I teoremi di Sylow

di Gabriel Antonio Videtta

Nota. Nel corso del documento con p si indicherà un numero primo, con G si indicherà un qualsiasi gruppo finito di ordine $p^n m$ tale per cui $\mathrm{MCD}(p, m) = 1$ (ossia n è la valutazione p-adica di $|G|$).

I teoremi di Sylow rappresentano, insieme al teorema di struttura per gruppi abeliani finiti, lo strumento più importante e applicabile dell'algebra elementare. Attraverso questi teoremi, lo studio e la classificazione dei gruppi finiti viene enormemente facilitata e ridotta ai suoi p-sottogruppi.

Prima di illustrare gli enunciati e le dimostrazioni di questi teoremi, si definisce preliminarmente cos'è un p-sottogruppo di Sylow, detto poi semplicemente p-Sylow:

Definizione (p-Sylow)**.** Sia $H \leq G$. Si dice che H è un p-**Sylow** di G se $|H| = p^n$, ossia se H è un p-sottogruppo di H con valutazione p-adica massima.

Si illustra adesso il Primo teorema di Sylow, che riguarda l'esistenza di p-sottogruppi di tutte le cardinalità possibili[1][2] in G:

Teorema (Primo teorema di Sylow, esistenza)**.** Per ogni $i \in \mathbb{N}$ tale per cui $0 \leq i \leq n$, esiste un sottogruppo $H \leq G$ tale per cui $|H| = p^i$.

Dimostrazione. Si consideri il sottoinsieme $\mathcal{M}$ di $\mathcal{P}(G)$ dato da:

$$\mathcal{M} = \{X \subseteq G \mid |X| = p^i\}.$$

Allora vale che:

$$|\mathcal{M}| = \binom{p^n m}{p^i} = \frac{(p^n m)!}{(p^i)!(p^n m - p^i)!} = \frac{p^n m(p^n m - 1) \cdots (p^n m - p^i + 1)}{p^i(p^i - 1) \cdots 1},$$

[1] A dire la verità il Primo teorema di Sylow si deduce anche solo mostrando l'esistenza di un p-Sylow. Infatti, per una proposizione nota sui p-gruppi, che discende direttamente dal Teorema di corrispondenza, in un p-gruppo esiste sempre una catena di p-sottogruppi normali che comprende p-sottogruppi di tutte le cardinalità. Dal momento però che la dimostrazione è molto istruttiva (e anche molto generale), si è preferito lasciare la generalizzazione.

[2] Si osserva che il Primo teorema di Sylow generalizza il Teorema di Cauchy alla sua massima estensione.

ossia, equivalentemente, che:

$$|\mathcal{M}| = p^{n-i} m \prod_{j=1}^{p^i-1} \frac{p^n m - j}{p^i - j}.$$

Si osserva che $p^{n-i} \parallel |M|$. Infatti, $p \nmid m$ perché $\mathrm{MCD}(p, m) = 1$ per ipotesi; inoltre, considerando il termine generico a_j della produttoria, vale che[3] $\nu_p(p^n m - j) = \nu_p(j) = \nu_p(p^i - j)$, e quindi che $\nu_p(a_j) = 0$.

Dal momento che, dato $X \in \mathcal{M}$, gX appartiene ancora ad $\mathcal{M}$ e $gX = hX \iff g = h$, $\forall\ g,\ h \in G$, si può considerare l'azione $\phi : G \to S(\mathcal{M})$ tale per cui $g \overset{\phi}{\mapsto} [X \mapsto gX]$. Dacché le orbite forniscono una partizione di $\mathcal{M}$, vale che:

$$|\mathcal{M}| = \sum_{X \in \mathcal{R}} \frac{|G|}{|\mathrm{Stab}(X)|},$$

dove $\mathcal{R}$ è un insieme di rappresentanti delle orbite e dove si è applicato il Teorema orbita-stabilizzatore. Dal momento che $p^{n-i} \parallel |M|$, esiste sicuramente un $X \in \mathcal{R}$ tale per cui $p^{n-i+1} \nmid |\mathrm{Orb}(X)|$, da cui si deduce che $p^i \mid |\mathrm{Stab}(X)|$.

Sia $x \in X$ e si consideri ora la mappa $\tau : \mathrm{Stab}(X) \to X$ tale per cui $g \overset{\tau}{\mapsto} gx$. Tale mappa è sicuramente iniettiva (infatti $gx = hx \implies g = h$), e quindi $|\mathrm{Stab}(X)| \leq |X| = p^i$. Si deduce dunque che $|\mathrm{Stab}(X)| = p^i$, da cui la tesi. $\square$

Esempio. Sia G un p-gruppo di ordine p^n con $n \geq 4$ tale per cui $|Z(G)| = p$. Si dimostra allora che G ammette un sottogruppo abeliano di ordine p^3.

