Monoidi e gruppi

mercoledì 3 gennaio 2024 14:48

# → MONOIDI E GRUPPI

1) def: Un semigruppo è una coppia $(M,*)$, $M$ è un insieme, $*: M\times M \to M$ operazione associativa su $M$

Associativa: $(a*b)*c = a*(b*c)$

oss: $*$ non è necessariamente commutativa, se lo è diciamo che il semigruppo è commutativo o abeliano

2) def: Un monoide è una tripla $(M,*,\lambda)$ dove $M$ insieme, $*$ operazione associativa su $M$, e $\lambda \in M$ elemento neutro per $*$

elemento neutro: $\lambda * a = a * \lambda = a$

lemma: l'elemento neutro di un monoide è unico

dim: $\mu \in M$ elemento neutro $(\mu * a = a * \mu = a)$, $\mu = \lambda * \mu = \lambda$ $\square$

es:

1) $(\mathbb{N}, +, 0)$ monoide commutativo
2) $(\mathbb{N}, \cdot, 1)$ monoide commutativo
3) $(\mathbb{N}, \cdot, 1)$ monoide commutativo
4) $(\mathbb{Z}, +, 0)$ $(\mathbb{Q}, +, 0)$ $(\mathbb{R}, +, 0)$ $(\mathbb{C}, +, 0)$ monoidi commutativo
   $(\mathbb{Z}, \cdot, 1)$ $(\mathbb{Q}, \cdot, 1)$ $(\mathbb{R}, \cdot, 1)$ $(\mathbb{C}, \cdot, 1)$
5) $(\mathbb{R} \setminus \mathbb{Q}, +)$ semigruppo? no
   numeri irrazionali
   $+: \mathbb{R}\setminus\mathbb{Q} \times \mathbb{R}\setminus\mathbb{Q} \to \mathbb{R}\setminus\mathbb{Q}$
   operazione associativa? no
   $\sqrt{2} + (-\sqrt{2}) = 0 \notin \mathbb{R}\setminus\mathbb{Q}$
6) $(\mathbb{Z}_n, +, \overline{0})$ monoidi commutativi
   $(\mathbb{Z}_n, \cdot, \overline{1})$
7) $X$ insieme, $X \neq 0$ $X^X = \{f: X \to X\}$
   $(X^X, \circ, Id_X)$ monoide non commutativo
   $f \circ g \neq g \circ f$ in generale
8) $X$ insieme, $X \neq 0$
   $(\mathcal{P}(X), \cup, \emptyset)$ monoide commutativo
   $A \in \mathcal{P}(X)$ $A \cup \emptyset = A$
   $\emptyset \cup A$
   $(\mathcal{P}(X), \cap, X)$ $A \cap X = A$
   $A \subseteq X$

def: $(M,*,\lambda)$ monoide, $a \in M$

1) $a$ è invertibile a sinistra se $\exists b \in M$ t.c. $b*a = \lambda$, $b$ si dice inverso sinistro di $a$
2) $a$ è invertibile a destra se $\exists c \in M$ t.c. $a*c = \lambda$, $c$ si dice inverso destro di $a$
3) $a$ è invertibile se $\exists d \in M$ t.c. $a*d = d*a = \lambda$, $d$ si dice inverso di $a$ e si denota con $a^{-1}$

prop:

1) $\lambda$ è inverso sx e dx di se stesso
2) dato $a \in M$, se $b \in M$ è inverso sx di $a$ e $c \in M$ è inverso dx di $a$, allora $b=c$
   In particolare, l'inverso è unico
3) se $(M,*,\lambda)$ è commutativo, allora un elemento ha inverso dx $\leftrightarrow$ ha inverso sx

dim:

1) $\lambda * \lambda = \lambda$
3) se $*$ è commutativa, $a \in M$
   $a*b = b*a = \lambda$
2) $b$ è inverso sinistro di $a \to b*a = \lambda$
   $c$ è inverso destro di $a \to a*c = \lambda$

