Universidade de Brasília

Sobre grupos finitos admitindo um grupo de *Frobenius* como grupo de automorfismos

Maria Edna Gomes da Silva

Orientador: Emerson Ferreira de Melo

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Dissertação apresentada como requisito parcial para obtenção do grau de
Mestre em Matemática

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre grupos finitos admitindo um grupo de Frobenius como grupo de automorfismos.

por

Maria Edna Gomes da Silva*

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

MESTRE EM MATEMÁTICA

Brasília, 28 de junho de 2019.

Comissão Examinadora:

Emerson Ferreira de Melo

Prof. Dr. Emerson Ferreira de Melo- MAT/UnB (Orientador)

Igor dos Santos Lima

Prof. Dr. Igor dos Santos Lima– MAT/UnB (Membro)

Prof. Dr. Ricardo Nunes de Oliveira– UFG (Membro)

* A autora foi bolsista do CNPq durante a elaboração desta dissertação.

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

Gs

Gomes da Silva, Maria Edna
Sobre grupos finitos admitindo um grupo de Frobenius como grupo de automorfismos / Maria Edna Gomes da Silva; orientador Emerson Ferreira de Melo. -- Brasília, 2019.
104 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2019.

1. Grupo de Frobenius. 2. Anéis de Lie. 3. Automorfismo. I. Ferreira de Melo, Emerson, orient. II. Título.

"Mas tu, Senhor, és o escudo que me protege; és a minha glória e me fazes andar de cabeça erguida.
Ao Senhor clamo em alta voz, e do seu santo monte ele me responde.
Eu me deito e durmo, e torno a acordar, porque é o Senhor que me sustém.
(Bíblia Sagrada-Salmos 3,3-5)

Agradecimentos

Dedico esse trabalho primeiramente a Deus por ter me dado força e discernimento para seguir em frente.

A minha família por ser meu porto seguro e entender as inúmeras vezes que não dava notícia, amo muitos vocês. Em especial ao meu pai(Gilvan) que me trouxe para essa aventura que foi fazer mestrado distante de casa. A minha tia(Maria) por toda preocupação e cuidado. A minha madrasta(Silvana) por todas as mensagem de força. A minha irmã(Érica) por toda força, por cuidar de mim, por cuidar por mim e por acreditar em mim hoje e sempre.

Ao meu namorado Deivid por toda ajuda no Latex e principalmente pela força, amor e carinho.

Aos meus amigos da sala mais top: Kelvin, Rosalina, Adler, Vitor, Junio, Claúdia, Mateus, Geovane, Bruna, Gabrielzinho, Gabriel e principalmente Paulo por toda força, conselhos e assistirem minhas inúmeras prévias. E a todos que me ajudaram nessa caminhada, muito obrigada.

Ao meu orientador, Emerson Ferreira de Melo por toda ajuda, dedicação e compromisso prestado na construção deste trabalho. Sem dúvida um dos melhores profissionais que pude ter a honra de trabalhar.

Aos professores que contribuíram para a minha formação como mestre, Carlos Alberto, Sheila Chagas, José Luis Teruel, Daniele, Maurício Ayala e principalmente a professora Cristina Acciari.

Aos funcionários do departamento de matemática que estiveram presentes em todas as aflições passadas. Em especial a Claúdia Messias, Emanoel e Otacílio.

Aos professores, Igor dos Santos Lima, Ricardo Nunes de Oliveira e Alex Carrazedo Dantas, pelas correções, sugestões e contribuições para a versão final desse trabalho.

Ao CNPq pelo financiamento durante a construção deste trabalho.

A todos vocês o meu sincero agradecimento.

Resumo

Esta dissertação apresenta um estudo sobre grupos finitos admitindo um grupo de *Frobenius* como grupo de automorfismos. Apresentamos as demonstrações de resultados inspirados nos problemas 17.72 e 18.67, propostos no *The Kourovka Notebook*, que tratam sobre a limitação da classe de nilpotência e do expoente de um grupo G, respectivamente. Além disso, apresentamos resultados importantes para Teoria de anéis de Lie, por exemplo, o Teorema de *Higman-Kreknin-Krostrikin*.

Palavras-Chave: Gupos de *Frobenius*, Anéis de Lie e Automorfismo.

Abstract

This dissertation presents a study about finite groups admitting a group of *Frobenius* as its group of automorphisms with emphasis on questions about nilpotency and group exponent. We present the solutions of results inspired by problems 17.72 and 18.67, proposed in 'The Kourovka Notebook' these problems deals with limitations for nilpotency class and the exponent of a group G, respectively. Moreover, we study important results from Lie Ring Theory for instance the theorem of *Higman-Kreknin-Krostrikin* whose proof is found in this work.

Keywords: *Frobenius* groups, Lie Rings and Automorphism.

Sumário

Introdução

Sejam G um grupo e φ um automorfismo de G, definimos o conjunto dos pontos fixos de G como o $C_G(\varphi) = \{g \in G \mid g^{\varphi} = g\}$ e dizemos que φ é um automorfismo regular ou φ é livre de pontos fixos se $C_G(\varphi) = \{1\}$. Os resultados sobre automorfismos livres de pontos fixos são importantes na Teoria de Grupos. Um dos primeiros resultados com automorfismos livres de pontos fixos é dado por *Burnside* por volta de 1902 e encontra-se em *Theory of Groups of Finite Order* [2], ele demonstra que se um grupo finito G admite um automorfismo φ de ordem 2 e livre de pontos fixos, então G é um grupo abeliano de ordem ímpar. Posteriormente, Neumann [22] provou que se G é um grupo que admite um automorfismo φ livre de pontos fixos de ordem 3 então G é necessariamente nilpotente.

Outro resultado que merece destaque é o apresentado por Higman [11] em 1957, ele mostrou que um grupo nilpotente com um automorfismo livre de pontos fixos de ordem prima p tem classe de nilpotência limitada por uma função $h(p)$, essa função depende apenas de p. Em 1959 Thompson [9, Teorema 10.2.1] provou que um grupo finito com automorfismo livre de pontos fixos de ordem prima é necessariamente nilpotente. Esses resultados juntos mostram que um grupo finito com automorfismo livre de pontos fixos de ordem p é nilpotente e sua classe é limitada em função apenas de p. Muitos resultados mostram a influência dos centralizadores de automorfismos, principalmente quando a ordem do grupo de automorfismo e a ordem do grupo são coprimas como o resultado provado por Khukhro e Shumyatsky [15]: Sejam p um primo, e um inteiro positivo e A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G, assuma que o expoente do $C_G(a)$ divide e para todo $a \in A \setminus \{1\}$. Então, o expoente de G é limitado por uma função dependendo somente de e e p. Nesse contexto é natural esperar que a estrutura do grupo G esteja relacionada com a estrutura dos $C_G(a)$, pois se A é um grupo abeliano não-cíclico e a ordem de A é coprima com a ordem de G então $G = \langle C_G(a) \mid a \in A \setminus \{1\} \rangle$.

Uma maneira de resolver problemas de grupos consiste em transcrever o problema para um anel de Lie associado, essa técnica cresceu no século passado com a solução positiva do Problema Restrito de Burnside dado por Efim Zelmanov em 1989. A investigação de problemas de grupos com enfoque em Nilpotência e Solubilidade trouxeram descobertas

de resultados importantes para teoria de anéis de Lie e desenvolveram novas técnicas para resolver problemas de grupos. Entre os resultados mais conhecidos destaca-se o teorema de *Higman-Kreknin-Krostrikin* [12] que afirma que se um anel de Lie A admite um automorfismo regular φ de ordem prima p, então ele é nilpotente de classe que depende apenas de p.

Motivados por problemas propostos no *The Kourovka Notebook* [21] desejamos apresentar a solução de alguns problemas que envolvem Nilpotência e Expoente de um grupo finito G admitindo um grupo de *Frobenius* como grupo de automorfismo. Um grupo G é dito grupo de *Frobenius* se G pode ser escrito como o produto semidireto dos subgrupos F e H com os mesmos sendo núcleo e complemento, respectivamente, tais que $C_F(h) = 1$ para todo $h \in H \setminus \{1\}$ e um grupo G é chamado *2-Frobenius* grupo se possui um subgrupo normal H que é subgrupo de *Frobenius* com núcleo A tal que G/A é de *Frobenius* com núcleo H/A.

Os grupos de *Frobenius* e 2-*Frobenius* aparecem naturalmente no estudo de *Grafos de Gruenberg-Kegel* (Grafos Primo): O espectro de um grupo finito G é o conjunto $\omega(G)$ das ordens dos elementos de G. O subconjunto de números primos é chamado de espectro primo de G e denotado por $\pi(G)$. O espectro $\omega(G)$ define o *Grafos de Gruenberg-Kegel* $\Gamma(G)$ de G cujos vértices são os elementos de $\pi(G)$ no qual dois vertices r e s são adjacentes se, e somente se, $rs \in \omega(G)$. O Teorema de *Gruenberg-Kegel* [20] diz que G é solúvel com Grafos de Gruenberg-Kegel desconexo se e somente se G é um grupo de *Frobenius* ou *2-Frobenius*.

Destacamos a seguir dois problemas encontrados no *The Kourovka Notebook* [21].

Problema 17.72: Seja FH um grupo de *Frobenius* com núcleo F e complemento H. Suponha que FH age em um grupo finito G de modo que GF é um grupo de *Frobenius* de núcleo G e complemento F.

1. Será que a classe de nilpotência de G é limitada em termos $|H|$ e da classe de nilpotência do $C_G(H)$?

2. Será que o expoente de G é limitada em termos da $|H|$ e do expoente do $C_G(H)$?

Problema 18.67: Suponha que um grupo finito G admita um grupo de *Frobenius* automorfismo de FH com núcleo F e complemento H tal que $C_G(F) = 1$. O expoente de G é limitado em termos da $|F|$ e do expoente $C_G(H)$?

Note que no Problema 17.72 o grupo GFH é um grupo 2-Frobenius. E no Problema 18.67 o grupo GFH não é 2-Frobenius, mas G admite um grupo de Frobenius como grupo de automorfismo.

O primeiro item do Problema 17.72 tem solução positiva, demonstrado por N. Yu. Makarenko e P. Shumyatsky no artigo *Frobenius Groups As Groups of Automorphisms* [19]. O item 2 encontram-se sem resposta. Outros problemas sobre grupos 2-Frobenius e sobre

grupos finitos com grupo de Frobenius como grupo de automorfismo podem ser encontrados no *The Kourovka Notebook*.

Neste trabalho apresentamos a demonstração do item 1 do Problema 17.72 e soluções parciais do item 2 do Problema 17.72 e do Problema 18.67.

No primeiro capítulo apresentamos resultados clássicos da Teoria de Grupos e Módulos. Alguns dos resultados apresentados são bem conhecidos e por isso omitiremos as demonstrações. Apresentamos ainda, uma seção destinada a propriedades e conceitos dos p-grupos *Powerful*.

O segundo capítulo é destinado ao estudo de grupos de *Frobenius* e 2-*Frobenius*. Apresentando resultados básicos sobre tais grupos e finalizamos o capítulo apresentando alguns resultados sobre grupos de *Frobenius* FH agindo como o grupo dos automorfismos sobre um grupo finito G.

O terceiro capítulo é destinado ao estudo de Anéis de Lie e anéis de Lie associados com ênfase na construção das Álgebras de Lie (ou anel de Lie) e resultados clássicos como o Teorema de Higman, Kreknin e Krostrikin demonstrado no final da seção. Apresentamos uma seção para falar sobre Álgebra de Jenning-Lazard popularizada por Enfim Zelmanov em 1989 para solucionar o Problema Restrito de Burnside.

No quarto capítulo apresentamos a demonstração dada por N. Yu. Makarenko e P. Shumyatsky no artigo *Frobenius Groups As Groups of Automorphisms* [19] para o item 1. do Problema 17.72 e os principais resultados do artigo.

Por fim, o quinto capítulo apresenta as demonstrações dos principais resultados dos artigos publicados por E.I Khukhro, N. Yu. Makarenko e P Shumyatsky *Frobenius groups of automorphisms and their fixed points* [14] e P. Shumyatsky [25], referentes ao item 2 do Problema 17.72 e ao Problema 18.67. Neles foram estudados os casos onde um grupo de Frobenius com núcleo cíclico ou o grupo de *Frobenius* $FH \cong \mathbb{A}_4$ agem como grupo de automorfismos. Para isso utilizamos resultados apresentados nos capítulos 2 e 3 .

Capítulo 1

Preliminares

1.1 Teoria de Grupos

Os resultados sobre teoria de grupos deste trabalho baseiam-se principalmente nos livros *A Course in the Theory of Groups* [23] e *Finite Groups* [9].

Seja G um grupo e a um elemento de G, o $C_G(a)$ é o subconjunto dos elementos de G que comutam com a;

$$C_G(a) = \{x \in G \mid ax = xa\}. \tag{1.1}$$

Para cada elemento a de um grupo G o centralizador de a em G é um subgrupo de G. Seja H um subgrupo de G o *Centralizador de H em G*, é o subgrupo:

$$C_G(H) = \{x \in G \mid yx = xy, \forall y \in H\} \tag{1.2}$$

De modo semelhante, definimos o conjuntos dos pontos fixos de um automorfismo ϕ de G por $C_G(\phi) = \{x \in G \mid x^\phi = x\}$. O automorfismo ϕ é dito regular se $C_G(\phi) = \{x \in G \mid x^\phi = x\} = 1$.

Definição 1.1.1. O subgrupo *Frattini* de G, denotado por $\Phi(G)$ é a interseção de todos subgrupos maximais de G.

Seja π um conjunto não vazio de primos, chamamos de π' o conjunto $\mathbb{P} \setminus \pi$, com $\mathbb{P}$ sendo o conjunto dos números primos.

Definição 1.1.2. Seja $m \in \mathbb{N}$, m é dito um π-número se para todo p tal que $p|m$ tivermos $p \in \pi$.

Definição 1.1.3. $H \leq G$ é dito π-subgrupo de G se $|H|$ é um π-número.

Definição 1.1.4. Um subgrupo H de G é dito π-subgrupo de *Hall*, se H é um π-subgrupo tal que $[G:H]$ é um π'-número.

Para um grupo arbitrário G, define-se o **expoente de** G como o menor número natural m tal que $g^m = 1$, para todo $g \in G$.

Seja G um grupo, o comutador de dois elementos x e y de G é dado por $[x,y] = x^{-1}y^{-1}xy$, além disso dizemos que x e y comutam se, e somente se, $[x,y] = 1$.

Podemos definir o comutador de s elementos do grupo G de forma indutiva da seguinte maneira: $[x] = x$, o comutador de $x_1, \cdots, x_s$ é definido por $[x_1,...,x_s] = [[x_1,...,x_{s-1}],x_s]$.

Seja X um conjunto. Definimos por recorrência o peso de um comutador em X. Definimos comutador de peso 1 como os elementos de X, se x_1 e x_2 são comutadores de peso s_1 e s_2, respectivamente, então $[x_1,x_2]$ é um comutador de peso s_1+s_2 em X. E o comutador $[x_1,...,x_s] = [[x_1,...,x_{s-1}],x_s]$, onde cada entrada é um comutador de peso 1, chamado de comutador simples de peso s.

Indicamos por subgrupo comutador de A e B ou A com B e denotamos por $[A,B]$, onde A e B são subconjuntos de G, o subgrupo:

$$[A,B] = \langle [a,b] \mid a \in A \text{ e } b \in B \rangle$$

É claro que de forma análoga podemos definir o comutador de s elementos. Dados $X_1,...,X_s$ subconjuntos de G, definimos $[X_1,...,X_s]$ como o subgrupo de G gerado por todos comutadores da forma $[x_1,...,x_s]$, onde $x_i \in X$.

Teorema 1.1.5. Seja G um grupo e considere x, y e z elementos de G. Então valem as seguintes propriedades:

1. $[x,y] = x^{-1}y^{-1}xy$
2. $[y,x] = [x,y]^{-1}$
3. $[xy,z] = [x,z]^y[y,z] = [x,z,y][y,z]$
4. $[x,yz] = [x,z]^y = [x,z][x,y][x,y,z]$
5. $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$ (Identidade de Hall-Witt)
6. $yx = xy[y,x]$

Teorema 1.1.6. Sejam G um grupo e L,K e H subgrupos de G. Então:

1. $[H,K] = [K,H]$;

2. $H \leq N_G(K)$ se, e somente se, $[H,K] \leq K$;
3. $H \leq C_G(K)$ se, e somente se, $[H,K] = 1$;
4. Se N é normal em G, então $\left[HN/N, KN/N\right] = [H,K]N/N$
5. Se H,K e L são subgrupos normais de G, então $[HK,L] = [H,L][K,L]$

Um resultado bastante conhecido e útil é o *lema dos três subgrupos*, usaremos esse resultado em algumas das demonstrações apresentadas nesse trabalho.

Lema 1.1.7 (Lema dos Três Subgrupos)**.** Sejam G um grupo, H,J e K subgrupos de G e $H \trianglelefteq G$ tal que $[K,H,J],[J,K,H] \leq N$. Então $[H,J,K] \leq N$.

1.2 Grupos Nilpotentes e Solúveis

Duas classes de grupos bastante importante para a teoria de grupo, bem como para este trabalho são os grupos nilpotentes ou solúveis.

Definição 1.2.1. Definimos a série central de um grupo G como:

$$1 = G_0 \leq G_1 \leq ..... \leq G_n = G$$

onde cada quociente G_i/G_{i-1} está contido no centro de G/G_{i-1}, para $0 \leq i \leq n$.

Definição 1.2.2. Os membros da série central inferior de um grupo G são definidos indutivamente como segue:

$$\begin{aligned} \gamma_1(G) &= G \\ \gamma_2(G) &= [\gamma_1(G), G] = [G,G] = G' \\ &\vdots \\ \gamma_{i+1}(G) &= [\gamma_i(G), G] \end{aligned}$$

Teorema 1.2.3. Seja G um grupo então $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$ para todo i e $j \in \mathbb{N}$, onde $\gamma_i(G)$ é o i-ésimo termo da série central inferior.

Se G possui uma série como na definição 1.2.2 tal que $\gamma_n(G) = 1$ então G é *Nilpotente.*

Teorema 1.2.4. Seja G um grupo e N um subgrupo normal de G. Então $[\gamma_k(N), G] \leq [N, \gamma_k(G)]$, para todo $k \geq 1$

Teorema 1.2.5. Seja G um grupo e N um subgrupo normal de G. Então $\gamma_k(G/N) = \gamma_k(G)N/N$, para todo $k \geq 1$.

Teorema 1.2.6. Se G é nilpotente então:

1. Se $N \lhd G$ então G/N é nilpotente.
2. Se $H \leq G$, então H é nilpotente.

Teorema 1.2.7. Se G é um p-grupo finito então G é nilpotente.

Definição 1.2.8. Definimos classe de nilpotência como o menor inteiro n tal que $\gamma_n(G) = 1$, denotaremos por $cl(G)$.

Teorema 1.2.9. Seja G grupo finito. São equivalentes:

1. G é nilpotente;
2. $H < N_G(H)$, para todo $H < G$;
3. Todo subgrupo maximal de G é normal;
4. Todo subgrupo de Sylow de G é normal (Portanto Único);
5. G é o produto direto de seus subgrupos de Sylow ($G \cong P_1 \times P_2 \times ... \times P_t$);
6. Dado um n divisor de $|G|$, existe algum $H \lhd G$ tal que $|H| = n$;
7. Dados a e $b \in G$, com $mdc(o(a), o(b)) = 1$, tem-se $ab = ba$;
8. Para todo $N \lhd G$ tem-se que $Z(G/N)$ não é trivial.

Definição 1.2.10. Um grupo G diz-se solúvel se contém uma cadeia de subgrupos:

$$1 = G_0 \leq G_1 \leq ... \leq G_n = G$$

tal que $G_{i+1} \rhd G_i$ e G_{i+1}/G_i é abeliano para $1 \leq i \leq n$.

Definição 1.2.11. Podemos definir a *série derivada* de G indutivamente como segue:

$$\begin{aligned} G^{(0)} &= G; \\ G^{(1)} &= [G, G] = G'; \\ &\vdots \\ G^{(i)} &= [G^{(i-1)}, G^{(i-1)}]. \end{aligned}$$

Lema 1.2.12. *G* é solúvel se, e somente se, existe $m \geq 0$ tal que $G^{(m)} = 1$.

Definição 1.2.13. Indicamos por $dl(G)$ o comprimento derivado de *G*, ou seja, o menor *m* tal que a série derivada é 1.

Definição 1.2.14. Seja *G* um grupo, definimos a série δ como:

$$\begin{aligned} \delta_1(x_1) &= x_1; \\ \delta_2(x_1,x_2) &= [x_1,x_2]; \\ &\vdots \\ \delta_{n+1}(x_1,\cdots,x_{2^{n+1}}) &= [\delta_n(x_1,\cdots,x_{2^n}),\delta_n(x_{2^n+1},\cdots,x_{2^{n+1}})]. \end{aligned}$$

Teorema 1.2.15. Seja *G* um grupo solúvel então:

1. Se $H \leq G$, então *H* é solúvel;
2. Se $N \lhd G$ então G/N é solúvel.

Teorema 1.2.16. Sejam $N \lhd G$ e se ambos *N* e G/N são solúveis. Então *G* é solúvel.

Teorema 1.2.17. Se *G* é nilpotente então *G* é solúvel.

Teorema 1.2.18. *(Burnside-1904)* Seja *G* um grupo finito e *p* e *q* números primos. Se $|G| = p^a q^b$ então *G* é solúvel.

Teorema 1.2.19. *(Feit-Thompson-1963)* [8] Se $|G|$ é ímpar então *G* é solúvel.

1.2.1 Grupos e Automorfismos

Sejam *G* um grupo e *H* um subconjunto de $Aut(G)$. Dizemos que um subconjunto *X* de *G* é *H*-invariante se tivermos $X^h \subseteq X$, para todo $h \in H$, onde X^h é a imagem do subconjunto *X* pelo automorfismo *h*.

Teorema 1.2.20. [9, Teorema 10.1.4] Se ρ é um automorfismo livre de pontos fixos de *G*, tal que $|\rho| = 2$, então *G* é abeliano e $x^\rho = x^{-1}$ para todo $x \in G$.

Proposição 1.2.21. [9, Teorema 2.1.1] Seja *A* um subgrupo de $Aut(G)$ e seja *H* um subgrupo *A*-invariante de *G*. Então:

1. $N_G(H)$ e $C_G(H)$ são *A*-invariante;
2. Para cada $\phi \in A$, a restrição $\phi|_H$ de ϕ a *H* é um automorfismo de *H* e a aplicação $\phi \mapsto \phi|_H$ é um homomorfismo de *A* em $Aut(H)$;

3. Se N é normal em G e $\phi \in A$ a aplicação $\phi* : {}^{G}\!/_{N} \mapsto {}^{G}\!/_{N}$ definida por $(Hx)\phi* = H(x\phi)$ para todo $x \in G$ é um automorfismo e a aplicação $\phi \mapsto \phi*$ é um homomorfismo de A em $Aut({}^{G}\!/_{N})$.

Teorema 1.2.22. [9, Teorema 6.2.2] Seja A um π'-subgrupo dos automorfismos de um π-grupo G e suponha que G ou A são solúveis. Então para cada primo $p \in \pi$, temos:

1. A deixa invariante algum p-Sylow de G;
2. Dois p-Sylow A-invariante de G são conjugados por um elemento do $C_G(A)$;
3. Qualquer p-subgrupo A-invariante de G está contido em um p-sylow A-invariante de G:
4. Se H é qualquer subgrupo normal A-invariante de G então $C_{{}^{G}\!/_{H}}(A)$ é a imagem do $C_G(A)$ em ${}^{G}\!/_{H}$.

Lema 1.2.23. [9, Lema 10.5.1] Seja A um 4-grupo de automorfismo livre de pontos fixos de G, seja ϕ_i uma involução de A e o conjunto $G_i = C_G(\phi_i)$, $1 \leq i \leq 3$. Então as seguintes condições são verdadeiras:

1. G_i é abeliano, $1 \leq i \leq 3$;
2. $G = \langle G_1, G_2, G_3 \rangle$ e se G tem ordem potência de um primo então $G = G_1G_2G_3$;
3. Se P_i é o S_p-subgrupo de G_i então $P = P_1P_2P_3$ é o único S_p-subgrupo A-invariante de G;
4. Se H_i é um subgrupo de G_i então $H_i \subseteq Z(N_G(H_i))$;
5. Se um S_p-subgrupo de G_i é um S_p-subgrupo de G então G tem um p-complemento normal;
6. Se H é um subgrupo A-invariante de G então A induz um grupo de automorfismos livre de ponto fixo de ${}^{G}\!/_{H}$.

Teorema 1.2.24. [9, Teorema 5.3.16] Seja P um p-grupo abeliano elementar e seja Q um q-grupo abeliano não cíclico do $Aut(P)$ com $p \neq q$. Então

$$P = \prod_{x \in Q \setminus \{1\}} C_P(x)$$

Em particular, P é gerado pelos subgrupos $C_P(x)$ com $x \in Q \setminus \{1\}$.

1.3 Grupos Powerful

Essa seção tratará de uma família importante de p-grupos, grupos nos quais a ordem é uma potência de primo, os p-grupos finitos *powerful*, baseado nos livros *The Structure of Groups of Prime Power Order* [18] e *P-Automorphisms of Finite P-Groups* [13]. Um fato importante que também veremos nesta seção é como encontrar um subgrupo *powerful* de posto limitado contido em um p-grupo de posto finito. No estudo sobre p-grupos encontramos algumas famílias como as de p-grupos regulares cujo seus subgrupos são ainda regulares, porém isso não ocorre em p-grupos *powerful*, no final da seção daremos o exemplo.

Definição 1.3.1. Seja G um p-grupo finito. Dizemos que G é *powerful* se $G' = [G,G] \leq G^p$, se p é ímpar, ou se $G' \leq G^4$, se $p = 2$.

Quando p é ímpar, G será *powerful* se, e somente se, $\Phi(G) = G^p$, lembre que em geral em um p-grupo finito vale $\Phi(G) = G^p G'$.

Definição 1.3.2. Um subgrupo N de um p-grupo finito G é dito *powerful embedded* em G, onde denotamos por $Np.e.G$, se $[N,G] \leq N^p$, se p é ímpar, ou $[N,G] \leq N^4$, se $p = 2$.

Lema 1.3.3. Se $N \trianglelefteq G$ tal que $[N,G] \leq N^p[N,G,G]$ então N *p.e.* G.

Demonstração. Tome o comutador $[N,G]$ como o subgrupo de G, obtemos que $[N,G,G] \leq [N^p,G][N,G,G,G]$ de modo que $[N,G] \leq N^p[N,G,G,G]$ e assim por diante. Como resultado, $[N,G] \leq N^p[N,\underbrace{G,\cdots,G}_{\text{c-fatores}}]$para todo $c \in \mathbb{N}$, como G é nilpotente $[N,\underbrace{G,\cdots,G}_{\text{c-fatores}}] = 1$, então $[N,G] \leq N^p$. □

Teorema 1.3.4. Se M e N são subgrupos normais de G tal que $[M,N,G,G] = 1$, então $[M^p,N] \leq [M,N]^p$.

Demonstração. Aplicando a formula $[ab,c] = [a,c]^b[b,c]$ várias vezes, nos obtemos, para quaisquer $m \in M$ e $n \in N$.

$$\begin{aligned}[m^p,n] &= [m^{p-1},n]^m[m,n] = ([m^{p-2},n]^m[m,n])^m[m,n]\cdots \\ &= (\cdots(([m,n]^m[m,n])^m[m,n])^m\cdots)^m[m,n].\end{aligned}$$

Como $a^b = a[a,b]$ e $[a,b,m,n] = 1$ para $a,b \in G$, $m \in M$ e $n \in N$. De maneira geral

$$[m,n]^p = [m,n,m]^{\frac{p(p-1)}{2}} \in [M,N]^p$$

Logo $[m^p,n] \in [M,N]^p = 1$, logo $m^p \in C_G(N)$. Como $[M^p,N]$ e o $C_G(N)$ são subgrupos então $[M^p,N] = 1$ □

Teorema 1.3.5. Se M,N *p.e.* G então:

1. $[M,N]$ *p.e.* G;
2. M^p *p.e.* G;
3. MN *p.e.* G.

Demonstração.

1. Pelo 1.3.3 assumimos que $[M,N,G,G] = 1$. O lema dos três subgrupos garante $[M,N,G] \leq [M,G,N][M,[N,G]]$, como por hipótese M e N são *powerful embedded* obtemos $[M,N,G] \leq [M^p,N][M,N^p]$, mas pelo 1.3.4 $[M^p,N] \leq [M,N]^p$, assim $[M,N,G] \leq [M,N]^p$.
2. Assuma que $[M^p,G,G] = 1$, pois $[\underbrace{M,\cdots,M}_{\text{p-fatores}},G,G] = 1$, devemos mostrar $[M^p,G] \leq (M^p)^p$. Mas, por hipótese M *p.e.* G, ou seja, $[M,G] \leq M^p$ e $[M^p,G] \leq [M,G]^p \leq (M^p)^p$. Logo, M^p*p.e.*G.
3. Como M,N e G são subgrupos normais de G, temos que:

$$[MN,G] \leq [M,G][N,G] \leq M^pN^p \leq (MN)^p.$$

□

Corolário 1.3.6. Se G é *powerful*, então:

1. $[G,G]$ é *p.e.* G;
2. G^p é *p.e.* G;
3. $\Phi(G)$ é *p.e.* G;
4. $G^{(k)}$ é *p.e.* G;
5. $\gamma_k(G)$ é *p.e.* G.

Demonstração.

1. Como G é um p-grupo *powerful* então G *p.e.* G, logo pelo $1.3.5(1.)$ temos que $[[G,G],G] \leq [G,G,G]^p$.
2. Como G*p.e.*G então pelo teorema $1.3.5(2.)$, G^p*p.e.*G.

