

Def. (Omorfismo tra gruppi):

Dati  $G_1, G_2$  gruppi,  $f: G_1 \rightarrow G_2$  si dice **OMORFISMO** se  $\forall a, b \in G_1 \quad f(ab) = f(a)f(b)$

es.)

1)  $G_1 = (\mathbb{R}, +)$ ,  $G_2 = (\mathbb{C} \setminus \{0\}, \cdot)$

$$\Rightarrow f(x) = \cos(2\pi x) + i \sin(2\pi x) \Rightarrow f(x+y) = f(x) \cdot f(y)$$

$\Rightarrow f$  è un omorfismo.

2) Dato  $g \in G$ , definiamo:

$$\begin{aligned} t_g: G &\longrightarrow G \\ x &\longmapsto g \times g^{-1} \end{aligned} \Rightarrow t_g(x) t_g(y) = \begin{array}{c} | \\ g \times g^{-1} g \times g^{-1} \\ = \\ g \times y \times g^{-1} \\ = \\ t_g(xy) \end{array}$$

$\Rightarrow t_g$  è unomorfismo.

2.1) Dati:

$$G = S_3, \quad g = (12) \Rightarrow t_{(12)}(x) = (12) \times (12)^{-1}$$

$$\Rightarrow \text{es. } x = (123) \Rightarrow t_{(12)}((123)) = \begin{array}{c} | \\ (12)(123)(12)^{-1} \\ = \\ (12)(123)(12) \\ = \\ (132) \end{array}$$

esercizio:

Dim. che  $t_g$  è biiettiva (N.B. basta trovare l'inversa  $t_g^{-1}$ )

Studiamo ora gli omorfismi e le loro azioni sugli elementi di  $G_1, G_2$ :

### Proposizione:

Dato  $f: G_1 \rightarrow G_2$  omomorfismo, si ha:

1)  $f(1) = 1 \in G_2$  (con  $1 \in G_1$ )

2)  $f(a^{-1}) = f(a)^{-1} \quad \forall a \in G_1$

### Dim.

1)  $f(1) = f(1 \cdot 1) = f(1)f(1) \Rightarrow [x = x \cdot x \Leftrightarrow xx^{-1} = xxxx^{-1}$   
 $\Leftrightarrow x = 1] \Rightarrow f(1) = 1$

2)  $f(a)f(a^{-1}) = f(aa^{-1}) = f(1) = 1 \Leftrightarrow f(a^{-1}) = f(a)^{-1}$

q.e.d.

### N.B.

In generale, per  $f$  omomorfismo, si ha  $f(a^n) = f(a)^n$   
(Dim. per induzione su  $n$ )

### N.B.

Sia  $f: X \rightarrow Y$ . Dato  $A \subseteq X$  si denota:

$$f^{\rightarrow}(A) = \{f(x) \mid x \in A\} = \{y \in Y \mid \exists x \in X \text{ t.c. } y = f(x)\}$$

e spesso si indica con  $f(A)$ . Dato  $B \subseteq Y$  si denota:

$$f^{\leftarrow}(B) = \{x \in X \mid f(x) \in B\} \text{ e spesso si indica con } f^{-1}(B)$$

### Proposizione:

Dati  $f: G_1 \rightarrow G_2$  omomorfismo,  $A \subseteq G_1$ ,  $B \subseteq G_2$

sottogruppi, si ha:

1)  $f^{\rightarrow}(A)$  è sottogruppo di  $G_2$

2)  $f^{\leftarrow}(B)$  è sottogruppo di  $G_1$

Dim.:

$$1) f^{-\rightarrow}(A) \neq \emptyset \Rightarrow x, y \in f^{-\rightarrow}(A) \Leftrightarrow \exists a, b \in A \text{ t.c.}$$

$$f(a) = x \wedge f(b) = y$$

$$\Rightarrow xy^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in f^{-\rightarrow}(A)$$

$$2) f^{-\leftarrow}(B) \neq \emptyset \quad (f(1) = 1 \in B \Rightarrow 1 \in f^{-\leftarrow}(B))$$

$$\Rightarrow a, b \in f^{-\leftarrow}(B) \Rightarrow f(a b^{-1}) = f(a)f(b^{-1}) = f(a) \underset{\cap B}{f(b)} = f(a) \underset{\cap B}{f(b)^{-1}}$$

$$\Rightarrow f(a b^{-1}) \in B$$

q.e.d.