2) $b$ è inverso sinistro di $a \to b*a=\lambda$

$c$ è inverso destro di $a \to a*c=\lambda$

$b = b*\lambda = b*(a*c) \overset{ASS}{=} (b*a)*c = \lambda*c = c \to b=c$ $\square$

es:

- $(\mathbb{Z},+,0)$ ogni elemento ha inverso
  $\mathbb{Q},\mathbb{R},\mathbb{C}$
- $(\mathbb{N},+,0)$ solo 0 ha inverso
- $(\mathbb{Z},\cdot,1)$ $\{-1,1\}$ sono gli unici elementi invertibili
- $(\mathbb{Q},\cdot,1)$ tutti invertibili tranne 0
  $\mathbb{R},\mathbb{C}$
- $(\mathbb{Z}_n,+,\bar{0})$ tutti invertibili risp a +
- $(\mathbb{Z}_n,\cdot,\bar{1})$ $\bar{x}$ è invertibile $\leftrightarrow MCD(x,n)=1$
  $U(\mathbb{Z}_n)=\{\bar{x}\in\mathbb{Z}_n \mid \bar{x}$ è invertibile$\}$
- $X$ insieme, $X\neq\emptyset$ $(X^X,\circ,Id)$ invertibili?
  $f\in X^X$ $f: X\to X$
  è invertibile $\exists g: X\to X$ $g\circ f = f\circ g = Id$
  $f$ invertibile $\leftrightarrow f$ bigettiva
  $f$ invertibile a sx $\leftrightarrow f$ iniettiva
  $f$ invertibile a dx $\leftrightarrow f$ suriettiva

def: Un gruppo è un monoide $(M,*,\lambda)$ t.c. ogni elemento è invertibile
Se $*$ è commutativa diciamo che il gruppo è commutativo o abeliano
La cardinalità di $M$ si chiama ordine del gruppo

es:

- $(\mathbb{Z},+,0)$ gruppo
- $(\mathbb{Q},+,0),(\mathbb{R},+,0),(\mathbb{C},+,0)$ gruppo comm
- $(\mathbb{N},+,0)$ non è un gruppo
- $(\mathbb{Z},\cdot,1)$ non è un gruppo
- $(\mathbb{Q},\cdot,1)$ non è un gruppo (0 non invertibile)
- $(\mathbb{Q}^*,\cdot,1)$ gruppo
  $=\mathbb{Q}\setminus\{0\}$
- $(\mathbb{R}^*,\cdot,1),(\mathbb{C}^*,\cdot,1)$ gruppi
- $(\mathbb{Z}_n,+,\bar{0})$ gruppo
- $(\mathbb{Z}_n,\cdot,\bar{1})$ non è un gruppo, $\bar{0}$ non è invertibile
- $(U(\mathbb{Z}_n),\cdot,\bar{1})$ gruppo
  gli elementi invertibili di $\mathbb{Z}_n$ $|U(\mathbb{Z}_n)|=\varphi(n)$
- $(X^X,\circ,Id)$ non è un gruppo

se consideriamo:

$(\{f: X\to X$ bigettiva$\},\circ,Id)$ gruppo

se $X=\{1,\dots,n\}$

$S_n=\{f: X\to X$ bigettiva$\}$ gruppo delle permutazioni di $n$ elementi

- $S_n$ non è commutativo $(n\geq 3)$
- $|S_n| = n\cdot(n-1)\dots 2\cdot 1 = n!$

vediamo nel dettaglio $S_2=\{Id, f\}$

$Id: \{1,2\}\to\{1,2\}$ $\quad$ $f: \{1,2\}\to\{1,2\}$

$1\mapsto 1$ $\quad$ $1\mapsto 2$

$2\mapsto 2$ $\quad$ $2\mapsto 1$

$(S_2,\circ,Id)$ gruppo commutativo

$S_3=\{f:\{1,2,3\}\to\{1,2,3\}$ bigettive$\}$

$|S_3| = 3! = 6 \quad S_3 = \{Id, \varnothing, \psi, \psi\circ\varnothing, \varnothing\circ\psi, \psi^2\}$