3. Sabemos que em um p-grupo finito G, o $\Phi(G) = G'G^p$, logo pelos itens anteriores:

$$\begin{aligned}[\Phi(G), G] =& [G'G^p, G] \leq [G', G][G^p, G] \leq \\ & [G', G]^p [G^p, G]^p \leq ([G', G][G^p, G])^p \leq \\ & [G'G^p, G]^p = [\Phi(G), G]^p\end{aligned}$$

4. Faremos por indução, para $k = 1$ temos $G^{(1)} = [G, G]$ como G é *powerful* então $[G, G] \leq G^p$. Suponha que vale para $k = n-1$, ou seja, $[G^{(n-1)}, G] \leq (G^{(n-1)})^p$. Provaremos que vale $k = n$, logo:

$$\begin{aligned}[G^{(k)}, G] =& [[G^{(n-1)}, G^{(n-1)}], G] \leq [[G^{(n-1)}, G], G^{(n-1)}][G^{(n-1)}, [G, G^{(n-1)}]] \leq \\ & [(G^{(n-1)})^p, G^{(n-1)}][G^{(n-1)}, (G^{(n-1)})^p] \leq \\ & [G^{(n-1)}, G^{(n-1)}]^p [G^{(n-1)}, G^{(n-1)}]^p = (G^{(n)})^p\end{aligned}$$

5. Por indução para $k = 1$ temos $[\gamma_1(G), G] = [G, G, G] \leq [\gamma_1(G), G]^p$, pois por definição $\gamma_n = [\gamma_{n-1}(G), G]$. Suponha que vale para $k = n-1$, ou seja, $[\gamma_{n-1}(G), G] \leq (\gamma_{n-1})^p$, logo pelo item $(2.)$:

$$[\gamma_n(G), G] = [[\gamma_{n-1}(G), G], G] \leq [(\gamma_{n-1}(G))^p, G] \leq [\gamma_{n-1}(G), G]^p = (\gamma_n(G))^p$$

□

Seja G um p-grupo finito, vamos definir a seguinte sequência de Subgrupos:

$$P_1(G) = G;\ P_{i+1}(G) = P_i(G)^p [P_i(G), G],\ i \geq 1.$$

Observe que essa cadeia é decrescente de subgrupos normais em G e ainda é uma série central, já que $[P_i(G), G] \leq P_{i+1}(G)$, temos também que $P_2(G) = \Phi(G)$. Para simplificar a notação escrevemos $G_i = P_i(G)$.

Se G é um p-grupo finito *powerful* algumas propriedades sobre essa série podem ser verificadas.

Lema 1.3.7. Seja G um p-grupo *powerful*.

1. G_i *p.e.* G e $G_{i+1} = G_i^p = \Phi(G_i)$ para cada i;
2. A aplicação $x \mapsto x^p$ induz um homomorfismo de G_i/G_{i+1} sobre G_{i+1}/G_{i+2} para cada i.

Demonstração.

1. Vamos provar por indução sobre i. Para $i = 1$ temos que $G_2 = \Phi(G) = \Phi(G_1)$ e como $[G,G] \leq G^p$, para qualquer primo p, segue que $\Phi(G) = G^p$. Logo é valido o primeiro passo de indução.

   Suponha por hipótese de indução que G_i *p.e.* G e que $G_{i+1} = G_i^p = \Phi(G_i)$. Mostraremos que é válido para $i+1$. Como $G_{i+1} = G_i^p$ e G_i *p.e.* G segue pelo item (2.) do corolário 1.3.6 que G_{i+1} *p.e.* G. Pela definição da série temos que $G_{i+2} = G_{i+1}^p[G_{i+1}, G]$ e como acabamos de mostrar G_{i+1} *p.e.* G, segue $G_{i+2} \leq G_{i+1}^p$. Mas já temos que $G_{i+1}^p \leq G_{i+2}$, dessa forma $\Phi(G_{i+1}) = G_{i+1}^p$.

2. Pelo item anterior temos que G_i *p.e.* G, lembrando que $[G_i, G_i] \leq [G_i, G]$ segue que G_i é *powerful*. Observe que pela definição da série e pelo item anterior $P_2(G_i) = P_1(G_i)^p[P_1(G_i), G] = G_{i+1}$, e da mesma forma $P_3(G) = G_{i+2}$ Provaremos o caso $i = 1$ e substituindo G por G/G_3, podemos assumir $G_3 = 1$. Veja que $[G,G] \leq G_2 = \Phi(G)$ e sabemos $[G_2, G] \leq G_3$, assim $G_2 \leq Z(G)$ e então $[G,G] \leq G_2 \leq Z(G)$.

   Com isso, temos que $[[G,G],G] \leq [Z(G),G] = 1$, ou seja, $\gamma_3(G) = 1$. Lembre que dados $x, y \in G$ temos:

   $$(xy)^n \equiv x^n y^n [y,x]^{\frac{n(n-1)}{2}} (mod(\gamma_3(G)))$$

   Considere p um primo ímpar, então temos $(xy)^p = x^p y^p [y,x]^{\frac{p(p-1)}{2}}$ e , nesse caso, p divide $\dfrac{p(p-1)}{2}$. Como $[y,x] \in G_2$, temos que $([y,x]^p)^{\frac{p(p-1)}{2}} \in G_2^p = G_3 = 1$, pelo item anterior. Isso significa que $(xy)^p = x^p y^p$. Agora, se $p = 2$, como G é *powerful*, então, $[G,G] \leq G^4 \leq (G^2)^2 \leq (\Phi(G))^2 = G_2^2 = G_3 = 1$. Assim, $(xy)^2 = x^2 y^2 [y,x] = x^2 y^2$, já que $[y,x] \in [G,G] \leq G_3 = 1$. Dessa forma, em qualquer caso temos $(xy)^p = x^p y^p$. Como $G_2^p = G_3 = 1$ e $G^p = G_2$, temos que $x \mapsto x^p$ induz um homomorfismo sobrejetivo de G/G_2 sobre G_2/G_3. A validade para $i = 1$, os demais raciocínio já que G_i é *powerful*, para todo i.

□

Lema 1.3.8. Se $G = \langle a_1, \cdots, a_d \rangle$ é um p-grupo *powerful*, então $G^p = \langle a_1^p, \cdots, a_d^p \rangle$.

Demonstração. Considere o homomorfismo sobrejetivo $\theta : G/G_2 \longrightarrow G_2/G_3$ do lema anterior. Por hipótese G é gerado por $\{a_1, \cdots, a_d\}$, então G/G_2 é gerado pelo conjunto $\{a_1 G_2, \cdots, a_d G_2\}$. Pelo homomorfismo sobrejetivo G_2/G_3 será gerado por $\{\theta(a_1 G_2), \cdots, \theta(a_d G_2)\}$, sendo esse homomorfismo $x \longmapsto x^p$, teremos que $G_2 = \langle a_1^p G_2^p, \cdots, a_d^p G_2^p \rangle G_3 = \langle a_1^p, \cdots, a_d^p \rangle G_3$, pois $G_3 = G_2^p$. Agora temos que $G_2 = G^p$ e $G_3 = \Phi(G_2)$. Como o subgrupo de *Frattini* é composto pelos elementos não-geradores do grupo, temos que $G^p = \langle a_1^p, \cdots, a_d^p \rangle$. □

Denotemos por $d(G)$ a quantidade mínima de geradores para o grupo G.

Definição 1.3.9. O posto de um grupo G é definido por:

$$rk(G) = sup\{d(H)|H \leq G\}.$$

Uma característica interessantes dos p-grupos de posto finito G é a existência de um subgrupo característico *powerful* de índice limitado em função do posto $rk(G)$. Os próximos resultados serão sobre analisar propriedades do grupo G no grupos das matrizes em especial as matrizes $GL_r(\mathbb{F}_p)$.

Definição 1.3.10. Sejam G um p-grupo finito e r um inteiro positivo. Definimos $V(G,r)$ como sendo a interseção dos núcleos de todos os homomorfismos de G em $GL_r(\mathbb{F}_p)$.

A imagem de qualquer homomorfismo de um p-grupo G aplicado em $GL_r(\mathbb{F}_p)$ é um p-subgrupo de $GL_r(\mathbb{F}_p)$ é conjugado a um subgrupo do grupo inferior uni-triangular $U_r(\mathbb{F}_p)$, esse grupo é formado pelas matrizes A_{ij} que satisfazem $a_{ij} = 0$, se $j > 1$, $a_{ij} = 1$, se $i = j$, e se $i > j$, a_{ij} pode ser qualquer elemento de $\mathbb{F}_p$, ou seja ,matrizes de tamanho r e entradas em $\mathbb{F}_p$ satisfazendo as propriedades descritas. Dessa forma definiremos igualmente $V(G,r)$ sendo a interseção dos núcleos de todos os homomorfismos de G em $U_r(\mathbb{F}_p)$. Observe que um elemento g de G pertence a $V(G,r)$ se, e somente se, g age trivialmente em qualquer representação linear de G sobre qualquer $\mathbb{F}_p$-espaço vetorial de dimensão no máximo r. Para $r \in \mathcal{N}$ defina $\lambda(r)$ por

$$2^{\lambda(r)} \leq r < 2^{\lambda(r)-1}$$

Lema 1.3.11.

1. O grupo $U_r(\mathbb{F}_p)$ tem uma série, de comprimento $\lambda(r)$, de subgrupos normais, com quocientes abelianos elementares.
2. Se G é um p-grupo finito, então $G/V(G,r)$ tem uma série com essas propriedades.

Demonstração.

1. A demonstração seguirá por indução sobre r. Para $r = 1$, temos que $\lambda(1) = 1$ e $U_r(\mathbb{F}_p) = (\mathbb{F}_p)$, assim o resultado é válido já que $(\mathbb{F}_p)$ é um p-grupo abeliano elementar. Suponha por hipótese de indução que o resultado seja válido para qualquer $l < r$. Considere $l = \left(\lfloor \frac{r}{2} \rfloor\right)$ e observe que dado $X \in U_r(\mathbb{F}_p)$ podemos reescrevê-lo da seguinte forma

$$X = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

, Com $A \in U_l(\mathbb{F}_p)$ e $C \in U_{r-l}(\mathbb{F}_p)$. Defina a aplicação, que é um homomorfismo, da seguinte forma

$$\begin{aligned} \varphi : U_r(\mathbb{F}_p) &\to U_l(\mathbb{F}_p) \times U_{r-l}(\mathbb{F}_p) \\ X &\to (A,C) \end{aligned}$$

Considerando $K = Ker(\varphi)$ pela definição temos que $K = \{X \in U_r(\mathbb{F}_p) | \varphi(X) = (A,C) = (Id_l, Id_{r-l})\}$, ou seja, os elementos de K são da forma

$$X = \begin{pmatrix} Id_l & 0 \\ B & Id_{r-l} \end{pmatrix}$$

Com isso, temos que K é um p-grupo abeliano elementar. Pelo primeiro teorema do Isomorfismo $U_r(\mathbb{F}_p)/K \cong Im(\varphi) \leq U_l(\mathbb{F}_p) \times U_{r-l}(\mathbb{F}_p)$.

Agora, pela hipótese de indução $U_l(\mathbb{F}_p)$ e $U_{r-l}(\mathbb{F}_p)$ possuem tais séries, então $Im(\varphi)$ também possui tal série. Pelo isomorfismo temos que $U_r(\mathbb{F}_p)/K$ possuem uma série tal que seus quocientes são p-grupos abelianos elementares. Vimos que K é um p-grupo abeliano elementar, dessa forma temos que $U_r(\mathbb{F}_p)$ possui uma série com essas propriedades.

2. Seja G um p-grupo finito e por definição $V(G,r)$ é a interseção dos núcleos de todos os homomorfismos de G em $U_r(\mathbb{F}_p)$. Mas, sendo G finito, temos que essa intercessão é constituída por uma quantidade de núcleos, ou seja, $V(G,r) = \cap_{i=1}^{k} N_i$, sendo $N_i = ker\varphi_i$ com $\varphi_i : G \to U_r(\mathbb{F}_p)$. E pelo Primeiro Teorema do Isomorfismo $G/N_i \cong Im(\varphi_i(G)) = H_i \leq U_r(\mathbb{F}_p)$. Agora considere o homomorfismo

$$\begin{aligned} \psi : G &\to G/N_1 \times G/N_2 \times \cdots \times G/N_k \\ g &\to (gN_1, \cdots, gN_k) \end{aligned}$$

Observe que $Ker(\psi) = \{g \in G | (gN_1, \cdots, gN_k) = (\overline{1}, \cdots, \overline{1})\} = \cap_{i=1}^{k} N_i = V(G,r)$. E, novamente pelo Primeiro Teorema do Isomorfismo temos que $G/V(G,r) \cong H_1 \times \cdots \times H_k \leq U_r(\mathbb{F}_p) \times \cdots \times U_r(\mathbb{F}_p)$. Pelo item anterior temos que cada $U_r(\mathbb{F}_p)$ possui uma série de comprimento $\lambda(r)$ com cada quociente abeliano elementar, então, pelo isomorfismo, $G/V(G,r)$ também possui tal série.

□

Proposição 1.3.12. Sejam G um p-grupo finito e r un inteiro positivo. Coloque $V = V(G,r)$ e sejam $W = V$ se $p > 2$ ou $W = V^2$ se $p = 2$. Se $N \lhd G$, $d(N) \leq r$, e $N \leq W$, então N *p.e.* W.

Demonstração. Vamos mostrar por indução sobre a ordem de N. Se $|N| = 1$, o resultado é satisfeito. Suponha por hipótese de indução que o resultado seja válido para todo grupo de ordem do que $|N|$ e vejamos ser válido para a ordem de N. Primeiro vamos supor $p > 2$ e nesse caso $V = W$. Suponha por absurdo que $[N,V] \nleq N^p$, podemos assumir que $N^p = 1$ e $|[N,V]| = p$. Como G é um p-grupo, então existe $N \lhd G$ tal que $[N,V] \leq M < N$ e $|N : M| = p$ Sendo $N/[N,V]$ é p-grupo abeliano elementar, segue que $d\left(M/[N,V]\right) = \left|N/[N,V]\right| - 1 \leq r-1$, já que $|N : M| = p$ e $d(N) \leq r$. Também pelo fato de $[N,V]$ ter ordem p, temos que ele é cíclico, ou seja, possue aenas um gerador e isso acarreta que $d(M) \leq r$. Observe ainda que $M < N \leq V$, ou seja, $M < V$. Com isso, pela hipótese de indução aplicada a M, M *p.e.* V, ou seja, $[M,V] \leq M^p = 1$. Assim $[M,N] \leq [M,V] = 1$ e isso significa que os elementos de M comutam com os de N, ou seja, $M \leq Z(N) \leq N$. Mas sendo N/M um grupo cíclico e $M \leq Z(N)$, temos que N é abeliano e assim é um $\mathbb{F}_p$-espaço vetorial de dimensão no máximo r. Agora, observamos que $g \in V(G,r)$ se, e somente se, g age trivialmente em toda representação linear de G sobre qualquer $\mathbb{F}_p$-espaço vetorial de dimensão no máximo r. Em particular, age trivialmente em N. Então $[N,V] = 1$, um absurdo já que $|[N,V]| = p$. Portanto, nesse caso, N *p.e.* $V = W$.

Considere $p = 2$ e, assim, $W = V^2$. Suponha por absurdo que N não é *powerful embedded* em W. Da mesma forma, podemos assumir que $N^4 = 1$ e $|[N,W]| = 2$. Considerando $x,y \in N$, como $N \leq W$ então $(xy)^2 \equiv x^2y^2 mod([N,W])$. Segue que $(N^2)^2 = 1$, pois elevamos ao quadrado novamente e obtemos N^4 e $[N,W]^2$, mas ambos são triviais. Ocorre que $[x^2,y] = [x,y]^2[[x,y],y]$. Mas $[[x,y],y] = 1$, pois $[[N,W],N] < N$ e assim $|[[N,W],N]| = 1$. Então $[x^2,y] = [x,y]^2 \in [N,N]^2 \leq [N,W] = 1$. Como $[x^2,y] \in [N^2,N]$ segue que $[N^2,N] = 1$, ou seja, $N^2 \leq Z(N)$.

Agora, observe que N/N^2 é abeliano pois todo elemento possui ordem 2, ou seja, N/N^2 é um $\mathbb{F}_p$-espaço vetorial de dimensão no máximo r. Assim $dim(N/N^2) = dim(N/\Phi(N)) \leq r$, pela hipótese. Isso, acarreta que $[N,V] \leq N^2$.

Consequentemente, para $a \in N$ e $v \in N$, escrevemos $[a,v] = b$, para algum $b \in N^2$ e assim temos $a^v = ab$ Mas, $(a^v)^2 = (ab)^2 = a^2b^2[b,a]$. Temos que $b^2 = 1$, pois $b \in N^2$ e $(N^2)^2 = 1$ e também $[b,a] = 1$, pois $N^2 \leq Z(N)$ e assim $[N^2,N] = 1$. Isso acarreta que $[N^2,V] = 1$.

Dessa forma, observe que $[[N,V],V] \leq [N^2,V] = 1$. Assim pela Fórmula de Compilação de Hall temos $[N,W] = [N,V^2] \leq [N,V]^2[[N,V],V] \leq (N^2)^2[[N,V],V]$, pelo que foi mostrado acima. Então $[N,W] = 1$, o que é um absurdo, já que supomos $|[N,W]| = |[N,V^2]| = 2$. Portanto, N *p.e.* $W = V^2$. □

Teorema 1.3.13. Seja G um p-grupo finito de posto r. Então G possui um subgrupo *powerful* característico de índice no máximo $p^{r\lambda(r)}$, se p é ímpar ou $2^{r+r\lambda(r)}$ se $p=2$.

Demonstração. Considere $V = V(G,r)$. Pelo Lema 1.3.11, $G/V(G,r)$ possui uma série de subgrupos normais com comprimento no máximo $\lambda(r)$, nos quais os quocientes são abelianos elementares. Agora G tem uma série $V \leq N_1 \leq \cdots \leq N_l = G$, com $l \leq \lambda(r)$ e N_i/N_{i+1} é um p-grupo abeliano elementar. Por hipótese G tem posto r, então cada um desses fatores tem ordem no máximo p^r, pois $d(N_i) \leq d(G) = r$. Com isso $|G:V| \leq p^{r\lambda(r)}$.

Para o caso $p > 2$, pela definição de V temos que ele é característico em G, logo $V \lhd G$. Pela hipótese, G tem posto r, temos $d(V) \leq r$. Pela Proposição 1.3.12 temos que V *p.e.* V, logo V é *powerful*. Portanto, se $p > 2$, V é um subgrupo característico *powerful* de índice no máximo $p^{r\lambda(r)}$.

Para $p = 2$, observe que V^2 é característico em V, de fato, por definição $V^2 = \langle v^2 | v \in V \rangle$ e dado ϕ um automorfismo de V temos que $\phi(v^2) = (\phi(v))^2$ e este é um gerador em V^2, pois $\phi(v) \in V$. Assim V^2 é característico em V e V é característico em G, logo V^2 é característico em G e portanto $V^2 \lhd G$. Também temos que $d(V^2) \leq r$ e novamente pela Proposição 1.3.12 temos que V^2 *p.e.* V^2, ou seja, V^2 é *powerful*.

Assim temos que $|G:V^2| = |G:V||V^2:V| \leq 2^{r\lambda(r)}2^r$. Portanto, nesse caso, o subgrupo característico *powerful* de índice no máximo $2^{r+r\lambda(r)}$ de G que existe é V^2. □

Como mencionado no início dessa seção apresentaremos um exemplo de um p-grupo *powerful* que possue um subgrupo que não é *powerful*. O D_8(Diedral de ordem 8) não é *powerful*, pois $D_8' = \langle r^2 \rangle$ e $D_8^4 = e$, assim claramente $D_8' \not\leq D_8^4$. A ideia é construir um grupo que irá conter uma cópia isomorfa do D_8 como subgrupo próprio. Seja $G = D_8 \times C_8$, com C_8 sendo o cíclico de ordem 8 gerado por z e $D_8 = \langle r,s | r^4 = s^2 = e, r^s = r^{-1} \rangle$, considere o seguinte subgrupo normal em G, $N = \langle r^2 z^4 \rangle$. Agora considere o grupo quociente $K = D_8 \times C_8/N$, temos que:

$$[K,K] = [(D_8 \times C_8)/N, (D_8 \times C_8)/N] = [G,G]N/N = \langle r^2 N \rangle = \langle s^4 N \rangle \leq K^4.$$

Assim K é *powerful*, mas observe que $H = \langle rN, sN \rangle$ é uma cópia isomorfa a D_8, com o isomorfismo $\sigma : D_8 \to H$, dado por $r \to rN$ e $s \to sN$, como D_8 não é *powerful* segue que H não é *powerful*.

1.4 Módulos

Definição 1.4.1. Seja R um anel (não necessariamente comutativo e com unidade). Um grupo abeliano (aditivo) M é dito um *R-Módulo* (à esquerda ou a direita) se R age linearmente

em M, ou seja, se existe uma aplicação

$$\begin{aligned} R \times M &\longrightarrow M \\ (r,m) &\longrightarrow rm \end{aligned}$$

Satisfazendo as seguintes propriedades, $\forall m, m_1$ e $m_2 \in M$,$\forall r, r_1, r_2$ e $s \in R$, temos:

1. $1_R m = m$;
2. $(r_1 + r_2)m = r_1 m + r_2 m$;
3. $r(m_1 + m_2) = rm_1 + rm_2$;
4. $(rs)m = r(sm)$

As propriedades descritas acima podem ser vistas como homomorfismo de grupos e aneis. O item 3 diz que para todo r em R, f_r é um homomorfismo de grupos. De fato;

$$\begin{aligned} f_r : M &\longrightarrow M \\ m &\longrightarrow rm \end{aligned}$$

Os itens $1, 2$ e 4 dizem que $f : R \longrightarrow End(M)$ é um homomorfismo de aneis, ou seja:

$$\begin{aligned} r \longrightarrow f_r : M &\longrightarrow M \\ m &\longrightarrow rm \end{aligned}$$

Definição 1.4.2. Seja M um *R-módulo*. Um *R-submódulo* de M é um $H \subseteq M$ tal que H é fechado com respeito a todas operações de M, isto é:

1. $(H, +)$ é subgrupo de M;
2. $rh \in H$, para todo $r \in R$ e $h \in H$.

Para dar uma breve noção sobre *R-Módulo* daremos exemplos de estruturas que são *R-Módulo*.

Exemplo 1.4.3. Considere $(A, +)$ um grupo abeliano, este é sempre um $\mathbb{Z}$-Módulo. De fato basta considerar

$$\begin{aligned} \mathbb{Z} \times A &\longrightarrow A \\ (n,a) &\longrightarrow na = \underbrace{a + a \cdots + a}_{\text{n-fatores}} \quad (n > 0) \end{aligned}$$

Observe que os itens da definição de módulo são todos satisfeitos.

Exemplo 1.4.4. Seja I um ideal à esquerda de A, então I é um *A-Módulo*, bastando definir a operação:

$$\begin{aligned} A \times I &\longrightarrow I \\ (x,i) &\longrightarrow xi \end{aligned}$$

Definição 1.4.5. Seja $S \subset M$, o R-submódulo gerado por S é definido:

$$\begin{aligned} {}_+\langle S\rangle &= \langle \textit{todas as R-combinações lineares de elementos de } S\rangle \\ &= \{\lambda_1 S_{i1} + \cdots + \lambda_t S_{it} \mid t \geq 1, S_{ij} \in S, \lambda_j \in R\} \end{aligned}$$

Definição 1.4.6. Sejam M e N *R-Módulos*. Uma função $f : M \longrightarrow N$ é um homomorfismo de módulos (ou R-homomorfismo) se para todo m e $n \in M$ e todo $r \in R$ se verifica:

1. f é um homomorfismo de grupos, ou seja, $f(m_1 + m_2) = f(m_1) + f(m_2)$;
2. f é compatível com a ação de R em M e N, ou seja, $f(rm) = rf(m)$ para todo $r \in R$ e $m \in M$.

Capítulo 2

Grupos de Frobenius

O estudo de Grupos de *Frobenius* motivou vários avanços na Teoria de Grupos finitos, tais como a Teoria de Caracter e o clássico Teorema de *Thompson* sobre grupos com automorfismo livre de pontos fixos.

O objetivo deste capítulo, além de mostrar propriedades básicas de grupos de *Frobenius* e grupos 2-*Frobenius* é demonstrar alguns resultados sobre grupo de *Frobenius* agindo como Automorfismo.

2.1 Grupos de Frobenius

Definição 2.1.1. Dado um grupo G, dizemos que um subgrupo H é disjunto de seus conjugados se $H^x \cap H = 1$ ou $H^x \cap H = H$ para todo $x \in G$ H é dito complemento de G.

Definição 2.1.2. Grupo de *Frobenius* Seja H um subgrupo não-trivial de um grupo finito G. Dizemos que G é um grupo de *Frobenius* com complemento H se H é disjunto de seus conjugados e é seu próprio normalizador em G.

Um grupo de *Frobenius* também pode ser visto como um grupo de permutações transitivo sobre um conjunto finito tal que nenhum elemento não trivial fixa mais que um ponto e algum elemento não trivial fixa um ponto. Nesse contexto H é o subgrupo que fixa um ponto e F é o subgrupo que contém a identidade e elementos que não fixa nenhuma ponto, chamamos F do núcleo de G. Caracterizaremos um grupo de *Frobenius* através da estrutura de seu complemento, um subgrupo H. Este resultado pode ser encontrado [9, Teorema 2.7.5].

Teorema 2.1.3. Sejam F um grupo finito e H um subgrupo de $Aut(F)$. Suponha que para todo elemento não-trivial de $h \in H$ temos $C_F(h) = 1$. Então o produto semidireto $G = F \rtimes H$ é um grupo de *Frobenius* com núcleo F e complemento H.

Demonstração. Pela definição 2.1.2 mostraremos que H é seu próprio normalizador e é disjunto de seus conjugados. Primeiro mostraremos que H é seu próprio normalizador. Assim, dado $x \in G$ temos que $H^x = H^f$ para algum $f \in F$, pois $G = FH$. Suponha que $H^f = H$ para algum $f \in F$. Então $[f,h] \in H$ para todo $h \in H$. Por outro lado, como F é normal em G, temos $[f,h] \in F$. Assim, $[f,h] = 1$, pois $H \cap F = 1$. Mas isso significa que $f^h = f$, para todo H, ou seja, $f \in C_F(H) = 1$.

Precisamos mostrar que $H \cap H^f = 1$ ou $H \cap H^f = H$ para todo $f \in F$. Suponha que $H \cap H^f \neq 1$ e fixe $h \in H \cap H^f$. Então $[f,h] \in H \cap F = 1$ Portanto, $f \in C_H(f) = 1$ e temos $H \cap H^f = H$. □

A estrutura do grupo de *Frobenius* é definida pela seguinte proposição.

Teorema 2.1.4. Seja G um grupo de *Frobenius* com núcleo F e complemento H, então:

1. H induz um grupo regular de automorfismo de F;
2. $|H|$ divide $|F| - 1$;
3. F é nilpotente e abeliano se $|H|$ é par;
4. Os S_p-subgrupos de H são cíclicos para p ímpar e são cíclicos ou quatérnios generalizados para $p = 2$;
5. Qualquer subgrupo de H de ordem pq, com p e q primos são cíclicos;
6. Se $|H|$ é ímpar então H é metacíclico, enquanto se $|H|$ é par, H possui uma involução única que necessariamente está contida em $Z(H)$.

Demonstração encontrada em [9]. Um grupo G é dito grupo de Frobenius, se G pode ser escrito como o produto semidireto dos subgrupos F e H com os mesmos sendo núcleo e complemento, respectivamente, tais que $C_F(h) = 1$ para todo $h \in H \setminus \{1\}$.

2.2 Grupos 2-Frobenius.

Essa seção é destinada a conhecer conceitos básicos sobre grupos finitos chamados de 2-*Frobenius*.

Definição 2.2.1. Um grupo G é chamado 2-*Frobenius* se possui um subgrupo normal H que é subgrupo de *Frobenius* com núcleo A tal que G/A é de *Frobenius* com núcleo H/A.

O próximo resultado tem como objetivo caracterizar os grupos $2-$*Frobenius* através do produto semi-direto.

Lema 2.2.2. Se G é um grupo 2-*Frobenius*, então $G = ABC$, com A e AB subgrupos normais de G e AB e BC grupos de *Frobenius* com núcleos A e B, respectivamente. E ainda, B e C são grupos cíclicos e a ordem de B é ímpar.

Demonstração. Como G é um $2-Frobenius$ então pela defição, G possui um subgrupo normal H que é um grupo de *Frobenius* com núcleo A. Então $(|H|, |H:A|) = 1$, pelo teorema de *Schur-Zassenhaus* H contém um complemento B para A e esses são conjugados. Portanto, $G = AN_G(B)$. Como A e B são conjugados, o $N_A(B) = 1$, temos $N_G(A) \cap A = N_A(A) = 1$ e

$$G/A = AN_G(B)/A \cong N_G(B)/N_G(B) \cap A \cong N_G(B) \tag{2.1}$$

Assim, $N_G(B)$ é um grupo de *Frobenius* com núcleo B, pois

$$H/A \cong BA/A \cong B/A \cap B \cong B \tag{2.2}$$

Mais uma vez $(|B|, |N_G(B):B|) = 1$, então novamente pelo Teorema de *Schur-Zassenhaus* temos $N_G(B)$ contém um complemento C para B, ou seja, $N_G(B) = BC$ é um grupo de *Frobenius* por 2.1. Como B é o núcleo e complemento de dois grupos de *Frobenius* diferentes pelo item (6) da Teorema 2.1.4 temos que $|B|$ é ímpar. Pelas afirmações (2) e (4) da Teorema 2.1.4 temos que B é cíclico como C induz um grupo regular de automorfismo por (1) da mesma Teorema, como o grupo de automorfismo de um grupo cíclico é abeliano, pela item (4) da Teorema 2.1.4, C é cíclico. □

2.3 Grupos de *Frobenius* agindo como Automorfismo

Diferente da seção anterior, nessa seção G é um grupo finito qualquer, tal que $Aut(G)$ contém um grupo de *Frobenius*.

Lema 2.3.1. Suponha que um grupo finito G admita um grupo de automorfismo F nilpotente tal que $C_G(F) = 1$. Então G é solúvel.

