Università degli Studi di Padova

Facoltà di Scienze MM.FF.NN.

Dipartimento di Matematica Pura ed Applicata

Tesi di Laurea in Matematica

Sui p-sottogruppi dei gruppi simmetrici

RELATORE: Ch.mo Prof. F. Menegazzo

LAUREANDO: Pablo Spiga

Anno Accademico 1999-2000

2

.

Alla mia Francesca

4

.

Indice dei simboli

C_p il gruppo ciclico con p elementi

S_n il gruppo simmetrico su n oggetti

P_{p^n} il p-Sylow del gruppo simmetrico su p^n oggetti

a^b il coniugato di a tramite b

$|X|$ l'ordine dell'insieme X

$\prod_{i\in I} G_i$ il prodotto cartesiano della famiglia di gruppi $\{G_i\}_{i\in I}$

$\coprod_{i\in I} X_i$ l'unione disgiunta della famiglia di insiemi $\{X_i\}_{i\in I}$

$N_A(B) = \{a \in G |\ a \in A,\ B^a = B\}$ se A e B sono sottogruppi di G

$AWr_X B$ il prodotto intrecciato di A con B su X

$A \wr B$ il prodotto intrecciato standard di A con B

$Z(G)$ il centro del gruppo G

$Z_i(G)$ l'i-esimo termine della serie centrale ascendente di G

$\gamma_i(G)$ l'i-esimo termine della serie centrale discendente di G

$G^{(i)}$ l'i-esimo termine della serie derivata di G

$InnG$ il gruppo degli automorfismi interni di G

$Inn_A B$ siano A e B sottogruppi di G e supponiamo che $A \leq N_G(B)$ allora $Inn_A B = \{\varphi_{a|B} |\ \varphi_a \in InnG,\ a \in A\}$

$FrattG$ l'intersezione dei sottogruppi massimali di G

$\mathbb{F}_p$ il campo con p elementi

$N_{AutG}(A)$ sia $A \leq G$ allora $N_{AutG}(A) = \{\alpha \in AutG |\ A^\alpha = A\}$

$core - free$ sia A un sottogruppo di G allora A si dice core-free in G se l'unico sottogruppo normale di G contenuto in A è l'identità

$Der(A, B) = \{\delta : A \to B |\ (a_1 a_2)^\delta = (a_1^\delta)^{a_2} a_2^\delta,\ \forall a_1, a_2 \in A\}$

$\mathbb{C}_A(B)$ siano $A, B \leq G$ allora $\mathbb{C}_A(B) = \{a \in A |\ b^a = b\ \forall b \in B\}$

Indice

Capitolo 1

Introduzione

La teoria asintotica dei gruppi è quel ramo della matematica che si occupa della numerazione dei gruppi che godono di una fissata proprietà. In sostanza, fissata una classe $\mathfrak{X}$ di gruppi, la teoria vuole stimare il numero degli elementi di $\mathfrak{X}$ a meno di isomorfismo. Nella classe $\mathfrak{X}$ si introduce la relazione di equivalenza di isomorfismo: $G_1, G_2 \in \mathfrak{X}$ sono equivalenti se e solo se sono isomorfi. Le stime in esame hanno per oggetto tali classi di equivalenza. Ad esempio, nel diaciannovesimo secolo sono state date molte limitazioni asintotiche su gruppi di permutazione in base al numero di generatori, all'ordine e ad altri invarianti per isomorfismo. In tali problemi lo strumento più efficace si è rivelato la classificazione dei gruppi finiti semplici. Esistono però questioni asintotiche sulla classe dei p-gruppi finiti in cui per ovvie ragioni tale classificazione non è molto utile. Una di queste questioni prevede la generalizzazione del teorema di Gauss sulla distribuzione dei numeri primi. La congettura formulata in un articolo da L.Pyber è: i gruppi finiti sono *quasi tutti* nilpotenti? In termini precisi, la congettura dice che se $g(n)$ è il numero di tutti i gruppi, a meno di isomorfismo, di ordine al più n, e $g_{nil}(n)$ è il numero dei gruppi nilpotenti dello stesso ordine, allora:

$$\lim_{n\to+\infty} \frac{g_{nil}(n)}{g(n)} = 1$$

È già stato provato, sempre da Pyber, che:

$$\lim_{n\to+\infty} \frac{\ln(g_{nil}(n))}{\ln(g(n))} = 1$$

Inoltre, dato che ogni gruppo nilpotente finito è prodotto diretto di p-gruppi, la nostra attenzione può essere limitata al numero dei p-gruppi. Un passo in avanti per la dimostrazione della congettura citata è stato fatto da Higman e

Sims. Denotando con $f(n)$ il numero dei gruppi di ordine n, abbiamo il loro seguente risultato:

$$f(p^k) = p^{\frac{2}{27}k^3+o(k^3)}$$

dove $o(k^3)$ dipende solo da k e non da p. La questione non è ancora conclusa e queste pagine vogliono essere una prima indagine sui p-sottogruppi dei gruppi simmetrici.
In questa tesi si è posto il problema di calcolare, a meno di isomorfismo, il numero di p-sottogruppi di un gruppo simmetrico finito. Se n è un naturale, S_n è il gruppo simmetrico su n oggetti e $Sub_p(n)$ è il numero di p-sottogruppi di S_n a meno di isomorfismo, l'obiettivo è di trovare due funzioni, $m_p(n)$ e $M_p(n)$ tali che

$$m_p(n) \leq Sub_p(n) \leq M_p(n)$$

$$\lim_{n\to\infty} \frac{M_p(n)}{m_p(n)} = 1.$$

Per i teoremi di Sylow ogni p-sottogruppo di S_n è contenuto in un p-Sylow ed inoltre i p-Sylow sono coniugati tra loro; quindi, il primo passo consiste nel studiare un p-Sylow di S_n. Vale il seguente

Teorema *Il p-Sylow di S_{p^n} è isomorfo al prodotto intrecciato standard di n copie del gruppo ciclico con p elementi.*

$$P_{p^n} \cong C_p \wr C_p \wr \cdots \wr C_p$$

Se $n = a_0 + a_1 p + \cdots + a_s p^s$, con $0 \leq a_i < p$, allora il p-Sylow di S_n è isomorfo a

$$\underbrace{P_p \times \cdots \times P_p}_{a_1 \text{ volte}} \times \underbrace{P_{p^2} \times \cdots \times P_{p^2}}_{a_2 \text{ volte}} \times \cdots \times \underbrace{P_{p^s} \times \cdots \times P_{p^s}}_{a_s \text{ volte}}$$

I p-Sylow di S_n sono isomorfi a prodotti diretti di prodotti intrecciati iterati del gruppo ciclico con p elementi.

Dal teorema precedente la nostra attenzione è rivolta a P_{p^n}. Per tale gruppo vale la seguente

Proposizione

1. *L'ordine di P_{p^n} è $p^{p^{n-1}+p^{n-2}+\cdots+1}$.*
2. *P_{p^n} è un gruppo risolubile di lunghezza derivata n.*
3. *P_{p^n} è un gruppo nilpotente di classe p^{n-1}.*
4. *Il centro di P_{p^n} ha ordine p.*

5. *I termini della serie centrale discendente di P_{p^n} coincidono con i termini della serie centrale ascendente.*

6. *Se $p \neq 2$ allora P_{p^n} ha un unico sottogruppo normale abeliano elementare massimale. Tale sottogruppo lo denoteremo con A^{n-1} e ha dimensione p^{n-1}.*

7. *P_{p^n} è un'estensione spezzante di A^{n-1} con un sottogruppo isomorfo a $P_{p^{n-1}}$, perciò, a meno di tale identificazione, $P_{p^n} = P_{p^{n-1}}A^{n-1}$ ed inoltre $P_{p^{n-1}} \cap A^{n-1} = 1$.*

8. *$[P_{p^n} : FrattP_{p^n}] = p^n$ e quindi P_{p^n} contiene $\frac{p^n-1}{p-1}$ massimali distinti.*

9. *Sia $N_{S_{p^n}}(P_{p^n})$ il normalizzante di P_{p^n} in S_{p^n} allora $N_{S_{p^n}}(P_{p^n})/P_{p^n} \cong Inn_{N_{S_{p^n}}}(P_{p^n})/InnP_{p^n} \cong (\mathbb{Z}/(p-1)\mathbb{Z})^n$. $N_{S_{p^n}}(P_{p^n})$ è un'estensione spezzante di P_{p^n}.*

Tramite semplici argomentazioni sull'ideale di aumentazione di P_{p^n} si può verificare questa

Proposizione

1. *$\gamma_i(P_{p^n})/\gamma_{i+1}(P_{p^n})$ è un p-gruppo abeliano elementare.*

2. *$\gamma_{p^i}(P_{p^n})/\gamma_{p^{i+1}}(P_{p^n})$ è un p-gruppo di esponente p.*

Il secondo passo consiste nel studiare il gruppo degli automorfismi di P_{p^n}. Per fare questo ci restringiamo al caso $p \neq 2$. Dato che A^{n-1} è caratteristico in P_{p^n} possiamo definire l'omomorfismo

$$\phi : AutP_{p^n} \longrightarrow AutP_{p^{n-1}}$$

$$\alpha \longmapsto \alpha^{\phi} : \quad \frac{P_{p^{n-1}}A^{n-1}}{A^{n-1}} \longrightarrow \frac{P_{p^{n-1}}A^{n-1}}{A^{n-1}}$$

$$\sigma f A^{n-1} \longmapsto (\sigma f)^{\alpha} A^{n-1}$$

Teorema *$AutP_{p^n} = Ker\phi Inn_{N(P_{p^n})}P_{p^n}$, dove $Inn_{N(P_{p^n})}P_{p^n}$ è il gruppo degli automorfismi interni di P_{p^n} indotti dal normalizzante del p-Sylow nel gruppo simmetrico.*

Un altro risultato essenziale per la determinazione dei massimali di P_{p^n} consiste nella dimostrazione dell'esistenza di una base $\mathfrak{E}$ di $P_{p^n}/\gamma_2(P_{p^n})$ per cui

valga la seguente
Proposizione *Sia $-$ l'omomorfismo sotto definito.*

$$- : AutP_{p^n} \longrightarrow AutP_{p^n}/\gamma_2(P_{p^n})$$

$$\alpha \longmapsto \overline{\alpha} : \qquad P_{p^n}/\gamma_2(P_{p^n}) \longrightarrow P_{p^n}/\gamma_2(P_{p^n})$$

$$\sigma\gamma_2(P_{p^n}) \longmapsto \sigma^{\alpha}\gamma_2(P_{p^n})$$

Allora $Ker\phi = InnP_{p^n} Ker-$ e, nella base $\mathfrak{E}$, $Imm-$ è costituita dalle matrici $n \times n$ a coefficienti in $\mathbb{F}_p$ diagonali.

I risultati fino ad ora riportati permettono di dimostrare il seguente
Teorema *In P_{p^n} ci sono $2^n - 1$ classi di isomorfismo di massimali. Inoltre due massimali sono isomorfi se e solo se coniugati nel normalizzante del p-Sylow del gruppo simmetrico.*

Lo studio del gruppo P_{p^2} non si presenta particolarmente difficile e infatti si riesce a ottenere la seguente
Proposizione *In P_{p^2} ci sono $3p-1$ sottogruppi a meno di isomorfismo. Le classi di isomorfismo di sottogruppi non abeliani coincidono con le classi di coniugio in $N_{S_{p^2}}(P_{p^2})$, tali classi sono univocamente determinate dall'ordine e dall'esponente di un rappresentante. In P_{p^2} ci sono $p^{p-1} - 1/p - 1$ gruppi non abeliani.*

I risultati ottenuti per P_{p^2} si riescono ad estendere parzialmente per induzione a P_{p^n}. In aggiunta, alcuni lemmi tecnici sui sottogruppi abeliani elementari normali massimali di p-sottogruppi di P_{p^n} permettono di dimostrare il teorema sotto riportato.
Teorema *Il p-Sylow di S_{p^n} contiene almeno*

$$f(n,p) = \binom{2(p-2)^{n-2}p^{\binom{n-2}{2}} + p}{p-1} \left(\frac{2(p-2)^{n-2}p^{\binom{n-2}{2}} + p^{n-1} + 1}{p} \right)$$

classi di isomorfismo di p-sottogruppi.

Con la formula di Stirling si stabilisce che

$$f(n,p) \in O\Big(\frac{1}{\sqrt{2\pi}} p^{\frac{(n(n-3))}{2}+1} \Big)$$

Naturalmente questo risultato risponde solo parzialmente all'obiettivo proposto. Non possediamo alcuna stima per eccesso che possa stabilire la bontà

del risultato ottenuto.

Concludiamo questa introduzione provando che $f(p^k) \leq p^{\frac{k^3}{6}+o(k^3)}$.
Se G ha ordine p^k allora ammette una serie principale

$$G = G_0 \geq G_1 \geq \cdots \geq G_k = 1$$

tale che $[G_{i-1} : G_i] = p$, per ogni $i = 1, \cdots, k$.
Sia $g_i \in G_{i-1} \backslash G_i$. Allora, $g_i^p \in G_i$ e $[g_i, g_j] \in G_j$, se $i < j$.
Dunque un elemento di G può essere scritto in modo unico nella forma

$$g_1^{\alpha_1} \cdots g_k^{\alpha_k}$$

per $0 \leq \alpha_i < p$, e il prodotto di due tali elementi è univocamente determinato da g_i^p e $[g_i, g_j]$ per $i < j,\ i = 1, \cdots, p$.
Ovviamente

$$g_i^p = g_{i+1}^{e_{i,i+1}} \cdots g_k^{e_{i,k}},\ [g_i, g_j] = g_{j+1}^{c_{i,j,j+1}} \cdots g_k^{c_{i,j,k}}$$

dove $0 \leq e_{i,j} < p$ e $0 \leq c_{l,m,n} < p$.
La classe di isomorfismo di G è determinata dall'insieme $\{e_{i,j}, c_{l,m,n}\}_{i,j,l,m,n}$.
Il numero di tali costanti è

$$\frac{k(k-1)}{2} + \frac{k(k-1)(k-2)}{6} = \frac{k^3 - k}{6}$$

Questo prova che $f(p^k) \leq p^{\frac{k^3-k}{6}}$.
Il vero lavoro di Higman e Sims consiste nel dare una stima inferiore e nel migliorare la costante precedente, da 1/6 a 2/27.

