

e - e - e - e - e - e

$(G, +, \lambda)$ GRUPPO, $H \in G$ sottogruppo

$$\left. \begin{array}{l} g \sim g' \leftrightarrow g^{-1} * g' \in H \\ g \sim g' \leftrightarrow g + (g')^{-1} \in H \end{array} \right\}$$

[Epilepsie]

$G/\langle \eta_s \rangle$ la cardinalità di $G/\langle \eta_s \rangle$ si denota con $[G : H]$ detta INDICE di H in G

Se H è normale in G (ogni classe $gH = Hg$), allora no e no coincidono

• $G/n_s = G/n_D = G/H$ esclude una struttura di gruppo

$$\underline{\text{Es}} \quad nZ = Z \quad \text{sotto gruppo} \quad Z_{\frac{n}{n}} = Z_n$$

Teorema (Lagrange) Sia G un gruppo finito e sia H un sottogruppo ($\subseteq G$). Allora:

$$* G = [G : H] \cdot *H$$

 Tutti i sottogruppi di un gruppo finito hanno cardinalità un divisore di 6

$$\underline{\text{Ex}} \quad G = S_3 = \{ \text{Id}, \varphi, \psi, \varphi \circ \psi, \psi \circ \varphi, \psi^2 \} \quad * \quad G = G$$

$\bullet H = \{Id, \varphi\}$ e sottogruppo

de classi laterale sinistra sono H , $\psi_0 H$, $\psi^2_0 H$

$$6 = \frac{3 \cdot 2}{\text{è divisore di } 6}$$

$$G_{HS} = \{ \text{insieme classi lat. } \Delta x \} = \{ H, \psi = H, \psi^2 = H \} \quad [G : H] = 3$$

• $T = \{Jd, \rho, \psi, \psi^2\}$ * $T = 4 \times 6 \xrightarrow{\text{LAGRANGE}} T$ non e' soleggiato di

• $P = \{p, q\}$ * $p = 2$ $16 = 6$ TUTTAVIA P non è un sottogruppo di G ,
es. $\frac{p}{q} \notin P$
↳ E.L. NEUTRA

Def (G, \ast, λ) gruppo, $g \in G$. Chiamiamo **ordine** di g (o perodo di g) il più piccolo $n \in \mathbb{Z}_+$ (se esiste), per cui $g^n = \lambda$. Si denota con $\text{ord}(g)$.

$$g + \underbrace{-} + g$$

n volte

La cardinalità di G si chiama ordine di G .

Esercizio $(\mathbb{Z}, +, \circ)$ per $\exists x \in \mathbb{Z}$ tale che $x^2 = 0$? $\text{red}(\circ) = 1$

perche' $0 \neq 0$ = 0 (effuso 2^o alla prima volta, n'è più perbole)

$g=3$ puol e' l'ordine di 3? $\text{ord}(3) = \infty$ — allora $\exists n \in \mathbb{Z}^+$

o zero quante volte deve sommare 3 per ottenere 0
* * * * * volte

$$F(17 - \bar{z}) = 1 - \bar{z} \quad \text{and} \quad F(\bar{z}) = 7 \quad \text{so} \quad 1 - \bar{z} = 7 \quad \text{or} \quad \bar{z} = -6$$

*

λ

Ese $(\mathbb{Z}_{12}, +, \bar{0})$ $g = \bar{2}$ $\text{ord}(\bar{2}) = ?$ il più piccolo $n \in \mathbb{Z}_+$ t.c. $\bar{2} + \dots + \bar{2} = \bar{0}$

$$\bar{2} + \bar{2} = \bar{4} \neq 0$$

$$\bar{2} + \bar{2} + \bar{2} = \bar{6} \neq 0$$

$$\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8} \neq 0$$

$$\rightarrow \text{ord}(\bar{2}) = 6$$

$$\bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{10} = \bar{0}$$

Ese $(U(\mathbb{Z}_{12}), \cdot, \bar{1})$ $M(\mathbb{Z}_{12}) = \{\bar{n} \mid \text{gcd}(n, 12) = 1\} = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

$$\text{ord}(\bar{5})?$$

Teorema di Eulero:

$$\varphi(12) = 4$$

$$\bar{5}^{\varphi(12)} = \bar{1} \quad \text{allora } \bar{5}^4 = \bar{1}$$

ma non so se $\varphi(12)$ è il più piccolo: lo verifichiamo

$$\begin{array}{l} \bar{5}^1 = \bar{5} \\ \bar{5}^2 = \bar{25} = \bar{2} \bar{5} + \bar{1} = \textcircled{1} \\ \text{ "0 in } \mathbb{Z}_{12} \end{array}$$

$$\text{ord}(\bar{5}) = 2$$

sviluppamente non
 > 4

Per (G, \star, λ) gruppo, $g \in G$.

