Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Variedades de Grupos e Generalizações Verbais para o Problema Restrito de Burnside

por

Jhone Caldeira Silva

Brasília

2009

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Variedades de Grupos e Generalizações Verbais para o Problema Restrito de Burnside

por

Jhone Caldeira Silva

Orientador: Prof. Dr. Pavel Shumyatsky

À memória de meu pai, José Martins da Silva, que profetizou em minha vida que um dia eu seria "doutor".

Ao meu orientador, Pavel Shumyatsky, pelos anos de convivência.

À Nossa Senhora, Mãe de Deus, cuidado constante em minha vida.

Agradecimentos

> "Pedi e se vos dará. Buscai e achareis. Batei e vos será aberto. Porque todo aquele que pede, recebe. Quem busca, acha. A quem bate, abrir-se-á. Quem dentre vós dará uma pedra a seu filho, se este lhe pedir pão? E, se lhe pedir um peixe, dar-lhe-á uma serpente? Se vós, pois, que sois maus, sabeis dar boas coisas a vossos filhos, quanto mais vosso Pai celeste dará boas coisas aos que lhe pedirem."
>
> Mt 7, 7-11.

Toda a sabedoria vem do Senhor Deus!

Agradeço a Deus, por permitir mais esta conquista e por me conduzir todos os dias.

À minha família.

Pessoas que amo. O que representam para mim está acima de qualquer conquista intelectual ou material.

Minha mãe, Rita Caldeira da Silva.

Meus irmãos, Adriana, Ângela, Dalton, Eliane, Eustáquio, Giovani, Jean, Rosângela (*in memorian*), Solange e Sueli.

Em especial à minha irmã Andrea por sempre afirmar que se realiza com minhas conquistas.

Meus sobrinhos, Aline, Ana Luiza, Andressa, Dávila, Débora, Dener, Deise, Diego, Elisa, Fernando, Jéssica, Joyce, Laís, Marcos Vinícius, Thiago, Yan Gabriel e Yasmin.

Meus cunhados, José Aparecido e Raquel, pela amizade e por todo incentivo.

Ao Professor Pavel Shumyatsky.

Pela orientação e por acreditar em mim até mais do que eu mesmo em muitos momentos.

Ao Professor Andrei Jaikin Zapirain.

Por todo apoio e pelo acompanhamento de minhas atividades durante o Doutorado Sandwich na *Universidad Autónoma de Madrid.*

Aos grandes amigos de profissão, Islândia, José Martins (Momeco) e Marinês Guerreiro.

Pelas motivações e todas as palavras de encorajamento.

Às amigas Aline, Raquel Lehrer e Sandra (Macu).

Por serem profundamente especiais e por todo impulso que me deram nos momentos mais relevantes.

Aos estimados amigos de república, Aline, Fernando, Jorge, Ricardo e Sandra.

Por serem a minha "família em Brasília".

Aos amigos, Dona Margarida, Dona Marli, Dona Silvinha, Sr. Benedito e Sr. Urbano.

Por todo carinho, pelas orações e por me acolherem como a um filho.

Aos amigos especiais, Adriana Barbosa (Dri), Alexandre Zaghetto, Aline Carraro (Amiga), Ana Paula Carraro (Aninha), Ana Sheila, Andreia Londres, Cláudia Rosane (Claudinha), Cristiane Gajo (Cris), Cristiane Rogéria (Cris), David Nascimento, Éric Duarte, Esmeralda Venzi (Esmel), Fabiana Carvalho (Fá), Fabiana Vieira, Fausto Camelo, Fernando Laércio, Gessiane Sieben (Gessy), Iara Nascimento (Iarinha), Jorge Cássio, Juliana Rabelo (Ju), Leandro Dalvi (Amigo), Márlon Crislei, Olimpio Ribeiro, Renata Rocha (Rê), Rogério César, Ruth Guimarães, Sandra Baccarin, Sheila Cristina (Danote) e Tatiana Angélica (Taty).

Por serem uma verdadeira expressão do amor de Deus em minha vida.

Aos amigos do MAT/UnB, Abílio, Adail, Anderson, André Galdino, Anyelle, Bianka, Daniel, Débora, Élida, Elenilson, Eunice, Evander, Karise, Kélem, Lineu, Manuela, Porfírio, Rosângela, Tânia, Thiago Porto, Tonires e Walter.

Pela convivência, amizade e partilha de conhecimentos, imprescindíveis para a realização deste projeto.

Aos amigos, Andrea Marcos, Hudson, Karina Romagnia, Mariella e Tatiana Rios.

Pela companhia e apoio durante a experiência na Europa.

Aos professores, Aline Pinto, Marinês Guerreiro, Noraí Rocco e Plamen Kochloukov.

Pelas correções, sugestões e contribuições para a versão final deste trabalho.

Aos professores e funcionários do MAT/UnB e a todos que de alguma forma contribuíram para a realização deste trabalho.

Ao CNPq e à CAPES pelo suporte financeiro.

Resumo

Neste trabalho abordamos os seguintes problemas, que generalizam o Problema Restrito de Burnside.

1. Sejam n um inteiro positivo e w uma palavra. Seja $\mathfrak{X}$ a classe de todos os grupos G satisfazendo a identidade $w^n \equiv 1$ e tendo o subgrupo verbal $w(G)$ localmente finito. Será que $\mathfrak{X}$ é uma variedade?

2. Sejam n um inteiro positivo e w uma palavra. Suponhamos que G é um grupo residualmente finito tal que todo w-valor tem ordem dividindo n. Será que o subgrupo verbal $w(G)$ é localmente finito?

No caso em que $w = x$, ambos tratam exatamente do Problema Restrito de Burnside que, de acordo com Zelmanov, tem resposta positiva. Discutimos resultados que apresentam respostas para muitas outras palavras w. Nossas principais contribuições são generalizações de resultados envolvendo comutadores multilineares e palavras de Engel. No desenvolvimento, somos levados a aplicar as técnicas Lie-teóricas introduzidas por Zelmanov.

Palavras chaves: Variedades de Grupos, Problema Restrito de Burnside, Álgebras de Lie.

Abstract

We study the following questions that generalize the Restricted Burnside Problem.

1. Let n be a positive integer and w a group-word. Consider the class of all groups G satisfying the identity $w^n \equiv 1$ and having the verbal subgroup $w(G)$ locally finite. Is that a variety?

2. Let n be a positive integer and w a group-word. Suppose that G is a residually finite group in which any w-value has order dividing n. Is the verbal subgroup $w(G)$ locally finite?

In the case $w = x$ the questions are precisely the Restricted Burnside Problem. According to Zelmanov this has positive solution. We show that the answer is positive for many other words w. The new results that we present are about multilinear commutators and Engel words. Our main tool is Zelmanov's techniques created in his solution of the Restricted Burnside Problem.

Key words: Varieties of Groups, Restricted Burnside Problem, Lie Algebras.