$\varnothing: X \to X$
$1 \mapsto 2$
$2 \mapsto 1$
$3 \mapsto 3$
trasposizione $(1,2)$

$\psi: X \to X$
$1 \mapsto 2$
$2 \mapsto 3$
$3 \mapsto 1$
3-ciclo $(1,2,3)$

$\varnothing\circ\varnothing = Id$

$\psi^2 = \psi\circ\psi: X \to X$
$1 \mapsto 3$
$2 \mapsto 1$
$3 \mapsto 2$

$\psi\circ\varnothing: X \to X$
$1 \mapsto 3$
$2 \mapsto 2$
$3 \mapsto 1$

$\varnothing\circ\psi: X \to X$
$1 \mapsto 1$
$2 \mapsto 3$
$3 \mapsto 2$

$\psi\circ\varnothing \neq \varnothing\psi \to S_3$ non comm

def: $(M, *, \lambda)$ monoide
$g \in M,\ n \in M^*$ $\quad g^n = \underbrace{g * \dots * g}_{n \text{ volte}} \quad g^0 = \lambda$

$g$ invertibile $\quad g^{-1}$ inverso di $g \quad g^{-1} * g = g * g^{-1} = \lambda \quad g^n = \underbrace{(g^{-1}) * \dots * (g^{-1})}_{n \text{ volte}}$

def: $(M_1, *_1, \lambda_1), (M_2, *_2, \lambda_2)$ monoidi
$(M_1 \times M_2, *_1 \times *_2, (\lambda_1, \lambda_2))$ prodotto diretto di $M_1$ e $M_2$

es:
- $(N, +, 0), (N, +, 0)$
  $(2,3), (0,6) \in N \times N \quad (2,3)+(0,6) = (2+0, 3+6) = (2,9)$
  l'elemento neutro è $(0,0)$
- $(\mathbb{Z}_3, +, \bar{0}), (\mathbb{Z}_4, +, \bar{0})$ $\quad \bar{0}$ per $\mathbb{Z}_3$, $[0]$ per $\mathbb{Z}_4$
  $\mathbb{Z}_3 + \mathbb{Z}_4$ monoide prodotto $\quad$ elemento neutro $(\bar{0}, [0])$
  $(\bar{2}, [3]), (\bar{1}, [2]) = (\bar{2} + \bar{1}, [2] + [2]) = (\bar{3}, [4]) = (\bar{0}, [0])$

# SOTTOGRUPPI

$(G, *, \lambda)$ gruppo
Un sottoinsieme $H \subseteq G$ è un sottogruppo se valgono tre condizioni:
1) $\lambda \in H$
2) $a, b \in H \to a * b \in H$
3) $a \in H \to a^{-1} \in H$

es:
- $(\mathbb{R}, +, 0)$ gruppo
- $(\mathbb{Z}, +, 0)$ sottogruppo
- $(\mathbb{Q}, +, 0)$ sottogruppo
- $(\mathbb{N}, +, 0)$ no sottogruppo
- $\mathbb{R} \setminus \mathbb{Q}$ no sottogruppo

- $(\mathbb{R}^*, \cdot, 1)$ gruppo
- $\mathbb{Q}^* \subseteq \mathbb{R}^*$ sottogruppo
- $\mathbb{R} \setminus \mathbb{Q} \subseteq \mathbb{R}^*$ no sottogruppo, $1 \notin \mathbb{R} \setminus \mathbb{Q}$
- $\mathbb{Z}^* \subseteq \mathbb{R}^*$ no sottogruppo
- $\{1, -1\} \subseteq \mathbb{R}^*$ sottogruppo
- $\{1\} \in \mathbb{R}^*$ sottogruppo

oss: In generale, $(G, *, \lambda)$ gruppo, $\{\lambda\} \subseteq G$ sottogruppo banale