Demonstração. A demonstração é feita pela classificação simples dos grupos finitos e pode ser encontrada em [1]. □

Definição 2.3.2. Um subgrupo H de um grupo finito G é chamado de subgrupo *Carter* se é nilpotente e autonormalizante, ou seja, $N_G(H) = H$.

Teorema 2.3.3. Seja G um grupo finito admitindo um grupo de automorfismo F nilpotente tal que $C_G(F) = 1$. Se N é um subgrupo normal F-invariante de G, então $C_{G/N}(F) = 1$.

Demonstração. F é um subgrupo de *Carter* de GF, pois F é nilpotente por hipótese. Para o autonormalizante, sabemos pelas propriedades de normalizador $F \subseteq N_{GF}(F)$. Por outro lado, seja $x \in N_{GF}(F)$, ou seja, $x \in GF$, tal que $[x,F] \subseteq F$. Logo

$$\begin{aligned} x^{-1}f_1^{-1}xf_1 &= f \\ \underbrace{f_1^{-1}xf_1}_{\in F} f^{-1} &= x \end{aligned}$$

A última igualdade se dá pelo fato do $Aut(GF) \leq Aut(G) = F$, e $f_1^{-1}xf_1 \in Aut(GF)$.

Mostraremos que o quociente ${}^{NF}\!/_{N}$ é um subgrupo de *Carter* de ${}^{GF}\!/_{N}$. Para isso, observe que, ${}^{NF}\!/_{N} \cong {}^{F}\!/_{F\cap N}$, novamente pela hipótese F é nilpotente e pelo item 1. da proposição 1.2.6 com $F \cap N \trianglelefteq F$ segue que ${}^{NF}\!/_{N}$ é nilpotente. Por outro lado, sabemos que o normalizador é um subgrupo de ${}^{GF}\!/_{N}$ contendo ${}^{NF}\!/_{N}$. Para a outra inclusão temos que dado $x \in N_{{}^{GF}\!/_{N}}({}^{NF}\!/_{N}) = \left\{x \in {}^{GF}\!/_{N}; [x, {}^{NF}\!/_{N}] \subseteq {}^{NF}\!/_{N}\right\}$ temos que dado $y,a \in {}^{NF}\!/_{N}$:

$$\begin{aligned} x^{-1}y^{-1}xy &= a \\ x &= a^{-1}yxy^{-1} \end{aligned}$$

Assim como anteriormente teremos que $x^y \in Aut({}^{GF}\!/_{N}) \leq {}^{NF}\!/_{N}$, note que o $Aut({}^{GF}\!/_{N})$ e bem definido pelo item 3. da Proposição 1.2.21 , assim $x \in {}^{NF}\!/_{N}$, ou seja, ${}^{NF}\!/_{N}$ é um subgrupo de Carter de ${}^{GF}\!/_{N}$. Para finalizar basta supor que $C_{{}^{G}\!/_{N}}(F) \neq 1$ assim contrariamos o fato de ${}^{NF}\!/_{N}$ ser um subgrupo de Carter de ${}^{GF}\!/_{N}$. □

Teorema 2.3.4. Suponha que um grupo finito G admite um grupo de Frobenius de automorfismo FH com núcleo F e complemento H. Se N é um subgrupo normal FH-invariante de G tal que $C_N(F) = 1$, então $C_{{}^{G}\!/_{N}}(H) = {}^{C_G(H)N}\!/_{N}$.

Demonstração. Como F é o núcleo do grupo de *Frobenius* então F é nilpotente. Pelo lema 2.3.1 e pela hipótese $C_N(F) = 1$ temos que N é solúvel. A demonstração seguirá por indução em k para encontrar um elemento de $C_G(H)$ em qualquer $gN \in C_{{}^{G}\!/_{N}}(H)$, logo considere uma série maximal de subgrupos normais FH-invariantes, com fatores ${}^{N_i}\!/_{N_{i+1}}$ abelianos elementares

$$G > N = N_1 > N_2 > \cdots > N_k > N_{k+1} = 1.$$

Seja $k = 1$ então $N = N_k$ é um p-grupo algum primo p. Seja $F = F_p \times F_{p'}$, com F_p é o p-subgrupo de Sylow de F Uma vez que $C_N(F_p')$ é F_p-invariante então $C_N(F_p') = 1$, caso contrário o p-grupo F_p teria pontos fixos não-triviais no p-grupo $C_N(F_p')$. Seja $B = C_N(F_p') =$

$\{n \in N; y^n = y \ n \in F_p'\}$ e $C_B(F_p) = \{b \in B; x^b = x, x \in F_p\}$. Dado $a \in C_{C_N(F_p')}(F_p)$ mostraremos que $a \in C_N(F)$. Por definição a é um elemento de $C_N(F_p')$ que comuta com um elemento $y \in F_p$, mas por $a \in C_N(F_p')$ temos que $a \in N$ tal que a comuta com x, logo temos as seguintes igualdades

$$x^a = x \ \ e \ \ y^a = y.$$

Assim, $(xy)^a = xy$, ou seja, $a \in C_N(F)$. Obtendo a seguinte inclusão $C_{C_N(F_p')}(F_p) \subseteq C_N(F)$, como por hipótese $C_N(F) = 1$ então $C_{C_N(F_p')}(F_p) = 1$ contrariando a suposição $C_{C_N(F_p')}(F_p)$ ter pontos fixos, logo $C_N(F_p') = 1$. As hipóteses do teorema mantêm G com o grupo de frobenius de automorfismo $F_{p'}H$ satisfazendo a condição adicional $(N, F_p') = 1$, o resultado [16, Teorema 1] pode ser aplicado para produzir um ponto fixo como queríamos, ou seja, uma classe lateral gN fixada por H contém um ponto fixo de H. Para $k > 1$ considere o quociente G/N_k e o grupo de automorfismo FH. Como $N_k < N$ e $C_{N_k}(F) \subseteq C_N(F) = 1$, assim $C_{N_k}(F) = 1$, e como N_k é F-invariante pelo Teorema 2.3.3 $C_{G/N_k}(F) = 1$ então o resultado é verdade para G/N_k, uma classe gN fixada por H contém uma classe xN_k fixada por H. Pelo caso $k = 1$ como N_k é abeliano elementar, xN_k possui um elemento fixado por H. Portanto, toda classe lateral gN fixada por H contém um ponto fixo de H.

□

Para cada grupo A e um corpo k, um kA-módulo livre de dimensão n é uma soma direta de n cópias da álgebra de um grupo kA, cada uma das bases pode ser considerada como um espaço vetorial sobre k de dimensão $|A|$ com uma base $\{v_g | g \in A\}$ denominados por elementos de A em que A atua em uma representação regular $v_g h = v_{gh}$.

Considere a série maximal de subgrupos normais FH-invariante de G, essas série será usada nas demontrações dos próximos dois resultados.

$$G = G_1 > G_2 > \cdots > G_k > G_{k+1} = 1 \tag{2.3}$$

Lema 2.3.5. Seja $S = G_i/G_{i+1}$ então cada fator de 2.3 é um F_pH-módulo livre para um primo p apropriado.

Demonstração. Seja $S = G_i/G_{i+1}$ um p-grupo elementar $F = F_p \times F_{p'}$ como na prova do teorema 2.3.4, assim como na prova $C_S(F_{p'}) = 1$. Refinando S por uma série normal não-refinável de $F_{p'}H$, obtemos fatores que são irredutíveis $\mathbb{F}_pF_{p'}H$-módulo. Com a condição adicional que $p \nmid |F_{p'}|$. Podemos aplicar [16, Lema 2], nesse resultado é necessário que $(|N|, |F|) = 1$ para obter que cada um dos quocientes é um F_pH-móduo livre e, portanto, S também é um F_pH-módulo livre. □

O próximo resultado mostra uma maneira de apresentar o grupo G atráves do centralizador. Um fato tecnico e de importância é o Teorema de Clifford's, ele fala que dado uma representação irredutível de um grupo G sobre V, podemos saber como o espaço V se decompõe em relação a ação de um subgrupo H de G.

Teorema 2.3.6. Clifford [9, Teorema 3.4.1] Sejam V um G-módulo irredutível e H um subgrupo normal de G. Então V é a soma direta de espaços H-invariantes V_i, $1 \leq i \leq r$, os quais satisfazem as seguintes condições:

1. $V_i = X_{i1} \oplus X_{i2} \oplus \cdots \oplus X_{it}$, com cada $X_i j$ sendo um H-submódulo irredutível, $1 \leq i \leq r$, t é independente de i, e X_{ij},$X_{i'j'}$ são H-submódulo isomorfos se e somente se $i = i'$;

2. Para qualquer H-submódulo U de V , temos $U = U_1 \oplus \cdots \oplus U_r$, com $U_i = U \cap V_i$, $1 \leq i \leq r$. Em particular, qualquer H-submódulo irredutível de V está contido em algum dos V_i;

3. Para cada $x \in G$, a aplicação $\Pi(x) : V_i \to xV_i$, $1 \leq i \leq r$ é uma permutação do conjunto $S = V_1, V_2, \cdots, V_r$ e Π induz um representação transitiva de G sobre S por grupo de permutações. Além disso, o subgrupo $HC_G(H)$ está contido no núcleo de Π.

Teorema 2.3.7. Suponha que um grupo finito G admite um grupo de automorfismo de um grupo de Frobenius FH com núcleo F e complemento H tal que $C_G(F) = 1$. Então $G = \langle C_G(H)^f | f \in F \rangle$.

Demonstração. O grupo G é solúvel pelo lema 2.3.1. Considere a série normal não-refinada FH-invariante de G, descrita em 2.3. E suficiente provar que todo fator $S = {}^{G_i}\!/_{G_{i+1}}$ desta série é coberto $\langle C_{G_i}(H)^f | f \in F \rangle$, isto é,

$$\langle C_{G_i}(H)^f | f \in F \rangle^{G_{i+1}/G_{i+1}} = {}^{G_i}\!/_{G_{i+1}}$$

Pelo teorema 2.3.4, isto é $S = \langle C_{G_i}(H)^f | f \in F \rangle$. Então o teorema de *Clifford* pode ser aplicado para mostrar que $C_S(G) \neq 1$. Pelo lema 2.3.5, S é um $\mathbb{F}_p H$-módulo livre, ou seja, $S = \bigoplus_{h \in H} Th$ para algum $F_p H$-submódulo T Assim, $C_S(H) \neq 0$, como $\sum_{h \in H} th \neq 0 \in C_S(H)$ para todo $0 \neq t \in T$.

Como a série não é refinada, o $\mathbb{F}_p FH$-módulo S é irredutível. Portanto,

$$0 \neq \langle C_S(H)^{HF} \rangle = \langle C_S(H)^F \rangle = S$$

□

Para o próximo lema, lembremos as definições de Sistema de Sylow e Normalizador de Sistema de um grupo G.

Definição 2.3.8. (Sistema de Sylow) Seja G um grupo finito e denote $p_1, \cdots, p_k$ primos distintos divisores da $|G|$. Seja Q_i um p_i'-subgrupo de Hall de G, então $\{Q_1, \cdots, Q_k\}$ é chamado Sistema de Sylow de G.

Definição 2.3.9. (Normalizador de Sistema) Seja $\{Q_1, \cdots, Q_k\}$ um sistema de Sylow de um grupo finito solúvel G Então o subgrupo

$$N = \bigcap_{i=1}^{k} N_G(Q_i)$$

É chamado de Normalizador de Sistema de G.

Suponha que G seja um grupo e seja $K \lhd H \leq G$ e $L \leq G$. Então L *cobre* H/K se $HL = KL$, ou equivalentemente, se $H = K(H \cap L)$. Por outro lado, se $H \cap L = K \cap L$, isto é, se $H \cap L \leq K$, então L *evita* H/K.

Lema 2.3.10. (P.Hall) [23, Teorema 9.2.6] Se N é um Normalizador de Sistema de um grupo finito solúvel G então N cobre os principais fatores centrais e evita os principais fatores não-centrais de G.

Lema 2.3.11. Suponha que um grupo finito G admite um grupo de Frobenius de automorfismos FH com núcleo F e complemento H tal que $C_G(F) = 1$. Então para cada primo p dividindo $|G|$ existe um p-subgrupo de Sylow FH-invariante de G.

Demonstração. Pelas hipóteses G e F são solúveis então GF é solúvel. Pela demonstração do Teorema 2.3.3, F é um subgrupo de *Carter* de GF, ele contém um normalizador de sistema de G. Pelo lema de *P.Hall* 2.3.10, um Sistema Normalizador cobre todos os fatores centrais de qualquer série principal de GF. O fato de F ser um subgrupo de *Carter* de GF, segue que F é nilpotente e $F = N_{GF}(F)$, então F é um normalizador de sistema.

Além disso, F normaliza um único p-subgrupo de Sylow. De fato, se P e P^g para $g \in G$ são dois p-subgrupos de Sylow normalizados por F, isto é, $fPf^{-1} \subseteq P$ e $f_1 P^g f_1^{-1} \subseteq P^g$ para f e $f_1 \in F$. Então temos que $F^{g^{-1}}$ normaliza P, pois para $g \in G$ e $f \in F$:

$$P^{f^{g^{-1}}} = P^{g^{-1}fg} = g^{-1}fgPg^{-1}f^{-1}g \subseteq g^{-1}P^g g = P$$

P também é normalizado por F. Com isso F e $F^{g^{-1}}$ são subgrupos de *Carter* do $N_G(P)$, pois F é nilpotente por hipótese e dado $x \in F$, temos $x \in N_G(P)$, pois P é normalizado

por F e é claro que $F^x = F$, logo $x \in N_{N_G(P)}(F)$. Como dois subgrupos de *Carter* são conjugados $F = (F^{g^{-1}})^n$ para algum $n \in N_G(F)$, com $g^{-1}n = 1$. Tendo $N_G(F) = C_G(F) = 1$, assim $P^g = P^n = P$ Como F é normal em FH, a unicidade de P implica que também é H-invariante.

□

Capítulo 3

Anéis de Lie

Este capítulo é dedicado ao estudo de Álgebras de Lie com enfoque nas propriedades de grupos que podem ser traduzidas para a Álgebra e vice-versa. O objetivo é apresentar as demonstrações de resultados famosos como o Teorema *Higman, Kreknin e Krostrikin* e ainda apresentar a série formada pelos subgrupos D_i, chamada de série de *Jennings-Zassenhaus* e a aplicação desta a alguns resultados. Além disso, assim como no capítulo anterior, as noções e resultados aqui apresentados servirão como ferramentas para os próximos capítulos.

3.1 Anéis de Lie

A seção apresentada tratará de uma das teorias usada para resolver problemas de *grupos*.

Definição 3.1.1. Seja R um anel comutativo com unidade, uma R-Álgebra de Lie L é um R-módulo com uma nova operação binária definida em L, chamada de **colchete de Lie** .

$$\begin{aligned}[\cdot,\cdot] : & L \times L \longrightarrow L \\ & (l,m) \longrightarrow [l,m]\end{aligned}$$

satisfazendo as seguintes propriedades:

1. Lei anticomutativa:

$$[l,l] = 0$$

2. Identidade de Jacobi.
   Para m,n e $l \in L$, tem-se:

$$[[l,m],n] + [[m,n],l] + [[n,l],m] = 0$$

3. Leis distributivas.

   Para todo $r,s \in R$ e para todo l,m e $n \in L$, tem-se:

   (a) $[rl+sm,n] = r[l,n]+s[m,n]$;

   (b) $[l,rm+sn] = r[l,m]+s[l,n]$.

Observação 3.1.2. Se R é um corpo então L é uma Álgebra de Lie. Quando $R = \mathbb{Z}$ então $\mathbb{Z}$-Álgebra de Lie é dito uma anel de Lie.

Seja A um grupo abeliano aditivo. Um anel de Lie L é graduado em A se

$$L = \bigoplus_{a\in A} L_a \ \ e \ \ [L_a, L_b] \subseteq L_{a+b};$$

onde os L_a são subgrupos do grupo aditivo de L. Os elementos dos componentes de graduação La são denominados homogêneos.

O $[\cdot,\cdot]$ não é associativo por causa da identidade de Jacobi, pois para todo l,m e $n \in L$ temos $[[l,m],n] \neq [l,[m,n]]$. E além disso não existe $1 \in L$, pois caso exista se $y = 1$ então para todo $l \in L$, o comutador $[y,l] = [l,y] = l$ em particular $[y,y] = y \neq 0$.

Definição 3.1.3. Dados duas R-Álgebras de Lie L_1 e L_2, um homomorfismo de R-álgebras de Lie é uma aplicação $\rho : L_1 \longrightarrow L_2$ tal que:

1. ρ é um homomorfismo de R-módulos;

2. ρ é compatível com $[,]$, ou seja, $[l,n]^\rho = [l^\rho, n^\rho]$

Definição 3.1.4. Dados U e V subconjuntos de L definimos o comutador de U e V, como:

$$[U,V] = {}_+\langle [u,v] | u \in U \text{e} v \in V \rangle$$

Definição 3.1.5. Dado L um R-Álgebra de Lie, $M \subseteq L$ é uma R-Álgebra de Lie se M é um R-submódulo tal que $[M,M] \subseteq M$

Definição 3.1.6. Um ideal I de L é um R-módulo tal que $[I,L] \subseteq I$.

Observação 3.1.7. Se I_1 e I_2 são ideais então $I_1 + I_2 = \{a+b | a \in I_1 \ \ e \ \ b \in I_2\}$ é um ideal, além disso se I_1 e I_2 são subálgebras então $I_1 + I_2$ também o é. Mas o mesmo não ocoorre se ambos forem ideais. Por fim se I_1 e I_2 são ideais então $[I_1, I_2]$ é um ideal.

Definição 3.1.8. Dado $X \subseteq L$, a subálgebra gerada por X é definida pela interseção de todas as subálgebras de L que contém X.

Analogamente, definimos o ideal gerado por X, pela interseção de todos os ideias de L que contém X.

Apresentamos até o momento uma R-Álgebra definida com a operação $[,]$, o intuito é entender que o colchete nessa seção apresentado tem as propriedades semelhantes ao apresentado nas preliminares , podemos definir um comutador de Lie simples de tamanho n.

Definição 3.1.9. Um comutador de Lie simples w de peso 1 é um elemento $l \in l$, qualquer comurador de Lie w de peso $n \geq 1$ é da forma $w = [w_1, w_2]$, com w_1 e w_2 comutadores de peso u_1 e u_2, respectivamente com $u_1, u_2 \leq n$, tais que $u_1 + u_2 = n$.

Definição 3.1.10. O multipeso de um comutador de Lie w nas indeterminadas $a_1, \cdots, a_s$ é uma lista $(n_1, \cdots, n_s)$ de números $n_i \in \mathbb{N}$ tal que $n_1 + n_2 + \cdots + n_s = n$, onde cada n_i é o peso de w com respeito a indeterminada a_i.

Exemplo 3.1.11. Seja $w = [a_1, [a_2, [[a_3, a_1], a_2]]]$, ou seja, w é um comutador de peso $n = 5$, onde $(n_1, n_2, n_3) = (2, 2, 1)$.

Lema 3.1.12. Seja L uma R-Álgebra de Lie, então:

1. Todo comutador de Lie w nas entradas $a_1, \cdots, a_k \in L$ é uma R-combinação linear de comutadores de Lie simples nas mesmas entradas de w e com os mesmos multipesos de w em $a_1, \cdots, a_k$;

2. Os comutadores de Lie simples usados no item 1. também podem ser escolhidos todos com a mesma primeira entrada $a \in a_1, \cdots, a_k$.

Denotamos ${}_{+}\langle X \rangle$ e ${}_{id}\langle X \rangle$, a subálgebra gerado pelo conjunto X e o ideal gerado por X, respectivamente.

Proposição 3.1.13. Seja X um conjunto tal que $X \subseteq L$, então:

1. $\langle X \rangle = {}_{+}\langle [x_1, \cdots, x_{n-1}, x_n] | n \geq 0, x_i \in X \rangle$;

2. Suponha que $L = \langle Y \rangle$ então: ${}_{id}\langle X \rangle = \langle [x, y_1, \cdots, y_n] \mid n \geq 0, x \in X \text{ e } y_i \in Y \rangle$.

Definição 3.1.14. Seja $X = \{x_1, x_2, \cdots\}$, com $X \subseteq L$. Se $L =< X >$ uma R-álgebra de Lie, definimos:

$$L_k = {}_{+}\langle \text{Todos os comutadores de Lie de peso } k \text{ nos elementos de } X \rangle.$$

Definição 3.1.15. Um ideal (subálgebra ou submódulo) H de L é dito homogêneo se

$$H = \bigoplus_{k=1}^{\infty} (H \cap L_k).$$

Definição 3.1.16. Seja L uma Álgebra de Lie, definamos a série central superior:

$$\begin{aligned} Z_0(L) =& L \\ Z_1(L) =& Z(L) \\ & \vdots \\ Z_{i+1}(L) =& \{x \in L \mid \ [x,L] \subseteq Z_i(L)\} \end{aligned}$$

com

$$Z_0(L) \subseteq Z_1(L) \subseteq \cdots Z_i(L) \subseteq \cdots$$

Definição 3.1.17. Assim como em G definimos a série central inferior para L:

$$\begin{aligned} \gamma_1(L) =& L \\ \gamma_2(L) =& [\gamma_1(L), L] = [L,L] \\ & \vdots \\ \gamma_{i+1}(L) =& [\gamma_s(L), L] \end{aligned}$$

Observe que $\gamma_n(L) = \langle \underbrace{L, \cdots, L}_{\text{n-fatores}} \rangle = {}_+\langle [l_1, l_2, \cdots, l_n] | l_i \in L \rangle$, ou seja, $\gamma_n(L)$ é um ideal para todo $n \geq 1$, e assim,$\gamma_{n+1}(L) = [\gamma_n(L), L] \subseteq \gamma_n(L)$. Como consequência temos uma cadeia de ideais:

$$\gamma_1(L) \supseteq \gamma_2(L) \supseteq \cdots \supseteq \gamma_i(L) \supseteq \cdots$$

Lema 3.1.18. Seja L uma R-álgebra de Lie , então para todo $k \geq 1$, temos:

1. $\gamma_k(L)$ contém todos comutadores de Lie de peso $l \geq k$ nos elementos de L.
2. Se $L = \langle X \rangle$ então $\gamma_k(L) = {}_+\langle [x_1, x_2, \cdots, x_n] | x_i \in X, n \geq k \rangle$ para todo $k \geq 1$.
3. $[\gamma_n(L), \gamma_m(L)] \subseteq \gamma_{m+n}(L)$, para todo $m, n \geq 1$.

Algumas propriedades de G se traduzem para L e algumas definições parecem semelhantes. As próximas definições e resultados diz respeita a nilpotência e solubilidade de uma R-álgebra de Lie.

Definição 3.1.19. Seja L uma R-álgebra de Lie, L é dita nilpotente se existe n tal que $\gamma_n(L) = 0$. O menor n inteiro com essa propriedade é dita classe de Nilpotência de L.

Teorema 3.1.20. As seguintes afirmações são equivalentes para qualquer L R-álgebra de Lie.

1. $\gamma_{c+1}(L) = 0$;
2. L possui uma série de ideais:

$$L = L_1 \supseteq L_2 \supseteq \cdots \supseteq L_i \supseteq \cdots \supseteq L_c \supseteq L_{c+1} = 0$$

   Tal que $[L_i, L] \subseteq L_{i+1}$
3. Para todos $l_1, l_2, \cdots, l_{c+1} \in L$ temos que $[l_1, l_2, \cdots, l_{c+1}] = 0_L$
4. $\gamma_i(L) \subseteq Z_{k-i+1}(L)$ para cada $i = 1, \cdots, k+1$

Corolário 3.1.21. Seja $L = \langle X \rangle$, então L é nilpotente de classe no máximo $c+1$ se, e somente se, $[x_{i_1}, \cdots, x_{i_{c+1}}] = 0$ para todo $x_i \in X$.

Demonstração. Suponha que L é nilpotente de classe $c+1$, então $\gamma_{c+1}(L) = 0_l$, mas pelo lema 3.1.18 temos, $0_l = \gamma_{c+1}(L) = {}_+\langle [x_1, x_2, \cdots, x_n] | x_i \in X, n \geq c+1 \rangle$, assim para todo $x_i \in X$ temos

$$[x_{i_1}, x_{i_2}, \cdots, x_{i_{c+1}}] = 0.$$

Agora, suponha $[x_{i_1}, \cdots, x_{i_{c+1}}] = 0$, observe que cada $x_{i_1}, \cdots, x_{i_{c+1}} \in L$ então pela implicação 3. em 1. do teorema acima temos que $\gamma_{c+1}(L) = 0_l$ então por definição L é nilpotente de classe no máximo $c+1$. □

Alguns conceitos de grupo e anéis são semelhantes como o R-módulo quociente $L/I = l + I$ para todo $l \in L$, onde L é uma R-álgebra de Lie e I é um ideal de L.

Definição 3.1.22. No R-módulo L/I vale o seguinte produto de Lie $[x+I, y+I] = [x,y]_L + I$

Assim ,$(L/I, +, [\cdot,\cdot]_{L/I})$ é uma R-álgebra de Lie.

Teorema 3.1.23. Seja L uma R-álgebra de Lie, então:

1. Seja I um ideal de L. Então L/I é nilpotente de classe no máximo c se, e somente se, $\gamma_{c+1}(L) \subseteq I$;
2. Se L é nilpotente de classe no máximo c, então qualquer subálgebra e qualquer quociente de L são nilpotentes de classe no máximo c.

Definição 3.1.24. Seja L uma R-álgebra de Lie, podemos definir indutivamente a série derivada de L, usando a operação $[,]$ os seguintes ideais.

$$\begin{aligned} L^{(0)} =& L \\ L^{(1)} =& [L,L] = \gamma_2(L) \\ & \vdots \\ L^{(i)} =& [L^{(i-1)}, L^{(i-1)}] \end{aligned}$$

L é ideal, pois $L^{(1)} = [L,L] \subseteq L$ e assim para todo i, temos, $L^{(i)} \subseteq L^{(i-1)}$. Assim, temos a seguinte cadeia:

$$L^{(0)} = L \supseteq L^{(1)} \supseteq \cdots \supseteq L^{(i)} \supseteq \cdots$$

Observe que $L^{(n-1)}/L^{(n)}$ é uma R-álgebra de Lie abeliana, pois:

$$\gamma_2\left(L^{(n-1)}/L^{(n)}\right) = \gamma_2(L^{(n-1)}) + L^{(n)}/L^{(n)} = L^{(n)}/L^{(n)} = 0.$$

Definição 3.1.25. Seja L uma R-álgebra de Lie. Dizemos que L é solúvel se existe $n \geq 0$ inteiro tal que $L^{(n)} = 0$

Teorema 3.1.26. Seja L uma R-álgebra de Lie. As seguintes relações são equivalentes:

1. $L^{(d)} = 0$;
2. L tem uma série de ideais de comprimento d com fatores abelianos

$$L = L_0 \supseteq L_1 \supseteq \cdots \supseteq L_d = 0$$

   Tal que $[L_i, L_i] \leq L_{i+1}$ para todo $i = 0, \cdots, d-1$;

3. $\delta_d(x_1, x_2, \cdots, x_{2^d}) = 0$.

Um anel de Lie satisfazendo essas condições é dito ser solúvel e o menor número d com a propriedade indicada, é chamado comprimento derivado de L. Muitas vezes é dito que um anel de Lie é solúvel de comprimento derivado d, significando que é solúvel de comprimento derivado $\leq d$.

3.2 Anéis de Lie associadas a Grupo

As definições e resultados apresentados até esse momento servem como base para a construção de um anel de Lie. Para construir o anel de Lie associado ao grupo G, consideremos a série central descendente como em 1.2.2. Lembremos que $\gamma_i(G)/\gamma_{i+1}(G)$ é um $\mathbb{Z}$-módulo abeliano. Para simplificar a notação usaremos γ_i/γ_{i+1} para denotar $\gamma_i(G)/\gamma_{i+1}(G)$

Definição 3.2.1. Definamos $L(G)$

$$L(G) = \bigoplus_{i=1}^{\infty} \gamma_i/\gamma_{i+1}.$$

Definimos $+$ e $[,]$ em cada componente de $L(G)$, ou seja, dados $\overline{x_1}, \overline{x_2} \in \gamma_i/\gamma_{i+1}$, temos:

1. $\overline{x_1} + \overline{x_2} = \overline{x_1 x_2} = x_1 x_2 \gamma_{i+1}$;
2. $[\overline{x_1}, \overline{x_2}]_L = [x_1, x_2]\gamma_{i+j+1}$.

