CAPITOLO D

Teoremi di Sylow ed Applicazione

Il teorema di Lagrange asserisce che l'ordine di un sottogruppo di un gruppo finito è un divisore dell'ordine del gruppo. Il viceversa è però falso. Non vi sono molti teoremi che garantiscono l'esistenza di un sottogruppo di ordine assegnato in un gruppo finito arbitrario. Il più significativo è un lavoro dovuto al matematico norvegese Sylow.

In questo capitolo tratteremo i teoremi di Sylow che descrivono i sottogruppi di un gruppo finito arbitrario, aventi come ordine una potenza di un numero primo. Il primo teorema garantisce l'esistenza di tali sottogruppi, il secondo mette in evidenza la relazione di coniugio tra i p-sottogruppi di Sylow dello stesso ordine, mentre il terzo mostra le proprietà di divisibilità e congruenza del numero dei p-sottogruppi di Sylow, che in alcuni casi ci consentono di determinare con precisione il loro numero, come del resto avremo occasione di vedere in qualche applicazione. Infine concludiamo con un approfondimento della conoscenza di questi sottogruppi, studiando il loro comportamento in strutture quoziente e prodotti diretti.

D1. Teoremi di Sylow

Definizione D1.1. *Se G è un gruppo finito, p un numero primo e*

$$p^n \big| |G| \quad e \quad p^{n+1} \nmid |G| \quad con \quad n \in \mathbb{N}$$

un sottogruppo di G di ordine p^n si chiama p-sottogruppo di Sylow. Si tratta quindi di un sottogruppo il cui ordine è la massima potenza di p che divide l'ordine di G.

Lemma D1.2. *Siano p un numero primo e m un numero intero positivo. Allora vale la seguente congruenza*

$$\binom{mp^n}{p^n} \equiv m \pmod{p}.$$

DIMOSTRAZIONE. Per definizione di coefficiente binomiale si ha

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k} \equiv_p \begin{cases} 1, & k = 0,\ p; \\ 0, & 0 < k < p; \end{cases}$$

dove con $\equiv_p$ si indica la congruenza modulo p. Ora introdotte due variabili x, y consideriamo lo sviluppo binomiale

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

che ci conduce alle congruenze

$$(x+y)^p \equiv_p \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \equiv_p x^p + y^p,$$
$$(x+y)^{p^2} \equiv_p (x^p + y^p)^p \equiv_p x^{p^2} + y^{p^2}.$$

Continuando così abbiamo

$$(x+y)^{p^n} \equiv_p x^{p^n} + y^{p^n},$$
$$(x+y)^{mp^n} \equiv_p (x^{p^n} + y^{p^n})^m.$$

Sulla base di quest'ultima congruenza, considerando il coefficiente del termine $x^{p^n} y^{(m-1)p^n}$ si ha

$$\binom{mp^n}{p^n} \equiv_p \binom{m}{1} \equiv_p m. \qquad \square$$

Teorema D1.3 (Primo Teorema di Sylow). *Siano G un gruppo finito e p un primo che divide l'ordine di G. Allora G ha un p-sottogruppo di Sylow.*

DIMOSTRAZIONE. Per ipotesi $p \big| |G|$, allora possiamo scrivere

$$|G| = mp^n \quad \text{dove} \quad p \nmid m \quad \text{e} \quad n \geq 1.$$

Dimostriamo che esiste un sottogruppo di ordine p^n. Definiamo l'insieme Ω nel seguente modo

$$\Omega = \left\{ T \subseteq G \;\middle|\; |T| = p^n \right\}$$

e determiniamone la cardinalità.

Poiché il numero di modi di scegliere un sottoinsieme di p^n elementi da un insieme di mp^n è dato dal coefficiente binomiale, si ha

$$|\Omega| = \binom{mp^n}{p^n}.$$

Considerando ora l'azione di G su Ω così definita

$$(g, T) \longmapsto T^g = Tg \quad \text{per ogni} \quad T \in \Omega \quad \text{e} \quad g \in G$$

si ha che

$$\Omega = \bigcup_{T \in C} T^G$$

dove C è un sistema di rappresentanti per le orbite dei membri di Ω, quindi

$$|\Omega| = \sum_{T \in C} |T^G|.$$

Per il Lemma **D1.2**, vale la seguente congruenza

$$\binom{mp^n}{p^n} \equiv m \pmod{p} \quad \Longrightarrow \quad |\Omega| \equiv m \pmod{p}.$$

Dato che $p \nmid |\Omega|$, esiste un'orbita T^G tale che $p \nmid |T^G|$. Ora, considerando lo stabilizzatore di T, per il Teorema **C2.4** si ha $|T^G| = [G : G_T]$. G_T è un sottogruppo di G, se proviamo che $|G_T| = p^n$ abbiamo la tesi.

Dalla relazione $|G| = [G : G_T] \cdot |G_T|$ si ha che

$$|G_T| = \frac{|G|}{[G : G_T]}$$

pertanto

$$p^n \big| |G| \quad \text{e} \quad p \nmid [G : G_T] \quad \Longrightarrow \quad p^n \big| \, |G_T| \quad \Longrightarrow \quad |G_T| \geq p^n.$$

Inoltre dalla definizione di stabilizzatore si ha

$$\forall\, g \in G_T : \quad T^g = Tg = T \quad \Longrightarrow \quad \forall t \in T : \quad tG_T \subseteq T$$

quindi

$$|G_T| = |tG_T| \leq |T| = p^n \quad \Longrightarrow \quad |G_T| \leq p^n.$$

Dalla doppia disuguaglianza si ha $|G_T| = p^n$, pertanto G_T è proprio un p-sottogruppo di Sylow. □

Proposizione D1.4. *Sia G un gruppo finito tale che $|G| = mp^n$, dove p è un primo con* $\mathrm{mcd}(p, m) = 1$. *Allora nel gruppo G esistono p-sottogruppi di ordine $p, p^2, \cdots, p^n$.*

DIMOSTRAZIONE. Procediamo per induzione su $|G|$.

Quando $|G| = p$, la tesi è ovviamente vera. Supponiamo la tesi vera per tutti i gruppi di ordine minore di mp^n e dimostriamo che vale per $|G| = mp^n$.

