Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre Grupos Finitos Admitindo Automorfismos Coprimos

por

Sara Raissa Silva Rodrigues

Brasília
2021

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre Grupos Finitos Admitindo Automorfismos Coprimos

por

Sara Raissa Silva Rodrigues

sob orientação do

Prof. Dr. Pavel Shumyatsky - UnB

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática da Universidade de Brasília, como parte dos requisitos necessários para obtenção do título de Doutora em Matemática.

Brasília

2021

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

RR696s

Rodrigues, Sara Raissa Silva
Sobre Grupos Finitos Admitindo Automorfismos Coprimos / Sara Raissa Silva Rodrigues; orientador Pavel Shumyatsky. - Brasília, 2021.
74 p.

Tese (Doutorado - Doutorado em Matemática) -- Universidade de Brasília, 2021.

1. Grupos finitos. 2. Automorfismos. 3. Posto. 4. Expoente. 5. Álgebras de Lie. I. Shumyatsky, Pavel, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre grupos finitos admitindo Automorfismos Coprimos

Sara Raissa Silva Rodrigues*

Tese apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

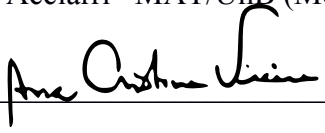
DOUTORA EM MATEMÁTICA

Brasília, 18 de janeiro de 2021.

Comissão Examinadora:

Prof. Dr. Pavel Shumyatsky- MAT/UnB (Orientador)

Profa. Dra. Cristina Acciarri– MAT/UnB (Membro)



Profa. Dra. Ana Cristina Vieira– UFMG (Membro)

Prof. Dr. Mikhailo Dokuchaev - USP(Membro)

* O autor foi bolsista da CAPES durante a elaboração desta tese.

"Não fui eu que ordenei a você? Seja forte e corajoso! Não se apavore nem desanime, pois o Senhor, o seu Deus, estará com você por onde você andar."

Josué 1:9

"Totus Tuus Mariae."

São João Paulo II

"Nunca desista dos seus sonhos, faça a sua parte e confie em Deus que tudo dará certo."

Agradecimentos

A Deus por ser a minha base, o meu tudo, por sempre estar presente em minha vida, dando-me sabedoria e força para superar qualquer adversidade que a vida me impõe. À Nossa Senhora de Nazaré por ser a minha fiel intercessora junto ao seu filho Jesus. Sem eles eu não daria conta de nada. E aos meus santinhos queridos pela intercessão junto ao Pai.

À minha mãe Ana Maria, por ser o meu esteio, a minha base, o meu amor maior, por sempre fazer o possível e o impossível para que eu possa realizar todos os meus sonhos, por sempre estar ao meu lado incondicionalmente me dando apoio, pelas suas poderosas orações e pelo seu imenso amor. O melhor de mim eu devo à ela. Esta conquista também é sua e ela é muito mais especial, pois a senhora está comigo. Obrigada por ter sido a primeira a acreditar em mim, sem a sua ajuda nada disso seria possível. Agora, a senhora tem uma filha doutora!! Minha gratidão a senhora é eterna. Ao meu pai Adinilson Fialho (in memoriam), que em vida sempre me orientou a nunca desistir dos meus sonhos e a dar sempre o meu melhor em tudo, com certeza se estivesse vivo estaria muito feliz em ver que a filha dele virou doutora. Ao meu irmão Diogo, cunhada, as minhas tias Davina, Hozana, Naza e Rita por sempre acreditarem, torcerem e rezarem por mim, aos tios, primos, enfim, a todos os meus familiares pelo apoio, torcida e pelas orações.

Ao meu querido orientador professor Pavel Shumyatsky, não somente pelas excelentes, pacientes, eficientes e precisas orientações, mas também pelos conselhos, pelo seu comprometimento para com os seus alunos, pela amizade que construímos durante esses quatro anos, pelo seu cuidado, preocupação, carinho, pela sua humanidade para comigo, por entender as minhas limitações e ainda sim acreditar em mim. Saiba que foi um enorme prazer e uma honra poder trabalhar com um

matemático tão brilhante quanto o senhor. Obrigada por tudo! Minha gratidão é eterna ao senhor.

À querida professora Cristina Acciarri por ter sido muito importante durante a minha trajetória de Unb, por todos os seus ensinamentos, pela força, pelos conselhos valiosos, pelos puxões de orelha, por me incentivar a perder os meus medos e a ir sempre mais além, por ter dito a frase "eu acredito em você" no momento certo, na data certa e no local certo. Aquilo mudou a minha vida! Agradeço pelas suas maravilhosas e profundas aulas que fizeram eu amar a teoria de grupos e sobretudo, obrigada por sempre ter acreditado em mim. Minha gratidão a senhora é eterna.

À minha amada madrinha e professora Nazaré Bezerra por estar comigo todos esses anos, desde 2010, me acompanhando, especialmente pelo apoio dado na semana que antecedeu a minha defesa. Obrigada pela torcida, amizade, carinho, pelas orações, incentivos, conselhos, puxões de orelha, por todos os seus ensinamentos, por acreditar em mim, por ter me influenciado fortemente a amar à álgebra, por ser a minha psicóloga sem diploma e principalmente, obrigada por me motivar a terminar de escrever a tese e defender logo. Sua ajuda nesta fase final foi muito importante. Minha gratidão a senhora é eterna.

À professora Rúbia Nascimento, por ter sido a primeira professora que me incentivou à pesquisa, por todos os seus ensinamentos, pela sua torcida, amizade, conselhos, carinho, ajuda, incentivos e por sempre acreditar em mim.

À professora Joelma Morbach, por não ter cortado as minhas asas lá no início da graduação quando eu disse à ela que queria fazer doutorado em trigonometria, por sempre acreditar em mim, pela torcida, amizade, carinho, conselhos, ajuda e por todos os seus ensinamentos.

À professora Adma Muriel, que me acompanha desde a sétima série e que me influenciou a amar ainda mais a matemática. Obrigada por todas as suas orações, amizade, carinho, torcida e por ficar feliz com as minhas conquistas.

À professora Sandra Imaculada pela amizade, carinho, torcida, orações, conselhos, pelos inúmeros passeios que fizemos por Brasília e pelos seus ensinamentos.

À professora Luciana Ávila, por me acompanhar durante toda a minha trajetória de UnB, por torcer por mim e por todo o seu carinho.

À professora Alda Regina pela amizade, carinho e por sempre torcer por mim.

À professora Cristina Vaz por acreditar em mim, pela amizade, carinho, torcida e pelos seus ensinamentos.

Ao professor João Pablo por ter me incentivado, lá na graduação, a me inscrever no mestrado da UnB e com isso fez com que eu conhecesse a UnB e pela torcida.

Aos professores Ana Cristina, Cristina Acciarri e Mikhailo Dokuchaev por terem aceitado participar da minha banca examinadora e pelas suas valiosas sugestões para a melhoria deste trabalho.

De um modo geral gostaria de agradecer a todos os meus professores da UnB que de alguma forma contribuíram para a minha formação, dentre os quais destaco os professores: Alex, Alexei, Aline, Cátia, Cristina Acciarri, Daniela Amato, Emerson, Giovany, Irina, Luciana, Noraí, Ricardo Ruviaro e Victor. E a todos os servidores do Mat/UnB.

Agradeço de modo bem especial à Renata, por toda amizade, carinho, ajuda, cuidado, orações, por ter estado ao meu lado durante toda esta caminhada do meu doutorado, torcendo, chorando, por ter me escutado várias vezes, por cada comemoração que fizemos, enfim por sempre me apoiar em tudo, por compartilhar os momentos alegres e tristes e pela parceria. Ao José Carlos por toda amizade, carinho, torcida, orações, ajuda no inglês e no latex e por sempre me escutar. Vocês foram um dos melhores presentes que o doutorado me deu. À Nathália, por me acompanhar desde o mestrado, obrigada por toda a amizade, carinho, cuidado, ajuda, orações, por compartilhar as alegrias e tristezas, pelos puxões de orelhas, pelas inúmeras vezes que me escutou, enfim por todo o apoio dado. E ao Túlio pela amizade, torcida, cuidado, atenção e por compartilhar muitas alegrias. Vocês queridos deixaram o meu doutorado muito mais leve com as suas amizades!! Obrigada de coração.

Aos amigos queridos que conquistei ao longo destes anos em Brasília, de modo especial os da matemática: Bruno, Christe, João, John, José Carlos, Karen, Nathália, Marcos, Mattheus, Regiane, Renata e Túlio. E aos amigos queridos que o pensionato me deu: Antônia, Busson, Claúdia, Dariana, Eliete, Giovana, Ivo, Larissa, Luciana, Marcelo, Marisa, Milena, Willyane e Zé Pedro. Obrigada a todos pela cumplicidade, ajuda, apoio, torcida, orações, amizade, por me aguentarem todos estes anos e por me escutarem. Vocês deixaram a minha estadia em Brasília muito mais feliz com as suas amizades e tornaram-se a minha família daqui!! Gratidão a todos!

Aos meus queridos amigos que sempre me acompanham: Ana Lídia, Arlena, Érico, Francimaria, Haissa, Layane, Mayara, Priscyla, Renan e Thays pela torcida, apoio, orações, amizade e por me escutarem nos momentos que precisei conversar. Obrigada por tudo gente!! Vocês moram no meu coração.

As irmãs do Instituto Vicenta Maria, onde destaco as irmãs Suely e Valdeci, por terem me acolhido super bem durante os anos que morei nesta residência, por terem me proporcionado excelentes amizades e grandes experiências.

À querida Elza Líbia e as suas irmãs pelas orações, carinho, amizade, apoio, torcida, pelas palavras de incentivo e por sempre estarem ao meu lado.

Ao Padre Antônio, à Maria José e à Violanda pela amizade e pelas orações.

À Andrelina, Angélica, Dr. Elenilson e Iranilde por todo apoio, amizade, carinho e torcida.

À minha madrinha Charlane pelas orações, carinho e torcida.

À Cristine, Emerson e Iolanda (in memoriam), pessoas especiais, queridas e amigas que me acolheram muito bem em Brasília.

À CAPES e ao CNPq pelo apoio financeiro ao longo de todo o meu doutorado.

Enfim, obrigada a todos que acreditaram em mim e que de certa forma contribuíram para a minha formação acadêmica.

Dedicatória

A Deus e à Nossa Senhora.
Aos meus pais Ana Maria e Adinilson Fialho (in memoriam).
À minha madrinha Nazaré Bezerra.

Resumo

Seja G um grupo finito admitindo um automorfismo ϕ. Denote por G_ϕ o centralizador de ϕ em G e por $G_{-\phi}$ o conjunto $\{x^{-1}x^\phi \mid x \in G\}$. O subgrupo gerado por $G_{-\phi}$ será denotado por $[G, \phi]$. Existem vários estudos que mostram a relação entre a estrutura do grupo G e propriedades dos G_ϕ e $G_{-\phi}$.

Neste trabalho, apresentamos resultados limitando o expoente de G e $[G, \phi]$. Eles estão concentrados em grupos finitos que admitem um automorfismo coprimo, com atenção especial para grupos de ordem ímpar que admitem um automorfismo involutório.

Assim, se G é um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ, os seguintes resultados foram obtidos: suponha que G_ϕ é nilpotente de classe c. Se $x^e = 1$ para cada $x \in G_{-\phi}$ e o subgrupo $\langle x, y\rangle$ tem comprimento derivado no máximo d para todos $x, y \in G_{-\phi}$, então o expoente de $[G, \phi]$ é limitado em termos de c, d e e. Além disso, se G_ϕ tem posto r (ver Definição 1.1.27) e $x^e = 1$ para cada $x \in G_{-\phi}$, então o expoente de $[G, \phi]$ é limitado em termos de e e r.

Agora, supondo que G é um grupo finito admitindo um automorfismo coprimo ϕ de ordem n. Provamos que se todo elemento de $G_\phi \cup G_{-\phi}$ pertence a um subgrupo ϕ-invariante de expoente dividindo e, então o expoente de G é limitado em termos de e e n. Para a demonstração deste resultado foram utilizadas ferramentas Lie-teóricas desenvolvidas por Zelmanov. Além disso, estendemos o primeiro resultado: suponha que G_ϕ é nilpotente de classe c. Se $x^e = 1$ para cada $x \in G_{-\phi}$ e quaisquer dois elementos de $G_{-\phi}$ pertencem a um subgrupo solúvel ϕ-invariante de comprimento derivado d, então o expoente de $[G, \phi]$ é limitado em termos de c, d, e e n.

Palavras-chave: Grupos finitos, Automorfismos, Posto, Expoente, Álgebras de Lie.

Abstract

Let G be a finite group admitting an automorphism ϕ. Denote by G_ϕ the centralizer of ϕ in G and by $G_{-\phi}$ the set $\{x^{-1}x^\phi \mid x \in G\}$. The subgroup generated by $G_{-\phi}$ will be denoted by $[G, \phi]$. There are many results relating the structure of the group G and the properties of G_ϕ and $G_{-\phi}$.

In this work, we present results bounding the exponent of G and $[G, \phi]$. They are concentrated in finite groups that admit a coprime automorphism, with special attention to odd order groups that admit an involutory automorphism.

Thus, if G is a finite group of odd order admitting an involutory automorphism ϕ, the following results were obtained: suppose that G_ϕ is nilpotent of class c. If $x^e = 1$ for each $x \in G_{-\phi}$ and the subgroup $\langle x, y\rangle$ has derived length at most d for every $x, y \in G_{-\phi}$, then the exponent of $[G, \phi]$ is bounded in terms of c, d and e. On the other hand, if G_ϕ has rank r (see Definition 1.1.27) and $x^e = 1$ for each $x \in G_{-\phi}$, then the exponent of $[G, \phi]$ is bounded in terms of e and r.

Further, assume that G is a finite group admitting a coprime automorphism ϕ of order n. We prove that if every element from $G_\phi \cup G_{-\phi}$ belongs to a ϕ-invariant subgroup of exponent dividing e, then the exponent of G is bounded in terms of e and n. To demonstrate this result, Lie-theoretic tools created by Zelmanov were used. In addition, we extend the first result as follows: suppose that G_ϕ is nilpotent of class c. If $x^e = 1$ for each $x \in G_{-\phi}$ and any two elements of $G_{-\phi}$ belong to a ϕ-invariant soluble subgroup of derived length d, then the exponent of $[G, \phi]$ is bounded in terms of c, d, e and n.

Keywords: Finite groups, Automorphisms, Rank, Exponent, Lie algebras.

Lista de Símbolos

Símbolo	**Significado**
(a, b)	máximo divisor comum de a e b
$[x, y]$	comutador dos elementos $x, y \in G$ definido por $x^{-1}y^{-1}xy$
$\langle X \rangle$	subgrupo gerado pelo conjunto X
$\langle X \rangle^{\langle \phi \rangle}$	subgrupo minimal ϕ-invariante de G contendo X
$G_\phi, C_G(\phi)$	centralizador de ϕ em G
$G_{-\phi}$	conjunto de G definido por $\{x^{-1}x^\phi \mid x \in G\}$
$[G, \phi]$	subgrupo gerado por $G_{-\phi}$
$[H, K]$	subgrupo comutador de H e K
G'	subgrupo derivado do grupo G
$Z(G)$	centro do grupo G
$C_G(X)$	centralizador de X em G
$\langle X^G \rangle$	fecho normal de X em G
$N_G(X)$	normalizador de X em G
$H \subseteq G$	H é subconjunto de G
$H \leq G$	H é subgrupo de G
$H \lhd G, H \trianglelefteq G$	H é subgrupo normal de G
$\lvert G \rvert$	ordem de G
$F(G)$	subgrupo de Fitting de G
$\Phi(G)$	subgrupo de Frattini de G
$[G : H]$	índice do subgrupo H em G
$h(G)$	altura de Fitting de G
$r(G)$	posto de G

$\gamma_i(G)$	i-ésimo termo da série central inferior de G
$Z_i(G)$	i-ésimo termo da série central superior de G
$G^{(i)}$	i-ésimo termo da série derivada de G
$F_i(G)$	i-ésimo termo da série de Fitting de G
D_i	i-ésimo termo da série central p-dimensional de G
G^i	subgrupo gerado pelas i-ésimas potências dos elementos de G
$Aut\, G$	grupo dos automorfismos de G
$\pi(G)$	conjunto de primos que dividem $\|G\|$
p	número primo
p'	número primo diferente de p
$\mathbb{F}_p$	corpo com p elementos
$\mathbb{P}$	conjunto dos números primos
$O_{p'}(G)$	p'-subgrupo normal maximal de G
ω	raiz n-ésima primitiva da unidade

Sumário

Introdução

Seja G um grupo finito admitindo um automorfismo ϕ. Denote por G_ϕ o subgrupo dos pontos fixos de ϕ em G, ou centralizador de ϕ em G, que é definido como $\{x \in G \mid x^\phi = x\}$ e por $G_{-\phi}$ o conjunto $\{x^{-1}x^\phi \mid x \in G\}$. O subgrupo gerado por $G_{-\phi}$ será denotado por $[G, \phi]$. Sabemos que $[G, \phi]$ é um subgrupo normal ϕ-invariante de G e que ϕ induz o automorfismo trivial em $G/[G, \phi]$.

Existe uma importante linha de pesquisa em teoria de grupos que estuda a relação entre a estrutura do grupo G e propriedades dos G_ϕ e $G_{-\phi}$. Por exemplo, na literatura existem vários resultados que mostram como propriedades do subgrupo dos pontos fixos de ϕ em G exercem influência sobre a estrutura do grupo G. Um resultado elementar que evidencia este fato afirma que se G é um grupo finito admitindo um automorfismo ϕ de ordem 2 tal que $G_\phi = 1$, então G é um grupo abeliano de ordem ímpar. Além disso, combinando dois famosos resultados devido a G. Higmam, em [**9**], e a J. G. Thompson, em [**31**], obtém-se que se G é um grupo finito admitindo um automorfismo ϕ de ordem prima p tal que $G_\phi = 1$, então G é nilpotente de classe de nilpotência limitada por uma função que depende apenas de p. Um outro resultado, mais geral, que utiliza na sua prova a classificação de grupos finitos simples diz que se G é um grupo finito admitindo um automorfismo ϕ de ordem n tal que $G_\phi = 1$, então G é solúvel. No entanto, não é conhecido se o comprimento derivado de G depende apenas de n.

Assim, o objetivo central desta tese é estudar a relação entre a estrutura do grupo G e propriedades não somente de G_ϕ mas também do conjunto $G_{-\phi}$ e contribuir nessa direção com resultados novos. Mais especificamente, vamos obter resultados limitando o expoente de G e de $[G, \phi]$.

O expoente de um grupo G é o menor inteiro positivo e tal que $x^e = 1$ para todo $x \in G$. Se existir tal inteiro, dizemos que G possui expoente finito, caso contrário, dizemos que o expoente de G é infinito.

Um automorfismo involutório significa um automorfismo de ordem 2 e um automorfismo ϕ de um grupo finito G é chamado de coprimo se temos $(|G|, |\phi|) = 1$.

Assim sendo, os nossos resultados estão concentrados em grupos finitos que admitem um automorfismo coprimo, com atenção especial para grupos de ordem ímpar que admitem um automorfismo involutório.

Ao longo deste trabalho, vamos usar a expressão "(a, b, c, d)-limitado" ou "limitado em termos de a, b, c e d" para dizer que uma quantia é limitada superiormente por uma função que depende apenas dos parâmetros a, b, c e d.

Em 2013, E. Bettio, G. Busetto e E. Jabara estudaram a classe de p-grupos finitos que admitem um automorfismo involutório, onde p é um número primo ímpar. Mais precisamente, em [**2**, Teorema 3.9], eles provaram que se G é um p-grupo finito admitindo um automorfismo involutório ϕ tal que G_ϕ é nilpotente de classe c, $x^p = 1$ para cada $x \in G_{-\phi}$ e o comprimento derivado de G é no máximo d, então a classe de nilpotência de $[G, \phi]$ é (c, d, p)-limitada.

Assim, como $[G, \phi]$ tem classe de nilpotência (c, d, p)-limitada e é gerado por elementos de ordem dividindo p, concluímos que o expoente de $[G, \phi]$ é limitado em termos de c, d e p. Desta maneira, obtém-se de forma imediata o próximo corolário.

Corolário. *Sejam p um primo ímpar e G um p-grupo finito admitindo um automorfismo involutório ϕ tal que G_ϕ é nilpotente de classe c e $x^p = 1$ para cada $x \in G_{-\phi}$. Suponha que o comprimento derivado de G é no máximo d. Então, o expoente de $[G, \phi]$ é (c, d, p)-limitado.*

A partir deste resultado investigamos a seguinte pergunta:

Pergunta. *Se relaxarmos as hipóteses do Corolário é possível concluir que o expoente de $[G, \phi]$ é limitado em termos de parâmetros relevantes?*

A resposta é afirmativa e obtemos, a seguir, o nosso primeiro resultado nesta direção. Denotemos por $\langle X \rangle$ o subgrupo gerado pelo conjunto X.

Teorema A. *Sejam c, d, e inteiros não negativos e G um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que G_ϕ é nilpotente de classe c e $x^e = 1$ para cada $x \in G_{-\phi}$. Suponha que o subgrupo $\langle x, y \rangle$ tem comprimento derivado no máximo d para todos $x, y \in G_{-\phi}$. Então, o expoente de $[G, \phi]$ é (c, d, e)-limitado.*

Uma importante ferramenta usada na prova do Teorema A, é o teorema devido a P. Shumyatsky provado em [**29**], que afirma se e é um inteiro positivo e G é um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que todos os elementos em $G_\phi \cup G_{-\phi}$ possuem ordem dividindo e, então o expoente de G é e-limitado. Para demonstração do mesmo, usa-se técnicas criadas por Zelmanov em sua solução para o Problema Restrito de Burnside.

