rangle & \quad \text{Im } f = \mathbb{Z}_7 \\ z &\rightarrow \bar{z}_7 \end{aligned}$$

OPTIONAL

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_7 \quad \ker f = \langle 7 \rangle \quad \text{Im } f = \mathbb{Z}_7$$

$$z \mapsto \bar{z}_7$$

$$\mathbb{Z}/\langle 7 \rangle \cong \mathbb{Z}_7$$

$$G/\ker f \cong \text{Im } f$$

$$\mathbb{Z} / \langle m \rangle$$

$$\mathbb{Z}_{\langle m \rangle} = \{ z + \langle m \rangle \mid z \in \mathbb{Z} \}$$

$$z + \langle m \rangle = \{ z + hm \mid h \in \mathbb{Z} \} \cong \{ \bar{0}, \bar{1}, \bar{2}, \dots, \bar{m-1} \}$$

$$\langle 7 \rangle = \{ 0 + \langle 7 \rangle, 1 + \langle 7 \rangle, \dots, 6 + \langle 7 \rangle \}$$

$$f: (\text{GL}_n(\mathbb{R}), \cdot) \rightarrow (\mathbb{R}^+, \cdot)$$

$$A \rightarrow \det A$$

$$\ker f = \{ A \in \text{GL}_n(\mathbb{R}) \mid \det A = f(A) = 1 \}$$

È un omomorfismo

$$A_1, A_2 \in \text{GL}_n(\mathbb{R}), \quad f(A_1 A_2) = f(A_1) \cdot f(A_2)$$

||

$$\det(A_1 A_2) = \det A_1 \cdot \det A_2$$

f è suriettiva? $\forall z \in \mathbb{R}^*$

$$A = \begin{pmatrix} z & & \\ & \ddots & \\ & & 1 \end{pmatrix} \quad \det A = z$$

Per il teorema di omomorfismo $\frac{\text{GL}_n(\mathbb{R})}{\text{SL}_n(\mathbb{R})} \cong \mathbb{R}^*$

$$G_1, G_2 \quad G_1 \times G_2 = \{ (g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2 \}$$

$$(g_1, g_2) \cdot (h_1, h_2) \stackrel{\text{def}}{=} (g_1 \cdot h_1, g_2 \cdot h_2)$$

$G_1 \times G_2$ prodotto diretto: è un gruppo

$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid b \in \mathbb{Q}, a, d \in \mathbb{Q}^* \right\}$ è un gruppo rispetto al \cdot ?

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & dz \end{pmatrix} \quad \text{È UN GRUPPO RISPETTO A PRODOTTO}$$

$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Q} \right\}$ Dimostrare che N è un sottogruppo normale e dedurre che $G/N \cong \mathbb{Q}^* \times \mathbb{Q}^*$

N sottogruppo $\forall \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in N$

$$\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \right)^{-1} \right) \in N \Rightarrow \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & -a+b \\ 0 & 1 \end{pmatrix} \in N$$

è normale $\forall \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \quad \forall \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N$

$$\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} \left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) \right) \right)$$

g⁻¹ m g

$$\begin{aligned} & \frac{1}{ad} \left(\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) \right) \right) = \frac{1}{ad} \left(\begin{pmatrix} d & dx-b \\ 0 & a \end{pmatrix} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) \right) \\ & = \frac{1}{ad} \left(\begin{pmatrix} da & db+(dx-b)d \\ 0 & ad \end{pmatrix} \right) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N \end{aligned}$$

$$G/N \cong \mathbb{Q}^* \times \mathbb{Q}^*$$

$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Q} \right\}$

$$G \rightarrow \mathbb{Q}^* \times \mathbb{Q}^*$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \rightarrow (a, d)$$

$$\# = f(A_1) \cdot f(A_2)$$

$$A_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \quad A_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$$

$$A_1 \cdot A_2 = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix}$$

$$\begin{aligned} f(A_1 \cdot A_2) &= (a_1 a_2, d_1 d_2) \\ &= (a_1, d_1) \cdot (a_2, d_2) = f(A_1) \cdot f(A_2) \end{aligned}$$

f é surjetivo

$$\text{Ker } f = \left\{ A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \mid f(A) = (1, 1) \right\} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}$$

$$f(A) = (a, d) = (1, 1) \Rightarrow a = 1 = d$$

Per il teorema di omomorfismo $G/N \cong \mathbb{Q}^* \times \mathbb{Q}^*$

Esercizio

$$f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_2 \times \mathbb{Z}_3, +)$$

$$a \rightarrow (\bar{a}_2, \bar{a}_3)$$

È un omomorfismo

$$\forall a, b \in \mathbb{Z} \quad f(a+b) = f(a) + f(b)$$

$$\begin{aligned} f(a+b) &= (\bar{a+b}_2, \bar{a+b}_3) = (\bar{a}_2 + \bar{b}_2, \bar{a}_3 + \bar{b}_3) \\ &= (\bar{a}_2, \bar{a}_3) + (\bar{b}_2, \bar{b}_3) = f(a) + f(b) \end{aligned}$$

ZOO.00

$$\text{Ker } f = \left\{ a \in \mathbb{Z} \mid f(a) = (0, 0) \right\} = \left\{ 6h \mid h \in \mathbb{Z} \right\}$$

$$f(a) = (\bar{a}_2, \bar{a}_3) = (0, 0)$$

$$\begin{aligned} \bar{a}_2 = 0 &\Rightarrow a \equiv 0 \pmod{2} & a = 2t & \Rightarrow a = 6h \\ \bar{a}_3 = 0 &\Rightarrow a \equiv 0 \pmod{3} & a = 3t \end{aligned}$$

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$$

$$a \mapsto (\bar{a}_2, \bar{a}_3)$$

f è suriettiva? $\nexists (\bar{a}, \bar{b}) \in \mathbb{Z}_2 \times \mathbb{Z}_3$

$$\begin{aligned} \exists c \in \mathbb{Z} \mid f(c) = (\bar{a}, \bar{b}) \quad ? \\ (\bar{c}_2, \bar{c}_3) = (\bar{a}, \bar{b}) \end{aligned}$$
$$\begin{cases} \bar{c}_2 = \bar{a} \\ \bar{c}_3 = \bar{b} \end{cases} \quad \left\{ \begin{array}{l} c \equiv a \pmod{2} \\ c \equiv b \pmod{3} \end{array} \right.$$

Per il teorema chiuso del resto $\exists c$

Per il teorema di omomorfismo

$$G/\ker f \cong \text{Im } f$$

$$\mathbb{Z}_6 \cong \mathbb{Z}_{\langle 6 \rangle} \cong \mathbb{Z}_2 \times \mathbb{Z}_3$$

$$G = \langle a \rangle \quad G \text{ è c.clico}$$

$$a \text{ è aperiodico} \quad a^h = a^t \Leftrightarrow h=t$$

$$a \text{ è periodico di periodo } m \quad a^h = a^t \Leftrightarrow h \equiv t \pmod{m}$$

$G = \langle a \rangle$

Se G è infinito

i generatori di G sono a ed a^{-1}

Se G è finito di ordine m ($d(a) \geq m$)

i generatori di G sono

$$a^t \text{ con } (t, m) = 1 \quad 0 \leq t < m$$

DIMOSTRAZIONE

$$G = \langle a \rangle$$

Supponiamo che $G = \langle a^t \rangle = \langle a \rangle$

$$\Rightarrow a \in \langle a^t \rangle \Rightarrow a = (a^t)^h = a^{th}$$

$$\Rightarrow a = a^{th} \Rightarrow 1 = a^{th-1} = a^0$$

Se G è infinito ovvero a è aperiodico

$$\begin{aligned} th-1 &= 0 \Rightarrow th = 1 \Rightarrow \\ t &= h = \pm 1 \end{aligned}$$

Se G è finito di ordine m

$$th-1 \equiv 0 \pmod{m}$$

$$th-1 \geq km \Rightarrow th - km = 1 \Rightarrow$$

$$\Rightarrow d(t, m) | 1 \Rightarrow (t, m) = 1$$

$$\Rightarrow G = \langle a^t \rangle \text{ con } (t, m) = 1 \quad 0 \leq t < m$$

$\Rightarrow G$ gruppo c.clico di ordine 21

$$G = \langle g \rangle$$

I generatori di G , g^t con $(t, m) = 1 \quad 0 \leq t \leq m$

$$t = 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20$$

$$\varphi(21) = \varphi(3 \cdot 7) = \varphi(3) \cdot \varphi(7) = 12$$

$$\mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle$$

$G = \langle g \rangle$ G è infinito (è aperiodico) gli unici generatori sono
 g e g^{-1}