Lista de Símbolos

$G^{(n)}$	n-ésima derivada de G
$\gamma_n(G)$	n-ésimo termo da série central inferior de G
G^n	subgrupo gerado pelo conjunto das n-ésimas potências dos elementos de G
$N_G(H)$	normalizador de H em G
$C_G(H)$	centralizador de H em G
$\|G\|$	ordem de G
$\|G : H\|$	índice de H em G
$\langle S \rangle$	subgrupo gerado pelos elementos de S
$F(G)$	subgrupo de Fitting de G
$h(G)$	altura de Fitting de G
$h(n)$	número de divisores de n contando multiplicidades
$Frat(G)$	subgrupo de Frattini de G
$B(m, n)$	grupo livre de Burnside m-gerado de expoente n
adx	operador adjunto determinado por x

D_i	subgrupo de G definido por $D_i = D_i(G) = \prod_{jp^k \geq i} \gamma_j(G)^{p^k}$
$\mathbb{F}_p$	corpo formado por p elementos
$w(G)$	subgrupo verbal de G correspondente à palavra w
w_i	palavra que é produto de i δ_k-comutadores
u_i	palavra que é produto de i k-Engel valores
$O_{p'}(G)$	produto de todos os p'-subgrupos normais de G, onde p' é um número primo diferente de p
$\pi(G)$	conjunto de todos os números primos divisores de $\|G\|$

Sumário

Introdução **12**

1 Resultados Preliminares **17**

1.1 Grupos Solúveis e Grupos Nilpotentes 17

1.2 Produtos Cartesianos e Grupos Residualmente $\mathfrak{X}$ 21

1.3 Grupos Livres e Variedades de Grupos 22

1.4 Geradores de Subgrupos 26

1.5 O Teorema de Schur 27

1.6 O Teorema da Base de Burnside 30

2 O Problema de Burnside e Generalizações **31**

2.1 O Problema de Burnside: Breve Histórico 31

2.2 Variedades de Grupos e o Problema Restrito de Burnside 36

2.3 O Problema Restrito de Burnside para Grupos Residualmente Finitos . . . 42

3 Métodos Lineares em Grupos Nilpotentes **45**

3.1 Propriedades Imediatas de p-Grupos Regulares 46

3.2 Álgebras de Lie Associadas a p-Grupos 47

3.3 A Série de Jennings-Lazard-Zassenhaus 51

4 O Problema Restrito de Burnside para Comutadores Multilineares **59**

4.1 Limitando a Altura de Fitting de um Grupo Solúvel Finito 60

4.2 O Caso dos δ_k-Comutadores 64

4.3 O Caso dos Comutadores Multilineares 73

5 O Problema Restrito de Burnside para Palavras de Engel **76**

5.1 Limitando a Altura de Fitting de um Grupo Solúvel Finito 77

5.2 O Caso das Potências de Primos 81

5.3 O Caso Geral 85

6 Corolários para Grupos Residualmente Finitos **92**

Considerações Finais **95**

Referências Bibliográficas **97**

Índice Remissivo **103**

Introdução

Em 1902, William Burnside, em seu trabalho intitulado '*On an unsettled question in theory of discontinuous groups*', levantou a seguinte questão:

É verdade que todo grupo periódico é localmente finito?

Esta questão ficou conhecida como *O Problema Geral de Burnside*.

Outra formulação muito natural ficou conhecida como *O Problema de Burnside*:

É verdade que todo grupo de expoente n é localmente finito?

Ambos os problemas supracitados têm respostas negativas (na Seção 2.1 descrevemos maiores detalhes). Ainda no mesmo contexto, surgiu outro tema de investigação:

Será que dados inteiros $m, n \geq 2$, existe apenas um número finito de grupos m-gerados de expoente n que são finitos?

Esta questão é conhecida como *O Problema Restrito de Burnside* e foi respondida afirmativamente no ano de 1989 por meio de trabalhos de Zelmanov, os quais foram celebrados pela comunidade matemática.

A solução do Problema Restrito de Burnside por Zelmanov [59, 60] ofereceu grandes contribuições ao desenvolvimento da Teoria dos Grupos. Com a utilização dos métodos envolvidos, outros problemas vêm sendo resolvidos de maneira efetiva.

É bem conhecido que a solução do Problema Restrito de Burnside é equivalente a cada uma das seguintes afirmações:

2.2.2. *A classe de todos os grupos localmente finitos de expoente n é uma variedade.*

2.2.5. *A classe de todos os grupos localmente nilpotentes de expoente n é uma variedade.*

A equivalência das Afirmações 2.2.2 e 2.2.5 segue do famoso Teorema de Redução de Hall-Higman [11].

A partir das técnicas empregadas, generalizações do Problema Restrito de Burnside podem ser discutidas e algumas variedades de grupos interessantes têm sido descobertas.

Entendemos por variedade de grupos uma classe de grupos definida por equações. Mais precisamente, se W é um conjunto de palavras nas variáveis $x_1, x_2, \ldots$, a classe de todos os grupos G tais que $W(G) = 1$ é chamada de *variedade determinada por* W. Pelo Teorema de Birkhoff, variedades são aquelas classes de grupos fechadas com respeito a subgrupos, quocientes e produtos cartesianos de seus membros. Se w é uma palavra nas variáveis $x_1, x_2, \ldots, x_m$, podemos ver w como uma função de m variáveis definida sobre qualquer grupo dado G. Denotamos por $w(G)$ o subgrupo verbal de G gerado pelos valores de w. Nosso principal interesse é discutir certas generalizações para o Problema Restrito de Burnside. Nossas discussões estão focadas em fatos relacionados aos problemas abaixo, os quais foram propostos em [47].

Problema 2.2.7. *Sejam $n \geq 1$ e w uma palavra. Será que a classe de todos os grupos G satisfazendo a identidade $w^n \equiv 1$ e tendo $w(G)$ localmente finito é uma variedade?*

Problema 2.2.8. *Sejam $n \geq 1$ e w uma palavra. Será que a classe de todos os grupos G satisfazendo a identidade $w^n \equiv 1$ e tendo $w(G)$ localmente nilpotente é uma variedade?*

A palavra w é chamada de *comutador* se a soma dos expoentes de cada variável envolvida em w é igual a zero. De acordo com a solução do Problema Restrito de Burnside, as respostas para os Problemas 2.2.7 e 2.2.8 são positivas no caso particular em que $w = x$. Na verdade, a resposta é afirmativa sempre que w é uma palavra não-comutador (isto será demonstrado no Capítulo 2). Desta forma, os Problemas 2.2.7 e 2.2.8 são essencialmente sobre palavras comutadores. Não é conhecido se eles são equivalentes.

Em [46], o Problema 2.2.8 foi resolvido positivamente no caso em que w é a palavra central inferior $[x_1, x_2, \ldots, x_k]$. Em [47, 48] respostas positivas foram apresentadas para outras palavras. Com respeito ao Problema 2.2.7, em [49] Shumyatsky apresentou uma solução positiva no caso em que w é um produto de determinada quantidade de comutadores da forma $[x_1, x_2, \ldots, x_k]$. Mais precisamente, em [49] foi demonstrado o seguinte resultado:

Teorema 2.2.15. *Para quaisquer inteiros positivos k e n existe um inteiro positivo $t = t(k, n)$, dependendo apenas de k e n, tal que a classe de todos os grupos G tendo $\gamma_k(G)$ localmente finito e satisfazendo a propriedade de que todo produto de t comutadores da forma $[x_1, x_2, \ldots, x_k]$ tem ordem dividindo n é uma variedade.*

Um dos principais resultados que apresentamos nesta tese refere-se a uma resposta positiva para o Problema 2.2.7 quando w é um produto de certa quantidade de comutadores multilineares. Dizemos que w é um *comutador multilinear de peso k* quando w possui a forma de um monômio multilinear de Lie em exatamente k variáveis independentes. Exemplos particulares de comutadores multilineares são as palavras derivadas e as palavras centrais inferiores.

A seguir enunciamos nosso resultado, que foi apresentado em [51].

Teorema 4.0.1. *Seja w um comutador multilinear. Para qualquer inteiro positivo n existe um inteiro positivo $\mu = \mu(n)$, dependendo apenas de n, tal que a classe de todos os grupos G tendo o subgrupo verbal $w(G)$ localmente finito e satisfazendo a propriedade de que todo produto de μ w-valores em G tem ordem dividindo n é uma variedade.*

Observamos que o Teorema 4.0.1 melhora o Teorema 2.2.15 de duas formas:

(i) primeiramente, o novo resultado é provado para qualquer comutador multilinear (o resultado anterior refere-se apenas à palavras do tipo $[x_1, x_2, \ldots, x_k]$);

(ii) além disso, μ depende apenas de n (no resultado anterior, t depende de n e da palavra w).

Estas conquistas foram possíveis devido a uma conveniente aplicação do Teorema de Segal, que afirma que o grupo derivado de um grupo prosolúvel finitamente gerado é fechado [40].

