Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA TULLIO LEVI-CIVITA
Corso di Laurea in Matematica

Tesi di Laurea Magistrale

I teoremi di Marshall Hall sul numero di p-sottogruppi di Sylow

Candidata:
Busetti Elena
Matricola 1180212

Relatore:
Prof. Andrea Lucchini

A.A. 2018/2019
18 Ottobre 2019

Indice

Introduzione

Lo scopo di questo lavoro è quello di mostrare alcune generalizzazioni dei teoremi di Sylow, ed esplorare alcuni risultati e proprietà riguardanti il numero di p-sottogruppi di Sylow di un gruppo finito, ma anche, più in generale, il numero di p-sottogruppi. Il punto di partenza saranno quindi i classici teoremi di Sylow, che richiamiamo ora per inquadrare il contesto.
Consideriamo un gruppo finito G e sia p un divisore primo di $|G|$. Ricordiamo innanzitutto la definizione di p-sottogruppo di Sylow di G (spesso per brevità detto anche p-Sylow di G).

Definizione 0.1. Un sottogruppo P di G è detto p-sottogruppo di Sylow se $|P| = p^n$ con $p^n \mid |G|$ e $p^{n+1} \nmid |G|$ (ovvero se l'ordine di P è la massima potenza di p che divide l'ordine di G).

Il primo teorema di Sylow ci assicura l'esistenza di un tale sottogruppo.

Teorema 0.2 (Primo teorema di Sylow)**.** *G ha un p-sottogruppo di Sylow.*

Teorema 0.3 (Secondo teorema di Sylow)**.** *Se S e T sono due p-sottogruppi di Sylow di G, allora esiste $g \in G$ tale che $T = gSg^{-1}$.*

Teorema 0.4 (Terzo teorema di Sylow)**.** *Se R è un p-sottogruppo di G, R è contenuto in qualche p-Sylow di G.*

Indichiamo con $Syl_p(G)$ l'insieme di tutti i p-Sylow di G e con $n_p(G)$, o talvolta n_p quando è chiaro quale gruppo si stia considerando, il numero di p-Sylow di G, ovvero $n_p(G) = |Syl_p(G)|$. Vediamo alcune importanti conseguenze dei teoremi di Sylow.

Corollario 0.5. *Sia $P \in Syl_p(G)$; vale $n_p(G) = [G : N_G(P)]$.*

Corollario 0.6. *Sia $|G| = p^a m$ per qualche intero $a \geq 1$ e m intero tale che $(m, p) = 1$; allora $n_p(G)$ divide m.*

Corollario 0.7. *$n_p(G) \equiv 1 \ mod \ p$.*

Il primo capitolo sarà dedicato ad alcune generalizzazioni dei teoremi di Sylow; in particolare partiremo dal teorema di Philip Hall, che generalizza i teoremi di Sylow a gruppi risolubili di ordine mn, con $(m, n) = 1$ e m non necessariamente potenza di primo; dopo aver osservato, tramite alcuni controesempi, che tale teorema non vale per gruppi semplici, chiuderemo il capitolo con un risultato più generale, di Marshall Hall, sul numero di p-Sylow di un generico gruppo finito; scopriremo che tale numero si può scrivere come prodotto di fattori di due tipi: potenza di primo congrua a 1 modulo p e numero di p-Sylow di un gruppo semplice finito.
Non sorprende quindi che l'attenzione si sposti ai gruppi semplici finiti, protagonisti del secondo capitolo; in particolare dimostreremo alcuni risultati nel caso del gruppo lineare speciale proiettivo $PSL(2, q)$ e del gruppo A_n delle permutazioni pari su n elementi.
Ricordando ancora una volta un'importante conseguenza dei teoremi di Sylow sul numero di p-Sylow, ovvero che $n_p \equiv 1 \bmod p$, nel terzo capitolo andremo ad indagare se valga o meno una sorta di viceversa, ovvero ci domandiamo se, dato un primo p, ogni intero positivo n congruo a 1 modulo p sia il numero di p-Sylow di qualche gruppo; la risposta sarà negativa: porteremo degli esempi di pseudo numeri di p-Sylow, ovvero di interi congrui a 1 modulo p che non sono il numero di p-Sylow di qualche gruppo.
Domande analoghe saranno il punto di partenza del quarto capitolo, dove, più in generale, prenderemo in considerazione p-sottogruppi, quindi non necessariamente p-Sylow. Grazie ad un teorema di Frobenius riusciremo a generalizzare ai p-sottogruppi il corollario 0.7; inoltre porteremo degli esempi di pseudo p-numeri di Frobenius, ovvero interi congrui a 1 o a $1+p$ modulo p^2 che non sono il numero di p-sottogruppi di qualche gruppo, e faremo alcune considerazioni sul loro legame con gli pseudo numeri di p-Sylow.

Capitolo 1

Generalizzazioni dei teoremi di Sylow

1.1 Teorema di Sylow per gruppi risolubili

Nel teorema di Philip Hall vediamo come nel caso di un gruppo G risolubile e di ordine mn, con m e n coprimi tra loro, si possa omettere l'ipotesi che m sia potenza di un primo, cosa che invece richiedevamo nei teoremi di Sylow richiamati nell'introduzione. Ricordiamo innanzitutto alcune definizioni.

Definizione 1.1. Un gruppo G si dice risolubile se esiste una catena di sottogruppi

$$\{1\} = N_0 \leq N_1 \leq ... \leq N_k = G$$

tale che $\forall i = 0, ..., k-1$:

- $N_i \trianglelefteq N_{i+1}$;
- il fattore $\frac{N_{i+1}}{N_i}$ è abeliano.

Osservazione 1.2. Nel caso di gruppi risolubili finiti si riesce a costruire una catena i cui fattori siano ciclici.

Definizione 1.3. Sia G un gruppo; una serie principale di G è una serie normale massimale, ovvero una catena di sottogruppi

$$\{1\} = N_0 \leq N_1 \leq ... \leq N_k = G$$

tale che $\forall i = 0, ..., k-1$:

- $N_i \trianglelefteq G$;

- $\frac{N_{i+1}}{N_i}$ è un sottogruppo normale minimale di $\frac{G}{N_i}$

Definizione 1.4. Dato un gruppo G, si dicono fattori principali di G i fattori di una serie principale di G.

Osservazione 1.5. Se G è un gruppo risolubile, i suoi fattori principali hanno ordine potenza di primo.

Ci sono utili anche alcuni richiami sulle azioni di gruppo.

Definizione 1.6. Siano G un gruppo finito e Ω un insieme finito non vuoto. Un'azione di G su Ω è una mappa

$$\begin{aligned} G \times \Omega &\to \Omega \\ (g, \omega) &\mapsto \omega^g \end{aligned}$$

tale che per ogni $\omega \in \Omega$ e $g, h \in G$:

- $\omega^1 = \omega$;
- $\omega^{gh} = (\omega^g)^h$.

Ad ogni azione possiamo associare un omomorfismo di gruppi $\sigma \colon G \to Sym(\Omega)$ che manda un elemento $g \in G$ nella permutazione $\omega \mapsto \omega^g$ di Ω; il nucleo $ker(\sigma)$ viene detto nucleo dell'azione; se tale nucleo è banale l'azione di G su Ω è detta fedele.
L'insieme $\omega^G = \{\omega^g : g \in G\} \subseteq \Omega$ è detto l'orbita di $\omega \in \Omega$; l'azione di G su Ω è detta transitiva se c'è un'unica orbita, ovvero se $\omega^G = \Omega \ \forall \omega \in \Omega$. Inoltre, l'insieme $G_\omega = \{g \in G : \omega^g = \omega\}$ è detto lo stabilizzatore di un elemento $\omega \in \Omega$; è legato alla cardinalità dell'orbita dalla seguente famosa proprietà:

$$|\omega^G| = [G : G_\omega].$$

Un'importante azione di un gruppo G è quella di coniugio su se stesso; in questo caso lo stabilizzatore di un elemento $x \in G$ è detto centralizzante ed è indicato con $C_G(x)$. Possiamo poi considerare l'azione di G sull'insieme dei suoi sottogruppi; lo stabilizzatore di un sottogruppo $H \leq G$ prende il nome di normalizzante ed è indicato con $N_G(H)$. L'azione che più spesso considereremo in questo contesto è quella di un gruppo G sull'insieme dei suoi p-sottogruppi di Sylow.
Possiamo ora enunciare la generalizzazione dei teoremi di Sylow per gruppi risolubili.

Teorema 1.7 (P. Hall)**.** *Sia G un gruppo risolubile di ordine mn, con $(m, n) = 1$. Valgono le seguenti affermazioni:*

a) G ha almeno un sottogruppo di ordine m;

b) sottogruppi di ordine m sono coniugati;

c) ogni sottogruppo di G il cui ordine divide m è contenuto in qualche sottogruppo di ordine m;

d) sia h_m il numero di sottogruppi di G di ordine m; esso è del tipo $h_m = q_1^{t_1} \cdots q_r^{t_r}$, dove $\forall i$:

- *q_i primo;*
- *$q_i^{t_i} \equiv 1 \ mod\ p_i$, con p_i un primo che divide m;*
- *$q_i^{t_i}$ divisore dell'ordine di uno dei fattori principali di G.*

Dimostrazione. Dimostriamo il teorema per induzione sull'ordine di G; supponiamo quindi che il teorema valga per tutti i gruppi risolubili di ordine minore di mn. Distinguiamo 2 casi:

1. G ha almeno un sottogruppo H normale, non banale, e tale che $(|H|, n) < n$.
   Possiamo scrivere $|H| = m_1 n_1$, $m = m_1 m_2$ e $n = n_1 n_2$ con $n_1 < n$.

   a) Consideriamo il quoziente $\frac{G}{H}$; vale $|\frac{G}{H}| = m_2 n_2 < |G|$ e $(m_2, n_2) = 1$, quindi possiamo applicare l'ipotesi induttiva: $\frac{G}{H}$ ha un sottogruppo di ordine m_2; di conseguenza G ha un sottogruppo L di ordine $|L| = m_2 \cdot |H| = m_2 m_1 n_1 = m n_1$. Applicando ancora l'ipotesi induttiva, L ha un sottogruppo di ordine m; in particolare quindi possiamo concludere che G ha un sottogruppo di ordine m.

   b) Consideriamo M e M' sottogruppi di ordine m; $\langle M, H\rangle = MH$ e $\langle M', H\rangle = M'H$ sono sottogruppi di G; facciamo alcune considerazioni sul loro ordine: sicuramente divide il prodotto degli ordini dei generatori, ovvero divide $m m_1 n_1$, e divide mn essendo sottogruppi di G; questo ci porta a dire che il loro ordine divide $m n_1$; usando poi i teoremi di isomorfismo, abbiamo $|\frac{MH}{H}| = |\frac{M}{M \cap H}|$, che è un multiplo di m (e analogamente per M'), quindi l'ordine dei sottogruppi MH e $M'H$ è un multiplo di mn_1. Questo ci permette di concludere che il loro ordine è esattamente mn_1.
   Segue quindi che $\frac{MH}{H}$ e $\frac{M'H}{H}$ sono sottogruppi di $\frac{G}{H}$ di ordine m_2; applicando l'ipotesi induttiva sono sottogruppi coniugati in $\frac{G}{H}$: $\exists \tilde{a} \in \frac{G}{H}$ tale che $\tilde{a}^{-1} \frac{MH}{H} \tilde{a} = \frac{M'H}{H}$; segue che $\exists a \in G$ tale che $a^{-1} M H a = M'H$; ora $a^{-1} M a$ e M' sono sottogruppi di $M'H$ di ordine m e applicando l'ipotesi induttiva sono coniugati. In particolare, quindi, M e M' sono coniugati in G.

c) Sia M' un sottogruppo di G di ordine m' che divide m; dobbiamo mostrare che M' è contenuto in un sottogruppo di G di ordine m. Consideriamo $\frac{M'H}{H}$: il suo ordine divide m_2; inoltre è un sottogruppo di $\frac{MH}{H}$, che dal punto precedente ha ordine esattamente m_2; possiamo quindi applicare l'ipotesi induttiva a $\frac{MH}{H}$ e affermare che $\frac{M'H}{H}$ è contenuto in un sottogruppo di $\frac{G}{H}$ di ordine m_2; segue quindi che $M'H$ è contenuto in un sottogruppo D di G di ordine mn_1. Applicando ora l'ipotesi induttiva a D, possiamo concludere che M' è contenuto in un sottogruppo di G di ordine m.

d) Chiamiamo h_m il numero di coniugati di un sottogruppo M di ordine m, h_{m_2} il numero di sottogruppi di $\frac{G}{H}$ di ordine m_2 e h il numero di coniugati di M in $D := MH$; seguendo la dimostrazione del punto b), si ha che $h_m = h_{m_2}h$. Osserviamo ora due fatti:

- i fattori principali di $\frac{G}{H}$ costituiscono un sottoinsieme dei fattori principali di G;
- gli ordini dei fattori principali di D dividono alcuni di quelli di G (osserviamo infatti che ogni sottogruppo normale di G contenuto in H è normale in D).

Applicando l'ipotesi induttiva a $\frac{G}{H}$ e a D abbiamo che h_{m_2} e h sono prodotti di fattori che soddisfano la tesi. Allora anche il loro prodotto h_m soddisfa la tesi.

2. G non ha sottogruppi normali H con $(|H|, n) < n$.
Sia K un sottogruppo normale minimale di G: per ipotesi n divide $|K|$, quindi, essendo l'ordine di K una potenza di primo, si deduce che $n = p^a$ per un opportuno primo p e che K è l'unico sottogruppo normale minimale di G (in particolare K è abeliano).

a) Sia L un sottogruppo normale contenente K propriamente e in particolare sia L minimale rispetto a questa proprietà; sia $|\frac{L}{K}| = q^b$; dunque q è un divisore primo di m e quindi $q \neq p$. Sia Q un q-Sylow di di L (che quindi ha ordine q^b) e definisco $M := N_G(Q)$ e $T := M \cap K$; il nostro scopo è dimostrare che M ha ordine m.
Osserviamo che T è abeliano, in quanto sottogruppo di K, ed è un sottogruppo normale di M. Ora ogni elemento di T commuta con ogni elemento di Q: sia infatti $t \in T$ e $q \in Q$; $[t, q] \in T \cap Q = M \cap K \cap Q = K \cap Q = 1$. Allora T centralizza Q e di conseguenza $T \leq Z(L)$; ora, essendo $Z(L)$ un sottogruppo caratteristico di L e L normale in G, possiamo affermare che $Z(L)$ è normale in G; ma per ipotesi K è l'unico sottogruppo normale minimale di G,

quindi tutti i sottogruppi normali di G non identici lo contengono; dunque ci sono 2 possibilità:

1. $K \leq Z(L) \Rightarrow L = K \times Q \Rightarrow Q \triangleleft G$, contraddizione con l'unicità di K.
2. $Z(L) = 1 \Rightarrow T = 1 \Rightarrow Q = N_L(Q)$; in questo caso il numero di coniugati di Q in L è $[L : Q] = p^a$; essendo L normale in G, ogni coniugato di Q in G sta in L e dunque il numero di coniugati di Q in G è esattamente p^a; concludiamo quindi che $[G : M] = [G : N_G(Q)] = p^a = n \Rightarrow |M| = m$.

b) Con le stesse notazioni del punto precedente, i normalizzanti degli $n = p^a$ coniugati di Q sono coniugati e distinti; abbiamo dunque p^a sottogruppi coniugati di ordine m. Sia M' un sottogruppo di ordine m e mostriamo che è sicuramente uno dei p^a normalizzanti; $M'L$ ha ordine divisibile per m e n dunque è sicuramente tutto G; vale $\frac{m}{q^b} = |\frac{G}{L}| = |\frac{M'L}{L}| = |\frac{M'}{M' \cap L}|$; segue che $M' \cap L$ ha ordine q^b ed è quindi un coniugato di Q; inoltre, essendo un sottogruppo normale di M', abbiamo che $N_{M'}(M' \cap L) = M'$, ovvero M' è il normalizzante di un coniugato di Q. Questo prova che tutti i sottogruppi di ordine m sono coniugati.

c) Sia M un sottogruppo di ordine m e M' un sottogruppo di ordine m' divisore di m. Si consideri $M^* = M \cap (M' \cup K)$; ha ordine m' e quindi, applicando b) a $M' \cup K$, possiamo affermare che $M^*(\subseteq M)$ e M' sono coniugati, concludendo che M' è contenuto in un coniugato di M, che è sicuramente un sottogruppo di G di ordine m.

d) Verifichiamo che p^a soddisfa la tesi:

- è potenza di primo;
- $p^a \equiv 1 \bmod q$, essendo il numero di q-Sylow di G;
- è un fattore principale di G, in quanto ordine del sottogruppo K. □

Osserviamo che l'ipotesi di risolubilità è fondamentale; vediamo alcuni esempi di gruppi semplici in cui il teorema di Philip Hall non è valido.