$G = \langle g \rangle$ $|G| = m$ i generatori sono g^t con $(t_m) = 1$ $0 \leq t < m$

PROPOSIZIONE

Ogni sottogruppo di un gruppo ciclico è ciclico

DIMOSTRAZIONE

Sia H sottogruppo di $G = \langle g \rangle$ Se $H = \{1_G\} = \langle 1_G \rangle$

Supponiamo che $H \neq \{1_G\} \Rightarrow \exists g^t \in H$ con $t > 0$

Sia g^t la potenza di $g \in H$ con esponente $t > 0$ più piccolo

Dimostriamo che $H = \langle g^t \rangle$

$g^t \in H \Rightarrow \langle g^t \rangle \subseteq H$

$H \subseteq \langle g^t \rangle$ Sia $g^h \in H$, dividendo h per t

$$h = tq + r \quad 0 \leq r < t \Rightarrow g^h = g^{tq+r} = g^{tq} \cdot g^r = (g^t)^q \cdot g^r$$

$$\begin{aligned} g^r = g^h \cdot (g^t)^{-q} &\in H \Rightarrow g^r \in H \text{ per la minimalità di } t \\ &\Rightarrow r = 0 \Rightarrow g^h = (g^t)^q \end{aligned}$$

$$g^h \in \langle g^t \rangle \Rightarrow H \subseteq \langle g^t \rangle$$

TEOREMA

Sia G un gruppo ciclico $G = \langle g \rangle$

1) Se G è infinito allora $G \cong \mathbb{Z}$

2) Se G è finito di ordine $m \Rightarrow G \cong \mathbb{Z}_m$

Dimostrazione

$$\text{Se } f: \mathbb{Z} \rightarrow G \\ t \mapsto g^t$$

È un'applicazione. Infatti se $t_1 = t_2 \Rightarrow f(t_1) = f(t_2)$
 $g^{t_1} = g^{t_2}$

È un omomorfismo $\forall t_1, t_2 \in \mathbb{Z}$

$$f(t_1 + t_2) = f(t_1) \cdot f(t_2)$$

$$g^{t_1 + t_2} = g^{t_1} \cdot g^{t_2} = f(t_1) \cdot f(t_2)$$

$$f: \mathbb{Z} \rightarrow G \\ t \mapsto g^t$$

È suriettivo $\forall g^t \in G \quad \exists t \in \mathbb{Z} \mid f(t) = g^t$

$$\ker f = \{ t \in \mathbb{Z} \mid g^t = 1_G \}$$

⇒ G è infinito $g^t = 1_G \Rightarrow t = 0 \Rightarrow \ker f = \{0\}$

Per il teorema di omomorfismo

$$\mathbb{Z}/\{0\} \cong G = \text{Im } f$$

$$\mathbb{Z}/\{0\} \cong \{ z + \{0\} \mid z \in \mathbb{Z} \} = \mathbb{Z}$$

$$\mathbb{Z} = \mathbb{Z}/\{0\} \cong G$$

⇒ $G = \langle g \rangle$ è finito di ordine m ($\text{ord } g = m$)

$$\ker f = \{ t \in \mathbb{Z} \mid g^t = 1_G \} = \langle m \rangle \quad g^t = 1_G \Rightarrow g^0 \Rightarrow t \equiv 0 \pmod{m}$$

$$\text{Ker } \varphi = \{t \in \mathbb{Z} \mid g^t = 1_G\} = \langle m \rangle \quad g^t = 1_G \Rightarrow t \equiv 0 \pmod{m}$$

$$t = km$$

$$t \in \langle m \rangle$$

$$\mathbb{Z}/\text{Ker } \varphi = \mathbb{Z}/\langle m \rangle \cong \mathbb{Z}_m$$

$$\mathbb{Z}/\text{Ker } \varphi \cong G = \text{Im } \varphi$$

$$G \cong \mathbb{Z}_m$$

PROPOSIZIONE

Sia G un gruppo ciclico di ordine m

Per ogni divisore d di m $\exists!$ un sottogruppo di ordine d

$$d|m \quad G = \langle g \rangle$$

Il sottogruppo di ordine d è $H = \langle g^{\frac{m}{d}} \rangle$

ESERCIZIO

Sia G gruppo ciclico $|G| = 12$

Desunvere tutti i generatori di G e tutti i sottogruppi

$G = \langle g \rangle$ i generatori sono g^t con (t, m)

Sono in numero di $\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2) \cdot \varphi(3) = (2^2 - 2)(2) = 4$

$$(t, 12) = 1 \Rightarrow t = 1, 5, 7, 11$$

$$G = \langle g \rangle = \langle g^5 \rangle = \langle g^7 \rangle = \langle g^{11} \rangle$$

I sottogruppi suono di ordine = 1, 2, 3, 4, 6, 12

$$|G| = 12$$

$$d \mid 12$$

CORDINE

$$\textcircled{1} \quad \{1_G\} \quad \langle g^m \rangle = \langle g^{12} \rangle = \langle 1_G \rangle$$

$$\textcircled{12} \quad G$$

$$\textcircled{2} \quad G = \langle g^{\frac{12}{2}} \rangle = g^6 = \{g^0, 1_G\}$$

$$\textcircled{3} \quad G = \langle g^{\frac{12}{3}} \rangle = \langle g^4 \rangle = \{g^4, g^8, 1_G\}$$

$$\textcircled{4} \quad G = \langle g^{\frac{12}{4}} \rangle = \langle g^3 \rangle = \{g^3, g^6, g^9, 1_G\}$$

$$\textcircled{6} \quad G = \langle g^2 \rangle = \{g^2, g^4, g^6, g^8, g^{10}, 1_G\}$$

Esercizio

$$S_2 \quad G = (M_2(\mathbb{Z}), +) \quad S_2 \quad H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid a = 18k \quad k \in \mathbb{Z} \right\}$$

1) Dimostrare che H è un sottogruppo normale di G

2) Data $x = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} + H \in G/H$ calcolare il periodo di x
e determinare $\langle x \rangle$

3) Determinare i generatori dei sottogruppi di K

$$\forall A_1, A_2 \in H \Rightarrow A_1 - A_2 \in H$$

$$A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in H \quad \begin{array}{l} a_1 = 18h \\ a_2 = 18k \end{array}$$

$$A_1 - A_2 = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ c_1 - c_2 & d_1 - d_2 \end{pmatrix} = \begin{pmatrix} 18(h-k) & * \\ * & * \end{pmatrix} \in H$$

$$2) \quad x = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} + H \in G/H$$

Il periodo è il più piccolo intero positivo m tale che $m \cdot x = H$

$$m \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} + H = \begin{pmatrix} 2m & m \\ 0 & m \end{pmatrix} + H = H \Leftrightarrow \begin{pmatrix} 2m & m \\ 0 & m \end{pmatrix} \in H$$

$$\Rightarrow m=9 \Rightarrow \text{ord}(x)=9$$

$$|\langle x \rangle| = 9 \quad K = \langle x \rangle = \langle tx \rangle \quad (t, 9) = 1$$

$$\langle x \rangle = \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} + H, \quad \begin{matrix} 2x \\ \parallel \\ 3x, 4x, 5x, 6x, 7x, 8x \\ \parallel \\ H \end{matrix}, \quad \begin{pmatrix} 4 & 2 \\ 0 & 2 \end{pmatrix} + H \right\}$$

$$1, 2, 4, 5, 7, 8 \quad \varphi(9) = \varphi(3^2 - 1) = (3^2 - 3) = 6$$

$$K = \langle x \rangle = \langle 2x \rangle = \langle 4x \rangle = \langle 5x \rangle = \langle 7x \rangle = \langle 8x \rangle$$

$$I \text{ sottogruppi: hanno ordine } 1, 3, 9 \\ \begin{matrix} & & \\ & " & " \\ \{H\} & & K \end{matrix}$$

$$\langle \frac{m}{d}x \rangle = \langle 3x \rangle = \left\langle \begin{pmatrix} 6 & 3 \\ 0 & 3 \end{pmatrix} + H \right\rangle$$

ESERCIZI SUGLI OMOMORFISMI

sabato 7 maggio 2022 22:10

$$f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

$$(x, y) \rightarrow x - 3y$$

Dimostrare che è un omomorfismo suriettivo (epimorfismo)

$$\text{Calcolare } \text{Ker } f = N$$

N è ciclico? È abeliano? G/N è ciclico?