Ricordiamo l'equazione delle classi

$$|G| = |Z(G)| + \sum_{k=1}^{\ell} |\mathrm{Cl}(x_k)|$$

dove $\{x_k\}_{k=1}^{\ell}$ è un sistema di rappresentanti delle classi di coniugio che contengono più di un elemento. Supponiamo che $p \big| |Z(G)|$, allora per il teorema

di Cauchy, esiste un sottogruppo in $Z(G)$ di ordine p. Ora, indicando con P_1 tale sottogruppo, non è difficile vedere che P_1 risulta un sottogruppo normale di G. Consideriamo il gruppo quoziente G/P_1 il cui ordine è dato da:

$$|G/P_1| = \frac{|G|}{|P_1|} = mp^{n-1} < mp^n$$

quindi, per l'ipotesi induttiva in G/P_1 esistono i sottogruppi

$$P_2/P_1,\ P_3/P_1,\ \cdots,\ P_n/P_1$$

di ordine rispettivamente $p, p^2, \cdots, p^{n-1}$. Ne segue che $P_1, P_2, \cdots, P_n$ sono p-sottogruppi di G di ordine rispettivamente $p, p^2, \cdots, p^n$.

Se $p \nmid |Z(G)|$ per l'equazione delle classi esiste una classe di coniugio $\mathrm{Cl}(x_k)$ tale che $p \nmid |\mathrm{Cl}(x_k)|$; ma

$$|\mathrm{Cl}(x_k)| = [G : C_G(x_k)] = \frac{|G|}{|C_G(x_k)|} \quad \Longrightarrow \quad |C_G(x_k)| = \frac{|G|}{|\mathrm{Cl}(x_k)|}$$

pertanto

$$p^n \big| |G| \quad \text{e} \quad p \nmid |\mathrm{Cl}(x_k)| \quad \Longrightarrow \quad p^n \big| |C_G(x_k)|.$$

Inoltre possiamo dire che

$$|C_G(x_k)| < |G| = mp^n \quad \text{perché} \quad x_k \notin Z(G).$$

Quindi applicando l'ipotesi induttiva si ha che in $C_G(x_k)$ esistono i sottogruppi $P_1, P_2, \cdots, P_n$ di ordine rispettivamente $p, p^2, \cdots, p^n$. Questi sono anche sottogruppi di G perché $C_G(x_k) \leq G$. □

Teorema D1.5 (Secondo Teorema di Sylow). *Siano G un gruppo finito e p un primo che divide l'ordine di G. Se P è un p-sottogruppo di G ed S un p-sottogruppo di Sylow di G, esiste $g \in G$ tale che $P \subseteq S^g$. In particolare:*

- *due p-sottogruppi di Sylow sono coniugati.*
- *ogni p-sottogruppo è un sottogruppo di qualche p-sottogruppo di Sylow.*
- *ogni p-elemento appartiene a qualche p-sottogruppo di Sylow.*

Dimostrazione. Poniamo $\Omega = \{Sg |\ g \in G\}$. Se $|G| = mp^n$ con $\mathrm{mcd}(m, p) = 1$, poiché S è un p-Sylow si ha $|S| = p^n$ e inoltre

$$|\Omega| = [G : S] = \frac{|G|}{|S|} = m \quad \Longrightarrow \quad p \nmid |\Omega|.$$

Definiamo ora un'azione di P su Ω come segue

$$(P, \Omega): \quad (x, Sg) \longmapsto (Sg)^x = Sgx$$

per la Proposizione **C2.6** abbiamo che

$$|\Omega| \equiv |\Omega_0| \pmod{p}$$

dove

$$\begin{aligned}\Omega_0 &= \Big\{Sg \in \Omega \mid Sgx = Sg \quad \forall\, x \in P\Big\} \\ &= \Big\{ \quad Sg \in \Omega \mid (Sg)^P \;=\; \{Sg\} \quad \Big\}.\end{aligned}$$

Poiché $p \nmid |\Omega|$ si ha che $p \nmid |\Omega_0|$; quindi Ω_0 è non vuoto cioè

$$\exists\, Sg \in \Omega_0 : \;\; Sgx = Sg \quad \forall\, x \in P$$

pertanto

$$gxg^{-1} \in S \quad \Longrightarrow \quad x \in S^g \quad \Longrightarrow \quad P \subseteq S^g.$$

Nel caso in cui P è un p-sottogruppo di Sylow

$$|P| = p^n \quad \text{e} \quad P \subseteq S^g \quad \Longrightarrow \quad P = S^g$$

perché $|S^g| = |S| = p^n$ e quindi P ed S risultano coniugati. Come conseguenza immediata, seguono le altre due affermazioni. □

Teorema D1.6 (Terzo Teorema di Sylow). *Siano G un gruppo finito e p un primo che divide l'ordine di G. Se n_p è il numero dei p-sottogruppi di Sylow di G ed S è un tale sottogruppo, allora*

$$n_p \;\Big|\; [G : S] \qquad e \qquad n_p \equiv 1 \pmod{p}.$$

DIMOSTRAZIONE. Ponendo Ω come l'insieme dei p-sottogruppi di Sylow di G, consideriamo la seguente azione di G su Ω

$$(G, \Omega): \quad (g, T) \quad \longmapsto \quad T^g = g^{-1}Tg$$

quindi l'orbita di un membro T, è la classe dei sottogruppi coniugati a cui T appartiene. Ma per il Teorema **D1.5** tutti i p-sottogruppi di Sylow sono coniugati, ne segue che l'azione considerata è transitiva. Pertanto

$$|\Omega| = |S^G| \quad \Longrightarrow \quad n_p = [G : G_S] = [G : N_G(S)].$$

Poiché $n_p = [G : N_G(S)]$ ed $S \leq N_G(S) \leq G$, si ha

$$n_p \;=\; \frac{[G : S]}{[N_G(S) : S]} \quad \Longrightarrow \quad n_p \mid [G : S].$$

Consideriamo un'altra azione

$$(S, \Omega): \quad (s, T) \;\longmapsto\; T^s = s^{-1}Ts.$$

Ricordando la congruenza nella Proposizione **C2.6**

$$|\Omega| \equiv |\Omega_0| \pmod{p}$$

dove

$$\Omega_0 = \big\{T \in \Omega \mid T^S = \{T\}\big\}$$

se proviamo che $|\Omega_0| = 1$ abbiamo subito la tesi dato che $|\Omega| = n_p$.

