Normalizzatore e teorema di Cayley

di Gabriel Antonio Videtta

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

Sia $X = \{H \subseteq G \mid H \leq G\}$ l'insieme dei sottogruppi di G. Allora si può costruire un'azione $\varphi : G \to S(X)$ in modo tale che:

$$g \overset{\varphi}{\mapsto} \left[H \mapsto gHg^{-1}\right].$$

Si definisce **normalizzatore** lo stabilizzatore di un sottogruppo H (e si indica con $N_G(H)$), mentre $\mathrm{Orb}(H)$ è l'insieme dei **coniugati** di H. In particolare $N_G(H)$ è il massimo sottogruppo per inclusione in cui H è normale.

Si osserva ora in modo cruciale che $H \trianglelefteq G$ se e solo se $\mathrm{Orb}(H) = \{H\}$, e quindi se e solo se $N_G(H) = G$. Analogamente si osserva che H è normale se e solo se:

$$H = \bigcup_{h \in H} \mathrm{Cl}(h).$$

Tramite la stessa azione φ possiamo illustrare un importante relazione tra gli stabilizzatori, dettata dalla:

Proposizione. Sia $x \in X$ e sia $g \in G$. Allora vale che $\mathrm{Stab}(g \cdot x) = g \, \mathrm{Stab}(x) g^{-1}$, e i coniugati di $\mathrm{Stab}(x)$ sono esattamente altri stabilizzatori.

Dimostrazione. Si osserva che se $ghg^{-1} \in g \, \mathrm{Stab}(x) g^{-1}$, allora:

$$(ghg^{-1}) \cdot (g \cdot x) = gh \cdot x = g \cdot x \implies ghg^{-1} \in \mathrm{Stab}(g \cdot x),$$

e viceversa che se $h \in \mathrm{Stab}(g \cdot x)$:

$$(g^{-1}hg) \cdot x = g^{-1} \cdot (h \cdot (g \cdot x)) = (g^{-1}g) \cdot x = x \implies g^{-1}hg \in \mathrm{Stab}(x) \implies h \in g \, \mathrm{Stab}(x) g^{-1},$$

da cui si deduce che $\mathrm{Stab}(g \cdot x) = g \, \mathrm{Stab}(x) g^{-1}$. □

Da questa proposizione segue immediatamente il seguente:

Corollario. Sia φ un'azione transitiva. Allora tutti gli stabilizzatori sono coniugati tra loro.

Dimostrazione. Siano x e $y \in X$. Poiché φ è transitiva, esiste un'unica orbita e dunque esiste $g \in G$ tale per cui $g \cdot y = x$. Allora $\operatorname{Stab}(x) = \operatorname{Stab}(g \cdot y) = g \operatorname{Stab}(y) g^{-1}$. □

Infine, si verifica una proprietà dei sottogruppi coniugati:

Proposizione. Se H e K sono coniugati, allora sono in particolare anche isomorfi.

Dimostrazione. Poiché H e K sono coniugati, esiste un $g \in G$ tale per cui $K = gHg^{-1}$. Un isomorfismo tra i due gruppi è allora naturalmente dato dall'azione di coniugio tramite g, ossia dall'omomorfismo $\zeta : H \to K$ tale per cui $h \overset{\zeta}{\mapsto} ghg^{-1}$. Tale mappa è sicuramente un omomorfismo; è ben definita e surgettiva perché i gruppi sono coniugati ed è iniettiva perché $ghg^{-1} = e \implies h = e$ (e quindi $\operatorname{Ker} \zeta = \{e\}$). □

Si illustra adesso un risultato principale della teoria dei gruppi che mette in relazione ogni gruppo con il proprio gruppo di bigezioni, ed ogni gruppo finito con i sottogruppi dei gruppi simmetrici.

Teorema (di Cayley)**.** Ogni gruppo è isomorfo a un sottogruppo del suo gruppo di bigezioni. In particolare, ogni gruppo finito G è isomorfo a un sottogruppo di un gruppo simmetrico.

