TEOREMI DI SYLOW

Sia G un gruppo finito, sia p un numero primo

1) G ha almeno un p-Sylow.
   [se p non divide $|G|$ è banale]

2) Due p-Sylow sono coniugati

3) Ogni p-sottogruppo di G è contenuto in un p-Sylow

4) Il numero dei p-Sylow è un divisore di $|G|$ ed è congruente a 1 modulo p

Dimostrazione [molte dimostrazioni; questa dovuta principalmente a Wielandt (1910-2001)]

Supponiamo p divide $|G|$ e consideriamo n, m t.c $|G| = p^n m$ con $MCD(p, m) = 1$

Definiamo:

$$\Omega = \{ A \subseteq G \mid A \text{ ha } p^n \text{ elementi} \}$$

[insieme dei sottoinsiemi di G con p^n elementi]

Osserviamo che:

- G agisce su $\mathcal{A}$ considerando

$$g : \mathcal{A} \longrightarrow \mathcal{A}$$
$$A \to Ag$$

- p non divide la cardinalità di $\mathcal{A}$

Esercizio: verificare che $|\mathcal{A}| \neq 0 \bmod p$

Questa azione dà la seguente formula:

$$|\mathcal{A}| = \sum_{A \in \Gamma} |\mathcal{O}_G(A)|$$

dove Γ contiene un rappresentante per ogni orbita

- Siccome $|\mathcal{A}| \neq 0 \bmod p$ allora esiste A_0 tale che $|\mathcal{O}_G(A_0)| \neq 0 \bmod p$

$$\Rightarrow |\mathcal{O}_G(A_0)| = \frac{|G|}{|\mathrm{stab}_G A_0|} \neq 0 \bmod p$$

$$\Rightarrow p^n \mid \mathrm{stab}_G A_0$$

D'altra parte per $a \in A$

$$\underbrace{a\ stab_G(A_0)}_{\text{laterale di } a \text{ rispetto } stab_G(A_0)} \subseteq A_0$$

Quindi

$$p^n \leq |stab_G A_0| = |a\ stab_G A_0| \leq |A_0| = p^n$$

$\Rightarrow$ $stab_G A_0$ è un p-Sylow ◭

Si consideri ora U un p-sottogruppo di G

U agisce su $O_G(A_0)$ $\left(\begin{array}{c} u : O_G(A_0) \to O_G(A_0) \\ B \to Bu \end{array} \right)$

e abbiamo che $|U| = p^k$ e $|O_G(A_0)| \not\equiv 0 \pmod p$

Per proposizione su azione di gruppi abbiamo che:

> esiste $B_0 \in O_G(A_0)$ fissato dall'azione di U i.e $stab_G(B_0) \supseteq U$

Inoltre per esercizio già visto siccome $B_0 \in O_G(A_0)$ allora esiste $n \in G$ t.c $stab_G A_0 = (stab_G B_0)^n$

Sottogruppi coniugati hanno lo stesso ordine

quindi $stab_G(B_0)$ è un p-Sylow che contiene U (questo dimostra punto 3))

Inoltre $U^{x^{-1}} \subseteq stab_G A_0$ e se U è un p-Sylow otteniamo $|U^{x^{-1}}| = |stab_G A_0| = p^n$ e $U^{x^{-1}} = stab_G A_0$

$\Rightarrow$ tutti i p-Sylow sono coniugati ad un p-Sylow fissato e siccome il coniugio è una relazione di equivalenza sono tutti coniugati fra di loro

(fine dim punto 2)

Per dimostrare la prima parte del punto 1) basta osservare che

$$|\{p\text{-Sylow di } G\}| = |\{\text{coniugati } S_0\}| = \frac{|G|}{|N_G(S_0)|}$$

dove S_0 p-Sylow fissato da cui si ottiene $|\{p\text{-Sylow di } G\}| \setminus |G|$

Per dimostrare le seconde parte del punto 4) dimostreremo prima un Lemma e poi una proposizione:

Lemma: Sia S un p-Sylow di G

U p-sottogruppo di $N_G(S) \Rightarrow U \leq S$

Dim: S è l'unico p-Sylow di $N_G(S)$

infatti

- $|N_G(S)| \setminus |G| \Rightarrow |S|$ è la massima potenza di p che divide $|N_G(S)|$
- S' p-Sylow di $N_G(S) \Rightarrow$

$\Rightarrow \exists x \in N_G(S)$ t.c. $S' = S^x$

ma $x \in N_G(S)$ e quindi $S' = S^x = S$

per 3) del Teor. di Sylow abbiamo che $U \subseteq S$ ∎

Proposizione Sia U p-sottogruppo di G allora:

$$|\{S \supseteq U \mid S \ p\text{-Sylow}\}| \equiv 1 \mod p$$

[Questa proposizione implica la 2ª parte di 4) basta prendere $U = \{1_G\}$]

Dim. Sia U p-sottogruppo fissato e sia S p-Sylow di G. Definiamo $H \overset{\text{def}}{=} N_G(S)$

I laterali doppi HxU formano una partizione di G

Definiamo $X \subseteq G$ contenente esattamente un elemento per ogni laterale doppio.

