I Teorema di Omomorfismo

Note Title 11/16/2017

$f : G \longrightarrow H$ omomorfismo

$\ker f = \{ id_G \} \iff f$ è iniettivo

$\ker f$ è un sottogruppo normale di G

Se K è un sottogr. norm. di G, l'insieme

$$G/K = \{ \text{classi lat. di } K \text{ in } G \}$$

è un gruppo con l'operazione

$$(aK) \cdot (bK) = abK$$

Teorema G, H gruppi, $f : G \to H$ omomorf.

(i) se K è un sottogr. normale di G e

$K \subseteq \ker f$,

allora esiste un unico omomorfismo di gruppi $f_K : G/K \longrightarrow H$ t.c.

$f = f_K \circ \pi$ e $\operatorname{Im} f_K = \operatorname{Im} f$

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/K \arrow[ur, "f_K"'] & \end{tikzcd}$$

"passa al quoziente per K"

"f fattorizza tramite G/K"

(ii) Scegliendo $K = \ker f$ abbiamo un omomorfismo $f_{\ker f} : G/_{\ker f} \longrightarrow H$.

$f_{\ker f}$ è iniettivo

In particolare, $\operatorname{Im}(f) \simeq G/_{\ker f}$

Dimostrazione

(i) $(*)$ $f = f_K \circ \pi$ VOGLIO

Un elemento di $G/_K$ è della forma gK, in particolare è della forma $\pi(g)$

(infatti $\pi : G \longrightarrow G/_K$ è definita essere $\pi(g) = gK$)

Calcolando i due membri di $(*)$ in g

trovo $f(g) = f_K(gK) \quad \forall g \in G$

Questo ci costringe a definire:

$$f_K(gK) = f(g)$$

Problema Bisogna verificare che $f_K(gK)$ non dipenda dal rappresentante scelto, ovvero: se $gK = g'K$, allora deve valere $f_K(gK) = f_K(g'K)$

(In $\mathbb{Z}/m\mathbb{Z}$ $\quad [0] = [m]$

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z} \\ [i] &\longmapsto i \end{aligned}$$

NON E' UNA FUNZIONE)

Le classi gK e $g'K$ sono uguali

$\Longleftrightarrow \{gh \mid h \in K\} = \{g'h \mid h \in K\}$

$\Longrightarrow \exists h \in K : \underset{\cup}{g} = g'h$

(è vero anche il viceversa: se $g = g'h$, $h \in K$, allora $gK = g'K$. Infatti:

$$gK = g' \underbrace{hK}_{K} = g'K)$$

Ci siamo ridotti a verificare che

$$gK = g'K \overset{?}{\Longrightarrow} f(g) = f(g')$$

$$\Updownarrow$$

$$\exists h \in K \text{ t.c. } g = g'h \overset{?}{\Longrightarrow} f(g) = f(g')$$

Infatti $f(g') = f(gh) = f(g)f(h)$

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

$$= f(g)$$

ipotesi: $K \subseteq \ker f$

La definizione $f_K(gK) = f(g)$ e'

quindi ben posta

Ora bisogna verificare che $f_K : G/K \to H$

sia un omomorf. di gruppi, ovvero che

$\forall\, aK, bK$

$$f_K((aK)(bK)) \overset{?}{=} f_K(aK)\, f_K(bK)$$

$$\quad\; \| \qquad\qquad\qquad\qquad \|$$

$$\begin{array}{ccc} \parallel & & \\ f_K(abK) & = f(ab) & \parallel \\ & & f(a)\cdot f(b) \end{array}$$

$f(ab)$ e $f(a)\,f(b)$ sono uguali perché f è un omomorfismo.

