Universidade Federal de Goiás
Instituto de Matemática e Estatística

Yerko Contreras Rojas

Sobre a Influência dos Centralizadores dos Automorfismos de Ordem Dois em Grupos de Ordem Ímpar

Goiânia
2013

sistema de bibliotecas ufg

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[x] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação

Autor (a):	Yerko Contreras Rojas					
E-mail:	zaxeco@hotmail.com					
Seu e-mail pode ser disponibilizado na página? [x]Sim [ ] Não						
Vínculo empregatício do autor						
Agência de fomento:		Coordenação de Aperfeiçoamento de Pessoal de Nível Superior		Sigla:	CAPES	
País:	Brasil	UF:	GO	CNPJ:	00889834/0001-08	
Título:	Sobre a Influência dos Centralizadores dos Automorfismos de Ordem Dois em Grupos de Ordem Ímpar					
Palavras-chave:	Grupos finitos, Grupos nilpotentes, Centralizadores de automorfimos, Automorfismos involutivos.					
Título em outra língua:	Centralizers of involutory automorphisms of groups of odd order					
Palavras-chave em outra língua:	Finite groups, nilpotent groups, centralizer of automorphisms, involutory automorphisms.					
Área de concentração:	Álgebra					
Data defesa: (dd/mm/aaaa)	05/07/2013					
Programa de Pós-Graduação:	Matématicas					
Orientador (a):	Aline de Souza Lima					
E-mail:	alinelima@mat.ufg.br					

*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

_____________________________________ Data: ____ / ____ / _____

Assinatura do (a) autor (a)

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Yerko Contreras Rojas

Sobre a Influência dos Centralizadores dos Automorfismos de Ordem Dois em Grupos de Ordem Ímpar

Dissertação apresentada ao Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de concentração: Álgebra.

Orientador: Prof. Aline de Souza Lima

Goiânia
2013

Dados Internacionais de Catalogação na Publicação na (CIP)
GPT/BC/UFG

C764s

Contreras Rojas, Yerko.

Sobre a influência dos centralizadores de automorfismos de Ordem dois em grupos de ordem ímpar [manuscrito] / Yerko Contreras Rojas. - 2013.

xv, 59 f. : il., tabs.

Orientadora: Profª. Drª. Aline de Souza Lima.

Dissertação (Mestrado) – Universidade Federal de Goiás, Instituto de Matemática e Estatística, 2013.

Bibliografia.

1. Automorfismo - Grupos finitos. 2. Teoria dos grupos. 3. Automorfismo – Centralizadores. I. Título.

CDU: 512.542.2

YERKO CONTRERAS ROJAS

SOBRE A INFLUÊNCIA DOS CENTRALIZADORES DE AUTOMORFISMOS DE ORDEM DOIS EM GRUPOS DE ORDEM ÍMPAR

Dissertação defendida no Programa de Pós-Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás como requisito parcial para obtenção do título de Mestre em Matemática, aprovada no dia 05 de julho de 2013, pela Banca Examinadora constituída pelos professores:

Aline de Souza Lima

Profa. Dra. Aline de Souza Lima
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Pavel Zalesski

Prof. Dr. Pavel Zalesski
Departamento de Matemática-UnB

Ticianne P. Bueno

Profa. Dra. Ticianne Proença Bueno Adorno
Instituto de Matemática e Estatística-UFG

Yerko Contreras Rojas

Bacharel em Matemática pela Universidad Distrital Francisco José de Caldas, Bogotá, Colômbia.

Este trabalho foi orientado na parte gramatical e ortográfica pelo Daniel Pimenta.

a meus pais, Nubia Rojas e Carlos Contreras, e meus irmãos Paula e Andres.

"Deux mains c'est peu, peut-être, car le monde est infini."

Alexander Grothendieck,

.

Agradecimentos

A minha familia e amigos, por ter sido meu principal estimulo.

Finalmente, a todas aquelas pessoas que de alguma forma colaboraram e alentaram na finalização deste trabalho.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) pelo apoio finaceiro.

Resumo

Contreras Rojas, Yerko. **Sobre a Influência dos Centralizadores dos Automorfismos de Ordem Dois em Grupos de Ordem Ímpar** . Goiânia, 2013. 57p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

O trabalho baseia-se na apresentação e desenvolvimento de alguns resultados expostos por Shumyatsky em [14, 15, 16, 17, 18], onde trabalha com automorfismos de ordem dois em grupos de ordem ímpar, mostrando fundamentalmente a influência da estrutura do centralizador do automorfismo na estrutura do grupo. Seja G um grupo de ordem ímpar e ϕ um automorfismo de G, de ordem dois, tal que $G = [G, \phi]$, dada uma limitação na ordem do centralizador de ϕ em G, $C_G(\phi)$, a mesma induz uma limitação na ordem do grupo derivado G' do grupo G, além disso verificamos que G tem um subgrupo H normal ϕ-invariante, tal que $H' \leq G_\phi$ e o índice $[G : H]$ é limitado dependendo da limitação inicial de $C_G(\phi)$. Nas mesmas hipóteses do grupo G e com a mesma limitação da ordem do centralizador do automorfismo, seja V um p-grupo abeliano, tal que $G\langle\phi\rangle$ age fiel e irredutivelmente sobre V, então existe uma constante k, limitada por uma função que depende só da limitação de $C_G(\phi)$, e elementos $x_1, \ldots x_k \in G_{-\phi}$, tal que $V = \rho^{\phi}_{x_1,\ldots,x_k}(V_{-\phi})$.

Palavras–chave

Grupos finitos, Grupos nilpotentes, Centralizadores de automorfismos, Automorfismos involutivos.

Abstract

Contreras Rojas, Yerko. **Centralizers of involutory automorphisms of groups of odd order**. Goiânia, 2013. 57p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

This document presents an approach and development of some of the results of Shumyatsky in [14, 15, 16, 17, 18], where he worked with automorphisms of order two in finite groups of odd order, mainly showing the influence that the structure of the centralizer has on that of Group. Let G be a group with odd order, and ϕ an automorphism on G, of order two, where $G = [G, \phi]$, and given a limitation in the order of the centralizer of ϕ regard to G, $C_G(\phi)$, which induces a limitation in the order of derived group G' of group G, and we also verified that G has a normal subgroup H that is ϕ-invariant, such that $H' \leq G_\phi$ and its index $[G : H]$ is bounded with the initial limitation. With the same hypothesis of the group G and with the same limitation of the order of the centralizer of the automorphism, let V a abelian p-group such that $G\langle\phi\rangle$ act faithful and irreductible on V, then there is a bounded constant k, limitated by a function depending only on the parameter m, where m is tha limitation in the order of $C_G(\phi)$, and elements $x_1, \ldots x_k \in G_{-\phi}$ such that $V = \rho^{\phi}_{x_1,\ldots,x_k}(V_{-\phi})$.

Keywords

Finite groups, nilpotent groups, centralizer of automorphisms, involutory automorphisms.

Sumário

Introdução

O estudo da teoria de grupos é uma das áreas de destaque no desenvolvimento da álgebra moderna. Um dos principais objetivos dos trabalhos nessa área é dar uma caracterização de um determinado grupo ou a uma classe de grupos e daí apresentar uma nova variedade de grupos. Uma das técnicas para fazer tal caracterização é o estudo de centralizadores de automorfismos e sua influência na estrutura do grupo e é segundo esta linha de pensamento que desenvolvemos este trabalho.

No presente trabalho, G representa um grupo de ordem finita, dado que estudamos automorfismos de ordem 2 em grupos de ordem ímpar. Tais automorfismos recebem o nome de automorfismos involutivos, ou involuções.

Como o estudo baseia-se nas implicações que a estrutura do centralizador do automorfismo impõe à estrutura de G, começamos apresentando o conjunto, $C_G(\phi)$, também conhecido como subgrupo de pontos fixos, sendo o conjunto de elementos de um grupo, fixados pelo automorfismo ϕ. Quando o centralizador é o subgrupo trivial se diz que ϕ é livre de pontos fixos. Pode-se verificar que tal conjunto é um subgrupo de G, denotado por,

$$C_G(\phi) = G_\phi = \{g \in G | \phi(g) = g\}.$$

Apresentamos alguns dos resultados mais importantes da relação entre a estrutura do centralizador de um automorfismo $C_G(\phi)$ e a do grupo G.

Burnside mostrou em seu livro [2], que um grupo G admitindo um automorfismo de ordem 2, livre de pontos fixos é abeliano. Este é o primeiro resultado significativo de que temos registro sobre o fato da existência de automorfismos livres de pontos fixos implicar conclusões substanciais em relação ao grupo. Burnside analisou também o caso em que o automorfismo é de ordem 3, e provou que tal grupo é necessariamente nilpotente de classe no máximo 2.

Os resultados mais importantes que exemplificam tal relação são os Teoremas de Higman [8] e Thompson [19]. Higman mostrou que existe uma função $h(p)$, dependendo somente de p, tal que todo grupo nilpotente, admitindo um automorfismo livre de pontos fixos de ordem prima p, é nilpotente de classe no máximo $h(p)$. E Thompson, por sua vez, mostrou que todo grupo, admitindo um automorfismo ϕ de ordem prima, tal que $C_G(\phi) = 1$, é nilpotente. Esses dois resultados juntos formam o Teorema de Higman-Thompson, o qual diz que todo grupo finito admitindo um automorfismo livre de pontos fixos de ordem prima p é nilpotente de classe limitada por uma função que depende apenas de p.

Hartley e Meixner mostram em [7], que dado um grupo de ordem ímpar G com um automorfismo ϕ de ordem prima p, tal que $C_G(\phi)$ tem ordem menor ou igual a m, então G possui um subgrupo normal N nilpotente de classe de nilpotência p-limitada e tem índice $[G:N]$, limitado por uma função dependendo só de m e p. Assumindo este resultado para os automorfismos involutivos, os autores obtiveram em [6] que, se $C_G(\phi)$ tem ordem m, então G possui um subgrupo N nilpotente de classe de nilpotência no máximo dois e tem índice $[G:N]$, limitado por uma função dependendo só de m (m-limitada). Observe que se o grupo tem ordem ímpar, então é solúvel pelo famoso Teorema de W. Feit e L. G. Thompson [3].

Kovács e Wall mostram em [12] que se G tem ordem ímpar e $C_G(\phi)$ é abeliano, então G' é nilpotente. Já o caso em que $C_G(\phi)$ é nilpotente, foi tratado por Ward em [21], onde prova que nestas condições, G coincide com o terceiro termo da série superior de Fitting.

Asar em [1], usa o resultado obtido por Ward em [21], para provar que se $C_G(\phi)$ é nilpotente. Então $[G,\phi]'$ e $G/[G,\phi]$ também são, onde $[G,\phi]$ é o subgrupo de G, gerado pelos elementos da forma $x^{-1}x^{\phi}$, isto é,

$$[G,\phi] = \left\langle \{g^{-1}g^{\phi} | g \in G\} \right\rangle.$$

O subgrupo definido acima é sempre normal em G. Segue que, se $G = [G,\phi]$ e G_ϕ é nilpotente, então $G_\phi \leq F(G)$. Em [14] Shumyatsky apresentou outra prova do resultado de Asar. No mesmo artigo, [14], Shumyatsky deu um exemplo (devido a Hartley) do fato que, mesmo que $G = [G,\phi]$, o subgrupo $F(C_G(\phi))$ não está necessariamente contido em $F(G)$. Lembramos o importante Teorema de Thompson em [20], o qual afirma que dado um automorfismo ϕ de ordem prima, de um grupo finito G, tal que $(|G|,|\phi|) = 1$, então $F(C_G(\phi)) \leq F_4(G)$ e $F(C_G(\phi)) \leq F_3(G)$ no caso em que a ordem de G for ímpar.

Para concluir temos o resultado de Shumyatsky em [15] que mostra que se G tem sua série derivada de comprimento d, e $C_G(\phi)$ é abeliano, então $[G,\phi]'$ é nilpotente de classe no máximo 4^{d-2}.

O objetivo principal deste trabalho é apresentar as ferramentas necessárias para a compreensão de alguns resultados expostos por Shumyatsky em [18]:

Teorema A *Seja G um grupo de ordem ímpar e ϕ um automorfismo de ordem 2, tal que $G = [G, \phi]$ e o centralizador $C_G(\phi)$ tem ordem limitada $|C_G(\phi)| \leq m$ esta limitação induz uma limitação na ordem do grupo derivado G', isto é $|G'| \leq f(m)$, além disso verificamos que G tem um subgrupo H normal ϕ-invariante, tal que $H' \leq G_\phi$ e o índice $[G : H]$ é limitado por uma outra função dependendo de m.*

Teorema B *Seja G um grupo de ordem ímpar e ϕ um automorfismo de ordem 2, tal que $G = [G, \phi]$ e o centralizador $C_G(\phi)$ tem ordem limitada $|C_G(\phi)| \leq m$. Dado um grupo abeliano V, e $G\langle\phi\rangle$ agindo fiel e irredutivelmente sobre V, então existe uma constante k, limitada por uma função dependendo de m, $g(m)$, e elementos $x_1, \ldots x_k \in G_{-\phi}$, tal que $V = \rho^{\phi}_{x_1,\ldots,x_k}(V_{-\phi})$.*

Com o propósito de atingir o objetivo acima, desenvolvemos alguns dos pré-requisitos usados para apresentar tais demonstrações, para tanto dividimos a dissertação em capítulos.

No primeiro capítulo, apresentamos alguns resultados básicos de teoria de grupos, sobre commutadores, grupos solúveis, nilpotentes e p-grupos abelianos elementares, além de outros temas, como ação de grupos e representação de grupos, importantes para o bom entendimento deste trabalho.

No segundo capítulo mostramos as propriedades satisfeitas pelos centralizadores de automorfismo coprimos do grupo G, isto é, a ordem do automorfismo é coprima com a ordem do grupo. E apresentamos os primeiros resultados que falam da influência de tais centralizadores na estrutura de G.

Já no terceiro capítulo falamos dos automorfismos de ordem dois, as involuções, e apresentamos a demostração do Teorema A.

No quarto capítulo, falamos sobre a influência da ação fiel e irredutível em um p-grupo abeliano, e apresentamos a demostração do Teorema B.

CAPÍTULO 1

Resultados Preliminares

Nesse capítulo apresentamos alguns resultados concernentes à teoria de grupos. A maioria dos resultados expostos neste capítulo são bem conhecidos desta teoria, pelo qual muitas das suas provas são omitidas.

Na primeira seção, damos a definição de homomorfismo de grupo e as classes especiais de homomorfismo, dando ênfase aos automorfismos e alguns resultados importantes sobre os mesmos. Na segunda seção falamos do produto direto e do produto semidireto de grupos e na seção seguinte trabalhamos ações de grupos, tópico que é tradicionalmente utilizado na demonstração dos teoremas de Sylow, mas aqui será útil no entendimento da ação dos automorfismos no grupo. Na quarta seção, lembramos alguns resultados de comutadores para introduzir as definições e propriedades dos grupos solúveis e nilpotentes. Na última seção introduzimos dois tipos especiais de grupos, primeiramente os p-grupos e por último os p-grupos abelianos elementares.

1.1 Automorfismos de Grupos

Quando tratamos de automorfismos de ordem coprima, fazemos alusão aos automorfismos ϕ de G, tais que a ordem de ϕ é coprima com a ordem do grupo G, isto é, $(|G|,|\phi|) = 1$. Generalizado esta idéia temos que um subgrupo A de automorfismos de G se diz que é coprimo, se temos a propriedade acima para todo elemento de A, isto é $(|G|,|a|) = 1$, para todo $a \in A$.

Definição 1.1.1 *Um subgrupo H de um grupo G é um subgrupo característico, e denota-se como H Char G, se $H^{\phi} = H$ para todo automorfismo $\phi \in Aut(G)$.*

Proposição 1.1.2 *Dados H,K subgrupos do grupo G, tal que H Char G e $K \trianglelefteq H$, então $K \trianglelefteq G$*

A propocição acima encontra-se demonstrada em [13]

Definição 1.1.3 *Um subgrupo H de um grupo G é um subgrupo totalmente invariante, se $H^{\phi} = H$ para todo endomorfismo $\phi \in End(G)$.*

1.2 Ação de Grupos e Representações

Definição 1.2.1 *Um grupo permutador G agindo sobre o conjunto S se diz transitivo em S, se para qualquer dois $s,s' \in S$ existe $x \in G$, tal que $x(s) = s'$. Do mesmo modo, se diz que G é bi-transitivo em S, se para qualquer dois pares $\{s_1,s_2\}\{s'_1,s'_2\} \subset S$ ($s_2 \neq s_1$, $s'_2 \neq s'_1$), existe $x \in G$ tal que $x(s_i) = s'_i$, para $i = 1,2$.*

O inteiro $|S|$ é chamado grau de G ou grau da representação μ.

Sejam $H \subset G$ e $S = \{x_iH | x_i \in G,\ \ i = 1,2,...,n\}$ um conjunto completo de classes laterais de H. Então para $x \in G$ definimos $\pi_x : S \to S$, tal que $\pi_x(x_iH) = (xx_i)H$ com $1 \leq i \leq n$. Temos que π_x é uma permutação de S, e $\pi_x\pi_y = \pi_{xy}$. Em geral seja

$$\begin{array}{rcccccl} \pi_H : & G & \longrightarrow & A(S) & & & \\ & x & \longmapsto & \pi_x : & S & \longrightarrow & S \\ & & & & x_iH & \longmapsto & \pi_x(x_iH) = xx_iH. \end{array}$$

Temos que π_H é uma representação permutacional transitiva, chamada de representação permutacional transitiva de G nas classes laterais de H e, reciprocamente, temos o seguinte teorema:

Teorema 1.2.2 *Toda representação permutacional transitiva de G é equivalente a uma representação permutacional transitiva de G, nas classes laterais de H para algum $H \leq G$.*

A prova deste resultado encontra-se em [4]. O caso especial, onde $H = 1$, $\pi_{\{1\}}$ é chamado de representação regular de G, e cumpre a propriedade de que só a imagem da identidade pelo homomorfismo $\pi_{\{1\}}$ deixa fixo mais de um elemento.

$$\begin{array}{rccccl} \pi_{\{1\}}: & G & \longrightarrow & A(S) & & \\ & x & \longmapsto & \pi_x: & S & \longrightarrow S \\ & & & & x_i\{1\} & \longmapsto \pi_x(x_i\{1\}) = xx_i\{1\} = \{xx_i\}, \end{array}$$

onde o grau de $\pi_{\{1\}}$ é igual a $|G|$, dado que o conjunto completo das classes laterais de $\{1\}$, S, é a coleção dos conjuntos unitários dos elementos de G, isto é, $S = \{\{g\}|g \in G\}$.

