

Centro de Ciências Exatas
Universidade Estadual de Maringá
Programa de Pós-Graduação em Matemática
(Mestrado)

Uma Generalização do Critério de Solubilidade de Thompson

por Laerte Bemm

Orientadora: Prof.^a Dr.^a Irene Naomi Nakaoka

Maringá - PR

2008

Livros Grátis

<http://www.livrosgratis.com.br>

Milhares de livros grátis para download.

Centro de Ciências Exatas
Universidade Estadual de Maringá
Programa de Pós-Graduação em Matemática
(Mestrado)

Uma Generalização do Critério de Solubilidade de Thompson

por Laerte Bemm

Orientadora: Prof.^a Dr.^a Irene Naomi Nakaoka

Maringá - PR

2008

Dedico este trabalho a Deus

Agradecimentos

Quero manifestar aqui minha sincera gratidão a todas as pessoas que de alguma forma me ajudaram a conquistar mais essa vitória, dentre a quais destaco:

- a meus pais Cacildo e Terezinha, por sempre estarem do meu lado e por nunca terem podado “minhas asas” e o meu sonho de conseguir, mesmo que em lugares distantes, meu diploma de graduação e certificado de mestre;
- a minhas tias Eusébia e Eli, a minha avó Gisela, a minha prima Cleidi e a meu irmão Charles pela torcida, pelas rezas para que esse dia chagasse;
- aos meus amigos do peito Waldir, Flávio, Rodrigo e Robson por terem dividido comigo não apenas o teto, mas também as angústias e alegrias que o curso nos proporcionou;
- a minha orientadora, Prof^a Irene, pela coragem de me orientar, pelos incentivos constantes, pela escolha do tema e, principalmente, pela excelente orientação;
- a minha namorada Priscila, pela paciência, compreensão e, especialmente, por ter suportado meu stress no últimos meses;

Finalmente, quero agradecer ao departamento de Matemática da UEM pela oportunidade de estudar e a CAPES pelo incentivo financeiro.

Resumo

Um resultado conhecido da Teoria de Grupos, devido a J. Thompson, diz que se um subgrupo maximal de um grupo finito G é nilpotente de ordem ímpar, então G é solúvel. Neste trabalho, apresentamos uma generalização deste resultado, devido a Y. Wang, o qual estabelece que se G é um grupo finito, A é um grupo $\pi(G)$ -solúvel agindo sobre G por automorfismos e existe um subgrupo A -invariante maximal M de G tal que M é nilpotente e o 2-subgrupo de Sylow de M não possui grupo quociente isomorfo ao grupo diedral de ordem 8, então G é solúvel.

Abstract

A known result of Theory of Groups, due to J. Thompson, establishes that if a maximal subgroup of a finite group G is nilpotent of odd order, then G is soluble. In this work, we study a generalization of this result, due to Y. Wang, which states that if G is a finite group, A is a $\pi(G)$ -solvable group that acts on G by automorphism and there is a nilpotent maximal A -invariant subgroup M of G such that M does not has quotient group isomorphic to the dihedral group of order 8, then G is solvable.

Índice de Notações

\emptyset	conjunto vazio.
Imf	imagem do conjunto A pela f .
(m, n)	máximo divisor comum entre m e n .
$[x, y]$	$x^{-1}y^{-1}xy$
$\langle X \rangle$	subgrupo gerado por X .
$[X, Y]$	$\langle [x, y] : x \in X \text{ e } y \in Y \rangle$
$\gamma_n(G)$	n -ésimo termo da série central inferior de G .
$\Phi(G)$	subgrupo de Frattini de G .
$\xi_n(G)$	n -ésimo termo da série central superior de G .
\mathbb{Z}	conjunto dos números inteiros.
\mathbb{Z}_n	$\frac{\mathbb{Z}}{n\mathbb{Z}}$.
$ A $	cardinalidade do conjunto A .
$J(P)$	subgrupo de Thompson de P .
$K \times H$	produto direto de K por H .
$N_G(H)$	normalizador de H em G .
$O_\pi(G)$	π -subgrupo normal maximal de G .
$SL(2, 3)$	$\{A \in GL(2, \mathbb{Z}_3) \mid \det A = 1\}$.
$Sym(S)$	grupo simétrico do conjunto S .
$ G : H $	índice do subgrupo H em G .
$\circ(x)$	ordem do elemento x .
$A \subset B$	A é um subconjunto próprio de B .
$A \subseteq B$	A é um subconjunto de B .
$H \leq G$	H é um subgrupo de G .

$Aut(G)$	grupo de automorfismos de G .
$C_G(H)$	centralizador de H em G .
$C_G(\phi)$	$\{x \in G : \phi(x) = x\}$, onde $\phi \in Aut(G)$
$dim_F V$	dimensão de V sobre F .
$stab(i)$	estabilizador da letra i .
G'	subgrupo derivado de G .
$G^{(n)}$	n -ésimo termo da série derivada de G .
$\frac{G}{H}, G/H$	grupo quociente de G por um subgrupo normal H .
$GF(p^n)$	corpo finito com p^n elementos.
$GL(n, F)$	grupo das matrizes não singulares sobre F .
$GL(V F)$	grupo dos operadores lineares não singulares de $V F$.
$H \triangleleft G$	H é um subgrupo normal de G .
$H \text{ char } G$	H é um subgrupo característico de G .
$H \rtimes K$	produto semi-direto de K por H .
H^x	$\{x^{-1}hx : h \in H\}$.
Hx	$\{hx : h \in H\}$.
$V F$	V é um espaço vetorial sobre F .
x^y	$y^{-1}xy$.
XY	$\{xy : x \in X \text{ e } y \in Y\}$.
yHx	$\{yhx : h \in H\}$.
$Z(G)$	centro de G .
D_n	grupo diedral de ordem n .
$\pi(G)$	conjunto dos divisores primos de $ G $.
$Mat(n, F)$	conjunto das matrizes $n \times n$ com entradas em F .
$tr(M)$	traço da matriz M .
$ch(G)$	anel caracter de G .
X^Y	$\{x^y : x \in X, y \in Y\}$.
$H \wr G$	produto entrelaçado de H por G .
H_G	interseção de todos os conjugados de H .
S_p	p -subgrupo de Sylow

Sumário

Introdução	1
1 Resultados Preliminares	3
1.1 Subgrupo Comutador e Subgrupos Característicos	3
1.2 Grupos Solúveis e Nilpotentes	6
1.3 Apresentação de Grupos	10
1.4 Produto Semi-Direto	12
1.5 Grupo de Frobenius	13
1.6 Representações de Grupos	15
1.7 Grupo Linear $GL(2, q)$	18
2 π-Separabilidade	20
2.1 O Teorema de Schur-Zassenhaus	22
2.2 Grupos π -Separáveis	28
3 p-Estabilidade	36
3.1 Grupos p -Estáveis	36
3.2 p -Estabilidade em Grupos p -Solúveis	47
4 Os Teoremas de Glauberman-Thompson	53
4.1 Subgrupo de Thompson	54
4.2 Grupos p -Nilpotentes	66
5 p-Singularidades	72

5.1	Caracteres	73
5.2	Transfer de Caracter	77
5.3	Singularidades	85
6	O Critério de Solubilidade de Wang	97
6.1	Teorema de Wang	97
	Bibliografia	103
	Referências Bibliográficas	104

Introdução

Uma classe de grupos que vem sendo intensamente estudada ao longo dos anos é a dos *grupos solúveis*. Tais grupos foram e, ainda são, alvos de pesquisa de matemáticos do mundo inteiro, dentre os quais destacamos P. Hall, J. Thompson, Z. Janko e O. J. Schmidt. Descobrir propriedades destes grupos e condições suficientes para um grupo ser solúvel, são alguns dos tópicos pesquisados por estes matemáticos e que continuam a render excelentes trabalhos na área de Álgebra.

O. J. Schmidt provou que se todos os subgrupos maximais de um grupo finito G são nilpotentes, então G é solúvel. Alguns anos mais tarde, J. Thompson mostrou que para obter-se a conclusão de Schmidt, é suficiente que o grupo G possua um subgrupo maximal nilpotente de ordem ímpar.

Em seguida, Z. Janko mostrou que um grupo finito G é solúvel se contém um subgrupo maximal M nilpotente com 2-subgrupo de Sylow de classe de nilpotência no máximo 2.

Num trabalho publicado em 1998, [10], Y. Wang demonstrou o seguinte:

Teorema. *Seja G um grupo finito e A um grupo agindo por automorfismos sobre G . Suponhamos que A é $\pi(G)$ -solúvel. Se existe um subgrupo A -invariante maximal nilpotente M de G tal que o 2-subgrupo de Sylow de M não possui grupo quociente isomorfo a D_8 , então G é solúvel.*

O objetivo deste trabalho é apresentar a demonstração do Teorema de Wang, constante no Capítulo 6. Nos cinco capítulos anteriores, encontram-se a maioria dos conceitos e resultados necessários para um bom entendimento desta e das demais demonstrações estabelecidas no Capítulo 6.

No primeiro capítulo, apresentamos alguns requisitos mínimos para o desenvolvimento

deste trabalho, tais como: subgrupos comutadores e característicos, grupos solúveis e nilpotentes, grupos livres, grupo de Frobenius, produto semi-direto, representações de grupos e propriedades do grupo linear $GL(2, q)$.

No Capítulo 2, expomos, primeiramente, a demonstração do Teorema de Schur-Zassenhaus, que fornece uma condição suficiente para a existência e conjugação de π -subgrupos de Hall. Na sequência, introduzimos as definições e algumas propriedades dos grupos π -separáveis e π -solúveis, onde π é um conjunto não vazio de primos.

Em seguida, no Capítulo 3, estudamos um assunto pouco abordado na literatura matemática. Trata-se dos chamados *grupos p -estáveis*, onde p é um primo. O objetivo primeiro é estabelecer condições suficientes para um grupo finito ser p -estável, através do Teorema 3.6, para que na sequência possamos obter propriedades dos grupos fortemente p -solúveis, onde p é um primo.

No início do Capítulo 4, apresentamos a construção do chamado subgrupo de Thompson e obtemos algumas de suas propriedades. Como veremos, o normalizador do centro de tal subgrupo desempenha o papel de “protagonista” no Teorema da p -Nilpotência de Glauberman-Thompson, que nos dá uma condição suficiente para que um grupo finito seja p -nilpotente. Para finalizar o capítulo, vamos demonstrar o Teorema de Thompson.

Com a teoria estabelecida nos Capítulos 1, 2, 3 e 4, é possível demonstrarmos o Teorema de Wang, desde que 2 não divida $|M|$. Se 2 divide $|M|$, precisamos recorrer ao Teorema de T. Yoshida, que diz o seguinte:

Teorema *Se P é um S_p -subgrupo de um grupo finito G que não possui grupo quociente isomorfo a $\mathbb{Z}_p \wr \mathbb{Z}_p$, então $P \cap G' = P \cap N_G(P)'$.*

Como a demonstração do Teorema de Yoshida envolve o conceito de p -singularidade em um grupo, onde p é um primo, dedicamos o Capítulo 5 ao estudo de transfer de caracter e p -singularidades.

Finalmente, no Capítulo 6, demonstramos o Teorema de Wang e concluimos o trabalho com um exemplo, onde mostramos que existe um grupo solúvel que não possui um subgrupo maximal nilpotente, mas tem um subgrupo A -invariante maximal nilpotente, para um grupo A conveniente.

Capítulo 1

Resultados Preliminares

Neste primeiro capítulo vamos estabelecer alguns conceitos e resultados da Teoria de Grupos que nos serão úteis para o desenvolvimento do trabalho. Em geral não apresentamos as demonstrações destes resultados, mas tomamos o cuidado de sempre indicar uma bibliografia na qual o leitor interessado poderá obtê-las. Esperamos que o leitor domine tópicos básicos da Teoria de Grupos e Teoria de Módulos. Observamos que as notações aqui usadas são as clássicas e encontradas na maioria dos livros relacionados a grupos. Caso o leitor tenha dúvidas quanto a isso, basta consultar nosso índice de notação no início do trabalho.

1.1 Subgrupo Comutador e Subgrupos Característicos

Neste primeiro capítulo, convencionamos que G sempre denotará um grupo arbitrário, a menos que se mencione o contrário. A notação $X \subset Y$ significa que X é um subconjunto próprio de Y , enquanto que $X \subseteq Y$ significa que X é um subconjunto de Y . Usamos a notação $H \leq G$ para indicar que H é um subgrupo de G .

Se $a, b \in G$, o conjugado $b^{-1}ab$ é escrito a^b e o elemento $a^{-1}b^{-1}ab$ é chamado de *comutador* de a e b e denotado por $[a, b]$. O subgrupo de G gerado por todos os comutadores é chamado *subgrupo comutador* ou *subgrupo derivado* de G e denotado por G' .

Tal subgrupo tem sua importância, pois através dele é possível determinar quando um grupo quociente é abeliano, como mostra a

Proposição 1.1 ([6], pág. 33) *O subgrupo comutador G' de G é normal em G . Além disso, se $H \triangleleft G$, então $\frac{G}{H}$ é abeliano se, e somente se, $G' \leq H$.*

Se H e K são subconjuntos não vazios de G , o subgrupo $\langle [h, k] : h \in H, k \in K \rangle$ de G é denotado por $[H, K]$. Nós podemos estender a definição dos comutadores $[h, k]$ (e $[H, K]$) para um número arbitrário de elementos (e subconjuntos) de G da seguinte maneira: se $x_i \in G$, $1 \leq i \leq n$, $n \geq 2$, definimos $[x_1, x_2, \dots, x_n]$, recursivamente, colocando $[x_1, x_2, \dots, x_n] = [[x_1, x_2, \dots, x_{n-1}], x_n]$. Analogamente, se X_i , $1 \leq i \leq n$, $n \geq 2$, são subconjuntos não vazios de G , colocamos $[X_1, X_2, \dots, X_n] = [[X_1, X_2, \dots, X_{n-1}], X_n]$. Para simplificar, escrevemos (indutivamente sobre m) $[X_i, X_j; m] = [[X_i, X_j; m-1], X_j]$ para $m > 0$ e $[X_i, X_j; 0] = X_i$.

Os comutadores possuem várias propriedades que apresentamos nos dois próximos resultados.

Proposição 1.2 ([2], pág. 18-20) *Sejam $x, y, z \in G$ e $H, K, L \leq G$. Temos*

- (i) $[xy, z] = [x, z]^y [y, z]$ e $[x, yz] = [x, z][x, y]^z$
- (ii) *Se y comuta com z e $[x, G]$ é abeliano, então $[x, y, z] = [x, z, y]$;*
- (iii) $[x, y]^{-1} = [y, x]$;
- (iv) $[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$;
- (v) *Se $[x, y]$ comuta com ambos x e y , então $[x, y]^{-1} = [x^{-1}, y] = [x, y^{-1}]$;*
- (vi) *[Lema dos Três Subgrupos]. Se $[H, K, L] = [K, L, H] = 1$, então $[L, H, K] = 1$;*
- (vii) $[H, K] \triangleleft \langle H, K \rangle$;
- (viii) $[H, K] = [K, H]$.

Proposição 1.3 ([6], pág. 112) *Se $H, K \leq G$ e $f : G \rightarrow L$ for um homomorfismo de grupos, então $f([H, K]) = [f(H), f(K)]$.*

Os p -grupos finitos possuem duas propriedades interessantes, dadas pela

Proposição 1.4 ([2], pág. 7 e 31) *Seja G um p -grupo finito. Temos que:*

(i) *Se H é um subgrupo próprio de G , então $N_G(H) \supset H$;*

(ii) *Se K é um subgrupo normal não trivial de G , então $K \cap Z(G) \neq 1$.*

Dado um subgrupo H de G e $g \in G$, o subconjunto $g^{-1}Hg = \{g^{-1}hg : h \in H\}$ é chamado de *conjugado* de H por g e denotado por H^g . Observe que $H \triangleleft G$ se, e somente se, $H = H^g$ para todo $g \in G$. O *normalizador* de H em G é o subgrupo $N_G(H) = \{a \in G : H^a = H\}$, enquanto o *centralizador* de H em G é o subgrupo $C_G(H) = \{a \in G : ah = ha, \forall h \in H\}$.

Escrevemos sempre a expressão “ S_p -subgrupo de G ” querendo dizer “ p -subgrupo de Sylow de G ”. Se G é um grupo finito, ele pode ser escrito como um produto de certos subgrupos, como mostra o

Teorema 1.5 (Argumento de Frattini) ([6], pág. 81) *Seja K um subgrupo normal de um grupo finito G . Se P é um S_p -subgrupo de K (para algum primo p), então $G = KN_G(P)$.*

Demonstração: Seja $g \in G$. Então, $g^{-1}Pg \leq g^{-1}Kg = K$, pois $K \triangleleft G$. Como $|g^{-1}Pg| = |P|$, temos que $g^{-1}Pg$ é um S_p -subgrupo de K e, assim, existe $k \in K$ tal que $k^{-1}Pk = g^{-1}Pg$. Portanto, $P = (gk^{-1})^{-1}P(gk^{-1})$, de modo que $gk^{-1} \in N_G(P)$. Logo, $g = (gk^{-1})k \in N_G(P)K = KN_G(P)$. \square

Um grupo finito G isomorfo a $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, p primo, é chamado *p -grupo abeliano elementar*. Claramente, um p -grupo abeliano elementar G pode ser visto como um espaço vetorial sobre o corpo \mathbb{Z}_p . Neste caso, temos o

Teorema 1.6 ([2], pág. 30) *Seja G um p -grupo abeliano elementar. Então $\text{Aut}(G)$ é isomorfo ao grupo dos operadores lineares de G .*

Dizemos que um elemento $g \in G$ é um p -elemento, p primo, se g tem ordem potência de p .

É fácil ver que todo elemento de $N_G(H)$ induz por conjugação um automorfismo de G . Isto juntamente com o teorema anterior dão sentido ao enunciado do

Teorema 1.7 ([2], pág. 32) *Seja H um p -subgrupo abeliano elementar de um grupo finito G e x um p -elemento de $N_G(H)$. Se ϕ_x denota o operador linear de H , visto como espaço vetorial sobre \mathbb{Z}_p , então o polinômio minimal de ϕ_x é $(X - 1)^r$, onde r é o menor inteiro tal que $[h, \underbrace{x, x, \dots, x}_r \text{ vezes}] = 1$ para todo $h \in H$.*

Observe que se $a \in G$, a aplicação $\gamma_a : G \rightarrow G$, dada por $\gamma_a(x) = a^{-1}xa$, para todo $x \in G$, define um automorfismo de G . Claramente, um subgrupo N é normal em G se, e somente se, $\gamma_a(N) = N$, para todo $a \in G$. Porém, podem existir subgrupos H de G tais que $\phi(H) = H$ para todo automorfismo ϕ de G . Estes subgrupos são chamados *subgrupos característicos* de G . Escrevemos $H \text{ char } G$ se H é um subgrupo característico de G . Certamente, $Z(G) \text{ char } G$.

Suponhamos que H é um subgrupo de G tal que $\phi(H) \leq H$ para todo $\phi \in \text{Aut}(G)$. Como $\phi^{-1} \in \text{Aut}(G)$, temos $\phi^{-1}(H) \leq H$, de modo que $H = \phi(\phi^{-1}(H)) \leq \phi(H)$ e, assim, $\phi(H) = H$. Portanto, $H \text{ char } G$ se, e somente se, $\phi(H) \leq H$ para todo $\phi \in \text{Aut}(G)$. Usando-se isso, é fácil demonstrar a

Proposição 1.8 ([6], pág. 104) *Sejam $H, K, N \leq G$.*

- (i) *Se $H \text{ char } K$ e $K \text{ char } G$, então $H \text{ char } G$;*
- (ii) *Se $H \text{ char } K$ e $K \triangleleft G$, então $H \triangleleft G$;*
- (iii) *Se $N \text{ char } G$, $N \leq H$ e $\frac{H}{N} \text{ char } \frac{G}{N}$ então $H \text{ char } G$.*

1.2 Grupos Solúveis e Nilpotentes

O conceito de grupo solúvel é, certamente, um dos mais importantes da Teoria de Grupos. Um dos primeiros matemáticos a usar essa noção foi E. Galois quando estudou a possibilidade de um polinômio, com coeficientes sobre um determinado corpo, ter suas

raízes expressas por radicais. Daremos, neste seção, a definição de grupos solúveis e nilpotentes e, em seguida, veremos algumas propriedades dos mesmos. As demonstrações dos resultados podem ser encontradas em [6] e [2].

Seja H um subgrupo normal de um grupo G . Dizemos que H é um *subgrupo normal minimal* de G , se $H \neq 1$ e não existe um subgrupo normal K de G tal que $1 < K < H$. Por outro lado, se não existe um subgrupo normal K de G tal que $H < K < G$, dizemos que H é um *subgrupo normal maximal* de G .

Uma *série normal* de um grupo G é uma sequência de subgrupos

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

na qual $G_{i+1} \triangleleft G_i$ para todo i . Os *grupos fatores* desta série normal são os grupos quocientes $\frac{G_i}{G_{i+1}}$, para $i = 0, 1, \dots, n-1$.

Sejam

$$G = H_0 \geq H_1 \geq \cdots \geq H_m = 1 \tag{1.1}$$

e

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1 \tag{1.2}$$

duas séries normais de um grupo G . Dizemos que a série (1.2) é um *refinamento* da série (1.1), se G_0, G_1, \dots, G_n é uma subsequência de H_0, H_1, \dots, H_m . A série (1.1) é chamada uma *série de composição*, se G_{i+1} é um subgrupo normal maximal em G_i ou $G_{i+1} = G_i$, para todo i . Cada grupo fator de uma série de composição de G é chamado de *fator de composição* de G . Dizemos que (1.1) e (1.2) são *séries equivalentes* se existe uma correspondência biunívoca entre seus grupos fatores não triviais onde fatores correspondentes são isomorfos.

As séries de um grupo possuem uma propriedade peculiar dada pela

Proposição 1.9 (Jordan-Hölder) ([6], pág. 100) *Quaisquer duas séries de composição de um grupo G são equivalentes.*

Um grupo é chamado *grupo solúvel*, se ele possui uma série normal em que cada grupo fator é abeliano. É fácil ver que um grupo finito é solúvel se, e somente se, ele possui uma série normal cujos grupos fatores são cíclicos de ordem prima.

Vamos agora apresentar algumas propriedades de grupos solúveis.

Proposição 1.10 ([6], pág. 102-105)

- (i) Subgrupo e imagem homomórfica de grupo solúvel são solúveis;
- (ii) Se $H \triangleleft G$ e ambos, H e $\frac{G}{H}$ são solúveis, então G é solúvel;
- (iii) Produto direto de grupos solúveis é solúvel;
- (iv) Todo p -grupo finito é solúvel;
- (v) Se G for um grupo solúvel finito, então todo subgrupo normal minimal de G é um p -grupo abeliano elementar para algum primo p ;

Os subgrupos comutadores superiores de um grupo G são definidos indutivamente por

$$G^{(0)} = G; \quad G^{(i+1)} = G^{(i)'}$$

i.é, $G^{(i+1)}$ é o subgrupo comutador de $G^{(i)}$. A série

$$G = G^{(0)} \geq G^{(1)} \geq \dots \geq G^{(i)} \dots$$

é chamada de *série derivada* de G . É fácil mostrar, por indução sobre i , que $G^{(i+1)} \text{ char } G$.

Os grupos solúveis são caracterizados através de suas séries derivadas, como mostra o próximo resultado.

Proposição 1.11 ([6], pág. 105) Um grupo G é solúvel se, e somente se, $G^{(n)} = 1$ para algum n .

Note que se $H, K \text{ char } G$ e $\phi \in \text{Aut}(G)$, então pela Proposição 1.3, tem-se $\phi([H, K]) = [\phi(H), \phi(K)] = [H, K]$, isto é, $[H, K] \text{ char } G$. Assim, os subgrupos $\gamma_i(G)$ de G definidos indutivamente por: $\gamma_1(G) = G$ e $\gamma_{i+1}(G) = [\gamma_i(G), G]$, $i \geq 1$, são característicos em G . É claro que $\gamma_{i+1}(G) \leq \gamma_i(G)$, para todo $i \geq 1$. A série

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \dots \gamma_i(G) \geq \dots$$

é chamada *série central inferior* do grupo G . Note que esta série pode não ser normal, pois ela pode não atingir 1.

O próximo resultado nos dá uma propriedade da série central inferior.

Proposição 1.12 ([2], pág. 209) *Se G é um grupo finito, $x \in \gamma_i(G)$ e $y \in \gamma_j(G)$, então $[x, y] \in \gamma_{i+j}(G)$.*

Um grupo G é dito *nilpotente* se existe um inteiro c tal que $\gamma_{c+1}(G) = 1$. O menor de tais c é chamado *classe de nilpotência* do grupo G e denotada por $cl(G)$.

Um subgrupo M de G é dito *subgrupo maximal* de G se não existir subgrupo H de G tal que $M \subset H \subset G$.

A seguir vamos estabelecer algumas propriedades de grupos nilpotentes.

Proposição 1.13 ([6], pág. 115-117)

- (i) *Todo subgrupo H de um grupo nilpotente G é nilpotente e $cl(H) \leq cl(G)$;*
- (ii) *Se G é nilpotente e $H \triangleleft G$, então $\frac{G}{H}$ é nilpotente com classe de nilpotência $\leq cl(G)$;*
- (iii) *Produto direto de grupos nilpotentes é nilpotente;*
- (iv) *Todo p -grupo finito é nilpotente;*
- (v) *Todo grupo nilpotente é solúvel;*
- (vi) *Um grupo finito G é nilpotente se, e somente se, G é o produto direto de seus S_p -subgrupos;*
- (vii) *Se G é um grupo nilpotente, então todo subgrupo maximal H de G é normal em G e tem índice primo;*
- (viii) *Se $G \neq 1$ é nilpotente, então $Z(G) \neq 1$;*

Como $Z(S_3) = 1$, o item (viii) do teorema anterior mostra que S_3 não é nilpotente. No entanto, ambos $A_3 \cong \mathbb{Z}_3$ e $S_3/A_3 \cong \mathbb{Z}_2$ são abelianos e, portanto, nilpotentes. Isto mostra que o item (ii) da Proposição 1.10 não é válida para grupos nilpotentes.

Observe que se G for um grupo finito, então sempre existem subgrupos maximais. Isso não é válido para o caso em que G é infinito e um exemplo é o grupo aditivo dos racionais \mathbb{Q} . Isto motiva a

Definição 1.14 Se \mathcal{M} é o conjunto de todos os subgrupos maximais de G , define-se o subgrupo de Frattini de G , denotado por $\Phi(G)$, do seguinte modo:

$$\Phi(G) = \begin{cases} \bigcap_{M \in \mathcal{M}} M, & \text{se } \mathcal{M} \neq \emptyset \\ G, & \text{se } \mathcal{M} = \emptyset \end{cases}.$$

Claramente, $\Phi(G) \text{ char } G$ e, assim, $\Phi(G) \triangleleft G$. Além disso, temos a

Proposição 1.15 ([6], pág. 123)

- (i) [Frattini, 1885]. Se G é um grupo finito, então $\Phi(G)$ é nilpotente;
- (ii) Se G é um p -grupo finito, então $\Phi(G) = G'G^p$, onde G^p é o subgrupo de G gerado por todas as p -ésimas potências de elementos de G ;
- (iii) Se G é um p -grupo finito, então $\frac{G}{\Phi(G)}$ é um espaço vetorial sobre o corpo \mathbb{Z}_p .

Diremos que um automorfismo de ordem finita ψ de um grupo G é um p' -automorfismo, se sua ordem não é divisível por p .

Teorema 1.16 (Burnside) ([2], pág. 174) Seja ψ um p' -automorfismo de um p -grupo finito P que induz a identidade sobre $P/\Phi(P)$. Então, ψ é o automorfismo identidade de P .

1.3 Apresentação de Grupos

Um grupo F é dito *livre* sobre um conjunto $X \subseteq F$ se, para todo grupo G e toda função $\theta : X \rightarrow G$, existe um único homomorfismo $\theta' : F \rightarrow G$ tal que

$$\theta'(x) = \theta(x)$$

para todo $x \in X$. A cardinalidade de X é chamada de *posto* de F .

Proposição 1.17 ([4], pág. 7) Todo grupo é uma imagem homomórfica de algum grupo livre.

Seja G um grupo e $\phi : F \longrightarrow G$ um epimorfismo de um grupo livre $F = F(X)$ sobre G . Temos então que $G \cong \frac{F}{K}$, onde K é o kernel de ϕ . Agora, seja R um subconjunto de F que gera K como subgrupo normal de F , i.é, $\langle R \rangle^F = K$. Observamos que X e R determinam G , a menos de isomorfismo. Portanto, escrevemos $G = \langle X \mid R \rangle$ e chamamos esta uma *apresentação livre*, ou simplesmente *apresentação*, do grupo G . Os elementos de X são denominados *geradores* e os de R *relatores*. Dizemos que G é *finitamente apresentado* se existe uma apresentação $G = \langle X \mid R \rangle$, onde X e R são finitos. Quando $X = \{x_1, \dots, x_n\}$ e $R = \{r_1, \dots, r_m\}$ é comum escrevermos $G = \langle x_1, \dots, x_n \mid r_1 = 1, \dots, r_m = 1 \rangle$. Neste caso, chamamos $r_i = 1$, $1 \leq i \leq m$, de *relações definidoras* para G .

Exemplo 1.18 *Um grupo cíclico G de ordem m tem apresentação*

$$G \cong \langle x \mid x^m = 1 \rangle$$

e o grupo diedral de ordem $2n$, D_{2n} , tem apresentação

$$D_{2n} \cong \langle x, y \mid x^2 = 1, y^n = 1, y^x = y^{-1} \rangle$$

Teorema 1.19 [*Teste da Substituição*] ([4], pág. 29) *Sejam G um grupo com apresentação $G = \langle X \mid R \rangle$, H um grupo e $\theta : X \longrightarrow H$ uma função. Então, θ se estende a um homomorfismo $\theta' : G \longrightarrow H$ se, e somente se, θ é consistente com todas as relações definidoras para G , i.é, se para todo $x \in X$ e todo $r \in R$, o resultado da substituição de x por $\theta(x)$ em r dá a identidade de H .*

O próximo resultado nos fornece a apresentação do produto direto de dois grupos, a partir da apresentação dos mesmos.

Proposição 1.20 ([4], pág. 32). *Se G e H são grupos com apresentações $G = \langle X \mid R \rangle$ e $H = \langle Y \mid S \rangle$, respectivamente, então o produto direto $G \times H$ tem apresentação*

$$\langle X, Y \mid R, S, [X, Y] \rangle.$$

1.4 Produto Semi-Direto

Sejam A e G dois grupos. Diremos que A age (à direita) sobre G por automorfismos, se existe uma função

$$\begin{aligned}\phi : A \times G &\longrightarrow G \\ (\alpha, g) &\longmapsto g^\alpha\end{aligned}$$

tal que:

- (i) $g^1 = g$ para todo $g \in G$;
- (ii) $(g^\alpha)^\beta = g^{\alpha\beta}$ para todo $g \in G$ e $\alpha, \beta \in A$;
- (iii) Para todo $\alpha \in A$ a função $\phi_\alpha : G \longrightarrow G$ definida por $\phi_\alpha(g) = g^\alpha$, para todo $g \in G$, é um automorfismo de G .

A função ϕ é chamado de ação por automorfismos (a direita) de A sobre G . Um subgrupo H de G é chamado de *subgrupo A -invariante*, se $h^\alpha \in H$ para todo $h \in H$ e $\alpha \in A$.

Ressaltamos que neste trabalho todas as ações por automorfismos serão à direita, a menos que se mencione o contrário.

Um grupo G é um *produto semi-direto* de seus subgrupos H e K , se $K \triangleleft G$, $G = HK$ e $H \cap K = 1$.

Agora, seja $\phi : A \times K \longrightarrow K$, denotada por $(\alpha, k) \longmapsto k^\alpha$, uma ação de A sobre K por automorfismos. É fácil ver que o conjunto $G = \{(\alpha, k) : \alpha \in A, k \in K\}$ munido com a operação

$$(\alpha_1, k_1)(\alpha_2, k_2) = (\alpha_1\alpha_2, k_1^{\alpha_2}k_2)$$

é um grupo, cujo elemento neutro é $(1_A, 1_K)$ e o inverso de (α, k) é $(\alpha^{-1}, (k^{-1})^{\alpha^{-1}})$.

Consideremos os subconjuntos $A^* = \{(\alpha, 1_K) : \alpha \in A\}$ e $K^* = \{(1_A, k) : k \in K\}$ de G . É claro que A^* é um subgrupo de G isomorfo a A pelo isomorfismo $\alpha \longmapsto (\alpha, 1_K)$

e K^* é um subgrupo de G isomorfo a K pelo isomorfismo $k \mapsto (1_A, k)$. Obviamente, $G = A^*K^*$ e $A^* \cap K^* = (1_A, 1_K)$. Mais ainda, para todo $\alpha \in A$ e $k \in K$, temos

$$(\alpha, 1_K)^{-1}(1_A, k)(\alpha, 1_K) = (1_A, k^\alpha) \in K^* \quad (1.3)$$

e

$$(1_A, k)^{-1}(\alpha, 1_K)^{-1}(1_A, k)(\alpha, 1_K) = (1_A, k^{-1}k^\alpha) \in K^* \quad (1.4)$$

Observe que por (1.3), o elemento $(1_A, k)$ de K^* é transformado no elemento $(1_A, k^\alpha)$ pela conjugação por $(\alpha, 1_K)$. Isto mostra que $K^* \triangleleft G$. Pelos isomorfismos de A em A^* e de K em K^* definidos anteriormente, é natural identificarmos A e K com suas imagens A^* e K^* em G , respectivamente. Portanto, obtemos a seguinte conclusão: existe um grupo G tal que $G = AK$, $K \triangleleft G$, $A \cap K = 1$, $\alpha^{-1}k\alpha = k^\alpha$ e $k^{-1}\alpha^{-1}k\alpha = k^{-1}k^\alpha$. Tal grupo G é chamado de produto semi-direto de K por A com respeito a ação ϕ e denotado por $A \rtimes K$.

A relação (1.4), motiva a definirmos em G o comutador de k e α como sendo o elemento $[k, \alpha] = k^{-1}k^\alpha$ de K . Também, o subgrupo comutador de K e A é definido por $[K, A] = \langle [k, \alpha] : k \in K, \alpha \in A \rangle$.

O subconjunto $C_K(A) = \{k \in K : k^\alpha = k, \forall \alpha \in A\}$ de K é, certamente, um subgrupo A -invariante de K , chamado *centralizador de A sobre K* .

1.5 Grupo de Frobenius

Nesta seção, vamos definir e estabelecer algumas propriedades do chamado grupo de Frobenius. Trataremos apenas de grupos finitos. Se S for um conjunto, denotaremos por $Sym(S)$ o grupo de todas as permutações de S com a operação de composição de funções.

Seja G um grupo de permutações de um conjunto finito S , i.é, G é um subgrupo de $Sym(S)$. Diremos que G é um *grupo de permutações transitivo* sobre S , se para quaisquer $s, s' \in S$, existe $\gamma \in G$ tal que $\gamma(s) = s'$. É fácil ver que o conjunto de todos os elementos

de G que fixam um elemento s de S é um subgrupo de G . Tal subgrupo será chamado de *estabilizador* de s e denotado por $stab(s)$.

Sejam H um subgrupo de um grupo G e $S = \{x_1H, \dots, x_nH\}$ o conjunto de todas as classes laterais à esquerda distintas de H em G . Note que para cada $x \in G$, a função $\alpha_x : S \rightarrow S$ dada por $\alpha_x(x_iH) = xx_iH$ está bem definida e é uma permutação de S . Além disso, $\alpha_{xy} = \alpha_x\alpha_y$ para quaisquer $x, y \in G$, de modo que, a função $\alpha_H : G \rightarrow Sym(S)$, definida por $\alpha_H(x) = \alpha_x$ para todo $x \in G$, é um homomorfismo. Chamamos α_H de *representação permutacional transitiva* de G sobre o conjunto S das classes laterais à esquerda de H em G .

Mais geralmente, se G é um grupo e S é um conjunto, todo homomorfismo $\alpha : G \rightarrow Sym(S)$ é chamado uma *representação permutacional* de G sobre S . Também é usual dizer que G age sobre o conjunto S . Diremos que α é uma *representação permutacional transitiva* se $\alpha(G)$ for um grupo permutacional transitivo sobre S . Os elementos de S serão chamados de *letras*. Se α e α' são representações permutacionais transitivas sobre os conjuntos S e S' , respectivamente, diremos que α e α' são *equivalentes*, se existir uma bijeção $\theta : S \rightarrow S'$ tal que $\alpha'(g) = \theta\alpha(g)\theta^{-1}$, para todo $g \in G$. O primeiro resultado nos diz que toda representação permutacional transitiva é equivalente a uma representação particular.

Teorema 1.21 ([2], pág. 34) *Toda representação permutacional transitiva de um grupo finito G é equivalente a uma representação de um grupo G sobre o conjunto das classes laterais à esquerda de algum subgrupo de G .*

O caso particular $H = 1$ tem uma importância peculiar. Certamente $Ker \alpha_H = 1$ e, neste caso, $\rho = \alpha_H$ é um monomorfismo de G no grupo das permutações de grau $|G|$. Chamaremos esta representação permutacional de *representação regular à esquerda* de G . Tal representação tem a propriedade que somente a identidade fixa mais que uma letra.

A classe de grupos de permutações transitivas nos quais somente a identidade fixa mais de uma letra, mas $stab(i) \neq 1$ para alguma letra i , é fundamental para o nosso trabalho. Um grupo de permutações transitivo que satisfaz estas duas condições, é chamado *grupo*

de Frobenius, por ter sido ele o primeiro a estudá-los.

Frobenius descobriu uma propriedade muito interessante desta classe de grupos.

Teorema 1.22 ([2], pág. 140) *Sejam G um grupo de Frobenius e H o estabilizador de uma letra. Então o subconjunto K de G constituído da identidade juntamente com todos os elementos que não fixam letras é um subgrupo normal de G cuja ordem é $|G : H|$.*

O subgrupo K do teorema acima é chamado *kernel de Frobenius* de G e o estabilizador H é chamado de *complemento de Frobenius* de G .

Observação 1.23 *Como $K \setminus 1$ não fixa letra, temos $K \cap H = 1$. Além disso, segue do Teorema de Frobenius e do Teorema de Lagrange que $|G| = |H| \cdot |K| = \frac{|HK|}{|H \cap K|} = |HK|$ e, portanto, $G = K \rtimes H$.*

O resultado a seguir nos dá uma condição necessária e suficiente para que um grupo seja um grupo de Frobenius.

