

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 $\varphi : G \rightarrow S(X)$ in modo tale che:

$$g \mapsto [H \mapsto gHg^{-1}].$$

Si definisce **normalizzatore** lo stabilizzatore di un sottogruppo H (e si indica con $N_G(H)$), mentre $\text{Orb}(H)$ 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 $\text{Orb}(H) = \{H\}$, e quindi se e solo se $N_G(H) = G$. Analogamente si osserva che H è normale se e solo se:

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

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'azione¹ $\varphi : G \rightarrow S(G)$ tale per cui:

$$g \mapsto [h \mapsto gh].$$

Si mostra che φ è fedele². Sia infatti $\varphi(g) = \text{Id}$; allora vale che $ge = e \implies g = e$. Quindi $\text{Ker } \varphi$ è banale, e per il Primo teorema di isomorfismo vale che:

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

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

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

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

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

Proposizione. Sia³ $H \leq G$. 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 $\varphi_g \in \text{Inn}(G)$. 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 $\text{Aut}(H)$, 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

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 $\varphi : G \rightarrow S(G/H)$ tale per cui $g \xrightarrow{\varphi} [kH \mapsto gkH]$. Tale azione è sicuramente ben definita dal momento che $kH = k'H \implies gkH = gk'H$. Si studia $N := \text{Ker } \varphi$. 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 $\text{Im } \varphi \leq S(G/H)$, $[G : N] \mid |S(G/H)| = |S_n| = n!$ 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:

³Si 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.

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 $\text{MCD}(p!, n)$, 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). Sia⁴ 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.

Poiché K è normale, si può considerare la restrizione $\iota : \text{Inn}(G) \rightarrow \text{Aut}(K)$ tale per cui $\varphi_g \mapsto \varphi_g|_K$. Dal momento che K è ciclico, $\text{Aut}(K) \cong \text{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$. Quindi $[G : \text{Ker } \iota]$ deve dividere sia 4 che 15; dal momento che $\text{MCD}(4, 15) = 1$, $[G : \text{Ker } \iota] = 1$, 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 $\text{MCD}(3, 5) = 1$ 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:

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

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

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, \neq . 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 gli stabilizzatori sono tra di loro coniugati, e dunque isomorfi. Inoltre, se $|X| \geq 2$, allora esiste un g tale per cui $\text{Fix}(g) = \emptyset$.

Dimostrazione. Siano $x, y \in X$. Si verifica innanzitutto che esiste un $g \in G$ tale per cui $g \text{Stab}(x)g^{-1} = \text{Stab}(y)$. Poiché φ è un'azione transitiva, esiste $g \in G$ tale per cui $g \cdot y = x$. Allora vale che:

$$\text{Stab}(x) = \{h \in G \mid h \cdot x = x\} = \{h \in G \mid h \cdot (g \cdot y) = (g \cdot y)\},$$

da cui si deduce infine che:

$$\text{Stab}(x) = \{h \in G \mid (g^{-1}hg) \cdot y = y\} = g \text{Stab}(y)g^{-1}.$$

In particolare un isomorfismo tra i due gruppi è dato proprio dall'azione di coniugio tramite g , ossia dall'omomorfismo⁵ $\zeta : \text{Stab}(y) \rightarrow \text{Stab}(x)$ tale per cui $h \mapsto ghg^{-1}$.

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

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

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

⁵Tale omomorfismo è infatti surgettivo perché $\text{Stab}(x) = g \text{Stab}(y)g^{-1}$, mentre è iniettivo perché $ghg^{-1} = e \implies h = e$.