1) Se $g^m = \lambda$ per un $m \in \mathbb{Z}_+$ allora $\text{ord}(g) \mid m$

2) Se G finito, allora $\text{ord}(g) \mid \#G$

'ordine di un elemento divide l'ordine del gruppo'

DIM 1) $g^m = \lambda \rightarrow \text{ord}(g) \mid m$

DIVISIONE EUCLIDEA $m = k \cdot \text{ord}(g) + r$ $k, r \in \mathbb{Z}, 0 \leq r < \text{ord}(g)$

TESI: $r = 0 \rightarrow$ avere un multiplo di $\text{ord}(g)$ (che è divisore di m)

$$\begin{aligned} \lambda &= g^m = g^{k \cdot \text{ord}(g) + r} = g^{\text{ord}(g)} * g^r \\ &= (g^{\text{ord}(g)})^k * g^r = \lambda^k * g^r = \lambda * g^r = g^r \end{aligned}$$

Quindi $\underbrace{g^r * g * \dots * g}_{r \text{ volte}} = \lambda \rightarrow r = 0$ perché $\text{ord}(g)$ è il più piccolo $n > 0$
t.c. $g^n = \lambda$

2) Consideriamo $H = \{\lambda, g, g^2, \dots, g^{\text{ord}(g)-1}\} \subseteq G$

H è un sottogruppo di G :

$$- g^s, g^t \in H \quad g^s * g^t = g^{s+t} \in H$$

L'AGGIUNGE $\Rightarrow H \mid G$

$$\#H = \text{ord}(g)$$

□

Corollario $n \in \mathbb{Z}_+, n \geq 2, x \in \mathbb{Z}$ t.c. $\bar{x} \in M(\mathbb{Z}_n)$. Allora $\text{ord}(\bar{x}) \mid \varphi(n)$

D1H $* M(\mathbb{Z}_n) = \varphi(n) \circ$

Esempio $(\mathbb{C}^*, \cdot, 1)$ gruppo $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ perde o non sarebbe invertibile rispetto a $*$.

$\text{ord}(i) = ?$

$i^4 = 1 \rightarrow \text{ord}(i) \mid 4$ per la prop precedente
 $i^2 = -1 \neq 1 \rightarrow \text{ord}(i) \neq 2$

$\rightarrow \text{ord}(i) = 4$

$\text{ord}(z) = \infty$

Gli unici numeri complessi con ordine finito sono le radici n -esime dell'unità

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} \quad n \in \mathbb{Z}$$

Oss (G, \star, λ) Esiste un solo elemento di ordine 1: λ

$$\text{ord}(g) = 1 \rightarrow g^1 = \lambda \quad (\text{ord}(\lambda) = 1 \text{ infatti basta } g^1 \text{ } (n=1 \in \mathbb{Z}_+ \text{ più piccolo}) \text{ per ottenere } \lambda)$$

Oss (M, \star, λ) monoidi (gruppo), $L_i \subseteq M \Rightarrow$ sottomonoidi (sottogruppo) $i \in J$

$$\rightarrow \bigcap_{i \in J} L_i \text{ sottomonoidi (sottogruppo)}$$

! l'unione di sottogruppi non è necessariamente un sottogruppo, es $10\mathbb{Z} \cup 3\mathbb{Z}$ non è un sottogruppo di \mathbb{Z} perché $3 \in A, 10 \in A$ ma $10 + 3 = 13 \notin A$

DEF (M, \star, λ) monoidi, $A \subseteq M$ sottoinsieme. Il sottomonoide generato da A è l'intersezione di tutti i sottomonoidi che contengono A .

