GRUPPI (III PARTE)

Omomorfismi

<u>Def</u>: Siano $(G, \cdot)$ e $(H, *)$ due gruppi. Un <u>omomorfismo</u> da $(G,\cdot)$ a $(H,*)$ è una funzione $f: G \to H$ tale che

$$\forall g_1, g_2 \in G \qquad f(g_1 \cdot g_2) = f(g_1) * f(g_2)$$

operazione in G operazione in H

Questa definizione equivale a richiedere che il diagramma sia commutativo.

$$(g_1, g_2) \longmapsto g_1 \cdot g_2$$

$$\begin{tikzcd} G \times G \arrow[r, "\cdot"] \arrow[d, "f \times f"'] \arrow[dr, phantom, "/\!/"] & G \arrow[d, "f"] \\ H \times H \arrow[r, "*"] & H \end{tikzcd}$$

$$(f(g_1), f(g_2)) \longmapsto f(g_1) * f(g_2) \;/\!/\; f(g_1 \cdot g_2)$$

Esempi:

1) $(G, \cdot)$, $(H, *)$. Sia e_H l'elemento neutro di H.

$$\begin{aligned} f: G &\longrightarrow H \\ g &\longmapsto e_H \end{aligned}$$

costante è un omomorfismo: $\forall g \in G \; f(g) = e_H$

$$\left.\begin{aligned} f(g_1 \cdot g_2) &= e_H \\ f(g_1) * f(g_2) &= e_H * e_H = e_H \end{aligned}\right\} \text{ sono uguali}$$

2) $(G, \cdot)$ gruppo. $id_G: G \longrightarrow G$ è un omomorfismo.

3) $(\mathbb{Z},+)$ $\quad f:\mathbb{Z}\longrightarrow\mathbb{Z}$ è un omomorfismo, infatti: $\forall x_1,x_2\in\mathbb{Z}$

$n\in\mathbb{N}$ fissato $\quad x\longmapsto n\cdot x$

$$f(x_1+x_2)=n\cdot(x_1+x_2)\underset{\text{propr. distributiva}}{=}nx_1+nx_2=f(x_1)+f(x_2)$$

4) $(\mathbb{R}^\times,\cdot)$ $\quad f:\mathbb{R}\longrightarrow\mathbb{R}$, $x\longmapsto x^2$ è un omomorfismo da $(\mathbb{R}^\times,\cdot)$ in sé stesso

perché $f(x\cdot y)=(xy)^2=x^2y^2=f(x)f(y)$

$(\mathbb{R},+)$ $\quad f:\mathbb{R}\longrightarrow\mathbb{R}$, $x\longmapsto x^2$ non è un omomorfismo da $(\mathbb{R},+)$ in sé stesso

infatti, per esempio $f(1)+f(2)=1^2+2^2=5$

mentre $f(1+2)=f(3)=3^2=9$

sono diversi

5) $(\mathbb{R},+)\xrightarrow{f}(\mathbb{R}^\times,\cdot)$, $x\longmapsto 2^x$ è un omomorfismo perché $\forall x,y\in\mathbb{R}$

$$f(x+y)=2^{x+y}=2^x\cdot 2^y=f(x)\cdot f(y)$$

6) $((0,+\infty),\cdot)\xrightarrow{f^{-1}}(\mathbb{R},+)$, $x\longmapsto \log_2 x$ è un omomorfismo perché $\forall x,y\in(0,+\infty)$

$$f^{-1}(x\cdot y)=\log_2 xy\underset{\text{proprietà dei logaritmi}}{=}\log_2 x+\log_2 y=f^{-1}(x)+f^{-1}(y)$$

7) $n \in \mathbb{N}$ fissato $\quad (S_n, \circ) \xrightarrow{sg} (\{\pm 1\}, \cdot)$ $\qquad sg(\sigma) = \begin{cases} 1 & \text{se } \sigma \text{ è pari} \\ -1 & \text{se } \sigma \text{ è dispari} \end{cases}$

$\sigma \longmapsto sg(\sigma)$

Siano $\sigma, \tau \in S_n$ $\qquad sg(\sigma \circ \tau) = ?$

1) Se σ, τ pari $\sigma \circ \tau$ è pari $\quad sg(\sigma \circ \tau) = 1$
2) Se σ, τ dispari $\sigma \circ \tau$ è pari $\quad sg(\sigma \circ \tau) = 1$
3) Se σ, τ sono una pari e una dispari allora $\sigma \circ \tau$ dispari $\Rightarrow sg(\sigma \circ \tau) = -1$

1) $sg(\sigma) \cdot sg(\tau) = 1 \cdot 1 = 1$
2) $sg(\sigma) \cdot sg(\tau) = (-1)(-1) = 1$
3) $sg(\sigma) \cdot sg(\tau) = -1 \cdot 1 = -1$

coincidono con i precedenti $\Rightarrow$ sg è un omomorfismo

<u>Non esempi</u>:

8) $(\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$ $\quad$ non è un omomorfismo

$x \longmapsto \sin x$

Per esempio: $x = \frac{\pi}{2}$, $y = \frac{\pi}{4}$ $\qquad \sin x + \sin y = 1 + \frac{1}{\sqrt{2}}$

$\sin(x+y) = \frac{1}{\sqrt{2}}$

9) $(\mathbb{Z}, +) \xrightarrow{f} (\mathbb{Z}, +)$ $\quad$ non è un omomorfismo

$x \longmapsto 1$

$x = 0$, $y = 1$ $\qquad f(0+1) = f(1) = 1$

$f(0) + f(1) = 1 + 1 = 2$

$\forall x \in \mathbb{Z} \quad f(x) = 1$

Prop: $f:(G,\cdot) \longrightarrow (H,*)$ omomorfismo di gruppi. Valgono:

1) $f(e_G) = e_H$
2) $\forall g \in G \quad f(g)^{-1} = f(g^{-1})$
3) $\forall g \in G, \ \forall n \in \mathbb{Z}, \quad f(g)^n = f(g^n)$
4) Se $G_1 \leq G$, allora $f(G_1) \leq H$
5) Se $H_1 \leq H$, allora $f^{-1}(H_1) \leq G$

" $\leq$ " vuol dire sottogruppo.

