GRUPPI: ESERCIZI

Note Title 11/22/2017

Sottogruppi normali

$f: G \longrightarrow H$ omomorfismo

$K \triangleleft H$ sottogruppo normale

Tesi: $f^{-1}(K) \triangleleft G$

$$G \xrightarrow{f} H \xrightarrow{\pi} H/K$$

$\pi \circ f$ e' un omomorfismo.

$$\ker(\pi \circ f) = \{ g \in G \mid \pi(f(g)) = e_H K \}$$

$$= \{ g \in G \mid f(g) \in K \}$$

$= f^{-1}(K)$ che e' quindi un sottogruppo normale di G

Conteggio: elementi di ordine dato in $\mathbb{Z}/n\mathbb{Z}$

$\forall d$ intero positivo calcolare

$$\#\{g \in \mathbb{Z}/n\mathbb{Z} : \operatorname{ord}(g) = d\}$$

- Se $d \nmid n$ non ci sono elementi di ordine d (teo Lagrange)

- Sia invece $d \mid n$. Scriviamo $g = [m]$.

Allora $\operatorname{ord}([m]) = d$ vuol dire:

$a[m] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$ se e solo se $d \mid a$

$$am \equiv 0 \pmod{n} \iff d \mid a$$

$$a(m,n) \cdot \frac{m}{(m,n)} \equiv 0 \pmod{n} \iff d \mid a$$

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

$$a \equiv 0 \operatorname{mod} \frac{n}{(m,n)} \iff d \mid a$$

$$\Updownarrow$$

$$\frac{n}{(m,n)} \Big| a$$

$$\operatorname{ord}([m]) = \frac{n}{(m,n)}$$

Ovvero: per contare gli elementi di ordine d $\left(= \frac{n}{(m,n)}\right)$ dobbiamo contare gli m nell'intervallo $[1, \dots, n]$ con $(m, n) = \frac{n}{d}$

Un tale m si scrive $m = \frac{n}{d} \cdot K$ con K intero e ≥ 1 ; anzi $1 \leq k \leq d$

$$\frac{n}{d} = (n, m) = \left(n, \frac{n}{d} \cdot k\right) = \frac{n}{d} (d, k)$$

Quindi: k è un intero in $[1, \dots, d]$ relativamente primo con d

$\#$ scelte per $K = \varphi(d)$

Morale:

$$\#\{\text{elementi di ordine } d\} = \begin{cases} 0, & \text{se } d \nmid n \\ \varphi(d), & \text{se } d \mid n \end{cases}$$

In particolare:

$$n = \sum_{d=1}^{n} \#\{\text{el. di ordine } d\}$$

$$= \sum_{d|n} \varphi(d)$$

Quozienti di gruppi ciclici $\left(\begin{array}{l}= \text{img di gruppi} \\ \text{ciclici tramite omom.}\end{array}\right)$

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{f} \twoheadrightarrow \operatorname{Im} f \quad \text{omomorfismo}$$

$$\operatorname{Im} f \simeq \mathbb{Z}/m\mathbb{Z}$$

$$\left(\mathbb{Z}/4\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} \quad \text{non iniettiva} \right)$$

$$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \xrightarrow{f} \operatorname{Im} f$$ è un omomorfismo

$H = \ker(f \circ \pi)$ è un sottogruppo non banale

di $\mathbb{Z}$, quindi $H = m\mathbb{Z}$ (con $m \neq 0$)

Applicando il 1° teo di omomorfismo,

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/H \simeq \operatorname{Im}(f \circ \pi) = \operatorname{Im} f$$

Sappiamo qualcosa su m? Che m divide n

$$m\mathbb{Z} = \ker(f \circ \pi) \supset \ker(\pi) = n\mathbb{Z}$$

$$n \in n\mathbb{Z} \subset m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$$

Ovvero: $n = mk$ per un certo $k \in \mathbb{Z}$

" $m \mid n$

Sul gruppo $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Sia G un gruppo. $\exists$ p primo e H, K due sottogp normali di G, distinti, di indice p, e tali che $H \cap K = \{e\}$.

