Esercizi sui gruppi

(Fascia bene tutti i passaggi)
+ ben fondate.

Per ciascuna delle seguenti coppie (insieme, operazione binaria), stabilire se formano un gruppo:

1) $(\mathbb{Z}, *)$ dove $m * n = |m+n|$

2) $(\mathbb{N}, \bullet)$ dove $m \bullet n = MCD(m,n)$

3) $(\mathcal{P}(X), \Delta)$ dove X è un insieme e, per $S, T \subseteq X$, $S \Delta T = (S \cup T) \setminus (S \cap T)$

$2 \cdot 4 \cdot 4$ $\quad 1 \cdot y = y$ $\quad \bar{2} \times \bar{4} = \overline{2 \cdot 4} x = x$

obt. 4) $(\mathbb{Z}_7^\times, \diamond)$ dove $\bar{x} \diamond \bar{y} = \overline{2xy}$ → nota: ben def → evidente $\bar{2} \cdot \bar{x} \cdot \bar{y}$ (è ben definito)

5) $(\mathbb{Z} \times \mathbb{Z}, \square)$ dove $(x,y) \square (u,v) = (xv + yu, yv)$

Altri esercizi:

6) Sia $\sqrt{2}\mathbb{Q} = \{x \in \mathbb{R} \mid \exists t \in \mathbb{Q} \text{ tale che } x = \sqrt{2}t\}$.
Stabilire se $\sqrt{2}\mathbb{Q}$ è sottogruppo di $(\mathbb{Q}, +)$ e se $\sqrt{2}\mathbb{Q} - \{0\}$ è sottogruppo di $(\mathbb{R}^\times, \cdot)$.

lettorale

7) Individuare tutti i sottogruppi del gruppo $(\mathbb{Z}_{12}, +)$.

Caso gruppi diedrali

8)* Sia D_4 l'insieme delle isometrie (riflessioni o rotazioni) che mandano un quadrato in sé stesso. Mostrare che D_4 è un gruppo rispetto alla composizione di isometrie. Scrivere la tavola moltiplicativa di $(D_4, \circ)$.

gruppo quaternioni

9)* Sia $H = \{\pm 1, \pm i, \pm j, \pm k\}$ e $\cdot : H \times H \longrightarrow H$ un'operazione associativa tale che

$$(-1)\cdot(-1) = 1, \quad i \cdot j = k, \quad \forall \alpha \in \{i, j, k\} \; (-1)\cdot\alpha = -\alpha \;\text{ e }\; \alpha\cdot\alpha = -1.$$

Si mostri che $(H, \cdot)$ è un gruppo.

$\pm 1 \cdot \pm 1$ $\quad$ 1 el $\quad$ $\alpha = (-\alpha)^{-1}$ $\quad$ $-1 = (-1)^{-1}$

$\pm 1 \cdot \alpha = \pm \alpha$ $\quad$ $\alpha_1 \cdot \alpha_2$ $\quad$ $k\, i\, j = k \cdot k = -1$

10) Mostrare che
$$f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_{10}, +) \times (\mathbb{Z}_8, +) \qquad n \longmapsto ([n]_{10}, [n]_8)$$
è un omomorfismo di gruppi. Determinare il nucleo di f e stabilire se è iniettivo o suriettivo.

$ki = +j$

$ijk = kk$

$ijk = -1$

$jk = i$

è ben posta

11) Stabilire se
$$f : (\mathbb{Z}_3, +) \longrightarrow (\mathbb{Z}_6, +) \qquad [x]_3 \longmapsto [2x^3]_6$$
è un omomorfismo di gruppi.

12) Scrivere la tavola moltiplicativa di $(S_3, \circ)$, di $(\mathbb{Z}_6, +)$ e di $(\mathbb{Z}_7^\times, \cdot)$. Stabilire quali tra essi sono isomorfi ed esibire un isomorfismo.

13) Descrivere, a meno di isomorfismo, tutti i possibili gruppi di cardinalità 2, 3, 4.

