

Azione di coniugio e p -gruppi

di Gabriel Antonio Videtta

Nota. Nel corso del documento per (G, \cdot) si intenderà un qualsiasi gruppo.

Si consideri l'omomorfismo ζ che associa ad ogni $g \in G$ l'automorfismo interno che induce. Questo omomorfismo induce la cosiddetta:

Definizione (azione di coniugio). Si definisce **azione di coniugio** l'azione di G su sé stesso indotta da $\zeta : G \rightarrow \text{Aut}(G)$ dove:

$$g \xrightarrow{\zeta} \varphi_g = [h \mapsto ghg^{-1}].$$

L'orbita di un elemento $g \in G$ prende in questo particolare caso il nome di **classe di coniugio** (e si indica come $\text{Cl}(g)$), mentre il suo stabilizzatore viene detto **centralizzatore** (indicato con $Z_G(g)$). Si verifica facilmente che $Z_G(g)$ è composto da tutti gli elementi $h \in G$ che commutano con g , ossia tali che $gh = hg$. Allora vale in particolare che:

$$Z(G) = \text{Ker } \zeta = \bigcap_{g \in G} Z_G(g).$$

Si osserva inoltre che se $g \in Z(G)$, allora $\text{Cl}(g) = \{g\}$ (infatti, per $h \in G$, si avrebbe $hgh^{-1} = hh^{-1}g = g$). Si può dunque riscrivere la somma data dal Teorema orbita-stabilizzatore nel seguente modo:

$$|G| = \sum_{g \in \mathcal{R}} \frac{|G|}{|Z_G(g)|} = \sum_{g \in Z(G)} \underbrace{|\text{Cl}(g)|}_{=1} + \sum_{g \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(g)|} = (*),$$

che riscritta ancora si risolve nella **formula delle classi di coniugio**:

$$(*) = |Z(G)| + \sum_{g \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(g)|},$$

dove \mathcal{R} è un insieme di rappresentanti delle orbite dell'azione di coniugio (si osserva che ogni elemento di $Z(G)$ è un rappresentante dacché l'orbita di un elemento del centro è banale).

Utilizzando la nozione di centralizzatore, si può contare “facilmente” il numero di classi di coniugio di un gruppo. Infatti, si osserva crucialmente che $\text{Fix}(g)$ (il numero di elementi di G lasciati invariati sotto il coniugio di g) è lo stesso insieme $Z_G(g)$. Infatti vale che:

$$\text{Fix}(g) = \{h \in G \mid gh = hg\} = Z_G(g).$$

Allora, per il lemma di Burnside, se $k(G)$ è il numero di classi di coniugio di G , vale che:

$$k(G) = \frac{1}{|G|} \sum_{g \in G} |Z_G(g)|.$$

La formula delle classi di coniugio risulta in particolare utile nella discussione dei p -gruppi, definiti di seguito.

Definizione (p -gruppo). Sia G un gruppo finito. G si dice allora **p -gruppo** se $|G| = p^n$ per $n \in \mathbb{N}^+$ e un numero primo $p \in \mathbb{N}$.

Infatti, grazie alla formula delle classi di coniugio, si osserva facilmente che il centro di un p -gruppo non è mai banale (ossia composto dalla sola identità), come mostra la:

Proposizione. Sia G un p -gruppo. Allora $|Z(G)| > 1$.

Dimostrazione. Dalla formula delle classi di coniugio si ha che:

$$|G| = |Z(G)| + \sum_{g \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(g)|}.$$

Si osserva in particolare che il secondo termine della somma a destra è divisibile per p . Infatti, poiché $g \notin Z(G)$ per ipotesi, $Z_G(g) \neq Z(G)$; da cui si deduce che $|Z_G(g)|$ deve essere un divisore stretto di p^n , e dunque che $p \mid |G|/|Z_G(g)|$. Prendendo l'identità di sopra modulo p , si deduce allora che:

$$|Z(G)| \equiv 0 \pmod{p}.$$

Combinando questo risultato col fatto che $|Z(G)| \geq 1$ (infatti $Z(G) \leq G$), si conclude che deve valere necessariamente la tesi. \square

Quest'ultima proposizione spiana il terreno per un risultato interessante sui gruppi di ordine p^2 , come mostra il:

Teorema. Ogni gruppo G di ordine p^2 è abeliano.