Osserviamo che

$$\forall\, x \in S : \;\; S^x = S \quad \Longrightarrow \quad S \in \Omega_0 \quad \Longrightarrow \quad \Omega_0 \neq \emptyset.$$

Verifichiamo che S è l'unico membro di Ω_0. Infatti supponendo che esista $T \in \Omega$ tale che $T^S = T$, si ha che

$$\forall\, x \in S: \quad T^x = T \quad \Longrightarrow \quad S \leq N_G(T)$$

quindi S e T sono entrambi p-sottogruppi di Sylow contenuti in $N_G(T)$. Notiamo che T è l'unico p-sottogruppo di Sylow del suo normalizzante $N_G(T)$. Inoltre S e T sono coniugati in $N_G(T)$ per il secondo teorema di Sylow. Allora $S = T$ e $|\Omega_0| = 1$. □

Corollario D1.7. *Sia G un gruppo abeliano finito. Allora*

(a) *G ha uno ed un solo p-sottogruppo di Sylow per ogni primo p che divide l'ordine di G.*
(b) *G è ciclico se e solo se i suoi sottogruppi di Sylow sono ciclici.*

DIMOSTRAZIONE. Procediamo per ordine, partendo dal primo punto.

[a] L'esistenza è garantita dal primo teorema di Sylow. L'unicità deriva dal fatto che due qualsiasi p-sottogruppi di Sylow sono coniugati.

Infatti, se S è un p-sottogruppo di Sylow, poiché G è abeliano, ogni suo sottogruppo è normale. Ne segue che l'insieme dei sottogruppi coniugati ad S in G coincide con S, quindi per ogni primo p che divide l'ordine di G esiste un unico p-sottogruppo di Sylow.

[b] La condizione necessaria segue dal fatto che ogni sottogruppo di un gruppo ciclico è ciclico. Ora dimostriamo la condizione sufficiente. Sia G un gruppo abeliano finito, allora possiamo scomporre l'ordine di G come segue:

$$|G| = \prod_{k=1}^{n} p_k^{m_k}$$

dove $\{p_k\}$ sono primi distinti e $\{m_k\}$ numeri naturali. Poiché G è abeliano, per ogni k esiste un unico p_k-sottogruppo di Sylow che indichiamo con S_k. Ora poiché ogni S_k è ciclico, se denotiamo con g_k il suo generatore si ha:

$$|S_k| = |\langle g_k \rangle| = p_k^{m_k} \quad \text{per} \quad k = 1, 2, \cdots, n.$$

Possiamo dunque definire un elemento $g = g_1 \cdot g_2 \cdots g_n$ che ovviamente appartiene a G, inoltre gli ordini dei generatori $g_1, g_2, \cdots, g_n$ sono coprimi, pertanto

$$o(g) = o(g_1) \cdot o(g_2) \cdots o(g_n) = \prod_{k=1}^{n} p_k^{m_k}.$$

Ne segue che G è un gruppo ciclico generato da g. □

D2. Applicazione e gruppi ciclici

Proposizione D2.1. *Dimostrare che per un primo p il numero dei p-sottogruppi di Sylow di S_p, gruppo simmetrico, è uguale a $(p-2)!$, da cui si deduce il teorema di Wilson*

$$(p-1)! \equiv -1 \pmod{p}.$$

DIMOSTRAZIONE. Indichiamo con n_p il numero dei p-sottogruppi di Sylow del gruppo simmetrico S_p. Se $n_p = (p-2)!$, allora per il terzo teorema di Sylow, si ha che

$$n_p \equiv 1 \pmod{p} \quad \Longrightarrow \quad (p-2)! \equiv 1 \pmod{p}.$$

Sfruttando la proprietà moltiplicativa delle congruenze, possiamo scrivere

$$(p-1)! \;=\; (p-1)(p-2)! \;\equiv_p\; p-1 \;\equiv_p\; -1.$$

A questo punto dimostriamo che il numero dei p-sottogruppi di Sylow di S_p è effettivamente $(p-2)!$. Poiché

$$|S_p| = p! : \qquad p \mid p! \qquad e \qquad p^2 \nmid p!$$

l'ordine di un p-sottogruppo di Sylow non può che essere p. Adesso, essendo p primo, ogni p-sottogruppo di Sylow è ciclico con $p-1$ generatori aventi tutti lo stesso ordine p. Quindi il numero totale dei generatori dei gruppi ciclici di ordine p è uguale a $(p-1)n_p$. Ogni elemento di ordine p in S_p risulta un p-ciclo. Dunque, se calcoliamo il numero dei p-cicli, questo deve coincidere con il numero totale dei generatori dei p-sottogruppi di Sylow. Considerando l'applicazione $\phi: \; S_p \longrightarrow S_p$ con

$$\begin{pmatrix} 1 & 2 & \cdots & p \\ x_1 & x_2 & \cdots & x_p \end{pmatrix} \longmapsto \begin{pmatrix} x_1 & x_2 & \cdots & x_p \\ x_2 & x_3 & \cdots & x_1 \end{pmatrix}$$

per $k = 1, 2, \cdots, p$, le permutazioni

$$\begin{pmatrix} 1 & 2 & \cdots & p-k & p-k+1 & \cdots & p \\ x_{k+1} & x_{k+2} & \cdots & x_p, & x_1 & \cdots & x_k \end{pmatrix}$$

hanno la stessa immagine. Dunque ϕ induce una corrispondenza p a 1, pertanto il numero dei p-cicli è:

$$\frac{p!}{p} = (p-1)! = n_p(p-1) \quad \Longrightarrow \quad n_p = \frac{(p-1)!}{p-1} = (p-2)!$$

che è la formula che volevamo dimostrare. □

Esempio D2.2. *Un gruppo di ordine* $15 = 3 \times 5$ *è ciclico.*

DIMOSTRAZIONE. Sia G un gruppo di ordine 15, indichiamo con n_3 il numero dei sottogruppi di Sylow di ordine 3 e con n_5 il numero dei sottogruppi di Sylow di ordine 5. Per il terzo teorema di Sylow si deve avere:

$$n_3 \equiv 1 \pmod 3 \quad \text{e} \quad n_3 \mid [15:3] = 5 \quad \Longrightarrow \quad n_3 = 1,$$

$$n_5 \equiv 1 \pmod 5 \quad \text{e} \quad n_5 \mid [15:5] = 3 \quad \Longrightarrow \quad n_5 = 1.$$

Quindi questi sottogruppi risultano essere normali in quanto essendo unici sottogruppi di Sylow di ordini 3 e 5 rispettivamente. Inoltre, poiché ogni gruppo finito il cui ordine è un numero primo è ciclico, possiamo scrivere

$$\begin{aligned} X &= \langle x \rangle : \quad \text{sottogruppo normale di ordine 3;} \\ Y &= \langle y \rangle : \quad \text{sottogruppo normale di ordine 5.} \end{aligned}$$

Ora poiché X e Y hanno in comune solo l'elemento neutro, risultano permutabili, infatti

$$x^{-1}y^{-1}xy = \begin{cases} x^{-1}x^y \in X, \\ (y^{-1})^x y \in Y; \end{cases}$$

pertanto

$$x^{-1}y^{-1}xy \in X \cap Y \implies x^{-1}y^{-1}xy = e \implies xy = yx.$$

Allora si ha che

$$o(xy) = \operatorname{mcm}\big(o(x), o(y)\big) = 15 = |G|.$$

Possiamo così concludere che G è ciclico. □

Questo esempio si generalizza con il seguente risultato.