Entendemos que o estudo mais relevante de comutadores não multilineares é certamente o caso das palavras de Engel. Estas são definidas indutivamente pelas equações:

$$[x,{}_0y]=x,$$

$$[x,{}_ky]=[[x,{}_{k-1}y],y].$$

Em [50], Shumyatsky apresentou o seguinte resultado:

Teorema 2.2.16. *Sejam q uma potência de primo e k um inteiro positivo. Existe um inteiro positivo $t=t(q,k)$, dependendo apenas de q e k, tal que a classe de todos os grupos G satisfazendo a identidade $([x_1,{}_ky_1]\cdots[x_t,{}_ky_t])^q\equiv 1$ e tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito é uma variedade.*

Neste trabalho estendemos o Teorema 2.2.16 para o caso em que n não é mais uma potência de primo e sim um inteiro positivo qualquer. Isto é exatamente o que diz o teorema a seguir, apresentado em [52].

Teorema 5.0.1. *Sejam n e k inteiros positivos. Existe um inteiro positivo $\lambda=\lambda(n,k)$, dependendo apenas de n e k, tal que a classe de todos os grupos G satisfazendo a identidade $([x_1,{}_ky_1]\cdots[x_\lambda,{}_ky_\lambda])^n\equiv 1$ e tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito é uma variedade.*

As demonstrações dos Teoremas 4.0.1 e 5.0.1 envolvem as seguintes ferramentas: a classificação dos grupos simples finitos, a teoria de Hall-Higman, os resultados Lie-teóricos de Zelmanov e o Teorema de Segal [40].

Discutimos, ainda, alguns resultados sobre grupos residualmente finitos relacionados a generalizações do Problema Restrito de Burnside. Consideramos o seguinte problema:

Problema 2.3.4. *Sejam n um inteiro positivo e w uma palavra. Suponhamos que G é um grupo residualmente finito tal que todo w-valor tem ordem dividindo n. Será que o subgrupo verbal $w(G)$ é localmente finito?*

Mais precisamente, apresentamos corolários de nossos principais resultados sobre variedades. Estes se referem a respostas positivas para o Problema 2.3.4:

Corolário 6.0.1. *Sejam n inteiro positivo e $\mu = \mu(n)$ como no Teorema 4.0.1. Se w é um comutador multilinear e G é um grupo residualmente finito satisfazendo a propriedade de que todo produto de μ w-valores tem ordem dividindo n, então o subgrupo verbal $w(G)$ é localmente finito.*

Corolário 6.0.2. *Sejam n e k inteiros positivos e $\lambda = \lambda(n,k)$ como no Teorema 5.0.1. Suponhamos que G é um grupo residualmente finito satisfazendo a identidade $([x_1, {}_k y_1] \cdots [x_\lambda, {}_k y_\lambda])^n \equiv 1$. Então o subgrupo verbal correspondente à k-ésima palavra de Engel é localmente finito.*

Enfatizamos que nossas discussões baseiam-se principalmente em estudar condições sobre o inteiro n e a palavra w no intuito de obtermos respostas positivas para os problemas propostos. O primeiro capítulo traz uma miscelânia de resultados da Teoria dos Grupos necessários para o desenrolar de nossas argumentações. O Capítulo 2 apresenta um breve histórico sobre o Problema de Burnside, bem como considerações a respeito de outras questões que generalizam o Problema Restrito de Burnside. No Capítulo 3 abordamos alguns métodos lineares em grupos nilpotentes, focando as técnicas Lie-teóricas encontradas na solução apresentada por Zelmanov. O Capítulo 4 é dedicado à demonstração do Teorema 4.0.1, que generaliza o Problema Restrito de Burnside considerando palavras que são comutadores multilineares, e o Capítulo 5 é focado em uma discussão similar para as palavras de Engel, onde demonstramos o Teorema 5.0.1. Finalmente, o sexto capítulo apresenta outra abordagem, focada em grupos residualmente finitos. Neste último demonstramos corolários imediatos dos principais resultados dos Capítulos 4 e 5.

Capítulo 1

Resultados Preliminares

Em todo o texto desta tese, a expressão "$\{m, n, l, \dots\}$-limitado" significa "limitado por uma função que depende apenas dos parâmetros $m, n, l, \dots$".

1.1 Grupos Solúveis e Grupos Nilpotentes

Seja G um grupo e sejam $x, y \in G$. O elemento $x^{-1}y^{-1}xy$ é chamado *comutador* de x e y e é denotado por $[x, y]$. O subgrupo de G gerado por todos os comutadores $[x, y]$, onde $x, y \in G$, é chamado *grupo derivado* de G.

O lema a seguir trata de propriedades elementares de comutadores. Uma demonstração pode ser encontrada em [37].

Lema 1.1.1. *Se G é um grupo e $x, y, z \in G$, então:*

(a) $[x, y]^{-1} = [x^{-1}, y^{-1}]$;

(b) $[x, y]^z = [x^z, y^z]$;

(c) $[xy, z] = [x, z]^y [y, z]$;

(d) $[x, yz] = [x, z] [x, y]^z$.

Se N e M são subconjuntos de um grupo G, definimos o comutador entre N e M por

$$[N, M] = \langle [n, m] : n \in N, m \in M \rangle .$$

Lema 1.1.2. *Sejam M, N, H subgrupos de um grupo G. Se $N \leq N_G(M) \cap N_G(H)$, então $[MN, H] = [M, H]\,[N, H]$.*

A *série derivada* de um grupo G é definida indutivamente da seguinte maneira:

$$G' = [G, G]\,,$$

$$G^{(n)} = \left[G^{(n-1)}, G^{(n-1)}\right],$$

onde o subgrupo $G^{(n)}$ é chamado *n-ésima derivada* de G; e a *série central inferior* de G é definida por

$$\gamma_1(G) = G,$$

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

Definição 1.1.3. *Um grupo G é dito solúvel se possui uma série*

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

cujos quocientes G_{i+1}/G_i são abelianos para todo i. Uma tal série é chamada série abeliana de G.

Quando G é solúvel, o comprimento da menor série abeliana de G é chamado *comprimento derivado de G*.

Uma propriedade elementar diz que a classe dos grupos solúveis é fechada com respeito a subgrupos, quocientes e extensões de seus membros. Além disso, o produto de dois subgrupos normais solúveis de um grupo é solúvel.

Definição 1.1.4. *Um grupo G é dito nilpotente se possui uma série normal*

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

cujos quocientes G_{i+1}/G_i estão contidos no centro de G/G_i para todo i. Uma tal série é chamada série central de G.

Quando G é nilpotente, o comprimento da menor série central de G é chamado *classe de nilpotência de* G.

A classe dos grupos nilpotentes é fechada com respeito a subgrupos e quocientes de seus membros. Também é válido que o produto de dois subgrupos normais nilpotentes de um grupo é nilpotente.

Em argumentações futuras, necessitaremos de algumas caracterizações de grupos solúveis e grupos nilpotentes. Resumidamente, apresentamos estas propriedades nos próximos resultados.

Lema 1.1.5. *Seja G um grupo. As seguintes afirmações são equivalentes.*

(a) *G é solúvel de comprimento derivado n;*

(b) *$G^{(n)} = 1$;*

(c) *G satisfaz uma identidade*

$$\delta_n(x_1, \ldots, x_{2^n}) \equiv 1,$$

onde

$$\delta_0(x) = x,$$
$$\delta_n(x_1, \ldots, x_{2^n}) = [\delta_{n-1}(x_1, \ldots, x_{2^{n-1}}), \delta_{n-1}(x_{2^{n-1}+1}, \ldots, x_{2^n})].$$

Lema 1.1.6. *Seja G um grupo.*

(a) *G é nilpotente de classe menor do que ou igual a n se, e somente se, $\gamma_{n+1}(G) = 1$.*

(b) *G finito é nilpotente se, e somente se, G é o produto direto de seus subgrupos de Sylow.*

Observação 1.1.7. *É importante notar que, para qualquer $n \in \mathbb{N}$, temos*

$$\gamma_n(G) = \langle [x_1, \ldots, x_n] : x_1, \ldots, x_n \in G \rangle$$
e
$$G^{(n)} = \langle \delta_n(x_1, \ldots, x_{2^n}) : x_1, \ldots, x_{2^n} \in G \rangle \; .$$

Listamos também algumas propriedades de operações e cálculos combinatórios envolvendo comutadores.