Infine, $\operatorname{Im}(f_K) = \operatorname{Im}(f)$ perché π è surgettiva

$$f = f_K \circ \pi$$

- $\operatorname{Im} f \subseteq \operatorname{Im} f_K$: $\quad y \in \operatorname{Im} f \Rightarrow \exists\, x \in G$ t.c. $y = f(x) = f_K(\pi(x)) \Rightarrow y \in \operatorname{Im} f_K$
- $\operatorname{Im} f \supseteq \operatorname{Im} f_K$: $\quad y \in \operatorname{Im} f_K \Rightarrow \exists\, \bar{x} \in G/K$ t.c. $f_K(\bar{x}) = y$. Siccome
$$\pi : G \longrightarrow G/K$$
è surgettiva, $\exists\, x \in G$ t.c. $\pi(x) = \bar{x}$
$$\Rightarrow y = f_K(\bar{x}) = f_K(\pi(x)) = f(x)$$
$$\Rightarrow y \in \operatorname{Im} f$$

(ii) Scelgo $K = \ker f$, ottengo

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/\ker f \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Voglio dimostrare che $\bar{f}$ è iniettiva.

Sia $aK \in \ker(\bar{f})$.

$$id_H = \bar{f}(aK) = f(a)$$

$\Rightarrow a \in \ker f \Rightarrow aK = a(\ker f) = id_G \cdot K$

ovvero $aK = id_{G/\ker f}$

Quindi $\ker \bar{f} = \{ id_{G/\ker f} \} \Rightarrow \bar{f}$ iniettiva

In particolare $\bar{f} : G/\ker f \longrightarrow \mathrm{Im}\, \bar{f} = \mathrm{Im}\, f$

è un isomorfismo di gruppi (perché è sia iniettiva che surgettiva) $\square$

ESEMPI

- Gruppi ciclici "fatti bene"

G gruppo, $g \in G$ elemento di ordine n

Allora $\langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

Infatti: (da ieri) esiste un omomorfismo

$$f : \mathbb{Z} \longrightarrow G$$
$$1 \longmapsto g$$

$$f(m) = f(\underbrace{1+1+\dots+1}_{m \text{ volte}}) = f(1)\cdot f(1)\cdot\ldots\cdot f(1)$$
$$= g^m$$

$$\ker(f) = \{m \mid g^m = id_G\} = (\text{ord } g)\cdot \mathbb{Z}$$
$$= n\mathbb{Z}$$

$$\text{Im}(f) = \langle g \rangle = \{\text{potenze di } g \text{ in } G\}$$

Applico il I teo di omomorfismo:

$$\text{Im } f = \langle g \rangle \simeq \mathbb{Z}/\ker f \simeq \mathbb{Z}/n\mathbb{Z}$$

- Non e' vero che $G \simeq G/H \times H$

Per esempio: sia $G = \mathbb{Z}/4\mathbb{Z}$

$$H = \{[0],[2]\} \triangleleft G$$

Oss Se G e' abeliano, OGNI sottogruppo H e' normale. Devo verificare $\forall g \in G$ valga

$$\underset{\{gh \mid h \in H\}}{\underset{\shortparallel}{gH}} = \underset{\underset{\{gh \mid h\in H\}}{\underset{\shortparallel}{\{hg \mid h \in H\}}}}{\underset{\shortparallel}{Hg}}$$

$$G/H \simeq \mathbb{Z}/2\mathbb{Z} \qquad |G/H| = |G|/|H| = 4/2 = 2$$

$$\begin{aligned} \mathbb{Z}/4\mathbb{Z} &\xrightarrow{f} \mathbb{Z}/2\mathbb{Z} \\ [m] &\longmapsto [m] \end{aligned}$$

$$\mathrm{Im}\, f = \mathbb{Z}/2\mathbb{Z} \qquad \ker f = \{[0],[2]\} = H$$

$$\xRightarrow{\text{I teo}} \quad \frac{\mathbb{Z}/4\mathbb{Z}}{\ker f} \simeq \mathrm{Im}\, f = \mathbb{Z}/2\mathbb{Z}$$

$$G \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = G/H \times H$$

$\mathbb{Z}/4\mathbb{Z}$ $\uparrow$ contiene un elemento di ordine 4

$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ $\uparrow$ tutti gli elementi hanno ordine ≤ 2