Esempio 1.8. Il gruppo alterno A_5 ha ordine $60 = 15 \cdot 4$ ma non ha sottogruppi di ordine 15 (contraddicendo il punto a) del teorema).

Supponiamo per assurdo che A_5 abbia un sottogruppo H di ordine 15. Sia $\Lambda := \{Hg | g \in A_5\}$ l'insieme delle classi laterali destre di H; ha ordine 4. Sia

$S(\Lambda)$ il gruppo delle permutazioni su Λ e consideriamo il seguente morfismo naturale di gruppi: $\varphi\colon A_5 \to S(\Lambda)$, che ad un elemento x di A_5 associa la permutazione definita da $\lambda \mapsto \lambda x$.
Ora $ker\varphi \trianglelefteq A_5$ ma A_5 è un gruppo semplice dunque abbiamo 2 possibilità:

1. $ker\varphi = \{1\}$ e dunque φ è iniettivo, ma questo è impossibile poiché $|S(\Lambda)| = 4! < |A_5|$;

2. $ker\varphi = A_5$ e dunque $\forall x\ \varphi(x) = id$, ma questo è impossibile poiché se $x \in A_5 \setminus H$ allora $\varphi(x)$ è una permutazione non identica di Λ.

Esempio 1.9. Il gruppo $G := Aut(A)$, dove $A = C_2 \times C_2 \times C_2$, ha ordine $168 = 24 \cdot 7$ ma non tutti i suoi sottogruppi di ordine 24 sono coniugati (contraddicendo il punto b) del teorema).

Infatti G agisce transitivamente sui 7 sottogruppi di A di ordine 2 e sui 7 sottogruppi di A di ordine 4, dunque G ha due distinte classi di coniugio di sottogruppi di ordine 24.

Esempio 1.10. A_5 ha un sottogruppo di ordine 6 che non è contenuto in alcun sottogruppo di ordine 12 (contraddicendo il punto c) del teorema).

Osserviamo infatti che $|A_5| = 12 \cdot 5$ ma il sottogruppo $\langle (123), (12)(45) \rangle$ di ordine 6 non è contenuto in alcun sottogruppo di ordine 12.

Esempio 1.11. Il numero di sottogruppi di ordine 5 di A_5 non è prodotto di fattori congrui a 1 mod 5 (contraddicendo il punto d) del teorema).

Dai teoremi di Sylow sappiamo che il numero di 5-Sylow è $6 = 2 \cdot 3$, ma $2 \not\equiv 1 \bmod 5$.

1.2 Teorema di Sylow per un gruppo finito qualsiasi

Abbiamo appena constatato che il teorema di P. Hall non si può applicare a gruppi semplici. Come anticipato nell'introduzione, vedremo in questa sezione un teorema più generale, di Marshall Hall, sul numero n_p di p-Sylow di un qualsiasi gruppo finito. Per arrivare a questo, dimostriamo alcuni risultati preliminari.

Lemma 1.12. *Sia G un gruppo con $K \trianglelefteq G$ e un p-Sylow P; allora:*

1. *$K \cap P$ è un p-Sylow di K;*
2. *$\frac{PK}{K}$ è un p-Sylow di $\frac{G}{K}$.*

Dimostrazione. Osserviamo innanzitutto che un p-Sylow P di G è un p-Sylow di $P \cup K = PK$.
Essendo $K \trianglelefteq G$, si ha che $K \cap P \trianglelefteq P$; in particolare quindi $|K \cap P| = p^s \ \exists s$; inoltre $|\frac{P}{K \cap P}|$ è una certa potenza p^r; segue quindi che l'ordine di P, ovvero la massima potenza di p che divide $|G|$, è p^{r+s}. Abbiamo quindi:

1. $\frac{PK}{K} \leq \frac{G}{K}$ e $|\frac{PK}{K}| = |\frac{P}{K \cap P}| = p^r$, dunque $\frac{PK}{K}$ è un p-Sylow di $\frac{G}{K}$;
2. $K \cap P \leq K$ e $|K \cap P| = p^s$, dunque $K \cap P$ è un p-Sylow di K. $\square$

Vediamo ora una prima caratterizzazione, data da M. Hall, del numero n_p di p-Sylow di un gruppo.

Teorema 1.13. *Sia G un gruppo con $K \trianglelefteq G$ e un p-Sylow P.*
Allora $n_p = a_p \cdot b_p \cdot c_p$ dove:

- *a_p è il numero di p-Sylow di $\frac{G}{K}$;*
- *b_p è il numero di p-Sylow di K;*
- *c_p è il numero di p-Sylow di $\frac{N_{PK}(P \cap K)}{P \cap K}$.*

Dimostrazione. Dai teoremi di Sylow abbiamo $n_p = [G : N_G(P)]$; essendo $K \trianglelefteq G$, vale l'inclusione $N_G(P) \subseteq N_G(PK)$ e dunque $n_p = [G : N_G(P)] = [G : N_G(PK)] \cdot [N_G(PK) : N_G(P)]$. Dobbiamo mostrare che questo prodotto è esattamente $n_p = a_p \cdot b_p \cdot c_p$.
Chiamiamo $H := \frac{G}{K}$ e $P^* := \frac{PK}{K}$, che per il lemma precedente è un p-Sylow di H; considerando la mappa quoziente $G \to H$, notiamo che $N_G(PK)$ non è altro che l'immagine inversa di $N_H(P^*)$; allora il numero a_p di p-Sylow di H è $a_p = [H : N_H(P^*)] = [G : N_G(PK)]$.
Dunque $n_p = a_p \cdot [N_G(PK) : N_G(P)]$.

Dobbiamo ora dimostrare che $[N_G(PK) : N_G(P)] = b_p \cdot c_p$.
Abbiamo già osservato in precedenza che un p-Sylow P di G è un p-Sylow di PK; dunque, essendo $[N_G(PK) : P] = \frac{[G:P]}{[G:N_G(PK)]}$coprimo con p, P è un p-Sylow di $N_G(PK)$; quindi il numero di p-Sylow in $N_G(PK)$ è uguale al numero di p-Sylow in PK, ovvero $[N_G(PK) : N_G(P)] = [PK : N_{PK}(P)]$.
L'uguaglianza da dimostrare è quindi $[PK : N_{PK}(P)] = b_p \cdot c_p$.
Osserviamo che $N_{PK}(P) \geq P$ e valgono le seguenti relazioni, che sfrutteremo

poi nel seguito della dimostrazione:

$$P(K \cap N_{PK}(P)) = PK \cap N_{PK}(P) = N_{PK}(P)^1 \tag{1.1}$$

$$P \cap (K \cap N_{PK}(P)) = P \cap K \tag{1.2}$$

Ora, essendo $N_{PK}(P) \cap K \trianglelefteq N_{PK}(P)$, possiamo considerare l'indice $[N_{PK}(P) : N_{PK}(P) \cap K] = [P : P \cap K]$, dove l'uguaglianza segue intersecando i sottogruppi con P e ricordando che $N_{PK}(P) \geq P$; allora $[N_{PK}(P) : P] = [N_{PK}(P) \cap K : P \cap K]$, dove effettivamente $N_{PK}(P) \cap K \geq P \cap K$ grazie alla 1.2.
Vediamo quindi come poter riscrivere l'indice $[PK : N_{PK}(P)]$:

$$\begin{aligned}[PK : N_{PK}(P)] &= \frac{[PK : P]}{[N_{PK}(P) : P]} \\ &= \frac{[K : P \cap K]}{[N_{PK}(P) \cap K : P \cap K]} \\ &= [K : K \cap N_{PK}(P)].\end{aligned}$$

L'equazione da dimostrare diventa quindi $[K : K \cap N_{PK}(P)] = b_p \cdot c_p$.
Sia $y \in K$ tale che $y \in PK$ e $y^{-1}Py \in P$ (ovvero $y \in N_{PK}(P)$). Dimostriamo che $y \in N_{PK}(P \cap K)$:

$$y^{-1}(P \cap K)y = y^{-1}Py \cap y^{-1}Ky = P \cap K.$$

Questo prova che $N_{PK}(P \cap K) \geq N_{PK}(P)$ e dunque $N_K(P \cap K) = K \cap N_{PK}(P \cap K) \geq K \cap N_{PK}(P)$.
Allora possiamo riscrivere l'indice sopra come:

$$\begin{aligned}[K : K \cap N_{PK}(P)] &= [K : N_K(P \cap K)] \cdot [N_K(P \cap K) : K \cap N_{PK}(P)] \\ &= [K : N_K(P \cap K)] \cdot [K \cap N_{PK}(P \cap K) : K \cap N_{PK}(P)].\end{aligned}$$

Osserviamo che il primo fattore di questo prodotto è proprio b_p, ovvero il numero di p-Sylow di K, dato che il lemma 1.12 ci assicura che $P \cap K$ sia un p-Sylow di K.

Rimane quindi da dimostrare che l'indice $[K \cap N_{PK}(P \cap K) : K \cap N_{PK}(P)]$ è esattamente c_p, ovvero il numero di p-Sylow del quoziente $\frac{N_{PK}(P \cap K)}{P \cap K}$.
Per alleggerire le notazioni, chiamiamo $M = N_{PK}(P \cap K)$. Abbiamo già osservato in precedenza che $M \geq N_{PK}(P) \geq P$ e dunque vale:

$$M \cup K = N_{PK}(P) \cup K = P \cup K = PK.$$

[1] La prima uguaglianza vale per il seguente lemma di Dedekind: siano R, S e T sottogruppi di un gruppo G, e $S \subseteq T$; allora $S(R \cap T) = SR \cap T$.

Ricordando che $K \trianglelefteq G$ e $\frac{PK}{K} = \frac{M \cup K}{K} = \frac{M}{M \cap K}$, valgono le seguenti uguaglianze:

$$[PK : K] \overset{a}{=} [M : M \cap K] \overset{b}{=} [N_{PK}(P) : N_{PK}(P) \cap K] \overset{c}{=} [P : P \cap K]$$

dove c segue intersecando i sottogruppi con P. Ora:

$a \Rightarrow [PK : M] = [K : M \cap K]$
$b \Rightarrow [M : N_{PK}(P)] = [M \cap K : N_{PK}(P) \cap K]$
$c \Rightarrow [N_{PK}(P) : P] = [N_{PK}(P) \cap K : P \cap K]$.

Inoltre ricordiamo che $M \cap K = N_{PK}(P \cap K) \cap K$, $N_{PK}(P \cap K) = N_{PK}(P) \cap K$ e $M \geq N_{PK}(P)$ (quindi in particolare $N_M(P) = N_{PK}(P)$); possiamo ora riscrivere l'indice $[K \cap N_{PK}(P \cap K) : K \cap N_{PK}(P)]$ in questo modo:

$$\begin{aligned}[K \cap N_{PK}(P \cap K) : K \cap N_{PK}(P)] &= [M \cap K : N_{PK}(P \cap K)] \\ &= [M : N_{PK}(P)] \\ &= [M : N_M(P)].\end{aligned}$$

Sappiamo che quest'ultimo indice è il numero di p-Sylow di $M = N_{PK}(P \cap K)$, ma è anche c_p, il numero di p-Sylow di $\frac{N_{PK}(P \cap K)}{P \cap K}$; infatti $P \cap K$, essendo un p-sottogruppo normale di $N_{PK}(P \cap K)$, è contenuto in ogni p-Sylow di $N_{PK}(P \cap K)$. $\square$

Possiamo ora enunciare e dimostrare il teorema più generale di M.Hall, che caratterizza il numero di p-Sylow di un gruppo finito G, senza ulteriori ipotesi.

Teorema 1.14. *Sia G un gruppo finito e n_p il numero dei suoi p-Sylow. Allora n_p è un prodotto di fattori di questo tipo:*

- *s_p, dove con s_p indichiamo il numero di p-Sylow di un gruppo semplice S;*
- *q^t, dove q è un numero primo e $q^t \equiv 1 \ mod \ p$.*

Dimostrazione. Osserviamo innanzitutto che nei casi banali in cui $|G| = p^r$ $\exists r$, $|G| = q$ con q e p coprimi, oppure G semplice, la tesi è sicuramente soddisfatta.
Dimostriamo per induzione su $|G|$.
Avendo già commentato il caso in cui G è semplice, possiamo ora supporre che esista un sottogruppo normale proprio di G, che chiamiamo K. Dal teorema precedente sappiamo che il numero di p-Sylow di G è $n_p = a_p \cdot b_p \cdot c_p$ dove a_p, b_p e c_p sono, rispettivamente, il numero di p-Sylow di $\frac{G}{K}$, K e $\frac{N_{PK}(P \cap K)}{P \cap K}$.

Sicuramente $|\frac{G}{K}| < |G|$ e $|K| < |G|$, quindi applicando l'ipotesi induttiva il teorema vale per $\frac{G}{K}$ e $|K|$; se vale inoltre $|\frac{N_{PK}(P\cap K)}{P\cap K}| < |G|$, allora anche $\frac{N_{PK}(P\cap K)}{P\cap K}$ soddisfa il teorema e abbiamo concluso.
Supponiamo invece che valga $|\frac{N_{PK}(P\cap K)}{P\cap K}| = |G|$. Questo significa che $P\cap K = \{1\}$, cioè che K ha ordine coprimo con p, e che $G \subseteq PK$, ma allora $G = PK$ e dunque $\frac{G}{K} = P$.
Distinguiamo ora due casi.

1. Supponiamo che $|P| = p^r$ con $r > 1$.
   Sia $P_1 \leq P$ con $|P_1| = p^{r-1}$, dunque P_1 è un sottogruppo normale massimale in P. Definiamo poi $K_1 := KP_1$ e osserviamo che $K_1 \triangleleft G = PK$ e $P \cap K_1 = P_1$; allora G, avendo un sottogruppo normale K_1 e un p-Sylow P, soddisfa le ipotesi del teorema 1.13 e possiamo quindi affermare che il numero di p-Sylow di G è $n_p = a_p \cdot b_p \cdot c_p$ dove a_p, b_p e c_p sono, rispettivamente, il numero di p-Sylow di $\frac{G}{K_1}$, K_1 e $\frac{N_{PK_1}(P\cap K_1)}{P\cap K_1} = \frac{N_{PK_1}(P_1)}{P_1}$. Questi tre gruppi hanno ordine minore di quello di G, quindi il teorema vale per induzione.

2. Supponiamo che $|P| = p$.
   In questo caso dunque il p-Sylow P è ciclico: chiamando a il generatore, abbiamo $P = \langle a \rangle$ con $a^p = 1$. Sia α l'automorfismo di K indotto dal coniugio tramite a, ovvero $\alpha\colon K \to K$, $x \mapsto x^a = a^{-1}xa$. Definiamo $F := \{x \in K | x^a = x\}$, ovvero l'insieme degli elementi di K fissati da α. Dimostriamo che $N_{PK}(P) \cap K = F$.

