Capitolo 3: I teoremi di Sylow:

Introduzione:
I teoremi di Sylow ci permettono di individuare alcune proprietà di un gruppo conoscendone esclusivamente la cardinalità. Fissato il numero di elementi di un gruppo si va s scomporlo nei suoi fattori primi e da essi si individuano particolari sottogruppi. Usando i teoremi aggiuntivi riportati in fondo si può determinare il rapporto fra questi gruppi stabilendo se si tratta di un prodotto diretto o semidiretto e se si d quale tipo.

Sia G un gruppo finito di ordine $n = p^a m$, $(p, m) = 1$

Teorema 1 (Teorema di Esistenza):

G possiede un sottogruppo di ordine p^a

Corollario:
$\forall b \leq a$, G possiede un sottogruppo di ordine p^b

Teorema 2 (Teorema di Coniugio) :

Sia $H < G$ un p-gruppo (Ossia $|H| = p^b$, $b \leq a$) e sia P un p-sottogruppo di Sylow di $G \to H$ è contenuto in un coniugato di P $(H \subseteq P' = xPx^{-1})$

Notazione:
p-sottogruppo di Sylow o p-Sylow è un sottogruppo di cardinalità p^a con a il massimo esponente di p nella cardinalità del gruppo.

Corollario:
I p-Sylow di G sono tutti coniugati.

Corollario:
Se esiste un solo p-Sylow questo è normale (In quanto l'unico coniugato è se stesso).

Teorema 3 (Teorema del numero):

Il numero dei p-Sylow $\equiv 1\ (\mathrm{p})$
Il numero dei p-Sylow divide l'indice di un generico p-Sylow.

Osservazione:
Questo teorema ci permette di capire quasi sempre il numero esatto dei p-Sylow in quanto la doppia informazione ci riduce ad una manciata di casi facilmente studiabili.
Inoltre nei Sylow abbiamo sempre degli elementi facili a individuare (Quelli di ordine il primo) che possiamo sfruttare per portare ad un assurdo nel caso di un numero troppo alto di p-Sylow ipotizzati.

Gli altri teoremi che sono spesso utili nello studio dei gruppi mediante i teoremi di Sylow sono:

Proprietà 1 (Cardinalità):

G finito, $H, K < G \rightarrow |H||K| = |H \cap K||HK|$

> **Osservazione:**
> Questa proprietà è insiemistica, ossia è valida a prescindere dal fatto che HK, detto **Prodotto di Frobenius** sia un gruppo.

Proprietà 2 (Due gruppi commutano):

$H, K \lhd G$ e $H \cap K = \{e\} \rightarrow hk = kh \; \forall h \in H \; \forall k \in K$

Condizioni per il prodotto diretto:

Siano G gruppo e $H, K < G$ |

1- $H \lhd G \wedge K \lhd G$
2- $H \cap K = \{e\}$
3- $HK = G$

Allora $G \cong H \times K$

Condizioni per il prodotto semidiretto:

Siano G gruppo e $H, K < G$ |

1- $H \lhd G$
2- $H \cap K = \{e\}$
3- $HK = G$

Allora $G \cong H \rtimes_{\varphi} K$ con $\varphi: K \rightarrow \mathrm{Aut}(H)$ l'omomorfismo che associa ad ogni $k \in K$ l'automorfismo interno $\varphi_k: \varphi_k(h) = khk^{-1}$

> **Attenzione:**
> Siccome $\varphi: K \rightarrow \mathrm{Aut}(H)$ è possibile da questo ricavare alcune ulteriori informazioni. Infatti se abbiamo K gruppo ciclico generato da x allora $\mathrm{ord}\big(\varphi(x)\big) \mid |\mathrm{Aut}(H)|$ etc.

> **Osservazione sull'esistenza:**
> Se ci interessa solamente dimostrare l'esistenza di un dato prodotto semidiretto possiamo ricordarci che assegnato G, se $n \mid |\mathrm{Aut}(G)|$ allora per il teorema di Cauchy esiste un elemento n $\mathrm{Aut}(G)$ di ordine n e quindi esiste il prodotto semidiretto $G \rtimes_{\varphi} \mathbb{Z}_n$ con φ che associa al generatore di $\mathbb{Z}_n$ proprio l'elemento f.

Esercizi ed esempi

Gli esercizi riguardanti i p-Sylow riguardano principalmente lo studio di un gruppo di cui non sappiamo altro che la cardinalità.
Viene richiesto ad esempio di dimostrare che un gruppo di cardinalità data non può essere semplice (Esibendo un Sylow normale) o che esiste un gruppo ciclico di ordine dato (Mostrando che è prodotto diretto di gruppi ciclici).
I gruppi di Sylow sono facili da studiare in quanto si scambiano per coniugio e, di conseguenza, se ne esiste uno solo è normale.