14) Sia $(G,*)$ un gruppo. Dimostrare che:

i) Se $H, K \leq G$, allora $H \cap K \leq G$;

ii) In generale non è vero che $H, K \leq G \Rightarrow H \cup K \leq G$ (trovare un controesempio)

* iii) $Z = \{ z \in G \mid \forall g \in G \quad z*g = g*z \}$ è un sottogruppo di G.

iv) $\forall x \in G$ fissato, $\begin{array}{rcl} c_x : (G,*) & \longrightarrow & (G,*) \\ g & \longmapsto & x*g*x^{-1} \end{array}$ è un omomorfismo.

* v) $\begin{array}{rcl} * : (G,*) \times (G,*) & \longrightarrow & (G,*) \\ (g_1, g_2) & \longmapsto & g_1 * g_2 \end{array}$ è un omomorfismo se e solo se $(G,*)$ è un gruppo abeliano.

\- 15) Dimostrare che, per $m, n \in \mathbb{N}$, con $n \mid m$.

$$\begin{array}{rcl} (\mathbb{Z}_m, +) & \longrightarrow & (\mathbb{Z}_n, +) \\ [x]_m & \longmapsto & [x]_n \end{array}$$

è un epimorfismo di gruppi.

Vedo sud – 16)* Dimostrare che, per $m, n \in \mathbb{N} \setminus \{0\}$:

$$\begin{array}{rcl} (\mathbb{Z}_{mn}, +) & \longrightarrow & (\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +) \\ [x]_{mn} & \longmapsto & ([x]_m, [x]_n) \end{array}$$

è un omomorfismo di gruppi ed è un isomorfismo se e solo se $MCD(m,n) = 1$.

1) $(\mathbb{Z}, *)$ dove $m * n = |m+n|$

ass. el. neutro inverso comm

$||m+n|+k|$ $\qquad (a\cdot b)\cdot c$

$a\cdot(b\cdot c)$

$8 = ||-2+2|+4| = |-2 * \underset{2}{|4-2|}| = 0$

non gruppo

2) $(\mathbb{N}, \cdot)$ dove $m\cdot n = MCD(m,n)$

semigrup.

- è associa
- $MCD(n,0)=n$ monoide $\qquad$ comm $0=el$
- $MCD(n,n^{-1})=0$ $\qquad 0|n \quad 0|n^{-1}$ $\Rightarrow n=0$, $n^{-1}=0$

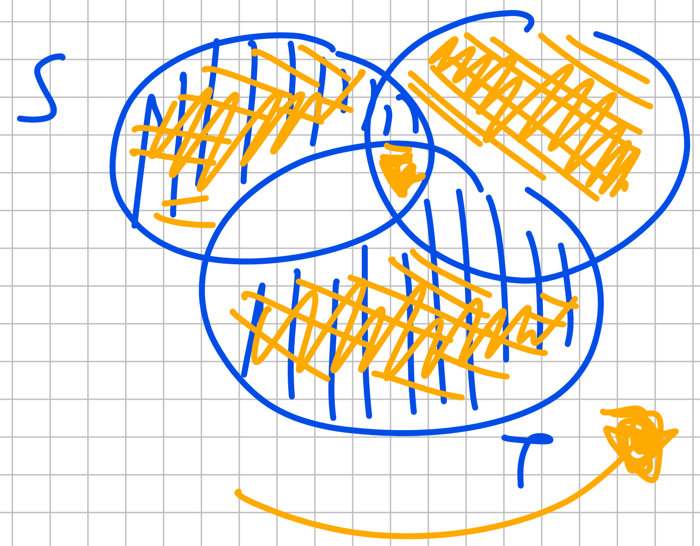
$\downarrow$ $mcd(n, 1 \text{ oppure } 0)\neq 0$ ✓

non gruppo

3) $(P(x),\Delta)$ $\qquad S\Delta T=(S\cup T)\setminus(S\cap T)$

- comm ovvio
- $[(S\cup T)\setminus(S\cap T)]=A$

$(A\cup B)\setminus(A\cap B)$



associat.