Per il Primo teorema di Sylow, in ogni tale gruppo G si può estrarre un p-sottogruppo H di ordine p^4. Pertanto è sufficiente dimostrare la tesi per $n = 4$, dacché un sottogruppo di H è in particolare un sottogruppo di G.

Poiché G è un p-gruppo tale per cui $|Z(G)| = p$, esiste $x \in G$ tale per cui $Z_G(x)$ ha ordine p^3. Chiaramente $Z(G) \leq Z(Z_G(x))$, e analogamente $\langle x \rangle \leq Z(Z_G(x))$. Pertanto $|Z(Z_G(x))|$ ha almeno p^2 elementi. Se però valesse $|Z(Z_G(x))| = p^2$, $Z_G(x)/Z(Z_G(x))$ sarebbe ciclico, e quindi $Z_G(x)$ abeliano, $\lightning$. Quindi $Z(Z_G(x))$ ha ordine p^3 e coincide con $Z_G(x)$, da cui la tesi.

Si dimostra adesso il Secondo teorema di Sylow, che mostra che i p-Sylow sono tra loro coniugati e che dimostra l'esistenza di un'inclusione più generale tra i p-sottogruppi con i p-sottogruppi di cardinalità maggiore. Da questo teorema discenderà in particolare uno dei due risultati del Terzo teorema di Sylow sul numero di p-Sylow di un gruppo G.

Teorema (Secondo teorema di Sylow, coniugio e inclusione)**.** Tutti i p-Sylow di G sono coniugati (e quindi isomorfi) tra loro. Inoltre, ogni p-sottogruppo di ordine p^i, se $i \neq n$, è contenuto in un p-sottogruppo di ordine p^{i+1} (in particolare questi sottogruppi sono sottogruppi di un p-Sylow)[4].

[3] Infatti j può valere al più $p^i - 1$.

[4] Il Secondo teorema di Sylow implica in particolare che se H è un p-sottogruppo di ordine p^i, esiste sempre un p-sottogruppo K di G di ordine p^j con $j \geq i$ tale per cui $H \leq K$.

Dimostrazione. Sia[5] S un p-Sylow di G. Sia H un p-sottogruppo di ordine p^i e si consideri l'azione $\varphi : H \to S(X)$ su $X = G/S$ tale per cui $h \overset{\varphi}{\mapsto} [gS \mapsto hgS]$. Dal momento che $|X| = [G : S] = m$, per il Teorema orbita-stabilizzatore vale allora che:

$$m = \sum_{gS \in \mathcal{R}} \frac{p^i}{|\mathrm{Stab}(gS)|},$$

dove $\mathcal{R}$ è un insieme di rappresentanti delle orbite tramite φ.

Dal momento che $p \nmid m$ per ipotesi, deve esistere $gS \in \mathcal{R}$ tale per cui $|\mathrm{Stab}(gS)| = p^i$, da cui si deduce che $\mathrm{Stab}(gS) = H$. Pertanto vale che $hgS = gS \; \forall \, h \in H$, e quindi $hg \in gS$, da cui si ricava infine che $h \in gSg^{-1}$. Allora $H \subseteq gSg^{-1}$. Se allora H è un p-Sylow, $H = gSg^{-1}$ per cardinalità, e quindi tutti i p-Sylow sono coniugati tra loro, dimostrando la prima parte dell'enunciato.

Sia ora $i \neq n$. Allora H è un p-sottogruppo proprio di $P = gSg^{-1}$, che è un p-Sylow di G. Allora vale che $H \lneq N_P(H)$ dal momento che P è un p-gruppo. Dacché $H \triangleleft N_P(H)$, $N_P(H)/H$ è un p-gruppo non banale. Allora, per il Teorema di Cauchy, esiste $x \in N_P(H)$ tale per cui $\mathrm{ord}(xH) = p$. Allora $\pi_H^{-1}(\langle xH \rangle)$ è un sottogruppo di $N_P(H)$ di ordine $p \cdot p^i = p^{i+1}$ che contiene H, da cui la tesi. □

Osservazione. In particolare, se G è un gruppo abeliano finito, per il Secondo teorema di Sylow vale che $G(p)$, la p-componente di G, è unica in quanto p-Sylow di un gruppo abeliano (infatti l'insieme dei coniugati di un sottogruppo in un gruppo abeliano è sempre banale). Allora G è esattamente il prodotto diretto dei suoi p-Sylow.