Capitolo 2

p-Sylow di S_{p^n}

Siano A e B due gruppi,

$$\varphi : A \times B \longrightarrow A$$

$$(a, b) \longmapsto a^b$$

un'azione destra di B su A. Se $(a_1 a_2)^b = a_1^b a_2^b$ per ogni $a_1, a_2 \in A$, $b \in B$, allora diremo che B agisce su A come gruppo. In tale situazione la posizione:

$$(b_1, a_1)(b_2, a_2) = (b_1 b_2, a_1^{b_2} a_2)$$

per ogni $a_1, a_2 \in A, b_1, b_2 \in B$, introduce una struttura di gruppo nel prodotto cartesiano di B con A. Tale gruppo verrà indicato con $A \rtimes_\varphi B$ e si dirà il prodotto semidiretto di A con B tramite φ. Ovviamente $\{(1_B, a) |\ a \in A\}$ è un sottogruppo normale di $A \rtimes_\varphi B$ ed il quoziente è isomorfo a B.
Siano A, B gruppi, X un B-insieme destro e sia $\{A_x\}_{x \in X}$ una famiglia di gruppi tale che $A_x \cong A$, $\forall x \in X$. Posto $f^b(x) = f(x^{b^{-1}})$ per ogni $f \in \prod_{x \in X} A_x, b \in B, x \in X$, la mappa

$$\theta : \prod_{x \in X} A_x \times B \longrightarrow \prod_{x \in X} A_x$$

$$(\quad f \quad , b\,) \longmapsto f^b$$

è un'azione e B agisce sul prodotto diretto $\prod_{x \in X} A_x$ come gruppo. Il prodotto semidiretto di $\prod_{x \in X} A_x$ con B tramite θ si indica con $AWr_X B$ e si chiama il prodotto intrecciato completo di A con B su X con riguardo all'azione θ. Come prima, il sottogruppo $\{(1_B, f) |\ f \in \prod_{x \in X} A_x\}$ è normale, lo indichiamo con $A^{[X]}$ e si chiama base del prodotto intrecciato.
Se A, B e X sono come sopra e sono finiti allora $|AWr_X B| = |A|^{|X|}|B|$.

Se assegno a B struttura di B-insieme destro tramite la rappresentazione regolare di Cayley, allora $AWr_B B$ lo si denota con $A \wr B$ e lo si chiama prodotto intrecciato standard completo di A con B.
Sia Y un A-insieme destro allora $Y \times X$ è un $AWr_X B$-insieme destro tramite:

$$(y,x)bf = (y^{f(x^b)}, x^b) \qquad \forall x \in X, y \in Y, f \in A^{[X]}, b \in B.$$

Se X e Y sono rispettivamente B-insieme e A-insieme transitivi con azione fedele, allora $Y \times X$ è un $AWr_X B$-insieme transitivo con azione fedele; inoltre $X \coprod Y$ è un $A \times B$-insieme con azione fedele, dove l'azione è:

$$s(a,b) = \begin{cases} s^a & \text{se} \quad s \in X \\ s^b & \text{se} \quad s \in Y \end{cases}$$

Sia p un primo e C_p il gruppo ciclico di ordine p, definiamo ricorsivamente:

$$P_{p^0} = 1, \quad P_{p^1} = C_p, \quad P_{p^{n+1}} = P_{p^n} \wr C_p \qquad \forall n \in \mathbb{N}$$

Ovviamente: $|P_{p^{n+1}}| = p^{p^n + p^{n-1} + \cdots + p + 1}$.
Sia $n \in \mathbb{N}$ e $l(n)$ la massima potenza di p che divide $n!$. È immediato vedere che: $l(n) = [\frac{n}{p}] + l([\frac{n}{p}])$, e dunque induttivamente si ottiene:
$l(n) = [\frac{n}{p}] + [\frac{n}{p^2}] + \cdots + [\frac{n}{p^s}] + \cdots$.
Se $n = a_0 + a_1 p + \cdots + a_s p^s$ con $0 \leq a_i < p$, allora dalla formula precedente otteniamo: $l(n) = a_1 + a_2(1+p) + \cdots + a_s(1 + \cdots + p^{s-1})$.
Sia $G = \prod_{i=1}^{a_1} P_{p^1} \times \prod_{i=1}^{a_2} P_{p^2} \times \cdots \times \prod_{i=1}^{a_s} P_{p^s} = \prod_{j=1}^{s} \prod_{i=1}^{a_j} P_{p^j}$ allora
$|G| = p^{a_1} p^{a_2(1+p)} \cdots p^{a_s(1+\cdots+p^{s-1})} = p^{a_1 + a_2(1+p) + \cdots + a_s(1+\cdots+p^{s-1})} = p^{l(n)}$.
G è un p-gruppo che opera fedelmente su un insieme di cardinalità minore o uguale a n. Quindi G si immerge in S_n, dunque G è isomorfo a un p-sottogruppo di S_n. Per questioni di ordine G è un p-Sylow di S_n.
Osserviamo che se $n = p^m$ allora $l(n) = 1 + \cdots + p^{m-1}$ e quindi P_{p^m} è isomorfo ad un p-Sylow di S_{p^m}. Notiamo inoltre che ogni p-gruppo è isomorfo ad un sottogruppo di un prodotto intrecciato standard iterato di C_p.
Sia $n \in \mathbb{N}$ e sia $m \leq n$ allora P_{p^m} è un gruppo di permutazione transitivo su $X = \{1, \cdots, p^m\}$, dunque $P_{p^{n-m+1}} Wr_X P_{p^m}$ è un gruppo di permutazione transitivo di grado p^{n+1} e di ordine $|P_{p^{n-m+1}}|^{p^m} |P_{p^m}| = p^{1+\cdots+p^n}$, quindi ovviamente $P_{p^{n-m+1}} Wr_X P_{p^m} \cong P_{p^{n+1}}$.
In particolare $P_{p^{n+1}} = C_p Wr_X P_{p^n} = P_{p^n}(C_p^{[X]})$, posto $C_p^{[X]} = A^n$ e ricordato che il prodotto di un sottogruppo con un sottogruppo normale è ancora un sottogruppo, si ottiene:

$$P_{p^{n+1}} = P_{p^n} A^n = P_{p^{n-1}} A^{n-1} A^n = \cdots = A^0 A^1 \cdots A^n$$

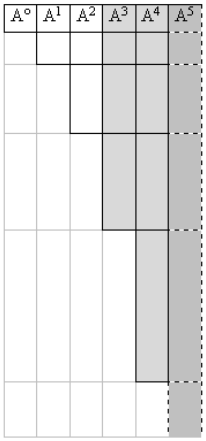


Figura 2.1: Rappresentazione grafica di $P_{p^{n+1}}$

con A^i p-gruppo abeliano elementare di ordine p^{p^i}. Rappresentando i gruppi A^i come rettangoli di base 1 e altezza p^i possiamo vedere $P_{p^{n+1}}$ tramite il disegno sopra riportato.

Diamo la seguente
Osservazione. Se il gruppo G è un'estensione spezzante di A tramite B e se $\phi : G \to B$ è la proiezione naturale allora $\phi_{k-1} = \phi_{|\gamma_k(G)} : \gamma_k(G) \to \gamma_k(B)$ è un omomorfismo suriettivo e $\gamma_k(G) = \gamma_k(B)Ker\phi_{k-1}$. Inoltre, posto ricorsivamente $A_0 = A$ e $A_{k+1} = [A_k, G]$, si ha che $A_k = Ker\phi_k$ per ogni $k \in \mathbb{N}$.

Dimostrazione: Iniziamo con il verificare che $[\gamma_r(G), A_s] \leq A_{r+s}$. Proviamolo per induzione su r. Se $r = 1$ allora $[\gamma_1(G), A_s] = [G, A_s] = A_{s+1}$ per ogni s, assumiamo che $[\gamma_{r-1}(G), A_s] \leq A_{r+s-1}$ per ogni s. Per ipotesi induttiva $[G, A_s, \gamma_{r-1}(G)] \leq [A_{s+1}, \gamma_{r-1}(G)] \leq A_{r+s}$ e analogamente $[A_s, \gamma_{r-1}(G), G] \leq [A_{r+s-1}, G] \leq A_{r+s}$. Quindi per il lemma dei tre sottogruppi $[\gamma_{r-1}(G), G, A_s] = [\gamma_r(G), A_s] \leq A_{r+s}$. In particolare $[\gamma_k(G), A] \leq A_k$ per ogni k. Possiamo ora dimostrare che $A_k = Ker\phi_k$. Se $k = 0$ il risultato è evidente; supponiamolo vero per k e proviamolo per $k + 1$. $A_{k+1}^{\phi_{k+1}} = A_{k+1}^{\phi} = [A_k, G]^{\phi} = [A_k^{\phi}, G^{\phi}] = [Ker\phi_k^{\phi}, G^{\phi}] = 1$. Viceversa, gli elementi di $A \cap \gamma_{k+2}(G) = Ker\phi_{k+1}$ sono prodotto di commutatori, perciò basta notare che se $[y_k x_k, yx] \in Ker\phi_{k+1}$ con $x \in B, x_k \in \gamma_{k+1}(B), y \in A$ e $y_k \in A_k$, allora $[y_k x_k, yx]^{\phi} = [x_k, x] = 1$ e $[y_k x_k, yx] = [y_k x_k, x][y_k x_k, y]^x = [y_k, x]^{x_k}[y_k, y]^{x_k x}[x_k, y]^x$. Dunque $Ker\phi_{k+1} \leq \langle [A_k, G]^g, [\gamma_{k+1}(G), A]^g | g \in G \rangle = \langle [A_k, G], [\gamma_{k+1}(G), A] \rangle = [A_k, G] = A_{k+1}$.

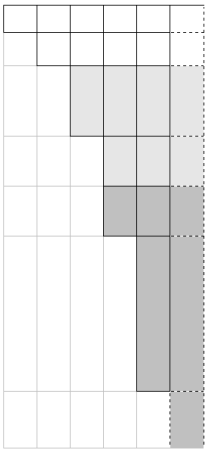


Figura 2.2: Termini della serie discendente di $P_{p^{n+1}}$

Applicando quanto appena visto a $P_{p^{n+1}}$ si ottiene per induzione su n

$$\gamma_k(P_{p^{n+1}}) = A^0_{k-1}A^1_{k-1}\cdots A^n_{k-1}.$$

Usando l'interpretazione grafica precedente di $P_{p^{n+1}}$ possiamo notare che per ottenere i termini della serie centrale discendente è sufficiente cancellare ad una ad una le righe dalla figura.
Inoltre, con argomentazioni simili a quelle appena esposte, si può dimostrare che

$$(P_{p^{n+1}})^{(k)} = A^0_{p^{k-1}}A^1_{p^{k-1}}\cdots A^n_{p^{k-1}}$$

dove, come al solito, si denota con $G^{(k)}$ il k-esimo termine della serie derivata.

Proposizione 2.1 *Sia $P_{p^{n+1}} = P_{p^n}A^n_0$ allora $[A^n_k : A^n_{k+1}] = p$ per ogni $k = 0, \cdots, p^n - 1$.*

Dimostrazione: Iniziamo con l'osservare che $A^n_{k+1} = [A^n_k, P_{p^{n+1}}] = [A^n_k, P_{p^n}]$. Introduciamo una base in A^n_0 che ci sarà molto utile in seguito. Sia $\mathfrak{E} = \{e_1, \cdots, e_{p^n}\}$ base di A^n_0 e σ p^n-ciclo di P_{p^n} tali che $e^\sigma_i = e_{i+1}$ per $i = 1, \cdots, p^n - 1$ e $e^\sigma_{p^n} = e_1$. Questa ipotesi non è ovviamente restrittiva, basta ricordare che ogni p^n-ciclo di S_{p^n} è contenuto in un p-Sylow di S_{p^n} e che questi ultimi sono tutti coniugati. Definiamo ora la seguente base:

$$y_0 = e_1 \quad \text{e} \quad y_{i+1} = [y_i, \sigma]$$

per $i = 0, \cdots, p^n - 1$. $\mathfrak{F} = \{y_i\}_{i=0,\cdots,p^n-1}$ è base di A_o^n; infatti y_i è prodotto soltanto dei primi $i+1$ elementi della base di $\mathfrak{E}$, ed in generale

$$y_k = \prod_{i=0}^{k} (e_{i+1})^{(-1)^{(k-i)}\binom{k}{i}}$$

$A_k^n = \langle y_k, \cdots, y_{p^n-1} \rangle$; se $k = 0$ dipende dal fatto che $\mathfrak{F}$ è base di A_0^n. Se $k > 0$ e $A_{k-1}^n = \langle y_{k-1}, \cdots, y_{p^n-1} \rangle$ allora $A_k^n = [A_{k-1}^n, P_{p^n}] \geq [A_{k-1}^n, \langle \sigma \rangle] = [\langle y_{k-1}, \cdots, y_{p^n-1} \rangle, \langle \sigma \rangle] = \langle [y_{k-1}, \sigma], \cdots, [y_{p^n-1}, \sigma] \rangle = \langle y_k, \cdots, y_{p^n-1} \rangle$, a questo punto la tesi è immediata.

Proposizione 2.2 *La classe di nilpotenza di $P_{p^{n+1}}$ è p^n e $Z(P_{p^{n+1}}) = A_{p^n-1}^n = \langle y_{p^n-1} \rangle = \langle e_1 \cdots e_{p^n} \rangle$. Ogni sottogruppo normale H di $P_{p^{n+1}}$ contenuto in A^n è della forma A_i^n.*

Dimostrazione: I primi due asserti seguono immediatamente dalla proposizione precedente; l'ultima affermazione dipende dal fatto che se $y_i \in H$ allora $y_{i+1} \in H$, per normalità.

Proposizione 2.3 *La lunghezza derivata di P_{p^n} è n.*

Dimostrazione: Si noti che $(P_{p^n})^{(n-1)} = A_{p^{n-2}}^0 \cdots A_{p^{n-2}}^{n-1} = A_{p^{n-2}}^{n-1}$ è abeliano.

Teorema 2.1 *I termini della serie centrale discendente di $P_{p^{n+1}}$ coincidono con i termini della serie centrale ascendente.*

Dimostrazione Per una dimostrazione diretta si può procedere per induzione su n. Se $n = 0$ il risultato è banale. Ovviamente $\gamma_{i+1}(P_{p^{n+1}}) \leq Z_{p^n-i}(P_{p^{n+1}})$. Per l'altra inclusione si veda ad esempio A.J.WEIR [9].

Definizione 2.1 *Sia G un gruppo, per ogni intero positivo n poniamo:*

$$\lambda_n(G) = \gamma_1(G)^{p^{n-1}} \gamma_2(G)^{p^{n-2}} \cdots \gamma_n(G)^1$$

Allora $\lambda_n(G)$ è un sottogruppo caratteristico di G e

$$G = \lambda_1(G) \geq \lambda_2(G) \geq \cdots \geq \lambda_n(G) \geq \cdots$$

Teorema 2.2 $[\lambda_m(G), \lambda_n(G)] \leq \lambda_{n+m}(G)$.
$\lambda_n(G)^{p^m} \leq \lambda_{n+m}(G)$.
Per $n > 1$, $\lambda_n(G) = [\lambda_{n-1}(G), G]\lambda_{n-1}(G)^p$.

Dimostrazione: Omessa (si veda ad esempio B.HUPPERT-N.BLACKBURN [3]).

Corollario 2.1 *Supponiamo di avere*

$$G = G_1 \geq G_2 \geq \cdots \geq G_n \geq G_{n+1} \geq \cdots$$

dove $G_i \trianglelefteq G$, $G_i/G_{i+1} \leq Z(G/G_{i+1})$ *e* G_i/G_{i+1} *è un p-gruppo abeliano elementare. Allora* $\lambda_n(G) \leq G_n$.

Dimostrazione: Omessa (si veda ad esempio B.HUPPERT-N.BLACKBURN [3]).

Proposizione 2.4 $\lambda_m(P_{p^n}) = \gamma_m(P_{p^n})$ *per ogni* $n, m \in \mathbb{N}$.