Não sabemos se todas as hipóteses do Teorema A são necessárias. É concebível que o expoente de $[G, \phi]$ possa ser limitado somente em termos de c e e ou em termos de d e e. No entanto, isto parece ser um problema difícil.

Um grupo finito G é dito ser de posto r, se r é o menor número tal que qualquer subgrupo de G é r-gerado. O nosso segundo teorema estabelece uma limitação do expoente de $[G, \phi]$ em apenas dois parâmetros, a saber, de e e do posto de G_ϕ. Ele é um resultado melhor, pois nem sequer precisamos assumir que G_ϕ é nilpotente. Mais precisamente, mostramos o seguinte resultado.

Teorema B. *Sejam e, r inteiros não negativos e G um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que G_ϕ tem posto r e $x^e = 1$ para cada $x \in G_{-\phi}$. Então, o expoente de $[G, \phi]$ é (e, r)-limitado.*

Na prova do Teorema B, utilizamos um resultado de P. Shumyatsky que se encontra em [**28**] que afirma se G é um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que o posto de G_ϕ é r, então o posto de $[G, \phi]'$ é r-limitado. Para demonstrá-lo, usa-se teoria de p-grupos powerful, onde p é um número primo, desenvolvida por A. Lubotzky e A. Mann, em [**20**].

A partir dos Teoremas A e B investigamos se eles poderiam de alguma forma serem generalizados para o caso onde ϕ não é necessariamente de ordem dois. Respondemos afirmativamente a esta questão, quando consideramos o Teorema A.

É bem conhecido que se G é um grupo de ordem ímpar e ϕ é um automorfismo involutório de G, então $G = G_{-\phi}G_\phi$. Para estendermos o Teorema A, examinamos a seguinte questão de interesse próprio.

Questão. *A igualdade $G = G_{-\phi}G_\phi$ vale para qualquer automorfismo coprimo ϕ?*

Em geral, esta igualdade pode falhar. No Capítulo 2, veremos com um pouco mais de detalhes, o exemplo que mostra isto. Para verificar que a igualdade não vale em geral foi preciso provar o resultado a seguir.

Lema 2.1.3. *Seja ϕ um automorfismo coprimo de um grupo finito G. Então, $G = G_{-\phi}G_\phi$ se, e somente se, nenhum elemento não trivial de $G_{-\phi}$ possui conjugados em G_ϕ.*

O seguinte exemplo foi comunicado a P. Shumyatsky por G. Glauberman. Sejam K o corpo com 5^3 elementos e ϕ o automorfismo de ordem 3 de K que leva cada $x \in K$ em x^5. Denotemos por A o grupo aditivo de K e por B o grupo multiplicativo de K. Seja $G = AB$ o produto semi-direto natural de A por B. Temos que B age transitivamente em $A \setminus \{0\}$ e claramente ϕ induz um automorfismo coprimo em G. É possível observar que A_ϕ é um subgrupo próprio de A e $A_{-\phi}$ é não trivial. Assim, como B age transitivamente em $A \setminus \{0\}$ segue que todos os elementos não triviais de $A_{-\phi}$ são conjugados em G com alguns elementos em A_ϕ. Portanto, aplicando o Lema 2.1.3, obtemos que $G \neq G_{-\phi}G_\phi$.

Contudo, conseguimos provar, ainda no Capítulo 2, que a igualdade $G = G_{-\phi}G_\phi$ vale para grupos nilpotentes. Mais especificamente, obtemos o próximo resultado.

Lema 2.1.5. *Seja ϕ um automorfismo coprimo de um grupo nilpotente finito G. Então, qualquer elemento $x \in G$ pode ser escrito unicamente na forma $x = gh$, onde $g \in G_{-\phi}$ e $h \in G_\phi$.*

Por outro lado, assumindo que um grupo finito G admite um automorfismo coprimo ϕ de ordem n tal que cada elemento em $G_\phi \cup G_{-\phi}$ tem ordem dividindo e, não se sabe, se o expoente de G pode ser limitado somente em termos de e. No entanto, obtemos o seguinte teorema que nos fornece uma limitação do expoente de G em dois parâmetros e é um dos principais resultados desta tese.

Teorema C. *Sejam e, n inteiros positivos e G um grupo finito admitindo um automorfismo coprimo ϕ de ordem n tal que cada elemento de $G_\phi \cup G_{-\phi}$ pertence a um subgrupo ϕ-invariante de expoente dividindo e. Então, o expoente de G é (e, n)-limitado.*

O Problema Restrito de Burnside foi proposto nos anos 30 do século XX e tem a seguinte pergunta:

Pergunta. *É verdade que todo grupo finito m-gerado e de expoente n tem sua ordem limitada por uma função que depende apenas de m e n?*

Diversos matemáticos tentaram resolver este problema. Em 1956, P. Hall e G. Higman em seu artigo, que se encontra em [**6**], reduziram o problema restrito para o caso de grupos que possuem expoente uma potência de primo. Eles utilizaram para a redução o teorema de classificação de grupos finitos simples. Em 1959, A. I. Kostrikin, em [**17**], resolveu o problema para grupos de expoente

primo. Sua prova consiste de um estudo aprofundado em álgebras de Lie de característica prima com condição de Engel. Anteriormente, em estudos independentes, W. Magnus, em [**21**] e I. N. Sanov, em [**27**], reduziram o famoso problema para álgebras de Lie. Finalmente, no ano de 1989, E. Zelmanov respondeu completamente a este problema em seu trabalho que lhe rendeu Medalha Fields e pode ser encontrado em [**37**] e [**38**]. A partir desta resposta, vários avanços na teoria de grupos foram realizados. As ferramentas desenvolvidas por Zelmanov basearam-se nos métodos de Lie que foram criados por W. Magnus e H. Zassenhaus nos anos 30 do século XX, e se mostraram tão eficazes que muitos problemas de teoria de grupos foram resolvidos utilizando tais técnicas. Até hoje, elas são usadas por matemáticos em suas pesquisas. A demonstração do Teorema C é técnica e depende dessas ferramentas, por isso, elas serão brevemente tratadas no Capítulo 3. É possível notar que o teorema de P. Shumyatsky, mencionado anteriormente e provado em [**29**], pode ser visto como um corolário do nosso Teorema C.

Utilizando o Teorema C, mostramos o resultado a seguir que é uma extensão do Teorema A.

Teorema D. *Seja G um grupo finito admitindo um automorfismo coprimo ϕ de ordem n tal que G_ϕ é nilpotente de classe c e $x^e = 1$ para cada $x \in G_{-\phi}$. Suponha que quaisquer dois elementos de $G_{-\phi}$ pertencem a um subgrupo solúvel ϕ-invariante de comprimento derivado d. Então, o expoente de $[G, \phi]$ é limitado em termos de c, d, e e n.*

Para demonstrar o Teorema D, usamos o resultado obtido por M. Y. Wang e M. Z. Chen, em [**34**], que diz se um grupo finito G admite um automorfismo coprimo ϕ tal que G_ϕ é nilpotente, então G é solúvel. Sua prova utiliza a classificação de grupos finitos simples.

Vale recordar que a altura de Fitting de um grupo solúvel finito G é o menor inteiro positivo h tal que G possui uma série normal de comprimento h, cujos quocientes são nilpotentes. A demonstração do Teorema D é feita por indução na altura de Fitting do grupo G.

Outro resultado que utilizamos para provar o Teorema D é um célebre teorema, devido a Thompson, mostrado em [**32**] que afirma se um grupo solúvel finito G admite um automorfismo coprimo ϕ, então a altura de Fitting de G é limitada em termos da altura de Fitting de G_ϕ e o número de primos divisores da ordem de ϕ, contando multiplicidades.

Note, no Teorema D, que no caso onde $n = 2$, sempre temos $x^\phi = x^{-1}$ para todo $x \in G_{-\phi}$. Logo, qualquer subgrupo gerado por um subconjunto de $G_{-\phi}$

é ϕ-invariante. Desta forma, concluímos que o Teorema D é uma extensão do Teorema A.

Terminamos observando que esta tese está dividida em cinco capítulos. No Capítulo 1, recordamos definições e conceitos da teoria de grupos que serão essenciais ao longo deste trabalho. Definiremos, por exemplo, grupos nilpotentes, solúveis, subgrupo de Fitting e p-grupos powerful. Alguns resultados serão omitidos, por serem bem conhecidos, muitos desses serão dados a referência e outros apresentaremos uma prova.

No Capítulo 2, falaremos de automorfismos de grupos de forma geral, posteriormente nos concentraremos em automorfismos coprimos e involutórios. Mostraremos também alguns resultados necessários que obtivemos a partir de nossas investigações.

No Capítulo 3, vamos definir o conceito de álgebra de Lie, veremos alguns resultados sobre automorfismos dessa álgebra. Além de apresentar algumas ferramentas Lie-teóricas desenvolvidas por Zelmanov, veremos como associar uma álgebra de Lie a um grupo qualquer. De modo particular, descreveremos propriedades da série de Zassenhaus que é uma N_p-série de grande importância para o nosso estudo. Este capítulo tem caráter preliminar referente ao Capítulo 5.

O Capítulo 4 está dedicado a apresentar as demonstrações dos Teoremas A e B, relacionados a grupos de ordem ímpar que admitem um automorfismo involutório.

Por fim, no Capítulo 5, provaremos os Teoremas C e D, referentes a grupos finitos que admitem um automorfismo coprimo.

Vale destacar que os resultados obtidos nesta tese foram publicados em [**25**] e [**26**]. Mais especificamente, os Teoremas A e B estão publicados em [**25**], os Teoremas C e D e os Lemas 2.1.3 e 2.1.5 encontram-se em [**26**].

1

Preliminares

Este capítulo tem por objetivo recordar definições e propriedades da teoria de grupos que serão utilizadas ao longo desta tese. Na primeira seção, definiremos conceitos como os de grupos nilpotentes, solúveis, subgrupo de Fitting, expoente de um grupo, posto de um grupo finito e destacaremos alguns resultados relacionadas a estes conceitos. Já na segunda seção, falaremos de forma sucinta sobre os p-grupos finitos powerful, onde p é um primo qualquer.

1.1. Conceitos Elementares da Teoria de Grupos

Seja G um grupo. Dados x e y em G, o *comutador* de x e y é o elemento de G definido por $[x, y] = x^{-1}y^{-1}xy$. Definimos de maneira recursiva comutadores da seguinte forma: por convenção $[x_1] = x_1$ e $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$, para todos $x_1, \ldots, x_n \in G$ e $n \geqslant 2$. Dados x e y elementos de G, o *conjugado* de x por y é o elemento $x^y = y^{-1}xy$. Assim, podemos escrever $[x, y] = x^{-1}x^y$.

A proposição a seguir reúne algumas propriedades elementares de comutadores.

Proposição 1.1.1. *Sejam G um grupo e x, y e z elementos de G. As seguintes identidades de comutadores valem:*
(i) $x^y = x[x, y]$;
(ii) $[x, y] = [y, x]^{-1}$;
(iii) $[xy, z] = [x, z]^y[y, z]$;
(iv) $[x, yz] = [x, z][x, y]^z$;
(v) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$ *(Identidade de Hall-Witt).*

Sejam H e K dois subgrupos de um grupo G. O *subgrupo comutador* de H e K é definido como o subgrupo gerado por todos os comutadores $[h, k]$, onde $h \in H$

e $k \in K$. Denotamos este subgrupo por $[H, K]$. Assim, temos

$$[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle.$$

Um caso particular de subgrupo comutador é quando consideramos $H = K = G$, isto é,

$$G' = [G, G] = \langle [x, y] \mid x, y \in G \rangle,$$

este subgrupo é chamado de *subgrupo derivado* de G.

O *centro* de um grupo G é o subgrupo definido por

$$Z(G) = \{x \in G \mid [x, g] = 1, \text{ para todo } g \in G\}.$$

Seja X um subconjunto não vazio de um grupo G. O *centralizador de X em G* é o subgrupo dado por

$$C_G(X) = \{g \in G \mid gx = xg, \text{ para todo } x \in X\}.$$

Seja g um elemento de G, o *conjugado* de X por g é o conjunto definido por $X^g = \{x^g \mid x \in X\}$. O *fecho normal* de X em G é a interseção de todos os subgrupos normais de G que contém X. Vamos denotar este subgrupo por $\langle X^G \rangle$. Claramente, $\langle X^G \rangle$ é um subgrupo normal de G e pode-se mostrar que $\langle X^G \rangle = \langle X^g \mid g \in G \rangle$. O *normalizador* de X em G é o subgrupo definido por $N_G(X) = \{g \in G \mid X^g = X\}$.

Utilizando as definições de centralizador e de subgrupo comutador o próximo lema pode ser facilmente obtido.

Lema 1.1.2. *Sejam H, K e L subgrupos de um grupo G. As seguintes afirmações valem.*
(i) *$K \leq C_G(H)$ se, e somente se, $[K, H] = 1$;*
(ii) *Se H, K e L são subgrupos normais de G, então $[HK, L] = [H, L][K, L]$.*

Seja $H \leq G$. Dizemos que H é um subgrupo *característico* em G se $H^\phi = H$ para todo ϕ automorfismo de G.

Uma observação que será usada posteriormente é a seguinte.

Observação 1.1.3. *Sejam G um grupo abeliano aditivo finito e $k \geq 1$ um inteiro tal que $(k, |G|) = 1$. Para cada k, definimos a seguinte aplicação*

$$\begin{array}{rccc} \phi_k : & G & \longrightarrow & G \\ & g & \longmapsto & kg. \end{array}$$

Claramente temos que ϕ_k é um automorfismo e isto implica que $kG = G$, onde $kG = \{kg \mid g \in G\}$.

O lema a seguir conhecido como a Lei Modular de Dedekind será usado no último capítulo.

Lema 1.1.4 (**Lei Modular de Dedekind**). *Sejam G um grupo e H, K e L subgrupos de G. Se $K \subseteq L$, então $(HK) \cap L = (H \cap L)K$.*

Demonstração. Claramente $(H \cap L)K \subseteq HK$ e $(H \cap L)K \subseteq LK = L$. Assim, obtemos que $(H \cap L)K \subseteq (HK) \cap L$. Por outro lado, vejamos que $(HK) \cap L \subseteq (H \cap L)K$. De fato, seja $g \in (HK) \cap L$, então $g = hk$ com $h \in H$ e $k \in K$. Isto implica que $h = gk^{-1} \in LK = L$. Desta forma, segue que $h \in H \cap L$. Logo, tem-se que $g \in (H \cap L)K$. Portanto, concluímos que $(HK) \cap L = (H \cap L)K$. □

Vamos agora definir uma classe de grupos importante para o nosso estudo que são os grupos nilpotentes. Antes disso, vejamos a definição de série normal e série central.

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

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G,$$

com $N_i \lhd G$ para todo $0 \leq i \leq r$.

Uma *série central* de G é uma série normal tal que

$$N_i/N_{i-1} \leq Z(G/N_{i-1}),$$

para todo $1 \leq i \leq r$.

Definição 1.1.5. *Dizemos que um grupo G é nilpotente se G possui uma série central.*

Vejamos a seguir uma série central, que será útil para verificar se um dado grupo G é nilpotente.

Seja G um grupo. Definimos os subgrupos $Z_i(G)$ recursivamente da seguinte forma: $Z_0(G) = 1$ e para cada $i \geqslant 1$ temos que $Z_i(G)$ é o único subgrupo normal em G tal que

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)).$$

Assim, obtém-se a seguinte sequência ascendente de subgrupos

$$1 = Z_0(G) \leq Z_1(G) = Z(G) \leq \cdots$$

Esta sequência é chamada *série central superior* de G. Observe que pela definição dos $Z_i(G)$, os mesmos são característicos em G.

Note que sempre temos a série central superior de um dado grupo G, mas não necessariamente esta série alcança G. Pode-se mostrar que quando existir um inteiro $r \geqslant 1$ tal que $Z_r(G) = G$, o grupo G será nilpotente. Assim, G é nilpotente se, e somente se, existe um inteiro $r \geqslant 1$ tal que $Z_r(G) = G$.

A próxima proposição nos fornece uma caracterização dos elementos de $Z_i(G)$, e explica melhor como estes elementos se comportam com respeito ao fazer comutadores com outros elementos em G. O resultado pode ser mostrado com um argumento indutivo sobre n.

Proposição 1.1.6. *Seja G um grupo. Para todo $n \geqslant 1$, temos que o n-ésimo termo da série central superior de G é dado por*

$$Z_n(G) = \{x \in G \mid [x, g_1, \ldots, g_n] = 1, \quad \text{para todos} \quad g_1, \ldots, g_n \in G\}.$$

É possível mostrar que quando G é um grupo nilpotente, a série central superior é a série de comprimento menor possível entre todas as séries centrais de G. Desta maneira, podemos definir o conceito de classe de nilpotência de um grupo.

Seja G um grupo nilpotente. O *menor* natural r tal que $Z_r(G) = G$ é chamado de *classe de nilpotência* de G.

Agora, vamos definir mais uma série central relevante no estudo de grupos nilpotentes.

Dado um grupo G, definimos os subgrupos $\gamma_i(G)$ recursivamente da seguinte forma: $\gamma_1(G) = G$ e $\gamma_{i+1}(G) = [\gamma_i(G), G]$ para $i \geqslant 1$.

Assim, temos a seguinte sequência descendente de subgrupos

$$G = \gamma_1(G) \geqslant \gamma_2(G) \geqslant \cdots$$

Esta sequência é chamada *série central inferior* de G. Note que os subgrupos $\gamma_i(G)$ são característicos em G.

Pode-se mostrar que um grupo G é nilpotente se, e somente se, existe um inteiro c tal que $\gamma_{c+1}(G) = 1$ e que a série superior e inferior de um grupo nilpotente possuem o mesmo comprimento. Assim, o menor inteiro c tal que $\gamma_{c+1}(G) = 1$, coincide com a classe de nilpotência de G.

É possível verificar que subgrupo de um grupo nilpotente é nilpotente e quociente de grupo nilpotente é também nilpotente.

A seguinte proposição é uma propriedade elementar de grupos nilpotentes que pode ser facilmente provada.

Proposição 1.1.7. *Seja G um grupo nilpotente de classe c e $H \lhd G$. Se $H \neq 1$, então $[H, G] < H$.*

Usando a definição de grupos nilpotentes podemos mostrar a proposição a seguir.

Proposição 1.1.8. *Sejam G um grupo e $H \lhd G$. Se G/H é nilpotente e $H \leq Z(G)$, então G é nilpotente.*

O próximo lema nos mostra uma caracterização de $\gamma_n(G)$ em termos dos geradores do grupo G.

Lema 1.1.9. *Sejam G um grupo e M um subconjunto de G. Se $G = \langle M \rangle$, então o n-ésimo termo da série central inferior de G é dado por*

$$\gamma_n(G) = \langle [m_1, \ldots, m_n]^g \mid m_1, \ldots, m_n \in M, g \in G \rangle .$$

Sabemos que em grupos abelianos o produto de n-ésimas potências é uma n-ésima potência. A seguinte Fórmula de Hall e Petresco fornece uma substituição para este conhecido fato. Para sua prova veja [**3**, Appendix A].

Teorema 1.1.10 (**Fórmula de Hall e Petresco**)**.** *Sejam x e y elementos de um grupo G e $n \geq 1$ um inteiro, então*

$$x^n y^n = (xy)^n g_2^{\binom{n}{2}} \ldots g_i^{\binom{n}{i}} \ldots g_{n-1}^n g_n,$$

onde $g_i \in \gamma_i(\langle x, y \rangle)$, para cada $i \geq 2$.

Seja p um primo. Um grupo G é dito ser um *p-grupo* se para todo g em G a ordem de g é uma potência de p. Se G é um grupo finito, então G é um p-grupo se, e somente se, $|G| = p^n$ para algum $n \in \mathbb{N}$.

O teorema a seguir fornece uma das classes mais importantes de grupos nilpotentes. Sua prova pode ser encontrada em [**14**, Theorem 4.1].

Teorema 1.1.11. *Todo p-grupo finito é nilpotente.*

O próximo lema relaciona um subgrupo de um p-grupo com um determinado termo da série central superior.

Lema 1.1.12. *Seja G um p-grupo finito. Se $H \lhd G$ tal que $|H| = p^n$ para algum $n \geq 1$, então $H \leq Z_n(G)$.*

Demonstração. Faremos a prova por indução em n. Se $n = 1$, então $|H| = p$ e como G é nilpotente, temos pela Proposição 1.1.7, que $[H, G] < H$. Agora, pelo Teorema de Lagrange, deduzimos que $[H, G] = 1$. Logo, $H \leq Z(G)$. Então, suponhamos que $n \geq 2$. Como $[H, G] < H$ temos que $|[H, G]| \in \{1, p, \ldots, p^{n-1}\}$. Desta forma, por hipótese de indução, obtém-se $[H, G] \leq Z_{n-1}(G)$. E isto implica que $H \leq Z_n(G)$, como queríamos. □

Seja G um grupo e H um subgrupo de G. Lembramos que H é dito um *subgrupo minimal* de G se H é próprio e sempre que existir $K \leq G$ tal que $1 \leq K \leq H$, então $K = 1$ ou $K = H$. Analogamente, define-se *subgrupo maximal* de G.

Se considerarmos a interseção de todos os subgrupos maximais em G, obtemos um importante subgrupo característico.