Teorema 1.24 ([2] pág. 39) *Seja H um subgrupo não trivial de um grupo finito G . Então G é um grupo de Frobenius com complemento H se, e somente se, $H \cap H^x = 1$ para todo $x \in G \setminus H$.*

1.6 Representações de Grupos

Na seção 1.5, chamamos de representação permutacional a um homomorfismo de um grupo G no grupo $Sym(S)$, onde S é um conjunto. Na presente seção, iremos estudar algumas propriedades de homomorfismos de um grupo no grupo dos operadores lineares inversíveis de um espaço vetorial de dimensão finita sobre um corpo F . Todos os grupos desta seção serão finitos.

Sejam G um grupo, V/F um espaço vetorial de dimensão finita sobre um corpo F e $GL(V, F)$ o grupo dos operadores lineares inversíveis de V . Um homomorfismo $\phi : G \longrightarrow GL(V, F)$ é chamado de *representação* de G sobre V/F . Se ϕ leva todos os elementos de G no operador identidade, dizemos que a representação é *trivial*. A

dimensão de V/F é chamada *grau da representação* ϕ . Se A é um subgrupo de $\phi(G)$ e W um subespaço de V tal que $A(W) \subseteq W$, diremos que W é *A-invariante*.

Há dois tipos de representações muito importantes: as *fiéis* e as *irredutíveis*. Se o kernel de uma representação ϕ for igual a 1, diremos que ϕ é uma *representação fiel*. Se 0 e V forem os únicos subespaços $\phi(G)$ -invariantes de V , diremos que ϕ é uma *representação irredutível*.

O próximo resultado nos fornece informações sobre representações irredutíveis de p -grupos e sobre a existência de subgrupos normais em grupos que possuem representações fiéis irredutíveis.

Proposição 1.25 ([2], pág. 62)

- (i) *Toda representação irredutível de um p -grupo sobre um espaço vetorial sobre um corpo de característica p é trivial. Equivalentemente, um p -grupo não trivial não possui uma representação fiel e irredutível sobre um espaço vetorial sobre um corpo de característica p .*
- (ii) *Se G possui uma representação fiel e irredutível sobre um espaço vetorial V/F , onde F é um corpo de característica p , então G não possui p -subgrupos normais não triviais.*

No último resultado desta seção, vamos ver uma condição para que uma representação seja trivial.

Proposição 1.26 ([2], pág. 69) *Seja ϕ uma representação de G sobre V/F e assumamos que F tenha característica nula ou relativamente prima com $|G|$. Se*

$$V = V_1 \supset V_2 \supset \cdots \supset V_{n+1} = 0$$

é uma sequência de subespaços $\phi(G)$ -invariantes tal que $\phi(G)$ age trivialmente sobre cada $\frac{V_i}{V_{i+1}}$, então ϕ é a representação trivial sobre V .

Observação 1.27 *Sejam V um espaço vetorial de dimensão finita n sobre um corpo F , $\beta = \{v_1, v_2, \dots, v_n\}$ uma base de V e denotemos por $GL(n, F)$ o grupo das matrizes*

inversíveis $n \times n$ com entradas em F . Como é usual, nós associaremos a cada T pertencente a $GL(V, F)$ a matriz T_β de T com respeito a base β dada. Sabemos que a aplicação $\alpha_\beta : GL(V, F) \longrightarrow GL(n, F)$ dada por $\alpha_\beta(T) = T_\beta$ é um isomorfismo. Assim, toda representação ϕ de G sobre V induz um homomorfismo de G em $GL(n, F)$ através da composição $\alpha_\beta \circ \phi$. De um modo geral, um homomorfismo $\psi : G \longrightarrow GL(n, F)$ é chamado de F -representação matricial de G . O número n é chamado grau da representação matricial. Duas representações matriciais ϕ e ψ de G são ditas equivalentes, se existe uma matriz $M \in GL(n, F)$ tal que $\psi(g) = M^{-1} \cdot \phi(g) \cdot M$, para todo $g \in G$. Observamos que representações matriciais obtidas de uma representação ϕ de G sobre V por bases diferentes são equivalentes. As representações matriciais nos serão muito úteis quando estudarmos os caracteres de um grupo no Capítulo 5.

Seja G um grupo, F um corpo e consideremos o conjunto $FG = \{ \sum_{x \in G} a_x x : a_x \in F \}$. Sobre FG , definimos a soma de dois elementos $\sum_{x \in G} a_x x$ e $\sum_{x \in G} b_x x$ por

$$\sum_{x \in G} a_x x + \sum_{x \in G} b_x x = \sum_{x \in G} (a_x + b_x) x$$

e o produto por

$$\left(\sum_{x \in G} a_x x \right) \left(\sum_{x \in G} b_x x \right) = \sum_{x \in G} \sum_{y \in G} (a_x b_y) xy.$$

É fácil ver que, com estas operações, FG é um anel.

Se $\phi : G \longrightarrow GL(V/F)$ é uma representação, façamos a seguinte identificação:

$$xu = \phi(x)(u), \quad \forall u \in V, \quad \forall x \in G.$$

Definindo $(\sum_{x \in G} a_x x) \cdot u = \sum_{x \in G} a_x (xu)$, para todo $u \in V$ e todo $\sum_{x \in G} a_x x \in FG$, temos que V/F torna-se um FG -módulo à esquerda. Neste caso, diremos simplesmente que V/F é um G -módulo. Quando isso é feito, cada elemento de G torna-se um operador linear de V e podemos adaptar para G -módulos todos os conceitos anteriormente definidos para representações. Assim, um subespaço de V $\phi(G)$ -invariante torna-se G -submódulo de V ; V é um G -módulo irredutível se 0 e V são os únicos G -submódulos e V é um G -módulo fiel se apenas o elemento neutro de G determina o operador identidade de V . Os demais conceitos de representações possuem interpretações análogas.

Reciprocamente, se V/F é um G -módulo, então para cada $x \in G$, a aplicação $T_x : V \longrightarrow V$ dada por $T_x(v) = xv$, para todo $v \in V$, é um operador linear inversível de V . Assim, a aplicação $\phi : G \longrightarrow GL(V, F)$ definida por $\phi(x) = T_x$, é uma representação de G sobre V/F . Portanto, as noções de representação de G e G -módulo são equivalentes e nós usaremos o conceito que for mais conveniente em cada ocasião.

1.7 Grupo Linear $GL(2, q)$

O grupo $GL(2, q)$ das matrizes 2×2 inversíveis com entradas no corpo finito $GF(q)$ de q elementos, possui uma importância particular no nosso trabalho, principalmente quando estudarmos os grupos p -estáveis no Capítulo 3. Por isso nós estabeleceremos algumas de suas propriedades, que não serão demonstradas, mas o leitor poderá encontrá-las em [2] e [6].

$GL(2, q)$ é conhecido como *grupo linear geral* (de dimensão 2); seu subgrupo constituído das matrizes de determinante 1, é chamado o *grupo linear especial* e é denotado por $SL(2, q)$. O centro de $GL(2, q)$ consiste de todas as matrizes escalares e o grupo quociente correspondente, $PGL(2, q)$, é chamado de *grupo linear projetivo*. Finalmente, a imagem $L_2(q)$ de $SL(2, q)$ em $PGL(2, q)$ é chamado *grupo linear projetivo especial*.

Os resultados a seguir nos fornecem a descrição dos S_2 -subgrupos de $SL(2, q)$ e uma condição necessária e suficiente para que $L_2(q)$ seja simples.

Proposição 1.28 ([2], pág. 42 e [6], pág. 225)

- (i) Um S_2 -subgrupo de $SL(2, q)$ é abeliano elementar se q for par e é quatérnio generalizado se q for ímpar;
- (ii) $SL(2, p)$ não é solúvel para todo primo $p \geq 5$.
- (iii) $L_2(q)$ é simples se, e somente se, $q > 3$;

Também temos o

Teorema 1.29 (Dickson) ([2], pág. 44) *Sejam λ um gerador de $GF(p^r)$ sobre o corpo primo de ordem p , p ímpar, e $L = \left\langle \left(\begin{array}{cc} 1 & 0 \\ \lambda & 1 \end{array} \right), \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \right\rangle$. Então uma das seguintes condições se verifica:*

(i) $L = SL(2, p^r)$

(ii) $p^r = 9$, $|Z(L)| = 2$, $L/Z(L)$ é isomorfo a A_5 e L contém um subgrupo isomorfo a $SL(2, 3)$.

Capítulo 2

π -Separabilidade

Seja π um conjunto não vazio de primos. Um número inteiro n é dito ser um π -número se todos seus fatores primos estão em π e é um π' -número, se nenhum de seus fatores primos está em π .

Enfatizamos que, ao longo do trabalho, π **sempre** denotará um conjunto não vazio de primos e todos os grupo serão finitos, a menos que se mencione o contrário. Ressaltamos ainda, que se G é um grupo, denotaremos por $\pi(G)$ o conjunto de todos os divisores primos de $|G|$.

Um grupo G é um π -grupo, se a ordem de cada um dos seus elementos é um π -número e é um π' -grupo se a ordem de cada elemento é um π' -número.

Observe que π -subgrupos maximais de um grupo G sempre existem, mas eles não são necessariamente conjugados quando π contém mais que um primo. Se G é um grupo, um π -subgrupo H de G tal que $|G : H|$ é um π' -número é chamado de *π -subgrupo de Hall de G* . Note que, se H é um π -subgrupo de Hall de G , então segue direto da definição que H é um π -subgrupo maximal de G . Além disso, é fácil ver que os termos “ p -subgrupos de Hall” e “ p -subgrupos de Sylow” são sinônimos.

Em contraste com os π -subgrupos maximais, os π -subgrupos de Hall nem sempre existem. Por exemplo, se $G = A_5$ e $\pi = \{3, 5\}$, um π -subgrupo de Hall de A_5 deveria ter índice 4. Porém, A_5 não possui subgrupo de ordem 15. Logo, A_5 não possui um $\{3, 5\}$ -subgrupo de Hall. Veremos adiante que em um grupo solúvel, os π -subgrupos de

Hall sempre existem e formam uma única classe de conjugação.

Os π -subgrupos normais desempenham um papel especial. Suponhamos que H e K são π -subgrupos de G com $K \triangleleft G$. Então, claramente, $H \cap K$ e $\frac{HK}{K} \cong \frac{H}{H \cap K}$ são π -grupos de modo que HK é um π -grupo. Conseqüentemente, o subgrupo gerado por todos os π -subgrupos normais de G é um π -grupo. Este é o único π -subgrupo normal maximal de G e é denotado por $O_\pi(G)$. Note que se $\phi \in \text{Aut}(G)$, então $\phi(O_\pi(G)) \triangleleft G$, pelo Teorema da Correspondência, de modo que $\phi(O_\pi(G)) \leq O_\pi(G)$ por definição. Portanto, $O_\pi(G) \text{ char } G$.

Definição 2.1 *Um subgrupo H de G é dito ser subnormal em G , quando existem subgrupos $H_0 = H, H_1, \dots, H_l = G$ de G , distintos dois a dois, tais que $H = H_0 \triangleleft H_1, H_1 \triangleleft H_2, \dots, H_{l-1} \triangleleft H_l = G$.*

Proposição 2.2 *Seja G um grupo e π um conjunto não vazio de primos.*

- (i) *Se H é um π -subgrupo subnormal de G , então $H \leq O_\pi(G)$;*
- (ii) *$O_\pi(G)$ é a interseção de todos os π -subgrupos maximais de G . Em particular, $O_\pi(G)$ está contido em todo π -subgrupo de Hall de G .*

Demonstração: (i) Por hipótese, existe uma série $H = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_l = G$ de subgrupos de G distintos dois a dois. Faremos a demonstração por indução sobre l , observando que se $l \leq 1$, então $H \triangleleft G$ e $H \leq O_\pi(G)$. Suponha $l > 1$. A hipótese de indução garante que $H \leq O_\pi(H_{l-1})$.

Como $O_\pi(H_{l-1}) \text{ char } H_{l-1}$ e $H_{l-1} \triangleleft G$, temos da Proposição 1.8 (ii) que $O_\pi(H_{l-1}) \triangleleft G$ e, portanto, $O_\pi(H_{l-1}) \leq O_\pi(G)$. Logo, pela hipótese de indução, $H \leq O_\pi(G)$.

(ii) Sejam $R = O_\pi(G)$ e S um π -subgrupo maximal qualquer de G . Então RS é um π -subgrupo de G . Portanto, $R \leq S$, pela maximalidade de S . Por outro lado, a interseção de todos os π -subgrupos maximais de G é certamente normal em G e, portanto, está contido em R . □

2.1 O Teorema de Schur-Zassenhaus

O teorema a seguir, deve ser encarado como um dos principais resultados da Teoria de Grupos, por ser uma recíproca fraca do Teorema de Lagrange, ou seja, sob algumas condições ele nos garante a existência de subgrupos de certa ordem.

Teorema 2.3 (Schur-Zassenhaus) *Seja N um subgrupo normal de um grupo G . Suponhamos que $|N| = n$ e $|G : N| = m$ sejam relativamente primos. Então G contém subgrupos de ordem m e quaisquer dois deles são conjugados em G .*

Demonstração: (i) Caso: N abeliano.

Seja $Q = \frac{G}{N}$. Visto que N é abeliano, é fácil mostrar que a aplicação $a^{gN} = a^g$, para todo $gN \in Q$ e todo $a \in G$, é uma ação bem definida. Para cada x em Q , nós escolhemos um representante t_x de modo que o conjunto $T = \{t_x : x \in Q\}$ é uma transversal de N em G , i.é., um subconjunto de G constituído de um representante de cada classe lateral de N em G . Como $t_x t_y$ pertence a classe $t_x t_y N = t_{xy} N$, existe $c(x, y) \in N$ tal que $t_x t_y = t_{xy} c(x, y)$. Aplicando esta equação e a lei associativa $(t_x t_y) t_z = t_x (t_y t_z)$, obtemos a relação

$$c(xy, z) c(x, y)^z = c(x, yz) c(y, z), \quad (2.1)$$

que é válida para todo $x, y, z \in Q$.

Agora, considere o elemento $d(y) = \prod_{x \in Q} c(x, y)$, o qual está em N . Tomando o produto das equações (2.1) para todo $x \in Q$ temos, do fato de N ser abeliano, que

$$\prod_{x \in Q} c(xy, z) \prod_{x \in Q} c(x, y)^z = \prod_{x \in Q} c(x, yz) \prod_{x \in Q} c(y, z). \quad (2.2)$$

Note que $\prod_{x \in Q} c(y, z) = c(y, z)^m$, pois $|Q| = m$ e $c(y, z)$ não envolve x . Também temos

$\prod_{x \in Q} c(x, y)^z = \left(\prod_{x \in Q} c(x, y) \right)^z$ e $\prod_{x \in Q} c(xy, z) = d(z)$, pois xy percorre Q quando x percorre Q . Assim, obtemos da equação (2.2) que $d(z) d(y)^z = d(yz) c(y, z)^m$, ou ainda,

$$d(yz) = d(y)^z d(z) c(y, z)^{-m}. \quad (2.3)$$

Como $(m, n) = 1$, temos do Teorema de Bezout, que existem a e b inteiros tais que $am + bn = 1$. Tomando $e(y) = d(y)^{-a}$, temos $e(y)^m = d(y)^{-am} = d(y)^{-1+bn} = d(y)^{-1}$. Deste modo, existe um elemento $e(y)$ em N tal que $e(y)^m = d(y)^{-1}$ e (2.3) torna-se $e(yz)^{-m} = (e(y)^z e(z) c(y, z))^{-m}$. Visto que N é abeliano e $(m, n) = 1$, obtemos $e(yz) = e(y)^z e(z) c(y, z)$. Colocando $S_x = t_x e(x)$, para todo $x \in G$, temos

$$S_y S_z = t_y t_z t_z^{-1} e(y) t_z e(z) = t_y t_z e(y)^z e(z) = t_{yz} c(y, z) e(y)^z e(z) = t_{yz} e(yz) = S_{yz}.$$

Isto mostra que a aplicação $\theta : Q \longrightarrow G$ dada por $\theta(x) = S_x$ é um homomorfismo. Além disso, se $x \in \text{Ker}\theta$, então $S_x = 1$ e, assim, $t_x = e(x)^{-1} \in N$, i.é., o representante da classe lateral $x \in Q$ está em N . Logo, $x = N = 1_Q$, o que implica $\text{Ker}\theta = 1$ e então $|\text{Im}\theta| = |Q| = m$. Portanto, G possui um subgrupo de ordem m , a saber, $\text{Im}\theta$.

Suponhamos agora que H e H^* são dois subgrupos de G de ordem m . Vamos mostrar que existe $c \in G$ tal que $H^* = c^{-1} H c$. Como $|H| = |H^*| = m = |G : N|$, $NH, NH^* \leq G$ e $(|H|, |N|) = 1$, temos $G = HN$, $H \cap N = 1$, $G = H^*N$ e $H^* \cap N = 1$. Além disso, se $x \in Q$, então $x = gN$ para algum $g \in G$. Mas, $g = h_x n'$ para algum $h_x \in H$ e $n' \in N$, o que implica $x = h_x N$. Analogamente, $x = h_x^* N$ para algum $h_x^* \in H^*$.

Considere os homomorfismos $\phi_1 : Q = \frac{HN}{N} \longrightarrow H$ e $\phi_2 : Q = \frac{H^*N}{N} \longrightarrow H^*$ dados por $\phi_1(x) = h_x$ e $\phi_2(x) = h_x^*$, respectivamente. Como $h_x N = x = h_x^* N$, $h_x^* = h_x a(x)$ para algum $a(x) \in N$. No entanto, $h_{xy} a(xy) = h_{xy}^* = h_x^* h_y^* = h_x a(x) h_y a(y) = h_x h_y h_y^{-1} a(x) h_y a(y) = h_{xy} a(x)^y a(y)$ e deduzimos, portanto, a relação

$$a(xy) = a(x)^y a(y). \quad (2.4)$$

Defina $b = \prod_{x \in Q} a(x)$. Fazendo o produto das equações (2.4) sobre todo $x \in Q$, obtemos

$$b = \prod_{x \in Q} a(xy) = \prod_{x \in Q} a(x)^y \prod_{x \in Q} a(y) = b^y a(y)^m.$$

Visto que $(m, n) = 1$, existem $k_1, k_2 \in \mathbb{Z}$ tais que $k_1 m + k_2 n = 1$ e, assim, $b = b^{k_1 m + k_2 n} = (b^{k_1})^m$, i.é., existe $c \in N$ tal que $b = c^m$. Deste modo, a equação $b = b^y a(y)^m$ torna-se $c^m = (c^m)^y a(y)^m = (c^y a(y))^m$ e então $c = c^y a(y)$, ou ainda, $a(y) = c^{-y} c$. Portanto, levando-se em conta que $c^{-y} = (c^{-1})^{h_y}$, temos

$$h_y^* = h_y a(y) = h_y c^{-y} c = h_y (h_y^{-1} c^{-1} h_y) c = c^{-1} h_y c.$$

Logo, $H^* = c^{-1}Hc = H^c$.

(ii) Existência - Caso geral

Procederemos por indução sobre $|G|$, notando ser óbvio se $|G| = 1$. A hipótese de indução garante que o teorema é válido para todo grupo que está nas hipóteses e tenha ordem menor que $|G|$.

Sejam p um divisor primo de $|N|$ e P um S_p -subgrupo de N . Coloquemos $L = N_G(P)$ e $C = Z(P)$. Como $C \text{ char } P$, segue que $L \leq N_G(C) = M$. Pelo Argumento de Frattini, temos $G = LN$ e, como $L \leq M$, segue que $G = MN$. Denotemos por N_1 o subgrupo normal $N \cap M$ de M e note que $|M : N_1| = |G : N| = m$. Visto que $C \neq 1$, pela Proposição 1.13 (iv) e (viii), temos $|\overline{M}| < |G|$, onde $\overline{M} = M/C$. Além disso, $C \leq N_1 \leq M$ com $C, N_1 \triangleleft M$. Então, pelo Terceiro Teorema do Isomorfismo, $\overline{N}_1 = N_1/C \triangleleft \overline{M}$ e $|\overline{M} : \overline{N}_1| = |M : N_1| = m$. Como N_1 é subgrupo de N , temos que $|\overline{N}_1|$ é relativamente prima com $|\overline{M} : \overline{N}_1|$. Assim, pela hipótese de indução, existe um subgrupo $\overline{X} = \frac{X}{C}$ de \overline{M} cuja ordem é m , de modo que, $\overline{X} \cap \overline{N}_1 = 1$. Disso temos $\overline{M} = \overline{X}\overline{N}_1$, o que implica $M = XN_1$. Uma vez que $C \leq X$ e $C \leq N_1$, $C \leq X \cap N_1$. Se $C < X \cap N_1$, então existe x em $X \cap N_1$ que não está em C . Mas daí, a classe xC é diferente de C e pertence a $\overline{X} \cap \overline{N}_1$, o que não ocorre. Logo, $C = X \cap N_1$. Além disso, $|X : C| = m$ é relativamente prima com $|C|$. Visto que C é abeliano, temos do caso anterior que X tem um subgrupo de ordem m . Portanto, G também possui.

(iii) Conjugação - caso $\frac{G}{N}$ solúvel.

Denotemos por π o conjunto de divisores primos de m e escrevamos $R = O_\pi(G)$. Sejam H e K dois subgrupos de G , ambos de ordem m . Então $|G : H| = |G : K| = n$ que é um π' -número, de modo que H e K são π -subgrupos de Hall. Pela Proposição 2.2 (ii), $R \leq H \cap K$. Passando para o quociente $\overline{G} = \frac{G}{R}$, temos que, $\overline{H} = \frac{H}{R}$ e $\overline{K} = \frac{K}{R}$ são π -subgrupos de Hall. Note que se \overline{H} e \overline{K} forem conjugados, então existe $g \in G$ tal que $\overline{K} = \overline{H}^g$ e, portanto, $K = H^g$, ou seja, K e H serão conjugados. Além disso, pela maximilidade de $O_\pi(G)$, tem-se $O_\pi(\overline{G}) = 1$. Deste modo, basta mostrar o teorema para o caso em que $O_\pi(G) = 1$. Claro que podemos assumir $m \neq 1$ e, assim, $N \neq G$.

Seja L/N um subgrupo normal minimal de G/N . Visto que este último é solúvel, temos da Proposição 1.10 (v) que $\frac{L}{N}$ é um p -grupo abeliano elementar para algum primo

p em π . Agora $H \cap L$ é um S_p -subgrupo de L , pois $H \cap L \cong \frac{(H \cap L)N}{N} \leq \frac{L}{N}$. Além disso $|L : H \cap L| = |LH : (H \cap L)H| = |LH : H|$ de modo que $|L : H \cap L|$ é um divisor de n e, assim, $|L : H \cap L|$ é um π' -número e, conseqüentemente, um p' -número. O mesmo ocorre com $K \cap L$. Então, pelo Teorema de Sylow, existe $g \in G$ tal que $H \cap L = (K \cap L)^g$. Mas como $\frac{L}{N} \triangleleft \frac{G}{N}$, segue do Teorema da Correspondência que $L \triangleleft G$ e, assim, $H \cap L = (K \cap L)^g = K^g \cap L$. Escrevendo S no lugar de $H \cap L$ nós concluimos que $S \triangleleft J$, onde $J = \langle H, K^g \rangle$.

Suponhamos que $J = G$. Então $S \triangleleft G$, e como S é um π -grupo, pois $S \leq H$, segue que S é um π -subgrupo normal de G e, conseqüentemente, $S \leq R = 1$. Assim, $L \cap H = 1$ e isto força L a ser um p' -grupo. Mas isso não pode ocorrer, uma vez que $\frac{L}{N}$ é um p -grupo. Disso segue que $|J| < |G|$. Como H e K^g são subgrupos de J de ordem m , temos da hipótese de indução que H e K^g são conjugados em J e, portanto, H e K são conjugados em G .

(iv) Conjugação - caso N solúvel.

Sejam H e K subgrupos de G de ordem m . Como N/N' é abeliano e $N/N' \triangleleft G/N'$, segue do item (i) que existe $g \in G$ tal que $(HN'/N')^{gN'} = KN'/N'$. Daí, $H^g \leq KN'$. Agora, note que $N^{(i)} \text{ char } G \triangleleft G$, de modo que $N^{(i)} \triangleleft G$ para todo i . Como $N^{(1)}/N^{(2)}$ é abeliano e $N/N^{(2)} \triangleleft G/N^{(2)}$, temos do item (i) que existe $g_2 \in G$ tal que $(HN^{(2)}/N^{(2)})^{g_2N^{(2)}} = KN^{(2)}/N^{(2)}$. Daí, $H^{g_2} \leq KN^{(2)}$. Repetindo-se esse processo, podemos mostrar que existe $g_k \in G$ tal que $H^{g_k} \leq KN^{(k)}$, para todo k . Como N é solúvel, existe um inteiro l tal que $N^{(l)} = 1$ e, portanto, existe $g_l \in G$ tal que $H^{g_l} \leq K$. Disso e de $|H^{g_l}| = |K|$, temos $H^{g_l} = K$. Logo, H e K são conjugados.

(v) Conjugação - caso geral

Uma vez que m e n são relativamente primos, um dos dois deve ser ímpar. Se n é ímpar, então pelo Teorema de Feit-Thompson (que diz que todo grupo de ordem ímpar é solúvel) temos que N é solúvel e recaímos no caso (iv). Se m é ímpar, então $\frac{G}{N}$ é solúvel e recaímos no caso (iii). Logo, o resultado segue. \square

Observe que o Teorema de Feit-Thompson é apenas usado para provar a conjugação e somente no caso de não sabermos a priori que N ou $\frac{G}{N}$ é solúvel.

Corolário 2.4 *Com a notação do Teorema de Schur-Zassenhaus, seja m_1 um divisor de m . Se K é um subgrupo de G de ordem m_1 , então K está contido em um subgrupo de ordem m .*

Demonstração: Sejam H e K subgrupos de G de ordem m e m_1 , respectivamente. Então $G = HN$ e, conseqüentemente, $KN = (KN) \cap G = (KN) \cap (HN) = ((KN) \cap H)N$. Disto, do Segundo Teorema do Isomorfismo e de $H \cap N = 1$, segue que $\frac{KN}{N} \cong KN \cap H$. Por outro lado, do Segundo Teorema do Isomorfismo e de $N \cap K = 1$, vem que $\frac{KN}{N} \cong K$. Portanto, $|KN \cap H| = |KN : N| = |K| = m_1$, de modo que K e $KN \cap H$ tem a mesma ordem. Pelo Teorema de Schur-Zassenhaus, existe $g \in G$ tal que $K = (KN \cap H)^g \leq H^g$. Como $|H^g| = m$, o resultado segue. \square

Seja K um subgrupo de um grupo G não necessariamente normal. Dizemos que um subgrupo H de G é um *complemento de K em G* se $G = KH$ e $K \cap H = 1$.

Note que na demonstração do Teorema de Schur-Zassenhaus, nós tomamos π como o conjunto de primos divisores de m . Podemos tomar π como sendo o conjunto dos primos divisores de $|N| = n$. Neste caso, o teorema tem a seguinte formulação:

Teorema 2.5 *Seja N um π -subgrupo de Hall normal em G . Então, G possui um π' -subgrupo de Hall K que é um complemento de N em G e quaisquer dois π' -subgrupos de Hall são conjugados.*

Usaremos esta formulação para a demonstração dos próximos dois teoremas.

Teorema 2.6 *Seja A um π' -grupo de automorfismos do π -grupo G . Então para cada primo p em π , temos:*

- (i) *A deixa invariante algum S_p -subgrupo de G ;*
- (ii) *Quaisquer dois S_p -subgrupos A -invariantes de G são conjugados por elementos de $C_G(A)$;*
- (iii) *Qualquer p -subgrupo A -invariante de G está contido em um S_p -subgrupo A -invariante de G .*

Demonstração: Como $A \leq \text{Aut}(G)$, A age naturalmente por automorfismos sobre G . Seja G^* o produto semi-direto de G por A . Assim, G é um π -subgrupo de Hall normal de G^* e A é um π' -subgrupo de Hall de G^* que também é um complemento de G em G^* . Pelas observações anteriores, qualquer outro π' -subgrupo de Hall de G^* é conjugado a A por algum elemento de G^* . Visto que $G^* = AG$, podemos claramente assumir que este elemento de conjugação está em G .

(i) Tomemos P um S_p -subgrupo de G e seja $N = N_{G^*}(P)$. Pelo Argumento de Frattini, $G^* = GN$ e, assim, $A \cong \frac{G^*}{G} = \frac{GN}{G} \cong \frac{N}{N \cap G}$, de modo que $|N : N \cap G| = |A|$. Como $|A|$ é um π' -número, $N \cap G$ é um π -subgrupo de Hall de N . Uma vez que $G \cap N \triangleleft N$, $G \cap N$ é um π -subgrupo de Hall normal de N . Logo, pela observação anterior, N possui um π' -subgrupo de Hall B , que é um complemento de $G \cap N$ em N e assim, $|B| = |N : G \cap N| = |A|$. Portanto, B é um π' -subgrupo de Hall de G^* e, então, $A = B^x$ para algum $x \in G$. Porém, B deixa P invariante, pois $B \leq N$ e, conseqüentemente, B^x deixa P^x invariante. Logo, A deixa o S_p -subgrupo P^x invariante, provando (i).

(ii) Sejam P e Q dois S_p -subgrupos de G A -invariantes. Vamos mostrar que existe $z \in C_G(A) = \{g \in G : g^\phi = g, \forall \phi \in A\}$ tal que $P = Q^z$. Pelo Teorema de Sylow, existe $x \in G$ tal que $P = Q^x$ e, conseqüentemente, A^x deixa $Q^x = P$ invariante. Visto que A e A^x deixam P invariante, ambos estão contidos em $N = N_{G^*}(P)$. Assim cada um deles é um π' -subgrupo de Hall de N , pois A e A^x são π' -subgrupos de Hall de G^* . Como vimos no item (i), $G \cap N$ é um π -subgrupo de Hall normal de N . Logo, pelo Teorema de Schur-Zassenhaus, existe $y \in G \cap N$ tal que $A = (A^x)^y$. Tomemos $z = xy$, de modo que $z \in G$, pois $x, y \in G$. Agora, como y normaliza P , pois $y \in N$, temos que $Q^z = (Q^x)^y = P^y = P$. Afirmamos que $z \in C_G(A)$. De fato, em G^* tem-se que $[z, A] = \langle z^{-1}\phi^{-1}z\phi : \phi \in A \rangle \subseteq A$, pois como z normaliza A , $z^{-1}\phi^{-1}z \in A$ e então $z^{-1}\phi^{-1}z\phi \in A$. Por outro lado, como $G \triangleleft G^*$ temos que $z^{-1}\phi^{-1}z\phi \in G$, para todo $\phi \in A$ e assim, $[z, A] \subseteq G$. Logo, $[z, A] \subseteq G \cap A = 1$ e, com isso, $z^\phi = z$ para todo $\phi \in A$, ou seja, $z \in C_G(A)$.

(iii) Seja Q um p -subgrupo A -invariante de G e seja P um p -subgrupo A -invariante maximal de G contendo Q . Vamos mostrar que P é um S_p -subgrupo de G . Como A é um grupo de automorfismos de G e P é A -invariante, temos que para todo $y \in P$,

existe $x \in P$ tal que $\phi(x) = y$ para todo $\phi \in A$. Assim, se $g \in N = N_G(P)$, então $y^{\phi(g)} = \phi(x)^{\phi(g)} = \phi(x^g) \in P$, pois $x^g \in P$. Deste modo N é A -invariante e, portanto, A age como um grupo de automorfismos sobre N . Pelo item (i), existe um S_p -subgrupo R de N que é A -invariante. Agora note que P é um p -grupo normal de N e como consequência do Teorema de Sylow temos que P está contido em todo S_p -subgrupo de N , em particular, $P \subseteq R$. Uma vez que $Q \subseteq R$, pela escolha maximal de P , devemos ter $P = R$. Por outro lado, como P é um p -subgrupo de G segue do Teorema de Sylow que existe um S_p -subgrupo S de G tal que $P \subseteq S$. Se $P \subset S$, então pela Proposição 1.4 (i) temos $P \subset N_S(P)$. Mas $N_S(P) \subseteq S \cap N_G(P) = S \cap N$. Daí, $P \subset N \cap S$, ou seja, um S_p -subgrupo de N está contido estritamente num p -subgrupo de N , absurdo. Logo, $P = S$, como queríamos. \square

2.2 Grupos π -Separáveis

Estudaremos agora uma classe de grupos extremamente importantes para a Teoria de Grupos. Trata-se dos grupos π -separáveis. A propriedade mais interessante destes grupos é que qualquer um de seus π -subgrupos sempre está contido em um π -subgrupo de Hall e quaisquer dois π -subgrupos de Hall são conjugados. Este resultado deve-se a P. Hall e S. Cunihin, e será demonstrado mais adiante, no Teorema 2.11. Por hora vamos definir grupos π -separáveis e obter algumas propriedades básicas desta classe de grupos.

Definição 2.7 *Um grupo G é dito ser π -separável se ele possui uma série normal na qual cada fator é um π -grupo ou um π' -grupo.*

Por exemplo, se G for um grupo finito solúvel, então G é π -separável para todo conjunto de primos não vazio π , pois G possui uma série normal cujos fatores tem ordem prima.

Note que os conceitos de π -separabilidade e π' -separabilidade são equivalentes. Também é fácil provar que subgrupos e imagem homomórfica de grupo π -separável é π -separável.

Dado um grupo G , construiremos agora uma série especial de subgrupos normais. Esta série nos permitirá dar uma caracterização para grupos π -separáveis.

Definição 2.8 *Se G é um grupo, a $\pi'\pi$ -série superior de G é a série*

$$1 = P_0 \triangleleft N_0 \triangleleft P_1 \triangleleft N_1 \triangleleft \cdots \triangleleft P_m \triangleleft N_m \cdots, \quad (2.5)$$

definida por

$$\frac{N_i}{P_i} = O_{\pi'}\left(\frac{G}{P_i}\right) \text{ e } \frac{P_{i+1}}{N_i} = O_{\pi}\left(\frac{G}{N_i}\right).$$

Assim temos, por exemplo, que $N_0 = O_{\pi'}(G)$ e

$$\frac{P_1}{O_{\pi'}(G)} = \frac{P_1}{N_0} = O_{\pi}\left(\frac{G}{N_0}\right) = O_{\pi}\left(\frac{G}{O_{\pi'}(G)}\right).$$

Deste modo, P_1 é a imagem inversa em G do π -subgrupo normal maximal de $\frac{G}{O_{\pi'}(G)}$.

Algumas vezes é conveniente escrever os primeiros termos da $\pi'\pi$ -série superior N_0, P_1, N_1, \dots como

$$O_{\pi'}(G), O_{\pi'\pi}(G), O_{\pi'\pi\pi'}(G), \dots$$

Como $O_{\pi'}(G/P_i)$ e $O_{\pi}(G/N_i)$ são característicos em G/P_i e G/N_i , respectivamente, segue que N_i/P_i e P_{i+1}/N_i são característicos em G/P_i e G/N_i , respectivamente. Além disso, $N_0 \text{ char } G$, de modo que indutivamente e pelo Lema 1.8 (iii), a série (2.5) é uma série de subgrupos característicos de G cujos fatores são alternadamente π' -grupos e π -grupos.

Além da $\pi'\pi$ -série superior de um grupo, podem existir outras $\pi'\pi$ -séries, i.é, séries normais cujos fatores são, alternadamente, π' e π -grupos. O resultado a seguir relaciona estas séries de subgrupos.

Proposição 2.9 *Sejam G um grupo π -separável e*

$$1 = H_0 \triangleleft K_0 \triangleleft H_1 \triangleleft K_1 \triangleleft \cdots \triangleleft H_m \triangleleft K_m = G$$

uma $\pi'\pi$ -série, i.é, $\frac{K_i}{H_i}$ é um π' -grupo e $\frac{H_{i+1}}{K_i}$ é um π -grupo. Então $H_i \leq P_i$ e $K_i \leq N_i$, onde P_i e N_i são termos da $\pi'\pi$ -série superior de G . Em particular $N_m = G$.

Demonstração: Faremos a demonstração por indução sobre i , observando que para $i = 0$ temos $H_i \leq P_i$. Suponhamos que para algum i , $0 < i < m$, $H_i \leq P_i$. Então, $K_i P_i / P_i$ é um π' -grupo subnormal de G / P_i , pois

$$\frac{K_i P_i}{P_i} \triangleleft \frac{H_{i+1} P_i}{P_i} \triangleleft \cdots \triangleleft \frac{K_m P_i}{P_i} = \frac{G}{P_i},$$

pelo Segundo Teorema do Isomorfismo. Além disso, $|K_i P_i : P_i| = |K_i : K_i \cap P_i|$ e como $H_i \leq K_i$ e $H_i \leq P_i$, tem-se $H_i \leq K_i \cap P_i$. Logo, $|K_i P_i : P_i|$ é um divisor de $|K_i : H_i|$, que é um π' -número. Portanto, $K_i P_i / P_i$ é um π' -subgrupo subnormal de G / P_i e, assim, pela Proposição 2.2, $K_i P_i / P_i \leq O_{\pi'}(G / P_i) = N_i / P_i$, de modo que $K_i \leq K_i P_i \leq N_i$. Assim, pelo mesmo motivo de antes $H_{i+1} N_i / N_i$ é um π -subgrupo subnormal de G / N_i e novamente pela Proposição 2.2, $H_{i+1} \leq P_{i+1}$. Logo, o resultado segue por indução. \square

Segue imediatamente do resultado anterior que um grupo G é π -separável se, e somente se, ele coincide com algum termo de sua $\pi' \pi$ -série superior. Mais ainda, a $\pi' \pi$ -série superior é uma $\pi' \pi$ -série mais curta.

Para demonstrarmos o próximo resultado, precisamos de algumas definições.

Dado um grupo G , sabemos que para todo $g \in G$, a função $\mu_g : G \rightarrow G$ definida por $\mu_g(x) = g^{-1} x g$ é um automorfismo de G e o subconjunto $\text{Inn}(G) = \{\mu_g : g \in G\}$ é um subgrupo de $\text{Aut}(G)$. Uma $\text{Inn}(G)$ -série de G é uma série normal $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_l = G$, onde cada G_i $1 \leq i \leq l$ é $\text{Inn}(G)$ -invariante. Uma $\text{Inn}(G)$ -série que não admite refinamento próprio por subgrupos $\text{Inn}(G)$ -invariantes é chamado uma *série principal* de G . Cada grupo quociente da série principal é chamado um *fator principal*. Note que uma série principal não pode ser refinada por subgrupos $\text{Inn}(G)$ -invariantes, mas pode ser refinada por subgrupos que não sejam $\text{Inn}(G)$ -invariantes. Além disso, cada elemento de uma série principal é normal em G , pois cada elemento é $\text{Inn}(G)$ -invariante.