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$$

$$f((x_1, y_1) + (x_2, y_2)) = f(x_1, y_1) + f(x_2, y_2)$$

||

$$f((x_1 + x_2, y_1 + y_2)) = (x_1 + x_2) - 3(y_1 + y_2) = (x_1, -3y_1) + (x_2, -3y_2)$$

OK

$$\forall z \in \mathbb{Z} \quad z = f((z, 0))$$

$$\exists (z, 0) \in \mathbb{Z} \times \mathbb{Z} \text{ tale che } f((z, 0)) = z$$

$y < 0, 1$

||

$$\text{Ker } f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid f(x, y) = 0\} = \{(3y, y) \mid y \in \mathbb{Z}\}$$

$$f((x, y)) = x - 3y = 0 \Rightarrow x = 3y$$

||

$\langle (3, 1) \rangle$

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (3, 1) \rangle} \cong \mathbb{Z}$$

È ciclico

ESERCIZI SUGLI OMOMORFISMI 2

sabato 7 maggio 2022 22:23

$$f: \mathbb{Z}_3 \rightarrow \mathbb{Z}_{12}$$

$$[a]_3 \rightarrow [4a]_{12}$$

f è un omomorfismo

$$\forall [a]_3, [b]_3 \quad f([a]_3 + [b]_3) = f([a]_3) + f([b]_3)$$

$$\qquad\qquad\qquad // \qquad\qquad\qquad \backslash\backslash \qquad\qquad\qquad //$$

$$f([a+b]_3) = [4(a+b)]_{12} = [4a]_{12} + [4b]_{12}$$

f iniettiva $\Leftrightarrow \text{Ker } f = \{[0]_3\}$

$$\text{Ker } f = \{[a]_3 \in \mathbb{Z}_3 \mid f([a]_3) = [0]_{12}\} = \{[0]_3\}$$

$$[4a]_{12} = [0]_{12}$$

$\hat{\text{E}} \text{ INIETTIVA}$

$$4a \equiv 0 \pmod{12} \quad [a]_3 = [3h]_3 \cdot [3]_3$$

$$a = 3h$$

$$S_2 H = f(\mathbb{Z}_3) \circ \text{Im } f$$

H è ciclico? In caso affermativo calcolare i generatori

\downarrow
Sì, perché sottogruppi di un gruppo ciclico \mathbb{Z}_{12}

$$H = f(\mathbb{Z}_3) = \{f([a]_3) \mid [a] \in \mathbb{Z}_3\}$$

$$= \{[0]_{12}, [4]_{12}, [8]_{12}\} = \langle [4]_{12} \rangle = \langle [8]_{12} \rangle$$

$$f: \mathbb{Z}_3 \rightarrow \mathbb{Z}_{12}$$

$$\text{Ker } f = \{[0]_3\}$$

Calcolare

$$[\mathbb{Z}_{12}; H]$$

$$\text{Im } f = \langle [4]_{12}, [8]_{12} \rangle$$

$$|\mathbb{Z}_{12}| = |H| \cdot [\mathbb{Z}_{12} : H]$$

$$\mathbb{Z}_3 \cong \text{Im } f$$

$$[\mathbb{Z}_{12} : H] = \frac{12}{3} = 4$$

DEFINIZIONE

Un insieme $A \neq \emptyset$ dotato di 2 operazioni

$(A, +, \cdot)$ è un anello se

- 1) $(A, +)$ è un gruppo abeliano
- 2) $\forall a, b, c \in A \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- 3) $\forall a, b, c \in A \quad a \cdot (b + c) = a \cdot b + a \cdot c$
 $(b + c) \cdot a = b \cdot a + c \cdot a$

Se $\exists 1_A$, A è un anello con 1_A

Se \cdot commutativo A è un anello commutativo

Se $\forall a \neq 0 \in A^* \exists a^{-1} \in A$, A si dice **corpo**

Un corpo commutativo si dice **campo** (A^*, \cdot) gruppo abeliano

ESEMPIO

$(\mathbb{Z}, +, \cdot)$ anello commutativo con 1

$(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ $(\mathbb{C}, +, \cdot)$ campi

$(M_n(\mathbb{R}), +, \cdot)$ anello con 1

$(2\mathbb{Z}, +, \cdot)$ anello commutativo

CORPO DEI QUATERNIONI: \mathbb{H}

$$\mathbb{H} = \{ a_0 + a_1 i + a_2 j + a_3 k \mid a_i \in \mathbb{R} \}$$

$$i^2 = j^2 = k^2 = -1$$

$$\begin{array}{lll} ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

$$(\mathbb{H}, +, \cdot) \quad (a_0 + a_1i + a_2j + a_3k) + (b_0 + b_1i + b_2j + b_3k)$$

$$(a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k$$

ESEMPIO

$$(5 + 7i + 3j + k) + (-2 + 3i - 5j) = 3 + 10i - 4j + k$$

$$(a_0 + a_1i + a_2j + a_3k) + (b_0 + b_1i + b_2j + b_3k)$$

$$= a_0b_0 + a_0b_1i + a_0b_2j + a_0b_3k + a_1b_1 + a_1b_2k + a_1b_3 \text{ ... } \text{...}$$

ESEMPIO

$$(3 + 7i + 5j)(2 - 6j) = 6 \cdot 18j + 14i - 42k + 10k + \text{...} \text{...}$$

$$= 6 + 44i - 14j - 32k \text{ ... } \text{...}$$

$(\mathbb{H}, +)$ è un gruppo abeliano $e = 0$

$$-(a_0 + a_1i + a_2j + a_3k) = -a_0 - a_1i - a_2j - a_3k$$

$(\mathbb{H}, +, \cdot)$ è un anello (non commutativo $ij = k \quad ji = k$)

ha unità 1

$$(a_0 + a_1i + a_2j + a_3k)^{-1} = \frac{a_0 - a_1i - a_2j - a_3k}{a_0^2 + a_1^2 + a_2^2 + a_3^2}$$

$$hh^{-1} = h^{-1}h = 1$$

$(A, +, \cdot)$

DEFINIZIONE

$0 \neq a \in A$ è un divisore dello zero se $ab = 0$ con $b \neq 0$

$$\mathbb{Z}_6 \quad \bar{2} \cdot \bar{3} = \bar{6} = \bar{0} \Rightarrow \bar{2} \text{ e } \bar{3} \text{ sono divisori dello zero}$$

DEFINIZIONE

Un anello commutativo è un dominio d'integrità se è privo di divisori dello zero

ESEMPIO

$$(\mathbb{Z}, +, \cdot) \quad ab=0 \Rightarrow a=0 \text{ o } b=0$$

PROPOSIZIONE

Un campo è un dominio d'integrità

DIMOSTRAZIONE

$$\text{Se } ab=0 \quad \text{Se } a \neq 0 \quad \exists a^{-1} \in A$$

$$a^{-1}(ab) = a^{-1} \cdot 0$$

$b=0 \Rightarrow$ un campo non possiede divisori dello zero

DEFINIZIONE

$(A, +, \cdot)$. L'insieme $U(A) = \{ a \in A \mid \exists a^{-1} \in A \}$ detto gruppo delle unità

$U(A)$ è un gruppo rispetto al \cdot

$$\text{Se } a, b \in U(A) \quad a \cdot b \in U(A) \quad (ab)^{-1} = b^{-1}a^{-1} \in U(A)$$

$$\text{Se } a \in U(A) \Rightarrow a^{-1} \in U(A)$$

ESEMPIO

$$(\mathbb{Z}, +, \cdot) \quad U(\mathbb{Z}) = \{ 1, -1 \}$$

$$\mathbb{Z}_6 \quad U(\mathbb{Z}_6) = \{\bar{k} \mid (k, 6) = 1\} = \{\bar{1}, \bar{5}\}$$

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

Se m è primo \mathbb{Z}_m è un campo $U(\mathbb{Z}_m) = \mathbb{Z}_m^*$

$$\text{Se } m \text{ non è primo} \Rightarrow m = m_1 \cdot m_2 \Rightarrow \bar{m}_1 \cdot \bar{m}_2 = \bar{m} = \bar{0}$$

$\Rightarrow \mathbb{Z}_m$ possiede divisori di zero

$$U(\mathbb{Z}_m) = \{\bar{k}, (k, m) = 1\} \quad \bar{a} \in U(\mathbb{Z}_m) \Rightarrow \exists \bar{x} \in \mathbb{Z}_m$$

$$\bar{a}\bar{x} = \bar{1} \pmod{m}$$

$$ax = 1 \pmod{m} \Leftrightarrow (x, m) = 1$$

\mathbb{Z}_{12} Descrivere le unità e i divisori della zero

$$U(\mathbb{Z}_{12}) = \{\bar{k}, (k, 12) = 1\} \quad k: \bar{1}, \bar{5}, \bar{7}, \bar{11}$$

$$= \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\} \quad |U(\mathbb{Z}_{12})| = \varphi(12) =$$

$$= \varphi(2^2) \cdot \varphi(3) = \\ (2^{2-1})(2) = 4$$

$$(\bar{1})^{-1} = \bar{1} \quad (\bar{5})^{-1} = \bar{5} \quad (\bar{7})^{-1} = \bar{7} \quad (\bar{11})^{-1} = \bar{11} \\ \bar{5} \cdot \bar{5} = \bar{1} \quad \bar{7} \cdot \bar{7} = \bar{49} = \bar{1}$$