Seja π uma representação permutacional de um grupo G em um conjunto S, podemos considerar S como uma base de um espaço vetorial V sobre um corpo arbitrário F. Suponha $|S| = n$, podemos ver os elementos de $\pi(G)$ como sendo transformações lineares de V. Então isto induz um homomorfismo de G no grupo de transformações lineares não singulares de V, denotado por $GL(V,F)$, onde F é o corpo associado ao espaço vetorial V, ou o que resulta equivalente, a um homomorfismo de G no grupo das matrizes invertíveis $n \times n$ com coeficientes no corpo F, denotado por $GL(n,F)$.

Um homomorfismo $\phi : G \to GL(V,F)$ é chamado uma representação de G e V é chamado o espaço de representação ou módulo de representação. Se ϕ é injetora então ϕ é chamado de representação fiel, o que é equivalente a dizer que só o elemento identidade de G ($e \in G$) vai ser levado por ϕ na aplicação identidade (ou elemento identidade de $GL(V,F)$).

A prova do teorema seguinte pode ser encontrada em [4]

Teorema 1.2.3 *Toda representação ϕ induz uma representação fiel, dada por*

$$\begin{array}{rccc} \phi: & G/Ker(\phi) & \longrightarrow & GL(V,F) \\ & xKer(\phi) & \longmapsto & \phi(x)Ker(\phi), \end{array}$$

onde ϕ ser injetiva segue do Teorema de Isomorfismo.
Seja W um subespaço de V, W é dito $\phi(G)$-invariante se para todo $g \in G$, temos que $\phi_g(W) = W$.

Dado W um subespaço invariante de V pelas transformações lineares $\phi(G)$, então ϕ induz uma representação $\phi|_W : G \to GL(W,F)$, chamada de restrição de ϕ a W.

A seguir apresentamos algumas classes especiais de representação, as quais são usadas no desenvolvimento do trabalho:

- Uma representação $\phi : G \to GL(V,F)$ é irredutível se os únicos subespaços invariantes pelas transformações $\phi(G)$ são 0 e V.

- Uma representação ϕ não tem descomposição se não é possível escrever V como a soma direta de dois subespaços $\phi(G)$-invariantes (não triviais).
- Uma representação ϕ é completamente redutível se $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$, onde V_i são subespaços não triviais $\phi(G)$-invariantes e $\phi|_{V_i}$ é irredutível para todo $i = 1,2,...,r$.

Sejam $\phi : G \to GL(V,F)$ e $\phi' : G \to GL(V',F)$ representações de G, onde $dim(V) = dim(V') = n$ e $v = \{v_1, v_2, ..., v_n\}$, $v' = \{v'_1, v'_2, ..., v'_n\}$ são bases de V e V', respectivamente. Considere o isomorfismo ψ, tal que

$$\begin{array}{rccc} \psi : & V & \longrightarrow & V' \\ & v_i & \longmapsto & v'_i. \end{array}$$

Sejam P a matriz associada ao isomorfismo ψ, $(\phi'(x))'_v$ e $(\phi(x)_v)$ as representações matriciais de $\phi'(x)$ e $\phi(x)$ nas bases v' e v respectivamente. Então $\phi'(x)$ e $\phi(x)$ são equivalentes se: $(\phi'(x))'_v = P^{-1}(\phi(x)_v)P$. Expressando isso em termos de transformações lineares temos que $\phi'(x) = \psi^{-1}\phi(x)_v\psi$.

A noção de equivalência de representações é uma relação de equivalência na categoria de todas as representações do grupo G em espaços vetoriais sobre um corpo dado (F).

1.3 Comutadores

Nesta seção trabalhamos o conceito de comutador, não só para fazer uma boa introdução ao conceito de grupo solúvel, mas também para introduzir alguns comutadores de elementos do grupo de automorfismos de G com elementos do grupo G.

Definição 1.3.1 *Sejam G um grupo e $x, y \in G$. O comutador de x e y é definido por $[x,y] = x^{-1}y^{-1}xy$, um comutador de comprimento $n \geq 2$ define-se indutivamente por $[x_1, x_2, ..., x_n] = [[x_1, x_2, ..., x_{n-1}], x_n]$. Dados H e K subconjuntos de G o subgrupo comutador de H e K é o menor subgrupo de G que contém todos os comutadores da forma $[h,k]$, onde $h \in H$ e $k \in K$, isto é, $[H,K] = \langle\{[h,k] | h \in H \;\; e \;\; k \in K\}\rangle$.*

Um importante subgrupo definido a partir dos comutadores é o subgrupo derivado ou subgrupo comutador de G, o qual denotamos por G' e está definido como

$$G' = [G,G] = \langle\{[g,h] | g,h \in G\}\rangle .$$

Da definição acima, temos que G é abeliano se, e somente se, $G' = 1$.

O subgrupo derivado é o subgrupo normal minimal que tem a condição de, ter fator abeliano (G/G' é abeliano).
Um conjunto de subgrupos de G, os quais têm um ordem total com respeito à inclusão (uma cadeia) se diz uma série de G.

Podemos definir indutivamente a série derivada de G, definindo $G^{(n)}$ da seguinte maneira $G^{(1)} = G'$ e $G^{(n)} = (G^{(n-1)})' = [G^{(n-1)}, G^{(n-1)}]$, $G^{(i)}$ é chamado de i-ésimo subgrupo derivado de G. Tal construção gera uma cadeia de subgrupos $G \geq G' \geq G^{(2)} \geq \cdots$, onde do teorema acima temos que $G^{(i)} \lhd G^{(i-1)}$.

Exibimos agora algumas propriedades dos comutadores:

Teorema 1.3.2 *Sejam x,y,z,t elementos de um grupo G. Então*

1. $[x,y] = 1$ *se, e somente se,* $xy = yx$.
2. $[x,y]^{-1} = [y,x]$.
3. $[x,y]^z = [x^z, y^z]$.
4. $[xy,z] = [x,z]^y[y,z] = [x,z][[x,z],y][y,z]$.
5. $[x,yz] = [x,z][x,y]^z = [x,z][x,y][[x,y],z]$.
6. $[x,y]z = z[x^z,y^z]$.
7. $[x^y,z] = [x,z]^{[x,y]}[x,y,z]$.
8. $[x^{y^z},t] = [x^y,t]^{[x^y,z]}[x^y,z,t]$.
9. $[x,y,z] = [x,y]^{-1}[x,y]^z$.

A prova do teorema acima pode ser encontrada em vários resultados expostos em [13].

Proposição 1.3.3 *Sejam G um grupo finito e $N \trianglelefteq G$, então $[u,v]N = [uN,vN]$ para todo $u,v \in G$. Além disso, dados subgrupos $H_i \leq G$, temos $[H_1N, H_2N, \ldots, H_nN] = [H_1, H_2, \ldots, H_n]N$*

Demonstração.
Seja $N \lhd G$. Temos $[u,v]N = u^{-1}v^{-1}uvN = u^{-1}Nv^{-1}NuNvN = [uN,vN]$. Generalizando para os subgrupos H, K do grupo G, temos que $[K,H]N = [KN,HN]$ pois se tem para cada elemento $k \in K$ e $h \in H$. Logo, fazendo indução sobre o resultado anterior obtemos $[H_1N, H_2N, \ldots, H_nN] = [H_1, H_2, \ldots, H_n]N$. ■

1.4 Grupos Solúveis e Grupos Nilpotentes

Os grupos solúveis e nilpotentes constituem a mais importante generalização do conceito de grupo abeliano.

Definição 1.4.1 *Seja $1 = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$ uma série de subgrupos de G, esta série se diz subnormal se satisfaz a condição de $G_i \trianglelefteq G_{i+1}$, $i = 0, \cdots, n-1$.*

Dada uma série subnormal, os grupos quocientes G_i/G_{i-1} são chamados os fatores da série.

Definição 1.4.2 *Um grupo G que possui uma série subnormal finita com fatores abelianos se diz um grupo solúvel.*

Definição 1.4.3 *Dizemos que uma série e normal, se $G_i \trianglelefteq G$ para todo $i = 1, ..., n$. É claro que toda série normal é subnormal.*

Seja $G \supset G' = [G,G] \supset \cdots \supset G^{(n-1)} \supset \cdots$, a série derivada de G, é um exemplo de série normal.

Teorema 1.4.4 *Seja G um grupo, então as seguintes afirmações são equivalentes:*

1. *G é solúvel.*
2. *A série derivada de G possui um número finito de termos ($G^{(n)} = 1$ para algum $n \in \mathbb{N}$).*
3. *G possui uma série subnormal finita com fatores abelianos.*
4. *G possui uma série normal finita com fatores abelianos.*

A prova do teorema acima pode ser encontrada como resultado de vários teoremas em [9].
Das equivalências acima podemos observar o porque de falar que os grupos solúveis constituem uma generalização dos grupos abelianos. Todo grupo abeliano é solúvel; além disso, com a definição de grupo solúvel a partir da série normal com fatores abelianos, temos que o último elemento da série (não trivial) resulta ser abeliano. E daí por diante

o grupo resulta ser a extensão , um número finito de vezes, de um grupo abeliano, onde percebemos a estreita relação entre grupos solúveis e os grupos abelianos.

Um resultado importante sobre grupos solúveis é o Teorema de W. Feit e L. G. Thompson [3] que fala que todo grupo de ordem ímpar é solúvel.

As séries como vistas acima exercem um papel fundamental no estudo da teoria de grupos. Agora com o estudo das séries centrais que se faz logo adiante temos a definição de outro tipo de grupos. Trata-se dos grupos nilpotentes, os quais são caracterizados pela propriedade de possuir uma série central finita. Estes grupos, da mesma maneira que os grupos solúveis, constituem uma geralização dos grupos abelianos, mas com o fato de que todo grupo nilpotente resulta ser solúvel, temos que a classe dos grupos nilpotentes é um pouco mais refinada que a classe dos grupos solúveis, estes grupos são uma classe intermediária entre a classe de grupos abelianos e a dos grupos solúveis.

Uma série normal se diz central se seus fatores são centrais, isto é, $G_i/G_{i-1} \subset Z(G/G_{i-1})$.

Definição 1.4.5 *Um grupo G que possui uma série central finita é dito um grupo nilpotente.*

Seja G um grupo, obtemos a série central inferior de G definindo $\gamma_1 = G$, $\gamma_2 = G'$ e indutivamente definimos os outros termos da série como sendo $\gamma_i = [\gamma_{i-1}, G]$, o que nos leva a uma expressão da forma:

$$\gamma_1 = G \supset \gamma_2 = G' \supset \gamma_3 = [\gamma_2, G] \supset \cdots \supset \gamma_n = [\gamma_n - 1, G] \supset \cdots$$

A série central superior ou ascendente de um grupo G é obtida por $Z_0 = \langle e \rangle$, $Z_1 = Z(G)$, $Z_2 = \pi_1^{-1}(Z(G/Z))$ e indutivamente definimos os outros termos da série como sendo $Z_i = \pi_{n-1}^{-1}(Z(G/Z_{n-1}))$, onde π_i é a projeção canônica de G no grupo quociente G/Z_i e $Z(G/Z_{n-1})$ representa o centro do grupo quociente, o que completa a série

$$Z_0 = \langle e \rangle \subset Z_1 = Z(G) \subset \cdots \subset Z_n = \pi^{-1}(Z(G/Z_{n-1})) \subset \cdots$$

As séries centrais acima definidas são importantes no estudo dos grupos nilpotentes e é compreenssível os nomes dados às mesmas, porque elas constituem uma limitação para toda série central do grupo G, isto é:

Teorema 1.4.6 *Seja $A_0 = 1 \subset A_1 \subset \cdots \subset A_n = G$ uma série central do grupo G. Então $\gamma_{n-i} \subset A_i \subset Z_i$.*

A seguir apresentamos equivalências para a definição de nilpotência para um grupo G.

Teorema 1.4.7 *Se G é um grupo, então as seguintes afirmações são equivalentes:*

1. *G é nilpotente*
2. *A série inferior de G possui um número finito de termos ($\gamma_n = e$ para algum $n \in \mathbb{N}$)*
3. *A série superior de G possui um número finito de termos ($Z_{n-1} = G$ para algum $n \in \mathbb{N}$)*

As provas dos teoremas acima pode ser encontrada em [11].
O menor comprimento, c, tal que $\gamma_{c+1} = e$ e $Z_c = G$ é chamado de classe de nilpotência.

O centro de um grupo nilpotente intercepta todos os subgrupos normais (não trivialmente), isto é:

Proposição 1.4.8 *Sejam G um grupo nilpotente e $H \neq e$, $H \trianglelefteq G$, então $H \cap Z(G) \neq e$.*

Em particular temos que um subgrupo normal minimal N de um grupo nilpotente G está contido no centro, provas desta Proposição, do teorema acima e da Proposição 1.4.9 podem ser encontadas em [13].

Dado que o objetivo da presente dissertação é o estudo de centralizadores de automorfismos em grupos finitos expomos a seguir algumas propriedades de grupos nilpotentes de ordem finita.

O primeiro resultado relativo a grupos nilpotentes finitos que será exposto neste trabalho nos dá uma propriedade importante de normalizadores de subgrupos.

Proposição 1.4.9 *Seja H um subgrupo próprio de um grupo nilpotente finito G, então $H \subset N_G(H)$ propriamente.*

Definição 1.4.10 *Um grupo G cumpre a condição do normalizador se ele satisfaz a condição enunciada acima. Isto é, dado H um subgrupo próprio do grupo G, então $H \subset N_G(H)$ propriamente.*

Definição 1.4.11 *Um subgrupo H de G, se diz subnormal se ele pertence a uma série subnormal de G.*

Com as definições acima podemos enunciar mais equivalências, ao fato de um grupo finito ser nilpotente:

Teorema 1.4.12 *Seja G um grupo de ordem finita. Então temos as seguintes equivalências:*

1. *G é nilpotente.*
2. *G cumpre a condição do normalizador.*
3. *Todo subgrupo de Sylow de G é normal em G.*
4. *G é o produto direto dos seus subgrupos de Sylow.*
5. *Todo subgrupo de G é subnormal.*
6. *Todo subgrupo maximal é normal.*

A prova do teorema anterior pode ser encontrada fragmentada em vários teoremas em [4].

1.5 p-grupos e p-grupos Abelianos Elementares

Definimos agora alguns tipos de grupos úteis para alguns resultados.

Definição 1.5.1 *Seja p um número inteiro primo, então dizemos que G finito é um p-grupo, se sua ordem é uma potência de p. Um grupo H se diz um p'-grupo se sua ordem não é divisível por p, isto é, se $|H| = n$, então $p \nmid n$.*

Definição 1.5.2 *Dado um grupo G, finito, de ordem n ($|G| = n$) um p-subgrupo de Sylow de G (S_p-grupo), é um subgrupo P de G com a propriedade que P é um p-grupo e se $|P| = p^n$, então $p^{n+1} \nmid n$, isto é, a ordem de P é a maior potência de p que divide a ordem do grupo.*

Definição 1.5.3 *Seja π um conjunto de inteiros primos ($\pi = \{p_1, p_2, ..., p_n\}$). Dizemos que um grupo G é um π-grupo se a ordem de G é produto de potências de primos pertencentes a π, isto é, $|G| = \prod_{i=1}^{n} p_i^{\alpha_i}$. Um grupo H se diz um π'-grupo se a decomposição primária da sua ordem não contém nenhum elemento de π, isto é, $p_i \nmid |H|$ para todo $i = 1, ..., n$.*

Definição 1.5.4 *Sejam π um conjunto de inteiros primos ($\pi = \{p_1, p_2, ..., p_n\}$) e um grupo G de ordem n ($|G| = n$), um subgrupo H se diz S_π-grupo de G, se H é um π-grupo e o índice de H em G não é divisível por nenhum $p_i \in \pi$, isto é, $p_i \nmid [G : H]$ para todo $i = 1, ..., n$.*

Quando o conjunto de primos π tem só um elemento, um S_π-grupo diz-se um subgrupo de Sylow de G.

Teorema 1.5.5 *Um p-grupo abeliano finito G é o produto direito de subgrupos cíclicos C_i, $1 \leq i \leq n$, $n \in \mathbb{Z}$. Além disso, o inteiro n e as ordens de C_i, estão unicamente determinadas (a exceção da sua ordenação).*

A prova do teorema acima pode ser encontrada em [4].

Definição 1.5.6 *Dado um p-grupo abeliano finito G denotamos o n, dado no teorema, por m(G) dada sua unicidade, e $|H_i| = p^{e_i}$, assim, dizemos que G é da forma $(p^{e_1}, p^{e_2}, ..., p^{e_n})$, além disso, se $H_i = \langle x_i \rangle$, então chamamos $B = \{x_i | H_i = \langle x_i \rangle \quad \text{para algum } i = 1, .., n\}$ a base de G, e para todo elemento $x \in G$ temos que $x = x_1^{\alpha_1} x_1^{\alpha_2} ... x_n^{\alpha_n}$ onde $0 \leq \alpha_i < p^{e_i}$, $i = 1, ..., n$.*

Definição 1.5.7 *Um p-grupo abeliano finito G da forma $(p, p, p, ..., p)$ é chamado um p-grupo abeliano elementar.*

A seguir enunciamos uma propriedade de grupos de ordem ímpar.