Allora $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

$$\pi_1 : G \longrightarrow G/H \simeq \mathbb{Z}/p\mathbb{Z} \quad |G/H| = p$$

$$\pi_2 : G \longrightarrow G/K \simeq \mathbb{Z}/p\mathbb{Z} \quad |G/K| = p$$

Vorremmo quindi un isomorfismo

$$\varphi : G \longrightarrow G/H \times G/K$$
$$x \longmapsto (xH, xK)$$

φ e' un omomorfismo di gruppi:

$$\varphi(xy) = (xyH, xyK)$$

normalità di H, K

$$= (xHyH, xKyK)$$

$$= (xH, xK) \cdot (yH, yK)$$

$$= \varphi(x) \cdot \varphi(y)$$

Domanda: φ è iniettivo?

φ è surgettivo?

$$\ker(\varphi) = \{x \in G \mid (xH, xK) = (eH, eK)\}$$

$$= \{x \in G \mid x \in H \text{ e } x \in K\}$$

$$= H \cap K = \{e\}$$

$\varphi(G)$ è un s. gruppo di

Finora sappiamo che $\boxed{\varphi \text{ inietta } G \text{ in}}$

$$G/H \times G/K,$$

che ha cardinalità p^2.

Quindi $|G| \mid |G/H \times G/K| = p^2$, ovvero

$$|G| \in \{\cancel{1}, p, p^2\}$$

H, K sono sottogp diversi da G

Se fosse $|G| = p$ (ovvero $G \simeq \mathbb{Z}/p\mathbb{Z}$), G non avrebbe 2 sottogruppi distinti di indice p. Quindi per esclusione

$$|G| = p^2$$

e quindi φ e' surgettiva, dunque un isom.

② Determinare il n° di sottogp di G di ordine p.

Innanzitutto basta rispondere a questa domanda nel caso $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

$$F: \{g \in G \mid ord(g) = p\} \longrightarrow \{H < G : |H| = p\}$$

$$g \longmapsto \langle g \rangle$$

* F e' surgettiva
* $|F^{-1}(H)| = p-1$ "F e' $\varphi(p)$ - a - 1"

$$\#\{H < G : |H| = p\} = \frac{\#\{g \in G : ord(g) = p\}}{p-1}$$

$g \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \qquad g = (x, y)$

$x, y \in \mathbb{Z}/p\mathbb{Z}$

$$\operatorname{ord}(g) = \operatorname{mcm}(\operatorname{ord}(x), \operatorname{ord}(y))$$

$$= \begin{cases} 1 & \operatorname{ord}(x) = \operatorname{ord}(y) = 1, \text{ ovvero } (x,y) = ([0],[0]) \\ p & \text{altrimenti} \end{cases}$$

$$\#\{g \in G \mid \operatorname{ord}(g) = p\} = p^2 - 1$$

$$\#\{H < G \mid |H| = p\} = \frac{p^2-1}{p-1} = p+1$$

Sottogruppo di torsione

G = gruppo abeliano

$$H = \{g \in G \mid \operatorname{ord}(g) < +\infty\}$$

(Se $G = \mathbb{Z}$, $H = \{0\}$)

① H e' un sottogruppo di G

(a) $e \in H$: infatti $\operatorname{ord}(e) = 1 < \infty$

(b) $x, y \in H \quad \text{ord}(x) = m, \quad \text{ord}(y) = n$

Allora $mn(x+y) =$

$$= mnx + mny$$

$$= \underbrace{(x+y) + (x+y) + \dots + (x+y)}_{mn \text{ volte}}$$

G abeliano

$$= \underbrace{x + x + \dots + x}_{mn \text{ volte}} + \underbrace{y + y + \dots + y}_{mn \text{ volte}}$$

$$= n(\underbrace{x + \dots + x}_{m}) + m(\underbrace{y + \dots + y}_{n \text{ volte}})$$

$$= n \cdot e + m \cdot e = e$$

(c) $x \in H \quad \text{ord}(x) = m$

$$\underbrace{(-x) + (-x) + \dots + (-x)}_{m \text{ volte}} = -(x + \dots + x)$$

$$= -e = e$$

② Dim. che ogni elemento di G/H (con l'eccezione dell'identità) ha ordine ∞

$x \in G/H$; supponiamo $mx = e_{G/H}$

$$x = gH \Rightarrow eH = mx = (mg)H$$

ovvero: $mg \in H \Rightarrow ord(mg) = n < \infty$

In particolare $(mn)g = e_G$

$$\Rightarrow g \in H \Rightarrow x = gH = eH$$

3. Sia $f: G \longrightarrow \mathbb{Z}$ un omomorf. Allora

$\ker f \supseteq H$.