Um grupo que não possui subgrupos característicos próprios não triviais é chamado *caracteristicamente simples*. Um subgrupo normal minimal N de um grupo G é caracteristicamente simples, pois se existisse $1 \neq H < N$ tal que $H \text{ char } N$, teríamos $H \triangleleft G$, pela Proposição 1.8 (ii), contrariando a minimalidade de N .

Daremos agora uma caracterização dos grupos π -separáveis, através da

Proposição 2.10 *As seguintes propriedades de um grupo G são equivalentes:*

(i) G é π -separável;

(ii) Todo fator principal de G é um π -grupo ou um π' -grupo;

(iii) Todo fator de composição de G é um π -grupo ou um π' -grupo.

Demonstração: (i) implica (ii). Seja $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_m = G$ uma série principal de G . Como G é π -separável, cada $\overline{G_{i+1}} = \frac{G_{i+1}}{G_i}$ é π -separável. Mas estes últimos são caracteristicamente simples, pois se existir um subgrupo próprio não trivial $\overline{H_{i+1}}$ de $\overline{G_{i+1}}$ que é característico em $\overline{G_{i+1}}$, então, em particular, $\overline{H_{i+1}} \triangleleft \overline{G_{i+1}}$, o que implica $H_{i+1} \triangleleft G_{i+1}$. Além disso, H_{i+1} é $\text{Inn}(G)$ -invariante. Com efeito, se $h \in H_{i+1}$ e $\gamma_a \in \text{Inn}(G)$, então $\bar{\gamma}_a : \overline{G_{i+1}} \rightarrow \overline{G_{i+1}}$ dada por $\bar{\gamma}_a(xG_i) = (\gamma_a(x))G_i$ é um isomorfismo, pois G_{i+1} é γ_a -invariante e, assim, $\gamma_a(h) \in H_{i+1}$ se, e somente se, $\bar{\gamma}_a(hG_i) \in \overline{H_{i+1}}$. Porém, $\bar{\gamma}_a(hG_i)$ realmente pertence a $\overline{H_{i+1}}$, já que $\overline{H_{i+1}} \text{ char } \overline{G_{i+1}}$. Logo, $\gamma_a(h) \in H_{i+1}$ e H_{i+1} é $\text{Inn}(G)$ -invariante. Portanto, H_{i+1} pode ser acrescentado na série principal de modo que ela possui um refinamento próprio, contradição. Como $O_{\pi'}(\overline{G_{i+1}}) \text{ char } \overline{G_{i+1}}$, segue que $O_{\pi'}(\overline{G_{i+1}}) = 1$ ou $O_{\pi'}(\overline{G_{i+1}}) = \overline{G_{i+1}}$. Se ocorrer a segunda igualdade, então $\overline{G_{i+1}}$ é um π' -grupo e o resultado segue. Se ocorrer a primeira igualdade, então o elemento P_1 da $\pi'\pi$ -série de $\overline{G_{i+1}}$ é igual a $O_{\pi}(\overline{G_{i+1}})$. Como $O_{\pi}(\overline{G_{i+1}}) \text{ char } \overline{G_{i+1}}$ temos $O_{\pi}(\overline{G_{i+1}}) = 1$ ou $O_{\pi}(\overline{G_{i+1}}) = \overline{G_{i+1}}$. Visto que a primeira não ocorre, pois $\overline{G_{i+1}}$ é π -separável e, então, sua $\pi'\pi$ -série superior termina em $\overline{G_{i+1}}$, segue que $\overline{G_{i+1}}$ é um π -grupo e o resultado segue.

(ii) implica (iii). Refine a série principal até uma série de composição. Como cada fator de composição continua sendo um π ou π' -grupo, a implicação segue da Proposição 1.9.

(iii) implica (i). É óbvio. □

Finalmente estamos aptos a demonstrar o Teorema de P.Hall-Cunihin.

Teorema 2.11 (P.Hall-Cunihin) *Seja G um grupo π -separável. Então todo π -subgrupo de G está contido em algum π -subgrupo de Hall e quaisquer dois π -subgrupos de Hall são conjugados.*

Demonstração: Note que todo π -subgrupo de G está contido em algum π -subgrupo maximal de G , pois G é finito. Assim, é suficiente provarmos que todo π -subgrupo

maximal P é um π -subgrupo de Hall e que quaisquer dois π -subgrupos de Hall são conjugados. Isto será feito por indução sobre $|G|$, observando que o resultado é óbvio para $|G| = 1$. A hipótese de indução garante que para todo grupo π -separável \bar{G} tal que $|\bar{G}| < |G|$, o teorema é válido.

Seja $R = O_\pi(G)$ e suponhamos primeiro que $R \neq 1$. Visto que a interseção de todos os π -subgrupos maximais está contida em P , temos da Proposição 2.2 que $R \leq P$ e também $R \triangleleft P$, pois $R \triangleleft G$. Como P é um π -subgrupo maximal de G , tem-se que $\bar{P} = P/R$ é um π -subgrupo maximal de $\bar{G} = G/R$ e, pela hipótese de indução, \bar{P} é um π -subgrupo de Hall de \bar{G} , i.é, $|G : P| = |\bar{G} : \bar{P}|$ é um π' -número e, deste modo, P é um π -subgrupo de Hall de G . Se Q for outro π -subgrupo de Hall de G , então $\bar{Q} = Q/R$ é um π -subgrupo de Hall de \bar{G} . Pela hipótese de indução, existe $g \in G$ tal que $\bar{Q} = (\bar{P})^{gN} = \bar{P}^g$. Logo, $Q = P^g$, como desejado.

Agora suponhamos que $R = 1$. Como G é π -separável, G coincide com um dos termos de sua $\pi'\pi$ -série superior. Assim, temos $S = O_{\pi'}(G) \neq 1$. Sendo PS/S um π -grupo, pela hipótese de indução, PS/S está contido em algum π -subgrupo de Hall Q/S de G/S . Agora, tomando $N = S$, $G = Q$ no Corolário 2.4, temos que o π -subgrupo P está contido em algum π -subgrupo de Hall P^* de Q . Note que pela maximalidade de P , devemos ter $P = P^*$ e, conseqüentemente, P é um π -subgrupo de Hall de Q . Assim, $|G : P| = |G : Q| \cdot |Q : P|$ é um π' -número, ou seja P é um π -subgrupo de Hall de G . Se P_1 for um outro π -subgrupo de Hall de G , então do Segundo Teorema do Isomorfismo e de $P \cap S = P_1 \cap S = 1$ resulta que P_1S/S e PS/S são π -subgrupos de Hall de G/S . Pela hipótese de indução, existe $g \in G$ tal que $(P_1S/S)^{gS} = PS/S$. Assim, $P_1^g \leq PS$. Aplicando o Teorema de Schur-Zassenhaus, (com $G = PS$ e $N = S$), obtemos que P e P_1 são conjugados, e o teorema está demonstrado. \square

Demonstraremos agora um teorema que nos será muito útil futuramente.

Teorema 2.12 *Se G é um grupo π -separável, então $C_{\bar{G}}(O_\pi(\bar{G})) \leq O_\pi(\bar{G})$, onde $\bar{G} = G/O_{\pi'}(G)$.*

Demonstração: Basta supormos que $O_{\pi'}(G) = 1$ e provar que $C_G(O_\pi(G)) \leq O_\pi(G)$. De fato, se $O_{\pi'}(G) \neq 1$, vamos para o grupo quociente \bar{G} , onde teremos $O_{\pi'}(\bar{G}) = 1$ e \bar{G}

π -separável. Daí, pelo caso $O_{\pi'}(G) = 1$ obteremos que $C_{\overline{G}}(O_{\pi}(\overline{G})) \leq O_{\pi}(\overline{G})$.

Coloquemos $P = O_{\pi}(G)$ e $C = C_G(P)$. Como $P \triangleleft G$ temos $C \triangleleft G$. Pela Proposição 1.8 (ii), $P \cap C = Z(P) \triangleleft G$ e, então, tem-se $Z(P) \triangleleft C$, de modo que $Z(P) \leq O_{\pi}(C)$. Por outro lado, de $O_{\pi}(C) \text{ char } C \triangleleft G$, vem que $O_{\pi}(C) \triangleleft G$ e, assim, $O_{\pi}(C) \leq O_{\pi}(G)$. Daí, $O_{\pi}(C) \leq P \cap C = Z(P)$ e disto segue que $Z(P) = O_{\pi}(C)$.

Suponhamos que $C \not\leq P$. Então, $Z(P) < C$, de onde temos $O_{\pi}(C) = Z(P) < C$. Como C é π -separável, pois G o é, C coincide com um dos termos de sua π' -série superior. Sabemos que os subgrupos que formam esta série são característicos em C cujos fatores são alternadamente π' -grupos e π -grupos. Disso, de $O_{\pi'}(C) \leq O_{\pi'}(G) = 1$ e do fato que $O_{\pi}(C) < C$ segue que existe um subgrupo característico L de C tal que $O_{\pi}(C) < L$ e $\frac{L}{O_{\pi}(C)}$ é um π' -grupo. Assim, $O_{\pi}(C) \triangleleft L$ e $(|O_{\pi}(C)|, |L : O_{\pi}(C)|) = 1$. Pelo Teorema de Schur-Zassenhaus, existe um subgrupo K de L tal que $|K| = |L : O_{\pi}(C)|$ e, conseqüentemente, $L = KO_{\pi}(C)$ e $K \cap O_{\pi}(C) = 1$. Agora, $L = K \times O_{\pi}(C)$. De fato, $K \leq C = C_G(O_{\pi}(G))$, ou seja, os elementos de K comutam com todos os elementos de $O_{\pi}(G)$ e, em particular, com os elementos de $O_{\pi}(C)$. Disso obtemos que $K \triangleleft L$ e $L = K \times O_{\pi}(C)$. Observamos que K é um π' -subgrupo de Hall de L , pois $|K|$ é um π' -número e $(|K|, |L : K|) = 1$. Logo, segue do Teorema de Schur-Zassenhaus que se existe outro subgrupo de L com ordem igual a $|K|$, então eles são conjugados. Mas, como $K \triangleleft L$, K é o único π' -subgrupo de Hall de L e pela Proposição 2.2, $K = O_{\pi'}(L)$. Assim, $K \text{ char } L \text{ char } C \triangleleft G$ e isto implica em $K \triangleleft G$. Logo, $K \leq O_{\pi'}(G) = 1$ e, então, $L = O_{\pi}(C)$. Mas isto contradiz a escolha de L . \square

Um grupo G é π -solúvel se todo fator de composição de G é um π' -grupo ou um p -grupo para algum primo $p \in \pi$. Note que todo grupo π -solúvel é em particular π -separável. No caso em que π possui um único primo p , p -solubilidade e p -separabilidade são obviamente equivalentes, mas em geral um grupo π -separável não é π -solúvel. Por exemplo, o grupo das permutações S_5 é $\{2, 3, 5\}$ -separável mas não é $\{2, 3, 5\}$ -solúvel. Além disso, se G é um grupo solúvel então todo fator de composição é um p -grupo, de modo que para qualquer conjunto de primos π , teremos G π -solúvel. Se H for um π -grupo π -solúvel, então é claro que todo fator de composição é um p -grupo para algum primo $p \in \pi$. Também, como no caso de π -separabilidade, subgrupos e imagens homomorfas de

grupos π -solúveis são π -solúveis.

Um caso particularmente interessante de grupo π -solúvel é quando π é constituído de um único primo. Neste caso temos o

Teorema 2.13 (Hall-Higman) *Seja G um grupo p -solúvel, com $O_{p'}(G) = 1$ e coloquemos $H = O_p(G)$. Então a conjugação induz uma representação fiel de G/H sobre o espaço vetorial $H/\Phi(H)$ sobre \mathbb{Z}_p .*

Demonstração: Denotemos o grupo $\frac{H}{\Phi(H)}$ por \bar{H} . Do Teorema 1.15 (ii) segue que $\Phi(H) = H'H^p$ onde H^p é o subgrupo de G gerado por todas as p -ésimas potências de elementos de H e que $\Phi(H) \text{ char } H$. Como $H \triangleleft G$, temos $\Phi(H) \triangleleft G$. Para cada $x \in G$, definimos $\phi_x : \bar{H} \longrightarrow \bar{H}$ por $\phi_x(\bar{h}) = \overline{hxh^{-1}}$. Claramente ϕ_x é um automorfismo de \bar{H} de modo que ϕ_x é um operador linear não singular de \bar{H} , visto como espaço vetorial sobre \mathbb{Z}_p . É fácil ver que a aplicação, $\psi : G \longrightarrow GL(\bar{H}, \mathbb{Z}_p)$, definida por $\psi(x) = \phi_x$, é um homomorfismo. Deste modo, $\frac{G}{\text{Ker}\psi}$ é fielmente representado sobre $GL(\bar{H}, \mathbb{Z}_p)$.

Mostraremos que $\text{Ker}\psi = H$. Com efeito,

$$\begin{aligned} \text{Ker}\psi &= \{g \in G : \phi_g(\bar{h}) = \bar{h}, \forall h \in H\} \\ &= \{g \in G : \overline{ghg^{-1}} = \bar{h}, \forall h \in H\} \\ &= \{g \in G : [h, g^{-1}] \in \Phi(H), \forall h \in H\}. \end{aligned}$$

Assim, $H \subseteq \text{Ker}\psi$, uma vez que $H' \subseteq \Phi(H)$. Agora coloquemos $C = \text{Ker}\psi$ e $D = C_G(H)$. Sendo $H \triangleleft G$, $D \triangleleft G$. Obviamente, $D \subseteq C$ e, pelo Teorema 2.12, $D \subseteq H$, de modo que D é um p -grupo. Assim, se mostrarmos que $\frac{C}{D}$ é um p -grupo, obteremos que C é um p -grupo. Como também $C \triangleleft G$, teremos $C \subseteq O_p(G) = H$ e $H \subseteq C$, de modo que $C = H$, como desejamos.

Suponhamos que exista um p' -elemento \bar{x} não trivial em C/D e seja x um representante de \bar{x} em C . Se $\circ(x) = p^s b$, onde $s \geq 0$ e $(p, b) = 1$, então $y = x^{p^s}$ e $\bar{y} = x^{p^s} D$ são p' -elementos. Agora, $\phi : H \longrightarrow H$ dada por $\phi(h) = yhy^{-1}$ é um p' -automorfismo de H e induz a função identidade de \bar{H} , pois $y \in \text{Ker}\psi$. Assim, pelo Teorema 1.16, ϕ é o automorfismo identidade de H e, então, $y \in C_G(H) = D$. Isso nos dá que y é um p -elemento, uma contradição. Portanto, C/D é um p -grupo. \square

Teorema 2.14 *Se P é um S_p -subgrupo de um grupo p -solúvel, então*

$$C_G(P \cap O_{p'p}(G)) \subseteq O_{p'p}(G).$$

Em particular, $Z(P) \subseteq O_{p'p}(G)$.

Demonstração: Seja $Q = P \cap O_{p'p}(G)$ e $\bar{G} = G/O_{p'p}(G)$. Como $O_{p'p}(G) \triangleleft G$, segue que Q é um S_p -subgrupo de $O_{p'p}(G)$. Note que $O_{p'p}(G)$ é aplicado sobrejetivamente sobre $O_{p'p}(G)/O_{p'}(G) = O_p(\bar{G})$. A imagem de Q em $O_p(\bar{G})$ é $QO_{p'}(G)/O_{p'}(G)$, e pelo Segundo Teorema do Isomorfismo, $|QO_{p'}(G) : O_{p'}(G)| = |Q|$. Como $O_p(\bar{G})$ é um p -grupo e $|O_p(\bar{G})|$ divide $|O_{p'p}(G)| = |Q| \cdot b$, onde $p \nmid b$, temos da igualdade anterior que Q é aplicado sobrejetivamente sobre $O_p(\bar{G})$. Se $x \in C_G(Q)$, então $\bar{x} \in C_{\bar{G}}(O_p(\bar{G}))$ e, assim, $C_G(Q)$ é aplicado em $C_{\bar{G}}(O_p(\bar{G}))$. Pelo Teorema 2.12, temos que $C_{\bar{G}}(O_p(\bar{G})) \subseteq O_p(\bar{G})$ e, então, a imagem de $C_G(Q)$ está contida em $O_p(\bar{G})$, de modo que $C_G(Q) \subseteq O_{p'p}(G)$.

Visto que os elementos de $Z(P)$ comutam com os elementos de Q , temos que $Z(P) \subseteq C_G(Q) \subseteq O_{p'p}(G)$. □

Capítulo 3

p -Estabilidade

No Capítulo 1, apresentamos alguns resultados e definições de representações de um grupo finito G e também estabelecemos algumas propriedades dos grupos lineares. No que segue, estamos interessados em aplicar aqueles conceitos e resultados para obtermos informações de uma classe de grupos chamados *grupos p -estáveis*.

3.1 Grupos p -Estáveis

Se V/F é um G -módulo fiel, onde F é um corpo de característica p , nós podemos perguntar se algum p -elemento de G tem um *polinômio minimal quadrático*. A resposta para esta pergunta é de fundamental importância para o desenrolar deste trabalho. Se $p = 2$, qualquer elemento x de G de ordem 2 satisfaz o polinômio $X^2 - 1 = (X - 1)^2$ de grau 2 (sobre F) e este deve ser o polinômio minimal de x , pois caso contrário $p(X) = X - 1$ seria seu polinômio minimal e, assim, para todo $v \in V$, $(x - 1)v = 0$, de modo que $xv = v$ para todo $v \in V$, contradizendo o fato de V/F ser um G -módulo fiel. Nós vemos então que a questão levantada anteriormente é significativa apenas quando p é ímpar.

Se $G = SL(2, p)$ age de forma natural sobre um espaço vetorial bidimensional V sobre \mathbb{Z}_p , então todo elemento de G tem um polinômio característico quadrático. Assim, um p -elemento não trivial certamente tem um polinômio minimal quadrático neste caso.

Portanto, existem grupos G e G -módulos fiéis V sobre corpos de característica p , p ímpar, em que um p -elemento de G tem um polinômio minimal quadrático. Nós estamos interessados em grupos G e G -módulos onde isso não ocorra, e daremos a tais grupos um nome especial através da

Definição 3.1 *Seja G um grupo que não possui p -subgrupos normais não triviais, p ímpar. Uma representação fiel ϕ de G sobre um espaço vetorial V sobre o corpo $GF(p^n)$ será chamada p -estável se nenhum p -elemento de $\phi(G)$ tem um polinômio minimal quadrático sobre V . Mais ainda, nós dizemos que G é um grupo p -estável se todas representações fiéis de G são p -estáveis.*

Nesta seção daremos, através do Teorema 3.6, condições suficientes para que um grupo sem p -subgrupos normais não triviais seja p -estável. Este resultado pode ser visto como o mais importante desta seção e será de grande importância na seção seguinte.

Nossa análise de p -estabilidade depende do seguinte resultado:

Teorema 3.2 *Seja G um grupo de transformações lineares agindo fiel e irredutivelmente sobre um espaço vetorial V sobre um fecho algébrico F de \mathbb{Z}_p e suponha que G é gerado por dois p -elementos que têm um polinômio minimal quadrático sobre V . Então G contém um subgrupo isomorfo a $SL(2, p)$.*

Demonstração: Sejam x_1, x_2 os dois geradores dados de G . Seja $V_i = C_V(x_i) = \{v \in V : x_i v = v\}$, $1 \leq i \leq 2$. Visto que x_i é um p -elemento e F tem característica p , segue facilmente do Binômio de Newton que x_i anula $(X - 1)^2$. Além disso, x_i não anula $X - 1$ pois senão x_i seria a transformação identidade. Consequentemente, $(x_i - 1)^2 V = 0$, $1 \leq i \leq 2$, onde 1 denota a transformação identidade de V . Colocando $W_i = (x_i - 1)V$, segue que $(x_i - 1)W_i = 0$ e, assim, $W_i \subseteq V_i$, $1 \leq i \leq 2$. Daí temos $(x_i - 1)V \subseteq V_i$ e $(x_i - 1)W_i = 0$. Portanto, $x_i - 1$ é uma transformação linear de V em V_i com $Ker(x_i - 1) = V_i$. Mas $dim_F V = dim_F Ker(x_i - 1) + dim_F (x_i - 1)V = dim_F(V_i) + dim_F(x_i - 1)V \leq dim_F V_i + dim_F V_i$, pois $(x_i - 1)V \subseteq V_i$. Se escrevemos $d = dim_F V$ e $d_i = dim_F V_i$, temos que $d \leq 2d_i$, i.é, $\frac{d}{2} \leq d_i$, $1 \leq i \leq 2$.

Suponhamos que d_1 ou d_2 seja maior que $\frac{d}{2}$. Neste caso $W = V_1 \cap V_2 \neq 0$, pois se $V_1 \cap V_2 = 0$, então $\dim_F(V_1 + V_2) = d_1 + d_2 > d = \dim_F V$, absurdo. Mas W é G -invariante, pois x_1 e x_2 , que geram G , agem trivialmente sobre W . Visto que G age irreduzivelmente sobre V , obtemos $V = W$, i.é, todo elemento de G age como a transformação identidade sobre os elementos de V , contrariando o fato de G agir fielmente sobre V . Portanto, $d_1 = d_2 = \frac{d}{2}$, o que implica, $d = 2m$, onde $d_1 = d_2 = m$ e $W = 0$. Em particular, $V = V_1 \oplus V_2$.

Agora, se $v \in V_2$ então $(x_1 - 1)v \in V_1$, ou seja, $x_1 - 1$ aplica V_2 em V_1 . Como $V_1 \cap V_2 = 0$ e as dimensões de V_1 e V_2 são iguais, segue que $x_1 - 1$ é um isomorfismo de V_2 sobre V_1 . Analogamente, $x_2 - 1$ é um isomorfismo de V_1 sobre V_2 . Seja $\{v_i : 1 \leq i \leq m\}$ uma base de V_2 e $v_{m+i} = (x_1 - 1)v_i, 1 \leq i \leq m$. Então os v_{m+i} formam uma base de V_1 , de modo que $\beta_V = \{v_i : 1 \leq i \leq 2m\}$ forma uma base de V . Relativa a essa base podemos calcular a matriz das transformações $x_1, x_2 : V \rightarrow V$. Como $v_{m+i} = (x_1 - 1)v_i = x_1 v_i - v_i$, temos $x_1 v_i = v_i + v_{m+i}, 1 \leq i \leq m$. Deste modo a matriz da transformação de x_1 em relação a base β_V é

$$A_1 = \begin{pmatrix} I & 0 \\ I & I \end{pmatrix} \quad (3.1)$$

Calculemos a matriz da transformação x_2 de ordem $2m \times 2m$. Como $\{v_i : 1 \leq i \leq m\}$ é uma base de V_2 temos $x_2 v_i = v_i, 1 \leq i \leq m$. Visto que $v_{m+i} = (x_1 - 1)v_i$, obtém-se $(x_2 - 1)(v_{m+i}) = (x_2 - 1)(x_1 - 1)v_i$, e daí, $x_2(v_{m+i}) = (x_2 - 1)(x_1 - 1)v_i + v_{m+i}$, para $1 \leq i \leq m$. Mas, $(x_2 - 1)(x_1 - 1)v_i = a_{1i}v_1 + \dots + a_{mi}v_m, a_{ij} \in F$. Logo, a matriz da transformação de x_2 em relação a base $\{v_i : 1 \leq i \leq 2m\}$ é

$$A_2 = \begin{pmatrix} I & R \\ 0 & I \end{pmatrix} \quad (3.2)$$

onde R é a matriz do isomorfismo de V_1 em V_2 determinado por $x_2 - 1$ em relação a base $\{v_i : 1 \leq i \leq m\}$ de V_2 . Assim, R é não singular.

Visto que F é algebricamente fechado, existe uma matriz não singular $Q, m \times m$, tal que $S = Q^{-1}RQ$ está na forma canônica de Jordan. Se nós conjugamos as matrizes A_1

e A_2 pela matriz

$$D = \begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix} \quad (3.3)$$

o qual corresponde a uma mudança de base de V , as matrizes de x_1 e x_2 com respeito a essa nova base são, respectivamente:

$$B_1 = D^{-1}(A_1 D) = A_1 \quad (3.4)$$

$$B_2 = D^{-1}(A_2 D) = \begin{pmatrix} I & S \\ 0 & I \end{pmatrix} \quad (3.5)$$

onde $S = Q^{-1}RQ$.

Visto que S é não singular, (por ser produto de matrizes não singulares), na forma canônica de Jordan, as entradas de sua diagonal são não nulas e S é uma matriz triangular inferior. Seja λ a entrada de S no canto superior esquerdo. Finalmente, seja P a matriz permutacional $2m \times 2m$ obtida pela troca da linha 2 pela linha $m+1$ da matriz identidade e conjugue B_1 e B_2 por P . É fácil ver que com respeito a nova base correspondente $\{u_i : 1 \leq i \leq 2m\}$ de V , as matrizes C_1 e C_2 de x_1 e x_2 têm respectivamente a forma

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ & * & * & & \\ & & & & \end{pmatrix}_{2m \times 2m} \quad e \quad C_2 = \begin{pmatrix} 1 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ & * & * & & \\ & & & & \end{pmatrix}_{2m \times 2m} \quad (3.6)$$

Assim, nós vemos que x_1 e x_2 deixa invariante o subespaço U de V gerado por u_1 e u_2 . Desde que $G = \langle x_1, x_2 \rangle$, G deixa U invariante e pela irreduzibilidade de G sobre V temos $U = V$. Portanto, $\dim_F V = 2$ e G é isomorfo a um grupo gerado por $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ e $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$. Visto que $\mathbb{Z}_p(\lambda)$ é um corpo finito, nós podemos concluir do Teorema 1.29 que G contém um subgrupo isomorfo a $SL(2, p)$. \square

A seguir veremos um resultado que não diz respeito diretamente a grupos p -estáveis, mas este, juntamente com o Teorema 3.2, nos darão uma propriedade de relevo dos grupos p -estáveis.

Teorema 3.3 *Seja K uma classe de conjugação de p -elementos de um grupo G . Se todo par de elementos de K gera um p -grupo, então K está contido em um p -subgrupo normal de G .*

Demonstração: Seja $K = \{g^{-1}ag : g \in G\}$ a classe de conjugação de a cuja ordem é p^r e note que os elementos de K são p -elementos. Provaremos o teorema por indução sobre $|G|$, observando que se $|G| = 1$, o teorema é imediato. O teorema é obviamente válido para o caso $K = 1$ e, portanto, basta considerarmos dois casos:

- (i) $O_p(G) \neq 1, K \neq 1$
- (ii) $O_p(G) = 1, K \neq 1$.

Suponhamos que temos (i). Se $\phi : G \rightarrow \bar{G}$ é um homomorfismo sobrejetor de grupos, então a imagem \bar{K} de K em \bar{G} é uma classe de conjugação de p -elementos de \bar{G} e cada par de elementos de \bar{K} gera um p -grupo. Portanto, \bar{K} está nas hipóteses do teorema e se $|\bar{G}| < |G|$, pela hipótese de indução, $\bar{K} \subseteq O_p(\bar{G})$. Como $O_p(G) \neq 1$, podemos tomar, em particular, o homomorfismo canônico $\alpha : G \rightarrow \frac{G}{O_p(G)} = \bar{G}$ e concluir que $\bar{K} \subseteq O_p(\bar{G})$. Mas o Teorema da Correspondência garante que a imagem inversa L de $O_p(\bar{G})$ por α é um subgrupo normal de G que contém $\text{Ker}\alpha = O_p(G)$. Além disso, $\alpha|_L : L \rightarrow O_p(\bar{G})$ é um homomorfismo sobrejetor, de modo que pelo Primeiro Teorema do Isomorfismo, $\frac{L}{\text{Ker}(\alpha|_L)} \cong O_p(\bar{G})$. Uma vez que $\text{Ker}(\alpha|_L) \leq \text{Ker}(\alpha) = O_p(G)$ e $O_p(\bar{G})$ são p -grupos, tem-se que L é um p -grupo e, assim, L é um p -subgrupo normal de G . Visto que $K \subseteq L$, pois $\bar{K} \subseteq O_p(\bar{G})$, temos K contido em um p -subgrupo normal de G e o teorema segue.

Agora, mostraremos que o caso (ii) não pode ocorrer. Mas primeiro provaremos o seguinte:

(A) Se H é um subgrupo próprio de G , então $K \cap H \subseteq O_p(H)$.

De fato, se H é um subgrupo próprio de G , então certamente $K \cap H$ é a união de algumas classes de conjugação K_1, K_2, \dots, K_r de p -elementos de H . Visto que cada par de elementos de K_i gera um p -grupo, pois $K_i \subseteq K$, segue da hipótese de indução que cada K_i está contido em algum p -subgrupo normal de H e, assim, $K_i \subseteq O_p(H)$, para todo $1 \leq i \leq r$. Logo, $K \cap H \subseteq O_p(H)$.

Agora, introduziremos duas famílias de p -grupos:

$\mathcal{H} = \{H : H \neq 1, H \text{ não é um } S_p\text{-subgrupo de } G \text{ e } H = O_p(N_G(H))\};$

$\mathcal{H}_0 = \{H : H \neq 1, O_p(N_G(H)) \text{ não é um } S_p\text{-subgrupo de } N_G(H)\}.$

Segue do Teorema de Sylow e da definição de \mathcal{H} que se $H \in \mathcal{H}$, então $H \subset P$ para algum S_p -subgrupo P de G . Daí, temos da Proposição 1.4 (i) que $H \subset N_P(H) \subseteq N_G(H)$. Assim, $H \subset P \cap N_G(H)$ e, portanto, $H = O_p(N_G(H))$ não é um S_p -subgrupo de $N_G(H)$, de modo que $H \in \mathcal{H}_0$. Logo, $\mathcal{H} \subseteq \mathcal{H}_0$.

Vamos provar as seguintes duas propriedades dos conjuntos \mathcal{H} e \mathcal{H}_0 .

(B) Se $H_0 \in \mathcal{H}_0$, então existe $H \in \mathcal{H}$ contendo H_0 tal que $N_G(H_0) \subseteq N_G(H)$.

(C) Se $H \in \mathcal{H}$ e L é um subgrupo de G contendo $N_G(H)$, então $O_p(L) \subseteq H$.

Para provarmos (B), escolhemos um p -subgrupo H de G com $H_0 \subseteq H$ de ordem maximal tal que $N_0 = N_G(H_0) \subseteq N_G(H) = N$. Mostraremos que $H \in \mathcal{H}$. Obviamente $H \triangleleft N$ e, então, $H \subseteq H^* = O_p(N)$. Assim, $H_0 \subseteq H^*$. Além disso, como $H^* \triangleleft N$, segue que $N_0 \subseteq N_G(H^*)$. Portanto, encontramos um p -subgrupo H^* de G contendo H tal que $H_0 \subseteq H^*$ e $N_G(H_0) \subseteq N_G(H^*)$. Pela maximalidade da ordem de H , temos $|H| = |H^*|$ e, conseqüentemente, $H = H^* = O_p(N_G(H))$. Assim, para que H pertença a \mathcal{H} , resta mostrarmos que H não é um S_p -subgrupo de G . Suponhamos o contrário. Então H também será um S_p -subgrupo de $L = HN_0 \leq N_G(H)$, e disso temos que L/H será um p' -grupo. Portanto, pelo Segundo Teorema do Isomorfismo, temos que $N_0/H \cap N_0$ é um p' -grupo. Mas, como $H \cap N_0$ é um p -subgrupo normal de N_0 , então $N_0/H \cap N_0$ é um p' -grupo somente se $|H \cap N_0|$ é a maior potência de p que divide $|N_0|$, ou seja, somente se $H \cap N_0 = O_p(N_0)$ e $H \cap N_0$ é um S_p -subgrupo de N_0 . Logo, temos $O_p(N_0) = O_p(N_G(H_0))$ um S_p -subgrupo de $N_G(H_0)$ contradizendo o fato que $H_0 \in \mathcal{H}_0$. Portanto, H não é um S_p -subgrupo de G e (B) está demonstrado.

Provemos a propriedade (C). Sejam $H \in \mathcal{H}$ e L um subgrupo de G tal que $N = N_G(H) \subseteq L$. Não é difícil ver que $O_p(L)$ é a interseção de todos os S_p -subgrupos de L . Portanto, se provarmos que H é a interseção de alguns S_p -subgrupos R_i de L teremos $O_p(L) \subseteq H$.

Novamente, $O_p(N)$ é a interseção de todos os S_p -subgrupos de N que nós denotaremos por P_i , $1 \leq i \leq n$. Também temos $H = O_p(N)$, pois $H \in \mathcal{H}$. Como cada P_i é um p -subgrupo de L , temos do Teorema de Sylow que cada P_i está contido em algum S_p -

subgrupo Q_i de L . Coloquemos $M = \bigcap_{i=1}^n Q_i$ e notemos que $H = O_p(N) = \bigcap_{i=1}^n P_i \subseteq M$.

Por outro lado, $N_M(H) \subseteq M \cap N = \bigcap_{i=1}^n Q_i \cap N = \bigcap_{i=1}^n P_i = H$. Como $H \subseteq N_M(H)$, tem-se $H = N_M(H)$. Assim, se $H \subset M$, então segue da Proposição 1.4 (i) que $H \subset N_M(H)$, o que não ocorre. Deste modo, $H = M = \bigcap_{i=1}^n Q_i$, provando (C).

Para provarmos que (ii) não ocorre basta mostrarmos a seguinte afirmação:

(D) Se P e Q são quaisquer dois S_p -subgrupos de G tais que $K \cap P \cap Q \neq \emptyset$, então $K \cap P \subseteq Q$.

De fato, suponhamos que (D) seja válido. Se existir um S_p -subgrupo P de G que não contém K , então existe x em K que não está em P . Temos também que $K \cap P \neq \emptyset$, pois como a é um p -elemento, a pertence a algum S_p -subgrupo A de G . Mas, pelo Teorema de Sylow, existe $g \in G$ tal que $P = A^g$, de modo que $a^g \in A^g \cap K = P \cap K$. Tomemos $y \in K \cap P$. Deste modo, $x, y \in K$ e pela hipótese $\langle x, y \rangle$ é um p -grupo e, portanto, $\langle x, y \rangle$ está contido em algum S_p -subgrupo Q de G . Assim, $y \in K \cap P \cap Q$, e item (D) implica que $K \cap P \subseteq Q$, de modo que $K \cap P \subseteq K \cap Q$. Analogamente, pelo item (D) temos que $K \cap Q \subseteq P$, e então $K \cap Q \subseteq K \cap P$. Portanto, $K \cap P = K \cap Q$. Porém, x pertence a $K \cap Q$ e não pertence a $K \cap P$, uma contradição. Logo, o S_p -subgrupo tomado acima não existe, e, deste modo, $K \subseteq O_p(G) = 1$, contradição, pois $K \neq 1$.

Suponhamos que (D) seja falso. Então existe pelo menos um par de S_p -subgrupos P e Q de G tais que $K \cap P \cap Q \neq \emptyset$ com $K \cap P \not\subseteq Q$. Dentre todos tais pares vamos escolher P e Q de tal maneira que $H = P \cap Q$ tenha ordem maximal. Note que $P \neq Q$, e disso obtemos facilmente que $H \subset P$ e $H \subset Q$. Seja $N = N_G(H)$ e sejam R e S S_p -subgrupos de G tais que $R \cap N$ e $S \cap N$ são S_p -subgrupos de N com $N_P(H) \subseteq R \cap N$ e $N_Q(H) \subseteq S \cap N$. Como, pela Proposição 1.4 (i), $H \subset N_P(H)$ e $H \subset N_Q(H)$, $H \subset P \cap R$ e $H \subset Q \cap S$. Disso obtemos $K \cap P \cap R \neq \emptyset$ e $K \cap S \cap Q \neq \emptyset$. Pela escolha de P e Q , devemos ter $K \cap P \subseteq R$ e $K \cap S \subseteq Q$. Assim sendo, (D) deve ser falso para o par R, S , pois caso contrário, teríamos $K \cap R \subseteq S$ e, conseqüentemente, $K \cap P \subseteq K \cap R \subseteq K \cap S \subseteq Q$, o que não ocorre. Mais ainda, como $R \cap N$ e $S \cap N$ são S_p -subgrupos de N e $O_p(N) \triangleleft N$, temos $O_p(N) \subseteq R \cap N$ e $O_p(N) \subseteq S \cap N$, de modo que $O_p(N) \subseteq R \cap S$. Além disso,

visto que H é um p -grupo e $H \triangleleft N$, segue que $H \subseteq O_p(N)$. Assim, $H \subseteq R \cap S$ e então $\emptyset \neq K \cap H \subseteq K \cap R \cap S$. Logo, encontramos dois S_p -subgrupos R, S de G tais que $K \cap R \cap S \neq \emptyset$ e $K \cap R \not\subseteq S$. Pela escolha maximal de P e Q temos $|R \cap S| \leq |H|$. Visto que $H \subseteq R \cap S$, segue que $|H| = |R \cap S|$ e $H = R \cap S$. Daí, como $H \subseteq O_p(N) \subseteq R \cap S$, tem-se $H = O_p(N)$. Disso, de $H \neq 1$ e de H não ser S_p -subgrupo de G , segue que $H \in \mathcal{H}$. Note que $R \cap N$ e $S \cap N$ são S_p -subgrupos de N . Uma vez que $|R \cap S|$ é também maximal e (D) é falso para R, S , podemos substituir P, Q por R, S , se necessário. Assim, podemos supor que $P \cap N$ e $Q \cap N$ são S_p -subgrupos de N .

Nós produzimos, portanto, um par (H, P) com $H \in \mathcal{H}$ e P um S_p -subgrupo de G tal que $H \subseteq P$, $K \cap H \neq \emptyset$, $K \cap P \not\subseteq H$ e $P \cap N_G(H)$ é um S_p -subgrupo de $N_G(H)$. Dentre todos os pares que satisfazem estas condições, escolhamos (H^*, P^*) tal que $|P^* \cap N_G(H^*)|$ seja maximal. Para obtermos uma contradição basta mostrarmos que

$$(E) \quad P^* \subseteq N_G(H^*).$$

De fato, suponhamos (E) válido e seja $N^* = N_G(H^*)$. Visto que $H^* = O_p(N^*)$, e $O_p(G) = 1$, temos $N^* \subset G$. Assim, por (A) obtemos $K \cap N^* \subseteq H^*$. Por (E) , $K \cap P^* \subseteq K \cap N^*$ e, assim, $K \cap P^* \subseteq H^*$, contradizendo a escolha de (H^*, P^*) .