DIVISORI DELLA ZERO

$$\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}$$

$$[\bar{2} \cdot \bar{6}] = \bar{12} = \bar{0}$$

$$[\bar{3} \cdot \bar{4}] = \bar{12} = \bar{0}$$

$$[\bar{2} \cdot \bar{9}] = \bar{18} = \bar{0}$$

~~W~~ = ~~W~~ + ~~W~~

$$[\bar{8}, \bar{9}] = \bar{7}_2 = \bar{0}$$

$$[\bar{1}_0, \bar{6}] = \bar{6}_0 = \bar{0}$$

DIVISORI DELLO ZERO

giovedì 12 maggio 2022 08:07

$$\mathbb{Z}_{15}$$

$$U(\mathbb{Z}_{15}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$$

$$(\bar{2})^{-1} = \bar{8} \quad \text{perché} \quad \bar{2} \cdot \bar{8} = \bar{16} = \bar{1}$$

$$(\bar{4})^{-1} = \bar{8} \quad \bar{4} \cdot \bar{8} = \bar{16} = \bar{1}$$

$$(\bar{7})^{-1} = \bar{13} \quad \bar{7} \cdot \bar{13} = \bar{91} = \bar{1}$$

$$(\bar{11})^{-1} = \bar{11} \quad \bar{11} \cdot \bar{11} = \bar{121} = \bar{1}$$

$$(\bar{14})^{-1} = \bar{106} = \bar{1}$$

DIVISORI DELLO ZERO

$$\{\bar{3}, \bar{5}, \bar{6}, \bar{9}, \bar{10}, \bar{12}\}$$

$$\bar{3} \cdot \bar{5} = \bar{15} = \bar{0}$$

$$\bar{6} \cdot \bar{5} = \bar{30} = \bar{0}$$

$$\bar{5} \cdot \bar{9} = \bar{45} = \bar{0}$$

$$\bar{3} \cdot \bar{10} = \bar{30} = \bar{0}$$

$$\bar{12} \cdot \bar{5} = \bar{60} = \bar{0}$$

DEFINIZIONE

$(A, +, \cdot)$ anello. Se $S \subseteq A$. Si è un sottoanello di A se $(S, +, \cdot)$ è un anello

PROPOSIZIONE

S è sottoanello di $(A, +, \cdot)$ se

- 1) $\forall a, b \in S \quad a - b \in S$
- 2) $\forall a, b \in S \quad a \cdot b \in S$

SOTTOANELLI BANALI

$$\{0\} \quad A$$

ESEMPIO

\mathbb{Z} è sottoanello di $(\mathbb{R}, +, \cdot)$

- 1) $\forall a, b \in \mathbb{Z} \Rightarrow a - b \in \mathbb{Z}$
- 2) $\forall a, b \in \mathbb{Z} \Rightarrow a \cdot b \in \mathbb{Z}$

$M_2(\mathbb{R}) \quad S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$ è sottoanello

- $\Rightarrow \forall \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in S$
- $\Rightarrow \forall \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in S$

IDEALE DESTRO E SINISTRO

martedì 17 maggio 2022 07:20

DEFINIZIONE

$(A, +, \cdot)$ anello. $I \subseteq A$ è ideale destro se

$$1) \forall a, b \in I \Rightarrow a \cdot b \in I$$

$$2) \forall a \in I, \forall x \in A \Rightarrow ax \in I$$

è: ideale sinistro se

$$1) \forall a, b \in I \quad a \cdot b \in I$$

$$2) \forall a \in I, \forall x \in A \Rightarrow xa \in I$$

Se I è ideale destro e sinistro $\Rightarrow I$ è ideale bilatero

ESEMPIO

$M_2(\mathbb{R})$

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

È ideale destro? È bilatero?

$$1) \forall \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} \in I$$

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 \cdot a_2 & b_1 \cdot b_2 \\ 0 & 0 \end{pmatrix} \in I$$

$$2) \forall A \in I \quad \forall X \in M_2(\mathbb{R}) \Rightarrow AX \in I$$

$$A = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \quad X = \begin{pmatrix} c & d \\ e & f \end{pmatrix}$$

$$AX = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} ac+be & ad+bf \\ 0 & 0 \end{pmatrix} \in I$$

È ideale sinistro?

$$\forall A \in I, \forall X \in M_2(\mathbb{R}) \Rightarrow XA \in I ?$$

$$XA = \begin{pmatrix} c & d \\ e & f \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ca & cb \\ ea & eb \end{pmatrix} \notin I$$

OSSERVAZIONE

Ogni ideale è sottonegro. Non è vero il viceversa

ESEMPIO

\mathbb{Z} è sottonegro di $(\mathbb{R}, +, \cdot)$

non è ideale $\forall z \in \mathbb{Z}, \forall t \in \mathbb{R} \quad zt \notin \mathbb{Z}$

$$\begin{aligned} z &= 7 & t &= \sqrt{7} \\ 7\sqrt{7} &\notin \mathbb{Z} \end{aligned}$$

IDEALI BANALI E PRINCIPALI

martedì 17 maggio 2022 07:36

IDEALI BANALI

$$(0), A$$

PROPOSIZIONE

Ogni campo è privo di ideali non banali.

DIMOSTRAZIONE

$$\text{Se } I \text{ un ideale, } I \neq (0) \Rightarrow \exists x \in I$$

$$x \neq 0, x \in A \Rightarrow \exists x^{-1} \in A$$

$$\begin{aligned} I \text{ ideale } x \cdot x^{-1} \in I &\Rightarrow 1 \in I \Rightarrow \forall a \in A \\ a \in I \in A &\quad a = 1 \cdot a \in I \Rightarrow I = A \end{aligned}$$

\mathbb{Z} ideali:

$$\begin{aligned} I \text{ ideale di } \mathbb{Z} &\Leftrightarrow I \text{ sottogruppo additivo di } \mathbb{Z} \Leftrightarrow I = \langle m \rangle, m \in \mathbb{Z} \\ I &= \{mh \mid h \in \mathbb{Z}\} \end{aligned}$$

DEFINIZIONE

I è ideale principale destro di A se $I = (z) = \{az \mid x \in A\}$

I è ideale principale sinistro di A se $I = (z) = \{zx \mid x \in A\}$

PROPOSIZIONE

$I = (z) = \{az \mid x \in A\}$ è un ideale di A

DIMOSTRAZIONE

$$\text{D) } \forall i_1, i_2 \in I \quad i_1 - i_2 \in I$$

$$az_1, az_2 \in I \quad az_1 - az_2 = a(z_1 - z_2) \in I$$

2) $\forall i, \in I, \forall \alpha \in A \Rightarrow a_i \alpha \in I$

$$i, \in I, \quad (a_i x)_\alpha = \alpha(x, i) \in I$$

DEFINIZIONE

Un anello commutativo si dice ad ideali principali se tutti gli ideali sono principali.

ESEMPPIO

\mathbb{Z} è un anello ad ideali principali:

$$I = (m) = \{mh \mid h \in \mathbb{Z}\} = (m)$$

$$\mathbb{Z} = (1)$$

A anello I : ideale bilatero

$$A/I = \{a+I \mid a \in A\}$$

$(A/I, +)$ è un gruppo abeliano

$$(a+I) + (b+I) = (a+b) + I$$

$$(a+I) \cdot (b+I) \stackrel{\text{def}}{=} ab + I$$

$(A/I, +)$ l'elemento neutro I

$(A/I, \cdot)$ l'elemento neutro $1+I$

DEFINIZIONE

I ideale bilatero di A è primo se $ab \in I \Rightarrow a \in I$ oppure $b \in I$

\mathbb{Z} $I = (2)$ è un ideale primo

$$ab \in I = (2) \Rightarrow ab = 2h \Rightarrow 2 \mid ab \Rightarrow 2 \mid a \text{ oppure } 2 \mid b \Rightarrow a = 2 \cdot t_1 \text{ o } b = 2 \cdot t_2 \Rightarrow a \in I \text{ o } b \in I$$

$$I = (6) \quad 2 \cdot 3 \in I \text{ ma } 2 \notin I \text{ e } 3 \notin I$$

ANELLO COMMUTATIVO

martedì 17 maggio 2022 16:45

PROPOSIZIONE

A anello commutativo, P è ideale primo di A se e solo se A/P è un dominio d'integrità