Dimostrazione. Si consideri l'azione[1] $\varphi : G \to S(G)$ tale per cui:

$$g \overset{\varphi}{\mapsto} [h \mapsto gh] .$$

Si mostra che φ è fedele[2]. Sia infatti $\varphi(g) = \mathrm{Id}$; allora vale che $ge = e \implies g = e$. Quindi $\operatorname{Ker} \varphi$ è banale, e per il Primo teorema di isomorfismo vale che:

$$G \cong \operatorname{Im} \varphi \leq S(G).$$

Se G è finito, $S(G)$ è isomorfo a S_n, dove $n := |G|$, e quindi $\operatorname{Im} \varphi$ è a sua volta isomorfo a un sottogruppo di S_n, da cui la tesi. □

A partire dall'*embedding* di Cayley si può dimostrare un risultato sui gruppi di ordine $2d$ con d dispari:

Proposizione. Sia G un gruppo di ordine $2d$ con d dispari. Allora G ammette un sottogruppo H di ordine d.

Dimostrazione. Consideriamo l'*embedding* di Cayley di G. In particolare, poiché $S(G) \cong S_{2d}$, possiamo identificare $S(G)$ con S_{2d}, studiando tale *embedding* direttamente su quest'ultimo sottogruppo.

[1]Tale azione prende il nome di **rappresentazione regolare a sinistra** o ***embedding* di Cayley**. Si può definire un'azione analoga a destra ponendo $g \mapsto \left[h \mapsto hg^{-1}\right]$, costruendo dunque una *rappresentazione regolare a destra.*

[2]L'azione φ è molto più che fedele; è infatti innanzitutto libera.

Sia allora $\varphi : G \to S_{2d}$ la composizione $\xi \circ \lambda$ dove ξ è un isomorfismo tra $S(G)$ e S_{2d} e $\lambda : G \to S(G)$ è l'*embedding* di Cayley associato a G. Si osserva che $\varphi^{-1}(\mathcal{A}_{2d}) = \{g \in G \mid \varphi(g) \in \mathcal{A}_{2d}\} = \mathrm{Ker}(\pi_{\mathcal{A}_{2d}} \circ \varphi)$. Per il Primo teorema di isomorfismo vale che:

$$G/\mathrm{Ker}(\pi_{\mathcal{A}_{2d}} \circ \varphi) \cong \mathrm{Im}(\pi_{\mathcal{A}_{2d}} \circ \varphi) \leq S_{2d}/\mathcal{A}_{2d} \cong \{\pm 1\},$$

e quindi[3] $[G : \mathrm{Ker}(\pi_{\mathcal{A}_{2d}} \circ \varphi)]$ vale 1 o 2.

Se $[G : \mathrm{Ker}(\pi_{\mathcal{A}_{2d}} \circ \varphi)]$ fosse uguale a 1, varrebbe che $G = \mathrm{Ker}(\pi_{\mathcal{A}_{2d}} \circ \varphi) = \varphi^{-1}(\mathcal{A}_{2d})$, e quindi che $\varphi(G) \subseteq \mathcal{A}_{2d}$. Si mostra che ciò è impossibile esibendo un elemento $g \in G$ tale per cui $\varphi(g)$ sia dispari. Dacché $2 \mid |G|$, esiste $g \in G$ con $\mathrm{ord}(g) = 2$ per il teorema di Cauchy. Allora la decomposizione in cicli di $\varphi(g)$ sarà la stessa di $\lambda(g)$, ossia[4]:

$$\lambda(g) = (g_1, gg_1)(g_2, gg_2) \cdots (g_d, gg_d).$$

Poiché $\lambda(g)$ è allora prodotto di d trasposizioni, $\lambda(g)$ è dispari, e così pure $\varphi(g)$. Pertanto $\varphi(g) \notin \mathcal{A}_{2d} \implies [G : \mathrm{Ker}(\pi_{\mathcal{A}_{2d}} \circ \varphi)] = 2$, e quindi $|\mathrm{Ker}(\pi_{\mathcal{A}_{2d}} \circ \varphi)| = d$, concludendo la dimostrazione. $\square$

Si presentano adesso due risultati interessanti legati ai sottogruppi normali di un gruppo G.

Proposizione. Sia[5] $H \leq G$. Allora, se $[G : H] = 2$, H è normale in G.

Dimostrazione. Poiché $[G : H] = 2$, le uniche classi laterali sinistre rispetto ad H in G sono H e $gH = G \setminus H$, dove $g \notin H$. Analogamente esistono due sole classi laterali destre, H e $Hg = G \setminus H$. In particolare gH deve obbligatoriamente essere uguale a Hg, e quindi $gHg^{-1} = H$, da cui la tesi. $\square$

Proposizione. Siano $K \leq H \leq G$. Allora, se H è normale in G e K è caratteristico in H, K è normale in G.

