Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 17-04-2020

Il teorema di Sylow (prima parte)

Teorema (Sylow)

G gruppo finito, p numero primo, $l \in \mathbb{N}$ tali che $p^l \mid \#G \implies \exists\, H < G$ tale che $\#H = p^l$.

Corollario (teorema di Cauchy)

G gruppo finito, p numero primo tale che $p \mid \#G \implies \exists\, H < G$ tale che $\#H = p$ e $\exists\, g \in G$ tale che $\mathrm{ord}(g) = p$.

Osservazione

Per dimostrare il teorema di Cauchy basta trovare $a \in G$ tale che $\mathrm{ord}(a) = pm$ per qualche $m > 0$, (poi $g := a^m$ e $H := \langle g \rangle$).
Se G è abeliano, ciò può essere dimostrato facilmente per induzione su $n := \#G$. Per $n > p$ (il caso $n = p$ è chiaro) sia $b \in G \setminus \{1\}$:

- $p \mid \mathrm{ord}(b) \implies a := b$;
- $p \nmid \mathrm{ord}(b) \implies \overline{G} := G/\langle b \rangle$ tale che $p \mid \#\overline{G} < n \implies$ per induzione $\exists\, \bar{a} \in \overline{G}$ (con $a \in G$) tale che $p \mid \mathrm{ord}(\bar{a}) \mid \mathrm{ord}(a)$.

Dimostrazione della prima parte del teorema di Sylow

Per induzione su $n := \#G$. Per $n > p^l$ (il caso $n = p^l$ è chiaro) considero l'equazione delle classi:

$$\#Z(G) = \#G - \sum_{i=1}^{m} [G : C(a_i)]$$

con $1 < [G : C(a_i)] \mid n$ (quindi $C(a_i) \subsetneq G$) $\forall\, i = 1, \ldots, m$.

- Se $\exists\, i = 1, \ldots, m$ tale che $p^l \mid \#C(a_i)$, allora per induzione $\exists\, H < C(a_i) < G$ tale che $\#H = p^l$.
- Altrimenti $p \mid [G : C(a_i)]$ $\forall\, i = 1, \ldots, m$.
- Posso supporre $l > 0 \implies p \mid \#G \implies p \mid \#Z(G)$.
- Per il teorema di Cauchy per gruppi abeliani $\exists\, K < Z(G)$ tale che $\#K = p$; inoltre $K \triangleleft G$.
- $\overline{G} := G/K$ tale che $p^{l-1} \mid \#\overline{G} = n/p < n \implies$ per induzione $\exists\, \overline{H} < \overline{G}$ tale che $\#\overline{H} = p^{l-1}$.
- $\exists!\, H < G$ tale che $\overline{H} = H/K \implies \#H = (\#\overline{H})(\#K) = p^l$.

Il teorema di Sylow (seconda parte)

Definizione

G gruppo finito, p numero primo, r, m interi positivi tali che $\#G = p^r m$ e $p \nmid m$. Un p-sottogruppo di Sylow (o semplicemente un p-Sylow) di G è un sottogruppo di G di ordine p^r.
Indichiamo con $s_p = s_p(G)$ il numero di p-Sylow di G.

Osservazione

$s_p \geq 1$ per la prima parte del teorema di Sylow.

Teorema (Sylow)

G gruppo finito, p numero primo, r, m interi positivi tali che $\#G = p^r m$ e $p \nmid m$ $\Longrightarrow$

1. *due qualunque p-Sylow di G sono coniugati;*
2. *$s_p \equiv 1 \mod p$ e $s_p = [G : N(H)] \mid m$ $\forall$ H p-Sylow di G;*
3. *ogni p-sottogruppo di G è contenuto in un p-Sylow di G.*

Orbite di un p-Sylow

$\forall\, H, K < G$ sia $[K]_H := \{aKa^{-1} \,:\, a \in H\} \subseteq [K] = [K]_G$.
Chiaramente $[K]_H = \{K\} \iff H \subseteq N(K)$.

Lemma

$H, K < G$ con H p-gruppo e K p-Sylow.
Allora $[K]_H = \{K\} \iff H \subseteq K$. Altrimenti $p \mid \#[K]_H$.

Dimostrazione.