Lema 1.1.8. *Seja G um grupo e sejam M, N subconjuntos de G.*

(a) *Se $G = \langle M \rangle$, então $\gamma_n(G) = \langle [x_1, \ldots, x_n]^g : x_1, \ldots, x_n \in M, g \in G \rangle$.*

(b) *Se $G = \langle M \rangle$, então $\gamma_n(G) = \langle [x_1, \ldots, x_n], \gamma_{n+1}(G) : x_1, \ldots, x_n \in M \rangle$.*

(c) *Se $G = \langle a, b \rangle$, então $\gamma_2(G) = G' = \langle [a, b], \gamma_3(G) \rangle$. Em particular, $\gamma_2(G)/\gamma_3(G)$ é cíclico.*

Para um subconjunto M de um grupo G e $n \in \mathbb{N}$, denotamos $H^n = \langle x^n : x \in H \rangle$.

Lema 1.1.9 (Fórmula de Compilação de P. Hall)**.** *Sejam G um grupo e $x, y \in G$. Existem elementos $g_i = g_i(x, y) \in \gamma_i(\langle x, y \rangle)$ tais que*

$$x^n y^n = (xy)^n g_2^{\binom{n}{2}} g_3^{\binom{n}{3}} \ldots g_n,$$

para todo $n \in \mathbb{N}$. Em outras palavras,

$$x^n y^n \equiv (xy)^n \mod \gamma_2(\langle x, y \rangle)^{\binom{n}{2}} \gamma_3(\langle x, y \rangle)^{\binom{n}{3}} \ldots \gamma_n(\langle x, y \rangle).$$

Outros conceitos importantes em nossas discussões são o subgrupo de Fitting e a altura de Fitting de G. Definimos por *subgrupo de Fitting* de G, denotado por $F(G)$, como sendo o produto de todos os subgrupos normais nilpotentes de G. Claramente, se G é um grupo finito, então $F(G)$ é nilpotente. A *série de Fitting* de G é definida indutivamente da seguinte maneira:

$$F_0(G) = 1, \quad F_1(G) = F(G), \quad F_{i+1}(G)/F_i(G) = F(G/F_i(G)), \quad i = 1, 2, \ldots \quad .$$

Definição 1.1.10. *O menor número $h = h(G)$ com a propriedade $F_h(G) = G$, é chamado altura de Fitting de G.*

No caso em que G é um grupo solúvel finito, este número minimal sempre existe. Além disso, G é nilpotente se, e somente se, $h(G) = 1$.

Lema 1.1.11. *Seja G um grupo finito e seja $H \leq G$.*

(a) *Se H é subnormal em G, então $F(H) = H \cap F(G)$;*

(b) *H é nilpotente e subnormal em G se, e somente se, $H \leq F(G)$.*

1.2 Produtos Cartesianos e Grupos Residualmente $\mathfrak{X}$

Sejam $G_1, G_2, \ldots, G_n$ grupos. É fácil ver que o conjunto $G = G_1 \times G_2 \times \cdots \times G_n$, formado pelos elementos $(g_1, g_2, \ldots, g_n)$, onde $g_i \in G_i$, munido da multiplicação

$$(g_1, g_2, \ldots, g_n) \cdot (h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n)$$

é um grupo. Podemos estender esta ideia para uma família de grupos G_i, com $i \in I$. Denotemos por $G = \prod_{i \in I} G_i$ o conjunto das funções $f : I \to \bigcup_{i \in I} G_i$ satisfazendo a condição $f(i) \in G_i$, para todo $i \in I$. Agora definamos em G uma multiplicação dada por $(fg)(i) = f(i)g(i)$. Obtemos que G é um grupo, chamado *produto cartesiano dos grupos* G_i.

O valor da função f em um elemento $i \in I$ é chamado *projeção* de f sobre o *fator* G_i. Considerando os homomorfismos (projeções) $\prod_i : G \to G_i$, com $\prod_i(f) = f(i)$, temos $\prod_i(G) = G_i$. Esta propriedade motiva a definição a seguir.

Definição 1.2.1. *Seja G um produto cartesiano dos grupos G_i, $i \in I$. Qualquer subgrupo H de G com a propriedade $\prod_i(H) = G_i$, para todo $i \in I$, é chamado produto subcartesiano dos grupos G_i.*

Teorema 1.2.2 (Remak)**.** *Sejam G um grupo e N_i, $i \in I$, uma família de subgrupos normais de G. Se $N = \bigcap_{i \in I} N_i$, então G/N é isomorfo a um produto subcartesiano dos grupos G/N_i.*

Demonstração. Basta definir $\varphi : G \to \prod_{i \in I} G/N_i$ tal que se $g \in G$, então $\varphi(g) = f$, onde $f(i) = gN_i \in G/N_i$ e verificar que φ é homomorfismo cujo núcleo é N. ∎

Introduzimos agora a noção de grupo residualmente $\mathfrak{X}$ e um resultado relacionado que será importante neste trabalho.

Definição 1.2.3. *Seja $\mathfrak{X}$ uma classe de grupos. Um grupo G é dito residualmente $\mathfrak{X}$ se para todo $1 \neq g \in G$ existe um subgrupo normal N_g de G tal que $g \notin N_g$ e $G/N_g \in \mathfrak{X}$.*

Observamos que, nestas circunstâncias, $\bigcap_{1\neq g\in G} N_g = 1$.

Ainda é importante notar que um grupo residualmente $\mathfrak{X}$ não pertence necessariamente à classe $\mathfrak{X}$. Por exemplo, $\mathbb{Z}$ é um grupo infinito que é residualmente finito. De fato, consideremos $0 \neq z \in \mathbb{Z}$ e escolhamos um inteiro positivo n que não é um divisor de z. Seja $N = n\mathbb{Z}$. Temos que $z \notin N$ e N possui índice finito, pois $\mathbb{Z}/N \cong \mathbb{Z}_n$.

Teorema 1.2.4. *Seja $\mathfrak{X}$ uma classe de grupos. Um grupo G é residualmente $\mathfrak{X}$ se, e somente se, G é isomorfo a um produto subcartesiano de grupos em $\mathfrak{X}$.*

Demonstração. Supondo que G é um grupo residualmente $\mathfrak{X}$, consideremos $N = \bigcap_{1\neq g\in G} N_g$. Pelo Teorema de Remak, G/N é isomorfo a um produto subcartesiano de todos G/N_g. Mas, pela escolha, temos $N = 1$.

Agora, supondo que G é isomorfo a um produto subcartesiano D de grupos $G_i \in \mathfrak{X}$, consideremos $1 \neq g \in G$ e suponhamos $g_i \neq 1_{G_i}$. A projeção $\prod_i : D \to G_i$ induz um homomorfismo $\prod_i^* : G \to G_i$ tal que $\prod_i^*(G) = G_i$ e $g \notin ker \prod_i^* = N_i$. Agora basta ver que $G/N_i \cong G_i \in \mathfrak{X}$. ■

1.3 Grupos Livres e Variedades de Grupos

Variedades são classes de grupos definidas por equações. Por exemplo, a classe de todos os grupos abelianos é a variedade definida pela equação $x^{-1}y^{-1}xy = 1$, enquanto que a classe dos grupos nilpotentes de classe no máximo c de expoente n é a variedade definida pelo conjunto de equações $\{[x_1, x_2, \ldots, x_{c+1}] = 1, x^n = 1\}$.

Definição 1.3.1. *Sejam F um grupo e X um subconjunto de F. Dizemos que F é um grupo livre com base X se, para todo grupo G, qualquer aplicação $f : X \longrightarrow G$ pode ser estendida a um único homomorfismo $\varphi : F \longrightarrow G$. Em outras palavras, existe um único homomorfismo $\varphi : F \longrightarrow G$ tal que $\varphi(x) = f(x)$, para todo $x \in X$.*

Em geral denotamos $F = F(X)$. A cardinalidade do conjunto X é chamada *posto* do grupo livre $F(X)$.