- el neut $=\emptyset$ $\quad$ 1260 $\quad \{\}$

$(S\cup e)\setminus(S\cap e)=S$

$S \quad S - S$

- inverso $(S\cup S)\setminus(S\cap S)=\emptyset$ $\qquad S=S^{-1}$ inverso

gruppo abeliano

④ $(\mathbb{Z}_7^{\times}, \bullet)$ $\quad \bar{x} \bullet \bar{y} = \overline{2xy} \rightarrow \overline{(2xy)}$

• comm $\Rightarrow$ x prop. molt.

$2 \cdot x \cdot y \Rightarrow \overline{2xy}$

• asso $\nearrow$ → semigruppo

• el ~~non esiste~~ $\longrightarrow$ $\overline{2x \cdot e} = \bar{x}$

$\overline{2 \cdot x \cdot 0} \neq x$

+ inve ⇒ grup. abeliano

esiste $\bar{2} \cdot \bar{4} \cdot \bar{x} = \bar{1}x = x$

$\bar{2}\bar{x} \cdot \bar{4} = \bar{1}x = x$

⑤ $(\mathbb{Z} \times \mathbb{Z}, \bullet)$ $\quad (x,y) \cdot (u,v) = (xv + yu, yv)$

• associativo

$(xv + yu, yv) \bullet (a,b) = ((xv+yu)b + yv \cdot a, yv \cdot b)$

$(u,v)(a,b) \; (ub + va, vb)$

$\rightarrow (x,y)(ub+va, vb) = [x(vb) + y(ub+va), y \cdot vb]$

• el neutr

monoide

$(\overset{x}{xe_1} + \overset{0}{ye_2}, \overset{=y}{ye_1})$ $\quad (x,y)(1,0) = (x,y)$

$e_2 = 0 \quad e_1 = 1$

• inverso

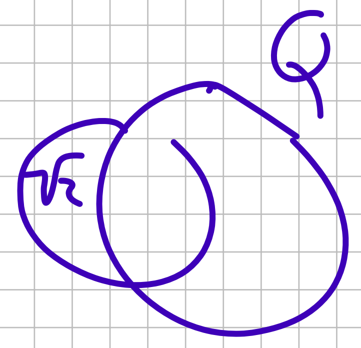
$(x,y)(x^{-1}, y^{-1})$ $\begin{cases} xy^{-1} + y \cdot x^{-1} = 1 \\ y \cdot y^{-1} = 0 \end{cases}$ $= (1,0)$

$\frac{1}{y} \quad 0$

ma siamo in Z

6) $H=\sqrt{2}\,\mathbb{Q} = \{x\in\mathbb{R} / \exists\, t\in\mathbb{Q}$ t.c. $x=\sqrt{2}\cdot t\}$

↳ $\frac{m}{n}\sqrt{2}$



1) → è sottogruppo $(\mathbb{Q},+)$ → No in quanto $t=1 \Rightarrow \sqrt{2}\cdot 1 \notin \mathbb{Q}$

$\sqrt{2}\,\mathbb{Q} \not\subseteq \mathbb{Q}$

2) $\mathbb{R}^{\times} = \mathbb{R}-\{0\}$

$(H,\cdot)\leq(\mathbb{R}^{\times},\cdot)$

1) sottoins. $t=0$

$\sqrt{2}\cdot 0 = 0 \notin \mathbb{R}^{\times}$

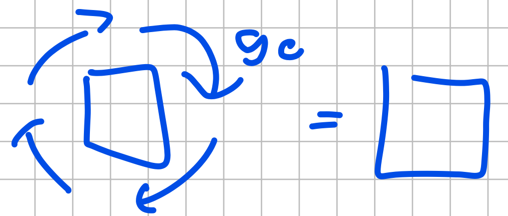
7) Individuare i sot. di $(\mathbb{Z}_{12},+)$

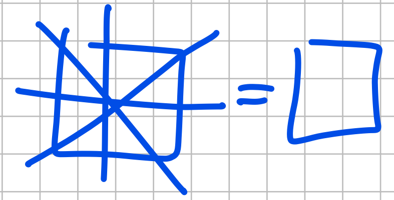
$n\mathbb{Z}_{12}$ 1) $\{0\}$ 2) $\mathbb{Z}_{12}$ 3) $2\mathbb{Z}_{12}=\{0,2,\dots,10\}$ 4) $3\mathbb{Z}_{12}\{0,3,6,9\}$.