   ($\subseteq$) Sia $x \in N_{PK}(P) \cap K$; allora:

   $$x^{-1}(a^{-1}xa) = (x^{-1}a^{-1}x)a \in K \cap P = \{1\}$$
   $$\Rightarrow x^{-1}a^{-1}xa = 1 \Rightarrow a^{-1}xa = x \Rightarrow x \in F.$$

   ($\supseteq$) Sia $x \in F$; sicuramente $x \in K$ poiché $F \leq K$; mostriamo che x appartiene anche a $N_{PK}(P)$: in particolare, preso un elemento in P, che quindi è del tipo a^q con $q \leq p$, dimostriamo che $x^{-1}a^q x = a^q$.

   $$x^{-1}a^q x = x^{-1}a^{q-1}ax = x^{-1}a^{q-1}xa$$

   dove l'ultima uguaglianza segue dal fatto che $ax = xa$, dato che $x \in F$ per ipotesi. Possiamo continuare in questo modo fino a far "risalire" x:

   $$x^{-1}a^q x = x^{-1}a^{q-1}xa = x^{-1}a^{q-2}xa^2 = ... = x^{-1}xa^q = a^q.$$

Da $N_{PK}(P) \cap K = F$ segue che $N_{PK}(P) = PF$. Allora il numero n_p di p-Sylow di $G = PK$ è:

$$n_p = [PK : N_{PK}(P)] = [PK : PF] = [K : F].$$

Denotando gli ordini di K e F come $|K| = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$ e $|F| = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$, dove sicuramente $(q_i, p) = 1$ e $e_i \geq f_i \ \forall i$, il numero di p-Sylow risulta dunque:

$$n_p = [K : F] = q_1^{e_1 - f_1} q_2^{e_2 - f_2} \cdots q_r^{e_r - f_r}.$$

Per concludere dobbiamo dimostrare che $q_i^{e_i - f_i} \equiv 1 \bmod p \ \forall i$.
Sia Q_1 un q_i-Sylow di F (dunque $|Q_1| = q_i^{f_i}$).
Se Q_1 è un q_i-Sylow anche di K (ricordiamo che $K \geq F$), allora $e_i = f_i$ e dunque $q_i^{e_i - f_i} = 1 \equiv 1 \bmod p$, concludendo la dimostrazione.
Possiamo quindi supporre ora che Q_1 sia q_i-Sylow soltanto di F e non di K; in altre parole K ha un sottogruppo di ordine $q_i^{e_i}$ con $e_i > f_i$; in particolare quindi $e_i - f_i \geq 1$ e quindi $q_i^{e_i - f_i} \geq q_i$; allora $\exists Q^*$ tale che $[Q^* : Q_1] = q_i$ (quindi $|Q^*| = q_i^{f_i + 1}$) e dunque $Q_1 \triangleleft Q^*$; segue che $N_K(Q_1)$, contenendo Q^*, ha ordine multiplo di $q_i^{f_i+1}$ e dunque $[N_K(Q_1) : Q_1] \equiv 0 \bmod q_i$.
Dimostriamo poi che $N_K(Q_1)^a = N_K(Q_1)$; sia $y \in N_K(Q_1)$:

$$\begin{aligned} y^{-1} Q_1 y &= Q_1 \\ (y^a)^{-1} {Q_1}^a y^a &= {Q_1}^a \\ (y^a)^{-1} Q_1 y^a &= Q_1 \end{aligned}$$

dove abbiamo usato il fatto che ${Q_1}^a = Q_1$ dato che $Q_1 \subseteq F$.
Ora ogni sottogruppo H di K (compreso K stesso), ha un q_i-Sylow che ammette l'automorfismo α, poiché il numero di q_i-Sylow di H divide l'ordine di H e quindi non è multiplo di p. α agisce con cicli di lunghezza p sui q_i-Sylow di H che non fissa ma allora esiste almeno un q_i-Sylow di H fissato da α.
Otteniamo in questo modo una catena di q_i sottogruppi
$Q_1 \subset Q_2 \subset ... \subset Q_s$ in cui:

- Q_j è un q_i-Sylow di $N_K(Q_{j-1}) \ \forall j = 1, ..., s$
- $Q_j = {Q_j}^a \ \forall j = 1, ..., s$
- $Q_s =: Q$ è un q_i-Sylow di K.

Ricordando che Q_1 era un q_i-Sylow di F, il sottogruppo di K fissato da α, non esiste in Q un sottogruppo più grande fissato da α; dunque

α agisce sui $q_i^{e_i} - q_i^{f_i}$ elementi di $Q \setminus Q_1$ con cicli di lunghezza p, ma allora $q_i^{e_i} - q_i^{f_i} \equiv 0 \bmod p$, ovvero p divide $q_i^{e_i} - q_i^{f_i} = q_i^{f_i}(q_i^{e_i - f_i} - 1)$; essendo $(q_i^{f_i}, p) = 1$ per ipotesi, sicuramente p deve dividere $q_i^{e_i - f_i} - 1$ ovvero $q_i^{e_i - f_i} \equiv 1 \bmod p$, che è ciò che dovevamo dimostrare. □

Osservazione 1.15. Tutti i numeri che soddisfano il teorema di Marshall Hall sono numeri di p-Sylow per qualche gruppo opportuno; infatti osserviamo i due seguenti fatti:

- se due gruppi G_1 e G_2 hanno rispettivamente n_1 e n_2 p-Sylow, il loro prodotto diretto $G_1 \times G_2$ ha $n_1 n_2$ p-Sylow (sono prodotti diretti dei p-Sylow di G_1 con i p-Sylow di G_2);

- se q è un primo diverso da p e t un esponente tale che $p | q^t - 1$, allora il prodotto semidiretto di F_{q^t} con C_p ha q^t p-Sylow.

Capitolo 2

Sul numero di p-Sylow di gruppi semplici

Abbiamo visto nel capitolo precedente, grazie al teorema di M. Hall, che il numero di p-Sylow di un qualunque gruppo finito si può scrivere come prodotto di fattori di due tipi:

- q^t con q primo e $q^t \equiv 1 \bmod p$;
- il numero di p-Sylow di un gruppo semplice finito.

Ci possiamo quindi chiedere se è possibile caratterizzare in qualche modo il numero di p-Sylow di gruppi semplici finiti.
Ci servono innanzitutto alcune definizioni e risultati preliminari.

Definizione 2.1. Un numero primo di Mersenne è un numero primo esprimibile come $M_p = 2^p - 1$ con p primo.

Esempio 2.2. $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$, $127 = 2^7 - 1$ sono primi di Mersenne.

Osservazione 2.3. Nella definizione di numero primo di Mersenne M_p potremmo omettere la richiesta che p sia primo; infatti se M_p è primo, allora anche p è necessariamente primo (se fosse invece $p = rs$, allora $2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + ... + 2^r + 1)$).
Il viceversa invece non vale, ovvero dato un primo p, il numero $2^p - 1$ non è necessariamente primo, come si vede ad esempio per $2^{11} - 1 = 23 \cdot 89$.

Denotiamo con $(m)_l$ la l-parte di un intero positivo m, ovvero la massima potenza di l che divide m.

Definizione 2.4. Sia G un gruppo finito e n_p il numero dei suoi p-Sylow. n_p è detto risolubile se, per ogni primo l, si ha $(n_p)_l \equiv 1 \bmod p$.

Definizione 2.5. Un gruppo finito G è detto gruppo SSN (Solvable Sylow Numbered) se n_p è risolubile per ogni primo p.

Osservazione 2.6.

1. Sicuramente in ogni gruppo finito il numero di 2-Sylow è risolubile, dato che n_2 è un prodotto di numeri dispari.

2. Dal teorema di P. Hall segue che gruppi finiti risolubili sono gruppi SSN.

3. Dato un primo p, n_p è sempre risolubile per un gruppo p-risolubile (gruppo che ammette una serie subnormale in cui tutti i quozienti o sono p-gruppi oppure hanno ordini coprimi con p); si dimostra ripetendo la prova di M. Hall per induzione, notando infatti che la proprietà p-risolubile si eredita a quozienti e sottogruppi.

Studiare il numero di p-Sylow di gruppi risolubili risulta difficile; riusciamo invece ad ottenere più facilmente qualche informazione sui gruppi semplici, in particolare vedremo un risultato che mette in relazione numeri n_p risolubili e primi di Mersenne. Per arrivare a questo ci servono ancora alcune nozioni e lemmi preliminari.

Definizione 2.7. Siano p un primo e $t, n > 1$ interi; p è detto divisore primo di Zsigmondy di $t^n - 1$ se $p|t^n - 1$ ma $p \nmid t^m - 1$ per $0 < m < n$.

Osservazione 2.8. Denotando con $ord_p(t)$ l'ordine moltiplicativo di t modulo p, ovvero il più piccolo intero k tale che $t^k \equiv 1 \bmod p$, possiamo riscrivere la definizione precedente come: p è detto divisore primo di Zsigmondy di $t^n - 1$ se $ord_p(t) = n$.

Teorema 2.9. *Siano $n, t > 1$ interi positivi. Allora $t^n - 1$ ha un divisore primo di Zsigmondy, a meno che non si presenti uno dei seguenti due casi:*

1. *$n = 6$ e $t = 2$;*

2. *$n = 2$ e $t = 2^e - 1$ per qualche intero e.*

Seguono ora alcuni richiami sui gruppi proiettivi lineari.
Sia V uno spazio vettoriale, e siano $GL(V)$ e $SL(V)$ rispettivamente il gruppo lineare generale e il gruppo lineare speciale di V. In particolare, se V è uno spazio vettoriale n-dimensionale su un campo finito F_q con q elementi, $GL(V)$ e $SL(V)$ si denotano anche con $GL(n, q)$ e $SL(n, q)$. Ricordiamo i loro ordini: $|GL(n, q)| = \prod_{k=0}^{n-1}(q^n - q^k)$ e $|SL(n, q)| = \frac{\prod_{k=0}^{n-1}(q^n - q^k)}{q-1}$. Ricordiamo inoltre come sono definiti il gruppo lineare generale proiettivo e il gruppo lineare speciale proiettivo:

- $PGL(V) = \frac{GL(V)}{Z(V)}$, dove $Z(V)$ è il sottogruppo di tutte le trasformazioni scalari non nulle di V;
- $PSL(V) = \frac{SL(V)}{Z(SL(V))}$, dove $Z(SL(V))$, centro di $SL(V)$, è il sottogruppo di tutte le trasformazioni scalari di V con determinante 1.

Vediamo alcune proprietà di $PSL(2,q)$, che è il caso che ci interessa per i prossimi risultati.

1. $PSL(2,q)$ è un gruppo finito semplice tranne nei casi $q = 2$, $q = 3$ in cui abbiamo i gruppi risolubili $PSL(2,2) \cong S_3$ e $PSL(2,3) \cong A_4$.
2. L'ordine del gruppo è:
   - $|PSL(2,q)| = |PGL(2,q)| = q^3 - q = (q-1)q(q+1)$, se la caratteristica del campo è 2;
   - $|PSL(2,q)| = \frac{1}{2}|PGL(2,q)|$, se la caratteristica del campo è diversa da 2.

Vediamo un ultimo lemma prima di enunciare il teorema principale.

Lemma 2.10. *Sia G un gruppo finito, H un sottogruppo normale di G, e p un primo. Se $p \nmid [G : H]$, allora $n_p(\frac{H}{Z(H)}) = n_p(G)$.*

Dimostrazione. Sia $\overline{H} := \frac{H}{Z(H)}$ e P un p-Sylow di G. P è anche un p-Sylow di H, poiché per ipotesi $p \nmid [G : H]$ ma allora $n_p(H) = n_p(G)$. Osserviamo che $Z(H) \leq N_H(P)$ e che $\overline{P} = \frac{P}{Z(H)}$ è p-Sylow di $\overline{H}$; inoltre $N_{\overline{H}}(\overline{P}) = \overline{N_H(P)}$, dato che il p-sylow di $Z(H)$ è contenuto in P e quindi $PZ(H) = P \times T$, con T sottogruppo di $Z(H)$ di ordine coprimo con p. Possiamo ora calcolare il numero di p-Sylow di $\overline{H}$:

$$n_p(\overline{H}) = [\overline{H} : N_{\overline{H}}(\overline{P})] = [\overline{H} : \overline{N_H(P)}] = [H : N_H(P)] = n_p(H) = n_p(G). \ \square$$

Possiamo ora enunciare il teorema che caratterizza i gruppi semplici SSN.

Teorema 2.11. *Sia G un gruppo finito, non abeliano e semplice. Allora G è un gruppo SSN $\Leftrightarrow G \cong PSL(2,q)$ per qualche primo di Mersenne q.*

Dalla classificazione dei gruppi semplici finiti, un gruppo finito, non abeliano e semplice (ipotesi del teorema) è uno dei seguenti:

- un gruppo alterno A_n con $n \geq 5$;
- un gruppo semplice finito di tipo Lie;

- uno dei 26 gruppi semplici sporadici.

Quindi, per quanto riguarda l'implicazione $\Rightarrow$, la strategia è quella di passare in rassegna le 3 tipologie di gruppi appena elencate (escluso il caso $PSL(2,q)$ con q primo di Mersenne), e dimostrare che non sono gruppi SSN, ovvero, ricordando la definizione, dimostrare che esiste un primo p per cui n_p non è risolubile (cioè esiste un primo l tale che $(n_p)_l \not\equiv 1 \bmod p$). In questa tesi andremo a vedere la dimostrazione per A_n, con $n \geq 5$ e per $PSL(2,q)$ con $q \neq 2$ non primo di Mersenne.

Osservazione 2.12.

1. È noto che per $n \leq 4$ A_n è risolubile, quindi non rientra tra le ipotesi del teorema, e in particolare è un gruppo SSN grazie al teorema di P. Hall.

2. Se $q = 2$ abbiamo $PSL(2,2) \cong S_3$, che è risolubile e quindi SSN.

Dimostrazione.
($\Rightarrow$)

1. Caso A_n (con $n \geq 5$).
   Da [6, tabella 3], se $n \geq 5$ e $n \neq 6, 10$, esistono due primi p e l tali che $n \geq p > l > \frac{n}{2}$. Inoltre (guardando ad esempio [14, lemmi 4.3 e 4.4]) sappiamo che il numero di p-Sylow del gruppo alterno A_n è $n_p = \frac{n!}{(n-p)!p(p-1)}$; consideriamo quindi i diversi casi.

   (a) Sia $n \neq 6, 10$. Allora esistono p, l primi tali che $n \geq p > l > \frac{n}{2}$ e $(n_p)_l = l \not\equiv 1 \bmod p$, ricordando che $p > l$.
   Dunque A_n non è un gruppo SSN per $n \geq 5$ e $n \neq 6, 10$.

   (b) Sia $n = 6$. Mostriamo che il numero di 5-Sylow di A_6 non è risolubile:

   $$n_5(A_6) = 2^2 \cdot 3^2 \Rightarrow (n_5(A_6))_2 = 4 \not\equiv 1 \bmod 5.$$

   Dunque A_6 non è un gruppo SSN.

   (c) Sia $n = 10$. Mostriamo che il numero di 7-Sylow di A_{10} non è risolubile:

   $$n_7(A_{10}) = 2^6 \cdot 3^2 \cdot 5^2 \Rightarrow (n_7(A_{10}))_3 = 9 \not\equiv 1 \bmod 7.$$

   Dunque A_{10} non è un gruppo SSN.

2. Caso $PSL(2,q)$ (con $q \neq 2$ non primo di Mersenne).
Ricordiamo innanzitutto che q è del tipo $q = r^f$ con r primo e f intero positivo.
Supponiamo esista un primo p di Zsigmondy di $q^2 - 1$.
Dalla definizione allora $p|q^2 - 1$ ma $p \nmid q - 1$, o equivalentemente $ord_p(q) = 2$; in termini di r, $p|r^{2f} - 1$ ma $p \nmid r^m - 1$ per $m < 2f$, ovvero $ord_p(r) = 2f$.
Sia $G := GL(2,q)$; sappiamo che $|G| = (q-1)^2 q(q+1) = (r^f - 1)^2 r^f (r^f + 1)$ e in particolare quindi $(|G|)_r = r^f$.
Vogliamo applicare il lemma 2.10 a $G = GL(2,q)$ e $H = SL(2,q)$; verifichiamo che le ipotesi sono soddisfatte:

- $SL(2,q) \triangleleft GL(2,q)$, essendo $SL(2,q)$ il nucleo dell'omomorfismo che associa a una matrice il suo determinante;
- $[GL(2,q) : SL(2,q)] = q - 1$, e $p \nmid q - 1$ per quanto visto sopra.