Dimostrazione: Dalla definizione segue che $\gamma_m(P_{p^n}) \leq \lambda_m(P_{p^n})$. Dal coral-lario precedente basterà verificare che $\gamma_m(P_{p^n})/\gamma_{m+1}(P_{p^n})$ è un p-gruppo abeliano elementare. A tal fine è necessario provare che $\gamma_i(P_{p^n})^{p^{m-i}} \leq \gamma_m(P_{p^n})$. Lo dimostriamo per induzione su n. Se $n = 0$ il risultato è ovvio. Sia $n > 0$ e supponiamo l'asserto vero per $n-1$. Sia $k = m - i$, se $k = 0$ otteniamo un'identità; proviamolo per induzione su k.
$\gamma_{m-k}(P_{p^n})^{p^k} \leq ((\gamma_{m-k}(P_{p^n}))^{p^{k-1}})^p \leq ((\gamma_{(m-1)-(k-1)}(P_{p^n}))^{p^{k-1}})^p \leq \gamma_{m-1}(P_{p^n})^p$.
Sia $\sigma f \in \gamma_{m-1}(P_{p^n})$ con $\sigma \in \gamma_{m-1}(P_{p^{n-1}})$ e $f \in A_{m-2}^{n-1}$ allora

$$(\sigma f)^p = \sigma^p f^{\sigma^{p-1}} f^{\sigma^{p-2}} \cdots f^{\sigma^1} f.$$

$\sigma^p \in (\gamma_{m-1}(P_{p^{n-1}}))^p \leq \gamma_m(P_{p^{n-1}})$, per ipotesi induttiva.
$f^{\sigma^{p-1}} f^{\sigma^{p-2}} \cdots f^{\sigma^1} f = [f^{\sigma^{p-2}}, \sigma][(f^2)^{\sigma^{p-3}}, \sigma] \cdots [(f^{(p-2)})^{\sigma}, \sigma][f^{(p-1)}, \sigma] \in A_{m-1}^{n-1}$.
Quindi $(\sigma f)^p \in \gamma_m(P_{p^{n-1}}) A_{m-1}^{n-1} = \gamma_m(P_{p^n})$.

Corollario 2.2 $exp(\gamma_m(P_{p^n})/\gamma_{m+1}(P_{p^n})) = p$ *per ogni* $n, m \in \mathbb{N}$.

Dimostrazione: È ovvio dalla proposizione precedente.

Corollario 2.3 $Fratt(P_{p^n}) = \gamma_2(P_{p^n})$ *e* $[P_{p^n} : Fratt(P_{p^n})] = p^n$.

Dimostrazione: P_{p^n} è un p-gruppo dunque $Fratt(P_{p^n}) = (P_{p^n})^p \gamma_2(P_{p^n})$, con la proposizione precedente si conclude che $(P_{p^n})^p = (\gamma_1(P_{p^n}))^p \leq \gamma_2(P_{p^n})$.
$[P_{p^n} : Fratt(P_{p^n})] = [A^0 A^1 \cdots A^{n-1} : A_1^0 A_1^1 \cdots A_1^{n-1}] = p^n$.

Diamo alcuni cenni sull'algebra gruppale che ci saranno utili in seguito.
Sia A un anello commutativo con identità, l'anello gruppale di G su A lo denoteremo con AG. L'ideale di aumentazione $\mathfrak{I}$ di AG è definito da:

$$\mathfrak{I} = \Big\{ \sum_{g \in G} a_g g \in AG | \sum_{g \in G} a_g = 0_A \Big\}$$

$\mathfrak{I}$ ha A-base $\{g - 1 \in AG |\ g \in G,\ g \neq 1\}$.
Indicheremo con $\mathbb{F}_p$ il campo con p elementi e con $\mathbb{F}_p G$ l'algebra gruppale di G su $\mathbb{F}_p$.

Proposizione 2.5 *Sia $\gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \cdots$ la serie centrale discendente di G e sia $\mathfrak{I}_n$ l'ideale di aumentazione dell'anello gruppale $A\gamma_n(G)$. Allora $\mathfrak{I}_n \subseteq \mathfrak{I}_1^n$.*

Dimostrazione: Per induzione su n, se $n = 1$ è ovvio. Sia $n > 1$ e supponiamo la proposizione vera per $n - 1$. Basterà provare l'asserto per un sistema di generatori di $\mathfrak{I}_n$.
$\mathfrak{I}_n = \langle g - 1 |\ g \in \gamma_n(G),\ g \neq 1 \rangle_A$ dove $\gamma_n(G) = \langle [h,k] |\ h \in G,\ k \in \gamma_{n-1}(G) \rangle$.
A questo punto è sufficiente notare che:

$$[h,k] - 1 = h^{-1}k^{-1}(\underbrace{(h-1)}_{\mathfrak{I}_1}\ \underbrace{(k-1)}_{\mathfrak{I}_{n-1} \subseteq \mathfrak{I}_1^{n-1}} - \underbrace{(k-1)}_{\mathfrak{I}_{n-1} \subseteq \mathfrak{I}_1^{n-1}}\ \underbrace{(h-1)}_{\mathfrak{I}_1}) \in \mathfrak{I}_1^n$$

e che

$$[h_1,k_1][h_2,k_2] - 1 = (\underbrace{[h_1,k_1]-1}_{\mathfrak{I}_1^n})(\underbrace{[h_2,k_2]-1}_{\mathfrak{I}_1^n}) + (\underbrace{[h_1,k_1]-1}_{\mathfrak{I}_1^n}) + (\underbrace{[h_2,k_2]-1}_{\mathfrak{I}_1^n})$$

da cui la tesi.

P_{p^n} opera fedelmente su $\{1, \cdots, p^n\}$ dunque P_{p^n} ha una rappresentazione permutazionale fedele in ogni k-spazio vettoriale di dimensione p^n. In particolare sia

$$\rho : P_{p^n} \longrightarrow GL_{\mathbb{F}_p}\mathbb{F}_p^{p^n}$$

l' $\mathbb{F}_p$-rappresentazione di P_{p^n}. Tale rappresentazione dota $\mathbb{F}_p^{p^n}$ di struttura di $\mathbb{F}_p P_{p^n}$-modulo destro. $P_{p^{n+1}} = P_{p^n} A^n$ e A^n è un $\mathbb{F}_p$-spazio vettoriale di dimensione p^n, perciò abbiamo immediatamente che A^n è un $\mathbb{F}_p P_{p^n}$-modulo destro. Inoltre se $\mathfrak{I}$ è l'ideale di aumentazione allora:

$$A^n\mathfrak{I} = A_1^n \text{ e più in generale } A_m^n \mathfrak{I}^k = A_{m+k}^n$$

dato che $f^{g-1} = [f,g]$.

Definizione 2.2 *Sia G un gruppo, per ogni intero n positivo poniamo:*

$$K_n(G) = \prod_{ip^k \geq n} (\gamma_i(G))^{p^k}$$

Allora $K_n(G)$ è un sottogruppo caratteristico di G ed inoltre

$$G = K_1(G) \geq K_2(G) \geq \cdots \geq K_n(G) \geq \cdots$$

Teorema 2.3 $[K_m(G), K_n(G)] \leq K_{n+m}(G)$.
$K_n(G)^p \leq K_{pn}(G)$.
$[K_{n-1}(G), G]K_m(G)^p = K_n(G)$ *per* $n > 1$, *dove* m *è il minimo intero per cui* $pm \geq n$.

Dimostrazione: Omessa (si veda ad esempio B.HUPPERT-N.BLACKBURN [3]).

Corollario 2.4 *Supponiamo che* $G = G_1 \geq G_2 \geq \cdots \geq G_n \geq \cdots$ *sia una catena dove* $G_n \trianglelefteq G$, $[G_n, G] \leq G_{n+1}$ *e* $G_n^p \leq G_{np}$ *per ogni* $n \geq 1$. *Allora* $K_n(G) \leq G_n$.

Dimostrazione: Omessa (si veda ad esempio B.HUPPERT-N.BLACKBURN [3]).

Proposizione 2.6 $K_m(P_{p^n}) = \gamma_m(P_{p^n})$ *per ogni* n, m *naturali.*

Dimostrazione: Dalla definizione precedente si ottiene subito che $\gamma_m(P_{p^n}) \leq K_m(P_{p^n})$ e dal corollario precedente segue che è sufficiente verificare che $\gamma_m(P_{p^n})^p \leq \gamma_{mp}(P_{p^n})$. Se $n = 0$ la proposizione è triviale. Sia $n > 0$ e supponiamo l'asserto vero per $P_{p^{n-1}}$. Sia $\sigma f \in \gamma_m(P_{p^n})$ allora

$$(\sigma f)^p = \sigma^p f^{\sigma^{p-1}} f^{\sigma^{p-2}} \cdots f^{\sigma^1} f = \sigma^p f^{\sigma^{p-1}+\sigma^{p-2}+\cdots+\sigma+1} = \sigma^p f^{(\sigma-1)^{p-1}}.$$

$\sigma \in \gamma_m(P_{p^{n-1}})$, da cui $\sigma^p \in \gamma_{mp}(P_{p^{n-1}})$ per ipotesi induttiva.
$\sigma - 1 \in \mathfrak{I}_m$ ideale di aumentazione di $\mathbb{F}_p\gamma_m(P_{p^{n-1}})$, segue che $(\sigma-1)^{p-1} \in \mathfrak{I}_m^{p-1}$. Ma $\mathfrak{I}_m^{p-1} \subseteq (\mathfrak{I}^m)^{p-1} = \mathfrak{I}^{mp-m}$, dunque $f^{(\sigma-1)^{p-1}} \in A_{m-1}^{n-1}\mathfrak{I}^{mp-m} = A_{mp-1}^{n-1}$, perciò $(\sigma f)^p \in \gamma_{mp}(P_{p^{n-1}})A_{mp-1}^{n-1} = \gamma_{mp}(P_{p^n})$, come volevasi dimostrare.

Corollario 2.5 $exp(\gamma_{p^m}(P_{p^n})/\gamma_{p^{m+1}}(P_{p^n})) = p$ *per ogni* $n, m \in \mathbb{N}$.

Dimostrazione: Ovvio dalla proposizione precedente.

Osserviamo, da quanto fino ad ora riportato, che

$$[\gamma_m(P_{p^n}) : \gamma_{m+1}(P_{p^n})] = p^d \quad \text{per } m = [p^{n-d-1}] + 1, \cdots, p^{n-d} \text{ e } d = 1, \cdots, n.$$

e che

$$[(P_{p^n})^{(m)} : (P_{p^n})^{(m+1)}] = p^{(n-m+1)(p^{m-1}-[p^{m-2}])}$$

A questo punto si riesce a calcolare $dim_{\mathbb{F}_p}\mathfrak{I}^n/\mathfrak{I}^{n+1}$ usando il seguente:

Teorema 2.4 (Formula di Jennings) *Sia G un p-gruppo finito, k un campo di caratteristica p e $\mathfrak{I}$ l'ideale di aumentazione di kG. Supponiamo che $K_l(G) > K_{l+1}(G) = 1$ e che $[K_n(G) : K_{n+1}(G)] = p^{d_n} \quad n = 1, \cdots, l$. Sia $s = (p-1)\sum_{n=1}^{l} n d_n$, e definiamo gli interi c_n con*

$$\prod_{i=1}^{l}(1 + t^i + \cdots + t^{(p-1)i})^{d_i} = \sum_{n=0}^{s} c_n t^n.$$

Allora $c_n = dim_{\mathbb{F}_p}\mathfrak{I}^n/\mathfrak{I}^{n+1}$.

Dimostrazione: Omessa (si veda ad esempio B.HUPPERT-N.BLACKBURN [3]).

Proposizione 2.7 *Se $p \neq 2$ allora A^n è l'unico sottogruppo normale abeliano massimale di $P_{p^{n+1}}$.*

Dimostrazione: Consideriamo $P_{p^{n+1}} = P_{p^n}A^n$ e sia $B \trianglelefteq P_{p^{n+1}}$ abeliano massimale, allora per ogni $\sigma f \in B$ e per ogni $g \in A^n$ risulta che $(\sigma f)^{-1}(\sigma f)^g = (g^{-1})^\sigma g \in B$ e $[\sigma f, (g^{-1})^\sigma g] = 1$, da cui $(g^{-1})^\sigma g = (g^{-1})^{\sigma^2} g^\sigma$. Se per assurdo $\sigma \neq 1$ allora non è restrittivo supporre che $1^\sigma \neq 1$. Usando le notazioni precedenti per la base di A^n, dalla formula appena scritta otteniamo: $e_{1^\sigma}^{-1} e_1 = e_{1^{\sigma^2}}^{-1} e_{1^\sigma}$. Quindi $1^{\sigma^2} = 1$, per cui $p = 2$.

Corollario 2.6 *Sia $p \neq 2$ allora A^n è un sottogruppo caratteristico di $P_{p^{n+1}}$.*

Dimostrazione: Ovvio dalla proposizione precedente.

Teorema 2.5 *Il sottogruppo $A_{i_s}^s \cdots A_{i_n}^n$ è caratteristico in $P_{p^{n+1}}$ se e solo se $i_r \leq p^s$ per ogni r.*

Dimostrazione: Omessa (si veda ad esempio A.J.WEIR [9]).

Proposizione 2.8 *Sia $\mathfrak{E} = \{e_1, \cdots, e_{p^n}\}$ una base di A^n per cui esista σ, p^n-ciclo di P_{p^n}, tale che $e_i^\sigma = e_{i+1}$ per $i = 1, \cdots, p^n - 1$ ed $e_{p^n}^\sigma = e_1$. Allora A_1^n è l'iperpiano di A^n di equazione*

$$X_1 \cdots X_{p^n} = 1.$$

Dimostrazione: A_1^n è generato dall'insieme $\{[e_i, \sigma^j] |\ i, j = 1, \cdots, p^n\} = \{e_i e_j^{-1} |\ i, j = 1, \cdots, p^n\}$. Con la base sopra descritta i generatori di A_1^n stanno sull'iperpiano. Per concludere basta ricordare che A_1^n ha codimensione uno in A^n.

Proposizione 2.9 *Il gruppo $P_{p^{n+1}}$ è generato da permutazioni senza punti fissi che sono il prodotto di cicli disgiunti dello stesso ordine.*

Dimostrazione: Proviamolo per induzione su n; se $n = 0$ allora P_p è generato da un p-ciclo. Supponiamo il risultato vero per n e sia $\{\sigma_i\}_{i\in I}$ un sistema di generatori per P_{p^n} come nell'enunciato.
$P_{p^{n+1}} = P_{p^n} A^n$, $\{\sigma_i\}_{i\in I}$ come permutazioni di $P_{p^{n+1}}$ sono senza punti fissi e rimangono prodotto di cicli disgiunti dello stesso ordine, infatti

$$(k,t)\sigma_i = (k, t^{\sigma_i}) \quad \forall i \in I$$

Non è restrittivo, a meno di induzione, supporre che esista $i_0 \in I$ per cui σ_{i_0} sia un p^n-ciclo.
L'insieme $\{\sigma_i, \sigma_{i_0} e_1 |\ i \in I\}$ genera $P_{p^{n+1}}$, inoltre

$$(\sigma_{i_0} e_1)^{p^n} = e_1^{\sigma_{i_0}^{(p^n-1)}} \cdots e_1^{\sigma_{i_0}} e_1 = e_1 e_2 \cdots e_{p^n} \neq 1$$

Da cui $\sigma_{i_0} e_1$ è un p^{n+1}-ciclo.