Dimostrazione. Sia $\varphi_g \in \mathrm{Inn}(G)$. Poiché H è normale in G, $\varphi_g(H) = H$. Pertanto si può considerare la restrizione di φ_g su H, $\varphi_g|_H$. In particolare $\varphi_g|_H$ è un automorfismo di $\mathrm{Aut}(H)$, e quindi, poiché K è caratteristico in H, $\varphi_g|_H(K) = K$, da cui si deduce che $gKg^{-1} = K$ per ogni $g \in G$. $\square$

[3] Si può arrivare alla stessa conclusione mediante un ragionamento leggermente diverso. Se si considera $K = \varphi(G)$, $K \cap \mathcal{A}_{2d} = \varphi(G) \cap \mathcal{A}_{2d}$ è esattamente $\mathrm{Ker}(\mathrm{sgn}|_{\varphi(G)})$, e quindi $[K : (K \cap \mathcal{A}_{2d})] \in \{1, 2\}$. Pertanto, dal momento che φ è un isomorfismo tra G e $\mathrm{Im}\,\varphi = \varphi(G)$, $\varphi^{-1}(\mathcal{A}_{2d}) = \varphi^{-1}(\mathcal{A}_{2d} \cap \varphi(G))$ può avere solo indice 1 o 2, ed ha indice 1 se e solo se $\varphi(G) \subseteq \mathcal{A}_{2d}$.

[4] In generale, se $\mathrm{ord}(g) = k$, la sua decomposizione tramite λ sarà:

$$(g_1, gg_1, \ldots, g^{k-1}g_1)(g_2, gg_2, \ldots, g^{k-1}g_2) \cdots (g_s, gg_s, \ldots, g^{k-1}g_s),$$

con $s = 2d/k$, ossia $\lambda(g)$ sarà prodotto di $2d/k$ k-cicli.

[5] Si osserva che questa proposizione risulta superflua se si dimostra, come succede sul finire di questo documento, che per il più piccolo primo p che divide $|G|$, i sottogruppi corrispondenti di indice p sono normali. Vista tuttavia la semplicità della dimostrazione, si è preferito lasciarla per motivi didattici.

Si illustra adesso un risultato riguardante l'esistenza di sottogruppi normali in G:

Teorema (di Poincaré)**.** Sia H un sottogruppo di G di indice n. Allora esiste sempre un sottogruppo N di G tale per cui:

(i) N è normale in G,

(ii) N è contenuto in H,

(iii) $n \mid [G : N] \mid n!$.

Dimostrazione. Si consideri l'azione $\varphi : G \to S(G/H)$ tale per cui $g \overset{\varphi}{\mapsto} [kH \mapsto gkK]$. Tale azione è sicuramente ben definita dal momento che $kH = k'H \implies gkH = gk'H$. Si studia $N := \operatorname{Ker} \varphi$. Chiaramente N è normale in G, e si verifica facilmente che N è contenuto anche in H, infatti, se $n \in N$, allora:

$$H = \varphi(n)(H) = nH \implies n \in H.$$

Poiché G/N è isomorfo a $\operatorname{Im} \varphi \leq S(G/H)$, $[G : N] \mid |S(G/H)| = |S_n| = n!$ considerando che $S(G/H) \cong S_n$. Dal momento allora che N è un sottogruppo di H, vale che:

$$[G : N] = [G : H][H : N] = n[H : N],$$

e quindi $n \mid [G : N]$. Si è dunque esibito un sottogruppo N con le proprietà indicate nella tesi. $\square$

Dal precedente teorema sono immediati i seguenti due risultati:

Corollario. Sia H un sottogruppo di G con indice n. Se $n! < |G|$ e $n > 1$, allora G non è semplice.

Corollario. Sia H un sottogruppo di G con indice p, dove p è il più piccolo primo che divide $n = |G|$. Allora H è normale.

Dimostrazione. Per il Teorema di Poincaré, esiste un sottogruppo N di H tale per cui N sia normale e $p \mid [G : N] \mid p!$ con $p = [G : H]$. In particolare $[G : N]$ deve dividere anche n, e quindi $[G : N]$ deve dunque dividere $\mathrm{MCD}(p!, n)$, che è, per ipotesi, p stesso. Si conclude dunque che $[G : N] = p = [G : H]$, e quindi che $N = H$, ossia che H stesso è normale. $\square$

Esempio (Tutti i gruppi di ordine 15 sono ciclici)**.** Sia[6] G un gruppo di ordine 15. Per il teorema di Cauchy esistono due elementi h ed k, uno di ordine 3 e l'altro di ordine 5. In particolare, si consideri $K = \langle k \rangle$; poiché $|K| = 5$, $[G : K] = 3$, il più piccolo primo che divide 15. Pertanto K è normale per il corollario di sopra.