Dim: 1) $f(e_G) = f(e_G \cdot e_G) \underset{\substack{\uparrow \\ f \text{ omom.}}}{=} f(e_G) * f(e_G) \underset{\substack{\uparrow \\ \text{leggi di cancellazione}}}{\Longrightarrow} e_H = f(e_G)$

2) $e_H = f(e_G) = f(g \cdot g^{-1}) = f(g) * \underbrace{f(g^{-1})}$ è l'inverso di $f(g)$

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

3) $n \in \mathbb{N}$. $n=0 \quad g^0 = e_G \quad f(g^0) = f(e_G) = e_H = f(g)^0$

$n=1 \quad f(g^1) = f(g) = f(g)^1$

PASSO INDUTTIVO: supponiamo che $f(g^n) = f(g)^n$ per un certo n fissato.

$f(g^{n+1}) = f(g^n \cdot g) \underset{\substack{\uparrow \\ f \text{ omom.}}}{=} f(g^n) * f(g) \underset{\substack{\uparrow \\ \text{hp induttiva}}}{=} f(g)^n * f(g) = f(g)^{n+1}$

(caso $n \in \mathbb{Z}$ per esercizio)

4) Siano $h_1, h_2 \in f(G_1)$. Allora $\exists g_1, g_2 \in G$ t.c. $f(g_1) = h_1$, $f(g_2) = h_2$, quindi

$$h_1 * h_2^{-1} = f(g_1) * f(g_2)^{-1} \underset{\substack{\uparrow \\ \text{usiamo il} \\ \text{punto 2)}}}{=} f(g_1) * f(g_2^{-1}) \underset{\substack{\uparrow \\ \text{usiamo il fatto} \\ \text{che } f \text{ è omomorfismo}}}{=} f(g_1 \cdot g_2^{-1}) \implies h_1 * h_2^{-1} \in f(G_1)$$

5) Siano $g_1, g_2 \in f^{-1}(H_1)$. Allora $\exists h_1, h_2 \in H_1$ t.c. $f(g_1) = h_1$, $f(g_2) = h_2$

$$f(g_1 \cdot g_2^{-1}) \underset{\substack{\uparrow \\ f \text{ omom.}}}{=} f(g_1) * f(g_2^{-1}) \underset{\substack{\uparrow \\ 2)}}{=} f(g_1) * f(g_2)^{-1} = h_1 * h_2^{-1} \in H_1 \implies g_1 \cdot g_2^{-1} \in f^{-1}(H_1).$$

$\boxtimes$

Questa proposizione si può usare in negativo:

<u>Es</u>:
$$\begin{aligned} f : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ x &\longmapsto 2x + 1 \end{aligned}$$

$f(0) = 2 \cdot 0 + 1 = 1 \neq 0$

$\Rightarrow$ f non soddisfa la proprietà 1)

$\Rightarrow$ f <u>non</u> è un omomorfismo.

Def: $f:(G,\cdot)\longrightarrow(H,*)$ omomorfismo di gruppi, si dice

1) **monomorfismo** se è iniettivo,
2) **epimorfismo** se è suriettivo,
3) **isomorfismo** se è biettivo,
4) **endomorfismo** se $(G,\cdot)=(H,*)$,
5) **automorfismo** se è un endomorfismo biettivo.

Es. $f:((0,+\infty),\cdot)\longrightarrow(\mathbb{R},+)$ è un isomorfismo.
$x \longmapsto \log_2 x$

Def: $f:(G,\cdot)\longrightarrow(H,*)$ omomorfismo di gruppi. Si dice **nucleo** di f il sottoinsieme:

$$Ker(f)=\{g\in G \text{ t.c. } f(g)=e_H\}=f^{-1}(e_H)$$

Teorema: $f:(G,\cdot)\longrightarrow(H,*)$ omomorfismo di gruppi è iniettivo se e solo se $Ker(f)=\{e_G\}$.

Dim: "solo se": sia f iniettivo, allora $|f^{-1}(e_H)|\leq 1$ e poiché $f(e_G)=e_H \Rightarrow Ker(f)=f^{-1}(e_H)=\{e_G\}$.
"se": Sia $Ker(f)=\{e_G\}$ e siano $g_1,g_2\in G$ tali che $f(g_1)=f(g_2)$. Allora $f(g_1g_2^{-1})=f(g_1)*f(g_2^{-1})=$
$=f(g_1)*f(g_2)^{-1}=f(g_1)*f(g_1)^{-1}=e_H$, quindi $g_1g_2^{-1}\in Ker(f) \Rightarrow g_1g_2^{-1}=e_G \Rightarrow g_1g_2^{-1}g_2=g_2 \Rightarrow g_1=g_2$ $\boxtimes$