Allora $n_p(G) = n_p(\frac{SL(2,q)}{Z(SL(2,q))}) = n_p(PSL(2,q))$.
Sia P un p-Sylow di G; da un risultato di F. Gross [1, pp. 321-322] abbiamo che $(|N_{GL(n,q)}(P)|)_r = (n)_r$. Nel nostro caso $n = 2$ e quindi $(|N_G(P)|)_r = 2^k$ con $k \in \{0, 1\}$. Allora:

$$(n_p(PSL(2,q))_r = (n_p(G))_r = ([G : N_G(P)])_r = r^{f-k}.$$

Ma abbiamo visto prima che $ord_p(r) = 2f$, quindi $r^{f-k} \not\equiv 1 \bmod p$. Concludiamo quindi che $PSL(2,q)$ non è un gruppo SSN.

Se dimostriamo che, sotto le ipotesi del teorema, esiste sempre un primo p di Zsigmondy di $q^2 - 1$, abbiamo concluso.
Supponiamo che non esista un primo di Zsigmondy di $q^2 - 1$: dal teorema di Zsigmondy q deve essere del tipo $q = 2^e - 1$ per qualche intero e; ricordiamo però che per ipotesi $q = r^f$ con r primo e f intero positivo, quindi deve valere $2^e - 1 = r^f$; sicuramente $r \neq 2$; supponiamo $f > 1$; per il teorema di Zsigmondy esiste un primo p tale che $p|r^{2f} - 1$ e $p \nmid r^f - 1$, ma allora $p|r^f + 1$; osserviamo inoltre che la condizione $p \nmid r^f - 1$, dove ricordiamo che r è dispari, implica che $p \neq 2$. Ma allora $r^f + 1$ non può essere potenza di 2.
Questo ci permette di affermare che per $f > 1$ non si presenta mai il caso $q = r^f = 2^e - 1$. Rimane solamente da controllare cosa succede per $f = 1$; in questo caso $q = r$ e $2^e - 1 = r$ ovvero $2^e - 1$ è un primo, e in particolare quindi q è un primo di Mersenne: contraddizione con le ipotesi del teorema.

($\Leftarrow$)
Consideriamo $PSL(2,q)$ con q primo di Mersenne (quindi $q = 2^a - 1$ per qualche primo a) e mostriamo che è un gruppo SSN.
L'ordine del gruppo è $|PSL(2,q)| = \frac{(q-1)q(q+1)}{2} = \frac{(2^a-2)(2^a-1)2^a}{2}$, quindi i suoi divisori primi sono 2, q e gli altri divisori primi di $q-1$ (oltre a 2).

- n_2 è sempre risolubile, come già osservato in precedenza.
- Dalla lista di Dickson dei sottogruppi di $PSL(2,q)$ (vedere ad esempio [9, teorema 2.1]) abbiamo che:

  $n_q = q + 1 = 2^a \equiv 1 \bmod q$;

  quindi n_q è risolubile.
- Sia p un divisore primo di $q-1$ (diverso da 2).
  Osserviamo che $q-1 = 2^a - 2$ dunque $p|\frac{q-1}{2}$; inoltre (sempre basandoci sulla lista dei sottogruppi di $PSL(2,q)$) $n_p = \frac{q(q+1)}{2}$, quindi i divisori primi di n_p sono q e 2.
  $(n_p)_q = q \equiv 1 \bmod p$ per ipotesi.
  $(n_p)_2 = \frac{q+1}{2} \equiv 1 \bmod p$, avendo già osservato che $p|\frac{q-1}{2} = \frac{q+1}{2} - 1$.
  Dunque anche n_p è risolubile. $\square$

Capitolo 3

Pseudo numeri di Sylow

Ricordando ancora una volta i classici teoremi di Sylow, è ben noto che $n_p \equiv 1 \mod p$; ci chiediamo ora se vale il viceversa, ovvero se dato un primo p, ogni intero positivo n tale che $n \equiv 1 \mod p$, è il numero di p-Sylow di qualche gruppo.
Introduciamo quindi la seguente definizione.

Definizione 3.1. Un intero positivo $n \equiv 1 \mod p$ è detto pseudo numero di p-Sylow se non esiste un gruppo finito che abbia esattamente n p-Sylow.

Se $p = 2$, ogni intero dispari n è il numero di 2-Sylow del gruppo diedrale di ordine $2n$ (i 2-Sylow sono in biiezione con le riflessioni).
Se invece p è un primo dispari, non tutti i numeri congrui a 1 mod p sono il numero di p-Sylow di qualche gruppo, come possiamo vedere ad esempio grazie al seguente teorema di M. Hall.

Teorema 3.2. *Sia p un primo e r un intero tale che $1 < r < \frac{p+3}{2}$. Allora gli interi $n = 1 + rp$ sono pseudo numeri di p-Sylow, a meno che non si presenti uno dei seguenti casi:*

1. *$n = q^t$ con q primo, $t \geq 1$ intero;*
2. *$r = \frac{p-3}{2}$ e $p > 3$ è un primo di Fermat (primo esprimibile come $p = 2^{2^m} + 1$ per qualche m intero non negativo).*

Osservazione 3.3. Il teorema non ci permette di escludere che qualche numero congruo a 1 mod 3 sia il numero di 3-Sylow; infatti se $p = 3$, l'ipotesi $1 < r < \frac{p+3}{2}$ concede di considerare solamente $r = 2$; avremmo quindi $n = 7$, che ricade nel primo dei due casi esclusi. Fuori dalle ipotesi del teorema abbiamo però esempi di pseudo numeri di 3-Sylow: M. Hall dimostrò che non esistono gruppi con 22 3-Sylow.

Con considerazioni simili, notiamo subito che il teorema non ci permette di escludere neanche che qualche intero congruo a 1 mod 5 sia il numero di 5-Sylow, ma ancora una volta M. Hall ci fornisce un esempio di pseudo numeri di 5-Sylow, dimostrando che non esistono gruppi con 21 5-Sylow.
È con $p = 7$ che iniziamo a vedere le prime applicazioni del teorema: 15 e 22 sono pseudo numeri di 7-Sylow.

La dimostrazione generale del teorema, che non riportiamo, utilizza un risultato di Brauer e Reynolds nell'ambito della teoria della rappresentazione modulare; ci sono alcuni casi in cui invece la dimostrazione risulta più elementare: mostriamo ad esempio che 15 è pseudo numero di 7-Sylow e 35 è pseudo numero di 17-Sylow. Prima richiamiamo alcune nozioni e risultati che ci serviranno.

Lemma 3.4. *Sia p un primo dispari e σ un prodotto di due p-cicli disgiunti in A_{2p}. Allora $|C_{A_{2p}}(\sigma)| = p^2$.*

Dimostrazione.

($\geq$) Osserviamo innanzitutto che σ è effettivamente una permutazione pari e quindi $\sigma \in A_{2p}$; possiamo assumere, senza perdita di generalità, che $\sigma = (1, ..., p)(p+1, ..., 2p)$; allora $\langle (1, ..., p), (p+1, ..., 2p) \rangle \leq C_{A_{2p}}(\sigma)$ e $|C_{A_{2p}}(\sigma)| \geq p^2$.

($\leq$) Consideriamo $\tau \in C_{S_{2p}}(\sigma)$; ci sono al più $2p$ possibili scelte per $\tau(1)$; inoltre, per $i = 2, ..., p$, vale $\tau(i) = \tau(\sigma^{i-1}(1)) = \sigma^{i-1}(\tau(1))$; dunque, fissato $\tau(1)$, rimangono p possibilità per $\tau(p+1)$; come prima, per $i = 2, ..., p$ vale $\tau(p+i) = \tau(\sigma^{i-1}(p+1)) = \sigma^{i-1}(\tau(p+1))$; in totale quindi ci sono $2p^2$ scelte per τ e vale $|C_{S_{2p}}(\sigma)| \leq 2p^2$. Ora, se definiamo $\tau = (1, p+1)(2, p+2) \cdots (p, 2p)$, abbiamo $\tau \in C_{S_{2p}}(\sigma)$, ma $\tau \notin A_n$ essendo p dispari. Allora $C_{A_{2p}}(\sigma) \subset C_{S_{2p}}(\sigma)$ e $|C_{A_{2p}}(\sigma)| \leq \frac{|C_{S_{2p}}(\sigma)|}{2} \leq p^2$. $\square$

Proposizione 3.5 (Brodkey)**.** *Sia G un gruppo e supponiamo che G abbia un p-Sylow abeliano per qualche primo p. Allora esistono $P, Q \in Syl_p(G)$ tali che $P \cap Q = O_p(G)$, dove $O_p(G)$ è l'intersezione di tutti i p-Sylow di G.*

Dimostrazione.

($\geq$) Per definizione $P \cap Q \geq O_p(G)$.

($\leq$) Scegliamo P, $Q \in Syl_p(G)$ tali che la loro intersezione $P \cap Q$ sia più piccola possibile. Definiamo $N := N_G(P \cap Q)$; essendo P e Q abeliani per ipotesi, abbiamo $P \cap Q \trianglelefteq P$ e $P \cap Q \trianglelefteq Q$, e dunque P e Q sono due

p-Sylow di N. Sia $S \in Syl_p(G)$; ricordando che, per il secondo teorema di Sylow, ogni p-sottogruppo di G è coniugato a un sottogruppo di un p-Sylow, segue che $\exists g \in N$ tale che $S^g \cap N = (S \cap N)^g \leq P$, dove indichiamo con S^g i coniugati di S tramite g. Allora $S^g \cap Q = S^g \cap N \cap Q \leq P \cap Q$; ma questo implica, per la minimalità di $P \cap Q$, che $P \cap Q = S^g \cap Q$, quindi in particolare $P \cap Q \leq S^g$; coniugando tramite g^{-1} entrambi i membri, e osservando che $(P \cap Q)^{g^{-1}} = P \cap Q$, otteniamo $P \cap Q \leq S$. Avendo scelto S in modo arbitrario, possiamo concludere che $P \cap Q \leq O_p(G)$. $\square$

Lemma 3.6. *Sia G un gruppo con un p-Sylow P di ordine p. Allora $\frac{N_G(P)}{C_G(P)}$ è ciclico e il suo ordine divide $p-1$.*

Dimostrazione. Ricordando che $N_G(P)$ agisce per coniugio su P e che il nucleo di tale azione è $C_G(P)$, per il primo teorema di isomorfismo si ha che $\frac{N_G(P)}{C_G(P)}$ è isomorfo a un sottogruppo di $Sym(P)$; dato che il coniugio induce isomorfismi su P, possiamo considerare $\frac{N_G(P)}{C_G(P)}$ come un sottogruppo di $Aut(P)$; per ipotesi $P \cong \mathbb{Z}/p\mathbb{Z}$, dunque $Aut(P) \cong (\mathbb{Z}/p\mathbb{Z})^\times$; è noto che $(\mathbb{Z}/p\mathbb{Z})^\times$ è ciclico di ordine $p-1$, quindi possiamo concludere, per il teorema di Lagrange, che $\frac{N_G(P)}{C_G(P)}$ è ciclico e il suo ordine divide $p-1$. $\square$

Lemma 3.7. *Sia G un gruppo con un 2-Sylow Q ciclico. Allora esiste un unico $N \triangleleft G$ tale che $[G:N] = |Q|$.*

Dimostrazione. Dimostriamo per induzione su $|Q| = 2^n$.
Per $n = 0$, G non ha 2-Sylow quindi la tesi è soddisfatta prendendo $N = G$. Sia ora $n \geq 1$. G agisce su se stesso tramite moltiplicazione a sinistra: $x^g := gx$ per g,$x \in G$; sappiamo che questa azione induce un omomorfismo $\sigma\colon G \to Sym(G)$, e osserviamo che il nucleo è banale. Possiamo quindi considerare G come un sottogruppo di $Sym(G)$ e vedere ogni elemento non banale di G come una permutazione senza punti fissi. Sia x un generatore di Q; x è prodotto di $\frac{|G|}{2^n}$ 2^n-cicli disgiunti; in particolare x è una permutazione dispari. Definiamo $H := G \cap A_{|G|}$ dove indichiamo con $A_{|G|}$ il gruppo alterno con $|G|$ elementi; osserviamo che H è un sottogruppo normale di G con indice $[G:H] = 2$. Inoltre $Q \cap H$ è un 2-Sylow ciclico di H; possiamo quindi applicare l'ipotesi induttiva ad H: esiste un unico $N \trianglelefteq H$ con $[H:N] = |Q \cap H| = 2^{n-1}$. Sia $g \in G$; vale $gNg^{-1} \trianglelefteq gHg^{-1} = H$ e $[H : gNg^{-1}] = [H:N]$; ma dall'unicità di N segue $N = gNg^{-1}$, quindi $N \trianglelefteq G$ e $[G:N] = [G:H][H:N] = 2^n$. Infine, se $M \trianglelefteq G$ con $[G:M] = 2^n$, allora $M \trianglelefteq H$ e per l'unicità di N concludiamo che $M = N$. $\square$

Lemma 3.8. *Sia G un gruppo di ordine $p^\alpha n$ con p primo e $(p,n) = 1$. Se $N \triangleleft G$ ha indice coprimo con p, allora N contiene tutti i p-Sylow di G.*

Lemma 3.9. *Sia G un gruppo abeliano di ordine q^n, con q primo. Allora $Aut(G) = GL(n, q)$.*

Proposizione 3.10. *Sia G un gruppo finito tale che tutti i suoi sottogruppi di Sylow siano ciclici; allora G è risolubile.*

Dimostrazione. Possiamo assumere G non banale e dimostrare per induzione su $|G|$; sia p il più piccolo divisore primo di $|G|$; allora G ha un p-complemento normale N (conseguenza del teorema di Burnside, vedere [8, corollario 5.14]), ovvero un sottogruppo normale N tale che l'indice $[G : N]$ sia uguale all'ordine di un p-Sylow di G . Inoltre, $|N| < |G|$ e tutti i sottogruppi di Sylow di N sono ciclici, allora per ipotesi induttiva N è risolubile; anche $\frac{G}{N}$, essendo un p-gruppo, è risolubile, dunque possiamo concludere che G è risolubile.

Teorema 3.11. *Non esistono gruppi finiti con 15 7-Sylow.*

Dimostrazione. Supponiamo esista un gruppo finito G con 15 7-Sylow, in particolare prendiamo G minimale per questa proprietà. Per non appesantire la notazione continuiamo ad usare n e p, ricordando che corrispondono a 15 e 7 rispettivamente.
Procediamo per passi.

Passo 1: dimostriamo che G agisce fedelmente, ovvero con nucleo banale, su $Syl_p(G)$, l'insieme di tutti i p-Sylow di G, e che $G \leq A_n$.
Sia $\{1\} \neq K \triangleleft G$ il nucleo dell'azione di G su $Syl_p(G)$ e mostriamo che la mappa

$$\gamma \colon Syl_p(G) \to Syl_p\left(\frac{G}{K}\right)$$
$$P \mapsto \frac{PK}{K}$$

è biiettiva.

- Suriettività. Ricordiamo che $\frac{PK}{K}$ è un p-Sylow di $\frac{G}{K}$ e che tutti i p-Sylow di $\frac{G}{K}$ sono coniugati in $\frac{G}{K}$, quindi ogni p-Sylow di $\frac{G}{K}$ è del tipo $(gK)(\frac{PK}{K})(gK)^{-1} = \frac{gPg^{-1}K}{K}$ per qualche $g \in G$.