Claim: esiste una biezione

$$\{x \in X \mid U \subseteq S^x\} \longleftrightarrow \{T \ p\text{-Sylow} \mid U \subseteq T\}$$

Definisco $\phi : \{x \in X \mid U \subseteq S^x\} \to \{T \ p\text{-Sylow} \mid U \subseteq T\}$

$$\phi(x) = S^x$$

ϕ è iniettivo: $S^x = S^y \Rightarrow x^{-1} S x = y^{-1} S y$

$\Rightarrow x y^{-1} S y x^{-1} = S \Rightarrow y x^{-1} \in N_G(S) = H$

$\Rightarrow \exists h \in H$ t.c. $y = hx$

$\Rightarrow HyU = HhxU = HxU$

Siccome $x, y \in X \Rightarrow x = y$

ϕ è suriettivo:

Sia T p-Sylow tale che $T \supseteq U$

$\Rightarrow T = S^y$ con $y \in G$

punto 2)

Per definizione di X e siccome i laterali doppi sono una partizione esiste $x \in X$ tale che $y \in HxU$

$\Rightarrow \exists h \in H, u \in U$ t.c $y = hxu$

$\Rightarrow S^y = y^{-1} S y = \underbrace{(hxu)^{-1}}_{u^{-1}x^{-1}h^{-1}} S hxu$

$\Rightarrow u S^y u^{-1} = x^{-1} \underbrace{h^{-1} S h}_{S \text{ perchè } h \in H = N_G(S)} x$

$\Rightarrow \quad S^g = x^{-1} S x = S^x$

$U \leq S^g$

$\Rightarrow \quad \phi(x) = S^g = T$

Questo conclude la dimostrazione del Claim ◀

Abbiamo dimostrato parlando di laterali doppi la seguente formula:

$$|G : H| = \sum_{x \in X} |U : U \cap H^x|$$

Siccome U è un p-gruppo abbiamo che $|U : U \cap H^x|$ è una potenza di p

Quando $|U : U \cap H^x| = p^0 = 1$?

$|U : U \cap H^x| = 1 \iff U \leq H^x \iff$

$\iff x U x^{-1} \leq H = N_G(S) \iff$

$\iff x U x^{-1} \leq S \iff U \leq S^x$

↖ Lemma

$$|G:H| = \sum_{\substack{x \in X \\ |U : U \cap H^x| \neq 1}} |U : U \cap H^x| + n(U)$$

dove $n(U) = |\{x \in X \mid U \subseteq S^x\}|$

$$n(U) = |\{T \text{ } p\text{-Sylow} \mid U \subseteq T\}|$$

se $|U : U \cap H^x| \neq 1$ allora $p \mid |U : U \cap H^x|$

quindi

$$|G:H| \equiv n(U) \pmod{p}$$

Se $U = S$ allora $n(S) = 1$

Quindi otteniamo per ogni U

$$1 = n(S) \equiv |G:H| \equiv n(U) \pmod{p}$$

[Questo conclude la dim della proposizione e del teorema di Sylow] ∎

Corollario G gruppo tale che $|G| = pq$ p, q due primi distinti

Allora G ammette un sottogruppo normale

Dim: Supponiamo che $q > p$

Consideriamo S_q un q-Sylow di G

$$|\{\text{coniugati di } S_q\}| = \frac{|G|}{|N_G(S_q)|} \quad \begin{cases} \nearrow p \\ \searrow 1 \end{cases}$$

$$\| \\ |\{q\text{-Sylow di } G\}|$$

- nel II caso $N_G(S_q) = G$ e S_q è normale
- nel I caso

Teor. di Sylow $\Rightarrow |\{\text{coniugati di } S_q\}| \equiv 1 \bmod q$

$\Rightarrow p \equiv 1 \bmod q \Rightarrow p = 1 + kq > q + 1$

e ottengo una contraddizione con $q > p$

∎

Problema: il teorema di Sylow sembra invertire il teorema di Lagrange

Se $p^k \mid |G|$ allora $\exists H \leq G$ t.c $|H| = p^k$

Vale anche per un qualsiasi divisore di $|G|$? In realtà non vale

Trovare un controesempio