Sejam G um grupo e $\mathcal{M}$ o conjunto de todos os subgrupos maximais de G. O *subgrupo de Frattini* de G, denotado por $\Phi(G)$, é definido como

$$\Phi(G) = \begin{cases} \bigcap\limits_{M \in \mathcal{M}} M & se \quad \mathcal{M} \neq \emptyset \\ G & se \quad \mathcal{M} = \emptyset. \end{cases}$$

Recordemos que o subgrupo de um grupo G gerado pelas n-ésimas potências, denotado por G^n, é definido como sendo $G^n = \langle x^n \mid x \in G \rangle$. Pode-se mostrar que G^n é um subgrupo característico de G.

O próximo resultado descreve em detalhe o subgrupo de Frattini de um p-grupo finito G e, como consequência, fornece uma propriedade interessante sobre a cardinalidade dos conjuntos de geradores de G. Sua demonstração pode ser encontrada em [**24**, Theorem 5.3.2].

Teorema 1.1.13 (**Burnside**). *Seja G um p-grupo finito. Então, valem as seguintes afirmações.*
(i) $\Phi(G) = G'G^p$;
(ii) *Se $[G : \Phi(G)] = p^d$, então dado X um subconjunto de geradores de G existe Y subconjunto de X tal que $G = \langle Y \rangle$ e Y tem d elementos.*

A partir do teorema anterior a seguinte observação pode ser facilmente deduzida.

Observação 1.1.14. *Sejam p um primo e G um p-grupo. Suponha que um subgrupo de G gerado por um subconjunto $X \subseteq G$ pode ser gerado por m elementos. Então, $\langle X \rangle$ pode ser gerado por m elementos do conjunto X.*

O teorema a seguir é uma propriedade útil de grupos nilpotentes. Podemos encontrar sua prova em [**24**, Theorem 5.2.3].

Teorema 1.1.15. *Se A é um subgrupo normal abeliano maximal de um grupo nilpotente G, então $A = C_G(A)$.*

O próximo resultado nos dá várias caracterizações para grupos finitos nilpotentes. A demonstração pode ser vista em [**12**, Theorem 1.26].

Teorema 1.1.16. *Seja G um grupo finito. São equivalentes as seguintes afirmações.*
(i) *G é nilpotente;*
(ii) *$H < N_G(H)$, para todo subgrupo próprio $H < G$;*
(iii) *Todo subgrupo maximal de G é normal;*
(iv) *Todo p-subgrupo de Sylow de G é normal;*
(v) *G é o produto direto de seus p-subgrupos de Sylow.*

O teorema a seguir nos diz que o produto de dois subgrupos normais nilpotentes é um subgrupo nilpotente e nos fornece informações sobre a classe de nilpotência do produto em termos das classes de nilpotência dos dois fatores. A demonstração pode ser encontrada em [**24**, 5.2.8].

Teorema 1.1.17 (**Fitting**). *Sejam G um grupo, H e K subgrupos normais de G. Se H e K são nilpotentes de classes de nilpotência c e d respectivamente, então HK é nilpotente de classe de nilpotência no máximo $c + d$.*

O resultado anterior nos permite definir um subgrupo muito relevante na teoria de grupos.

Definição 1.1.18. *Seja G um grupo. O subgrupo de Fitting de G, denotado por $F(G)$, é definido como*

$$F(G) = \langle N \mid N \trianglelefteq G \text{ e } N \text{ nilpotente} \rangle.$$

Note que se G é finito, então $F(G)$ é nilpotente e é o único maior subgrupo normal nilpotente de G. Claramente, $F(G)$ é um subgrupo característico de G.

Agora, lembraremos a definição de outra classe importante de grupos para esta tese que são os grupos solúveis. Antes disso, vejamos a definição de série subnormal.

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

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G,$$

com $N_i \lhd N_{i+1}$ para todo $0 \leq i \leq r$.

Definição 1.1.19. *Um grupo G é dito solúvel se possui uma série subnormal*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_r = G,$$

tal que cada quociente G_i/G_{i-1} é abeliano para cada $1 \leq i \leq r$.

Assim como fizemos em grupos nilpotentes, vamos também aqui definir algumas séries que nos ajudam a ver se um dado grupo G é solúvel.

Dado um grupo G, definimos os subgrupos $G^{(i)}$ recursivamente da seguinte forma: $G^{(0)} = G$ e $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ para $i \geqslant 0$.

Assim, temos a seguinte sequência descendente de subgrupos

$$G = G^{(0)} \geqslant G^{(1)} \geqslant \cdots$$

Esta sequência é chamada *série derivada* de G. Note que os subgrupos $G^{(i)}$ são característicos em G.

Pode-se mostrar que um grupo G é solúvel se, e somente se, existe um inteiro $d \geqslant 1$ tal que $G^{(d)} = 1$. Além disso, subgrupos, quocientes e extensões de um grupo solúvel por um grupo solúvel são solúveis.

Seja G um grupo solúvel. Sendo a série derivada de G a de comprimento menor entre as séries normais descendentes de G com fatores abelianos que alcança 1, podemos definir o *comprimento derivado* de G como o *menor* inteiro positivo d tal que $G^{(d)} = 1$.

Ao longo deste trabalho, usaremos o conhecido Teorema de Feit e Thompson, sem explicitar referências. Para sua prova veja [**4**].

Teorema 1.1.20. *Todo grupo finito de ordem ímpar é solúvel.*

O seguinte lema nos fornece uma relação entre o comprimento derivado de um grupo solúvel finito não trivial e sua ordem.

Lema 1.1.21. *Seja G um grupo solúvel não trivial de ordem m e comprimento derivado d. Então, $d < m$.*

Demonstração. Faremos a prova por indução em d. Se $d = 1$, então claramente o resultado vale. Assim, suponhamos que $d \geq 2$. Considerando o grupo quociente $G/G^{(d-1)}$ temos, por hipótese de indução, que $d-1 < [G : G^{(d-1)}]$. Logo, $d < [G : G^{(d-1)}] + 1$. Como $G^{(d-1)}$ é um subgrupo próprio, segue que $d < m$. □

O próximo lema mostra como relacionam-se os subgrupos $\gamma_i(G), Z_i(G), G^{(i)}$ de um grupo G. Para a prova do mesmo veja [**24**, 5.1.11, 5.1.12].

Lema 1.1.22. *Sejam i, j inteiros positivos e G um grupo. Então, temos*
(i) $[\gamma_i(G), Z_j(G)] \leq Z_{j-i}(G)$ *se* $j \geq i$;
(ii) $G^{(i)} \leq \gamma_{2^i}(G)$.

Falaremos a seguir de mais uma série relevante no estudo de grupos solúveis.

Seja G um grupo finito. Definimos os subgrupos $F_i(G)$ recursivamente da seguinte forma: $F_0(G) = 1$ e para cada $i \geqslant 1$, temos que $F_i(G)$ é o único subgrupo

normal em G tal que

$$F_i(G)/F_{i-1}(G) = F(G/F_{i-1}(G)).$$

Assim, temos a seguinte sequência ascendente de subgrupos

$$1 = F_0(G) \leq F_1(G) = F(G) \leq F_2(G) \leq \cdots$$

Esta sequência é chamada *série de Fitting* de G. Note que para qualquer grupo solúvel finito G, existe a série de Fitting e a série alcança G. De fato, pode-se mostrar que G é solúvel se, e somente se, existe um inteiro $n \geqslant 1$ tal que $F_n(G) = G$.

Dado G um grupo solúvel finito, definimos o conceito de *altura de Fitting* de G como sendo o *menor* inteiro positivo n tal que $F_n(G) = G$ e o denotamos por $h(G)$.

Vejamos um lema sobre a altura de Fitting que será usado posteriormente.

Lema 1.1.23. *Seja G um grupo solúvel finito não trivial. Então,*

$$h(G) = h(G/F(G)) + 1.$$

Demonstração. Seja $\overline{G} = G/F(G)$ e suponhamos que $h(\overline{G}) = n$. Então, temos que a série de Fitting para $\overline{G}$ é dada por

$$1 = F_0(\overline{G}) \leq F_1(\overline{G}) \leq \cdots \leq F_n(\overline{G}) = \overline{G}.$$

Para cada $0 \leq i \leq n$, seja $F_i(G)$ a imagem inversa de $F_i(\overline{G})$ em G. Assim, obtemos a seguinte série para G

$$F_0(G) = F(G) \leq F_1(G) \leq \cdots \leq F_n(G) = G. \tag{1.1.1}$$

Como

$$F_{i+1}(\overline{G})/F_i(\overline{G}) = F\left(\overline{G}/F_i(\overline{G})\right),$$

segue, pelo terceiro Teorema do Isomorfismo, que

$$F_{i+1}(G)/F_i(G) = F\left(G/F_i(G)\right),$$

para todo $0 \leq i \leq n-1$. E como $F(G)$ é nilpotente, temos que a série (1.1.1) torna-se

$$1 \leq F(G) \leq F_1(G) \leq \cdots \leq F_n(G) = G,$$

que é uma série de Fitting para G de comprimento $n+1$. Claramente, temos que $h(G) = n+1$, pois caso contrário, poderíamos ter uma série de Fitting para $\overline{G}$

de altura menor do que n, que é um absurdo. Portanto, $h(G) = n + 1$ e assim o resultado segue. □

Vamos agora definir um conceito que será bastante utilizado ao longo desta tese.

Definição 1.1.24. *Seja G um grupo. O expoente de G é o menor inteiro positivo e tal que $g^e = 1$ para todo $g \in G$.*

Se existir tal inteiro dizemos que G possui *expoente finito*, caso contrário, dizemos que o expoente de G é infinito.

Assim, para cada grupo finito G, temos pelo Teorema de Lagrange, que o expoente de G, se existir, divide $|G|$, também para cada grupo G que possui expoente finito tem-se que a ordem de cada elemento divide o expoente de G.

Note ainda que o expoente de qualquer subgrupo ou grupo quociente de G divide o expoente de G. Além disso, dois grupos isomorfos possuem o mesmo expoente.

Pode-se mostrar que G^n é o menor subgrupo normal em G tal que o grupo quociente G/G^n possui expoente n.

O lema a seguir é bem conhecido, sua prova segue da definição de expoente.

Lema 1.1.25. *Sejam e um inteiro positivo, G um grupo e N_1 e N_2 subgrupos normais de G. Se G/N_1 e G/N_2 possuem expoente dividindo e, então $G/(N_1 \cap N_2)$ também possui expoente dividindo e.*

O seguinte lema será muito utilizado ao longo deste trabalho. A demonstração do mesmo pode ser encontrada em [**13**, Corollary 2.5.4].

Lema 1.1.26. *Se G é um grupo nilpotente de classe c gerado por elementos de ordem dividindo m, então o expoente de G divide m^c.*

Sejam G um grupo e r um inteiro positivo. Dizemos que G é *r-gerado* se existe um subconjunto X de G com r elementos tal que $G = \langle X \rangle$.

Outro conceito relevante nesta tese é o de posto de um grupo finito. Vejamos a sua definição.

Definição 1.1.27. *Um grupo finito G é dito ser de posto r se r é o menor número tal que qualquer subgrupo de G é r-gerado. Vamos denotar por $r(G)$ o posto de G.*

Um fato conhecido relativo à altura de Fitting de um grupo solúvel é o seguinte lema. Para sua prova veja [**16**, Lemma 2.4].

Lema 1.1.28. *Um grupo solúvel finito G de posto r tem altura de Fitting limitada em termos de r.*

Outro resultado que vamos precisar é o lema a seguir.

Lema 1.1.29. *A ordem de um grupo finito G de expoente e com posto r é (e, r)-limitada.*

Demonstração. Com efeito, se G é um p-grupo o resultado segue de [**14**, Corollary 11.21]. Suponhamos que G não seja um p-grupo, então a sua ordem é o produto das ordens de seus subgrupos de Sylow. Agora, como os primos divisores da ordem de G são divisores de e, o resultado está provado. □

Finalizamos esta seção relembrando o conceito de π-subgrupo de Hall.

Sejam π um conjunto não vazio de primos e π' o seu complementar, isto é, $\pi' = \mathbb{P}\backslash\pi$, onde $\mathbb{P}$ é o conjunto de todos os primos. Dizemos que um inteiro m é um *π-número* se todo primo divisor de m pertence a π e um *π'-número* é um número inteiro sem divisores primos em π.

Seja G um grupo finito. Um subgrupo H de G é dito um *π-subgrupo de Hall* de G se $|H|$ é um π-número e $[G : H]$ é um π'-número.

É claro que se $\pi = \{p\}$, então a definição de π-subgrupo de Hall coincide com a definição de p-subgrupo de Sylow.

O próximo lema, conhecido como *Argumento de Frattini* é uma consequência simples da teoria de Sylow. Para demonstração deste fato veja [**5**, 1.3.7].

Lema 1.1.30 (**Argumento de Frattini**)**.** *Seja H um subgrupo normal finito de um grupo G. Se P é um p-subgrupo de Sylow de H, então $G = HN_G(P)$.*

Seja G um grupo finito. Sabemos por teoria de Sylow que, em G, sempre existe p-subgrupo de Sylow para todo primo p que divide $|G|$ e quaisquer dois deles são conjugados em G. No entanto, se π consiste de dois ou mais primos, então pode ou não existir π-subgrupo de Hall em G e, caso exista, pode ou não acontecer que quaisquer dois π-subgrupos de Hall são conjugados em G. Porém, é conhecido, por exemplo, que em grupos solúveis, existem π-subgrupos de Hall e quaisquer dois deles são conjugados.

O Teorema de Schur e Zassenhaus a seguir nos fornece uma importante condição para a existência e conjugação de π'-subgrupos de Hall em G. Sua prova pode ser encontrada em [**5**, 6.2.1].

Teorema 1.1.31 (**Schur e Zassenhaus**). *Seja H um π-subgrupo de Hall normal de um grupo finito G. As seguintes afirmações valem.*
(i) *G possui um π'-subgrupo de Hall K tal que $G = HK$ e $H \cap K = 1$;*
(ii) *Se H ou G/H é solúvel, então quaisquer dois π'-subgrupos de Hall de G são conjugados.*

1.2. p-Grupos Finitos Powerful

Finalizamos este capítulo tratando brevemente da teoria de p-grupos finitos powerful. Esta teoria foi basicamente criada por A. Lubotzky e A. Mann, em [**20**], no ano de 1987. Os p-grupos powerful possuem muitas propriedades boas e várias aplicações em, por exemplo, p-grupos finitos. Essa classe de grupos compartilha de algumas propriedades que os grupos abelianos possuem. Nesta seção, vamos definir e enunciar alguns resultados acerca desses grupos e a prova dos mesmos podem ser encontradas, por exemplo, em [**3**].

Para não confundir o leitor, optamos por não traduzir o termo *powerful* para o português, pois é conhecido que existe outra definição de *"potent group"* e ela não será usada neste trabalho.

Vamos agora definir o objeto de estudo desta seção.

Definição 1.2.1. *Um p-grupo finito G é chamado de powerful se $G' \leq G^p$ para $p \neq 2$, ou se $G' \leq G^4$ para $p = 2$.*

Precisa-se fazer diferença, na definição anterior, entre $p = 2$ e $p \neq 2$, pois sabemos que se G é um 2-grupo, então sempre temos que $G' \leq G^2$.

Obviamente, todo p-grupo finito abeliano é powerful. No entanto, se p for ímpar e G um p-grupo finito não abeliano de expoente p, então G não é powerful, pois $1 \neq G' \not\leq G^p = 1$. Um exemplo concreto de um grupo que não é powerful é o diedral de ordem 8, isto é, D_4, que é definido por $D_4 = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1} \rangle$. Uma vez que $(D_4)' = \langle x^2 \rangle \not\leq 1 = (D_4)^4$.

Um fato curioso sobre esses grupos é que nem todo subgrupo de um p-grupo powerful é powerful. Com efeito, seja o grupo $G = D_4 \times C_8$, onde D_4 é o diedral de ordem 8 que tem apresentação conforme vista anteriormente e $C_8 = \langle c \rangle$ é o grupo cíclico de ordem 8. Sejam $x, y \in D_4$ e $c \in C_8$, definimos

$$N = \left\langle [x, y]^{-1} c^4 \right\rangle = \left\langle x^2 c^4 \right\rangle \leq G.$$

Evidentemente, N é normal em G. Assim, consideremos o grupo quociente $\overline{G} = G/N$. Note que $\overline{G}$ é um 2-grupo powerful, pois

$$\overline{G}' = [G/N, G/N] = [G, G]N/N = \left\langle x^2 N \right\rangle = \left\langle c^4 N \right\rangle \leq \overline{G}^4.$$

Agora, fazendo $\overline{H} = \langle xN, yN\rangle$, temos que $\overline{H}$ é um subgrupo próprio de $\overline{G}$ e isomorfo a D_4. E como D_4 não é powerful, segue que $\overline{H}$ também não é powerful. Portanto, $\overline{G}$ é powerful, mas contém um subgrupo próprio que não é, como queríamos.

Por outro lado, é conhecido que se G é um p-grupo finito powerful, então os subgrupos $\gamma_i(G), G^{p^i}$ e $G^{(i)}$ são powerful, para todo inteiro positivo i.

Esses grupos possuem boas propriedades e destacamos a seguir uma que será usada posteriormente e de fácil demonstração.

Lema 1.2.2. *Se G é um p-grupo finito powerful gerado por elementos de ordem dividindo m, então o expoente de G divide m.*

Um outro resultado que usaremos envolvendo esses grupos será mencionado no Capítulo 3. Finalizamos esta seção, com uma proposição que exemplifica que p-grupos powerful possuem propriedades semelhantes a de grupos abelianos. Para sua prova veja [**3**, Proposition 2.6, Theorem 2.7, Corollary 2.8].

Proposição 1.2.3. *Seja G um p-grupo finito powerful.*
(i) *Então $G^{p^i} = \{x^{p^i} \mid x \in G\}$ para todo inteiro positivo i;*
(ii) *Se $G = \langle x_1, \ldots, x_d\rangle$, então $G = \langle x_1\rangle \cdots \langle x_d\rangle$;*
(iii) *Se $G = \langle x_1, \ldots, x_d\rangle$, então $G^{p^i} = \langle x_1^{p^i}, \ldots, x_d^{p^i}\rangle$ para todo inteiro positivo i.*

2

Automorfismos de Grupos

Neste capítulo, definiremos conceitos que serão amplamente utilizados ao longo desta tese e ressaltaremos alguns fatos bem conhecidos a respeito de automorfismos. Também provaremos resultados que surgiram ao longo das nossas investigações e que serão usados nos capítulos seguintes. Primeiramente, daremos uma noção geral de automorfismos em um grupo qualquer, depois nos concentraremos em grupos finitos que admitem um automorfismo coprimo, conforme mostra a primeira seção, e por fim, em grupos de ordem ímpar que admitem um automorfismo involutório.

Sejam G um grupo e ϕ um automorfismo de G. Definimos o *subgrupo dos pontos fixos* de ϕ em G, denotado por G_ϕ, como

$$G_\phi = \{x \in G \mid x^\phi = x\}.$$

O subgrupo G_ϕ também é chamado de *centralizador* de ϕ em G e algumas vezes será usada a notação $C_G(\phi)$ para denotar este subgrupo.

Denotemos por $G_{-\phi}$ o conjunto $\{x^{-1}x^\phi \mid x \in G\}$. O subgrupo gerado por $G_{-\phi}$ será denotado por $[G, \phi]$.

Dados G um grupo e ϕ um automorfismo de G, dizemos que um subgrupo H de G é *ϕ-invariante* se $[H, \phi] \leq H$. Sabemos que $[G, \phi]$ é um subgrupo normal ϕ-invariante de G.

Sejam G um grupo, ϕ um automorfismo de G e N um subgrupo normal ϕ-invariante de G. Consideremos a aplicação $\overline{\phi}$ do grupo quociente G/N, induzida por ϕ, definida por $(xN)^{\overline{\phi}} = x^\phi N$. Note que $\overline{\phi}$ está bem definida, pois N é ϕ-invariante e obviamente $\overline{\phi}$ é um automorfismo de G/N chamado de *automorfismo induzido* de G/N. Faremos um abuso de notação indicando $\overline{\phi}$ por apenas ϕ. Note que ϕ induz o automorfismo trivial de $G/[G, \phi]$, pois se $g \in G$, então podemos

escrever $g^\phi = g(g^{-1}g^\phi)$, daí aplicando o automorfismo induzido de $G/[G,\phi]$, temos

$$(g[G,\phi])^\phi = g^\phi[G,\phi] = g[G,\phi].$$

Seja ϕ um automorfismo de um grupo G. Dizemos que ϕ é um *automorfismo involutório* se a ordem de ϕ for dois. Um automorfismo ϕ de um grupo finito G é chamado de *coprimo* se $(|G|,|\phi|) = 1$.

2.1. Automorfismos Coprimos

O lema a seguir reúne alguns fatos bem conhecidos sobre automorfismos coprimos que serão amplamente utilizados ao longo deste trabalho.

Lema 2.1.1. *Seja ϕ um automorfismo coprimo de um grupo finito G. As seguintes afirmações valem.*
(i) *Se N é um subgrupo normal ϕ-invariante de G, então $(G/N)_\phi = G_\phi N/N$;*
(ii) $G = G_\phi[G,\phi]$;
(iii) $[G,\phi] = [G,\phi,\phi]$;
(iv) *Seja $\pi(G)$ o conjunto de todos os primos divisores de $|G|$. Para cada primo $p \in \pi(G)$, ϕ deixa invariante algum p-subgrupo de Sylow de G.*

Demonstração. (i) Claramente, temos que $G_\phi N/N \leq (G/N)_\phi$. Agora, vejamos que $(G/N)_\phi \leq G_\phi N/N$. Para isto, mostraremos que toda classe ϕ-invariante gN de N contém um elemento de G_ϕ. A prova será feita por indução em $|\phi|$.