- Iniettività.
  Siano P e Q due p-Sylow di G tali che $\frac{PK}{K} = \frac{QK}{K}$; in particolare vale $PK = QK$. Essendo K il nucleo dell'azione, K agisce banalmente su $Syl_p(G)$; allora P è l'unico p-Sylow di PK e Q è l'unico p-Sylow di QK, ma ricordando che $PK = QK$ per ipotesi, allora $P = Q$.

Ora, essendo γ biiettiva, abbiamo che anche $\frac{G}{K} < G$ ha n p-Sylow, contro la minimalità di G. Concludiamo quindi che deve essere $K = \{1\}$, ovvero che l'azione di G su $Syl_p(G)$ è fedele.
Sappiamo che ogni azione induce un morfismo di gruppi $G \to S_n$, e dunque in particolare G è isomorfo ad un sottogruppo del gruppo simmetrico S_n; supponiamo che $G \cap A_n < G$. A_n, contenendo tutti gli elementi di ordine dispari, sicuramente contiene ogni p-Sylow di G e quindi anche $G \cap A_n < G$ ha n p-Sylow, contro la minimalità di G. Concludiamo dunque che deve essere $G \cap A_n = G$, ovvero $G \leq A_n$.

Passo 2: dimostriamo che l'ordine di un p-Sylow è p.
Fissiamo un p-Sylow P. Sapendo che $G \leq A_n$, abbiamo che $|G|$ divide $\frac{n!}{2}$, quindi in particolare $|P|$ divide $\frac{n!}{2}$; osserviamo inoltre che $p^3 \nmid \frac{n!}{2}$ dunque $|P| = p$ oppure $|P| = p^2$; in entrambi i casi P è abeliano, quindi per la proposizione 3.5 $O_p(G) = P \cap Q$ $\exists Q \in Syl_p(G)$; poiché $O_p(G)$ è contenuto nel nucleo dell'azione su $Syl_p(G)$, che abbiamo dimostrato essere banale, abbiamo $P \cap Q = O_p(G) = \{1\}$.
Consideriamo $N_P(Q)$; sicuramente è contenuto in P, ma è contenuto anche in Q, infatti $N_P(Q)$ è un p-gruppo e $N_P(Q) \subseteq N_G(Q)$, ma allora $N_P(Q)$ sta nell'unico p-Sylow Q di $N_G(Q)$ (sicuramente $N_G(Q) \supseteq Q$ e Q è unico perché il numero di p-Sylow di $N_G(Q)$ è dato da $[N_G(Q) : N_{N_G(Q)}(Q)] = [N_G(Q) : N_G(Q)] = 1$. Allora $N_P(Q) \subseteq P \cap Q = \{1\}$, cioè $N_P(Q) = \{1\}$. Indicando con Q^P l'insieme dei coniugati di Q tramite elementi di P, concludiamo che:

$$|P| = [P : N_P(Q)] = |Q^P| \leq n < p^2 \Rightarrow |P| = p.$$

Passo 3: dimostriamo che $\frac{N_G(P)}{P}$ è ciclico di ordine $p-1$.
Osserviamo che $N_G(P)$ è per costruzione lo stabilizzatore di P e dal passo 1 abbiamo:

$$P \leq N_G(P) \leq S_{n-1} \cap A_n = A_{n-1} = A_{2p}.$$

Se $P \leq N_G(Q)$ per qualche p-Sylow Q, allora $P = Q$, avendo osservato in precedenza che Q è l'unico p-Sylow di $N_G(Q)$. Inoltre P è generato da un prodotto di due p-cicli disgiunti in A_{2p}; dal passo 1 e dal lemma 3.4 segue che:

$$P \leq C_G(P) \leq C_{A_{2p}} \cap G = P \Rightarrow P = C_G(P).$$

Allora $\frac{N_G(P)}{P} = \frac{N_G(P)}{C_G(P)}$, che per il lemma 3.6 è ciclico di ordine che divide $p-1$.

Passo 4: contraddizione.
Abbiamo visto che $\frac{N_G(P)}{P}$ è ciclico di ordine che divide $p - 1 = 6$; possiamo quindi distinguere 4 casi.

1. $|\frac{N_G(P)}{P}| = 1$.
   In questo caso $|G| = 3 \cdot 5 \cdot 7$; sappiamo che in un gruppo di ordine qrs, con $q < r < s$ primi, l's-Sylow è normale e dunque c'è un unico s-Sylow; nel nostro caso quindi ci sarebbe un unico 7-Sylow, contro l'ipotesi $n_7 = 15$.

2. $|\frac{N_G(P)}{P}| = 2$.
   Essendo $[G : N_G(P)]$ dispari, $N_G(P)$ contiene un 2-Sylow ciclico Q di G e applicando il lemma 3.6, troviamo un sottogruppo $N \triangleleft G$ di ordine $|N| = [G : Q] = 3 \cdot 5 \cdot 7$; ma allora N ha un unico 7-Sylow S normale; osserviamo poi che per il lemma 3.7 il numero di p-Sylow di G è uguale al numero di p-Sylow di N; segue quindi che G ha un unico 7-Sylow, contro l'ipotesi $n_7 = 15$.

3. $|\frac{N_G(P)}{P}| = 3$.
   In questo caso $|G| = 3^2 \cdot 5 \cdot 7$; dai classici teoremi di Sylow otteniamo $n_3 \in \{1, 7\}$, $n_5 \in \{1, 21\}$; distinguiamo 2 casi:

   - Se un 3-Sylow o un 5-Sylow è normale, allora G è risolubile e, per il teorema di P. Hall, n_7 è prodotto di fattori del tipo $q_i^{t_i}$ con q_i primo e $q_i^{t_i} \equiv 1 \bmod 7$ $\forall i$; per ipotesi $n_7 = 15 = 3 \cdot 5$ ma $3 \not\equiv 1 \bmod 7$, contraddizione.
   - Supponiamo che $n_3 = 7$ e $n_5 = 21$. Osserviamo che i 5-Sylow, avendo ordine 5, sono ciclici e allo stesso modo i 7-Sylow, avendo ordine 7, sono ciclici; invece, per un 3-Sylow T, avendo ordine 9, dobbiamo considerare separatamente il caso in cui $T \cong C_9$ e $T \cong C_3 \times C_3$.
     a) Se anche i 3-Sylow sono ciclici, allora per la proposizione 3.10 il gruppo G è risolubile e come prima troviamo che $n_7 = 15$ contraddice il teorema di P. Hall.
     b) Consideriamo ora il caso in cui $T \cong C_3 \times C_3$; dal lemma 3.9 sappiamo che $Aut(C_3 \times C_3) = GL(2, 3)$ e quindi $|Aut(C_3 \times C_3)| = |GL(2, 3)| = 48$; dunque detto S un 7-Sylow, non essendoci automorfismi di ordine 7, S centralizza T; ma allora $S \subseteq N_G(T)$; segue che $[G : N_G(T)]$ non è divisibile per 7, contraddicendo l'ipotesi $n_3 = 7$ (ricordiamo che $[G : N_G(T)] = n_3$).

4. $|\frac{N_G(P)}{P}| = 6$.
   Essendo $[G : N_G(P)]$ dispari, $N_G(P)$ contiene un 2-Sylow ciclico Q di G e, applicando il lemma 3.7, troviamo un sottogruppo $N \triangleleft G$ di ordine

$|N| = [G : Q] = 3^2 \cdot 5 \cdot 7$. Ricordando che per il lemma 3.8 il numero di p-Sylow di N è uguale al numero di p-Sylow di G per $p \in \{3, 5, 7\}$, possiamo ora applicare ad N le stesse considerazioni fatte per G nel punto 3, escludendo quindi anche questo caso. □

Teorema 3.12. *Non esistono gruppi finiti con 35 17-Sylow.*

Dimostrazione. Supponiamo esista un gruppo finito G con 35 17-Sylow, in particolare prendiamo G minimale per questa proprietà.
Quanto fatto nei primi 3 passi della dimostrazione precedente vale in generale per $n_p = 1 + 2p$. In particolare quindi, anche per $p = 17$ e $n = 35$, detto P un 17-Sylow di G, abbiamo che $\frac{N_G(P)}{P}$ è ciclico di ordine che divide $16 = 2^4$. Allora $N_G(P)$ contiene un 2-Sylow ciclico e riusciamo a trovare, in maniera del tutto analoga a quanto fatto nella dimostrazione precedente, un sottogruppo normale N di ordine $|N| = 5 \cdot 7 \cdot 17$. Ma allora N ha un unico 17-Sylow ed essendo, sempre per il lemma 3.8, $n_{17}(G) = n_{17}(N)$, concludiamo che G ha un unico 17-Sylow, contro l'ipotesi $n_{17} = 35$. □

Vediamo ora una conseguenza del teorema 3.2 che ci permette di escludere alcuni interi in modo più immediato, dato che l'unica ipotesi questa volta è $p \geq 7$.

Corollario 3.13. *Sia p un primo, $p \geq 7$. Non esistono gruppi con $n = 1+3p$ p-Sylow.*

Dimostrazione. $p \geq 7 \Rightarrow \frac{p+3}{2} \geq 5$ quindi $r = 3$ rientra nelle ipotesi del teorema 3.2. Per concludere quindi che non esistano gruppi con $n = 1 + 3p$ p-Sylow, dobbiamo controllare che non possano presentarsi i 2 casi esclusi dal teorema.

1. Supponiamo che $n = 1+3p$ sia potenza di qualche primo q. In particolare, essendo $1+3p$ sicuramente pari per $p \neq 2$, deve valere $1+3p = 2^t$ $\exists t$. Osservando poi che $2^t - 1$ non è divisibile per 3 se t è dispari, questo implica che t sia pari; considerando quindi $t = 2s$, abbiamo l'uguaglianza $3p = 2^{2s} - 1 = (2^s - 1)(2^s + 1)$, resa possibile solamente in questi casi:

   - $2^s - 1 = 1$ e $(2^s + 1) = 3p$, ma allora $s = 1 \Rightarrow 3p = 3 \Rightarrow p = 1$, assurdo;
   - $2^s - 1 = 3$ e $(2^s + 1) = p$, ma allora $s = 2 \Rightarrow 3p = 15 \Rightarrow p = 5$, contraddicendo l'ipotesi $p \geq 7$;
   - $2^s - 1 = p$ e $(2^s + 1) = 3$, ma allora $s = 1 \Rightarrow 3p = 3 \Rightarrow p = 1$, assurdo.

Possiamo quindi concludere che, per $p \geq 7$, $1 + 3p$ non è mai potenza di primo.

2. Il caso $r = \frac{p-3}{2}$, ricordando che qui $r = 3$, si presenta solo per $p = 9$, che però non è un primo di Fermat, quindi neanche il caso 2 descritto dal teorema può presentarsi. □

Osservazione 3.14. L'ipotesi $p \geq 7$ è fondamentale, infatti:

- il gruppo alterno A_5 ha $10 = 1 + 3 \cdot 3$ 3-Sylow;
- il prodotto semidiretto di F_{16} con C_5 ha $16 = 1 + 3 \cdot 5$ 5-Sylow.

Riassumendo, sappiamo che per ogni primo p dispari esiste uno pseudo numero di p-Sylow.

Capitolo 4

Pseudo numeri di Frobenius

In questo capitolo cerchiamo di capire quali risultati visti nei capitoli precedenti sui p-Sylow si possano generalizzare a sottogruppi di ordine p^k per qualche $k \geq 0$.
Iniziamo a indagare sul numero di p-sottogruppi di un gruppo. Consideriamo un gruppo G tale che p^k divide $|G|$ per qualche intero $k \geq 0$ e indichiamo con $m_{p^k}(G)$ il numero di sottogruppi di G di ordine p^k.

Proposizione 4.1. *Sia P un p-Sylow di G; $\forall k \geq 0$ vale:*

$$m_{p^k}(P) \equiv m_{p^k}(G) \ mod\ p.$$

Dimostrazione. Definiamo i seguenti insiemi:

- $\Omega := \{X \leq G \mid |X| = p^k\}$;
- $\tilde{\Omega} := \{X \in \Omega \mid P \text{ normalizza } X\}$ (osserviamo che $X \in \tilde{\Omega} \Rightarrow X \subseteq P$);
- $\Lambda := \{X \leq P \mid |X| = p^k\}$.

Facendo agire P per coniugio su Ω, si deduce che $|\Omega| \equiv |\tilde{\Omega}| \bmod p$; facendo agire P per coniugio su Λ, si deduce che $|\Lambda| \equiv |\tilde{\Omega}| \bmod p$. Si conclude quindi che $|\Lambda| \equiv |\Omega| \bmod p$, ovvero $m_{p^k}(P) \equiv m_{p^k}(G) \bmod p$. $\square$

Vediamo ora il seguente risultato di Frobenius.

Teorema 4.2 (Frobenius)**.** *Siano G un gruppo finito, p un primo e $k \geq 0$ intero tali che p^k divida l'ordine di G. Allora $m_{p^k}(G) \equiv 1$ mod p.*

Grazie alla proposizione 4.1, è sufficiente dimostrare il teorema di Frobenius per p-gruppi finiti, ovvero:

Teorema 4.3. *Sia G un p-gruppo finito e $k \geq 0$ intero tale che p^k divida l'ordine di G. Vale $m_{p^k}(G) \equiv 1$ mod p.*

Dimostrazione. Sia $Z \leq Z(G)$ con $|Z| = p$. Definiamo i seguenti insiemi:

- $\Omega := \{X \leq G \mid |X| = p^k\}$;
- $\Omega_1 := \{X \in \Omega \mid Z \subseteq X\}$;
- $\Omega_2 := \{X \in \Omega \mid Z \not\subseteq X\}$;
- $\Delta := \{Y \leq G \mid |Y| = p^{k+1}, Z \subseteq Y\}$.

Ovviamente $m_{p^k}(G) = |\Omega| = |\Omega_1| + |\Omega_2|$; per ipotesi induttiva vale $|\Omega_1| = m_{p^{k-1}}(\frac{G}{Z}) \equiv 1 \bmod p$; basta quindi provare che $|\Omega_2| \equiv 0 \bmod p$.
Sia $Y \in \Delta$. Definiamo:

- $\Omega_Y := \{K \subseteq Y \mid |K| = p^k\}$;
- $A_Y := \{K \in \Omega_Y \mid Z \subseteq K\}$;
- $B_Y := \{K \in \Omega_Y \mid Z \not\subseteq K\}$.

Ora, se consideriamo $X \in \Omega_2$, si ha $Y = XZ \in \Delta$ ed è l'unico elemento di Δ con $X \in B_Y$. Quindi $|\Omega_2| = \sum_{Y \in \Delta} |B_Y|$, dunque basta provare che per ogni $Y \in \Delta$ vale $|B_Y| \equiv 0 \bmod p$.
Ma $|B_Y| = |\Omega_Y| - |A_Y|$, dove $|\Omega_Y| = m_{p^k}(Y) \equiv 1 \bmod p$ e $|A_Y| = m_{p^{k-1}}(\frac{Y}{Z}) \equiv 1 \bmod p$, perciò si conclude che $|B_Y| \equiv 0 \bmod p$. □

4.1 Il teorema di Kulakoff-Hall

Definizione 4.4. Un intero positivo n è detto p-numero di Frobenius se esiste un gruppo finito che abbia esattamente n sottogruppi di ordine p^k, per qualche intero $k \geq 0$.

In modo analogo a quanto fatto per i numeri di p-Sylow, potremmo ora definire gli pseudo p-numeri di Frobenius; ne daremo una definizione appropriata dopo aver studiato il teorema di Kulakoff-Hall sul numero di p-sottogruppi di un gruppo; in particolare vedremo la dimostrazione data da Hall, che generalizza il risultato di Kulakoff sui p-gruppi.
Partiamo da un risultato di Herzog, sul numero di elementi di ordine p di un gruppo G, nel caso particolare in cui siano soddisfatte le ipotesi del teorema di Kulakoff-Hall, ovvero si suppone che p sia un primo dispari e che i p-Sylow di G non siano ciclici.

