# GRUPPI

Note Title 11/15/2017

FATTO ESSENZIALE

$f: G \longrightarrow H$ omomorfismo di gruppi

$$f(g_1 \cdot_G g_2) = f(g_1) \cdot_H f(g_2)$$

$f$ iniettiva $\iff \ker f = \{id_G\}$

Dim $f(g_1) = f(g_2) \iff f(g_1) \cdot_H \underbrace{f(g_2)^{-1}}_{f(g_2^{-1})} = id_H$

$\iff f(g_1) \cdot_H f(g_2^{-1}) = id_H$

$\iff f(g_1 \cdot_G g_2^{-1}) = id_H$

$\iff \boxed{g_1 \cdot_G g_2^{-1} \in \ker(f)}$

$\iff$ "$g_1, g_2$ appartengono alla stessa classe laterale rispetto a $\ker(f)$"

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

Se $\ker f = \{id_G\}$, $\square \Rightarrow g_1 \cdot g_2^{-1} = id_G$

$\Rightarrow g_1 = g_2$

Se invece $\ker f \neq \{id_G\}$, sia $g \in \ker f \setminus \{id_G\}$:

allora $f(id_G) = id_H = f(g)$

nonostante $g \neq id_H$, e quindi $f$ non è iniettiva.

Oss: un omomorfismo manda inversi in inversi

$$f(g^{-1})\, f(g) = f(id_G) = id_H$$

$$f(g)^{-1} \cdot f(g) = id_H$$

Sottogruppi Se $G$ è un gruppo **finito** e $H \subseteq G$ è un sottoinsieme NON VUOTO t.c.

$$h_1 \in H,\ h_2 \in H \Rightarrow h_1 \circ_G h_2 \in H$$

allora $H$ è un sottogruppo

⚠ $G = \mathbb{Z}$ $H = \{\text{positivi}\} \Rightarrow H$ **NON** è un sottogruppo

Dim $h \in H$. Allora $h \cdot h \in H$, $h \cdot h \cdot h \in H$, ...

$\forall n$ $h^n \in H$. Ma siccome $G$ è finito,

$h^{|G|} = id_G$. Quindi in particolare:

$$H \ni h^{|G|} = id_G, \quad H \ni h^{|G|-1}$$

e $\underbrace{\left(h^{|G|-1}\right)}_{h^{-1}} \cdot h = h^{|G|} = id_G$

$h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H$

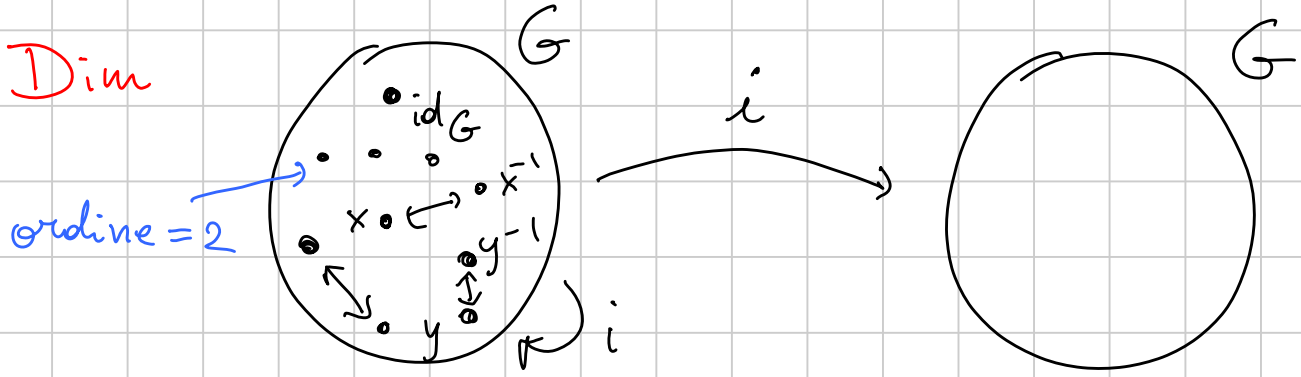
$H$ è stabile per $h \mapsto h^{-1}$ e prodotto, e $H \ni id$, quindi $H$ è un sottogruppo

$h \in H \Rightarrow h^{-1} \in H$

**Esercizio** Sia $G$ un gruppo finito, $|G|$ pari.

Allora $\#\{g \in G \mid ord(g) = 2\}$ è dispari

**Dim**




$i : G \to G$ è una bigezione, con punti fissi ($i(x) = x$) l'identità e gli elementi di ordine 2

$$|G| = \underbrace{1}_{\text{identità}} + \#\{g \mid g^{-1} = g,\ g \neq id_G\} +$$

NUMERO PARI

tutti gli altri elementi compaiono a coppie $\{x, x^{-1}\}$

Modulo 2, $0 \equiv 1 + \underbrace{\#\{g \mid \text{ord}(g)=2\}}_{\text{dispari}}$ (2)

**Corollario** $|G|$ pari $\Rightarrow$ $G$ contiene un elemento di ordine 2

($\#\{g \mid \text{ord}(g)=2\}$ dispari $\Rightarrow \neq 0$)

## Gruppi di ordine 6

$|G|=6$ $\quad\quad$ $\mathbb{Z}/6\mathbb{Z}$

Guardiamo gli ordini. Sia $g \in G$, $g \neq id_G$

$\text{ord}(g) \in \{2, 3, 6\}$

* se $\text{ord}(g)=6$, $\quad id, g, g^2, g^3, g^4, g^5$

distinti $\Rightarrow$ $G \simeq \mathbb{Z}/6\mathbb{Z}$

* se $\nexists\, g \in G$ di ordine 6, vuol dire che ogni elemento ha ordine 2 o 3

$\neq id_G$

Supponiamo siano tutti di ordine 2.

