Un **GRUPPO** è una struttura algebrica

$$(G, *)$$

ove G insieme, $*: G \times G \to G$ operazione binaria su G tale che

1) $\exists e \in G : \forall g \in G : e * g = g * e = g$ (el. neutro)
2) $\forall g \in G \; \exists g' \in G : g * g' = g' * g = e$ (el. inverso)
3) $\forall a, b, c \in G : a * (b * c) = (a * b) * c$. (prop. associativa).

Def: Un Gruppo è detto **commutativo** o **abeliano** se $\forall a, b \in G : a * b = b * a$.

Es. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ } GRUPPI ABELIANI

$0 \in \mathbb{Z}$ & $a + 0 = 0 + a = a \quad \forall a \in \mathbb{Z}$

$\forall a \in \mathbb{Z} \; \exists (-a) \in \mathbb{Z} : \; a + (-a) = 0$

$\forall a, b, c \in \mathbb{Z} : \; a + (b + c) = (a + b) + c$

$\forall a, b \in \mathbb{Z} : \; a + b = b + a$

OSS: $(\mathbb{Z}, -)$ NON È UN GRUPPO!!

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

$+$ → operazione. $(-b)$ → elemento

$(\mathbb{N}_0, +)$ NON È UN GRUPPO:

Valgono prop. associativa, commutativa
ed $\exists$ elemento neutro
ma non esiste l'opposto di $n \in \mathbb{N}$ $n \neq 0$.

$(\mathbb{Q}^\times, \cdot)$
$(\mathbb{R}^\times, \cdot)$ ove $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$.] gruppi abeliani

N.B. $(\mathbb{R}, \cdot)$ NON È UN GRUPPO PERCHÉ 0 NON AMMETTE INVERSO! (= reciproco)

$a/b := a\, b^{-1}$ $\quad a, b \neq 0$

per definizione.

Siano $(G, *)$ e (H, Δ) due gruppi.

Allora $G \times H$ può essere dotato di una struttura di gruppo considerando l'operazione $\overset{\vee}{*}$ data da

$$(g_1, h_1) \overset{\vee}{*} (g_2, h_2) = (g_1 * g_2, h_1 \Delta h_2)$$

DATI 2 GRUPPI È POSSIBILE DOTARE IL LORO PRODOTTO CARTESIANO DI UNA STRUTTURA DI GRUPPO LAVORANDO COMPONENTE PER COMPONENTE.

→ $(G, *)$ e consideriamo $(G^n, *)$

Sia $(\mathbb{R}, +)$

Consideriamo $\mathbb{R}^n = \{(a_1 \dots a_n) \mid a_i \in \mathbb{R}\}$.

esempio $\mathbb{R}^3 = \{(a_1, a_2, a_3) \mid a_1, a_2, a_3 \in \mathbb{R}\}$.

Definiamo in $\mathbb{R}^3$ l'operazione $\dot{+}$

$$(a_1, a_2, a_3) \dot{+} (b_1, b_2, b_3) =$$

$$= (a_1 + b_1, a_2 + b_2, a_3 + b_3)$$

somma componente per componente.

Es. $(1, 5, 7) \dot{+} (3, 6, 9) =$

$$= (1+3, 5+6, 7+9) =$$

$$= (4, 11, 15)$$

(discorso analogo in $\mathbb{R}^n$).

$(\mathbb{R}^3, +)$ è un gruppo abeliano.

1) $(a_1, b_1, c_1) + (0,0,0) = (a_1+0, b_1+0, c_1+0) =$

$= (a_1, b_1, c_1)$ el. neutro ✓

$(0,0,0) + (a_1, b_1, c_1) = (a_1, b_1\ c_1)$

NON FARE CONFUSIONE

$(ab, cd) \neq (a, b, c, d)$

$(ab\ cd)\ ?\ (a\ b\ c\ d)$

2) $\forall (a_1, b_1, c_1) \in \mathbb{R}^3\ \exists\ (-a_1, -b_1, -c_1) \in \mathbb{R}^3$:

$(a_1, b_1, c_1) + (-a_1, -b_1, -c_1) = (a_1 - a_1, b_1 - b_1, c_1 - c_1)$

$=$

$(0,0,0)$ $\exists$ inverso per ogni elemento.