def: Dato $n \in \mathbb{Z}_+$ $(\mathbb{Z} > 0)$
$U_n = \{x \in \mathbb{C} \mid x^n = 1\}$ radici n-esime dell'unità
$\# U_n = n$ $\quad U_1 = \{1\} \quad U_2 = \{1, -1\} \quad U_3 = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\} \quad U_4 = \{1, -1, i, -i\}$
Un sottogruppo di $(\mathbb{C}^*, \cdot, 1)$
1) $1 \in U_n$ perchè $1^n = 1$
2) $x, y \in U_n \to x^n = 1,\ y^n = 1 \to (x \cdot y)^n = x^n \cdot y^n = 1$
3) $x \in U_n \to x^n = 1 \to (x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$

es:
- $(\mathbb{Z}, +, 0)$ gruppo

3) $x \in U_n \to x = 1 \to (x\ ) = (x\ ) = 1 = 1$

es:
- $(\mathbb{Z}, +, 0)$ gruppo
  - {numeri pari} $\subseteq \mathbb{Z}$ è un sottogruppo
  - {numeri dispari} $\subseteq \mathbb{Z}$ non è un sottogruppo
  - $n\mathbb{Z} = \{m \in \mathbb{Z} \mid m = n \cdot k, k \in \mathbb{Z}\}$ è un sottogruppo
    ↳ tutti i sottogruppi di $(\mathbb{Z}, +, 0)$ sono di questa forma
- $S_3 = \{Id, \phi, \psi, \phi \circ \psi, \psi \circ \phi, \psi^2\}$

  $\phi: X \to X$    $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 3$

  $\psi: X \to X$    $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$

  Sottogruppi di $S_3$?

  $T = \{Id, \phi, \psi\}$ no $\phi, \psi \in T$ ma $\phi \circ \psi \notin T$

  $R = \{Id, \phi\}$ si

  $A = \{Id, \psi\}$ no

**teorema di Lagrange:** dato un gruppo finito $G$, $H$ sottogruppo $\to \#H \mid \#G$

Sia $G$ un gruppo finito e sia $H$ un suo sottogruppo. Allora $\#H \mid \#G$, cioè la cardinalità di $H$ è un divisore della cardinalità di $G$

# SOTTOGRUPPI CICLICI

$(G, *, \lambda)$ gruppo    $H \subseteq G$ sottogruppo    se:

1) $\lambda \in H$
2) $a, b \in H \to a * b \in H$
3) $a \in H \to a^{-1} \in H$

$g \in G$    $g * g = g^2$    $g * g * g = g^3$    $g^1 = g$    $g^0 = \lambda, g^{-1}, g^{-2} = g^{-1} * g^{-1}$

$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\} \subseteq G$

sottogruppo ciclico generato da $g$

è un sottogruppo:

1) $\lambda \in \langle g \rangle$ perchè $g^0 = \lambda$
2) $g^n, g^m \in \langle g \rangle \to \underbrace{g^n * g^m}_{= g^{n+m}} \in \langle g \rangle$ ?
3) $g^n \in \langle g \rangle \to g^{-n} \in \langle g \rangle$

   $g^{-n}$ è l'inverso di $g^{-n}$ perchè $g^{-n} * g^n = g^{-n*n} = g^0 = \lambda$

def: $G$ gruppo è detto ciclico se $\exists g \in G$ t.c. $G = \langle g \rangle$

in tal caso $g$ si dice generatore di $G$

oss: $G$ è ciclico $\to$ $G$ è commutativo

$g^n, g^m$    $g^n * g^m = g^{n+m} = g^m * g^n = g^{m+n}$

es: $(\mathbb{Z}, +, 0)$ gruppo ciclico

1 è generatore perchè dato $n \in \mathbb{Z}$

$n = \underbrace{1 + \dots + 1}_{n \text{ volte}}$ se $n > 0$, $n = \underbrace{(-1) + \dots + (-1)}_{-n \text{ volte}}$ se $n$ negativo

$-1$ è l'inverso di $1$ rispetto al $+$

$\langle 2 \rangle = \{2, 2+2, 2+2+2, \dots, -2, -2-2, \dots\} = \{\text{numeri pari}\} = 2\mathbb{Z} \subsetneq \mathbb{Z}$