Proposizione D2.3. *Siano p e q due primi con $p < q$ e $p \nmid (q-1)$. Allora ogni gruppo G di ordine pq è ciclico.*

DIMOSTRAZIONE. Indichiamo con n_p ed n_q i numeri dei p e q sottogruppi di Sylow. Per il terzo teorema di Sylow

$$n_p \mid q \quad \text{e} \quad n_p \equiv 1 \pmod p \implies n_p = 1,$$

$$n_q \mid p \quad \text{e} \quad n_q \equiv 1 \pmod q \implies n_q = 1;$$

dove si escludono i casi :

- $n_p = q$ perché per ipotesi $p \nmid (q-1) \implies q \not\equiv 1 \pmod p$;
- $n_q = p$ perché per ipotesi $p < q \implies p \not\equiv 1 \pmod q$.

Ovviamente questi sottogruppi sono ciclici, quindi possiamo scrivere

$$\begin{aligned} A &= \langle a \rangle : \quad \text{sottogruppo normale di ordine } p; \\ B &= \langle b \rangle : \quad \text{sottogruppo normale di ordine } q. \end{aligned}$$

Inoltre si ha che $A \cap B = \{e\}$ perché per qualunque $x \in A \cap B$, risulta che

$$\left.\begin{array}{l} x \in A \implies o(x) | p = |A| \\ x \in B \implies o(x) | q = |B| \end{array}\right\} \quad o(x) = 1 \quad \text{e} \quad x = e.$$

Dato che A è normale in G, consideriamo il gruppo quoziente G/A. Allora $G = \langle A, B \rangle$ se possiamo dimostrare che

$$G/A = \left\{ Ab^k \mid k = 1, 2, \cdots, q \right\}.$$

Infatti, basta verificare che questi q-laterali sono distinti. Supponiamo che esistono i e j con $1 \leq i < j \leq q$, tali che $Ab^i = Ab^j$, allora $A = Ab^{j-i}$ che è equivalente alla relazione $b^{j-i} \in A$. Dunque $o(b^{j-i}) = q | p = |A|$, che è impossibile.

Secondo il Teorema **A4.2**, si ha che G è prodotto diretto di A e B, cioè $G = A \otimes B$. Quindi a e b sono permutabili e $o(a \cdot b) = o(a) \cdot o(b) = pq$, che significa $|G| = pq = o(a \cdot b)$ e $G = \langle ab \rangle$ è ciclico. □

Esempio D2.4. *Un gruppo di ordine* 455 *è ciclico.*

DIMOSTRAZIONE. Se G è un gruppo di ordine 455, si ha che

$$|G| = 455 = 5 \cdot 7 \cdot 13.$$

usando la notazione dell'esempio precedente, denotiamo con

$$\left\{ \begin{array}{l} n_5 \\ n_7 \\ n_{13} \end{array} \right\} \quad \text{numero dei sottogruppi di Sylow di ordini} \quad \left\{ \begin{array}{l} 5 \\ 7 \\ 13 \end{array} \right\}.$$

Per il terzo teorema di Sylow si deve avere:

$$\begin{array}{lllllll} n_{13} \equiv 1 & (\text{mod } 13) & \text{e} & n_{13} \mid [455 : 13] = 35 & \implies & n_{13} = 1; \\ n_7 \equiv 1 & (\text{mod } 7) & \text{e} & n_7 \mid [455 : 7] = 65 & \implies & n_7 = 1; \\ n_5 \equiv 1 & (\text{mod } 5) & \text{e} & n_5 \mid [455 : 5] = 91 & \implies & n_5 = 1, 91. \end{array}$$

I sottogruppi di Sylow di ordine 5, 7, 13 ovviamente sono ciclici ed hanno in comune solo l'elemento neutro. Se proviamo che $n_5 \neq 91$ allora risultano anche tutti normali. Ne segue che G è uguale al prodotto diretto di tali sottogruppi per il Corollario **A4.3**. Dunque G è ciclico in quanto gli ordini dei suddetti sottogruppi sono numeri primi.

Supponiamo per assurdo $n_5 = 91$. Ogni sottogruppo di Sylow di ordine 5 ha 4 generatori di ordine 5, pertanto il numero totale degli elementi di ordine 5 è $91 \cdot 4 = 364$. Siano S_7 l'unico sottogruppo di Sylow di ordine 7 e S_{13} l'unico sottogruppo di Sylow di ordine 13. Allora

$$S_7, S_{13} \trianglelefteq G \quad \text{e} \quad S_7 \cap S_{13} = \{e\} \quad \implies \quad S_7 S_{13} = S_7 \otimes S_{13}.$$

Tutti gli elementi di $S_7 \otimes S_{13}$ hanno ordine coprimo con 5, inoltre

$$|S_7 \otimes S_{13}| = 7 \cdot 13 = 91.$$

Ora, sommando questi elementi con quelli di ordine 5 si ha $91 + 364 = 455$. Se troviamo un altro elemento il cui ordine non appartiene all'insieme

$$\{5, 7, 13, 91\} \quad \text{si ha} \quad |G| > 455$$

e necessariamente $n_5 = 1$ e G è ciclico.

Sia P_5 un qualunque sottogruppo di G di ordine 5. Posto $P = P_5P_7$, dimostriamo che P è un gruppo ciclico.

Siano $xy,\ x_1y_1 \in P$ con $x, x_1 \in P_5$ e $y, y_1 \in P_7$

$$xy = x_1y_1 \implies x_1^{-1}x = y_1y^{-1} \in P_5 \cap P_7 = \{e\}$$

$$\implies \begin{cases} x_1^{-1}x = e \\ y_1y^{-1} = e \end{cases} \implies \begin{cases} x = x_1 \\ y = y_1 \end{cases}$$

ne segue che la rappresentazione di P è unica e $|P| = 35$.