Vamos provar (E) . Suponhamos que $P^* \not\subseteq N^*$ e sejam $H_0 = \langle K \cap H^* \rangle$ e $N_0 = N_G(H_0)$. Claramente, os elementos de $K \cap H^*$ são permutados pela conjugação por elementos de N^* . Disso obtemos $H_0 \triangleleft N^*$ e, portanto, $N^* \subseteq N_0$. Além disso, como no parágrafo anterior, tem-se $K \cap N^* \subseteq H^*$. Visto que $H^* \subseteq P^*$, segue que $K \cap N^* \cap P^* \subseteq H^*$ e isto implica, $K \cap P^* \cap N^* \subseteq K \cap H^*$. Por outro lado, como H^* é um p -grupo, $H^* \triangleleft N^*$ e $P^* \cap N^*$ é um S_p -subgrupo de N^* , temos que $H^* \subseteq P^* \cap N^*$ de modo que $K \cap H^* \subseteq K \cap P^* \cap N^*$. Logo, $K \cap P^* \cap N^* = K \cap H^*$. Isto implica que $N_{P^*}(P^* \cap N^*)$ permuta por conjugação os elementos de $K \cap H^*$ e, portanto, $N_{P^*}(P^* \cap N^*)$ normaliza H_0 , ou ainda $N_{P^*}(P^* \cap N^*) \subseteq N_0$. Visto que $P^* \cap N^* \subset P^*$, nós obtemos da Proposição 1.4 (i) que $P^* \cap N^* \subset N_{P^*}(P^* \cap N^*) \subseteq N_0 \cap P^*$. Logo, $P^* \cap N^* \subset P^* \cap N_0$. Por outro lado, como $H^* \in \mathcal{H}$ e N_0 contém N^* , tem-se do item (C) que $O_p(N_0) \subseteq H^*$. Portanto, $O_p(N_0) \subset P^* \cap N_0$ e, assim sendo, $O_p(N_0)$ não é um S_p -subgrupo de N_0 concluindo-se que $H_0 \in \mathcal{H}_0$.

Finalmente, pela propriedade (B) existe $H_1 \in \mathcal{H}$ com $H_0 \subseteq H_1$ tal que $N_0 \subseteq N_1$,

onde $N_1 = N_G(H_1)$. Seja P_1 um S_p -subgrupo de G tal que $P_1 \cap N_1$ é um S_p -subgrupo de N_1 . Como $N_0 \subseteq N_1$, segue que $P^* \cap N_0 \subseteq P^* \cap N_1$. Deste modo, $|P_1 \cap N_1| \geq |P^* \cap N_0| > |P^* \cap N^*|$ e $\emptyset \neq K \cap H^* \subseteq K \cap H_1$. Assim encontramos um par (H_1, P_1) , com $H_1 \in \mathcal{H}$ e P_1 um S_p -subgrupo de G , tal que $K \cap H_1 \neq \emptyset$ e $|P_1 \cap N_G(H_1)| > |P^* \cap N_G(H^*)|$. Também, H_1 é um p -subgrupo normal de N_1 , de modo que H_1 está contido em todos os S_p -subgrupos de N_1 , em particular, $H_1 \subseteq P_1 \cap N_1 \subseteq P_1$. Pela escolha de (H^*, P^*) , temos $K \cap P_1 \subseteq H_1$. Uma vez que $N^* \subseteq N_1$, outra aplicação de (C) resulta que $H_1 = O_p(N_1) \subseteq H^*$. Assim, $K \cap P_1 \subseteq H_1 \subseteq H^*$, e visto que $H^* \subseteq P^*$, obtemos $K \cap P_1 \subseteq K \cap P^*$. Mas, pelo Teorema de Sylow, existe $g \in G$ tal que $P^* = P_1^g$ de modo que $|K \cap P_1| = |K \cap P^*|$. Logo, $K \cap P^* = K \cap P_1 \subseteq H^*$, contradizendo a escolha de (H^*, P^*) . Isto conclui a prova de (E). \square

Observação 3.4 *Seja V/F um espaço vetorial sobre um corpo F de característica p e $T \in GL(V, F)$ um p -elemento. Então, existe $r \in \mathbb{N}$ tal que $T^{p^r} = 1$, de modo que T satisfaz o polinômio $P(X) = X^{p^r} - 1$ sobre F . Por outro lado, pelo Binômio de Newton, e por F ter característica p , temos $P(X) = (X - 1)^{p^r}$. Como o polinômio minimal $m(X)$ de T divide $P(X)$, $m(X) = (X - 1)^s$, para algum $s \in \mathbb{N}$.*

Dizemos que um grupo K está envolvido em G se K é isomorfo a uma imagem homomorfa de um subgrupo H de G . O nosso próximo resultado nos diz que sob determinadas condições um grupo não p -estável envolve $SL(2, p)$.

Teorema 3.5 *Seja G um grupo sem p -subgrupos normais além dos triviais, p ímpar. Se G não é p -estável, então G envolve $SL(2, p)$.*

Demonstração: Nós precisamos mostrar que uma imagem homomórfica de algum subgrupo de G é isomorfa a $SL(2, p)$. Como G não é p -estável, existe uma representação fiel ϕ de G sobre um espaço vetorial V sobre $GF(p^n)$, para algum n , que não é p -estável, i.é., algum p -elemento de $\phi(G)$ tem polinômio minimal quadrático. Nós olharemos V como um espaço vetorial sobre o fecho algébrico F de $GF(p^n)$ e V/F como um G -módulo, lembrando que a ação de $g \in G$ sobre $u \in V$ é dada por $gu = (\phi(g))u$. Seja $x \in G$ um p -elemento de G com polinômio minimal quadrático.

Se K é a classe de conjugação contendo x , então todo elemento de K possui polinômio minimal quadrático sobre V , pois se $P(X) = X^2 + aX + b$, $a, b \in F$ é o polinômio minimal de x sobre V e se $g^{-1}xg \in K$, com $g \in G$, então para todo $v \in V$, tem-se $(P(g^{-1}xg))(v) = 0$. Além disso, $g^{-1}xg$ não anula $X - 1$, pois ϕ é fiel. Também, como G não possui p -subgrupos normais não triviais, a contra-positiva do Teorema 3.3 garante a existência de um elemento $y \in K$ tal que $H = \langle x, y \rangle$ não é um p -grupo.

Seja

$$V = V_1 \supset V_2 \supset \cdots \supset V_{m+1} = 0 \quad (3.7)$$

um seqüência de subespaços H -invariantes de V tal que H age irreduzivelmente sobre cada $\bar{V}_i = \frac{V_i}{V_{i+1}}$, $1 \leq i \leq m$ e seja N_i o kernel da representação de H sobre \bar{V}_i . Mostraremos agora que $N_i \subset H$ para algum i , $1 \leq i \leq m$. Suponhamos que para todo i , $1 \leq i \leq m$, tenhamos $H = N_i$. Como H não é um p -grupo, existe um primo $q \neq p$, tal que q divide $|H|$. Assim sendo, H possui um p' -subgrupo não trivial Q . Uma vez que $H = N_i$ para todo i e $Q \subset H$, temos $Q \subset N_i$ para todo i , ou seja, Q induz a transformação identidade sobre \bar{V}_i . Em resumo temos: Q age sobre V/F ; a característica de F é relativamente prima com $|Q|$; na seqüência (3.7) cada V_i é Q -invariante; Q age trivialmente sobre cada \bar{V}_i . Então pela Proposição 1.26, Q age trivialmente sobre V , contradizendo o fato de G ser um G -módulo fiel.

Assim, $N_i \subset H$ para algum i . Para tal i , sejam $\bar{H} = \frac{H}{N_i}$ e \bar{x}, \bar{y} , respectivamente, as imagens de x, y em \bar{H} pelo homomorfismo canônico de modo que $\bar{H} = \langle \bar{x}, \bar{y} \rangle$. Como o polinômio minimal de x tem grau 2, o polinômio minimal de \bar{x} sobre \bar{V}_i é $(X - 1)^2$ ou $(X - 1)$, pela observação anterior. Se for $X - 1$, então \bar{x} age trivialmente sobre \bar{V}_i , de modo que $\bar{x} = 1$ e $\bar{H} = \langle \bar{y} \rangle$ é um p -grupo. Como \bar{H} age irreduzivelmente sobre \bar{V}_i e \bar{H} age fielmente sobre \bar{V}_i , pois apenas os elementos de N_i agem trivialmente sobre \bar{V}_i e N_i é o elemento neutro de \bar{H} , temos que \bar{H} é um p -grupo não trivial agindo fiel e irreduzivelmente sobre \bar{V}_i/F . Pela Proposição 1.25 (i), $\bar{H} = 1$ e, então, $N_i = H$, contradizendo nossa escolha de i . Logo, \bar{x} tem polinômio minimal de grau 2 sobre \bar{V}_i . Analogamente, \bar{y} tem polinômio minimal de grau 2.

Agora, \bar{H} pode ser visto como um grupo de transformações lineares agindo fiel e irreduzivelmente sobre \bar{V}_i/F onde F é o fecho algébrico de \mathbb{Z}_p . Além disso, \bar{H} é gerado

por dois elementos \bar{x} e \bar{y} que possuem polinômio minimal quadrático. Sendo essas exatamente as hipóteses do Teorema 3.2, temos que \bar{H} contém um subgrupo isomorfo a $SL(2, p)$. Portanto, $SL(2, p)$ é isomorfo a uma imagem homomorfa de algum subgrupo de G , provando o teorema. \square

O último resultado é o mais importante dessa seção e ele nos dará condições suficientes para que um grupo seja p -estável.

Teorema 3.6 *Seja G um grupo que não possui p -subgrupos normais não triviais, com p ímpar, satisfazendo uma das seguintes condições:*

- (a) G é de ordem ímpar;
- (b) Um S_2 -subgrupo de G é abeliano;
- (c) G é solúvel e ou $p \geq 5$, ou $p = 3$ e $SL(2, 3)$ não está envolvido em G .

Então, G é p -estável.

Demonstração: (a) Suponhamos que G tenha ordem ímpar e seja ϕ um homomorfismo qualquer de G e H um subgrupo de G . Então $|\phi(H)|$ é ímpar. Uma vez que $SL(2, p)$ tem ordem par a contra-positiva do Teorema 3.5 garante que G é p -estável.

(b) Agora seja S um S_2 -subgrupo de G e suponhamos que G não é p -estável. Então pelo Teorema 3.5 existem um subgrupo H de G e um homomorfismo de grupos $\phi : H \rightarrow J$ tal que $SL(2, p)$ é isomorfo a J . Como todos os S_p -subgrupos de J são isomorfos, temos que todo S_2 -subgrupo K de J é isomorfo ao grupo dos quatérnios generalizado pela Proposição 1.28 (i). Visto que ϕ é sobrejetora, existem subgrupos R, Q de S tais que $Q \triangleleft R$ e $\frac{R}{Q} \cong K$. Assim, $\frac{R}{Q}$ é isomorfo a um grupo quatérnio. Como este grupo não é abeliano, S também não é.

(c) Se G é solúvel, $p = 3$ e $SL(2, 3)$ não está envolvido em G então G é p -estável pelo Teorema 3.5. Suponha que G seja solúvel e $p \geq 5$. Note que pelo Lema 1.28 (iii), $SL(2, p)$ não é solúvel para $p \geq 5$. Por outro lado, grupos solúveis não envolvem grupos não solúveis, pelo Proposição 1.10 (i). Assim, $SL(2, p)$ não está envolvido em G e, portanto, G é p -estável, pelo Teorema 3.5. \square

3.2 p -Estabilidade em Grupos p -Solúveis

Nesta seção vamos estudar p -estabilidade para o caso particular em que os grupos são p -solúveis. Nossos resultados sobre p -estabilidade juntamente com as propriedades gerais de grupos p -solúveis estabelecidos nas duas seções anteriores nos dão três resultados muito interessantes. O primeiro deles, nos dá uma condição suficiente para que um grupo p -solúvel seja p -estável, para p um primo ímpar.

Teorema 3.7 *Seja G um grupo p -solúvel em que $O_p(G) = 1$ e suponhamos que $p \geq 5$ ou $p = 3$ e $SL(2, 3)$ não está envolvido em G . Então G é p -estável.*

Demonstração: Suponhamos que G não seja p -estável, i.é, existe uma representação fiel ϕ de G sobre um espaço vetorial V sobre $GF(p^n)$ tal que algum p -elemento $\phi(x) \in \phi(G)$ possui um polinômio minimal quadrático.

Sejam $P = \langle x \rangle$ e $|P| = p^r$, $H = O_{p'}(G)$. Visto que $O_{(p')'}(G) = O_p(G) = 1$, tomando $\pi = \{p'\}$ no Teorema 2.12 temos $C_G(H) \leq H$. Daí, como $P \cap H = 1$, $C_P(H) = 1$. Assim, a aplicação $\phi : P \longrightarrow \text{Aut}(H)$ definida por $\phi(a) = \gamma_{a^{-1}}$ é um homomorfismo injetor, onde $\gamma_a(h) = h^a$ para todo $h \in H$. Deste modo, $P \cong \text{Im } \phi$ e $|\text{Im } \phi| = p^r$. Então P pode ser visto como um grupo de automorfismos de H . Tomando π como sendo o conjunto dos divisores primos de H e $G = H$ no Teorema 2.6 (i), temos que P deixa um S_q -subgrupo Q de H invariante por conjugação, para cada primo $q \in \pi$. Visto que $\Omega_1(P) = \langle g \in P : \circ(g) = p \rangle$ não centraliza H , temos que $\Omega_1(P)$ não centraliza algum Q e, claramente, para tal Q , temos $C_P(Q) = 1$.

Seja $K = PQ$. Então $O_p(K) \subseteq P$. Como para todo $h \in O_p(K)$ e $g \in Q$, $h^{-1}g^{-1}hg \in O_p(K)$, pois $O_p(K) \triangleleft K$, temos $[O_p(K), Q] \subseteq O_p(K) \subseteq P$. Também, $h^{-1}g^{-1}hg \in Q$, pois P deixa Q invariante por conjugação, de modo que $h^{-1}g^{-1}hg \in Q$, i.é, $[O_p(K), Q] \subseteq Q$. Disso temos $[O_p(K), Q] \subseteq P \cap Q = 1$. Portanto, $O_p(K)$ centraliza Q e do fato de $O_p(K) \subseteq P$, segue que $O_p(K) \subseteq C_P(Q) = 1$. Como $|K| = |P||Q| = p^r q^s$, temos do Teorema de Burnside que K é solúvel. Além disso, K não possui nenhum p -subgrupo normal não trivial, pois $O_p(K) = 1$. Mais ainda, $SL(2, 3)$ não está envolvido em K para

$p = 3$. Portanto, K é p -estável pelo Teorema 3.6 (iii). Visto que $x \in K$ e K é fielmente representado sobre V , pois G o é, temos que x não possui polinômio minimal quadrático, contradizendo nossa escolha. \square

Chamaremos um grupo p -solúvel de *fortemente p -solúvel* se $p \geq 5$ ou se $p = 3$ e $SL(2, 3)$ não está envolvido em G . Por exemplo, S_3 é fortemente 3-solúvel. De fato, S_3 é 3-solúvel por ser solúvel. Uma imagem homomorfa de qualquer subgrupo de S_3 tem ordem 1, 2, 3 ou 6. Visto que $SL(2, 3)$ tem ordem 24, temos que $SL(2, 3)$ não está envolvido em S_3 e, portanto, S_3 é fortemente 3-solúvel. Além disso, todo grupo \mathbb{Z}_p , $p \geq 5$, é fortemente p -solúvel.

Note que com este novo conceito, o Teorema 3.7 pode ser enunciado da seguinte forma: *Todo grupo G fortemente p -solúvel com $O_p(G) = 1$ é p -estável.*

Os subgrupos abelianos normais de um S_p -subgrupo de um grupo fortemente p -solúvel G estão contidos em um subgrupo particular de G como nos mostra o

Teorema 3.8 *Se P é um S_p -subgrupo de um grupo fortemente p -solúvel G , então todo subgrupo abeliano normal de P está contido em $O_{p'}(G)$.*

Demonstração: Basta supormos $O_{p'}(G) = 1$ e mostrarmos que todo subgrupo abeliano normal A de P é tal que $A \subseteq O_p(G)$. De fato, sejam $G_1 = G/O_{p'}(G)$ e $P_1 = P/O_{p'}(G)$. Como $O_{p'}(G_1) = 1$ e P_1 é um S_p -subgrupo de G_1 , $A_1 = A/O_{p'}(G)$ é um subgrupo abeliano normal de P_1 e claramente G_1 é fortemente p -solúvel. Segue então que $A_1 \subseteq O_p(G_1) = O_{p'}(G)/O_{p'}(G)$, o que implica $A \subseteq O_{p'}(G)$. Portanto, suponhamos que $O_{p'}(G) = 1$. Sejam $R = O_p(G)$, $V = R/\Phi(R)$ e $\overline{G} = G/R$. Então, pelo Teorema 2.13, \overline{G} é fielmente representado sobre o espaço vetorial V sobre \mathbb{Z}_p . Mas \overline{G} também é fortemente p -solúvel e $O_p(\overline{G}) = \overline{1}$. Portanto, pelo Teorema 3.7, \overline{G} é p -estável, de modo que a representação de \overline{G} sobre V é p -estável.

Agora seja A um subgrupo normal abeliano de P e \overline{A} a sua imagem em \overline{G} . Visto que $A \triangleleft P$, $[P, A] \subseteq A$ e como A é abeliano, temos $[P, A, A] = 1$. Como R é a interseção de todos os S_p -subgrupos de G , $R \subseteq P$, de modo que $[R, A, A] = 1$. Consequentemente, $\left[\begin{array}{ccc} R & A\Phi(R) & A\Phi(R) \\ \Phi(R) & \Phi(R) & \Phi(R) \end{array} \right] = 1$. Como a ação de \overline{G} sobre V é a induzida por conjugação, (veja Teorema 2.13), temos $[V, \overline{A}, \overline{A}] = 1$.

Pelo Teorema 1.7, cada $\bar{x} \in \bar{A}$ induz um operador linear de V que satisfaz o polinômio $(X - 1)^2$. Visto que seu polinômio minimal divide $(X - 1)^2$ e que a representação de \bar{G} sobre V é p -estável, segue que o polinômio minimal de \bar{x} é $X - 1$, para todo $\bar{x} \in \bar{A}$. Assim, \bar{A} age trivialmente sobre V . Como a representação de \bar{G} sobre V é fiel, temos que $\bar{A} = \bar{1}$ e, portanto, $A \subseteq R = O_p(G)$. \square

Lema 3.9 *Seja G um grupo fortemente p -solúvel e P um p -subgrupo de G . Se $N \leq N_G(P)$, então existe um subgrupo normal K de P invariante por conjugação por elementos de N tal que $\frac{P}{K}$ é um p -grupo abeliano elementar e tal que N age irreduzivelmente por conjugação sobre P/K .*

Demonstração: Visto que $\Phi(P) \text{ char } P$, $\Phi(P)$ é invariante pela conjugação por elementos de N . Além disso, $\bar{P} = \frac{P}{\Phi(P)}$ é um p -grupo abeliano elementar. Assim, se N age irreduzivelmente por conjugação sobre \bar{P} então o teorema segue. Senão, existe um subgrupo K satisfazendo as seguintes condições: $P \supset K \supset \Phi(P)$, $K \triangleleft P$ e K é invariante pela conjugação por elementos de N . Dentre todos os subgrupos de P que satisfazem essas condições, seja K um de ordem maximal. Logo, N age irreduzivelmente sobre $\frac{P}{K}$. Agora, seja $gK \in \frac{P}{K}$. Como \bar{P} é um p -grupo abeliano elementar, temos que existe um inteiro r tal que $g^{p^r} \Phi(P) = \Phi(P)$, ou seja, $g^{p^r} \in \Phi(P) \subset K$. Além disso, $P' \subseteq P'P^p = \Phi(P) \subset K$. Da Proposição 1.1, temos que $\frac{P}{K}$ é abeliano. Portanto $\frac{P}{K}$ é um p -grupo abeliano elementar e o lema está provado. \square

Sejam G um grupo, A um subgrupo de $\text{Aut}(G)$. É fácil ver que se N é um subgrupo normal A -invariante de G e $\phi \in A$, então a aplicação $\phi^* : G/N \rightarrow G/N$ definida por $\phi^*(gN) = \phi(g)N$ é um automorfismo de G/N . Diremos que A age trivialmente sobre G/N se ϕ^* é a função identidade de G/N para todo $\phi \in A$.

Sejam G um grupo, A um subgrupo de $\text{Aut}(G)$ e

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1 \tag{3.8}$$

uma série normal de G . Dizemos que A estabiliza a série (3.8), se cada G_i é A -invariante e A age trivialmente sobre cada fator $\frac{G_{i-1}}{G_i}$, $1 \leq i \leq n$.

Veremos agora uma condição necessária e suficiente para que um subgrupo de $\text{Aut}(G)$ estabilize uma série normal de G .

Lema 3.10 *Um subgrupo A de $\text{Aut}(G)$ estabiliza a série normal*

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1 \quad (3.9)$$

se, e somente se, cada G_i é A -invariante e $[G_i, A] \subseteq G_{i+1}$, $0 \leq i \leq n - 1$.

Demonstração: Isso segue do fato que $\phi^*(xG_{i+1}) = xG_{i+1}$ para todo $x \in G_i$ e $\phi \in A$ se, e somente se, $x^{-1}\phi(x) = [x, \phi] \in G_{i+1}$ para todo $x \in G_i$ e $\phi \in A$. \square

Com este lema podemos provar o

Teorema 3.11 *Seja A um p' -grupo de automorfismos do p -grupo P que estabiliza alguma série normal de P . Então, $A = 1$.*

Demonstração: Seja $P = P_0 \supseteq P_1 \supseteq \cdots \supseteq P_n = 1$ uma série normal de P estabilizada por A . Procederemos por indução sobre n , observando que o resultado é óbvio para $n = 1$. A hipótese de indução garante que se A estabiliza uma normal de comprimento $< n$ de um p -grupo, então $A = 1$. Note que se $\phi \in A$, $\phi|_{P_1} \in \text{Aut}(P_1)$ e, então, A induz um p' -grupo de automorfismos de P_1 e A estabiliza a série normal $P_1 \supseteq \cdots \supseteq P_n = 1$ de P_1 . Pela hipótese de indução, A age trivialmente sobre P_1 . Além disso, A age trivialmente sobre $\frac{P}{P_1}$, por hipótese. Logo, $[x, \phi] \in P_1$, para todo $x \in P$ e $\phi \in A$. Daí, $\phi(x) = xz$, para algum $z \in P_1$. Como ϕ age trivialmente sobre P_1 , $\phi^2(x) = \phi(xz) = \phi(x)\phi(z) = (xz)z = xz^2$. Segue facilmente, por indução, que $\phi^i(x) = xz^i$, para todo i . Em particular, se $m = o(\phi)$, temos $x = \phi^m(x) = xz^m$, de modo que $z^m = 1$. Como p não divide m e z é um p -elemento, temos que $z = 1$ e, assim, $\phi(x) = x$ para todo $x \in P$ e todo $\phi \in A$, ou seja, $A = 1$. \square

A forma mais conveniente deste resultado é dado pelo

Corolário 3.12 *Se A é um subgrupo do grupo dos automorfismos de um p -grupo P tal que A estabiliza alguma série normal de P , então A é um p -grupo.*

Demonstração: Se $\phi \in A$ e p não é um divisor de $\circ(\phi)$, pelo Teorema 3.11, $\langle \phi \rangle = 1$. Em outras palavras, A não possui p' -automorfismos não triviais. Portanto, A é um p -grupo. \square

Para finalizar esta seção, apresentaremos um resultado que será de grande utilidade para o estudo dos Teoremas de Glauberman e de Thompson no próximo capítulo.

Teorema 3.13 *Sejam G um grupo fortemente p -solúvel e P um p -subgrupo de G tal que $O_{p'}(G)P \triangleleft G$. Então, se A é um p -subgrupo de $N_G(P)$ com a propriedade $[P, A, A] = 1$, temos*

$$\frac{AC_G(P)}{C_G(P)} \subseteq O_p\left(\frac{N_G(P)}{C_G(P)}\right).$$

Demonstração: Seja $N = N_G(P)$. Aplicando o Lema 3.9 tantas vezes quantas forem necessárias, construímos uma série normal N -invariante de P ,

$$P = P_1 \supset P_2 \supset \cdots \supset P_{n+1} = 1 \tag{3.10}$$

tal que cada $\bar{P}_i = \frac{P_i}{P_{i+1}}$ é abeliano elementar e N age irreduzivelmente sobre \bar{P}_i por conjugação.

Seja H_i o kernel da representação de N sobre \bar{P}_i . Como $\bar{N}_i = \frac{N}{H_i}$ age fiel e irreduzivelmente sobre \bar{P}_i , visto como um espaço vetorial sobre \mathbb{Z}_p , temos que $O_p(\bar{N}_i) = \bar{1}$ pelo Teorema 1.25 (ii). Logo, como \bar{N}_i é fortemente p -solúvel, pois N o é, segue do Teorema 3.7 que \bar{N}_i é p -estável.

Por outro lado, como $[P, A, A] = 1$, da mesma maneira que no Teorema 3.8, temos $[\bar{P}_i, \bar{A}_i, \bar{A}_i] = 1$, onde \bar{A}_i é a imagem de A em \bar{N}_i . Mas segue do Teorema 1.7, como na prova do Teorema 3.8, que $\bar{A}_i = \bar{1}$ e portanto, $A \subseteq H_i$, para todo i , $1 \leq i \leq n$. Concluimos que $A \subseteq H = \bigcap_{i=1}^n H_i$. Mas como $H \leq N$, segue que cada P_i é H -invariante, $1 \leq i \leq n+1$ e pela definição de cada H_i , temos que H age trivialmente sobre cada \bar{P}_i , $1 \leq i \leq n+1$. Como $C = C_G(P)$ fixa, por conjugação, os elementos de P , temos, claramente, que C fixa cada \bar{P}_i por conjugação. Assim, $C \subseteq H$. Uma vez que $H \leq N$, cada elemento $a \in H$ induz por conjugação um automorfismo γ_a de P , de modo que a aplicação $\gamma : H \rightarrow \text{Aut}(P)$

definida por $\gamma(a) = \gamma_a$, é um homomorfismo, com $Ker \gamma = C \cap H = C$. Portanto, $\frac{H}{C} \cong Im \gamma$ e, assim, podemos ver H/C como um subgrupo de $Aut(P)$. Disso e do que vimos antes, temos que H/C estabiliza a série (3.10) e, então, pelo Corolário 3.12 temos que H/C é um p -grupo. Mas, $H/C \triangleleft N/C$, e, portanto, $H/C \leq O_p(N/C)$. Como $A \subseteq H$ e $C \triangleleft H$, temos $AC \leq H$, de modo que, $AC/C \leq H/C$. Logo, $AC/C \leq O_p(N/C)$. \square

Capítulo 4

Os Teoremas de Glauberman-Thompson

Neste capítulo iremos estudar vários resultados, e muitos destes são atribuídos aos grandes matemáticos George Glauberman e John Thompson. No entanto, nosso principal objetivo é demonstrar dois teoremas notáveis na Teoria de Grupos. O primeiro deles, conhecido como Teorema da p -Nilpotência de Glauberman-Thompson, diz simplesmente que se o normalizador de um determinado subgrupo H de um grupo finito G é p -nilpotente, p primo ímpar, então o grupo G também é p -nilpotente, enquanto o segundo dá uma condição suficiente para que um grupo finito seja solúvel. As demonstrações são relativamente extensas, mas não difíceis de serem entendidas e dependem basicamente de vários resultados preliminares, dos quais alguns já foram vistos em seções anteriores e outros serão apresentados no decorrer deste capítulo. Mais ainda, ambas as demonstrações dependem da construção do subgrupo H mencionado acima. Isto não é uma tarefa complicada, porém, nós precisaremos de várias propriedades deste subgrupo até estarmos aptos para ver estes dois resultados.

Neste capítulo todos os grupo serão finitos, a menos que se mencione o contrário.

4.1 Subgrupo de Thompson

Seja G um grupo fortemente p -solúvel, com p ímpar, e P um S_p -subgrupo. Nesta seção, iremos construir um subgrupo H de P tal que $Z(H) \triangleleft G$. Estabeleceremos este resultado posteriormente e ressaltamos que sua demonstração é devida a G. Glauberman e depende, em partes, de resultados e conceitos de J. Thompson.

Para qualquer p -grupo P , definimos $\mathcal{A}(P)$ como sendo o conjunto de todos os subgrupos abelianos de P de ordem maximal.

Exemplo 4.1 *Considere o clássico grupo multiplicativo $\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$, chamado Grupo Quatérnio, que satisfaz as seguintes relações: $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$. É fácil ver que os únicos subgrupos abelianos de ordem maximal de \mathbb{H} são $\langle i \rangle, \langle j \rangle, \langle k \rangle$ e, assim, $\mathcal{A}(\mathbb{H}) = \{\langle i \rangle, \langle j \rangle, \langle k \rangle\}$.*

Os elementos de $\mathcal{A}(P)$ possuem a seguinte propriedade básica:

Lema 4.2 *Se $A \in \mathcal{A}(P)$, então $A = C_P(A)$; em particular, $Z(P) \subseteq A$.*

Demonstração: Claramente $A \subseteq C_P(A)$. Agora, tomemos $x \in C_P(A)$ e consideremos o subgrupo $\langle A, x \rangle$ de P . Como A é abeliano e $x \in C_P(A)$ temos que $\langle A, x \rangle$ é abeliano e contém A . Pela maximalidade de A , devemos ter $x \in A$. Logo, $A = C_P(A)$. Visto que $Z(P) \subseteq C_P(A)$, tem-se $Z(P) \subseteq A$. \square

Seja P um p -grupo. O subgrupo $\mathcal{J}(P) = \langle A : A \in \mathcal{A}(P) \rangle$, é chamado *subgrupo de Thompson de P* .

Exemplo 4.3 *Para os grupo \mathbb{H} do exemplo anterior, temos que $\mathcal{J}(\mathbb{H}) = \mathbb{H}$.*

Como o subgrupo de Thompson está definido apenas para p -grupos, daqui por diante P denotará um p -grupo a menos que se mencione o contrário.

Observação 4.4 *Seja P um p -grupo, $\phi \in \text{Aut}(P)$ e $A \in \mathcal{A}(P)$. Claramente $\phi(A)$ é abeliano e $|\phi(A)| = |A|$, de modo que ϕ permuta os elementos de $\mathcal{A}(P)$ entre si. Disso segue que $\mathcal{J}(P)$ é invariante para todo automorfismo de P , de modo que $\mathcal{J}(P) \text{ char } P$.*

Como $Z(\mathcal{J}(P))$ char $\mathcal{J}(P)$, tem-se $Z(\mathcal{J}(P))$ char P e, assim sendo, $\mathcal{J}(P)$ possui propriedades interessantes e que nos ajudarão mais adiante.

As propriedades de $\mathcal{J}(P)$ mostradas na observação anterior são válidas para todo p -grupo P . Mas se P fosse um S_p -subgrupo de um grupo G , então $\mathcal{J}(P)$ teria mais propriedades? O próximo resultado responde esta pergunta.

Proposição 4.5 *Seja P um S_p -subgrupo de G . Então temos:*

(i) *Se R é um subgrupo de P que contém um elemento de $\mathcal{A}(P)$, então $\mathcal{A}(R) \subseteq \mathcal{A}(P)$ e $\mathcal{J}(R) \subseteq \mathcal{J}(P)$. Em particular, se $\mathcal{J}(P) \subseteq R$, então $\mathcal{J}(P) = \mathcal{J}(R)$.*

(ii) *Se $Q = P^x$, $x \in G$, então $\mathcal{J}(Q) = \mathcal{J}(P)^x$.*

(iii) *Se Q é um S_p -subgrupo de G contendo $\mathcal{J}(P)$, então $\mathcal{J}(Q) = \mathcal{J}(P)$.*

(iv) *$\mathcal{J}(P)$ é característico em qualquer p -subgrupo de G em que está contido.*

Demonstração: (i) Seja $A \in \mathcal{A}(P)$ tal que $A \subseteq R \subseteq P$. Então, obviamente, $A \in \mathcal{A}(R)$. Disso e do fato de todos os elementos de $\mathcal{A}(R)$ terem a mesma ordem, segue que os elementos de $\mathcal{A}(R)$ tem a mesma ordem dos elementos de $\mathcal{A}(P)$. Portanto, $\mathcal{A}(R) \subseteq \mathcal{A}(P)$ e, conseqüentemente, $\mathcal{J}(R) \subseteq \mathcal{J}(P)$. Em particular, se $\mathcal{J}(P) \subseteq R$, então R contém todos os elementos de $\mathcal{A}(P)$. Assim, todo elemento de $\mathcal{A}(P)$ é um elemento de $\mathcal{A}(R)$, de modo que $\mathcal{J}(P) \subseteq \mathcal{J}(R)$ e segue então que $\mathcal{J}(P) = \mathcal{J}(R)$, provando (i).

(ii) Seja $Q = P^x$, com $x \in G$. Como Q e P são isomorfos, segue que se $A \in \mathcal{A}(P)$ então $A^x \in \mathcal{A}(Q)$. Por outro lado, se $B^x \in \mathcal{A}(Q)$, então $B \leq P$ é abeliano e como $|B| = |B^x|$ segue que $B \in \mathcal{A}(P)$. Assim, $\mathcal{A}(Q) = \{A^x : A \in \mathcal{A}(P)\}$ e, portanto, $\mathcal{J}(Q) = \mathcal{J}(P)^x$.

(iii) Suponhamos que $\mathcal{J}(P) \subseteq Q$. Então certamente $A \subseteq Q$, para todo $A \in \mathcal{A}(P)$. Disso e de $Q = P^x$, para algum $x \in G$, segue que todo $A \in \mathcal{A}(P)$ também pertence a $\mathcal{A}(Q)$, i.é, $\mathcal{A}(P) \subseteq \mathcal{A}(Q)$. Logo, $\mathcal{J}(P) \subseteq \mathcal{J}(Q)$. Além disso, pelo item (ii), $|\mathcal{J}(Q)| = |\mathcal{J}(P)^x| = |\mathcal{J}(P)|$. Portanto, $\mathcal{J}(P) = \mathcal{J}(Q)$ e (iii) é válido.

(iv) Finalmente, suponhamos que $\mathcal{J}(P) \subseteq S$, onde S é um p -subgrupo de G . Seja Q um S_p -subgrupo de G contendo S . Daí, $\mathcal{J}(P) \subseteq S \subseteq Q$ e por (iii), temos $\mathcal{J}(P) = \mathcal{J}(Q)$.

Logo, por (i), $\mathcal{J}(Q) = \mathcal{J}(S)$. Visto que $\mathcal{J}(S) \text{ char } S$, temos $\mathcal{J}(P) \text{ char } S$ e o lema está provado. \square

Lema 4.6 *Seja $A \in \mathcal{A}(P)$ e B um subgrupo de P . Então B normaliza A se, e somente se, $[B, A, A] = 1$.*

Demonstração: Se B normaliza A , então $[B, A] \subseteq A$ e como A é abeliano, $[B, A, A] = 1$. Reciprocamente, se $[B, A, A] = 1$, então $[B, A]$ centraliza A , i.é, $[B, A] \subseteq C_P(A)$ e, portanto, pelo Lema 4.2, obtemos $[B, A] \subseteq A$. Isto implica que B normaliza A . \square

Agora vamos demonstrar um resultado devido a Thompson e que é mais uma propriedade de $\mathcal{A}(P)$.

Teorema 4.7 (Thompson) *Seja $A \in \mathcal{A}(P)$ e $x \in P$. Se $M = [x, A]$ é abeliano, então $MC_A(M) \in \mathcal{A}(P)$.*

Demonstração: Seja $C = C_A(M)$. Visto que M é abeliano, claramente MC é um grupo abeliano. Portanto, necessitamos apenas mostrar que $|MC| \geq |A|$, pois então $MC \in \mathcal{A}(P)$ pela definição de $\mathcal{A}(P)$. De M ser abeliano, segue trivialmente que $C \cap M = A \cap M$. Pelo Lema 4.2, $A = C_P(A)$ e assim, $C \cap M = A \cap M = C_P(A) \cap M = C_M(A)$. Portanto, $|MC| = \frac{|M||C_A(M)|}{|C_M(A)|}$ e a conclusão desejada $|MC| \geq |A|$ seguirá da igualdade anterior, se mostrarmos que

$$\frac{|M|}{|C_M(A)|} \geq \frac{|A|}{|C_A(M)|} \quad (4.1)$$

Porém para estabelecermos (4.1), é suficiente mostrarmos que se u e v são elementos de A pertencentes a classes laterais distintas de $C_A(M)$, então os elementos $[x, u]$ e $[x, v]$ de M pertencem a classes laterais distintas de $C_M(A)$.

Suponhamos que $[x, u]$ e $[x, v]$ pertençam a mesma classe lateral de $C_M(A)$. Então, $y = [x, u]^{-1}[x, v] \in C_M(A)$. Mas $y = (x^{-1}x^u)^{-1}(x^{-1}x^v) = (x^u)^{-1}x^v$, e como y centraliza A , segue que $y = uyu^{-1} = y^{u^{-1}}$. Destas duas últimas igualdades, obtemos $y = [x, vu^{-1}]$. Visto que y centraliza A , segue que $[x, vu^{-1}, a] = 1$, para todo $a \in A$. Mas como vu^{-1} e a comutam por A ser abeliano e como $[x, A]$ também é abeliano, segue da Proposição 1.2(ii) que $[x, vu^{-1}, a] = [x, a, vu^{-1}]$, de modo que $[x, a, vu^{-1}] = 1$. Assim, vu^{-1} centraliza $[x, a]$

para todo $a \in A$. Portanto, $vu^{-1} \in C_A(M)$ e, assim, $vC_A(M) = uC_A(M)$ contrariando a escolha de v e u . \square

Suponhamos que um elemento A de $\mathcal{A}(P)$ normaliza um subgrupo abeliano B de P , mas que B não normaliza A . Sob essas hipóteses, o resultado a seguir mostra a existência de um elemento de $\mathcal{A}(P)$ com duas propriedades importantes.

Teorema 4.8 (Teorema da Substituição de Thompson) *Sejam $A \in \mathcal{A}(P)$ e B um subgrupo abeliano de P . Se A normaliza B , mas B não normaliza A , então existe um elemento A^* em $\mathcal{A}(P)$ com as seguintes propriedades:*

(i) $A \cap B \subset A^* \cap B$;

(ii) A^* normaliza A .

Demonstração: Como A normaliza B , segue trivialmente que AB é um grupo e B é normal em AB . Temos também que $N = N_B(A) \triangleleft AB$ e como B não normaliza A , segue que $N \subset B$. Do Teorema da Correspondência, temos $B/N \triangleleft AB/N$ e, assim, B/N é um subgrupo normal não trivial do p -grupo AB/N . Então pela Proposição 1.4 (ii), $B/N \cap Z(AB/N) \neq 1$ e portanto, podemos escolher $x \in B \setminus N$ tal que sua imagem xN está em $Z(AB/N)$. Assim, para todo $a \in A$, obtemos $[x, a]N = N$ e portanto, $[x, A] \subseteq N$. Tomando $M = [x, A]$, temos que M é abeliano, pois $M \leq N < B$. Logo, $A^* = MC_A(M) \in \mathcal{A}(P)$, pelo Teorema 4.7. Vamos mostrar que A^* tem as propriedades requeridas.