5) $4\mathbb{Z}=\{0,4,8\}$ 6) $6\mathbb{Z}_{12}\{0,6\}$

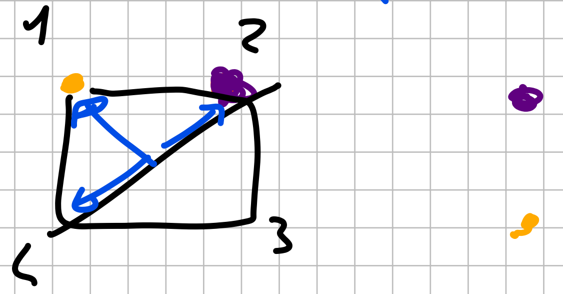
8 D_4 isometrie (rifless e rotazioni)

↳ quadro → quadro





• $(D_4, \circ)$ è gruppo



$(1, 2)$

$(1, 2, 3)$ $(0, 90)$

9 S_{10} $H = \{\pm 1, \pm i, \pm j, \pm k\}$

$\cdot : H \times H \to H$

$(-1) \cdot (-1) = 1$

$i \cdot j = k$

$\forall \alpha \in \{i, j, k\}$

$-1 \cdot \alpha = -\alpha$

$\alpha \cdot \alpha = -1$

$(H, \cdot)$ è un gruppo

10 $f : (\mathbb{Z}, +) \to (\mathbb{Z}_{10}, +) \times (\mathbb{Z}_8, +)$

è un omomorfismo

$n \to ([n]_{10}, [n]_8)$

$f(g+h) = f(g) + f(h)$

$f(g+h) \overset{def}{=} ([g+h]_{10}, [g+h]_8) =$

$([g]_{10}, [g]_8) + ([h]_{10}, [h]_8)$

$f(g) + f(h)$

$\ker(f) = (0_{10}, 0_8)$ $\{f(0), f(40), \dots$
$f(40 \cdot k \mid k \in \mathbb{Z})\}$

↳ $|\ker(f)| > 1$

non è iniettiva f

2 1 $f(n)$

$n = 10 \cdot k + 2$ $n = 8 \cdot k' + 1$ → sia pari che dispari IMP

(11) $f : (\mathbb{Z}_3, +) \to (\mathbb{Z}_6, +)$ è omomor.

$[x]_3 \to [2x^3]_6$

$f(x_3 + y_3) = f(x_3) + f(y_3)$

$6k \bmod 6 = 0$

$f(x_3 + y_3) = [2(x+y)^3]_6 \to 2x^3 + 6x^2y + 6xy^2 + 2y^3 \bmod 6 = 2x^3 + 0 + 0 + 2y^3$

$\hookrightarrow [2x^3 + 2y^3]_6$

$f(x_3) + f(y_3) = [2x^3]_6 + [2y^3]_6$

$= [2x^3 + 2y^3]_6$ = cvd

(12) $(S_3, \circ)$ $(\mathbb{Z}_6, +)$ $(\mathbb{Z}_7^\times, \cdot)$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$a \circ b$

$a \backslash b$	Id	(1,2)	(2,3)	(1,3)	(1,2,3)	(3,2,1)
Id	Id	(1,2)	(2,3)	(1,3)	(1,2,3)	(3,2,1)
(1,2)	(1,2)	Id	(1,2,3)	(1,3,2)	(2,3)	(3,1)
(2,3)	(2,3)	(1,3,2)	Id	(1,2,3)	(1,3)	(2,1)
(1,3)	(1,3)	(1,2,3)	(2,1,3)	Id	(1,2)	(3,2)
(1,2,3)	(1,2,3)	(2,3,1)	(2,1)	(3,2)	(1,3,2)	Id
(3,2,1)	(3,2,1)	(2,3)	(3,1)	(1,2)	Id	(1,2,3)