Veremos que $L(G)$ está bem definido, ou seja as operações definidas acima independem da escolha de representantes da classe. Para isso, seja $\overline{x_1} = \bar{x}$ e $\overline{x_2} = \bar{y}$, logo $x = x_1 z_1$ e $y = x_2 z_2$ para z_1 e $z_2 \in \gamma_{i+1}$, assim:

$$\begin{aligned} \bar{x} + \bar{y} &= xy\gamma_{i+1} \\ &= (x_1 z_1 x_2 z_2)\gamma_{i+1} \\ &= (x_1 z_1 x_2)\gamma_{i+1} \\ &= (x_1 x_2 z_1)[z_1, x_2]\gamma_{i+1} \\ &= x_1 x_2 \gamma_{i+1} \\ &= \overline{x_1} + \overline{x_2}. \end{aligned} \tag{3.1}$$

Observe que (3.1) surge do fato de $z_1 \in \gamma_{i+1}$ e $x_2 \in \gamma_i$, ou seja, o comutador está em γ_{2i+1} pelo Teorema 3.1.18 e do fato de $\gamma_{2i+1} \subseteq \gamma_{i+1}$. Para o $[,]$, sejam $\bar{x} = \overline{x_1} \in \gamma_i/\gamma_{i+1}$ e

$\overline{y} = \overline{y_1} \in \gamma_j/\gamma_{j+1}$, logo $x_1 = xz_1$ e $y_1 = yw_1$ com z_1 e $w_1 \in \gamma_{i+1}$ e γ_{j+1} respectivamente, logo:

$$\begin{aligned}
[\overline{x_1}, \overline{y_1}]_L &= [x_1, y_1]\gamma_{i+j+1} \\
&= [xz_1, yw_1]\gamma_{i+j+1} \\
&= [x, yw_1]^{z_1}[z_1, yw_1]\gamma_{i+j+1} \\
&= [x, yw_1]^{z_1}[z_1, yw_1]\gamma_{i+j+1} \\
&= [x, yw_1]^{z_1}[z_1, yw_1]\gamma_{i+j+1} \\
&= [x, yw_1]^{z_1}[z_1, yw_1]\gamma_{i+j+1} \\
&= [x, yw_1]^{z_1}[z_1, yw_1]\gamma_{i+j+1} \\
&= [x, yw_1][[x, yw_1], z_1][z_1, yw_1]\gamma_{i+j+1} \qquad (3.2) \\
&= [x, w_1][x, y][[x, y], w_1]\gamma_{i+j+1} \qquad (3.3) \\
&= [x, y]\gamma_{i+j+1} = [\overline{x}, \overline{y}]_L
\end{aligned}$$

As equações (3.2) e (3.3) surgem do fato dos comutadores pertencerem a γ_{i+j+1} e γ_{2j+i+1}.O fato de $L(G)$ ser uma R-álgebra de Lie segue da operação $[,]$ satisfazer as propriedades da definição 3.1.1. Para ilustrar a construção do anel de Lie associado a o grupo G e mostrar as diferenças entre o anel de Lie e o grupo G, considere os seguintes grupos.

$$\begin{aligned}
D_8 &= \langle a, b | a^4 = b^2 = 1, a^b = a^{-1} \rangle; \\
Q_8 &= \langle u, v | u^4 = v^4 = 1, u^v = u^3 \rangle.
\end{aligned}$$

Sabemos que $|D_8| = |Q_8| = 8$, porém Q_8 tem *um* elemento de ordem 2, enquanto D_8 tem 5 elementos de ordem 2, ou seja, não há isomorfismo entre Q_8 e D_8. Exibiremos a série central inferior para ambos os grupos.

$$\begin{aligned}
\gamma_1(D_8) = D_8, \gamma_2(D_8) = \langle a^2 \rangle, \gamma_3(D_8) = 1. \\
\gamma_1(Q_8) = Q_8, \gamma_2(Q_8) = \langle u^2 \rangle, \gamma_3(Q_8) = 1.
\end{aligned}$$

Assim,

$$\begin{aligned}
L(Q_8) &= \gamma_1(Q_8)/\gamma_2(Q_8) \bigoplus \gamma_2(Q_8)/\gamma_3(Q_8) \\
&= \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z} \qquad \text{e} \\
L(D_8) &= \gamma_1(D_8)/\gamma_2(D_8) \bigoplus \gamma_2(D_8)/\gamma_3(D_8) \\
&= \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}.
\end{aligned}$$

Então $L(D_8)$ é um espaço vetorial sobre o corpo de dois $\mathbb{F}_2$ com base $\{\overline{a},\overline{b},\overline{c}\}$ e $L(Q_8)$ é um espaço vetorial sobre o corpo de dois elementos $\mathbb{F}_2$ com base $\{\overline{u},\overline{v},\overline{w}=\overline{[u,v]}\}$. As álgebras de Lie são iguais, mesmo que os grupos não sejam isomorfos.

Lema 3.2.2. Seja $L(G)$ a $\mathbb{Z}$-álgebra de Lie de um grupo G definida anteriormente, então:

1. Para todo $\overline{a} \in \gamma_1/\gamma_2$ e w é um comutador de Lie de peso k, então temos que:

$$w(\overline{a_1},\cdots,\overline{a_k}) = w(a_1,\cdots,a_k)\gamma_{k+1}.$$

2. Para todo $k \geq 1$, temos:

$$\gamma_k/\gamma_{k+1} = {}_+\langle [\overline{a_1},\cdots,\overline{a_k}] | \overline{a_j} \in \gamma_1/\gamma_2 \rangle.$$

3. $L(G)$ é gerado como $\mathbb{Z}$-álgebra por γ_1/γ_2 e para $k \geq 1$:

$$\gamma_k(L(G)) = \bigoplus_{i\geq k} \gamma_i/\gamma_{i+1}.$$

Demonstração.

1. Provaremos por indução em k. Para $k = 1$, temos:

$$w(\overline{a_1})_L = [\overline{a_1}] = a_1\gamma_2,$$

Pois $\overline{a_1} \in \gamma_1/\gamma_2$ e $a_1 = [a_1]$, assim, $w(\overline{a_1})_L = w(a_1)\gamma_2(G)$. Suponha que é válido para $k-1$, mostraremos que é válido para k. Seja w um monômio de Lie de grau k, então, $w = [b_1, b_2]$, onde b_1 e b_2 são comutadores de grau n_1 e n_2 respectivamente, tais que $n_1 + n_2 = k$. Aplicando a hipótese de indução, temos:

$$\begin{aligned} b_1(\overline{a_1},\cdots,\overline{a_{n_1}}) &= [\overline{a_1},\cdots,\overline{a_{n_1}}] = [a_1,\cdots,a_{n_1}]\gamma_{n_1+1}(G) \\ b_2(\overline{a_{n_1+1}},\cdots,\overline{a_{n_1+n_2}}) &= [\overline{a_{n_1+1}},\cdots,\overline{a_{n_2}}] = [a_{n_1},\cdots,a_{n_1+n_2}]\gamma_{n_1+n_2+1}(G) \end{aligned}$$

E assim, temos:

$$\begin{aligned} w[\overline{a_1},\cdots,\overline{a_k}] =& w(\overline{a_1},\cdots,\overline{a_{n_1+n_2}}) = [b_1,b_2](\overline{a_1},\cdots,\overline{a_{n_1+n_2}}) \\ =& [b_1(\overline{a_1}\cdots,\overline{n_1}), b_2(\overline{a_{n_1+1}}\cdots,\overline{n_1+n_2})]_L \\ =& [b_1(a_1\cdots,a_{n_1})\gamma_{n_1+1}(G), b_2(a_{n_1+1}\cdots,a_{n_1+n_2})\gamma_{n_1+n_2+1}(G)] \\ =& [b_1(a_1\cdots,a_{n_1}), b_2(a_{n_1+1}\cdots,a_{n_1+n_2})]\gamma_{n_1+n_2+1}(G) \end{aligned}$$

2. Sabemos que $\gamma_k(G)$ é gerado por comutadores simples de peso $\geq k$. Portanto γ_k/γ_{k+1} é gerado por $[a_1,\cdots,a_k]\gamma_{k+1}$, onde $a_i \in G$, mas pela definição de multiplicação em $L(G)$ temos:

$$\begin{aligned}[a_1\gamma_2, a_2\gamma_2] &= [a_1,a_2]\gamma_3\\ [a_1\gamma_2, a_2\gamma_2, a_3\gamma_2] &= [a_1,a_2,a_3]\gamma_4\\ &\vdots\\ [a_1\gamma_2,\cdots,a_{k-1}\gamma_2, a_k\gamma_2] &= [a_1,a_2,a_3,\cdots,a_k]\gamma_{k+1}\end{aligned}$$

   Para todo $k \geq 1$, segue $\gamma_k/\gamma_{k+1} = \langle [a_1\cdots,a_k] \mid a_i \in \gamma_i(G)/\gamma_{i+1}(G)\rangle$.

3. Observe que $[a_1,a_2,a_3,\cdots,a_k]\gamma_{k+1} \in \gamma_k(L(G))$. Segue do item (ii) que

$$\bigoplus_{i=k}^{\infty} L_i \subseteq \gamma_k(L(G)).$$

   A inclusão inversa segue do fato $[\gamma_i(G),\gamma_j(G)] \leq \gamma_{i+j}$ para todo i e $j \in \mathbb{N}$.

□

Teorema 3.2.3. Seja G um grupo nilpotente. Então valem os seguintes resultados:

1. $L(G)$ é nilpotente e possue a mesma classe de nilpotência de G. Além disso, se G é finito então $|G| = |L(G)|$;

2. Se G é solúvel de comprimento derivado d então $L(G)$ possui comprimento derivado $\leq d$;

3. Seja Φ um automorfismo do grupo G. Então Φ induz um automorfismo no anel de Lie $L(G)$ por sua ação sobre os grupos quocientes γ_i/γ_{i+1}. Além disso, se G é finito e $(|G|,|\Phi|) = 1$ então Φ atua em $L(G)$ e $|C_{L(G)}(\Phi)| = |C_G(\Phi)|$.

Demonstração.

1. Como a ordem de G é finita então por l Lagrange e sendo G nilpotente,ou seja, $\gamma_{c+1}(G) = 1$ e $\gamma_1(G) = G$, temos:

$$|G| = \prod_{i=1}^{c} [\gamma_i : \gamma_{i+1}] = \prod_{i=1}^{c} |\gamma_1/\gamma_{i+1}| = |L(G)|$$

. Para provarmos a nilpotência de $L(G)$, temos por hipótese que G é nilpotente, ou seja, $\gamma_c(G) \neq 1$ e $\gamma_{c+1}(G) = 1$, mas pelo lema 3.2.2 item 3., temos:

$$\gamma_{c+1}(L(G)) = \bigoplus_{i=c+1}^{\infty} \gamma_i \diagup \gamma_{i+1} = 0$$

Devemos mostrar que a classe de nilpotência é c para tanto suponha $\gamma_c(L(G)) = 0$, novamente pelo lema 3.2.2 item 3 temos que $L_c = \gamma_c(G) \diagup \gamma_{c+1}(G) = 0$, mas como $\gamma_{c+1}(G) = 1$ então $\gamma_c(G) = 1$, o que contradiz o fato de $\gamma_c(G) \neq 1$, logo a classe de nilpotência de $L(G)$ é c.

2. Se G é solúvel temos $\delta_d(x_1, \cdots, x_{2^d}) = 1$ sobre todos os elementos de G. Essa identidade é multilinear e pelo fato de como definimos multiplicação em $L(G)$ temos a identidade é satisfeita para um número menor ou igual a d, com elementos homogêneos de $L(G)$.

3. Seja Φ um automorfismo de G e sejam $a_i = a\gamma_{i+1} \in L_i$ e $b_j = b\gamma_{j+1} \in L_j$, como cada $\gamma_i(G)$ é característico em G, segue que Φ induz um automorfismo em cada L_i. Assim, $x_i \in L_i$ e $x \in \gamma_i(G)$, se $x = x_1\gamma_2(G) + x_2\gamma_3(G) + \cdots$ definimos $x^\Phi = x_1^\Phi\gamma_2(G) + x_2^\Phi\gamma_3(G) + \cdots$. Como cada $\gamma_i(G)$ é característico em G, segue que Φ induz um automorfismo em $L(G)$. Basta mostrar que Φ preserva o colchete de Lie. Assim, pela definição de $[,]$, temos:

$$\begin{aligned}
[a_i, b_j]^\Phi &= [a\gamma_{i+1}, b\gamma_{j+1}]^\Phi \\
&= [a,b]^\Phi\gamma_{i+j+1} = [a^\Phi, b^\Phi]\gamma_{i+j+1} \\
&= [a^\Phi\gamma_{i+1}, b^\Phi\gamma_{j+1}] = [a_i^\Phi, b_j^\Phi].
\end{aligned}$$

Usaremos a linearidade de $[,]$ para estender a ação induzida Φ sobre $L(G)$. Sejam x e $y \in L(G)$ tal que $x = x_1 + \cdots + x_s$ e $y = y_1 + \cdots + y_r$, no qual $x_i \in L_i$ e $y \in L_j$ elementos arbitrários em $L(G)$. Temos:

$$\begin{aligned}
[x,y]^\Phi = &[\sum_i^s x_i, \sum_j^r x_j]^\Phi = \left(\sum_{j,i}[x_i, x_j]\right)^\Phi \\
&= \sum_{i,j}[x_i^\Phi, x_j^\Phi] = [\sum_i^s x_i^\Phi, \sum_j^r x_j^\Phi] = [x_i^\Phi, x_j^\Phi].
\end{aligned}$$

Portanto, Φ é de fato um automorfismo do anel de Lie $L(G)$. Uma vez que Φ atua em trivialmente em $L(G)$ se, e somente se, centraliza todos os fatores da série central inferior de G,assim, decorre pelo Teorema 1.2.22 item 4. segue que $|C_G(\Phi)| = |C_{L(G)}(\Phi)|$

□

3.3 Álgebras de Zassenhaus-Jennings-Lazard

Nessa seção apresentaremos um novo Anel de Lie, na verdade álgebra de Lie associada ao grupo G. Tal álgebra foi popularizada nos estudos para solucionar o problema restrito de Burnside que consitiu em responder a pergunta:"será que existe apenas um número finito de quocientes finitos não isomorfos de $B(m,n)$?", a notação $B(m,n)$ é dada para o quociente F_m/N, no qual F_m é o grupo livre com m geradores e N é gerado pelo conjunto $x^n : x \in F_m$. A pergunta pode ser reformulada, ou seja, "será que dados inteiros $m,n \geq 2$, existe apenas um número finito de grupos m-gerados de expoente n que são finitos?", a resposta a essa pergunta foi respondida em 1989 no premiado trabalho de Efim Zelmanov [26], com resposta positiva. Nesse trabalho apresentaremos algumas das propriedades da tecnica usada por Zelmanov.

Definição 3.3.1. Seja G um um grupo e p um número primo arbitrário, fixamos:

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

Cada $D_i(G)$ é subgrupo característico de G, assim, obtemos a seguinte série:

$$G = D_1(G) \geq D_2(G) \geq \cdots \geq D_i(G) \geq \cdots$$

A série formada pelos subgrupos D_i é chamada de série de Zassenhaus-Jennings-Lazard do grupo G. Algumas propriedades dessa série permite construir uma álgebra de Lie $DL(G)$ sobre $\mathbb{F}_p$. A demonstração de algumas propriedades que são de fundamental relevância para a construção do anel de Lie associado, serão basedos no livro *Analytic Pro-P Groups* [7] e do artigo *Applications of Lie ring methods to group theory* [19].

Teorema 3.3.2. Seja G um grupo e $x,y \in G$. Então existem $C_i \in \gamma_i(\langle x,y \rangle)$ tal que para todo $n \in \mathbb{N}$, temos:

$$x^n y^n = (xy)^n C_2^{\binom{n}{2}} C_3^{\binom{n}{3}} \cdots C_n^{\binom{n}{n}}$$

A demonstração pode ser encontrada no livro *Analytic Pro-P Groups* [[7], Apêndice A]. A fórmula de compilação estabelece uma expressão para C como um produto de comutadores.

Lema 3.3.3. Sejam x e y elementos do grupo G e sejam $H = \langle x, [x,y] \rangle$, p um primo fixado, então para todo $n \geq 1$, temos:

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

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

A demonstração pode ser encontrada no livro *Analytic Pro-P Groups* [7, Lema 11.9].

Lema 3.3.4. Sejam G um grupo e $n \geq 0$ então para $i, j \geq 0$, temos:

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

Demonstração. Sejam $x, y \in \gamma_i$ e $z \in \gamma_j$ temos:

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

Assim, pelo item 2 do Lema 3.3.3 temos:

$$[x^{p^n}, z] \equiv [x,z]^{p^n} mod \gamma_2(H)^{p^n} \prod_{s=1}^{n} \gamma_{p^s}(H)^{p^{n-s}}$$

Denote por $N = \prod_{r=0}^{n} \gamma_{j+ip^r}(G)^{p^{n-r}}$ com $N \trianglelefteq G$. Seja $H = \langle x, [x,z] \rangle$ então:

$$\gamma_i(H) = \langle [m_1, \cdots, m_i]^h \mid h \in H, m_i \in \{x, [x,z]\} \rangle.$$

Ou seja, $\gamma_2(H) \leq \gamma_{2i+j}(G)$, pois $\gamma_2 = \langle \langle [m_1, m_2]^h \mid h \in H, m_i \in \{x, [x,z]\} \rangle$, se

$$\gamma_2 = \langle [x, [x,z]]^h \mid h \in H \rangle \leq [\gamma_i(G), \gamma_{i+j}(G)] \leq \gamma_{2i+j}(G).$$

Assim para todo $m \geq 2$ temos $\gamma_m(H) \leq \gamma_{mi+j}(G)$, basta aplicar indução em m. Em particular quando $r = 0, 1, \cdots, n$ temos que:

$$\gamma_{p^r}(H)^{p^{n-r}} \leq \gamma_{p^r i+j}(G)^{p^{n-r}} \leq N.$$

E $[x,z]^{p^n} \in \gamma_{i+j}(G)^{p^n} \in N$, por fim, $[x^{p^n}, z] \in N$ então $[\gamma_i(G)^{p^n}, \gamma_j(G)] \leq N$. □

Lema 3.3.5. Suponha que $i \geq 1, j \geq 1$ e $h \geq 0$. Seja $N = \prod_{r=0}^{h} \gamma_{i+jp^r}(G)^{p^{h-r}}$. 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 demonstração será por indução sobre n. Para $n = 2$ temos que:

$$\gamma_2(\langle x,N\rangle) = [\langle x,N\rangle, \langle x,N\rangle] = [R, \langle x,N\rangle].$$

Como $\langle x,N\rangle \leq \gamma_i(G)$, segue que $\gamma_2(\langle x,N\rangle) = [N, \gamma_i(G)]$. Portanto para $n \geq 2$, temos $\gamma_n(\langle x,N\rangle) = [\gamma_{n-1}(\langle x,N\rangle), \langle x,N\rangle] \leq [\gamma_{n-1}(\langle x,N\rangle), \gamma_i(G)]$. Usando a definição de N para $n = 2$ e a hipótese de indução, temos que para $n \geq 2$, temos:

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

Pelo item 5. do Teorema 1.1.6 temos que:

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

Mas, pelo Lema 3.3.4 temos:

$$\begin{aligned}
\gamma_n(\langle x,N\rangle) &\leq \prod_{r=0}^{h} \prod_{s=0}^{h-r} [\gamma_{i+p^s(in-1+jp^r)}(G)^{p^{h-r-s}}, \gamma_i(G)] \\
\gamma_n(\langle x,N\rangle) &\leq \prod_{r+s\leq h} \gamma_{i+p^s(in-1+jp^r)+i}(G)^{p^{h-r-s}} \\
\gamma_n(\langle x,N\rangle) &\leq \prod_{r+s\leq h} \gamma_{in+jp^{r+s}}(G),
\end{aligned}$$

pois $ip^s in - p^s \geq in$. □

Lema 3.3.6. Se $i \geq 1, j \geq 1, h \geq 0, k \geq 0$, então:

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

Demonstração. Suponha $x \in \gamma_i(G)$ e $y \in \gamma_j(G)$. Sejam $z = [x, y^{p^h}]$ e $H = \langle x,z\rangle$ pelo item 2. do lema 3.1.12 temos:

$$[x^{p^k}, y^{p^h}] \equiv [x, y^{p^h}]^{p^k} \equiv z^{p^k} \equiv [x,y]^{p^k} mod\, \gamma_2(H)^{p^k} \prod_{s=1}^{n} \gamma_{p^s}(H)^{p^{k-s}}.$$

Para $n = 1, \cdots, p^k$ defina $H_n = \prod_{r=0}^{h} \gamma_{in+jp^r}(G)^{p^{h-r}}$. Pelo Lema 3.3.4 $z \in H_1$, assim temos $H = \langle x, [x, y^{p^h}] \rangle \leq \langle x, H_1 \rangle$. Pelo lema 3.3.5, temos:

$$\gamma_n(H) \leq \gamma_n(\langle x, H_1 \rangle) \leq H_n \qquad e$$
$$\gamma_2(H)^{p^k} \leq H_2^{p^k} \leq H_1^{p^k}.$$

Portanto, $[x^{p^k}, y^{p^h}] \in \prod_{m=0}^{n} H_{p^m}^{p^{k-m}}$. Faça $R = D_{ip^k+jp^h}(G)$, se $m+h-r \geq k$, então pela definição de D_i, $\gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq R$. Assim, $s = \max\{m+h-k+1, 0\}$, temos:

$$H_{p^n} \leq R \prod_{r=0}^{h} \gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq R\gamma_{ip^m+jp^s}(G).$$

Logo,

$$H_{p^n}^{p^{k-m}} \leq R\gamma_{ip^m+jp^{k-m}}(G) = R.$$

Pois, $ip^k + jp^{s+k-m} \geq ip^k + jp^h$. Logo $[x^{p^k}, y^{p^h}] \in R$ e $(x^{p^k})R$ comuta com $(y^{p^h})R$, ou seja, cada elemento de $\gamma_i^{p^k}(G)R/R$ comuta com $\gamma_j^{p^h}(G)R/R$ e $[\gamma_i^{p^k}(G), \gamma_j^{p^h}(G)] \leq R$. □

Proposição 3.3.7. Seja D_i a série de *Jennings-Zassenhaus* do grupo G, então:

1. $[D_n, D_m] \leq D_{m+n}$;
2. $D_n(G)^p \leq D_{pn}(G)$;
3. Para $n \geq 1$, temos $D_n(G) = [D_{n-1}(G), G]D_m(G)^p$, com m é o menor número natural tal que $pm \geq n$;
4. Suponha que $G = R_1 \geq R_2 \geq \cdots$ é uma série do grupo G tal que $R_n \trianglelefteq G$, $[R_n, G] \leq R_{n+1}$ e $R_n^p \leq R_{np}$ para todo $n \geq 1$. Então $D_n(G) \leq R_n$.

Demonstração.

1. Basta considerar $D_m = \prod_{ip^k \geq m} \gamma_i(G)^{p^k}$ e $D_n = \prod_{jp^h \geq n} \gamma_j(G)^{p^h}$ no Lema 3.3.6, logo:

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

Pois, $ip^k \geq m$ e $jp^h \geq n$.

2. Pelo item 1 $\gamma_p(D_n) \leq \gamma_{pn}(G)$, assim ${}^{D_n}\!/_{D_{pn}}$ é regular, pois a classe de nilpotência é no máximo $p-1$. Mas, ${}^{D_n}\!/_{D_{pn}}$ é gerado por elementos de ordem p, pois se $ip^k \geq n$ e $x \in \gamma_i$, então $(x^{p^k})^p \in D_{ip^{k+1}} \leq D_{pn}$. Portanto, temos $\left({}^{D_n(G)}\!/_{D_{pn}}\right)^p = 1$. E assin $D_n(G)^p \leq D_{pn}$.

3. Como m é o menor número natural tal que $pm \geq n$ temos pelo item 1.:

$$[D_{n-1}(G), D_1] \leq D_n.$$

Mas, pelo item 2. e como $pm \geq n$ segue que:

$$D_m(G)^p \leq D_{mp}(G) \leq D_n(G).$$

Seja $k = 0$ na definição 3.3.1,com $i \geq n$ logo:

$$\gamma_i(G)^{p^k} = \gamma_i(G) \leq \gamma_n(G) = [\gamma_{n-1}, G] \leq [D_{n-1}(G), G].$$

Se $k \geq 0$, então $ip^{k-1} \geq m$, pela definição de m, temos:

$$\gamma_i(G)^{p^k} \leq \left(\gamma_i(G)^{p^{k-1}}\right)^p \leq \left(D_{ip^{k-1}}(G)\right)^p \leq D_m(G)^p.$$

Assim, $\gamma_i(G)^{p^k} \leq [D_{n-1}(G), G]D_m(G)^p$.

4. A demonstração segue do item 3 por indução em n.

□

Os itens 1. e 2. da Proposição 3.3.7 caracterizam a série de *Jennings-Zassenhaus* como uma N e N_p-série, respectivamente. A partir de uma N_p-série de um grupo G, podemos construir um anel de Lie $LD(G)$ da forma:

$$LD(G) = \bigoplus_{i=1} L_i \qquad \text{e} \qquad L_i = {}^{D_i}\!/_{D_{i+1}}.$$

A comutação em G induz a operação $[,]$, para elementos homogêneos $xD_{i+1} \in L_i$ e $yD_{j+1} \in L_j$, a operação é definida por:

$$[xD_{i+1}, yD_{j+1}] = [x,y]D_{j+i+1} \in L_{i+j}.$$

Suponha que $a'D_{i+1} = aD_{i+1}$ e $b'D_{j+1} = bD_{j+1}$, com a, a', b e $b' \in G$, assuma também que $g_1 \in D_{i+1}$ e $g_2 \in D_{j+1}$, tais que, $a' = ag_1$ e $b' = bg_2$, mas pelo itens (3) e (4) do teorema

1.1.5:

$$[a',b'] = [ag_1,b'] = [a,b'][a,b',g_1][g_1,b].$$

Mas,

$$[a,b',g_1] \subseteq D_{i+j+1} \qquad \text{e} \qquad [g_1,b] \subseteq D_{i+j+1}.$$

Por outro lado:

$$[a,b'] = [a,bg_2] = [a,g_2][a,b,a,b,g_2].$$

De maneira análoga:

$$[a,g_2] \subseteq D_{i+j+1} \qquad \text{e} \qquad [a,b,g_2] \subseteq D_{i+j+1}.$$

Então:

$$[a',b'] = [a,b']D_{i+j+1} = [a,b]D_{i+j+1}.$$

O comutador $[,]$ está bem definido. Basta verificar que as propriedades do $[,]$ são satisfeitas como na definição 3.1.1, verificaremos os itens 1 e 2, logo sejam $\overline{a} \in {}^{D_i}\!/_{D_{i+1}}, \overline{b} \in {}^{D_j}\!/_{D_{j+1}}$ e $\overline{c} \in {}^{D_k}\!/_{D_{k+1}}$:

1. $[a',a'] = 0$

   $$[a',a'] = [aG_{i+1},aG_{i+1}] = [a,a]G_{2i+1}$$

   Pois $L_i = {}^{G_i}\!/_{G_{i+1}}$.

2. $[\overline{a},\overline{b},\overline{c}] + [\overline{b},\overline{c},\overline{a}] + [\overline{c},\overline{a},\overline{b}] = 0$ Assim $[\overline{a},\overline{b},\overline{c}]$

   $$\begin{aligned}
   &[\overline{a},\overline{b},\overline{c}] + [\overline{b},\overline{c},\overline{a}] + [\overline{c},\overline{a},\overline{b}] = \\
   &[aD_{i+1},bD_{j+1},cD_{k+1}] + [bD_{j+1},cD_{k+1},aD_{i+1}] + [cD_{k+1},aD_{i+1},bD_{j+1}] = \\
   &[a,b,c]D_{i+j+k+1} + [b,c,a]D_{i+j+k+1} + [c,a,b]D_{i+j+k+1} = \\
   &[a,b,c][b,c,a][c,a,b]D_{i+j+k+1} = \\
   &[a,b^{-1},c]^{-b}[b,c^{-1},a]^{-c}[c,a^{-1},b]^{-a}D_{i+j+k+1} = \\
   &[c,a^{-1},b]^{-a}[b,c^{-1},a]^{-c}[a,b^{-1},c]^{-b}D_{i+j+k+1} = \\
   &([a,b^{-1},c]^{b}[b,c^{-1},a]^{c}[c,a^{-1},b]^{a})^{-1}D_{i+j+k+1}.
   \end{aligned}$$

   Pelo identidade de Hall-Witt , temos:

   $$[a,b^{-1},c]^{b}[b,c^{-1},a]^{c}[c,a^{-1},b]^{a} = 1$$

Segue que:

$$[\overline{a},\overline{b},\overline{c}]+[\overline{b},\overline{c},\overline{a}]+[\overline{c},\overline{a},\overline{b}]=0.$$

Portanto $LD(G)$ é uma anel de Lie.

Na seção anterior vimos que se A age sobre G, essa ação pode ser induzida sobre todo quocientes invariantes, em particular ${}^{D_j}\!/_{D_{j+1}}$, e assim estendendo para a soma $\bigoplus {}^{D_j}\!/_{D_{j+1}}$.

Podemos ver A como um grupo agindo sobre a subálgebra $L_p(G)=\langle L_1\rangle$ de $LD(G)$, como automorfismo de álgebras de Lie.

Proposição 3.3.8. Seja G um grupo gerado pelos elemento $a_1,\cdots,a_m$ e assuma que $L_p(G)$ seja nilpotente de classe no máximo c. Sejam $\rho_1,\cdots,\rho_s$ todos os comutadores gerados pelos elemento $a_1,\cdots,a_m$ de peso $\leq c$. Então para qualquer inteiro não negativo i, o grupo G pode ser escrito como:

$$G=\langle\rho_1\rangle\cdots\langle\rho_s\rangle D_{i+1}.$$

Demonstração. Primeiramente observe que o subgrupo $D_i=\langle D_{i+1},[b_1,\cdots,b_j]^{p^k}\,|\,jp^k\geq i\rangle$. Essa igualdade pode ser demonstrada usando a identidade de *Witt* e pelo Lema 3.3.3. Faremos a demonstração por indução em i, para $i=0$ temos que $G=D_1(G)$ trivial. Assuma que $i\geq 1$ e

$$G=\langle\rho_1\rangle\cdots\langle\rho_s\rangle D_i.$$

Então qualquer $x\in G$ pode ser escrito como:

$$x=\rho_1^{\alpha_1}\rho_2^{\alpha_2}\cdots\rho_s^{\alpha_s}y. \tag{3.4}$$

com $y\in D_i$. Sem perda de generalidade podemos assumir que $D_{i+1}=1$. Pela obervação feita inicialmente podemos escrever:

$$y=(\sigma_1^{p^{k_1}})^{\beta_1}(\sigma_2^{p^{k_2}})^{\beta_2}\cdots(\sigma_t^{p^{k_t}})^{\beta_t}. \tag{3.5}$$

com cada $\sigma_n\in[b_1,\cdots,b_j]$ com $jp^k\geq i$ e $b_1\cdots b_j\in\{a_1\cdots a_m\}$.