DIMOSTRAZIONE

\Leftarrow P primo dimostriamo che A/P è un dominio d'integrità

$\Leftarrow z+P, b+P \in A/P$ tale che

$$(z+P)(b+P) = P \Rightarrow zb+P = P \Rightarrow zb \in P \Rightarrow z \in P \circ b \in P$$

$z+P = P \circ b+P = P$. Abbiamo dimostrato che se

$$(z+P)(b+P) = P \Rightarrow z+P = P \circ b+P = P$$

Viceversa sia A/P dominio d'integrità $\Rightarrow P$ è primo

$$\Leftarrow zb \in P \Rightarrow zb+P = P \Rightarrow (z+P)(b+P) = P$$

$$\Rightarrow (z+P) \circ P \circ (b+P) = P \Rightarrow z \in P \circ b \in P \Rightarrow P \text{ è primo}$$

PROPOSIZIONE

Gli ideali primi di \mathbb{Z} sono $I = (p)$ con p primo

DIMOSTRAZIONE

$I = (m)$ è primo $\Leftrightarrow \mathbb{Z}/(m)$ è un dominio d'integrità

$\Leftrightarrow \mathbb{Z}/(m) \cong \mathbb{Z}_m \Leftrightarrow \mathbb{Z}_m$ è un dominio d'integrità $\Leftrightarrow m$ è primo $m = p$

PROPOSIZIONE

A anello commutativo con 1

M \bar{e} ideale massimale di A cos $\ A/\mathcal{M}$ è un campo?

Se M \bar{e} massimale A/\mathcal{M} è un campo $\Rightarrow A/\mathcal{M}$ è un dominio d'integrità $\Rightarrow \mathcal{M}$ primo

$$A = M_2(\mathbb{Z})$$

$$M_m(A), \text{ Anello}$$

$X \in M_m(A)$ è invertibile
se $\det X \in U(A)$

$$S \subset B = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{Z} \right\}$$

1) B è sottanello di A, commutativo con 1 e determinarne i divisori dello zero e gli elementi invertibili

$$B = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{Z} \right\}$$

B è sottanello d. $M_2(\mathbb{Z})$ se

- 1) $\forall A_1, A_2 \in B \quad A_1 - A_2 \in B$
 2) $\forall A_1, A_2 \in B \quad A_1 \cdot A_2 \in B$

$$A_1 = \begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix} \quad A_1 - A_2 = \begin{pmatrix} a_1 - a_2 & 0 \\ 0 & d_1 - d_2 \end{pmatrix} \in B$$

$$A_1 \cdot A_2 = \begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & d_1 d_2 \end{pmatrix} \in B$$

B è sottanello commutativo $A_1 A_2 = A_2 A_1$

$$X = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \text{ è invertibile se } \det A \in U(\mathbb{Z}) = \{1, -1\}$$

$$\det X = ab = \pm 1 \quad a = b = \pm 1$$

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

ESERCIZI SUGLI IDEALI

martedì 17 maggio 2022 17:19

$$I = \left\{ \begin{pmatrix} 5^h & 0 \\ 0 & 3^k \end{pmatrix} \mid h, k \in \mathbb{Z} \right\} \subseteq B$$

I è ideale se

- 1) $\forall A_1, A_2 \in I \Rightarrow A_1 - A_2 \in I$
- 2) $\forall A_1 \in I, \forall x \in B \Rightarrow Ax \in I$

$$A_1 = \begin{pmatrix} 5^h & 0 \\ 0 & 3^k \end{pmatrix}, \quad A_2 = \begin{pmatrix} 5^{h'} & 0 \\ 0 & 3^{k'} \end{pmatrix} \quad A_1 - A_2 = \begin{pmatrix} 5^{h-h'} & 0 \\ 0 & 3^{k-k'} \end{pmatrix} \in B$$

$$x = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad Ax = \begin{pmatrix} 5^h a & 0 \\ 0 & 3^k d \end{pmatrix}$$

$$\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix} \in I$$

$\notin I \quad \notin I \Rightarrow I$ non è primo

$$I \text{ è primo se } ab \in I \Rightarrow a \in I \circ b \in I$$

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

$$+(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$U(A \times B) = U(A) \times U(B)$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

$(A \times B, +, \cdot)$ è un anello

$A \times B$ è dominio d'integrità? $(0, b) (a, 0) = (0, 0)$

$\mathbb{Z}_2 \times \mathbb{Z}_4$ non è un dominio d'integrità

$$(\bar{0}, \bar{5}) (\bar{a}, \bar{0})$$

$$\mathbb{Z}_4 \times \mathbb{Z}_4 \quad (\bar{2}, \bar{2}) \cdot (\bar{2}, \bar{2}) = (\bar{0}, \bar{0})$$

$$\begin{aligned} U(\mathbb{Z}_2 \times \mathbb{Z}_4) &= U(\mathbb{Z}_2) \times U(\mathbb{Z}_4) & U(\mathbb{Z}_2) &= \{\bar{1}\} \\ &= \{(\bar{1}, \bar{1}), (\bar{1}, \bar{3})\} & U(\mathbb{Z}_4) &= \{\bar{1}, \bar{3}\} \end{aligned}$$

DEFINIZIONE

A, B anelli. Un omomorfismo di A in B è un'applicazione

$f: A \rightarrow B$ tale che

- 1) $\forall a_1, a_2 \in A \quad f(a_1 + a_2) = f(a_1) + f(a_2)$
- 2) $\forall a_1, a_2 \in A \quad f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$

ESEMPIO

$f: \mathbb{Z} \rightarrow \mathbb{Z}_6$ è un omomorfismo?
 $a \rightarrow 3\bar{a}$

$$\textcircled{1} \quad \forall a_1, a_2 \in \mathbb{Z} \quad f(a_1 + a_2) = 3\overline{a_1 + a_2} = 3(\bar{a}_1 + \bar{a}_2) = 3\bar{a}_1 + 3\bar{a}_2 = f(a_1) + f(a_2)$$

$$2) \forall a_1, a_2 \in \mathbb{Z} \quad f(a_1 \cdot a_2) = 3\overline{a_1 a_2} = (3\bar{a}_1)(3\bar{a}_2) = 9\overline{a_1 a_2} = 3\overline{a_1 a_2}$$

ESEMPIO

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

$$a \mapsto 2a$$

$$f(a \cdot b) = 2ab \neq 2a \cdot 2b = f(a) \cdot f(b)$$

Non è un omomorfismo

$$f: A \rightarrow B \quad \text{OMOMORFISMO NUOVO}$$

$$a \mapsto \alpha_B$$

$$\begin{array}{ll} f: A \rightarrow B & \text{INIEZIONE} \quad \text{MONOMORFISMO} \\ & \text{SURGETTIVITÀ} \quad \text{EPIMORFISMO} \\ & \text{BIETTIVO} \quad \text{ISOMORFISMO} \end{array}$$

PROPRIETÀ

$$\begin{aligned} f(\alpha_A) &= \alpha_B \\ f(-a) &= -f(a) \end{aligned}$$

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}) \mid a \in \mathbb{R} \right\} \text{ sotto spazio di } M_2(\mathbb{R})$$

$$\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in A \Rightarrow \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix} \in A \right)$$

$$\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \right) = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in A$$

$$\left(\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \right) = \begin{pmatrix} ba & 0 \\ 0 & 0 \end{pmatrix} \in A$$

$$\text{Ha unità } \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$f: A \rightarrow M_2(\mathbb{R}) \quad \text{È un omomorfismo?}$$

$$\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \right) \quad f(1_A) = f\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \rightarrow \text{non è unità di } M_2(\mathbb{R})$$

D) $\forall A_1, A_2 \in A$

$$f(A_1 + A_2) = f(A_1) + f(A_2)$$

$$A_1 + A_2 = \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix}$$

$f: A \rightarrow B$ omomorfismo di anelli

DEFINIZIONE

Il nucleo di f , $\ker f$, è

$$\ker f = \{ a \in A \mid f(a) = 0_B \} \subseteq A$$

L'immagine di f è

$$\text{Im } f = \{ f(a) \mid a \in A \} \subseteq B$$

PROPOSIZIONI

D) $\ker f$ è un ideale bilatero di A

2) $\text{Im } f$ è un sottogetto di B

DIMOSTRAZIONE

1)

D) $\forall a_1, a_2 \in \ker f \Rightarrow a_1 - a_2 \in \ker f$

$$f(a_1 - a_2) = f(a_1) - f(a_2) = 0_B - 0_B = 0_B$$

2) $\forall a \in \ker f, \forall x \in A \Rightarrow ax \in \ker f$

$$f(ax) = f(a) \cdot f(x) = 0_B f(x) = 0_B$$

2)

