Esercitazione 30 - 09 - 2020

Gruppi di Ordine p^2

Sia G di ord p^2, p primo. Classificarli.

Sol. L'ordine di ogni elemento divide p^2 e l'unico el di ordine 1 è id $\Rightarrow$ gli altri el hanno ord p o p^2. Se ce n'è uno di ordine p^2 allora genera $\Rightarrow$ $G \simeq \mathbb{Z}/p^2\mathbb{Z}$. Altrimenti tutti gli el. hanno ordine p: vogliamo mostrare $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

[Se sappiamo il Teorema di Classificazione dei Gruppi Abeliani Finiti allora è facile:
G è di ordine $p^2 \Rightarrow$ è abeliano $\Rightarrow G \simeq \mathbb{Z}/p^2\mathbb{Z}$ oppure $(\mathbb{Z}/p\mathbb{Z})^2$]

Altrimenti: sia $g_1 \in G \setminus \{id\}$, $(\operatorname{ord}(g_1) = p)$. Allora

$$G_1 := \langle g_1 \rangle \simeq \mathbb{Z}/p\mathbb{Z}$$

Prendiamo ora $g_2 \in G \setminus G_1$, $G_2 := \langle g_2 \rangle \simeq \mathbb{Z}/p\mathbb{Z}$.

Osserviamo che $\langle g_1 \rangle \cap \langle g_2 \rangle = \{e\}$: infatti può avere ordine 1 o p, ma se avesse ordine p i due gruppi sarebbero uguali (assurdo)

Consideriamo
$$\varphi : G \longrightarrow G/G_1 \times G/G_2 \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$
$$g \longmapsto (gG_1, gG_2)$$

È omomorfismo; è surgettivo sicuramente e

$$\begin{aligned}\operatorname{Ker}\varphi &= \{ g \in G : gH_1 = H_1 ,\ gH_2 = H_2 \} \\ &= \{ g \in G : g \in H_1 ,\ g \in H_2 \} \\ &= \{ g \in G : g \in H_1 \cap H_2 \} = H_1 \cap H_2 = \{e\}.\end{aligned}$$

Sottogruppi caratteristici

$H < G$ è **caratteristico** se $\forall \varphi \in Aut(G)$ si ha $\varphi(H) = H$.

(1) Sia $G = K \times H$, K, H finiti e $(\# H, \# K) = 1$.
Allora $K \times \{e_H\}$, $\{e_K\} \times H$ sono caratteristici in G.

DIM Vorremo una caratterizzazione di $K \times \{e_H\}$ e $\{e_K\} \times H$ che si preservi sotto automorfismo.
$\Rightarrow$ ORDINE : un automorfismo preserva l'ordine degli el.
Ricordiamo infatti che $ord((h, k)) = mcm\{ord(k), ord(h)\}$

Sia $m := |K|$, $n := |H|$. Allora gli el. di $K \times \{e_H\} \ni (k, e_H)$ sono tutti e soli quelli tali che $ord((k, e_H)) \mid |K| = m$.

Infatti $(k, e_H)^m = (k^m, e_H{}^m) = (e_K, e_H)$;
d'altro canto se $(k, h) \in G$ ha ordine che divide m, ovvero $(k, h)^m = (k^m, h^m) = (e_K, e_H)$, segue in particolare che $h^m = e_H$, ovvero $ord\, h \mid m$. Ma $ord\, h \mid |H| = n$, dunque $ord\, h \mid (m, n) = 1 \Rightarrow h = e_H$.

Sia allora $\varphi \in Aut(G)$, $(k, e_H) \in K \times \{e_H\}$. Allora

$\varphi((k, e_H))$ ha ordine che divide m poiché φ preserva gli ordini.
Segue che $\varphi((k, e_H)) \in K \times \{e_H\} \Rightarrow \varphi(K \times \{e_H\}) = K \times \{e_H\}$.
$\hookrightarrow$ è CARATTERISTICO

(2) Sia $G = H \times K$, con H, K finiti.
Allora $Aut(G) \cong Aut(H) \times Aut(K) \iff$ $H \times \{e_K\}$, $\{e_H\} \times K$ sono caratteristici

OSS : dati $\varphi_1 \in Aut(H)$, $\varphi_2 \in Aut(K)$ posso considerare

$$\varphi_1 \times \varphi_2 \in \begin{array}{ccc} H \times K & \xrightarrow{\sim} & H \times K \\ (h, k) & \longmapsto & (\varphi_1(h), \varphi_2(k)) \end{array}$$