Primeiramente, suponhamos que $|\phi| = p$, onde p é um número primo. Seja gN uma classe ϕ-invariante de N. Consideremos a ação de $\langle\phi\rangle$ em gN. Temos que o tamanho de qualquer $\langle\phi\rangle$-órbita em gN divide p. Logo, cada tamanho é 1 ou p. Sabemos que a classe gN é a união disjunta dessas órbitas. Assim, se todas as órbitas são de tamanho p, então p dividiria $|gN| = |N|$, o que é uma contradição, pois ϕ é um automorfismo coprimo de G. Desta forma, concluímos que existe pelo menos uma órbita de tamanho 1 e isto implica que gN contém um elemento de G_ϕ.

Agora, suponhamos que $|\phi| = mn$ é um número composto, com $m, n > 1$. Por hipótese de indução e pelo Teorema do Isomorfismo, temos

$$C_{G/N}(\phi^n) = C_G(\phi^n)N/N \cong C_G(\phi^n)/(C_G(\phi^n) \cap N). \tag{2.1.1}$$

Observe que $gN \in C_{G/N}(\phi^n)$, pois gN é ϕ^n-invariante. Assim, por (2.1.1), existe $g_0 \in C_G(\phi^n)$ tal que $g_0N = gN$. Isto implica que $g_0^\phi \in g_0N$. Por outro lado, sabendo que $C_G(\phi^n)$ é ϕ-invariante, obtemos $g_0^\phi \in C_G(\phi^n)$. Desta maneira, tem-se $g_0^{-1}g_0^\phi \in C_G(\phi^n) \cap N$. Logo, a classe $g_0(C_G(\phi^n) \cap N)$ é também ϕ-invariante.

Além disso, como ϕ age como um automorfismo de ordem n em $C_G(\phi^n)$ segue, por hipótese de indução, que a classe $g_0(C_G(\phi^n) \cap N)$ contém um elemento g_1 de $C_G(\phi)$. Este elemento é o desejado, uma vez que

$$g_1 \in g_0(C_G(\phi^n) \cap N) \subseteq g_0 N = gN.$$

Logo, obtemos $(G/N)_\phi \leq G_\phi N/N$. Portanto, concluímos que $(G/N)_\phi = G_\phi N/N$.
(ii) Sabemos que ϕ induz o automorfismo trivial em $G/[G,\phi]$. Então, tem-se $(G/[G,\phi])_\phi = G/[G,\phi]$. Agora, usando o item (i), deste lema obtemos

$$G/[G,\phi] = G_\phi[G,\phi]/[G,\phi].$$

Isto implica que $G = G_\phi[G,\phi]$, como queríamos.
(iii) Com efeito, utilizando o item (ii), deste lema tem-se

$$\begin{aligned}
[G,\phi] &= [G_\phi[G,\phi],\phi] \\
&= \left\langle x^{-1}x^\phi \mid x \in G_\phi[G,\phi] \right\rangle \\
&= \left\langle (ab)^{-1}(ab)^\phi \mid a \in G_\phi, b \in [G,\phi] \right\rangle \\
&= \left\langle b^{-1}b^\phi \mid b \in [G,\phi] \right\rangle \\
&= [[G,\phi],\phi].
\end{aligned}$$

Como desejado.
(iv) Façamos $A = \langle\phi\rangle$ e $\pi = \pi(G)$. Seja $G^* = GA$ o produto semi-direto de G por A. Como $(|A|,|G|) = 1$, temos que G é um π-subgrupo de Hall normal de G^* e A é um π'-subgrupo de Hall de G^*. Além disso, segue que A ou G é solúvel. Assim, como A é isomorfo a G^*/G, obtém-se que G ou G^*/G é solúvel. Agora, o Teorema de Schur e Zassenhaus 1.1.31, item (ii), aplicado em G^*, afirma que qualquer outro π'-subgrupo de Hall de G^* é conjugado a A. Uma vez que $G^* = GA$, podemos assumir que o elemento conjugador pertence a G, pois seja H um π'-subgrupo de Hall de G^*, então pelo Teorema de Schur e Zassenhaus 1.1.31, existe $x = ga \in G^*$ com $g \in G$ e $a \in A$ tal que $A = H^x$. Daí, tem-se $A = H^g$.

Agora, sejam P um p-subgrupo de Sylow de G e $N = N_{G^*}(P)$. Pelo Argumento de Frattini 1.1.30, temos que $G^* = GN$. Isto implica que $N/G\cap N$ é isomorfo a A. Observe que $G\cap N$ é um π-subgrupo de Hall normal de N. Então, pelo Teorema de Schur e Zassenhaus 1.1.31, item (i), segue que N possui um π'-subgrupo de Hall B. Claramente, B é também um π'-subgrupo de Hall de G^*. Então, tem-se $A = B^x$ para algum $x \in G$. Agora, como $B \leq N$, resulta que B deixa P invariante. Disto segue que A deixa invariante P^x, o p-subgrupo de Sylow de G. Pois, seja $a \in A$,

como $A = B^x$, temos que existe $b \in B$ tal que $a = x^{-1}bx$. Isto implica que

$$(P^x)^a = x^{-1}b^{-1}x(x^{-1}Px)x^{-1}bx = P^x.$$

Portanto, concluímos que A deixa invariante algum p-subgrupo de Sylow de G. Como o primo p foi tomado arbitrariamente, o resultado vale para todo $p \in \pi$. □

Vamos precisar também do resultado a seguir. Além disso, usaremos a seguinte notação $y^{-\phi} = (y^{-1})^{\phi}$.

Lema 2.1.2. *Seja ϕ um automorfismo coprimo de um grupo finito G. Se N é um subgrupo normal ϕ-invariante de G contido em G_ϕ, então $[G, \phi]$ centraliza N.*

Demonstração. Sejam $x \in N$ e $y \in G$. Note que os elementos x e x^y pertencem a G_ϕ, logo temos $x^y = (x^y)^\phi = x^{y^\phi}$. Isto implica que $x = x^{yy^{-\phi}}$. Assim, como os elementos da forma $yy^{-\phi}$ geram $[G, \phi]$, o lema está provado. □

É conhecido e trataremos na próxima seção, que se G é um grupo finito de ordem ímpar e ϕ é um automorfismo involutório de G, então $G = G_{-\phi}G_\phi$. Uma pergunta de interesse próprio que surgiu ao longo do nosso estudo foi a seguinte: a igualdade $G = G_{-\phi}G_\phi$ vale para qualquer automorfismo coprimo ϕ? Veremos que em geral esta igualdade pode falhar. No entanto, percebemos que a igualdade $G = G_{-\phi}G_\phi$ vale quando o grupo em questão é nilpotente. Este fato foi muito relevante nas nossas investigações e será usado para provar os Teoremas C e D. Portanto, vamos agora nos concentrar em demonstrar este fato, além de exibirmos um contra-exemplo de quando a igualdade não se verifica.

O próximo lema nos fornece uma caracterização muito útil de quando a igualdade $G = G_{-\phi}G_\phi$ vale.

Lema 2.1.3. *Seja ϕ um automorfismo coprimo de um grupo finito G. Então, $G = G_{-\phi}G_\phi$ se, e somente se, nenhum elemento não trivial de $G_{-\phi}$ possui conjugados em G_ϕ.*

Demonstração. Assumamos que $G = G_{-\phi}G_\phi$. Como $|G| = |G_{-\phi}||G_\phi|$, segue que cada elemento $x \in G$ pode ser escrito unicamente na forma $x = gh$, com $g \in G_{-\phi}$ e $h \in G_\phi$. Agora, suponhamos que existem elementos $1 \neq a \in G_\phi$ e $b, c \in G$ tal que

$$(b^{-1}b^\phi)^{c^{-1}} = a.$$

Isto implica que

$$b^{-1}b^\phi = c^{-1}ac,$$

de onde obtemos

$$c^{\phi^{-1}}b^{-1}b^{\phi}c^{-1} = c^{\phi^{-1}}c^{-1}a. \tag{2.1.2}$$

Note que existem pelo menos duas maneiras de escrever o elemento $x = c^{\phi^{-1}}b^{-1}b^{\phi}c^{-1}$ na forma $x = gh$ com $g \in G_{-\phi}$ e $h \in G_{\phi}$. De fato, por um lado, em (2.1.2), faça $g = c^{\phi^{-1}}c^{-1}$ e $h = a$. Observe que $g \in G_{-\phi}$, pois fazendo $y = (c^{-1})^{\phi^{-1}} \in G$ tem-se $y^{\phi} = c^{-1}$. Daí, $g = y^{-1}y^{\phi} \in G_{-\phi}$ e claramente $h = a \in G_{\phi}$. Por outro lado, em (2.1.2), faça $g_1 = c^{\phi^{-1}}b^{-1}b^{\phi}c^{-1}$ e $h_1 = 1$. Note que $g_1 \in G_{-\phi}$, pois fazendo $y = b(c^{-1})^{\phi^{-1}} \in G$ tem-se $y^{\phi} = b^{\phi}c^{-1}$. Daí, $g_1 = y^{-1}y^{\phi} \in G_{-\phi}$ e $h_1 = 1 \in G_{\phi}$. Assim, obtemos que existem duas maneiras de escrever o elemento x, o que é uma contradição. Portanto, concluímos que nenhum elemento não trivial de $G_{-\phi}$ tem conjugados em G_{ϕ}.

Agora, assumamos que nenhum elemento não trivial de $G_{-\phi}$ possui conjugados em G_{ϕ}. Queremos provar que $G = G_{-\phi}G_{\phi}$. Suponhamos que isto seja falso. Como $|G| = |G_{-\phi}||G_{\phi}|$, temos $gh = g_1h_1$ para algum par distinto de elementos $g, g_1 \in G_{-\phi}$ e $h, h_1 \in G_{\phi}$. Em particular, segue que existem elementos $x, y \in G$ e $1 \neq a \in G_{\phi}$ tal que $x^{-1}x^{\phi} = y^{-1}y^{\phi}a$. Isto implica que

$$(yx^{-1}x^{\phi}y^{-\phi})^{y^{\phi}} = a.$$

Além disso, note que $yx^{-1}x^{\phi}y^{-\phi} \in G_{-\phi}$ é não trivial e possui um conjugado em G_{ϕ}. Isto é uma contradição com a hipótese. Portanto, concluímos que $G = G_{-\phi}G_{\phi}$ e o lema segue. □

O próximo exemplo mostra que em geral $G \neq G_{-\phi}G_{\phi}$. O mesmo foi comunicado a P. Shumyatsky por G. Glauberman.

Exemplo 2.1.4. *Sejam K o corpo com 5^3 elementos e ϕ o automorfismo de ordem 3 de K que leva cada $x \in K$ em x^5. Denotemos por $A = (K, +)$ o grupo aditivo de K e por $B = (K \setminus \{0\}, \cdot)$ o grupo multiplicativo de K. Seja $G = AB$ o produto semi-direto natural de A por B. Temos que B age transitivamente em $A \setminus \{0\}$ e claramente ϕ induz um automorfismo coprimo em G. Observe que*

$$A_{\phi} = \{a \in A \mid a^4 = 1\} \cup \{0\}$$

é um subgrupo próprio de A e $A_{-\phi} = \{-a + a^5 \mid a \in A\} \neq 0$. Assim, como B age transitivamente em $A \setminus \{0\}$ segue que todos os elementos não triviais de $A_{-\phi}$ são conjugados em G com alguns elementos em A_{ϕ}. Desta forma, aplicando o Lema 2.1.3, obtemos que $G \neq G_{-\phi}G_{\phi}$.

Observe que o grupo G no exemplo anterior não é nilpotente. Assim, o seguinte lema mostra que nenhum exemplo deste tipo pode ser encontrado entre grupos nilpotentes.

Lema 2.1.5. *Seja ϕ um automorfismo coprimo de um grupo nilpotente finito G. Então, qualquer elemento $x \in G$ pode ser escrito unicamente na forma $x = gh$, onde $g \in G_{-\phi}$ e $h \in G_{\phi}$.*

Demonstração. Suponhamos que G seja um contra-exemplo de ordem mínima possível de que o lema não vale. Então, pelo Lema 2.1.3, podemos escolher elementos $x, g \in G$ e $1 \neq h \in G_{\phi}$ tal que

$$(x^{-1}x^{\phi})^{g} = h. \tag{2.1.3}$$

Note que, por hipótese de indução, $G/Z(G)$ não é um contra-exemplo do lema, uma vez que $1 \neq |G/Z(G)| < |G|$. Então, o resultado vale para $G/Z(G)$. Agora, considerando o epimorfismo canônico de G em $G/Z(G)$, tem-se

$$(x^{-1}x^{\phi}Z(G))^{gZ(G)} = hZ(G).$$

Isto implica que $h \in Z(G)$. De fato, se $h \notin Z(G)$ teríamos

$$(x^{-1}x^{\phi}Z(G))^{gZ(G)} = hZ(G) \neq Z(G).$$

o que não ocorre, pois em $G/Z(G)$, o Lema 2.1.3 vale, logo $h \in Z(G)$. Assim, segue de (2.1.3) que $x^{-1}x^{\phi} = h$. Então, considerando o produto semi-direto natural $G\langle\phi\rangle$, obtemos

$$x^{-1}x^{\phi}\phi^{-1} = h\phi^{-1}.$$

Que implica em

$$(\phi^{-1})^{x} = h\phi^{-1}. \tag{2.1.4}$$

Observe que a ordem do elemento $(\phi^{-1})^{x}$ é n, onde n é a ordem de ϕ. E como $h \in G_{\phi}$, temos que a ordem do elemento $h\phi^{-1}$ é $|h|n \neq n$. O que é uma contradição com (2.1.4). Portanto, o resultado vale para G. □

Utilizando o lema anterior, obtemos o seguinte resultado que será usado posteriormente.

Lema 2.1.6. *Seja G um grupo finito nilpotente admitindo um automorfismo coprimo ϕ. Se K é um subgrupo ϕ-invariante de G gerado por um subconjunto S de $G_{-\phi}$, então $K = [K, \phi]$.*

Demonstração. Claramente, temos $[K, \phi] \leq K$. Assim, precisamos provar que $K \leq [K, \phi]$. Para isto, note que como $K = \langle S\rangle$ com $S \subseteq G_{-\phi}$, é suficiente

mostrar que $s \in [K, \phi]$ para todo $s \in S$. De fato, seja $s \in S$. Uma vez que K é ϕ-invariante, segue pelo Lema 2.1.5, que $s = xy$ com $x \in K_\phi$ e $y \in K_{-\phi}$. Agora, pela unicidade de s, obtemos que $s = y \in K_{-\phi}$. Logo, $s \in [K, \phi]$. Portanto, $K = [K, \phi]$. □

O próximo teorema é devido a A. Mann. Sua demonstração pode ser encontrada em [**22**].

Teorema 2.1.7 (A. Mann). *Seja G um grupo tal que $G/Z(G)$ é localmente finito e tem expoente e. Então, G' é localmente finito e possui expoente finito que é e-limitado.*

A proposição a seguir será bastante utilizada nos capítulos subsequentes.

Proposição 2.1.8. *Seja G um grupo finito admitindo um automorfismo coprimo ϕ e assuma que G é solúvel com comprimento derivado d. Suponha que $G = [G, \phi]$ e $x^e = 1$ para cada $x \in G_{-\phi}$. Então, G possui expoente (d, e)-limitado.*

Demonstração. A prova será feita por indução em d. Se $d = 1$, o resultado é óbvio, então assumamos que $d \geq 2$. Seja $M = G^{(d-1)}$ o último termo não trivial da série derivada de G. Como o comprimento derivado de G/M é menor do que d, segue por hipótese de indução, que o expoente de G/M é (d, e)-limitado. Agora, pelo Lema 2.1.5, tem-se $M = M_{-\phi}M_\phi$. Além disso, como M é abeliano e $(M_{-\phi})^e = 1$, deduzimos que $M^e \leq M_\phi$. Aplicando o Lema 2.1.2, resulta em $M^e \leq Z(G)$. Consequentemente, o expoente de $G/Z(G)$ é (d, e)-limitado. O Teorema de Mann 2.1.7 garante que G' possui expoente (d, e)-limitado. Isto implica que M também possui expoente (d, e)-limitado. Portanto, concluímos que o expoente de G é (d, e)-limitado, como queríamos. □

2.2. Automorfismos Involutórios

O próximo lema é uma coleção de fatos conhecidos sobre automorfismos involutórios.

Lema 2.2.1. *Seja G um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ. As seguintes afirmações valem.*
(i) *$G = G_\phi G_{-\phi} = G_{-\phi}G_\phi$ e cada elemento $x \in G$ pode ser escrito unicamente na forma $x = gh$, onde $g \in G_{-\phi}$ e $h \in G_\phi$;*
(ii) *Se N é um subgrupo normal ϕ-invariante de G, então*

$$(G/N)_{-\phi} = \{xN \mid x \in G_{-\phi}\};$$

(iii) *Se N é um subgrupo normal ϕ-invariante de G tal que $N = N_{-\phi}$ ou $N = N_{\phi}$, então $[G, \phi]$ centraliza N;*
(iv) *O fecho normal de G_{ϕ} contém G';*
(v) *G_{ϕ} normaliza o conjunto $G_{-\phi}$.*

Demonstração. (i) Primeiramente, note que se $y = x^{-1}x^{\phi} \in G_{-\phi}$, então

$$y^{\phi} = (x^{-1}x^{\phi})^{\phi} = (x^{\phi})^{-1}x = y^{-1}, \tag{2.2.1}$$

pois ϕ tem ordem dois. Agora, consideremos $\{x_i \mid 1 \leq i \leq n\}$ um conjunto completo de representantes de classes laterais à direita de G_{ϕ} em G e o conjunto $I = \{y_i = x_i^{-1}x_i^{\phi} \mid 1 \leq i \leq n\}$. Claramente, temos que $y_i \in G_{-\phi}$ para todo $i \in \{1, \ldots, n\}$. Desejamos provar que I é também um conjunto completo de representantes de classes laterais à direita de G_{ϕ} em G. De fato, suponhamos por absurdo que isto não ocorre, então temos $y_j = zy_i$ para algum $z \in G_{\phi}$ e $i \neq j$. Aplicando ϕ na última igualdade e usando (2.2.1), resulta em $y_j^{-1} = zy_i^{-1}$. Isto implica que $y_j = y_i z^{-1}$. Assim, $zy_i = y_i z^{-1}$. Daí, tem-se $z^{y_i} = z^{-1}$. Com isto, deduzimos que $z^{y_i^2} = z$. Logo, y_i^2 centraliza z. Agora, uma vez que $|G|$ é ímpar segue que y_i centraliza z. Então, temos $z^{y_i} = z = z^{-1}$, e consequentemente, $z = z^{-1}$. Além disso, como a ordem de z é ímpar, resulta em $z = 1$. Assim, $y_i = y_j$. Logo, $x_i^{-1}x_i^{\phi} = x_j^{-1}x_j^{\phi}$ e disto segue que

$$(x_i x_j^{-1})^{\phi} = x_i x_j^{-1}.$$

Daí, concluímos que $x_i x_j^{-1} \in G_{\phi}$. Então x_i e x_j determinam a mesma classe lateral à direita de G_{ϕ} em G, o qual é um absurdo, pois $i \neq j$. Portanto, I é um conjunto completo de representantes de classes laterais à direita de G_{ϕ} em G, como desejado.

Agora, vejamos que $I = G_{-\phi}$. Com efeito, já sabemos que $I \subseteq G_{-\phi}$, resta mostrarmos que $G_{-\phi} \subseteq I$. Para isto, suponhamos que $u = zy_i \in G_{-\phi}$ para algum $z \in G_{\phi}$ e algum $i \in \{1, \ldots, n\}$. Então, por (2.2.1), tem-se

$$u^{-1} = u^{\phi} = (zy_i)^{\phi} = zy_i^{-1},$$

de onde obtemos que $z^{y_i} = z^{-1}$. Assim, procedendo da mesma maneira que fizemos no parágrafo anterior, vamos concluir que $z = 1$. Logo, $u = y_i \in I$. Portanto, $I = G_{-\phi}$ que implica em $G = G_{\phi}G_{-\phi}$. Por outro lado, utilizando as classes laterais à esquerda de G_{ϕ} em G, obtemos de maneira similar que $G = G_{-\phi}G_{\phi}$. Desta forma, temos que $G = G_{\phi}G_{-\phi} = G_{-\phi}G_{\phi}$.

Por fim, notemos que $G_\phi \cap G_{-\phi} = 1$. De fato, seja $x \in G_\phi \cap G_{-\phi}$, então

$$x = x^\phi = x^{-1},$$

e isto implica que $x = 1$. Logo, $G_\phi \cap G_{-\phi} = 1$. Portanto, segue deste fato, que todo elemento $x \in G$ se escreve de modo único como $x = gh$ com $g \in G_{-\phi}$ e $h \in G_\phi$ e o item (i) está provado.