$\forall b_1, b_2 \in \text{Im } f \Rightarrow b_1 - b_2 \in \text{Im } f$

$$\forall b_1, b_2 \in \text{Im } f \Rightarrow b_1 - b_2 \in \text{Im } f$$

$$b_1, b_2 \in \text{Im } f$$

$$b_1 = f(a_1) \in b_2 = f(a_2)$$

$$b_1 - b_2 = f(a_1) - f(a_2) = f(a_1 - a_2) \in \text{Im } f$$

$$b_1 \cdot b_2 = f(a_1) \cdot f(a_2) = f(a_1 \cdot a_2) \in \text{Im } f$$

$$A/\ker f = \{a + \ker f \mid a \in A\} \quad \text{anello quoziente}$$

$$(a + \ker f) + (b + \ker f) = (a + b) + \ker f$$

$$(a + \ker f)(b + \ker f) = ab + \ker f$$

$$\ker f = 0_{A/\ker f}$$

Se $1 \in A$ è units di $A/\ker f$

PROPOSIZIONE

$f: A \rightarrow B$ è un omomorfismo iniettivo $\Leftrightarrow \ker f = \{0_A\}$

Per il teorema di omomorfismo tra anelli. Se $f: A \rightarrow B$ omomorfismo di anelli.
Allora

$$A/\ker f \cong \text{Im } f$$

In particolare se f è suriettivo $A/\ker f \cong B = \text{Im } f$

Dimostrazione

$f: A \rightarrow B$ omomorfismo. Definisco

$$h: A/\ker f \rightarrow \text{Im } f$$

$$a + \ker f \rightarrow f(a)$$

Un omomorfismo di anelli:

$$\begin{array}{c} a_1 + \ker f \\ a_2 + \ker f \end{array} \quad f((a_1 + \ker f) + (a_2 + \ker f)) = f(a_1) + f(a_2) \quad \begin{array}{c} a_1 \\ a_2 \end{array}$$

$$\begin{aligned} h(a_1 + a_2) &= h((a_1 + a_2) + \ker f) = f(a_1 + a_2) = f(a_1) + f(a_2) \\ &\qquad\qquad\qquad \parallel \\ &\qquad\qquad\qquad h(a_1 + \ker f) + h(a_2 + \ker f) \end{aligned}$$

$$h(A_1 \cdot A_2) = h(A_1) \cdot h(A_2)$$

$$\begin{aligned} h(A_1 \cdot A_2) &= h((a_1 \cdot a_2) + \ker f) = f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2) \\ &\qquad\qquad\qquad \parallel \\ &\qquad\qquad\qquad h(a_1 + \ker f) \cdot h(a_2 + \ker f) \end{aligned}$$

È suriettivo

$$\ker h = \{a + \ker f \mid h(a + \ker f) = 0\} \quad f(a) = 0 \Rightarrow a \in \ker f$$

Esercizio

$$A = \mathbb{Z} \times \mathbb{Z}$$

$$S_2 I = \{(2h, 10k) \in A \mid h, k \in \mathbb{Z}\}$$

Dimostrare che I è ideale

$\Rightarrow \forall i_1, i_2 \in I \quad i_1 + i_2 \in I$

$\Rightarrow \forall i_1 \in I, \forall x \in A \quad i_1 x = x i_1 \in I$

$$i_1 - i_2 = (2h_1, 10k_1) - (2h_2, 10k_2) = (2(h_1 - h_2), 10(k_1 - k_2)) \in I$$

$$i_1 x = (2h_1, 10k_1) \quad \forall x = (a, b)$$

$$i_1 x = (2h_1, 10k_1)(a, b) = (2h_1 a, 2k_1 b) \in I$$

Esercizio

$$S_2 f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_{10}$$

$$(a, b) \rightarrow (\bar{a}_2, \bar{b}_{10})$$

Dimostrare che f è un omomorfismo di anelli suriettivo

$$\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$$

$$f((a, b) + (c, d)) = f(a+b) + f(c+d)$$

$$f((a, b) \cdot (c, d)) = f(a \cdot c) \cdot f(c \cdot d)$$

$$f((a, b) + (c, d)) = f((a+c, b+d)) = (\bar{a+c}_2, \bar{b+d}_{10})$$

$$= (\bar{a}_2 + \bar{c}_2, \bar{b}_{10} + \bar{d}_{10}) = (\bar{a}_2, \bar{b}_{10}) + (\bar{c}_2, \bar{d}_{10}) = f((a, b)) + f((c, d))$$

$$f((a, b) \cdot (c, d)) = f((a \cdot c, b \cdot d)) = (\bar{a \cdot c}_2, \bar{b \cdot d}_{10})$$

$$= (\bar{a}_2, \bar{b}_{10})(\bar{c}_2, \bar{d}_{10}) = f((a, b)) \cdot f((c, d))$$

$$\begin{aligned} f((a,b) \cdot (c,d)) &= f((ac, bd)) = (ac_2, bd_{10}) \\ &= (\bar{a}_2, \bar{b}_{10})(\bar{c}_2, \bar{d}_{10}) = f((a,b)) \cdot f((c,d)) \end{aligned}$$

f è suriettiva $f(\bar{a}_2, \bar{b}_{10}) = f((a,b))$

Calcolare $\ker f$. I è un ideale primo?

$$\begin{aligned} \ker f &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid f(a,b) = (\bar{a}_2, \bar{b}_{10})\} \\ &\quad \| \\ &= (\bar{a}_2, \bar{b}_{10}) = (\bar{a}_2, \bar{b}_{10}) \end{aligned}$$

$$\bar{a}_2 = \bar{b}_2 \quad a \equiv 0 \pmod{2} \quad a \equiv 2h$$

$$\bar{b}_{10} = \bar{0}_{10} \quad b \equiv 0 \pmod{10} \quad b \equiv 10t$$

$$\ker f = \{(2h, 10k) \mid h, k \in \mathbb{Z}\} = I$$

$$A_{/\ker f} \cong \mathbb{Z}_2 \times \mathbb{Z}_{10} \text{ non è un dominio d'integrità}$$

$\Rightarrow I$ non è primo né massimale

$$(\mathbb{Z}_6, +, \cdot) \quad A = \mathbb{Z}_6 \times \mathbb{Z}_6$$

D) Determinare $|A|_1$, i divisori dello zero e le unità

$$|A|_1 = 36 \quad (\bar{0}, \bar{0}) \quad (\bar{0}, \bar{5})$$

$$\mathbb{Z}_6 \quad \bar{2} \cdot \bar{3} = \bar{6} \quad (\bar{2}, \bar{3}), (\bar{3}, \bar{2}), (\bar{2}, \bar{2}), (\bar{3}, \bar{3})$$

$$U(\mathbb{Z}_6) = \{ \bar{k} \mid (k, 6) = 1 \}$$

$$= \{ \bar{1}, \bar{5} \}$$

$$U(A) = \{ (\bar{1}, \bar{1}), (\bar{1}, \bar{5}), (\bar{5}, \bar{1}), (\bar{5}, \bar{5}) \}$$

$$|U(A)| = 4 \quad U(A) \text{ è circolo? No, tutti gli elementi hanno periodo 2}$$

$$\text{Se fosse circolo} \Rightarrow U(A) = \langle g \rangle \text{ con } \text{ord}(g) = 4 \Rightarrow g^4 = 1$$

$$(\bar{1}, \bar{5})^2 = (\bar{1}, \bar{5}) \cdot (\bar{1}, \bar{5}) = (\bar{1}, \bar{25}) = (\bar{1}, \bar{1})$$

$$S_3) \quad I = \{ (\bar{0}, \bar{z}) \mid \bar{z} \in \mathbb{Z}_6 \} \subseteq A \quad |I| = 6$$

Provare che I è ideale di $A = \mathbb{Z}_6 \times \mathbb{Z}_6$

$$\forall (\bar{0}, \bar{z}), (\bar{0}, \bar{b}) \in I \quad (\bar{0}, \bar{z}) - (\bar{0}, \bar{b}) = (\bar{0}, \bar{z} - \bar{b}) \in I$$

$$\forall (\bar{0}, \bar{z}) \in I \quad \forall (\bar{x}, \bar{y}) \in A \quad (\bar{0}, \bar{z}) \cdot (\bar{x}, \bar{y}) = (\bar{0}, \bar{zy}) \in I$$

$$J = \{ (\bar{x}, \bar{z}) \mid \bar{z} \in \mathbb{Z}_6 \} \text{ è ideale di } A?$$

$$|J| = 6$$

J è sottosanotto, non è ideale!