3) $(a_1,b_1,c_1)+((a_2,b_2,c_2)+(a_3,b_3,c_3)) =$

$= (a_1,b_1,c_1)+(a_2+a_3,\ b_2+b_3,\ c_2+c_3) =$

$= (a_1+(a_2+a_3),\ b_1+(b_2+b_3),\ c_1+(c_2+c_3)) =$

$= ((a_1+a_2)+a_3,\ (b_1+b_2)+b_3,\ (c_1+c_2)+c_3) =$

perché vale la prop. associativa in $(\mathbb{R},+)$

$=(a_1+a_2,\ b_1+b_2,\ c_1+c_2)+(a_3,b_3,c_3) =$

$=((a_1,b_1,c_1)+(a_2,b_2,c_2))+(a_3,b_3,c_3)$ ✓

N.B. $(\mathbb{R}^3, +)$ è anche abeliano.

$$(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$$

$$= (a_2 + a_1, b_2 + b_1, c_2 + c_1) =$$

$$= (a_2, b_2, c_2) + (a_1, b_1, c_1)$$

I gruppi visti finora sono tutti commutativi.

Esempio: il gruppo simmetrico su di un insieme X non comm.

X insieme $S(X) := \{f : X \to X \mid f \text{ biiettiva}\}$.

$(S(X), \circ)$ è un gruppo non commutativo

$\circ$ ↑ composizione di funzioni

oss: se $f: X \to X$ biiettiva

$g: X \to X$ biiettiva

$\Rightarrow (g \circ f): X \to X$ ed è ancora biiettiva.

- $S(X) \times S(X) \to S(X)$

  è una operazione su $S(X)$

2) Sia $\iota_x : \begin{cases} X \to X \\ x \to x \end{cases}$ la funzione identica su X.

   identità

$\Rightarrow (\iota_x \circ f)(x) = \iota_x(f(x)) = f(x) \quad \forall x$

$(f \circ \iota_x)(x) = f(\iota_x(x)) = f(x)$

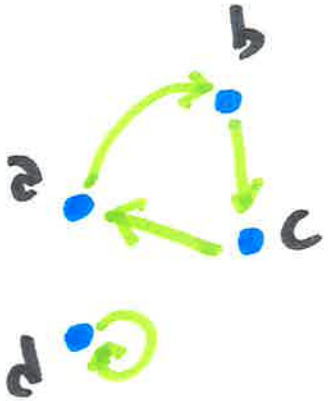
quindi $(\iota_x \circ f) = (f \circ \iota_x) = f$ ed esiste el. neutro.

3) Sappiamo che se $f: X \to X$ biiettiva

$\Rightarrow f^{opp}: X \to X$ è tale che

$$f \circ f^{opp} = 1_X = f^{opp} \circ f$$

$f^{opp} =: f^{-1}$ (inverso).