Capitolo 3

Automorfismi di P_{p^n}

Lemma 3.1 *Sia P un gruppo di permutazione transitivo sull'insieme I e $N_{S_I}(P)$ il normalizzante di P nel gruppo delle permutazioni di I. Sia K lo stabilizzatore in $N_{S_I}(P)$ di i_0 e sia $H = P \cap K$. Allora $K \cong N_{AutP}(H)$ e $N_{S_I}(P)/P \cong N_{AutP}(H)/Inn_H P$.*

Dimostrazione: Dato che P è transitivo segue, dall'argomento di Frattini, che $N_{S_I}(P) = PK$. Ovviamente gli elementi di I possono essere identificati con classi laterali di K in $N_{S_I}(P)$, ed inoltre ogni tale classe laterale contiene un elemento di P. Se $\alpha \in N_{AutP}(H)$, sia $\widetilde{\alpha}$ la mappa $Kx \mapsto K\alpha(x)$ per $x \in P$. $\widetilde{\alpha}$ è ben definita dato che α fissa H, $\widetilde{\alpha}$ è una permutazione su I, e $\widetilde{\alpha}^{-1}y\widetilde{\alpha}$ mappa Kx in $Kx\alpha(y)$ se x e y sono elementi di P. Perciò $\widetilde{\alpha}^{-1}y\widetilde{\alpha} = \alpha(y)$. Quindi $\widetilde{\alpha} \in N_{S_I}(P)$; inoltre dato che $\widetilde{\alpha}$ fissa la classe laterale K, $\widetilde{\alpha} \in K$. Abbiamo ottenuto una mappa da $N_{AutP}(H)$ in K ed è semplice verificare che si tratta di un omomorfismo. Se $\widetilde{\alpha}$ fissa ogni classe laterale Kx, allora $\alpha(x)x^{-1} \in K \cap P = H$ per ogni $x \in P$. Ma l'insieme $\{\alpha(x)x^{-1} |\ x \in P\}$ genera un sottogruppo normale di P (questo segue dal fatto che $y^{-1}(\alpha(x)x^{-1})y = (\alpha(y^{-1})y)^{-1}(\alpha(y^{-1}x)(y^{-1}x)^{-1})$ per ogni x e y in P), e, dato che H è lo stabilizzatore di un punto in un gruppo di permutazione transitivo, H deve essere core-free in P. Quindi, se $\widetilde{\alpha} = 1$, allora $\alpha = 1$. Infine, supponiamo che $y \in K$. Allora la coniugazione per y determina un automorfismo α di P. Dato che y normalizza H, α deve fissare H. Quindi $\alpha \in N_{AutP}(H)$. Ora $\alpha(x) = y^{-1}xy$ per ogni $x \in P$ e dunque $K\alpha(x) = Ky^{-1}xy = Kxy$. Perciò $\widetilde{\alpha}$ mappa la classe laterale Kx in Kxy. Segue che $\widetilde{\alpha} = y$. Abbiamo per ora dimostrato che la mappa $\alpha \mapsto \widetilde{\alpha}$ è un isomorfismo di $N_{AutP}(H)$ in K, quindi $N_{AutP}(H) \cong K$. In questo isomorfismo, il sottogruppo H corrisponde al sottogruppo $Inn_H P$. Quindi $K/H \cong N_{AutP}(H)/Inn_H P$. Ma questo è isomorfo a $N_{S_I}(P)/P$ dato che $N_{S_I}(P) = PK$ e $P \cap K = H$.

Prima di dare il teorema di struttura di $AutP_{p^n}$ vediamo come si possono costruire automorfismi di AWr_XB a partire da automorfismi di A e di B.

Lemma 3.2 *Sia A un gruppo e B un gruppo di permutazioni transitivo sull'insieme X. Se $\alpha \in AutA$, definiamo $\widetilde{\alpha}$ tramite*

$$(bf)^{\widetilde{\alpha}} = bf^{\widetilde{\alpha}} \qquad dove \quad f^{\widetilde{\alpha}}(x) = (f(x))^{\alpha}$$

per ogni $b \in B, f \in A^{[X]}, x \in X$. Allora $\widetilde{\alpha} \in Aut(AWr_XB)$ e la funzione $\sim: AutA \to Aut(AWr_XB)$ è un omomorfismo iniettivo di gruppi. Inoltre se $A_1 = \{\widetilde{\alpha} |\ \alpha \in AutA\}$ allora $A_1 \cong AutA$ e $[A_1, B] = 1$.

Dimostrazione: La verifica di ambo gli asserti è immediata.

Lemma 3.3 *Se $y \in N_{S_X}(B)$, definiamo $\widetilde{y}$ tramite*

$$(bf)^{\widetilde{y}} = b^y f^y \qquad dove \quad f^y(x) = f(x^{y^{-1}})$$

per ogni $b \in B, f \in A^{[X]}, x \in X$. Allora $\widetilde{y} \in Aut(AWr_XB)$ e la funzione $\sim: N_{S_X}(B) \to Aut(AWr_XB)$ è un omomorfismo iniettivo di gruppi. Inoltre se $A_2 = \{\widetilde{y} |\ y \in N_{S_X}(B)\}$ allora $[A_1, A_2] = A_1 \cap A_2 = 1$.

Dimostrazione: La verifica di ambo gli asserti è un immediata.

Lemma 3.4 *Sia B un gruppo di permutazione transitivo sull'insieme X e sia H lo stabilizzatore in B del punto x_0 di X. Per ogni $x \in X$ consideriamo $t_x \in B$ tale che $x = x_0^{t_x}$ e assumiamo che $t_{x_0} = 1$. Se $\lambda \in Hom(H, Z(A))$ e se $b \in B$, sia b^{λ} l'elemento di $A^{[X]}$ tale che*

$$b^{\lambda}(x) = \lambda(t_x b t_{x^b}^{-1})$$

per ogni $x \in X$. Definiamo $\widetilde{\lambda}$ tramite

$$(bf)^{\widetilde{\lambda}} = b(b^{\lambda} f)$$

per ogni $f \in A^{[X]}, b \in B$. Allora $\widetilde{\lambda} \in Aut(AWr_XB)$ e la funzione $\sim: Hom(H, Z(A)) \to Aut(AWr_XB)$ è un omomorfismo iniettivo di gruppi. Inoltre se $A_3 = \{\widetilde{\lambda} |\ \lambda \in Hom(H, Z(A))\}$ allora $A_3 \cong Hom(H, Z(A))$ e $A_3 \cap A_1A_2 = 1$.

Dimostrazione: La verifica di ambo gli asserti è un immediata.

Lemma 3.5 *Siano A, B due gruppi e $\beta \in AutB$, definiamo $\widetilde{\beta}$ in $A \wr B$ tramite*

$$(bf)^{\widetilde{\beta}} = b^{\beta} f^{\widetilde{\beta}} \qquad dove \quad f^{\widetilde{\beta}}(x) = f(x^{\beta^{-1}})$$

per ogni $b, x \in B, f \in A^B$.
Allora $\widetilde{\beta} \in Aut A \wr B$ e la funzione $\sim: AutB \to Aut A \wr B$ è un omomorfismo iniettivo di gruppi.

Dimostrazione: La verifica è banale.

È utile fare le seguenti
Osservazioni. Se $P_{p^{n+1}} = P_{p^k} Wr_X P_{p^m}$, con $X = \{1, \cdots, p^m\}$ e $k = n - m + 1$, sia $\alpha \in N_{S_{p^k}}(P_{p^k})$ tale che $1^{\alpha} = 1$ e sia $y \in N_{S_{p^m}}(P_{p^m})$ tale che $1^y = 1$. Allora $\widetilde{\alpha}$ e $\widetilde{y}$ sono automorfismi interni di $P_{p^{n+1}}$.

Dimostrazione: Per il lemma 3.1 basterà notare che $H = Stab_{P_{p^{n+1}}}((1,1))$ viene normalizzato da $\widetilde{\alpha}$ e da $\widetilde{y}$. Se $\sigma f \in H$ allora $(1,1)(\sigma f)^{\widetilde{\alpha}} = (1,1)\sigma f^{\widetilde{\alpha}} = (1^{f^{\widetilde{\alpha}(1^{\sigma})}}, 1^{\sigma}) = (1^{(f(1))^{\alpha}}, 1) = (1^{\alpha^{-1} f(1) \alpha}, 1) = (1,1)$. Analogamente per $\widetilde{y}$ $(1,1)(\sigma f)^{\widetilde{y}} = (1,1)\sigma^y f^y = (1^{f^y(1^{\sigma^y})}, 1^{\sigma^y}) = (1^{f(1^{\sigma})}, 1^{\sigma^y}) = (1,1)$, da cui la tesi.

Se $P_{p^{n+1}} = P_p Wr_X P_{p^n}$ e $\alpha \in AutP_p$ allora $\widetilde{\alpha}$ è un automorfismo interno. Se $P_{p^{n+1}} = P_{p^n} \wr P_p$ e $\beta \in AutP_p$ allora $\widetilde{\beta}$ è un automorfismo interno.

Dimostrazione: Per quanto riguarda il primo asserto se $\sigma f \in Stab_{P_{p^{n+1}}}((1,1))$ allora $(1,1)(\sigma f)^{\widetilde{\alpha}} = (1^{f^{\widetilde{\alpha}}(1^{\sigma})}, 1^{\sigma}) = (1,1)$. Per la seconda proposizione basta notare che $Stab_{P_{p^{n+1}}}((1,1)) = \{f \in A^n |\ f(1) = id\}$ e concludere come l'osservazione precedente.

Per proseguire lo studio del gruppo degli automorfismi di P_{p^n} è necessario introdurre una nuova scrittura degli elementi, detta a riduzione polinomiale. Sia C_p il gruppo ciclico con p elementi e sia $E_s = C_p \times \cdots \times C_p$ il prodotto diretto di s copie del gruppo C_p, per $0 \leq s \leq n$. Poniamo $E_0 = 1_{C_p}$ e $E = E_n$. Sia $a_s : E_{s-1} \to C_p$ una applicazione di E_{s-1} in C_p. In particolare $a_1 : E_0 \to C_p$ è una costante di C_p. Denotiamo a_s con la scrittura $a_s(x_1, \cdots, x_{s-1})$, per ricordare che è una funzione in $s-1$ variabili.
Rappresentiamo con la tabella

$$\mathfrak{a} = [a_1, a_2(x_1), \cdots, a_n(x_1, \cdots, x_{n-1})]$$

la permutazione dell'insieme E definita dalla corrispondenza

$$t = (t_1, \cdots, t_n) \mapsto t' = (a_1 t_1, a_2(t_1) t_2, \cdots, a_n(t_1, \cdots, t_{n-1}) t_n)$$

Quando le a_s descrivono l'insieme delle funzioni di E_{s-1} in C_p queste permutazioni formano un gruppo. Tale gruppo è isomorfo a P_{p^n}.
La funzione $a_s(x_1, \cdots, x_{s-1})$ si dice s-esima coordinata di $\mathfrak{a}$ e si denota con $[\mathfrak{a}]_s$. Le s-coordinate degli elementi di P_{p^n} possono essere rappresentate da polinomi in $x_1, \cdots, x_{s-1}$ a coefficienti in $\mathbb{F}_p$, in cui l'esponente di ogni x_i è minore o uguale a $p-1$. Questo perchè $\mathbb{F}_p(x_1, \cdots, x_{s-1})/(x_1^p, \cdots, x_{s-1}^p) \cong \mathbb{F}_p^{\mathbb{F}_p^{s-1}}$.
Non è difficile vedere che con questa notazione $\{[\mathfrak{a}]_s |\ \mathfrak{a} \in P_{p^n}\} = A^{s-1}$.
Insomma questa nuova scrittura ha il pregio di esprimere gli elementi del Sylow come tabelle di polinomi senza modificare in alcun modo la costruzione fino ad ora sviluppata.

Sia H un sottogruppo di P_{p^n}. Denotiamo con H_i le permutazioni di H che conservano le prime i coordinate di $(1, \cdots, 1) \in E$:

$$H_i = \{\mathfrak{a} \in P_{p^n} |\ \mathfrak{a} \in H,\ [\mathfrak{a}]_j(1, \cdots, 1) = 1 \text{ per } 1 \leq j \leq i\}.$$

Otteniamo una catena di sottogruppi di H

$$H = H_0 \geq H_1 \geq \cdots \geq H_n$$

in cui ciascuno è normale nel precedente. Tale serie si dice la serie canonica di H. L'applicazione $\phi_i : \mathfrak{a}H_i \mapsto [\mathfrak{a}]_i(1, \cdots, 1)$, con $\mathfrak{a} \in H_{i-1}$, è un isomorfismo di H_{i-1}/H_i in C_p e H_n è core-free in H, essendo lo stabilizzatore di $(1, \cdots, 1)$ in E.

Teorema 3.1 *Sia H un gruppo che possieda una catena di sottogruppi*

$$H = H_0 \geq H_1 \geq \cdots \geq H_n$$

tale che il quoziente H_{i-1}/H_i è isomorfo a C_p e H_n è core-free in H. Sia, per $i = 1, \cdots, n$, ψ_i un isomorfismo di H_{i-1}/H_i in C_p. Allora esiste un isomorfismo η di H su un sottogruppo transitivo G di P_{p^n} per cui $\eta(H_i) = G_i$ e $\psi_i = \phi_i \circ \eta$. Un tale isomorfismo η si dirà un C_p-isomorfismo relativo a $\{\psi_i\}_{1 \leq i \leq n}$.

Dimostrazione: Omessa (si veda P.LENTOUDIS [5], [6]).

Teorema 3.2 *Sia η un C_p-isomorfismo di H in P_{p^n} relativo a $\{\psi_i\}_{1 \leq i \leq n}$. Se $InnP_{p^n}$ è il gruppo degli automorfismi interni di P_{p^n} allora l'insieme dei C_p-isomorfismi di H in P_{p^n} relativi a $\{\psi_i\}_{1 \leq i \leq n}$ è $InnP_{p^n}\eta$. In particolare i C_p-automorfismi di P_{p^n} relativi a $\{\psi_i\}_{1 \leq i \leq n}$ formano il gruppo*

$$Aut^{C_p} P_{p^n} = InnP_{p^n}.$$

Dimostrazione: Omessa (si veda P.LENTOUDIS [5], [6]).

Ponendo $H = P_{p^n}$, i teoremi precedenti permettono di trovare $AutP_{p^n}$ conoscendo:
- le immagini della serie canonica tramite gli elementi di $AutP_{p^n}$
- l'insieme $Aut(P_{p^n}, *)$ degli automorfismi che stabilizzano la serie canonica.

Siano $\omega_1, \omega_2, \cdots, \omega_n$ degli automorfismi di C_p e poniamo $\omega = (\omega_1, \omega_2, \cdots, \omega_n)$ l'automorfismo di P_{p^n} tale che

$$[a_1, \cdots, a_i(x_1, \cdots, x_{i-1}), \cdots, a_n(x_1, \cdots, x_{n-1})] \mapsto$$

$$[\omega_1 a_1, \cdots, \omega_i a_i(\omega_1^{-1}x_1, \cdots, \omega_{i-1}^{-1}x_{i-1}), \cdots, \omega_n a_n(\omega_1^{-1}x_1, \cdots, \omega_{n-1}^{-1}x_{n-1})]$$

Tale automorfismo stabilizza la serie canonica di P_{p^n} ed induce gli automorfismi ω_i sui quozienti. L'insieme di questi automorfismi formano un gruppo isomorfo a $(\mathbb{Z}/(p-1)\mathbb{Z})^n$ e lo denoteremo con Ω_n. È evidente che

$$Aut(P_{p^n}, *) = \Omega_n Aut^{C_p} P_{p^n} = \Omega_n Inn P_{p^n}.$$

Inoltre per l'osservazione precedente è ovvio che

$$Inn_{N(P_{p^n})} P_{p^n} = \Omega_n Inn P_{p^n}.$$

Tale risultato ci permette di ricordare che $N(P_{p^n})/P_{p^n} \cong (\mathbb{Z}/(p-1)\mathbb{Z})^n$.