Proposição 1.5.8 *Seja G um grupo de ordem ímpar e $g \in G$, tal que $x^{-1}gx = xg^{-1}x^{-1}$, para algum $x \in G$. Então $g = 1$.*

Demonstração.
A prova desta proposição consiste basicamente em uma iteração do seguinte processo: A hipótese, $x^{-1}gx = xg^{-1}x^{-1}$ implica que $g^{-1} = x^{-2}gx^2$. Conjugando os dois lados por x temos que $x^{-1}g^{-1}x = x^{-3}gx^3$. Usando a hipótese novamente chegamos a $xgx^{-1} = x^{-3}gx^3$,

obtendo $g = x^{-4}gx^{4}$. Iterando o processo chegamos a $g^{-1} = x^{-2(2k+1)}gx^{2(2k+1)}$ e $g = x^{-4k}gx^{4k}$. Como a ordem de G é ímpar, em particular a ordem de x é ímpar, então dado um $k \in \mathbb{N}$ apropriado, $g^{-1} = g$, assim $g = 1$.

CAPÍTULO 2

Centralizadores de Automorfismos

2.1 Definições e Resultados Introdutórios

Dados dois grupos A e G dizemos que A age via automorfismos sobre G, se A age sobre G (como se definiu em 1.2) e existe um homomorfismo injetivo de grupos $\theta : A \to Aut(G)$, tal que $an = n^{\theta(a)}$ para todo $a \in A$ e $n \in G$. Isto é $a(nn_1) = (an)(an_1)$.

A notação para a ação dos elementos que agem como automorfismos sobre os elementos do grupo pode ser diferente, em algumas ocasiões podemos expressar essa ação como $a(n)$, mas usualmente temos a seguinte notação, n^a, o que pode confundir com a notação de conjugado. No entanto, o que observamos é que todo automorfismo age sobre um grupo como uma conjugação em um outro grupo apropriado (daí a importância do produto semidireto), a ação de todo automorfismo $a \in A$ de G pode ser visto como uma conjugação no produto semidireto do grupo A com o grupo G, $G \rtimes A$, onde temos que $a(n) = (n,1)^{(1,a)}$, sendo $(n,1),(1,a)$ as injeções canônicas dos elementos n e a no produto semidireto.

Seja A um grupo que age como automorfismos em um grupo G. Por definição A permuta os elementos de G, dado que em particular cada elemento de A é uma bijeção de G em G. Uma condição a mais dos automorfismos é que permutam muitos outros objetos da teoria de grupos, por exemplo permutam classes de conjugação. O estudo de elementos invariantes por todo tipo de aplicação é sempre importante para analisar algumas propriedades da estrutura. Temos os conjuntos A-invariantes, isto é, os conjuntos $H \subseteq G$, tais que $H^a \subseteq H$ para todo $a \in A$. Em particular, temos os elementos A-invariantes, que são chamados os pontos fixos por A, onde quando se fala dos pontos fixos estes são todos os $g \in G$, tal que $g^a = g$ para todo $a \in A$. O conjunto de todos os pontos fixos formam um subgrupo do grupo G, denotado por $C_G(A)$, este subgrupo é chamado de centralizador de A em G. Quando só temos um automorfismo ϕ, o conjunto dos pontos fixos por ϕ em G é o centralizador do automorfismo ϕ no grupo G, $C_G(\phi) = \{g \in G | g^\phi = g\}$, o qual também denotamos por G_ϕ, para maior simplicidade na escrita. Com as ferramentas até agora expostas, podemos entender o porquê do nome, centralizador de automorfismos.

Seja $L = G \rtimes A$. Como vimos acima, A age sobre G como conjugação em L, logo $g^a = g$ se, e somente se, g e a comutam em L (na realidade a notação anterior é um abuso de notação dado que os elementos que comutam são as injeções de g e a em L)[1]. Logo, o conjunto dos pontos fixos que chamamos de centralizador de A em G é precisamente os elementos de G, que comutam com todos os elementos de A , o qual é conhecido na teoria de grupos como $C_G(A)$ logo:

$$C_G(A) = \{x \in G | x^a = x \quad \forall a \in A\}.$$

Estudamos no capítulo anterior alguns comutadores de elementos do grupo, e sugerimos a possibilidade de fazer comutadores entre automorfismos e elementos do grupo sendo estes elementos pertencentes a grupos diferentes. A partir dos comentários anteriores podemos perceber que não se trata de comutadores de elementos de grupos diferentes, se trata realmente, de gerar um novo grupo onde esses comutadores fazem sentido e este grupo é o produto semidireto de G, com um subgrupo dos automorfismos de G, que contenha o automorfismo com o qual queremos fazer o comutador.

Em outras palavras, cada vez que temos um comutador da forma $[\phi, g]$, onde $\phi \in Aut(G)$ e $g \in G$, ele faz sentido no grupo $L = G \rtimes Aut(G)$, somando o fato que $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$ obtemos que:

$$[g, \phi] = (g^{-1})g^{\phi},$$

poderíamos obter o mesmo resultado se simplesmente operamos os automorfismo nos elementos do grupo, isto é:

$$[g, \phi] = ((g^{-1})^{(\phi)^{-1}}g)^{\phi} = ((g^{-1})^{(\phi)^{-1}})^{\phi}g^{\phi} = (g^{-1})g^{\phi}.$$

Com todas essas observações podemos dar uma definição já exposta na introdução.

Definição 2.1.1 *O subgrupo gerado pelos elementos da forma $[g, \phi]$ com $g \in G$ e ϕ um automorfismo de G fixo, é denotado por,*

$$[G, \phi] = \left\langle \{g^{-1}g^{\phi} | g \in G\} \right\rangle.$$

[1] O abuso de notação que usamos aqui vai ser usado em repetidas ocasiões no decorrer do trabalho sem fazer nova menção

Os elementos da forma $[g,\phi]$ não resultam ser fechados para a operação (para potências sim), a não ser que o grupo G seja abeliano.

Proposição 2.1.2 *Sejam G um grupo, e ϕ um automorfismo de G. Então o subgrupo $[G,\phi]$ é normal em G.*

Demonstração.
Para provar que $[G,\phi] \trianglelefteq G$, basta provar que para todo gerador de $[G,\phi]$ o conjugado deste gerador por qualquer elemento de G pertece a $[G,\phi]$, logo sendo $x,g \in G$, tome $[x,\phi] := x^{-1}\phi(x)$, então

$$g^{-1}[x,\phi]g = g^{-1}x^{-1}\phi(x)g = (xg)^{-1}\phi(xg)\phi(g)^{-1}g = [xg,\phi][g,\phi]^{-1}.$$

Portanto, $g^{-1}[x,\phi]g \in [G,\phi]$, de onde temos que, $[G,\phi] \trianglelefteq G$. ■

Generalizando a definição de comutador acima, definimos também o subgrupo $[G,A]$.

Definição 2.1.3 *Seja $A \subset Aut(G)$, denotamos por $[G,A]$ o subgrupo gerado por todos os elementos da forma $[g,a]$, onde $g \in G$ e $a \in A$, isto é,*

$$[G,A] = \left\langle \{g^{-1}g^a | g \in G \ \ e \ \ a \in A\} \right\rangle.$$

No desenvolvimento deste capítulo fazemos vários abusos de notação, dos quais falamos mais na frente, um dos mais usuais é usar o mesmo símbolo para denotar um automorfismo ϕ, e o correspondente automorfismo induzido por ϕ nas classes laterais de um subgrupo normal ϕ-invariante H, isto é:

Sejam G um grupo, $H \trianglelefteq G$ ϕ-invariante e ϕ um automorfismo de G. Então o automorfismo ϕ induz um automorfismo no grupo G/H, dado por:

$$\begin{array}{rccc} \bar{\Phi}: & G/H & \longrightarrow & G/H \\ & gH & \longmapsto & (gH)^{\bar{\Phi}} = g^{\phi}H. \end{array}$$

Pode-se comprovar que as propriedades de automorfismo são obtidas por herança das propriedades do automorfismo ϕ, pelo qual não vamos fazer distinção entre os dois.

2.2 Subgrupos de Automorfismos de Ordem Coprima

Começamos essa seção com um lema que faz parte dos resultados gerais para grupos finitos. Que fala sobre a ação de um grupo de automorfismos sobre um grupo finito G. Mais adiante no trabalho, tratamos de casos mas específicos deste lema, nos casos de automorfismos de ordem coprima com a ordem do grupo, e involuções em grupos de ordem ímpar.

Lembremos que um subgrupo A de automorfismos de G diz-se coprimo, se temos $(|G|,|a|) = 1$ para todo $a \in A$. O seguinte resultado é exposto e provado por Gorenstein em [4] (Teorema 5.3.5).

Lema 2.2.1 *Seja A um p'-grupo de automorfismos de um p-grupo P, então $P = CH$, onde $C = C_P(A)$ e $H = [P,A]$.*

Lema 2.2.2 *Seja A um p'-grupo de automorfismos de um p-grupo finito P. Se H é um subgrupo normal de P, A-invariante, então $C_{P/H}(A) = C_P(A)H/H$.*

Demonstração.
Para isso, definimos algumas notações.

Sejam $\bar{P} = P/H$, $\bar{K} = C_{P/H}(A)$ e $K = \pi^{-1}(\bar{K})$, onde π é a projeção canônica de P em P/H.
Temos que uma das inclusões se obtém de forma imediata, a saber $C_{P/H}(A) \supset C_P(A)H/H$.
Além disso, temos $C_P(A) \subset K$. Para ter a igualdade desejada, basta provar que:
$K = HC_K(A)$, o que provamos usando a seguinte afirmação a qual é devidamente provada a seguir,

$$\bar{K} = C_{P/H}(A) = K/H = C_K(A)H/H = C_P(A)H/H,$$

provamos a afirmação acima em três passos, verificando cada uma das igualdades acima mencionadas. Primeiro temos $C_{P/H}(A) = K/H$, dado que por definição $K = \pi^{-1}(\bar{K})$ de onde $K/H = \pi(K) = \pi(\pi^{-1}(\bar{K})) = \bar{K} = C_{P/H}(A)$, assim obtemos a primeira igualdade.

Agora, temos $C_K(A)H/H = C_P(A)H/H$. De fato a primeira inclusão se tem diretamente, já que $K \subset P$, então $C_K(A) \subset C_P(A)$, de onde obtemos que a projeção no grupo quociente P/H preserva tal inclusão. Para verificar a segunda inclusão, seja $pH \in C_P(A)H/H$, então $ph \in C_p(A)$ para algum elemento de pH, onde pela escolha de ph, temos $(ph)^a = ph$ para todo $a \in A$. Logo $(pH)^a = (phH)^a = phH = pH$ para todo $a \in A$, portanto

$phH \in C_{P/H}(A) = \bar{K}$ e assim $ph \in K$ dado que $ph \in \pi^{-1}(phH)$, logo $pH \in C_K(A)H/H$.

Por último $K/H = C_K(A)H/H$ se verifica se $K = HC_K(A)$, pelo qual a prova restringe-se à verificação de $K = HC_K(A)$.

Temos que K é A-invariante, dado que se $k \in K$, então $(kH)^a = kH$ pelo fato de $K = \pi^{-1}(\bar{K})$, com o qual temos que $k^a \in kH$ para todo $a \in A$. Logo $k^a \in \pi^{-1}(kH)$, pois $(kH) \in \bar{K}$, então $\pi^{-1}(kH) \subset \pi^{-1}(\bar{K}) = K$, e $k^a \in \pi^{-1}(\bar{K}) = K$.

K é subgrupo do grupo P e pelo fato de que K é A-invariante, então K é também um p-subgrupo e A um subgrupo de automorfismos de K (p'-subgrupo), onde podemos aplicar o Lema 2.2.1 que diz o seguinte.

Seja A um p'-grupo de automorfismos de um p-grupo P, então $P = CH$, onde $C = C_P(A)$ e $H = [P,A]$.

Obtemos

$$K = [K,A]C_K(A).$$

Temos $[K,A] \subset H$ dado que sendo $k \in K$ e $a \in A$ se tem $k^aH = kH$, então $k^{-1}k^a \in H$. Logo $K \subset HC_K(A)$. Agora, seja $c \in C_K(A)$, pela definição $c^a = c$ para todo $a \in A$,e seja $h \in H$, então percebemos que $hcH = cH$, dado que $c^{-1}Hc \in H$ para todo elemento de P, em particular para c, portanto $(hcH)^a = (cH)^a = c^aH = cH = hcH$, logo $hc \in K$ para todo $h \in H$ e $c \in C_K(A)$, de onde temos a outra inclusão $K \supset HC_K(A)$. Concluímos que

$$K = HC_K(A).$$

Portanto, obtemos $C_{P/H}(A) = C_P(A)H/H$, onde P é um p-grupo.

■

O seguinte resultado é exposto por Gorenstein em [4] Teorema 6.2.2.i.

Lema 2.2.3 *Seja A um π'-grupo de automorfismos do π-grupo G, e suponha G ou A solúvel. Então para cada primo $p \in \pi$, nos temos que A deixa invariante algum S_p-subgrupo de G.*

Lema 2.2.4 *Seja A um grupo de automorfismos de um grupo finito G onde G ou A é solúvel com $(|A|,|G|) = 1$.*

1. *Se N é um subgrupo de G, A-invariante, então $C_{G/N}(A) = C_G(A)N/N$.*

2. $G = C_G(A)[G,A]$.

3. $[G,A] = [G,A,A]$.

Demonstração.

1. Tendo o resultado para p-grupos (Lema 2.2.2), generalizamos este para um grupo G qualquer conforme pode-se ver a seguir.

   Sejam $N \trianglelefteq G$ e $(|A|,|G|) = 1$ onde A é um subgrupo do grupo dos automorfismos de G e N é A-invariante.

   Sejam $\bar{C} = C_{G/N}(A)$ e $\Pi(\bar{C}) = \{p_i|\ p_i$ é primo e $p_i||\bar{C}|\}$ e $C = C_G(A)$, temos que $\bar{C}$ contem a imagem de C em $\bar{G}$, onde $\bar{G} = G/N$, assim é suficiente provar, que para todo $p_i \in \Pi(\bar{C})$ um S_{p_i}-subgrupo (um p_i subgrupo de sylow) de C tem como imagem um S_{p_i}-subgrupo de $\bar{C}$ pela projeção natural, para obter que $C_{G/N}(A) = C_G(A)N/N$. É suficiente, pois todo S_p-subgrupo de $\bar{C}$ resulta isomorfo à imagem de um S_p-subgrupo de C, pelo epimosfismo canônico, projetada no quociente do grupo pelo kernel do epimorfismo (mas o kernel do epimorfismo canônico é o mesmo N), assim teríamos, dado o isomorfismo de cada subgrupo de sylow, que $C_{G/N}(A) = C_G(A)N/N$.

   Seja $\bar{P}$ um S_p-subgrupo de $\bar{C}$ e seja $K = \pi^{-1}(\bar{P}) = \{x \in G|xN \in \bar{P}\}$. Seja P um A-invariante S_p-subgrupo de K, o qual existe dado o Lema 2.2.3.

   Agora $P \subset K = \pi^{-1}(\bar{P})$ o que implica que A centraliza PN/N.

   Pelo fato do homomorfismo preservar ordem $PN/N \supset \bar{P}$, além disso, $PN/N \subset \bar{P}$ pela definição de P, assim $PN/N = \bar{P}$.

   Logo pelo Lema 2.2.2, obtemos

   $$C_{P/N\cap P}(A) = C_P(A)N \cap P/N \cap P.$$

   Como $PN/N \cong P/N \cap P = \bar{P}$, então

   $$C_{P/N\cap P}(A) = C_{\bar{P}}(A) = \bar{P},$$

   também temos

   $$C_P(A)N \cap P/N \cap P \cong C_P(A)/(C_P(A) \cap N \cap P) = C_P(A)/(C_P(A) \cap N) \cong C_P(A)N/N$$

assim, obtemos que para todo S_p-subgrupo de $C_{G/N}(A)$ existe um S_p-subgrupo de $C_G(A)$, a saber $C_P(A)$, tal que a projeção de $C_P(A)$ no grupo quociente coincide com $\bar{P}$, então temos que

$$C_{G/N}(A) = C_G(A)N/N.$$

2. Dada a normalidade de $[G,A]$ (a qual é obtida pela generalização da Proposição 2.1.2) temos que o quociente $G/[G,A]$ faz sentido, e denotamos ele por $\bar{G} = G/[G,A]$. Agora aplicando o item 1 deste lema, temos $C_{\bar{G}}(A) = C_G(A)[G,A]/[G,A]$, mas A age trivialmente em $G/[G,A]$ já que, $(g[G,A])^a = g^a[G,A] = g[G,A]$, pois $g^{-1}g^a \in [G,A]$ para todo $g \in G$ e para todo $a \in A$, de onde temos $C_{\bar{G}}(A) = G/[G,A]$, logo

$$G = C_G(A)[G,A].$$

3. Para garantir a igualdade desejada verificamos a dupla inclusão. Primeiramente $[G,A] \supset [G,A,A]$, dado que $[G,A] \subset G$. A outra inclusão, $[G,A] \subset [G,A,A]$, basea-se no resultado do item anterior o qual garante que $G = C_G(A)[G,A]$, assim, se $g \in G$, então $g = g_c x$, onde $g_c \in C_G(A)$ e $x \in [G,A]$. Agora, seja $a \in A$ temos que $[g_c,a] = e$, além disso, pelas propriedade de comutadores, Teorema 1.3.2 que:

$$[ab,c] = (ab)^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = [a,c]^b[b,c].$$

Temos $[g,a] = [g_c x,a] = [g_c,a]^x[x,a] = [x,a]$, de onde $[g,a] \in [G,A,A]$.