N.B.

Casi particolari della proposizione:

•  $f^{-\leftarrow}(\{1\}) = \text{Ker } f$  è il **Nucleo di  $f$  (Kernel)**

Lemme:

Dati  $f : G_1 \rightarrow G_2$  omomorfismo,  $a, b \in G_1$  si ha:

$$f(a) = f(b) \Leftrightarrow ab^{-1} \in \text{Ker } f$$

Dim.:

$$\Rightarrow f(a) = f(b) \Leftrightarrow f(a)f(b)^{-1} = f(b)f(b)^{-1}$$

$$\Leftrightarrow f(ab^{-1}) = 1 \Leftrightarrow ab^{-1} \in \text{Ker } f$$

$$\Leftarrow ab^{-1} \in \text{Ker } f \Leftrightarrow f(ab^{-1}) = 1 \Leftrightarrow f(a)f(b^{-1}) = 1$$

$$\Leftrightarrow f(a)f(b)^{-1} = 1 \Rightarrow f(a) = f(b)$$

q.e.d.

Proposizione:

Data  $f : G_1 \rightarrow G_2$  omomorfismo, si ha:

$$f \text{ iniettiva} \Leftrightarrow \text{Ker } f = \{1\}$$

Dim:

$$\Rightarrow a \in \text{Ker } f \Rightarrow f(a) = 1 = f(1) \Rightarrow a = 1$$

$$\Leftarrow f(a) = f(1) \Rightarrow ab^{-1} \in \text{Ker } f \Rightarrow ab^{-1} = 1 \Rightarrow a = b$$

q.e.d.

Teorema:

Dati  $G$  gruppo,  $H \subseteq G$  sottogruppo, si ha che le seguenti affermazioni sono equivalenti:

$$1) gH = Hg \quad \forall g \in G$$

$$2) gHg^{-1} = H \quad \forall g \in G$$

$$3) gHg^{-1} \subseteq H \quad \forall g \in G$$

$$4) ghg^{-1} \in H \quad \forall g \in G, h \in H$$

$$5) \sim_H, \sim_H \text{ sono uguali}$$

Ricordiamo che  $gH = \{gh \mid h \in H\}$ ,  $Hg = \{hg \mid h \in H\}$

$\Rightarrow gH = Hg$  **NON significa**  $gh = hg \quad \forall h \in H$ !!! Bensi:

$\forall h \in H \exists h_1 \in H$  t.c.  $gh = h_1g$  (e viceversa)

Moltre:

$gHg^{-1} = \{ghg^{-1} \mid h \in H\} = \xrightarrow{t_g}(H)$  con  $t_g$  definita come sopra.

$\Rightarrow gHg^{-1} = \xrightarrow{t_g}(H) \subseteq H$  per costruzione.

Dim:

1)  $\Leftrightarrow$  2) Ovvio:

$$gH = Hg \Leftrightarrow gHg^{-1} = Hg^{-1} = H$$

1)  $\Leftrightarrow$  5) Ovvio:

$$gH = \text{lassi di equivalenza di } \sim_H$$

$$Hg = \text{lassi di equivalenza di } \sim_H$$

$$\Rightarrow g \in gH \Rightarrow gH = Hg \Rightarrow \sim_H = \sim_{\widetilde{H}}$$

3)  $\Leftrightarrow$  4) Ovvio per costruzione di  $gH$ ,  $Hg$ ,  $gHg^{-1}$ .

3)  $\Leftrightarrow$  2):

$\Rightarrow$ :  $gHg^{-1} \subseteq H \quad \forall g \in G \Rightarrow$  pseudo  $g^{-1} \in G$  e  
mentre:

$$g^{-1}H(g^{-1})^{-1} = g^{-1}Hg \subseteq H$$

$$\Rightarrow H \subseteq gHg^{-1} \Rightarrow gHg^{-1} = H \quad \forall g \in G$$

$\Leftarrow$  Ovvio (2) è "più forte" di (3)

q.e.d.

Def. (Sottogruppo Normale o Invariante):

Dati  $G, H \subseteq G$  come sopra (ovvero  $H$  sottogruppo di  $G$  t.c. valga il Teorema),  $H$  si dice SOTTOGRUPPO NORMALE o INVARIANTE.

es.