Sia $p \neq 2$ per tutto il seguito di questo capitolo. Denotiamo con $D_i = \frac{\partial}{\partial x_i}$ l'usuale operatore di derivazione parziale e poniamo

$$D^{(j)} = D_{j+1} D_{j+2} \cdots D_{n-1} \qquad \text{per } 1 \leq j \leq n-1.$$

Allora la corrispondenza:

$$[a_1, a_2, \cdots, a_n] \mapsto [a_1, a_2, \cdots, a_{n-1}, a_n + \sum_{j=1}^{n-1} \sum_{k=1}^{p-1} f_{j,k} (D^{(j)})^{p-1} D_j^k a_n]$$

è un automorfismo di P_{p^n} per ogni $f_{j,k} \in \mathbb{F}_p$. L'insieme di questi automorfismi formano un gruppo che si denota con L_n.
Dal fatto che A^{n-1} è caratteristico in P_{p^n} e che $P_{p^n}/A^{n-1} \cong P_{p^{n-1}}$ si ottiene l'omomorfismo

$$\phi : AutP_{p^n} \longrightarrow AutP_{p^{n-1}}$$

proiezione sul quoziente. Esiste $C_n \leq Ker\phi$ tale che operi identicamente su A^{n-1} per cui valga il seguente

Teorema 3.3 *I sottogruppi* Ω_n, $InnP_{p^n}$, L_n *e* C_n *sono tali che* $AutP_{p^n} = \Omega_n InnP_{p^n} L_n C_n$. *Inoltre* $|AutP_{p^n}| = (p-1)^n p^{(p^{n-1}+p^{n-2}+\cdots+p^2+\frac{n^2-n+2}{2}(p-1))}$, $|InnP_{p^n}| = p^{p^{n-1}+p^{n-2}+\cdots+p+1}$, $|C_n| = p^{\frac{(n-1)(n-2)(p-1)}{2}}$, $|\Omega_n| = (p-1)^n$ *e* $|L_n| = p^{(n-1)(p-1)}$.

Dimostrazione: Omessa (si veda P.LENTOUDIS [5], [6]).

Sia $G = \{\alpha \in AutP_{p^n} |\ \alpha \in Ker\phi \text{ e } \alpha_{|A^{n-1}} = id\}$, allora la posizione $\sigma^{\delta_\alpha} = \sigma^\alpha \sigma^{-1}$ definisce un isomorfismo

$$\delta : G \longrightarrow Der(P_{p^{n-1}}, A^{n-1})$$

$$\alpha \longmapsto \delta_\alpha : P_{p^{n-1}} \longrightarrow A^{n-1}$$

$$\sigma \longmapsto \sigma^\alpha \sigma^{-1}$$

Lemma 3.6 $(P_{p^{n-1}})^\delta \subseteqq A_1^{n-1}$ *per ogni* $\delta \in Der(P_{p^{n-1}}, A^{n-1})$.

Dimostrazione: Iniziamo con il notare che $(\sigma_1\sigma_2)^\delta = (\sigma_1^\delta)^{\sigma_2}\sigma_2^\delta$ e dunque basterà provare l'asserto per dei generatori di $P_{p^{n-1}}$. Ricordiamo che $P_{p^{n-1}}$ è generato dal prodotto di cicli della stessa lunghezza per la proposizione 2.9. Sia $\{\sigma_i\}_{i\in I}$ una tale famiglia di generatori. $\delta = \delta_\alpha$ per qualche $\alpha \in G$, pertanto $\sigma_i^\delta = \sigma_i^\alpha \sigma_i^{-1} = f$ per qualche $f \in A^{n-1}$. Essendo α un automorfismo l'ordine di σ_i coincide con l'ordine di $\sigma_i f$, dunque

$$(\sigma_i f)^{o(\sigma_i)} = f^{\sigma_i^{o(\sigma_i)-1}} \cdots f^{\sigma_i} f = 1.$$

Quindi $(f^{\sigma_i^{o(\sigma_i)-1}} \cdots f^{\sigma_i} f)(x) = 1$ per ogni $x = 1, \cdots, p^{n-1}$. σ_i è prodotto di cicli disgiunti dello stesso ordine, segue che $\prod_{x=1}^{p^{n-1}} f(x) = 1$ e perciò $f \in A_1^{n-1}$ per la proposizione 2.8.

Capitolo 4

Sottogruppi di P_{p^2}

Sia come al solito p un primo.
$P_{p^2} = A^0A^1$, $A^0 = \langle\sigma\rangle$, $[P_{p^2} : A^1] = p$, $|A^1| = p^p$.
Sia G un sottogruppo di P_{p^2} allora $G_1 = G \cap A^1 \trianglelefteq G$ e $[G : G_1] \leq p$. Se $[G : G_1] = 1$ allora G è un p-gruppo abeliano elementare e la sua classe di isomorfismo è univocamente determinata dalla sua dimensione come $\mathbb{F}_p$-spazio vettoriale. Per tali sottogruppi abbiamo $p+1$ classi di isomorfismo.
Supponiamo che $[G : G_1] = p$ e sia $\sigma g \in G\backslash G_1$, con $g \in A^1$.
Dato che G_1 è contenuto nella base abbiamo che $G_1 = (G_1)^{\sigma g} = (G_1)^{\sigma}$, quindi $G_1 \trianglelefteq P_{p^2}$, per cui, dalla proposizione 2.2, $G_1 = A_i^1$ per qualche $i = 0, \cdots, p-1$.
Si consideri

$$\varphi : \langle\sigma g\rangle \longrightarrow AutA_i^1$$

l'omomorfismo di coniugazione.
$(\sigma g)^p \in A_i^1$, quindi $((\sigma g)^{\varphi})^p = 1$, allora $(\sigma g)^{\varphi}$ è unipotente e ammette forma canonica

$$(\sigma g)^{\varphi} = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_k \end{pmatrix}$$

con

$$J_l = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Ovviamente la forma canonica di $(\sigma g)^\varphi$ e l'ordine di σg determinano univocamente la classe di isomorfismo di G. L'ordine di σg è p oppure p^2. Analizziamo le possibili forme canoniche di Jordan.
Calcoliamo l'ordine dei centralizzanti degli elementi di P_{p^2}.
Se $f \in Z(P_{p^2}) = A^1_{p-1}$ allora $\mathbb{C}_{P_{p^2}}(f) = P_{p^2}$.
Se $f \in A^1 \backslash A^1_{p-1}$ allora $\mathbb{C}_{P_{p^2}}(f) = A^1$.
Se $\sigma f \in P_{p^2} \backslash A^1$ allora $\mathbb{C}_{P_{p^2}}(\sigma f) = \langle \sigma f \rangle A^1_{p-1}$.
I primi due sono immediati, per quanto riguarda il terzo se σf permuta con $\sigma^j h$ allora non è restrittivo supporre che $j = 0$ oppure $j = 1$. Se $j = 0$ allora $(\sigma f)h = h(\sigma f)$ se e solo se $h^\sigma = h$, se e solo se $h \in A^1_{p-1}$.
Se $j = 1$ allora $[\sigma f, \sigma h] = 1$ se e solo se $[\sigma, f] = [\sigma, h]$, se e solo se $h = f\xi$ con $\xi \in A^1_{p-1}$, da cui la tesi.
Dunque $\mathbb{C}_{P_{p^2}}(\sigma f)$ ha ordine p^2.
Questo prova che nella forma canonica di $(\sigma g)^\varphi$ posso avere un solo blocco di Jordan, dato che in ciascun blocco esiste un unico elemento non nullo che permuta con σg. Pertanto ho una sola forma canonica:

$$(\sigma g)^\varphi = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Si trovano a meno di isomorfismo, al più $2(p-2)$ gruppi G per cui $[G : G_1] = p$. Per trovare i sottogruppi di P_{p^2} dobbiamo aggiungere il gruppo stesso, i gruppi abeliani elementari ed il gruppo ciclico di ordine p^2. Insomma, in P_{p^2} ci sono al più

$$p + 1 + 2(p-2) + 2 = 3p - 1$$

gruppi a meno di isomorfismo. Per concludere che la stima appena data è esatta basta osservare che

$$\begin{array}{ll} P_{p^2} & \\ A^1_i & i = 0, \cdots, p \\ \langle \sigma \rangle A^1_i \leq P_{p^2} & i = 1, \cdots, p-2 \\ \langle \sigma e_1 \rangle A^1_i \leq P_{p^2} & i = 1, \cdots, p-1 \end{array}$$

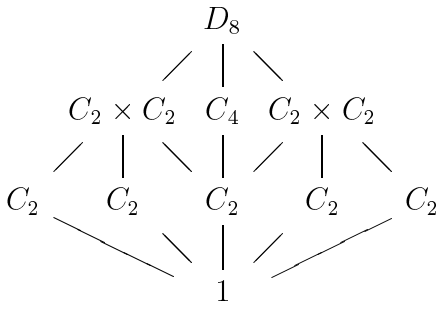
forniscono i $3p - 1$ rappresentanti delle classi di isomorfismo.

Teorema 4.1 *In P_{p^2} ci sono $3p - 1$ sottogruppi a meno di isomorfismo.*

Dimostrazione: Vista sopra.

Notiamo che l'esponente e la dimensione del sottogruppo abeliano elementare massimale determinano univocamente la classe di isomorfismo dei sottogruppi di P_{p^2}.

Osserviamo che se $p = 2$ allora troviamo che in D_8 ci sono 5 sottogruppi a meno di isomorfismo: $D_8, C_4, C_2 \times C_2, C_2, 1$.



Proposizione 4.1 *Se $G \leq P_{p^2}$ e $[G : G \cap A^1] = p$ allora G è coniugato in $N_{S_{p^2}}(P_{p^2})$ ad uno dei seguenti gruppi:*

$$P_{p^2} \quad \langle\sigma\rangle A_i^1 \quad \langle\sigma e_1\rangle A_i^1$$

Dimostrazione: Come si è visto precedentemente, se $G \leq P_{p^2}$ e soddisfa l'ipotesi della proposizione allora $G = \langle\sigma g\rangle A_i^1$, per qualche $g \in A^1$.
Se $g = e_1^a[f_1, \sigma][f_2, \sigma] \cdots [f_k, \sigma]$, poniamo $f = f_k \cdots f_2 f_1$ e consideriamo la coniugazione tramite f.

$$(\sigma g)^f = \sigma g[\sigma, f] = \sigma e_1^a[f_1, \sigma][f_2, \sigma] \cdots [f_k, \sigma][\sigma, f_k] \cdots [\sigma, f_2][\sigma, f_1] = \sigma e_1^a$$

Se $a = 0$ abbiamo concluso altrimenti si consideri l'automorfismo

$$\widetilde{a} : P_p \wr P_p \longrightarrow P_p \wr P_p$$

$$\sigma^j f \longmapsto \sigma^j f^a$$

Dal capitolo 3 è noto che $\widetilde{a}$ è un automorfismo interno, a questo punto basterà notare che $(\langle\sigma e_1\rangle A_i^1)^{\widetilde{a}} = \langle\sigma e_1^a\rangle A_i^1$.

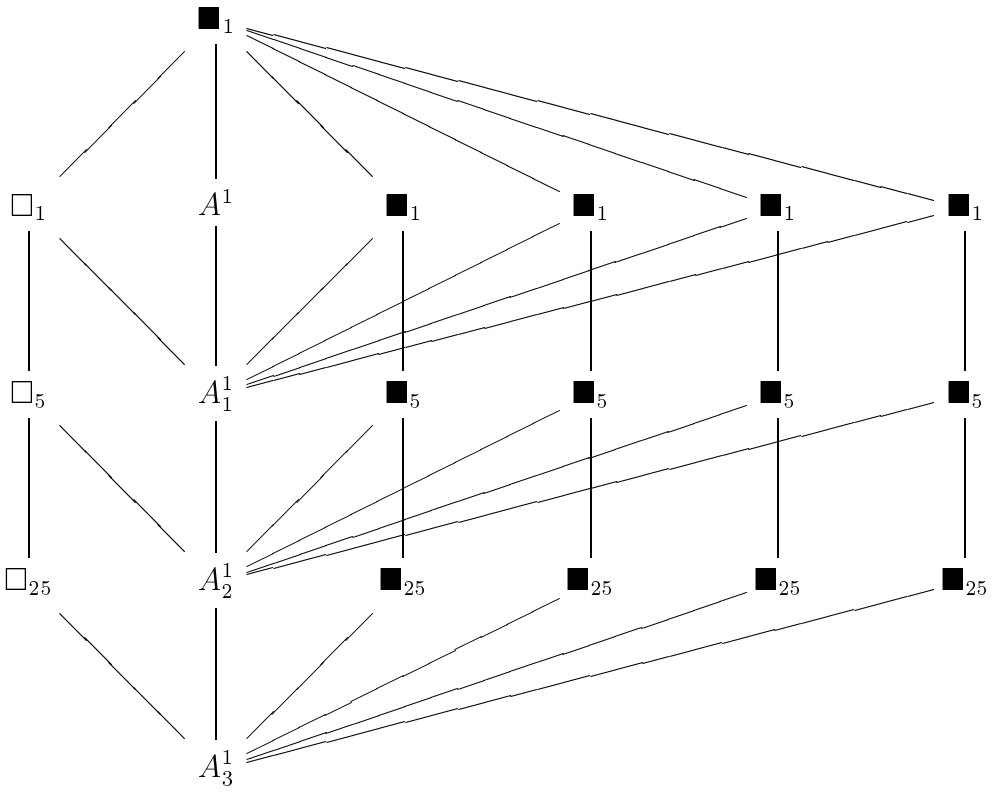
Concludiamo il capitolo calcolando il numero di sottogruppi non abeliani di P_{p^2}.

Proposizione 4.2 *In P_{p^2} ci sono $p^{p-1} - 1/p - 1$ sottogruppi non abeliani.*

Dimostrazione: Dalla proposizione precedente è noto che nell'azione di coniugio che P_{p^2} ha sui suoi sottogruppi non abeliani ci sono $(p-1)^2$ orbite. Basterà calcolare il numero di elementi per orbita. Ricordiamo che i rappresentanti di tali orbite sono i sottogruppi P_{p^2}, $\langle\sigma\rangle A_i^1$, $\langle\sigma e_1^a\rangle A_i^1$ per $i = 1, \cdots, p-2$ e $a = 1, \cdots, p-1$. È facile verificare che se G è uno di questi sottogruppi allora $\mathbb{C}_{P_{p^2}}(G) = GA_{i-1}^1$. Dunque $|\mathcal{O}(G)| = [P_{p^2} : \mathbb{C}_{P_{p^2}}(G)] = p^{i-1}$. Il numero di sottogruppi non abeliani di P_{p^2} è

$$\sum_{i=1}^{p-2} p^{i-1} + (p-1)\sum_{i=1}^{p-2} p^{i-1} + 1 = \sum_{i=0}^{p-2} p^i = \frac{p^{p-1}-1}{p-1}.$$

Mostriamo per $p = 5$ come è fatto il reticolo dei sottogruppi non abeliani di P_{25}.