Primeiro de tudo, M normaliza A , pois $M \subseteq N = N_B(A)$. Visto que $C_A(M) \subseteq A$, segue que A^* normaliza A , provando o item (ii). Mais ainda, visto que A e B são abelianos, e que $x \in B$, temos que $A \cap B$ centraliza ambos x e A , de modo que $A \cap B \subseteq C_A(M) \cap B \subseteq A^*$. Por outro lado, $M = [x, A] \not\subseteq A$, pois $x \notin N$, de modo que $A \cap B \subset M(A \cap B)$. Mas, $M \subseteq A^* \cap B$ e $A \cap B \subseteq A^* \cap B$. Logo, $A \cap B \subset M(A \cap B) \subseteq A^* \cap B$, provando o teorema. \square

Corolário 4.9 *Seja B um subgrupo normal abeliano de P . Então, existe um elemento A de $\mathcal{A}(P)$ tal que B normaliza A .*

Demonstração: Neste caso, todo elemento de $\mathcal{A}(P)$ normaliza B , pois $B \triangleleft P$. Escolha $A \in \mathcal{A}(P)$ tal que $A \cap B$ é maximal. Se B não normaliza A , então pelo teorema anterior, existe $A^* \in \mathcal{A}(P)$ tal que $A \cap B \subset A^* \cap B$, contradizendo a escolha de A . \square

Observe que o subgrupo B do Teorema da Substituição de Thompson é nilpotente, por ser abeliano. Este resultado pode ser estendido para o caso em que B é um subgrupo normal do p -grupo P com classe de nilpotência no máximo 2 tal que $B' \subseteq Z(\mathcal{J}(P))$. Porém, antes de demonstrarmos isto, nós introduziremos um lema, lembrando que para quaisquer grupos A e B definimos $[B, A; 0] = B$ e $[B, A; i] = [[B, A; i-1], A]$, $i \leq 1$.

Lema 4.10 *Seja P um p -grupo da forma $P = AB$ com $B \triangleleft P$, $B' \subseteq Z(P)$ e A abeliano. Seja n o menor inteiro positivo tal que $[B, A; n]$ é abeliano. Então valem as seguintes propriedades:*

(i) *Para $i \geq 2$, todo elemento $x \in \gamma_i(P)$ pode ser escrito da forma $x = bb'$, onde $b \in [B, A; i-1]$ e $b' \in B'$;*

(ii) $[B, A; i+1] \subseteq [B, A; i]$ para todo $i \geq 0$.

(iii) *Se $[B, A; n+1] = 1$ então $n \leq 2$ e a classe de nilpotência de P é ≤ 4 .*

Demonstração: Note que como P é nilpotente, existe um inteiro positivo k tal que $\gamma_k(P) = [\gamma_{k-1}(P), P] = 1$. Agora, claramente $[B, A; i] \subseteq \gamma_i(P)$ para todo i . Deste modo, $[B, A, k-1] \subseteq \gamma_{k-1}(P) = 1$. Mas, $[\gamma_{k-1}(P), \gamma_{k-1}(P)] \subseteq [\gamma_{k-1}(P), P]$ e, assim, $\gamma_{k-1}(P)$ é abeliano. Logo, $[B, A; k-1]$ é abeliano e n está bem definido.

(i) Vamos dividir a prova em dois casos:

1º caso: B é abeliano.

Como $\frac{P}{B} = \frac{AB}{B} \cong A$, o grupo $\frac{P}{B}$ é abeliano. Usando-se este fato, é fácil mostrar, por indução sobre i , que $\gamma_i(P) \subseteq B$, para $i \geq 2$. Visto que B é abeliano, para todos $b \in B$, $a \in A$ e $x \in \gamma_i(P)$, obtemos $[ba, x] = a^{-1}b^{-1}x^{-1}bax = a^{-1}x^{-1}b^{-1}bax = [a, x]$. Isto implica que para todo $i \geq 2$,

$$\gamma_{i+1}(P) = [\gamma_i(P), P] = [P, \gamma_i(P)] = [BA, \gamma_i(P)] = [A, \gamma_i(P)] = [\gamma_i(P), A]. \quad (4.2)$$

Usando (4.2) e indução sobre i nós provaremos que $\gamma_i(P) = [B, A; i-1]$ para todo $i \geq 2$.

Mostraremos primeiro que $\gamma_2(P) = [B, A]$. Pela Proposição 1.2 (i), temos que para $a \in A$, $b \in B$ e $x \in P$,

$$[ab, x] = [a, x]^b [b, x]. \quad (4.3)$$

Mas, como $[a, x] \in P' \subseteq B$, de B ser abeliano, tem-se $[a, x]^b = [a, x]$ e, portanto, (4.3) reduz-se a

$$[ab, x] = [a, x][b, x] \quad (4.4)$$

Assim, todo gerador de P' está em $[A, P][B, P]$. Logo, $P' \subseteq [A, P][B, P]$. Porém, usando-se que A , B são abelianos e que $P = BA$, mostra-se facilmente que $[B, P] = [B, A]$ e $[A, P] = [A, B] = [B, A]$. Assim, $P' \subseteq [B, A]$. Como $[B, A] \subseteq [P, P] = P'$, temos que $\gamma_2(P) = P' = [B, A]$.

A hipótese de indução garante que $\gamma_i(P) = [B, A; i - 1]$. Disso e de (4.2) tem-se $\gamma_{i+1}(P) = [B, A; i]$. Logo, (i) é válido.

2º caso: B não é abeliano.

Pela Proposição 1.1, $\frac{B}{B'}$ é abeliano e, pelo caso anterior,

$$\gamma_i\left(\frac{P}{B'}\right) = \left[\frac{B}{B'}, \frac{AB'}{B'}; i - 1\right]. \quad (4.5)$$

Mostremos que todo $x \in \gamma_i(P)$ é da forma $x = bb'$, com $b \in [B, A; i - 1]$ e $b' \in B'$. (*)

Notemos primeiro que tomando o homomorfismo canônico de P em $\frac{P}{B'}$ na Proposição 1.3, mostra-se que por indução sobre i que

$$\frac{\gamma_i(P)B'}{B'} = \gamma_i\left(\frac{P}{B'}\right) \quad \text{e} \quad \frac{[B, A; i - 1]B'}{B'} = \left[\frac{B}{B'}, \frac{AB'}{B'}; i - 1\right]. \quad (4.6)$$

Com estas igualdades, mostra-se (*). Portanto, o item (i) está provado.

(ii) Basta mostrarmos que A normaliza cada $[B, A; i]$, pois se isso é válido, então, $[B, A; i + 1] = [[B, A; i], A] \subseteq [B, A; i]$. Faremos a demonstração por indução sobre i , observando ser trivial para $i = 0$. A hipótese de indução garante que A normaliza $[B, A; i]$. Pela Proposição 1.2 (vi), segue que $[B, A; i + 1] = [[B, A; i], A] \triangleleft \langle [B, A; i], A \rangle$. Visto que $A \subseteq \langle [B, A; i], A \rangle$, temos que A normaliza $[B, A; i + 1]$, provando (ii).

(iii) Finalmente suponhamos que $[B, A; n + 1] = 1$. Pelo item (i) e pela hipótese, temos $\gamma_{n+2}(P) \subseteq B' \subseteq Z(P)$ e, conseqüentemente, $\gamma_{n+3}(P) = [\gamma_{n+2}(P), P] = 1$

Seja m o maior inteiro não excedendo $\frac{1}{2}(n+4)$. Visto que $n \geq 1$, temos $m \geq 2$. Além disso, segue da definição de m que $\frac{1}{2}(n+3) \leq m$, de modo que $2m \geq n+3$. Assim, pela Proposição 1.12, $[\gamma_m(P), \gamma_m(P)] \subseteq \gamma_{m+m}(P) = \gamma_{2m}(P)$. Mas de $2m \geq n+3$, obtemos $\gamma_{2m}(P) \leq \gamma_{n+3}(P)$, de modo que $[\gamma_m(P), \gamma_m(P)] = 1$ e, portanto, $\gamma_m(P)$ deve ser abeliano. Assim, de (4.5) e (4.6), $[B, A; m-1]$ abeliano também. Uma vez que $m-1$ é positivo, segue da nossa definição de n que $m-1 \geq n$. Logo, $n \leq m-1 \leq \frac{1}{2}(n+4)-1 = \frac{n+2}{2}$ e então $n \leq 2$. Como $\gamma_{n+3}(P) = 1$ é válido $\gamma_5(P) = 1$ e, conseqüentemente, $cl(P) \leq 4$, provando (iii). \square

Agora estamos em condições de estender o Teorema da Substituição de Thompson.

Teorema 4.11 (Teorema da Substituição de Glauberman) *Seja P um p -grupo, p ímpar e seja B um subgrupo normal de P de classe de nilpotência no máximo 2 tal que $B' \subseteq Z(\mathcal{J}(P))$. Se A é um elemento de $\mathcal{A}(P)$ que não é normalizado por B , então existe um elemento A^* em $\mathcal{A}(P)$ satisfazendo:*

(i) $A \cap B \subset A^* \cap B$;

(ii) A^* normaliza A .

Demonstração: Tomemos o produto $Q = AB$. Como $A \subseteq Q$, pelo Lema 4.5 (i), $\mathcal{A}(Q) \subseteq \mathcal{A}(P)$ e $\mathcal{J}(Q) \subseteq \mathcal{J}(P)$. Além disso, como $Z(\mathcal{J}(P))$ centraliza $A \subseteq \mathcal{J}(P)$, tem-se $Z(\mathcal{J}(P)) \subseteq C_P(A) = A$, pelo Teorema 4.2. Visto que $A \in \mathcal{A}(P)$, $Q \leq P$ e $A \subseteq Q$, o argumento usado no Lema 4.5 (i) mostra que $A \subseteq \mathcal{J}(Q)$ e, então $Z(\mathcal{J}(P)) \subseteq \mathcal{J}(Q)$. Disso e do fato de $\mathcal{J}(Q) \subseteq \mathcal{J}(P)$, segue que $Z(\mathcal{J}(P)) \subseteq Z(\mathcal{J}(Q))$. Portanto, $B' \subseteq Z(\mathcal{J}(Q))$ e assim as hipóteses do teorema valem para Q . Uma vez que $\mathcal{A}(Q) \subseteq \mathcal{A}(P)$, basta exibirmos um elemento A^* em $\mathcal{A}(Q)$ com as propriedades requeridas. Portanto, podemos assumir que $P = AB$. Como a classe de nilpotência de B é no máximo 2, temos claramente $B' \subseteq Z(B)$. Mas $B' \subseteq Z(\mathcal{J}(P)) \subseteq A$, de modo que $B' \subseteq A \cap Z(B) = Z(A) \cap Z(B) \subseteq Z(AB) = Z(P)$. Logo, $B' \subseteq Z(P)$. Considere n o menor inteiro positivo tal que $[B, A; n]$ é abeliano. Vamos separar a prova em dois casos:

1º caso: $[B, A, n+1] \neq 1$.

Seja r o menor inteiro positivo tal que $[B, A; r] = 1$. Então $r \geq n + 2 \geq 3$, pois $n \geq 1$. Portanto, $[B, A; r - 3]$ está bem definido. Além disso, $[B, A; r - 2]$ não centraliza A , pois caso contrário, teríamos $[B, A; r - 1] = [[B, A; r - 2], A] = 1$, o que não ocorre pelo modo como r foi tomado. Portanto, podemos tomar $x \in [B, A; r - 3]$ tal que A não centraliza $[x, A]$. Coloquemos $M = [x, A]$. Então, $M \subseteq [B, A; r - 2]$ e como $r \geq n + 2$, temos do Lema 4.10(ii) que $[B, A; r - 2] \subseteq [B, A; n]$, de maneira que $M \subseteq [B, A; n]$. Disso e da escolha de n , segue que M é abeliano. Portanto, $A^* = MC_A(M) \in \mathcal{A}(P)$ pelo Teorema 4.7.

Agora, $[B, A \cap B, A] \subseteq [B, B, A] = [B', A] \subseteq [Z(P), A] = 1$ e $[A \cap B, A, B] \subseteq [A, A, B] = [A', B] = [1, B] = 1$. Logo, pelo Lema dos Três Subgrupos, $[A, B, A \cap B] = 1$ e portanto, $A \cap B$ centraliza $[A, B] = [B, A] = [B, A; 1]$. Assim, pelo item (ii) do Lema 4.10, $A \cap B$ centraliza $[B, A; i]$ para todo $i \geq 1$. Em particular, $A \cap B$ centraliza $M \subseteq [B, A; n]$ e assim, centraliza A^* . Por outro lado, $M \not\subseteq A$, uma vez que A não centraliza M . Como A normaliza B temos claramente que $[B, A; r - 3] \subseteq B$. Assim, $x \in B$ e novamente por A normalizar B , $M = [x, A] \subseteq B$. Deste modo, $A \cap B \subset M(A \cap B) \subseteq B \cap A^*$. Além disso, como A é abeliano e $C_A(M) \subseteq A$, segue que os elementos de $C_A(M)$ comutam com os elementos de A e então $[A^*, A] = [MC_A(M), A] = [M, A]$. De $M \subseteq [B, A; r - 2]$, obtemos $[A^*, A, A] = [M, A, A] \subseteq [B, A; r] = 1$. Pelo Lema 4.6, A^* normaliza A . Portanto, A^* tem as propriedades requeridas.

2º caso: $[B, A; n + 1] = 1$

Neste caso, $n \leq 2$ pelo Lema 4.10 (iii). Visto que B não normaliza A por hipótese, segue do Lema 4.6 que $[B, A, 2] = [B, A, A] \neq 1$ e assim, $n = 2$. Provaremos agora que $[x, A]$ é abeliano para todo $x \in B$. Sejam $u, v \in A$ e apliquemos a Proposição 1.2 (iv) colocando x, u^{-1} e $w = [x, v]$ no lugar de x, y, z , respectivamente, para obtermos

$$[x, u, w]^{u^{-1}}[u^{-1}, w^{-1}, x]^w[w, x^{-1}, u^{-1}]^x = 1 \quad (4.7)$$

Como A normaliza B , segue que $[x, u], w \in B$, de modo que $[x, u, w] \in B' \subseteq Z(P)$. Pela mesma razão $[u^{-1}, w^{-1}, x] \in Z(P)$. Além disso, como $[w, x^{-1}] \in B' \subseteq Z(P)$, temos que $[w, x^{-1}, u^{-1}] = 1$. Portanto, (4.7) reduz-se a

$$[x, u, w][u^{-1}, w^{-1}, x] = 1. \quad (4.8)$$

Uma vez que $[u^{-1}, w^{-1}, x] \in Z(P)$, $[u^{-1}, w^{-1}, x]$ comuta, em particular, com $[u^{-1}, w^{-1}]$ e x . Logo, pela Proposição 1.2 (iii) e (v) obtemos

$$[u^{-1}, w^{-1}, x]^{-1} = [[u^{-1}, w^{-1}], x]^{-1} = [[u^{-1}, w^{-1}]^{-1}, x] = [[w^{-1}, u^{-1}], x]. \quad (4.9)$$

Agora (4.8) e (4.9) juntamente com $w = [x, v]$ dão:

$$[[x, u], [x, v]] = [[[x, v]^{-1}, u^{-1}], x] \quad (4.10)$$

Nós simplificaremos o termo $[[x, v]^{-1}, u^{-1}]$. Seja $\bar{P} = \frac{P}{B'}$, $\bar{A} = \frac{AB'}{B'}$ e $\bar{B} = \frac{B}{B'}$. Visto que $[[B, A, A], A] = 1$, temos $[[\bar{B}, \bar{A}, \bar{A}], \bar{A}] = 1$, de modo que $[\bar{B}, \bar{A}, \bar{A}]$ centraliza \bar{A} . Mas como $[B, A, A] \subseteq B$, segue que $[\bar{B}, \bar{A}, \bar{A}] \subseteq \bar{B} = Z(\bar{B})$, pois \bar{B} é abeliano. Portanto, $[\bar{B}, \bar{A}, \bar{A}] \subseteq Z(\bar{P})$. Logo, colocando $[[\bar{B}, \bar{A}], \bar{A}]$ no lugar de G e $\overline{[x, v]}$, \bar{u}^{-1} no lugar de x e y , respectivamente, na Proposição 1.2 (v) temos $\overline{[[x, v], \bar{u}^{-1}]}^{-1} = \overline{[[x, v]^{-1}, \bar{u}^{-1}]}$ e $\overline{[[x, v], \bar{u}^{-1}]}^{-1} = \overline{[\bar{x}, \bar{v}, \bar{u}]}$. Disso e da Proposição 1.3, obtemos $\overline{[[x, v], u^{-1}]}^{-1} = \overline{[[x, v]^{-1}, u^{-1}]}$ e $\overline{[[x, v], u^{-1}]}^{-1} = \overline{[x, v, u]}$. Logo,

$$[[x, v]^{-1}, u^{-1}] \equiv [[x, v], u^{-1}]^{-1} \pmod{B'} \text{ e } [x, v, u] \equiv \overline{[[x, v], u^{-1}]}^{-1} \pmod{B'}. \quad (4.11)$$

Visto que v e u comutam e $\frac{[x, A]B'}{B'} \subseteq \frac{B}{B'}$ é abeliano, temos que $\overline{[x, A]} = \overline{[x, \bar{A}]}$ é abeliano. Pela Proposição 1.2 (ii), $\overline{[\bar{x}, \bar{v}, \bar{u}]} = \overline{[\bar{x}, \bar{u}, \bar{v}]}$, o que implica $\overline{[x, v, u]} = \overline{[x, u, v]}$. Disso vem que

$$[x, v, u] \equiv [x, u, v] \pmod{B'}. \quad (4.12)$$

Como $B' \subseteq Z(P)$, segue de (4.10), (4.11) e (4.12) que

$$[[x, u], [x, v]] = [[x, u, v], x]. \quad (4.13)$$

Por simetria,

$$[[x, v], [x, u]] = [[x, v, u], x] = [[x, u, v], x]. \quad (4.14)$$

Visto que $[[x, v], [x, u]] = [[x, u], [x, v]]^{-1}$ pela Proposição 1.2 (iii), segue de (4.13) e (4.14) que $[[x, u], [x, v]]^2 = 1$. Como P é um p -grupo, com p ímpar, temos $[[x, u], [x, v]] = 1$. De u e v serem elementos arbitrários de A , segue que $[x, A]$ é abeliano para todo $x \in B$, como desejávamos.

Uma vez que B não normaliza A , temos do Lema 4.6 que $[B, A, A] \neq 1$ e, então, $[B, A]$ não centraliza A . Escolha $x \in B$ tal que $[x, A]$ não centraliza A . Colocando $M = [x, A]$ e aplicando o Teorema 4.7, obtemos $A^* = MC_A(M) \in \mathcal{A}(P)$. Como no 1º caso, $A \cap B$ centraliza $[B, A]$. Uma vez que $M \subseteq [B, A]$, temos, em particular, que $A \cap B \subseteq C_A(M)$. Além disso, $M \not\subseteq A$. Em suma, $A \cap B \subseteq C_A(M)$, $M \subseteq B$ e $M \not\subseteq A$. Logo, $A \cap B \subset M(A \cap B) \subseteq MC_A(M) = A^*$. Da mesma maneira que no 1º caso, como $C_A(M)$ centraliza A , segue que $[A^*, A, A] = [MC_A(M), A, A] = [M, A, A]$. Por outro lado, $M \subseteq [B, A]$ o que implica $[M, A, A] \subseteq [B, A, A, A] = [B, A; 3] = 1$. Logo, $[A^*, A, A] = 1$ e o Lema 4.6 garante que A^* normaliza A . Portanto, A^* possui as propriedades desejadas e o teorema está demonstrado. \square

Observação 4.12 *O fato de p ser ímpar foi usado somente no 2º caso, onde $[B, A; 3] = 1$. Portanto, o Teorema 4.11 é válido para $p = 2$ se assumirmos $[B, A; 3] \neq 1$.*

Como no caso do Teorema 4.8, para o teorema anterior temos o

Corolário 4.13 *Com as hipóteses do Teorema 4.11, existe um elemento A em $\mathcal{A}(P)$ tal que B normaliza A .*

Demonstração: A demonstração é análogo ao Corolário 4.9, porém usando o Teorema 4.11 no lugar do Teorema 4.8. \square

Observe que os Teoremas 2.14 e 3.13 mostram que para todo grupo fortemente p -solúvel G valem as seguintes afirmações:

- (I) Se Q é um S_p -subgrupo de $O_{p'p}(G)$, então $C_G(Q) \subseteq O_{p'p}(G)$.
- (II) Seja P um p -subgrupo de G tal que $O_{p'}(G)P \triangleleft G$. Então, se A é um p -subgrupo de $N_G(P)$ com a propriedade $[P, A, A] = 1$, temos $\frac{AC_G(P)}{C_G(P)} \subseteq O_p\left(\frac{N_G(P)}{C_G(P)}\right)$.

Os S_p -subgrupos de um grupo que satisfazem (II), p ímpar, possuem um propriedade peculiar:

Teorema 4.14 (Glauberman) *Seja B um p -subgrupo normal não trivial de um grupo G que satisfaz (II), p ímpar. Se P é um S_p -subgrupo de G , então $B \cap Z(\mathcal{J}(P)) \triangleleft G$.*

Demonstração: Suponhamos que o teorema seja falso e seja $B \neq 1$ um p -subgrupo normal de G de menor ordem tal que o teorema não valha. Sejam $Z = Z(\mathcal{J}(P))$ e B_1 o fecho normal de $Z \cap B$ em G , i.é, $B_1 = \langle x^g : x \in B \cap Z, g \in G \rangle$. De $B \triangleleft G$, resulta que $B_1 \subseteq B$ e como $Z \cap B \subseteq B_1$, temos $Z \cap B_1 = Z \cap B$. Assim, pela escolha minimal de B , devemos ter $B_1 = B$.

Agora, como B é nilpotente, por ser um p -grupo, temos claramente que $B' \subset B$, e, então, $Z \cap B'$ é um subgrupo normal de G , pela minimalidade de B . Visto que $Z \triangleleft P$, temos $[Z \cap B, B] \subseteq Z \cap B'$. Logo, para todo $x \in G$,

$$[(Z \cap B)^x, B] = [(Z \cap B)^x, B^x] = [(Z \cap B), B]^x \subseteq (Z \cap B')^x = Z \cap B', \quad (4.15)$$

pois B e $Z \cap B'$ são normais em G . Como $B = B_1$ é gerado por todos tais $(Z \cap B)^x$ obtemos $B' \subseteq Z \cap B' \subseteq Z$, e, então, $Z \cap B$ centraliza B' . Disso temos claramente que $(Z \cap B)^x$ centraliza B'^x , para todo $x \in G$. De $B' \text{ char } B$, $B \triangleleft G$, segue que $B'^x = B'$, para todo $x \in G$. Assim, $(Z \cap B)^x$ também centraliza B' , para todo $x \in G$. Mas, então, B centraliza B' e, portanto, $B' \subseteq Z(B)$. Logo, concluímos que $\gamma_3(B) = 1$ e, daí, $cl(B) \leq 2$. Assim, B tem a estrutura requerida para aplicarmos o Teorema da Substituição de Glauberman e seu corolário.

Seja L o maior subgrupo normal de G que normaliza $Z \cap B$. Então $P \cap L$ é um S_p -subgrupo de L . Como $\mathcal{J}(P \cap L) \text{ char } P \cap L$ e todo elemento de $N_G(P \cap L)$ induz, por conjugação, um automorfismo de $P \cap L$, temos $N_G(P \cap L) \subseteq N_G(\mathcal{J}(P \cap L))$. Pelo Argumento de Frattini, $G = LN_G(P \cap L) \subseteq LN_G(\mathcal{J}(P \cap L))$. Assim, $G = LN$, onde $N = N_G(\mathcal{J}(P \cap L))$. Se $\mathcal{J}(P) \subseteq P \cap L$, então $\mathcal{J}(P) = \mathcal{J}(P \cap L)$, pelo Teorema 4.5 (i). Neste caso, N normaliza Z , e de $B \triangleleft G$, segue que N normaliza $Z \cap B$. Mas então, $G = LN$ normaliza $Z \cap B$ e $Z \cap B \triangleleft G$, contrariando nossa escolha de B . Logo, $\mathcal{J}(P) \not\subseteq L \cap P$.

Pelo Corolário 4.13 e Lema 4.6, existe um elemento A em $\mathcal{A}(P)$ tal que $[B, A, A] = 1$. Como $B \triangleleft G$, temos $O_{p'}(G)B \triangleleft G$ e $A \subseteq N_G(B)$. Como G satisfaz (II), $AC/C \subseteq O_p(N_G(B)/C) = O_p(G/C)$, onde $C = C_G(B)$. Em particular, C também centraliza $Z \cap B$. Uma vez que $C \text{ char } B \triangleleft G$, temos $C \triangleleft G$ e, portanto, LC é um subgrupo normal em G que normaliza $Z \cap B$. Nossa escolha maximal de L força $C \subseteq L$. Disso

segue trivialmente que $\bar{\phi} : G/C \longrightarrow \bar{G} = G/L$ dado por $\bar{\phi}(xC) = xL$ está bem definida e é um homomorfismo sobrejetor. Daí, AC/C é levado sobre AL/L . Por outro lado, $\bar{\phi}\left(O_p\left(G/C\right)\right)$ é um p -subgrupo normal em \bar{G} e, portanto, $\bar{\phi}\left(O_p\left(G/C\right)\right) \subseteq O_p(\bar{G})$. Disso e de $AC/C \subseteq O_p\left(G/C\right)$ temos $AL/L \subseteq O_p(\bar{G})$. Porém, nós mostraremos que $O_p(\bar{G}) = \bar{1}$. De fato, seja K a imagem inversa de $O_p(\bar{G})$ em G . Então, $K \triangleleft G$ e, assim, $P \cap K$ é um S_p -subgrupo de K . Da mesma forma que na demonstração do Teorema 2.14 temos que $P \cap K$ é aplicado sobrejetivamente sobre $O_p(\bar{G})$, ou seja, $\frac{L(P \cap K)}{L} = O_p(\bar{G})$. Portanto, $K = L(P \cap K)$. Mas, $P \cap K$ normaliza $Z \cap B$ e, além disso, $P \cap K \triangleleft G$ pelo Teorema da Correspondência. Logo, pela escolha de L , temos $P \cap K \subseteq L$ e daí, $K = L$. Portanto, $O_p(\bar{G}) = \bar{1}$. Visto que $\frac{AL}{L} \subseteq O_p(\bar{G})$, temos $A \subseteq L \cap P$. Tomando $R = P \cap L$ no Lema 4.5(i), obtemos $\mathcal{J}(P \cap L) \subseteq \mathcal{J}(P)$. Como $A \in \mathcal{A}(P)$ e $A \subseteq P \cap L$, temos $A \subseteq \mathcal{J}(P \cap L)$. Note ainda que $Z \subseteq Z(A) = A$, de modo que $Z \subseteq A \subseteq \mathcal{J}(P \cap L)$, e isto implica que $Z \cap B \subseteq Z(\mathcal{J}(P \cap L))$. Escrevamos $X = Z(\mathcal{J}(P \cap L))$. De $X \text{ char}(P \cap L)$ obtemos $N_G(P \cap L) \subseteq N_G(X)$. Uma vez que $L \triangleleft G$ e $L \cap P$ é um S_p -subgrupo de L , temos do Argumento de Frattini que $G = LN_G(P \cap L)$ e, então, $G = LN_G(X)$. Agora, $Z \cap B \subseteq X$, de modo que $\langle (Z \cap B)^x : x \in N_G(X) \rangle \subseteq X$. Assim, como L normaliza $Z \cap B$, B é o fecho normal de $Z \cap B$ em G e $G = LN_G(X)$, obtemos $B \subseteq X$. Em particular, B é abeliano.

Uma vez que $\mathcal{J}(P) \not\subseteq L \cap P$, existe um elemento $A_1 \in \mathcal{A}(P)$ tal que $A_1 \not\subseteq L$. Nós afirmamos que $[B, A_1, A_1] \neq 1$. De fato, se $[B, A_1, A_1] = 1$, então o argumento utilizado anteriormente para A pode ser aplicado para A_1 afim de obter que $A_1 \subseteq L$, contradizendo a escolha de A_1 .

Finalmente, dentre todos os elementos de $\mathcal{A}(P)$ que não estão contidos em L , escolhemos A_1 tal que $|A_1 \cap B|$ é maximal. Pelo Lema 4.6, B não normaliza A_1 . Visto que A_1 normaliza B , o Teorema da Substituição de Thompson pode ser aplicado para mostrar que existe um elemento $A^* \in \mathcal{A}(P)$ tal que $A_1 \cap B \subset A^* \cap B$ e A^* normaliza A_1 . Devido a nossa escolha maximal de A_1 , devemos ter $A^* \subseteq L$ e, conseqüentemente, $A^* \subseteq P \cap L$. Logo, $A^* \subseteq \mathcal{J}(P \cap L)$. Assim, $X = Z(\mathcal{J}(P \cap L)) \subseteq C_P(A^*) = A^*$ pelo Lema 4.2. Mas, $B \subseteq X$, de modo que, $[B, A_1, A_1] \subseteq [X, A_1, A_1] \subseteq [A^*, A_1, A_1] = 1$, pois A^* normaliza A_1 , contradizendo o fato de $[B, A_1, A_1] \neq 1$. Portanto, o teorema está provado.

□

Como consequência do resultado anterior temos o

Teorema 4.15 (Glauberman) *Seja G um grupo fortemente p -solúvel com p ímpar e tal que $O_{p'}(G) = 1$. Se P for um S_p -subgrupo de G , então $Z(\mathcal{J}(P)) \triangleleft G$.*

Demonstração: Como $Z(\mathcal{J}(P))$ é um subgrupo normal abeliano de P , temos do Teorema 3.8 que $Z(\mathcal{J}(P)) \subseteq O_{p'p}(G) = O_p(G)$ já que por hipótese $O_{p'}(G) = 1$. Colocando $B = O_p(G)$ no Teorema 4.14, segue que $Z(\mathcal{J}(P)) = Z(\mathcal{J}(P)) \cap O_p(G) \triangleleft G$, como queríamos. □

4.2 Grupos p -Nilpotentes

Uma classe de grupos particularmente importantes no nosso trabalho são os chamados grupos p -nilpotentes. Nesta seção vamos definir este conceito e em seguida iremos apresentar uma condição suficiente para um grupo ser p -nilpotente. Para finalizar o capítulo, vamos estabelecer uma condição suficiente para um grupo ser solúvel.

Definição 4.16 *Um grupo G é p -nilpotente, onde p é um primo, se ele possui um p' -subgrupo de Hall normal.*

Se um grupo G é p -nilpotente e N é um p' -subgrupo de Hall normal de G , então claramente existe um S_p -subgrupo P de G tal que $G = NP$. Como $N \leq O_{p'}(G)$ e N é um p' -subgrupo de Hall, temos $N = O_{p'}(G)$ e, assim, $G = O_{p'}(G)P$. Reciprocamente, se $G = O_{p'}(G)P$, para algum S_p -subgrupo P de G , então $|G : O_{p'}(G)| = |P|$ e G será p -nilpotente. Logo, G é p -nilpotente se, e somente se, existe um S_p -subgrupo P tal que $G = O_{p'}(G)P$. Dessa equivalência, segue também que G é p -nilpotente se, e somente se, $G = O_{p'p}(G)$.

Sabemos que todo grupo finito nilpotente G é produto de seus subgrupos de Sylow, de modo que todo grupo finito nilpotente é p -nilpotente, para todo $p \in \pi(G)$.

Observação 4.17 *Seja G um grupo p -nilpotente, $H \leq G$ e $K \triangleleft G$. Se denotarmos por N o p' -subgrupo de Hall normal de G , então cálculos triviais mostram que $H \cap N$ e $\frac{KN}{K}$ são, respectivamente, p' -subgrupos de Hall normais em H e $\frac{G}{K}$. Isto mostra que subgrupos e quocientes de grupos p -nilpotentes são p -nilpotentes.*

No que segue, veremos uma caracterização de grupos p -nilpotentes, devido a Frobenius. Sua demonstração não será apresentada, mas o leitor poderá obtê-la em [2], página 253.

Teorema 4.18 (Frobenius) *Um grupo G é p -nilpotente se, e somente se, uma das seguintes condições está satisfeita:*

- (a) $\frac{N_G(H)}{C_G(H)}$ é um p -grupo para todo p -subgrupo $H \neq 1$ de G ;
- (b) $N_G(H)$ é p -nilpotente para todo p -subgrupo $H \neq 1$ de G .

Para p um primo ímpar, Thompson mostrou que se os normalizadores de certos dois subgrupos característicos de um S_p -subgrupo P de G são p -nilpotentes, então G também é p -nilpotente. O próximo resultado dá um refinamento deste resultado e, de fato, mostra que a p -nilpotência apenas de $N_G(Z(\mathcal{J}(P)))$ é suficiente para garantir que G também é p -nilpotente.

Teorema 4.19 (Glauberman-Thompson) *Se P é um S_p -subgrupo de G , p ímpar, e se $N_G(Z(\mathcal{J}(P)))$ é p -nilpotente, então G também é p -nilpotente.*

Demonstração: Faremos a demonstração por indução sobre $|G|$, observando que o teorema é óbvio para $|G| = 1$. Em particular, todo subgrupo próprio D de G contendo P é p -nilpotente, pois $N_D(Z(\mathcal{J}(P))) \subseteq N_G(Z(\mathcal{J}(P)))$. Suponhamos que $N_G(Z(\mathcal{J}(P)))$ é p -nilpotente, mas G não. Então, pelo Teorema de Frobenius, existe um p -subgrupo H não trivial de G tal que $N_G(H)$ não é p -nilpotente. Dentre todos tais subgrupos, vamos escolher H de forma que um S_p -subgrupo de $N = N_G(H)$ tenha ordem maximal. Se P_0 for um S_p -subgrupo de N , então claramente $H \subseteq P_0$. Por outro lado, P_0 está contido em um S_p -subgrupo Q de G e pelo Teorema de Sylow, $P_0 \leq Q = P^x$ para algum

$x \in G$. Observamos que pela Proposição 4.5 (ii), $J(Q) = J(P)^x$ e, então, $N_G(Z(J(Q)))$ é também p -nilpotente. Assim, substituindo P por um conjugado adequado, se necessário, podemos assumir $P_0 \leq P$, de modo que $H \leq P$. Como $P_0 \leq P \cap N$ temos $P_0 = P \cap N$. Portanto, sem perdas, podemos assumir que $P \cap N$ é um S_p -subgrupo de N .

Mostraremos que $P \subseteq N$. Suponhamos o contrário e coloquemos $R = P \cap N$, $L = N_N(Z(\mathcal{J}(R)))$ e $M = N_G(Z(\mathcal{J}(R)))$, de modo que $L \subseteq M$ e $R \subset P$. Mas então $R \subset N_P(R)$ pela Proposição 1.4 (i). Como $Z(\mathcal{J}(R)) \text{ char } R$, temos $N_P(R) \subseteq M$ e, assim, $R \subset M \cap P$. Portanto, um S_p -subgrupo de M tem ordem maior que a ordem de um S_p -subgrupo de N e então M é p -nilpotente, pela escolha maximal de H . Por outro lado, $|N| < |G|$ e $L \subseteq M$ é p -nilpotente. Por indução, N é p -nilpotente, contradizendo a escolha de H . Logo, $P \subseteq N$ e o primeiro parágrafo força $N = G$.

Claramente nossas hipóteses valem também para $G/O_{p'}(G)$. Portanto, se $O_{p'}(G) \neq 1$, então, por indução, $G/O_{p'}(G)$ é p -nilpotente e pelo Teorema da Correspondência e Terceiro Teorema do Isomorfismo, G também é, contradição. Logo, $O_{p'}(G) = 1$. Visto que $O_p(G) \neq 1$ e $N_G(H) = G = N_G(O_p(G))$, obtemos que H e $O_p(G)$ têm as mesmas propriedades e, portanto, podemos supor sem perda que $H = O_p(G)$. Assim $H \triangleleft G$. Observamos que $H \subset P$, pois, caso contrário, teríamos $P \triangleleft G$ e, então, $Z(\mathcal{J}(P)) \triangleleft G$, o que implicaria $G = N_G(Z(\mathcal{J}(P)))$ e, conseqüentemente, G seria p -nilpotente.

Agora, sejam $\bar{G} = \frac{G}{H}$ e \bar{P} a imagem de P em \bar{G} , de modo que $\bar{P} \neq 1$. Sejam $\bar{N}_1 = N_{\bar{G}}(Z(\mathcal{J}(\bar{P})))$ e N_1 e H_1 as imagens inversas de \bar{N}_1 e $Z(\mathcal{J}(\bar{P}))$ em G , respectivamente. Então $N_1 = N_G(H_1)$ e $H \subset H_1$. Também, $N_{\bar{G}}(\bar{P}) \subseteq \bar{N}_1$ e então $\bar{P} \subseteq \bar{N}_1$, de modo que $P \subseteq N_1$. Além disso, $N_1 \subset G$, pois de outro modo, H_1 seria um p -subgrupo normal de G e, então, teríamos $H_1 \subseteq O_p(G) = H \subset H_1$, uma contradição. Visto que N_1 contém P , N_1 é p -nilpotente pela hipótese de indução e, com isso, \bar{N}_1 também é p -nilpotente. Mas agora, aplicando indução sobre \bar{G} , cuja ordem é menor que a ordem de G obtemos que \bar{G} é p -nilpotente.

Assim, $\bar{G} = O_{p'}(\bar{G})$ e então $G = O_{pp'}(G)$, em particular, G é p -solúvel. Observamos que se G for fortemente p -solúvel, como $O_{p'}(G) = 1$, obtemos do Teorema 1.28 (i) que $Z(\mathcal{J}(P)) \triangleleft G$ de modo que $N_G(Z(\mathcal{J}(P))) = G$ e, pela hipótese sobre $N_G(Z(\mathcal{J}(P)))$, têm-se que G também é p -nilpotente. Vamos mostrar que, de fato, G é fortemente p -

solúvel. Mas por G ser um grupo p -solúvel, G será fortemente p -solúvel se $p \geq 5$ ou $p = 3$ e $SL(2, 3)$ não está envolvido em G . Logo, se $p \geq 5$ então a demonstração acaba aqui. Se $p = 3$, então pelo Teorema 1.28 (i), basta mostrarmos que os S_2 -subgrupos de G são abelianos.