Denotiamo con $I_p(G)$ l'insieme degli elementi di G di ordine p, con $i_p(G)$ la cardinalità di tale insieme e con E_{p^n} un gruppo abeliano elementare di ordine p^n; ricordiamo che in un gruppo abeliano elementare ogni elemento non banale ha ordine p e diamo per noto che ogni p-gruppo, sotto le nostre ipotesi, abbia un sottogruppo normale E_{p^2}, ovvero del tipo $C_p \times C_p$. Enunciamo innanzitutto un risultato preliminare che ci servirà nella dimostrazione.

Teorema 4.5. *Sia $E := E_{p^n}$ un sottogruppo di G, $T := I_p(N_G(E))$, $D := I_p(G) \setminus T$; supponiamo che se $a \in D$ e $H = C_E(a) \times \langle e \rangle$ per qualche $e \in E \setminus C_E(a)$ allora $a \notin N_G(H)$. Allora vale:*

$$i_p(G) \equiv |T| \ mod\ p^n.$$

Osservazione 4.6. Quando $|E| \leq p^2$ l'ipotesi di questo teorema è soddisfatta.

Lemma 4.7 (Herzog)**.** *Sia p un primo dispari e G un gruppo con p-Sylow non ciclici. Vale:*

$$i_p(G) \equiv -1 \ mod\ p^2.$$

Dimostrazione. Sia P un p-Sylow di G; essendo per ipotesi non ciclico ha ordine almeno p^2; come ricordato in precedenza, esiste $E = E_{p^2} \trianglelefteq P$. Grazie al teorema 4.5, è sufficiente considerare il caso $E \triangleleft G$. Se consideriamo $x \in G \setminus E$ tale che $x^p \in E$, si ha che $\langle x, E \rangle$ è un gruppo di ordine p^3; dalla classificazione dei gruppi di ordine p^3 si deduce che i suoi elementi di ordine p possono essere $p^2 - 1$ oppure $p^3 - 1$; inoltre, gruppi distinti di questo tipo si intersecano in E; allora possiamo calcolare il numero di elementi di G di ordine p nel seguente modo:

$$i_p(G) = i_p(E) + \sum_{\langle x,E \rangle} (i_p(\langle x, E \rangle) - i_p(E));$$

ora $i_p(E) = p^2 - 1$, mentre $i_p(\langle x, E \rangle)$ per quanto detto prima vale $p^2 - 1$ oppure $p^3 - 1$; in ogni caso si conclude che:

$$i_p(G) \equiv -1 \bmod p^2. \square$$

Lemma 4.8. *Sia p un primo dispari e G un gruppo con p-Sylow non ciclici; allora il numero di sottogruppi di G di ordine p soddisfa la seguente congruenza:*

$$m_p(G) \equiv 1 + p \ mod\ p^2.$$

Dimostrazione. Indicando, come fatto finora, con $m_p(G)$ il numero di sottogruppi di G di ordine p e con $i_p(G)$ il numero di elementi di G di ordine p, vale l'uguaglianza:

$$m_p(G)(p-1) = i_p(G).$$

Ora, per il lemma 4.7, si ha $i_p(G) \equiv -1 \bmod p$ e dunque:

$$m_p(G)(p-1) \equiv -1 \bmod p^2.$$

Moltiplicando per $-(1+p)$ otteniamo

$$m_p(G)(1-p^2) \equiv 1+p \bmod p^2$$

e possiamo quindi concludere che

$$m_p(G) \equiv 1+p \bmod p^2. \square$$

Abbiamo visto con la proposizione 4.1 che, se P è un p-Sylow di G, $\forall k \geq 0$ il numero di sottogruppi di P di ordine p^k è congruo modulo p al numero di sottogruppi di G di ordine p^k. Il prossimo risultato assicura che la congruenza continui a valere in particolare anche per sottogruppi ciclici. Indichiamo con $m_{p^k}(G;C)$ il numero di sottogruppi di G ciclici e di ordine p^k.

Proposizione 4.9. *Sia P un p-Sylow di G; $\forall k \geq 0$ vale:*

$$m_{p^k}(P;C) \equiv m_{p^k}(G;C) \ \textit{mod } p.$$

Dimostrazione. Sia P un p-Sylow si G; definiamo i seguenti insiemi:

- $\Omega := \{X \leq G \mid X \text{ ciclico}, |X| = p^k\}$;
- $\Omega_1 := \{X \in \Omega \mid X \not\subseteq P\}$;
- $\Omega_2 := \{X \in \Omega \mid X \subseteq P\}$.

Ovviamente vale $\Omega = \Omega_1 \cup \Omega_2$.
P agisce per coniugio su Ω_1; se $X \in \Omega_1$, la lunghezza della sua orbita è $|X^P| = [P : N_P(X)]$, dunque sicuramente un multiplo di p; allora $|\Omega_1| \equiv 0 \bmod p$. Segue che:

$$|\Omega| = |\Omega_1| + |\Omega_2| \equiv |\Omega_2| \bmod p.$$

Essendo $|\Omega| = m_{p^k}(G;C)$ e $|\Omega_2| = m_{p^k}(P;C)$, si conclude che:

$$m_{p^k}(G;C) \equiv m_{p^k}(P;C) \bmod p. \square$$

Alcuni richiami prima di dimostrare il risultato di Miller sul numero di p-sottogruppi ciclici.

Definizione 4.10. Sia G un gruppo; il suo sottogruppo di Frattini, denotato con $\Phi(G)$, è l'intersezione di tutti i sottogruppi massimali di G.

Osservazione 4.11. Se G è un p-gruppo finito valgono i due seguenti fatti:

1. $\Phi(G)$ è il più piccolo sottogruppo normale N di G tale che $\frac{G}{N}$ sia un p-gruppo abeliano elementare;

2. G è ciclico se e solo se $\frac{G}{\Phi(G)}$ è ciclico. L'implicazione $\Rightarrow$ è immediata dato che ogni quoziente di un gruppo ciclico è ciclico, mentre $\Leftarrow$ segue dal fatto che $\Phi(G)$ è l'insieme dei non-generatori di G, ovvero l'insieme degli elementi $x \in G$ tali che se $G = \langle X, x\rangle$ allora $G = \langle X\rangle$; infatti:

   ($\subseteq$) sia $x \in \Phi(G)$ e supponiamo $G = \langle X, x\rangle$; se $\langle X\rangle \neq G$, allora $\langle X\rangle$ è contenuto in un sottogruppo M massimale; ma $x \in \Phi(G) \leq M$ dunque $\langle X, x\rangle \leq M < G$, contraddicendo l'ipotesi iniziale;

   ($\supseteq$) sia x un non-generatore di G e M un sottogruppo massimale di G; $\langle M, x\rangle \geq M$ ma allora $\langle M, x\rangle = G$ oppure $\langle M, x\rangle = M$; se $\langle M, x\rangle = G$ allora $\langle M\rangle = G$, essendo x non-generatore; allora $\langle M, x\rangle = M$ cioè $x \in M$; per l'arbitrarietà di M, x appartiene ad ogni sottogruppo massimale di G, dunque $x \in \Phi(G)$.

   In particolare quindi se $\frac{G}{\Phi(G)}$ è ciclico, consideriamo $x \in G$ tale che $\langle x\Phi(G)\rangle = \frac{G}{\Phi(G)}$; allora $G = \langle x, \Phi(G)\rangle$ e dunque $G = \langle x\rangle$.

Teorema 4.12 (Miller)**.** *Siano p un primo dispari e G un gruppo con p-Sylow non ciclici; $\forall k > 1$ vale:*

$$m_{p^k}(G; C) \equiv 0 \ mod\ p.$$

Dimostrazione. Grazie alla proposizione 4.9 basta dimostrare il teorema per i p-gruppi.
Sia G un p-gruppo non ciclico. Grazie all'osservazione 4.11, possiamo affermare che $\frac{G}{\Phi(G)}$ è un p-gruppo abeliano elementare di ordine almeno p^2; allora $\frac{G}{\Phi(G)}$ ha un quoziente isomorfo a $C_p \times C_p$; dunque $\exists T \trianglelefteq G$ tale che $\frac{G}{T} \cong C_p \times C_p$; chiamiamo $\frac{F_1}{T}, ..., \frac{F_{p+1}}{T}$ i $p+1$ sottogruppi di $\frac{G}{T}$ di ordine p.
Possiamo calcolare il numero di sottogruppi ciclici di G di ordine p^k nel seguente modo:

$$m_{p^k}(G; C) = \sum_{1 \leq i \leq p+1} m_{p^k}(F_i; C) - m_{p^k}(T; C)p \tag{4.1}$$

Infatti, tale uguaglianza vale perché se consideriamo un sottogruppo ciclico $C < G$ di ordine p^k, con $k > 1$, sicuramente CT è un sottogruppo proprio di G, essendo $\frac{G}{T}$ non ciclico, e dunque possono presentarsi i due seguenti casi:

1. supponiamo che $C \subseteq F_i \ \forall i$; in particolare dunque $C \subseteq T$; allora il contributo del sottogruppo ciclico C in $\sum_{1\leq i\leq p+1} m_{p^k}(F_i; C) - m_{p^k}(T; C)p$ è $p + 1 - p = 1$;

2. supponiamo che $C \subseteq F_i \ \exists!\ i$ e dunque $C \not\subseteq T$; allora il contributo del sottogruppo ciclico C in $\sum_{1\leq i\leq p+1} m_{p^k}(F_i; C) - m_{p^k}(T; C)p$ è $1 - 0 = 1$.

Osserviamo che non possono presentarsi altri casi: se supponiamo che C sia contenuto in F_i e in F_j con $i \neq j$, allora C è contenuto in T ma in particolare quindi $C \subseteq F_i \ \forall i$, ovvero ritorniamo al caso 1.
Ora se nessuno degli F_i è ciclico, allora per induzione $m_{p^k}(F_i; C) \equiv 0 \mod p$ e grazie all'equazione 4.1 possiamo quindi concludere che $m_{p^k}(G; C) \equiv 0 \mod p$.
Supponiamo invece che G abbia un sottogruppo massimale ciclico; allora G è un prodotto semidiretto del tipo $\langle a\rangle \rtimes \langle b\rangle$ con $|a| = p^{n-1}$, $|b| = p$ e l'azione è definita da $a^b = a^{1+p^{n-2}}$; in particolare quindi $[a, b] = a^{p^{n-2}}$ e $[a, b] \in Z(G)$, dunque G è nilpotente di classe 2.
Consideriamo ora un elemento $g \in G$ di ordine p^k; sarà del tipo $a^i b^j$ per qualche i e j; calcoliamo $g^{p^{k-1}}$:

$$\begin{aligned} g^{p^{k-1}} &= (a^i b^j)^{p^{k-1}} \\ &= (a^i)^{p^{k-1}} (b^j)^{p^{k-1}} [b^j, a^i]^{\binom{p^{k-1}}{2}} \\ &= (a^i)^{p^{k-1}}. \end{aligned}$$

Se ne deduce che $\langle a^{p^{n-2}}\rangle \subseteq \langle g\rangle$, dunque contare i sottogruppi ciclici di G di ordine p^k equivale a contare i sottogruppi ciclici di $\frac{G}{\langle a^{p^{n-2}}\rangle}$ di ordine p^k, ovvero:

$$m_{p^k}(G; C) = m_{p^k}(\frac{G}{\langle a^{p^{n-2}}\rangle}; C);$$

infine, osservando che $\frac{G}{\langle a^{p^{n-2}}\rangle} \cong C_{p^{n-2}} \times C_p$, otteniamo:

$$m_{p^k}(G; C) = m_{p^k}(C_{p^{n-2}} \times C_p; C) \equiv 0 \mod p. \square$$

Vediamo ora i risultati di Hall sul numero di p-sottogruppi.

Lemma 4.13. *Sia G un gruppo con un p-Sylow P ciclico e di ordine p^n. Per $0 \leq k \leq n$ vale:*

$$m_{p^k}(G) \equiv 1 \ \textit{mod}\ p^{n-k+1}$$

Dimostrazione. Definiamo $\Omega_i := \{Q \in Syl_p(G) \mid |Q \cap P| = p^{n-i}\}$; osserviamo che P agisce per coniugio su Ω_i e che, preso $Q \in \Omega_i$, $N_P(Q) = Q \cap P$, quindi la cardinalità dell'orbita è $|Q^P| = [P : P \cap Q] = p^i$. Dunque $|\Omega_i| = \lambda_i p^i$ per qualche intero positivo λ_i. Se ne deduce che il numero di p-Sylow di G è:

$$m_{p^n}(G) = 1 + \lambda_1 p + \lambda_2 p^2 + ... + \lambda_n p^n.$$

Sia ora K un sottogruppo di G di ordine p^k per $0 \leq k \leq n$; non è restrittivo supporre che K sia l'unico sottogruppo di ordine p^k contenuto in P. Osserviamo che un p-Sylow contenente K sta in Ω_i se vale $n - i \geq n - k$, ovvero $i \leq k$; dunque, indicando con v_k il numero di p-Sylow contenenti K, per i ragionamenti precedenti vale:

$$v_k = 1 + \lambda_1 p + \lambda_2 p^2 + ... + \lambda_{n-k} p^{n-k}.$$

Osserviamo che $m_{p^k}(G)v_k = m_{p^n}(G)$; inoltre:

$$m_{p^n}(G) - v_k = \lambda_{n-k+1} p^{n-k+1} + ... + \lambda_n p^n \equiv 0 \bmod p^{n-k+1}$$

e dunque

$$m_{p^n}(G) \equiv v_k \bmod p^{n-k+1}.$$

Allora vale:

$$m_{p^k}(G)v_k = m_{p^n}(G) \equiv v_k \bmod p^{n-k+1} \Rightarrow (m_{p^k}(G) - 1)v_k \equiv 0 \bmod p^{n-k+1}$$

ma essendo $v_k \not\equiv 0 \bmod p$ si conclude che:

$$m_{p^k}(G) \equiv 1 \bmod p^{n-k+1}. \square$$

Osservazione 4.14. In particolare quindi, sotto le ipotesi del teorema, per ogni $k < n$ vale $m_{p^k}(G) \equiv 1 \bmod p^2$.

Teorema 4.15. *Sia $p \neq 2$ un primo, G un gruppo con p-Sylow non ciclici di ordine p^n; per $0 < k < n$ vale:*

$$m_{p^k}(G) \equiv 1 + p \ mod \ p^2.$$

Dimostrazione. Se $k = 1$, vale $m_p(G) \equiv 1 + p \bmod p^2$, grazie al lemma 4.8; dunque basta provare che $m_{p^k}(G) \equiv m_{p^{k-1}}(G) \bmod p^2$ per $1 < k < n$.
Indichiamo con $m_{p^k}(G; C)$ il numero di sottogruppi di G di ordine p^k ciclici e con $m_{p^k}(G; NC)$ il numero sottogruppi di G di ordine p^k non ciclici; quindi vale $m_{p^k}(G) = m_{p^k}(G; C) + m_{p^k}(G; NC)$. Osserviamo che ognuno di quelli ciclici contiene esattamente un sottogruppo di ordine p^{k-1}, mentre ognuno di quelli non ciclici ne contiene un certo numero congruo $1 + p \bmod p^2$.

Indichiamo con μ_k il numero di coppie (X, Y) di sottogruppi X e Y tali che $|X| = p^{k-1}$, $|Y| = p^k$ e $X \subset Y$; allora per quanto osservato vale:

$$\mu_k \equiv m_{p^k}(G; C) + m_{p^k}(G; NC)(1 + p) \bmod p^2;$$

essendo $m_{p^k}(G; C) \equiv 0 \bmod p$ per il teorema 4.12, possiamo aggiungere alla congruenza il termine $m_{p^k}(G; C)p$, ottenendo così:

$$\begin{aligned}\mu_k &\equiv m_{p^k}(G; C) + m_{p^k}(G; NC)(1 + p) + m_{p^k}(G; C)p \bmod p^2 \\ &\equiv m_{p^k}(G)(1 + p) \bmod p^2.\end{aligned}$$

Andiamo ora a definire alcuni insiemi:

- $\Omega_k := \{X \leq G \mid |X| = p^k\}$;
- $R := \{X \in \Omega_{k-1} \mid p\text{-Sylow di } \frac{N_G(X)}{X} \text{ non sono ciclici}\}$;
- $S := \{X \in \Omega_{k-1} \mid p\text{-Sylow di } \frac{N_G(X)}{X} \text{ sono ciclici e } p|[G : N_G(X)]\}$;
- $T := \{X \in \Omega_{k-1} \mid p\text{-Sylow di } \frac{N_G(X)}{X} \text{ sono ciclici e } p \nmid [G : N_G(X)]\}$.