Per ogni $x \in P_5$ e $y \in P_7$, verifichiamo che $xy \in P \implies yx \in P$. Poiché

$$yx = (xx^{-1})yx = x(x^{-1}yx) = xy^x$$

si ha $yx \in P$ in quanto $P_7 \trianglelefteq G$ e $y^x \in P_7$. Quindi

$$(xy)^{-1} = y^{-1}x^{-1} \in P$$

conferma che ogni elemento ha il suo inverso in P.

Analogamente per ogni $x, x_1 \in P_5$ e $y, y_1 \in P_7$ possiamo affermare che

$$xy, x_1y_1 \in P \implies (xy)(x_1y_1) \in P.$$

Infatti, si vede facilmente che

$$(xy)(x_1y_1) = x(x_1x_1^{-1})y(x_1y_1) = xx_1(x_1^{-1}yx_1)y_1 = (xx_1)(y^{x_1}y_1) \in P$$

grazie di nuovo alla normalità di P_7. Pertanto P è chiuso.

Allora P è un gruppo di ordine 35. Inoltre dalla Proposizione **D2.3** segue che P è ciclico, quindi sicuramente contiene un elemento di ordine 35. □

Proposizione D2.5. *Siano p, q due primi distinti. Allora un gruppo di ordine pq^2 non è semplice* (cioè contiene un sottogruppo normale non banale).

DIMOSTRAZIONE. Sia G un gruppo finito con $|G| = pq^2$. Denotiamo con n_p il numero dei p-sottogruppi di Sylow di ordine p e n_q il numero dei q-sottogruppi di Sylow di ordine q^2.

Per confermare la tesi occorre dimostrare che $n_p = 1$ o $n_q = 1$.

Per il terzo teorema di Sylow valgono le seguenti relazioni:

$$n_p \mid \frac{pq^2}{p} = q^2 \quad \text{e} \quad n_p \equiv 1 \pmod{p};$$

$$n_q \mid \frac{pq^2}{q^2} = p \quad \text{e} \quad n_q \equiv 1 \pmod{q}.$$

Supponendo $n_p > 1$ ed $n_q > 1$ si ha

$$n_q = p \implies p \equiv 1 \pmod{q} \implies q \mid (p-1) \implies p > q.$$

Poiché $n_p = q$ implica $p|(q-1)$ e $p < q$, che è incompatibile con $p > q$, ne segue $n_q = p$ e $n_p = q^2$.

Ora per ogni p-sottogruppo di Sylow, abbiamo $p-1$ elementi di ordine p e due qualsiasi p-sottogruppi di Sylow distinti hanno in comune solo l'elemento neutro, quindi il numero totale dei p-elementi è uguale a

$$n_p(p-1) = q^2(p-1).$$

Mentre, se Q_1 e Q_2 sono due q-sottogruppi di Sylow con $Q_1 \neq Q_2$, si ha:

$$|Q_1 \cap Q_2| \mid q^2 \implies |Q_1 \cap Q_2| \leq q.$$

Pertanto il numero dei q-elementi è certamente maggiore o uguale a

$$n_q(q^2-q) + q = p(q^2-q) + q.$$

Poiché G deve contenere tutti i p-elementi e tutti i q-elementi possiamo scrivere

$$|G| \geq q^2(p-1) + p(q^2-q) + q = pq^2 + (p-1)q(q-1) > pq^2.$$

Ma questo è impossibile, quindi necessariamente $n_p = 1$ o $n_q = 1$, cioè G deve contenere un sottogruppo normale non banale. □

D3. Sottogruppo e gruppo quoziente

Lemma D3.1. *Siano G un gruppo finito e H un sottogruppo proprio di G. Se P_1 e P_2 sono due p-sottogruppi di Sylow di H, allora i p-sottogruppi di Sylow di G che li contengono sono distinti. Ne segue che il numero dei p-sottogruppi di Sylow di H non supera il numero dei p-sottogruppi di Sylow di G.*

DIMOSTRAZIONE. Sia H un sottogruppo di G con $|G| < \infty$. Supponiamo che P_1 e P_2 siano due p-sottogruppi di Sylow distinti di H. Per il secondo

teorema di Sylow, esistono in G due p-sottogruppi di Sylow S_1 e S_2 che contengono rispettivamente P_1 e P_2 come sottogruppi. Dobbiamo dimostrare che $S_1 \neq S_2$.

Supponendo per assurdo che $S_1 = S_2$ si ha che:

$$P_1 \subset H \quad \text{e} \quad P_1 \subset S_1 \quad \Longrightarrow \quad P_1 = H \cap S_1;$$

$$P_2 \subset H \quad \text{e} \quad P_2 \subset S_2 \quad \Longrightarrow \quad P_2 = H \cap S_2;$$

perché P_1 e P_2 sono p-sottogruppi massimali in H. Allora

$$P_1 = H \cap S_1 = H \cap S_2 = P_2.$$

Questo è assurdo perché P_1 e P_2 per ipotesi sono due p-sottogruppi di Sylow distinti di H, pertanto si ha la tesi. □

Proposizione D3.2. *Sia H un sottogruppo normale di un gruppo finito G. Allora valgono le seguenti affermazioni:*

(a) *Se S è un qualsiasi sottogruppo di Sylow di G, allora $H \cap S$ è un p-sottogruppo di Sylow di H.*
(b) *Se $p \nmid [G : H]$, allora H contiene tutti i p-sottogruppi di Sylow di G.*

DIMOSTRAZIONE. Sia G un gruppo finito con $H \trianglelefteq G$.

[a] Se T è un p-sottogruppo di Sylow di H, allora per il secondo teorema di Sylow esiste $g \in G$ tale che $T \subseteq S^g$ dove S è un p-sottogruppo di Sylow di G. Inoltre $T = H \cap S^g$ ed essendo H normale in G si ha

$$H \cap S^g = H^g \cap S^g = (H \cap S)^g.$$

Quindi $T = (H \cap S)^g$ e, ricordando che due sottogruppi coniugati hanno lo stesso ordine, ne segue

$$|T| = |(H \cap S)^g| = |H \cap S|.$$

Dunque $H \cap S$ risulta un p-sottogruppo di Sylow di H.