Como $\bar{P} \subseteq \bar{G} = N_{\bar{G}}(O_{p'}(\bar{G}))$, cada $\bar{g} \in \bar{P}$ induz por conjugação um automorfismo $\gamma_{\bar{g}}$ de $O_{p'}(\bar{G})$. Além disso, $\gamma : \bar{P} \longrightarrow Aut(O_{p'}(\bar{G}))$ dada por $\gamma(\bar{g}) = \gamma_{\bar{g}^{-1}}$ é um homomorfismo. Logo, $\bar{P}/Ker\gamma \cong Im\gamma$ e assim $\bar{P}/Ker\gamma$ pode ser visto como um subgrupo de $Aut(O_{p'}(\bar{G}))$. Tomando $\pi' = \{p\}$, $A = \bar{P}/Ker\gamma$ e $G = O_{p'}(\bar{G})$ no Teorema 2.6, segue do item (i) que $\bar{P}/Ker\gamma$ normaliza um S_q -subgrupo \bar{Q} de $O_{p'}(\bar{G})$ para cada primo $q \neq p$, em particular, \bar{P} normaliza $Z(\bar{Q})$. Seja G_1 a imagem inversa de $\bar{P}Z(\bar{Q})$ em G , de modo que $G_1 = PQ_1$, onde Q_1 é um q -grupo abeliano isomorfo a $Z(\bar{Q})$. Mostremos que $G_1 = G$. Visto que $P \subseteq G_1$, se $G_1 \subset G$, então pela hipótese de indução, G_1 é p -nilpotente, ou seja, G_1 possui um p' -subgrupo de Hall normal, que neste caso deve ser o próprio Q_1 . Disso temos $[H, Q_1] \subseteq H \cap Q_1 = 1$, e, assim, Q_1 centraliza H . Porém, como G é p -separável, $O_{p'}(G) = 1$ e $H = O_p(G)$, segue do Teorema 2.12 que $C_G(H) \subseteq H \subset P$ e, então, $Q_1 \subseteq H$, uma contradição. Portanto, $G = G_1 = PQ_1$ e os S_2 -subgrupos de G são necessariamente abelianos. Logo, G é fortemente p -solúvel quando $p = 3$ e o teorema está provado. \square

Na verdade o resultado é falso para $p = 2$ como vemos no

Exemplo 4.20 *Sejam $G = S_4$ e $P = \langle (24), (1234) \rangle$. Colocando $\alpha = (1234)$ e $\beta = (24)$, temos que $\alpha^4 = \beta^2 = 1$ e $e = \beta\alpha\beta = \alpha^3$. Assim, P é um grupo diedral de ordem 8. Também é fácil ver que $Z(P) = \{Id, \alpha^2\} = \{Id, (13)(24)\}$.*

Como P não é abeliano e $\langle \alpha \rangle$ é abeliano de ordem 4, os subgrupos abelianos maximais de P têm ordem 4 e, assim, $\langle \alpha \rangle \in \mathcal{A}(P)$. Além disso, $A_1 = \{Id, \alpha^2, \beta, \alpha^2\beta\}$ é um subgrupo abeliano de P e, portanto, $A_1 \in \mathcal{A}(P)$. Logo, $P = \langle \alpha, A_1 \rangle \subseteq \mathcal{J}(P)$ e, como $P \supseteq \mathcal{J}(P)$, obtemos $\mathcal{J}(P) = P$. Portanto, $Z(\mathcal{J}(P)) = Z(P) = \{Id, (13)(24)\}$.

Calculemos $N_G(Z(\mathcal{J}(P)))$. Como $((13)(24))^\gamma = (13)(24)$ para todo $\gamma \in P$, segue que $P \leq N_G(Z(\mathcal{J}(P)))$ e, assim, $|N_G(Z(\mathcal{J}(P)))| \geq 8$. Pelo Teorema de Lagrange, $|N_G(Z(\mathcal{J}(P)))| = 8, 12$ ou 24 . Note que 12 não pode ser, pois senão $N_G(Z(\mathcal{J}(P)))$ teria um subgrupo de ordem 8. $N_G(Z(\mathcal{J}(P))) \neq S_4$, pois tomando $\gamma = (123) \in S_4$, temos

$((13)(24))^\gamma = (14)(32) \notin \langle (13)(24) \rangle$. Logo, $N_G(Z(\mathcal{J}(P))) = P$. Visto que P é nilpotente, por ser um 2-grupo, P é 2-nilpotente e, assim, $N_G(Z(\mathcal{J}(P)))$ é 2-nilpotente. Porém, S_4 não é 2-nilpotente, pois se fosse, então S_4 teria um subgrupo normal N de ordem 3. Mas então, N seria o único S_3 -subgrupo de S_4 , o que é um absurdo, já que $\langle (123) \rangle$ e $\langle (132) \rangle$ são S_3 -subgrupos distintos de S_4 .

Finalmente vamos ver uma condição suficiente para que um grupo seja solúvel.

Teorema 4.21 (Thompson) *Se um subgrupo maximal de um grupo G é nilpotente de ordem ímpar, então G é solúvel.*

Demonstração: Seja M um subgrupo maximal de G nilpotente de ordem ímpar. Faremos a demonstração por indução sobre $|G|$ notando que o teorema é óbvio se $|G| = 1$. Suponhamos primeiro que M contém um subgrupo normal não trivial H de G . Então, M/H é um subgrupo maximal de G/H e é nilpotente de ordem ímpar. Portanto, por indução, G/H é solúvel. Visto que $H \leq M$ é nilpotente, H é solúvel e pela Proposição 1.10 (iv), G é solúvel. Logo, podemos assumir que M não possui subgrupos normais não triviais de G .

Se $M = 1$, a maximilidade de M implica que G tem ordem prima e, portanto, G é solúvel. Assim, podemos assumir ainda que $M \neq 1$. Sejam P um S_p -subgrupo de M com $p \in \pi(M) = \pi$ e $N = N_G(P)$. Como M é nilpotente, a Proposição 1.13 (iv) mostra que $P \triangleleft M$ e disso temos $M \subseteq N$. Se $N = G$, então $P \triangleleft G$ e como $P \leq M$, temos uma contradição. Assim, $N \subset G$ e a maximilidade de M nos dá $M = N$. Disso e do fato de P estar contido em algum S_p -subgrupo S de G , temos $N_S(P) = S \cap N_G(P) = S \cap M = P$. Agora, a contrapositiva da Proposição 1.4 (i) nos dá $P = S$. Logo, $|G : M|$ e p são relativamente primos. Como isso vale para todo $p \in \pi$, temos que M é um π -subgrupo de Hall de G . Além disso, sabemos que $Z(\mathcal{J}(P)) \text{ char } P \triangleleft M$, de modo que $Z(\mathcal{J}(P)) \triangleleft M$ e um argumento análogo ao anterior mostra que $M = N_G(Z(\mathcal{J}(P)))$. Visto que todo grupo nilpotente é p -nilpotente, segue que $M = N_G(Z(\mathcal{J}(P)))$ é p -nilpotente. Como p é ímpar, o Teorema de Glauberman-Thompson implica que G possui um p' -subgrupo de Hall normal L_p . Este argumento é válido para todo $p \in \pi$. Coloquemos $L = \bigcap_{p \in \pi} L_p$ de modo que $L \triangleleft G$. Agora, $G = PL_p$ com $P \cap L_p = 1$ e portanto L_p contém todos os

p' -elementos de G . Vemos então que L é um π' -grupo. Logo, L é, de fato, um π' -subgrupo de Hall de G , pois $\frac{G}{L}$ é um π -grupo. Desta forma temos que $G = ML$ com $L \cap M = 1$ e $L \triangleleft G$. Mostraremos que L é nilpotente. Disso e do fato que M é também nilpotente, seguirá que L e $\frac{G}{L} \cong M$ são solúveis. Daí, pela Proposição 1.10 (ii), G será solúvel.

Seja Q um subgrupo de Sylow de L . Então $G = N_G(Q)L$ pelo Argumento de Frattini. De $L \triangleleft G$ segue claramente que $N_L(Q) \triangleleft N_G(Q)$. Pelo Teorema de Schur-Zassenhaus, $N_G(Q) = XN_L(Q)$ para algum subgrupo X de $N_G(Q)$. Isto dá $G = XN_L(Q)L = XL$, de modo que X é um outro complemento de L e, então, $X = M^g$ para algum $g \in G$, pela segunda parte do Teorema de Schur-Zassenhaus. Disso segue que X é um subgrupo maximal de G . Além disso, como X normaliza Q , pois $X \subseteq N_G(Q)$, temos que XQ é um subgrupo de G e $Q \triangleleft XQ$. Assim, $X \leq XQ \leq G$. Pela maximalidade de X , devemos ter $G = XQ$, pois $Q \not\subseteq X$. Logo, $Q \triangleleft XQ = G$. Concluimos então que todo subgrupo de Sylow de L é normal em G e, assim, em L . Portanto, L é nilpotente, como desejado. \square

Observação 4.22 *Para encerrarmos o capítulo, vamos mostrar que o Teorema de Thompson não vale se a ordem do subgrupo maximal nilpotente for par. De fato, pela Proposição 1.28 (ii), $L_2(17)$ é simples e como $L_2(17)$ não tem ordem prima, segue que $L_2(17)$ não é solúvel. Por outro lado, $L_2(17)$ possui um subgrupo maximal de ordem 32, que é nilpotente por ser um 2-grupo.*

Capítulo 5

p -Singularidades

Sejam G um grupo finito, P um S_p -subgrupo de G e K um subgrupo normal de G tal que G/K é um p -grupo abeliano. Então, $G' \subseteq K$ e $G = KP$, pois G/K é um p -grupo. Em particular, $P \cap G' \leq K$ e o homomorfismo canônico $\phi : P \rightarrow KP/K$ induz um epimorfismo $\bar{\phi} : P/P \cap G' \rightarrow KP/K = G/K$. Além disso, pelo Terceiro Teorema do Isomorfismo, existe um isomorfismo $\psi : G/K \rightarrow P/P \cap K$. Deste modo temos que, $\psi\bar{\phi} : P/P \cap G' \rightarrow P/P \cap K$ é um epimorfismo. Portanto, $G/K \cong \psi\bar{\phi}(P/P \cap G')$

Agora, G/G' é abeliano e, como $G' \triangleleft G$, temos que $P \cap G'$ é um S_p -subgrupo de G' . Seja N a imagem inversa de $O_{p'}(G/G')$ em G . É fácil ver que $P \cap G' = P \cap N$, $N \triangleleft G$ e G/N é um p -grupo abeliano isomorfo a $P/P \cap G'$. Portanto, concluímos que:

Se P é um S_p -subgrupo de um grupo finito G e K um subgrupo normal de G tal que G/K é um p -grupo abeliano, então $P \cap G' \leq K$ e G/K é isomorfo a uma imagem homomórfica de $P/P \cap G'$. Mais ainda, existe um subgrupo normal N de G tal que G/N é isomorfo a $P/P \cap G'$.

Isto mostra a importância do subgrupo $P \cap G'$, que é chamado de *subgrupo focal* de P em G . Há vários resultados que dão uma descrição mais simplificada deste subgrupo. Por exemplo, quando P é abeliano, o Teorema 7.4.4 de [6], afirma que $P \cap G' = P \cap N_G(P)'$.

Num trabalho publicado no final da década de 60, T. Yoshida mostrou que se P não possui grupo quociente isomorfo a $\mathbb{Z}_p \wr \mathbb{Z}_p$, também temos $P \cap G' = P \cap N_G(P)'$. Neste capítulo, o objetivo principal é apresentar a demonstração do Teorema de Yoshida. Para

tanto, iremos estudar algumas propriedades de dois novos conceitos: *transfer de caracter* e *p-singularidades*.

Observamos que neste capítulo G sempre denotará um grupo finito e p um primo.

5.1 Caracteres

Nesta seção apresentamos o conceito de *caracter* de um grupo e algumas de suas propriedades. Em seguida veremos um método para se obter, a partir de um caracter de um subgrupo, um caracter para o grupo todo.

Os resultados desta seção não serão provados, mas o leitor poderá encontrar suas demonstrações no Capítulo 2 de [1].

Seja ϕ uma \mathbb{C} -representação matricial de um grupo G , i.é, ϕ é um homomorfismo de G em $GL(n, \mathbb{C})$ e seja $\theta = \text{tr}\phi : G \rightarrow \mathbb{C}$ a função definida por $\theta(g) = \text{traço}(\phi(g))$ para todo $g \in G$, ou seja, $\theta(g)$ é a soma dos elementos da diagonal principal de $\phi(g)$. A função θ é chamada *o caracter de G admitido pela \mathbb{C} -representação ϕ* . Dizemos que θ é um *caracter de G* se θ é o caracter admitido por alguma \mathbb{C} -representação de G . O grau de um caracter é o grau de uma representação que o admite. Chamamos de *caracter principal*, e denotamos por 1_G , ao caracter admitido pela \mathbb{C} -representação $\tau : G \rightarrow GL(1, \mathbb{C})$ dada por $\tau(g) = 1$ para todo $g \in G$.

Vamos ver agora algumas propriedades de caracteres.

Lema 5.1 *O caracter θ admitido pela \mathbb{C} -representação ϕ de G satisfaz as seguintes propriedades:*

- (i) $\theta(1)$ é o grau de ϕ ;
- (ii) Para todo $g \in G$, $\theta(g)$ é uma soma de raízes complexas da unidade;
- (iii) Para todo $g \in G$, $\theta(g^{-1}) = \overline{\theta(g)}$
- (iv) θ é uma função constante nas classes de conjugação.

Sejam χ e θ dois caracteres de um grupo G . Definimos as aplicações $\theta + \chi : G \longrightarrow \mathbb{C}$ e $\theta \cdot \chi : G \longrightarrow \mathbb{C}$, respectivamente, por $(\theta + \chi)(g) = \theta(g) + \chi(g)$ e $(\theta \cdot \chi)(g) = \theta(g) \cdot \chi(g)$, para todo $g \in G$. Vamos mostrar que $\theta + \chi$ e $\theta \cdot \chi$ são caracteres de G , i.é, existem \mathbb{C} -representações Λ e Ψ de G que admitem $\theta + \chi$ e $\theta \cdot \chi$ como caracteres. Para isso precisamos da noção de soma direta e produto tensorial de \mathbb{C} -representações matriciais de um grupo.

Denotamos por $Mat(n, F)$ o conjunto das matrizes $n \times n$ com entradas no corpo F .

Sejam $M = (\alpha_{ij})_{i,j} \in Mat(m, F)$ e $N = (\beta_{kl})_{k,l} \in Mat(n, F)$, onde F é um corpo.

(i) Denotamos por $M \oplus N$ a matriz $(m + n) \times (m + n)$ sobre F , definida por

$$M \oplus N = \begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}. \text{ Tal matriz é chamada } \textit{soma direta de } M \text{ e } N,$$

(ii) Definimos o bloco P_{rs} de ordem m por $P_{rs} = \beta_{rs}M = (\beta_{rs} \cdot \alpha_{ij})_{1 \leq i, j \leq m}$. Denotamos por $M \otimes N$ a matriz $mn \times mn$ formada pelos blocos $(P_{rs})_{1 \leq r, s \leq n}$. Essa matriz é chamada *produto tensorial de } M \text{ e } N.*

Observamos que $(M \oplus N) \cdot (B \oplus C) = M \cdot B \oplus N \cdot C$, onde $M, C \in Mat(m, F)$ e $N, B \in Mat(n, F)$. Também temos, claramente, que se $M \in GL(m, F)$ e $N \in GL(n, F)$, então $M \otimes N \in GL(mn, F)$.

Sejam $\phi : G \longrightarrow GL(m, \mathbb{C})$ e $\psi : G \longrightarrow GL(n, \mathbb{C})$ duas \mathbb{C} -representações matriciais de G de graus n e m , respectivamente. Denotamos por $\phi \oplus \psi$, a função $\phi \oplus \psi : G \longrightarrow GL(m + n, \mathbb{C})$ dada por $(\phi \oplus \psi)(g) = \phi(g) \oplus \psi(g)$, para todo $g \in G$. É fácil ver que $\phi \oplus \psi$ é um homomorfismo e, portanto, $\phi \oplus \psi$ define uma \mathbb{C} -representação matricial de G de grau $n + m$, que é chamada de *soma direta de } \phi \text{ e } \psi. Analogamente, a função $\phi \otimes \psi : G \longrightarrow GL(mn, \mathbb{C})$ definida por $(\phi \otimes \psi)(g) = \phi(g) \otimes \psi(g)$, para todo $g \in G$, é um homomorfismo, de modo que $\phi \otimes \psi$ define uma \mathbb{C} -representação matricial de G de grau mn . Esta representação é chamada de *produto tensorial de } \phi \text{ e } \psi.**

Agora, sejam θ e χ são os caracteres admitidos pelas representações ϕ e ψ , respectivamente. Então, para todo $g \in G$, temos:

$$tr((\phi \oplus \psi)(g)) = tr(\phi(g) \oplus \psi(g)) = tr(\phi(g)) + tr(\psi(g)) = \theta(g) + \chi(g) = (\theta + \chi)(g) \quad (5.1)$$

$$tr((\phi \otimes \psi)(g)) = tr(\phi(g) \otimes \psi(g)) = tr(\phi(g)) \cdot tr(\psi(g)) = \theta(g) \cdot \chi(g) = (\theta \cdot \chi)(g) \quad (5.2)$$

Logo, as representações $\phi \oplus \psi$ e $\phi \cdot \psi$ admitem $\theta + \chi$ e $\theta \cdot \chi$ como caracter, respectivamente.

Observe que a operação de multiplicação de caracteres de G é associativo e distributivo em relação à operação de adição. Além disso, o conjunto dos caracteres de G não é um grupo com a operação de adição, pois a função nula de G em \mathbb{C} não é admitida como caracter por nenhuma representação de G . Para isso, definimos o conceito caracter generalizado de G . Dados dois caracteres θ e χ de G , chamamos $\chi - \theta$ de *caracter generalizado* de G .

Sejam $\chi = \chi_1 - \chi_2$ e $\theta = \theta_1 - \theta_2$ dois caracteres generalizados de G . Definimos $\chi + \theta = (\chi_1 + \theta_1) - (\chi_2 + \theta_2)$ e $\chi \cdot \theta = \chi_1 \cdot \theta_1 + \chi_2 \cdot \theta_2 - (\chi_1 \cdot \theta_2 + \chi_2 \cdot \theta_1)$. O conjunto de todos os caracteres generalizados munido com estas duas operações é um anel comutativo, com identidade 1_G , chamado *anel caracter de G* , que é denotado por $ch(G)$.

Um caso particular de caracter é aquele admitido por uma representação de grau 1. Tal caracter é chamado de *caracter linear*. O conjunto de todos os caracteres lineares de um grupo G é denotado por \hat{G} . Como $GL(1, \mathbb{C})$ é isomorfo a \mathbb{C}^* , existe um homomorfismo do grupo G em \mathbb{C}^* . É fácil ver que \hat{G} é um grupo com respeito a multiplicação de caracteres, onde o elemento neutro é o caracter 1_G .

Vamos estudar agora um método de construção de caracteres de um grupo a partir de caracteres de um subgrupo.

Se H é um subgrupo de um grupo G , chamamos de *transversal à direita de H em G* o subconjunto T de G constituído de um elemento de cada classe lateral à direita de H em G .

Seja H um subgrupo de um grupo G de índice m e sejam $T = \{g_1, g_2, \dots, g_m\}$ uma transversal à direita de H em G e $\phi : H \rightarrow GL(n, F)$ uma representação matricial de H de grau n . Definimos uma função $\hat{\phi} : G \rightarrow Mat(n, F)$ por $\hat{\phi}(g) = 0_n$, se $g \notin H$ e $\hat{\phi}(g) = \phi(g)$, se $g \in H$, onde 0_n denota a matriz nula $n \times n$.

Agora, se $g \in G$ e $i, j \in \{1, 2, \dots, m\}$, coloquemos $B_{ij}(g) = \hat{\phi}(g_i g g_j^{-1})$, de modo que $B_{ij}(g) = 0_n$ se $g_i g g_j^{-1} \notin H$. Definimos $\phi^G : G \rightarrow Mat(mn, F)$ por $\phi^G(g) = (B_{ij}(g))_{1 \leq i, j \leq m}$ para todo $g \in G$.

Lema 5.2 (i) ϕ^G definida acima é uma F -representação matricial de G de grau mn , chamada *representação induzida em G pela representação ϕ de H* .

(ii) Quaisquer duas F -representações induzidas em G , através de duas escolhas de transversais, são equivalentes.

Chamamos ϕ^G de *representação induzida* em G pela representação ϕ de H .

Observamos que se $\phi = 1_H$ é a representação unitária de H , então ϕ^G é uma representação permutacional de G .

Observação 5.3 Consideremos a notação estabelecida acima e tome $y \in G$. Sabemos que para cada i , existe uma única classe lateral Hg_i contendo $g_i y$, de modo que existe apenas um i' tal que $g_i y g_{i'}^{-1} \in H$. Daí, se $j \neq i'$, então $\phi(g_i y g_j^{-1}) = 0$ e portanto cada linha (ou coluna) da matriz $\phi^G(y)$ possui apenas um elemento não nulo. Em particular, $1_H^G(y)$ é uma matriz $m \times m$ cujas linha (ou colunas) possuem apenas um elemento 1 e os demais são todos nulos. Deste modo pode-se permutar as linhas (ou colunas) da matriz $1_H^G(y)$ até obtermos a matriz identidade de ordem m . Suponha que sejam k tais permutações. Assim, o número de permutações das linhas (ou colunas) da matriz $\phi^G(y)$ até se obter a matriz diagonal formada pelos blocos $\phi(g_i y g_{i'}^{-1})$ é mk .

Se ϕ^G é a representação induzida em G pela representação ϕ de H e $\text{tr}(\phi) = \theta$, denotamos $\text{tr}(\phi^G)$ por θ^G e diremos que θ^G é o *caracter induzido* em G pelo caracter θ de H .

O próximo resultado estabelece, entre outras, uma fórmula para calcular θ^G .

Lema 5.4 Sejam H um subgrupo de G e ϕ uma \mathbb{C} -representação de H com $\theta = \text{tr}\phi$. Considere a função $\hat{\theta} : G \rightarrow \mathbb{C}$ dada por

$$\hat{\theta}(g) = \begin{cases} 0, & \text{se } g \notin H \\ \theta(g), & \text{se } g \in H \end{cases}.$$

Temos:

(i) Se $g \in G$, então $\theta^G(g) = \frac{1}{|H|} \sum_{x \in G} \hat{\theta}(xgx^{-1})$;

(ii) θ^G independe da escolha da transversal à direita de H .

(iii) Se $\chi : H \rightarrow \mathbb{C}$ é um caracter de H , então $(\theta + \chi)^G = \theta^G + \chi^G$

Observação 5.5 Seria conveniente se pudéssemos calcular θ^G sem precisarmos percorrer x por todo o grupo G . Para tanto, tomemos $T = \{g_1, g_2, \dots, g_m\}$ uma transversal à direita de H em G . Como $G = Hg_1 \cup \dots \cup Hg_m$ e θ é constante nas classes de conjugação de H , temos

$$\theta^G(g) = \frac{1}{|H|} \sum_{i=1}^m \sum_{h \in H} \hat{\theta}(hg_i g_i^{-1} h^{-1}) = \frac{1}{|H|} \sum_{i=1}^m \sum_{h \in H} \hat{\theta}(g_i g_i^{-1}) = \sum_{i=1}^m \hat{\theta}(g_i g_i^{-1}).$$

Sejam $\mu = \theta - \chi$ um caracter generalizado de G . Definimos $\mu^G = \theta^G - \chi^G$. É fácil ver que a fórmula $\mu^G(g) = \frac{1}{|H|} \sum_{x \in G} \hat{\mu}(xgx^{-1})$ continua válida.

Lema 5.6 (Frobenius) *Sejam H e M subgrupos de G tais que $H \subseteq M \subseteq G$. Seja θ um caracter generalizado de H e μ um caracter generalizado de G . Então:*

$$(i) \text{ [Transitividade da indução]} (\theta^M)^G = \theta^G$$

$$(ii) \theta^G \cdot \mu = (\theta \cdot \mu|_H)^G$$

5.2 Transfer de Caracter

Sejam χ um caracter de G e ϕ é uma representação matricial que admite o caracter χ . Definimos $\det(\chi) : G \rightarrow \mathbb{C}^*$ por $\det(\chi)(g) = \det(\phi(g))$, para todo $g \in G$. É claro que $\det(\chi)$ é um homomorfismo de G em \mathbb{C}^* , de modo que $\det(\chi)$ é um caracter linear de G . Agora, dado um caracter generalizado $\chi = \chi_1 - \chi_2$ de G , definimos $\det(\chi)(g) = \det(\chi_1)(g) \cdot (\det(\chi_2)(g))^{-1}$, para todo $g \in G$. É fácil ver que \det é um homomorfismo do grupo aditivo dos caracteres generalizados de G no grupo multiplicativo dos caracteres lineares de G .

Se χ e θ são caracteres de G admitidos pelas representações matriciais ϕ e ψ , respectivamente, então para todo $g \in G$, temos

$$\det(\chi\theta)(g) = \det((\phi \otimes \psi)(g)) = (\det\phi(g))^n \cdot (\det\psi(g))^m = (\det(\chi))^n(g) \cdot (\det(\theta))^m(g),$$

onde n e m são, respectivamente, o grau de θ e χ . Assim, $\det(\chi\theta) = \det(\chi)^{\theta(1)}\det(\theta)^{\chi(1)}$. Esta última igualdade pode ser facilmente estendida para caracteres generalizados, i.é, se χ e θ são caracteres generalizados de G , então $\det(\chi\theta) = \det(\chi)^{\theta(1)}\det(\theta)^{\chi(1)}$.

Para todo subgrupo H de G e $\theta \in ch(H)$, definimos

$$T_H^G(\theta) = \det(\theta^G - \theta(1)1_H^G).$$

A aplicação $T_H^G : ch(H) \longrightarrow \hat{G}$ é chamada um *transfer de caracter*. Sempre que estiver explícito quem é o subgrupo H de G , denotamos um transfer de caracter simplesmente por T^G . Se não houver confusão, denotaremos a restrição de T^G aos subgrupos de \hat{H} pela mesma notação.

Em seguida vamos estabelecer quatro propriedades, que nada mais são que fórmulas para facilitar o cálculo do transfer de caracter.

Lema 5.7 *Sejam H um subgrupo de G e $\theta, \theta_1, \theta_2 \in ch(H)$. Então valem as seguintes afirmações:*

- (i) $T^G(\theta) = T^G(\det(\theta))$;
- (ii) $T^G(\theta_1\theta_2) = T^G(\theta_1)^{d_2} \cdot T^G(\theta_2)^{d_1}$, onde $d_i = \theta_i(1)$. Em particular, $T^G|_{\hat{H}}$ é um homomorfismo de \hat{H} em \hat{G} ;
- (iii) Se $H \leq K \leq G$, então $T_K^G(T_H^K(\theta)) = T_H^G(\theta)$;
- (iv) Se $\chi \in ch(G)$, então $T_H^G(\chi|_H) = \det(\chi)^{|G:H|}$;

Demonstração: (i) Vamos provar primeiro que (i) é válido se θ for um caracter de H . Seja ϕ uma representação matricial de H com caracter θ e grau d , i.é, $\theta(1) = d$. Seja $x_i, 1 \leq i \leq n$ um conjunto completo de representantes das classes laterais à direita de H em G . Sabe-se que a representação induzida $\phi^G : G \longrightarrow GL(nd, \mathbb{C})$ é tal que $\phi^G(y)$ é uma matriz $n \times n$ em blocos cuja entrada (i, j) é a matriz $d \times d$ $\hat{\phi}(x_i y x_j^{-1})$.

Seja $y \in G$. Para cada i , existe uma única classe lateral $Hx_{i'}$ contendo $x_i y$, de modo que existe apenas um i' tal que $x_i y x_{i'}^{-1} \in H$. Pela Observação 5.3, temos que

$\det(\theta^G)(y) = \det(\phi^G(y)) = (\text{sgn}(y))^d \prod_i \det(\phi(x_i y x_i^{-1}))$ onde $\text{sgn} = \det 1_H^G$. Substituindo ϕ por $\det\theta$, temos que

$$\begin{aligned}
\det((\det\theta)^G(y)) &= \text{sgn}(y) \prod_i \det((\det\theta)(x_i y x_i^{-1})) \\
&= \text{sgn}(y) \prod_i \det(\det(\phi(x_i y x_i^{-1}))) \\
&= \text{sgn}(y) \prod_i \det(\phi(x_i y x_i^{-1})) \\
&= \text{sgn}(y) \det(\theta^G)(y) (\text{sgn}(y))^d)^{-1} \\
&= \text{sgn}(y)^{1-d} \det(\theta^G)(y).
\end{aligned} \tag{5.3}$$

Agora,

$$\begin{aligned}
T^G(\theta)(y) &= \det(\theta^G - \theta(1)1_H^G)(y) \\
&= \det(\theta^G)(y) \cdot ((\det\theta(1)1_H^G)(y))^{-1} \\
&= \det(\theta^G)(y) \cdot \left(\det \underbrace{(1_H^G + \dots + 1_H^G)}_{\theta(1) \text{ vezes}}(y) \right)^{-1} \\
&= \det(\theta^G)(y) \cdot \left((\det(1_H^G)(y))^d \right)^{-1} \\
&= \det(\theta^G)(y) \cdot ((\text{sgn}(y))^d)^{-1}.
\end{aligned} \tag{5.4}$$

Disso segue finalmente que

$$\begin{aligned}
T^G(\det\theta)(y) &= \det((\det\theta)^G)(y) \cdot ((\det(\det\theta(1)1_H^G))(y))^{-1} \\
&= \det((\det\theta)^G)(y) \cdot ((\det(\det(\phi(1))1_H^G))(y))^{-1} \\
&= \det((\det\theta)^G)(y) \cdot ((\det 1_H^G)(y))^{-1} \\
&= \det((\det\theta)^G)(y) \cdot (\text{sgn}(y))^{-1} \\
&= \text{sgn}(y)^{1-d} \det(\theta^G)(y) \cdot (\text{sgn}(y))^{-1} \quad \text{por (5.3)} \\
&= \det(\theta^G)(y) \cdot (\text{sgn}(y))^d)^{-1} \\
&= T^G(\theta)(y) \quad \text{por (5.4)}.
\end{aligned}$$

Logo, $T^G(\theta) = T^G(\det(\theta))$, para todo caracter θ de H . Se θ for um caracter generalizado, então do fato de T^G ser um homomorfismo do grupo aditivo dos caracteres generalizados no grupo multiplicativo dos caracteres lineares de G , segue que $T^G(\theta) = T^G(\det(\theta))$.

(ii) Sejam χ_1 e χ_2 dois caracteres generalizados de H . Como \det e T^G são homomorfismos, temos $\det(\chi_1) \cdot \det(\chi_2) = \det(\chi_1 + \chi_2)$ e $T^G(\chi_1 + \chi_2) = T^G(\chi_1) \cdot T^G(\chi_2)$. Disso e de (i) temos $T^G(\det(\chi_1)\det(\chi_2)) = T^G(\chi_1 + \chi_2) = T^G(\chi_1) \cdot T^G(\chi_2) = T^G(\det(\chi_1)) \cdot T^G(\det(\chi_2))$. Assim,

$$T^G(\theta_1\theta_2) = T^G(\det(\theta_1\theta_2)) = T^G(\det(\theta_1)^{d_2} \cdot \det(\theta_2)^{d_1}) = T^G(\theta_1)^{d_2} \cdot T^G(\theta_2)^{d_1}.$$

Em particular, se $\theta_1, \theta_2 \in \hat{H}$, então $\theta(1) = \theta_2(1) = 1$ e, conseqüentemente, $T^G|_{\hat{H}}$ é um homomorfismo de \hat{H} em \hat{G} .

(iii) De (i) e de $(\theta^K)^G = \theta^G$, resulta que

$$\begin{aligned} T_K^G(T_H^K(\theta)) &= T_K^G(\theta^K - \theta(1)1_H^K) \\ &= \det((\theta^K - \theta(1)1_H^K)^G - (\theta^K(1) - \theta(1)1_H^K(1))1_K^G) \\ &= \det((\theta^K)^G - \theta(1)(1_H^K)^G - (\theta^K(1) - \theta(1)1_H^K(1))1_K^G) \\ &= \det(\theta^G - \theta(1)1_H^G - (|K:H| \cdot \theta(1) - \theta(1) \cdot |K:H| \cdot 1_H(1))1_K^G) \\ &= \det(\theta^G - \theta(1)1_H^G) \\ &= T_H^G(\theta). \end{aligned}$$

(iv) Sabemos do Lema 5.6 (ii) que $(\chi|_H)^G = \chi \cdot 1_H^G$. Assim, para todo $y \in G$,

$$\begin{aligned} T^G(\chi|_H)(y) &= \det(\chi \cdot 1_H^G - \chi(1)1_H^G)(y) \\ &= \det(\chi \cdot 1_H^G)(y) \cdot (\det(\chi(1)1_H^G)(y))^{-1} \\ &= \left[(\det(\chi))^{1_H^G(1)} \cdot (\det(1_H^G))^{\chi(1)} \right](y) \cdot ((\det 1_H^G)^{\chi(1)}(y))^{-1} \\ &= (\det(\chi))^{|G:H|}(y). \end{aligned}$$

□

Dados λ um caracter de H e $t \in G$, escrevemos $\lambda^{t^{-1}}(g) = \lambda(tgt^{-1})$ para todo $g \in G$. O próximo resultado nos dá uma maneira alternativa para calcular $\lambda^G|_K$.

Teorema 5.8 (Mackey) *Sejam H e K subgrupos de G , λ um caracter de H , $R = \{t_1, \dots, t_m\}$ um conjunto completo de representantes das (H, K) -classes duplas em G , $K_{t_i} = K \cap H^{t_i}$ e $\lambda_{t_i} = \lambda^{t_i^{-1}}|_{K_{t_i}}$, $1 \leq i \leq m$. Então, $\lambda^G|_K = \sum_{i=1}^m (\lambda_{t_i})^K$.*

Demonstração: Seja $U = \{u_1, \dots, u_r\}$ uma transversal à direita de H em $G = \bigcup_{i=1}^m Ht_iK$ tal que $\{u_1, \dots, u_{s_1}\}$, $\{u_{s_1+1}, \dots, u_{s_2}\}$, \dots , $\{u_{s_{m-1}+1}, \dots, u_{s_m}\}$ são conjuntos de representantes classes laterais à direita de H em Ht_1K , Ht_2K, \dots, Ht_mK , respectivamente. Note que: para $1 \leq i \leq s_1$, $u_i = h_{1i}t_1k_{1i}$; para $s_1 + 1 \leq i \leq s_2$, $u_i = h_{2i}t_2k_{2i}$; \dots ; para $s_{m-1} + 1 \leq i \leq s_m$, $u_i = h_{mi}t_mk_{mi}$, onde cada $h_{li} \in H$ e cada $k_{li} \in K$. Sabemos que o número de classes laterais de H em Ht_iK é $|K : H^{t_i} \cap K|$, $1 \leq i \leq m$. Assim, o número de elementos em uma transversal à direita de $H^{t_i} \cap K$ em K é igual ao número de representantes das classes laterais à direita de H em Ht_iK . Claramente, $\{k_{1i} : 1 \leq i \leq s_1\}$, $\{k_{2i} : s_1 + 1 \leq i \leq s_2\}$, \dots , $\{k_{mi} : s_{m-1} + 1 \leq i \leq s_m\}$ são transversais de $H^{t_1} \cap K$, $H^{t_2} \cap K$, \dots , $H^{t_m} \cap K$ em K , respectivamente.

Sejam $k \in K$ e λ um caracter de H admitido pela representação ϕ . Então,

$$\lambda^G(k) = \sum_{i=1}^r \hat{\lambda}(u_i k u_i^{-1}) = \sum_{i=1}^{s_1} \hat{\lambda}(u_i k u_i^{-1}) + \sum_{i=s_1+1}^{s_2} \hat{\lambda}(u_i k u_i^{-1}) + \dots + \sum_{i=s_{m-1}+1}^{s_m} \hat{\lambda}(u_i k u_i^{-1}).$$

Vamos analisar $\sum_{i=1}^{s_1} \hat{\lambda}(u_i k u_i^{-1})$. Note que $\sum_{i=1}^{s_1} \hat{\lambda}(u_i k u_i^{-1}) = \sum_{i=1}^{s_1} \hat{\lambda}(t_1 k_{1i} k k_{1i}^{-1} t_1^{-1})$, onde

$$\begin{aligned} \hat{\lambda}(t_1 k_{1i} k k_{1i}^{-1} t_1^{-1}) &= \begin{cases} 0, & \text{se } t_1 k_{1i} k k_{1i}^{-1} t_1^{-1} \notin H \\ \lambda(t_1 k_{1i} k k_{1i}^{-1} t_1^{-1}), & \text{se } t_1 k_{1i} k k_{1i}^{-1} t_1^{-1} \in H \end{cases} \\ &= \begin{cases} 0, & \text{se } k_{1i} k k_{1i}^{-1} \notin H^{t_1} \cap K \\ \lambda(t_1 k_{1i} k k_{1i}^{-1} t_1^{-1}), & \text{se } k_{1i} k k_{1i}^{-1} \in H^{t_1} \cap K \end{cases}. \end{aligned}$$

Agora, vamos calcular $(\lambda_{t_1})^K(k)$. Observe que

$$(\lambda_{t_1})^K(k) = \left(\lambda^{t_1^{-1}} \Big|_{H^{t_1} \cap K} \right)^K(k) = \sum_{i=1}^{s_1} \left(\lambda^{t_1^{-1}} \Big|_{H^{t_1} \cap K} \right)(k_{1i} k k_{1i}^{-1}),$$

onde

$$\begin{aligned} \left(\lambda^{t_1^{-1}} \Big|_{H^{t_1} \cap K} \right)(k_{1i} k k_{1i}^{-1}) &= \begin{cases} 0, & \text{se } k_{1i} k k_{1i}^{-1} \notin H^{t_1} \cap K \\ \lambda^{t_1^{-1}}(k_{1i} k k_{1i}^{-1}), & \text{se } k_{1i} k k_{1i}^{-1} \in H^{t_1} \cap K \end{cases} \\ &= \begin{cases} 0, & \text{se } k_{1i} k k_{1i}^{-1} \notin H^{t_1} \cap K \\ \lambda(t_1 k_{1i} k k_{1i}^{-1} t_1^{-1}), & \text{se } k_{1i} k k_{1i}^{-1} \in H^{t_1} \cap K \end{cases} \end{aligned}$$

Logo, $(\lambda_{t_1})^K(k) = \sum_{i=1}^{s_1} \hat{\lambda}(u_i k u_i^{-1})$. Procedendo da mesma forma com as outras parcelas de $\lambda^G(k)$, concluímos que $\lambda^G(k) = \sum_{i=1}^m (\lambda_{t_i})^K(k)$. \square

O próximo resultado nos dá uma fórmula alternativa para calcularmos $T^G(\lambda)(x)$, quando $\lambda \in \hat{H}$ e x é um elemento de G .