1) Se  $f: G_1 \rightarrow G_2$  è unomorfismo, allora  $\ker f$  è sottogruppo normale di  $G_1$   
 $(g \in G_1, h \in \ker f \Rightarrow f(g h g^{-1}) = f(g) f(h) f(g)^{-1} = f(g) f(g)^{-1} = 1)$

Gruppi quoziente:

Dato  $H$  sottogruppo normale di un gruppo  $G$ , si ha che

$\sim_H$  definisce una PARTIZIONE su  $G$  formata dalle classi laterali:

$$G/\sim_H = \{H\alpha \mid \alpha \in G\} = \underset{\substack{\uparrow \\ H \text{ sottogruppo NORMALE}}}{G/\sim}$$

$$\Rightarrow \text{dovremo allora } G/\sim_H = G/\sim = G/H.$$

Definiamo ora l'applicazione  $\pi: G \xrightarrow{\quad} G/H$  e un'operazione su  $G/H$  t.c.  $\pi$  sia unomorfismo.

$\Rightarrow$  deve essere necessariamente:

$$\pi(a)\pi(b) = \pi(ab) \text{ ovvero va definito}$$

$$(Ha)(Hb) = Hab$$

$\Rightarrow Ha$  potrebbe essere  $Hc$  per  $c \neq a$  e  $Hb$  potrebbe essere  $Hd$  per  $d \neq b$

$$\Rightarrow \text{allora deve essere } Hab = Hcd$$

Supponiamo  $a \sim_H c$  (cioè  $Ha = Hc$ ) e  $b \sim_H d$  (cioè  $Hb = Hd$ ), mostriamo  $Hab = Hcd$  (cioè  $ab \sim_H cd$ , ovvero  $(ab)(cd)^{-1}$  è elemento di  $H$ ):

$$\Rightarrow (ab)(cd)^{-1} = ab d^{-1} c^{-1} = \underbrace{a c^{-1} c}_{\in H} \underbrace{b d^{-1} c^{-1}}_{\in H} \in H \quad (\text{H NORMALE})$$

L'operazione  $(Ha)(Hb) = Hab$  è ben definita, verifichiamo ora che  $G/H$  sia un gruppo:

- 1)  $((Ha)(Hb))(Hc) = (Ha b)(Hc) = H(a b)c = Ha(b c)$   
 $= (Ha)(Hb c) = (Ha)((Hb)(Hc))$  (associatività ✓)
- 2)  $H1 = H$  ( $\exists$  elemento neutro)

$$3) (Ha)(Ha^{-1}) = Ha^{-1} = H \cdot 1 = H \quad (\exists \text{ elemento inverso})$$

$$(Ha^{-1})(Ha) = Ha^{-1}a = H \cdot 1 = H$$

$\Rightarrow G/H$  è un gruppo e  $\pi: G \rightarrow G/H$  è un omomorfismo,  
inoltre si ha che  $\ker \pi = H$

Abbiamo quindi verificato che i sottogruppi normali sono  
esattamente TUTTI e SOLI i nuclei di omomorfismi.

es.)

1) Nell'esempio iniziale si ha:

$$f(x) = \cos(2\pi x) + i \sin(2\pi x) \Rightarrow \ker f = \mathbb{Z}$$

(infatti deve essere:

$$f(x) = 1 \Leftrightarrow \begin{cases} \cos 2\pi x = 1 \\ \sin 2\pi x = 0 \end{cases} \Leftrightarrow x = k \in \mathbb{Z}$$

2) Dato  $n > 0 \in \mathbb{Z}$ , chi è  $\mathbb{Z}/n\mathbb{Z}$ ?

$a \sim_{n\mathbb{Z}} b \Leftrightarrow a - b \in n\mathbb{Z} \Leftrightarrow n \mid (a - b) \Leftrightarrow a, b$  hanno  
lo stesso resto nella divisione per  $n$ , ovvero:

$$a \equiv b \pmod{n}$$

I resti possibili sono  $0, 1, \dots, n-1$ , quindi:

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

dove  $[x]_n = \begin{cases} \text{classe di equivalenza di } x \text{ rispetto} \\ a \sim_{n\mathbb{Z}}, \text{ ovvero la congruenza mod } n \\ = x + n\mathbb{Z} \end{cases}$