Consideriamo allora

$$\Phi : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \hookrightarrow \mathrm{Aut}(\overset{H\times K}{\overset{\shortparallel}{G}})$$
$$(\varphi_1, \varphi_2) \longmapsto \varphi_1 \times \varphi_2$$

Questa mappa è omom ed è iniettiva

$\big(\ker \Phi = \{ (\varphi_1, \varphi_2) : \varphi_1 \times \varphi_2 = id \} = \{ (\varphi_1, \varphi_2) : \varphi_1 \times \varphi_2 (h,k) = (h,k) \}$
$= \{ (\varphi_1, \varphi_2) : \varphi_1(h) = h, \varphi_2(k) = k \} = \{ id \} \big)$

[$\Rightarrow$] Se $\mathrm{Aut}(G) \simeq \mathrm{Aut}(H) \times \mathrm{Aut}(K)$ allora Φ è bigettiva (per cardinalità). Allora ogni automorfismo di G agisce componente per componente, cioè ogni φ automorfismo di G è della forma $\varphi_1 \times \varphi_2$. Allora

$$\varphi_1 \times \varphi_2 (H \times \{e_K\}) = \varphi_1(H) \times \varphi_2(\{e_K\}) = H \times \{e_K\}$$

e similmente per $\{e_H\} \times K$

[$\Leftarrow$] Se $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici, preso $\varphi \in \mathrm{Aut}(G)$ posso considerare $\varphi|_{H \times \{e_K\}} =: \varphi_1$, $\varphi|_{\{e_H\} \times K} =: \varphi_2$.

Questi sono automorfismi di $H \times \{e_K\} \simeq H$ e $\{e_H\} \times K \simeq K$ poiché questi sottogr. sono caratteristici.

Allora $\varphi = \varphi_1 \times \varphi_2$: infatti

$$\varphi(h,k) = \varphi((h,e_K) \cdot (e_H,k))$$
$$= \varphi((h,e_K)) \cdot \varphi((e_H,k))$$
$$= (\varphi_1(h), e_K) \cdot (e_H, \varphi_2(k))$$
$$= (\varphi_1(h), \varphi_2(k)).$$

(iii) Siano $(m,n)=1$. Allora

$$\begin{tikzcd}
\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}) \arrow[r, phantom, "\simeq"] \arrow[d, phantom, "\cong" rotate=90] & \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})\times\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \arrow[d, phantom, "\cong" rotate=90] \\
\mathrm{Aut}(\mathbb{Z}/mn\mathbb{Z}) \arrow[d, phantom, "\cong" rotate=90] & (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \\
(\mathbb{Z}/mn\mathbb{Z})^\times \arrow[ur, phantom, "\simeq"] &
\end{tikzcd}$$

Siccome la Φ del punto 2 è iniettiva, $\forall m,n$ si ha

$$\begin{tikzcd}
\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}) \arrow[r, hook] \arrow[d, phantom, "\cong" rotate=90] & \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})\times\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \arrow[d, phantom, "\cong" rotate=90] \\
(\mathbb{Z}/mn\mathbb{Z})^\times \arrow[r, hook] & (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times
\end{tikzcd}$$

(iv) $H < G$ è caratt. $\Longrightarrow \exists\ \mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(H)$ omom. di res.

$H \triangleleft G \Longrightarrow \exists\ \mathrm{Inn}(G) \longrightarrow \mathrm{Aut}(H)$ " " "

Dove $\mathrm{Inn}\, G = \{\varphi_g \in \mathrm{Aut}\, G : \varphi_g(h) = ghg^{-1}\}$

$= \mathrm{Imm}\,\varphi$ con $\varphi : G \longrightarrow \mathrm{Aut}(G)$

$g \longmapsto (\varphi_g = h \longmapsto ghg^{-1})$

Se $H \triangleleft G$ la restrizione

$$\mathrm{Inn}(G) \longrightarrow \mathrm{Aut}(H)$$
$$\varphi_g \longmapsto \varphi_g\big|_H$$

è ben definita

ES: $G = S_3$, $H = \langle (1,2,3)\rangle$

$$\varphi_{(1,2)}((1,2,3)) = (1,2)^{-1}(1,2,3)(1,2) = (2,1,3)$$

$\Longrightarrow \varphi_{(1,2)}\big|_H \neq id$ ma $H/Z(H) \simeq \mathrm{Inn}(H) = \{id\}$ poiché H è abeliano.

Criterio per la Normalità ~ Sgrp. di indice minimo

Sia G finito, $H < G$, $[G:H] = p$ il più piccolo primo che divide $\#G$. Allora $H \trianglelefteq G$.