Esempio 1 (Ciclico):
Un gruppo G di ordine pq ; $p < q$; $p \nmid (q-1) \rightarrow G$ ciclico.

Il teorema di Sylow mi assicura l'esistenza dei due sottogruppi ciclici di ordine *p* e *q* , H_p , H_q.
Per dimostrare che G è ciclico posso mostrare che è prodotto diretto di questi due gruppi ciclici.
Condizioni per il prodotto diretto:

1- $H_p \cap H_q = \{1\}$, infatti se $x \in H_p \cap H_q \rightarrow ord(x)|p$; $ord(x)|q \rightarrow ord(x) = 1 \rightarrow x = 1$
2- $H_p \lhd G$, per farlo dimostro che è unico nella sua orbita, $\#p \equiv 1\ (p)$; $\#p|q \rightarrow \#q = 1$ oppure q, se $\#p = q \rightarrow q \equiv 1\ (p) \rightarrow p|(q-1)$ ASSURDO.
3- $H_q \lhd G$, allora $\#q = 1$ oppure p , se $\#q = p \rightarrow p \equiv 1\ (q) \rightarrow q|(p-1)$ ASSURDO.
Quindi $G = H_p \times H_q$.

Esempio 2 (Numero elementi):
Dato un gruppo G di ordine pqr ; $p < q < r \rightarrow \exists$ un Sylow normale

Idea:
I p-Sylow hanno la proprietà di avere un tot di elementi di facile individuazione (Quelli di ordine il primo), per verificare che non possano esserci un dato numero di p-Sylow si può controllare che la somma totale degli elementi individuati non porti ad un assurdo.

Se esistesse un solo Sylow → normale
Studiamo quindi quanti Sylow possono esistere per ogni primo:

$$\#r \equiv 1\ (r)\ ; \#r = \begin{cases} p \rightarrow r|(p-1) \text{ ASSURDO in quanto } r > p \\ q \rightarrow r|(q-1) \text{ ASSURDO in quanto } r > q \rightarrow \#r = pq \\ pq \end{cases}$$

Quindi siccome in ciascun r-Sylow ci sono $(r-1)$ elementi di ordine r, in totale ne avremo:
$pq(r-1)$
Per lo stesso motivo avremo almeno:
$q(p-1)$ elementi di ordine p.
$r(q-1)$ elementi di ordine q.
Quindi in totale: $pqr - pq + pq - q + qr - r = pqr - q + qr - r \geq pqr$ ASSURDO.

Esempio 3:

Un gruppo di ordine p^2q ; $p < q$ ha un p-Sylow o un q-Sylow.Se ha ordine dispari allora il q-Sylow è normale.

> Se $\#q \neq 1 \rightarrow \#q | p^2 \rightarrow \#q = p$ oppure p^2 ma $\#q \equiv 1\ (p)$ quindi $q|(p-1)$ ASSURDO.
> Allora se ho p^2 q-Sylow mi implica che ho $p^2(q-1)$ q-elementi.
> Quindi rimangono solamente p^2 elementi disponibili per i p-Sylow, quindi ne ho esattamente 1.
>
> Se ha ordine dispari il fatto che $q|(p^2-1)$ →uno dei due sia pari, questo è assurdo essendo l'ordine del gruppo dispari.

Esempio 4 (Sylow con numeri assegnati, 9/11/11):

a. Determinare a meno di isomorfismo i gruppi di ordine $5^2 \cdot 13$

b. Dimostrare che esiste un gruppo non abeliano di ordine $5^2 \cdot 11$

> **a.** Per il primo teorema di Sylow so che esistono due gruppi di Sylow P_5, P_{13} rispettivamente di cardinalità $5^2, 13$.
> P_{13} è ciclico e dunque abeliano, P_5 è abeliano in quanto ha cardinalità quadrato di un primo.
> $\#13\text{-Sylow} \equiv 1\ (13)$ e divide 5^2 quindi $\#13\text{-Sylow} = 1 \rightarrow P_{13} \lhd G$
> $\#5\text{-Sylow} \equiv 1\ (5)$ e divide 13 quindi $\#5\text{-Sylow} = 1 \rightarrow P_5 \lhd G$
> Siccome $P_5 \cap P_{13} = \{e\}$ per le cardinalità allora $G \cong P_5 \times P_{13}$ → abeliano.
> Dunque ci sono solo due possibilità: $G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{13}$ o $G \cong \mathbb{Z}_{25} \times \mathbb{Z}_{13}$
> **b.** Il modo più rapido per costruirlo è determinare un prodotto semidiretto fra $\mathbb{Z}_{11}$ e $\mathbb{Z}_5$ che esiste in quanto $5|\Phi(11) = 10$
> Il modo esplicito per descrivere l'azione è il seguente:
> $\varphi: \mathbb{Z}_5 \rightarrow \mathrm{Aut}(\mathbb{Z}_{11})$ | $\varphi(x) = f_x: \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}$ | $f_x(a) = 4^x a$
>
> Andrebbe ugualmente bene con 5, in pratica mi sono limitato a scegliere un elemento che in $\mathbb{Z}_{11}$ abbia ordine moltiplicativo 5. (Per 4 vale $4,5,9,3,1$ e per 5 vale $5,3,4,9,1$).
>
> Dunque un esempio di gruppo non abeliano di ordine $5^2 \cdot 11$ è $(\mathbb{Z}_{11} \rtimes_\varphi \mathbb{Z}_5) \times \mathbb{Z}_5$