$\#[K]_H = [H : N(K) \cap H] \mid \#H = p^l$ per qualche $l \in \mathbb{N}$, quindi
$p \mid \#[K]_H$ se $\{K\} \subsetneq [K]_H$.
Resta allora da dimostrare che $H \subseteq N(K) \implies H \subseteq K$.
$H < N(K)$, $K \triangleleft N(K) \implies HK < N(K) < G$.
$H' := H \cap K < H$ tale che $\#H' = p^{l'}$ (con $l' \leq l$). Se $\#K = p^r$,

$$\#(HK) = \frac{(\#H)(\#K)}{\#H'} = \frac{p^l p^r}{p^{l'}} = p^{r+l-l'} \mid \#G = p^r m$$

con $p \nmid m \implies r + l - l' \leq r \implies l' = l \implies H' = H \subseteq K$. □

Dimostrazione della seconda parte del teorema di Sylow

Sia H un p-Sylow di G.
Se $K \in [H]_G$, chiaramente $[K]_H \subseteq [K]_G = [H]_G$ e per il Lemma $[K]_H = \{K\} \iff H \subseteq K \iff H = K$ (perché $\#H = \#K$), e altrimenti $p \mid \#[K]_H$. Ne segue che

$$\#[H]_G \equiv 1 \mod p.$$

Sia ora $H' < G$ un p-gruppo: analogamente a prima $[K]_{H'} \subseteq [K]_G = [H]_G \ \forall K \in [H]_G$, e per il Lemma $p \mid \#[K]_{H'}$ se $H' \nsubseteq K$. Ne segue che $\exists K \in [H]_G$ tale che $H' \subseteq K$ (altrimenti $p \mid \#[H]_G \equiv 1 \mod p$).
Ciò dimostra sia il punto 1 che il punto 3. Si ha inoltre

$$s_p = \#[H]_G = [G : N(H)] \mid [G : H] = m$$

e $s_p \equiv 1 \mod p$, il che dimostra anche il punto 2.

Sottogruppi di Sylow normali

Osservazione

Se $H < G$ è un p-Sylow, allora

$$H \triangleleft G \iff H \text{ caratteristico in } G \iff s_p = 1.$$

È infatti chiaro che $s_p = 1 \implies H$ caratteristico in $G \implies H \triangleleft G$.
D'altra parte, $H \triangleleft G \implies N(H) = G$, quindi $s_p = [G : N(H)] = 1$.

Corollario

$\#G = \prod_{i=1}^{k} p_i^{n_i}$ *con* $p_1, \ldots, p_k$ *numeri primi distinti e* $n_1, \ldots, n_k > 0$. *Sia* H_i *un* p_i*-Sylow di* $G \ \forall\, i = 1, \ldots, k$.

1. $s_{p_1} = \cdots = s_{p_k} = 1 \implies G \cong \prod_{i=1}^{k} H_i$.
2. $G \cong \prod_{i=1}^{k} G_i$ *con* G_i p_i*-gruppo* $\forall\, i = 1, \ldots, k \implies s_{p_i} = 1$ *e* $G_i \cong H_i \ \forall\, i = 1, \ldots, k$.

Dimostrazione

1. Per ipotesi $H_i \triangleleft G$ e $\#H_i = p_i^{n_i}\ \forall\, i = 1, \dots, k$.
   Dimostro per induzione su j che

$$H'_j := H_1 \cdots H_j \triangleleft G \quad \text{e} \quad H'_j \cong \prod_{i=1}^{j} H_i \quad \forall\, j = 1, \dots, k.$$

   È ovvio per $j = 1$; se $j > 1$, per induzione $H'_{j-1} \triangleleft G$ e $H'_{j-1} \cong \prod_{i=1}^{j-1} H_i$ (per cui $\#H'_{j-1} = \prod_{i=1}^{j-1} p_i^{n_i}$). Allora $H'_j = H'_{j-1} H_j \triangleleft G$ e (tenendo conto che $H'_{j-1} \cap H_j = \{1\}$ perché $\mathrm{mcd}(\#H'_{j-1}, \#H_j) = 1$) $H'_j \cong H'_{j-1} \times H_j \cong \prod_{i=1}^{j} H_i$.
   Se ne deduce che $G = H'_k \cong \prod_{i=1}^{k} H_i$ perché $\#G = \#H'_k$.
2. $G' := \prod_{i=1}^{k} G_i \implies \forall\, i = 1, \dots, k$

$$G'_i := \{(a_1, \dots, a_k) \in G' \,:\, a_j = 1\ \forall\, j \neq i\} \triangleleft G,$$

   G'_i è un p_i-Sylow di G' e $G'_i \cong G_i$. Allora $s_{p_i}(G) = s_{p_i}(G') = 1$ e $H_i \cong G'_i \cong G_i\ \forall\, i = 1, \dots, k$.

Gruppi di ordine pq

$\#G = pq$ con $p < q$ numeri primi. Allora

- $s_q = 1$ (perché $s_q \equiv 1 \mod q$ e $s_q \mid p$), e quindi G non è semplice;
- $q \not\equiv 1 \mod p \implies s_p = 1$ (perché $s_p \equiv 1 \mod p$ e $s_p \mid q$) e

$$G \cong C_p \times C_q \cong C_{pq}$$

(perché per il Corollario $G \cong H_p \times H_q$ con $H_p \cong C_p$ p-Sylow e $H_q \cong C_q$ q-Sylow).