Abbiamo denotato con $\square_x$ le orbite di sottogruppi non abeliani di esponente p e con $\blacksquare_x$ le orbite di sottogruppi non abeliani di esponente p^2. Il pedice x riferisce il numero di elementi che contiene l'orbita.

Capitolo 5

Massimali di P_{p^n}

Lemma 5.1 *Sia $p \neq 2$ e $1 \leq m \leq p-2$ allora*

$$\sum_{x \in \mathbb{F}_p} x^m = 0$$

Dimostrazione: Se m è coprimo con $p-1$ allora il risultato è ovvio. Sia $mq = p-1$ allora $S = \{x^m |\ x \in \mathbb{F}_p^*\} = \{y \in \mathbb{F}_p^* |\ y^q = 1\}$, dunque gli elementi di S sono le radici del polinomio

$$p(t) = t^q - 1.$$

La somma degli elementi di S coincide con l'opposto del coefficiente di grado $q-1$ di $p(t)$. Tale coefficiente è zero dato che $q \neq 1$, da cui la tesi.

Teorema 5.1 *Sia $p \neq 2$ e $\mathfrak{X} = \{M \leq P_{p^n} |\ M$ massimale$\}$ allora nell'azione*

$$\begin{array}{ccc} Aut P_{p^n} \times \mathfrak{X} & \xrightarrow{\quad\theta\quad} & \mathfrak{X} \\ (\alpha \quad , M) & \longmapsto & M^\alpha \end{array}$$

ci sono esattamente $2^n - 1$ orbite.

Dimostrazione: Proviamo che se $M_1, M_2 \in \mathcal{O}(M)$ allora esiste $y \in N_{S_{p^n}}(P_{p^n})$ per cui $M_1^y = M_2$.
Se $n = 2$ il risultato è noto dal capitolo precedente; in P_{p^2} ci sono 3 massimali a meno di isomorfismo e le classi di isomorfismo coincidono con le classi di coniugio nel normalizzante.

Sia $n > 2$ e supponiamo il risultato vero per $n-1$.
Consideriamo

$$P_p Wr_X P_{p^{n-1}} \xrightarrow{\pi} P_{p^{n-1}}$$

$$\sigma f \longmapsto \sigma$$

la proiezione sul quoziente.
Se M è un massimale di P_{p^n} e $A^{n-1} \subseteq M$ allora $M^\pi = \mathcal{M}$ è un massimale di $P_{p^{n-1}}$. Inoltre $\mathcal{M} \subseteq M$, da cui $M = \mathcal{M}A^{n-1}$.
Siano $\mathcal{M}_1, \mathcal{M}_2$ massimali isomorfi in $P_{p^{n-1}}$ allora, per ipotesi induttiva, esiste $y \in N(P_{p^{n-1}})$ tale che $\mathcal{M}_1^y = \mathcal{M}_2$. La coniugazione in $P_{p^{n-1}}$ tramite y si estende ad una coniugazione, $\widetilde{y} : P_{p^n} \longrightarrow P_{p^n}$, tramite $\widetilde{y} \in N(P_{p^n})$. A^{n-1} è caratteristico in P_{p^n}, quindi $(\mathcal{M}_1 A^{n-1})^{\widetilde{y}} = \mathcal{M}_2 A^{n-1}$, dunque $M_1 = \mathcal{M}_1 A^{n-1} \cong \mathcal{M}_2 A^{n-1} = M_2$. Viceversa se $M_1 = \mathcal{M}_1 A^{n-1}$ e $M_2 = \mathcal{M}_2 A^{n-1}$ sono isomorfi allora esiste $\alpha \in Aut P_{p^n}$ tale che $M_1^\alpha = M_2$. Tale automorfismo si fattorizza nell'isomorfismo

$$\overline{\alpha} : \mathcal{M}_1 \cong \frac{\mathcal{M}_1 A^{n-1}}{A^{n-1}} \longrightarrow \mathcal{M}_2 \cong \frac{\mathcal{M}_2 A^{n-1}}{A^{n-1}}$$

A meno di automorfismi in P_{p^n} ci sono $2^{n-1} - 1$ massimali che contengono la base e le classi di automorfismo coincidono con le classi di coniugio.
Con la scrittura a riduzione polinomiale scegliamo la seguente base di $\frac{P_{p^n}}{\gamma_2(P_{p^n})}$

$$\mathfrak{E} = \{[e_1, 0, \cdots, 0]\gamma_2(P_{p^n}),\ [0, e_2, 0, \cdots, 0]\gamma_2(P_{p^n}),\ \cdots,\ [0, \cdots, 0, e_n]\gamma_2(P_{p^n})\}$$

dove $e_i(0, \cdots, 0) = 1$ e $e_i(j_1, \cdots, j_{i-1}) = 0$ se $(j_1, \cdots, j_{i-1}) \neq (0, \cdots, 0)$.
Sia M un massimale di P_{p^n} tale che $A^{n-1} \nsubseteq M$, allora M non è isomorfo a nessun massimale contenente la base, dato che contiene un sottogruppo abeliano elementare massimale di ordine inferiore a $p^{p^{n-1}}$.
$M/\gamma_2(P_{p^n})$ è un iperpiano di $P_{p^n}/\gamma_2(P_{p^n})$ che non contiene $\frac{(A^{n-1}\gamma_2(P_{p^n}))}{\gamma_2(P_{p^n})}$, per cui, nella base appena scritta, avrà equazione:

$$X_n = a_1 X_1 + a_2 X_2 + \cdots + a_{n-1} X_{n-1} \qquad \text{con} \quad a_i \in \mathbb{F}_p.$$

Il massimale M è pertanto generato da

$$\{[e_1, 0, \cdots, 0, a_1 e_n],\ [0, e_2, 0, \cdots, 0, a_2 e_n],\ \cdots,\ [0, \cdots, 0, e_{n-1}, a_{n-1} e_n]\}.$$

Se $\omega = (\omega_1, \cdots, \omega_n) \in \Omega_n$ allora

$$[0, \cdots, 0, e_i, 0, \cdots, 0, a_i e_n]^\omega = [0, \cdots, 0, \omega_i e_i, 0, \cdots, 0, \omega_n a_i e_n].$$

Tramite gli automorfismi di Ω_n possiamo mappare l'iperpiano $X_n = a_1X_1 + a_2X_2 + \cdots + a_{n-1}X_{n-1}$ nell'iperpiano di equazione $X_n = c_1X_1 + c_2X_2 + \cdots + c_{n-1}X_{n-1}$, dove $c_i = 0$ se $a_i = 0$ e $c_i = 1$ se $a_i \neq 0$. Quindi a meno degli automorfismi di Ω_n abbiamo 2^{n-1} massimali che non contengono la base.
Prendiamo in esame l'omomorfismo naturale

$$- : AutP_{p^n} \longrightarrow Aut(P_{p^n}/\gamma_2(P_{p^n}))$$

$$\alpha \longmapsto \overline{\alpha}$$

La base $\mathfrak{E}$ determina un isomorfismo $Aut\frac{P_{p^n}}{\gamma_2(P_{p^n})} \cong \mathrm{GL}(\mathbb{F}_p, n)$; per concludere la dimostrazione basterà dimostrare che $-$ ha per immagine il gruppo delle matrici diagonali.
Dal teorema 3.3 è noto che $AutP_{p^n} = \Omega_n InnP_{p^n} L_n C_n$.
Ovviamente $InnP_{p^n} \leq Ker-$.
Se $\alpha \in C_n$ allora, per il lemma 3.6,

$$(\sigma f)^\alpha \equiv \sigma f \mathrm{mod}\gamma_2(P_{p^n}).$$

Dunque $C_n \leq Ker-$.
Ricordiamo che un automorfismo in L_n è definito da

$$[a_1, \cdots, a_{n-1}, a_n] \longmapsto [a_1, \cdots, a_{n-1}, a_n + \sum_{j=1}^{n-1}\sum_{k=1}^{p-1} f_{j,k}(D^{(j)})^{p-1} D_j^k a_n]$$

a_n è una funzione polinomiale in $x_1, \cdots, x_{n-1}$ in cui l'esponente di x_i è al più $p-1$, dunque $\sum_{j=1}^{n-1}\sum_{k=1}^{p-1} f_{j,k}(D^{(j)})^{p-1} D_j^k a_n$ è somma di monomi in cui almeno un x_i, per ciascun monomio, ha grado minore o uguale a $p-2$.
Sia $x_1^{\varepsilon_1} \cdots x_{n-1}^{\varepsilon_{n-1}}$ un tale monomio e sia $0 \leq \varepsilon_1 \leq p-2$, allora

$$\sum_{(X_1,\cdots,X_{n-1})} X_1^{\varepsilon_1} \cdots X_{n-1}^{\varepsilon_{n-1}} = \sum_{(X_2,\cdots,X_{n-1})} \underbrace{\Big(\sum_{X_1 \in \mathbb{F}_p} X_1^{\varepsilon_1}\Big)}_{0} X_2^{\varepsilon_1} \cdots X_{n-1}^{\varepsilon_{n-1}} = 0$$

per il lemma 5.1. Dunque per la proposizione 2.8

$$[0, \cdots, 0, \sum_{j=1}^{n-1}\sum_{k=1}^{p-1} f_{j,k}(D^{(j)})^{p-1} D_j^k a_n] \in A_1^{n-1}$$

quindi $L_n \leq Ker-$.
Infine se $\omega = (\omega_1, \cdots, \omega_n) \in \Omega_n$ allora

$$\overline{\omega} = \begin{pmatrix} \omega_1 & 0 & \cdots & 0 \\ 0 & \omega_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \omega_n \end{pmatrix}$$

è diagonale, da cui la tesi.

Corollario 5.1 *Sia*

$$T : AutP_{p^n} \longrightarrow Sym\mathfrak{X}$$

la rappresentazione permutazionale associata a θ, allora $Inn_{N(P_{p^n})}P_{p^n}$ supplementa $KerT$ in $AutP_{p^n}$

Dimostrazione: Ovvio dalla dimostrazione precedente e dal teorema di struttura del gruppo degli automorfismi: $InnP_{p^n}\Omega_n = Inn_{N(P_{p^n})}P_{p^n}$

Lemma 5.2 *Sia $K \leq P_{p^n}$ abeliano elementare normalizzato da A_1^n allora $K \leq A^n$.*

Dimostrazione: I conti sono simili a quelli visti nella proposizione 2.7.

Siano M_1, M_2 due massimali non contenenti la base e sia η un isomorfismo di M_1 in M_2.
Le proiezioni

$$\pi_i : M_i \longrightarrow P_{p^{n-1}}$$

$$\sigma f \longmapsto \sigma$$

sono suriettive e $Ker\pi_i = A_1^{n-1}$. Pertanto passando al quoziente su A_1^{n-1} troviamo due isomorfismi

$$\varphi_i : \frac{M_i}{A_1^{n-1}} \longrightarrow P_{p^{n-1}}$$

Osserviamo che $(A_1^{n-1})^\eta \trianglelefteq M_2$, $(A_1^{n-1})^\eta$ é normalizzato da A_1^{n-1} allora, dal lemma 5.2 $(A_1^{n-1})^\eta = A_1^{n-1}$. Per cui posso passare al quoziente su A_1^{n-1} anche per η e trovare il seguente diagramma

$$P_{p^{n-1}} \xrightarrow{\varphi_1^{-1}} \frac{M_1}{A_1^{n-1}} \xrightarrow{\widetilde{\eta}} \frac{M_2}{A_1^{n-1}} \xrightarrow{\varphi_2} P_{p^{n-1}}$$

$\gamma_2(P_{p^{n-1}})$ è caratteristico in $P_{p^{n-1}}$ e $\varphi_1^{-1} \circ \widetilde{\eta} \circ \varphi_2 \in AutP_{p^{n-1}}$; dal fatto che $(\gamma_2(P_{p^{n-1}}))^{\varphi_i^{-1}} = \frac{\gamma_2(P_{p^{n-1}})A_1^{n-1}}{A_1^{n-1}} = \frac{\gamma_2(P_{p^n})}{A_1^{n-1}}$, segue che $\left(\frac{\gamma_2(P_{p^n})}{A_1^{n-1}}\right)^{\widetilde{\eta}} = \frac{\gamma_2(P_{p^n})}{A_1^{n-1}}$ ed infine $(\gamma_2(P_{p^n}))^\eta = \gamma_2(P_{p^n})$.
Per cui posso fattorizzare η, φ_i tramite $\gamma_2(P_{p^n})$ e trovare i seguenti isomorfismi

$$\frac{M_1}{\gamma_2(P_{p^n})} \xrightarrow{\overline{\eta}} \frac{M_2}{\gamma_2(P_{p^n})} \quad \text{e} \quad \frac{M_i}{\gamma_2(P_{p^n})} \xrightarrow{\overline{\varphi_i}} \frac{P_{p^{n-1}}}{\gamma_2(P_{p^{n-1}})}$$

Indicando con $-: AutP_{p^n} \to Aut\frac{P_{p^n}}{\gamma_2(P_{p^n})}$ l'omomorfismo di proiezione, otteniamo che $\overline{\varphi_1^{-1}\widetilde{\eta}\varphi_2} = (\overline{\varphi_1})^{-1}\ \overline{\eta}\ \overline{\varphi_2}$. Dunque $(\overline{\varphi_1})^{-1}\ \overline{\eta}\ \overline{\varphi_2}$ è un automorfismo diagonale nella base $\mathfrak{E}$. Abbiamo provato che se

$$M_1 = \langle [0, \cdots, 0, e_i, 0, \cdots, 0, a_i e_n] |\ a_i \in \mathbb{F}_p \rangle$$

$$M_2 = \langle [0, \cdots, 0, e_i, 0, \cdots, 0, a_i e_n] |\ b_i \in \mathbb{F}_p \rangle$$

allora

$$([0, \cdots, 0, e_i, 0, \cdots, 0, a_i e_n]\gamma_2(P_{p^n}))^\eta = ([0, \cdots, 0, \omega_i e_i, 0, \cdots, 0, \omega_i b_i e_n]\gamma_2(P_{p^n}))$$

per qualche $\omega_i \in \mathbb{F}_p^*$.

Da ora in poi non sarà più necessaria la notazione a riduzione polinomiale. Possiamo passare alla scrittura più comoda introdotta nel capitolo 2.