$\{id, a, b, a+b\}$ è un

sottogruppo, ma questo è assurdo per Lagrange ($4 \nmid 6$)

( Sia $G$ finito t.c. $g^2 = id_G \ \forall g \in G$.

Allora $G$ è abeliano, ed è uno spazio vettoriale su $\mathbb{Z}/2\mathbb{Z} \Rightarrow |G|$ = potenza di 2)
$G \simeq (\mathbb{Z}/2\mathbb{Z})^n$

* Quindi possiamo supporre $\exists\, g \in G,\ h \in G$ con $ord(g) = 3$ e $ord(h) = 2$

| $\mathbb{Z}/3\mathbb{Z}$ | | | |
|---|---|---|---|
| $\mathbb{Z}/2\mathbb{Z}$ | $id_G$ | $g$ | $g^2$ ← sottogruppo $K$ |
| | $h$ | $hg$ | $hg^2$ ← classe laterale di $h$ risp. a $K$ |

( Se $g^2 = h \Rightarrow g^4 = h^2 = id_G$, ma $ord(g) = 3$ )

Sono tutti distinti: se $g^i = h \cdot g^j$

$\Rightarrow g^{i-j} = h \Rightarrow id = h^2 = g^{2(i-j)}$

$\Rightarrow 3 \mid 2(i-j) \Rightarrow 3 \mid i-j \Rightarrow i = j$

$|i-j| < 3$

Ma allora $g^i = h \cdot g^i \Rightarrow h = id$, assurdo.

La tabella di moltiplicazione è determinata da $g \cdot h \in \{id, g, g^2, hg, hg^2, h\}$

- $id$: altrimenti $h = g^{-1} = g^2$
- $g$: altrimenti $h = id$
- $g^2$: altrimenti $g = h$
- $h$: altrimenti $g \cdot h = h \Rightarrow g \cdot h \cdot h^{-1} = h \cdot h^{-1} \Rightarrow g = id$

Se $g \cdot h = h \cdot g$, allora

$$hg^i \cdot hg^j = h\underbrace{g \dots g}_{i} h \underbrace{g \dots g}_{j}$$

$$= hh\, g^i g^j = g^{i+j}$$

e similmente si calcola $g^i \cdot hg^j = hg^{i+j}$

Ma allora $G \simeq \mathbb{Z}/6\mathbb{Z}$, con un generatore dato da $g \cdot h$

$$(gh)^2 = ghgh = ghhg = g \cdot id \cdot g = g^2$$

$$(gh)^3 = ghghgh = g\,gh\,hgh = ggggh = h$$

$\Rightarrow \text{ord}(gh) \in \{1, 2, 3, 6\}$

Chi è l'altro gruppo di ordine 6?

$g, h$ con $g^3 = h^2 = id_G$, $gh = hg^2$

- $S_3 = \{\text{permutazioni su 3 elementi}\}$

$$= \left\{ id, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \right\}$$

$h = (1 \leftrightarrow 2)$ $\qquad$ $g = \begin{pmatrix}1 \to 2\\ \uparrow \quad \swarrow\\ 3\end{pmatrix}$

$h^2 = id$ $\qquad$ $g^3 = id$

$gh = hg^2$

$g \circ h$ :

$$\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \ h \\ 2 & 1 & 3 \\ \downarrow & \downarrow & \downarrow \ g \\ 3 & 2 & 1 \end{array}$$

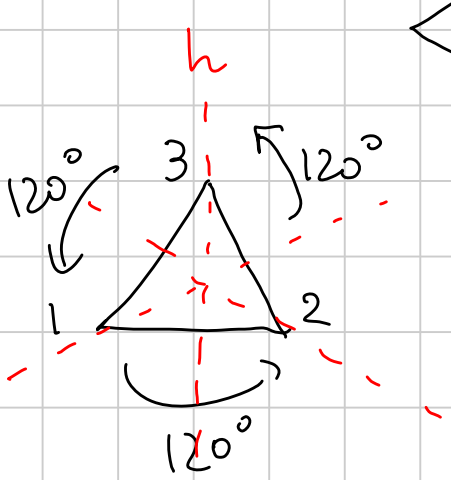
$h \circ g^2$ :

$$\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \ g^2 \\ 3 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \ h \\ 3 & 2 & 1 \end{array}$$

Sono la stessa permutazione:

$gh = hg^2$

- $D_3 = \{$ isometrie del piano che mandano $\triangleleft$ in sé $\}$




$g$ = rotaz. di $120°$

$h$ = simmetria $\longleftrightarrow$

$g^3 = id \qquad h^2 = id$

$$gh = hg^2$$

**Def** $S_n = \{ f : \{1, \dots, n\} \to \{1, \dots, n\}$ bigettive $\}$

$D_n = \{$ isometrie dell'$n$-agono regolare $\}$

$|D_n| = 2n$, $n$ rotazioni + $n$ simmetrie

$|S_n| = n!$

**Omomorfismi vari** $m, n$ interi positivi

$G_1 = \mathbb{Z}/m\mathbb{Z} \qquad G_2 = \mathbb{Z}/n\mathbb{Z} \qquad G_3 = \mathbb{Z}$

$\mathrm{Hom}(G_1, G_3) = \{ f : G_1 \to G_3$ omomorf. $\}$

Sia $f : G_1 \longrightarrow G_3$ omomorfismo.

Se $f([1]) = a$, allora

$$f([3]) = f([1]+[1]+[1])$$

$$= f([1]) + f([1]) + f([1])$$

$$= 3\, f([1]) = 3a$$

$$f([0]) = f([m]) = m\, f([1]) = m \cdot a$$

$[0] = 0$ ← $f(id_{G_1}) = id_{G_3}$

$$\Rightarrow \quad a = 0 \quad \Rightarrow \quad f([k]) = k\, f([1]) = ka = 0$$

$$\mathrm{Hom}(G_1, G_3) = \{0\}$$

↑ l'applicazione che manda ogni elem. in zero

Consideriamo ora $\mathrm{Hom}(\mathbb{Z}, G_1)$

Sia $b \in G_1$ l'immagine di $1$ ( $b = f(1)$ )

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

**Fatto** Se $f: G \to H$ è un omomorf. di gruppi, $f(g^n) = f(g)^n \quad \forall n \in \mathbb{Z}$

INDUZIONE

$$f(n \cdot g) = n \cdot f(g)$$

Se $f: \mathbb{Z} \to G_1$ è un omomorf,

$$f(n) = nb = \underbrace{b+b+\dots+b}_{n \text{ volte}}$$

① $f$ è univocamente determ. da $f(1) \in G_1$

② Dato $b \in G_1$, $\exists$ un omomorf.

$$f_b : \mathbb{Z} \longrightarrow G_1$$

t.c. $f_b(1) = b$

Tale $f_b$ è dato da $f_b(k) = [kb]$;

è un omomorfismo, infatti:

$$f_b(0) = [0] = id_{G_1}$$

$\forall k_1, k_2 \in \mathbb{Z}$ $f_b(k_1+k_2) = [(k_1+k_2)b]$

$$= [k_1 b] + [k_2 b]$$

$$= f_b(k_1) + f_b(k_2)$$

$\mathrm{Hom}(\mathbb{Z}, G_1)$ è in bigezione con $G_1$

$(f_b \longleftrightarrow b)$

# Determiniamo ora $\mathrm{Hom}(G_1, G_2)$

$G_1 = \langle [1] \rangle$ Sia $f: G_1 \to G_2$ un omom.,

allora $f([k]) = f(\underbrace{[1] + \dots + [1]}_{k>0}) =$

$= f([1]) + \dots + f([1]) = k f([1])$

Come prima, $f$ è determinato da $f([1])$

Quali $f([1])$ determinano effettivamente un omom?

$$m f([1]) = f([m]) = f([0]) = [0]$$

Condizione necessaria: $m \underbrace{f([1])}_{a} = 0$ in $\mathbb{Z}/n\mathbb{Z}$

$$\iff a \equiv 0 \left( \mathrm{mod}\ \frac{n}{(m,n)} \right)$$

Vogliamo vedere se è anche condiz. sufficiente.

Dato $a \in \mathbb{Z}/n\mathbb{Z}$ t.c. $a \equiv 0 \left( \frac{n}{(m,n)} \right)$,

sia $f_a : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

dato da $f_a([k]) = [ka]$

Affinché questa sia una buona definizione serve che $k \equiv k' \mod m$ implichi

$$ka \equiv k'a \mod n$$

Ora: $k \equiv k' \pmod m \Rightarrow k' = k + mt$ per un qualche $t \in \mathbb{Z}$

$$\Rightarrow k'a = ka + \underbrace{mat}$$

per ipotesi su $a$, questo è $\equiv 0 \ (n)$

$$\Rightarrow [k'a] = [ka] \text{ in } \mathbb{Z}/n\mathbb{Z}$$

Quindi $f_a$ è ben definita

Inoltre è un omomorfismo:

$$f_a([k_1] + [k_2]) = f_a([k_1]) + f_a([k_2])$$

$$\Leftrightarrow \quad a(k_1 + k_2) \equiv a \cdot k_1 + a \cdot k_2 \ (n)$$

Conclusione: $\#\,\mathrm{Hom}(G_1, G_2) =$ numero delle possibili scelte di $a$ =

$$= \#\left\{ a \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; a \equiv 0 \left( \frac{n}{(m,n)} \right) \right\} = \frac{n}{n/(m,n)} = (m,n)$$