Si dimostra infine il Terzo teorema di Sylow, che riguarda il numero di p-Sylow in G, indicato con n_p. Questo teorema, al di là del lato meramente computazionale, risulta spesso utile quando si cerca di dimostrare che un p-Sylow è caratteristico. Infatti è sufficiente verificare che n_p sia esattamente 1; in questo modo esiste un solo p-Sylow, e tale p-Sylow deve essere caratteristico, e quindi normale.

Teorema (Terzo teorema di Sylow, numero)**.** Sia n_p il numero di p-Sylow di G. Allora vale che:

- $n_p = [G : N_G(S_p)]$, e dunque n_p divide $|G|$, dove S_p è un p-Sylow,
- $n_p \equiv 1 \ (p)$, e quindi[6] $n_p \mid m$.

Dimostrazione. Poiché i coniugati di un p-Sylow S hanno la stessa cardinalità di S, tali coniugati sono ancora p-Sylow. Similmente, per il Secondo teorema di Sylow, tutti i p-Sylow sono a loro volta coniugati di S. Pertanto, se X è l'insieme dei p-Sylow

[5] Tale S esiste per il Primo teorema di Sylow.
[6] Poiché $n_p \mid |G| = p^n m$, ma $n_p \equiv 1 \ (p)$, n_p è coprimo con p^n, e quindi n_p deve dividere m.

di G, vale che X è esattamente l'insieme dei coniugati di S. Allora, per il Teorema orbita-stabilizzatore, vale che:

$$n_p = |X| = [G : N_G(S)],$$

che chiaramente divide $|G|$.

Sia $\varphi : S \to S(X)$ l'azione su X tale per cui $s \overset{\varphi}{\mapsto} [H \mapsto sHs^{-1}]$. Si mostra che $\mathrm{Orb}(S) = \{S\}$ è l'unica orbita banale. Se $\mathrm{Orb}(H)$ fosse banale, varebbe $sHs^{-1} = H$ $\forall\, s \in S$, e quindi varebbe $S \leq N_G(H)$. In tal caso esisterebbe il sottogruppo HS, che ha cardinalità:

$$|HS| = \frac{p^n p^n}{p^i} = p^{2n-i},$$

dove p^i è la cardinalità di $H \cap S$. Poiché n è il massimo esponente di un p-sottogruppo di G, deve valere $2n - i \leq n \implies n \leq i$. Allo stesso tempo, anche il massimo esponente di p in $H \cap S$, in quanto p-sottogruppo, deve essere minore o uguale a n, e quindi $n = i$. Pertanto $H = S$.

Allora, se $\mathcal{R}$ è un insieme di rappresentanti delle orbite di X tramite φ, vale che:

$$n_p = |X| = \sum_{H \in \mathcal{R}} \frac{p^n}{|\mathrm{Stab}(H)|} = 1 + \sum_{H \in \mathcal{R} \setminus \{S\}} \frac{p^n}{|\mathrm{Stab}(H)|}.$$

Poiché p divide la somma del membro a destra (infatti le orbite sono non banali, e quindi $|\mathrm{Stab}(H)| \neq p^n$), deve dunque valere $n_p \equiv 1 \pmod 1$, da cui la tesi. $\square$

Esempio. Si mostra che in un gruppo G di ordine $5 \cdot 11 \cdot 17$ esiste un elemento di ordine $11 \cdot 17$.

Si consideri un 11-Sylow P_{11} e un 17-Sylow P_{17}. Questi sottogruppi hanno ordine 11 e 17, e quindi sono ciclici. Pertanto esistono x, $y \in G$ tali per cui $P_{11} = \langle x \rangle$ e $P_{17} = \langle y \rangle$.

Si consideri n_{11}: n_{11} deve dividere $5 \cdot 17$, e quindi $n_{11} \in \{1, 5, 17, 5 \cdot 17\}$. Tuttavia $n_{11} \equiv 1$ (11) solo se $n_{11} = 1$. Quindi P_{11} è l'unico 11-Sylow, e pertanto è caratteristico, e dunque normale. Analogamente si verifica che $n_{17} = 1$, e quindi che anche P_{17} è normale.

Poiché P_{11} e P_{17} sono p-gruppi relativi a primi distinti, la loro intersezione è banale. Pertanto x e y commutano, e allora $\mathrm{ord}(xy) = \mathrm{ord}(x)\,\mathrm{ord}(y) = 11 \cdot 17$.