Se $A = \{x\}$ allora il sottomonoide generato da A si dice ciclico e si denota con $\langle x \rangle = \{x^m \mid m \in \mathbb{N}\}$

il sottogruppo generato da A (nel caso M sia un gruppo)

$$\text{si denota } \langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$$

Se $M = \langle x \rangle$ per un qualche $x \in M$ allora M si dice ciclico.

Esempio $(\mathbb{N}, +, 0)$ monoidi ciclico generato da 1 $\mathbb{N} = \langle 1 \rangle$

(posso scrivere ogni $n \in \mathbb{N}$ come somma di 1: $n = \underbrace{1 + \dots + 1}_{n \text{ volte}}$)

$$\langle 3 \rangle \subseteq \mathbb{N} \text{ sottomonoidi ciclico} \quad \langle 3 \rangle = \{0, 3, 6, 9, 12, \dots\}$$

$$\times [3^0, 3^1, 3^2, \dots]$$

$$\langle 3 \rangle \subseteq N \quad \text{sottomonoide ciclico} \quad \langle 3 \rangle = \{ 0, 3, 6, 9, 12, \dots \}$$

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, \dots\}$$

sono multipli di 3

* N.B. $\underbrace{g^n}_{n \text{ volte}} = g + \dots + g$ qui + è la somma quindi:

3^n significa fare $3 + \dots + 3$ volte
zero = 0

$$3^1 = 3, \quad 3^2 = 3+3 = 6$$

Res ($\mathbb{Z}, +, 0$) grupos cíclicos generados de 1

7 letti; i sottogruppi di 2 sono delle forme n² per qualche n ∈ ℤ

Ese Non tutti i sottomonoidi di $(\mathbb{N}, +, \circ)$ sono ciclici!

$\mathbb{N} - \{-1\}$ sottomenzione gli \mathbb{N}

$$\begin{aligned} 0 &\in \mathbb{N} \setminus \{1\} \\ a, b &\in \mathbb{N} \setminus \{1\} \quad \text{se } a=0 \rightarrow a+b=b \in \mathbb{N} \setminus \{1\} \\ &\text{se } a \neq 0 \rightarrow a, b > 1 \rightarrow a+b > 1 \\ &\rightarrow a+b \in \mathbb{N} \setminus \{1\} \end{aligned}$$

$N \setminus \{1\}$ non è ordinato, per assurdo $N \setminus \{1\} = \langle v \rangle$ $v \in N \setminus \{1\}$, $v \neq 1$

L'insieme è generato da un solo elemento
 ("A non è un singolo "che genera l'intero insieme")

$N \cdot \{1\}$ è generato da 2 elementi

$$\mathbb{N} \cdot \{1\} = \langle 2, 3 \rangle = \{2a + 3b \mid a, b \in \mathbb{N}\}$$

unter
 \downarrow
 sohländische
 (no sgragletto)

Def $(M, +, \lambda)$, $(L, \triangleright, \eta)$ sono s.t. una funzione $f: M \rightarrow L$ è un omorfismo

di monoidi se:

$$1) \quad g(\lambda) = \eta$$

Se \mathbb{N} e L sono gruppi allora f si dice omotomia di gruppi.

Prop $f: (\mathbb{N}, +, \lambda) \rightarrow (L, \nabla, \eta)$ omom. di gruppi, $x \in \mathbb{N}$ allora

$$f(x^{-1}) = f(x)^{-1}$$

inverso in \mathbb{N} inverso in L

l'inverso di un elemento viene inviato nell'inverso (di f)

$$\begin{aligned} \text{Hom } (\mathbb{N}, \mathbb{N}) &= \{f: \mathbb{N} \rightarrow \mathbb{N} \\ &\text{omom. di gruppi}\} \\ (\text{Hom } (\mathbb{N}, \mathbb{N}), \circ, \bar{\circ}) &\text{ gruppo} \end{aligned}$$