DIM. Consideriamo l'azione di G su G/H data da

$$\Phi : G \longrightarrow S(G/H) \simeq S_p \qquad \text{OSS: } |G/H| = p$$
$$g \longmapsto (g'H \mapsto gg'H)$$

Allora $\operatorname{Imm}\Phi < S_p \Rightarrow |\operatorname{Imm}\Phi| \mid |S_p| = p!$

D'altro canto

$$\operatorname{Imm}\Phi \simeq G/\operatorname{Ker}\Phi \Rightarrow |\operatorname{Imm}\Phi| = \frac{|G|}{|\operatorname{Ker}\Phi|} \;\Big|\; |G|$$

$$\Rightarrow |\operatorname{Imm}\Phi| \;\Big|\; (p!, |G|) = p$$
↳ più piccolo primo che divide $|G|$

$\Rightarrow |\operatorname{Imm}\Phi| \in \{1, p\}$ ma se fosse 1 allora $\Phi = id$,
$\Rightarrow \operatorname{Imm}\Phi \simeq \mathbb{Z}/p\mathbb{Z}$

SPERANZA: Da $G/\operatorname{Ker}\Phi \simeq \operatorname{Imm}\Phi \simeq \mathbb{Z}/p\mathbb{Z}$ mi viene la speranza
$\operatorname{Ker}\Phi = H$.

$\#\operatorname{Ker}\Phi = \#G/p$, $\#H = \#G/p$: mi basta $H \subseteq \operatorname{Ker}\Phi$ o
$H \supseteq \operatorname{Ker}\Phi$

Sia $g \in \operatorname{Ker}\Phi$: $\forall g'H \in G/H$ si ha che $gg'H = g'H$

Scegliamo $g'H = H$: allora $gH = H$, ovvero $g \in H$, da cui
$\operatorname{Ker}\Phi \subseteq H$. Ma allora $\operatorname{Ker}\Phi = H$, dunque H è il nucleo di un omomorfismo e quindi è normale. ∎

ESEMPIO Sia G di ordine 15. Mostriamo che $G \simeq \mathbb{Z}/_{15}\mathbb{Z}$.

DIM. Siccome il più piccolo primo che divide 15 è 3, voglio un sottogruppo di ordine 5. Per Cauchy $\exists\, \bar{g} \in G$ t.c. $\mathrm{ord}(\bar{g}) = 5 \Rightarrow$ se $H := \langle \bar{g} \rangle$ allora $[G : H] = 3$

$\Rightarrow H \trianglelefteq G$. Dato che voglio che G sia abeliano, deve valere che $H \leq Z(G)$; cioè

$$\forall h \in H : \forall g \in G : g h g^{-1} = h$$

$$\Leftrightarrow \forall g \in G : \forall h \in H : \varphi_g(h) = h$$

$$\Leftrightarrow \forall g \in G : \varphi_g(H) = H$$

$$\Leftrightarrow \forall g \in G : \varphi_g|_H = id$$

$$\Leftrightarrow \cdot|_H : \underset{\substack{\shortparallel \\ G/Z(G)}}{\mathrm{Inn}(G)} \longrightarrow \underset{\substack{\shortparallel \\ \mathbb{Z}/_5\mathbb{Z}^\times \simeq \mathbb{Z}/_4\mathbb{Z}}}{\mathrm{Aut}(H)} \text{ ha immagine } \{id\}$$

Abbiamo mostrato che $H \leq Z(G)$ se e solo se

$$\Phi : G/Z(G) \longrightarrow \mathbb{Z}/_4\mathbb{Z} \text{ ha immagine banale.}$$

Ma $\mathrm{Imm}\,\Phi$ da un lato è un sgrp di $\mathbb{Z}/_4\mathbb{Z}$, e dall'altro è

$$\mathrm{Imm}\,\Phi \simeq \frac{G/Z(G)}{\ker \Phi}$$ e quindi ha cardinalità che divide 15

$\Rightarrow \mathrm{Im}\,\Phi$ è banale e dunque $H \leq Z(G)$.

Segue dunque che $Z(G)$ ha 5 o 15 elementi. Ma se ne avesse 5 (cioè $H = Z(G)$) allora $G/_{Z(G)} \simeq \mathbb{Z}/_3\mathbb{Z}$ e se $G/_{Z(G)}$ è ciclico allora G è abeliano, da cui $G/Z(G)$ dovrebbe essere $\{e\}$

Dunque $Z(G)$ ha 15 el. e quindi G è ciclico.