Esercizio 1 (17/01/12):

Determinare l'insieme dei numeri primi p | ∃ almeno tre gruppi fra loro non isomorfi di ordine $25p$

Osserviamo per prima cosa che due gruppi siamo sempre in grado di individuarli, sono i due abeliani $\mathbb{Z}_{25} \times \mathbb{Z}_p$ e $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_p$

Ci basta dunque individuare un prodotto semidiretto fra le componenti del nostro gruppo.

Osserviamo per prima cosa che se $5 \mid \Phi(p) = p - 1$ allora esiste sempre un terzo gruppo (In questo caso non abeliano) $(\mathbb{Z}_p \rtimes \mathbb{Z}_5) \times \mathbb{Z}_5$, se p non rispetta questa condizione non possiamo mai individuare questo prodotto semidiretto.

Cerchiamo al contrario un prodotto semidiretto del tipo $(\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes \mathbb{Z}_p \to p || \mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_5)| = (5^2 - 1)(5^2 - 5) = 2^5 \cdot 3 \cdot 5 \to p = 2,3,5$ mi permettono di costruire il prodotto semidiretto cercato.

Esclusi questi casi non può esistere un ulteriore p che rispetti la condizione data, infatti $P_5 \lhd G$ in quanto #5-Sylow $\equiv 1(5)$ e divide $p \to$ #5-Sylow $= 1 \to P_5 \lhd G$

Inoltre #p-Sylow $\equiv 1\ (p)$ e divide $25 \to$ #p-Sylow $\in \{1,5,25\}$ ma se fosse $5 \to p = 2$, se fosse $25 \to p = 3$ o 2 dunque ce ne è 1 solo $\to P_p \lhd G \to G$ abeliano.

Esercizio 2 (14/02/12):

Determinare il numero di classi di isomorfismo dei gruppi di ordine 52.

Per prima cosa consideriamo li due gruppi abeliano fra loro non isomorfi di ordine 52:

$G_1 = \mathbb{Z}_4 \times \mathbb{Z}_{13}$; $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{13}$

Cerchiamo ora i casi nei quali G non sia abeliano.

Se non è abeliano sarà un prodotto semidiretto ma dobbiamo prestare attenzione al fatto che $P_{13} \lhd G$ in quanto fra i divisori di 4 l'unico che è congruo a $1\ (13)$ è proprio l'1.

I due casi possibili sono $\mathbb{Z}_{13} \rtimes \mathbb{Z}_2$ e $\mathbb{Z}_{13} \rtimes \mathbb{Z}_4$.

Nel primo esiste un'unica azione non banale fra $\mathbb{Z}_2$ e $\mathrm{Aut}(\mathbb{Z}_{13}) \cong \mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ con un solo elemento di ordine 6. Quindi la terza classe di isomorfismo è $G_3 = \mathbb{Z}_{13} \rtimes \mathbb{Z}_2 \cong D_{13}$

Nel secondo caso invece esistono due possibili azioni (Distinte) di $\mathbb{Z}_4$ su $\mathrm{Aut}(\mathbb{Z}_{13})$, quella che associa ad un elemento s di $\mathbb{Z}_4$ la funzione $\varphi_s(x) = 5^s x$ e la seconda $f_s(x) = (12)^s x$

Dobbiamo capire se i due gruppi così definiti sono isomorfi.

Osserviamo che un elemento (x, s) sta nel centralizzatore di un gruppo dato da un prodotto semidiretto per un'azione $h \leftrightarrow s \in \ker h$

Ma $\ker \varphi = \{0\}$; $\ker f = \{0,2\}$

Quindi $G_4 = \mathbb{Z}_{13} \rtimes_\varphi \mathbb{Z}_4$; $G_5 = \mathbb{Z}_{13} \rtimes_f \mathbb{Z}_4$