Dm $x + x^{-1} = x^{-1} + x = \lambda$ per definizione di inverso

applico f $f(x + x^{-1}) = f(x^{-1} + x) = f(\lambda)$

Domande. $f(x) \nabla f(x^{-1}) = f(x^{-1}) \nabla f(x) = \eta \rightarrow f(x^{-1}) \in \text{l'inverso (in } L\text{)} \\ \text{di } f(x)$

cioè $(f(x))^{-1} = f(x^{-1})$ \square

Esempio $f: (\mathbb{N}, +) \rightarrow (\mathbb{N}, +)$ omomorfismo di monoidi? no perché $f(0) \neq 0$

$$x \mapsto x+2$$

Esempio $f: (\mathbb{N}, +) \rightarrow (\mathbb{N}, +)$ " " " ? si $f(0) = 0$

$$x \mapsto 2x$$

$$\begin{aligned} f(a+b) &= 2(a+b) = 2a + 2b \\ &= f(a) + f(b) \end{aligned}$$

Esempio $f: (\mathbb{N}, \cdot) \rightarrow (\mathbb{N}, \cdot)$ " " " ? no, $f(1) = 2 \neq 1$

$$x \mapsto 2x$$

el. neutro

Esempio $f: (\mathbb{Z}, +, 0) \rightarrow (\mathbb{Q}_{>0}, \cdot, 1)$ omom. di monoidi? si $f(0) = 2^0 = 1$

$$x \mapsto 2^x \quad f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \circ f(b)$$

scambia + con \cdot

Esempio $f: (\mathbb{R}_{>0}, \cdot, 1) \rightarrow (\mathbb{R}, +, 0)$ è omom. di gruppi? si

$$x \mapsto \log x$$

scommuta \cdot con $+$

Esempio $f: (\mathbb{C}, +, 0) \rightarrow (\mathbb{C}, +, 0)$ è omom. di gruppi? • $f(0) = 0$ per le reg. dei \mathbb{C}
 $z \mapsto \bar{z}$ si • $f(a+b) = \bar{a+b} = \bar{a} + \bar{b}$

Esempio $f: (\mathbb{C}, +, 0) \rightarrow (\mathbb{C}, +, 0)$ è canon. un gruppo.

$$z \mapsto \bar{z}$$

coniugato

se $f(a+b) = \bar{a+b} = \bar{a}+\bar{b}$

$$= f(a) + f(b) \quad \checkmark$$

Prop $(\mathbb{N}, +, \lambda)$ risponde, \sim rel. d'equivalenza compatibile con $+$. Allora

$$\pi: (\mathbb{N}, +, \lambda) \rightarrow (\mathbb{N}/\sim, [x], [\lambda]) \quad \pi(x) = [x]$$

è un omomorfismo di monoidi detto **PROIEZIONE SUL SUBSISTENTE**

\mathbb{N}/\sim è compatibile con $+$ se $a \sim c, b \sim d \rightarrow (a+b) \sim (c+d)$ \mathbb{N}/\sim è rispondere $[a] + [b] := [a+b]$	Condizione di compatibilità $f(a+b) = f(a) + f(b)$ f compatibile con $+$	in generale (\times funzioni):
--	---	--------------------------------------

Esempio $(\mathbb{Z}, +, 0)$, $n \in \mathbb{Z}$, $n \geq 2$ $x \sim y \iff x \equiv y \pmod{n}$

$$\pi: \mathbb{Z} \rightarrow \mathbb{Z}_{n2} = \mathbb{Z}_n \quad \text{è un omomorfismo di gruppi.}$$

$$x \mapsto [x]$$

Oss π è sempre suriettivo, e.g. data $L \in \mathbb{Z}/n$ classe, prendiamo $x \in L$
 abbiamo $[x] = L$ e quindi $\pi(x) = [x] = L$

Esempio Cerchiamo degli omomorfismi di gruppi $\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}$

$$\begin{array}{l} [x] \rightarrow x \text{ non è ben definita} \\ \text{per } x \\ [x+n] \rightarrow x+n \end{array}$$

$$\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}$$

funzione DEFINITA

$$[x] \rightarrow x \quad x = kn+r \quad 0 \leq r < n$$

è un omomorfismo di gruppi?