(ii) Claramente tem-se $\{xN \mid x \in G_{-\phi}\} \subseteq (G/N)_{-\phi}$. Agora, vejamos que $(G/N)_{-\phi} \subseteq \{xN \mid x \in G_{-\phi}\}$. Seja $xN \in (G/N)_{-\phi}$, então $(xN)^\phi = x^{-1}N$. Nosso objetivo é mostrar que pelo menos um dos elementos de xN está em $G_{-\phi}$. Com efeito, suponhamos que $|N| = t + 1$, onde $t = 2k$ para algum $k \in \mathbb{N}$. Assim, $xN = \{xn_0, xn_1, \ldots, xn_t\}$, onde $n_0 = 1$ e $n_i \in N$ para todo $i \in \{0, \ldots, t\}$. Então, temos que $x^{-1}N = \{(xn_0)^{-1}, (xn_1)^{-1}, \ldots, (xn_t)^{-1}\}$. Agora, como $(xN)^\phi = x^{-1}N$, podemos pensar, em xN, que ϕ se comporta como uma permutação dos índices dos elementos de N, ou seja, $\phi(xn_i) = (xn_j)^{-1}$. Desta maneira, por simplicidade, vamos identificar esta última igualdade por

$$\phi(i) = j,$$

onde $i, j \in S = \{s \in \mathbb{N} \mid 0 \leq s \leq t\}$. Logo, mostrar que $xN \in \{xN \mid x \in G_{-\phi}\}$ equivale a mostrar que $\phi(i) = i$ para algum $i \in S$. Com efeito, suponhamos por absurdo, que $\phi(i) \neq i$ para todo $i \in S$. Além disso, observe que a permutação ϕ tem a seguinte propriedade: se $\phi(i) = j$, então $\phi(j) = i$, pois como ϕ possui ordem dois, tem-se

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

Logo, $\phi(j) = i$. Agora, combinando esta propriedade de ϕ com o fato que o conjunto S possui tamanho ímpar, obtemos uma contradição com a suposição inicial. Portanto, concluímos que $\phi(i) = i$ para algum $i \in S$, como queríamos e o resultado do item (ii) segue.

(iii) Se $N = N_\phi$, então $N \leq G_\phi$ e o resultado segue do Lema 2.1.2. Agora, suponhamos que $N = N_{-\phi}$. Sejam $x \in N$ e $g \in G$, temos que $x^g \in N_{-\phi}$, logo $(x^g)^\phi = (x^g)^{-1}$. Por outro lado, como $x \in N_{-\phi}$, tem-se $(x^g)^\phi = (x^{-1})^{g^\phi}$. Daí, obtemos $(x^{-1})^g = (x^{-1})^{g^\phi}$. E isto implica que $x^{-1} = (x^{-1})^{gg^{-\phi}}$. Assim, como os elementos da forma $gg^{-\phi}$ geram $[G, \phi]$ e a igualdade anterior vale para todo $x \in N$, concluímos que $N \leq Z([G, \phi])$.

(iv) Seja $N = \langle G_\phi^G \rangle$ o fecho normal de G_ϕ em G. Vamos mostrar que G/N é abeliano. De fato, pelo item (i), deste lema, tem-se

$$G/N = (G/N)_\phi (G/N)_{-\phi}$$

e

$$G = G_{-\phi}G_{\phi} = [G, \phi]N.$$

Agora, pelo Lema 2.1.1, item (i), obtemos

$$(G/N)_{\phi} = G_{\phi}N/N = N/N.$$

E isto implica que $G/N = (G/N)_{-\phi}$. Assim, usando o item (iii), deste lema, resulta que

$$G/N \leq Z([G, \phi]N/N) = Z(G/N).$$

Portanto, concluímos que G/N é abeliano.
(v) Mostraremos que $x^g \in G_{-\phi}$ para todo $g \in G_{\phi}$ e todo $x \in G_{-\phi}$. Com efeito, sejam $x = y^{-1}y^{\phi} \in G_{-\phi}$ e $g \in G_{\phi}$, então

$$x^g = g^{-1}y^{-1}y^{\phi}g^{\phi} = (yg)^{-1}(yg)^{\phi}.$$

Assim, $x^g \in G_{-\phi}$. Portanto, temos que G_{ϕ} normaliza $G_{-\phi}$. □

3

Ferramentas Lie-teóricas

O problema restrito de Burnside foi proposto nos anos 30 do século XX e tem a seguinte pergunta:

É verdade que todo grupo finito m-gerado e de expoente n tem sua ordem limitada por uma função que depende apenas de m e n?

A partir de 1956, vários matemáticos como P. Hall, G. Higman, A. I. Kostrikin, W. Magnus e I. N. Sanov deram soluções parciais para o problema. Mas, foi somente, em 1989, que E. Zelmanov obteve uma solução completa para o conhecido problema. Seu trabalho foi tão reconhecido pela comunidade científica da época que em 1994 foi premiado com Medalha Fields. Para mais detalhes sobre o assunto veja [**37**] e [**38**].

Em [**39**], Zelmanov provou a solução positiva para o problema restrito de Burnside a partir do seguinte teorema.

Teorema 3.0.1. *Seja L uma álgebra de Lie gerada por $a_1, \ldots, a_m$. Suponha que L satisfaz uma identidade polinomial e cada comutador em $a_1, \ldots, a_m$ é ad-nilpotente. Então, L é nilpotente.*

Uma prova detalhada do teorema acima foi publicada recentemente em [**40**]. A partir deste teorema e de ferramentas Lie-teóricas desenvolvidas por Zelmanov para resolver o famoso problema, foram obtidos vários resultados relevantes em teoria de grupos. Atualmente, muitos matemáticos utilizam estas ferramentas em suas investigações.

A prova do nosso Teorema C depende fortemente dessas técnicas. Portanto, este capítulo tem por objetivo descrever algumas dessas ferramentas Lie-teóricas que foram necessárias para demonstração do mesmo. As principais referências utilizadas neste capítulo foram [**11**], [**13**] e [**30**].

3.1. Álgebras de Lie

Nesta seção, veremos a definição de álgebra de Lie, objeto central deste capítulo e daremos alguns exemplos da mesma. Além disso, definiremos algumas estruturas e conceitos que valem nessa álgebra, como por exemplo, o conceito de nilpotência que é semelhante ao que se conhece em teoria de grupos.

Sejam R um anel comutativo com unidade e L um R-módulo (à esquerda). Consideremos que L esteja munido da seguinte operação binária

$$\begin{array}{ccc} L \times L & \longrightarrow & L \\ (x, y) & \longmapsto & [x, y] \end{array}$$

chamamos esta operação de *comutador de Lie* ou *produto de Lie*.

Definição 3.1.1. *Dizemos que L é uma R-álgebra de Lie ou uma álgebra de Lie sobre R se as seguintes propriedades são satisfeitas para quaisquer $x, y, z \in L$ e $r, s \in R$:*
(i) $[x, x] = 0$ *(anticomutatividade);*
(ii) $[rx + sy, z] = r[x, z] + s[y, z]$;
(iii) $[x, ry + sz] = r[x, y] + s[x, z]$;
(iv) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ *(Identidade de Jacobi).*

Seja L uma álgebra de Lie sobre R. Note que L não é associativa, pois vale a Identidade de Jacobi. E não possui unidade, uma vez que temos a anticomutatividade.

Se $R = \mathbb{Z}$, então uma $\mathbb{Z}$-álgebra de Lie é dita um *anel de Lie*.

Se considerarmos $\mathbb{R}^3$ munido com a adição usual e o produto de Lie como sendo o produto vetorial é fácil mostrar que $\mathbb{R}^3$ é uma álgebra de Lie sobre $\mathbb{R}$.

Uma R-álgebra associativa A sempre pode ser vista como uma R-álgebra de Lie. Com efeito, basta definir o produto de Lie por $[x, y] = xy - yx$ para todos $x, y \in A$.

Ao longo deste capítulo, a menos que se diga o contrário, R será um corpo e L uma R-álgebra de Lie.

Sejam k e n inteiros positivos e $x, y, x_1, x_2, \ldots, x_k$ elementos de L. Definimos indutivamente

$$[x_1] = x_1; \quad [x_1, x_2, \ldots, x_k] = [[x_1, x_2, \ldots, x_{k-1}], x_k]$$

e

$$[x, {}_0y] = x; \quad [x, {}_ny] = [[x, {}_{n-1}y], y].$$

Um elemento $a \in L$ é dito ser *ad-nilpotente* se existe um inteiro positivo n tal que $[x, {}_n a] = 0$ para todo $x \in L$. Se n é o menor inteiro com esta propriedade, então dizemos que a é *ad-nilpotente de índice* n.

Seja $X \subseteq L$. Definimos um *comutador* em elementos de X como sendo qualquer elemento de L que pode ser obtido como um produto de Lie nos elementos de X com algum sistema de colchetes de Lie. Um *R-submódulo gerado por X* é o conjunto de todas as R-combinações lineares de elementos de X e o denotaremos por ${}_+\langle X\rangle$.

Sejam U e V subconjuntos de L, definimos o *comutador de Lie* de U e V, denotado por $[U, V]$, da seguinte forma

$$[U, V] = {}_+\langle [u, v] \mid u \in U, v \in V\rangle .$$

De um modo geral, se $U_1, U_2, \ldots, U_n$ são subconjuntos de L definimos o comutador de Lie de $U_1, U_2, \ldots, U_n$, denotado por $[U_1, U_2, \ldots, U_n]$, como

$$[U_1, U_2, \ldots, U_n] = [[U_1, U_2, \ldots, U_{n-1}], U_n] = {}_+\langle [u_1, u_2, \ldots, u_n] \mid u_i \in U_i\rangle .$$

Dizemos que $M \subseteq L$ é uma *R-subálgebra* de Lie se M é um R-submódulo tal que $[M, M] \leq M$. Um *ideal* I de L é um R-submódulo tal que $[I, L] \leq I$.

Não é difícil ver que se U e V são ideias, então $[U, V]$ é também um ideal.

Uma *R-subálgebra de Lie gerada por um conjunto $X \subseteq L$* é definida como sendo todas as R-combinações lineares de todos os comutadores de Lie nos elementos de X. Vamos denotá-la por $\langle X\rangle$.

Dadas duas R-álgebras de Lie L_1 e L_2, um *homomorfismo de R-álgebras de Lie* ou um *R-homomorfismo* é uma aplicação $\phi : L_1 \longrightarrow L_2$ tal que ϕ é um homomorfismo de R-módulos e $[x, y]^\phi = [x^\phi, y^\phi]$ para todos $x, y \in L_1$. Um *automorfismo* de L é uma aplicação $\phi : L \longrightarrow L$ que é um R-homomorfismo e bijetora.

Assim como em teoria de grupos, define-se de modo análogo, em teoria de Lie, algumas séries importantes para o estudo de álgebras nilpotentes.

Em L, definimos indutivamente, os seguintes ideais: $\gamma_1(L) = L$ e para $n \geq 2$ tem-se $\gamma_n(L) = [\gamma_{n-1}(L), L]$.

Desta maneira, temos a seguinte série central inferior de L

$$L = \gamma_1(L) \geq \gamma_2(L) \geq \cdots \geq \gamma_i(L) \geq \cdots$$

Dizemos que L é *nilpotente* se existe um inteiro positivo c tal que $\gamma_{c+1}(L) = 0$. O menor inteiro c com esta propriedade é chamado de *classe de nilpotência* de L. De modo semelhante à teoria de grupos, podemos também definir álgebras de Lie solúveis.

3.2. Identidades Polinomiais em Álgebras de Lie

Nesta seção, veremos o que significa uma álgebra ser PI e vamos enunciar vários resultados clássicos envolvendo identidades polinomiais em álgebras de Lie que serão usados posteriormente. As demonstrações desses resultados serão omitidas, pois fogem do objetivo deste trabalho.

Denotemos por F a álgebra de Lie livre sobre R nos geradores $x_1, x_2, \ldots$. Seja $f = f(x_1, x_2, \ldots, x_n)$ um elemento não nulo de F. A álgebra L satisfaz a identidade $f \equiv 0$ se $f(a_1, a_2, \ldots, a_n) = 0$ para quaisquer $a_1, a_2, \ldots, a_n \in L$. Neste caso, dizemos que L é PI.

Usando o Teorema 3.0.1 e alguns argumentos universais, o próximo teorema pode ser deduzido. Para mais detalhes veja [**15**].

Teorema 3.2.1. *Seja L uma álgebra de Lie sobre um corpo R gerada por $a_1, a_2, \ldots, a_m$. Suponha que L satisfaz uma identidade $f \equiv 0$ e que cada comutador nos geradores $a_1, a_2, \ldots, a_m$ é ad-nilpotente de índice no máximo n. Então, L é nilpotente de classe (f, m, n, R)-limitada.*

Antes de apresentarmos o próximo teorema, precisamos introduzir a seguinte definição.

Seja L uma álgebra de Lie sobre um corpo R. Suponha que um grupo finito A age em L por automorfismos. Definimos a *subálgebra formada pelos elementos fixos*, denotada por $C_L(A)$, como

$$C_L(A) = \{l \in L \mid l^a = l \text{ para todo } a \in A \setminus \{1\}\}.$$

O resultado a seguir nos fornece um importante critério para uma álgebra de Lie ser PI.

Teorema 3.2.2. *Seja L uma álgebra de Lie sobre um corpo R. Suponha que um grupo finito A age em L por automorfismos de tal maneira que $C_L(A)$ é PI. Assuma, além disso, que a característica de R é 0 ou prima com a ordem de A. Então, L é PI.*

Em [**1**], Bahturin e Zaicev provaram este teorema para grupos solúveis A. Em [**19**], Linchenko estendeu para o caso geral. O seguinte resultado foi deduzido em [**29**].

Corolário 3.2.3. *Seja F a álgebra de Lie livre de posto enumerável sobre R. Denote por F^* o conjunto dos elementos não nulos de F. Para qualquer grupo finito A existe uma aplicação*

$$\theta : F^* \longrightarrow F^*$$

tal que se L e A são como no Teorema 3.2.2, e se $C_L(A)$ satisfaz uma identidade $f \equiv 0$, então L satisfaz a identidade $\theta(f) \equiv 0$.

Para poder usar o Teorema 3.2.1 precisamos de uma ferramenta que nos permita deduzir que certos elementos de L são ad-nilpotentes. Neste contexto, o seguinte lema provado em [**15**] é bastante útil.

Lema 3.2.4. *Suponha que L é uma álgebra de Lie, K uma subálgebra de L gerada por r elementos $h_1, \ldots, h_r$ tal que todos os comutadores nos h_i são ad-nilpotentes em L de índice t. Se K é nilpotente de classe c, então para algum número (c, r, t)-limitado u temos $[L, \underbrace{K, \ldots, K}_{u}] = 0$.*

3.3. Automorfismos de Álgebras de Lie

Nesta seção, veremos que a partir de uma álgebra de Lie é possível obter uma outra álgebra de Lie sobre um corpo que é a extensão do corpo base e, além disso, mostraremos algumas propriedades que essas álgebras possuem. Este tipo de construção será utilizada dentro da demonstração do Teorema C.

Sejam R um corpo, L um R-álgebra de Lie, ω uma raiz n-ésima primitiva da unidade e $R[\omega]$ a menor extensão de R que contém ω. Como L e $R[\omega]$ são R-módulos, podemos definir o produto tensorial $\overline{L} = L \otimes_R R[\omega]$. Para simplificar a notação, vamos denotá-lo apenas por $L \otimes R[\omega]$. Definindo em $L \otimes R[\omega]$ as seguintes operações

$$\alpha(l \otimes \beta) = l \otimes \alpha\beta$$

e

$$[l_1 \otimes \alpha, l_2 \otimes \beta] = [l_1, l_2] \otimes \alpha\beta,$$

para todos $\alpha, \beta \in R[\omega]$ e $l, l_1, l_2 \in L$ e estendendo de forma linear para todo $\overline{L}$, temos que $\overline{L}$ admite uma estrutura de $R[\omega]$-álgebra de Lie. Note que L pode ser imersa em $\overline{L}$, basta considerarmos a aplicação definida por $l \longmapsto l \otimes 1$. Não é difícil ver que L e $\overline{L}$ possuem estruturas semelhantes, por exemplo, se L é nilpotente, então $\overline{L}$ é nilpotente com mesma classe de nilpotência.

Seja ϕ um automorfismo de L de ordem n. A partir de ϕ podemos definir um automorfismo $\overline{\phi}$ de $\overline{L}$ por $\overline{\phi} = \phi \otimes 1$, isto é,

$$(l \otimes \alpha)^{\overline{\phi}} = l^{\phi} \otimes \alpha,$$

para todo $l \otimes \alpha \in \overline{L}$. Faremos um abuso de notação e denotaremos $\overline{\phi}$ apenas por ϕ.

Considere ϕ um automorfismo de $\overline{L}$ de ordem n. Para cada $i \in \{0, \ldots, n-1\}$, definimos o subconjunto

$$^{i}\overline{L} = \{l \in \overline{L} \mid l^{\phi} = \omega^{i} l\}.$$

Dizemos que $^{i}\overline{L}$ é o *autoespaço* associado ao autovalor ω^{i}. Claramente, $^{i}\overline{L}$ é um submódulo de $\overline{L}$ para cada i. Note que $^{0}\overline{L}$ é exatamente $C_{\overline{L}}(\phi)$.

Para cada $k \in \mathbb{Z}$, denotamos por kL o submódulo de L dado por $\{kl \mid l \in L\}$. Dizemos que uma álgebra de Lie L não tem *k-torção* se para qualquer $l \in L$ a igualdade $kl = 0$ implica que $l = 0$.

A importância dos submódulos $^{i}\overline{L}$ será expressada nos próximos lemas.

Lema 3.3.1. *Consideremos $\overline{L}$ e $^{i}\overline{L}$ como antes e suponha que n é a ordem do automorfismo ϕ. Então,*
(i) *a seguinte inclusão vale*

$$n\overline{L} \subseteq {}^{0}\overline{L} + {}^{1}\overline{L} + \cdots + {}^{n-1}\overline{L};$$

(ii) *se $l_0 + l_1 + \cdots + l_{n-1} = 0$, onde $l_i \in {}^{i}\overline{L}$, então $nl_i = 0$ para todo $i = 0, 1, \ldots, n-1$;*
(iii) *se $\overline{L}$ não tem n-torção, então a soma ${}^{0}\overline{L} + {}^{1}\overline{L} + \cdots + {}^{n-1}\overline{L}$ é direta.*

Demonstração. (i) Seja ϕ um automorfismo de $\overline{L}$, para cada $l \in \overline{L}$ e cada $i = 0, 1, \ldots, n-1$, definimos

$$^{i}l = \sum_{s=0}^{n-1} \omega^{-is} l^{\phi^{s}}.$$

Vejamos que $^{i}l \in {}^{i}\overline{L}$. Com efeito, temos que

$$(^{i}l)^{\phi} = \left(\sum_{s=0}^{n-1} \omega^{-is} l^{\phi^{s}}\right)^{\phi} = \sum_{s=0}^{n-1} \omega^{-is} l^{\phi^{s+1}} = \omega^{i} \sum_{s=0}^{n-1} \omega^{-i(s+1)} l^{\phi^{s+1}} = \omega^{i} \sum_{r=0}^{n-1} \omega^{-ir} l^{\phi^{r}} = \omega^{i}(^{i}l).$$

onde $r = s + 1$. Logo, $^{i}l \in {}^{i}\overline{L}$. Assim, obtém-se

$$\sum_{i=0}^{n-1} {}^{i}l \in {}^{0}\overline{L} + {}^{1}\overline{L} + \cdots + {}^{n-1}\overline{L}. \tag{3.3.1}$$

Por outro lado, note que

$$\sum_{i=0}^{n-1} {}^{i}l = \sum_{i=0}^{n-1} \left(\sum_{s=0}^{n-1} \omega^{-is} l^{\phi^{s}}\right) = \sum_{s=0}^{n-1} l^{\phi^{s}} \sum_{i=0}^{n-1} \omega^{-is} = nl^{\phi^{0}} = nl, \tag{3.3.2}$$

pois, para $s = 0$, temos $\sum_{i=0}^{n-1} \omega^{0} = n$ e, para $s \not\equiv 0 \bmod n$, tem-se $\sum_{i=0}^{n-1} \omega^{is} = 0$, uma vez que

$$\omega^s \sum_{i=0}^{n-1} \omega^{is} = \sum_{i=0}^{n-1} \omega^{(i+1)s} = \sum_{i=0}^{n-1} \omega^{is}.$$

Logo,

$$(\omega^s - 1) \cdot \left(\sum_{i=0}^{n-1} \omega^{is} \right) = 0.$$

Como $\omega^s \neq 1$, resulta que $\sum_{i=0}^{n-1} \omega^{is} = 0$. Então, segue por (3.3.1) e (3.3.2) que $nl \in {}^0\overline{L} + {}^1\overline{L} + \cdots + {}^{n-1}\overline{L}$. Portanto, concluímos que $n\overline{L} \subseteq {}^0\overline{L} + {}^1\overline{L} + \cdots + {}^{n-1}\overline{L}$.
(ii) Aplicando o automorfismo ϕ^k, com $k = 0, 1, \ldots, n-1$, em $\sum_{i=0}^{n-1} l_i = 0$, onde $l_i \in {}^i\overline{L}$, obtemos as seguintes n equações

$$\begin{array}{ccccccccc}
l_0 & + & l_1 & + & \cdots & + & l_{n-1} & = & 0 \\
l_0 & + & \omega l_1 & + & \cdots & + & \omega^{n-1} l_{n-1} & = & 0 \\
l_0 & + & \omega^2 l_1 & + & \cdots & + & \omega^{2(n-1)} l_{n-1} & = & 0 \\
\vdots & & \vdots & & \cdots & & \vdots & & \\
l_0 & + & \omega^{n-1} l_1 & + & \cdots & + & \omega^{(n-1)(n-1)} l_{n-1} & = & 0
\end{array}$$

A fim de mostrarmos que $nl_i = 0$, para algum i, multiplicamos cada uma dessas equações por uma potência apropriada de ω com o objetivo de tornar o coeficiente de l_i igual a 1 e então, somamos todas as n equações. Note que ao somarmos estas equações, o coeficiente de cada l_i é dado por $\sum_{k=0}^{n-1} \omega^{ik}$. Agora, multiplicando $\sum_{k=0}^{n-1} \omega^{ik}$ por ω^{-ik}, obtemos que o coeficiente de l_i é igual a 1 e o coeficiente de l_j com $j \neq i$ é igual a $\sum_{k=0}^{n-1} \omega^{(j-i)k}$, o qual sabemos, pela demonstração do item anterior, ser igual a 0. Com isto, deduzimos que $nl_i = 0$ e o resultado segue.
(iii) Suponhamos que

$$l_0 + l_1 + \cdots + l_{n-1} = l'_0 + l'_1 + \cdots + l'_{n-1},$$

onde $l_i, l'_i \in {}^i\overline{L}$. Isto implica que

$$(l_0 - l'_0) + (l_1 - l'_1) + \cdots + (l_{n-1} - l'_{n-1}) = 0,$$

com $l_i - l'_i \in {}^i\overline{L}$. Agora, utilizando o item (ii) deste lema, obtemos que $n(l_i - l'_i) = 0$ para todo $i = 0, 1, \ldots, n-1$. Como $\overline{L}$ não tem n-torção, segue que $l_i = l'_i$ para todo i. Assim, qualquer elemento l de ${}^0\overline{L} + {}^1\overline{L} + \cdots + {}^{n-1}\overline{L}$ se escreve de modo único. Portanto, temos que a soma ${}^0\overline{L} + {}^1\overline{L} + \cdots + {}^{n-1}\overline{L}$ é direta, como queríamos. □

O próximo lema nos diz em que condição podemos decompor $\overline{L}$ em termos dos autoespaços ${}^i\overline{L}$.