$f(a) = b$ $\quad f^{opp}(b) = a$

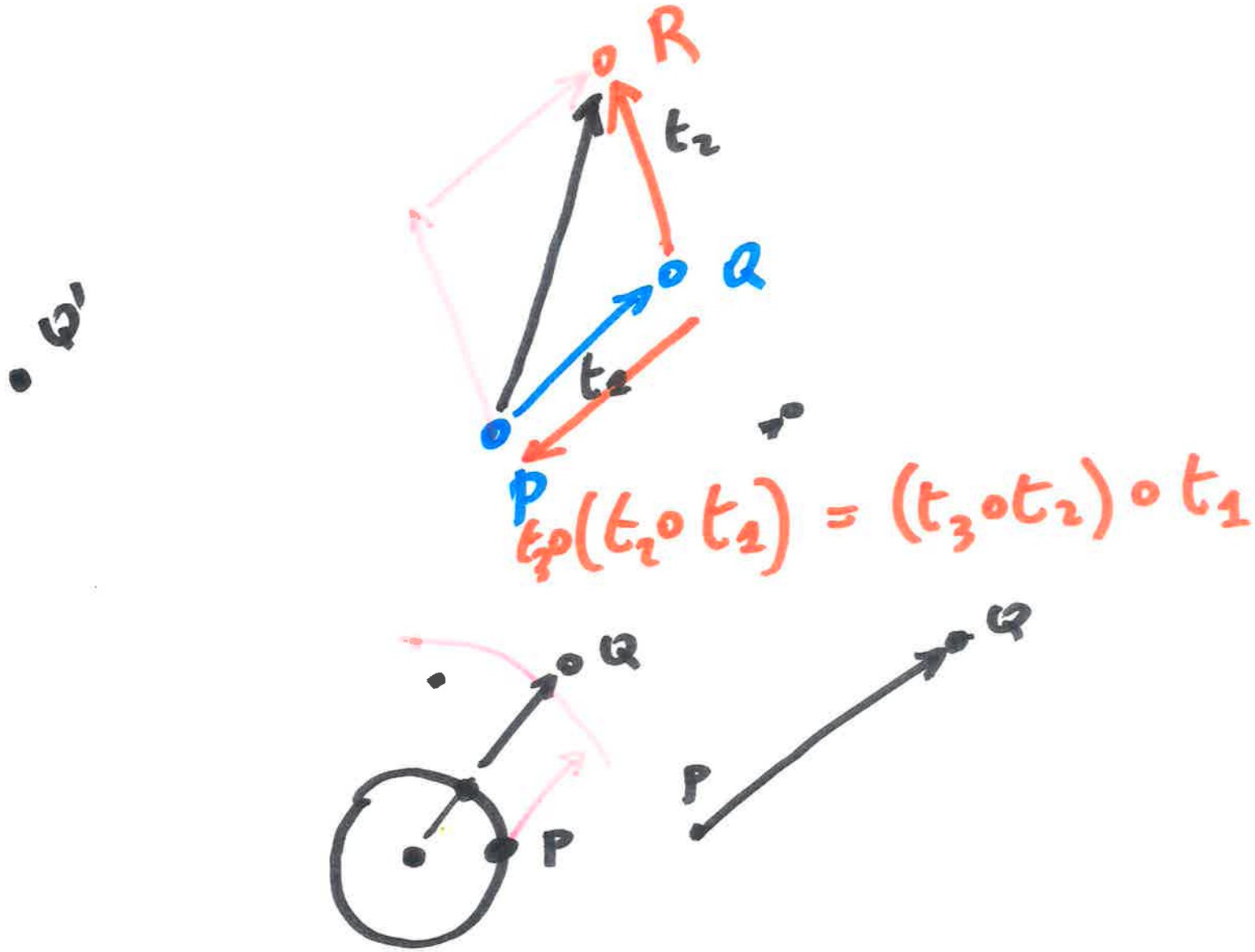
$f(b) = c$ $\quad f^{opp}(c) = b$

$f(c) = a$ $\quad f^{opp}(a) = c$

$f(d) = d$ $\quad f^{opp}(d) = d$

4) Vale la prop. associativa

$$(f \circ g) \circ h = f \circ (g \circ h)$$


R
t_2
Q
t_1
P
$t_3 \circ (t_2 \circ t_1) = (t_3 \circ t_2) \circ t_1$
Q
P
Q
P

Campo $(\mathbb{K}, +, \cdot)$ struttura algebrica con

$\mathbb{K}$ insieme

$+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ somma

$\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ prodotto

due operazioni binarie.

Tale che

1) $(\mathbb{K}, +)$ è un gruppo abeliano.
2) $(\mathbb{K} \setminus \{0\}, \cdot)$ è un gruppo abeliano
3) valgono le proprietà distributive della somma rispetto il prodotto

$\forall a, b, c \in \mathbb{K}$: $(a+b)c = ac + bc$

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

$(\mathbb{R}, +, \cdot)$

$(\mathbb{Q}, +, \cdot)$

Un campo è l'ambiente "giusto" dove studiare e risolvere una eq. di I grado

$$ax + b = 0$$

con $a \neq 0$ e verificare che $\exists!$ soluzione.

$$ax + b + (-b) = 0 + (-b)$$

$$ax = -b$$

$$x = a^{-1}ax = a^{-1}(-b) = -a^{-1}b$$

oss: $(\mathbb{Z}, +, \cdot)$ NON É UN CAMPO!

perché elementi $\neq \pm 1$ non hanno reciproco in $\mathbb{Z}$

$2X+3=0$ NON HA SOLUZIONE IN $\mathbb{Z}$

risolvere le equazioni a coeff in $\mathbb{Z}$ da risolvere in $\mathbb{Z}$ sono dette equazioni diofantee.

→ di solito non è facile studiarle (se deg > 1).

$a^n + b^n = c^n$ non ha soluzioni non banali in $\mathbb{Z}$ se $n > 2$

$(\mathbb{Z}_2, +, \cdot)$ $\quad \mathbb{Z}_2 = \{0, 1\}$.

+	0	1
0	0	1
1	1	0

XOR

·	0	1
0	0	0
1	0	1

AND

$1 + 1 = 0$

ca+cb

a	b	c	(a+b)	c(a+b)	ca	cb
0	0	1	0	0	0	0
0	1	0	1	0	0	0
0	1	1	1	1	0	1
1	0	0	1	1	1	0
1	0	1	1	1	0	1
1	1	0	0	0	0	0
1	1	1	0	0	0	0
0	0	0	0	0	0	0