13) 2, 3, 4 $= |H| \div (H, \diamond)$

el h

unico di ord 2

el	h	($h = h^{-1}$)
Id	(1,2)	

unico comb card 3

el h h^{-1}

el $h = h^{-1}$ $z = z^{-1}$

imp $h \circ z = ?$

- $h \cdot z = el \Rightarrow h = z^{-1} = z$
- $h \cdot z = h \Rightarrow z = el$
- $h \cdot z = z \Rightarrow h = el$

$el \quad h \quad h^{-1} \quad k = k^{-1}$ / $el \cdot k = k$
$h \cdot k = el \Rightarrow h^{-1} = k$
...

$h \cdot k = el \rightarrow h^{-1} = k$

$h \cdot k = h \rightarrow k = el$.

$h \cdot k$

$h \cdot k$ ...

$el \quad k = k^{-1} \quad r = r^{-1} \quad s = s^{-1} \Rightarrow ||G|| = 0 \Rightarrow$ tot 2

(vedi card 3)

---

sia $(G, *)$ gruppo

1) se $H, K \leq G \quad H \cap K \leq G$

$el \in H \cap K \Leftarrow el \in K \wedge el \in H$

$x \in H \cap K \Rightarrow x \in H \wedge x \in K$

$\Rightarrow x^{-1} \in H \wedge x^{-1} \in K \Rightarrow x^{-1} \in H \cap K$

$x, y \in H \cap K$ x gruppo

$x * y^{-1} \in H \cap K \qquad x * \cancel{z} \in H \cap K$

$y^{-1} \in H \cap K = z$

$$\left.\begin{array}{l} x \in H \wedge z \in H \Rightarrow x * z \in H \\ x \in K \wedge z \in K \Rightarrow x * z \in K \end{array}\right\} x * z \in H \cap Z$$

II) non è vero che $H, K \leq G \Rightarrow H \cup K \leq G$

$H = ((n, 0), +)$ $\qquad \{(n,0) \mid n \in \mathbb{Z}\}$

$K = ((0, n), +)$

$G = (\{(0, n), (n, 0)\}, +) \rightarrow (n, n) \notin G$

non è gruppo

III) $Z = \{ z \in G \mid \forall g \in G \quad z * g = g * z \}$

è un sottogruppo di G

$\{e\} \qquad G$

a • $e \in Z$ x def el neutro $\quad e \cdot g = g \cdot e = g$

b • $z \in Z$ $\qquad z^{-1} z \cdot g = z^{-1} g z$ $\qquad g = z^{-1} \cdot g \cdot z$

$g \cdot z^{-1} = z^{-1} \cdot g$

$c: x \cdot y^{-1} \in Z$ hp $x \in Z$, $y \in Z$

$\hookrightarrow y^{-1} \in Z$ x punto $y^{-1} = z \in Z$

$x \cdot z \in Z$

$\underline{(xz)g} = x(zg)$ x def Z

$= x(gz)$

$= (xg)z$

$(gx)z$ x def Z

$\underline{g(xz)}$

$x \cdot z \in Z$

IV) $\forall \bar{x} \in G$ fissato

$c_x : (G, *) \to (G, *)$

$g \to \bar{x} * g * \bar{x}^{-1}$

- $\cancel{e \to \bar{x} \cdot \bar{x}^{-1} = e}$ $\cancel{e}$
- $\underline{f(g * h^{-1}) = f(g) * f(h^{-1})}$ def omomorfismo

$f(g * h^{-1}) = \bar{x} g h^{-1} x^{-1}$ = cvd

$$f(g) * f(h^{-1}) = \bar{x}\, g\, \cancel{\bar{x}^{-1}} \cdot \cancel{\bar{x}} \cdot h^{-1} \cdot \bar{x}$$

$$\bar{x} \cdot g \cdot h^{-1} \cdot \bar{x} = f(g * h^{-1})$$

---

f $*: (G,*) \times (G,*) \to (G,*)$

$$(g_1, g_2) \to g_1 * g_2$$

· $*$ è un omomorfismo $\Leftrightarrow$ G è un gruppo abel.