$\langle k \rangle = k\mathbb{Z} = \{\text{multipli di } k\}$

es: $(\mathbb{Z}_n, +, \bar{0})$ ciclico generato da classe di $\bar{1}$

$(\mathbb{Z}_6, +, \bar{0})$ ciclico

generatori: $\bar{1}, \overline{-1} = \bar{5}$

$\langle \bar{2} \rangle = \{\bar{2}, \underbrace{\bar{2} + \bar{2}}_{\bar{4}}, \underbrace{\bar{2} + \bar{2} + \bar{2}}_{\bar{6} = \bar{0}}\} = \underbrace{\{\bar{0}, \bar{2}, \bar{4}\}}_{\text{sottogruppo}}$

generatori: $\bar{1}, -\bar{1} = \bar{5}$

$<\bar{2}> = \{\bar{2}, \underbrace{\bar{2}+\bar{2}}_{\bar{4}}, \underbrace{\bar{2}+\bar{2}+\bar{2}}_{\bar{6}=\bar{0}}\} = \{\bar{0},\bar{2},\bar{4}\}$ sottogruppo

$<\bar{3}> = \{\bar{3}, \underbrace{\bar{3}+\bar{3}}_{\bar{0}}\} = \{\bar{0},\bar{3}\}$ sottogruppo

$(\mathbb{Z}_5, +, \bar{0})$

generatori: $\bar{1}, -\bar{1} = \bar{4}, \bar{2}, \bar{3}$

$\bar{2} = \{\bar{2}, \underbrace{\bar{2}+\bar{2}}_{\bar{4}}, \underbrace{\bar{2}+\bar{2}+\bar{2}}_{\bar{6}=\bar{1}}, \underbrace{\bar{2}+\bar{2}+\bar{2}+\bar{2}}_{\bar{8}=\bar{3}}, \bar{0}\} = \mathbb{Z}_3$

In generale, $\bar{x} \in \mathbb{Z}_n$ è generatore di $\mathbb{Z}_n \leftrightarrow MCD(x,n)=1$

**es:** $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0},\bar{0}))$ gruppo

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}$ è ciclico

$<(\bar{1},\bar{0})> = \{(\bar{1},\bar{0}), \underbrace{(\bar{1},\bar{1})+(\bar{1},\bar{0})}_{(\bar{2},\bar{0})=(\bar{0},\bar{0})}\} = \{(\bar{1},\bar{0}),(\bar{0},\bar{0})\}$

$<(\bar{0},\bar{1})> = \{(\bar{0},\bar{1}),(\bar{0},\bar{0})\}$ sottogruppo di 2 elementi

$<(\bar{1},\bar{1})> = \{(\bar{1},\bar{1}), \underbrace{(\bar{1},\bar{1})+(\bar{1},\bar{1})}_{(\bar{0},\bar{0})}\} = \{(\bar{0},\bar{0}),(\bar{1},\bar{1})\}$ sottogruppo di 2 elementi

$\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico

**def:** $(G, *, \lambda)$ gruppo, $g \in G$. L'ordine o periodo di $g$ è il più piccolo intero $n>0$ (se esiste) t.c. $g^n = \underbrace{g * \dots * g}_{n \text{ volte}} = \lambda$

scriviamo $ord_G\ g = n$

Se tale $n$ non esiste diciamo che l'ordine di $g$ è infinito e $ord_G\ g = \infty$

oss: $ord(\lambda) = 1$

**es:**
1) $(\mathbb{Z}, +, 0)$ $ord(1)=\infty$ $ord(0)=1$ $ord(2)=\infty$ $ord(-2)=\infty$
2) $(\mathbb{C}^*, \cdot, 1)$ $ord(1)=1$ $ord(2)=\infty$ $ord(i)=4$ $ord(-1)=2$