A definição anterior refere-se à comutatividade do seguinte diagrama:

$$\begin{tikzcd} X \arrow[r, hook, "i"] \arrow[dr, "f"'] & F(X) \arrow[d, dotted, "\varphi"] \\ & G \end{tikzcd}$$

As demonstrações sobre a existência e a construção de grupos livres podem ser encontradas em [37, p. 159] e [38, p. 383].

Um resultado relevante é que a classe dos grupos livres é fechada com respeito a subgrupos. Além disso, qualquer grupo pode ser visto como um quociente de algum grupo livre. Este último é demonstrado aqui, pois nos será útil em discussões futuras.

Teorema 1.3.2. *Seja G um grupo. Então G é um quociente de algum grupo livre $F(X)$.*

Demonstração. Consideremos o conjunto $X = \{x_g : g \in G\}$ e a aplicação $f : X \longrightarrow G$ satisfazendo $f(x_g) = g$. É fácil ver que f é uma bijeção. Agora, se $F(X)$ é o grupo livre com base X, então existe um homomorfismo $\varphi : F(X) \longrightarrow G$ que estende f. Como f é sobrejetiva, segue que φ é sobrejetivo e, assim, $G \cong F(X)/ker\varphi$. ∎

Apresentamos agora um resultado que nos permite limitar em certo sentido o número de subgrupos H de um grupo G cujos índices $|G : H|$ são limitados.

Teorema 1.3.3. *Seja F_r o grupo livre de posto r. O número $h_{n,r}$ de subgrupos de índice n em F_r é dado recursivamente por*

$$h_{1,r} = 1,$$

$$h_{n,r} = n(n!)^{r-1} - \sum_{i=1}^{n-1}(n-i)!^{r-1}h_{i,r} .$$

Uma demonstração para este teorema pode ser encontrada em [18, Teorema 7.2.9]. É importante observar que $h_{n,r}$ é limitado em termos apenas de n e r.

Seja $F(X)$ um grupo livre com geradores em um conjunto infinito enumerável $X = \{x_1, x_2, \ldots\}$. Supondo que os índices i's dos x_i's são bem ordenados, definimos uma *palavra* no alfabeto X como sendo qualquer sequência finita de elementos de $X \cup X^{-1}$, onde $X^{-1} = \left\{x_1^{-1}, x_2^{-1}, \ldots\right\}$.

Se G é um grupo qualquer e $w = w(x_1, x_2, \ldots, x_r)$ é um elemento do grupo livre $F(X)$, então w pode ser visto como uma função de r variáveis definida sobre G. Sendo $g_1, g_2, \ldots, g_r$ elementos de G, a imagem da r-upla $(g_1, g_2, \ldots, g_r)$, denotada por $w(g_1, g_2, \ldots g_r)$, é chamada *valor de w* ou *w-valor* em G. O subgrupo de G gerado por todos os w-valores em G é chamado *subgrupo verbal correspondente a w* e é denotado por $w(G)$. Por exemplo, se $w = [x, y]$ e $u = [x_1, x_2, \ldots, x_k]$, então $w(G) = G'$ e $u(G) = \gamma_k(G)$.

De forma mais geral, podemos considerar W um conjunto de palavras no alfabeto X e, assim, $W(G)$ é o subgrupo verbal gerado por todos os *w-valores* em G, para todo $w \in W$.

Definição 1.3.4. *Uma palavra w é uma identidade (ou uma lei) em um grupo G se todos os w-valores em G são triviais.*

Para indicar que a palavra w é uma identidade em G, escrevemos $w \equiv 1$ em G.

Definição 1.3.5. *Seja W um conjunto de palavras num alfabeto X. A classe $\mathfrak{X}$ de todos os grupos G nos quais valem $W(G) \equiv 1$ é chamada variedade determinada por W.*

É fácil ver que a classe dos grupos abelianos, a classe dos grupos nilpotentes de classe no máximo c e a classe dos grupos solúveis de comprimento derivado no máximo d são exemplos de variedades. Já a classe dos grupos finitos não é uma variedade.

Comentamos anteriormente que um grupo residualmente $\mathfrak{X}$ não necessariamente pertence à classe $\mathfrak{X}$. Por outro lado, temos a

Proposição 1.3.6. *Seja $\mathfrak{X}$ uma variedade de grupos. Se G é um grupo residualmente $\mathfrak{X}$, então $G \in \mathfrak{X}$.*

O próximo teorema nos diz que variedades sempre possuem grupos livres e será utilizado na demonstração do conhecido Teorema de Birkhoff.

Teorema 1.3.7. *Seja $\mathfrak{X}$ uma variedade de grupos determinada por um conjunto de identidades W. Um grupo G está em $\mathfrak{X}$ se, e somente se, G é um quociente de $\dfrac{F(X)}{W(F(X))}$, para algum grupo livre $F(X)$.*

O grupo $\dfrac{F(X)}{W(F(X))}$ é conhecido como sendo o *grupo livre na variedade* $\mathfrak{X}$.

Podemos também tratar variedades como certas classes fechadas de grupos. Por um lado, é de fácil verificação que se $\mathfrak{X}$ é uma variedade de grupos, então $\mathfrak{X}$ é uma classe fechada com respeito a subgrupos, quocientes e produtos cartesianos de seus membros. Encerramos esta seção com a recíproca disso, que é um resultado muito utilizado e nos fornece uma equivalência para definirmos variedades de grupos [37].

Teorema 1.3.8 (Birkhoff)**.** *Seja $\mathfrak{X}$ uma classe de grupos. Se $\mathfrak{X}$ é fechada em relação a subgrupos, quocientes e produtos cartesianos de seus membros, então $\mathfrak{X}$ é uma variedade.*

Demonstração. Seja W o conjunto das identidades que valem em todos os grupos em $\mathfrak{X}$. Seja $\mathfrak{A}$ a variedade determinada por W. Claramente, $\mathfrak{X} \subseteq \mathfrak{A}$. Mostraremos que $\mathfrak{A} \subseteq \mathfrak{X}$. Vamos assumir que $\mathfrak{X}$ contém um grupo de ordem maior do que 1, caso contrário teríamos que $\mathfrak{A} = \mathfrak{X} = \{\text{Classe dos Grupos de Ordem } 1\}$.

Seja $\overline{F}$ um grupo livre em $\mathfrak{A}$. É suficiente mostrar que $\overline{F} \in \mathfrak{X}$, pois qualquer grupo em $\mathfrak{A}$ é um quociente de $\overline{F}$ e a classe $\mathfrak{X}$ é fechada com respeito a quocientes. Iremos construir um produto cartesiano de grupos em $\mathfrak{X}$ envolvendo o grupo livre $\overline{F}$ e isto implicará que $\overline{F} \in \mathfrak{X}$, uma vez que $\mathfrak{X}$ também é fechada para produtos cartesianos. Pelo Teorema 1.3.7, $\overline{F} \cong \dfrac{F(X)}{W(F(X))}$, para algum alfabeto $X = \{x_i : i \in I\}$. Para cada palavra $w(x_1, \ldots, x_r) \notin W$ e cada r-upla ordenada $i = (i_1, \ldots, i_r)$ de elementos distintos de I, escolhamos um grupo $G_{w,i}$ em $\mathfrak{X}$ e alguns de seus elementos $g^j_{w,i}$, $j \in I$, tais que $w(g^{i_1}_{w,i}, \ldots, g^{i_r}_{w,i}) \neq 1$. Desta forma, existe um homomorfismo

$$\varphi_w : \overline{F} \longrightarrow G_{w,i}, \quad \text{onde} \quad \varphi_w(wW(F)) \neq 1.$$

Definamos o produto cartesiano

$$G = \prod_{(w,i)} G_{w,i}$$

sobre todos os pares (w, i), tais que $w \notin W$. Como $\mathfrak{X}$ é fechada em relação a produtos cartesianos, $G \in \mathfrak{X}$. Consideremos agora o homomorfismo

$$\varphi : \overline{F} \longrightarrow G$$

tal que a imagem de um elemento x na w-ésima posição é $\varphi_w(x)$. Pela definição de φ, temos $ker\varphi = W(F)$. Portanto, $\overline{F} \cong \varphi(\overline{F}) < G$. Como $\mathfrak{X}$ é fechada em relação a subgrupos, a demonstração está concluída. ■

1.4 Geradores de Subgrupos

Nesta seção faremos uma breve discussão a respeito de um resultado que nos permite limitar o número de geradores de subgrupos em um grupo finitamente gerado. Para isto, introduzimos o conceito de transversal.