Lema 3.3.2. *Suponha que $\overline{L}$ é uma álgebra de Lie finita e $n \geq 1$ um número inteiro. Se $(n, |\overline{L}|) = 1$, então*

$$\overline{L} = \bigoplus_{i=0}^{n-1} {}^i\overline{L}.$$

Demonstração. Primeiramente, vejamos que $\overline{L}$ não tem n-torção. De fato, suponhamos o contrário, então existe $l \in \overline{L}$ com $l \neq 0$ tal que $nl = 0$. Isto implica que a ordem de l divide n e como $(n, |\overline{L}|) = 1$, deduzimos que $l = 0$, o que é uma contradição com a nossa suposição. Portanto, $\overline{L}$ não tem n-torção. Agora, usando o Lema 3.3.1, item (iii), e a Observação 1.1.3, segue que

$$\overline{L} = n\overline{L} \subseteq {}^0\overline{L} \oplus {}^1\overline{L} \oplus \cdots \oplus {}^{n-1}\overline{L}.$$

E como ${}^i\overline{L} \subseteq \overline{L}$ para todo $i \in \{0, \ldots, n-1\}$, concluímos que

$$\overline{L} = \bigoplus_{i=0}^{n-1} {}^i\overline{L},$$

como desejado. □

O lema a seguir nos diz que se $x, y \in \overline{L}$ são autovetores para ϕ, então $[x, y]$ também é um autovetor para ϕ.

Lema 3.3.3. *Para quaisquer i e j, temos*

$$[{}^i\overline{L}, {}^j\overline{L}] \leq {}^{i+j}\overline{L},$$

onde $i + j$ é calculado módulo n. Em particular, ${}^0\overline{L} + {}^1\overline{L} + \cdots + {}^{n-1}\overline{L}$ é uma subálgebra ϕ-invariante de L.

Demonstração. De fato, sejam $a \in {}^i\overline{L}$ e $b \in {}^j\overline{L}$, então

$$[a, b]^\phi = [a^\phi, b^\phi] = [\omega^i a, \omega^j b] = \omega^{i+j}[a, b].$$

Então, $[a, b] \in {}^{i+j}\overline{L}$. Logo, $[{}^i\overline{L}, {}^j\overline{L}] \leq {}^{i+j}\overline{L}$. Façamos $H = {}^0\overline{L} + {}^1\overline{L} + \cdots + {}^{n-1}\overline{L}$. Evidentemente, H é um submódulo ϕ-invariante de $\overline{L}$. Agora, pela linearidade de $\overline{L}$, obtemos

$$[H, H] = \left[\sum_{i=0}^{n-1} {}^i\overline{L}, \sum_{j=0}^{n-1} {}^j\overline{L}\right] = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} [{}^i\overline{L}, {}^j\overline{L}] \leq \sum_{i,j=0}^{n-1} {}^{i+j}\overline{L} = H.$$

Portanto, segue que H é uma subálgebra ϕ-invariante de L. □

Um fato geral que usaremos dentro da prova do Teorema C é a seguinte observação.

Observação 3.3.4. *Se $f \equiv 0$ é uma identidade multilinear em L, então f é também uma identidade em $\overline{L}$.*

3.4. Álgebra de Lie Associada a um Grupo

Nesta seção, vamos descrever a construção que associa uma álgebra de Lie $L^*(G)$ a qualquer grupo G a partir de uma N_p-série e também veremos alguns resultados que mostram a relação entre G e $L^*(G)$. Ao longo desta e da próxima seção, p denotará um número primo.

Primeiramente, precisamos definir uma série importante para o nosso estudo, a chamada N_p-série.

Uma *N-série* de um grupo G é uma série de subgrupos

$$G = G_1 \geq G_2 \geq \cdots \qquad (*)$$

tal que $[G_i, G_j] \leq G_{i+j}$ para todos i, j.

Claramente, qualquer N-série é central. Uma N-série é chamada *N_p-série* se $G_i^p \leq G_{pi}$ para todo i.

Lazard generalizou construções descobertas por Magnus em [**21**] e Zassenhaus em [**36**], e observou em [**18**] que o anel de Lie $L^*(G)$ pode ser associado a qualquer N-série $(*)$ de um grupo G. Ele também descobriu algumas propriedades relevantes de $L^*(G)$ quando $(*)$ é uma N_p-série. Neste caso, $L^*(G)$ é uma álgebra de Lie sobre $\mathbb{F}_p$, o corpo com p elementos. Vamos, a partir de agora, nos concentrar neste caso.

Dada uma N_p-série, vamos visualizar os quocientes $L_i^* = G_i/G_{i+1}$ como espaços lineares sobre $\mathbb{F}_p$ e seja $L^*(G)$ a soma direta desses espaços. A operação em G induz uma operação soma em $L^*(G)$, denotada por $+$, que é definida componente a componente, isto é, dados $xG_{i+1}, yG_{i+1} \in G_i/G_{i+1}$ definimos

$$xG_{i+1} + yG_{i+1} = xyG_{i+1}.$$

E a comutação em G induz uma operação binária em $L^*(G)$, denotada por $[,]$, da seguinte forma: para elementos homogêneos $xG_{i+1} \in L_i^*$ e $yG_{j+1} \in L_j^*$ definimos

$$[xG_{i+1}, yG_{j+1}] = [x, y]G_{i+j+1} \in L_{i+j}^*,$$

e estendemos a operação para elementos arbitrários de $L^*(G)$ por linearidade.

Não é difícil mostrar que estas operações estão bem definidas e que a proposição a seguir vale.

Proposição 3.4.1. *$L^*(G)$ com as operações $+$ e $[,]$ torna-se uma álgebra de Lie sobre $\mathbb{F}_p$.*

Agora, vamos nos concentrar na relação entre G e $L^*(G)$. Para qualquer elemento $x \in G_i \setminus G_{i+1}$ denotamos por x^* o elemento xG_{i+1} de $L^*(G)$.

Seja L uma álgebra de Lie. Dizemos que uma aplicação linear $\delta : L \longrightarrow L$ é uma *derivação* de L se temos $\delta([x,y]) = [x,\delta(y)] + [\delta(x),y]$ para todos $x, y \in L$. Um exemplo de derivação é a seguinte aplicação: fixe um elemento $x \in L$ e defina $adx : L \longrightarrow L$ por $adx(y) = [x,y]$. Pode-se mostrar utilizando a anticomutatividade e a Identidade de Jacobi que adx é uma derivação para qualquer $x \in L$. O próximo resultado é devido a Lazard e sua prova pode ser encontrada em [**18**].

Proposição 3.4.2 (**Lazard**)**.** *Para qualquer $x \in G$ temos $(adx^*)^p = ad(x^p)^*$. Consequentemente, se x é de ordem finita t, então x^* é ad-nilpotente de índice no máximo t.*

Denotemos por Fr o grupo livre nos geradores livres $x_1, x_2, \ldots$, e escolha um elemento não trivial $\mu = \mu(x_1, x_2, \ldots, x_s) \in Fr$. Dizemos que um grupo G satisfaz a identidade $\mu \equiv 1$ se $\mu(g_1, g_2, \ldots, g_s) = 1$ para quaisquer $g_1, g_2, \ldots, g_s \in G$. A seguinte proposição é imediata da prova do Teorema 1 do artigo de Wilson e Zelmanov que se encontra em [**35**].

Proposição 3.4.3. *Seja G um grupo satisfazendo uma identidade de grupo $\mu \equiv 1$. Então, existe um polinômio de Lie multilinear não nulo f sobre $\mathbb{F}_p$ dependendo somente de p e μ tal que para qualquer N_p-série $(*)$ de G, a álgebra $L^*(G)$ satisfaz a identidade $f \equiv 0$.*

Em [**35**], Wilson e Zelmanov descreveram um algoritmo efetivo que permite escrever f explicitamente para quaisquer p e μ. Mas, para o nosso resultado, não vamos precisar do mesmo.

A fim de exemplificar, enunciaremos a seguir um caso importante da proposição anterior. Sua prova pode ser encontrada em [**10**].

Proposição 3.4.4 (**Higman**)**.** *Sejam n uma potência de um primo p e G um grupo tal que $x^n = 1$ para todo $x \in G$. Então, para qualquer N_p-série $(*)$, a álgebra $L^*(G)$ satisfaz a identidade*

$$\sum_{\pi \in S_{n-1}} [x_0, x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n-1)}] = 0.$$

3.5. A Série de Zassenhaus

De um modo geral um grupo G possui muitas N_p-séries. Assim, existem várias maneiras de associar a G uma álgebra de Lie $L^*(G)$. Nesta seção, descreveremos uma N_p-série que é de suma importância para aplicações de resultados Lie-teóricos para a teoria de grupos.

Definição 3.5.1. *Seja G um grupo, para todo $i \geq 1$, definimos*

$$D_i = D_i(G) = \prod_{jp^k \geq i} \gamma_j(G)^{p^k}.$$

Os subgrupos D_i formam a seguinte série em G

$$G = D_1 \geq D_2 \geq D_3 \geq \cdots$$

Se G é um grupo abeliano, então $D_i = G^{p^k}$ onde k é o menor inteiro tal que $p^k \geq i$. Se G é um p-grupo finito, então $D_2 = \Phi(G)$. Se G é um grupo de expoente p, então $D_i = \gamma_i(G)$ para todo $i \geq 1$.

O nosso objetivo agora será mostrar que a série $\{D_i\}$ é uma N_p-série. Para isso, precisamos dos seguintes lemas conhecidos.

Lema 3.5.2. *Sejam G um grupo qualquer, $x, y \in G$ e p um primo fixado.*
(i) *Para todo $n \geq 1$, temos*

$$(xy)^{p^n} \equiv x^{p^n} y^{p^n} \bmod \gamma_2(G)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(G)^{p^{n-r}};$$

(ii) *Se $H \leq G$ tal que $x, [x, y] \in H$, então para todo $n \geq 1$, temos*

$$[x^{p^n}, y] \equiv [x, y]^{p^n} \bmod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}}.$$

Demonstração. (i) Seja,

$$N = \gamma_2(G)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(G)^{p^{n-r}}.$$

Usando, a Fórmula de Hall e Petresco 1.1.10, temos para todo $n \geq 1$, que

$$x^{p^n} y^{p^n} = (xy)^{p^n} g_2^{\binom{p^n}{2}} \dots g_{p^n-1}^{p^n} g_{p^n},$$

com $g_i \in \gamma_i(G)$ e $i = 1, \dots, p^n$.

Se $(i, p) = 1$, então p^n divide $\binom{p^n}{i}$. Por outro lado, se $i > 1$ e $(i, p) = 1$, então $g_i^{\binom{p^n}{i}} \in \gamma_2(G)^{p^n} \leq N$. Agora, se $i = p^r j$, onde $r \geq 1$ e $(j, p) = 1$, então p^{n-r} divide

$\binom{p^n}{i}$ e como $i \geq p^r$ resulta que $g_i^{\binom{p^n}{i}} \in \gamma_{p^r}(G)^{p^{n-r}} \leq N$. Desta forma, obtemos que

$$g_2^{\binom{p^n}{2}}, \ldots, g_{p^n-1}^{p^n}, g_{p^n} \in N.$$

Portanto,

$$x^{p^n} y^{p^n} \equiv (xy)^{p^n} \bmod N.$$

(ii) Usando o item (i) deste lema, para os elementos $x, [x, y] \in H$, tem-se

$$(x[x, y])^{p^n} \equiv x^{p^n} [x, y]^{p^n} \bmod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}}.$$

Agora, como $x[x, y] = x^y$, temos

$$(x^y)^{p^n} = (x^{p^n})^y = x^{p^n} [x^{p^n}, y].$$

Isto implica que

$$x^{p^n} [x^{p^n}, y] \equiv x^{p^n} [x, y]^{p^n} \bmod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}}.$$

Portanto,

$$[x^{p^n}, y] \equiv [x, y]^{p^n} \bmod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}}.$$

□

Lema 3.5.3. *Seja G um grupo. Se $n \geq 0$ e $i, j \geq 1$, então*

$$[\gamma_i(G)^{p^n}, \gamma_j(G)] \leq \prod_{r=0}^{n} \gamma_{j+ip^r}(G)^{p^{n-r}}.$$

Demonstração. Seja

$$N = \prod_{r=0}^{n} \gamma_{j+ip^r}(G)^{p^{n-r}}.$$

Observe que qualquer gerador de $[\gamma_i(G)^{p^n}, \gamma_j(G)]$ é da forma

$$[x^{p^n} y^{p^n}, z] = [x^{p^n}, z]^{y^{p^n}} [y^{p^n}, z],$$

onde $x, y \in \gamma_i(G)$ e $z \in \gamma_j(G)$. Como N é normal, é suficiente mostrar que $[x^{p^n}, y] \in N$ para quaisquer $x \in \gamma_i(G)$ e $y \in \gamma_j(G)$. Com efeito, sejam $x \in \gamma_i(G)$ e $y \in \gamma_j(G)$ e consideremos $H = \langle x, [x, y] \rangle$. Pelo Lema 3.5.2, item (ii), temos

$$[x^{p^n}, y] \equiv [x, y]^{p^n} \bmod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}}. \tag{3.5.1}$$

Utilizando o Lema 1.1.9, deduzimos que $\gamma_2(H) \leq \gamma_{2i+j}(G)$. Além disso, como $H \leq \gamma_i(G)$, podemos mostrar por indução sobre m, que $\gamma_m(H) \leq \gamma_{mi+j}(G)$, para todo $m \geq 2$. Em particular, obtemos $\gamma_{p^r}(H)^{p^{n-r}} \leq \gamma_{p^r i+j}(G)^{p^{n-r}}$ para $r = 1, \ldots, n$. Isto implica que

$$\prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}} \leq N.$$

Além disso, quando $r = 0$, temos $\gamma_2(H)^{p^n} \leq \gamma_{i+j}(G)^{p^n} \leq N$. Consequentemente, $[x, y]^{p^n} \in \gamma_{i+j}(G)^{p^n} \leq N$. Como

$$\gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}} \leq N,$$

segue de (3.5.1) que $[x^{p^n}, y]^{-1}[x, y]^{p^n} \in N$. Isto implica que $[x^{p^n}, y] \in N$. Portanto, concluímos que $[\gamma_i(G)^{p^n}, \gamma_j(G)] \leq N$, como queríamos. □

Lema 3.5.4. *Sejam G um grupo, $i, j \geq 1, h \geq 0$ e*

$$N = \prod_{r=0}^{h} \gamma_{i+jp^r}(G)^{p^{h-r}}.$$

Se $x \in \gamma_i(G)$ e $n \geq 2$, então

$$\gamma_n(\langle x, N\rangle) \leq \prod_{r=0}^{h} \gamma_{in+jp^r}(G)^{p^{h-r}}.$$

Demonstração. A prova será feita por indução sobre n. Se $n = 2$, deduzimos que $\gamma_2(\langle x, N\rangle) = [N, \langle x, N\rangle]$. Uma vez que $\langle x, N\rangle \leq \gamma_i(G)$, tem-se

$$\gamma_2(\langle x, N\rangle) = [N, \langle x, N\rangle] \leq [N, \gamma_i(G)].$$

Assim, obtemos o resultado para $n = 2$. Para $n \geq 2$, é fácil ver que

$$\gamma_n(\langle x, N\rangle) \leq [\gamma_{n-1}(\langle x, N\rangle), \gamma_i(G)]. \tag{3.5.2}$$

Por outro lado, utilizando, para $n = 2$, a definição de N e para $n > 2$, a hipótese de indução e (3.5.2), obtemos

$$\gamma_n(\langle x, N\rangle) \leq [\gamma_{n-1}(\langle x, N\rangle), \gamma_i(G)] \leq \left[\prod_{r=0}^{h} \gamma_{i(n-1)+jp^r}(G)^{p^{h-r}}, \gamma_i(G)\right].$$

Agora, usando o Lema 1.1.2, item (ii) e o Lema 3.5.3, resulta em

$$\gamma_n(\langle x, N\rangle) \leq \prod_{r=0}^{h} [\gamma_{in-i+jp^r}(G)^{p^{h-r}}, \gamma_i(G)] \leq \prod_{r=0}^{h} \prod_{s=0}^{h-r} \gamma_{i+p^s(in-i+jp^r)}(G)^{p^{h-r-s}}.$$

Como $i + p^s in - p^s i + jp^{r+s} \geq in + jp^{r+s}$, concluímos que

$$\gamma_n(\langle x, N\rangle) \leq \prod_{r+s\leq h} \gamma_{in+jp^{r+s}}(G)^{p^{h-(r+s)}}$$

e o resultado segue. □

Por fim, precisaremos do seguinte lema.

Lema 3.5.5. *Seja G um grupo. Se $i, j \geq 1$ e $h, k \geq 0$, então*

$$[\gamma_i(G)^{p^k}, \gamma_j(G)^{p^h}] \leq D_{ip^k+jp^h}(G).$$

Demonstração. Sejam $x \in \gamma_i(G), y \in \gamma_j(G)$, $z = [x, y^{p^h}]$ e $H = \langle x, z\rangle$. Pelo Lema 3.5.2, item (ii), temos

$$[x^{p^k}, y^{p^h}] \equiv z^{p^k} \bmod \gamma_2(H)^{p^k} \prod_{m=1}^{k} \gamma_{p^m}(H)^{p^{k-m}}. \tag{3.5.3}$$

Agora, para $n = 1, \ldots, p^k$, seja

$$H_n = \prod_{r=0}^{h} \gamma_{in+jp^r}(G)^{p^{h-r}}.$$

Se $n = 1$, temos

$$H_1 = \prod_{r=0}^{h} \gamma_{i+jp^r}(G)^{p^{h-r}}.$$

Pelo Lema 3.5.3, $z \in H_1$. Assim, $H \leq \langle x, H_1\rangle$. Além disso, usando o Lema 3.5.4, resulta que $\gamma_n(H) \leq H_n$, para todo $n \geq 2$. Com isto, deduzimos que

$$[x^{p^k}, y^{p^h}] \in \prod_{m=0}^{k} (H_{p^m})^{p^{k-m}}.$$

Façamos $D = D_{ip^k+jp^h}(G)$. Se $m + h - r \geq k$, então pela definição de D_i, temos que $\gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq D$. Seja $s = max\{m + h - k + 1, 0\}$, então

$$H_{p^m} \leq D \prod_{r=s}^{h} \gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq D\gamma_{ip^m+jp^s}(G).$$

Em particular, temos

$$(H_{p^m})^{p^{k-m}} \leq D\gamma_{ip^m+jp^s}(G)^{p^{k-m}} \leq D,$$

pois $ip^k + jp^{k-m+s} \geq ip^k + jp^h$. Logo, $[x^{p^k}, y^{p^h}] \in D$. Isto implica que $x^{p^k} D$ e $y^{p^h} D$ comutam. Consequentemente, $\gamma_i(G)^{p^k} D/D$ e $\gamma_j(G)^{p^h} D/D$ comutam. Portanto, concluímos que $[\gamma_i(G)^{p^k}, \gamma_j(G)^{p^h}] \leq D$, como gostaríamos. □

Agora, estamos prontos para mostrar a próxima proposição.

Proposição 3.5.6. *Seja G um grupo qualquer. Então, as seguintes afirmações valem para todos $m, n \geq 1$.*
(i) $[D_m, D_n] \leq D_{m+n}$;
(ii) $D_n^p \leq D_{pn}$.

Demonstração. (i) Com efeito, sabemos que

$$D_m = \prod_{ip^k \geq m} \gamma_i(G)^{p^k} \quad \text{e} \quad D_n = \prod_{jp^h \geq n} \gamma_j(G)^{p^h}.$$

Assim, pelo Lema 3.5.5, tem-se

$$[D_m, D_n] = \prod [\gamma_i(G)^{p^k}, \gamma_j(G)^{p^h}] \leq D_{ip^k + jp^h} \leq D_{m+n},$$

pois $ip^k + jp^h \geq m + n$. Portanto, $[D_m, D_n] \leq D_{m+n}$.
(ii) Pelo item (i), temos que $\gamma_p(D_n) \leq D_{pn}$. Isto implica que D_n/D_{pn} possui classe de nilpotência no máximo $p-1$. Agora, notemos que qualquer gerador de D_n/D_{pn} possui ordem p. De fato, se $jp^s \geq n$ e $x \in \gamma_j(G)$, então deduzimos que $(x^{p^s})^p \in D_{jp^{s+1}} \leq D_{pn}$. Assim, obtemos $(D_n/D_{pn})^p = 1$. Portanto, segue que $D_n^p \leq D_{pn}$, como desejado. □

Portanto, da Proposição 3.5.6, concluímos que a série $\{D_i\}$ é uma N_p-série e é chamada a série central *p-dimensional* de G. Ela é também conhecida como a série de *Zassenhaus* ou a série de *Jennings-Lazard-Zassenhaus*.