Lemma 5.3 *Siano M_1, M_2 due massimali di P_{p^n} non contenenti la base A^{n-1} e η un isomorfismo di M_1 in M_2. Se $1 \leq i_r \leq p^s$ per ogni r allora $(A^s_{i_s} \cdots A^{n-2}_{i_{n-2}} A^{n-1}_1)^\eta = A^s_{i_1} \cdots A^{n-2}_{i_{n-2}} A^{n-1}_1$.*

Dimostrazione: Passando al quoziente su A_1^{n-1} nell'isomorfismo η si ottiene un automorfismo $\overline{\eta}$ di $P_{p^{n-1}}$. Dal teorema 2.4 $A^s_{i_s} \cdots A^{n-2}_{i_{n-2}}$ è caratteristico in $P_{p^{n-1}}$ e dunque

$$\left(\frac{A^s_{i_s} \cdots A^{n-2}_{i_{n-2}} A^{n-1}_1}{A_1^{n-1}}\right)^{\overline{\eta}} = \left(\frac{A^s_{i_s} \cdots A^{n-2}_{i_{n-2}} A^{n-1}_1}{A_1^{n-1}}\right).$$

Infine $(A^s_{i_s} \cdots A^{n-2}_{i_{n-2}} A^{n-1}_1)^\eta = A^s_{i_s} \cdots A^{n-2}_{i_{n-2}} A^{n-1}_1$ perchè $(A_1^{n-1})^\eta = A_1^{n-1}$.

Osservazione. Si consideri in A^n la base $\mathfrak{F}$ introdotta nella dimostrazione della proposizione 2.1, allora l'elemento $y_0 y_{p^n-1} \in A^n \backslash A_1^n$, ha ordine p ed è senza punti fissi.

Lemma 5.4 *Siano $\sigma_i \in A^i \backslash A_1^i$ e $\sigma_{n-1} \in A^{n-1} \backslash A_1^{n-1}$ due permutazioni di ordine p senza punti fissi. Allora le due classi laterali $\mathcal{C}_1 = \sigma_i A_1^0 \cdots A_1^{n-1}$ e $\mathcal{C}_2 = (\sigma_i \sigma_{n-1} A_1^0 \cdots A_1^{n-1})$ sono tali che*

$$|\{\tau \in \mathcal{C}_1 |\ o(\tau) = p\}| \gneq |\{\tau \in \mathcal{C}_2 |\ o(\tau) = p\}|.$$

Dimostrazione: Denotiamo con τ_j un elemento di A^j. Se $\tau_0 \cdots \tau_i \cdots \tau_{n-1}$ ha ordine p allora $\tau_0 \cdots \tau_i \cdots \tau_{n-2}$ ha ordine minore o uguale a p. Dunque in entrambe le classi laterali la cardinalità degli elementi di ordine p della forma $\tau_0 \cdots \tau_i \cdots \tau_{n-2}$ è la stessa. Sia $\tau \in P_{p^{n-1}}$, $f \in A^{n-1}$ e τf di ordine p, allora τ sarà il prodotto di m p-cicli e

$$(\tau f)^p = f^{\tau^{p-1}} \cdots f^{\tau} f = 1. \qquad (*)$$

Andiamo a contare il numero di scelte che si hanno per f in base alla decomposizione di τ e a seconda che $\tau f \in \mathcal{C}_1$ oppure $\tau f \in \mathcal{C}_2$.
Si fissi l'usuale base $\mathfrak{E}$ in A^{n-1}, per cui $A^{n-1} \cong \mathbb{F}_p^{p^{n-1}}$.
Se $\tau = (i_1\ i_1^{\tau} \cdots i_1^{\tau^{p-1}})(i_2\ i_2^{\tau} \cdots i_2^{\tau^{p-1}}) \cdots (i_m\ i_m^{\tau} \cdots i_m^{\tau^{p-1}})$ allora $(*)$ fornisce le seguenti equazioni omogenee:

$$\begin{cases} X_{i_1} + X_{i_1^{\tau}} + \cdots + X_{i_1^{\tau^{p-1}}} = 0 \\ X_{i_2} + X_{i_2^{\tau}} + \cdots + X_{i_2^{\tau^{p-1}}} = 0 \\ \cdots \\ X_{i_m} + X_{i_m^{\tau}} + \cdots + X_{i_m^{\tau^{p-1}}} = 0 \end{cases}$$

La condizione che $f \in \mathcal{C}_1$ si esprime nell'equazione omogenea

$$\sum_{j=1}^{p^{n-1}} X_j = 0$$

La condizione che $f \in \mathcal{C}_2$ si esprime nell'equazione non omogenea

$$\sum_{j=1}^{p^{n-1}} X_j = \sum_{j=1}^{p^{n-1}} (\sigma_{n-1})_j$$

Se $1 \leq m < p^{n-2}$ allora il numero delle soluzioni in $\mathcal{C}_1$ e in $\mathcal{C}_2$ è lo stesso per il teorema di Rouchè-Capelli, se $m = p^{n-2}$ in $\mathcal{C}_2$ non ho soluzioni, mentre in $\mathcal{C}_1$ ho almeno la soluzione σ_i.

Teorema 5.2 *Sia $p \neq 2$ allora in P_{p^n} ci sono $2^n - 1$ massimali a meno di isomorfismo.*

Dimostrazione: Proviamolo per induzione su n. A meno di isomorfismo ci sono $2^{n-1} - 1$ massimali che contengono la base per ipotesi induttiva. Se i massimali non contengono la base allora il risultato segue dalle osservazioni fatte finora e dal lemma 5.4.

Capitolo 6

Stime asintotiche

Definizione 6.1 *Un gruppo G si dice indecomponibile se non esistono due sottogruppi propri non banali tali che G ne sia il prodotto diretto.*

Teorema 6.1 (Krull-Remak-Schmidt) *Sia G un gruppo finito e siano*

$$G = G_1 \times \cdots \times G_r = H_1 \times \cdots \times H_s$$

due decomposizioni di G in prodotto diretto di gruppi indecomponibili G_i, H_i non banali, allora $r = s$ e a meno di un riordino degli indici $G_i \cong H_i$.

Dimostrazione: Omessa (si veda ad esempio B.HUPPERT [2]).

Diamo il seguente
Esempio. È utile osservare che se A e B sono due gruppi indecomponibili e $C \leq A \times B$ allora in generale C non è isomorfo ad un prodotto diretto di sottogruppi di A e di B. Si consideri:
$G_1 = \langle a_1, b_1 |\ a_1^{p^2} = b_1^p = 1,\ b_1^{-1} a_1 b_1 = a_1^{p+1} \rangle$
$G_2 = \langle a_2, b_2 |\ a_2^{p^2} = b_2^p = 1,\ b_2^{-1} a_2 b_2 = a_2^{p+1} \rangle$
e $H = \langle (a_1, b_2), (1, a_2) \rangle_{G_1 \times G_2}$
Supponiamo per assurdo che H sia il prodotto diretto di sottogruppi di G_1 e di G_2. È facile verificare che $|H| = p^4$ e che H non è abeliano. Dunque $H \cong G_1 \times C_p$. Questo è impossibile perchè otterremo $H^p \cong G_1^p \times 1$, ma $(a_1^p, 1),\ (1, a_2^p) \in H^p$ e $G_1^p \cong C_p$.

Lemma 6.1 *In P_{p^2} ci sono $2p$ gruppi indecomponibili a meno di isomorfismo.*

Dimostrazione: Riprendiamo le notazioni del capitolo 4. Basterà verificare che se G è uno dei seguenti gruppi

$$\langle \sigma \rangle A_i^1 \ \text{ per } i = 0, \cdots, p-2 \quad \text{oppure} \quad \langle \sigma e_1 \rangle A_i^1 \ \text{ per } i = 1, \cdots, p-2$$

allora $|Z(G)| = p$.
$[\sigma^j f, g] = 1$ per ogni $g \in A_i^1$ se e solo se $g^{\sigma^j} = g$ per ogni $g \in A_i^1$, se e solo se $j = 0$. Quindi $Z(G) \leq G \cap A^1$.
Se $[f, \sigma] = 1$ allora $f \in Z(P_{p^2})$, da cui la tesi.

$P_{p^n} = P_{p^2} Wr_X P_{p^{n-2}}$, dunque P_{p^n} contiene un sottogruppo isomorfo al prodotto diretto di p^{n-2} copie di P_{p^2}. Pertanto detti

$$\{G_i\}_{i=1}^{2p-2} = \{C_{p^2}\} \cup \{\langle\sigma\rangle A_j^1\}_{j=0}^{p-2} \cup \{\langle\sigma e_1\rangle A_j^1\}_{j=1}^{p-2}$$

abbiamo che

$$\{G_{i_1} \times G_{i_2} \times \cdots \times G_{i_k} \times \underbrace{C_p \times \cdots \times C_p}_{l \text{ volte}} \mid l = 0, \cdots, (p^{n-2} - k)p\}$$

è una famiglia di sottogruppi di $\overbrace{P_{p^2} \times \cdots \times P_{p^2}}^{p^{n-2} \text{ volte}}$ a due a due non isomorfi. In sostanza, fissato k un naturale compreso tra 0 e p^{n-2} abbiamo occupato k fattori del prodotto diretto con sottogruppi indecomponibili di P_{p^2} diversi da C_p e dall'identità, i restanti $p^{n-2} - k$ fattori si possono occupare con un qualsiasi gruppo abeliano elementare di dimensione compresa tra 0 e $p^{n-1} - kp^{n-2}$. Per contare tale famiglia ricordiamo che il numero di liste non ordinate di n oggetti di lunghezza k è $\binom{n+k-1}{k}$ (sono le combinazioni con ripetizioni di n oggetti presi a k a k). Inoltre tramite una semplice induzione si può verificare che

$$\sum_{i=0}^{k} \binom{n+i-1}{i} = \binom{n+k}{k} \quad \text{e che} \quad \sum_{i=0}^{k} i\binom{n+i-1}{i} = n\binom{n+k}{k-1}$$

Dunque abbiamo almeno

$$\begin{aligned}
\sum_{k=0}^{p^{n-2}} (p^{n-1} - kp + 1)\binom{k-1+2p-2}{k} &= \\
(p^{n-1}+1)\left(\sum_{k=0}^{p^{n-2}} \binom{k-1+2p-2}{k}\right) - p\left(\sum_{k=0}^{p^{n-2}} \binom{k-1+2p-2}{k}\right) &= \\
(p^{n-1}+1)\binom{p^{n-2}+2p-2}{p^{n-2}} - (2p^2-2p)\binom{p^{n-2}+2p-2}{p^{n-2}-1} &= \\
\binom{p^{n-2}+2p-2}{p^{n-2}-1}\left(\frac{p^{n-1}+2p-1}{p^{n-2}}\right) \quad (*)
\end{aligned}$$

sottogruppi a meno di isomorfismo.

Teorema 6.2 (Formula di Stirling) *La funzione $N!$ è asintotica ad infinito a*

$$\sqrt{2\pi N}\left(\frac{N}{e}\right)^N.$$

Dimostrazione: Omessa (si veda ad esempio il riferimento [7]).

Grazie al teorema precedete si ottiene che

$$\binom{p^{n-2}+2p-2}{p^{n-2}-1}\left(\frac{p^{n-1}+2p-1}{p^{n-2}}\right) \geq \frac{\overbrace{(p^{n-2}+2p-2)\cdots(p^{n-2}+1)}^{2p-2 \text{ prodotti}}}{(2p-1)!}p^{n-1} \geq$$

$$\geq \frac{2p^{2(p-1)(n-2)+n}}{(2p)!} \sim \frac{2p^{2(p-1)(n-2)+n}}{\sqrt{2\pi(2p)}\left(\frac{2p}{e}\right)^{2p}} = \frac{1}{\sqrt{\pi}}p^{2(p-1)(n-2)+n-2p-1/2+2p\ln_p\frac{e}{2}} \geq$$

$$\geq \frac{1}{\sqrt{\pi}}p^{2(p-1)(n-2)+n-2p-1/2+2p\frac{\ln\frac{e}{2}}{p}} \geq \frac{1}{\sqrt{\pi}}p^{2(p-1)(n-2)+n-2p} = \frac{1}{\sqrt{\pi}}p^{(2p-1)(n-3)+1}$$

per n e p sufficientemente grandi.

Cerchiamo di migliorare la stima precedente coinvolgendo nel conto alcuni sottogruppi indecomponibili di P_{p^m}, per $2 \leq m \leq n$. Per fare questo usiamo alcuni lemmi sui sottogruppi abeliani elementari massimali. Il risultato che si otterà sarà valido per $p \neq 2$, mentre $(*)$ vale per qualsiasi primo.

Lemma 6.2 $\binom{a}{k} \equiv \binom{pa}{pk} mod(p\mathbb{Z})$ *e* $\binom{a-1}{k} \equiv \binom{pa-1}{pk} mod(p\mathbb{Z})$ *per ogni* a, k *naturali.*

Dimostrazione: In $\mathbb{Z}/p\mathbb{Z}[x]$ elevare alla potenza p-esima è un omomorfismo, dunque $(x^p+1)^a = \sum_{k=0}^{a}\binom{a}{k}x^{pk} = (x+1)^{pa} = \sum_{s=0}^{pa}\binom{pa}{s}x^s$. Se $s = pk$ otteniamo $\binom{a}{k} \equiv \binom{pa}{pk} \mathrm{mod}(p\mathbb{Z})$, per il principio di identità dei polinomi. L'altra affermazione è ora immediata.

Lemma 6.3 *Sia* $G \leq P_{p^{n-1}}$ *tale che* $\{\tau \in G |\ [\tau^\eta, \tau] = 1\ \forall \eta \in G\} \leq A^{n-2}$. *Se* $0 \leq i \leq p^{n-1} - 2p^{n-2} - 1$, *allora ogni sottogruppo normale abeliano di* GA_i^{n-1} *è contenuto in* A_i^{n-1}.