Infatti: sia $h \in H$, $ord(h) = m < \infty$.

Chi e' $f(h)$?

$$0 = f(e) = f(mh) = f(\underbrace{h + h + \dots + h}_{m \text{ volte}})$$

$$= f(h) + \dots + f(h)$$

$$= m\, f(h)$$

$\Rightarrow f(h) = 0$

4. Dim. che G/H e' isomorfo a G se e solo se $H = \{e\}$

Supponiamo che $f: G \longrightarrow G/H$ sia un isomorfismo. Allora

$$\forall g \in G \quad \operatorname{ord}(g) = \operatorname{ord}(f(g))$$

$$\forall h \in H \quad \underset{\text{finito}}{\underset{\uparrow}{\operatorname{ord}(h)}} = \underset{\text{finito}}{\underset{\uparrow}{\operatorname{ord}(f(h))}}$$

Tutti gli elem. di G/H hanno ordine ∞, tranne $e_{G/H}$, quindi $f(h) = e_{G/H}$

Siccome f è un isom ($\Rightarrow f$ iniettiva), e siccome $f(e_G) = e_{G/H}$, abbiamo ottenuto: $\forall h \in H$, $h = e_G$, ovvero $H = \{e_G\}$

Esempio • $(\mathbb{Q}, +) > (\mathbb{Z}, +)$

$$(\mathbb{Q}/\mathbb{Z}, +) \ni \frac{a}{b} + \mathbb{Z}$$

$$\left(\frac{a}{b} + \mathbb{Z}\right) + \dots + \left(\frac{a}{b} + \mathbb{Z}\right) = a + \mathbb{Z} = \mathbb{Z}$$

$$\operatorname{ord}\left(\frac{1}{n} + \mathbb{Z}\right) = n$$

• $(\mathbb{Q}^\times, \cdot)$ sottogp di torsione $= \{\pm 1\}$

Altri conteggi

$$G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

① $\# \{ g \in G \mid \operatorname{ord}(g) = 60 \} = ?$

Elementi di G : $g = (a_2, a_3, a_4, a_5)$

$$60 = \operatorname{ord}(a_2, a_3, a_4, a_5) =$$

$$= \operatorname{mcm}\left(o(a_2), o(a_3), o(a_4), o(a_5)\right)$$

$$\Rightarrow \quad \operatorname{ord}(a_5) = 5, \quad \operatorname{ord}(a_3) = 3, \quad \operatorname{ord}(a_4) = 4$$

$$\# \{ g : \operatorname{ord}(g) = 60 \} =$$

$$= \# \left\{ \begin{matrix} \text{scelte per} \\ a_2 \end{matrix} \right\} \times \# \left\{ \begin{matrix} \text{scelte di } a_3 \\ \operatorname{ord}(a_3) = 3 \end{matrix} \right\} \times$$

$$\times \# \{ a_4 : \operatorname{ord}(a_4) = 4 \} \times \# \{ a_5 : \operatorname{ord}(a_5) = 5 \}$$

$$= 2 \times \varphi(3) \times \varphi(4) \times \varphi(5) = 32$$

② $\# \{ H < G \mid H \simeq \mathbb{Z}/30\mathbb{Z} \}$

$$= \frac{1}{\varphi(30)} \# \{ g \in G \mid \operatorname{ord} g = 30 \}$$

$$= \frac{1}{1 \cdot 2 \cdot 4} \left(\begin{array}{l} \#\text{ scelte per } a_5 \quad \text{ord}(a_5) = 5 \times \\ \times \ \# \ \text{———} \quad a_3 \quad \text{ord}(a_3) = 3 \times \\ \times \ \#\text{ scelte di } (a_2, a_4) \ \text{ord}(a_2, a_4) = 2 \end{array} \right)$$

[Vediamo quali coppie (a_2, a_4) vanno bene:

$$\mathbb{Z}/_{2}\mathbb{Z} \times \mathbb{Z}/_{4}\mathbb{Z} \qquad \begin{array}{cccc} \cancel{(0,0)} & \cancel{(0,1)} & (0,2) & \cancel{(0,3)} \\ (1,0) & \cancel{(1,1)} & (1,2) & \cancel{(1,3)} \end{array}$$

]

$$= \frac{1}{8} \left(4 \times 2 \times 3 \right) = 3$$