[6] In realtà 15 è un numero molto speciale, in quanto è prodotto di due primi distinti (3 e 5) tali per cui 3 non divida $5 - 1 = 4$. In generale, ogni gruppo di ordine pq con p e q primi tali per cui $p < q$ e $p \nmid q - 1$ è ciclico.

Poiché K è normale, si può considerare la restrizione $\iota : \mathrm{Inn}(G) \to \mathrm{Aut}(K)$ tale per cui $\varphi_g \overset{\iota}{\mapsto} \varphi_g|_K$. Dal momento che K è ciclico, $\mathrm{Aut}(K) \cong \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$. Quindi $[G : \mathrm{Ker}\, \iota]$ deve dividere sia 4 che 15; dal momento che $\mathrm{MCD}(4, 15) = 1$, $[G : \mathrm{Ker}\, \iota] = 1$, e quindi che ι è l'omomorfismo banale. Poiché ι è banale, K è un sottogruppo di $Z(G)$.

In particolare $[G : Z(G)] \mid [G : K] = 3$, e quindi in particolare $G/Z(G)$ è ciclico, da cui si deduce che G è abeliano. Infine, dal momento che $\mathrm{MCD}(3, 5) = 1$ e h e k commutano, hk è un elemento di ordine 15, e dunque G è ciclico.

Si illustrano infine due risultati interessanti sui coniugati di G:

Proposizione. Sia $H \leq G$. Allora

$$\bigcup_{g \in G} gHg^{-1} = G \iff H = G.$$

Dimostrazione. Se $H = G$, allora $gGg^{-1} = G$ e quindi l'identità è vera. Viceversa, $gHg^{-1} = kHk^{-1} \iff gN_G(H) = kN_G(H)$. Preso dunque un'insieme $\mathcal{R}$ di rappresentanti per ogni classe in $G/N_G(H)$, vale che:

$$\bigcup_{g \in \mathcal{R}} gHg^{-1} = G.$$

In ogni gHg^{-1} ci sono $|H|$ elementi distinti, e quindi, poiché $|\mathcal{R}| = |G/N_G(H)|$, deve valere la seguente disuguaglianza:

$$\left| \bigcup_{g \in \mathcal{R}} gHg^{-1} \right| \leq |G/N_G(H)|\, |H| \leq \frac{|G|}{|N_G(H)|}\, |H| \leq |G|,$$

dove si è usato che $H \leq N_G(H)$. Se $|G/N_G(H)|$ non valesse 1, ci sarebbe più ripetizioni di e all'interno dell'unione, e quindi la prima disuguaglianza sarebbe stretta, $\lightning$. Quindi $N_G(H) = G \implies H \trianglelefteq G$. Allora la disuguaglianza si riscrive come:

$$|G| = \left| \bigcup_{g \in \mathcal{R}} gHg^{-1} \right| \leq |H| \leq |G|,$$

da cui si ricava che necessariamente $|H| = |G| \implies H = G$. □

Proposizione. Sia φ un'azione transitiva di G su X. Allora esiste sempre un $g \in G$ tale per cui $\mathrm{Fix}(g) = \varnothing$, se $|X| \geq 2$.

Dimostrazione. Se g non fissa alcun punto di X, allora $g \notin \bigcup_{x \in X} \mathrm{Stab}(x)$; pertanto tale g esiste se e solo se $\bigcup_{x \in X} \mathrm{Stab}(x) \neq G$. Poiché tali sottogruppi sono tutti coniugati, scelto $u \in U$ vale che:

$$\bigcup_{x \in X} \mathrm{Stab}(x) = \bigcup_{g \in G} g\, \mathrm{Stab}(u) g^{-1}.$$

Si conclude dunque che tale g esiste se e solo se $\mathrm{Stab}(u) \neq G$. Se $\mathrm{Stab}(u)$ fosse uguale a G, allora, per il Teorema orbita-stabilizzatore, varrebbe che $|\mathrm{Orb}(u)| = 1$; tuttavia φ è transitiva e quindi $X = \mathrm{Orb}(u) \implies |X| = |\mathrm{Orb}(u)| = 1$, $\lightning$. Pertanto $\mathrm{Stab}(u) \neq G$, e dunque l'unione non ricopre tutto G, concludendo la dimostrazione. □