Indicando con r, s e t le cardinalità, rispettivamente, di R, S e T, si ha:

$$m_{p^{k-1}} = r + s + t.$$

Vediamo ora quale contributo danno gli insiemi R, S e T al numero μ_k.

- Gli $Y \in \Omega_k$ contenenti un dato $X \in R$ corrispondono ai sottogruppi di ordine p di $\frac{N_G(X)}{X}$, che per ipotesi ha p-Sylow non ciclici; allora grazie al lemma 4.8 vale $m_p(\frac{N_G(X)}{X}) \equiv 1 + p \bmod p^2$; dunque R dà a μ_k un contributo congruo a $r(1 + p) \bmod p^2$.
- Consideriamo $X \in S$; $|X^G| = [G : N_G(X)]$ è un multiplo di p per ipotesi; quindi X ha λp coniugati in G per qualche $\lambda \geq 1$; i sottogruppi di ordine p^k contenenti uno di questi coniugati corrispondono ai sottogruppi di ordine p di $\frac{N_G(X)}{X}$; il numero di tali sottogruppi è congruo a 1 mod p, ricordando che i p-Sylow di $\frac{N_G(X)}{X}$ sono ciclici per ipotesi; quindi ognuno dei coniugati di X è contenuto in $1 + \mu p$ sottogruppi di ordine p^k per qualche $\mu \geq 1$; dunque la classe di coniugio di X dà a μ_k il seguente contributo:

  $$\lambda p(1 + \mu p) \equiv \lambda p \equiv \lambda p(1 + p) \bmod p^2;$$

  allora S dà a μ_k un contributo congruo a $s(1 + p) \bmod p^2$.

- Sia ora λ il numero di coppie (X, P) con $X \in T$, $P \in Syl_p(G)$ e $X \subseteq P$; il numero di p-sottogruppi di Sylow che contengono un dato $X \in T$ è congruo a 1 mod p (basta far agire per coniugio uno di questi p-Sylow sull'insieme dei rimanenti); vale quindi $\lambda \equiv t \bmod p$.
  Fissiamo un p-Sylow P di G e contiamo gli $X \in T$ contenuti in P: dobbiamo contare i sottogruppi X di P normali e tali che $\frac{P}{X} \cong C_{p^t}$ con $t = n - (k-1) \geq 2$; ricordiamo il seguente fatto generale: se A e B sono due gruppi finiti, il numero di omomorfismi $A \to B$ di immagine $I \leq B$ è pari al numero di sottogruppi normali $C \trianglelefteq A$ tali che $\frac{A}{C} \cong I$ moltiplicato per il numero di automorfismi di I. Nel nostro caso quindi possiamo calcolare il numero di sottogruppi normali $X \trianglelefteq P$ tali che $\frac{P}{X} \cong C_{p^t}$, dividendo il numero di epimorfismi $P \to C_{p^t}$ per il numero di automorfismi di C_{p^t}, ottenendo:

  $$\frac{p^{tn} - p^{(t-1)n}}{p^t - p^{t-1}} \equiv 0 \bmod p$$

  dato che $n, t \geq 2$. Allora $t \equiv 0 \bmod p$.
  Il numero degli $Y \in \Omega_k$ contenenti un dato $X \in T$ è il numero di sottogruppi di ordine p in $\frac{N_G(X)}{X}$ che ha i p-Sylow ciclici e di ordine almeno p^2; per il lemma 4.13 tale numero è congruo a 1 mod p^2; quindi il contributo di T a μ_k è congruo a t mod p^2; avendo provato che $t \equiv 0$ mod p, possiamo aggiungere il termine pt, ottenendo che il contributo di T a μ_k è congruo a $t(1+p)$ mod p^2.

Abbiamo quindi trovato che

$$\mu_k \equiv (r + s + t)(1 + p) \bmod p^2$$

e quindi, ricordando che $r + s + t = m_{p^{k-1}}$, vale:

$$\mu_k \equiv m_{p^{k-1}}(1 + p) \bmod p^2.$$

Confrontando questo risultato con la congruenza trovata in precedenza, ovvero $\mu_k \equiv m_{p^k}(G)(1 + p) \bmod p^2$, possiamo concludere che

$$m_{p^k}(G) \equiv m_{p^{k-1}}(G) \bmod p^2. \square$$

4.2 Esistenza degli pseudo numeri di Frobenius

In virtù dei risultati di Hall appena visti, possiamo ora dare la seguente definizione.

Definizione 4.16. Un intero positivo n è detto pseudo p-numero di Frobenius se valgono le seguenti proprietà:

1. $n \equiv 1 \bmod p^2$ oppure $n \equiv 1 + p \bmod p^2$;
2. non esiste un gruppo finito G con esattamente n sottogruppi di ordine p^k per qualche $k \geq 0$.

Osservazione 4.17. Segue dalle definizioni che ogni pseudo p-numero di Frobenius è anche pseudo numero di p-Sylow.

Vogliamo stabilire l'esistenza di uno pseudo p-numero di Frobenius. Vediamo innanzitutto quali casi possiamo subito escludere.

1. Per l'osservazione precedente, ricordando che ogni numero dispari n è il numero di 2-Sylow del gruppo diedrale di ordine $2n$, possiamo concludere che non esistono pseudo 2-numeri di Frobenius, ovvero per ogni intero n esiste un gruppo finito con n sottogruppi di ordine 2^k per qualche $k \geq 0$.
2. Consideriamo ora interi del tipo $n = 1 + p$ oppure $n = 1 + p^2$; non possono essere pseudo p-numeri di Frobenius, infatti in generale il gruppo $G = GL(2,^k)$ ha $1 + p^k$ p-Sylow $\forall k \geq 1$ (un p-Sylow di G è dato dalle matrici unitriangolari superiori).
3. $n = 1 + p + p^2$ è il numero di sottogruppi di ordine p di un gruppo abeliano di ordine p^3, quindi non è pseudo p-numero di Frobenius.
4. Consideriamo ora $p = 3$.
   - $1 + 3^2 = 10$ rientra nel caso 2.
   - $1 + 3 + 3^2 = 13$ rientra nel caso 3.
   - $1 + 2 \cdot 3^2 = 19$ soddisfa il teorema di M. Hall quindi, ricordando l'osservazione 1.15, è un numero di 3-Sylow e in particolare allora non è pseudo 3-numero di Frobenius;
   - $1+3+2\cdot 3^2 = 22$ è il numero di sottogruppi di ordine 9 del gruppo abeliano $C_9 \times C_3 \times C_3$, quindi non è pseudo 3-numero di Frobenius.
   - $1 + 3 \cdot 3^2 = 28 = 2^2 \cdot 7$ soddisfa il teorema di M. Hall quindi non è pseudo 3-numero di Frobenius.
   - $1 + 3 + 3 \cdot 3^2 = 31$ soddisfa il teorema di M. Hall quindi non è pseudo 3-numero di Frobenius.

- $1 + 4 \cdot 3^2 = 37$ soddisfa il teorema di M. Hall quindi non è pseudo 3-numero di Frobenius.
- $1 + 3 + 4 \cdot 3^2 = 40 = 10 \cdot 4$ è il numero di 3-Sylow di $A_5 \times A_4$, quindi in particolare non è pseudo 3-numero di Frobenius.

Quindi $1 + 5 \cdot 3^2 = 46$ è il più piccolo candidato pseudo numero di Frobenius. Dimostreremo come corollario del prossimo teorema che è effettivamente pseudo 3-numero di Frobenius.
Prima di enunciare il teorema, vediamo due risultati che ci serviranno nella dimostrazione: il primo è una conseguenza del teorema di Kulakoff Hall, il secondo una proposizione di Blau.

Proposizione 4.18. *Sia G un gruppo e P un suo p-Sylow per qualche $p > 2$; allora per $1 < p^k < |P|$ vale:*

$$m_{p^k}(G) \equiv 1 \ mod\ p^2 \Leftrightarrow P \ è\ ciclico.$$

Proposizione 4.19. *Sia G un gruppo semplice; se G ha un p-Sylow ciclico, allora l'intersezione di due p-Sylow distinti è sempre banale.*

Teorema 4.20. *Ogni p-numero di Frobenius $n \equiv 1\ mod\ p^2$ è un numero di p-Sylow.*

Dimostrazione. Se $p = 2$ la tesi è sicuramente verificata, dato che ogni intero $n \equiv 1 \bmod 4$ è in particolare dispari e quindi è un numero di 2-Sylow, come già osservato in precedenza.
Supponiamo ora che p sia dispari. Sia $n \equiv 1 \bmod p^2$ un controesempio minimale, ovvero supponiamo che:

- esista un gruppo G di ordine minimo con la proprietà di avere n sottogruppi di ordine p^k per qualche $k \geq 0$;
- non esista un gruppo con n p-Sylow.

Sicuramente $n > 1$, $k \geq 1$. Chiamiamo $Q = Q_1, ..., Q_n$ gli n sottogruppi di ordine p^k. Stiamo supponendo che n sia pseudo numero di p-Sylow, dunque in particolare n non è il numero di p-Sylow di G e p^{k+1} divide $|G|$. Sia P un p-Sylow di G; ricordando che $p \neq 2$ e che per ipotesi $n \equiv 1 \bmod p^2$, dalla proposizione 4.18 segue che P è ciclico. In particolare ogni p-Sylow contiene esattamente uno dei Q_i, dunque $Q, ..., Q_n$ formano una classe di coniugio in G. Il numero di p-Sylow di G è sicuramente maggiore di n per quanto detto finora, dunque $\exists i$ tale che Q_i sia contenuto in due distinti p-Sylow; segue quindi dalla proposizione 4.19 che il gruppo G non è semplice. Consideriamo

dunque un sottogruppo normale N non banale di G e sia n_i il numero di sottogruppi di Q_iN di ordine p^k; osserviamo che in realtà questo numero non dipende dall'indice i, essendo tutti i Q_iN coniugati; sia quindi, per esempio, n_1 il numero di sottogruppi di QN di ordine p^k. Consideriamo ora $\frac{PN}{N}$: è un p-Sylow di $\frac{G}{N}$, come dimostrato nel lemma 1.12, ed è ciclico in quanto quoziente di ciclico; quindi ogni sottogruppo di $\frac{G}{N}$ di ordine $|\frac{QN}{N}|$ è del tipo $\frac{Q_iN}{N}$ per qualche i. Se chiamiamo n_2 il numero di questi sottogruppi, abbiamo che n è dato da $n = n_1n_2$.
n_1 e n_2 sono, per costruzione, p-numeri di Frobenius. Verifichiamo ora che $n_1 \equiv n_2 \equiv 1 \bmod p^2$. Se così non fosse, ovvero se supponiamo che $n_i \not\equiv 1$ per $i = 1$ o $i = 2$, allora vale in realtà per entrambi ovvero $n_1 \not\equiv n_2 \not\equiv 1 \bmod p^2$, dato che $n_1n_2 = n \equiv 1 \bmod p^2$. Dalla proposizione 4.18 seguono i 2 seguenti fatti:

1. Q è p-Sylow di QN.
   Infatti, ricordando che P è un p-Sylow ciclico di G, P è un p-Sylow ciclico di PN; inoltre, i p-Sylow di QN sono sottogruppi di qualche coniugato di P, quindi ciclici. Ora, se supponiamo che Q non sia un p-Sylow di QN, detto R un p-Sylow di QN, si ha $1 < p^k < |R|$; allora, ricordando che $p \neq 2$, che n_1 è il numero di sottogruppi di ordine p^k di QN e che stiamo supponendo $n_1 \not\equiv 1 \bmod p^2$, dalla proposizione 4.18 segue che R non è ciclico, contraddicendo il fatto che i p-Sylow di QN siano ciclici. Allora Q è p-Sylow di QN.

2. $\frac{QN}{N}$ è p-Sylow di $\frac{G}{N}$.
   Infatti, sicuramente $\frac{QN}{N} \neq 1$, altrimenti N conterrebbe Q ma anche $Q_2, ..., Q_n$, essendo tutti coniugati a Q, contraddicendo la minimalità di G; inoltre, abbiamo già osservato che $\frac{PN}{N}$ è un p-Sylow ciclico di $\frac{G}{N}$, dunque se supponiamo che $\frac{QN}{N}$ non sia p-Sylow di $\frac{G}{N}$, vale $1 < |\frac{QN}{N}| < |\frac{PN}{N}|$; allora, ricordando che n_2 è il numero di sottogruppi di ordine $|\frac{QN}{N}|$ di $\frac{G}{N}$ e che stiamo supponendo $n_2 \not\equiv 1 \bmod p^2$, dalla proposizione 4.18 segue che $\frac{PN}{N}$ non è ciclico, contraddizione. Allora $\frac{QN}{N}$ è p-Sylow di $\frac{G}{N}$.

Da 1. e 2. segue che $[QN : Q] \not\equiv 0 \bmod p$ e $[\frac{G}{N} : \frac{QN}{N}] \not\equiv 0 \bmod p$, e quindi $[G : Q] = [G : QN][QN : Q] = [\frac{G}{N} : \frac{QN}{N}][QN : Q] \not\equiv 0 \bmod p$, contraddicendo il fatto che p^{k+1} divida $|G|$. Allora $n_1 \equiv n_2 \equiv 1 \bmod p^2$.
Avendo scelto G minimale, sicuramente $n_2 < n$; anche $n_1 < n$ poiché, se fosse $n_1 = n$, si avrebbe $G = QN$ e $P = QN \cap P = Q(N \cap P)$, dove l'ultima uguaglianza segue dal lemma di Dedekind; ma essendo P ciclico, vale $Q \subseteq N \cap P \subseteq N$ e dunque $G = QN = N$, contraddicendo l'ipotesi che

N sia sottogruppo proprio.
Abbiamo quindi che $n_1 < n$ e $n_2 < n$ sono p-numeri di Frobenius e per la minimalità di n devono essere numeri di p-Sylow, ovvero esistono due gruppi finiti H_1, H_2 tali che n_1 sia il numero di p-Sylow di H_1 e n_2 sia il numero di p-Sylow di H_2. Allora $n = n_1 n_2$ è il numero di p-Sylow di $H_1 \times H_2$, contraddicendo l'assunzione iniziale che n fosse uno pseudo numero di p-Sylow. □

Osservazione 4.21. Il teorema ci dice che se un intero $n \equiv 1 \bmod p^2$ è uno pseudo numero di p-Sylow, allora n è anche uno pseudo p-numero di Frobenius.

Partiremo da questa osservazione per dimostrare che 46 è pseudo 3-numero di Frobenius. Prima però richiamiamo ulteriori nozioni sulle azioni di gruppo. Supponiamo che un gruppo G agisca su un insieme non vuoto Ω.

Definizione 4.22. $\Delta \subseteq \Omega$ è detto blocco se $\Delta^g \cap \Delta \in \{\Delta, \emptyset\}$ $\forall g \in G$.

Definizione 4.23. Un'azione transitiva è detta primitiva se non ci sono blocchi Δ con $1 < |\Delta| < |\Omega|$.

Lemma 4.24. *L'azione di G su Ω è primitiva se e solo se G_ω è un sottogruppo massimale di G per ogni $\omega \in \Omega$.*

Definizione 4.25. Un'azione transitiva è detta doppiamente transitiva se G_ω agisce transitivamente su $\Omega \setminus \{\omega\}$ $\forall \omega \in \Omega$.