- $G = \mathbb{Z}^2$ $\quad f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$, $(x,y) \longmapsto ax+by$ omomorfismo

con $(a,b) = 1$

$$\operatorname{Im} f = \mathbb{Z}$$

$$\left[\ a(x_1+x_2)+b(y_1+y_2) = (ax_1+by_1)+(ax_2+by_2)\ \right]$$

$$\ker f = \{(x,y) \mid ax+by=0\}$$

$$= \{(x,y) \mid ax = -by\}$$

$$= \left\{(x,y) \;\middle|\; \begin{matrix} x = kb \\ y = ha \end{matrix} \quad ax+by=0\right\}$$

$$= \left\{(x,y) \;\middle|\; \begin{matrix} x = kb \\ y = -ha \end{matrix} \quad k = h\right\}$$

$$= \langle (b,-a) \rangle$$

$$\mathbb{Z}^2 / \langle (b,-a) \rangle \simeq \mathbb{Z} \quad \text{(I teo omom.)}$$

$$\begin{tikzcd}
\mathbb{Z}^2 \arrow[rr, "f"] \arrow[dr, "\pi"'] & & \mathbb{Z} \ni 1 \\
& \mathbb{Z}^2 / \langle (b,-a) \rangle \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

$$\{ (x,y) \mid ax+by = 1 \} = f^{-1}(\{1\})$$

$$= \pi^{-1} (\bar{f})^{-1} (1)$$

$$= (x_0, y_0) + \ker f$$

dove $f(x_0, y_0) = 1 \qquad a x_0 + b y_0 = 1$

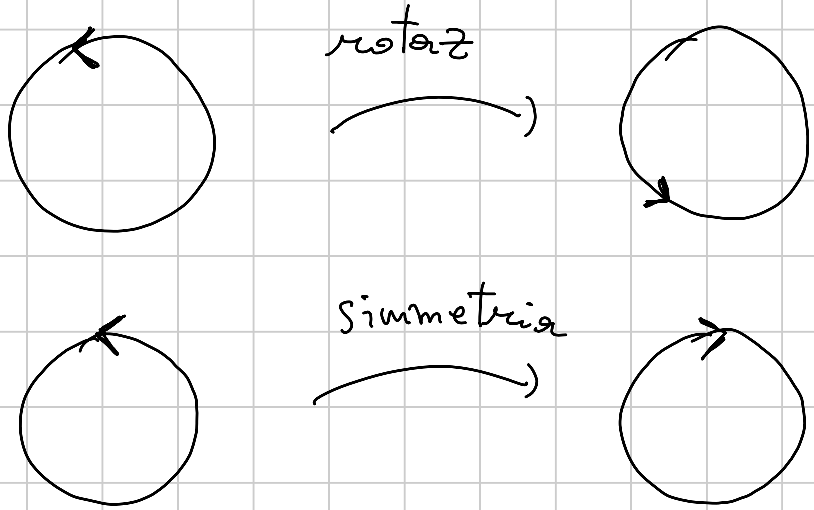
$$\ker f \simeq \{ (bk, -ak) \mid k \in \mathbb{Z} \}$$

ovvero: $f^{-1}(1) = \{ (x_0 + bk, \ y_0 - ak) \mid k \in \mathbb{Z} \}$

- $G = S_3 \simeq D_3 = \{ 1, r, r^2, s, sr, sr^2 \}$

$H = \{ 1, r, r^2 \}$ è normale

$$\begin{tikzcd}
G \arrow[rr, "\text{"segno"}"] \arrow[dr] & & \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \\
& G/H \arrow[ur, "\simeq"'] &
\end{tikzcd}$$



Esercizio G gruppo finito, $H < G$. Supponiamo

$$|G| = 2|H|.$$

Allora $H \trianglelefteq G$

Dim
- Una classe laterale di H in G ha $|H|$ elementi
- Classi laterali sono o disgiunte o coincidenti
- $H = id_G H$ e' una classe laterale
- $G = H$ unione disgiunta $G \setminus H$ e' la partizione in classi laterali (sia dx che sx)
- Dobbiamo dimostrare che $aH = Ha$ $\forall a \in G$