[b] Sia p^n la massima potenza di p tale che $p^n \big| |G|$. Poiché per ipotesi $p \nmid [G : H]$ si ha che $p^n \big| |H|$, allora, per il primo teorema di Sylow, esiste un p-sottogruppo di Sylow S contenuto in H con $|S| = p^n$. Ovviamente qualunque p-sottogruppo di Sylow T di G ha ordine p^n e, per il secondo teorema di Sylow, esiste $g \in G$ tale che $T = S^g$. Ora, essendo $H \triangleleft G$, esso contiene tutti i suoi coniugati quindi

$$T = S^g \subseteq H^g = H \quad \Longrightarrow \quad T \subseteq H.$$

Pertanto H contiene tutti i p-sottogruppi di Sylow di G. □

Teorema D3.3. *Siano G un gruppo finito e H un sottogruppo normale di G. Allora tutti e soli i p-sottogruppi di Sylow di G/H si ottengono come immagini dell'omomorfismo canonico dei p-sottogruppi di Sylow di G. Ne segue che il numero dei p-sottogruppi di Sylow di G/H non supera il numero dei p-sottogruppi di Sylow di G.*

DIMOSTRAZIONE. Poiché H è normale in G, possiamo considerare il gruppo quoziente G/H e l'omomorfismo canonico

$$\begin{aligned} \varphi: \quad G &\longrightarrow G/H; \\ g &\longmapsto Hg. \end{aligned}$$

Se S è un p-sottogruppo di Sylow di G, allora $\varphi(S) = HS/H$. Dobbiamo dimostrare che:

(a) HS/H è un p-sottogruppo di Sylow di G/H.
(b) tutti i p-sottogruppi di Sylow di G/H sono immagini di questo tipo, cioè se T/H è un p-sottogruppo di Sylow di G/H, allora esiste un p-sottogruppo di Sylow S di G tale che $\varphi(S) = HS/H = T/H$.

Queste due affermazioni vengono provate come segue.

[a] Per il teorema d'omomorfismo vale

$$\varphi(S) = \{Hx \mid x \in S\} = HS/H \leq G/H.$$

Non è difficile verificare che HS/H è un p-gruppo con l'ordine uguale a una potenza di p. Calcolando l'indice

$$[G/H : HS/H] = \frac{|G|}{|H|} \cdot \frac{|H|}{|HS|} = [G : HS]$$

risulta che

$$p \nmid [G/H : HS/H] = [G : HS] = \frac{[G : S]}{[HS : S]}$$

perché $S \leq HS \leq G$ e $p \nmid [G : S]$. Pertanto HS/H è un p-sottogruppo di G/H con l'ordine di massima potenza di p, cioè un p-sottogruppo di Sylow nel gruppo quoziente G/H.

[b] Se T/H è un p-sottogruppo di Sylow di G/H allora $p \nmid [G/H : T/H]$ e

$$[G/H : T/H] = \frac{|G|}{|H|} \cdot \frac{|H|}{|T|} = [G : T] \quad \Longrightarrow \quad p \nmid [G : T].$$

Allora, per il primo teorema di Sylow, esiste un p-sottogruppo di Sylow di T, denotato con S, che ovviamente è anche un p-sottogruppo di Sylow di G. Pertanto

$$S \leq T \quad \Longrightarrow \quad \varphi(S) \leq \varphi(T) \quad \Longrightarrow \quad HS/H \leq T/H.$$

Ma HS/H e T/H sono entrambi p-sottogruppi di Sylow di G/H quindi hanno lo stesso ordine, pertanto $T/H = HS/H$, cioè T/H risulta l'immagine di un p-sottogruppo di Sylow S di G mediante l'omomorfismo canonico. □

D4. Normalizzanti e sottogruppi di Sylow

Lemma D4.1. *Siano G un gruppo finito e S un p-sottogruppo di Sylow. Allora per un sottogruppo H con $S \leq N_G(S) \leq H \leq G$ si ha che $H = N_G(H)$. In particolare*

$$H = N_G(S) \quad \Longrightarrow \quad N_G(S) = N_G\big(N_G(S)\big).$$

DIMOSTRAZIONE. Secondo la definizione, vogliamo dimostrare che

$$N_G(H) = \{g \in G \mid H^g = H\} \;=\; H$$

cioè, che per ogni $g \in G$ vale l'implicazione: $H^g = H \implies g \in H$.

Sia $g \in G$ tale che $H^g = H$. Per ipotesi $S \leq H$, quindi S è un p-Sylow di H e $S^g \leq H^g = H$. Per il secondo teorema di Sylow S^g è ancora un p-Sylow di H, allora

$$\exists\, h \in H :\; S^g = S^h \quad \Longrightarrow \quad S^{gh^{-1}} = S.$$

Ne segue che

$$gh^{-1} \in N_G(S) \leq H \quad \Longrightarrow \quad g \in Hh = H. \qquad \square$$

Proposizione D4.2. *Siano G un gruppo finito e P un p-sottogruppo ma non di Sylow. Allora P è un sottogruppo proprio del suo normalizzante in G, cioè $P < N_G(P)$.*

DIMOSTRAZIONE. Per ipotesi P è un p-sottogruppo non di Sylow, quindi $p \,\big|\, [G : P]$. Distinguiamo ora due casi: $p \nmid [G : N_G(P)]$ e $p \mid [G : N_G(P)]$. Nel primo caso, abbiamo subito che $p|[N_G(P) : P]$ e $P < N_G(P)$ perché $[N_G(P) : P] = [G : P]/[G : N_G(P)]$.

Per il secondo caso, definiamo $\Omega := \{P^g | g \in G\}$. Allora seguendo la dimostrazione del Lemma **C4.2**, si ha che $p\big||\Omega| = [G : N_G(P)]$. Consideriamo ora la seguente azione

$$\begin{aligned}(P, \Omega) :\quad & P \times \Omega \;\longrightarrow\; \Omega;\\ & (g, Q) \;\longrightarrow\; Q^g = g^{-1}Qg.\end{aligned}$$

Secondo la Proposizione **C2.6**, vale la congruenza $|\Omega| \equiv |\Omega_0| \pmod p$ dove Ω_0 è l'insieme delle orbite aventi un solo membro. Osservando che $\Omega_0 \neq \emptyset$,

perché $P \in \Omega_0$ e $p \,\big|\, |\Omega_0| \equiv |\Omega| \pmod{p}$, abbiamo $|\Omega_0| > 1$. Pertanto

$$\exists\, Q \in \Omega_0 \text{ con } Q = P^g \neq P \text{ tale che } Q^P = Q \implies P \leq N_G(Q).$$