Dado um inteiro positivo m, dizemos que um grupo G é *m-gerado* se existe um subconjunto $\{g_1, g_2, \ldots, g_m\} \subseteq G$ tal que $G = \langle g_1, g_2, \ldots, g_m \rangle$. Quando não houver possibilidade de confusão, também pode significar gerado por no máximo m elementos. Dizemos que G é *finitamente gerado* se G é m-gerado, para algum m.

Definição 1.4.1. *Sejam G um grupo e H um subgrupo de G. Um conjunto formado por um representante de cada classe lateral à direita (à esquerda) de H em G é chamado transversal à direita (à esquerda) de H em G.*

É bem conhecido que a classe de todos os grupos finitamente gerados não é fechada a subgrupos, pois existem grupos finitamente gerados que possuem subgrupos que não são finitamente gerados. Podemos citar o exemplo do produto entrelaçado de $\mathbb{Z}$ por $\mathbb{Z}$. Porém no caso de um subgrupo H ter índice finito em um grupo finitamente gerado, podemos garantir que H é finitamente gerado. Isto é exatamente o que diz o teorema a seguir.

Teorema 1.4.2. *Seja G um grupo finitamente gerado. Se H é um subgrupo de índice finito de G, então H é finitamente gerado.*

Demonstração. Como G é finitamente gerado, consideremos um conjunto finito X tal que $G = \langle X \rangle$. Suponhamos que $|G : H| = n$ e seja $T = \{t_1, t_2, \ldots, t_n\}$ um transversal à direita de H em G escolhido de tal modo que $t_1 = 1$. Assim, $T(X \cup X^{-1})T^{-1}$ é um conjunto finito. Afirmamos que $H = \langle T(X \cup X^{-1})T^{-1} \cap H \rangle$.

De fato, dado $a \in H$, podemos escrever $a = x_1x_2 \cdots x_r$, onde $x_1, x_2, \ldots, x_r \in X \cup X^{-1}$. Para todo $i \in \{1, 2, \ldots, r\}$ e todo $g \in G$, existem $h = h(i, g)$ e $j = j(i, g)$ tais que $t_i g = ht_j$. Desta forma, $h = t_i g t_j^{-1} \in TgT^{-1}$ e, para certos $h_1, h_2, \ldots, h_r \in T(X \cup X^{-1})T^{-1} \cap H$ e $i_1, i_2, \ldots, i_r \in \{1, 2, \ldots, r\}$, podemos escrever:

$$\begin{aligned}
a &= t_1 a = (t_1 x_1)x_2x_3 \cdots x_r = (h_1 t_{i_1})x_2x_3 \cdots x_r \\
&= h_1(t_{i_1}x_2)x_3 \cdots x_r = h_1(h_2 t_{i_2})x_3 \cdots x_r \\
&\vdots \\
&= h_1h_2h_3 \cdots h_{r-2}(t_{i_{r-2}}x_{r-1}) \\
&= h_1h_2h_3 \cdots h_{r-2}h_{r-1}t_{i_{r-1}}x_r \\
&= h_1h_2h_3 \cdots h_{r-2}h_{r-1}h_r t_{i_r}
\end{aligned}$$

e daí segue que $t_{i_r} = h_r^{-1}h_{r-1}^{-1} \cdots h_3^{-1}h_2^{-1}h_1^{-1}a \in H$. Portanto, $t_{i_r} = t_1 = 1$ e, consequentemente, $a = h_1h_2 \cdots h_{r-1}h_r$, onde $h_1, \ldots, h_r \in T(X \cup X^{-1})T^{-1} \cap H$. ■

Observação 1.4.3. *A demonstração do teorema anterior nos dá que*

$$H = \langle T(X \cup X^{-1})T^{-1} \cap H \rangle.$$

É conhecido que se G é um grupo m-gerado e H um subgrupo de G tal que $|G : H| = n$, então $|T(X \cup X^{-1})T^{-1} \cap H|$ é, no máximo, $2(n-1)^2 m$. Assim, concluímos que o número de geradores de H é $\{m, n\}$-limitado.

1.5 O Teorema de Schur

Aqui apresentamos o Teorema de Schur. Para isto, necessitamos da noção de Homomorfismo Transfer.

Consideremos G um grupo e H um subgrupo de G com índice finito, digamos n. Escolhendo $T = \{t_1, t_2, \ldots, t_n\}$ um transversal à direita correspondente a H em G, temos $Hgt_i = Ht_{g(i)}$, com $g \in G$, onde a aplicação $i \longmapsto g(i)$ é uma permutação do conjunto $\{1, 2, \ldots, n\}$. Assim, $gt_i t_{g(i)}^{-1} \in H$, para todo $g \in G$.

Definição 1.5.1. *Seja $\theta : H \longrightarrow A$ um homomorfismo de um grupo H para um grupo abeliano A. Definimos o Homomorfismo Transfer de θ como sendo a aplicação $\theta^* : G \longrightarrow A$ dada por*

$$\theta^*(x) = \prod_{i=1}^{n} \theta(xt_i t_{x(i)}^{-1}).$$

Não há preocupação com a ordem dos fatores no produto, pois A é abeliano. Além disso, temos que:

(i) θ^* é um homomorfismo de grupos;

(ii) θ^* é determinado independentemente da escolha do transversal T.

Um caso de Homomorfismo Transfer de interesse especial ocorre quando H é central em G.

Teorema 1.5.2. *Sejam G um grupo e H um subgrupo de $Z(G)$. Se $|G : H| = n$, então o Homomorfismo Transfer de G em H é*

$$\begin{aligned} \theta^* : G &\longrightarrow H \\ x &\longmapsto x^n \ . \end{aligned}$$

Demonstrações para os resultados anteriores podem ser encontradas em [37]. Nosso interesse maior está no próximo teorema, pois será utilizado posteriormente.

Teorema 1.5.3 (Schur)**.** *Seja G um grupo tal que $Z(G)$ tem índice finito n. Então G' é finito de ordem $\{n\}$-limitada e $(G')^n = 1$.*

Demonstração. Denotemos $Z = Z(G)$ e consideremos $G/Z = \{Zx_1, \ldots, Zx_n\}$. Para quaisquer $z_i, z_j \in Z$ obtemos, utilizando identidades de comutadores, que $[z_i x_i, z_j x_j] = [x_i, x_j]$. Desta forma, G' é gerado pelos $\binom{n}{2}$ comutadores $[x_i, x_j]$ para $i < j$. Como $\dfrac{G'}{G' \cap Z} \cong \dfrac{G'Z}{Z}$ é finito de ordem $\{n\}$-limitada, pela Observação 1.4.3, segue que o número de geradores de $G' \cap Z$ é $\{n\}$-limitado. Sabemos, pelo Teorema 1.5.2, que o Homomorfismo Transfer de G para Z é

$$\begin{aligned} \theta^* : G &\longrightarrow Z \\ x &\longmapsto x^n \ , \end{aligned}$$

que possui núcleo $ker\theta^* = \{x \in G : x^n = 1\}$. Já que $G/ker\theta^*$ é isomorfo a um subgrupo de Z, temos $G' \leq ker\theta^*$ e, consequentemente, $(G')^n = 1$. Desta forma, concluímos que $G' \cap Z$ é abeliano, de expoente finito dividindo n, com número de geradores $\{n\}$-limitado e, portanto, é finito de ordem $\{n\}$-limitada. Segue que G' é também finito e de ordem $\{n\}$-limitada. ■