Assim, basta verificar a inclusão para os geradores, de onde concluímos

$$[G,A] = [G,A,A].$$

■

O próximo lema, faz parte da teoria geral de grupos finitos com automorfismos coprimos e finda os resultados globais que são tratados no desenvolvimento deste trabalho.

Lema 2.2.5 *Seja A um grupo de automorfismos de um grupo finito G com $(|A|,|G|) = 1$. Seja $\{N_i | i \in I\}$ uma família de subgrupos normais de G, A-invariantes e $N = \prod_i N_i$. Então $C_N(A) = \prod_i C_{N_i}(A)$.*

Demonstração.
Seja $C = C_N(A)$. Para todo $n \in N$, temos $n = \prod_{i \in I} n_i$, onde $n_i \in N_i$, então para todo $c \in C$, temos $c = \prod_{i \in I} n_i$. Seja $|I| = t < \infty$ e façamos indução sobre a cardinalidade de I. Se $|I| = 1$ o resultado é imediato. Suponha que o resultado vale para $t-1$. Então seja $M = N_1 N_2 \ldots N_{t-1}$ e $L = N_t$, pela hipótese de indução temos que $C_M(A) = M \cap C = \langle \{C \cap N_i | 1 \leq i \leq t-1\} \rangle$. Assim.

$$(C \cap N)M/M = (C \cap ML)M/M \leq C_{ML/M}(A) = C_L(A)M/M,$$

onde a última igualdade segue do item (1) do lema anterior. Portanto, $C_N(A) = C \cap ML \leq M(C \cap L)$ e $C \cap ML \leq (C \cap M)(C \cap L) \leq M(C \cap L)$, com o qual concluímos que $C_N(A) = C \cap ML = \langle C \cap N_1, C \cap N_2, \ldots, C \cap N_{t-1}, C \cap N_t \rangle$.

■

2.3 Automorfismos de Ordem Coprima

Com a terminologia e definições dadas anteriormente, apresentamos os pré-requisitos mais importantes usados na demonstração do resultado principal deste trabalho. O seguinte lema é um dos mais importantes da teoria de automorfismos de ordem coprima à ordem do grupo e é uma particularização em alguns dos seus itens do Lema 2.2.4 só que o item 1 deste lema não pode ser obtido apartir do lema anteriormente mencionado, por que se a ordem de ϕ é diferente de dois, então não existe $A \leq Aut(G)$ tal que $A = \{Id, \phi\}$.

Lema 2.3.1 *Seja G um grupo finito, admitindo um automorfismo ϕ de ordem coprima com a ordem de G, $(|G|, |\phi|) = 1$. Então tem-se que:*

1. *Se N é um subgrupo normal ϕ-invariante de G, temos $(G/N)_\phi = G_\phi N/N$.*
2. *$G = C_G(\phi)[G, \phi]$.*
3. *$[G, \phi] = [G, \phi, \phi]$.*

Demonstração.

1. Para provar que $(G/N)_\phi = G_\phi N/N$ basta provar a dupla inclusão. Primeiramente a inclusão $(G/N)_\phi \supset G_\phi N/N$ resulta imediata do fato de que $gN \in G_\phi N/N$, então $g \in G_\phi$, logo $(gN)^\phi = g^\phi N = gN$ e, assim, $gN \in G/N_\phi$. Para provar a outra inclusão, a saber $(G/N)_\phi \subset G_\phi N/N$, temos que garantir que para todo $gN \in G/N_\phi$ existe

$x \in gN$, tal que $x \in G_\phi$. Procedemos por indução na ordem de ϕ.

Suponha que $|\phi| = p$, onde p é um número primo. Seja $gN \in G/N_\phi$. Então ϕ restrito a gN é uma bijeção ou permutação. Lembramos que a órbita de gn com relação à bijeção $\phi|_{gN}$ é dada por[2].

$$Orb(gn) = \{gn' \in gN | \phi^i(gn) = gn', \text{ para algum } i \in \mathbb{N}, i \leq p\}.$$

As órbitas geram uma partição de gN, além disso o tamanho das órbitas divide a ordem de ϕ, logo o tamanho da órbita é 1 ou p. Suponha que toda órbita tem tamanho p, então p divide a $|gN|$, logo $p|N$ o qual garante que p divide a ordem de G, $p||G|$, o que é uma contradição, de onde pelo menos uma das órbitas tem tamanho 1, logo existe um elemento $x \in G_\phi$.

Seja $|\phi| = rq$, com $r > 1$ e $q > 1$ (q um número primo). Pela hipótese de indução temos que $G/N_{\phi^r} = G_{\phi^r}N/N$, além disso $G/N_\phi \subset G/N_{\phi^r}$ (dado que se $gN \in G/N_\phi$, então $(gN)^\phi = gN$, logo $(gN)^{\phi^r} = gN$, pelo qual $gN \in G/N_{\phi^r}$).

Agora, seja $\bar{g}N \in G/N_\phi$. Pelo argumento anterior, temos que $\bar{g}N \in G/N_{\phi^r}$, pela hipótese existe $g_0 \in (G_{\phi^r} \cap \bar{g}N)$. Seja $x \in G_{\phi^r}$, então $x^\phi \in G_{\phi^r}$ pois $(x^\phi)^{\phi^r} = (x^{\phi^r})^\phi = x^\phi$. Logo G_{ϕ^r} é ϕ-invariante, dado que $\bar{g}N \in G/N_\phi$, então $\bar{g}N$ também é, o que implica que $(G_{\phi^r} \cap \bar{g}N)$ é ϕ-invariante. Em particular, a classe lateral $g_0(G_{\phi^r} \cap \bar{g}N)$ também é ϕ-invariante.

Fazendo a restrição do automorfismo ϕ ao grupo G_{ϕ^r}, que é ϕ-invariante, obtemos um automorfismo de ordem r dado por

$$\phi|_{G_{\phi^r}} : G_{\phi^r} \longrightarrow G_{\phi^r}.$$

Logo, pela hipótese de indução, temos que $g_0(G_{\phi^r} \cap \bar{g}N)$ possui um elemento de G_ϕ, assim, existe $x \in \bar{g}N$, tal que $x \in G_\phi$, o que conclui a prova.

Os dois últimos itens, 2 e 3, constituem uma particularização do Lema 2.2.4 e suas demonstrações seguem diretamente, dado que estas provas estam feitas por

[2] Como feito em 1.2

elementos a prova resulta só da reconstrução da demonstração do lema citado, e por isso omitimos a prova. ■

Definição 2.3.2 *Um subgrupo H dos automorfismos de um grupo G, é chamado de subgrupo regular, se todos os automorfismos contidos em H são livres de pontos fixos.*
O Seguinte lema pode ser encontrado no Capítulo 5 de [4].

Lema 2.3.3 *Dado um subgrupo regular H de automorfismos de um p-grupo P, H é p'-grupo*

A prova do resultado acima é feita por contradição com o seguinte raciocínio, supomos que H possui um S_p-grupo B, então se expõe um subgrupo V de P o qual é abeliano elementar e $C_V(B) \neq 1$, assim temos que $B = 1$ dada a regularidade de H. De onde H é um p'-grupo.

CAPÍTULO 3

Involuções em Grupos de Ordem Ímpar

Dizemos que um automorfismo ϕ é uma involução se ϕ tem ordem dois, isto é, $\phi^2 = Id$ e $\phi \neq Id$. Neste capítulo tratamos da influência das involuções na estrutura dos grupos. De fato o objetivo aqui é mostrar que se ϕ é uma involução de um grupo G de ordem ímpar, tal que a ordem do centraliador de ϕ em G, $C_G(\phi)$, é limitado por m, isto é, $|C_G(\phi)| \leq m$ então temos que G' tem ordem limitado por uma função dependendo somente de m, $|G'|$ é m-limitada. Para tanto, apresentamos primeiramente alguns resultados que usamos como ferramentas na demonstração do resultado acima.

3.1 Propriedades dos Grupos de Ordem Ímpar que Admitem uma Involução e a Importância do Subgrupo $[G,\phi]$

Definição 3.1.1 *Temos que $G_{-\phi}$ é o subconjunto de G que contém todos os elementos g, tais que a imagem de g pelo automorfismo ϕ é seu inverso, isto é,*

$$G_{-\phi} = \{g \in G | g^{\phi} = g^{-1}\}.$$

Definição 3.1.2 *H^G é o fecho normal de H, definido como a interseção de todos os subgrupos normais de G que contêm H, isto é,*

$$H^G = \left\langle \{x^{-1}Hx | x \in G\} \right\rangle.$$

Uma parte do primeiro item do lema a seguir se tem do Lema 2.3.1, o lema a seguir é a reunião de vários resultados enunciados em [17, 18].

Lema 3.1.3 *Seja G um grupo finito de ordem ímpar, admitindo um automorfismo ϕ de ordem 2. Então, tem-se que*

1. *Se N é um subgrupo normal ϕ-invariante de G, temos que $(G/N)_\phi = G_\phi N/N$,*

   e $(G/N)_{-\phi} = \{gN | g \in G_{-\phi}\}$.

2. *$G = G_\phi G_{-\phi} = G_{-\phi}G_\phi$, e o subgrupo gerado por $G_{-\phi}$ é exatamente $[G,\phi]$.*

3. *Seja G um grupo finito de ordem ímpar, admitindo um automorfismo ϕ de ordem 2, e se N é um subgrupo normal ϕ-invariante de G, tal que $N = N_{-\phi}$. Então $N \subseteq Z([G,\phi])$*

4. *$G' \subseteq \{G_\phi\}^G$. Se G_ϕ é nilpotente de classe c, então $[G,\phi]$ contém $\gamma_{c+1}(G)$.*

5. *G_ϕ normaliza o conjunto $G_{-\phi}$.*

Demonstração.

1. A primeira parte deste item se reduz à aplicação do Lema 2.3.1 item (1). Basta então provar que $G/N_{-\phi} = \{gN | g \in G_{-\phi}\}$, verificando a dupla inclusão. Temos, que a verificação de que $G/N_{-\phi} \supset \{gN | g \in G_{-\phi}\}$ segue por definição. Agora para obter que $G/N_{-\phi} \subset \{gN | g \in G_{-\phi}\}$, seja $gN \in G/N_{-\phi}$, então $(gN)^\phi = g^{-1}N$. Devemos verificar que pelo menos um dos elementos de gN pertence a $G_{-\phi}$. Seja $gN = \{gn_0, gn_1, ..., gn_l\}$, onde $n_0 = e$ e $n_i \in N$, para todo $i = 0, ..., l$.

   Temos que tanto g quanto gn_i pertecem a gN, o que implica que tanto g^{-1}, quanto $(gn_i)^{-1}$ pertecem $g^{-1}N$, de onde temos que $g^{-1}N = \{(gn_0)^{-1}, (gn_1)^{-1}, ..., (gn_l)^{-1}\}$.

   Podemos olhar o automorfismo ϕ na classe lateral gN como sendo uma permutação dos índices dos elementos de N ($l+1$ elementos), isto é, $\phi(gn_i) = (gn_j)^{-1}$ assim para não sobrecarregar a leitura identificamos a igualdade anterior como $\phi(i) = j$ com $i, j \in S = \{x \in \mathbb{N} | 0 \leq x \leq l\}$. Assim, $gN \in \{gN | g \in G_{-\phi}\}$ é equivalente a ter que $\phi(i) = i$ para algum $i = 0, ..., l$.

Dado que $|G| = 2n+1$ para algum $n \in \mathbb{N}$, temos que a ordem de N também é ímpar ($|N| = |S| = l+1$, onde $l = 2k$, para algum $k \in \mathbb{N}$). A permutação ϕ tem a propriedade adicional de que se $\phi(i) = j$, então $\phi(j) = i$. De fato, como ϕ é uma involução temos que

$$i = \phi^2(i) = \phi(\phi(i)) = \phi(j).$$

Agora, suponha que $\phi(i) \neq i$, para todo $i = 0,...,l$. Porém, dada a propriedade da permutação exposta acima, temos que ela gera uma partição do conjunto $|S|$ em duas, mas tendo em conta que o conjunto S tem ordem ímpar, esta partição não é possível, logo existe pelo menos um $i \in S$, tal que $\phi(i) = i$, de onde se conclui a prova.

2. Para demonstrar que $G = G_\phi G_{-\phi} = G_{-\phi}G_\phi$, partimos da premissa que $[x,\phi] \in G_{-\phi}$, para todo $x \in G$. Além disso, se tivermos $[x,\phi] = [y,\phi]$

$$\begin{aligned} [x,\phi] = [y,\phi] \quad &\Leftrightarrow \quad x^{-1}x^\phi = y^{-1}y^\phi \quad \Leftrightarrow \quad (xy^{-1})^\phi = xy^{-1} \\ &\Leftrightarrow \quad xy^{-1} \in G_\phi \quad \Leftrightarrow \quad G_\phi x = G_\phi y, \end{aligned}$$

logo $G_{-\phi}$ tem pelo menos o índice de G_ϕ em G ($|G_{-\phi}| \leq [G : G_\phi]$) elementos.

Apresentamos a prova apenas para classes laterais à direita, pois é análoga para classes laterais à esquerda. Sejam $x,y \in G_{-\phi}$. Suponha $G_\phi x = G_\phi y$, então existe $f \in G_\phi$, tal que $x = fy$, logo

$$\begin{aligned} x^\phi = (fy)^\phi \quad &\Rightarrow \quad x^{-1} = fy^{-1} \quad \Rightarrow \quad x = yf^{-1} \\ &\Rightarrow \quad yf^{-1} = fy \quad \Rightarrow \quad f^{-1} = y^{-1}fy. \end{aligned}$$

Da propriedade acima, e fazendo uso das propriedades do automorfismo, temos que

$$\begin{aligned} (f^{-1})^\phi = (y^{-1}fy)^\phi = yfy^{-1} \quad &\Rightarrow \quad y^{-1}fy = yfy^{-1} \\ &\Rightarrow \quad y^{-2}fy^2 = f. \end{aligned}$$

Iterando o processo acima k-vezes chegamos em $y^{-2k}fy^{2k} = f$, para todo $k \in \mathbb{N}$. Particularmente, para $k = n+1$, onde $2n+1 = |G|$, temos que $y^{-1}fy = f$ e $y^{-1}fy = f^{-1}$, logo $f = f^{-1}$, então $f = e$ e temos que $x = y$. Portanto,

$$x = y \Leftrightarrow G_\phi x = G_\phi y.$$

Dos fatos provados acima, a saber $|G_{-\phi}| \leq [G, G_{\phi}]$ e $x = y \Leftrightarrow G_{\phi}x = G_{\phi}y$, obtemos que

$$G = \bigcup_{g\in G} G_{\phi}g \Rightarrow G = \bigcup_{x\in G_{-\phi}} G_{\phi}x.$$

Logo, $G = \{xf | x \in G_{-\phi} e f \in G_{\phi}\}$. Como $G_{\phi}x \neq G_{\phi}y$, concluímos que $G = G_{\phi}G_{-\phi}$.

Para provar que $\langle G_{-\phi}\rangle = [G,\phi]$, mostramos a dupla inclusão. Para a inclusão $\langle G_{-\phi}\rangle \subset [G,\phi]$: seja $x \in G_{-\phi}$, então dado que $[x^{-1},\phi] \in [G,\phi]$ e $[x^{-1},\phi] = x\phi(x^{-1}) = x^2$, temos $x^2 \in [G,\phi]$, usando o fato da ordem de G ser ímpar, temos que $x \in [G,\phi]$ e dessa forma concluímos que $\langle G_{-\phi}\rangle \subset [G,\phi]$. Agora, para provar $\langle G_{-\phi}\rangle \supset [G,\phi]$ tomamos $[x,\phi] \in [G,\phi]$ de onde temos

$$([x,\phi])^{\phi} = (x^{-1}x^{\phi})^{\phi} = (x^{-1})^{\phi}x = (x^{-1}x^{\phi})^{-1} = [x,\phi]^{-1}.$$

Logo $[x,\phi] \in G_{-\phi}$, de onde obtemos que $\langle G_{-\phi}\rangle = [G,\phi]$.

3. Seja $n \in N$ e $g \in G$, temos que $N \subset [G,\phi]$, dado que pelo item dois deste lema o subgrupo gerado por $G_{-\phi}$ é exatamente $[G,\phi]$ e $N \subset G_{-\phi}$, aplicando ϕ no conjugado de n por g temos $(n^g)^{\phi} = (n^g)^{-1}$ por outro lado $(n^g)^{\phi} = (n^{-1})^{g^{\phi}}$, de onde obtemos que $(n^{-1})^g = (n^{-1})^{g^{\phi}}$, assim $g^{-1}n^{-1}g = (g^{-1})^{\phi}n^{-1}g^{\phi}$ e obtemos que $n^{-1} = (g^{\phi})g^{-1}n^{-1}g(g^{-1})^{\phi} = (n^{-1})^{g(g^{-1})^{\phi}} = (n^{-1})^{[g^{-1},\phi]}$, assim concluímos que $N \subseteq Z([G,\phi])$, dado que os elementos da forma $[g^{-1},\phi]$ são os geradores de $[G,\phi]$.

4. Para provar que $G' \subset G_{\phi}^{G}$, é suficiente provar que G/G_{ϕ}^{G} é abeliano. Chamamos $H = G_{\phi}^{G}$, pelo item 2 do presente lema, temos que $G/H = G/H_{\phi}G/H_{-\phi}$, pelo mesmo item temos que $G = G_{-\phi}G_{\phi} = \langle G_{-\phi}\rangle H$, dado que $G_{-\phi} \subseteq \langle G_{-\phi}\rangle$ e $G_{\phi} \subseteq H$. Assim $\dfrac{G}{H}_{\phi} = \dfrac{G_{\phi}H}{H}$, pelo item 1 deste lema, de onde obtemos que $\dfrac{G}{H}_{\phi} = H = 1$, pelo qual $\dfrac{G}{H} = \dfrac{G}{H}_{-\phi}$. Agora, pelo item 3 deste lema,

$$\frac{G}{H} \leq Z\left(\frac{[G,\phi]H}{H}\right) = Z\left(\frac{\langle G_{-\phi}\rangle H}{H}\right) = Z\left(\frac{G}{H}\right),$$

assim provamos que G/H é abeliano.