$$\varphi(0) = 0 \quad \checkmark$$

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{ad es. preso } n=3 \quad \varphi(\bar{1} + \bar{2}) = ? \quad \varphi(\bar{1}) + \varphi(\bar{2}) = 1+2=3$$

non è un omomorfismo di gruppi

$$\varphi(\bar{3}) = 0 \quad \underline{0 \neq 3 \in \mathbb{Z}}$$

per come abbiamo definito $n=3$

$$\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}$$

$$\bar{x} \rightarrow 0$$

e' detto ROTORIZZAZIONE NULO (e' di gruppo \checkmark)

e' l'unico
 possibile
 per $\mathbb{Z}_n \rightarrow \mathbb{Z}$

Sia $\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}$ orot. di gruppi $\varphi \neq 0$

$$\varphi(\bar{a}) = a \in \mathbb{Z} \quad \text{e } f \neq 0 \quad \text{perché } f \neq 0$$

$$\varphi(\bar{n}) = \varphi(\bar{a} + \dots + \bar{a}) = \varphi(\bar{a}) + \dots + \varphi(\bar{a}) = a + \dots + a = n \cdot a$$

||

$$\varphi(\bar{0}) = 0 \quad \rightarrow \quad 0 = n \cdot a \quad \text{ma } n \neq 0, a \neq 0 \quad \text{in } \mathbb{Z}$$

Prop $f: (\mathbb{N}, +_{\mathbb{N}}, \lambda_{\mathbb{N}}) \longrightarrow (L, +_L, \lambda_L)$ omomorfismo di monoidi (**gruppi**). Allora:

1) L'immagine $f(\mathbb{N}) = \text{Im } f$ è un sottomonoido (**sottogruppo**) di L .

2) La controimmagine $f^{-1}(\lambda_L)$ è un sottomonoido (**sottogruppo normale**)

Si denota con $\ker f := f^{-1}(\lambda)$ ed è detto **NUCLEO** di f (omomorfismo).

Prop Sia $(\mathbb{N}, +_{\mathbb{N}}, \lambda_{\mathbb{N}}), (L, +_L, \lambda_L), (P, +_P, \lambda_P)$ monoidi. Allora

1) $\text{Id}_{\mathbb{N}}: \mathbb{N} \rightarrow \mathbb{N}$ è otorrifisso di rendita

2) $f: \mathbb{N} \rightarrow L, g: L \rightarrow P$ omomorfismi. Allora $g \circ f: \mathbb{N} \rightarrow P$ è omomorfismo.

3) Se $f: \mathbb{N} \rightarrow L$ è un omomorfismo bigettivo, allora $f^{-1}: L \rightarrow \mathbb{N}$ è omomorfismo

↳ In questo caso f si dice **isotorfisso** di monoidi e \mathbb{N} e L si dicono **isotorfici**.
(denotato $\mathbb{N} \cong L$)

Oss 1), 2), 3) valgono anche per i **gruppi**

Def $f: \mathbb{N} \rightarrow L$ è un **isotorfisso** di monoidi (**gruppi**) se f è un omomorfismo di monoidi (**gruppi**) e f è BIGETTIVO. \mathbb{N} e L si dicono **isomorfi**: $\mathbb{N} \cong L$

Oss $\mathbb{N} \in L$ isomorfi $\iff \mathbb{N} \in L$ equipotenti
non vale

D.17 1) **Eserc.**

$$\mathbb{N} \xrightarrow{f} L \xrightarrow{g} P$$

$$2) (g \circ f)(\lambda_L) = g(f(\lambda_N)) = g(\lambda_L) = \lambda_P$$

$$x, y \in \mathbb{N} \quad (g \circ f)(x +_N y) = g(f(x +_N y)) = g(f(x) +_L f(y)) = g(f(x)) +_P g(f(y))$$

composizione di omom. è omom.