$\Rightarrow$  si ha che  $\mathbb{Z}/n\mathbb{Z}$  è ciclico !!!

$$[x]_n + [y]_n = [x+y]_n$$

infatti:

$$(x + u\mathbb{Z}) + (y + u\mathbb{Z}) = (x+y) + u\mathbb{Z}$$

e:

$$u[x]_u = [ux]_u$$

In particolare:

$$[x]_u = [x \cdot 1]_u = x[1]_u$$

e quindi:

$$\mathbb{Z}/u\mathbb{Z} = \langle [1]_u \rangle$$

3) esempio banale:

data  $G$ ,  $\{1\}$  è sottogruppo normale di  $G$  e si ha:

$\pi: G \rightarrow G/\{1\}$  suriettiva con nucleo  $\{1\}$ , quindi iniettiva

Def. (Isomorfismo):

Dati  $G_1, G_2$  gruppi,  $f: G_1 \rightarrow G_2$  si dice ISOMORFISMO se è un omomorfismo biettivo ( $f$  è iniettiva e suriettiva)

N.B.

Data  $f$  isomorfismo,  $\exists f^{-1}$  anch' essa isomorfismo, infatti:

$$x, y \in G_2 \Rightarrow f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(x))f(f^{-1}(y)) \\ = xy = f(f^{-1}(xy))$$

oppure:

$$x, y \in G_2 \Rightarrow x = f(a), y = f(b) \text{ con } a, b \in G_1$$

$$\Rightarrow f^{-1}(x)f^{-1}(y) = f^{-1}(f(a))f^{-1}(f(b)) = ab$$

$$\Rightarrow f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab$$

$$\Rightarrow f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$$

es. (Isomorfismo interessante):

1) Siamo  $(\mathbb{R}_{>0}, \cdot)$ , ( $\mathbb{U} = \{z \in \mathbb{C} \mid |z|=1\}$ ,  $\cdot$ ). Definiamo  
 $f : \mathbb{R}_{>0} \times \mathbb{U} \rightarrow \mathbb{C} \setminus \{0\}$  (scrittura dei complessi)  
 $(r, u) \mapsto ru$  in forma trigonometrica)  
 $\Rightarrow f$  è un isomorfismo (la scrittura trigonometrica di un numero complesso è univoca).

2)  $f = \log : (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$  è un isomorfismo (per qualunque base):  $\log(ab) = \log a + \log b$

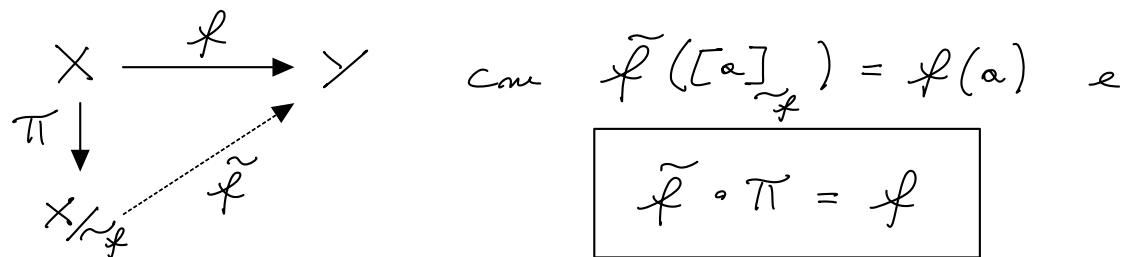
---

Sia  $f : X \rightarrow Y$  applicazione tra insiemi (qualsiasi).

Definiamo, per  $a, b \in X$ , la relazione:

$$a \sim_f b \Leftrightarrow a = b \vee f(a) = f(b)$$

$\Rightarrow \sim_f$  è relazione di equivalenza, consideriamo quindi  $X/\sim_f$ :



$\Rightarrow \tilde{f}$  è iniettiva:

$$\tilde{f}([\alpha]) = \tilde{f}([b]) \Leftrightarrow f(\alpha) = f(b) \Leftrightarrow \alpha \sim_f b$$

$$\Leftrightarrow [\alpha] = [b]$$

$\Rightarrow \pi$  è suriettiva (vista prima)

$\Rightarrow$  si ha che  $f$  (isomorfismo) è composizione di una funzione iniettiva dopo una funzione suriettiva.