Agora, para provar que se G_{ϕ} é nilpotente de classe c, então $[G,\phi]$ contém $\gamma_{c+1}(G)$, usamos a Proposição 1.3.3 na definição de série central inferior e temos que:

$$\gamma_{c+1}(G) = \underbrace{[G,...,G]}_{c+1-vezes} = \underbrace{[G_\phi[G,\phi],...,G_\phi[G,\phi]]}_{c+1-vezes} = \underbrace{[G_\phi,...,G_\phi]}_{c+1-vezes}[G,\phi]$$

$$\gamma_{c+1}(G) = [G,\phi],$$

de onde $\gamma_{c+1}(G) \subset [G,\phi]$.

5. Para mostrar que G_ϕ normaliza o conjunto $G_{-\phi}$ é suficiente mostrar que, para todo elemento $g \in G_{-\phi}$, o conjugado de g por qualquer elemento de G_ϕ pertence a $G_{-\phi}$, isto é, provamos que $f^{-1}gf \in G_{-\phi}$ para $f \in G_\phi$ e $g \in G_{-\phi}$, elementos arbitrários. Basta operar o automorfismo ϕ de onde temos que

$$(f^{-1}gf)^\phi = f^{-1}g^{-1}f = (f^{-1}gf)^{-1},$$

logo $f^{-1}gf \in G_{-\phi}$, então G_ϕ normaliza $G_{-\phi}$. ■

Dizemos que dois subconjuntos X,Y de G comutam se $xy = yx$ para todos $x \in X$ e $y \in Y$, equivalentemente temos que $[X,Y] = 1$.

Considerando o item dois do Lema 3.1.3 apresentamos a seguinte definição:

Sejam G um grupo finito de ordem ímpar, ϕ um automorfismo de ordem 2 de G e $X \subseteq G$. Então todo elemento $x \in X$ é em particular um elemento de G pelo qual tem-se que $x = x_\phi x_{-\phi}$, onde $x_\phi \in G_\phi$ e $x_{-\phi} \in G_{-\phi}$, assim podemos obter uma projeção que define de forma intrínseca os seguintes conjuntos:

$$X_\phi = \{x_\phi | x \in X\} \qquad X_{-\phi} = \{x_{-\phi} | x \in X\}.$$

Usando a definição acima obtemos o seguinte resultado, enunciado em [18].

Lema 3.1.4 *Sejam X, Y dois subconjuntos de G, que comutam e assuma que Y é ϕ-invariante. Então X_ϕ e $X_{-\phi}$ comutam com Y.*

Demonstração.
Por hipótese, temos que $X \subset C_G(Y)$, então $\langle X \rangle \leq C_G(Y)$. Além disso, dado que Y é ϕ-invariante, temos que ϕ age sobre Y como uma bijeção, de onde obtemos que para todo $y \in Y$ existe $y' \in Y$, tal que $(y')^\phi = y$. Como X comuta com Y, temos que $xy' = y'x$ e aplicando ϕ nos dois lados da igualdade obtemos $(xy')^\phi = (y'x)^\phi$, de onde temos que $x^\phi y = yx^\phi$,

para todo $y \in Y$, então concluímos que $X^{\phi} \subset C_G(Y)$, logo $\langle X^{\phi} \rangle \leq C_G(Y)$. Das afirmações anteriores obtemos que $\langle X, X^{\phi} \rangle \leq C_G(Y)$. Resta provar que $\langle X_{\phi}, X_{-\phi} \rangle \subset \langle X, X^{\phi} \rangle$ e deste jeito teríamos que $\langle X_{\phi}, X_{-\phi} \rangle \subset C_G(Y)$. Em particular, $X_{\phi} \subset C_G(Y)$ e $X_{-\phi} \subset C_G(Y)$, de onde obteríamos o resultado desejado.

Seja $x_{-\phi} \in X_{-\phi}$, então existe $x \in X$, tal que $x = x_{\phi}x_{-\phi}$, temos também $x^{-1}x^{\phi} \in \langle X, X^{\phi} \rangle$. Mas temos que $x^{-1}x^{\phi} = x_{-\phi}^{-1}x_{\phi}^{-1}x_{\phi}x_{-\phi}^{-1} = x_{-\phi}^{-2}$, o que implica que $x_{-\phi}^{-2}, x_{-\phi}^{2} \in \langle X, X^{\phi} \rangle$. Dada a ordem do grupo (pelo fato de ser ímpar) existe um número $n \in \mathbb{N}$ tal que $(x_{-\phi}^{2})^{n} = x_{-\phi}$, portanto $X, X_{-\phi} \subset C_G(Y)$ de onde $X_{\phi} \subset C_G(Y)$, dado que $X_{\phi} \subset \langle X, X_{-\phi} \rangle$.

Portanto, obtemos a inclusão desejada, a saber $\langle X_{\phi}, X_{-\phi} \rangle \subset \langle X, X^{\phi} \rangle$. ■

O seguinte lema foi enunciado em [18].

Lema 3.1.5 *Sejam $x \in G_{-\phi}$ e $a \in G_{\phi}$ e suponha que $[x, a] \in G_{\phi}$. Então $[x, a] = 1$.*

Demonstração.
Pelas hipóteses, temos que $x^{\phi} = x^{-1}$ e $a^{\phi} = a$, pelo fato de $[a, x] \in G_{\phi}$, temos que $([x, a])^{\phi} = [x, a]$ que é equivalente a falar $(x^{-1}a^{-1}xa)^{\phi} = x^{-1}a^{-1}xa$. Por outro lado, temos $(x^{-1}a^{-1}xa)^{\phi} = xa^{-1}x^{-1}a$ e das duas igualdades obtemos $x^{-1}a^{-1}x = xa^{-1}x^{-1}$. Aplicando o inverso nos dois lados da igualdade obtemos que $x^{-1}ax = xax^{-1}$. Agora, isolando a temos $x^{-2}ax^{2} = a$, e conjugando nos dois lados da igualdade por x obtemos que $(x^{-2}ax^{2})^{x} = a^{x}$, pelo qual $x^{-4}ax^{4} = a$. Iterando o processo concluímos que $x^{-2k}ax^{2k} = a$, para todo $k \in \mathbb{N}$, de onde segue que existe um número natural n adequado, tal que $x^{2n} = x$, dado que a ordem de G é ímpar ($n = r + 1$ onde $|G| = 2r + 1$). Logo $x^{-1}ax = a$, assim, $[x, a] = 1$. ■

O lema anterior mostra alguns resultados em relação à decomposição de G, feita no item 2 do Lema 3.1.3.

3.2 Implicações do Fato de $G = [G, \phi]$(para ϕ uma involução de G)

Nesta seção vemos um resultado que segue do fato do grupo G, o qual tem ordem ímpar, ser igual ao subgrupo $[G, \phi]$, onde ϕ é uma involução. Fazendo uma análise dos resultados anteriores temos que $G = \langle G_{-\phi} \rangle$, de onde obtemos que todo elemento do centralizador do automorfismo ϕ no grupo G pode ser visto como combinação linear de elementos de $G_{-\phi}$.

Lembramos que $[G, \phi] = \langle g^{-1}g^{\phi} | g \in G \rangle$, assim, temos que todo elemento de G pode se ver como combinação linear de elementos da forma $[x, \phi] = x^{-1}x^{\phi}$ ou como combinação linear de elementos de $G_{-\phi}$.

Lema 3.2.1 *Suponha que $G = [G, \phi]$. Seja N um subgrupo normal ϕ-invariante, tal que $N \leq G_{-\phi}$ ou $N \leq G_{\phi}$. Então $N \leq Z(G)$.*

Demonstração.
Vamos provar o lema em duas partes: na primeira parte tomamos $N \leq G_{\phi}$ e na segunda, vamos supor que $N \leq G_{-\phi}$. Para começar suponha $N \leq G_{\phi}$, então $[G, N] \subset N$ pela normalidade de N, logo $[g, n]^{\phi} = [g, n]$. Por outro lado $[g, n]^{\phi} = [g^{\phi}, n^{\phi}] = [g^{\phi}, n]$ de onde obtemos que $[g, n] = [g^{\phi}, n]$, assim

$$g^{-1}n^{-1}g = (g^{\phi})^{-1}n^{-1}g^{\phi} \text{ de onde } n^{-1} = (g^{\phi})g^{-1}n^{-1}g(g^{-1})^{\phi} = (n^{-1})^{g(g^{-1})^{\phi}}.$$

Obtemos então que $g(g^{-1})^{\phi} \in C_G(N)$ para todo $g \in G$. Já que $G = [G, \phi]$ temos que para todo $h \in G$, $h = g^{-1}(g)^{\phi}$ de onde todo $h \in G$ pertence ao centralizador de N, isto é, $C_G(N) = G$ assim $N \leq Z(G)$.
Analogamente, vamos supor que $N \leq G_{-\phi}$, logo $(n^g)^{\phi} = (n^g)^{-1}$, mas por outro lado temos que
$(n^g)^{\phi} = (n^{-1})^{g^{\phi}}$ de onde obtemos que $(n^{-1})^g = (n^{-1})^{g^{\phi}}$, assim

$$g^{-1}n^{-1}g = (g^{-1})^{\phi}n^{-1}g^{\phi} \text{ de onde } n^{-1} = (g^{\phi})g^{-1}n^{-1}g(g^{-1})^{\phi} = (n^{-1})^{g(g^{-1})^{\phi}}.$$

Então, como no caso anterior obtemos que $C_G(N) = G$, então $N \leq Z(G)$. ■

No lema acima vemos como o fato de $G = [G, \phi]$ tem implicações na estrutura dos subgrupos normais ϕ-invariantes de G.

3.3 Consequências da Limitação da Ordem de $C_G(\phi)$ no Grupo G (onde ϕ é uma involução e G é um grupo de ordem ímpar).

Nesta seção tratamos da influência da limitação da ordem do centralizador do automorfismo ϕ no grupo G ($C_G(\phi)$), tanto no índice de subgrupos ϕ-invariantes, como no grupo derivado de G. Tal resultado é um dos principais deste trabalho. A influência da limitação da ordem de $C_G(\phi)$ começou a ser trabalhada por Hartley [6] em 1980 que obtém que: dado um grupo periódico G contendo uma involução ϕ, tal que $|C_G(\phi)| = m$, então G contém um subgrupo nilpotente de classe de nilpotência no máximo 2 e índice menor ou igual a $f(m)$, onde $f(m)$ é uma função que depende só de m.

O mesmo Hartley em [5] (1981) prova que: dado um grupo periódico G contendo uma involução ϕ, tal que $|C_G(\phi)| \leq m < \infty$, então G contém um subgrupo normal, ϕ-invariante e nilpotente, H, de classe de nilpotência no maximo 2 e índice menor ou igual a $f(m)$, onde $f(m)$ é uma função que depende só de m, e $H' \leq G_\phi$.

Shumyatsky, em [16] (1998), estabelece um resultado de limitação nos geradores de G' obtendo que: Sejam p um número primo maior que 2 e G um p-grupo admitindo uma involução ϕ, tal que $G = [G,\phi]$. Assuma que G_ϕ é r-gerado. Então existe um número m r-limitado de forma que G' é m-gerado.

Agora apresentamos um dos teoremas principais desta dissertação, este resultado é enunciado e provado por Shumytsky em [18].

Teorema 3.3.1 *Sejam G um Grupo de ordem ímpar, ϕ um automorfismo de ordem dois e m um inteiro positivo, tal que $|G_\phi| \leq m$. Então,*

1. *G tem um subgrupo normal ϕ-invariante H, tal que $H' \leq G_\phi$ e o índice $[G:H]$ é m-limitado.*
2. *Se $G = [G,\phi]$, então a ordem de G' é m-limitada.*

Demonstração.

1. Assumimos que temos o resultado exposto por Hartley em [6], que diz que G contém um subgrupo L, nilpotente, ϕ-invariante, com classe de nilpotência menor ou igual a 2 e $[G:L] \leq f(m)$.

Definimos $H_1 = [L,\phi]$, então $|H_1| = |[L,\phi]|$. Pelo Item 2 do Lema 3.1.3, temos que $|[L,\phi]| = |L|/|L_\phi|$, de onde $|L|/|L_\phi| \geq |L|/|G_\phi|$. Juntamente com as hipóteses de que $|G_\phi| \leq m$ e $[G:L] \leq f(m)$ obtemos

$$[G:H_1] = [G:[L,\phi]] = \frac{|G|}{|[L,\phi]|} \leq \frac{|G|}{|L|/|G_\phi|} = |G_\phi||[G:L]| \leq mf(m).$$

Além disso, ϕ inverte todos os elementos da forma $[l,\phi]$, pois $([l,\phi])^\phi = (l^{-1}l^\phi)^\phi = (l^\phi)^{-1}l = ([l,\phi])^{-1}$, e H_1' é ϕ-invariante, dado que se $h,j \in H_1$, então

$$([h,j])^\phi = (h^{-1}j^{-1}hj)^\phi = ((h^\phi)^{-1}(j^\phi)^{-1}h^\phi j^\phi) = [h^\phi, j^\phi].$$

Como H_1 é ϕ-invariante segue que $h^\phi, j^\phi \in H_1$, logo $[h^\phi, j^\phi] \in H_1'$.

Temos que H_1/H_1' é abeliano, já que para $h,j \in H_1$, $[h,j] \in H_1$ por definição, então $h^{-1}j^{-1}hj \in H_1'$ pelo qual $h^{-1}j^{-1}H_1' = hjH_1'$. Pelas afirmações anteriores temos que todo elemento de H_1/H_1' é invertido por ϕ, $(hH_1')^\phi = h^\phi H_1' = h^{-1}H_1'$, pois pela comutatividade deduzimos que $\prod_{i=1}^n [h_i,\phi] = [h,\phi]$ $(hH_1')^\phi = h^\phi H_1' = h^{-1}H_1'$.

Sabemos que L é nilpotente com classe de nilpotência menor ou igual a 2, logo $[L',L] = 1$, de onde todo comutador da forma $[l,l_1,l_2]$ é igual a 1, para quaisquer $l,l_1,l_2 \in L$. Em particular, $[L,\phi] \subset L$, pois L é um subgrupo ϕ-invariante. Daí temos que para quaisquer $x,x_1,x_2 \in H_1$ se tem que $x,x_1,x_2 \in L$, logo $[H_1',H_1] = 1$. Assim, dados $x,x_1,\ldots,x_i \in H_1$, a imagem de $[x_1,x_2,\ldots,x_i]\gamma_{i+1}(H_1)$ por ϕ depende só da imagem de $[x_1H_1',x_2H_1',\ldots,x_iH_1']$ de onde concluímos que

$$\begin{aligned}
([x_1,x_2,\ldots,x_i]\gamma_{i+1}(H_1))^\phi &= ([x_1H_1',x_2H_1',\ldots,x_iH_1'])^\phi\gamma_{i+1}(H_1)\\
&= [x_1^{-1}H_1',x_2^{-1}H_1',\ldots,x_i^{-1}H_1']\gamma_{i+1}(H_1)\\
&= [x_1H_1',x_2H_1',\ldots,x_iH_1']^{-1^i}\gamma_{i+1}(H_1).
\end{aligned}$$

Do fato acima temos que ϕ inverte $\gamma_i(H_1)/\gamma_{i+1}(H_1)$ quando i é ímpar e centraliza $\gamma_i(H_1)/\gamma_{i+1}(H_1)$ se i é par. Daí $H_1' \subset G_\phi$. Portanto $H = \bigcap_{x\in G\langle\phi\rangle} H_1^x$ cumpre as condições do primeiro item deste teorema. Dado que, em primeiro lugar H é normal em G, dado que é o kernel do homomorfismo:

$$\begin{array}{rcccccl}
\Pi_{H_1}: & G\langle\phi\rangle & \longrightarrow & S_n & & & \\
& x & \longmapsto & \pi_x: & S & \longrightarrow & S\\
& & & & H_1x_i & \longmapsto & \pi_x(H_1x_i) = H_1x_ix.
\end{array}$$

H é nilpotente, dado que é subgrupo de H_1 motivo pelo qual, temos que $H' \subset G_\phi$, por último temos que $[G:H] \leq g(m)$ dado que $[G:H_1] \leq f(m)m$ e $[G:H\cap K] \leq [G:H][G:K]$, assim $[G:H] \leq [G:H_1]^2 = g(m)$.

2. Para provar o item dois, usamos indução sobre m. Seja H o subgrupo obtido no item 1. Dado que a classe de nilpotência de H é menor ou igual a 2, temos duas possibilidades:

   Caso1: Suponha que $H' \neq 1$, então o resultado segue para G/H', e além disso:

$$\begin{aligned}(G/H')' &= \{[aH', bH'] | a, b \in G\} \\ &= \{[a^{-1}b^{-1}abH'] | a, b \in G\} \\ &= G'/H'.\end{aligned}$$

   Logo, obtemos que $|G'| = |G'/H'||H'| \leq f(m)m = g(m)$.