Lema 5.9 (Decomposição de Mackey) (i) *Sejam $H, K \leq G$, $\lambda \in \hat{H}$, R um conjunto completo de representantes das (H, K) -classes duplas em G , $K_g = K \cap H^g$ e $\lambda_g = \lambda^{g^{-1}}|_{K_g}$ para todo $g \in R$. Então, $T_H^G(\lambda)|_K = \prod_{g \in R} T_{K_g}^K(\lambda_g)$.*

(ii) *Seja $H \leq G$, $x \in G$, $\lambda \in \hat{H}$, R um conjunto completo das (H, K) -classes duplas em G e $e_g = |\langle x \rangle : \langle x \rangle \cap H^g|$ para todo $g \in R$. Então, $T_H^G(\lambda)(x) = \prod_{g \in R} \lambda(gx^{e_g}g^{-1})$.*

Demonstração: (i) Pelo Teorema de Mackey, $\lambda^G|_K = \sum_{g \in R} \lambda_g^K$ e $1_H^G|_K = \sum_{g \in R} 1_{K_g}^K$.

Assim,

$$T_H^G(\lambda)|_K = \det\left(\sum_{g \in R} \lambda_g^K - \lambda(1) \sum_{g \in R} 1_{K_g}^K\right) = \det\left(\sum_{g \in R} (\lambda_g^K - \lambda_g(1)1_{K_g}^K)\right) = \prod_{g \in R} T^K(\lambda_g).$$

(ii) Agora, seja $K = \langle x \rangle$. Definimos K_g e λ_g como em (i). Então $e_g = |K : K_g|$, para todo $g \in R$. Seja $g \in R$. Visto que K é cíclico, K tem um caracter linear μ_g tal que $\mu_g|_{K_g} = \lambda_g$. Assim, $T_{K_g}^K(\lambda_g) = (\det \mu_g)^{|K:K_g|} = \mu_g^{e_g}$, pelo Lema 5.7 (iv) e porque $\mu_g \in \hat{K}$. Como $x^{e_g} \in K_g$ e μ_g é um homomorfismo, temos $T_{K_g}^K(\lambda_g)(x) = \lambda_g(x^{e_g}) = \lambda(gx^{e_g}g^{-1})$. Por (i), obtemos que $T_H^G(\lambda)(x) = \prod_{g \in R} T_{K_g}^K(\lambda_g)(x) = \prod_{g \in R} \lambda(gx^{e_g}g^{-1})$ e (ii) está provado. \square

Para subconjuntos X e Y de G , escrevemos $X^Y = \{x^y : x \in X, y \in Y\}$. Se $T^G(\lambda)(x) \neq 1$, $x \in G$, obtém-se um informação importante sobre o kernel de λ através do

Corolário 5.10 *Sejam $H \leq G$, $x \in G$ e $\lambda \in \hat{H}$. Se $T^G(\lambda)(x) \neq 1$, então*

$$\langle x \rangle^G \cap H \not\subseteq \text{Ker} \lambda.$$

Demonstração: Sejam $K = \langle x \rangle$, R um conjunto completo de representantes das (H, K) -classes duplas em G e $e_g = |K : K \cap H^g|$ para todo $g \in R$. Como $x^{e_g} \in K_g = K \cap H^g$, temos que $gx^{e_g}g^{-1} \in H \cap K^G$. Agora suponhamos que $K^G \cap H \subseteq \text{Ker} \lambda$. Então, $\lambda(gx^{e_g}g^{-1}) = 1$, para todo $g \in R$ e pelo Lema 5.9 (ii), segue que $T^G(\lambda)(x) = \prod_{g \in R} \lambda(gx^{e_g}g^{-1}) = 1$, contradizendo a hipótese. \square

No decorrer desta seção, usamos as seguintes notações: Sejam X um grupo e Y um subgrupo de X . Denotamos o homomorfismo restrição $\hat{X} \longrightarrow \hat{Y}$ por R_Y^X ou simplesmente R_Y , quando não houver confusão. Para qualquer subgrupo Λ de \hat{X} , colocamos $\Lambda^\perp = \{x \in X : \lambda(x) = 1, \forall \lambda \in \Lambda\}$. Este é chamado de *anulador* de Λ . Denotamos por \hat{X}_p o único S_p -subgrupo de \hat{H} . Escrevemos R_Y^X e T_Y^X no lugar de $R_Y^X|_{\hat{X}_p}$ e $T_Y^X|_{\hat{Y}_p}$, respectivamente, sempre que for conveniente e não houver confusão. Também, $O^p(X)$ é o subgrupo gerado por todos os p' -elementos de X e $X'(p) = X'O^p(X)$.

Lema 5.11 *Sejam p um primo e $H \leq G$ tal que $(|G : H|, p) = 1$. Então*

(i) *A composição $T^G \circ R_H : \hat{G}_p \longrightarrow \hat{H}_p \longrightarrow \hat{G}_p$ é um isomorfismo e $\hat{H}_p = (\text{Im} R_H) \times (\text{Ker} T^G)$.*

(ii) *Seja P um p -subgrupo de H e suponhamos que $P \cap H^p H' \leq K < P \cap G^p G'$. Então existe $\lambda \in \hat{H}$ tal que $\circ(\lambda) = p$, $K \leq \text{Ker} \lambda$ e $\lambda|_P \neq 1$.*

Demonstração: (i) Coloquemos $R = R_H$ e $T = T^G$. Pela definição de R e pelo Lema 5.7 (ii) temos que $T \circ R$ é um homomorfismo. Do Lema 5.7 (iv), segue que para todo $\mu \in \hat{G}_p$, $T(R(\mu)) = T(\mu|_H) = (\det(\mu))^{|G:H|} = \mu^{|G:H|}$. Seja $\mu \in \text{Ker}(T \circ R)$. Então $\mu^{|G:H|} = 1_{\hat{G}_p}$, onde $1_{\hat{G}_p}$ é o elemento neutro do grupo multiplicativo \hat{G}_p . Como $|\hat{G}_p| = p^r$, para algum inteiro r , $(|G : H|, p) = 1$ e $\mu^{|G:H|} = 1_{\hat{G}_p}$, segue que $\mu = 1_{\hat{G}_p}$ e, portanto, $T \circ R$ é injetora. Visto que \hat{G}_p é finito, temos que $T \circ R$ é um isomorfismo. Assim, R é um monomorfismo e T é um epimorfismo. Também, $\text{Im} R \cap \text{Ker} T = 1$. Disso e de $\text{Im} R \cong \hat{G}_p \cong \frac{\hat{H}_p}{\text{Ker} T}$, obtemos $\hat{H}_p = \text{Im} R \times \text{Ker} T$.

(ii) Suponhamos que não exista $\lambda \in \hat{H}$ tal que $\circ(\lambda) = p$, $T^G(\lambda) = 1$, $K \leq \text{Ker} \lambda$ e $\lambda|_P \neq 1$. Seja Λ o grupo de todos os caracteres $\lambda \in \hat{H}$ tais que $H^p H' K \subseteq \text{Ker} \lambda$ e

$M = R(\Omega_1(\hat{G}_p))$. Como \hat{G}_p é abeliano, e $\Omega_1(\hat{G}_p) = \{\mu \in \hat{G}_p : \circ(\mu) = p\} \cup \{1\}$, segue que os elementos não triviais de M têm ordem p .

Afirmamos que $M \leq \Lambda$.

De fato, como $M \leq \hat{H}_p \leq \hat{H}$, basta mostrarmos que $H^p H' K \subseteq \text{Ker} \lambda$, para todo $\lambda \in M$. Para cada $h \in H$, $\lambda(h^p) = \lambda^p(h) = 1_H(h) = 1$ e então $H^p \subseteq \text{Ker} \lambda$. É claro que $H' \subseteq \text{Ker} \lambda$. Para vermos que $K \subseteq \text{Ker} \lambda$, basta usarmos a hipótese $K < P \cap G^p G' \leq H \cap G^p G'$. Portanto, $H^p H' K \subseteq \text{Ker} \lambda$ e $M \leq \Lambda$. Disso segue que $\Lambda \supseteq (\text{Ker} T \cap \Lambda)M$. Vamos mostrar agora que $(\text{Ker} T \cap \Lambda)M \supseteq \Lambda$. Se $\lambda \in \Lambda$, então para todo $h \in H$ temos $\lambda^p(h) = \lambda(h)^p = \lambda(h^p) = 1$ e, assim, $\lambda \in \hat{H}_p$. Pelo item (i), $\lambda = R_H(\mu)\theta = \mu|_H \theta$, onde $\mu \in \hat{G}_p$ e $\theta \in \text{Ker} T$. Note que pelo Lema 5.7 (iv), temos $T(\lambda) = T(\mu|_H) = \mu^{|G:H|}$ e isto implica que $1_G = \mu^{|G:H|p}$, de modo que $\circ(\mu)|_{|G:H|p}$. Por outro lado, $\circ(\mu)|_{|\hat{G}_p|} = p^r$ e então $\circ(\mu)|_{\text{mdc}(p^r, |G:H|p)} = p$. Logo, $\circ(\mu) = p$, se $\mu \neq 1$. Assim, $R_H(\mu) \in M$. Por outro lado, $\theta = R_H(\mu)^{-1}\lambda \in \Lambda \cap \text{Ker} T$ e, portanto, $\Lambda = (\text{Ker} T \cap \Lambda)M$.

Agora, vamos provar que $P \leq (\Lambda \cap \text{Ker} T)^\perp$. Pelo que assumimos no início, segue que para todo $\lambda \in \hat{H}$, temos $\circ(\lambda) \neq p$ ou $T(\lambda) \neq 1$ ou $H \not\leq \text{Ker} \lambda$ ou $\lambda|_P = 1$. Tomemos $\lambda \in \Lambda \cap \text{Ker} T$. Como $\circ(\lambda) = p$ e $K < P \cap G^p G'$, da mesma maneira que antes, obtemos $K \leq \text{Ker} \lambda$. Logo, pelo que assumimos acima, devemos ter $\lambda|_P = 1$, ou seja, $P \leq (\Lambda \cap \text{Ker} T)^\perp$. Assim, $P \cap G^p G' \leq (\Lambda \cap \text{Ker} T)^\perp \cap M^\perp \leq ((\Lambda \cap \text{Ker} T)M)^\perp = \Lambda^\perp$, de modo que $P \cap G^p G' \leq P \cap H^p H' K \leq K$. Mas isso contraria a hipótese. Portanto, (ii) é válido e o lema está provado. \square

O último resultado desta seção é devido a Tate-Thompson e será utilizado no próximo tópico a ser estudado. Sua demonstração será omitida, mas o leitor interessado poderá encontrá-la em [8].

Teorema 5.12 (Tate-Thompson) *Seja H um subgrupo de um grupo G de índice relativamente primo com p , p primo e $K \leq H \cap G'(p)$. Suponhamos que $H \cap G^p G' = H^p H' K$. Temos:*

$$(i) \quad H \cap G'(p) = H'(p)K;$$

$$(ii) \quad \text{Se } K \triangleleft H \text{ e } K \leq O^p(G), \text{ então } H \cap O^p(G) = O^p(H)K.$$

5.3 Singularidades

A maior parte desta seção é uma preparação para demonstrarmos o resultado principal deste capítulo apresentado no Teorema 5.27. Para tanto, precisamos do conceito de singularidade.

Definição 5.13 *Sejam H um grupo finito, S um subgrupo de H , x um p -elemento de H e λ um caracter linear de S de ordem p . Dizemos que (S, λ, x) é uma p -singularidade em H se:*

- (a) $T^H(\lambda)(x) \neq 1$;
- (b) $\langle x^p \rangle^H \cap S \subseteq \text{Ker} \lambda$.

O subgrupo S , o caracter linear λ e o p -elemento x são chamados um *subgrupo singular* (ou simplesmente uma *singularidade*), um *caracter singular*, e um *elemento singular* da singularidade (S, λ, x) , respectivamente.

Exemplo 5.14 *Tome $H = A_4$, $S = \langle (123) \rangle$, $p = 3$ e λ o caracter linear de S de ordem 3 dado por $\lambda(1) = 1$, $\lambda(123) = \omega$, $\lambda(132) = \bar{\omega}$, onde $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Note que $\langle x^p \rangle^H \cap S \subseteq \text{Ker} \lambda$, onde $x = (123)$. Portanto, para mostrarmos que (S, λ, x) é uma 3-singularidade em H , basta checarmos que $T_S^H(\lambda)(x) \neq 1$. Para isso, precisamos encontrar as matrizes $\phi^H(x)$ e $\psi^H(x)$, onde ϕ e ψ são representações matriciais de S que admitem λ e 1_S como caracteres, respectivamente. É fácil ver que*

$$T = \{g_1 = 1, g_2 = (12)(34), g_3 = (13)(24), g_4 = (14)(23)\}$$

é uma transversal de S em H . Sabemos que $\phi^H(x) = (B_{ij}(x))_{1 \leq i, j \leq 4}$ onde $B_{ij}(x) = \hat{\lambda}(g_i x g_j^{-1}) \in \mathbb{C}^$*

Note que apenas $g_1 x g_1^{-1}, g_2 x g_3^{-1}, g_3 x g_4^{-1}, g_4 x g_3^{-1}$ estão em P e são todos iguais a (123) , de modo que $B_{11}(x) = B_{23}(x) = B_{34}(x) = B_{43}(x) = \omega$ e os demais $B_{ij}(x)$ são nulos. Portanto,

$$\phi^H(x) = \begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega \\ 0 & \omega & 0 & 0 \end{pmatrix} \quad e \quad \psi^H(x) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Logo, $T^H(\lambda)(x) = \det(\lambda^H(x)) \cdot (\det(1_S^H)(x))^{-1} = \omega \neq 1$ e (S, λ, x) é uma p -singularidade em A_4 .

O primeiro resultado desta seção é composto por 5 ítems e nos mostra como obtermos singularidades a partir de uma singularidade conhecida.

Lema 5.15 *Seja (S, λ, x) uma p -singularidade em um grupo finito H . Então valem as seguintes afirmações:*

- (i) Para $a, b \in H$, $(S^a, \lambda^{a^{-1}}, x^b)$ é também uma p -singularidade em H .
- (ii) Se N é um subgrupo normal de H contido em $\text{Ker}\lambda$, então $(\frac{S}{N}, \lambda', xN)$ é uma p -singularidade em $\frac{H}{N}$ onde λ' é o caracter linear de $\frac{S}{N}$ induzido por λ .
- (iii) Se P é um S_p -subgrupo de S , então $(P, \lambda|_P, x)$ é também uma p -singularidade em H .
- (iv) Se $S \leq R \leq H$, então $(R, T_S^R(\lambda), x)$ é também p -singularidade em H .
- (v) Se $x \in L \leq H$, então existe um conjugado $R = S^h$ de S tal que $(L \cap R, \lambda^{h^{-1}}|_{L \cap R}, x)$ é uma p -singularidade em L . Além disso, se $H = LS$, então $(S \cap L, \lambda|_{S \cap L}, x)$ é uma p -singularidade em L .

Demonstração: (i) Recordemos que $\lambda^{a^{-1}}(s) = \lambda(asa^{-1})$ para todo $s \in S$. É fácil ver que $S^a \leq H$, x^b é um p -elemento de H e $\lambda^{a^{-1}}$ é um caracter linear de S^a de ordem p . Portanto, resta provarmos (a) e (b) da definição 5.13. Note que $\langle (x^b)^p \rangle^H \cap S^a = \langle x^p \rangle^H \cap S^a$. Assim, se $g \in \langle (x^b)^p \rangle^H \cap S^a$ então $g = s^a \in \langle x^p \rangle^H$ para algum $s \in S$. Deste modo, $s \in \langle x^p \rangle^H \cap S$ e $\lambda^{a^{-1}}(g) = \lambda^{a^{-1}}(s^a) = \lambda(s) = 1$. Logo, $g \in \text{Ker}\lambda^{a^{-1}}$, i.é, $\langle (x^b)^p \rangle^H \cap S^a \subseteq \text{Ker}\lambda^{a^{-1}}$.

Para verificarmos (a), devemos calcular $(\psi^{a^{-1}})^H(y)$ e $(\phi_{S^a})^H(y)$, onde $y \in H$ e $\psi^{a^{-1}}$ e ϕ_{S^a} são, respectivamente, representações matriciais que admitem $\lambda^{a^{-1}}$ e 1_{S^a} como caracteres. Seja $T = \{g_1, \dots, g_m\}$ uma transversal de S^a em H . Então $U = \{ag_1, \dots, ag_m\}$ é uma transversal de S em H . Sabemos que $(\psi^{a^{-1}})^H(y) = (B_{ij}(y))_{1 \leq i, j \leq m}$, onde

$$B_{ij}(y) = \begin{cases} 0, & \text{se } g_i y g_j^{-1} \notin S^a \\ \lambda^{a^{-1}}(g_i y g_j^{-1}), & \text{se } g_i y g_j^{-1} \in S^a \end{cases}.$$

Disso e da definição de $\lambda^{a^{-1}}$, obtemos que $(\psi^{a^{-1}})^H(y) = \psi^H(y)$ e $(\phi_{S^a})^H(y) = \phi^H(y)$, onde ψ e ϕ são representações matriciais de H que admitem λ e 1_S como caracteres, respectivamente e as representações induzidas ψ^H e ϕ^H são determinadas pela transversal U . Deste modo, $T_{S^a}^H(\lambda^{a^{-1}})(x^b) = \det(\psi^H(x^b)) = \det(\phi^H(x^b))^{-1} \cdot T_S^H(\lambda)(x) \neq 1$.

(ii) Claramente basta verificar os itens (a) e (b) da definição 5.13. Como λ' é um caracter linear de $\frac{S}{N}$ induzido por λ temos que $\lambda'(gN) = \lambda(g)$, para todo $g \in S$ e, assim, $gN \in \text{Ker } \lambda'$ se, e somente se, $g \in \text{Ker } \lambda$. Se g é um elemento de S tal que $gN \in \langle x^p N \rangle^{H/N} \cap (S/N)$, então $gN = (x^{pr})^h N$ para algum inteiro r e $h \in H$. Assim, $(x^{pr})^h = gn$ para algum $n \in N$ e, daí, $(x^{pr})^h \in \langle x^p \rangle^H \cap S \subseteq \text{Ker } \lambda$. Como também $N \subseteq \text{Ker } \lambda$, temos $g = (x^{pr})^h n^{-1} \in \text{Ker } \lambda$ e, conseqüentemente, $gN \in \text{Ker } \lambda'$.

Vamos provar (a). Por hipótese, $N \triangleleft H$, $N \subseteq \text{Ker } \lambda \subseteq S \subseteq H$. Do Terceiro Teorema do Isomorfismo segue que $|\bar{H} : \bar{S}| = |H : S|$, onde $\bar{H} = H/N$ e $\bar{S} = S/N$. Seja $\{h_1, \dots, h_t\}$ uma transversal de S em H . Então $\{\bar{h}_1, \dots, \bar{h}_t\}$ é uma transversal de \bar{S} e \bar{H} . Assim, $\psi^{\bar{H}}(\bar{x}) = \left(\hat{\lambda}'(\bar{h}_i \bar{x} \bar{h}_j^{-1}) \right)_{1 \leq i, j \leq m}$, onde ψ' é uma representação matricial de S/N que admite λ' como caracter. Como $\bar{h}_i \bar{x} \bar{h}_j^{-1} \in \bar{S}$ se e somente se $h_i x h_j^{-1} \in S$, tem-se que $\hat{\lambda}'(\bar{h}_i \bar{x} \bar{h}_j^{-1}) \neq 0$ se e somente se $\hat{\lambda}(h_i x h_j^{-1}) \neq 0$. Assim, $\psi^{\bar{H}}(\bar{x}) = \left(\hat{\lambda}(h_i x h_j^{-1}) \right)_{1 \leq i, j \leq m}$ e, portanto, $T_{\bar{S}}^{\bar{H}}(\bar{x}) \neq 1$, pois $T_S^H(x) \neq 1$.

(iii) Claramente, $\langle x^p \rangle^H \cap P \subseteq \langle x^p \rangle^H \cap S \subseteq \text{Ker } \lambda$. Assim, para todo $y \in \langle x^p \rangle^H \cap P$ temos $\lambda(y) = 1$ e, conseqüentemente, $\lambda|_P = 1$. Portanto, $\langle x^p \rangle^H \cap P \subseteq \text{Ker } \lambda|_P$. Além disso, $P \subseteq S \subseteq H$ e assim, pelo Lema 5.7 itens (iii), (iv), (ii) e (i), valem as seguintes igualdades:

$$T_P^H(\lambda|_P) = T_S^H(T_P^S(\lambda|_P)) = T_S^H(\det(\lambda)^{|S:P|}) = (T_S^H(\det(\lambda)))^{|S:P|} = (T_S^H(\lambda))^{|S:P|}.$$

Deste modo, $T_P^H(\lambda|_P)(x) = T_S^H(\lambda)^{|S:P|}(x) = (T_S^H(\lambda)(x))^{|S:P|} \neq 1$, pois $T_S^H(\lambda)(x)$ é um p -elemento e $|S : P|$ é um p' -elemento.

(iv) Como $T_S^R(\theta) \in \hat{R}$, para todo $\theta \in \hat{S}$, basta mostrarmos os itens (a) e (b) da definição 5.13. Pelo Lema 5.7 (iii), $T_R^H(T_S^R(\lambda))(x) = T_S^H(\lambda)(x) \neq 1$ e (a) está provado. Suponhamos que $\langle x^p \rangle^H \cap R \not\subseteq \text{Ker} T_S^R(\lambda)$. Então, existem um inteiro k e h em H tais que $((x^p)^k)^h \in R$ e $T_S^R(\lambda)(x^{(pk)h}) \neq 1$. Assim, pelo Corolário 5.10, temos $\langle x^{(pk)h} \rangle^R \cap S \not\subseteq \text{Ker} \lambda$. Como $\langle x^{(pk)h} \rangle^R \cap S \leq \langle x^p \rangle^H \cap S$, segue que $\langle x^p \rangle^H \cap S \not\subseteq \text{Ker} \lambda$, contradizendo a hipótese. Portanto, (iv) está provado.

(v) Visto que $T^H(\lambda)(x) \neq 1$, $(T^H(\lambda)|_L)(x) \neq 1$. Por outro lado, segue do Teorema da Decomposição de Mackey que $(T^H(\lambda)|_L)(x) = \prod_h T^L(\lambda^{h^{-1}}|_{L \cap S^h})(x)$, onde h percorre um conjunto completo de representantes das (S, L) -classes duplas em H e, portanto, existe $h \in H$ tal que $T^L(\mu)(x) \neq 1$, onde $\mu = \lambda^{h^{-1}}|_{R \cap L}$ e $R = S^h$. Além disso, $\langle x^p \rangle^{Lh^{-1}} \cap S \cap L^{h^{-1}} \subseteq \langle x^p \rangle^H \cap S \subseteq \text{Ker} \lambda$ e é fácil ver que $(\text{Ker} \lambda)^h \subseteq \text{Ker} \mu$. Logo, $\langle x^p \rangle^L \cap R \cap L \leq (\langle x^p \rangle^{Lh^{-1}} \cap S \cap L^{h^{-1}})^h \leq (\text{Ker} \lambda)^h \subseteq \text{Ker} \mu$. Portanto o item (b) está provado e o lema segue. \square

Sejam H, G grupos finitos, Ω um conjunto finito e $\alpha : G \rightarrow \text{Sym}(\Omega)$ uma representação permutacional de G . Seja $\text{Map}(\Omega, H)$ o conjunto de todas as funções de Ω em H . Para $f, g \in \text{Map}(\Omega, H)$ definimos fg colocando $(fg)(i) = f(i)g(i)$ para todo $i \in \Omega$. É fácil ver que com este produto de funções, o conjunto $\text{Map}(\Omega, H)$ é um grupo, onde o elemento neutro é a função f_e dada por $f_e(i) = 1$ para todo $i \in \Omega$ e o elemento inverso de $f \in \text{Map}(\Omega, H)$ é a função f^{-1} definida por $f^{-1}(i) = f(i)^{-1}$ para todo $i \in \Omega$.

Agora, para toda $f \in \text{Map}(\Omega, H)$ e $x \in G$ definimos $f^x : \Omega \rightarrow H$, colocando $f^x(i) = f(xi)$, para todo $i \in \Omega$, onde xi indica a ação de x sobre i , i.é, $xi = \alpha(x)(i)$. Note que para todo $x \in G$, a aplicação $\psi^x : \text{Map}(\Omega, H) \rightarrow \text{Map}(\Omega, H)$ definida por $\psi^x(f) = f^x$ é um automorfismo de $\text{Map}(\Omega, H)$. Além disso, $(f^x)^y = f^{xy}$ para todo $x, y \in G$ e $f^1 = f$. Assim, G age sobre $\text{Map}(\Omega, H)$ por automorfismos e, portanto, podemos formar o produto semi-direto de $\text{Map}(\Omega, H)$ por G , que denotamos por $H \wr G$ e chamamos de *produto entrelaçado* de H por G construído da representação permutacional α . O subgrupo normal $\text{Map}(\Omega, H)$ é chamado *subgrupo base* de $H \wr G$.

Denote $n = |\Omega|$. Claramente a aplicação

$$\begin{aligned} \phi : \quad H \times \cdots \times H &\longrightarrow \text{Map}(\Omega, H) \\ h = (h_1, \dots, h_n) &\longmapsto \phi_h : \Omega \longrightarrow H \\ &\quad i \longmapsto h_i \end{aligned}$$

é um isomorfismo. Deste modo podemos dizer que $\text{Map}(\Omega, H)$ é isomorfo a n cópias de H .

Neste trabalho, o produto entrelaçado $\mathbb{Z}_p \wr \mathbb{Z}_p$ sempre será construído a partir da representação regular de \mathbb{Z}_p .

Exemplo 5.16 *Seja $\text{Map}(\mathbb{Z}_2, \mathbb{Z}_2) = \{f_0, f_1, f_2, f_3\}$, onde*

$$\begin{array}{cccc} f_0 : & 0 \longmapsto 0 & f_1 : & 0 \longmapsto 1 & f_2 : & 0 \longmapsto 0 & f_3 : & 0 \longmapsto 1 \\ & 1 \longmapsto 0 & & 1 \longmapsto 1 & & 1 \longmapsto 1 & & 1 \longmapsto 0 \end{array}$$

É fácil ver que $\alpha = (1, f_1)$ e $\gamma = (1, f_2)$ geram $\mathbb{Z}_2 \wr \mathbb{Z}_2$, $\alpha^2 = \gamma^4 = (0, f_0)$ e $\alpha\gamma\alpha = \gamma^3$. Portanto, $\mathbb{Z}_2 \wr \mathbb{Z}_2$ é isomorfo ao grupo diedral de ordem 8, D_8 .

Observação 5.17 *Suponhamos que na definição acima, H seja um grupo cíclico de ordem r gerado por h . É fácil ver que $\text{Map}(\Omega, H)$ é gerado pelas $|\Omega|$ funções v_i dadas por $v_i(j) = h$, se $i = j$ e $v_i(j) = 1$, se $i \neq j$.*

Observação 5.18 *Sejam G um grupo de permutações transitivo sobre $\Omega = \{1, \dots, n\}$ e Y o estabilizador de 1. Vamos mostrar que $|G : Y| = n$. Seja $i \in \Omega$. Visto que G é transitivo, existe $x_i \in G$ tal que $x_i(1) = i$. Então, para todo $y \in Y$, temos $x_i y(1) = i$. Reciprocamente, se $x(1) = i$, então $x_i^{-1}x(1) = 1$ e, assim, $x \in x_i Y$. Portanto, $x_i Y$ é um conjunto completo de elementos transformando 1 em i . Em particular, $x_i Y \neq x_j Y$, se $i \neq j$. Além disso, um elemento de G transforma 1 em i , para algum i , de modo que todo elemento de G está em $x_i Y$ para algum i , $1 \leq i \leq n$. Logo, o conjunto $\{x_i Y : 1 \leq i \leq n\}$ é um conjunto completo de classes laterais à esquerda de Y em G e, assim, $|G : Y| = n$. De modo geral, se G é um grupo de permutações transitivo sobre um conjunto finito Ω e Y o estabilizador de uma letra de Ω , então $|G : Y| = |\Omega|$.*

Com esta última observação, faz sentido o seguinte resultado:

Lema 5.19 *Sejam G um grupo de permutações transitivo sobre um conjunto finito Ω , Y o estabilizador de uma letra e C um grupo cíclico de ordem p gerado por c . Do grupo permutacional G , construa o produto entrelaçado $H = C \wr G$ com subgrupo base $V \cong C^{|\Omega|}$. Então, $Y \times V$ é uma p -singularidade em H com elemento singular pertencente a V .*

Demonstração: Sem perda de generalidade, podemos supor que $\Omega = \{1, \dots, n\}$. Da hipótese temos que G age transitivamente sobre $\Omega = \{1, \dots, n\}$. O subgrupo base V de H é gerado pelo conjunto $\{v_1, v_2, \dots, v_n\}$, onde cada v_i é dado pela Observação 5.17. É claro que $\{v_1, v_2, \dots, v_n\}$ é invariante pela ação de G . Como Y fixa um elemento de Ω , podemos assumir que Y fixa v_n . Seja $S = Y \times V \leq H$ e $K = Y \times \langle v_1 \cdots v_{n-1} \rangle$, de modo que $S = K \times \langle v_n \rangle$

Visto que $\frac{S}{K}$ é um grupo cíclico, $\frac{S}{K}$ possui caracteres lineares. Tomemos λ' um destes caracteres, de modo que $\lambda = \lambda' \circ \alpha : S \rightarrow \mathbb{C}^*$ seja um caracter linear de S cujo kernel contém K , onde α é o homomorfismo canônico de S em $\frac{S}{K}$.

Afirmção: Se $t \notin S$, então $tv_n t^{-1} \in K$. Com efeito, suponhamos que $v_n t^{-1} \notin K$. Então, como $\{v_1, v_2, \dots, v_n\}$ é G -invariante, devemos ter $v_n t^{-1} = v_n$, o que implica que t^{-1} fixa v_n . Logo, $t^{-1} \in Y \subseteq S$ e, portanto, $t \in S$.

Claramente, $|H : S| = |G : Y| = n$. Tomemos $\{1, t_2, \dots, t_n\}$ uma transversal de S em H . Então, $\lambda^H(v_n) = \sum_{i=1}^n \hat{\lambda}(v_n^{t_i^{-1}}) = \lambda(v_n) + \sum_{i=2}^n \hat{\lambda}(v_n^{t_i^{-1}})$. Agora, para $2 \leq i \leq n$, $v_n^{t_i^{-1}} \in K$, de modo que $\hat{\lambda}(v_n^{t_i^{-1}}) = \lambda(v_n^{t_i^{-1}}) = 1$. Logo, $\lambda^H(v_n) = n - 1 + \lambda(v_n)$. Analogamente, $1_S^H(v_n) = n$. Portanto, $(\lambda^H - 1_S^H)(v_n) = (\lambda - 1_S)(v_n)$, de modo que $T_S^H(\lambda)(v_n) = \lambda(v_n) \neq 1$. Além disso, como $v_n^p = 1$, temos que $\langle v_n^p \rangle \cap S = 1 \subseteq \text{Ker } \lambda$. Logo, (S, λ, v_n) é uma p -singularidade em H . \square

Observação 5.20 *No Lema 5.19, temos $|C \wr G| = |V| \cdot |G|$ e $|Y \times V| = |V| \cdot |Y|$, de modo que $|C \wr G : Y \times V| = |G : Y|$. Agora considere o caso particular $G = \mathbb{Z}_p$ agindo sobre \mathbb{Z}_p por soma, Y o estabilizador de $\bar{0} \in \mathbb{Z}_p$ e $C = \mathbb{Z}_p$. Então, $|Y| = 1$ e, portanto, existe um subgrupo singular V de $\mathbb{Z}_p \wr \mathbb{Z}_p$ (V é $Y \times V$ do Lema 5.19) tal que $|\mathbb{Z}_p \wr \mathbb{Z}_p : V| = |\mathbb{Z}_p : Y| = p$.*

Se H é um subgrupo de um grupo G , denotamos por H_G a interseção de todos os conjugados de H . Claramente, $H_G \triangleleft G$.

Observação 5.21 *Seja S um subgrupo de um grupo P e $V = S_P$. Denotemos por P/S o conjunto de todas as classes laterais à esquerda de S em P . Certamente, a aplicação*

$$\begin{aligned} \phi : P &\longrightarrow \text{Sym}(P/S) \\ x &\longmapsto \phi_x : P/S \longrightarrow P/S \\ &gS \longmapsto xgS \end{aligned}$$

é uma representação permutacional de P sobre P/S cujo kernel é $S_P = V$. Então, ϕ induz um homomorfismo $\bar{\phi} : P/V \longrightarrow \text{Sym}(P/S)$. Quando $S \triangleleft P$, então $V = S$ e a representação $\bar{\phi}$ é a representação regular de P/S .

A demonstração do próximo resultado será omitida, mas o leitor poderá encontrá-la na página 9 de [9].

Lema 5.22 *Sejam (S, λ, x) uma singularidade em um p -grupo P , $V = S_P$, $K = \text{Ker } \lambda$, $\bar{P} = P/K_P$ e $\bar{V} = V/K_P$. Assuma que x pertence a V . Então $\bar{P} \cong \mathbb{Z}_p \wr P/V$, onde o produto entrelaçado é construído da representação permutacional de P/V sobre o conjunto P/S e o subgrupo base é isomorfo a \bar{V} . Em particular, \bar{V} é abeliano elementar de dimensão $|P : S|$.*

Vamos estudar agora algumas propriedades de singularidades em p -grupos.

Lema 5.23 *Sejam P um p -grupo, M um subgrupo maximal de P , $\lambda \in \hat{M}$, $K = \text{Ker } \lambda$ e $u \in P \setminus M$. Então temos:*

(i) $T_M^P(\lambda)|_M = \lambda^{\bar{u}}$, onde $\bar{u} = 1 + u + \dots + u^{p-1}$ e $T_M^P(\lambda)(u) = \lambda(u^p)$;

(ii) Se (M, λ, x) é uma singularidade em P para um elemento x em P , então $\frac{P}{K_P} \cong \mathbb{Z}_p \wr \mathbb{Z}_p$.

Demonstração: (i) Como P é um p -grupo, P é nilpotente e, portanto, seu subgrupo maximal M é normal em P e disso segue que $|P : M| = p$. Claramente $\{1, u, \dots, u^{p-1}\}$ é

uma transversal de M em P . Sejam ψ e ϕ , respectivamente, representações matriciais de P que admitem λ e 1_M como caracteres. Se $x \in M$, então $u^i x (u^i)^{-1} \in M$, de modo que a matriz $\psi^P(x)$ é a matriz diagonal $(a_{ij})_{1 \leq i, j \leq p}$, onde $a_{ii} = \lambda(u^{i-1} x (u^{i-1})^{-1})$, $1 \leq i \leq p$ e a matriz $\phi^P(x)$ é a identidade $p \times p$. Assim, temos $T_M^P(\lambda)(x) = \det(\lambda^p - 1_M^P)(x) = \prod_{i=0}^{p-1} \lambda(u^i x (u^i)^{-1}) = \prod_{i=0}^{p-1} \lambda^{(u^i)^{-1}}(x) = \lambda^{\bar{u}}(x)$. Logo, $T_M^P(\lambda)|_M = \lambda^{\bar{u}}$.

Agora, provemos que $T_M^P(\lambda)(u) = \lambda(u^p)$. Dividimos em dois casos.

1º caso: $\langle u \rangle = P$. Nesta situação temos $M\langle u \rangle = P$, $M \cap \langle u \rangle = M$ e existe apenas uma $(M, \langle u \rangle)$ -classe dupla em P . Daí, temos $e_1 = |\langle u \rangle : M \cap \langle u \rangle| = |\langle u \rangle : M| = p$ e, pelo Lema 5.9 (ii), $T_M^P(\lambda)(u) = \lambda(u^p)$.

2º caso: $\langle u \rangle \neq P$. Neste caso, os fatos de M ser maximal e normal em P e $u \notin M$, garantem que $M\langle u \rangle = P$ e $M \cap \langle u \rangle = 1$ e, novamente, existe apenas uma $(M, \langle u \rangle)$ -classe dupla em P . Além disso, $e_1 = |\langle u \rangle : M \cap \langle u \rangle| = |\langle u \rangle| = p$. Pelo Lema 5.9 (ii), obtemos $T_M^P(\lambda)(u) = \lambda(u^p)$ e (i) está demonstrado.

(ii) Seja (M, λ, x) é uma singularidade em P . Afirmamos que $x \in M$. Com efeito, suponhamos que $x \notin M$. Como $[P : M] = p$, temos que $x^p \in M$. Por outro lado, como $x \in P \setminus M$, segue do ítem (i) e da definição de singularidade que $\lambda(x^p) = T_M^P(\lambda)(x) \neq 1$, de modo que $x^p \notin \text{Ker} \lambda$. Disso e de $\langle x^p \rangle^P \cap M \subseteq \text{Ker} \lambda$, obtemos $x^p \notin \langle x^p \rangle^P \cap M$. Como $x^p \in \langle x^p \rangle^P$, segue que $x^p \notin M$, contradição. Portanto, visto que $M_P = M$ e $x \in M$, podemos aplicar o Lema 5.22 e a Observação 5.21 para obter $\frac{P}{K_P} \cong \mathbb{Z}_p \wr \frac{P}{M} \cong \mathbb{Z}_p \wr \mathbb{Z}_p$. \square

No que segue, iremos apresentar uma caracterização de p -grupos que não possuem subgrupos singulares próprios.

Lema 5.24 *Seja P um p -grupo. Então P não possui subgrupo singular próprio se, e somente se, P não possui grupo quociente isomorfo a $\mathbb{Z}_p \wr \mathbb{Z}_p$.*

Demonstração: Suponhamos que P possui um subgrupo normal N tal que $P/N \cong \mathbb{Z}_p \wr \mathbb{Z}_p$. Por esse isomorfismo e pela Observação 5.20, P/N possui uma singularidade, digamos $(M/N, \lambda', xN)$, com $p = |P/N : M/N| = |P : M|$. Logo, M é um subgrupo próprio de P . Além disso, x é um p -elemento e $\lambda = \lambda' \circ \alpha : M \rightarrow \mathbb{C}^*$ é um caracter linear de M , onde α é o homomorfismo canônico de M em M/N . Note para todo $m \in M$, $\lambda^p(m) = \lambda(m^p) = \lambda'(\alpha(m^p)) = \lambda'(\alpha(m)^p) = \lambda'((mN)^p) = \lambda'^p(mN) = 1$.

Vamos mostrar que $\langle x^p \rangle^P \cap M \subseteq \text{Ker} \lambda$ e $T_M^P(\lambda)(x) \neq 1$.