$$\forall (\bar{x}, \bar{z}) \in J \quad \forall (\bar{x}, \bar{y}) \in A$$

$$(\bar{x}, \bar{z}) \cdot (\bar{x}, \bar{y}) = (\bar{x}\bar{x}, \bar{zy}) \notin J$$

Dimostrare che $A/I \cong \mathbb{Z}_6$

$$I = \{(\bar{a}, \bar{b}) \mid \bar{a} \in \mathbb{Z}_6\}$$

$$A = \mathbb{Z}_6 \times \mathbb{Z}_6$$

$$\begin{array}{ccc} f: \mathbb{Z}_6 \times \mathbb{Z}_6 & \rightarrow & \mathbb{Z}_6 \\ (\bar{a}, \bar{b}) & \mapsto & \bar{a} \\ & & \text{ker } f = \{(\bar{a}, \bar{b}) \mid f((\bar{a}, \bar{b}))\} = \{\bar{a}, \bar{0}\} \mid \bar{a} \in \mathbb{Z}_6\} = \\ & & \bar{a} \\ & & = \{(\bar{0}, \bar{b}) \mid \bar{b} \in \mathbb{Z}_6\} = I \end{array}$$

f è un omomorfismo di anelli

$$f((\bar{a}, \bar{b}) + (\bar{c}, \bar{d})) = f(\bar{a}, \bar{b}) + f(\bar{c}, \bar{d})$$

$$f((\bar{a}, \bar{b}) \cdot (\bar{c}, \bar{d})) = f((\bar{a}, \bar{b})) \cdot f((\bar{c}, \bar{d}))$$

$$\text{Suriettivo} \quad \forall \bar{a} \in \mathbb{Z}_6 \Rightarrow \bar{a} = f((\bar{a}, \bar{b})) \quad \forall \bar{b} \in \mathbb{Z}$$

$$G = GL_2(\mathbb{Z}_{10}) = \{ A \in M_2(\mathbb{Z}_{10}) \mid A \text{ è invertibile} \}$$

$\det A$ è invertibile in

$$S \cap H = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in G \mid \bar{a}\bar{c} = 1 \right\} \quad |H| = 40$$

$$|H| = ? \quad U(\mathbb{Z}_{10}) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$$

$$|U(\mathbb{Z}_{10})| = \varphi(10) = \varphi(2) \cdot \varphi(5) = 4$$

OMOMORFISMI DI ANELLI

lunedì 23 maggio 2022 08:00

ESEMPIO

H è sottogruppo di G

$$\text{Se } H_1 = \begin{pmatrix} \bar{\delta} & \bar{\alpha} \\ \bar{b} & \bar{c} \end{pmatrix}, \quad H_2 = \begin{pmatrix} \bar{\alpha} & \bar{\alpha} \\ \bar{\beta} & \bar{\gamma} \end{pmatrix} \in H$$

$$H_1 \cdot H_2^{-1} \in H \quad H_2^{-1} = \frac{1}{\det A} \begin{pmatrix} \bar{\delta} & \bar{\alpha} \\ \bar{\beta} & \bar{\alpha} \end{pmatrix}$$

$$H_2^{-1} = \begin{pmatrix} \bar{\delta} & \bar{\alpha} \\ \bar{b} & \bar{c} \end{pmatrix} \cdot \begin{pmatrix} \bar{\delta} & \bar{\alpha} \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} \bar{\delta}\bar{\delta} & \bar{\alpha} \\ \bar{b}\bar{\delta} - \bar{\beta}\bar{c} & \bar{c}\bar{\alpha} \end{pmatrix} \in H \quad \bar{\alpha}\bar{\delta}\bar{c}\bar{\alpha} = 1$$

ESEMPIO

$$S \subset K = \left\{ \begin{pmatrix} \bar{1} & \bar{\alpha} \\ \bar{b} & \bar{1} \end{pmatrix} \mid b \in \mathbb{Z}_{10} \right\}$$

$$K \trianglelefteq H$$

$$\forall k_1, k_2 \in K \quad k_1 \cdot k_2^{-1} \in K \quad k_2 = \begin{pmatrix} \bar{1} & \bar{\alpha} \\ \bar{b} & \bar{1} \end{pmatrix}$$

$$\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{b} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{\alpha} \\ \bar{b} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{\alpha} \\ \bar{b} \cdot \bar{b} & \bar{1} \end{pmatrix} \in K$$

$$\forall k_1 \in K, \quad \forall A \in H \quad A^{-1} k_1 A \in K$$

Verificare. Se $f: H \rightarrow U(\mathbb{Z}_{10})$ omomorfismo di gruppi

$$\begin{pmatrix} \bar{\delta} & \bar{\alpha} \\ \bar{b} & \bar{c} \end{pmatrix} \rightarrow \bar{a}$$

Calcolare $\text{Ker } f$. È sottovo? H/K è c.c.?

$$\bar{a} = \bar{1} \quad f \left(\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{b} & \bar{1} \end{pmatrix} \right) = \bar{1}$$

$$\bar{a} = \bar{3} \quad f \left(\begin{pmatrix} \bar{3} & \bar{0} \\ \bar{b} & \bar{1} \end{pmatrix} \right) = \bar{3}$$

$$\bar{a} = \bar{7} \quad f \left(\begin{pmatrix} \bar{7} & \bar{0} \\ \bar{b} & \bar{1} \end{pmatrix} \right) = \bar{7}$$

$$\bar{a} = \bar{9} \quad f \left(\begin{pmatrix} \bar{9} & \bar{0} \\ \bar{b} & \bar{1} \end{pmatrix} \right) = \bar{9}$$

$$S_2 \subset K = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{b} & \bar{1} \end{pmatrix} \mid \bar{b} \in \mathbb{Z}_{10} \right\} \quad H/K \cong U(\mathbb{Z}_{10}) \text{ non-cyclic}$$

$$\ker f = \left\{ A = \begin{pmatrix} \bar{a} & \bar{0} \\ \bar{b} & \bar{c} \end{pmatrix} \in H \mid f(A) = \bar{1} \right\}$$

$$= \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{b} & \bar{1} \end{pmatrix} \mid \bar{b} \in \mathbb{Z}_{10} \right\} = K$$

A anello commutativo con unità, x indeterminata

Indichiamo con

$$A[x] = \left\{ f(x) = \sum_{i=0}^m a_i x^i \mid \forall m \in \mathbb{N}, \forall a_i \in A \right\}$$

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m$$

a_0 = termine noto, a_m = coeff. diretto

$$\text{gr } f(x) = m \quad a_m \neq 0$$

$(A[x], +, \cdot)$ anello commutativo con 1

$$\forall f(x), g(x) \in A[x] \quad f(x) = \sum_{i=0}^m a_i x^i \quad m \geq m \\ g(x) = \sum_{i=0}^m b_i x^i$$

$$f(x) + g(x) = \sum_{i=0}^m (a_i + b_i) x^i$$

$$f(x) = x^3 + 2x + 1 \quad g(x) = x + 5$$

$$f(x) + g(x) = (1+5) + (2+1)x + 0x^2 + (1+0)x^3$$

$$f(x) \cdot g(x) = (a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m) \cdot (b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m) = \\ = a_0 b_0 + (a_0 b_1 + b_0 a_1) x + \dots + (a_m b_m) x^{m+m}$$

$(A[x], +)$ gruppo abeliano
0 elemento neutro

$(A[x], \cdot)$ 1 unità

$f(x) = a \neq 0 \quad a \in A \quad$ è un polinomio di grado zero

$f(x) = a + 0 \quad a \in A$ è un polinomio di grado zero

$f(x) = 0$ grado è indeterminato

PROPOSIZIONE

A dominio d'integrità \Rightarrow

- 1) $\text{gr}(f(x) + g(x)) \leq \max \text{gr}(f(x), g(x))$
- 2) $\text{gr}(f(x) \cdot g(x)) = \text{gr}(f(x)) + \text{gr}(g(x))$
- 3) $A[x]$ è un dominio d'integrità

DIMOSTRAZIONE

$$f(x) = \sum_{i=0}^m a_i x^i, \quad g(x) = \sum_{i=0}^n b_i x^i$$

Se $m > n \quad f(x) + g(x) = (a_0 + b_0) + \dots + a_n x^n$

Se $m = n \quad f(x) + g(x) = (a_0 + b_0) + \dots + (a_n + b_n) x^n$

Se $b_m \neq -a_n \quad a_m + b_m \neq 0$

Se $b_m = -a_n \Rightarrow \text{gr}(f(x) + g(x)) < n$

$$f(x) g(x) = \dots + a_n b_m x^{m+n} \quad a_n b_m \neq 0 \Rightarrow A \text{ è dominio di integrità}$$