   Caso2: Seja $H' = 1$, então temos que H é abeliano. Definamos $M = H \cap G_\phi$ e seja $N = \langle M^G \rangle$. Logo, temos que $M \subset G_\phi$, portanto $|M| \leq |G_\phi| \leq m$. Além disso, $[G:C_G(M)] \leq f(m)$, dado que $M \subset H$ e H é abeliano, de onde $H \subset C_G(M)$, o que implica que

$$|G|/|C_G(M)| \leq |G|/|H| = [G:H] \leq f(m).$$

   H é abeliano pelo qual M também é abeliano, assim $M \subset C_G(M) \trianglelefteq G$, então $|N|$ é limitada, dado que temos a limitacao de a ordem de M e do índice $[G:C_G(M)]$ e o fato adicional que $M^c = M$ para todo $c \in C_G(M)$. Com isso se $|N| \neq 1$ posso usar a hipótese de indção para o grupo G/N e obtemos que $|G'| = |G'/N||N|$, mas dado que $|G'/N|$ é limitado (pela hipótese de indução), e $|N|$ também pelo argumento anterior, então teriamos o resultado, pelo qual suponha que $N = 1$, então $H \cap G_\phi = 1$, assim $H \subset G_{-phi}$ pelo Lema 3.2.1 $H \leq Z(G)$. Então $[G:Z(G)]$ é m-limitado e usando o Teorema de Schur obtemos o resultado desejado (o teorema de Shur da a seguinte implicação: $[G:Z(G)] = n \Rightarrow |G'| \leq n$[1]) ■

[1] A prova deste teorema encontra-se em [10] e basea-se na construção de um homomorfismo que leve g em g^n.

CAPÍTULO 4

O Subgrupo $\rho_x^{\phi}(L)$

A seguir definimos um subgrupo do grupo G, de particular importância no desenvolvimento do presente capítulo.

Definição 4.0.2 *Dado um elemento $x \in G$ e um subconjunto $L \subseteq G$, denotamos por $\rho_x^{\phi}(L)$ o menor subgrupo ϕ-invariante de G que contém $x^{-1}Lx$. Dados vários elementos $x_1, \ldots, x_k \in G$, definimos indutivamente*

$$\rho^{\phi}_{x_1,\ldots,x_k}(L) = \rho^{\phi}_{x_k}(\rho^{\phi}_{x_1,\ldots,x_{k-1}}(L)).$$

As próximas seções contém lemas que são resultados em prol de demostrar o seguinte resultado, exposto e provado em [18]:

Teorema 4.2.3 Suponhamos que $G = [G, \phi]$ e $|C_G(\phi)| \leq m$. Seja $G\langle\phi\rangle$ atuando fiel e irredutivelmente em um p-grupo abeliano V, onde p é um primo ímpar. Então existe uma constante k, m-limitada, e elementos $x_1, \ldots, x_k \in G_{-\phi}$, tal que $V = \rho^{\phi}_{x_1,\ldots,x_k}(V_{-\phi})$.
O grupo abeliano V resulta ser p-grupo abeliano elementar, como será demonstrado no Lema 4.2.1 na frente.

No presente capítulo falamos do grupo $G\langle\phi\rangle$ como sendo o produto semidireto do grupo G pelo subgrupo $\langle\phi\rangle$ do grupo de automorfismo de G ($G\langle\phi\rangle = G \ltimes \langle\phi\rangle$), onde a operação entre os elementos de $G\langle\phi\rangle$ é dada por,

$$\begin{array}{rccc} \cdot : & G\langle\phi\rangle \times G\langle\phi\rangle & \longrightarrow & G\langle\phi\rangle \\ & (g,\phi^i)(\bar{g},\phi^j) & \longmapsto & (g,\phi^i)\cdot(\bar{g},\phi^j) = (g\bar{g}^{\phi^i},\phi^{i+j}). \end{array}$$

O fato da representação ser fiel quer dizer que é injetiva, como definimos na seção 1.2. E o fato de ser irredutível diz que só 0 e V são subespaços invariantes pela representação (só 0 e V são $G\langle\phi\rangle$-submódulos de V visto como $G\langle\phi\rangle$-módulo), como também definimos na seção 1.2.

4.1 Influência de G_ϕ e $G_{-\phi}$ em $\rho_x^\phi(L)$

A continuação, mostramos algumas proposições importantes para desenvolver as demostrações dos resultados deste capítulo.

Proposição 4.1.1 *Dado L um subgrupo abeliano, normal, ϕ-invariante de G e $x \in G_{-\phi}$, então temos que*

$$\left\langle x^{-1}Lx, (x^{-1}Lx)^\phi \right\rangle = \rho_x^\phi(L).$$

Demonstração.
Dado que $\rho_x^\phi(L)$ foi definido como o menor subgrupo de G que contém $x^{-1}Lx$ e é ϕ-invariante, além disso, temos que $x^{-1}Lx \subset \langle x^{-1}Lx, (x^{-1}Lx)^\phi \rangle$, nosso objetivo então é mostrar que $\langle x^{-1}Lx, (x^{-1}Lx)^\phi \rangle$ é ϕ-invariante, além disso que para todo $H \leq G$, tal que H é ϕ-invariante e $x^{-1}Lx \subset H$, temos $(x^{-1}Lx)^\phi \subset H$. Então fica mostrado que $\langle x^{-1}Lx, (x^{-1}Lx)^\phi \rangle = \rho_x^\phi(L)$.

O fato que $\langle x^{-1}Lx, (x^{-1}Lx)^\phi \rangle$ é ϕ-invariante resulta imediato da ordem de ϕ. Basta ver que dados dois geradores $k \in x^{-1}Lx$ e $f \in (x^{-1}Lx)^\phi$, temos que as imagens pelo automorfismo ϕ desses elementos pertecem a $\langle x^{-1}Lx, (x^{-1}Lx)^\phi \rangle$. Note que $k^\phi \in (x^{-1}Lx)^\phi$, e $f^\phi = ((k_0)^\phi)^\phi$, para algum $k_0 \in x^{-1}Lx$, dado que $f \in (x^{-1}Lx)^\phi$, mas como ϕ é uma involução, então $f^\phi = (k_0^\phi)^\phi = k_0$, onde $k_0 \in x^{-1}Lx$, pelo qual fica provado que $\langle x^{-1}Lx, (x^{-1}Lx)^\phi \rangle$ é ϕ-invariante.

Só resta provar que, para todo $H \leq G$, tal que H é ϕ-invariante e $x^{-1}Lx \subset H$, então $(x^{-1}Lx)^\phi \subset H$, o que é obtido do fato de H ser ϕ-invariante, de onde $H^\phi \subset H$ e, em particular, como $x^{-1}Lx \subset H$, logo $(x^{-1}Lx)^\phi \subset H$. Assim, concluímos a prova da Proposição.

$\blacksquare$

Lema 4.1.2 *Seja L um subgrupo abeliano, normal, ϕ-invariante de G e $x \in G_{-\phi}$. Então $\rho_x^\phi(L_{-\phi})$ contém $L_{-\phi}$.*

Demonstração.
Seja $K = x^{-1}L_{-\phi}x$. K é um subconjunto de L (dada a normalidade de L), temos que definindo:

$$\begin{array}{rrcl} \pi_1: & L = L_\phi L_{-\phi} & \longrightarrow & L_\phi = L/L_{-\phi} \\ & g = g_\phi g_{-\phi} & \longmapsto & \pi_1(g) = g_\phi. \end{array}$$

$$\begin{array}{rrcl} \pi_2: & L = L_\phi L_{-\phi} & \longrightarrow & L_\phi = L/L_{-\phi} \\ & g = g_\phi g_{-\phi} & \longmapsto & \pi_2(g) = g_{-\phi}. \end{array}$$

Onde π_1, π_2 são as projeções canônicas de L a L_ϕ e $L_{-\phi}$ respectivamente definidas intrinsecamente pelo item 2 do Lema 3.1.3, assim, temos que:

$$K_\phi = \{k_\phi \in L_\phi | \quad \exists k \in K, \quad \text{tal que} \quad k = k_\phi k_{-\phi} \quad (k_{-\phi} \in L_{-\phi})\},$$

o que resulta ser equivalente a dizer que $K_\phi = \pi_1(K)$.
Do mesmo modo, seja

$$K_{-\phi} = \{k_{-\phi} \in L_{-\phi} | \ \exists k \in K \quad \text{tal que} \ \ k = k_\phi k_{-\phi} \ \ (k_\phi \in L_\phi)\},$$

ou seja, $K_{-\phi} = \pi_2(K)$.

Então $K \subset \langle K_\phi, K_{-\phi} \rangle$ e $\langle K_\phi, K_{-\phi} \rangle$ é ϕ-invariante pelo fato de que

$$\langle K_\phi, K_{-\phi} \rangle = \{\prod_{i=1}^{n} (k_i)_\phi^{\alpha_i} (k_i)_{-\phi}^{\beta_i} \ | \ (k_i)_\phi \in G_\phi (k_i)_{-\phi} \in G_{-\phi}\},$$

de onde basta ver como age o automorfismo ϕ sobre um elemento deste tipo,

$$(\prod_{i=1}^{n} (k_i)_\phi^{\alpha_i} (k_i)_{-\phi}^{\beta_i})^\phi = \prod_{i=1}^{n} ((k_i)_\phi^{\alpha_i})^\phi ((k_i)_{-\phi}^{\beta_i})^\phi = \prod_{i=1}^{n} (k_i)_\phi^{\alpha_i} (k_i)_{-\phi}^{-\beta_i}.$$

O resultado acima deixa claro que $\langle K_\phi, K_{-\phi} \rangle$ é ϕ-invariante, então $\rho_x^\phi(L_{-\phi}) \subset \langle K_\phi, K_{-\phi} \rangle$.

Agora, para provar a outra inclusão ($\langle K_\phi, K_{-\phi} \rangle \subset \rho_x^\phi(L_{-\phi})$) levemos em conta a seguinte igualdade:

$$\left\langle x^{-1}Lx, (x^{-1}Lx)^\phi \right\rangle = \rho_x^\phi(L).$$

Usando o resultado exposto na Proposição (4.1.1) para $L_{-\phi}$, observamos que provar a última inclusão, resulta equivalente a provar que $\langle K_\phi, K_{-\phi} \rangle \subset \langle K, K^\phi \rangle$. Para isso tomamos dois elementos de $\langle K_\phi, K_{-\phi} \rangle$,um de cada conjunto gerador, isto é, $x_\phi \in K_\phi$ e $y_{-\phi} \in K_{-\phi}$. Então, pelas definições de K_ϕ e $K_{-\phi}$, temos que existem $x, y \in K$, tais que $x = x_\phi x_{-\phi}$ e $y = y_\phi y_{-\phi}$, logo $xx^\phi = x_\phi x_{-\phi} x_\phi x_{-\phi}^{-1}$ e, dado que $x_\phi, x_{-\phi}, y_\phi, y_{-\phi} \in L$, por definição de K_ϕ e $K_{-\phi}$, e eles comutam pela hipótese de L ser comutativo, o que implica que $xx^\phi = x_\phi^2$, logo

$x_\phi^2 \in \langle K, K^\phi \rangle$, e sendo que a ordem do grupo G e a de L são ímpares, então temos que $x_\phi \in \langle K, K^\phi \rangle$.

Agora, de forma análoga temos que $y(y^\phi)^{-1} = y_\phi y_{-\phi} y_{-\phi} y_\phi^{-1} = y_{-\phi}^2$, pelo mesmo argumento da comutatividade de L, segue que $y_{-\phi}^2 \in \langle K, K^\phi \rangle$, e $y_{-\phi} \in \langle K, K^\phi \rangle$.

Com as duas afirmações acima fica demostrado que $\langle K_\phi, K_{-\phi} \rangle \subset \langle K, K^\phi \rangle = \rho_x^\phi(L_{-\phi})$.

Se provarmos que $K_{-\phi} = L_{-\phi}$ teriamos que $L_{-\phi} = K_{-\phi} \subset \langle K_\phi, K_{-\phi} \rangle = \rho_x^\phi(L_{-\phi})$, com o que chegaríamos na tese exposta no lema.

Provar que $K_{-\phi} = L_{-\phi}$ é equivalente a provar que $K_{-\phi} \subset L_{-\phi}$ e $|K_{-\phi}| \geq |L_{-\phi}|$ [1]

Podemos verificar a inclusão mencionada, pois $K_{-\phi} = \pi_2(K) \subset \pi_2(L) = L_{-\phi}$.

Agora a prova de que $|K_{-\phi}| \geq |L_{-\phi}|$ é feita por contradição. Suponha $|K_{-\phi}| < |L_{-\phi}|$, então existem $l_1, l_2 \in L_{-\phi}$ distintos, tais que $\pi_2(x^{-1}l_1x) = \pi_2(x^{-1}l_2x)$, onde π_2 é a forma geral da segunda projeção canônica sobre todo o grupo L.

Fazendo um parênteses na prova temos o seguinte resultado: Dados dois elementos $g, \bar{g} \in G$, tais que as suas segundas projeções coincidem (a projeção canônica com respeito ao automorfismo dado pelo Lema 3.1.3), isto é, $g = g_\phi g_{-\phi}$ e $\bar{g} = \bar{g}_\phi g_{-\phi}$, então $\bar{g}g^{-1} = \bar{g}_\phi g_\phi^{-1}$, logo $\bar{g}g^{-1} \in G_\phi$.

Aplicando o resultado acima a $x^{-1}l_1x$ e $x^{-1}l_2x$, temos que

$x^{-1}l_1x \cdot (x^{-1}l_2x)^{-1} = x^{-1}l_1x \cdot (x^{-1}l_2^{-1}x) = x^{-1}l_1l_2^{-1}x$ pertece a L_ϕ, o que implica que $(x^{-1}l_1l_2^{-1}x)^\phi = x^{-1}l_1l_2^{-1}x$. Por outro lado, operando o automorfismo diretamente e usando as hipóteses que $x \in G_{-\phi}$, $l_1, l_2 \in L_{-\phi}$ e propriedades de automorfismo, obtemos que $(x^{-1}l_1l_2^{-1}x)^\phi = xl_1^{-1}l_2x^{-1}$, logo $x^{-1}l_1l_2^{-1}x = xl_1^{-1}l_2x^{-1}$, de onde $l_1l_2^{-1} = x^2l_1^{-1}l_2x^{-2}$.

Agora, retomando a prova do lema, temos que como $x^{-1}l_1l_2^{-1}x = xl_1^{-1}l_2x^{-1}$, pela Proposição 1.5.8 temos que $l_1l_2^{-1} = e$, logo $l_1 = l_2$, o que é uma contradição.

[1] Observemos que. Quando falamos do conjunto K, o $K_{-\phi}$ é a segunda projeção de K, $\pi_2(K)$, como se viu no começo dessa demonstração. Agora, quando falamos do subgrupo ϕ-invariante L, o $L_{-\phi}$ faz alusão ao conjunto dos elementos em L que são levados no seu inverso pelo automorfismo ϕ, isto é, $L_{-\phi} = \{l \in L | l^\phi = l^{-1}\}$, só que dado o item 2 do Lema 3.1.3 $L = L_\phi L_{-\phi}$ o conjunto $L_{-\phi}$ coincide com a segunda projeção de L, $\pi_2(L)$, onde essa projeção é definida de forma análoga à definida para K.

Portanto $|k_{-\phi}| \geq |L_{-\phi}|$, e chegamos na conclusão desejada, a saber $k_{-\phi} = L_{-\phi}$. Com o que obtemos $L_{-\phi} = K_{-\phi} \subset \langle K_\phi, K_{-\phi}\rangle = \rho_x^\phi(L_{-\phi})$ e se conclui a prova. ■

Lema 4.1.3 *Seja $x \in G_{-\phi}$ e $H \leq G_\phi$. Então $(H^x)_\phi$ possui ao menos o mesmo número de elementos de H, isto é, $|(H^x)_\phi| \geq |H|$.*

Demonstração.
Fazemos esta demonstração por contradição.

Suponha que $|(H^x)_\phi| < |H|$, então existem $h_1, h_2 \in H$ distintos, tais que $(x^{-1}h_2x) = g_\phi g_{-\phi}$ e $(x^{-1}h_1x) = g_\phi \bar{g}_{-\phi}$, assim $g^{-1}\bar{g} = g_{-\phi}^{-1}\bar{g}_{-\phi}$.
Temos que $(x^{-1}h_2^{-1}x)(x^{-1}h_1x) = x^{-1}h_2^{-1}h_1x = g_{-\phi}^{-1}\bar{g}_{-\phi}$, então $h_2^{-1}h_1 = xg_{-\phi}^{-1}\bar{g}_{-\phi}x^{-1}$ que pertence a G_ϕ, isto é, $xg_{-\phi}^{-1}\bar{g}_{-\phi}x^{-1} \in G_\phi$ dado que $h_1, h_2 \in H$ e por hipótese $H \subset G_\phi$. Por um lado obtemos que $(xg_{-\phi}^{-1}\bar{g}_{-\phi}x^{-1})^\phi = xg_{-\phi}^{-1}\bar{g}_{-\phi}x^{-1}$ e por outro, fazendo a operação do automorfismo diretamente, baseados no fato que $x, g_{-\phi}^{-1}, \bar{g}_{-\phi} \in G_{-\phi}$, obtemos que $(xg_{-\phi}^{-1}\bar{g}_{-\phi}x^{-1})^\phi = x^{-1}g_{-\phi}\bar{g}_{-\phi}^{-1}x$, então $x^{-1}g_{-\phi}\bar{g}_{-\phi}^{-1}x = xg_{-\phi}^{-1}\bar{g}_{-\phi}x^{-1}$ de onde, pela Proposição 1.5.8, chegamos a $g_{-\phi}\bar{g}_{-\phi}^{-1} = e$, assim $g_{-\phi} = \bar{g}_{-\phi}$, assim $(x^{-1}h_2x) = (x^{-1}h_1x)$, logo $h_1 = h_2$, o que é uma contradição.

Então $|(H^x)_\phi)| \geq |H|$ como se desejava. ■

Do resultado acima somado com os fatos que $|H^x| = |H|$ e $|(H^x)_\phi| \leq |H^x|$, obtemos que $|(H^x)_\phi| = |H|$.