Denote $\overline{a_l}$ o elemento $a_lD_2\in L_p(G)$ com $l=1,\cdots,m$. Por hipótese $L_p(G)$ é nilpotente de classe c, logo $[\overline{b_1},\cdots,\overline{b_{c+1}}]=0$ para quaisquer $b_1\cdots b_{c+1}\in\{a_1\cdots a_m\}$. Isso implica que $b_1\cdots b_{c+1}\in D_{c+2}$ para quaisquer $b_1\cdots b_{c+1}\in\{a_1\cdots a_m\}$ e $\gamma_{c+1}\leq D_{c+2}$ Como D_i é uma N_p-série, para qualquer $d\geq c+1$ temos $\gamma_d\leq D_{d+1}$.

Agora, se σ_n é da forma $[b_1,\cdots,b_j]$ com $j \geq c+1$ então

$$\sigma_n^{p^{kn}} \in \gamma_j^{p^{kn}} \leq D_{j+1}^{p^{kn}} \leq D_{(j+1)p^{kn}} \leq D_{i+1} = 1.$$

Portanto, podemos assumir que cada σ_n é da forma $[b_1,\cdots,b_j]$ com $j \leq c$ e nessa caso σ_n pertence a lista $\rho_1\rho_2\cdots\rho_s$.

Novamente, pelo fato $\{D_i\}$ ser uma N_p-série, temos $\sigma_n^{p^{kn}} \in Z(G)$. Comparando a maneira que escrevemos x e y em 3.5 temos:

$$x \in \langle\rho_1\rangle\cdots\langle\rho_s\rangle$$

como queríamos. □

3.4 Automorfismos Livres de Pontos Fixos

O principal objetivo desta seção é apresentar resultados conhecidos na teoria de álgebras de Lie. como por exemplo o resutado devido a *Kreknin-Krostrikin*

Teorema 3.4.1. ***(Kreknin,Krostrikin)*** Se um anel de Lie L é solúvel de comprimento derivado s e admite um automorfismo regular φ de ordem prima p, então L é nilpotente e sua classe de nilpotência é no máximo $\dfrac{(p-1)^s-1}{p-2}$.

Outro resultado que merece destaque é o resultado devido a *Higman*, *Kreknin e Krostrikin* o qual afirma

Corolário 3.4.2. ***(Higman, Kreknin e Kostrikin)*** Se um anel de Lie admite um automorfismo regular de ordem prima p, então ele é nilpotente e sua classe de nilpotência é limitada por algum número $h(p)$, com esse dependendo somente de p.

Para tanto precisamos de algumas propriedades básicas de produto tensorial. Dados A e B ambos K-espaços vetoriais sobre o corpo K, com bases formadas por $\{a_1,\cdots,a_n\}$ é $\{b_1,\cdots,b_m\}$, respectivamente. O **Produto Tensorial** $A\otimes_K B = A\otimes_K B$ de A e B é o espaço vetorial de base $\{a_i\otimes_K b_j \mid 1\leq i\leq n \text{ e } 1\leq j\leq m\}$. Dado $a\in A$ e $b\in B$ temos que $a=\sum_{i=1}^{n}\alpha_i a_i$ e $b=\sum_{j=1}^{m}\beta_j b_j$, definimos:

$$a\bigotimes b = \sum_{i=1}^{n}\alpha_i a_i \bigotimes \sum_{j=1}^{m}\beta_j b_j = \sum_{j=1}^{m}\sum_{i=1}^{n}\alpha_i\beta_j(a_i\otimes b_j)$$

Em que $\alpha_i, \beta_j \in K$. Os elementos $a \otimes b$, satisfazem as seguintes propriedades para $a_i \in A$, $b_j \in B$ e $k \in K$ com $1 \leq i, j \leq 2$:

1. $(a_1 + a_2) \otimes b = (a_1 \otimes b) + (a_2 \otimes b)$;
2. $a \otimes (b_1 + b_2) = (a \otimes b_1) + (a \otimes b_2)$;
3. $(ra) \otimes b = r(a \otimes b) = a \otimes rb$.

Podemos definir o conceito de produto tensorial para K-módulo.

Definição 3.4.3. Sejam A e B dois K-módulos. Seu produto tensorial $A \otimes_K B$ é definido como o módulo quociente de K-módulo livre com $a \otimes_K b$ geradores livres, $a \in A$ e $b \in B$, do submódulo gerado de todos os elementos de forma que:

1. $k(a_0 \otimes b_0) = ka_0 \otimes b_0 = a_0 \otimes kb_0$;
2. $a_0 \otimes (b1 + b2) = a_0 \otimes b_1 + a_0 \otimes b_2$;
3. $(a_1 + a_2) \otimes b_0 = a_1 \otimes b_0 + a_2 \otimes b_0$.

Para todo $k \in K, a_i \in A$ e $b_i \in B$ com $i = 0, 1, 2$. Se os elementos $a_1, \cdots, a_s$ geram um K-módulo A e os elementos $b_1, \cdots, b_r$ geram um K-módulo B , então os sr elementos $a_i \otimes b_j$, $i = 1, \cdots, s$ e $j = 1, \cdots, r$, geram o K- módulo $A \otimes_K B$.

Sejam $\phi(n)$ a função de *Euler* com soma e produto usual dos números complexos e ω uma n-ésima raiz da unidade, podemos constrir o anel:

$$\mathbb{Z}[\omega] = \mathbb{Z} \bigoplus \mathbb{Z}\omega \bigoplus \cdots \bigoplus \mathbb{Z}\omega^{\phi(n)-1}.$$

Sejam L e $\mathbb{Z}[\omega]$ ambos $\mathbb{Z}$-módulos, com L um anel de Lie, definimos o produto tensorial $L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$ denotando por $L \otimes \mathbb{Z}[\omega]$. Para todo $k \in \mathbb{Z}[\omega]$ e $a \otimes b \in L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$, $L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$ é um $\mathbb{Z}[\omega]$-módulo, com o produto definido:

$$ka \otimes b = a \otimes kb$$

Podemos ainda definir o produto de Lie do anel de Lie $L \otimes \mathbb{Z}[\omega]$ como

$$[a_1 \otimes b_1, a_2 \otimes b_2] = [a_1, a_2] \otimes b_1 b_2$$

Dado um automorfismo φ do anel de Lie L de ordem finita n, podemos considerar φ um automorfismo em $L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$ agindo trivialmente em $\mathbb{Z}[\omega]$ de tal modo que dado $a \otimes_K b \in L \otimes \mathbb{Z}[\omega]$ então $(a \otimes b)^{\varphi} = a^{\varphi} \otimes b$.

Veremos um Lema que permite verificar algumas propriedades de $L \otimes \mathbb{Z}[\omega]$, estas serão importantes para demonstração de alguns resultados.

Lema 3.4.4. Sejam $\overline{L} = L \otimes \mathbb{Z}[\omega]$ o anel de Lie como definido acima e φ um automorfismo de L agindo em $\overline{L}$ da forma que descrevemos. Valem as seguintes propriedades:

1. $C_{\overline{L}}(\varphi) = C_L(\varphi) \otimes \mathbb{Z}[\omega]$;
2. $\overline{L}^{(i)} = L^{(i)} \otimes \mathbb{Z}[\omega]$;
3. $\gamma_i(p\overline{L}) = \gamma_i(pL) \otimes \mathbb{Z}[\omega]$.

Demonstração.

1. A inclusão $C_L(\varphi) \otimes \mathbb{Z}[\omega] \subseteq C_{\overline{L}}(\varphi)$ é imediata devido o descrito acima. Para outra inclusão, considere:
$$\overline{L} = \bigoplus_{i=0}^{\phi(n)-1} L \otimes \mathbb{Z}\omega^i.$$
Para $i = 0, \cdots, \phi(n)-1$ basta mostrarmos que $C_{\overline{L}}(\varphi) \cap L \otimes \mathbb{Z}\omega^i = C_L(\varphi) \otimes \mathbb{Z}\omega^i$. Observe que $C_{\overline{L}}(\varphi) \cap L \otimes 1 = C_L(\varphi) \otimes 1$, o que implica $C_{\overline{L}}(\varphi) \cap L \otimes \mathbb{Z} = C_L(\varphi) \otimes \mathbb{Z}$. Para todo $l \in L$ e $m \in \mathbb{Z}$ temos que $ml \otimes 1 = m \otimes l$ resultando $L \otimes \mathbb{Z} = L \otimes 1$. Assim, $L \otimes \mathbb{Z}\omega^i = L \otimes \mathbb{Z}$. Dado $\overline{l} \in C_{\overline{L}}(\varphi) \cap L \otimes \mathbb{Z}$ podemos considerar $\overline{l} = l \otimes \omega^i$ para algum $l \in L$
$$\omega^{n-1}\overline{l} = l \otimes 1 \in C_{\overline{L}}(\varphi)$$
resultando que $l \in C_L(\varphi)$. Portanto, $l \otimes \omega^i \in C_L(\varphi) \otimes \mathbb{Z}\omega^i$ e consequentemente $C_{\overline{L}}(\varphi) \cap L \otimes \mathbb{Z}\omega^i = C_L(\varphi) \otimes \mathbb{Z}\omega^i$ para todo $i = 0, \cdots, \phi(n)-1$.
2. Bastar fazermos por indução, lembrando $\overline{L}^{(1)} = [\overline{L}, \overline{L}] = [L \otimes \mathbb{Z}[\omega], L \otimes \mathbb{Z}[\omega]] = [L, L] \otimes \mathbb{Z}[\omega] = L^{(1)} \otimes \mathbb{Z}[\omega]$. Uma vez que $\overline{L}^{(1)} = [\overline{L}, \overline{L}]$ é gerado pelo conjunto $\{[x, y] \mid x, y \in \overline{L}\}$;
3. A demonstração é imediata por indução e lembrando que $\gamma_2(p\overline{L}) = (p\overline{L})^{(1)}$ e $\gamma_i(p\overline{L}) = [\gamma_{i-1}(p\overline{L}), \overline{L}]$.

□

3.4.1 Anéis de Lie Solúvel com Automorfismos Regulares

Para adentrar a teoria de automorfismos regulares apresentaremos dois resultados de álgebra linear. O primeiro é o Teorema da Forma Normal de Jordan e o segundo sobre certas condições garante um limite para os blocos de Jordan de uma Matriz, tais resultados podem ser encontrados em [12] e [13].

Teorema 3.4.5. (Teorema da Forma Normal de Jordan) Seja φ uma transformação linear de um espaço vetorial V de dimensão finita sobre um corpo F. Se todos os autovalores de φ pertencem a F, então V tem uma base na qual a matriz de φ está na forma normal de Jordan, isto é, sua matriz pode ser escrita na forma de blocos diagonais, com cada bloco na forma J_i,

$$J_i = \begin{pmatrix} \lambda_i & 1 & \dots & 0 \\ 0 & \lambda_i & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_i, \end{pmatrix}$$

com os λ_i autovalores de φ (não necessariamente distintos).

Teorema 3.4.6. Sejam p um número primo e φ um elemento de ordem p^k em um grupo de transformações lineares de um espaço vetorial V sobre um corpo F de característica p. Então todos os autovalores de φ são iguais a 1 e V tem uma F-base na qual a matriz de φ na forma normal de Jordan possui todos seus blocos de tamanho no máximo $p^k \times p^k$, e existe pelo menos um bloco de tamanho exatamente $p^k \times p^k$.

Para os próximos resultados, definimos o conjunto dos pontos fixos de um automorfismo φ de G por $C_G(\varphi) = \{g \in G; g^\varphi = g\}$. O automorfismo φ é dito regular se $C_G(\varphi) = 1$.

Teorema 3.4.7. Seja p um número primo. Se φ é um automorfismo de ordem p^k de um p-grupo abeliano não trivial G, então $C_G(\varphi) \neq 1$.

Demonstração. Considere o subgrupo não trivial de G

$$V = \langle g \in G : g^p = 1 \rangle$$

que pode ser considerado como um espaço vetorial sobre o corpo $\mathbb{F}_p$ e cujo V restrito a φ é uma transformação linear. Por hipótese φ é um automorfismo de ordem p^k então pelo teorema 3.4.6 φ possui todos seus autovalores iguais a 1. Portanto, os autovetores não triviais de φ associados ao autovalor 1 são elementos não triviais que pertencem a $C_G(\varphi)$. □

Definição 3.4.8. Dado um automorfismo φ. O subgrupo aditivo do anel de Lie $\tilde{L}$

$$^i\tilde{L} = \{l \in \tilde{L} | l^\varphi = w^i l\}$$

é chamada uma φ-componente de $\tilde{L}$ com relação a w^i. Os elementos das φ-componentes são chamados φ-homogêneo. Embora $\tilde{L}$ não seja um espaço vetorial, "quase todo $\tilde{L}$ se decompõe em uma soma quase direta"de componentes.

Definição 3.4.9. Um ideal I do anel de Lie $\tilde{L}$ é φ-homogêneo, se:

$$I = \sum_{i=0}^{n-1} I \bigcap {}^{i}\mathrm{L}.$$

Lema 3.4.10. As seguintes inclusões são verdadeiras:

1. $nL \subseteq {}^{0}L + {}^{1}L + \cdots + {}^{n-1}L$;
2. Se $l_0 + l_1 + \cdots + l_{n-1} = 0$, com $l_i \in {}^{i}L$ então $nl_j = 0$ para $j = 0, 1, \cdots, n-1$.
3. Se o grupo aditivo L não tem n-torção, isto é, para todo $l \in L$ a equivalência $nl = 0$ implica em $l = 0$, então a soma de φ-componentes é direta.

Demonstração.

1. Para cada $a \in L$ e cada $i = 0, 1, \cdots, n-1$ definamos ${}^{i}a = \sum_{s=0}^{n-1} w^{-is} a^{\varphi^s}$. Temos ${}^{i}a \in {}^{i}L$.

$$({}^{i}a)^{\varphi} = (\sum_{s=0}^{n-1} w^{-is} a^{\varphi^s})^{\varphi} = \sum_{s=0}^{n-1} w^{-is} a^{\varphi^{s+1}}) =$$
$$w^{i} \sum_{s=0}^{n-1} w^{-i(s+1)} a^{\varphi^{s+1}}) = w^{i} \sum_{r=0}^{n-1} w^{-ir} a^{\varphi^r}) = w^{i}\, {}^{i}a$$

   com $r = s+1$, por outro lado, lembremos que $w^n = 1$ e $\varphi^n = 1$, e assim:

$$\sum_{i=0}^{n-1} {}^{i}a = \sum_{i=0}^{n-1} \sum_{s=0}^{n-1} w^{-is} a^{\varphi^s} = \sum_{i=0}^{n-1} w^{-is} \sum_{s=0}^{n-1} a^{\varphi^s} = na$$

   pois para $s = 0$ temos:

$$\sum_{i=0}^{n-1} w^0 = \underbrace{w^0 + \cdot + w^0}_{\text{n-vezes}} = nw^0 = n$$

   Assim, se $s \neq 0 (mod n)$ temos:

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

   Logo:

$$w^s \sum_{i=0}^{n-1} w^{is} - \sum_{i=0}^{n-1} w^{is} = 0.$$

como $w^s \neq 1$, temos $\sum_{i=0}^{n-1} w^{is} = 0$.

2. Aplicando φ^k para $k = 0, \cdots, n-1$ em $\sum_{i=0}^{n-1} l_i = 0$

$$\begin{aligned}
&l_0 + l_1 + \cdots + l_{n-1} = 0 \\
&l_0 + l_1 w + \cdots + w^{n-1} l_{n-1} = 0 \\
&l_0 + l_1 w^2 + \cdots + w^{2(n-1)} l_{n-1} = 0 \\
&l_0 + l_1 W^{n-1} + l_2 w^{2(n-1)} + \cdots + l_{n-1} w^{(n-1)(n-1)} = 0
\end{aligned}$$

Como demonstramos no item anterior para casa $s \neq 0(modn)$, temos:

$$\sum_{i=0}^{n-1} w^{is} = 0.$$

Assim para cada i, devemos multiplicar as equações acima por uma potência de w adequada, por exemplo, para l_0 multiplicamos por w^n. E assim:

$$nl_i = 0.$$

3. Como L não tem n-torção, se tivermos:

$$l_0 + \cdots + l_{n-1} = a_0 + \cdots + a_{n-1}.$$

com l_i e $a_i \in {}^iL$, então

$$(l_1 - a_1) + \cdots + (l_{n-1} - a_{n-1}) = 0.$$

Pelo item anterior $n(l_j - a_j) = 0$ para todo $j = 0, 1, \cdots, n-1$. Portanto $l_j = a_j$.

□

Lema 3.4.11. Para todos i e j, temos

$$[{}^iL, {}^jL] \subseteq {}^{i+j}L.$$

Com $i + j$ é calculado módulo n. Em particular a soma das φ-componentes ${}^0L + {}^1L + \cdots + {}^{n-1}L$ é um subanel do anel de Lie L.

Demonstração. Para $a \in {}^{i}L$ e $b \in {}^{j}L$, temos:

$$[a,b]^{\varphi} = [w^i a, w^j b] = w^{i+j}[a,b].$$

E assim $[a,b] \in {}^{i+j}L$. □

Pelo lema anterior, se φ é um automorfismo de ordem n de um anel de Lie L e sabendo que a φ-componente ${}^{0}L$ é subanel de pontos fixos de φ, concluímos que o grupo aditivo do ideal ${}_{id}\langle C_L(\varphi)\rangle$ é gerado pelo comutadores simples que possuem um subcomutador $[{}^{i_1}x_i, {}^{i_2}x_2, \cdots, {}^{i_r}x_r]$, onde ${}^{i_j}x_j \in {}^{i_j}L$ e $i_0 + \cdots + i_r \equiv 0(modn)$.

Lema 3.4.12. Seja p um número primo e sejam $i_1, \cdots, i_k$ elementos não nulos em $\mathbb{F}_p$(não necessariamente distintos). Seja M o conjunto

$$M = \{\sum_{s\in S} i_s : S \subseteq \{1, \cdots, k\}\}.$$

Por definição, a soma é zero para $S = \varnothing$. Então, ou $M = \mathbb{Z}_p$ ou $|M| \geq k+1$.

Demonstração. Por indução sobre k, chamaremos $M(S)$ o conjunto de todas as somas envolvendo $\{i_1, \cdots, i_s\}$. Para $k = 1$, temos:

$$|M(1)| = |\{0, i_1\}| = 2,$$

Com $i_1 \neq 0$, como $M(k) \subseteq M(k+1)$, se $M(k) = \mathbb{F}_p$ então $M(k+1) = \mathbb{F}_p$. Assim basta provar que $|M(k)| \geq k+1$. Para isso seja $\sigma \in M(k)$ e suponha que alguma soma $\sigma + i_{k+1} \notin M(k)$. Então:

$$|M(k)+1| \geq |M(k)| + 1 \geq (k+1)+1.$$

Por outro lado, se toda soma $\sigma + i_{k+1} \in M(k)$, então por recorrência e tomado $\sigma = 0$ temos $i_{k+1}, 2i_{k+1} \cdots, (p-1)i_{k+1} \in M(k)$. Como $0, i_{k+1}, \cdots, (p-1)i_{k+1}$ são distintos (pois $\mathbb{F}_p$ não possui subgrupos próprios não triviais e $i_i \neq 0$), temos que $|M(k)| = |M(k+1)| = p$, ou seja, $M(k+1) = \mathbb{Z}_p$. □

Proposição 3.4.13. Para todo s temos:

1. $[\gamma_n(H'), \underbrace{H, \cdots, H}_{\text{(p-1)-fatores}}] \subseteq \gamma_{n+1}(H') + {}_{id}\langle {}^{0}L\rangle$, $n \geq 1$;
2. $\gamma_{(p-1)n+2}(H) \subseteq \gamma_{n+1}(H') + {}_{id}\langle {}^{0}L\rangle$, $n \geq 0$;
3. $\gamma_{f(p,s)+1}(H) \subseteq H^{(s)} + {}_{id}\langle {}^{0}L\rangle$,

com $f(p,s) = 1 + (p-1) + \cdots + (p-1)^{s-1} = \dfrac{(p-1)^s - 1}{p-2}$.

Demonstração.

1. Temos que H' e $\gamma_n(H')$ são ideais de H e são φ-homogêneos, ou seja,

$$H' = \sum_{i=0}^{p-1} H' \cap {}^{i}L \quad e \quad \gamma_n(H') = \sum_{i=0}^{p-1} \gamma_n(H') \cap {}^{i}L.$$

   Assim basta mostrar que:

$$[{}^{i_0}c_0, {}^{i_1}y_1, \cdots, {}^{i_{p-1}}y_{p-1}] \in \gamma_{n+1}(H') + {}_{id}\langle {}^{0}L \rangle.$$

   Para todo elemento φ-homogêneo ${}^{i_0}c \in \gamma_n(H') \cap {}^{i_0}L$ e ${}^{i_k}y \in {}^{i_k}L$. Podemos assumir que $i_r \neq 0$ para todo $r = 0, 1, \cdots, p-1$ temos $[{}^{i_0}c_0, {}^{i_1}y_1, \cdots, {}^{i_{p-1}}y_{p-1}] \in {}_{id}\langle {}^{0}L \rangle$. Note que toda permutação de elementos ${}^{i_1}y_1, \cdots, {}^{i_{p-1}}y_{p-1}$ não altera o comutador módulo o subgrupo $\gamma_{n+1}(H')$, isso ocorre pela identidade de Jacobi para $[a,b,c] = [a,c,b] + [a,[b,c]]$ e portanto, se $a \in \gamma_n(H')$ e $[b,c] \in H'$ então $[a,[b,c]]$. O objetivo é reorganizar os elementos ${}^{i_1}y_1, \cdots, {}^{i_{p-1}}y_{p-1}$ de modo a obter a congruência, pelo lema 3.4.12 rearranjando os indíces obtem-se qualquer elemento de $\mathbb{Z}_p$, para $\pi \in S_{p-1}$ temos:

$$i_0 + i_{\pi(1)} + \cdots + i_{\pi(s)} \equiv 0 (mod p).$$

   Podemos escrever o comutador $[{}^{i_0}c_0, {}^{i_1}y_1, \cdots, {}^{i_{p-1}}y_{p-1}]$ como a soma de um comutador com o segmento inicial ${}^{0}L$ e consequentemente ${}_{id}\langle {}^{0}L \rangle$.

2. A demonstração será feita por indução em n. Para $n = 0$, temos $\gamma_2(H) = [H,H] = \gamma_1(H')$ e para $n > 0$.

$$\gamma_{(p-1)n+2}(H) = \gamma_{(p-1)(n-1)+2+p-1}(H) = [\gamma_{(p-1)(n-1)+2}(H), \underbrace{H, \cdots, H}_{\text{(p-1)-fatores}}].$$

   Pela hipótese de indução e pelo item 1., temos:

$$[\gamma_{(p-1)(n-1)+2}(H), \underbrace{H, \cdots, H}_{\text{(p-1)-fatores}}] \subseteq [\gamma_n(H'), \underbrace{H, \cdots, H}_{\text{(p-1)-vezes}}] + {}_{id}\langle {}^{0}L \rangle \subseteq \gamma_{n+1}(H') + {}_{id}\langle {}^{0}L \rangle.$$

3. A demonstração será feita por indução sobre s. Para $s = 1$, temos:

$$\gamma_{f(p,1)+1}(H) \subseteq H^{(1)} + {}_{id}\langle {}^{0}L \rangle.$$

$\gamma_2(H) = H'$ e para $s > 1$ usamos $\dfrac{(p-1)^s - 1}{p-2} = (p-1)\dfrac{(p-1)^{s-1}-1}{p-2} + 1$ e pelo item anterior, temos:

$$\gamma_{f(p,s)+1}(H) = \gamma_{(p-1)(f(p,s-1))+2}(H) \subseteq \gamma_{f(p,s-1)+2}(H') +_{id} \langle {}^0L \rangle.$$

Usando a hipótese de indução no anel de Lie solúvel H', concluímos que:

$$\gamma_{f(p,s-1)+2}(H') \subseteq (H')^{(s-1)} +_{id} \langle {}^0L \rangle = H^{(s)} +_{id} \langle {}^0L \rangle.$$

□

Teorema 3.4.14. Se φ é um automorfismo regular de ordem prima p de um anel de Lie L, então para todo número natural $s \geq 1$ temos:

$$\gamma_{f(p,s)+1}(pL) \subseteq_{id} \langle C_L(\varphi) \rangle + L^{(s)},$$

com $f(p,s) = \dfrac{(p-1)^s - 1}{p-2}$.

Demonstração. Observe que $pL \subseteq H = {}^0L + {}^1L + \cdots + {}^{p-1}L$ e $H^{(s)} \subseteq L^{(s)}$. A demonstração segue pelo item 3. da proposição 3.4.13. □

Lema 3.4.15. Seja A um anel de Lie. Denotamos por nA o subanel gerado por todos os elementos da forma $na = \underbrace{a + a + \cdots + a}_{\text{n-fatores}}$, com $a \in A$. Então:

1. $(nA)^{(k)} = n^{2^k} A^{(k)}$;
2. $\gamma_k(nA) = n^k \gamma_k(A)$.

Demonstração. Faremos por indução em k.

1. Para $k = 1$ temos $(nA)^{(1)} = [nA, nA] = n^2[A,A] = n^2 A^{(1)}$. Suponha que vale para k, então por nossa hipótese de indução temos que $(nA)^{(k)} = n^{2^k} A^{(k)}$. Portanto:

$$(nA)^{(k+1)} = [(nA)^k, (nA)^k] = n^{2^k} n^{2^k} [A^{(k)}, A^{(k)}] = n^{2^{k+1}} A^{(k+1)}.$$

2. Para o primeiro passo de indução, temos pela linearidade do colchete de Lie que $\gamma_1(nA) = nA = n\gamma_1(A)$. Suponha que vale para k,logo $\gamma_k(nA) = n^k \gamma_k(A)$, assim pelo primeiro passo de indução e pela hipótese indutiva, temos:

$$\gamma_{k+1}(nA) = [\gamma_k(nA), nA] = nn^k [\gamma_k(A), A] = n^{k+1} \gamma_k(A).$$

□

Teorema 3.4.16. ***(Kreknin,Krostrikin)*** Se um anel de Lie L é solúvel de comprimento derivado s e admite um automorfismo regular φ de ordem prima p, então L é nilpotente e sua classe de nilpotência é no máximo $\dfrac{(p-1)^s-1}{p-2}$.

Demonstração. Por hipótese L admite um automorfismo regular φ e é solúvel de comprimento derivado s, ou seja, ${}^0L = 0$ e $L^{(s)} = 0$. Pelo teorema 3.4.14 $\gamma_{f(p,s)+1}(pL) = 0$ por outro lado pelo Lema 3.4.15, temos:

$$0 = \gamma_{f(p,s)+1}(pL) = p^{f(p,s)+1}\gamma_{f(p,s)+1}(L).$$

Em particular isso implica que o grupo aditivo abeliano $\gamma_{f(p,s)+1}(L)$ é um p-grupo φ-invariante. Pelo teorema 3.4.7 aplicado a $\gamma_{f(p,s)+1}(L)$, supondo que $\gamma_{f(p,s)+1}(L)$ não seja trivial, então $C_L(\varphi) \subseteq C_{\gamma_{f(p,s)+1}(L)}(\varphi) \neq 1$ contrariando a hipótese, logo $\gamma_{f(p,s)+1}(L) = 0$. □

3.4.2 Anéis de Lie com Automorfismos Regulares

Nessa seção considere φ um automorfismo de ordem n e $f(n) = 2^{n-1} - 1$. O objetivo é demonstrar que nessas condições $(nL)^{(f)} \subseteq {}_{id}\langle {}^0L\rangle$ e com isso demonstrar o resultado de ***Higman, Kreknin e Krostrikin***. Assim como na seção anterior demonstraremos que podemos assumir sem perda de generalidade para $L = \tilde{L}$. Logo:

$$(nL)^{(f)} \otimes 1 = (n\tilde{L})^{(f)} \cap L \otimes 1 \subseteq {}_{id}\langle {}^0L\rangle \otimes_{\mathbb{Z}} \mathbb{Z}[\omega] \cap L \otimes 1 = {}_{id}\langle {}^0L\rangle \otimes 1.$$

Lema 3.4.17. Suponha que a, b e c sejam números naturais tais que $1 \leq a, b, c \leq n-1$. Se $a+b \equiv c(mod n)$, então ou ambos $a > c$ e $b > c$ ou ambos $a < c$ e $b < c$.

Demonstração. Como $a < n$ e $b < n$, temos $a+b < 2n$. Então $a+b = c$ ou $a+b = c+n$. No primeiro caso, claramente $a < c$ e $b < c$, enquanto no segundo ambos são maiores que c, pois caso contrário se algum fosse menor que c, digamos $a < c$, então como $b < n$ teríamos $a+b < c+n$, o que contraria o raciocínio anterior. Portanto, ou ambos $a > c$ e $b > c$ ou ambos $a < c$ e $b < c$. □

Proposição 3.4.18. Suponha que ω seja uma raiz n-ésima da unidade e que o anel de Lie H sobre $\mathbb{Z}[\omega]$ admita um automorfismo φ de ordem n, com H decomposto em soma direta de φ-componentes do seguinte modo:

$$H = {}^0H \oplus {}^1H \oplus \cdots \oplus {}^{n-1}H.$$

Então, para todo $k = 0, 1, \cdots, n-1$.

1. $H^{(2^k-1)} \cap^k H \subseteq \langle {}^{k+1}H, {}^{k+2}H, \cdots, {}^{n-1}H \rangle + {}_{id}\langle {}^0H \rangle$;
2. $H^{(2^k-1)} \subseteq \langle {}^{k+1}H, {}^{k+2}H, \cdots, {}^{n-1}H \rangle + {}_{id}\langle {}^0H \rangle$;
3. $H^{(2^{n-1}-1)} \subseteq {}_{id}\langle {}^0H \rangle$.