le radici n-esime dell'unità $U_n$ sono gli unici elementi di ordine finito

$U_n = \{x \in \mathbb{C} \mid x^n = 1\}$

$U_4 = \{\underset{1}{1}, \underset{2}{-1}, \underset{4}{i}, \underset{4}{-i}\}$ ← ordine

prop: $(G, *, \lambda)$ gruppo
1) $g \in G$ se $g^m = \lambda$ per un qualche $m \in \mathbb{Z}_+$ allora $ord\ g \mid m$
2) $G$ finito allora $ord\ g \mid \#G$
$\forall g \in G$ "ordine di un elemento divide l'ordine del gruppo"
3) $G$ finito, $g \in G$ allora $G = <g> \leftrightarrow ord\ g = |G|$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{\underset{1}{(\bar{0},\bar{0})}, \underset{2}{(\bar{1},\bar{0})}, \underset{2}{(\bar{0},\bar{1})}, \underset{2}{(\bar{1},\bar{1})}\}$ ← ordine

$(\mathbb{Z}_{12}, +, \bar{0})$ $ord(\bar{3})=4$

$\bar{3} \neq \bar{0}$, $\bar{3}+\bar{3} = \bar{6} \neq \bar{0}$ $\bar{3}+\bar{3}+\bar{3} = \bar{9} \neq \bar{0}$ $\bar{3}+\bar{3}+\bar{3}+\bar{3} = \overline{12} = \bar{0}$

$(U(\mathbb{Z}_n), \cdot, \bar{1})$ $\#U(\mathbb{Z}_n) = \varphi(n)$ ciclico $U(\mathbb{Z}_n) = \{\underset{1}{\bar{1}}, \underset{4}{\bar{2}}, \underset{4}{\bar{3}}, \underset{2}{\bar{4}}\}$ ← ordine

$\begin{cases} \bar{2} \cdot \bar{2} = \bar{4} \neq 1 \\ \bar{2}^4 = \bar{2}^{\varphi(5)} \end{cases}$ $\bar{2} \cdot \bar{2} \cdot \bar{2} = \bar{8} = \bar{3} \neq 1$ $\bar{2} \cdot \bar{2} \cdot \bar{2} \cdot \bar{2} = \overline{16} = \bar{1}$

$\begin{cases} \bar{3} \cdot \bar{3} = \bar{9} = \bar{4} \neq \bar{1} \\ \bar{3} \cdot \bar{3} \cdot \bar{3} \cdot \bar{3} = \overline{81} = \bar{1} \end{cases}$ $ord(\bar{3})=4$ $\underbrace{\bar{4} \cdot \bar{4}}_{(-\bar{1})(-\bar{1})=\bar{1}} = \overline{16} = 1 \rightarrow ord(\bar{4}) = 2$ $\bar{4}^{\varphi(5)} = \bar{1}$, $\bar{4}^4 = 1$

$(U(\mathbb{Z}_8), \cdot, \bar{1})$ $\varphi(8)=4$ $U(\mathbb{Z}_8) = \{\underset{1}{\bar{1}}, \underset{2}{\bar{3}}, \underset{2}{\bar{5}}, \underset{2}{\bar{7}}\}$ ← ordine

$\bar{7} = -\bar{1}$ $\bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$ $ord(\bar{3})=2$

$(-\bar{1})^2 = \bar{1}$ $\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$ $ord(\bar{5})=2$

# OMOMORFISMI DI GRUPPI

$(G_1, *_1, \lambda_1), (G_2, *_2, \lambda_2)$ gruppi

$\varphi: G_1 \rightarrow G_2$ è un omomorfismo di gruppi se soddisfa 2 condizioni:
1) $\varphi(\lambda_1) = \lambda_2$
2) $\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$ $\forall a, b \in G_1$

$\varphi: G_1 \to G_2$ è un omomorfismo di gruppi se soddisfa 2 condizioni:

1) $\varphi(\lambda_1) = \lambda_2$
2) $\varphi(g *_1 h) = \varphi(g) *_2 \varphi(h) \quad \forall g, h \in G_1$