Sabemos que podemos associar a G uma álgebra de Lie $DL(G) = \oplus L_i$ sobre $\mathbb{F}_p$ correspondendo a série central p-dimensional de G, onde $L_i = D_i/D_{i+1}$. Seja $L_p(G) = \langle L_1 \rangle$ a subálgebra de $DL(G)$ gerada por L_1. O seguinte resultado foi obtido em [**23**].

Lema 3.5.7. *Suponha que G é um p-grupo finito tal que a álgebra de Lie $L_p(G)$ é nilpotente de classe c. Então, D_{c+1} é powerful.*

Seja H um subgrupo de G. Façamos $H_j = D_j \cap H$ e denotamos

$$L(G, H) = \bigoplus_{j \geq 1} H_j D_{j+1}/D_{j+1}.$$

e

$$L_p(G, H) = L_p(G) \cap L(G, H).$$

Observação 3.5.8. *$L(G, H)$ é uma subálgebra de $DL(G)$. Além disso, $L(G, H)$ é isomorfa a álgebra de Lie associada a N_p-série $\{H_j\}$ de H.*

Seja ϕ um automorfismo do grupo G. Então, ϕ age naturalmente em cada quociente da série de Zassenhaus de G. Logo, esta ação induz um automorfismo da álgebra de Lie $DL(G)$. Assim, quando conveniente consideraremos ϕ como um automorfismo de $DL(G)$ ou de $L_p(G)$.

Utilizando o Lema 2.1.1, item (i), obtemos o resultado a seguir.

Lema 3.5.9. *Se G é um grupo finito e ϕ é um automorfismo de G tal que $(|G|, |\phi|) = 1$, então*

$$L_p(G, G_\phi) = C_{L_p(G)}(\phi).$$

Finalizamos esta seção, com um lema que será muito útil.

Lema 3.5.10. *Sejam G um p-grupo finito, H um subgrupo de G e $K = L(G, H)$. Então, existe um número u dependendo somente da ordem de H tal que*

$$[DL(G), \underbrace{K, \ldots, K}_{u}] = 0.$$

Demonstração. Se $x \in H$, então a ordem de x é no máximo $|H|$. Por outro lado, a Proposição de Lazard 3.4.2, mostra que o elemento correspondente x^* é ad-nilpotente em $DL(G)$ de índice no máximo $|H|$. Além disso, observe que a classe de nilpotência de K é no máximo a de H. Deste modo, aplicando o Lema 3.2.4, obtemos o resultado desejado. □

4

Grupos de Ordem Ímpar Admitindo um Automorfismo Involutório

O objetivo deste capítulo é demonstrar os resultados principais relacionados a grupos de ordem ímpar que admitem um automorfismo involutório. Para comodidade do leitor, vamos repetir o enunciado de cada teorema.

4.1. Prova do Teorema A

Para demonstrarmos o Teorema A, precisamos do lema a seguir.

Lema 4.1.1. *Seja G um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que $G = [G, \phi]$. Se S é o conjunto dos elementos $h \in G_\phi$ para os quais existem $x, y \in G_{-\phi}$ tais que $h \in \langle x, y\rangle$, então $G_\phi = \langle S\rangle$.*

Demonstração. Note que $S \neq \emptyset$, pois $1 \in S$. Agora, façamos $H = \langle S\rangle$. Claramente, $H \leq G_\phi$. Assim, precisamos provar que $G_\phi \leq H$. Seja $h \in G_\phi$. Como $G = [G, \phi]$, podemos escrever

$$h = g_1 \cdots g_m,$$

com $g_i \in G_{-\phi}$. Desejamos provar que $h \in H$. Faremos isto por indução em m. Se $m \leq 2$, obviamente $h \in H$. Assim, assuma que $m \geq 3$. Seja $K = \langle g_{m-1}, g_m\rangle$. Como K é ϕ-invariante, temos pelo Lema 2.2.1, item (i), que $g_{m-1}g_m = g_0h_0$ onde $g_0 \in K_{-\phi}$ e $h_0 \in K_\phi$. Evidentemente, $K_\phi \leq H$ e então $h_0 \in H$. Desta forma,

$$h = g_1 \cdots g_{m-2}g_0h_0.$$

Isto implica que

$$hh_0^{-1} = g_1 \cdots g_{m-2}g_0.$$

Então, por hipótese de indução, segue que $hh_0^{-1} \in H$, consequentemente $h \in H$. Portanto, concluímos que $H = G_\phi$, como queríamos. □

O teorema a seguir foi demonstrado em [**29**] (veja também em [**30**]). Sua prova está baseada em um resultado Lie-teórico de Zelmanov que se encontra em [**40**].

Teorema 4.1.2. *Sejam e um inteiro positivo e G um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que todos os elementos em $G_\phi \cup G_{-\phi}$ possuem ordem dividindo e. Então, o expoente de G é e-limitado.*

Agora, vejamos a prova do Teorema A.

Teorema A. *Sejam c, d, e inteiros não negativos e G um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que G_ϕ é nilpotente de classe c e $x^e = 1$ para cada $x \in G_{-\phi}$. Suponha que o subgrupo $\langle x, y\rangle$ tem comprimento derivado no máximo d para todos $x, y \in G_{-\phi}$. Então, o expoente de $[G, \phi]$ é (c, d, e)-limitado.*

Demonstração. Podemos supor sem perda de generalidade que $G = [G, \phi]$. Em vista do Teorema 4.1.2, é suficiente mostrar que G_ϕ possui expoente (c, d, e)-limitado. Para isto, consideremos S o conjunto dos elementos $h \in G_\phi$ para os quais existem $x, y \in G_{-\phi}$ tal que $h \in \langle x, y\rangle$. Pelo Lema 4.1.1, temos que $G_\phi = \langle S\rangle$. Afirmamos que os elementos de S possuem ordem (d, e)-limitada. Com efeito, seja $h \in S$, então existe $K = \langle x, y\rangle$ com $x, y \in G_{-\phi}$ tal que $h \in K$. Como K é ϕ-invariante, temos $K = [K, \phi]$. Agora, uma vez que K possui comprimento derivado no máximo d e $K_{-\phi}$ possui expoente dividindo e, segue da Proposição 2.1.8, que o expoente de K é (d, e)-limitado. Isto implica que a ordem de h é também (d, e)-limitada. Como h foi tomado arbitrariamente em S, concluímos que todo elemento de S possui ordem (d, e)-limitada. Assim, G_ϕ é um subgrupo nilpotente de classe c gerado por elementos de ordem (d, e)-limitada. Portanto, pelo Lema 1.1.26, obtemos que o expoente de G_ϕ é (c, d, e)-limitado e o resultado segue. □

4.2. Prova do Teorema B

Iniciemos esta seção com um teorema devido a P. Shumyatsky. Sua prova utiliza a teoria de p-grupos powerful, onde p é um primo e pode ser encontrada em [**28**]. O mesmo será usado dentro da demonstração do Teorema B.

Teorema 4.2.1. *Seja G um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que $r(G_\phi) = r$. Então, $r([G, \phi]')$ é r-limitado.*

Lembremos que um grupo G é dito *periódico* (ou de *torsão*) se todos os seus elementos possuem ordem finita. O próximo teorema nos fornece algumas informações a respeito de um subgrupo de um grupo periódico que admite uma involução. Para os detalhes da prova veja [**7**].

Teorema 4.2.2. *Existe uma função $f(m)$ tal que se G é um grupo periódico contendo uma involução ϕ com $|G_\phi| = m$, então G contém um subgrupo nilpotente de classe no máximo dois e índice menor ou igual a $f(m)$.*

A partir dos resultados anteriores, estamos em condições de demonstrar o Teorema B.

Teorema B. *Sejam e, r inteiros não negativos e G um grupo finito de ordem ímpar admitindo um automorfismo involutório ϕ tal que G_ϕ tem posto r e $x^e = 1$ para cada $x \in G_{-\phi}$. Então, o expoente de $[G, \phi]$ é (e, r)-limitado.*

Demonstração. Sem perda de generalidade, podemos supor que $G = [G, \phi]$. Seja $r' = r(G')$. Pelo Teorema 4.2.1, temos que r' é r-limitado. Segue do Lema 1.1.28, que a altura de Fitting de G' é também r-limitada. Argumentando por indução em $h(G')$ podemos assumir que o expoente de $G/F(G')$ é (e, r)-limitado. De fato, se $h(G') = 1$, então $F(G') = G'$. Assim, segue que o expoente de G/G' é e. Então, suponhamos que $h(G') \geq 2$. Agora, consideremos o grupo $G'/F(G')$, o Lema 1.1.23 afirma que $h(G'/F(G')) < h(G')$. Logo, por hipótese de indução, temos que o expoente de $G'/F(G')$ é (e, r)-limitado. Além disso, como o expoente do grupo quociente de $G/F(G')$ por $G'/F(G')$ é e, obtemos que $G/F(G')$ também possui expoente (e, r)-limitado. Assim, existe um inteiro positivo (e, r)-limitado f tal que o expoente de $G/F(G')$ é f e isto implica que $G^f \leq F(G')$. Façamos $M = G^f$. Sabendo que G/M tem expoente f e que o posto de G_ϕ é r resulta que o posto de $(G/M)_\phi$ é r também e o expoente de $(G/M)_\phi$ é (e, r)-limitado. Então, pelo Lema 1.1.29, obtemos que a ordem de $(G/M)_\phi$ é (e, r)-limitada. O Teorema 4.2.2 diz que G/M possui um subgrupo H/M de índice (e, r)-limitado que é nilpotente de classe no máximo dois. Sem perda de generalidade, podemos supor que $H/M \lhd G/M$, então o grupo quociente de G/M por H/M é solúvel de ordem (e, r)-limitada. O Lema 1.1.21 afirma que o comprimento derivado do grupo quociente de G/M por H/M é também (e, r)-limitado. Por outro lado, como a classe de nilpotência de H/M é dois, deduzimos que seu comprimento derivado é no máximo dois. Desta maneira, concluímos que o comprimento derivado de G/M é (e, r)-limitado.

Lembrando que $r' = r(G')$ e $M \leq F(G')$ segue que M é nilpotente. Assim, assumamos primeiramente que M é um p-grupo para algum primo p. Seja A um subgrupo normal abeliano maximal de M. Pelo Teorema 1.1.15, segue que $A = C_M(A)$. Denotemos por B o subgrupo característico minimal de M contendo A, isto é, $B = \langle A^\alpha \mid \alpha \in Aut\, G\rangle$ e como $A^\alpha \lhd B$ para todo $\alpha \in Aut\, G$, obtemos que B é um produto de no máximo r' subgrupos da forma A^α. Além disso, por A^α ser um subgrupo normal abeliano de B para todo α, segue pelo Teorema de Fitting 1.1.17, que a classe de nilpotência de B é no máximo r'. Seja D o subgrupo normal minimal de G contendo $B_{-\phi}$, isto é, $D = \langle (B_{-\phi})^x \mid x \in G\rangle$. Temos que D é um subgrupo de classe de nilpotência no máximo r', pois $D \lhd B$ e é gerado por elementos de ordem dividindo e. Então, pelo Lema 1.1.26, o expoente de D é (e,r)-limitado. Além disso, como o posto de D é no máximo r', resulta pelo Lema 1.1.29, que a ordem de D é também (e,r)-limitada. Assim, usando o Lema 1.1.12, segue que existe um número inteiro (e,r)-limitado j tal que $D \leq Z_j(M)$. Note que ϕ age trivialmente em B/D, logo $B/D = (B/D)_\phi$. Agora, aplicando, o Lema 2.2.1, item (iii), tem-se $B/D \leq Z(G/D)$. Isto implica que $[B,G] \leq D$. Portanto, $B \leq Z_{j+1}(M)$. Pois, seja $b \in B$, desejamos provar que $b \in Z_{j+1}(M)$. Com efeito, consideremos o seguinte comutador

$$[b, m_1, \ldots, m_{j+1}] = [[b, m_1], m_2, \ldots, m_{j+1}],$$

com $m_i \in M$ arbitrários. Temos que $[b, m_1] \in [B,G]$ e como $[B,G] \leq D \leq Z_j(M)$ obtemos que $[b, m_1] \in Z_j(M)$. Aplicando a Proposição 1.1.6, tem-se

$$[b, m_1, m_2, \ldots, m_{j+1}] = 1,$$

para todo $m_i \in M$. Logo, $b \in Z_{j+1}(M)$. Isto implica que $B \leq C_G(\gamma_{j+1}(M))$, pois como $B \leq Z_{j+1}(M)$, segue do Lema 1.1.22, item (i), que

$$[B, \gamma_{j+1}(M)] \leq [Z_{j+1}(M), \gamma_{j+1}(M)] \leq Z_{j+1-(j+1)}(M) = Z_0(M) = 1.$$

Daí, $[B, \gamma_{j+1}(M)] = 1$. Assim, pelo Lema 1.1.2, item (i), tem-se $B \leq C_G(\gamma_{j+1}(M))$. Claramente, $C_M(B) \leq B$, pois $A = C_M(A) \leq B$ e disto segue que $\gamma_{j+1}(M) \leq B$. Agora, vejamos que o comprimento derivado de M é (e,r)-limitado. Com efeito, sabendo que $\gamma_{j+1}(M) \leq C_G(\gamma_{j+1}(M))$ resulta que $\gamma_{j+1}(M)$ é abeliano e usando o Lema 1.1.22, item (ii), obtemos

$$M^{(j+1)} = [M^{(j)}, M^{(j)}] \leq [\gamma_{j+1}(M), \gamma_{j+1}(M)] = 1.$$

Assim, $M^{(j+1)} = 1$. Logo, segue que o comprimento derivado de M é (e,r)-limitado. Uma vez que o comprimento derivado de G/M é também (e,r)-limitado,

deduzimos que o comprimento derivado de G é (e,r)-limitado. Portanto, pela Proposição 2.1.8, concluímos que o expoente de G é (e,r)-limitado. Então, existe um inteiro positivo $e_0 = e_0(e,r)$ tal que o expoente de G divide e_0.

Assim, o teorema está provado no caso particular onde M é um p-grupo. Note que, neste caso, o limitante e_0 do expoente de G não depende do primo p. Em geral, M é o produto direto de seus p-subgrupos de Sylow. Para cada divisor primo p da ordem de M, considere $O_{p'}(M)$ o p'-subgrupo normal maximal de M. Temos que o expoente de $G/O_{p'}(M)$ divide e_0 para cada divisor primo p da ordem de M. Pois, consideremos p um primo que divide a ordem de M. Então, $M/O_{p'}(M)$ é um p-grupo. Assim, repetindo o mesmo argumento que fizemos no parágrafo anterior, só que em quocientes, vamos concluir que o comprimento derivado de $M/O_{p'}(M)$ é (e,r)-limitado. Além disso, como o comprimento derivado do grupo quociente de $G/O_{p'}(M)$ por $M/O_{p'}(M)$ é (e,r)-limitado, resulta que $G/O_{p'}(M)$ possui comprimento derivado (e,r)-limitado. Agora, usando a Proposição 2.1.8, segue que o expoente de $G/O_{p'}(M)$ divide e_0 para cada divisor primo p da ordem de M. Isto implica, pelo Lema 1.1.25, que o expoente de $G/\bigcap_{p\in\pi(M)} O_{p'}(M)$ divide e_0. Mas como, $\bigcap_{p\in\pi(M)} O_{p'}(M) = 1$, concluímos que o expoente de G divide e_0 e o resultado segue como queríamos. □

5

Grupos Finitos Admitindo um Automorfismo Coprimo

Neste capítulo, vamos demonstrar os resultados principais que obtivemos relacionados a grupos finitos que admitem um automorfismo coprimo. Na primeira seção, veremos os detalhes da prova do Teorema C e para isto utilizamos as ferramentas Lie-teóricas apresentadas no Capítulo 3. Na segunda seção, apresentamos alguns resultados técnicos que serão utilizados na prova do Teorema D e a demonstração do mesmo. Novamente, para comodidade do leitor, repetiremos o enunciado de cada teorema.

5.1. Prova do Teorema C

Teorema C. *Sejam e, n inteiros positivos e G um grupo finito admitindo um automorfismo coprimo ϕ de ordem n tal que cada elemento de $G_\phi \cup G_{-\phi}$ pertence a um subgrupo ϕ-invariante de expoente dividindo e. Então, o expoente de G é (e, n)-limitado.*

Demonstração. Pelo Lema 2.1.1, item (iv), temos que ϕ deixa invariante algum p-subgrupo de Sylow de G para qualquer divisor primo p da ordem de G. Assim, é suficiente provar o teorema adicionando a hipótese de que G é um p-grupo. De fato, suponhamos que o resultado vale para p-grupos finitos. Consideremos $\{P_1, \ldots, P_s\}$ os p_i-subgrupos de Sylow ϕ-invariantes de G. Então, obtemos que o expoente de P_i é (e, n)-limitado para todo $i \in \{1, \ldots, s\}$. Agora, como o expoente de G divide o produto dos expoentes de P_i, segue que o expoente de G é também (e, n)-limitado.

Assim, a partir de agora, G é um p-grupo e e é uma potência de p. Note que qualquer elemento de G pertence a um subgrupo ϕ-invariante n-gerado, pois basta

considerar $g \in G$ e $\langle g \rangle^{\langle \phi \rangle}$ o subgrupo minimal ϕ-invariante n-gerado de G contendo g. Então, podemos assumir que G é gerado por no máximo n elementos. Sejam $L = L_p(G)$ e $L_i = (D_i/D_{i+1}) \cap L$. Gostaríamos de decompor os espaços lineares L_i como somas diretas de autoespaços para ϕ, mas em geral, isso não é possível, pois o corpo $\mathbb{F}_p$ pode não conter uma raiz n-ésima primitiva da unidade. Para superar essa dificuldade, estendemos o corpo base $\mathbb{F}_p$. Sejam ω uma raiz n-ésima primitiva da unidade e o produto tensorial $\overline{L} = L \otimes \mathbb{F}_p[\omega]$. Sabemos que $\overline{L}$ é uma álgebra de Lie sobre $\mathbb{F}_p[\omega]$ e L é um subconjunto de $\overline{L}$. Para qualquer $\mathbb{F}_p$-subespaço S de L escrevemos $\overline{S}$ para $S \otimes \mathbb{F}_p[\omega]$. Agora, vejamos que o $\mathbb{F}_p[\omega]$-espaço $\overline{L}_1$ tem uma base consistindo de autovetores para ϕ. De fato, como $(n, |\overline{L}_1|) = 1$ temos, pelo Lema 3.3.2, que

$$\overline{L}_1 = \bigoplus_{i=0}^{n-1} {}^i\overline{L}_1,$$

onde ${}^i\overline{L}_1 = \{l \in \overline{L}_1 \mid l^\phi = \omega^i l\}$ é o autoespaço associado ao autovalor ω^i. Assim, a dimensão de $\overline{L}_1$ é a soma das dimensões de ${}^i\overline{L}_1$. Portanto, existe uma base de $\overline{L}_1$ consistindo de autovetores para ϕ. Por outro lado, como G é n-gerado, segue que a dimensão de L_1 é no máximo n. Isto implica que a dimensão de $\overline{L}_1$ é também no máximo n, uma vez que as dimensões de $\overline{L}_1$ e L_1 coincidem.