Dimostriamo che $Q \neq N_G(Q)$. Infatti, supponendo il contrario

$$Q = N_G(Q) \quad \text{e} \quad P \leq N_G(Q) \quad \Longrightarrow \quad P = Q$$

si giunge all'assurdo, pertanto $Q < N_G(Q)$. Allora possiamo concludere che

$$P = Q^{g^{-1}} < N_G^{g^{-1}}(Q) = N_G(Q^{g^{-1}}) = N_G(P)$$

grazie alle seguenti implicazioni bidirezionali:

$$\begin{aligned} x \in N_G^{g^{-1}}(Q) \quad &\Longleftrightarrow \quad g^{-1}xg \in N_G(Q); \\ Q^{(g^{-1}xg)} = Q \quad &\Longleftrightarrow \quad (Q^{g^{-1}})^{xg} = Q; \\ (Q^{g^{-1}})^x = Q^{g^{-1}} \quad &\Longleftrightarrow \quad x \in N_G(Q^{g^{-1}}). \end{aligned}$$

□

Corollario D4.3. *Sia P un p-gruppo finito. Allora ogni sottogruppo proprio non è uguale al suo normalizzante in P, cioè*

$$H < P \quad \Longrightarrow \quad H \neq N_P(H).$$

DIMOSTRAZIONE. Poiché P è un p-gruppo finito, ogni suo sottogruppo proprio non è di Sylow, quindi per la Proposizione **D4.2** segue la tesi.

Questo corollario può essere dimostrato direttamente per induzione su $|P|$.

Per $|P| = p$, non c'è nulla da dimostrare. Supponiamo la tesi vera per $|P| \leq p^n$, cioè ogni sottogruppo proprio di P è strettamente contenuto nel suo normalizzante. Sia $|P| = p^{n+1}$ e indichiamo con Z il centro di P. Dal Teorema **C3.4**, sappiamo che un p-gruppo finito ha il centro non banale, pertanto $|Z| > 1$ e $p \,||Z|$.

Sia H un qualunque sottogruppo proprio di P. Se $Z \nsubseteq H$, allora abbiamo subito che $H \neq N_P(H)$ perché $Z \subseteq N_P(H)$.

Invece nel caso $Z \subset H$, considerando i due gruppi quozienti H/Z e P/Z, si ha che

$$H < P \quad \Longrightarrow \quad H/Z < P/Z.$$

Poiché Z è non banale si ha $|P/Z| \leq p^n$. Per l'ipotesi induttiva $H/Z \neq N_{P/Z}(H/Z)$ dove

$$N_{P/Z}(H/Z) = N_P(H)/Z \qquad (\star)$$

pertanto

$$H/Z \neq N_P(H)/Z \quad \Longrightarrow \quad H \neq N_P(H).$$

La dimostrazione viene completata dalla conferma dell'equazione ($\star$):

$$\begin{aligned} N_{P/Z}(H/Z) &= \{xZ \in P/Z \mid (H/Z)^{xZ} = H/Z\} \\ &= \{xZ \in P/Z \mid H^x/Z = H/Z\} \\ &= \{xZ \in P/Z \mid x \in N_G(H)\} = N_G(H)/Z. \end{aligned}$$ □

D5. Prodotto diretto

Teorema D5.1. *Un gruppo finito G è prodotto diretto dei suoi sottogruppi di Sylow se e solo se ogni sottogruppo di Sylow è normale.*

DIMOSTRAZIONE. Secondo il teorema fondamentale dell'aritmetica vale la seguente scomposizione

$$|G| = \prod_{k=1}^{\ell} p_k^{m_k}$$

dove $p_1, p_2, \cdots, p_\ell$ sono primi distinti e $m_1, m_2, \cdots, m_\ell$ numeri naturali. Allora per ogni k con $1 \leq k \leq \ell$, esiste un p_k-sottogruppo S_k di Sylow in G.

"$\Longrightarrow$" Se $G = S_1 \otimes S_2 \otimes \cdots \otimes S_n$ dove $n \geq \ell$ e gli $\{S_k\}_{k=1}^n$ sono tutti i suoi sottogruppi di Sylow, allora per definizione di prodotto diretto, risultano $n = \ell$ ed ogni S_k compare una sola volta nel prodotto diretto. Quindi per ogni k con $k = 1, 2, \cdots, \ell$, esiste un unico p_k-sottogruppo S_k di Sylow in G, che è anche un sottogruppo normale.

"$\Longleftarrow$" Se $S_i \trianglelefteq G$ con $i = 1, 2, \cdots, \ell$ allora per ogni i esiste un unico p_i-sottogruppo di Sylow. Possiamo quindi considerare il prodotto degli S_i per $i = 1, 2, \cdots, \ell$ e dimostrare che $G = S_1 \otimes S_2 \otimes \cdots \otimes S_\ell$.

Banalmente $|G| = \prod_{i=1}^{\ell} |S_i|$. Ora, consideriamo S_i e S_j con $1 \leq i < j \leq \ell$:

$$\forall\, x \in S_i,\ \forall\, y \in S_j : \quad xy = yx \quad \Longleftrightarrow \quad x^{-1}y^{-1}xy = e.$$

Osserviamo che

$$\begin{cases} x^{-1}y^{-1}xy = x^{-1}x^y \in S_i; \\ x^{-1}y^{-1}xy = (y^{-1})^x y \in S_j. \end{cases}$$

Inoltre, il teorema di Lagrange asserisce che

$$\left.\begin{array}{l} |S_i \cap S_j| \,\big|\, |S_i| \\ |S_i \cap S_j| \,\big|\, |S_j| \end{array}\right\} \quad \Longrightarrow \quad |S_i \cap S_j| = 1.$$

Abbiamo quindi

$$x^{-1}y^{-1}xy \in S_i \cap S_j = \{e\} \quad \Longrightarrow \quad xy = yx.$$

Secondo il Corollario **A4.3**, la tesi segue dal fatto che i sottogruppi $\{S_i\}_{i=1}^{\ell}$ permutano elemento per elemento. □

Corollario D5.2. *Un gruppo finito G è prodotto diretto dei suoi sottogruppi di Sylow se solo se non esiste un sottogruppo proprio in G che è uguale al suo normalizzante.*

DIMOSTRAZIONE. Supponiamo come prima che G sia un gruppo finito con $|G| = \prod_{i=1}^{\ell} p_i^{m_i}$ dove p_i sono primi distinti e m_i numeri naturali.