Definição 1.5.4. *Seja $\mathfrak{X}$ uma classe de grupos. Dizemos que um grupo G é <u>localmente $\mathfrak{X}$</u> se todo subgrupo finitamente gerado de G pertence a $\mathfrak{X}$.*

No caso em que $\mathfrak{X}$ é a classe dos grupos finitos, temos o

Corolário 1.5.5. *Se $G/Z(G)$ é localmente finito, então G' é localmente finito.*

Demonstração. Consideremos em G' um subgrupo $H = \langle x_1, x_2, \ldots, x_n \rangle$. Basta mostrar que H é finito. De acordo com a demonstração do Teorema 1.5.3, temos $x_i = c_{1i}c_{2i}\cdots c_{ri}$, onde $c_{ji} = [g_{ji}, l_{ji}]$, $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, r\}$. Assim, $H \leq K'$, onde $K = \langle g_{ij}, l_{ij} : i \in \{1, \ldots, n\}, j \in \{1, \ldots, r\} \rangle$ é finitamente gerado. Logo $K/K \cap Z(G)$ é finitamente gerado e, portanto, finito. Notemos que $K \cap Z(G) \leq Z(K)$, donde $K/Z(K)$ é finito. Pelo Teorema 1.5.3, K' é finito e, assim, H é finito. ■

Observamos que é bastante simples verificar que a classe formada por todos os grupos localmente finitos é fechada com respeito a subgrupos e quocientes. A seguir vemos que também não é difícil mostrar que esta classe é fechada com respeito a extensões.

Teorema 1.5.6 (Schmidt)**.** *Se $N \lhd G$ e ambos G e G/N são localmente finitos, então G é localmente finito.*

Demonstração. Consideremos H um subgrupo arbitrário finitamente gerado de G e mostremos que H é finito. Temos $H/H \cap N \cong HN/N$, que é finito. Pelo Teorema 1.4.2, $H \cap N$ é finitamente gerado, logo, finito. Portanto, H é finito. ■

1.6 O Teorema da Base de Burnside

O estudo de p-grupos finitos tem relevância fundamental na Teoria dos Grupos, de modo especial na investigação de propriedades em grupos nilpotentes finitos. Nesta seção apresentamos o Teorema da Base de Burnside, que nos permite mostrar que em qualquer conjunto de geradores de um p-grupo finito m-gerado P é possível escolher um subconjunto de m elementos que também gera P.

Dado um grupo G, definimos o *subgrupo de Frattini* de G, $Frat(G)$, como sendo a interseção de todos os subgrupos maximais de G. Ressaltamos que, no caso em que G não possui subgrupos maximais, definimos $Frat(G) = G$.

É bem conhecido que $Frat(G)$ é igual ao conjunto dos elementos não-geradores de G [37, p. 135].

Teorema 1.6.1 (Teorema da Base de Burnside)**.** *Se P é um p-grupo finito, então o quociente $P/Frat(P)$ é um grupo abeliano elementar. Além disso, se $|P : Frat(P)| = p^m$, então todo conjunto de geradores de P contém um subconjunto de m elementos que gera P.*

Demonstração. Denotemos $F = Frat(P)$ e $\overline{P} = P/F$. Se M é um subgrupo maximal de P, então M é normal em P e M possui índice p em P. Assim, P/M é cíclico de ordem p. Segue que a p-ésima potência e todo comutador de elementos em P estão contidos em M. Como F é a interseção dos subgrupos maximais de P, F contém todas as p-ésimas potências e todos os comutadores de elementos em P. Portanto, $\overline{P}$ é abeliano elementar.

Agora suponhamos $|P : F| = p^m$. Toda base de $\overline{P}$ possui m elementos. Como F é o conjunto dos elementos não-geradores de P, temos que $P = \langle x_1, x_2, \ldots, x_r\rangle$ se, e somente se, $\overline{P} = \langle x_1F, x_2F, \ldots, x_rF\rangle$. Já que $\overline{P}$ pode ser visto como espaço vetorial de dimensão m sobre um corpo com p elementos, existe uma base $\{x_{i_1}F, x_{i_2}F, \ldots, x_{i_m}F\}$ para $\overline{P}$. Escolhendo $X = \{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$, concluímos que $P = \langle X, F\rangle$ e, finalmente, $P = \langle X\rangle$. ■

Assim, podemos escrever uma consequência imediata:

Corolário 1.6.2. *Se P é um p-grupo finito m-gerado, então qualquer conjunto de geradores de P contém um subconjunto gerador de P possuindo m elementos.*

Capítulo 2

O Problema de Burnside e Generalizações

2.1 O Problema de Burnside: Breve Histórico

Nesta seção apresentamos breves comentários a respeito da história do Problema de Burnside sobre grupos periódicos.

Um grupo G é dito *periódico* (ou *de torção*) se todo subgrupo cíclico de G é finito, ou seja, se todo elemento de G tem ordem finita. Assim, todo grupo localmente finito é periódico. Já a discussão da recíproca disto foi tema de grandes investigações no século anterior e muitas outras questões foram levantadas e vem sendo discutidas desde então. Em 1902, William Burnside, em seu trabalho intitulado '*On an unsettled question in theory of discontinuous groups*', levantou o seguinte problema:

(I) *É verdade que todo grupo periódico é localmente finito?*

Equivalentemente,

(II) *É verdade que todo grupo periódico finitamente gerado é finito?*

Esta questão ficou conhecida como *O Problema Geral de Burnside* e permaneceu em aberto por algum tempo até que, em 1964, Golod [6] apresentou um contra-exemplo: construiu, para todo primo p e todo $d \geq 2$, um p-grupo infinito, d-gerado, tal que todo subgrupo $(d-1)$-gerado é finito. Esta tinha sido a primeira resposta negativa para (II) e outros contra-exemplos foram surgindo por meio de diferentes técnicas, com trabalhos de Aleshin em 1972 utilizando a teoria dos autômatas [2], de Sushchansky em 1979 utilizando grupos de permutações [54], de Grigorchuk em 1980 utilizando técnicas de análise funcional [8], de Gupta e Sidki em 1983 utilizando automorfismos de árvores [10].

Quando as ordens dos elementos de G são finitas e limitadas, dizemos que G tem expoente finito. Assim, G tem expoente n se $x^n = 1$, para todo $x \in G$. Seja F_m o grupo livre com m geradores e consideremos N o subgrupo normal de F_m gerado pelo conjunto $\{x^n : x \in F_m\}$ (o subgrupo verbal correspondente à palavra $w(x) = x^n, x \in F_m$). Denotemos por $B(m,n)$ o quociente F_m/N, geralmente chamado de *Grupo Livre de Burnside m-gerado de expoente n.* Qualquer grupo G m-gerado de expoente n é uma imagem homomórfica de $B(m,n)$. Isto porque $G \cong F_m/K$, onde $K \supseteq N$ (uma vez que pode existir outra relação definidora de G além de $g^n = 1$) e podemos observar que

$$\frac{B(m,n)}{K/N} = \frac{F_m/N}{K/N} \cong F_m/K \cong G.$$

Além disso, o grupo $B(m,n)$ é livre na variedade dos grupos de expoente n. Com estas considerações, apresentamos outra versão de (I) conhecida como *O Problema de Burnside.* Esta versão também despertou grande interesse da comunidade científica e podemos escrevê-la de algumas maneiras, todas equivalentes:

(III) *É verdade que todo grupo de expoente n é localmente finito?*

(IV) *É verdade que todo grupo de expoente n finitamente gerado é finito?*

(V) *É verdade que $B(m,n)$ é finito?*

Observamos que respostas negativas para (III), (IV) e (V) implicam respostas negativas para (I) e (II) e que respostas afirmativas para (I) e (II) não implicam respostas afirmativas para (III), (IV) e (V).