3) Sia $f: \mathbb{N} \rightarrow L$ bigettiva oram. Tesi: $f^{-1}: L \rightarrow \mathbb{N}$ omomorfismo

$$f^{-1}(\lambda_L) \text{ effettuato } f \quad f(g^{-1}(\lambda_L)) = \lambda_L \quad \boxed{\text{ma } f(\lambda_N) = \lambda_L, \text{ } f \text{ bigettiva}} \quad \Rightarrow \quad f^{-1}(\lambda_L) = \lambda_N$$

per rispettare
ci identità
dell'el. centro

$$\text{Prendiamo } a, b \in L \quad \underline{f^{-1}(a +_L b)} = f^{-1}(a) +_N f^{-1}(b)$$

$$\text{arit. diamo } f \quad f(f^{-1}(a +_L b)) = a +_L b$$

||

Prendiamo $a, b \in L$ $\underline{f^{-1}(a *_L b) = f^{-1}(a) *_R f^{-1}(b)}$

applichiamo f $f(\underline{f^{-1}(a *_L b)}) = a *_L b$
 $f(f^{-1}(a) *_R f^{-1}(b)) = \xrightarrow{\text{def. omom.}} f(f^{-1}(a) *_L f(f^{-1}(b))) = a *_L b$ || ↗

f BIETIVIA $\rightarrow f^{-1}(a *_L b) = f^{-1}(a) *_R f^{-1}(b)$ \square

(B) $U(\mathbb{Z}_6) = \{ \bar{x} \mid \text{ord}(x, 6) = 1 \} = \{ \bar{1}, \bar{5} \}$ $(U(\mathbb{Z}_6), \cdot, \bar{1})$ gruppo
 d. invertibili

•	$\bar{1}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$

\mathbb{Z}_{6+1}

* $U(\mathbb{Z}_6) = \mathbb{Z} = * \mathbb{Z}_2$

$(\mathbb{Z}_2, +, 0)$

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

$\varphi: \mathbb{Z}_2 \rightarrow U(\mathbb{Z}_6) \subseteq \mathbb{Z}_6$

$\bar{0} \mapsto \bar{1}$
 $\bar{1} \mapsto \bar{5}$

v.g. Che $\bar{1}$ in \mathbb{Z}_2
 è diverso da
 $\bar{1}$ in \mathbb{Z}_6

φ è isomorfismo di gruppi

• φ BIETIVA ($\star 1, *$)

• φ isomorfismo di gruppi $\varphi(\bar{a} + \bar{b}) = \varphi(\bar{a}) + \varphi(\bar{b})$ $\forall \bar{a}, \bar{b} \in \mathbb{Z}_2$

Bisogna farlo con tutti:

es. $\bar{0} = 0, \bar{1} = 1$

$$\begin{aligned} \varphi(\bar{0} + \bar{1}) &= \varphi(\bar{0}) + \varphi(\bar{1}) \\ \bar{1} &= \varphi(\bar{1}) \end{aligned}$$

$\varphi(\bar{0}) + \varphi(\bar{1})$

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

Lemma $\varphi: G \rightarrow H$ isomorfismo di gruppi, $g \in G$ allora $\text{ord}_G(g) = \text{ord}_H(\varphi(g))$.

D $\text{dim} \text{ord}_G(g) \rightarrow g^n = \lambda_G$

$\varphi(g)^n = \varphi(g) *_H \dots *_H \varphi(g) = \varphi(g *_G \dots *_G g) = \varphi(g^n) = \varphi(\lambda_G) = \lambda_H$

$\rightarrow \text{ord}_H \varphi(g) \leq n$

e non può essere più piccolo:

P. A. $\text{ord}_H \varphi(g) = m < n$

In particolare $\varphi(g)^m = \lambda_H$

$\varphi(g^m)$

applico φ^{-1} $\varphi^{-1}(\varphi(g^m)) = \varphi^{-1}(\lambda_H) = \lambda_G$

δ^m

$g^m = \lambda_G \rightarrow \text{ord}_G(g) \leq m < n = \text{ord}_G(g)$

ma $\text{ord}_G(g) < \text{ord}_G(g)$

↗ \square

$$\text{ma } \text{ord}_G(y) < \text{ord}_G(g) \quad \leftarrow \quad \square$$

(es) $(\mathbb{Z}_4, +, \bar{0})$, $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$ gruppi abeliani

* $\mathbb{Z}_4 = \{0, 1, 2, 3\} = \mathbb{Z} \cdot 2$ * $(\mathbb{Z}_2 \times \mathbb{Z}_2)$

ma non sono isomorfi.