In seguito considereremo l'azione transitiva di coniugio di G su $Syl_p(G)$ e ricordiamo che se P è un p-Sylow di G, il suo stabilizzatore è il normalizzante $N_G(P)$.
Vediamo due ulteriori risultati, il primo di Wielandt e il secondo di Brauer.

Proposizione 4.26. *Sia G un gruppo di permutazione primitivo di grado $2q$, dove con grado intendiamo la cardinalità dell'insieme su cui agisce G. Allora G è doppiamente transitivo oppure $2q - 1$ è un quadrato.*

Ricordiamo che, data una rappresentazione ρ di un gruppo G, il carattere della rappresentazione è definito come la mappa che associa ad un elemento $g \in G$ la traccia della matrice che rappresenta l'automorfismo $\rho(g)$. Inoltre, il carattere di una rappresentazione valutato in 1 dà il grado, ovvero la dimensione, della rappresentazione stessa. Nel seguente enunciato denotiamo con $Irr(G)$ l'insieme di tutti i caratteri complessi irriducibili di G e con 1_G il carattere della rappresentazione banale.

Proposizione 4.27. *Sia G un gruppo con un p-Sylow P di ordine p tale che $C_G(P) = P$, e sia $e := |\frac{N_G(P)}{P}|$. Allora esiste un insieme di caratteri irriducibili $B = \{1_G = \chi_1, ..., \chi_e, \psi_1, ..., \psi_{\frac{p-1}{e}}\} \subseteq Irr(G)$ tale che:*

- $\chi_i(1) \equiv \epsilon_i \ mod\ p$ *per* $1 \leq i \leq e$;
- $\psi_j(1) = |\sum_{i=1}^{e} \epsilon_i \chi_i(1)|$ *per* $1 \leq j \leq \frac{p-1}{e}$;
- $\mu(1) \equiv 0 \ mod\ p \ \forall \mu \in Irr(G) \setminus B$

con $\epsilon_1, ..., \epsilon_e \in \{\pm 1\}$.

Osservazione 4.28. Nel caso particolare in cui $e = |\frac{N_G(P)}{P}| = 1$, si ha $B = \{1_G = \chi_1, \psi_1, ..., \psi_{p-1}\}$ con $1_G(1) = \chi_1(1) = 1$ e $\psi_j(1) = 1$ per $1 \leq j \leq p-1$; dalla teoria dei caratteri si ha $|\frac{G}{[G,G]}| = p$.

Osservazione 4.29. Ad ogni azione di G su un insieme Ω possiamo associare un "carattere permutazione" π che conta i numeri di punti fissi, ovvero $\pi(g) = |\{\omega \in \Omega : \omega^g = \omega\}| \ \forall g \in G$. Inoltre, l'azione di G su Ω è doppiamente transitiva se e solo se $\pi = 1_G + \chi$ per qualche $\chi \in Irr(G) \setminus \{1_G\}$.

Corollario 4.30. *46 è uno pseudo 3-numero di Frobenius.*

Dimostrazione. $46 \equiv 1 \bmod 3^2$, quindi grazie al teorema 4.20 basta dimostrare che 46 è uno pseudo numero di 3-Sylow, ovvero che non esistono gruppi con 46 3-Sylow. Osserviamo che 46 non soddisfa le ipotesi dei teoremi visti nel capitolo precedente, quindi non possiamo utilizzare quei risultati per concludere subito che è pseudo numero di 3-Sylow.
Sia G gruppo di ordine minimo con la proprietà di avere 46 3-Sylow. Vediamo quali proprietà ha l'azione di G sull'insieme $Syl_3(G)$.

- L'azione è transitiva.
  Segue dal fatto che tutti i 3-Sylow sono coniugati.

- L'azione è fedele.
  Sia K il nucleo dell'azione; analogamente a quanto visto nel primo passo della dimostrazione del teorema 3.11, si trova che $\frac{G}{K}$ ha lo stesso numero di 3-Sylow di G, ma avendo scelto G minimale segue che $K = 1$. In particolare possiamo vedere G come sottogruppo di S_{46} o più precisamente di A_{46} dato che ogni 3-Sylow sta in A_{46}.

- L'azione è primitiva.
  Per il lemma 4.24 basta mostrare che, se P è un 3-Sylow di G, $N_G(P)$ è un sottogruppo massimale di G. Sia quindi $N_G(P) < M \leq G$; osserviamo che $N_M(P) = N_G(P) \cap M = N_G(P)$; inoltre P è sicuramente un

3-Sylow di M quindi:

$|Syl_3(M)| = [M : N_M(P)] = [M : N_G(P)] \in \{2, 23, 46\}$

dove l'ultima relazione segue dal fatto che $[M : N_G(P)]$ deve dividere 46, in quanto $46 = [G : N_G(P)] = [G : M][M : N_G(P)]$, e non è 1 dato che M contiene propriamente $N_G(P)$; ma $2 \not\equiv 1 \bmod 3$ e $23 \not\equiv 1 \bmod 3$, quindi $|Syl_3(M)| = 46$ e per minimalità di G si ha $M = G$, dunque $N_G(P)$ è massimale.

- L'azione è doppiamente transitiva.
  Segue dalla proposizione 4.26, dato che $2 \cdot 23 - 1 = 45$ non è un quadrato.

Consideriamo $Q \in Syl_3(G) \setminus \{P\}$; allora $Q^{N_G(P)} = Syl_3(G) \setminus \{P\}$, $N_G(P)_Q = \{x \in N_G(P) : xQ = Qx\} = N_G(P) \cap N_G(Q)$ e ricordando che la cardinalità di un'orbita è uguale all'indice del normalizzante si ha:

$[N_G(P) : N_G(P)_Q] = [N_G(P) : N_G(P) \cap N_G(Q)] = |Q^{N_G(P)}| = |Syl_3(G) \setminus \{P\}| = 45$.

Avendo dimostrato che $N_G(P)$ è un sottogruppo massimale di G, i 3-Sylow di G sono 3-Sylow di $N_G(P)$; in particolare quindi $N_P(Q) = P \cap N_G(Q)$ è un 3-Sylow di $N_G(P) \cap N_G(Q)$ quindi vale $|Q^P| = [P : N_P(Q)] = 9$.
Consideriamo $g \in N_G(P)$; vale $(Q^P)^g = Q^{gP} = Q^{Pg} = (Q^g)^P$.
Essendo le orbite di P disgiunte, Q^P è un blocco di $N_G(Q)$; abbiamo visto che $N_G(P)$ è transitivo su $Syl_3(G) \setminus \{P\}$, dunque i coniugati distinti di Q^P formano una partizione di $Syl_3(G) \setminus \{P\}$ in 5 blocchi di 9 elementi ciascuno, e l'azione di $N_G(P)$ permuta i blocchi.
Due osservazioni sull'ordine di $N_G(P)$:

- $|N_G(P)|$ non è divisibile per 11; se $x \in N_G(P)$ avesse ordine 11, allora fisserebbe ognuno dei 5 blocchi, ma x non può permutare 9 elementi con un'azione non banale; in particolare anche $|G| = 46 \cdot |N_G(P)|$ non è divisibile per 11;

- con considerazioni analoghe $|N_G(P)|$ non è divisibile per 23.

Consideriamo ora un 23-Sylow di G, che chiamiamo S; $|S| = 23$ e S è generato dal prodotto di due 23-cicli disgiunti, essendo $|N_G(P)|$ non divisibile per 23; allora per il lemma 3.4 si ha $|C_{A_{46}}(S)| = 23^2$; quindi $|C_G(S)| \leq |C_{A_{46}}(S)| = 23^2$, ma essendo $|G|$ non divisibile per 23^2, deve essere $|C_G(S)| = 23$ e dunque $C_G(S) = S$. Ora, grazie al lemma 3.6, $|\frac{N_G(S)}{S}|$ divide 22; sicuramente $|\frac{N_G(S)}{S}|$

non è divisibile per 11 essendo $\frac{N_G(S)}{S} \leq G$, dunque $|\frac{N_G(S)}{S}| \in \{1, 2\}$. Se fosse $|\frac{N_G(S)}{S}| = 1$, allora per l'osservazione 4.28 si ha $|\frac{G}{[G,G]}| = 23$, che non è divisibile per 3, quindi ogni 3-Sylow di G è 3-Sylow di $[G, G]$, contraddicendo la minimalità di G.
Allora $|\frac{N_G(S)}{S}| = 2$.
Il carattere permutazione π di G è della forma $\pi = 1_G + \chi$, con χ carattere irriducibile di G di grado 45. Per la proposizione 4.27, $\chi_2(1) \equiv \epsilon_2 \bmod 23$ quindi è del tipo $\chi_2(1) = \epsilon_2 + 23k$ per qualche intero k; inoltre $\psi_j(1) = |\epsilon_1\chi_1(1) + \epsilon_2\chi_2(1)| = |1 + \epsilon_2(\epsilon_2 + 23k)| = |1 + {\epsilon_2}^2 + 23k\epsilon_2| = |2 + 23k\epsilon_2| \equiv \pm 2 \bmod 23$.
Allora $\chi = \chi_2$, $\epsilon_2 = -1$ e $\psi_1(1) = |1 - 45| = 44$; ricordando che il grado di ogni rappresentazione irriducibile divide l'ordine del gruppo, si ha che 44 divide $|G|$, contraddicendo il fatto che 11 non divide $|G|$. $\square$

Conclusione

Ripercorriamo i punti salienti di questo lavoro.
Abbiamo visto una prima generalizzazione dei teoremi di Sylow, data da Philip Hall, per gruppi risolubili di ordine mn, con m e n coprimi. Questo teorema non vale per gruppi semplici, come si può evincere ad esempio considerando il gruppo alterno A_5 di ordine 60 che non ha sottogruppi di ordine 15.
Grazie ai teoremi di Marshall Hall si riesce a caratterizzare il numero di p-Sylow di un gruppo G finito, senza ulteriori ipotesi; tale numero è il prodotto di fattori che sono o il numero di p-Sylow di qualche gruppo semplice, oppure potenze di primo congrue a 1 modulo p.
Ci siamo quindi concentrati sui gruppi semplici: gruppi finiti, non abeliani e semplici sono gruppi SSN se e solo se sono isomorfi ad un gruppo del tipo $PSL(2, q)$ per qualche q primo di Mersenne. In particolare in questa tesi abbiamo dimostrato che A_n, per $n \geq 5$, e $PSL(2, q)$, con $q \neq 2$ non primo di Mersenne, non sono gruppi SSN, mostrando che esistono dei divisori primi p dell'ordine per cui il numero di p-Sylow non è risolubile.
Riportando l'attenzione al numero di p-Sylow, ci siamo poi chiesti se tutti gli interi positivi congrui a 1 modulo un certo primo p siano il numero di p-Sylow di qualche gruppo; quelli che soddisfano il teorema di M. Hall sicuramente lo sono, ma abbiamo visto altri risultati di Hall che invece ne escludono diverse tipologie: ad esempio per ogni primo $p \geq 7$ non esistono gruppi con $1 + 3p$ p-Sylow; inoltre abbiamo dimostrato, con metodi elementari, che non esistono gruppi finiti con 35 17-Sylow, né con 15 7-Sylow.
Infine abbiamo considerato più in generale i p-sottogruppi; innanzitutto, il teorema di Frobenius estende ai p-sottogruppi il corollario 0.7, ovvero dimostra che per ogni $k \geq 0$ e primo p tali che p^k divida l'ordine del gruppo, il numero di sottogruppi di ordine p^k è congruo a 1 modulo p. Un'ulteriore importante congruenza ci è data dal teorema di Hall per gruppi con p-Sylow non ciclici, per p primo dispari, ovvero il numero di sottogruppi di ordine p^k è congruo a $1 + p$ modulo p^2. Utilizzando tale teorema si dimostra poi che ogni p-numero di Frobenius congruo a 1 modulo p^2 è un numero di p-Sylow;

detto in altre parole se un intero congruo a 1 modulo p^2 è uno pseudo numero di p-Sylow, allora esso è anche uno pseudo p-numero di Frobenius. Grazie a questa osservazione abbiamo concluso il lavoro portando un esempio di pseudo numero di Frobenius, ovvero abbiamo dimostrato che non esistono gruppi con 46 sottogruppi di ordine potenza di 3.

Bibliografia

[1] F. Gross, Odd order Hall subgroups of the classical linear groups, Math. Z. 220 (1995), 317-336.

[2] L. C. Grove, Classical groups and geometric algebra, Graduate Studies in Mathematics, 39, American Mathematical Society, Providence, RI, (2002).

[3] M. Hall, On the number of Sylow subgroups in a finite group, J. Algebra 7 (1967), 363-371.

[4] P. Hall, A note on soluble groups, J. London Math. Soc. 3 (1928), 98-105.

[5] P. Hall, On a theorem of Frobenius, Proc. London Math. Soc. (2) 40 (1935), 468-501.

[6] H. Harborth and A. Kemnitz, Calculations for Bertrand's postulate, Math. Mag. 54 (1981), 33-34.

[7] M. Herzog, Counting Group Elements of Order p Modulo p^2, Proc. Amer. Math. Soc. Vol. 66, 2 (1977), 247-250.

[8] I.M. Isaacs. Finite Group Theory, Graduate studies in mathematics, American Mathematical Society, (2008).

[9] O. H. King, The subgroup structure of finite classical groups in terms of geometric configurations, scaricabile qui: https://www.staff.ncl.ac.uk/o.h.king/KingBCC05.pdf

[10] T.-Z. Li and Y.-J. Liu, Mersenne primes and solvable Sylow numbers, Journal of Algebra and its Applications, Vol. 15, 9 (2016), 1-16.

[11] G. A. Miller, An extension of Sylow's theorem, Proc. London Math. Soc. 2 (1905), 142-143.

[12] B. Sambale, Pseudo Frobenius numbers, ArXiv (2018)

[13] B. Sambale, Pseudo Sylow Numbers, Amer. Math. Monthly, 126:1, (2019), 60-65.

[14] M. Stather, Constructive Sylow theorems for the classical groups, J. Algebra 316 (2007), 536-559.

Ringraziamenti

Al termine di questo percorso universitario vorrei ringraziare innanzitutto il mio relatore, il Professor Lucchini, che con la sua efficienza e celerità nelle risposte ha contribuito in maniera significativa alla realizzazione di questo lavoro.
Ringrazio mia cugina Giulia, per aver agevolato il mio ingresso nel mondo universitario facendomi da guida, prestandomi i libri e dandomi quei consigli preziosi di chi ci è già passato.
Un pensiero va poi alle persone che mi sono state vicine in questi anni. A partire dagli amici "storici", come le GEGE, gli atleti, ECE; seppure spesso fisicamente distanti, sapevano annullare i chilometri in un istante con un messaggio o una chiamata, qualche parola di conforto o una risata; per arrivare poi ai familiari acquisiti: coinquilini vecchi e nuovi, con le visite improvvisate di Alessandro in camera che sono state sempre un toccasana per il mio umore, la chitarra, le chiacchierate spensierate, e gli immancabili "Divertiti"/"In bocca al lupo" pre-esame.
Una piacevole costante in questi anni è stata l'amicizia con Betta, Benni, Lavi e Vero, nata tra lezioni, depressione pre-esami, fughe da personaggi molesti, ma anche aperitivi dai chimici, pranzi, amori platonici e karaoke (ma quale karaoke??).
Ringrazio Elia, per aver creduto più di me nelle mie capacità, per aver sopportato le mie fissazioni, manie di organizzazione e rigidità nella routine, ma soprattutto per avermi fatto sentire sempre me stessa.
Fondamentale è stato anche il supporto della mia famiglia, i loro incoraggiamenti nelle difficoltà e la condivisione della gioia nei piccoli successi.
Infine ringrazio Giacomo, per le pause caffè rigorosamente di 15 minuti, i consigli su matematica, atletica, musica e tanti altri ambiti, per avermi trasmesso sempre molta serenità ed essere riuscito anche nei momenti più cupi a strapparmi un sorriso.