Lema 4.1.4 *Seja L um subgrupo abeliano, normal e ϕ-invariante de G e $x \in G_{-\phi}$. Suponha que $C_L(x) = 1$. Então $\rho_x^\phi(L_{-\phi}) = L$.*

Demonstração.
Usando a notação do Lema 4.1.2, e tendo em conta que o resultado do mesmo lema é aplicável aqui, dado que as hipóteses coincidem, é suficiente mostrar que $K_\phi = L_\phi$, dado que $L = \langle L_\phi, L_{-\phi}\rangle$ pelo item dois do Lema 3.1.3 aplicado a L.
Temos que $L_{-\phi} \subset L$, pois L é ϕ-invariante e $L_{-\phi} = \{l \in L | l^\phi = l^{-1}\} = \pi_2(L)$ de acordo com o Lema 4.1.2, de onde obtemos que $K = x^{-1}L_{-\phi}x \subset x^{-1}Lx$. Pela normalidade de L, concluímos que $K = x^{-1}L_{-\phi}x \subset x^{-1}Lx = L$. Juntando este fato à definição de K_ϕ e $K_{-\phi}$ obtemos que $K_\phi \subset L_\phi$ e $K_{-\phi} \subset L_{-\phi}$. Resta provar então que $|K_\phi| \geq |L_\phi|$, para obtermos a igualdade desejada ($K_\phi = L_\phi$). Fazemos esta prova por contradição.

Suponha $|K_\phi| < |L_\phi|$, então, temos duas cituações, ou existem $l_1, l_2 \in L_{-\phi}$ diferentes, tais que $\pi_1(x^{-1}l_1x) = \pi_1(x^{-1}l_2x)$ que chamamos Caso 1 ou $|L_{-\phi}| < |L_\phi|$ que chamamos Caso 2.

A divisão nos dois casos acima expostos é o resultado da análise dos seguintes fatos:

Observemos que ao comparar a ordem de $L_{-\phi}$ com a ordem de L_ϕ temos duas possibilidades: $|L_{-\phi}| < |L_\phi|$ ou $|L_{-\phi}| \geq |L_\phi|$. Uma das opções já corresponde com um dos casos (a saber $|L_{-\phi}| < |L_\phi|$ Caso2). Agora, tendo em conta que $L_{-\phi} = K_{-\phi}$ pelo Lema 4.1.2 e $|L_{-\phi}| = |K| = |(L_{-\phi})^x|$ temos que $|L_{-\phi}| \geq |L_\phi|$ é equivalente a dizer que $|K| \geq |L_\phi|$. Temos, além disso, que $|K| \geq |K_\phi|$ e a desigualdade é estrita, isto é, $|K| > |K_\phi|$ se, e somente se, existem $k, \bar{k} \in K$ diferentes, tais que $\pi_1(k) = \pi_1(\bar{k})$ o que resulta equivalente a dizer que existem $l_1, l_2 \in L_{-\phi}$ diferentes, tais que $\pi_1(x^{-1}l_1x) = \pi_1(x^{-1}l_2x)$, que é o Caso 1. Estas observações justificam, a divisão nos casos mencionados.

Caso 1 Por um raciocínio análogo ao feito na Proposição 1.5.8, temos que $k\bar{k}^{-1} = k_{-\phi}\bar{k}_{-\phi}^{-1}$, de onde $k\bar{k}^{-1} \in L_{-\phi}$ dado que $L_{-\phi}$ é fechado para a soma pelo fato de L ser abeliano. Portanto, temos que $(x^{-1}l_1x)(x^{-1}l_2x)^{-1} \in L_{-\phi}$ e então $x^{-1}l_1l_2^{-1}x \in L_{-\phi}$, o que implica que, por um lado $(x^{-1}l_1l_2^{-1}x)^\phi = x^{-1}l_1^{-1}l_2x$ (pela comutatividade de L), por outro lado $(x^{-1}l_1l_2^{-1}x)^\phi = xl_1^{-1}l_2x^{-1}$, então $x^{-1}l_1^{-1}l_2x = xl_1^{-1}l_2x^{-1}$. Logo, $x^{-2}l_1^{-1}l_2x^2 = l_1^{-1}l_2$ e conjugando iteradamente em ambos os lados da igualdade, um número apropriado de vezes, temos que $x^{-1}l_1^{-1}l_2x = l_1^{-1}l_2$, então $l_1^{-1}l_2x = xl_1^{-1}l_2$. Assim, $l_1^{-1}l_2$ pertece ao centralizador de x em L, ou seja, $l_1^{-1}l_2 \in C_L(x)$, mas pela hipótese, temos que $C_L(x) = e$, logo $l_1 = l_2$, o que é uma contradição.

Caso 2 Em primeiro lugar, verificamos a seguinte implicação: Se $|L_{-\phi}| < |L_\phi|$, então $L_\phi \cap x^{-1}L_\phi x \neq 1$. Provamos esta última afirmação por contradição. Suponha que $L_\phi \cap x^{-1}L_\phi x = 1$, então dado que $L_\phi \subset L$ e $x^{-1}L_\phi x \subset L$ temos que $L_\phi(x^{-1}L_\phi x) \subset L$. Agora pela suposição, temos que $|L_\phi(x^{-1}L_\phi x)| = |L_\phi||(x^{-1}L_\phi x)|/L_\phi \cap x^{-1}L_\phi x = |L_\phi||(x^{-1}L_\phi x)| = |L_\phi|^2$, dado que $|L_\phi| = |(x^{-1}L_\phi x)|$. Pelo item 2 do Lema 3.1.3, chegamos a $L = L_\phi L_{-\phi}$ e pela definição dos subgrupos L_ϕ e $L_{-\phi}$ o elemento 1 é o único elemento pertencente à interseção dos mencionados subgrupos,isto é $L_\phi \cap L_{-\phi} = 1$, daí $|L| = |L_\phi||L_{-\phi}|$, e pela hipótese temos que $|L| < |L_\phi|^2$. Das desigualdades acima, temos que $|L| < |L_\phi||(x^{-1}L_\phi x)|$, o que é uma contradição, dado que $L_\phi(x^{-1}L_\phi x) \subset L$. Portanto, temos que $L_\phi \cap x^{-1}L_\phi x \neq 1$.

Agora, dado que $L_\phi \cap x^{-1}L_\phi x \neq 1$ podemos tomar $a \neq 1$, tal que $a \in L_\phi \cap x^{-1}L_\phi x$. Então, como $a \in x^{-1}L_\phi x$, existe $b \neq 1$, $b \in L_\phi$, tal que $a = x^{-1}bx$, de modo que $b^{-1}x^{-1}bx \in L_\phi$. Isso equivale a dizer que $[b,x] \in L_\phi$, logo, temos também que $[x,b] \in G_\phi$, o que nos dá as hipóteses do Lema 3.1.5, de onde obtemos que $[x,b] = 1$. Logo $b \in C_L(x)$, o qual é uma contradição, dado que o centralizador de x em L é trivial.

Como nos dois casos chegamos numa contradição, temos que $K_\phi \geq L_\phi$, o que implica que $K_\phi = L_\phi$, de onde obtemos que $\langle K_\phi, K_{-\phi}\rangle = \langle L_\phi, L_{-\phi}\rangle$, o que equivale à igualdade desejada, a saber $\rho_x^\phi(L_{-\phi}) = L$. ■

Lema 4.1.5 *Seja L um subgrupo ϕ-invariante de G e $x \in G_{-\phi}$. Suponha que a ordem de $\rho_x^\phi(L)$ é igual à ordem de L. Então x normaliza L.*

Demonstração.
Pela Proposisão 4.1.1, temos que $\langle x^{-1}Lx, (x^{-1}Lx)^\phi\rangle = \rho_x^\phi(L)$. Por hipótese, temos que $|L| = |\rho_x^\phi(L)| = |x^{-1}Lx|$, então o único subgrupo que contém $x^{-1}Lx$ e tem a mesma ordem que ele, é ele mesmo, o que implica que ele é ϕ-invariante. Logo, temos que $x^{-1}Lx = (x^{-1}Lx)^\phi = xLx^{-1}$, de onde obtemos que $x^{-2}Lx^2 = L$ e, dado que a ordem de G é ímpar temos que $x^{-1}Lx = L$, como queriamos provar. ■

4.2 Ação Fiel e Irredutível de $G\langle\phi\rangle$ Sobre um p-grupo Abeliano

Agora passamos ao resultado principal desse capítulo, que é mostrar o seguinte teorema que como já temos falado é provado em [18]:

Teorema 4.2.3 Suponha que $G = [G, \phi]$ e $|C_G(\phi)| \leq m$. Seja $G\langle\phi\rangle$ atuando fiel e irredutivelmente num p-grupo abeliano V, onde p é um primo ímpar. Então existe uma constante k, m-limitada e elementos $x_1, \ldots x_k \in G_{-\phi}$, tal que $V = \rho_{x_1,\ldots,x_k}^\phi(V_{-\phi})$.

Os lemas das seções anteriores são as principais ferramentas para desenvolvermos a demonstração do resultado exposto acima.

Relembremos que podemos fazer uma identificação do automorfismo ϕ com sua imersão canônica no produto semidireto $G\langle\phi\rangle$, isto é, $(1,\phi)$. Deste jeito, o automorfismo age sobre o grupo V, mas não conhecemos a forma explícita da ação.

Sabemos também que todo grupo abeliano pode ser visto como um módulo sobre o anel dos inteiros, logo a afirmação de $G\langle\phi\rangle$ agir irredutivelmente sobre V faz sentido, dado que as ações irredutíveis só estão definidas para um grupo agindo sobre um módulo.

Ainda mais, se um grupo G age fiel e irredutivelmente sobre um p-grupo abeliano V, implica que V é abeliano elementar, como mostra o seguinte lema:

Lema 4.2.1 *Sejam G um grupo e V um p-grupo abeliano, tal que G age fiel e irredutivelmente sobre V. Então V é abeliano elementar.*

Demonstração.
Seja ψ a representação da ação de G em V isto é,

$$\begin{array}{rccccccc} \psi: & G & \longrightarrow & Aut(V) & & & \\ & g & \longmapsto & \psi_g: & V & \longrightarrow & V \\ & & & & v & \longmapsto & \psi_g(v), \end{array}$$

agora, ψ é injetiva dado que a ação é fiel. O Teorema de isomorfismo garante que $G \cong K$, onde $K = Img(\psi) \leq Aut(V)$, por outro lado a ação é irredutível, logo os únicos subgrupos G-invariantes de V são 1 e V, assim seja $H = \{x \in V | x^p = 1\}$. Temos que H é não vazio pelo teorema de Cauchy [9], e além disso, é sempre característico no p-grupo V, logo é G-invariante, dado que todo elemento do grupo age como automorfismo em V, assim concluímos que $H = V$, pela irredutivilidade da ação. Portanto, V é abeliano elementar.

■

Proposição 4.2.2 *Seja G grupo de ordem ímpar ($|G| = 2k+1$), V um p-grupo abeliano elementar, $\phi \in Aut(G)$, tal que $|\phi| = 2$, $G = [G,\phi]$, e $G\langle\phi\rangle$ age fiel e irredutivelmente sobre V. Dado $c \in Z(G)$ e $v_0 \in C_V(c)$, então $v_0^\phi \in C_V(c)$, equivalentemente $(v_0^c)^\phi = (v_0^\phi)^c$.*

Demonstração.
Pretendo provar que $c^\phi = c^{-1}$, assim obteria que,

$$v_0^\phi = (v_0^c)^\phi = (c^{-1}v_0c)^\phi = v_0^{c^\phi} = (v_0^\phi)^{c^{-1}}$$

a ideia para obter que $c^\phi = c^{-1}$ é provar que $c = [g,\phi]$ para algum elemento $g \in G$ como se prova a seguir.

Lembremos que $G = [G,\phi] = G_\phi G_{-\phi}$ por hipótese e resultados anteriores, então

$$c = \prod_{i=1}^{n} [x_i, \phi],$$

provamos que $c = [g,\phi]$ por indução sobre n, a base da indução é trivial, dado que se $n = 1$, então $c = [x_1,\phi]$. Suponha que se tem para l. Seja $n = l+1$, então

$$c = \prod_{i=1}^{l+1}[x_i,\phi] = \prod_{i=1}^{l}[x_i,\phi][x_{l+1},\phi] = [x,\phi][x_{l+1},\phi].$$

Pela hipótese de indução.

Basta provar então que se $c = [x,\phi][y,\phi]$, então existe $z \in G$, tal que $c = [z,\phi]$.

Suponha $c = [x,\phi][y,\phi]$ e seja $x = x_\phi x_{-\phi}$ e $y = y_\phi y_{-\phi}$ onde $x_\phi, y_\phi \in G_\phi$ e $x_{-\phi}, y_{-\phi} \in G_{-\phi}$, dado que $x^{-1} = x_{-\phi}^{-1}x_\phi^{-1}$ e $x^\phi = x_\phi x_{-\phi}^{-1}$ junto com a suposição acima, temos que

$$c = [x,\phi][y,\phi] = x^{-1}x^\phi y^{-1}y^\phi = x_{-\phi}^{-2}y_{-\phi}^{-2},$$

como $c \in Z(G)$ então $c = c^{(y^\phi)^{-1}} = y^\phi x^{-1}x^\phi y^{-1}y^\phi(y^\phi)^{-1}$ do mesmo modo temos que $c = c^y = y^{-1}y^\phi x^{-1}x^\phi y^{-1}y = y^{-1}y^\phi x^{-1}x^\phi$ de onde obtemos

$$c = [y,\phi][x,\phi] = [x,\phi][y,\phi]$$

pela igualdade acima, temos que $c = x_{-\phi}^{-2}y_{-\phi}^{-2} = y_{-\phi}^{-2}x_{-\phi}^{-2}$ deste modo

$$c^\phi = x_{-\phi}^2 y_{-\phi}^2 = y_{-\phi}^2 x_{-\phi}^2 = (x_{-\phi}^{-2}y_{-\phi}^{-2})^{-1} = c^{-1}.$$

Dada a ordem de G ($|G| = 2k+1$), denotemos $k+1 = m$, assim $c^{-1} = (c^{-1})^{2m} = (c^{-m})^2$, logo $c = (c^{-m})^{-2}$ onde $c^{-m} \in G_{-\phi}$ pelo fato que $c \in G_{-\phi}$, seja $z = g_\phi c^{-m}$ onde $g_\phi \in G_\phi$, assim $c = (c^{-m})^{-2} = [z,\phi]$ com o que concluímos a prova da indução.

Para concluir, dado que $c = [z,\phi]$, temos que $c^\phi = c^{-1}$ como queriamos provar, de onde $(v_0^c)^\phi = (v_0^\phi)^c$.

■

Teorema 4.2.3 *Suponha que $G = [G,\phi]$ e $|C_G(\phi)| \leq m$. Seja $G\langle\phi\rangle$ agindo fiel e irredutivelmente em um p-grupo abeliano V, onde p é um primo ímpar. Então existe uma constante k, m-limitada e elementos $x_1,\ldots x_k \in G_{-\phi}$, tal que $V = \rho^\phi_{x_1,\ldots,x_k}(V_{-\phi})$.*

Demonstração.
Com o lema 4.2.1, temos que V é abeliano elementar.
Dado um elemento $c \in Z(G)$, diferente de e, o centralizador em V de c. Agora, provamos que $C_V(c)$ é $G\langle\phi\rangle$-invariante, além disso como $C_V(c) \neq V$ pois $c \neq 1$, concluímos que $C_V(c)$ é trivial pelo fato de $G\langle\phi\rangle$ agir sobre V de forma irredutível.

Mostramos que $C_V(c)$ é $G\langle\phi\rangle$-invariante verificando dois fatos: o primeiro que $C_V(c)$ é G-invariante e o segundo que $C_V(c)$ é ϕ-invariante. Para o primeiro, seja $g \in G$ e

$v_0 \in C_V(c)$. Vamos provar que v_0^g pertence a $C_V(c)$ e para isso basta fazer $(v_0^g)^c$, o qual por propriedades da ação é igual a v_0^{cg}. Dado que $c \in Z(G)$, temos que $v_0^{cg} = v_0^{gc}$ e pelas propriedades da ação temos que $v_0^{gc} = (v_0^c)^g$. Já que $v_0 \in C_V(c)$, temos que $(v_0^c)^g = (v_0)^g$, de onde obtemos que $(v_0^g)^c = (v_0)^g$, logo $v_0^g \in C_V(c)$, pelo qual $C_V(c)$ é G-invariante. Por outro lado, temos que pelo Lema 4.2.1 V é um p-grupo abeliano elementar, então ele pode se ver como um espaço vetorial sobre $\mathbb{Z}_p$, onde a dimensão do espaço V é no máximo igual à ordem de G. Assim temos que os automorfismos de V podem ser vistos como transformações lineares, as quais comutan entre si pela Proposição 4.2.2, consequentemente $(v_0^\phi)^c = (v_0^c)^\phi = v_0^\phi$, logo $v_0^\phi \in C_V(c)$. Temos então que $C_V(c)$ é G-invariante e ϕ-invariante. Dado que ϕ é uma involução, temos $\langle\phi\rangle = \{\phi, Id\}$, de onde temos $C_V(c)$ é $\langle\phi\rangle$-invariante, e portanto $C_V(c)$ é $G\langle\phi\rangle$-invariante.

Logo obtemos que $C_V(c)$ é trivial para todo $c \in Z(G)$, isto é, todo elemento c do centro de G é livre de pontos fixos como ação sobre V.

Suponha que $Z(G)_{-\phi} \neq 1$, então existe $x \in Z(G)$, tal que $x^\phi = x^{-1}$, além disso, pelo resultado acima temos que x é livre de pontos fixos. Seja $M = V \ltimes G$, então, temos que V é normal em M por definição de produto semidireto. E V segue sendo ϕ-invariante e abeliano por hipótese. Resta provar que se $x \in G_{-\phi}$, então $x \in M_{-\phi}$, mas esta implicação se tem pelo fato que x imerso em M é $(1,x)$, logo $(1,x)^\phi = (1,x^{-1}) = (1,x)^{-1}$. Por último, temos que como as ordens de G e de V são ímpares temos que M também tem ordem ímpar, o que nos leva as hipóteses do Lema 4.1.4, de onde obtemos que $\rho_x^\phi(V_{-\phi}) = V$, concluíndo a prova.