Osservazione

Si vedrà che $q \equiv 1 \mod p \implies \exists!$ (a meno di isomorfismo) un gruppo non abeliano di ordine pq. Un esempio (per $p = 2$) è il gruppo diedrale D_q.

Gruppi di ordine p^2q

$\#G = p^2q$ con p e q numeri primi distinti $\implies$ $s_p = 1$ o $s_q = 1$ (quindi G non è semplice).

- Se $p > q$, allora $s_p = 1$ (perché $s_p \equiv 1 \mod p$ e $s_p \mid q$).
- Se $p < q$ e $s_q > 1$, allora $s_q = p^2$ (perché $s_q \equiv 1 \mod q$ e $s_q \mid p^2$). Poiché ogni q-Sylow ha $q-1$ elementi di ordine q e q-Sylow distinti si intersecano banalmente,

$$T := \{a \in G \,:\, \mathrm{ord}(a) = q\}$$

è tale che $\#T = s_q(q-1) = p^2(q-1)$.
H p-Sylow $\implies$ $H \subseteq G \setminus T$ $\implies$ $H = G \setminus T$ (perché $\#(G \setminus T) = p^2 = \#H$) $\implies$ $s_p = 1$.

Osservazione

Se $p < q$ e $s_q > 1$, allora $p = 2$ e $q = 3$:
infatti $s_q = p^2 \equiv 1 \mod q$, cioè $q \mid (p^2-1) = (p-1)(p+1)$;
poiché $q \nmid (p-1)$, deve essere $q \mid (p+1) \leq q$, e quindi $q = p+1$.
Un esempio di questo tipo è $G = A_4$ (esercizio).

Gruppi di ordine pqr

$\#G = pqr$ con $p < q < r$ numeri primi $\implies$ $s_q = 1$ o $s_r = 1$ (quindi G non è semplice).

- $T_n := \{a \in G : \mathrm{ord}(a) = n\}$ $\forall\, n > 0$ $\implies$ analogamente a prima $\#T_q = s_q(q-1)$ e $\#T_r = s_r(r-1)$. Deve essere

$$s_q(q-1) + s_r(r-1) = \#(T_q \cup T_r) \leq \#G = pqr,$$

  dato che $T_q \cap T_r = \emptyset$.
- $s_r > 1 \implies s_r = pq$ (perché $s_r \equiv 1 \mod r$ e $s_r \mid pq$) $\implies$ $s_q(q-1) \leq pq \implies s_q \leq q$ (dato che $q - 1 \geq p$) $\implies$ $s_q = 1$ (perché $s_q \equiv 1 \mod q$).

Osservazione

In effetti necessariamente $s_r = 1$: indicando con H_q un q-Sylow e con H_r un r-Sylow, $H_q \triangleleft G$ o $H_r \triangleleft G \implies H := H_q H_r < G$ e $\#H = qr \implies H_r \triangleleft H \implies H \subseteq N_G(H_r) \implies$ $s_r = [G : N_G(H_r)] \mid [G : H] = p \implies s_r = 1$.

I gruppi semplici non hanno sottogruppi di indice piccolo

$\{1\} \neq H < G$ tale che $2 \leq [G : H] \leq 4 \implies G$ non semplice.

- Per assurdo G semplice $\implies L\colon G \to S(G/H)$ è un omomorfismo iniettivo $\implies G' := \mathrm{im}(L) < S(G/H) \cong S_m$ (con $m := [G : H]$) tale che $G' \cong G$ e $n := \#G = \#G'$ soddisfa $m \mid n \mid m!$ (per il teorema di Lagrange) e $n > m$ (perché $H \neq \{1\}$).
- $m = 2 \implies 2 \mid n \mid 2$ e $n > 2$, impossibile.
- $m = 3 \implies 3 \mid n \mid 6$ e $n > 3 \implies n = 6 = 2 \cdot 3 \implies G$ non semplice, assurdo.
- $m = 4 \implies 4 \mid n \mid 24$ e $n > 4 \implies n = 8 = 2^3$ o $n = 12 = 2^2 \cdot 3$ o $n = 24$ ($\implies G \cong S_4$) $\implies G$ non semplice, assurdo.

Osservazione

Segue che G non è semplice se $\exists\, p$ primo tale che $p \mid \#G$ e $s_p = 3$ ($\implies p = 2$) o $s_p = 4$ ($\implies p = 3$).