"$\Longleftarrow$" Sia S_i un p_i-sottogruppo di Sylow, allora per il Lemma **D4.1**

$$N_G(S_i) = N_G\big(N_G(S_i)\big).$$

Ma per ipotesi, non esiste un sottogruppo proprio in G che è uguale al suo normalizzante, per cui $N_G(S_i) = G$. Allora S_i è normale, quindi per ogni indice i esiste un unico p_i-sottogruppo di Sylow S_i e per il Teorema **D5.1** risulta che G è uguale al prodotto diretto dei suoi p-sottogruppi di Sylow.

"$\Longrightarrow$" Siano $\{S_i\}_{i=1}^{\ell}$ sottogruppi di Sylow con $|S_i| = p_i^{m_i}$ tali che

$$G = S_1 \otimes S_2 \otimes \cdots \otimes S_\ell.$$

Per ogni sottogruppo proprio H di G, dobbiamo provare che $H \neq N_G(H)$. Affermiamo prima che vale il seguente prodotto diretto:

$$H = \bigotimes_{k=1}^{\ell} (H \cap S_k). \qquad (\star)$$

Per ogni $h \in H$, si ha che $o(h) \mid |G|$. Allora esistono ℓ-numeri naturali $\{n_i\}$ tali che $o(h) = \prod_{i=1}^{\ell} p_i^{n_i}$ con $0 \leq n_i \leq m_i$. Secondo il Lemma **B2.3**, h si scrive in modo unico come prodotto $h = h_1 h_2 \cdots h_\ell$, dove h_i risulta una potenza di h con $o(h_k) = p_k^{n_k}$. Ricordando che S_k è l'unico p_k-sottogruppo di Sylow di G, allora $h_k \in S_k$. Inoltre, $h_k \in H$ perché h_k è una potenza di h. Dunque $h_k \in H \cap S_k$ e $h \in \bigotimes_{k=1}^{\ell}(H \cap S_k)$. Notando il fatto ovvio $\bigotimes_{k=1}^{\ell}(H \cap S_k) \subseteq H$, otteniamo che $H = \bigotimes_{k=1}^{\ell}(H \cap S_k)$.

Ma H è un sottogruppo proprio di G, perciò esiste k con $1 \leq k \leq m$ tale che $H \cap S_k < S_k$. Grazie al Corollario **D4.3** si ha che

$$H \cap S_k < N_{S_k}(H \cap S_k).$$

Dal prodotto diretto risulta che

$$H = (H \cap S_k) \bigotimes_{i=1,\, i\neq k}^{\ell} (H \cap S_i)$$

$$< N_{S_k}(H \cap S_k) \bigotimes_{i=1,\, i\neq k}^{\ell} (H \cap S_i)$$

$$\leq N_{S_k}(H \cap S_k) \bigotimes_{\substack{i=1\\ i\neq k}}^{\ell} N_{S_i}(H \cap S_i).$$

Il risultato finale $H \neq N_G(H)$ viene conseguito se proviamo la seguente equazione:

$$N_G(H) = \bigotimes_{k=1}^{\ell} N_{S_k}(H \cap S_k). \qquad (\star\star)$$

Ricordando $(\star)$, si ha

$$N_G(H) = \bigotimes_{k=1}^{\ell} \Big\{ S_k \cap N_G(H) \Big\}$$

che implica $(\star\star)$ se possiamo provare che per ogni $1 \leq k \leq \ell$, vale

$$N_{S_k}(H \cap S_k) = S_k \cap N_G(H).$$

Questa equazione si verifica tramite doppia inclusione. Infatti, per ogni $x \in S_k \cap N_G(H)$, abbiamo

$$(H \cap S_k)^x = H^x \cap S_k^x = H \cap S_k$$

che equivale a $x \in N_{S_k}(H \cap S_k)$. Viceversa per ogni $y \in N_{S_k}(H \cap S_k)$, si ha ovviamente $y \in S_k$. Richiamando il prodotto diretto, deduciamo che

$$H^y = \bigotimes_{i=1}^{\ell} (H \cap S_i)^y = (H \cap S_k)^y \bigotimes_{i\neq k} (H \cap S_i)^y = (H \cap S_k) \bigotimes_{i\neq k} (H \cap S_i) = H$$

perché y commuta con tutti gli elementi di $H \cap S_i$ con $i \neq k$. Dunque $y \in N_G(H)$ e conseguentemente $y \in S_k \cap N_G(H)$.

Possiamo anche dimostrare $(\star\star)$ direttamente tramite doppia inclusione.

Per ogni $x \in N_G(H)$, esistono $x_k \in S_k$ e $x_k \in \langle x \rangle$ con $1 \leq k \leq \ell$ tali che

$$x = x_1 x_2 \cdots x_\ell \in \bigotimes_{k=1}^{\ell} N_{S_k}(H \cap S_k)$$

grazie al Lemma **B2.3** ed al prodotto diretto $G = \bigotimes_{k=1}^{\ell} S_k$.

Invece per ogni $y \in \bigotimes_{k=1}^{\ell} N_{S_k}(H \cap S_k)$ esistono $y_k \in N_{S_k}(H \cap S_k)$ tali che $y = y_1 y_2 \cdots y_\ell$. Allora per ogni k con $1 \leq k \leq \ell$, si verifica che

$$\begin{aligned} H^{y_k} &= \left\{ \bigotimes_{i=1}^{\ell} (H \cap S_i) \right\}^{y_k} = \bigotimes_{i=1}^{\ell} (H \cap S_i)^{y_k} \\ &= (H \cap S_k)^{y_k} \bigotimes_{i \neq k} (H \cap S_i)^{y_k} \\ &= (H \cap S_k) \bigotimes_{i \neq k} (H \cap S_i) = H. \end{aligned}$$

Quindi $H^y = H^{y_1 y_2 \cdots y_\ell} = H$, che implica $y \in N_G(H)$. □

Teorema D5.3. *Siano G un gruppo finito e N un sottogruppo normale. Se P è un p-sottogruppo di Sylow di N, allora*

$$G = N_G(P)N.$$

DIMOSTRAZIONE. L'inclusione " $\supseteq$" è ovvia. Per ogni $g \in G$, si vede facilmente che $P \leq N$ implica $P^g \leq N^g = N$; pertanto P e P^g risultano p-sottogruppi di Sylow di N. Per il secondo teorema di Sylow, esiste $x \in N$ tale che $P^g = P^x$. Quest'ultimo equivale a $P^{gx^{-1}} = P$, cioè $gx^{-1} \in N_G(P)$ e quindi $g \in N_G(P)x$, che implica $g \in N_G(P)N$. □