Demonstração. Os itens 1 e 2 são demonstrados simultaneamente por indução em k. Para $k = 1$ temos

$$H^{(s)} \cap^w H = \sum_{u+v=w} [H^{(s-1)} \cap^u H, H^{(s-1)} \cap^v H],$$

Logo $H' \cap^1 H$ é gerado por todos os comutadores $[x,y]$ com $x \in {}^i H$, $y \in {}^j H$ e $i + j \equiv 1(modn)$. Se i ou j é igual 0, temos $[x,y] \in {}_{id}\langle {}^0H \rangle$. Se ambos são maiores que 0, pelo Lema 3.4.17, ambos são maiores que 1 e assim $[x,y] \in \langle {}^2H, {}^3H, \cdots, {}^{n-1}H \rangle$. Para o item 2, temos $H' = \bigoplus_{i=0}^{n-1} H' \cap^i H$ e do fato ${}^iH \subseteq \langle {}^2H, {}^3H, \cdots, {}^{n-1}H \rangle + {}_{id}\langle {}^0H \rangle$, para $i = 0, 1, 2, \cdots, n-1$, junto com o item 1, temos $H' \cap^i H \subseteq \langle {}^2H, {}^3H, \cdots, {}^{n-1}H \rangle + {}_{id}\langle {}^0H \rangle$ para todo i. Portanto, $H' \subseteq \langle {}^2H, {}^3H, \cdots, {}^{n-1}H \rangle + {}_{id}\langle {}^0H \rangle$.

Para $k > 1$ provamos 1. usando as hipoteses de indução de 1. e 2.. O subanel $H^{(2^{k-1})} \cap^k H$ é gerado por todos os comutadores $[x,y]$, com $x \in H^{(2^{k-1}-1)} \cap^i H$,$y \in H^{(2^{k-1}-1)} \cap^j H$ e $i + j \equiv k(modn)$. Se algum i, j é igual a zero, então $[x,y] \in {}_{id}\langle {}^0H \rangle$. Se ambos são maiores que zero, então pelo Lema 3.4.17 ou ambos são maiores que k ou ambos são menores que k. O primeiro caso é imediato. Já o segundo caso, aplicamos 2. ao subanel $H^{(2^{k-1}-1)}$ o qual contém x e y:

$$H^{(2^{k-1}-1)} \subseteq \langle {}^{k+1}H, {}^{k+2}H, \cdots, {}^{n-1}H \rangle + {}_{id}\langle {}^0H \rangle$$

Assim, o elemento $y \in H^{(2^{k-1}-1)}$ é igual módulo ${}_{id}\langle {}^0H \rangle$ a uma combinação linear da forma

$$[u_1, u_2, \cdots, u_q], u_s \in {}^{i_s} H, i_s \geq k \quad \sum_{s=1}^{q} i_s \equiv j(modn).$$

Aplicando a identidadede de Jacobi $[a,[b,c]] = [a,b,c] - [a,c,b]$ repetidas vezes, todo comutador $[x,[u_1,u_2,\cdots,u_q]]$ pode ser expresso como combinação linear de comutadores simples da forma

$$[x, u_{\pi(1)}, \cdots, u_{\pi(q)}], \quad com \ \ \pi \in S_q.$$

Logo o comutador $[x,y]$ é igual módulo ${}_{id}\langle {}^{0}H\rangle$ a uma combinação linear de comutadores simples da forma

$$[x,v_1,v_2,\cdots,v_q], v_s \in {}^{j_s}H,\ j_s \geq k \quad \sum_{s=1}^{q} j_s \equiv j(modn),$$

Onde é satisfeito

$$i+j_1+j_2+\cdots+j_q \equiv k(modn), pois \quad i+j \equiv k(modn).$$

Se tivermos $j_q = k$, então

$$i+j_1+j_2+\cdots+j_{q-1} \equiv 0(modn).$$

Significando $[x,v_1,v_2,\cdots,v_{q-1}] \in {}^{0}H$. Consequentemente,

$$[x,v_1,v_2,\cdots,v_q] \in {}_{id}\langle {}^{0}H\rangle.$$

Se, no entanto, $j_q > k$ então temos

$$i+j_1+j_2+\cdots+j_{q-1} \equiv t \not\equiv 0(modn).$$

E pelo Lema 3.4.17, temos $t > k$. Assim,

$$[x,v_1,v_2,\cdots,v_{q-1},v_q] \in \langle {}^{t}H, {}^{j_q}H\rangle \subseteq \langle {}^{k+1}H, {}^{k+2}H,\cdots, {}^{n-1}H\rangle.$$

Logo, em todos os casos, os comutadores $[x,v_1,v_2,\cdots,v_{q-1},v_q]$ estão contidos em

$$\langle {}^{k+1}H, {}^{k+2}H,\cdots, {}^{n-1}H\rangle + {}_{id}\langle {}^{0}H\rangle.$$

Portanto, este subanel também contém $[x,y]$, como desejado. Agora para o item 2. usamos a hipótese de indução para $k-1$ no anel de Lie $H^{(2^{k-1})}$:

$$(H^{(2^k-1)})^{(2^{k-1}-1)} \subseteq \langle H^{(2^{k-1})} \cap^{k} H, H^{(2^{k-1})} \cap^{k+1} H,\cdots, H^{(2^{k-1})} \cap^{n-1} H\rangle + {}_{id}\langle {}^{0}H\rangle.$$

Os subgrupos aditivos $H^{(2^{k-1})} \cap^{k} H, H^{(2^{k-1})} \cap^{k+1} H,\cdots, H^{(2^{k-1})} \cap^{n-1} H$ estão contidos no subanel $\langle {}^{k+1}H,\cdots, {}^{n-1}H\rangle$, que pelo item 1. também contém o subgrupo aditivo $H^{(2^k-1)} \cap^{k} H$. Portanto,

$$H^{(2^k-1)} = (H^{(2^k-1)})^{(2^{k-1}-1)} \subseteq \langle {}^{k+1}H,\cdots, {}^{n-1}H\rangle + {}_{id}\langle {}^{0}H\rangle.$$

como queríamos. Para demonstrar o item 3 basta refazer o item 2. colocando $k = n-1$. □

Teorema 3.4.19. Seja n um número natural e $f(n) = 2^{2^{n-1}-1}$. Se ${}^{i_1}y_1, {}^{i_2}y_2, \cdots, {}^{i_{f(n)}}y_{f(n)}$ são alguns elementos de um anel de Lie arbitrário com índices superiores arbitrários $i_1, i_2, \cdots, i_f(n) \in \mathbb{Z}$, então o comutador

$$\delta_{2^{n-1}-1}({}^{i_1}y_1, {}^{i_2}y_2, \cdots, {}^{i_{f(n)}}y_{f(n)})$$

pode ser representado como uma combinação linear de comutadores cada qual possuindo o mesmo conjunto de entradas ${}^{i_1}y_1, {}^{i_2}y_2, \cdots, {}^{i_{f(n)}}y_{f(n)}$ e contendo um subcomutador com índices superiores de soma igual a zero módulo n.

Demonstração. Seja ω uma raiz p-ésima da unidade e seja F um anel de Lie livre sobre $\mathbb{Z}[\omega]$ com geradores livres ${}^{i_1}y_1, {}^{i_2}y_2, \cdots, {}^{i_{f(n)}}y_{f(n)}$. Para cada $i = 1, 2, \cdots, n-1$, denotamos por ${}^{i}F$ o subgrupo aditivo de F gerado por todos os comutadores nos geradores livres ${}^{i_1}y_1, {}^{i_2}y_2, \cdots, {}^{i_{f(n)}}y_{f(n)}$, tais que a soma dos índices superiores de suas entradas é igual a i módulo n. Definimos um automorfismo φ de F de ordem n colocando $l^{\varphi} = \omega^i l$ para todo $l \in {}^{i}F$, $i = 0, 1, \cdots, n-1$, e por linearidade a ação se estende para a soma $F = \sum_i {}^{i}\mathrm{F}$. Dessa forma os subgrupos aditivos ${}^{i}F$ são as φ-componentes. Como o grupo aditivo F não possui torção, pelo item 3 do Lema 3.4.10, temos

$$F = {}^{0}F \oplus {}^{1}F \oplus \cdots \oplus {}^{n-1}F.$$

Pela Proposição 3.4.18, item 3. segue que

$$\delta_{2^{n-1}-1}({}^{i_1}y_1, {}^{i_2}y_2, \cdots, {}^{i_{f(n)}}y_{f(n)}) \in {}_{id}\langle {}^{0}H \rangle.$$

□

Teorema 3.4.20. Se φ é um automorfismo de ordem finita n de um anel de Lie L, então

$$(nL)^{(f(n))} \subseteq {}_{id}\langle {}^{0}L \rangle.$$

Com ${}^{0}L = \{l + l^{\varphi} + l^{\varphi^2} + \cdots + l^{\varphi^{n-1}} : l \in L\}$ e $f(n) = 2^{n-1} - 1$.

Demonstração. Pelo Lema 3.4.10, $nL \subseteq {}^{0}L + {}^{1}L + \cdots + {}^{n-1}L$ e , portanto, pelo Teorema 3.4.19 temos

$$(nL)^{(f(n))} \subseteq {}_{id}\langle {}^{0}L \rangle.$$

□

Corolário 3.4.21. Suponha o grupo aditivo de L, admita um automorfismo regular de ordem finita n.

a Se o grupo aditivo de L não possui n-torção (ou seja, $nl = 0$ implica $l = 0$), então L é solúvel de comprimento derivado no máximo $2^{n-1} - 1$.

b Se n é um número primo, então L é solúvel de comprimento derivado no máximo $2^{n-1} - 1$.

Demonstração.

a Pelo Teorema 3.4.20, temos

$$n^{2^{2^{n-1}-1}} L^{2^{n-1}-1} = (nL)^{2^{(n-1)}-1} \subseteq {}_{id}\langle {}^0L\rangle \subseteq {}_{id}\langle C_L(\varphi)\rangle = 0.$$

Portanto

$$n(n^{2^{2^{n-1}-2}} L^{2^{n-1}-1}) = 0.$$

e como L não possui n-torção, obtemos $n^{2^{2^{n-1}-2}} L^{2^{n-1}-1} = 0$ Procedendo do mesmo modo, temos $L^{2^{n-1}-1} = 0$.

b Se $n = p$ é primo, suponha que $L^{2^{n-1}-1} \neq 0$ isso diz que $L^{2^{n-1}-1}$ é p-grupo abeliano não trivial. Logo, pelo Teorema 3.4.7, φ possui um ponto fixo não trivial. Portanto, necessariamente $L^{2^{n-1}-1} = 0$.

□

O próximo teorema permite obter um limite superior para classe de solubilidade de L e esse só depende da ordem de um automorfismo regular que é n.

Teorema 3.4.22. ***(Kreknin)*** Se um anel de Lie L admite um automorfismo regular de ordem n, então L é solúvel e seu comprimento derivado não é maior que $2^n - 2$.

Demonstração. Sejam L um anel de Lie, $\varphi \in Aut(L)$ com $|\varphi| = n$ e $C_L(\varphi) = 0$. Defina

$$T = \{a \in L : n^k a = 0, \text{para algum } \ k = k(a) \in \mathbb{N}\}$$

Claramente T é um ideal φ-invariante. Pelo Teorema 3.4.20,

$$0 = (nL)^{f(n)} = n^{f(n)} L^{(2^{n-1}-1)},$$

com $f(n) = 2^{2^{n-1}-1}$. Assim, $L^{(2^{n-1}-1)} \subseteq T$. Logo é suficiente mostrar que $T^{(2^{n-1}-1)} = 0$ pois,

$$L^{(2^n-2)} = (L^{(2^{n-1}-1)})^{(2^{n-1}-1)} \subseteq T^{(2^{n-1}-1)} = 0$$

Como todo elemento de T possui ordem finita e igual a uma potência de n, podemos decompor o grupo periódico abeliano T em uma soma direta de seus subgrupos de Sylow.

$$T = T_{p_1} \oplus T_{p_2} \oplus \cdots \oplus T_{p_r}$$

com $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ a decomposição de potências de primos. Note que estes subgrupos de Sylow são subanéis φ-invariantes e $[x_i, x_j] \neq 0$ com $x_i \in T_{p_i}$ e $x_j \in T_{p_j}$, com $i \neq j$. Então é suficiente provar que cada subanel T_{p_i} é solúvel de comprimento no máximo $2^n - 1$. Temos $n = p^k s$, $p \in \{p_1, p_2, \cdots, p_r\}$ e $(p,s) = 1$. Podemos obter a seguinte decomposição $\langle\varphi\rangle = \langle\varphi\rangle_p \oplus \langle\varphi\rangle_{p'}$ com $|\langle\varphi\rangle_p| = |\langle\varphi^s\rangle| = p^k$ e $|\langle\varphi\rangle_{p'}| = |\langle\varphi^{p^k}\rangle| = s$. Então $C_{T_p}(\varphi^{p^k}) = 0$, pois se $C_{T_p}(\varphi^{p^k}) = A \neq 0$, temos $C_A(\varphi^s) \neq 0$, uma vez que $|\langle\varphi^s\rangle| = p^k$ e A é φ^s-invariante (veja Teorema 3.4.7). Logo,$C_{T_p}(\varphi^{p^k}) \cap C_{T_p}(\varphi^{p^s}) = C_{T_p}(\varphi) \neq 0$, o que é uma contradição. Portanto, $C_{T_p}(\varphi^{p^k}) = 0$. Assim T_p admite um automorfismo regular φ^{p^k} de ordem coprima com todos os elementos de seu grupo aditivo, logo pelo item *a.* do Corolário 3.4.21, T_p é solúvel de comprimento derivado no máximo $2^{n-1} - 1$. □

Corolário 3.4.23. ***(Higman, Kreknin e Kostrikin)*** Se um anel de Lie admite um automorfismo regular de ordem prima p, então ele é nilpotente e sua classe de nilpotência é limitada por algum número $h(p)$, com esse dependendo somente de p.

Demonstração. Dado um anel de Lie L que admite um automorfismo de ordem prima p. Pelo item *b.* do Corolário 3.4.21 L é solúvel de comprimento derivado no máximo $2^{p-1} - 1$ e, portanto, pelo Teorema 3.4.16, temos que L é nilpotente de classe no máximo $\dfrac{(p-1)^{2^{p-1}-1} - 1}{p-2}$. □

A função $h(p)$ é chamada de função de *Higman*, e a mesma é utilizada em outros trabalhos.

Capítulo 4

Nilpotência de Grupos admitindo um Grupo de *Frobenius* como Grupo de Automorfismo.

Este capítulo é destinado a apresentar uma solução positiva para o item 1 do **Problema 17.72** do *The Kourovka Notebook* [21] dada no artigo *Frobenius Groups As Groups of Automorphisms* [19] por N. Yu. Makarenko e P. Shumyatsky.

Teorema 4.0.1. Seja FH um grupo de *Frobenius* com núcleo F e complemento H. Suponha que FH age em um grupo finito G de modo que GF é um grupo com *Frobenius* de núcleo G e complemento F. A classe de nilpotência de G é limitada em termos $|H|$ e da classe de nilpotência do $C_G(H)$.

Para isso estudaremos primeiro condições combinatórias em Álgebra de Lie graduadas.

4.1 Álgebras de Lie Graduadas: Uma condição combinatória.

Seja q um inteiro positivo arbitrário mas fixado. Escolha um primo p tal que $r^q \equiv 1(mod\, p)$. Considere $a_1, \cdots, a_k$ elementos não necessariamente distintos e não nulos em $\mathbb{Z}/p\mathbb{Z}$.

Definição 4.1.1. A sequência $(a_1, \cdots, a_k)$ é dita r-dependente se e somente se existe distintos $i_1, \cdots, i_m \in \{1, 2, \cdots, k\}$ e $\alpha_1, \cdots, \alpha_m \in \{1, 2, \cdots, q-1\}$ não necessariamente distintos, tais que

$$a_{i_1} + \cdots + a_{i_m} = r^{\alpha_1} a_{i_1} + \cdots + r^{\alpha_m} a_{i_m}.$$

Se a sequência $(a_1, \cdots, a_k)$ não é r-dependente, chamamos de **r-independente**.

Denote por F_k o conjunto de todas sequências r-independentes de comprimento k e por Z_k o conjuntos de todos dependentes de r. Para a sequência $(d_1, \cdots, d_k) \in F_k$ denote por $M(d_1, \cdots, d_k)$ o conjunto de todos $j \in \mathbb{Z}/p\mathbb{Z}$ tal que $(d_1, \cdots, d_k, j) \in Z_{k+1}$.

Lema 4.1.2. Se $(d_1, \cdots, d_k) \in F_k$ então $|M(d_1, \cdots, d_k)| \leq q^{k+1}$.

Demonstração. Suponha que $(d_1, \cdots, d_k, j) \in Z_{k+1}$. Temos:

$$d_1 + d_2 + \cdots + d_k + j = r^{i_1} d_1 + \cdots + r^{i_k} d_k + r^{i_0} j.$$

Para adequado $0 \leq i_s \leq q-1$, com não todos os i_s iguais a 0. Note que $i_0 \neq 0$, pois caso contrário a sequência seria r-independente. Vemos que

$$j = \frac{r^{i_1} d_1 + \cdots + r^{i_k} d_k - d_1 - d_2 - \cdots - d_k}{1 - r^{i_0}}$$

Como para os i_s tem q possibilidades e a sequência $(d_1, \cdots, d_k, j) \in Z_{k+1}$ de comprimento $k+1$, temos q^{k+1} possibilidades para j. □

Lema 4.1.3. Seja K um corpo de característica 0 contendo uma raiz primitiva da unidade ω. Suponha que para soma de inteiros positivos m e alguns $0 \leq i_1, \cdots, i_m \leq q-1$ temos $m = \omega^{i_1} + \cdots + \omega^{i_m}$. Então $i_1 = \cdots = i_m = 0$.

Demonstração. Sem perda de generalidade podemos supor $K = \mathbb{Q}[\omega]$. Como $m = |\omega^{i_1}| + \cdots + |\omega^{i_m}|$, pela desigualdade triangular temos $i_1 = \cdots = i_m = 0$. □

Lema 4.1.4. [19, Lema 2.3] Se a sequência $(a_1, \cdots, a_k)$ é r-dependente e $a_1 = \cdots = a_k$ então $p \leq n^{q-1}(2q-2)!$.

Os próximos resultados apresentam uma condição suficiente para concluir que a sequência $(a_1, \cdots, a_k)$ contém uma subsequência r-independente.

Lema 4.1.5. Suponha que para algum m a sequência $(a_1, \cdots, a_n)$ contém no máximo $q^m + m$ valores diferentes. Então pode-se escolher uma subsequência r-independente $(a_1, a_{i_1}, \cdots, a_{i_m})$ de m elementos que contenha a_1.

Demonstração. Se $m = 1$, o Lema está demonstrado, mostraremos por indução em m. Por indução podemos escolher uma subsequência r-independente $(a_1, a_{i_1}, \cdots, a_{i_{m-1}})$ de $m-1$ elementos. Sem perda de generalidade podemos supor $i_2 = 2, \cdots, i_{m-1} = m-1$. Portanto, $(a_1, a_2, \cdots, a_{m-1})$ é uma subsequência r-independente. Pelo Lema 4.1.2 existe no máximo

q^m elementos distintos $M(a_1, a_2, \cdots, a_{m-1})$. Por hipótese temos que a sequência $(a_1, \cdots, a_n)$ contém no máximo $q^m + m$ valores diferentes. Assim, a sequência $a_m, a_{m+1}, \cdots, a_n$ contém no máximo $q^m + 1$ valores diferentes. Então podemos sempre escolher b entre $a_m, a_{m+1}, \cdots, a_n$ tal que a sequência $a_1, a_2, \cdots, a_{n-1}, b$ é r-independente. □

Seja $i \in \mathbb{Z}/p\mathbb{Z}$, denotamos um elemento homogêneo na componente graduada L_i com indíce indicando a componente a qual esse elemento pertence, $x_i \in L_i$. Não usaremos índices de numeração para elementos de L_i, de modo que diferentes elementos possam ser denotados pelo mesmo símbolo quando só importa a qual componente os elementos pertencem, ou seja, x_i e x_i podem ser elementos diferentes de L_i, de modo que $[x_i, x_i]$ pode ser um elemento diferente de zero de L_{2i}. Note que sob essa convenção de índice, um comutador homogêneo pertence a componente L_s, onde s é a soma dos índices de todos os elementos envolvidos neste comutador.

No que segue assumimos que existe um inteiro positivo c tal que o anel L satisfaz a condição que:

$$[x_{d_1}, \cdots, x_{d_{c+1}}] = 0$$

sempre que $(d_1, \cdots, d_{c+1}) \in F_{c+1}$.

Lema 4.1.6. Para cada $b \in \mathbb{Z}/p\mathbb{Z}$ existem no máximo

$$max\{q^{c+1}, c^{q-1}(2q-2)!\}$$

elementos $a \in \mathbb{Z}/p\mathbb{Z}$ tal que $[L_a, \underbrace{L_b, \cdots, L_b}_{\text{c}}] \neq 0$.

Demonstração. Suponha que $[L_a, \underbrace{L_b, \cdots, L_b}_{\text{c}}] \neq 0$. Então a sequência $(a, \underbrace{b, \cdots, b}_{\text{c}})$ pertence a Z_{c+1} e temos $a + b + \cdots + b = r^{i_0}a + r^{i_1}b + \cdots + r^{i_c}b$ para um adequado $0 \leq i_j \leq q-1$ com pelo menos um $i_j \neq 0$. Se $i_0 \neq 0$, vemos que:

$$a = \frac{r^{i_1}b + \cdots + r^{i_c}b - cb}{1 - r^{i_0}}$$

Há q^{c+1} possibilidades para a pelo argumento usado no Lema 4.1.2. Se $i_0 = 0$, então para alguns $1 \leq m \leq c$ e algum $1 \leq j_1, \cdots, j_m \leq q-1$, temos $m = r^{j_1} + \cdots + r^{j_m}$. Neste caso, o Lema 4.1.4 $p \leq n^{q-1}(2q-2)!$. □

Lema 4.1.7. Existe um número w (c,d)-limitado tal que para todo $a,b \in \mathbb{Z}/p\mathbb{Z}$ temos $[L_a,\underbrace{L_b,\cdots,L_b}_{\text{w}}] = 0$.

Demonstração. Seja $b \in \mathbb{Z}/p\mathbb{Z}$, denotamos por $N(b)$ o conjunto de todos $a \in \mathbb{Z}/p\mathbb{Z}$ tal que $[L_a,\underbrace{L_b,\cdots,L_b}_{\text{c}}] \neq 0$. De acordo com o Lema 4.1.6, $N = |N(b)| \leq max\{q^{c+1}, c^{q-1}(2q-2)!\}$. Se para todo $t \geq 1$ temos $[L_a,\underbrace{L_b,\cdots,L_b}_{\text{c+1}}] \neq 0$, então todos elementos $a, a+b, a+2b, a+tb$ pertence a $N(b)$. Resultando que $[L_a,\underbrace{L_b,\cdots,L_b}_{\text{c+N}}] = 0$ para todo $a \in \mathbb{Z}/p\mathbb{Z}$ ou $tb = 0$ para todo $t \leq N$. No último caso concluímos que $p \leq N$. Claramente, para todo a,b existe, um inteiro s tal que $0 \leq s \leq p-1$ e $a+sb = 0$. Portanto $[L_a,\underbrace{L_b,\cdots,L_b}_{\text{N-1}}] = 0$ □

Escolha $(d_1,\cdots,d_c) \in F_c$ e fixe um comutador $U = [u_{d_1},\cdots,u_{d_c}]$

Lema 4.1.8. Todo comutador da forma

$$[U, x_{i_1},\cdots,x_{i_t}] \tag{4.1}$$

pode ser escrito como combinação linear de comutadores da forma

$$[U, m_{j_1},\cdots,m_{j_k}] \tag{4.2}$$

com $j_s \in M(d_1,\cdots,d_c)$ e $h \leq t$. No caso $t = h$ é possível se $i_s \in M(d_1,\cdots,d_c)$ para todo $s = 1,\cdots,t$.

Demonstração. Para $t = 0$ é óbvio, pois o comutador (4.1) se resume $[u_{d_1},\cdots,u_{d_c}]$. Seja $t = 1$ e $i_1 \in M(d_1,\cdots,d_c)$ então $[U,x_{i_1}] = [[u_{d_1},\cdots,u_{d_c}],x_{i_1}]$ é da forma requerida. Se $i_1 \notin M(d_1,\cdots,d_c)$ então $[U,x_{i_1}] = 0$ por 4.1.

Assuma que $t > 1$ e use indução em t. Se todos os índices $i_j \in M(d_1,\cdots,d_c)$ então o comutador $[U,x_{i_1},\cdots,x_{i_t}]$ estão na forma requerida com $h = t$. Suponha que em (4.1) exista um elemento x_{i_k} com índice $i_k \notin M(d_1,\cdots,d_c)$. Escolhemos um elemento k tão pequeno quanto possível e usamos k como segundo parâmetro de indução. Se $k = 1$, o comutador (4.1) é zero e está provado. Suponha que $k \geq 2$ e escreva

$$[U,\cdots,x_{i_{k-1}},x_{i_k},\cdots,x_{i_t}] = [U,\cdots,x_{i_k},x_{i_{k-1}},\cdots,x_{i_t}] + [U,\cdots,[x_{i_{k-1}},x_{i_k}],\cdots,x_{i_t}]$$

A hipótese de indução diz que o comutador $[U,\cdots,[x_{i_{k-1}},x_{i_k}],\cdots,x_{i_t}]$ é uma combinação linear de comutadores da forma (4.2) pois é menor que (4.1). Por outro lado, o comutador

$[U,\cdots,x_{i_k},x_{i_{k-1}},\cdots,x_{i_t}]$ é uma combinação linear de comutadores da forma (4.2), pois o índice não pertence a $M(d_1,\cdots,d_c)$ □

Corolário 4.1.9. O ideal de L gerado por U é a subálgebra gerada por comutadores da forma (4.2).

A partir do corolário acima, desejamos obter informações detalhadas sobre o ideal gerado por U. Assim, sejam $M = |M(d_1,\cdots,d_c)|$ e w da forma do Lema 4.1.8.

Lema 4.1.10. O ${}_{id}\langle U\rangle$ é a subálgebra gerada por todos os comutadores da forma (4.2) com $h \leq (w-1)M$.

Demonstração. Se R é a subálgebra gerada por comutadores da forma (4.2) com $h \leq (w-1)M$. É suficiente mostrar que todo comutador da forma (4.2) pertence a R. Então escolha um comutador $W = [U, m_{j_1},\cdots,m_{j_h}]$ da forma (4.3). Se $h \leq (w-1)M$ é claro que $W \in R$, assuma que $h > (w-1)M$ e use indução em h. Escreva

$$[U,\cdots,x_{i_{k-1}},x_{i_k},\cdots,x_{i_t}] = [U,\cdots,x_{i_k},x_{i_{k-1}},\cdots,x_{i_t}] + [U,\cdots,[x_{i_{k-1}},x_{i_k}],\cdots,x_{i_t}]$$

Se $j_{t-1}+j_t \in M(d_1,\cdots,d_c)$, então a segunda soma é da forma (4.2). Como este é menor que W, este pertence a R por hipótese indutiva. Se $j_{t-1}+j_t \notin M(d_1,\cdots,d_c)$, aplicando o Lem 4.1.8 e concluímos que a segunda soma pode ser escrita como combinação linear de comutadores da forma (4.2).

Portanto, neste caso $[U,\cdots,[x_{i_{k-1}},x_{i_k}],\cdots,x_{i_t}] \in R$. Segue que o comutador W não muda módulo R por nenhuma permutação m_{j_k}. Por nossa suposição o número h é grande o suficiente para garantir que entre os elementos m_{j_k} há pelo menos w que não pertence a componente L_i. Como W não muda módulo R por nenhuma permutação m_{j_k}, sem perda de generalidade podemos assumir $m_{j_1},\cdots,m_{j_w} \in L_i$. Mas agora pelo Lema 4.1.7 temos que $W = 0$. □

Corolário 4.1.11. O ideal ${}_{id}\langle[L_{d_1}\cdots,L_{d_c}]\rangle$ tem uma quantidade (c,q)-limitada de componentes não-triviais na graduação induzida.

Demonstração. Como em (5.2) $j_i \in M(d_1,\cdots,d_c)$ para todo $i = 1,\cdots,h$ a soma de todos os índices em (5.2) assumi valores no máximo M^h. Pelos Lemas 4.1.2 e 4.1.7 o número h é (c,q)-limitado. Então ${}_{id}\langle U\rangle$ tem (c,q)-limitadas componentes não triviais. Pelas provas dos Lemas 4.1.8 e 4.1.10 temos que o conjunto das possibilidades das componentes não-triviais no ${}_{id}\langle U\rangle$ é completamente determinada pela n-upla $(d_1,\cdots,d_c)$ e não depende da escolha de $U = [u_{d_1},\cdots,u_{d_c}]$. Como o ideal ${}_{id}\langle[L_{d_1}\cdots,L_{d_c}]\rangle$ é a soma do ideais ${}_{id}\langle[u_{d_1}\cdots,u_{d_c}]\rangle$. □

Lema 4.1.12. Suponha que um ideal homogêneo T de L tem apenas e componentes não-triviais. Então L tem no máximo e^2 componentes que não centralizam T.

Demonstração. Seja $T_{i_1},\cdots,T_{i_e}$ componentes homogêneas não-triviais de T. Então para alguns $j \in S$ temos $i+j \in S$. Então há no máximo $|S|\times|S|$ possibilidades para i. □

Proposição 4.1.13. O anel L é solúvel com classe (c,q)-limitada.

Demonstração. Se $c=0$ então $L=0$ por 4.1 e está provado. Assuma que $c \geq 1$ e use indução em c. Seja I o ideal de L gerado por todos comutadores $[L_{i_1},\cdots,L_{i_c}]$ com $(i_1,\cdots,i_c)$ variando em de F_c. A hipótese de indução diz que L/I é solúvel com comprimento derivado f_0.

Escolha $(i_1,\cdots,i_c) \in F_c$ e seja $T = {}_{id}\langle [L_{d_1}\cdots,L_{d_c}]\rangle$, pelo Corolário 4.1.11 o número de componentes da graduação não-triviais em T é (c,q)-limitado. Pelo Lema 4.1.12 existem no máximo e^2 componentes que não centralizam T. Como $C_L(T)$ é um ideal homogêneo, segue que o quociente $L/C_L(T)$ tem no máximo e^2 componentes não-triviais. Pelo Teorema de Aner Shalev [24], temos que $L/C_L(T)$ é solúvel de comprimento e-limitado, digamos f_1. Portanto $L^{(f_1)}$, corresponde ao termo da série derivada, centraliza T. Como f_1 não depende da escolha da n-upla $(i_1,\cdots,i_c) \in F_c$, segue que $[L^{f_1},I]=0$. Lembre-se que $L^{(f_0)} \leq I$. Assim, $[L^{f_0},L^{f_1}]=0$. Deduzimos que L é solúvel de comprimento derivado limitado por $max\{f_0,f_1\}+1$. □

Teorema 4.1.14. O anel L é nilpotente de classe (c,q)-limitada.