Se $\varphi$ è bigettivo si dice isomorfismo di gruppi e $G_1$ e $G_2$ si dicono isomorfi

lemma: $\varphi\, G_1 \to G_2$ omomorfismo di gruppi, $g \in G_1$ allora: $\varphi(g^{-1}) = (\varphi(g))^{-1}$

es: $(\mathbb{Z}, +, 0) \quad \varphi: \mathbb{Z} \to \mathbb{Z} \quad \varphi(x) = 2x$

omomorfismo di gruppi

$\varphi(0) = 0$ ✓

$\forall m, n \in \mathbb{Z} \quad \varphi(m+n) = \varphi(m) + \varphi(n) \to 2(m+n) = 2m + 2n \to 2(m+n) = 2(m+n)$ ✓

- non è isomorfa perchè non è bigettiva perchè non è suriettiva
- i due gruppi però sono isomorfi perchè esiste $f$ bigettiva $f = Id: \mathbb{Z} \to \mathbb{Z}$

es: $(\mathbb{Z}, +, 0)$

$f: \mathbb{Z} - \mathbb{Z}$

$x \to x+2$

1) $f(0) = 0 + 2 = 2 \neq 0$ ✗ no omomorfismo di gruppi

es: $(\mathbb{Z}, +, 0), (\mathbb{Q}^*, \cdot, 1)$

$f: \mathbb{Z} \to \mathbb{Q}$, $x \mapsto 2^x$

1) $f(0) = 2^0 = 1$ ✓

2) $\forall m, n \in \mathbb{Z} \quad f(m+n) = f(m) \cdot f(n) \to 2^{m+n} = 2^m \cdot 2^n \to 2^{m+n} = 2^{m+n}$ ✓

omomorfismo di gruppi

es: $(\mathbb{Z}, +, 0) \quad (\mathbb{Z}_n, +, \bar{0})$

$f: \mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto \bar{x}$

1) $f(0) = \bar{0}$ ✓

2) $f(x+y) = f(x) + f(y) \to \overline{x+y} = \bar{x} + \bar{y} \to \overline{x+y} = \overline{x+y}$ ✓

omomorfismo di gruppi

es: $f: \mathbb{Z}_n \to \mathbb{Z}$, $\bar{x} \mapsto f(\bar{x})$

supponiamo che $f_n$ sia un omomorfismo

$\bar{1} \in \mathbb{Z}_n \to f(\bar{1}) \in \mathbb{Z}$

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

$f(\bar{1} + \bar{1}) = f(\bar{2}) = f(\bar{1}) + f(\bar{1})$

$\underbrace{\bar{1} + \bar{1} + \ldots + \bar{1}}_{n \text{ volte}} = \bar{n} = \bar{0}$

$f(\bar{1}) + \ldots + f(\bar{1}) = f(\bar{0}) = 0 = n f(\bar{1})$

proprietà: $\varphi: G_1 \to G_2$ omomorfismo di gruppi

1) l'immagine di $\varphi$ è un sottogruppo di $G_2$

$\varphi(G_1) \leq G_2$

2) $\varphi^{-1}(\lambda_2)$ controimmagine dell'elemento neutro è un sottogruppo, si chiama nucleo di $\varphi$

3) $\psi: G_2 \to G_3$ omomorfismo di gruppi, allora $\psi \circ \varphi$ è un omomorfismo di gruppi

es: $\varphi: \mathbb{Z} \to \mathbb{Z}$, $x \to 2x$ $\quad Im\ \varphi = 2\mathbb{Z} = \{pari\}$ sottogruppo di $\mathbb{Z}$

$Ker\ \varphi = \varphi^{-1}(0) = \{0\}$ sottogruppo di $\mathbb{Z}$

$\varphi: \mathbb{Z}_6 \to \mathbb{Z}_6$, $\bar{x} \to \bar{2} \cdot \bar{x}$ $\quad$ omomorfismo di gruppo

$Im\ \varphi = \{\bar{0}, \bar{2}, \bar{4}\} \quad Ker\ \varphi = \{\bar{0}, \bar{3}\}$