Se $a \in H$, $aH = H = Ha$

Se $a \notin H$ $aH \neq H \Rightarrow aH = G \setminus H$

$$\begin{array}{ccc} & & \parallel \qquad\quad \parallel \\ Ha \neq H & \Rightarrow & Ha = G \setminus H \end{array}$$

$\blacksquare$

Il caso delle rotazioni in D_3

Verifichiamo a mano che rotazioni $\triangleleft D_3$

$H = \{1, r, r^2\}$ $G = \{1, r, r^2, s, sr, sr^2\}$

$rH = Hr$ $\{r, r^2, 1\} = \{r, r^2, 1\}$

$sH \overset{?}{=} Hs$ $\{s, sr, sr^2\} = \{s, sr^2, sr\}$

$(sr)H \overset{?}{=} H(sr)$

$\Leftrightarrow s \underbrace{rHr^{-1}}_{H} = Hs$

SOTTOGRUPPI AVANTI E INDIETRO

$$f: \begin{array}{ccc} G_1 & \longrightarrow & G_2 \\ \vee & & \vee \\ H_1 & & H_2 \end{array}$$

1. $f(H_1)$ è un sottogr. di G_2? (sì)
2. $f^{-1}(H_2)$ ——— G_1? (sì)
3. Se $H_1 \triangleleft G_1$, $f(H_1) \triangleleft G_2$? (no)
4. Se $H_2 \triangleleft G_2$, $f^{-1}(H_2) \triangleleft G_1$? (sì)

La risposta a (3) è <u>NO</u>.

$G \simeq D_3$ $\quad H = \langle s \rangle = \{1, s\}$ $\quad$ H non è normale in G

$$\left(\begin{array}{c} rH = Hr \\ \{r, rs\} \neq \{r, sr\} \end{array} \right)$$

$G_1 = H$, $\quad G_2 = D_3$, $\quad f$ l'immersione

$H \triangleleft G_1$ (perché sono uguali), ma

$f(H)$ NON è normale in D_3

1. $H_1 < G_1$. $\quad f(H_1)$ è sottogruppo?

- $id_{G_2} \in f(H_1)$? Sì, $id_{G_2} = f(\underset{H_1}{\underset{\cap}{id_{G_1}}})$

- $x \in f(H_1) \overset{?}{\Longrightarrow} x^{-1} \in f(H_1)$

$\Updownarrow$

$\exists h_1 \in H_1$ t.c. $x = f(h_1)$

$$\Rightarrow x^{-1} = f(\underset{H_1}{\underset{\cap}{h_1}})^{-1} = f(\underset{H_1}{\underset{\cap}{h_1^{-1}}}) \in f(H_1)$$

- $x, y \in f(H_1)$ $\quad x = f(a) \quad y = f(b)$

con $a, b \in H_1 \Rightarrow ab \in H_1$ (H_1 sottogp)

$$\Rightarrow xy = f(a)f(b) = f(ab) \in f(H_1)$$

(4) $H_2 \triangleleft G_2$; è vero che $f^{-1}(H_2) \triangleleft G_1$?

Ovvero: $\forall a \in G_1$ vorrei

$$a \cdot f^{-1}(H_2) = f^{-1}(H_2) \cdot a$$

$$\Longleftrightarrow \quad a\, f^{-1}(H_2)\, a^{-1} = f^{-1}(H_2)$$

Prendiamo un elemento a sinistra, ovvero un elemento della forma $a g a^{-1}$ con $f(g) \in H_2$

Allora $aga^{-1} \in f^{-1}(H_2) \Longleftrightarrow$

$$f(aga^{-1}) \in H_2$$

$$\Longleftrightarrow \quad f(a)\underbrace{f(g)}_{\in H_2}f(a)^{-1} \in H_2 \quad \text{ok}$$

perché H_2 normale

$$\left(H \triangleleft G \Longleftrightarrow \forall g \in G \ \forall h \in H \quad ghg^{-1} \in H \right)$$

FINITEVI LE VERIFICHE!

Dim veloce

$$G_1 \xrightarrow{f} G_2 \xrightarrow{\pi} G_2/H_2$$

$$\ker(\pi \circ f) = f^{-1}(H_2)$$

è normale perché è un nucleo