Demonstração. Pela Proposição anterior L é solúvel de comprimento (c,q)-limitado. Iremos usar indução no comprimento derivado de L. Se L é abeliano, o resultado é verdadeiro. Suponha que L é metabeliano. Neste caso $[x,y,z]=[x,z,y]$ para todo $x \in [L,L]$ e $y,z \in L$. Uma vez que $[L,L]$ é abeliano e pela identidade de Jacobi

$$[x,y,z] = \underbrace{[x,[y,z]]}_{\in L'} + [x,z,y]$$

Para cada $a \in \mathbb{Z}/p\mathbb{Z}$ denotemos por $L'_a := L' \cap L_a$. Seja $w = w(c,q)$ pelo Lema 4.1.7 e coloque $n=(w-1)(q^{c+1}+c)+2$. Escolha uma sequência de n elementos $(a_1,\cdots,a_n)$ em $\mathbb{Z}/p\mathbb{Z}$ e considere o comutador $[L'_{a_1},L_{a_2},\cdots,L_{a_n}]$, assuma que esse comutador é diferente de zero e suponha que $(a_1,\cdots,a_n)$ contenha uma subsequência r-independente de comprimento $c+1$ começando com a_1. Usando que $[x,y,z]=[x,z,y]$ podemos assumir que $a_1,\cdots,a_{c+1}$ é uma subsequência r-independente. Então, por 4.1 o comutador $[L'_{a_1},L_{a_2},\cdots,L_{a_n}]$ é zero, uma contradição. Segue do Lema 4.1.5 que a sequência $a_1,\cdots,a_n$ contém no máximo $q^{c+1}+c$

valores diferentes. O número n é escolhido grande o suficiente para garantir que a_1 ocorra em $a_1, \cdots, a_n$ pelo menos $w+1$ vezes ou mais, para outro valores diferentes de a_1, ocorra pelo menos w vezes. Usando $[x,y,z] = [x,z,y]$ assumimos $a_2 = \cdots = a_w$, neste caso segue pelo Lema 4.1.7 que $[L'_{a_1}, L_{a_2}, \cdots, L_{a_n}]$ é zero. Portanto, concluímos que L é nilpotente de classe no máximo n.

Agora, suponha que o comprimento derivado de L é pelo menos 3. Por hipótese indutiva $[L,L]$ é nilpotente de classe limitada. Juntos, isso dá nilpotência de L de classe limitada pelo análogo ao anel de Lie [5] do teorema de P. Hall [10], demonstrando o Teorema.

□

Os próximos resultados tratam sobre o centralizador $C_G(H)$. No primeiro, o resultado temos uma forma de ver o $C_{G/N}(H) = {C_G(H)N}/{N}$ com H sendo um grupo solúvel de automorfismos de um grupo finito G. O segundo resultado envolve a igualdade $C_{G/\gamma_i}(H) = {C_G(H)\gamma_i}/{\gamma_i}$ com γ_i termo da série central inferior e a classe de nilpotência do subgrupo $C_{L(G)}(H)$ não excedendo a classe de nilpotência do centralizador $C_G(H)$.

Lema 4.1.15. [19, Lema 3.2] Sejam H um grupo solúvel de automorfismos de um grupo finito G, e N um p-subgrupo abeliano elementar H-invariante de G contido no centro $Z(G)$. Se N, considerado como um módulo $\mathbb{F}_pH$, é um módulo $\mathbb{F}_pH$ livre, então $C_{G/N}(H) = {C_G(H)N}/{N}$.

Lema 4.1.16. [19, Lema 3.3] Seja GFH um grupo 2-*Frobenius* , onde G é um subgrupo normal, GF é um grupo *Frobenius* com kernel G e complemento F, e FH é um grupo *Frobenius* com kernel F e complemento H. Então:

1. Para cada termo da série central inferior $\gamma_i = \gamma_i(G)$ temos que $C_{G/\gamma_i}(H) = {C_G(H)\gamma_i}/{\gamma_i}$;
2. A classe de nilpotência do subgrupo de ponto fixo $C_{L(G)}(H)$ para o grupo de automorfismos H induzidos não excede a classe de nilpotência do centralizador $C_G(H)$.

Até essa parte do texto utilizamos a condição 4.1 para demonstrar resultados importantes como a limitação da classe de nilpotência e o comprimento derivado, mostraremos que a condição 4.1 é importante para a demonstração do resultado principal. Assim, o Teorema 4.1.14 é uma ferramenta indispensável para lidar com situações em que um grupo Frobenius age em outro grupo ou em um anel de Lie.

Teorema 4.1.17. Seja FH um grupo de *Frobenius* com núcleo F de ordem prima e complemento H de ordem q. Assuma que FH aja por automorfismo em um anel de Lie K de tal forma que $C_K(F) = 0$ e a classe de nilpotência de $C_K(H)$ é c. Então K é nilpotente de classe (c,q)-limitada.

Demonstração. Seja F de ordem p com $C_K(F) = 0$ então K é nilpotente de classe p-limitada por **??**. Seja ω a raiz primitiva da unidade e $\tilde{K} = K \oplus_{\mathbb{Z}} \mathbb{Z}[\omega]$ a extensão de ω a partir do $\mathbb{Z}$-módulo K. Vemos que $\tilde{K}$ é uma álgebra de Lie sobre $\mathbb{Z}$. O grupo FH age de formal natural em $\tilde{K}$ e a ação e tal que $C_{\tilde{K}}(F) = 0$ e $C_{\tilde{K}}(H)$ é nilpotente de classe c. Seja ϕ um gerador de F e para cada $i = 0, \cdots, p-1$ definimos $L_i = \{x \in \tilde{K} \mid x^{\phi} = \omega^i x\}$ com $L = \sum_i L_i$. Como K admite automorfismo livre de pontos fixos de ordem p concluimos que K não tem p-torção por ([12], Corolário 1.7.3). Como L é a soma direta dos L_i, e L é naturalmente tem uma $\mathbb{Z}/p\mathbb{Z}$-graduação tal que $L_0 = 0$. Pelo resultado [[12], Lema 4.1.1], $p\tilde{K} \leq L$.

Segue que a classe de nilpotência de L é igual a de $\tilde{K}$ e portanto a de K. Suponha que a classe de nilpotência de L seja u então $\gamma_{u+1}(p\tilde{k}) = 0$ e assim, $p^{u+1}\gamma_{u+1}(\tilde{K}) = 0$, o que implica que $\gamma_{u+1}(\tilde{K}) = 0$, pois $\tilde{K}$ é livre de p-torção, $\tilde{K}$ é nilpotente de classe u.

Como F é cíclico de ordem prima, H é cíclico. Seja $H = \langle h \rangle$ logo $\phi^{h^{-1}} = \phi^r$. Então r tem ordem multiplicativa q módulo p. O grupo H permuta as componentes L_i tal que $L_i^h = L_{ri}$ para todo $i \in \mathbb{Z}/p\mathbb{Z}$ De fato, se $x_i \in L_i$, então $(x_i^h)^{\phi} = x_i^{h\phi h^{-1}h} = (x_i^{\phi^r})^h = \omega^{ir} x_i^h$.

Dado $u_k \in L_k$, denotamos $u_k^{h^i}$ por $u_{r^i k}$. A soma de qualquer H-órbita pertence ao $C_L(H)$ e portanto

$$u_k + u_{rk} + \cdots + u_{r^{q-1}k} \in C_L(H).$$

Seja $x_{a_1}, \cdots, x_{a_{c+1}}$ elementos homogêneos em $L_{a_1}, \cdots, L_{a_{c+1}}$, respectivamente. Considere os elementos

$$\begin{aligned} X_1 &= x_{a_1} + x_{ra_1} + \cdots + x_{r^{q-1}a_1}, \\ &\vdots \\ X_{c+1} &= x_{a_{c+1}} + x_{ra_{c+1}} + \cdots + x_{r^{q-1}a_{c+1}}. \end{aligned}$$

Já que todos eles estão em $C_L(H)$ e $C_L(H)$ é nilpotente de classe c, segue que

$$[X_1, \cdots, X_{c+1}] = 0$$

Depois de expandir os colchetes, o lado esquerdo envolve o termo $[x_{a_1}, \cdots, x_{a_{c+1}}]$. Suponha que o comutador $[x_{a_1}, \cdots, x_{a_{c+1}}]$ não é zero. Em seguida, deve haver outros termos diferentes de zero na expressão expandida que pertencem a mesma componente $L_{a_1+\cdots+a_{c+1}}$. Então existem $i_1, \cdots, i_m \in \{1, 2, \cdots, c+1\}$ e $\alpha_1, \cdots, \alpha_m \in \{1, 2, \cdots, q-1\}$ tal que

$$a_{i_1} + \cdots + a_{i_m} = r^{\alpha_1} a_{i_1} + \cdots + r^{\alpha_m} a_{i_m}.$$

Assim, mostramos que $[x_{a_1}, \cdots, x_{a_{c+1}}] = 0$ onde a sequência $a_1, \cdots, a_{c+1}$ é r-independente. Portanto, estamos nas condições de aplicar o Teorema 4.1.14 para concluir que L é nilpotente de classe (c,q)-limitada. □

Teorema 4.1.18. Seja FH um grupo de *Frobenius* com núcleo F e complemento H. Suponha que FH age em um grupo finito G de modo que GF é um grupo com *Frobenius* de núcleo G e complemento F. A classe de nilpotência de G é limitada em termos $|H|$ e da classe de nilpotência do $C_G(H)$.

Demonstração. Note que o subgrupo G é nilpotente de classe limitada em termos do divisor primo da ordem de F. Mas queremos mostrar que a classe de nilpotência de G é limitada em termos da $|H|$ e da classe de nilpotência do $C_G(H)$. Como um complemento de Frobenius em GF, o grupo F não tem subgrupos não-cíclicos de ordem p^2 para qualquer p primo. Portanto, os subgrupos de F de Sylow são quaternários cíclicos ou generalizados. Sendo o núcleo Frobenius de FH, o grupo F é nilpotente. Segue-se que o 2-subgrupo de Sylow de F é trivial, pois de outro modo seu centro conteria um ponto fixo não-trivial para H. Assim, F é cíclico. Podemos supor que F tem ordem prima p, caso contrário existe um subgrupo de F de ordem prima p H-invariante.

Seja $L(G)$ o anel de Lie associado ao grupo G. Então temos:

$$L(G) = \bigoplus_{i=1}^{n} \gamma_i \diagup \gamma_{i+1}$$

com n sendo a classe de nilpotência de G e os γ_i termos da série central inferior de G. Como vimos no Capítulo 3 a nilpotência de G coincide com a nilpotência de $L(G)$. A ação do grupo FH em G induz uma ação natural do grupo FH em $L(G)$. Como F age livres de pontos fixos em $\gamma_i \diagup \gamma_{i+1}$ [[9],Lema 10.1.3] temos que $C_{L(G)}(F) = 0$. O item 2. do Lema 4.1.16 diz que $C_{L(G)}(H)$ é nilpotente e não excede a classe de nilpotência de $C_G(H)$. Então pelo Teorema 4.1.17, $L(G)$ é nilpotente de classe limitada em termos da $|H|$ e da classe de nilpotência do $C_G(H)$. Como a classe de nilpotência de $L(G)$ coincide com a classe de nilpotência de G, o teorema está demonstrado. □

Capítulo 5

Expoente de Grupos admitindo um Grupo de *Frobenius* como Grupo de Automorfismo.

A ideia deste capítulo é apresentar as demonstrações das soluções parciais do **Problema Problema 18.67** e do item 2 do textbfProblema Problema 17.77.

Teorema 5.0.1. Suponha que um grupo finito de Frobenius FH com núcleo cíclico F e complemento H age em um grupo finito G de tal maneira que $C_G(F) = 1$ e $C_G(H)$ tem expoente e. Então o expoente de G é limitado unicamente em termos de e e $|FH|$.

Teorema 5.0.2. Suponha que o grupo de *Frobenius* de ordem 12 aja de forma coprima sobre um grupo finito G de tal maneira que $C_G(F) = 1$ e $C_G(H)$ tem expoente e. Então o expoente de G é limitado em termos de e.

Ou seja, apresentamos uma solução positiva os casos onde um grupo de Frobenius com núcleo cíclico ou o grupo de Frobenius $FH \cong \mathbb{A}_4$ agem como grupo de automorfismos do **Problema 18.67** quando F é cíclico e $FH \cong \mathbb{A}_4$, resultados estudados nos artigos *On the exponent of a finite group with an automorphism group of order twelve* [25] e *Frobenius groups of automorphisms and their fixed points* [14] que utilizam de ferramentas vistas nas seções 1.3 e 3.3 e no Capítulo 2.

5.1 Grupos de *Frobenius* Metacíclico como Automorfismos.

Um grupo E é dito *metacíclico* se possui em subgrupo normal cíclico K tal que E/K é cíclico. A apresentação de um grupo *metacíclico* é dada por:

$$E = \langle a, b | a^n = 1, b^m = a^u, a^b = a^s \rangle$$

com m, n, u, s inteiros positivos que satisfazem $s^m \equiv 1(modn)$ e $u(s-1) \equiv 0(modn)$. O primeiro exemplo de grupos *metacíclico* é o produto direto de grupo cíclicos, outra interessante observação é que E' é sempre cíclico, ou seja, o grupo derivado de um grupo *metacíclico* é cíclico.

O Teorema 1.2.24 pode ser usado para provar que um grupo de *Frobenius* com núcleo cíclico F e complemento H deve ser necessariamente metacíclico, pois nesse caso H deve ser abeliano e, como todo elemento do complemento age sem pontos fixos o teorema 1.2.24 implica que H deve ser cíclico.

Um elemento $y \in$ Álgebra de Lie L é dito ad-nilpotente se existe um inteiro positivo n tal que $(ady)^n = 0$, isto é, $[x, \underbrace{y, \cdots, y}_{\text{n-fatores}}]$, se n é o menor inteiro com essa propriedade, então y é ad-nilpotente de índice n.

Teorema 5.1.1. Se K ém ideal de um anel de Lie solúvel então a nilpotênca de L é dada nas seguintes hipóteses:

$$\text{Se } \gamma_{c+1}(L) \subseteq [K,K] \text{ e } \gamma_{k+1}(K) = 0, \text{ então } \gamma_{c\binom{k+1}{2}-\binom{k}{2}+1}(L) = 0$$

O resultado acima pode ser considerado como análogo ao anel de Lie do teorema de *P. Hall* [10]. Denotamos por $L_p(G)$ a subálgebra gerada por $L_1 = D_1/D_2$ e para um elemento $x \in D_i/D_{i+1}$ denotamos por $\overline{x}$ o elemento xD_i de $DL(G)$.

Lema 5.1.2. [17](Lazard) Para todo $x \in G$ temos $(ad\overline{x})^p = ad\overline{x^p}$. Consequentemente, se x tem ordem finita p^t, então $\overline{x}$ é ad-nilpotent de índice limitado por p^t.

Lema 5.1.3. [6](Dade) Se G admite um automorfismo livre de pontos fixos de ordem n , então a altura de Fitting de G é limitado por uma função que depende apenas de n .

Lema 5.1.4. Suponha que X é um p-grupo d-gerado tal que a Álgebra de Lie $L_p(X)$ é nilpotente de classe c. Então X possui um subgrupo powerful característico de índice (p,c,d)-limitado.

Demonstração. Sejam $\rho_1, \cdots, \rho_r$ todos os comutadores simples de peso $\leq c$ nos geradores de X. Com r um número limitado por uma função que depende de d e c. A nilpotência de

$L_p\langle X\rangle$ de classe c implica que para qualquer $s \in \mathbb{N}$, cada elemento $g \in \langle X\rangle$ podemos escrever por 3.3.8 da forma $g = \rho_1^{k_1}\cdots\rho_r^{k_r}\lambda$, com $\lambda \in D_s$, $k_i \in \mathbb{Z}$. Com

$$D_s = \langle [a_1,\cdots,a_i]^{p^t} | ip^t \geq s, a_k \in G\rangle$$

Seja X um p-grupo finito, com $D_s = 1$ para algum $s \in \mathbb{N}$. Portanto todo elemento $g \in P$ pode ser escrito na forma $g = \rho_1^{k_1}\cdots\rho_r^{k_r}$, como $p_i^{p^m} \in P^{p^m}$, segue-se que, para cada $m \in \mathbb{N}$, todo elemento $g \in P$ pode ser escrito na forma:

$$g = \rho_1^{k_1}\cdots\rho_r^{k_r}v, \;\; 0 \leq k_i \leq p^m - 1.$$

para todo i e consequentemente, $|{}^{P}\!/_{P^{p^m}}| \leq p^{rm}$ para qualquer $m \in \mathbb{N}$. Seja V a interseção dos núcleos do homomorfismo de P em $GL_r(\mathbb{F}_p)$. Seja $W = V$ se $p \neq 2$ ou $W = V^2$ se $p = 2$. Os expoentes dos p-subgrupos de Sylow de $GL_r(\mathbb{F}_p)$ é um número limitado por uma função que depende de p e r. Então $P^{p^a} \leq W$ para algum a limitado por p e r que também é limitado por uma função que depende p, c e d. Desde que r seja (c,d)-limitada. Existe um número (p,c,d)-limitado $u \geq a$ tal que $|{}^{P^{p^u}}\!/_{P^{p^{u+1}}}| \leq p^r$, por outro lado a desigualdade $|{}^{P}\!/_{P^{p^m}}| \leq p^{rm}$ será violada para alguns m. Então $P^{p^u} \leq P^{p^a} \leq W$ e P^{p^u} é r-gerado, desde $|{}^{P^{p^u}}\!/_{\Phi(P^{p^u})}| \leq |{}^{P^{p^u}}\!/_{P^{p^{u+1}}}| \leq p^r$. Agora, pela proposição 1.3.12, P^{p^u} é um subgrupo *Powerful*. O índice de P^{p^u} é no máximo p^{ur} é (p,c,d)-limitada. □

Para os próximos resultados, lembremos o conceito de Anel graduado apresentado no capítulo 3. Seja A um grupo abeliano aditivo. Um anel de Lie L é A-graduado se

$$L = \bigoplus_{a\in A} L_a, \qquad \text{e} \qquad [L_a, L_b] \subseteq L_{a+b},$$

com L_a sendo o subgrupo do grupo aditivo L.

Lema 5.1.5. Seja $L = \bigoplus L_i$ uma $\mathbb{Z}$-graduada Álgebra de Lie sobre um corpo tal que $L = \langle L_1\rangle$ e assuma que toda componente homogênea L_i sejam geradas por elementos que são ad-nilpotentes de índice no máximo r. Suponha que L seja solúvel de comprimento derivado k e que L_1 tenha dimensão finita d. Então L é nilpotente de classe (d,r,k)-limitada.

Demonstração. A demonstração seguirá por indução em $k \geq 2$. Seja M, o último termo não nulo da série derivada 3.1.24, por indução assumimos que ${}^{L}\!/_{M}$ é nilpotente de classe (d,r,k)-limitado. Em particular, concluí-se que a dimensão de ${}^{L}\!/_{M}$ é (d,r,k)-limitada. Denote por f a função que depende de (d,r,k), pela nilpotência de ${}^{L}\!/_{M}$ segue pelo teorema 3.1.23 que $\gamma_{f+1}(L) \subseteq M$. Analisaremos os casos em que: $M \leq Z(L)$ e $M \nleq Z(L)$. Para o primeiro temos

que $\gamma_{f+1}(L) \subseteq M \leq Z(L)$, pelas equivalências do Teorema 3.1.20 segue que L é nilpotente de índice (d,r,k)-limitado.

Para o segundo caso, considere j o maior índice tal que L_j não está contido em $C_L(M)$. Seja $K = L_j + C_L(M)$ e um ideal de L, pois:

$$[K,L] = [L_j + C_L(M), L] = [L_j, L] + [C_L(M), M] \subseteq L_j + C_L(M) = K.$$

Além disso, K não é abeliano:

$$[K,K] = [L_j, L_j] + 2[C_L(M), L_j] \subseteq L_{2j} + 2[C_L(M), L_j].$$

Desde que a dimensão de L/M é (d,r,k)-limitada, existem alguns elementos $a_1, \cdots, a_m \in L_j$ tal que $K = \langle a_1, \cdots, a_m, C_L(M) \rangle$ e cada um dos elementos $a_1, \cdots, a_m$ são ad-nilpotentes de índice no máximo r. Mais ainda, o j é (d,r,k)-limitado, podemos usar indução reverso em j, assim por indução $L/[K,K]$ é nilpotente de classe (d,r,k)-limitada.

Defina $s = m(r-1)+1$ e considere o ideal $[M, K, \cdots, K]$, com K aparecendo s vezes. Então S é gerado por comutadores $[m, b_1, \cdots, b_s]$, com $m \in M$ e $b_1, \cdots, b_s$ elementos de $\{a_1, \cdots, a_m\}$ não necessariamente distintos, já que s é grande o suficiente existem alguns índices $i_1, \cdots, i_r$ tal que $b_{i_1} = \cdots = b_{i_r}$. Observe que $K/C_L(M)$ é abeliano, pois:

$$[K/C_L(M), K/C_L(M)] = [K,K]C_L(M)/C_L(M) = \\ [C_L(M), K]C_L(M)/C_L(M) \subseteq C_L(M)/C_L(M),$$

pois $[C_L(M), K] \subseteq C_L(M)$. Assim para $x, y \in K$ e $m \in M$ temos $[m,y,x] = [x,y,m] + [m,x,y]$, como $[x,y,m] \in K/C_L(M)$, logo $[m,y,x] = [m,x,y]$. Assumimos sem perda de generalidade que $b_1 = \cdots = b_r$, como b_1 é ad-nilpotente de índice no máximo r, segue que

$$[m, b_1, \cdots, b_r, \cdots, b_s] = 0.$$

Logo $S = 0$, conclímos que M está contido em algum termo da série central superior de K, sendo assim $\gamma_{s+1}(K) = 0$. Portando, juntando o fato que $L/[K,K]$ é nilpotente de classe (d,r,k)-limitada e K é nilpotente de classe s segue pela observação do início do capítulo que $\gamma_{s\binom{k+1}{2} - \binom{k}{2} + 1}(L) = 0$, logo L é (d,r,k)-limitada.

□

Teorema 5.1.6. Suponha que um grupo finito de *Frobenius* FH com núcleo cíclico F e complemento H age em um grupo finito G de tal maneira que $C_G(F) = 1$ e $C_G(H)$ tem expoente e. Então o expoente de G é limitado unicamente em termos de e e $|FH|$.

Demonstração. Pelo Lema 2.3.1 G é solúvel, lembremos que o *Fitting* de G é o produto de $M \leq G$ tais que M é o maior subgrupo normal nilpotente de G. A série de *Fitting* é definida fixando $F_0(G) = 1$ e definimos ${}^{F_{i+1}(G)}\!/_{F_i(G)} = F\left({}^{G}\!/_{F_i(G)}\right)$, além disso como G é solúvel, o menor valor $h = h(G)$ tal que $G = F_h(G)$ é chamado de altura de Fitting de G. Essa altura é limitada por uma função que depende apenas $|F|$ pelo Lema 5.1.3. Usaremos indução sobre a altura de *Fitting* de G . Note que basta demonstramos para G nilpotente pois o quociente dos termos da série de *Fitting* são nilpotentes. Consideremos G um p-grupo onde p é um primo arbitrário, uma vez que G é nilpotente ele escrito como produto direto de seus subgrupos de Sylow.

A demonstração será feita no caso em que reduzimos G para um grupo *Powerful* utilizando as propriedades mencionadas na seção 1.3.

Pelo teorema 2.3.7, p divide e, logo podemos assumir que e é uma potência de p. Seja $x \in G$ e considere o subgrupo $S = \langle x^j; j \in FH\rangle$, S é FH-invariante com no máximo $|FH|$ geradores. Portanto, podemos assumir que $G = \langle x^j; j \in FH\rangle$, ou seja, podemos assumir que G é $|FH|$-gerado e seu conjunto gerador é FH-invariante.

Qualquer grupo de automorfismo do grupo G atua de forma natural sobre os grupos quocientes $L_i = {}^{D_i}\!/_{D_{i+1}}$ formados pelos termos da série de *Jennings-Zassenhaus* de G. Esta ação induz uma ação por grupos de automorfismo sobre a Álgebra de Lie $L = L_p(G)$. Pelo teorema 2.3.3 o subgrupo F é livre ponto fixo em todos quocientes L_i da série de *Jennings-Zassenhaus* e 2.3.4 temos $C_{{}^{D_i}\!/_{D_{i+1}}}(H) = {}^{C_{D_i}(H)D_{i+1}}\!/_{D_{i+1}}$. Como $C_L(F) = 0$, temos:

$$C_L(H) = \bigoplus {}^{C_{D_i}(H)D_{i+1}}\!/_{D_{i+1}}$$

Além disso,o Teorema 2.3.7 garante que L_i é gerado pelo centralizador $C_{L_i}(H)^f$, com $f \in F$ e o Teorema 2.3.4 garante que todo elemento $C_{L_i}(H)^f$ é imagem de alguns elementos $C_G(H)^f$, cuja ordem divide e.

Pelo lema de *Lazard* 5.1.2, segue que o grupo aditivo de L_i é gerado por elementos que são ad-nilpotentes de índice no máximo e, usando o Teorema de *Kreknin* 3.4.22 vemos que L é solúvel de comprimento $|FH|$-limitado, segue pelo Lema 5.1.5 que L é nilpotente de classe $(e,|FH|)$-limitada. A nilpotência de $L_p(G)$ implica pelo Lema 5.1.4, G possui um subgrupo powerful característico. Sendo assim é suficiente limitar o expoente de tal subgrupo *powerful*, ou seja, podemos assumir que G é um p-grupo *powerful* e pelo Lema 1.3.8, o expoente de G divide a ordem de seus geradores. Portanto, como G é gerado por elementos do $C_G(H)^f$ para $f \in F$, então G tem expoente e. □

5.2 Grupos de *Frobenius* de ordem 12 como Automorfismo

O objetivo desta seção é apresentar a demonstração do seguinte resultado:

Teorema 5.2.1. Suponha que o grupo de *Frobenius* de ordem 12 aja de forma coprima sobre um grupo finito G de tal maneira que $C_G(F) = 1$ e $C_G(H)$ tem expoente e. Então o expoente de G é limitado em termos de e.

Nessa seção trabalhamos com um grupo *Frobenius* FH com núcleo F de ordem 4 e o complemento H da ordem 3, ou seja, $\mathbb{A}_4 = (C_2 \times C_2) \rtimes C_3$, aja coprimamente sobre um grupo finito G e a álgebra de Lie L tem as subálgebras L_1, L_2 e L_3 abelianas tal que

$$L = \bigoplus_{1 \leq i \leq 3} L_i \quad \text{e} \quad [L_1, L_2] \leq L_3, [L_2, L_3] \leq L_1, [L_3, L_1] \leq L_2. \tag{5.1}$$

Para todo $x \in L$, escrevemos $x = x_1 + x_2 + x_3$, com cada $x_i \in L_i$. Assumimos que L admite um automorfismo ϕ de ordem 3, tal que:

$$L_1^{\phi} = L_2, \quad L_2^{\phi} = L_3, \quad L_3^{\phi} = L_1. \tag{5.2}$$

Denote L_ϕ a subálgebra de ponto fixo ϕ. É evidente que $x \in L_\phi$ se, e somente se, $x_2 = x_1^{\phi}$ e $x_3 = x_2^{\phi}$.

Lema 5.2.2. Sejam $a, b \in L$ e suponha que $[a,b] = 0$. Então:

$$[a_2 + a_3, b_2 + b_3] = [a_1 + a_2, b_1 + b_2] = [a_1 + a_3, b_1 + b_3] = 0.$$

Demonstração. Lembre-se que cada L_i é abeliana. Assim podemos escrever o comutador $[a,b]_1 = [a_2 + a_3, b_2 + b_3] = \underbrace{[a_2, b_3]}_{\in L_1} + \underbrace{[a_3, b_2]}_{\in L_1}$. Consequentemente $[a_2 + a_3, b_2 + b_3] = 0$ e similarmente temos para $[a_1 + a_3, b_1 + b_3] = [a_1 + a_2, b_1 + b_2] = 0$. □

Lema 5.2.3. Sejam $a, b \in L$ e suponhamos que $[a,b] = 0$. Assuma que $b_1 = 0$. Então b_2 e b_3 comutam com a_1. Se adicionarmos $b_2 = 0$, então b_3 comuta com cada um dos elementos a_1, a_2, a_3.

Demonstração. Pelo Lema 5.2.2 e pelo fato de cada L_i ser abeliano, temos $0 = [a_1 + a_3, b_3] = [a_1, b_3]$ e $0 = [a_1 + a_2, b_2] = [a_1, b_2]$, ou seja, b_2 e b_3 comutam com a_1.

Se adicionarmos $b_2 = 0$ então:

$$[a_2 + a_3, b_3] = 0 \Rightarrow [a_2, b_3] = 0$$
$$[a_1 + a_3, b_3] = 0 \Rightarrow [a_1, b_3] = 0$$

Logo, b_3 comuta com cada um dos elementos a_1, a_2, a_3. □

Lema 5.2.4. Seja $a \in L$ ad-nilpotente de índice m e suponha que os elementos a_1, a_2 e a_3 comutam emparelhados. Então cada a_1, a_2 e a_3 é ad-nilpotente de índice no máximo $2m-1$.