Seja $y \in \langle x^p \rangle^P \cap M$. Então, $y = (x^{p^r})^g \in M$ onde $g \in P$. Então, $\alpha(y) = yN \in M/N$ e $\alpha(y) = yN = g^{-1}x^{p^r}gN = g^{-1}Nx^{p^r}gN = (x^{p^r}N)^{gN}$, ou seja, $\alpha(y) \in \langle x^p \rangle^{P/N} \cap M/N \subseteq \text{Ker} \lambda'$. Assim, $\lambda(y) = \lambda'(\alpha(y)) = 1$. Portanto, $\langle x^p \rangle^P \cap M \subseteq \text{Ker} \lambda$.

Agora, como $|P/N : M/N| = |P : M|$, um raciocínio análogo aquele realizado no item (ii) do Lema 5.15 nos dá que $T_M^P(\lambda)(x) \neq 1$. Logo, (M, λ, x) é uma p -singularidade em P com M um subgrupo próprio de P .

Suponhamos que P possui um subgrupo singular próprio S . Afirmamos que P possui um subgrupo maximal singular. De fato, se S for maximal, a afirmação segue. Se S não for maximal, então existe um subgrupo R tal que $S < R < P$. Como S é singular em H , segue do Lema 5.15 (iv) que R também é singular em H . Se R for maximal, a afirmação está provada. Senão, repete-se o processo até encontrarmos um subgrupo singular M que seja maximal. Pelo Lema 5.23 (ii), P possui um grupo quociente isomorfo a $\mathbb{Z}_p \wr \mathbb{Z}_p$. \square

O próximo resultado será o último antes de enunciarmos e demonstrarmos o teorema que é o objetivo central dessa seção.

Lema 5.25 *Sejam H um subgrupo de um grupo G com índice relativamente primo com p , P um p -subgrupo de H e P^* um subgrupo de P . Suponhamos que uma das seguintes condições esteja satisfeita:*

- (a) P é um S_p -subgrupo de G e $P \cap H' \leq P^* < P \cap G'$;
- (b) $P \cap H^p H' \leq P^* < P \cap G^p G'$;

Então temos:

- (i) Existe $\lambda \in \hat{H}$ tal que $\circ(\lambda) = p$, $T_H^G(\lambda) = 1$, $P^* \leq \text{Ker} \lambda$ e $\lambda|_P \neq 1$;
- (ii) Seja $x \in P \setminus \text{Ker} \lambda$ tal que $\langle x^p \rangle^G \cap H \subseteq \text{Ker} \lambda$. Para cada $g \in G$, escreva

$$\begin{aligned} H_g &= H \cap H^g, & \lambda_g &= \lambda^{-1}|_{H_g} \cdot \lambda^{g^{-1}}|_{H_g} \\ P_g &= P \cap H^g, & \lambda'_g &= \lambda_g|_{P_g}. \end{aligned}$$

Então existe $g \in G \setminus H$ tal que (H_g, λ_g, x) e (P_g, λ'_g, x) são p -singularidades em H e P , respectivamente.

Demonstração: Suponhamos (a) válido. Neste caso afirmamos que $\Phi(P)P^p < P \cap G^p G'$. De fato, como P é um p -grupo finito, $\Phi(P) = P^p P'$ e, então, de $P^* < P \cap G'$, resulta $\Phi(P)P^* \leq P \cap G^p G'$. Se $\Phi(P)P^* = P \cap G^p G'$, aplicando o item (i) do Teorema 5.12, obtemos $P \cap G'(p) = P'(p)P^*$. Assim, como $P \cap G' \leq P \cap G'(p)$ e $P'(p)P^* = P^*$ (pois $P' \subseteq P^*$), chegamos a $P \cap G' \leq P^* < P \cap G'$, uma contradição. Portanto, $\Phi(P)P^* < P \cap G^p G'$. Além disso, $P \cap H^p H' \leq \Phi(P)P^*$. Assim, $P \cap H^p H' \leq \Phi(P)P^* < P \cap G^p G'$, de modo que é suficiente provarmos o lema assumindo apenas (b).

(i) Para mostrarmos o item (i), basta tomarmos $K = P^*$ no Lema 5.11 (ii).

(ii) Seja R um conjunto completo de representantes das (H, H) -classes duplas em G . Sabemos que para todo $g \in R$, HgH é a união de $|H : H \cap H^g|$ classes laterais à direita distintas de H em HgH . Disso e da cardinalidade de uma classe lateral de H em G ser $|H|$, temos que $|HgH| = |H : H \cap H^g| \cdot |H|$. Como $G = \bigcup_{g \in R} HgH$ (união disjunta), segue que $|G| = \sum_{g \in R} |HgH| = |H| \sum_{g \in R} |H : H \cap H^g|$ de onde obtemos que $|G : H| = \sum_{g \in R} |H : H \cap H^g|$.

Do item (i), existe $\lambda \in \hat{H}$ tal que $\circ(\lambda) = p$, $T_H^G(\lambda) = 1$ e $\lambda|_P \neq 1$. Por hipótese, $x \in P \setminus Ker \lambda$ e $(p, |G : H|) = 1$. Disso obtemos $1 \neq \lambda^{-|G:H|}(x)$ e $T_H^G(\lambda)(x) = 1$, de modo que

$$1 \neq \lambda^{-|G:H|}(x) \cdot T_H^G(\lambda)(x) \quad (5.5)$$

Tomando $K = H$ no Lema 5.9 (i), temos

$$T_H^G(\lambda)(x) = \prod_{g \in R} T_{H_g}^H(\lambda^{g^{-1}}|_{H_g})(x) \quad (5.6)$$

Além disso, como λ é um caracter linear, temos $det \lambda = \lambda$ e, portanto, tomando $\chi = \lambda$, $G = H$ e $H = H_g$ no Lema 5.7 (iv), obtemos

$$\lambda^{-|G:H_g|}(x) = (\lambda^{|G:H_g|})^{-1}(x) = (T_{H_g}^H(\lambda|_{H_g}))^{-1}(x),$$

para todo $g \in R$. Portanto,

$$\prod_{g \in R} (T_{H_g}^H(\lambda|_{H_g}))^{-1}(x) = \prod_{g \in R} \lambda^{-|G:H_g|}(x) = \lambda^{-\sum_{g \in R} |G:H_g|}(x) = \lambda^{-|G:H|}(x). \quad (5.7)$$

Logo, de (5.5), (5.6) e (5.7) obtemos

$$\begin{aligned}
1 &\neq \prod_{g \in R} (T_{H_g}^H(\lambda|_{H_g}))^{-1}(x) \cdot \prod_{g \in R} (T_{H_g}^H(\lambda^{g^{-1}}|_{H_g}))(x) \\
&= \prod_{g \in R} (T_{H_g}^H(\lambda|_{H_g}))^{-1}(x) (T_{H_g}^H(\lambda^{g^{-1}}|_{H_g}))(x) \\
&= \prod_{g \in R} T_{H_g}^H(\lambda_g)(x).
\end{aligned}$$

Assim, existe $g \in G$ tal que $T_{H_g}^H(\lambda_g)(x) \neq 1$. Visto que λ tem ordem p , $\lambda^{-1}|_{H_g}$ e $\lambda^{g^{-1}}|_{H_g}$ também possuem ordem p . Como o produto de caracteres é comutativo, segue que λ_g tem ordem p . Além disso, $g \notin H$, pois caso contrário, teríamos $H_g = H$, de modo que para todo $h \in H = H_g$, $ghg^{-1} \in H$ e de λ ser homomorfismo obteríamos $\lambda_g(h) = \lambda^{-1}(h)\lambda^{g^{-1}}(h) = \lambda^{-1}(h)\lambda(ghg^{-1}) = 1$, de onde viria que $T_{H_g}^H(\lambda_g)(x) = 1$, contradição. Portanto, para mostrarmos que (H_g, λ_g, x) é uma p -singularidade em H , resta provarmos que $\langle x^p \rangle^H \cap H_g \subseteq \text{Ker} \lambda_g$. Por hipótese, $\langle x^p \rangle^G \cap H \subseteq \text{Ker} \lambda$, de onde temos $\langle x^p \rangle^H \cap H \subseteq \text{Ker} \lambda$ e $\langle x^p \rangle^H \cap H^g \subseteq (\text{Ker} \lambda)^g$. Mais ainda, se $y \in \text{Ker} \lambda \cap (\text{Ker} \lambda)^g$, então $y \in \text{Ker} \lambda$ e $y = g^{-1}hg$ para algum $h \in \text{Ker} \lambda$, e daí obtemos que $\lambda_g(y) = \lambda^{-1}(y)\lambda^{g^{-1}}(y) = (\lambda(y))^{-1} \lambda(h) = 1$, ou seja, $y \in \text{Ker} \lambda_g$. Logo, $\langle x^p \rangle^H \cap H_g \subseteq \text{Ker} \lambda \cap (\text{Ker} \lambda)^g \subseteq \text{Ker} \lambda_g$.

Antes de demonstrarmos a segunda afirmação do ítem (ii), observamos que $P \cap H_g^h = P \cap (H \cap H^g)^h = P \cap H \cap H^{gh} = P \cap H^{gh}$ e $\lambda_g^{h^{-1}}|_{P \cap H_g^h} = \lambda'_{gh}$. Visto que (H_g, λ_g, x) é uma p -singularidade em H e $x \in P \leq H$, obtemos do Lema 5.15 (v) que existe $h \in H$ tal que $(P_{gh}, \lambda'_{gh}, x) = (P \cap H_g^h, \lambda_g^{h^{-1}}|_{P \cap H_g^h}, x)$ é uma p -singularidade em P . Se necessário, substituímos g por gh^{-1} e temos, portanto, que (P_g, λ'_g, x) é uma p -singularidade em P . \square

Observação 5.26 *Sejam $H \leq G$ e P um S_p -subgrupo de H . Se $x \in P^G \cap H$, então $x = y^g \in H$, para algum $y \in P$ e $g \in G$. Como $\circ(x) = \circ(y^g) = \circ(y)$, temos que x é um p -elemento de H e, portanto, $x \in Q$, onde Q é um S_p -subgrupo de H . Pelo Teorema de Sylow, existe $h \in H$ tal que $Q = P^h$ e, então $x \in P^H$. Assim, $P^G \cap H \subseteq P^H$. Uma vez que a inclusão contrária é óbvia, temos $P^G \cap H = P^H$.*

Agora, consideremos o caso particular em que $H = N_G(P)$, $\lambda \in \hat{H}$ e tomemos $x \in P \setminus \text{Ker} \lambda$ um elemento de ordem minimal. Iremos mostrar que $\langle x^p \rangle^G \cap H \subseteq \text{Ker} \lambda$.

Com efeito, seja $((x^p)^k)^g \in \langle x^p \rangle^G \cap H$, onde $k \in \mathbb{Z}$ e $g \in G$. Então, $((x^p)^k)^g \in P^g \cap H \subseteq P^G \cap H \subseteq P^H$. Assim sendo, existem $y \in P$ e $h \in H$ tais que $((x^p)^k)^g = y^h$. Mas como $H = N_G(P)$, segue que $((x^p)^k)^g \in P$. Logo, devemos ter $((x^p)^k)^g \in \text{Ker}\lambda$, pois caso contrário $((x^p)^k)^g$ seria um elemento em $P \setminus \text{Ker}\lambda$ com ordem menor que $\circ(x)$, o que contraria a escolha de x .

Finalmente temos o resultado desejado.

Teorema 5.27 (T.Yoshida) *Se P é um S_p -subgrupo de um grupo G que não possui grupo quociente isomorfo a $\mathbb{Z}_p \wr \mathbb{Z}_p$, então $P \cap G' = P \cap N_G(P)'$*

Demonstração: Suponhamos que $P \cap N_G(P)' < P \cap G'$ e seja $H = N_G(P)$. Como P é um S_p -subgrupo de G e $P \subseteq H$, $|G : H|$ é relativamente primo com p . Assim, pelo Lema 5.25 (i), existe $\lambda \in \hat{H}$ tal que $\circ(\lambda) = p$ e $T_H^G(\lambda) = 1$. Seja $x \in P \setminus \text{Ker}\lambda$ de ordem minimal. Então pela Observação 5.26, $\langle x^p \rangle^G \cap H \subseteq \text{Ker}\lambda$. Assim, pelo Lema 5.25 (ii), existe $g \in G \setminus H$ tal que $P \cap H^g$ é um subgrupo singular de P com elemento singular x . Agora, $P \cap H^g < P$. De fato, se $P \cap H^g = P$, então $P \subseteq H^g$, o que implica $P^{g^{-1}} \subseteq H$. Visto que $|P^{g^{-1}}| = |P|$ e P é um S_p -subgrupo de H , segue que $P^{g^{-1}}$ é um S_p -subgrupo de H e, portanto, existe $h \in H$ tal que $P^{g^{-1}} = P^h$. Assim, $P^{hg} = P$ e, conseqüentemente, $hg \in N_G(P) = H$. Uma vez que $h \in H$, temos $g \in H$, contradição. Logo P possui um subgrupo singular próprio e, então, pelo Lema 5.24, P possui um subgrupo quociente isomorfo a $\mathbb{Z}_p \wr \mathbb{Z}_p$, e o teorema está provado. \square

Capítulo 6

O Critério de Solubilidade de Wang

Como vimos no final do Capítulo 3, o Teorema de Thompson (4.21) afirma que se um grupo finito G possui um subgrupo maximal nilpotente de ordem ímpar, então G é solúvel. Janko generalizou este resultado substituindo a hipótese “subgrupo maximal nilpotente de ordem ímpar” por “subgrupo maximal nilpotente possuindo um S_2 -subgrupo de classe de nilpotência no máximo 2”. Em 1998, Y. Wang publicou um artigo no qual ele generaliza o Teorema de Thompson e de Janko. Nós apresentamos este resultado de Wang através do Teorema 6.2, que nos diz o seguinte:

Sejam G um grupo finito e A um grupo agindo sobre G por automorfismos. Suponhamos que A é $\pi(G)$ -solúvel. Se existe um subgrupo A -invariante maximal M de G tal que M é nilpotente e o S_2 -subgrupo de M não possui grupo quociente isomorfo a D_8 , então G é solúvel.

6.1 Teorema de Wang

Nesta seção, todos os grupos serão finitos. Em geral, se A for um grupo que age sobre um grupo G , denotamos por letras gregas os elementos de A e seus subconjuntos e utilizamos letras latinas para denotar os elementos de G e seu subconjuntos. Dizemos que a ação de A sobre G é *irredutível* se 1 e G são os únicos subgrupos

A -invariantes de G .

Seja G um grupo. Quando um grupo $\pi(G)$ -solúvel A age sobre G por automorfismos e a ação é irredutível, é possível concluir algo sobre a estrutura de G , como veremos no próximo resultado. Além de seu belíssimo teor matemático, este resultado desempenha um papel crucial na demonstração do Teorema de Wang, como veremos adiante.

Lema 6.1 *Sejam G um grupo finito e A um grupo agindo sobre G por automorfismos. Suponhamos que A é $\pi(G)$ -solúvel. Se A age irredutivelmente sobre G , então G é um p -grupo abeliano elementar.*

Demonstração: Se $A = 1$, então todos os subgrupos de G são A -invariantes. Por outro lado os únicos subgrupos de G A -invariantes são 1 e G , pois A age irredutivelmente sobre G . Portanto, os únicos subgrupos de G são 1 e G , de modo que $|G| = p$, para algum primo p e o lema segue. Seja K o kernel da ação de A sobre G i.é., $K = \{\alpha \in A; g^\alpha = g, \forall g \in G\}$. Claramente $K \triangleleft A$. A ação de A sobre G induz naturalmente uma ação de A/K sobre G e, certamente, A age irredutivelmente sobre G se, e somente se, $\frac{A}{K}$ age irredutivelmente sobre G . Assim, podemos supor que A age fielmente sobre G , ou seja, $K = 1$. Consideremos $A \neq 1$ e seja L um subgrupo normal minimal de A . O subgrupo $C_G(L) = \{g \in G : g^\gamma = g, \forall \gamma \in L\}$ de G é A -invariante. Visto que A age irredutivelmente sobre G , $C_G(L) = 1$ ou $C_G(L) = G$. Se $C_G(L) = G$, então todos os elementos de G são fixados pelos elementos de L . Como A age fielmente sobre G , temos $L = 1$, contradizendo a definição de L ser normal minimal. Portanto, $C_G(L) = 1$.

Afirmção: $(|G|, |L|) = 1$.

Com efeito, como L é um subgrupo normal minimal de A , existe uma série de composição de A contendo L e L sendo o primeiro subgrupo não trivial contendo 1 . Logo, $L \cong \frac{L}{1}$ é um p -grupo para algum $p \in \pi(G)$ ou um $\pi(G)'$ -grupo, pois A é $\pi(G)$ -solúvel. Suponhamos que L seja um p -grupo com $p \in \pi(G)$. Sabemos que para todo $g \in G$, a L -órbita de g é o conjunto $\mathcal{O}(g) = \{g^\gamma : \gamma \in L\}$ e $|\mathcal{O}(g)|$ divide $|L|$, i.é., $|\mathcal{O}(g)|$ é uma potência de p . Além disso, as L -órbitas de G formam uma partição de G e se $g \in C_G(L)$, então $\mathcal{O}(g) = \{g\}$. Deste modo, se $R = \{g_1, g_2, \dots, g_r\}$ é um subconjunto de G tal que $G = \bigcup_{i=1}^r \mathcal{O}(g_i)$ (união disjunta), então

$$|G| = \sum_{g \in R} |\mathcal{O}(g)| = |C_G(L)| + \sum_{g \in R \setminus C_G(L)} |\mathcal{O}(g)| = 1 + kp \equiv 1 \pmod{p}$$

e, assim, $(|G|, p) = 1$, contradição. Portanto, L é um $\pi(G)'$ -subgrupo e $(|G|, |L|) = 1$, como queríamos.

Assim, L pode ser visto como um $\pi(G)'$ -grupo de automorfismos de G e, então, pelo Teorema 2.6 item (i), para todo primo $p \in \pi(G)$ existe um S_p -subgrupo P de G que é L -invariante. O mesmo teorema, item (ii), fornece que P é o único S_p -subgrupo com esta propriedade, visto que $C_G(L) = 1$. Uma vez que $L \triangleleft A$, temos $(P^\alpha)^L = (P^L)^\alpha = P^\alpha$, para todo $\alpha \in A$. A unicidade de P mostra que $P^\alpha = P$ e, assim, P é A -invariante. Pela irreduzibilidade da ação de A sobre G temos $P = G$. Além disso, como $\Phi(P) \text{ char } P$, temos que $\Phi(P)$ é A -invariante e, daí a irreduzibilidade da ação de A nos dá que $\Phi(P) = 1$, uma vez que $\Phi(P) < P$. Portanto, $G \cong \frac{P}{\Phi(P)}$ é um p -grupo abeliano elementar. \square

Se um grupo M possui apenas um S_2 -subgrupo, ele será denotado por M_2 .

O lema anterior juntamente com os Teoremas 4.19 e 5.27 nos serão extremamente úteis para obtermos a generalização dos Teorema de Thompson e Jancko mencionada na introdução deste capítulo.

Teorema 6.2 (Wang) *Sejam G um grupo e A um grupo agindo sobre G por automorfismos. Suponhamos que A é $\pi(G)$ -solúvel. Se existe um subgrupo A -invariante maximal M de G tal que M é nilpotente e M_2 não possui grupo quociente isomorfo a D_8 , então G é solúvel.*

Demonstração: Suponhamos que o resultado seja falso e seja G um contra exemplo de ordem minimal. Assim, todo grupo que está nas hipóteses do teorema e tem ordem menor que $|G|$ é solúvel. Então:

(1) M não contém subgrupos normais A -invariantes não triviais de G .

De fato, suponhamos que exista um subgrupo normal não trivial N de G A -invariante contido em M . O grupo A age sobre G/N da seguinte forma: se $\alpha \in A$ e $Ng \in G/N = \bar{G}$, então $(Ng)^\alpha = N(g^\alpha)$. Disso e da hipótese sobre M , obtemos que M/N é um subgrupo A -invariante maximal nilpotente de \bar{G} . Além disso, $(M/N)_2$ não tem grupo quociente isomorfo a D_8 , pois M_2 não possui. Assim \bar{G} satisfaz as hipóteses do teorema e $|\bar{G}| < |G|$.

Logo, \bar{G} é solúvel. Como $N \leq M$ segue que N é nilpotente e, portanto, solúvel. Pela Proposição 1.10 (ii), G é solúvel, contradição.

(2) M é um subgrupo de Hall de G .

De fato, sejam $p \in \pi(M)$ e P um S_p -subgrupo de M . Pela Proposição 1.13 (vi), $P \triangleleft M$ e, assim, P é o único S_p -subgrupo de M . Visto que M é A -invariante e que A age sobre G como um grupo de automorfismos, temos $P^\alpha \subseteq M$ e $|P^\alpha| = |P|$, para todo $\alpha \in A$. Logo, P^α é um S_p -subgrupo de M e, então, $P^\alpha = P$, para todo $\alpha \in A$. Agora, tome $g \in N_G(P)$, $\alpha \in A$ e $y \in P$. Uma vez que A age sobre G por automorfismos e P é A -invariante, temos $y = x^\alpha$ para algum $x \in P$. Assim, $y^{g^\alpha} = (g^{-1}xg)^\alpha \in P$. Portanto, P e $N_G(P)$ são ambos subgrupos A -invariantes de G . De $P \triangleleft M$, segue que $M \leq N_G(P)$. Se $M < N_G(P)$, então existe um subgrupo A -invariante de G contendo propriamente M . Pela maximilidade de M devemos ter $G = N_G(P)$, o que implica $P \triangleleft G$, contradizendo (1). Logo, $M = N_G(P)$. Como P está contido em algum S_p -subgrupo S de G , temos $N_S(P) = S \cap N_G(P) = S \cap M = P$, pois $S \cap M$ é um p -subgrupo de M que contém P . Agora, a contrapositiva da Proposição 1.4 (i), implica $P = S$, ou seja, P é um S_p -subgrupo de G . Logo, $|G : M|$ é relativamente primo com p . Como isso vale para todo $p \in \pi(M)$, concluímos que M é um $\pi(M)$ -subgrupo de Hall de G , provando (2).

(3) G é p -nilpotente, para todo $p \in \pi(M)$.

Sejam $p \in \pi(M)$ e P um S_p -subgrupo de M . Visto que $J(P)$ é um p -grupo, $Z(J(P)) \neq 1$. Além disso, $Z(J(P)) \text{ char } J(P) \text{ char } P$ e P é A -invariante, pelo parágrafo anterior, de modo que $Z(J(P))$ é A -invariante. Mais ainda, visto que A age sobre $Z(J(P))$ como um grupo de automorfismos, é fácil mostrar, como no parágrafo anterior, que $N_G(Z(J(P)))$ também é A -invariante. Como $Z(J(P)) \leq M$, temos de (1) que $N_G(Z(J(P))) < G$. De $Z(J(P)) \text{ char } P$ resulta que $N_G(P) \leq N_G(Z(J(P)))$ e, assim, $M \leq N_G(P) \leq N_G(Z(J(P))) < G$. Portanto, $N_G(Z(J(P)))$ é um subgrupo A -invariante próprio de G , contendo M . Pela maximilidade de M , obtémos $M = N_G(Z(J(P)))$ e, assim, $N_G(Z(J(P)))$ é p -nilpotente, para todo $p \in \pi(M)$. Se p é ímpar, então o Teorema de Glauberman Thompson (4.19) implica que G é p -nilpotente. Se $p = 2$, então de (2) segue que P é um S_2 -subgrupo de G e $N_G(P) = M$, de modo que $N_G(P)$ é 2-nilpotente. Por outro lado, $Z_2 \wr Z_2 \cong D_8$. Uma vez que $P = M_2$, a hipótese sobre M_2 garante

que P não possui grupo quociente isomorfo a $Z_2 \wr Z_2$. Daí, pelo Teorema 5.27 temos $P \cap G' = P \cap N_G(P)' = P \cap M'$. Isto implica que G é 2-nilpotente.

Por (3), $G = O_{p'}(G)P$ para todo $p \in \pi(M)$, onde P é um S_p -subgrupo de G . Assim como na demonstração do Teorema de Thompson (4.21), temos que se $K = \bigcap_{p \in \pi(M)} O_{p'}(G)$ então $K \triangleleft G$ e $G = KM$, com $K \cap M = 1$. Mais ainda, como $O_{p'}(G) \text{ char } G$, para todo $p \in \pi(M)$, segue que $K \text{ char } G$. Por outro lado, visto que A age sobre G por automorfismos, e M é A -invariante, podemos formar o produto semi-direto $A \rtimes M = \{(\alpha, m) : \alpha \in A, m \in M\}$. Claramente $A \rtimes M$ age sobre G por automorfismos pela ação $g^{(m, \alpha)} = m^{-1}g^\alpha m$, para todo $(\alpha, m) \in A \rtimes M$ e todo $g \in G$. Além disso, de $K \text{ char } G$, segue que K é $(A \rtimes M)$ -invariante. Vamos mostrar que $A \rtimes M$ age irreduzivelmente sobre K . De fato, suponhamos que exista $1 \neq K_1 < K$ tal que K_1 é $(A \rtimes M)$ -invariante. Logo, M normaliza K_1 e, assim, K_1M é um subgrupo de G . Além disso, K_1 é A -invariante e, como M também é A -invariante, K_1M é um subgrupo A -invariante de G , com $M < K_1M < KM = G$, contradizendo a escolha de M . Como M é nilpotente temos que M é solúvel e, conseqüentemente, M é p -solúvel para todo primo p e, assim, M é $\pi(G)$ -solúvel. Visto que A é $\pi(G)$ -solúvel, por hipótese, temos que $A \rtimes M$ é $\pi(G)$ -solúvel. Pelo Lema 6.1, K é um grupo abeliano elementar e, portanto, K é solúvel. Como $\frac{G}{K} \cong M$ é solúvel, segue da Proposição 1.10 (ii) que G é solúvel, contradizendo nossa escolha de G . \square

No exemplo a seguir vamos exibir um grupo solúvel que não possui subgrupo maximal nilpotente, mas tem um subgrupo A -invariante maximal nilpotente, para um grupo conveniente A . Isso mostra que o Teorema 6.2 não é uma generalização trivial do Teorema de Thompson.

Exemplo 6.3 Denotemos por C_p um grupo cíclico de ordem p . Consideremos os produtos diretos $C_{11} \times C_{11} = \langle a, b \mid a^{11} = b^{11} = [a, b] = 1 \rangle$ e $C_5 \times C_5 = \langle c, d \mid c^5 = d^5 = [c, d] = 1 \rangle$. Definindo

$$\begin{array}{ll}
\phi_c : \{a, b\} \longrightarrow C_{11} \times C_{11} & \phi_d : \{a, b\} \longrightarrow C_{11} \times C_{11} \\
a \longmapsto a^c = a^4 & a \longmapsto a^d = a^5 \\
b \longmapsto b^c = b^5 & b \longmapsto b^d = b^4
\end{array}$$

é fácil ver que ϕ_c e ϕ_d são consistentes com as relações definidoras de $C_{11} \times C_{11}$. Logo, pelo Teste da Substituição, ϕ_c se estende a um homomorfismo $\phi_c'' : C_{11} \times C_{11} \longrightarrow C_{11} \times C_{11}$ e ϕ_d se estende a um homomorfismo $\phi_d'' : C_{11} \times C_{11} \longrightarrow C_{11} \times C_{11}$.

Vamos mostrar que ϕ_c'' e ϕ_d'' são automorfismos de $C_{11} \times C_{11}$. Para tanto, basta mostrarmos que ϕ_c'' e ϕ_d'' são epimorfismos, já que $C_{11} \times C_{11}$ é finito. Mas isto segue do fato que $\langle a^4 \rangle = \langle a \rangle = \langle a^5 \rangle$ e $\langle b^5 \rangle = \langle b \rangle = \langle b^4 \rangle$.

Consideremos a seguinte aplicação:

$$\begin{array}{ll}
\phi : \{c, d\} \longrightarrow \text{Aut}(C_{11} \times C_{11}) & . \\
c \longmapsto \phi_c'' & \\
d \longmapsto \phi_d'' &
\end{array}$$

É fácil ver que ϕ se estende a um homomorfismo $\phi'' : C_5 \times C_5 \longrightarrow \text{Aut}(C_{11} \times C_{11})$. Logo, podemos formar o produto semi-direto $G = (C_5 \times C_5) \ltimes (C_{11} \times C_{11})$ de $C_{11} \times C_{11}$ por $C_5 \times C_5$. Visto que $C_{11} \times C_{11}$ e $\frac{G}{C_{11} \times C_{11}} \cong C_5 \times C_5$ são solúveis por serem p -grupos, segue que G é solúvel.

Tomemos agora a função $\alpha : \{a, b, c, d\} \longrightarrow G$ definida por $\alpha(a) = b$, $\alpha(b) = a$, $\alpha(c) = d$ e $\alpha(d) = c$. É claro que α é consistente com todas as relações definidoras de G , de modo que, pelo Teste da Substituição, α se estende a um endomorfismo α' de G . Mais ainda, pelo modo como α está definida, é fácil ver que α' é bijetora e, assim, α' é um automorfismo de G . Além disso, certamente α' tem ordem 2. Portanto, $A = \langle \alpha' \rangle$ age por automorfismos sobre G .

(1) G não possui subgrupo maximal nilpotente de G .

De fato, seja M um subgrupo maximal de G . Não é difícil verificar que $|G : M| = 5$ ou 11. Suponhamos que $|G : M| = 5$. Então $|M| = 11^2 \cdot 5$, de modo que $M = \langle m \rangle (\langle a \rangle \times \langle b \rangle)$, onde m é um elemento de ordem 5 em M . Assim, $\langle m \rangle$ é um S_5 -subgrupo de M . Se M é nilpotente, então, pelo Teorema 1.13, $\langle m \rangle \triangleleft M$. Consequentemente, $m^a = m = m^b$. Podemos supor, sem perda de generalidade, que $m = c^i d^j$. Agora, note que $a^{c^i} = a^{4^i}$,

$a^{d^j} = a^{5^j}$, $b^{c^i} = b^{5^i}$ e $b^{d^i} = b^{4^i}$. Disso e de $m^a = m = m^b$, obtemos $a = a^m = a^{4^i 5^j}$ e $b = b^m = b^{5^i 4^j}$, i.é, $4^i 5^j \equiv 1(\text{mod } 11)$ e $5^i 4^j \equiv 1(\text{mod } 11)$. Visto que $5 \equiv 4^2(\text{mod } 11)$, obtemos $4^{i+2j} \equiv 1(\text{mod } 11)$ e $4^{2i+j} \equiv 1(\text{mod } 11)$. Disso e de $4^5 \equiv 1(\text{mod } 11)$, temos $i + 2j \equiv 0(\text{mod } 5)$ e $2i + j \equiv 0(\text{mod } 5)$. Assim, $5|(i + j)$ e $5|(i - j)$. Logo, $5|i$ e $5|j$, de onde temos que $m = 1$, uma contradição. Portanto, M não é nilpotente.

Suponhamos $|G : M| = 11$. Então, $|M| = 5^2 \cdot 11$ e, como $M \leq G$, podemos assumir, sem perda de generalidade, que M contém $\langle c \rangle \times \langle d \rangle$ e M possui um elemento $m = a^i b^j$ de ordem 11. De $[a, b] = 1$, obtemos $b^j = b^{5j} b^{-4j} = a^{4i} b^{5j} a^{-4i} b^{-4j} = m^c m^{-4} \in M$. Se $b^j \neq 1$, então j é relativamente primo com $11 = |b|$, de onde obtemos que $M = (\langle c \rangle \times \langle d \rangle) \rtimes \langle b \rangle$. Se $b^j = 1$, então $a^i \neq 1$ e, uma argumentação análoga a anterior mostra-se que $M = (\langle c \rangle \times \langle d \rangle) \rtimes \langle a \rangle$. Porém, nenhum destes é nilpotente.

(2) $\langle c \rangle \times \langle d \rangle$ é um subgrupo $\langle \alpha' \rangle$ -invariante maximal nilpotente.

Claramente, $\langle c \rangle \times \langle d \rangle$ é um subgrupo $\langle \alpha' \rangle$ -invariante e nilpotente. Mais ainda, se existir um subgrupo M de G tal que $\langle c \rangle \times \langle d \rangle < M < G$, então, como foi provado anteriormente, $M = (\langle c \rangle \times \langle d \rangle) \rtimes \langle a \rangle$ ou $M = (\langle c \rangle \times \langle d \rangle) \rtimes \langle b \rangle$. Certamente, nenhum destes é $\langle \alpha' \rangle$ -invariante, pois $\alpha'(a) = b$ e $\alpha'(b) = a$

Bibliografia

- [1] GONÇALVES, A., *Tópicos em representação de grupos*. 9º Colóquio Brasileiro de Matemática, Poços de Caldas, 1973.
- [2] GORENSTEIN, D., *Finite Groups*. New York: Chelsea n Publishing Company, 2.ed., 1980.
- [3] ISAACS, I.M., *Character Theory of Finite Groups*. New York: Academic Press, 1976.
- [4] JOHNSON, D.L., *Topics in the Theory of Group Presentations*. London Mathematical Society Lecture Note Series, Great Britain, 1980.
- [5] ROBINSON, D. J. S., *A Course in the Theory of Groups*. New York: Springer-Verlag, 1993.
- [6] ROTMAM, J. J., *An Introduction to the Theory of Groups*. New York: Springer-Verlag, 4.ed., 1994.
- [7] SANTOS, J.N.T.N dos, *Grupos Finitos Admitindo Automorfismos Livres de Ponto fixo*. Dissertação de Mestrado, UEM, 2005.
- [8] THOMPSON, J.G., *Normal p -Complements and Irreducible Character*. Journal of Algebra 14 (1970), 129-134.
- [9] YOSHIDA, Y., *Character-Theoretic Transfer*. Journal of Algebra 52 (1978), 1-38.
- [10] WANG, Y., *Finite Groups Admitting a p -Solvable Operator Group*. Journal of Algebra 204, (1998), 42-48.

Índice

- A -invariante, 16
- G -módulo, 17
- G -módulo fiel, 17
- G -módulo irredutível, 17
- G -submódulo, 17
- π -grupo, 20
- π -número, 20
- π -subgrupo de Hall, 20
- π' -grupo, 20
- π' -número, 20
- $\pi\pi'$ -série, 29
 - superior, 29
- p -elemento, 5
- p -grupo abeliano elementar, 5
- p -nilpotente, 66
- p -singularidade, 85
- \det , 77
- ação por automorfismos, 12
- anel caracter, 75
- anulador, 83
- apresentação livre, 11
- Argumento de Frattini, 5
- caracter, 73
 - generalizado, 75
 - linear, 75
 - principal, 73
- caracter induzido, 76
- caracter singular, 85
- caracteristicamente simples, 30
- centralizador, 5
- classe de nilpotência, 9
- complemento, 26
- complemento de Frobenius, 15
- comutador, 3
- conjugado, 5
- elemento singular, 85
- estabilizador, 14
- fator de composição, 7
- fator principal, 30
- finitamente apresentado, 11
- fortemente p -solúvel, 48
- geradores, 11
- grau, 17
- grau da representação, 16
- grupo
 - π -separável, 28
 - π -solúvel, 33
 - p -estável, 37

- de Frobenius, 15
- de permutações transitivo, 13
- está envolvido, 44
- linear especial, 18
- linear geral, 18
- linear projetivo, 18
- linear projetivo especial, 18
- livre, 10
- nilpotente, 9
- solúvel, 7
- grupos fatores, 7
- kernel de Frobenius, 15
- letras, 14
- normalizador, 5
- posto, 10
- produto entrelaçado, 88
- produto semi-direto, 12
- produto tensorial, 74
- refinamento, 7
- relações definidoras, 11
- relatores, 11
- representação, 15
 - p -estável, 37
 - fiel, 16
 - induzida, 76
 - irredutível, 16
 - matricial, 17
 - permutacional, 14
 - permutacional transitiva, 14
 - permutacionasl transitiva, 14
 - regular à esquerda, 14
 - trivial, 15
- série
 - central
 - inferior, 8
 - de composição, 7
 - derivada, 8
 - normal, 7
 - principal, 30
- séries equivalentes, 7
- singularidade, 85
- soma direta de matrizes, 74
- soma direta de representações, 74
- subgrupo
 - A -invariante, 12
 - base, 88
 - característico, 6
 - comutador, 3
 - de Frattini, 10
 - de Thompson, 54
 - derivado, 3
 - focal, 72
 - maximal, 9
 - normal maximal, 7
 - subnormal, 21
 - normal minimal, 7
 - singular, 85
- subgrupos comutadores superiores, 8

Teorema

da Substituição de Glauberman, 60

da Substituição de Thompson, 57

de Frobenius, 67

de Glauberman, 63, 66

de Glauberman-Thompson, 67

de P.Hall, Cunihin, 31

de Tate-Thompson, 84

de Thompson, 56, 70

da Decomposição de Mackey, 82

de Mackey, 80

de Schur-Zassenhaus, 22

transfer de caracter, 78

transversal à direita, 75

Livros Grátis

(<http://www.livrosgratis.com.br>)

Milhares de Livros para Download:

[Baixar livros de Administração](#)

[Baixar livros de Agronomia](#)

[Baixar livros de Arquitetura](#)

[Baixar livros de Artes](#)

[Baixar livros de Astronomia](#)

[Baixar livros de Biologia Geral](#)

[Baixar livros de Ciência da Computação](#)

[Baixar livros de Ciência da Informação](#)

[Baixar livros de Ciência Política](#)

[Baixar livros de Ciências da Saúde](#)

[Baixar livros de Comunicação](#)

[Baixar livros do Conselho Nacional de Educação - CNE](#)

[Baixar livros de Defesa civil](#)

[Baixar livros de Direito](#)

[Baixar livros de Direitos humanos](#)

[Baixar livros de Economia](#)

[Baixar livros de Economia Doméstica](#)

[Baixar livros de Educação](#)

[Baixar livros de Educação - Trânsito](#)

[Baixar livros de Educação Física](#)

[Baixar livros de Engenharia Aeroespacial](#)

[Baixar livros de Farmácia](#)

[Baixar livros de Filosofia](#)

[Baixar livros de Física](#)

[Baixar livros de Geociências](#)

[Baixar livros de Geografia](#)

[Baixar livros de História](#)

[Baixar livros de Línguas](#)

[Baixar livros de Literatura](#)
[Baixar livros de Literatura de Cordel](#)
[Baixar livros de Literatura Infantil](#)
[Baixar livros de Matemática](#)
[Baixar livros de Medicina](#)
[Baixar livros de Medicina Veterinária](#)
[Baixar livros de Meio Ambiente](#)
[Baixar livros de Meteorologia](#)
[Baixar Monografias e TCC](#)
[Baixar livros Multidisciplinar](#)
[Baixar livros de Música](#)
[Baixar livros de Psicologia](#)
[Baixar livros de Química](#)
[Baixar livros de Saúde Coletiva](#)
[Baixar livros de Serviço Social](#)
[Baixar livros de Sociologia](#)
[Baixar livros de Teologia](#)
[Baixar livros de Trabalho](#)
[Baixar livros de Turismo](#)