Dimostrazione. Dal momento che G è un p -gruppo, per la precedente proposizione $|Z(G)| > 1$. Allora $|Z(G)|$ è pari a p o p^2 , per il Teorema di Lagrange. Se $|Z(G)|$ fosse pari a p , allora $|G/Z(G)| = |G|/|Z(G)| = p$. Pertanto $G/Z(G)$ sarebbe ciclico, e dunque G sarebbe abeliano; assurdo, dal momento che si era presupposto che $Z(G)$ fosse un sottogruppo proprio di G , \neq . Allora $Z(G)$ ha ordine p^2 , e dunque $Z(G) = G$. \square

Esempio. Si mostra che¹ G è obbligatoriamente isomorfo a \mathbb{Z}_{p^2} o a $\mathbb{Z}_p \times \mathbb{Z}_p$ se $|G| = p^2$.

Se G ammette un generatore, allora G è ciclico e quindi isomorfo a \mathbb{Z}_{p^2} . Altrimenti, sia $g \in G$ un elemento di ordine² p e sia³ $h \in G$ tale che $h \notin \langle g \rangle$. Per il teorema precedente G è abeliano, e quindi $\langle g \rangle \langle h \rangle$ è un sottogruppo di G .

Inoltre $\langle g \rangle \cap \langle h \rangle$ è banale: se non lo fosse avrebbe ordine p , e quindi $\langle g \rangle$ e $\langle h \rangle$ coinciderebbero insiemisticamente, \neq . Pertanto $\langle g \rangle \langle h \rangle \cong \langle g \rangle \times \langle h \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Infine, poiché $|\langle g \rangle \langle h \rangle| = p^2$, vale anche che $G = \langle g \rangle \langle h \rangle$, da cui la tesi.

Si mostra infine una proposizione riguardante il normalizzatore di un sottogruppo proprio di un p -gruppo:

Proposizione. Sia G un p -gruppo. Allora $H \leq G \implies H \leq N_G(H)$.

Dimostrazione. Sia $|G| = p^n$. Si dimostra la tesi per induzione su n . Se $n = 1$, la tesi è banale. Sia ora $n > 1$. Si distinguono due casi, in base a se $Z(G) \leq H$ o meno.

Se $Z(G) \not\leq H$, allora esiste sicuramente un elemento $x \in Z(G) \setminus H$, e quindi un elemento x appartenente a $N_G(H)$, ma non ad H . In tal caso, si deduce facilmente che $H \leq N_G(H)$.

Se invece $Z(G) \leq H$, si può applicare il Teorema di corrispondenza. Poiché $G/Z(G)$ è un p -gruppo di ordine strettamente minore di p^n (infatti il centro di un p -gruppo è sempre non banale), per induzione $H/Z(G) \leq N_{G/Z(G)}(H/Z(G))$. Allora, per il Teorema di corrispondenza, $H = \pi_{Z(G)}^{-1}(H/Z(G)) \leq \pi_{Z(G)}^{-1}(N_{G/Z(G)}(H/Z(G)))$. È sufficiente mostrare che $\pi_{Z(G)}^{-1}(N_{G/Z(G)}(H/Z(G))) \subseteq N_G(H)$ per dedurre la tesi. Sia allora $g \in \pi_{Z(G)}^{-1}(N_{G/Z(G)}(H/Z(G)))$. Allora, per ipotesi, vale che:

$$\pi_{Z(G)}(gHg^{-1}) = gZ(G)\pi_{Z(G)}(H)g^{-1}Z(G) \subseteq \pi_{Z(G)}(H),$$

per cui $gHg^{-1} \subseteq H$. □

¹Il risultato è facilmente dimostrabile attraverso il Teorema di struttura dei gruppi abeliani finitamente generati.

²Questo elemento deve esistere obbligatoriamente, non solo per il Teorema di Cauchy, ma anche perché solo l'identità ammette ordine 1 e perché si è supposto che nessun elemento abbia ordine p^2 (altrimenti il gruppo sarebbe ciclico).

³Tale h deve esistere, altrimenti G sarebbe ciclico.