Demonstração. Provaremos apenas para a_1 é ad-nilpotente de índice no máximo $2m-1$, os demais casos são análogos. Para todo elemento $x \in L$ escreva $\overline{x} = x_1 - x_2 - x_3$. Para todo $x, y \in L$ temos:

$$[\overline{x}, \overline{y}] = [x_1 - x_2 - x_3, y_1 - y_2 - y_3] =$$
$$[x_1, y_1] - [x_1, y_2] - [x_1, y_3] - [x_2, y_1] + [x_2, y_2] + [x_2, y_3] - [x_3, y_1] + [x_3, y_2] + [x_3, y_3] =$$
$$\underbrace{([x_2, y_3] + [x_3, y_2])}_{\in L_1} - \underbrace{([x_1, y_3] + [x_3, y_1])}_{\in L_2} - \underbrace{([x_2, y_2] + [x_1, y_2])}_{\in L_2} = \overline{[x, y]}$$

Nas igualdades acima usamos o fato que L_i é abeliana. Considere a seguinte função

$$\vartheta : L \longrightarrow L$$
$$x \longrightarrow \overline{x}$$

Observe que ϑ é um automorfismo de L. Por hipótese $a \in L$ é ad-nilpotente de índice m então $\overline{a}$ é ad-nilpotente de índice no máximo m pelo automorfismo acima. Como $2a_1 = a + \overline{a}$ temos que $2a_1$ é ad-nilpotente de índice no máximo $2m-1$. Agora, o resultado segue do fato de que $2L = L$. □

Lema 5.2.5. Suponha que $a \in L_i$ e $b \in L_j$ para todo $i \neq j$ e $[a, b] = 0$. Então $I([b, L_i]) \leq C_L(a)$.

Demonstração. É suficiente mostrar que para qualquer conjunto $c_1, \cdots, c_t$ tal que $c_1 \in L_1$ e $c_i \in L_{k_i}$ com cada $k_i \in \{1, 2, 3\}$, temos:

$$[b, c_1, \cdots, c_t, a] = 0 \tag{5.3}$$

Provaremos usando indução em t, para $t = 1$, temos:

$$[b, c_1, a]. \tag{5.4}$$

Como a e $c_1 \in L_1$ e L_1 é abeliano então $c_1 \in C_L(a)$, por hipótese b também está em $C_L(a)$ e assim (5.4) é igual a zero. Suponha que vale para $t \geq 2$ e valores menores que t é válido a equação 5.3. Se $c_2 \in L_1$ denotemos $[b,c_1] = d$ e observe que $d \in L_3$ e $[d,a] = 0$ por 5.4. Então podemos reescrever o comutador dado na equação 5.4 por:

$$[b,c_1,\cdots,c_t,a] = [d,c_2,\cdots,c_t,a]$$

No último comutador temos $b \in L_2 \cap C_L(a)$ com $d \in L_3 \cap C_L(a)$. Se $c_2 \in L_3$ então $[b,c_1,c_2] = 0$ pois $[b,c_1]$ e $c_2 \in L_3$. Assim, podemos supor que $c_2 \in L_2$ e portanto $[b,c_1,c_2,a] = 0$, pois $[b,c_1,c_2] \in L_1$. Para $t \geq 3$ considere os casos:

1. $c_3 \in L_1$.

   Como L_1 é abeliano, teríamos $[b,c_1,c_2,c_3] = 0$, assim 5.4 é verdadeira.

2. $c_3 \in L_2$

   Para este item e o outro item, considere o seguinte comutador $[x_1,\cdots,x_s] = 0$ sempre existe um inteiro positivo k e alguns $i \in \{1,2,3\}$ tais que $[x_1,\cdots,x_k] \in L_i$ e $x_k + 1 \in L_i$. Como L_i é abeliano, descartamos tal comutador. Para $c_3 \in L_2$ temos:

   $$\begin{aligned}[b,c_1,c_2,c_3] =& [[b,c_1],[c_2,c_3]] + [c_2,[c_3,[b,c_1]]] = \\ & [b,[c_1,[c_2,c_3]]] + [c_1,[[c_2,c_3],b]] + [c_3,[[c_1,b],c_2]] + [[c_1,b],[c_2,c_3]]\end{aligned}$$

   Faça $a_1 = [c_1,c_2,c_3] \in L_1$. Quando o comutador 5.4 pode ser escrito da forma

   $$[b,a_1,c_4,\cdots,c_t,a]$$

   por hipótese é igual a zero.

3. $c_3 \in L_3$.

   O comutador $[b,c_1,c_2,c_3] = [[b,c_1],c_3,c_2] + [b,c_1,[c_2,c_3]]$. Se fizermos $a_2 = [c_2,c_3] \in L_1$ e $b_1 = [b,c_1] \in C_L(a)$ então o comutador em 5.4 pode ser reescrito como

   $$[b_1,a_2,c_4,\cdot,c_t,a]$$

   A forma do último comutador difere do comutador 5.4 apenas por $b \in L_2 \cap C_L(a)$ então $b_1 \in L_3 \cap C_L(a)$. Podemos aplicar a hipótese de indução. Assim:

   $$[b_1,a_2,c_4,\cdots,c_t,a] = 0.$$

□

Lema 5.2.6. Sejam y,z elementos do $C_L(x)$ para todo elemento $x \in L_\phi$. Então os elementos $[y,z]_1,[y,z]_2,[y,z]_3$ pertencem ao $C_L(x)$.

Demonstração. Mostraremos que $[y,z]_1 \in C_L(x)$, as demais são análogas. Pela consideração feitas no início desta seção $x = x_1+x_2+x_3$. Por hipótese $y,z \in C_L(x)$, ou seja, $C_y(x) = 0$ e $C_z(x) = 0$ pelo Lema 5.2.2 temos y_2+y_3 e z_2+z_3 comutam com x_2+x_3. Na demonstração do Lema 5.2.2 utilizamos o fato do comutador $[y,z]_1 = [y_2+y_3, z_2+z_3]$, a igualdade vem do fato do comutador $[y,z]_1 \in L_1$ e representamos em termos de comutadores de L como elementos de L_1. Assim, $[y,z]_1 \in C_L(x_2+x_3)$. Como L_1 é abeliano $[y,z]_1 \in C_L(x_1)$. Logo,$[y,z]_1 \in C_L(x_1+x_2+x_3) = C_L(x)$. □

Se $X \subseteq L$, denotamos por $ID(X)$ o menor ideal K de L ϕ-invariante contendo X e satisfazendo as condições que $K = \bigoplus_{1\leq i\leq 3} K_i$, com $K_i = K \cap L_i$. Dado um elemento $x = x_1+x_2+x_3$, colocamos $x^{(1)} = x$ e denote por $x^{(2)}$ o elemento $[x_1,x_2]+[x_1,x_3]+[x_2,x_3]$. Indutivamente para $i \geq 3$ temos $x^{(i)} = (x^{(i-1)})^{(2)}$.

Lema 5.2.7. Seja a um elemento ad-nilpotente em L_1 e seja N o ideal de L gerado por a. Então $[L,L] \leq \langle L_1,L_2\rangle$.

Demonstração. Denote por $N = \langle L_1,L_2\rangle$. As inclusões $[L_1,L_3] \leq L_2$ e $[L_2,L_3] \leq L_1$ mostram que L_3 normaliza N. Como $L = L_1+L_2+L_3$ temos que N é um ideal de L. O quociente L/N deve ser abeliano pois L_3 é abeliano. □

Lema 5.2.8. Seja $a \in L_1 \cup L_2 \cup L_3$ e suponha que a é ad-nilpotente de índice m. Então $I(a)$ é nilpotente de classe no máximo $2m-1$.

Demonstração. Seja n o menor número tal que:

$$[L,\underbrace{a,\cdots,a}_{\text{n}}] = 0.$$

Assumimos que $n \geq 1$ e provamos a nilpotência de N usando indução em n. Seja

$$[L_2,\underbrace{a,\cdots,a}_{\text{n-1}}] = 0$$

Então $M \leq C_L(a) \cap L_2$ se n é ímpar e $M \leq C_L(a) \cap L_2$ se n é par. Assuma que $M \leq L_2$. Seja $\overline{L} = L/C_L(N)$ e denote $\overline{X}$ a imagem de qualquer subconjunto $X \subseteq L$ em $\overline{L}$. O ideal minimal T de L contém a subálgebra gerada por $[M,L_1]$ por comutadores da forma $[b,c_1,\cdots,c_t]$, com

$c_1 \in L_1$ e $c_i \in L_1 \cup L_2 \cup L_3$ com $i \geq 2$. Portanto, pelo Lema 5.2.5 a centraliza T. Isso implica que $T \leq C_L(N)$ então obtemos $[\overline{M}, \overline{L_1}] = 0$. Como $\overline{M} \leq \overline{L_2}$ e $\overline{L_2}$ é abeliano, concluímos que:

$$\overline{M} \leq C_{\overline{L}}(\langle L_1, L_2 \rangle)$$

Pelo Lema anterior $[\overline{L}, \overline{L}] \leq \langle L_1, L_2 \rangle$. Como $\overline{M}$ centraliza a subálgebra $\overline{R} = \langle [\overline{L}, \overline{L}], \overline{a} \rangle$ de $\overline{L}$ segue que $\overline{M} \leq Z(\overline{N})$. Como $\overline{L} = {}^{L}\!/_{C_L(N)}$ concluímos que $M \leq Z_2(N)$. Usamos o mesmo argumento substituindo L_2 por L_i, logo:

$$[L_i, \underbrace{a, \cdots, a}_{\text{n-1}}] \leq Z_2(N)$$

para qualquer $i = 1, 2, 3$. Como $L = \sum_{1 \leq i \leq 3} L_i$ obtemos

$$[L, \underbrace{a, \cdots, a}_{\text{n-1}}] \leq Z_2(N)$$

Vamos considerar a álgebra quociente $\tilde{L} = {}^{L}\!/_{Z_2(N)}$. Denote $\tilde{X}$ a imagem do subconjunto $X \subseteq L$ em $\tilde{L}$. Então

$$[\tilde{L}, \underbrace{\tilde{a}, \cdots, \tilde{a}}_{\text{n-1}}] = 0$$

E assim por indução $\tilde{N}$ é nilpotente. Como $\tilde{N} = {}^{N}\!/_{Z_2(N)}$ deduzimos que N é nilpotente. Observe que a prova mostra que N é de classe de nilpotência máximo $2m-1$. □

Lema 5.2.9. Seja $a \in L_1 \cup L_2 \cup L_3$ e suponha que a comuta com todos os elementos $x \in L_\phi$. Então a centraliza o ideal $I(x^{(4)})$.

Demonstração. Seja $a = a_1 + a_2 + a_3$, podemos assumir que $a \in L_1$ então $a_1 = a_2 = 0$ Então, pelo Lema 5.2.3 a comuta com cada um dos elementos x_1, x_2 e x_3. Pelo Lema 5.2.5 a centraliza o ideal $I([x_1, x_2])$. Seja $y = x^{(4)}$ da definição y_1, y_2 e $y_3 \in I([x_1, x_2])$, como $y \in L_\varphi$ então $Id(y) = Id(y_1) + Id(y_2) + Id(y_3)$. Assim como a comuta com $I([x_1, x_2])$ e y_1, y_2 e $y_3 \in I([x_1, x_2])$ logo temos que $y = x^{(4)}$ comuta com a. □

Lema 5.2.10. Seja L uma álgebra de Lie gerada por um conjunto finito X em relação ao qual todo componente homogêneo é a subálgebra gerada por elementos que são ad-nilpotentes de índice no máximo r. Suponha que L seja solúvel com o comprimento derivado k. Então L é nilpotente de classe $f(|X|, r, k)$-limitada.

A demostração desse Lema é semelhante ao Lema 5.1.5.

Para os demais resultados, suponha que a Álgebra L é gerada por um conjunto finito $X \subseteq L_1 \cup L_2 \cup L_3$ para o qual existem inteiros positivos m e n tais que todo elemento homogêneo contido em L_ϕ é ad-nilpotente em L de índice no máximo m e cada par de elementos homogêneos contidos em L_ϕ gera uma subálgebra que é nilpotente de classe no máximo n.

Lema 5.2.11. A componente homogênea de peso w é uma subálgebra gerada por elementos que são ad-nilpotentes de índice no máximo m.

Demonstração. Denotemos L_w a componente homogênea de peso w. Considere o $L_w = \oplus_{1\leq i\leq 3}(L_i \cap L_w)$, assim é suficiente mostrar que todo elemento $a \in L_i \cap L_w$ pode ser escrito como a soma de elementos que são ad-nilpotentes de índice no máximo m. Escreva $a = \frac{1}{2}(a + a^\varphi + a^{\varphi^2} + a - a^\varphi - a^{\varphi^2})$. Por hipótese $a + a^\varphi + a^{\varphi^2}$ é ad-nilpotente em L de índice no máximo m. Como o homomorfismo que leva $x = x_1 + x_2 + x_3$ em $\bar{x} = x_1 - x_2 - x_3$ é um automorfismo de L. Logo, $a - a^\varphi - a^{\varphi^2}$ é ad-nilpotente de índice no máximo m. □

Um elemento $y \in L$ é dito **crítico**, se $L/ID(y)$ é nilpotente de classe (m,n)-limitada.

Teorema 5.2.12. Suponha que exista um elemento $x \in L_\phi$ tal que $X = \{x_1, x_2, x_3\}$. Então L é nilpotente de classe (m,n)-limitada.

Demonstração. Para essa demonstração se $y \in L_\phi$ é um elemento crítico homogêneo, então é $y^{(i)}$ para todo $i = 1,2,3,4$. De fato, suponha que $y^{(2)} = 0$, isso significa que os elementos y_1, y_2 e y_3 comutam e assim pelo Lema 5.2.4 cada um dos ideais $I(y_1), I(y_2)$ e $I(y_3)$ são nilpotentes de classe no máximo $4m-3$. Como $y \in L_\phi$ temos $ID(y) = I(y_1) + I(y_2) + I(y_3)$ e assim $ID(y)$ é nilpotente de classe no máximo $12m-9$. Como consideramos que $L/ID(y)$ é nilpotente de classe limitada por uma função que depende de m e n, digamos $f(m,n)$, concluímos que L é solúvel de comprimento derivado $f(m,n)$. Pelo Lema 5.2.11 as componentes homogêneas de peso w é uma subálgebra gerada por elementos que são ad-nilpotentes de índice no máximo m. Assim, pelo Lema 5.2.10 L é nilpotente de classe no máximo $f(m,n)$. Isso mostra que $y^{(2)}$ é crítico. Para $y^{(3)}$ e $y^{(4)}$ é análogo. A demonstração será feita por indução. Seja k o menor número com a propriedade:

$$[x_1 - x_2, \underbrace{x, \cdots, x}_{\text{k}}] = 0.$$

Suponha que $k \leq m$. Se $k = 1$, então o Lema 5.2.3 mostra que x_1 e x_2 comutam com x_3. Portanto $x_3 \in Z(L)$ e assim L é abeliano, portanto segue também que $x_1, x_2 \in Z(L)$. E assim podemos supor que $k \geq 2$ e usar indução em k. Segue em particular que $[x_1 - x_2, \underbrace{x, \cdots, x}_{\text{i}}]$ é critical com $i \leq k-1$.

Seja $d_1 = [x_1 - x_2, \underbrace{x, \cdots, x}_{\text{k-1}}]_1$ e $d = d_1 + d_1^{\phi} + d_1^{\phi^2}$. Desde que $[x_1 - x_2, \underbrace{x, \cdots, x}_{\text{k-1}}]$ tenha a forma $l - l^{\phi}$ para um $l \in L$ adequado e como $3L = L$, segue-se que $[x_1 - x_2, \underbrace{x, \cdots, x}_{\text{k-1}}] \notin L_{\phi}$ enquanto $d \in L_{\phi}$. Suponha primeiramente que $[x,d] = 0$. Seja $g = [x_1 - x_2, \underbrace{x, \cdots, x}_{\text{k-1}}] - d$. Então $[x,g] = 0$, enquanto $g \in L_{\phi}$ e $g_1 = 0$. O Lema 5.2.3 diz g_2 e g_3 comutam com x_1. Pelo Lema 5.2.8 g_2 centraliza o ideal $I([x_1,x_2])$, argumentando de maneira similar ao Lema 5.2.9, concluímos que g_2 centraliza o ideal $ID(x^{(4)})$. De fato, se $y = x^{(4)}$ é imediato que os elementos y_1, y_2 e $y_3 \in I([x_1,x_2])$ e portanto $ID(y) \leq I([x_1,x_2])$ como $x^{(4)}$ é critíco, segue que existe um r limitado por $f(m,n)$ tal que $\gamma_r(L) \leq ID(x^{(4)})$. Portanto $g_2 \in C_L(\gamma_r(L))$. Similarmente concluimos que $g_3 \in C_L(\gamma_r(L))$. Segue que

$$[x_1 - x_2, \underbrace{x, \cdots, x}_{\text{k-1}}] \in L_{\phi} + C_L(\gamma_r(L)).$$

Por indução $L/C_L(\gamma_r(L))$ é nilpotente de classe limitada $f(m,n)$. Como L é solúvel com comprimento derivado $f(m,n)$. Como vimos acima, o Lema 5.2.11 e o Lema 5.2.10 permitem concluir que L é nilpotente de classe $f(m,n)$-limitada. Portanto, podemos supor $[x,d] \neq 0$, usaremos o número de comutadores distintos em x e d como segundo parâmetro de indução. Pela hipótese, este número é n-limitado. Portanto, todos os comutadores em x e d são elementos críticos. Escolha z um comutador em x e d tal que $0 \neq z \in Z(\langle d,x \rangle)$. Ambos os elementos x e d estão em $C_L(z)$. Portanto o Lema 5.2.6 diz que $a = [x,d]_1$ centraliza z. Assim pelo Lema 5.2.9 centraliza $J = ID(z^{(4)})$. Em seguida, observamos que $ID(a) = ID([x,d])$ pois $[x,d] \in L_{\phi}$. Como $[x,d]$ é crítico, a é crítico. Seja $K = ID(a)$ combinando os fatos que $[K,J] = 0$ e ambos as álgebras de Lie L/J e L/K são nilpotentes de classe $f(m,n)$-limitada deduzimos que L é solúvel com comprimento derivado $f(m,n)$-limitada. Isso implica que a classe de nilpotência de L é $f(m,n)$-limitada. □

O próximo resultado tem as hipóteses parecidas com o Teorema 5.1.6, porém não precisamos que o núcleo do grupo de *Frobenius* seja cíclico e ainda obtemos uma melhor limitação para o expoente do grupo G. Entretando pede-se que o grupo de *Frobenius* tenha ordem 12 e atue de maneira coprima sobre o grupo G.

Teorema 5.2.13. Suponha que o grupo de *Frobenius* de ordem 12 aja de forma coprima sobre um grupo finito G de tal maneira que $C_G(F) = 1$ e $C_G(H)$ tem expoente e. Então o expoente de G é limitado em termos de e.

Demonstração. A demonstração consiste em limitar os expoentes dos p-grupos de Sylow de G, onde G é um p-grupo, utilizando o metódo de Álgebras de Lie de *Jennings-Zassenhaus*.

Assim, sejam v_1, v_2 e v_3 as involuções de F e ϕ um gerador de H tal que $v_1^{\phi} = v_2$ e $v_2^{\phi} = v_3$. Denote $G_i = C_G(v_i)$ para $i = 1,2$ e 3, como por hipótese $(|G|, |FH|) = 1$ pelo Teorema 1.2.22, segue que FH normaliza um p-subgrupo de Sylow de G para cada primo dividido a ordem de G. Suponha que G seja um p-grupo finito ($p \geq 5$) e e uma potênca de p, no artigo [15], foi mostrado que o expoente de um grupo finito age por um grupo abeliano não-ciclíco A de ordem q^2 é limitado em termos de q e o expoente do $C_G(a)$, onde $a \in A \setminus \{1\}$,nesse caso F tem ordem q^2, com $q = 2$. Sob a hipótese do Teorema temos $G_1^{\phi} = G_2$ e $G_2^{\phi} = G_3$. Basta mostrarmos que G_1 é limitado por e. Observe que v_2 e v_3 atuam em G_1 tomando todos os elementos em seus inversos por Teorema 1.2.20. Portanto se $x \in G_1$, o subgrupo $\langle x, x^{\phi}, x^{\phi^2} \rangle$ é FH-invariante. Assim, podemos supor que existe um $x \in G_1$, tal que $G = \langle x, x^{\phi}, x^{\phi^2} \rangle$.

Seja $L = L_p(G) = \langle {}^{G}\!/_{D_2} \rangle$, denote por x_1, x_2 e x_3 as imagens de x, x^{ϕ} e x^{ϕ^2} respectivamente em ${}^{G}\!/_{D_2}$. Então $L = \langle x_1, x_2, x_3 \rangle$, observe que a ação do grupo FH em G pode ser traduzida para L como uma ação de automorfismo. Abusando da notação, denote FH o grupo de automorfismos de G e L. Como $p \neq 2,3$ segue-se que $C_{G/N}(V) = {}^{C_G(V)N}\!/_{N}$ para cada subgrupo V de FH e todo subgrupo normal N V-invariante de G. Como L é construido de quocientes FH-invariantes de G, muitas propriedades são traduzidas do $C_G(V)$ para $C_L(V)$. Pela hipótese $C_G(\phi)$ é um p-grupo de expoente e. Portanto, a solução de *Zelmanov* para o problema restrito de *Burnside* diz que dado dois elementos de $C_G(\phi)$ geram um subgrupo de classe de nilpotência e-limitada. Em L cada dois elementos homogêneos em $C_L(\phi)$ que geram uma subálgebra de classe e-limitada. Além disso, pela consequência do Lema 5.1.2 como todo elemento $C_L(\phi)$ tem ordem e então qualquer elemento do $C_L(\phi)$ é ad-nilpotente em L de índice no máximo e. Observe que $x_1^{\phi} = x_2$ e $x_2^{\phi} = x_3$.

Seja $L_i = C_L(v_i)$ para $i = 1,2,3$, lembre-se que v_1, v_2 e v_3 são involuções, logo L_i admite um automorfismo de ponto fixo de ordem 2 e assim cada L_i é abeliano. Além disso, temos $[L_1, L_2] \leq L_3, [L_2, L_3] \leq L_1$ e $[L_3, L_1] \leq L_2$. Logo, pelo Teorema 5.2.12 L é nilpotente de classe e-limitada. Assim, podemos deduzir pelo Lema 5.1.4 que G possui um subgrupo powerful de índice limitado por e. Portanto podemos supor que G é powerful. De acordo com Teorema 2.3.7 G é gerado pelos centralizadores $C_G(\phi^v)$, onde $v \in F$. Portanto G é gerado por elementos de ordem dividindo e. Os p-subgrupos powerful têm a propriedade de que se um p-grupo powerful é gerado por elementos de ordem dividindo p^k então o expoente do grupo divide p^k como mostra o Lema 1.3.8. Portanto, o expoente de G divide e. □

Capítulo 6

Considerações Finais

No decorrer deste trabalho vimos que se um grupo *Frobenius* age por automorfismos em um grupo finito G podemos conseguir algumas propriedades importantes sobre o grupo G. As propriedades encontradas tratam sobre nilpotência e expoente do grupo G. Alguns outros resultados relacionados ao estudo de nilpotência, solubilidade e expoente de um grupo G merecem ser destacados.

Um dos resultados que apresentamos neste trabalho foi a demonstração do item 1 do Problema 17.72 o qual trata de grupos 2-*Frobenius*. Uma generalização desse resultado foi obtida no artigo *Frobenius groups of automorphisms and their fixed points* [14], E. I. Khukhro, N. Yu. Makarenko e P. Shumyatsky onde foi provado o seguinte resultado.

Teorema 6.0.1. Suponha que um grupo finito G admita um grupo Frobenius FH com núcleo F e complemento H como grupo automorfismos tal que $C_G(F) = 1$ e $C_G(H)$ é nilpotente de classe c. Então G é nilpotente de classe limitada por c e $|H|$.

Outros resultados foram influenciados pelos Problemas do *The Kourovka Notebook* como no artigo *Supersolvable Frobenius groups with nilpotent centralizers* [3] onde Jhone Caldeira e Emerson de Melo provaram o seguinte resultado.

Teorema 6.0.2. Seja FH um grupo de *Frobenius* supersolúvel com núcleo F e complemento H. Suponha que um grupo finito G admite FH como grupo de automorfismo tal que $C_G(F) = 1$ e $C_G(H)$ é nilpotente de classe c. Então G é nilpotente de classe $(c, |FH|)$-limitada.

No contexto do Teorema acima, dizemos que um grupo G é supersolúvel se ele possui uma série normal

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

em que cada fator ${}^{G_i}\!/_{G_{i+1}}$ é cíclico e cada $G_i \trianglelefteq G$, para todo $i = 0, 1, \cdots, n-1$.

Além dos resultados anteriores, citamos outros dois resultados que limitam a classe de nilpotência de um grupo G. Os resultados são apresentados por Jhone Caldeira, Emerson de Melo e Pavel Shumyatsky no artigo *On groups and Lie algebras admitting a Frobenius group of automorphisms* [4] que mostram.

Teorema 6.0.3. Seja FH um grupo de *Frobenius* com núcleo não-cíclico abeliano F e complemento H de ordem t. Suponha que FH age coprimamente em um grupo finito G de tal maneira que $C_G(H)$ é nilpotente de classe c e $[C_G(u), \underbrace{C_G(v), \cdots, C_G(v)}_{\text{k}}]$ para qualquer $u, v \in F \setminus \{1\}$. Então G é nilpotente de classe (c,k,t)-limitada.

Teorema 6.0.4. Seja FH um grupo Frobenius com núcleo abeliano F de rank pelo menos três e com complemento H de ordem q. Suponha que FH atue coprimamente em um grupo finito G de tal maneira que $C_G(H)$ é nilpotente de classe c e $C_G(a)$ seja nilpotente de classe no máximo d para qualquer $a \in F \setminus \{1\}$. Então G é nilpotente de classe (c,d,q)-limitada.

Bibliografia

[1] Belyaev, V. V. and Hartley, B. (1996). Centralizers of finite nilpotent subgroups in locally finite groups. *Algebra and Logic*, 35(4):217–228.

[2] Burnside, W. (2012). *Theory of Groups of Finite Order*. Cambridge Library Collection - Mathematics. Cambridge University Press.

[3] Caldeira, J. and de Melo, E. (2019). Supersolvable frobenius groups with nilpotent centralizers. *Journal of Pure and Applied Algebra*, 223(3):1210 – 1216.

[4] Caldeira, J., de Melo, E., and Shumyatsky, P. (2012). On groups and lie algebras admitting a frobenius group of automorphisms. *Journal of Pure and Applied Algebra*, 216(12):2730 – 2736.

[5] Chao, C.-Y. (1968). Some characterizations of nilpotent lie algebras. *Mathematische Zeitschrift*, 103:40–42.

[6] Dade, E. C. (1969). Carter subgroups and fitting heights of finite solvable groups. *Illinois J. Math.*, 13(3):449–514.

[7] Dixon, J., Du Sautoy, M., Mann, A., and Segal, D. (2003). *Analytic Pro-P Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press.

[8] Feit, W. and Thompson, J. G. (1963). Chapter i, from solvability of groups of odd order, pacific j. math, vol. 13, no. 3 (1963). *Pacific J. Math.*, 13(3):775–787.

[9] Gorenstein, D. (1967). *Finite groups*. Harper's series in modern mathematics. Harper & Row.

[10] Hall, P. (1958). Some sufficient conditions for a group to be nilpotent. *Illinois J. Math.*, 2(4B):787–801.

[11] Higman, G. (1957). Groups and rings having automorphisms without non-trivial fixed elements. *Journal of the London Mathematical Society*, s1-32(3):321–334.

[12] Khukhro, E. (2011). *Nilpotent Groups and their Automorphisms*. De Gruyter Expositions in Mathematics. De Gruyter.

[13] Khukhro, E., Khoukhro, E., Society, L. M., and Hitchin, N. (1998). *P-Automorphisms of Finite P-Groups*. Lecture note series / London mathematical society. Cambridge University Press.

[14] Khukhro, E., Makarenko, N., and Shumyatsky, P. (2011). Frobenius groups of automorphisms and their fixed points. *Forum Mathematicum*, 26.

[15] Khukhro, E. and Shumyatsky, P. (1999). Bounding the exponent of a finite group with automorphisms. *Journal of Algebra*, 212(1):363 – 374.

[16] Khukhro, E. I. (2010). Fixed points of the complements of frobenius groups of automorphisms. *Siberian Mathematical Journal*, 51(3):552–556.

[17] Lawson, H. B. (1954). Sur les groupes nilpotents et les anneaux de lie. *Annales scientifiques de l'École Normale Supérieure*, 3e série, 71(2):101–190.

[18] Leedham-Green, C., McKay, S., McKay, S., McKay, L., and Society, L. M. (2002). *The Structure of Groups of Prime Power Order*. London Mathematical Society monographs. Oxford University Press.

[19] Makarenko, N. and Shumyatsky, P. (2010). Frobenius groups as groups of automorphisms. *Proceedings of the American Mathematical Society*, 138:3425–3425.

[20] Maslova, N. (2017). Gruenberg-kegel graphs of finite groups.

[21] Mazurov, V. D. and Khukhro, E. I. (2014). Unsolved problems in group theory. the kourovka notebook. no. 18 (english version). cite arxiv:1401.0300Comment: A few new solutions and references have been added. Preparation of the next 19th issue is underway, new problems are welcome, as well as comments on previous editions.

[22] Neumann, B. H. (1956). Groups with automorphisms that leave only the neutral element fixed. *Archiv der Mathematik*, 7(1):1–5.

[23] Robinson, D., Axler, S., Gehring, F., and Halmos, P. (1996). *A Course in the Theory of Groups*. Graduate Texts in Mathematics. Springer New York.

[24] Shalev, A. (1993). Automorphisms of finite groups of bounded rank. *Israel Journal of Mathematics*, 82(1):395–404.

[25] Shumyatsky, P. (2011). On the exponent of a finite group with an automorphism group of order twelve. *Journal of Algebra*, 331(1):482 – 489.

[26] Zel'manov, E. I. (1991). SOLUTION OF THE RESTRICTED BURNSIDE PROBLEM FOR GROUPS OF ODD EXPONENT. *Mathematics of the USSR-Izvestiya*, 36(1):41–60.