a)

$$f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2)$$

$$f\big[\overset{d}{(g_1, g_2)} \cdot \overset{d}{(g_3, g_4)}\big] \overset{?}{=} f\big[\overset{d}{(g_1, g_2)}\big] \cdot f\big[\overset{d}{(g_3, g_4)}\big]$$

$$\underbrace{f[(g_1,g_2)]}_{g_1 \cdot g_2} \cdot (g_3 \cdot g_4)$$

a)

$$f((g_1 \cdot g_3,\ g_2 \cdot g_4)) \overset{?}{=} g_1 \cdot g_2 \cdot g_3 \cdot g_4$$

$$g_1 \cdot g_3 \cdot g_2 \cdot g_4 \qquad R \quad \text{(a)} = g_1 \cdot g_3 \cdot g_2 \cdot g_4$$

xche comm

cvd

b) $\cancel{g_1} \cdot g_3 \cdot g_2 \cdot \cancel{g_4} = \cancel{g_1} \cdot g_2 \cdot g_3 \cdot \cancel{g_4}$ xche gruppo

$g_3 \cdot g_2 = g_2 \cdot g_3 \Rightarrow$ comm. cvd

(15) $m, n \in \mathbb{N}$ t.c $n \mid m$

$f: (\mathbb{Z}_m, +) \longrightarrow (\mathbb{Z}_n, +)$ è un epimorfismo

$[x]_m \mapsto [x]_n$

(a) omomorf

(b) suriettivi

(a) $f([x]_m + [y]_m)$

$= f([x+y]_m) = [x+y]_n$

$= [x]_n + [y]_n = f([x]_m) + f([y]_m)$

cvd

=> omomorf.

(b) $\forall_k \; \exists_x \mid f([x]_m) = [k]_n$

$\mathbb{Z}_0 = \mathbb{N} = \mathbb{Z}_n \geq n \; \forall_n$

- $n \mid m \quad nh = m$ ↗ $m = 0$; ↘ $m \neq 0 \Rightarrow h \neq 0$ $\Rightarrow n \leq m$

$\forall_{k \leq n \leq m} \; f([k]_m) = [k]_n$

$\forall_{k \leq n} \exists \cancel{k} \mid f([x]_m) = [k]_n$

16 $m, n \in \mathbb{N} \setminus \{0\}$

$$f: (\mathbb{Z}_{mn}, +) \to (\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)$$

$$[x]_{mn} \to ([x]_m, [x]_n)$$

a) omorfismo

b) biet $\Leftarrow\!\!\Rightarrow$ MCD $(m,n)=1$

a)

$$f([x]_{mn} + [y]_{mn}) = f([x+y]_{mn}) =$$

$$([x+y]_m, [x+y]_n) \quad \text{cvd}$$

$$f([x]_{mn}) + f([y]_{mn}) = ([x]_m, [x]_n) + ([y]_m, [y]_n)$$

$$= ([x+y]_m, [x+y]_n)$$

b) 1 hp MCD $(m,n)=1$

a) iniettiva?

$$f(x) = f(y) \implies x = y$$

$$([x]_m, [x]_n) = ([y]_m, [y]_n)$$

$\Rightarrow$ membro a membro

$$\begin{cases} [x]_m = [y]_m \\ [x]_n = [y]_n \end{cases}$$

$\Rightarrow [x]_{mn} = [y]_{mn}$

(b) suriett?

$$([a]_m, [b]_n) = f(x)$$

$x = a + m \cdot k \qquad x = b + n \cdot k'$

$\cancel{x}$ MCD $= 1$

$2x = a + b + mk + nk'$

$2 | m \Rightarrow 2 \nmid n$

$2 | n \Rightarrow 2 \nmid m$

GUARDO Testi

su oltre X°

(17 - 19)