$\varphi(\bar{0}) = \bar{0}$
$\varphi(\bar{1}) = \bar{2}$
$\varphi(\bar{2}) = \bar{4}$
$\varphi(\bar{3}) = \bar{0}$

$\varphi(\bar{0}) = \bar{0}$
$\varphi(\bar{1}) = \bar{2}$
$\varphi(\bar{2}) = \bar{4}$
$\varphi(\bar{3}) = \bar{0}$
$\varphi(\bar{4}) = \bar{2}$
$\varphi(\bar{5}) = \bar{4}$

lemma: $\varphi: G_1 \to G_2$ isomorfismo di gruppo

$\forall g \in G_1 \quad ord(\underbrace{\varphi(g)}_{\text{ORDINE IN } G_2}) = \underbrace{ord(g)}_{\text{ORDINE IN } G_1}$

l'isomorfismo preserva l'ordine degli elementi

es: $\underbrace{\mathbb{Z}_4}_{\bar{1} \text{ ORDINE } 4}$ e $\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2}_{\text{non c'è nessun elemento di ordine 4}}$ isomorfi

$(\mathbb{Z}, +, 0)$ e $(\mathbb{Q}, +, 0)$ non sono isomorfi

$U(\mathbb{Z}_5) \to$ ordine 4

ha un elemento di ordine 4: $\bar{2}$

è isomorfo a $\mathbb{Z}_4$?

$\varphi: \mathbb{Z}_4 \to U(\mathbb{Z}_5)$ $\quad \bar{1}+\bar{1}+\bar{1} = \bar{3} \to \bar{3} = \bar{8} = \bar{2}\cdot\bar{2}\cdot\bar{2}$

$\bar{0} \to \bar{1}$

$\bar{1} \to \bar{2}$ $\quad \bar{1}+\bar{1} = \bar{2} \to \bar{4} = \bar{2}\cdot\bar{2}$

$U(\mathbb{Z}_8)$ 4 elementi, nessuno di ordine 4 $\to U(\mathbb{Z}_8)$ non è isomorfo a $\mathbb{Z}_4$

$U(\mathbb{Z}_8)$ è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$

$\varphi: \mathbb{Z}_2 \times \mathbb{Z}_2 \to U(\mathbb{Z}_8)$

$(\bar{0}, \bar{0}) \to \bar{1}$
$(\bar{1}, \bar{0}) \to \bar{3}$
$(\bar{0}, \bar{1}) \to \bar{5}$
$(\bar{1}, \bar{1}) \to \overline{15} = \bar{7}$

# ANELLI E CAMPI

Un anello è un insieme con 2 operazioni $(A, +, \cdot)$

$+: A \times A \to A$

$\times: A \times A \to A$

Due operazioni t.c.

1) $(A, +)$ gruppo commutativo
2) associativo: $a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \forall a,b,c \in A$
3) proprietà distributiva: $(a+b)\cdot c = (a\cdot b)+(b\cdot c) \qquad a(b+c) = (a\cdot b)+(a\cdot c)$

- L'elemento neutro della somma si denota con $0_A$
- Il prodotto non ha necessariamente un elemento neutro
- Se lo ha si denota con $1_A$ e l'anello si dice unitario
- Se il prodotto è commutativo l'anello si dice commutativo

es: $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Z}_n, +, \cdot)$ anello unitario commutativo

# CAMPO

Sia $(A, +, \cdot)$ un anello unitario

Ogni elemento $\neq 0_A$ ha inverso rispetto al prodotto, allora A si dice corpo (skew-field);

se $\cdot$ è commutativo A si dice campo (field)

$(\mathbb{Z}, +, \cdot)$ non è campo

$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ campi

$(\mathbb{Z}_n, +, \cdot)$ campi?

$\bar{x} \in \mathbb{Z}_n$

$\bar{x}$ invertibile $\leftrightarrow MCD(x, n) = 1$

se $n$ è primo $U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{0\}$

$(\mathbb{Z}_n, +, \cdot)$ campo $\leftrightarrow n = p$ primo