Assumamos então que $Z(G)_{-\phi} = 1$. Pelo Teorema 3.3.1, G contém um subgrupo normal, ϕ-invariante H, de indice m-limitado, $[G:H] \leq f(m)$, tal que $H' \leq C_G(\phi)$. Então pelo Lema 3.2.1, $H' \leq Z(G)$.
Suponha que existem dois elementos $x, y \in H_{-\phi}$ que não comutam entre si e seja $h = [x,y]$. Temos que H é um p'-subgrupo de G, ϕ-invariante. De fato podemos ver H como transformações lineares bijetivas, que só deixam invariante o 1, logo são automorfismos regulares, assim podemos aplicar o Lema 2.3.3 e temos que H é um p'-grupo.
Sejam $U = [V,x] = \langle\{v^{-1}v^x | v \in V\}\rangle$ e $W = [V,y] = \langle\{v^{-1}v^y | v \in V\}\rangle$. Temos que x normaliza todo subgrupo de V que contém U, dado que sendo $\bar{U} \leq V$, tal que $U \subset \bar{U}$, $\bar{u} \in \bar{U}$, então temos que $\bar{u}^{-1} \in \bar{U}$ e $\bar{u}^{-1}\bar{u}^x \in \bar{U}$, pois $\bar{u}^{-1}\bar{u}^x \in U$ e $U \subset \bar{U}$. Logo $\bar{u}^x \in \bar{U}$, o que mostra que x normaliza todo subgrupo de V que contém U. Analogamente, temos que y normaliza todo subgrupo de V que contenha W. Mais ainda, temos que x, y são livres de pontos fixos em U e W, respectivamente, o que obtemos ao verificar que todo elemento da forma $[v,x]$ é enviado por x em $(v^{-1})^x v^{x^2}$ e que $[v,x] = (v^{-1})^x v^{x^2}$ ocorre se,

e somente se, $v^{-1}v^x = (v^{-1})^x v^{x^2}$. Então $[v,x] = 1$, dado que a representação é regular, então o único elemento fixo por um elemento de $G\langle\phi\rangle$ é 1 , portanto, x é livre de pontos fixos em U. Analogamente obtemos que y é livre de pontos fixos em W. Então pelo Lema 4.1.4 temos que $\rho_x^\phi(U_{-\phi}) = U$ e $\rho_y^\phi(W_{-\phi}x) = W$, onde o grupo do lema é $U \ltimes H$ e $W \ltimes H$, respectivamente. O fato de U e W serem ϕ-invariantes vem ao observar que $(v^{-1}v^x)^\phi = (v^{-1})^\phi(v^x)^\phi = (v^\phi)^{-1}(v^\phi)^x$, dado que são transformações lineares, logo comutar entre si,e a última expresão pertence a U. Analogamente temos o resultado para W.

Observe que x^y age trivialmente em V/U^y, pois se $vU^y \in V/U^y$ e fazemos a ação de x^y no elemento vU^y, temos que $(vU^y)^{x^y} = v^{x^y}U^y$, temos por definição de U que $v^{-1}v^x \in U$, e em particular $(v^{y^{-1}})^{-1}(v^{y^{-1}})^x \in U$, então $[(v^{y^{-1}})^{-1}(v^{y^{-1}})^x]^y \in U^y$ o que é equivalente a falar que $v^{-1}[(v^{y^{-1}})^x]^y \in U^y$, assim por propriedades de ação $v^{-1}v^{x^y} \in U^y$. Considerando o fato anterior conseguimos a seguinte igualdade de classes, $vU^y = v^{x^y}U^y$, de onde obtemos que $(vU^y)^{x^y} = v^{x^y}U^y = vU^y$, pelo que x^y age trivialmente em V/U^y. Com isso temos que x^y age trivialmente em $V/\rho_y^\phi(U)$ dado que $U^y \subset \rho_y^\phi(U)$ por definição. Logo se $v^{-1}v^{x^y} \in U^y$, então $v^{-1}v^{x^y} \in \rho_y^\phi(U)$, de onde $v\rho_y^\phi(U) = v^{x^y}\rho_y^\phi(U)$, pelo qual x^y age trivialmente em $V/\rho_y^\phi(U)$.

Sabemos também que y age trivialmente em $V/\rho_y^\phi(V_{-\phi})$, pois $v^{-1}v^y \in W$, mas temos que $W = \rho_y^\phi(W_{-\phi}) \subset \rho_y^\phi(V_{-\phi})$, dado que $W_{-\phi} \subset V_{-\phi}$, então $v^{-1}v^y \in \rho_y^\phi(V_{-\phi})$, de onde $v^y\rho_y^\phi(V_{-\phi}) = v\rho_y^\phi(V_{-\phi})$, o que mostra que y age trivialmente em $V/\rho_y^\phi(V_{-\phi})$.

Pelo Lema 4.1.2, $\rho_x^\phi(V_{-\phi})$ contém $V_{-\phi}$, e dado que $U = \rho_x^\phi(U_{-\phi}) \subset \rho_x^\phi(V_{-\phi})$, tanto $V_{-\phi}$ como U estão contidos em $\rho_x^\phi(V_{-\phi})$, das inclusões anteriores temos que

$$V_{-\phi} \subset \rho_x^\phi(V_{-\phi}) \quad \Rightarrow \quad \rho_y^\phi(V_{-\phi}) \subset \rho_y^\phi(\rho_x^\phi(V_{-\phi})) = \rho_{x,y}^\phi(V_{-\phi}) \quad \text{e}$$

$$U \subset \rho_x^\phi(V_{-\phi}) \quad \Rightarrow \quad U^y \subset (\rho_x^\phi(V_{-\phi}))^y \subset \rho_y^\phi(\rho_x^\phi(V_{-\phi})) = \rho_{x,y}^\phi(V_{-\phi}).$$

Pelo fato de x^y agir trivialmente em V/U^y, temos que x^y age trivialmente em $V/\bar{V}$ para todo $\bar{V}$, tal que $\bar{V} \supset U^y$, pois por um procedimento análogo ao já feito acima, temos que se $v^{-1}v^{x^y} \in U^y$, então $v^{-1}v^{x^y} \in \bar{V}$, logo $v^{x^y}\bar{V} = v\bar{V}$. Em particular x^y age trivialmente em $V/\rho_{x,y}^\phi(V_{-\phi})$, analogamente temos que y age trivialmente em $V/\rho_{x,y}^\phi(V_{-\phi})$ o que implica que qualquer combinação de x^y e y também age trivialmente sobre $V/\rho_{x,y}^\phi(V_{-\phi})$, logo $y(x^y)^{-1}y^{-1}x^y = x^{-1}y^{-1}xy = [x,y] = h$ age trivialmente em $V/\rho_{x,y}^\phi(V_{-\phi})$, mas dado que h é central, pois $H' \subset Z(G)$, então h é livre de pontos fixos em V, pelo item 1 do Lema 2.3.1, temos que

$$C_{V/\rho^{\phi}_{x,y}(V_{-\phi})}(h) = \frac{C_V(h)\rho^{\phi}_{x,y}(V_{-\phi})}{\rho^{\phi}_{x,y}(V_{-\phi})},$$

logo $C_{V/\rho^{\phi}_{x,y}(V_{-\phi})}(h) = \rho^{\phi}_{x,y}(V_{-\phi})$, então h é livre de pontos fixos em $V/\rho^{\phi}_{x,y}(V_{-\phi})$, e portanto ao ser trivial e livre de pontos fixos só pode acontecer que $V = \rho^{\phi}_{x,y}(V_{-\phi})$ com o que concluiríamos a demonstração.

Agora vamos assumir que quaisquer par de elementos de $H_{-\phi}$ comutam entre si. Então $H_{-\phi}$ é um subgrupo abeliano ϕ-invariante de índice m-limitado de G, de onde o fato de ser ϕ-invariante vem de ser abeliano, já que ser abeliano implica ser fechado para a operação entre elementos, isto é, $(h_{-\phi}\bar{h}_{-\phi})^{\phi} = h^{-1}_{-\phi}\bar{h}^{-1}_{-\phi} = \bar{h}^{-1}_{-\phi}h^{-1}_{-\phi} = (h_{-\phi}\bar{h}_{-\phi})^{-1}$. O fato de ter índice m-limitado está dado pelos seguintes argumentos.
H tem índice m-limitado e por hipótese $|G_{\phi}| \leq m$, daí temos que $|G|/|H| \leq f(m)$, e pelo Lema 3.1.3, item 2, temos que $|G| = |G_{\phi}||G_{-\phi}|$, então $|G|/|G_{-\phi}| = |G_{\phi}| \leq m$. Das duas desigualdades acima obtemos $\frac{|G|^2}{|G_{-\phi}||H|} \leq mf(m)$. Pela normalidade de H, temos que $G_{-\phi}H$ é um subgrupo de G, de onde

$$\frac{|G||G_{-\phi}H|}{|G_{-\phi}||H|} \leq \frac{|G|^2}{|G_{-\phi}||H|} \leq mf(m),$$

mas temos que a ordem de $G_{-\phi}H$ é igual a $\dfrac{|G_{-\phi}||H|}{|G_{-\phi}\cap H|}$, sustituíndo temos que

$$\frac{|G|}{|G_{-\phi}||H|}\frac{|G_{-\phi}||H|}{|G_{-\phi}\cap H|} \leq mf(m)$$

de onde obtemos $\dfrac{|G|}{|G_{-\phi}\cap H|} \leq mf(m)$, mas $G_{-\phi}\cap H$ é precisamente $H_{-\phi}$, logo $\dfrac{|G|}{|H_{-\phi}|} \leq mf(m)$, o que mostra que $[G : H_{-\phi}]$ é m-limitado.

Seja A a interseção de todos os conjugados de $H_{-\phi}$. Então A é normal em G. De fato seja $x \in G$ arbitrário e $a \in A$, então para todo $y \in G$ existe $a_y \in H_{-\phi}$, tal que $a = y^{-1}a_y y$, então $x^{-1}ax = x^{-1}y^{-1}a_y yx$, mas yx percorre todos os elementos do grupo G quando y os percorre, de onde $x^{-1}ax$ pode ser visto como o conjugado de um elemento de $H_{-\phi}$ para todo elemento do grupo, logo $x^{-1}ax \in A$. Dada a arbitrariedade do x temos que A é normal em G. Temos também que A está contido em $G_{-\phi}$, pelo fato do conjugado de $H_{-\phi}$ por qualquer elemento dele mesmo ser $H_{-\phi}$, portanto $A \subset H_{-\phi} \subset G_{-\phi}$. Pelo Lema 3.2.1, $A \leq Z(G)$, então $A \subset Z(G)_{-\phi}$, mas, temos que $Z(G)_{-\phi} = 1$, logo $A = 1$.

Seja S o conjunto completo das classes laterais do subgrupo $H_{-\phi}$ em G, chamemos $n = |S| = [G : H_{-\phi}]$. Podemos definir a ação transitiva de G sobre S como sendo $\Pi_{H_{-\phi}}$, isto é,

$$\begin{array}{rcccccl} \Pi_{H_{-\phi}}: & G & \longrightarrow & S_n & & & \\ & x & \longmapsto & \pi_x: & S & \longrightarrow & S \\ & & & & H_{-\phi}x_i & \longmapsto & \pi_x(H_{-\phi}x_i) = H_{-\phi}x_ix. \end{array}$$

O kernel do homomorfismo $\Pi_{H_{-\phi}}$ é o conjunto de todos os $k \in G$, tais que $\Pi_{H_{-\phi}}(k) = id$, pela definição acima de $\Pi_{H_{-\phi}}$ temos que

$$\begin{array}{rccl} \pi_k: & S & \longrightarrow & S \\ & H_{-\phi}x_i & \longmapsto & \pi_k(H_{-\phi}x_i) = H_{-\phi}kx_i. \end{array}$$

Para obter que $\pi_k = id$ devemos ter $H_{-\phi}x_ik = H_{-\phi}x_i$, para todo $i = 1,\dots,n$ o que é equivalente a ter $x_i^{-1}H_{-\phi}x_ik = x_i^{-1}H_{-\phi}x_i$, mudando um poco a notação temos que garantir $H_{-\phi}^{x_i} = H_{-\phi}^{x_i}k$, para todo $i = 1,\dots,n$, então $k \in H_{-\phi}^{x_i}$, logo

$$ker(\Pi_{H_{-\phi}}) = \bigcap_{i=1}^{n} H_{-\phi}^{x_i} = A.$$

Pelo Teorema de isomorfismo, temos que o diagrama comuta,isto é,$f \circ \pi = \Pi_{H_{-\phi}}$

$$\begin{tikzcd} G \arrow[r, "\Pi_{H_{-\phi}}"] \arrow[d, "\pi"'] & S_n \\ G/A \arrow[ur, "f"'] & \end{tikzcd}$$

de onde $|G/A| = |S_n| = n! = [G : H_{-\phi}]!$, o que mostra que a ordem de G é m-limitada, digamos k. Dado que G age em V, V é p-grupo abeliano elementar, logo a ordem de V é menor ou igual a p^k. Seja $V_0 = V_{-\phi}$, se $V_0 = V$, o lema é obtido. Seja $V_0 \neq V$, se para todo $x \in G_{-\phi}$ temos $|\rho_x^{\phi}(V_0)| = |V_0|$, então teríamos $(V_0^x)^{\phi} = V_0^x$ para todo $x \in G_{-\phi}$, de onde $(V_0)^{\phi} = V_0$, pelo Lema 4.1.5, $(V_0)^x = V_0$ para todo $x \in G_{-\phi}$. Dado que $G = [\phi, x] = \langle G_{-\phi} \rangle$, temos que V_0 é $G\langle\phi\rangle$-invariante, logo sabendo que V_0 não é trivial (se é trivial a ordem de ϕ seria 1 o que contradiz a hipótese), temos $V_0 = V$, pois $G\langle\phi\rangle$ age irredutivelmente em V, o que contradiz nossa suposição, logo existe $x_1 \in G_{-\phi}$, tal que $|V_0| \leq |\rho_{x_1}^{\phi}(V_0)|$. Definimos agora $V_1 = \rho_{x_1}^{\phi}(V_0)$, usando o mesmo raciocínio acima, obtemos que $V_1 = V$ ou $V_1 \neq V$ de onde existe $x_2 \in G_{-\phi}$ tal que a ordem de $V_2 = \rho_{x_2}^{\phi}(V_1)$ é maior que a ordem de V_1. Iterando o argumento obtemos uma sequência de longitude no máximo k, dado que $|V_n| \leq |V|$, e a ordem de V_0 é uma potência de p por ser subgrupo de V e ser abeliano, digamos $|V_0| = p^s$, logo $|V_n| = (p^s)^n$, depois de k passos, no máximo, temos que $|V_n| = |V|$, garantindo que $V_k = \rho_{x_1,\dots,x_k}^{\phi}(V_{-\phi}) = V$. ■

Referências Bibliográficas

[1] ASAR, A. **Involutory automorphisms of groups of odd order**. Arch. Math.36, p. 97–103, 1981.

[2] BURNSIDE, W. **Theory of Groups**. Dover, New York, 1955.

[3] FEIT, W. THOMPSON, J. **Solvability of groups of odd order**. Pacific J Math 13, p. 773–1029, 1963.

[4] GORENSTEIN, D. **Finite Groups**. Harper and Row, New York, 1968.

[5] HARTLEY, B. **Periodic locally soluble groups containing an element of prime order with cêrnikov centralizer**. Q. J Math, Oxford,2 33, p. 309–323, 1982.

[6] HARTLEY, B. MEIXNER, T. **Periodic groups in which the centralizer of an involution has bounded order**. J Algebra, 64:285–291, 1980.

[7] HARTLEY, B. MEIXNER, T. **Finite soluble groups in which the centralizer of an element the prime order is small**. Arch. Math., 36:211–213, 1981.

[8] HIGMAN, G. **Groups and rings having automorphisms without non-trivial fixed elements**. J. London Math. Soc., 2(32):321–334, 1957.

[9] HUNDERFORD, T. **Algebra**. Springer-Verlag, New York, 1980.

[10] ISAACS, M. **Finite Group Theory**. Volumen 92 de Graduate Studies in Mathematics, American Mathematical Soc, 2008.

[11] KHUKHRO, E. **Nilpotent Groups and their Automorphisms**. de Gruyter-Verlag, Berlin, 1993.

[12] KOVACS, L.G. WALL, G. **Involutory automorphisms of groups of odd order and their fixed point groups**. Nagoya Math J, (27):113–120, 1966.

[13] ROTMAN, J. **An Introduction to the Theory of Groups**. Springer-Verlag, fourth edition, 1994.

[14] SHUMYATSKY, P. **Involutory automorphisms of locally soluble periodic groups**. J Algebra, (155):36–44, 1993.

[15] SHUMYATSKY, P. **Involutory automorphisms of periodic groups**. Internat J Algebra Comput, (6):745–749, 1996.

[16] SHUMYATSKY, P. **Involutory automorphisms of finite groups and their centralizers**. Arch Math (Basel), (71):425–432, 1998.

[17] SHUMYATSKY, P. **Involutory automorphisms of groups of odd order**. Monatsh. Math, (146):77–82, 2005.

[18] SHUMYATSKY, P. **Centralizer of involutory automorphisms of groups of odd order**. Journal of Álgebra, (315):954–962, 2007.

[19] THOMPSON, J. **Finite groups with fixed point-free-automorphisms of prime order**. Proc. Natl. Acad. Sci. U.S.A., (45):578–581, 1959.

[20] THOMPSON, J. **automorphisms of solvable groups**. Journal. Algebra, (1):259–267, 1964.

[21] WARD, J. **Involutory automorphisms of groups of odd order**. J Austral Math Soc, (6):480–494, 1966.