Siano allora $g_1 \in G$, $g_2 \in G$ di ordine 5 e 3. (esistono per Cauchy)

$$\begin{aligned} \Psi : G &\longrightarrow G/\langle g_1 \rangle \times G/\langle g_2 \rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ g &\longmapsto (g\langle g_1 \rangle, g\langle g_2 \rangle) \end{aligned}$$

Tale mappa è un omomorfismo, è iniettiva poiché

$$\ker \Psi = \langle g_1 \rangle \cap \langle g_2 \rangle = \{e\}$$

Dunque Ψ è bigettiva $\Rightarrow G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$ $\blacksquare$

OSS: $\operatorname{ord}(g_1 g_2) = \operatorname{ord}(g_1)\operatorname{ord}(g_2)$ se $(\operatorname{ord}(g_1), \operatorname{ord}(g_2)) = 1$
e G è abeliano

$\Rightarrow$ nel nostro caso $\operatorname{ord} g_1 g_2 = 15 \Rightarrow$ genera $\mathbb{Z}/15\mathbb{Z}$.

TEOREMA DI CAUCHY ~ DIM. ALTERNATIVA

G gruppo, $p \mid \#G$. Allora $\exists g \in G : \operatorname{ord}(g) = p$.

DIM Sia X l'insieme dato da

$$X := \{(g_1, \dots, g_p) \in G^p : g_1 \cdots g_p = e\}$$

OSS: $g_1 g_2 g_3 = e \iff \underbrace{(g_1 g_2)}_{\hookrightarrow\, g_1 g_2 = g_3^{-1}}\underbrace{(g_3)}_{} = e \iff g_3 g_1 g_2 = e$

$\iff g_2 g_3 g_1 = e$

Consideriamo l'azione di $\mathbb{Z}/p\mathbb{Z}$ su X:

la classe $\bar{i} \in \mathbb{Z}/p\mathbb{Z}$ manda $(g_1, \dots, g_p)$ in

$$(g_{1+i \bmod p}, \dots, g_{p+i \bmod p}).$$

Come sono fatte le orbite di quest'azione?

LEMMA ORB-STAB $\quad Orb(x) \longleftrightarrow \dfrac{\mathbb{Z}/p\mathbb{Z}}{Stab(x)} \simeq \begin{cases} \mathbb{Z}/p\mathbb{Z} \\ \{\bar{0}\} \end{cases}$

Ci sono dunque due tipi di orbite
- di cardinalità $p \longleftrightarrow Stab(x) = \{\bar{0}\}$
- $\qquad\qquad\qquad 1 \longleftrightarrow Stab(x) = \mathbb{Z}/p\mathbb{Z}$

Orb di cardinalità 1? $\quad (g_1, \dots, g_p)$ tale che $\forall \bar{\imath} \in \mathbb{Z}/p\mathbb{Z}$

$$\bar{\imath} \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p)$$

$$\Rightarrow (g_1, \dots, g_p) = (g, \dots, g)$$

Ma per def. di X dovremmo avere $g^p = e$, cioè $g = e$ oppure g di ordine p.

Inoltre $\quad X = \bigsqcup_{x \in R} orb(x) \Rightarrow |X| = \sum_{x \in R} |orb(x)|$

$\hookrightarrow$ insieme di rappresentanti $\longleftarrow$

Ma $|X| = |G|^{p-1}$: posso scegliere i primi $p-1$ el. come voglio e l'ultimo è determinato da $g_p = (g_1 \cdots g_{p-1})^{-1}$.

Dunque $\quad |X| = \sum_{x \in R} |orb(x)| = p \cdot (n^\circ \text{ orb. di lung. } p) + 1 \cdot (n^\circ \text{ orb. di lungh } 1)$

$\quad \| $

$|G|^{p-1}$. $\quad$ Ma $p \mid |G| \mid |G|^{p-1}$, quindi modulo p:

$$0 \equiv \cancel{0 \cdot (n^\circ \text{ orb. } p)} + 1 \cdot (n^\circ \text{ orb. } 1) \quad (p)$$

$$\equiv (n^\circ \text{ orb } 1) \quad (p)$$

cioè $(n^\circ \text{ orb } 1) = 0$ oppure è un multiplo di p. Ma non è 0 perché

$\# \, orb((e, e, \ldots, e)) = 1$, dunque deve esistere almeno un el. di ordine p. $\blacksquare$

OSS: Segue che $\# \{ g \in G : ord(g) = p \} \equiv -1 \ (p)$.

Infatti $\underbrace{(n^\circ \text{ orb lungh. } 1)}_{\equiv \, 0 \bmod p} = 1 + (n^\circ \text{ el. di ordine } p)$

$\Rightarrow (n^\circ \text{ el. ordine } p) \equiv -1 \ (p)$