ESEMPIO

$$\begin{aligned} f(x) &= \bar{1} + \bar{2} \cdot x + \bar{3} x^2 \in \mathbb{Z}_6[x] \\ g(x) &= \bar{1} + \bar{2} \cdot x^3 \end{aligned}$$

$$f(x) g(x) = (\bar{1} + \bar{2}x + \bar{3}x^2)(\bar{1} + \bar{2}x^3)$$

$$\begin{aligned} &= \bar{1} + \bar{2}x^3 + \bar{2}x + \bar{9}x^4 + \bar{3}x^2 + \bar{6}x^2 \\ &\quad " \\ &\quad \bar{0}x^2 \end{aligned}$$

ESERCIZI ANELLO DEI POLINOMI

mercoledì 1 giugno 2022 17:53

$$U(A[x])$$

$$U(A) \subseteq U(A[x])$$

$$U(A) = \{ a \in A \mid a \text{ è invertibile} \}$$

$$f(x) = a \in U(A) \quad f(x) \text{ è invertibile ed ha inverso } a^{-1}$$

$$U(A[x]) = U(A)$$

$$\text{Se } f(x) \in U(A[x]) \Rightarrow \exists g(x) \in A[x] \text{ tale che}$$

$$f(x) \cdot g(x) = 1$$

$$\text{gr}(f(x) \cdot g(x)) = \text{gr}(1)$$

$$\text{gr } f(x) + \text{gr } g(x) = 0 \Rightarrow f(x) = a \in A$$

ESEMPIO

$$f(x) \in \mathbb{Z}[x] \quad U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{1, -1\}$$

$$f(x) \in \mathbb{Z}_{12}[x] \quad U(\mathbb{Z}_{12}[x]) = U(\mathbb{Z}_{12}) \\ = \{\pm 1, \pm 5, \pm 7, \pm 11\}$$

$$f(x) \in K[x] \quad K = \text{campo}$$

$$U(K[x]) = U(K) = K^*$$

K campo, $K[x]$

PROPOSIZIONE

$$\forall f(x), g(x) \in K[x] \quad \exists q(x), r(x) \in K[x]$$

$$\text{tale che } f(x) = g(x)q(x) + r(x)$$

$$\text{con } r(x) = 0 \quad \text{oppure} \quad \text{gr}(r(x)) < \text{gr}(g(x))$$

DEFINIZIONE

Sono $f(x), g(x) \in K[x]$

$g(x)$ divide $f(x)$ se $\exists q(x) \in K[x]$ tale che $f(x) = g(x) \cdot q(x)$

ESEMPIO

$$f(x) = x^4 + 2x^3 + 5x + 1 \quad g(x) = x^2 - 2 \in \mathbb{R}[x]$$

$$\begin{array}{r}
 3x^4 + 2x^3 \quad + 5x + 1 \\
 \underline{- 3x^4} \quad \underline{- 6x^2} \\
 2x^3 \quad 6x^2 + 5x + 1 \\
 \underline{- 2x^3} \quad \underline{- 4x} \\
 6x^2 + 4x + 1 \\
 \underline{- 6x^2} \quad \underline{- 12} \\
 4x + 13
 \end{array}
 \left| \begin{array}{l}
 x^2 - 2 \\
 \hline
 \{ 3x^2 + 2x + 6 \} \quad q(x) \\
 \hline
 r(x)
 \end{array} \right.$$

$$f(x) = g(x)q(x) + r(x)$$

$$3x^4 + 2x^3 + 5x + 1 = (x^2 - 2)(3x^2 + 2x + 6) + (4x + 13)$$

ESEMPIO

$$f(x) = 2x^4 + x^3 - x^2 + 2x + 1 \in \mathbb{Z}_3[x]$$

$$g(x) : x^2 + 2$$

$ \begin{array}{r} 2x^4 + x^3 - x^2 + 2x + 1 \\ \underline{- 2x^4} \quad + x^2 \\ \hline x^3 - 2x^2 + 2x + 1 \\ \underline{- x^3} \quad + 2x \\ \hline - 2x^2 \quad + 1 \\ \underline{- - 2x^2} \quad - 1 \\ \hline \underline{\underline{1}} \end{array} $	$ \begin{array}{c} x^2 + 2 \\ \hline \{ 2x^2 + x - 2 \} = q(x) \end{array} $
--	--

MCD TRA POLINOMI

mercoledì 1 giugno 2022 18:49

DEFINIZIONE

Dati $f(x), g(x) \in K[x]$, il massimo comun divisor tra $f(x) \in g(x)$ è un polinomio $d(x) \in K[x]$ tale che

$$1) d(x) | f(x) \text{ e } d(x) | g(x)$$

$$2) \text{ Se } d'(x) | f(x) \text{ e } d'(x) | g(x) \Rightarrow d'(x) | d(x)$$

PROPOSIZIONE

Dati $f(x), g(x) \in K[x]$ esiste il loro M.C.D. = $d(x)$

Se $d'(x)$ è un altro M.C.D. allora $d'(x) = c \cdot d(x)$, $c \in K$

Si determina con il metodo delle divisioni successive
(sarà l'ultimo resto non nullo)

DEFINIZIONE

$$\text{Se } I = (f(x)) = \{ f(x) \cdot g(x) \mid g(x) \in K[x] \}$$

è detto generato da $f(x)$

$$K[x] = (1) = \{ 1 \cdot g(x) \mid g(x) \in K[x] \}$$

PROPOSIZIONE

$K[x]$ è un anello ad ideali principali

DIMOSTRAZIONE

Se I idale di $k[x]$

Se $I = (0)$ OK

Supponiamo che $I \neq (0) \Rightarrow \exists f(x) \neq 0 \in I$
considero $f(x) \in I$ di grado più piccolo

Dimostra che $I = (f(x))$

Naturalmente $(f(x)) \subseteq I$

Dimostra che $I \subseteq (f(x))$

Se $h(x) \in I$. Divido $h(x)$ per $f(x)$

$$\begin{aligned} \Rightarrow h(x) &= f(x)q(x) + r(x) & r(x) = 0 \text{ oppure} \\ \Rightarrow r(x) &= h(x) - f(x)q(x) & \text{gr } r(x) < \text{gr } f(x) \\ &\in I & \end{aligned}$$

$\Downarrow r(x) = 0$

$$\begin{aligned} \Rightarrow h(x) &= f(x)q(x) \Rightarrow h(x) \in (f(x)) \\ \Rightarrow I &\subseteq (f(x)) \end{aligned}$$

POLINOMI IRRIDUCIBILI

mercoledì 1 giugno 2022 19:04

DIFINIZIONE

Se $f(x) \in K[x]$. $f(x)$ è irriducibile

Se $f(x) = g(x) \cdot h(x) \Rightarrow g(x) \in K$ oppure $h(x) \in K$

ESEMPIO

$$2(x^2 + 1) \in \mathbb{R}[x]$$

TEOREMA DI RUFFINI

$f(x)$ è divisibile per $(x-a) \Leftrightarrow f(a)=0$

DIMOSTRAZIONE

Se $f(x)$ divisibile per $(x-a) \Rightarrow f(x) = (x-a)q(x)$.

$$\Rightarrow f(a) = 0 \cdot q(a) = 0$$

Viceversa se a radice di $f(x)$, divide $f(x)$ per $(x-a)$

$$f(x) = (x-a)q(x) + r(x)$$

$$\text{gr}(r(x)) < \text{gr}(x-a) \Rightarrow \text{gr}(r(x)) = 0$$

$$f(a) = r(a) = 0 \Rightarrow r(x) = 0$$

ESEMPPIO

$$f(x) = (x^2+1)(x^2+5) \text{ in } \mathbb{R}[x]$$

PROPOSIZIONE

$$f(x) \in K[x], \deg(f(x)) = 2, 3$$

è irriducibile \Leftrightarrow non ammette radici

$$\deg(f(x)) = 2 \text{ riducibile} \Rightarrow f(x) = (ax+b)(cx+d)$$

$$f(x) = (ax+b)(cx^2+dx+e)$$

POLINOMI IRRIDUCIBILI 2

mercoledì 1 giugno 2022 19:21

DEFINIZIONE

$f(x)$ è irriducibile se $f(x) = g(x) \cdot h(x) \Rightarrow g(x) \in k^*$ o $h(x) \in k^*$

PROPOSIZIONE

Se $f(x) \in k[x]$ allora $f(x)$ si decomponga in prodotto di polinomi irriducibili (un modo unico a meno dell'ordine e di segni)

$$f(x) = h_1(x) \cdot h_2(x) \cdot \dots \cdot h_t(x)$$

$$f(x) = g_1(x) \cdot g_2(x) \cdot \dots \cdot g_m(x)$$

$$\text{t.c.m } h_i = g_j \quad h_i = c_i$$