Omomorfismi di gruppi

26 October 2022 11:50

Def. Dati due gruppi G_1 e G_2, una funzione $f: G_1 \to G_2$ si dice OMOMORFISMO se $\forall g, h \in G_1$, $f(gh) = f(g)f(h)$

es. un'app. lineare è un omomorfismo

Prop. Sia $\varphi: G_1 \to G_2$ un omomorfismo, allora:

(i) $\varphi(e_1) = e_2$

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$

(iii) $o(\varphi(g)) \mid o(g)$

Dimostrazione

(i) $(e_1) = \varphi(e_1 \cdot e_1) = \varphi(e_1)\varphi(e_1)$

$$\Updownarrow$$

$$\varphi(e_1) = e_2$$

(ii) $\varphi(e_1) = \varphi(g \cdot g^{-1}) = \varphi(g)\varphi(g^{-1})$

$$\Updownarrow$$

$$\varphi(g)\varphi(g^{-1}) = e_2$$

$$\Updownarrow$$

$$\varphi(g^{-1}) = \varphi(g)^{-1}$$

(iii) $e_2 = \varphi(e_1) = \varphi(g^{o(g)}) =$

$= \varphi(g)^{o(g)}$. Quindi

$o(\varphi(g)) \mid o(g)$.

$\boxtimes$

Esempi di omomorfismo

$\boxtimes$

Esempi di omomorfismo

$$g : \mathbb{Z}_{20} \to \mathbb{Z}_{10} \quad \text{ben definita}$$
$$[a]_{20} \mapsto [a]_{10}$$

$$g([a]_{20} + [b]_{20}) = g([a+b]_{20}) =$$
$$= [a+b]_{10} = [a]_{10} + [b]_{10} =$$
$$= g([a]_{20}) + g([b]_{20}) \quad \text{omomorfismo}$$

Def. Data $\varphi : G_1 \to G_2$ omomorfismo si dice **NUCLEO** l'insieme $\ker \varphi =$
$= \{ g \in G_1 \mid \varphi(g) = e_2 \}$

OSS. $\ker \varphi$ è un SOTTOGRUPPO di G_1

Dimostrazione

$g_1, g_2 \in \ker \varphi$

(i) $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = e_2 e_2 = e_2$

Quindi $g_1 g_2 \in \ker \varphi$

(ii) $e_1 \in \ker \varphi$ (infatti $\varphi(e_1) = e_2$)

(iii) $\varphi(g_1^{-1}) = \varphi(g_1)^{-1} = e_2^{-1} = e_2 \Rightarrow$
$\Rightarrow g_1^{-1} \in \ker \varphi$

$\boxtimes$

Def. Data $\varphi : G_1 \to G_2$, si dice **IMMAGINE** l'insieme $\operatorname{Imm} \varphi = \{ g \in G_2 \mid$
$\exists h \in G_1 \mid \varphi(h) = g \}$

OSS. $\operatorname{Imm} \varphi$ è un SOTTOGRUPPO di G_2

(i) $e_2 \in \operatorname{Imm} \varphi$ ($\varphi(e_1) = e_2$)

(ii) $h_1, h_2 \in \operatorname{Imm} \varphi \Rightarrow \exists g_1, g_2 \in G_1 \mid$

$\varphi(g_1) = h_1 \wedge \varphi(g_2) = h_2.$

$\varphi(g_1 g_2) = h_1 h_2 \Rightarrow h_1 h_2 \in \mathrm{Imm}\,\varphi$

(iii) $h_1 \in \mathrm{Imm}\,\varphi \Rightarrow \exists\, g_1 \in G_1 \mid$

$\varphi(g_1) = h_1.$ $\varphi(g_1^{-1}) = \varphi(g_1)^{-1} =$

$= h_1^{-1} \Rightarrow h_1^{-1} \in \mathrm{Imm}\,\varphi.$

$\boxtimes$

Teorema Data $\varphi : G_1 \to G_2$ omomorfismo,

$\underset{(1)}{\varphi \text{ iniettiva}} \Longleftrightarrow \underset{(2)}{\ker\varphi} = \{e_1\}$

Dimostrazione

$(1) \Rightarrow (2)$ $\varphi(e_1) = e_2$. Poiché φ iniettiva, $\nexists\, g \neq e_1 \mid \varphi(g) = e_2 \rightarrow \ker\varphi = \{e_1\}$

$(2) \Rightarrow (1)$ Se φ non fosse iniettiva, $\exists\, g_1 \neq g_2 \mid \varphi(g_1) = \varphi(g_2)$.
Allora $\varphi(g_1^{-1} g_2) = \varphi(g_1)^{-1}\varphi(g_2) = e_2 \Rightarrow$
$\Rightarrow g_1^{-1} g_2 \in \ker\varphi \rightarrow g_1^{-1} g_2 = e_1 \rightarrow g_1 = g_2;$
che è un assurdo.

$\boxtimes$

Coniugio in un gruppo

Sia G un gruppo e sia fissato un $g \in G$.

$$C_g : G \to G \qquad \underbrace{x \mapsto g x g^{-1}}_{\text{def.}}$$

$$C_g(xy) = g x y g^{-1} = g x \underbrace{g^{-1} g}_{e_1} y g^{-1} = \underbrace{C_g(x)\, C_g(y)}_{\text{OMOMORFISMO}}$$

OSS. per G abeliano, $C_g : x \mapsto g x g^{-1} =$
$= g g^{-1} x = x \quad (= \mathrm{Id}_G)$

OMOMORFISMO

OSS. per G abeliano, $C_g : x \mapsto gxg^{-1} =$
$= gg^{-1}x = x \ (= Id_g)$.

es. In S_3, con $g = (1,2,3)$

$$C_g : x \longmapsto \underbrace{(1,2,3)}_{g}\, x\, \underbrace{(1,3,2)}_{g^{-1}}$$

$$C_g((1,2)) = (1)(2,3) = (2,3)$$

Automorfismi e isomorfismi

Def. Si dice che un omomorfismo $\varphi : G_1 \to G_2$ è un ISOMORFISMO tra G_1 e G_2 quando φ è bigettiva. In tal caso si dice che G_1 e G_2 sono isomorfi e si scrive:

$$G_1 \cong G_2$$

OSS. Due gruppi finiti di cardinalità distinte NON ammettono isomorfismi.

es. $(g) \cong \mathbb{Z}_{o(g)}$

Infatti $\varphi : (g) \to \mathbb{Z}_{o(g)}$, $\underset{0 \le k < o(g)}{g^k \mapsto k}$ si può dimostrare bigettiva.

Poiché $|\mathbb{Z}_{o(g)}| = card\,(g)$, è sufficiente dimostrare che φ sia iniettiva:

$$k_1 = k_2 \implies g^{k_1} = g^{k_2}.$$

$\boxtimes$

Def. Un isomorfismo da G in sé stesso si dice AUTOMORFISMO. Si indica con $Aut(G)$ l'insieme di tutti gli si dice AUTOMORFISMO. Si indica con $Aut(G)$ l'insieme di tutti gli automorfismi di G.

Prop. $(Aut(G), \circ)$ è un gruppo

Dimostrazione

- la composizione di funzioni è associativa.
- Id_G è l'automorfismo identità
- $\forall f \in Aut(G), \exists f^{-1} \in Aut(G) \mid f \circ f^{-1} = Id_G$. Infatti l'inversa di un automorfismo è un automorfismo. $\boxtimes$