\mathbb{Z}_4	ord
$\bar{0}$	1
$\bar{1}$	4 $\bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}$
$\bar{2}$	2
$\bar{3}$	4 $\bar{3} + \bar{3} + \bar{3} + \bar{3} = \bar{0}$

$\mathbb{Z}_2 \times \mathbb{Z}_2$	ord
$(\bar{0}, \bar{0})$	1
$(\bar{1}, \bar{0})$	2
$(\bar{0}, \bar{1})$	2
$(\bar{1}, \bar{1})$	2

$$(\bar{1}, \bar{0}) + (\bar{1}, \bar{0}) = (\bar{0}, \bar{0})$$

no ord 4

$\exists \rho: \mathbb{Z}_4 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ isomorfismo perche' $\bar{1}$ ha ordine 4 in \mathbb{Z}_4 ma non ci sono elementi di ordine 4 in $\mathbb{Z}_2 \times \mathbb{Z}_2$.

con identità:

Def A è un anello \Leftrightarrow se è un insieme dotato di due operazioni binarie $+, \cdot : A \times A \rightarrow A$ tali che:

1) $(A, +)$ gruppo abeliano (sono con commutatività, assoc. ed \exists inverso)

2) \cdot associativo $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in A$

3) Distributiva di $+$ su \cdot $(a+b) \cdot c = a \cdot c + b \cdot c$

(non è detto che sia $a \cdot (b \cdot c) = a \cdot b + a \cdot c$
commutativo, né che abbia inverso)

Def Un anello si dice commutativo se \cdot è commutativo

Un anello si dice con identità se $\exists e \in A$ t.c. $e \cdot a = a \cdot e = a \quad \forall a \in A$

Ese $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono anelli

\mathbb{Z}_n sono anelli

Se \cdot è commutativo ($a \cdot b = b \cdot a \quad \forall a, b \in A$) allora A si dice ANELLO COMMUTATIVO

Se \cdot è commutativo e $\forall a \in A \setminus \{0\} \exists b \in A$ t.c. $b \cdot a = a \cdot b = 1$ allora A si dice

elemento inverso di a

o anche

$(\mathbb{F}, +, \cdot, 0, 1)$ campo

o rispetto a \cdot

anello

CORPO.

$$0 = 0 + 0 \cdot i$$

$$1 = 1 + 0 \cdot i$$

contatti già al $\neq 0$

ha un inverso

$(\mathbb{R}, +, \cdot, 0, 1)$ campo

$(\mathbb{Q}, +, \cdot, 0, 1)$ campo

$(\mathbb{R}, +, \cdot, 0, 1)$ anello commutativo con identità, non un campo (es. $\sqrt{-1}$ non ha inverso)

$(\mathbb{Z}_n, +, \cdot, 0, 1)$ anello commutativo con identità, è campo? no

Prop \mathbb{Z}_n è un campo $\Leftrightarrow n$ è primo

Dim $\bar{x} \in \mathbb{Z}_n$ è invertibile $\Leftrightarrow \text{GCD}(\bar{x}, n) = 1$

$\frac{n}{d}$

Se $n=p$ primo allora $\bar{x} \neq \bar{0}$ $\text{GCD}(\bar{x}, p) = 1$ $0 < x < p$

Se $n = m_1 \cdot m_2$ $m_1, m_2 < n$ allora $\text{GCD}(n, m_1) = m_1 > 1$ quindi m_1 non è invertibile

D

$$E \cup (\mathbb{Z}_n) \ni x, y \quad x+y \in \cup (\mathbb{Z}_n)$$

$$U(\mathbb{Z}_6) = \{1, 5\} \quad 1+1 = 2 \notin U(\mathbb{Z}_6) \text{ non est un annel}$$

così non puo' essere immesso rispetto a ciò:

$$0 \cdot a = a \cdot 0 = 0 \quad \forall a \quad (\text{even 1})$$

oggi nego l'inverso

infetti

$$\underline{\underline{0 \cdot \alpha = (0+0) \cdot \alpha}} = \underline{\underline{(0 \cdot \alpha) + (0 \cdot \alpha)}} \rightarrow \underline{\underline{- (0 \cdot \alpha) + (0 \cdot \alpha)}} = \underline{\underline{-(0 \cdot \alpha)}} + \underline{\underline{(0 \cdot \alpha) + (0 \cdot \alpha)}} \\ \text{el neutro} \\ \text{delle somme}$$