Dimostrazione: Fissiamo $t = p^{n-1} - 2p^{n-2} - 1$. Sia $H \trianglelefteq GA_i^{n-1}$, H abeliano e sia $\sigma f \in H$ con $\sigma \in G$ e $f \in A_i^{n-1}$. Se $[(\sigma f)^\eta, \sigma f] = 1$ per ogni $\eta \in G$, allora $[\sigma^\eta, \sigma] = 1$ per ogni $\eta \in G$. Quindi, per l'ipotesi nell'enunciato, $H \leq A^{n-2}A_i^{n-1}$. Se $[(\sigma f)^g, \sigma f] = 1$ per ogni $g \in A_i^{n-1}$, allora $[g, \sigma, \sigma] = 1$ per ogni $g \in A_i^{n-1}$. Notiamo che se x è un qualsiasi p^{n-1}-ciclo di $P_{p^{n-1}}$ e

se $x^{p^{n-2}} = \sigma_1\sigma_2\cdots\sigma_{p^{n-2}}$, con σ_i p-cicli a due a due disgiunti, allora $A^{n-2} = \langle \sigma_i |\ i = 1, \cdots, p^{n-2}\rangle$. Dunque $\sigma = \sigma_{i_1}^{k_1}\sigma_{i_2}^{k_2}\cdots\sigma_{i_l}^{k_l}$, con $i_j \in \{1, \cdots, p^{n-2}\}$ e $1 \leq k_j < p-1$. Non è restrittivo supporre che $x = (1\ 2\ \cdots\ p^{n-1})$.
Sia $\mathfrak{E} = \{e_i\}_{i=1}^{p^{n-1}}$ una base di A^{n-1} tale che $e_i^x = e_{i+1}$ e poniamo $g = g_{i_1}\cdots g_{i_l}h$ tramite la seguente definizione

$$g_{i_j}(s) = \begin{cases} 1 & \text{se } s^{\sigma_{i_j}} = s \\ g(s) & \text{se } s^{\sigma_{i_j}} \neq s \end{cases}$$

$$h(s) = \begin{cases} 1 & \text{se } s^{\sigma_{i_j}} \neq s \\ g(s) & \text{se } s^{\sigma_{i_j}} = s \end{cases}$$

Insomma, le coordinate di g_{i_j} nella base $\mathfrak{E}$ sono uguali a 1 se σ_{i_j} agisce banalmente, altrimenti coincidono con le coordinate di g.
È facile verificare che

$$[g,\sigma] = [g_{i_1}, \sigma_{i_1}^{k_1}]\cdots[g_{i_l}, \sigma_{i_l}^{k_l}] \ \text{ e } \ [g,\sigma,\sigma] = [g_{i_1}, \sigma_{i_1}^{k_1}, \sigma_{i_1}^{k_1}]\cdots[g_{i_l}, \sigma_{i_l}^{k_l}, \sigma_{i_l}^{k_l}].$$

Per $j_1 \neq j_2$, $[g_{i_{j_1}}, \sigma_{i_{j_1}}^{k_{j_1}}, \sigma_{i_{j_1}}^{k_{j_1}}]$ e $[g_{i_{j_2}}, \sigma_{i_{j_2}}^{k_{j_2}}, \sigma_{i_{j_2}}^{k_{j_2}}]$ hanno supporto disgiunto; dunque $[g,\sigma,\sigma] = 1$ se e solo se $[g_{i_j}, \sigma_{i_j}^{k_j}, \sigma_{i_j}^{k_j}] = 1$ per ogni j. Sia

$$y = [e_1, \underbrace{x, \cdots, x}_{t \text{ volte}}] = e_1^{(x-1)^t} = \prod_{s=0}^{t}(e_{s+1})^{(-1)^{(t-s)}\binom{t}{s}} \in A_t^{n-1}$$

e

$$y_i(s) = \begin{cases} 1 & \text{se } s^{\sigma_i} = s \\ y(s) & \text{se } s^{\sigma_i} \neq s \end{cases}$$

Proviamo che se $[y_1, \sigma_1^{k_1}, \sigma_1^{k_1}] = 1$ allora $k_1 = 0$, il ragionamento è poi lo stesso per ogni y_i. Ricordiamo che $\sigma_1 = (1\ \ (p^{n-2}+1)\ \cdots\ ((p-1)p^{n-2}+1))$. Consideriamo $P_{p^2} = \langle\tau\rangle A^1$, con $\tau = (1\ 2\ \cdots\ p)$. Sia $\mathfrak{F} = \{f_1,\ \cdots,\ f_p\}$ una base di A^1 tale che $f_i^\tau = f_{i+1}$ e sia

$$z = f_1^{(\tau-1)^{p-3}} = \prod_{k=0}^{p-3} f_{k+1}^{(-1)^{(p-3-k)}\binom{p-3}{k}} \in A_{p-3}^1 \backslash A_{p-2}^1.$$

Allora la $k+1$-esima coordinata di z coincide con la $kp^{n-2}+1$-esima coordinata di y_1.

$$z(k+1) = y_1(kp^{n-2}+1) \qquad \text{per ogni } k = 0, \cdots, p-1$$

Infatti è facile verificare che $(-1)^{t-kp^{n-2}} = (-1)^{p-3-k}$, e dal lemma 6.2

$$\binom{p^{n-1}-2p^{n-2}-1}{p^{n-2}k} = \binom{p-3}{k}.$$

Per concludere basta notare che l'azione di $\sigma_1^{k_1}$ su y_1 coincide con l'azione che τ^{k_1} ha su z. Dunque $[y_1, \sigma_1^{k_1}, \sigma_1^{k_1}] = 1$ se e solo se $[z, \tau^{k_1}, \tau^{k_1}] = 1$. Se $k_1 \neq 1$ allora $[z, \tau^{k_1}, \tau^{k_1}] \in A_{p-1}^1 \backslash A_p^1 = A_{p-1}^1 \backslash 1$, da cui la tesi.

Osservazione. Siano $G_1 A_i^{n-1}$ e $G_2 A_j^{n-1}$ due sottogruppi di P_{p^n} come nel lemma precedente. Se $G_1 A_i^{n-1} \cong G_2 A_j^{n-1}$ allora $i = j$ e $G_1 \cong G_2$.

Lemma 6.4 *Sia G un sottogruppo di $P_{p^{n-1}}$ tale che $Z(G) = Z(P_{p^{n-1}})$, allora $Z(GA_i^{n-1}) = Z(P_{p^n})$, per $0 \leq i \leq p^{n-1} - 2p^{n-2} - 1$.*

Dimostrazione: Fissiamo $t = p^{n-1} - 2p^{n-2} - 1$. Se $\sigma f \in Z(GA_i^{n-1})$ allora $\sigma \in Z(G) = Z(P_{p^{n-1}})$ e $(\sigma f)^g = \sigma f$ per ogni $g \in A_i^{n-1}$. Allora $g^\sigma = g$ per ogni $g \in A_t^{n-1}$.
Supponiamo per assurdo che $\sigma \neq 1$ allora esiste x p^{n-1}-ciclo di $P_{p^{n-1}}$ tale che $x^{p^{n-2}} = \sigma$ e, come al solito, non è restrittivo suppore che $x = (1\ 2\ \cdots\ p^{n-1})$. Utilizzando le medesime notazioni introdotte nella dimostrazione della proposizione 2.1 abbiamo che $A_t^{n-1} = \langle y_t, \cdots, y_{p^{n-1}-1} \rangle$. Ovviamente $y_t^\sigma \neq y_t$ perchè esiste j tale che $y_t(j) \neq 1$ e $y_t^\sigma(j) = 1$. Per l'esistenza di tale j basta rileggere la dimostrazione del lemma 6.3.

Osservazione. Se G è un sottogruppo di $P_{p^{n-1}}$ tale che $Z(G) = Z(P_{p^{n-1}})$ allora GA_i^{n-1} è un gruppo indecomponibile per $0 \leq i \leq p^{n-1} - 2p^{n-2} - 1$.

Lemma 6.5 *Sia $G \leq P_{p^{n-1}}$ tale che $\{\tau \in G |\ [\tau^\eta, \tau] = 1\ \forall \eta \in G\} \leq A^{n-2}$. Se $0 \leq i \leq p^{n-1} - 2p^{n-2} - 1$, allora $\{\sigma f \in GA_i^{n-1} |\ [(\sigma f)^{\tau g}, \sigma f] = 1\ \tau g \in GA_i^{n-1}\} \leq A^{n-1}$.*

Dimostrazione: Se $[(\sigma f)^\tau, \sigma f] = 1$ per ogni $\tau \in G$ allora $\sigma \in A^{n-2}$. Se $[(\sigma f)^g, \sigma f] = 1$ per ogni $g \in A_i^{n-1}$ allora $[g, \sigma, \sigma] = 1$ per ogni $g \in A_i^{n-1}$. Seguendo la dimostrazione del lemma 6.3 si ottiene che $\sigma = 1$, da cui la tesi.

Osservazione. Il lemma 6.5 prova che se G è un sottogruppo di $P_{p^{n-1}}$ tale che ogni sottogruppo normale abeliano sia contenuto nella base allora GA_i^{n-1} gode della medesima proprietà, per $0 \leq i \leq p^{n-1} - 2p^{n-2} - 1$.

Lemma 6.6 *A meno di isomorfimo in P_{p^2} ci sono $2p - 5$ sottogruppi G per cui $Z(G) = Z(P_{p^2})$, e tali che ogni sottogruppo normale abeliano sia contenuto nella base.*

Dimostrazione: Basterà verificare che i gruppi $\langle \sigma \rangle A_i^1$, per $0 \leq i \leq p-3$, e $\langle \sigma e_1 \rangle A_i^1$, per $1 \leq i \leq p-3$, godono delle proprietà richieste. Ovviamente tali gruppi sono non abeliani e $Z(G) = Z(P_{p^2})$. Se $[(\sigma f)^g, \sigma f] = 1$ per ogni $g \in A_i^1$ allora $[g, \sigma, \sigma] = 1$, dunque $i \geq p - 2$.

In P_{p^2} ci sono $2p-2$ sottogruppi indecomponibili non contenuti in P_p, tra questi ce ne sono $2p-5$ che si estendono a sottogruppi indecomponibili di P_{p^3} moltiplicandoli con A_i^2, per $i = 0, \cdots, p^2-2p-1$. Dunque in P_{p^3} ci sono almeno $(2p-5)p(p-2)$ gruppi indecomponibili. È facile verificare che se x è un p^2-ciclo di P_{p^2} allora i gruppi $\langle x \rangle A_i^2$, per $0 \leq i \leq p^2-2p-1$, contengono un unico sottogruppo normale abeliano massimale. Inoltre tali gruppi sono indecomponibili e non sono isomorfi a nessun sottogruppo precedente. Insomma in P_{p^3} ci sono almeno $(2p-5)p(p-2) + p(p-2) = 2(p-2)^2 p$ gruppi indecomponibili a meno di isomorfismo. Tramite una semplice induzione si può verificare che in P_{p^n} ci sono almeno $2p^{\binom{n-1}{2}}(p-2)^{n-1}$ sottogruppi indecomponibili. Notiamo che $P_{p^n} = P_{p^{n-1}} \wr P_p$, dunque P_{p^n} contiene un sottogruppo massimale isomorfo al prodotto diretto di p copie di $P_{p^{n-1}}$. Se $\{G_i\}_i$ è l'insieme dei sottogruppi indecomponibili di $P_{p^{n-1}}$ allora per il teorema 6.1 la famiglia

$$\{G_1 \times \cdots \times G_k \times \underbrace{C_p \times \cdots \times C_p}_{l \text{ volte}} \mid 0 \leq i \leq 2(p-2)^{n-2} p^{\binom{n-2}{2}},\ 0 \leq l \leq p^{n-2}(p-k)\}$$

è formata da gruppi a due a due non isomorfi. Ripetendo il medesimo ragionamento fatto per $(*)$ otteniamo la seguente stima sui sottogruppi di P_{p^n}

$$\sum_{k=0}^{p} (p^{n-1} - kp^{n-2} + 1) \binom{2(p-2)^{n-2} p^{\binom{n-2}{2}} + k - 1}{k} =$$

$$(p^{n-1}+1)\left(\sum_{k=0}^{p} \binom{2(p-2)^{n-2} p^{\binom{n-2}{2}} + k - 1}{k} \right) -$$

$$-p^{n-2}\left(\sum_{k=0}^{p} \binom{2(p-2)^{n-2} p^{\binom{n-2}{2}} + k - 1}{k} \right) =$$

$$(p^{n-1}+1)\binom{2(p-2)^{n-2} p^{\binom{n-2}{2}} + p}{p} -$$

$$-p^{n-2} 2(p-2)^{n-2} p^{\binom{n-2}{2}} \binom{2(p-2)^{n-2} p^{\binom{n-2}{2}} + p}{p-1} =$$

$$\binom{2(p-2)^{n-2} p^{\binom{n-2}{2}} + p}{p-1} \left(\frac{2(p-2)^{n-2} p^{\binom{n-2}{2}} + p^{n-1} + 1}{p} \right) \qquad (**)$$

Osserviamo che la stima in esame è il prodotto di un coefficiente binomiale e di una funzione razionale in p. È facile verificare che la funzione razionale è

asintotica a $p^{\frac{n(n-3)}{2}}$, mentre per il coefficiente binomiale non abbiamo alcuna stima esatta. Usando la formula di Stirling vista nel teorema 6.2 otteniamo

$$\binom{2(p-2)^{n-2}p^{\binom{n-2}{2}}+p}{p-1}\left(\frac{2(p-2)^{n-2}p^{\binom{n-2}{2}}+p^{n-1}+1}{p}\right)\geq$$

$$\geq \frac{\overbrace{(2(p-2)^{n-2}p^{\binom{n-2}{2}}+p)\cdots(2(p-2)^{n-2}p^{\binom{n-2}{2}}+2)}^{p-1 \text{ prodotti}}}{p!}2(p-2)^{n-2}p^{\binom{n-2}{2}}\geq$$

$$\geq \frac{2^p(p-2)^{p(n-2)}p^{p\binom{n-2}{2}}}{p!}\sim\frac{2^pp^{p\binom{n-1}{2}}}{p!}\sim\frac{2^pp^{p\binom{n-1}{2}}}{\sqrt{2\pi p}\left(\frac{p}{e}\right)^p}=\frac{(2e)^p}{\sqrt{2\pi}}p^{p\binom{n-1}{2}-p-1/2}=$$

$$=\frac{(2e)^p}{\sqrt{2\pi}}p^{p\frac{n(n-3)}{2}-1/2}=\frac{1}{\sqrt{2\pi}}p^{p\frac{n(n-3)}{2}+p\frac{\ln 2e}{\ln p}-1/2}\geq\frac{1}{\sqrt{2\pi}}p^{p\frac{n(n-3)}{2}+1}$$

per n e p sufficientemente grandi.
Quindi la stima $(**)$ è migliore della stima $(*)$, per n grande.

$$\frac{1}{\sqrt{\pi}}p^{(2p-1)(n-3)+1}\lll\frac{1}{\sqrt{2\pi}}p^{p\frac{n(n-3)}{2}+1}$$

Concludiamo il capitolo mettendo in confronto l'ordine di grandezza delle approssimazioni delle stime $(*)$ e $(**)$ per $p=5$ e $p=7$.

p=5	stima		p=7	stima	
	$(*)$	$(**)$		$(*)$	$(**)$
n=3	0	0	n=3	0	0
n=4	10^6	10^7	n=4	10^{11}	10^{12}
n=5	10^{13}	10^{17}	n=5	10^{22}	10^{30}
n=6	10^{19}	10^{31}	n=6	10^{33}	10^{53}
n=7	10^{25}	10^{49}	n=7	10^{44}	10^{81}
n=8	10^{31}	10^{70}	n=8	10^{55}	10^{118}
n=9	10^{38}	10^{94}	n=9	10^{66}	10^{160}
n=10	10^{44}	10^{122}	n=10	10^{77}	10^{207}

Bibliografia

[1] F.GROSS: Automorphism of Permutational Wreath Products, Journal of Algebra vol.117(1988) pp472-493

[2] B.HUPPERT: Endliche Gruppen I, Springer-Verlag Berlin Heidelberg New York (1967)

[3] B.HUPPERT-N.BLACKBURN: Finite Groups II, Springer-Verlag Berlin Heidelberg New York (1982)

[4] L.KALOUJNINE: La structure des p-groupes de Sylow des groupes simétriques finis, Ann.École.Norm.(3) vol.65(1948) pp239-276

[5] P.LENTOUDIS: Determination du groupe des automorphismes du p-groupes de Sylow du groupe symétrique de degreé p^m: l'idéede la méthod, C.R.Math.Rep.Acad.Sci.Canada vol.7(1985) pp67-71, Errata: p325

[6] P.LENTOUDIS: Determination du groupe des automorphismes du p-groupes de Sylow du groupe symétrique de degreé p^m: résultats, C.R.Math.Rep.Acad.Sci.Canada vol.7(1985) pp133-136

[7] D.S.MITRINOVIC-J.SANDOR-B.CRSTICI: Handbook of number theory

[8] M.SUZUKI: Group Theory II, Springer-Verlag Berlin Heidelberg Tokyo (1986)

[9] A.J.WEIR: The Sylow subgroup of the symmetric group, Proc.Amer.Soc vol.6(1955) pp534-541