Agora, fixemos um arbitrário i e seja $a \in \overline{L}_i$ um autovetor para ϕ. Assim, $a \in \overline{K}$ onde $\overline{K} = {}_+\left\langle a^{\langle \phi \rangle} \right\rangle$ é o $\mathbb{F}_p[\omega]$-subespaço minimal ϕ-invariante de $\overline{L}_i$ e $K = {}_+\left\langle (a')^{\langle \phi \rangle} \right\rangle$ com $a' \in L_i$ é o $\mathbb{F}_p$-subespaço minimal ϕ-invariante de L_i com a propriedade que $a \in \overline{K}$. Então, como $\overline{K}$ é ϕ-invariante e $a \in \overline{K}$ é autovetor, temos que $a \in \overline{K}_\phi$ ou $a \in [\overline{K}, \phi]$, logo $\overline{K} = \overline{K}_\phi$ ou $\overline{K} = [\overline{K}, \phi]$. Isto implica que $K = K_\phi$ ou $K = [K, \phi]$. Afirmamos que K é um $\mathbb{F}_p \langle \phi \rangle$-módulo gerado por um único elemento que corresponde a um elemento x de G, onde $x \in G_\phi$ ou $x \in G_{-\phi}$. De fato, sabemos que

$$\mathbb{F}_p \langle \phi \rangle = \left\{ \sum_{s=0}^{n-1} \beta_s \phi^s \mid \beta_s \in \mathbb{F}_p, \phi^s \in \langle \phi \rangle \right\}$$

e fazendo $K = {}_+\langle (a') \rangle$ o $\mathbb{F}_p$-subespaço de L_i, podemos definir a seguinte ação de $\mathbb{F}_p \langle \phi \rangle$ sobre K da seguinte maneira

$$\begin{array}{ccc} \mathbb{F}_p \langle \phi \rangle \times K & \longrightarrow & K \\ \left(\sum_{s=0}^{n-1} \beta_s \phi^s, a' \right) & \longmapsto & \sum_{s=0}^{n-1} \beta_s (a')^{\phi^s}. \end{array}$$

Logo, concluímos que K é um $\mathbb{F}_p \langle \phi \rangle$-módulo gerado por a'. Resta ver que $a' \in L_i$ é um elemento que corresponde a um elemento x de G, onde $x \in G_\phi$ ou

$x \in G_{-\phi}$. Com efeito, temos que $a \in C_{\overline{L}_i}(\phi)$ ou $a \in [\overline{L}_i, \phi]$, pois $a \in \overline{L}_i$ é autovetor. Por outro lado, sabendo que $C_{\overline{L}_i}(\phi) = \overline{C_{L_i}(\phi)}$ e $[\overline{L}_i, \phi] = \overline{[L_i, \phi]}$ obtemos que $a \in \overline{C_{L_i}(\phi)} = C_{L_i}(\phi) \otimes \mathbb{F}_p[\omega]$ ou $a \in \overline{[L_i, \phi]} = [L_i, \phi] \otimes \mathbb{F}_p[\omega]$. Isto implica que $a' \in C_{L_i}(\phi)$ ou $a' \in [L_i, \phi]$. Se $a' \in C_{L_i}(\phi)$, então

$$a' \in C_{D_i/D_{i+1}}(\phi) = \frac{C_{D_i}(\phi)D_{i+1}}{D_{i+1}}.$$

Assim, existem $x \in C_{D_i}(\phi)$ e $d \in D_{i+1}$ tal que

$$a' = xdD_{i+1} = xD_{i+1}.$$

Logo, $a' = xD_{i+1}$ com $x \in G_\phi$. Se $a' \in [L_i, \phi]$, então podemos facilmente concluir que $a' = xD_{i+1}$ com $x \in G_{-\phi}$. Desta maneira, a afirmação está verificada. Agora, seja X o subgrupo minimal ϕ-invariante de G contendo x. Segue que o expoente de X é um divisor de e. Portanto, pela solução do Problema Restrito de Burnside, a ordem de X é (e, n)-limitada. Em contrapartida, fazendo $K' = L(G, X)$ tem-se $K \leq K'$ e aplicando o Lema 3.5.10, segue que existe um número (e, n)-limitado u tal que

$$[L, \underbrace{K, \ldots, K}_{u}] \leq [DL(G), \underbrace{K', \ldots, K'}_{u}] = 0.$$

Logo, $[L, \underbrace{K, \ldots, K}_{u}] = 0$. Claramente, isto implica que $[\overline{L}, \underbrace{\overline{K}, \ldots, \overline{K}}_{u}] = 0$. Em particular, como $a \in \overline{K}$, obtemos $[\overline{L}, {}_u a] = 0$.

Assim, mostramos que um autovetor arbitrário contido em $\overline{L}_i$ é ad-nilpotente com índice (e, n)-limitado no máximo u. Logo, se a e b são autovetores contidos em $\overline{L}_i$ e $\overline{L}_j$ respectivamente, então pelo Lema 3.3.3, o comutador $[a, b]$ é um autovetor para ϕ contido em $\overline{L}_{i+j}$. Desta maneira, temos que $\overline{L}$ é gerado por no máximo n autovetores para ϕ, e pela observação anterior, segue que qualquer comutador nos geradores é ad-nilpotente de índice no máximo u. Agora, vejamos que $C_L(\phi)$ satisfaz certa identidade polinomial multilinear (e, n)-limitada. De fato, tem-se que G_ϕ tem expoente dividindo e. Assim, $x^e = 1$ para todo $x \in G_\phi$. Então, usando a Proposição 3.4.3, aplicada a G_ϕ e a identidade $x^e \equiv 1$, tem-se que existe um polinômio de Lie multilinear não nulo f sobre $\mathbb{F}_p$, dependendo apenas de p e x^e, tal que para qualquer N_p-série de G_ϕ, a álgebra $L^*(G_\phi)$ satisfaz a identidade $f \equiv 0$. Assim, como $L(G, G_\phi) \cong L^*(G_\phi)$, obtém-se que $L(G, G_\phi)$ também satisfaz uma identidade polinomial. Usando o Lema 3.5.9, resulta que $C_L(\phi) = L_p(G, G_\phi) \leq L(G, G_\phi)$. Desta forma, concluímos que $C_L(\phi)$ satisfaz uma certa identidade polinomial multilinear (e, n)-limitada. Por outro lado, sabendo

que $C_{\overline{L}}(\phi) = \overline{C_L(\phi)}$ temos, pela Observação 3.3.4, que $C_{\overline{L}}(\phi)$ também satisfaz uma certa identidade polinomial multilinear (e,n)-limitada. Portanto, o Corolário 3.2.3, implica que $\overline{L}$ satisfaz uma identidade polinomial (e,n)-limitada. Agora, segue do Teorema 3.2.1, que $\overline{L}$ é nilpotente de classe (e,n)-limitada, digamos c. Isto implica que L é também nilpotente de classe c. O Lema 3.5.7, nos diz que $H = D_{c+1}$ é powerful. Pelo Lema 2.1.5, $H = H_\phi H_{-\phi}$. Em particular, H é gerado por elementos de ordem dividindo e. Como H é powerful, obtemos pelo Lema 1.2.2, que o expoente de H divide e. Por fim, vejamos que o expoente de G/H divide p^c. Com efeito, sabemos que H contém G^{p^k} onde $p^k \geq c+1$. Particularmente, $G^{p^c} \leq H$. Logo, o expoente do grupo quociente de G/G^{p^c} por H/G^{p^c} divide o expoente de G/G^{p^c}. Isto implica que o expoente de G/H divide p^c. Portanto, concluímos que o expoente de G é (e,n)-limitado e o resultado está provado. □

Observe que o Teorema 4.1.2 também pode ser visto como um corolário do Teorema C.

5.2. Prova do Teorema D

A prova do Teorema D exigirá o seguinte resultado que se encontra em [**34**] cuja prova usa a classificação de grupos finitos simples.

Teorema 5.2.1. *Se um grupo finito G admite um automorfismo coprimo ϕ tal que G_ϕ é nilpotente, então G é solúvel.*

O próximo resultado é um célebre teorema, devido a Thompson. Para sua prova veja [**32**][veja também [**33**] para uma pesquisa sobre resultados de natureza semelhante].

Teorema 5.2.2. *Se um grupo solúvel finito G admite um automorfismo coprimo ϕ, então $h(G)$ é limitado em termos de $h(G_\phi)$ e o número de primos divisores da ordem de ϕ, contando multiplicidades.*

Para um subconjunto X de um grupo admitindo um automorfismo ϕ, escreveremos $\langle X\rangle^{\langle\phi\rangle}$ para denotar o subgrupo minimal ϕ-invariante contendo X.

O lema a seguir será muito útil na prova do Teorema D.

Lema 5.2.3. *Seja G um grupo nilpotente finito admitindo um automorfismo coprimo ϕ tal que $G = [G,\phi]$. Se S é o conjunto dos elementos $h \in G_\phi$ para os quais existem $x_1, x_2 \in G_{-\phi}$ tais que $h \in \langle x_1, x_2\rangle^{\langle\phi\rangle}$, então $G_\phi = \langle S\rangle$.*

Demonstração. Note que $S \neq \emptyset$, pois $1 \in S$. Agora, façamos $H = \langle S\rangle$. Claramente, temos $H \leq G_\phi$. Assim, precisamos provar que $G_\phi \leq H$. Seja $h \in G_\phi$.

Como $G = [G, \phi]$, podemos escrever $h = g_1 \cdots g_m$ com $g_i \in G_{-\phi}$. Desejamos provar que $h \in H$. Isto será mostrado por indução em m. Com efeito, se $m \leq 2$, então obviamente $h \in H$. Assim, assuma que $m \geq 3$. Seja $K = \langle g_{m-1}, g_m \rangle^{\langle \phi \rangle}$. Como K é ϕ-invariante, temos pelo Lema 2.1.5, que $g_{m-1}g_m = g_0h_0$, onde $g_0 \in K_{-\phi}$ e $h_0 \in K_\phi$. Evidentemente, $K_\phi \leq H$ e então $h_0 \in H$. Assim,

$$h = g_1 \cdots g_{m-2}g_0h_0.$$

Isto implica que

$$hh_0^{-1} = g_1 \cdots g_{m-2}g_0.$$

Então, por hipótese de indução, segue que $hh_0^{-1} \in H$ e consequentemente $h \in H$. Portanto, concluímos que $H = G_\phi$. □

O próximo lema segue direto de um resultado de Hartley que se encontra em [**8**, Lemma 2.6].

Lema 5.2.4. *Seja ϕ um automorfismo coprimo de um grupo finito G. Sejam $\{N_i \mid i \in I\}$ uma família de subgrupos normais ϕ-invariantes de G e $N = \prod_{i\in I} N_i$. Então, $N_\phi = \prod_{i\in I}(N_i)_\phi$.*

Demonstração. Suponhamos que I seja um conjunto com t elementos. Faremos a prova por indução em t. Se $t = 1$, então o resultado é óbvio. Sejam $t \geq 2, M = N_1N_2 \cdots N_{t-1}$ e $L = N_t$. Aplicando, a hipótese de indução em M, obtemos

$$M_\phi = N_\phi \cap M = \prod_{i=1}^{t-1}(N_i)_\phi. \tag{5.2.1}$$

Agora, considerando o epimorfismo canônico de G em G/M e usando o Lema 2.1.1, item (i), tem-se

$$(N_\phi \cap ML)M/M \leq (ML/M)_\phi = L_\phi M/M.$$

Logo, $N_\phi \cap ML \leq M(N_\phi \cap L)$. Usando a Lei Modular de Dedekind, Lema 1.1.4, resulta que

$$N_\phi \cap ML = (N_\phi \cap M)(N_\phi \cap L).$$

Então, por (5.2.1), temos

$$\begin{aligned} N_\phi &= \prod_{i=1}^{t-1}(N_i)_\phi \cdot (N_t)_\phi \\ N_\phi &= \prod_{i=1}^{t}(N_i)_\phi. \end{aligned}$$

como queríamos. □

Estamos agora prontos para provar o Teorema D.

Teorema D. *Seja G um grupo finito admitindo um automorfismo coprimo ϕ de ordem n tal que G_ϕ é nilpotente de classe c e $x^e = 1$ para cada $x \in G_{-\phi}$. Suponha que quaisquer dois elementos de $G_{-\phi}$ pertencem a um subgrupo solúvel ϕ-invariante de comprimento derivado d. Então, o expoente de $[G, \phi]$ é limitado em termos de c, d, e e n.*

Demonstração. Sem perda de generalidade podemos assumir que $G = [G, \phi]$. Pelo Teorema 5.2.1, segue que G é um grupo solúvel. Agora, o Teorema 5.2.2 nos diz que a altura de Fitting de G é limitada por uma constante dependendo somente de n. Assim, o teorema será provado por indução em $h(G)$.

Se $h(G) = 1$, então G é nilpotente. Para arbitrários $x_1, x_2 \in G_{-\phi}$ considere $K = \langle x_1, x_2 \rangle^{\langle \phi \rangle}$ o subgrupo minimal ϕ-invariante de G contendo x_1 e x_2. Temos, pelo Lema 2.1.6, que $K = [K, \phi]$. Agora, utilizando as hipóteses do teorema e a Proposição 2.1.8 obtemos que o expoente de K é (d, e)-limitado. Assim, mostramos que qualquer elemento de $G_{-\phi}$ está contido em um subgrupo ϕ-invariante de expoente (d, e)-limitado. Para usarmos o Teorema C, resta limitar o expoente de G_ϕ. De fato, pelo Lema 5.2.3, o subgrupo G_ϕ é gerado pelas interseções $G_\phi \cap \langle x_1, x_2 \rangle^{\langle \phi \rangle}$, onde x_1 e x_2 variam em $G_{-\phi}$. Desejamos mostrar que G_ϕ é gerado por elementos de ordem limitada. Com efeito, note que o expoente do subgrupo cíclico gerado por h é (d, e)-limitado para todo $h \in G_\phi \cap K$, uma vez que K possui expoente (d, e)-limitado. Desta forma, G_ϕ é gerado por elementos de ordem (d, e)-limitada e por ser nilpotente de classe c obtemos pelo Lema 1.1.26, que o expoente de G_ϕ é (c, d, e)-limitado. Assim, pelo Lema 2.1.5, $G = G_{-\phi} G_\phi$, então concluímos que qualquer elemento de $G_\phi \cup G_{-\phi}$ está contido em um subgrupo ϕ-invariante de expoente (c, d, e)-limitado. Portanto, o Teorema C afirma que o expoente de G é (c, d, e, n)-limitado, como queríamos.

Assumamos agora que $h(G) \geq 2$. Sejam $F = F(G)$ o subgrupo de Fitting de G e $N = \left\langle [F, \phi]^G \right\rangle$ o fecho normal de $[F, \phi]$ em G. Afirmamos que $h(G/N) \leq h(G) - 1$. De fato, seja $h = h(G)$, então existe uma série normal

$$F_0(G) = 1 \leq F_1(G) = F \leq F_2(G) \leq \cdots \leq F_h(G) = G,$$

tal que $F_{i+1}(G)/F_i(G)$ é nilpotente para todo $0 \leq i \leq h - 1$. Observe que $F/N \leq Z(G/N)$, pois ϕ age trivialmente em F/N e consequentemente $F/N \leq (G/N)_\phi$. Então, aplicando o Lema 2.1.2, em G/N, concluímos que $F/N \leq Z(G/N)$. Isto implica que $F/N \leq Z(F_2(G)/N)$. Assim, aplicando a Proposição 1.1.8, resulta

que $F_2(G)/N$ é nilpotente. Com isto, obtemos uma série normal em G/N de comprimento no máximo $h-1$ cujos quocientes são nilpotentes. Logo, concluímos que $h(G/N) \leq h-1$. Portanto, por hipótese de indução, segue que o expoente de G/N é (c,d,e,n)-limitado. Consequentemente, é suficiente mostrar que o expoente de N é (c,d,e,n)-limitado. Para isto, note que $N = N_\phi[F,\phi]$, pois como $[F,\phi] = [F,\phi,\phi] \leq [N,\phi]$, obtemos $[F,\phi] = [N,\phi]$. E sabendo que o teorema vale para grupos nilpotentes, temos que o expoente de $[F,\phi]$ é (c,d,e,n)-limitado. Desta maneira, pelo Teorema C, precisamos provar que o expoente de N_ϕ é também limitado.

Com efeito, sejam $x \in G$ e N_x o subgrupo minimal ϕ-invariante de G contendo $[F,\phi]^x$. Sabendo que o expoente de $[F,\phi]$ é (c,d,e,n)-limitado e que N_x é um produto de no máximo n subgrupos da forma $([F,\phi]^x)^{\phi^i}$, onde cada subgrupo $([F,\phi]^x)^{\phi^i}$ normaliza o outro e possui expoente limitado, concluímos que o expoente de N_x é também (c,d,e,n)-limitado. Em particular, o expoente de $N_x \cap G_\phi$ é (c,d,e,n)-limitado. Assim, pelo Lema 5.2.4, aplicado em N_x, obtemos que N_ϕ é o produto de subgrupos $N_x \cap G_\phi$, com $x \in G$. Logo, N_ϕ é um grupo nilpotente de classe no máximo c gerado por elementos de ordem (c,d,e,n)-limitada. Então, pelo Lema 1.1.26, segue que o expoente de N_ϕ é (c,d,e,n)-limitado. Portanto, o expoente de N é limitado em termos de c,d,e e n e a prova está completa. □

Note que no caso onde $n = 2$, sempre temos $x^\phi = x^{-1}$ para todo $x \in G_{-\phi}$. Consequentemente, obtém-se que qualquer subgrupo gerado por um subconjunto de $G_{-\phi}$ é ϕ-invariante. Portanto, concluímos que o Teorema D é uma extensão do Teorema A e assim finalizamos os resultados desta tese.

Referências Bibliográficas

[1] Yu. A. Bahturin, M. V. Zaicev, Identities of graded algebras, J. Algebra, **205** (1998), 1-12.

[2] E. Bettio, G. Busetto, E. Jabara, Automorfismi involutori di p-gruppi finiti, Rend. Sem. Mat. Univ. Padova, **129** (2013), 1-15.

[3] J. D. Dixon, M. P. F. du Sautoy, A. Mann, D. Segal, *Analytic pro-p groups* (London Math. Soc. Lecture Note Series **157**), Cambridge Univ. Press., 1991.

[4] W. Feit, J. Thompson, Solvability of groups of odd order, Pacific J. Math., **13** (1963), 773-1029.

[5] D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.

[6] P. Hall, G. Higman, The p-length of a p-soluble group and reduction theorems for Burnside's problem, Proc. London. Math. Soc. (3), **6** (1956), 1-42.

[7] B. Hartley, Th. Meixner, Periodic groups in which the centralizer of an involution has bounded order, J. Algebra, **64** (1980), 285-291.

[8] B. Hartley, Periodic locally soluble groups containing an element of prime order with Černikov centralizer, Quart. J. Math. Oxford, **33** (1982), 309-323.

[9] G. Higman, Groups and rings which have automorphisms without non-trivial fixed elements, J. London Math. Soc. (2), **32** (1957), 321-334.

[10] G. Higman, Lie ring methods in the theory of finite nilpotent groups, in "Proc. Intern. Congr. Math. Edinburgh, 1958", Cambridge Univ. Press, 1960, 307-312.

[11] B. Huppert, N. Blackburn, *Finite Groups II*, Springer Verlag, Berlin, 1982.

[12] I. M. Isaacs, *Finite Group Theory*, Amer. Math. Soc., 2008.

[13] E. I. Khukhro, *Nilpotent Groups and their Automorphisms*, Berlin; New York: Walter de Gruyter, (1993).

[14] E. I. Khukhro, *p-Automorphisms of finite p-groups*, Cambridge University Press, (1997).

[15] E. I. Khukhro, P. V. Shumyatsky, Bounding the exponent of a finite group with automorphisms, J. Algebra, **212** (1999), 363-374.

[16] E. Khukhro, P. Shumyatsky, Finite groups with Engel sinks of bounded rank, Glasgow Math. J., **60** (2018), 695-701.

[17] A. I. Kostrikin, On the Burnside problem, Izv. AN SSSR, Ser. Mat. **23** (1959), 3-34.

[18] M. Lazard, Sur les groupes nilpotents et les anneaux de Lie, Ann. Sci. École Norm. Supr., **71** (1954), 101-190.

[19] V. Linchenko, Identities of Lie algebras with actions of Hopf algebras, Commun. Algebra, **25** (1997), 3179-3187.

[20] A. Lubotzky, A. Mann, Powerful p-groups. I: Finite groups, J. Algebra, **105** (1987), 484-505; II: p-adic analytic groups, *ibid.*, 506-515.

[21] W. Magnus, A connection between the Baker-Hausdorff formula and a problem of Burnside, Ann. of Math. (2), **52** (1950), 111-126.

[22] A. Mann, The exponents of central factor and commutator groups, J. Group Theory, **10** (2007), 435-436.

[23] D. M. Riley, Analytic pro-p groups and their graded group rings, J. Pure Appl. Algebra, **90** (1993), 69-76.

[24] D. J. S. Robinson, *A course in the theory of groups*, Second edition. Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[25] S. R. S. Rodrigues, P. Shumyatsky, Exponent of a finite group of odd order with an involutory automorphism, Archiv der Mathematik, **113** (2019), 113-118.

[26] S. R. S. Rodrigues, P. Shumyatsky, Exponent of a finite group admitting a coprime automorphism, J. Pure Appl. Algebra, **224** (2020), 106370.

[27] I. N. Sanov, Establishment of a connection between periodic groups with period a prime number and Lie rings, Izv. Akad. Nauk SSSR, Ser. Mat., **16** (1952), 23-58 (Russian).

[28] P. Shumyatsky, Involutory automorphisms of finite groups and their centralizers, Arch. Math., **71** (1998), 425-432.

[29] P. Shumyatsky, Exponent of a finite group with an involutory automorphism, J. Group Theory, **2** (1999), 367-372.

[30] P. Shumyatsky, Applications of Lie ring methods to group theory, Nonassociative Algebra and Its Applications, (Eds R. Costa et al.), Marcel Dekker, New York, (2000), 373-395.

[31] J. G. Thompson, Finite groups with fixed-point-free automorphisms of prime order, Proc. Natl. Acad. Sci. USA, **45** (1959), 578-581.

[32] J. G. Thompson, Automorphisms of solvable groups, J. Algebra, **1** (1964), 259-267.

[33] A. Turull, Character theory and length problems, in: Finite and locally finite groups, Istanbul, 1994, in: NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 471, Kluwer Acad. Publ., Dordrecht, (1995), 377-400.

[34] M. Y. Wang, M. Z. Chen, Solubility of finite groups admitting a coprime order operator group, Boll. Un. Mat. Ital., **7** (1993), 325-331.

[35] J. S. Wilson, E. Zelmanov, Identities for Lie algebras of pro-p groups, J. Pure Appl. Algebra, **81** (1992), 103-109.

[36] H. Zassenhaus, Ein Verfahren, jeder endlischen p-gruppe einen Lie-Ring mit der Charakteristik p zuzuordnen, Abh. Math. Seminar Hans. Univ. Hamburg, **13** (1940), 200-207.

[37] E. Zelmanov, The solution of the restricted Burnside problem for groups of odd exponent, Math. USSR Izv., **36** (1991), 41-60.

[38] E. Zelmanov, The solution of the restricted Burnside problem for 2-groups, Math. Sb., **182** (1991), 568-592.

[39] E. Zelmanov, *Nil Rings and Periodic Groups*, The Korean Math. Soc. Lecture Notes in Math., Seoul, 1992.

[40] E. I. Zelmanov, Lie algebras and torsion groups with identity, J. Combin. Algebra, **1** (2017), 289-340.