É fácil ver que $B(1,n)$ e $B(m,2)$ são ambos finitos, pois o primeiro é o grupo cíclico de ordem n e o segundo é um 2-grupo abeliano elementar. Burnside provou em 1902 que $B(m,3)$ é finito; Sanov [39], em 1940, mostrou que $B(m,4)$ é finito; e já em 1958, Marshall Hall Jr. [17] mostrou que $B(m,6)$ é finito. A resposta para *O Problema de Burnside* também é negativa e o primeiro contra-exemplo apareceu com Novikov e Adian [33], em 1968, em um trabalho onde demonstraram que, para todo $n \geq 4381$, n ímpar, e para todo $m > 1$, existe um grupo infinito $\Gamma(m,n)$ que é m-gerado e possui expoente n. Em 1975, Adian [1] melhora este último resultado considerando $n \geq 665$, n ímpar. Outros resultados neste sentido foram obtidos, por exemplo, com trabalhos de Olshanskii [34], que construiu o grupo que ficou conhecido como *Monstro de Tarsky* (grupo infinito onde todo subgrupo próprio tem ordem prima p, com p suficientemente grande); de Ivanov [15], que em 1992 mostrou que $B(m,n)$ é infinito para todo $m > 1$ e n suficientemente grande, a saber, $n \geq 2^{48}$; e de Lysionok [27], que apresentou solução negativa para $n \geq 8000$, n divisível por 16. Muitos pesquisadores se dedicaram à investigação da finitude ou não de $B(m,n)$, procurando descobrir quais valores de m e n levariam a grupos finitos e quais poderiam levar a grupos infinitos. Contudo, ainda há problemas em aberto e podemos citar que as finitudes de $B(m,n)$, para $n = 5, 8, 9, 12$, ainda são desconhecidas.

Vimos que a resposta para *O Problema de Burnside* é negativa, ou seja, $B(m,n)$ em geral é infinito. Sendo assim, podemos apresentar outra pergunta:

Será que existe apenas um número finito de quocientes finitos
não isomorfos de $B(m,n)$?

Em outras palavras, será que dados inteiros $m, n \geq 2$, existe apenas um número finito de grupos m-gerados de expoente n que são finitos? Esta questão ficou conhecida como *O Problema Restrito de Burnside* e foi respondida afirmativamente em 1989 com um trabalho premiado de Zelmanov [59, 60]. Em 1956, P. Hall e G. Higman [11] apresentaram importantíssimos resultados relacionados com este problema, onde reduzem o Problema Restrito de Burnside ao caso de grupos com expoente potência de primo e obtêm, assim, contribuições relevantes para uma resposta afirmativa por meio de conjecturas sobre a classificação dos grupos simples finitos (tais conjecturas foram confirmadas na década de 80 do século passado). Em 1959, A. I. Kostrikin [25] apresentou uma solução parcial, demonstrando o caso em que o expoente do grupo é um número primo. Suas discussões basearam-se em um profundo estudo de álgebras de Lie de característica prima com condições de Engel.

As técnicas utilizadas por Zelmanov em sua solução consideram álgebras de Lie com condições de Engel e resultados de P. Hall e G. Higman. Seus métodos inspiraram a muitos outros investigadores e ainda hoje são aplicados na resolução de problemas em Teoria dos Grupos. Os principais resultados que discutimos nesta tese estão relacionados com o Problema Restrito de Burnside e por esta razão apresentamos a seguir formas equivalentes de escrevê-lo.

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

(VII) *É verdade que $B(m,n)$ possui somente um número finito de subgrupos de índice finito?*

(VIII) *É verdade que todo grupo residualmente finito de expoente n é localmente finito?*

(IX) *É verdade que a classe de todos os grupos localmente finitos de expoente n é uma variedade?*

De fato (VI)-(IX) são equivalentes. Sigamos com a demonstração.

(*i*) (VI) $\Rightarrow$ (VIII): Consideremos G um grupo residualmente finito de expoente n e podemos assumir que G é m-gerado. Como G é residualmente finito, existe uma série $G \triangleright N_1 \triangleright N_2 \triangleright N_3 \triangleright \cdots$ tal que $\bigcap\limits_i N_i = 1$ e G/N_i é finito, para todo i. Além disso, temos $|G/N_1| \leq |G/N_2| \leq |G/N_3| \leq \cdots$ e, como G/N_i é finito, m-gerado e de expoente dividindo n, temos por (VI) que a série acima é estacionária a partir de algum j. Sendo G residualmente finito, segue que $N_j = 1$ e, portanto, G é finito.

(ii) (VIII) $\Rightarrow$ (VII): Consideremos $K = \bigcap_{\substack{H \leq B(m,n) \\ |B(m,n):H| < \infty}} H$. Temos $K \lhd B(m,n)$ e $B(m,n)/K$ residualmente finito. Por (VIII), $B(m,n)/K$ é finito. Existe uma correspondência biunívoca entre os subgrupos de índice finito de $B(m,n)$ e os subgrupos de $B(m,n)/K$ e, como este último é finito, existe somente um número finito de subgrupos de índice finito em $B(m,n)$.

(iii) (VII) $\Rightarrow$ (VI): Seja G um grupo finito m-gerado de expoente n. Sabemos que G é isomorfo a um quociente de $B(m,n)$ e, assim, (VII) nos dá que existe o maior quociente finito de $B(m,n)$, digamos $Q(m,n)$. Portanto, $|G| \leq |Q(m,n)|$.

(iv) (VIII) $\Rightarrow$ (IX): Seja $\mathfrak{X}$ a classe de todos os grupos localmente finitos de expoente n. É fácil ver que $\mathfrak{X}$ é fechada com respeito a subgrupos e quocientes de seus membros. Assim, pelo Teorema de Birkhoff, basta mostrar que sendo $D = \prod_i G_i$ um produto cartesiano de grupos em $\mathfrak{X}$, então $D \in \mathfrak{X}$. Claramente D tem expoente n e, assim, basta tomar H um subgrupo finitamente gerado de D e mostrar que H é finito. Seja $H_i \leq G_i$ a projeção de H em G_i. Como H é finitamente gerado, concluímos que H_i também é finitamente gerado e, portanto, finito, pois $H_i \leq G_i$ e G_i é localmente finito. Assim, $\prod_i H_i$ é residualmente finito e possui expoente n. Por (VIII), $\prod_i H_i$ é localmente finito. Sendo H finitamente gerado e $H \leq \prod_i H_i$, temos que H é finito.

(v) (IX) $\Rightarrow$ (VI): Consideremos G um grupo finito m-gerado de expoente n e seja F_m o grupo livre de posto m na variedade $\mathfrak{X}$ de todos os grupos localmente finitos de expoente n. Como G é finito, m-gerado e de expoente n, temos que $G \in \mathfrak{X}$. Desta forma, G é isomorfo a um quociente de F_m. Por outro lado, F_m é finito e, portanto, $|G| \leq |F_m|$ e $|F_m|$ depende apenas de m e n. ■

2.2 Variedades de Grupos e o Problema Restrito de Burnside

A seguir introduzimos algumas questões que generalizam o Problema Restrito de Burnside e apresentamos os principais resultados relacionados.

A partir da solução de Zelmanov para o Problema Restrito de Burnside [59, 60] novas variedades de grupos bastante interessantes têm sido descobertas.

Vimos que as seguintes afirmações são equivalentes:

2.2.1. *Sejam m e n inteiros positivos. Então a ordem de qualquer grupo finito m-gerado de expoente n é $\{m, n\}$-limitada.*

2.2.2. *A classe de todos os grupos localmente finitos de expoente n é uma variedade.*

2.2.3. *Todo grupo residualmente finito de expoente n é localmente finito.*

De acordo com o Teorema de Redução de Hall-Higman [11], o problema de demonstrar as Afirmações 2.2.1, 2.2.2 e 2.2.3 é equivalente a demonstrar cada uma das afirmações:

2.2.4. *Sejam m e n inteiros positivos. Então a ordem de qualquer grupo nilpotente m-gerado de expoente n é $\{m, n\}$-limitada.*

2.2.5. *A classe de todos os grupos localmente nilpotentes de expoente n é uma variedade.*

2.2.6. *Todo grupo residualmente nilpotente de expoente n é localmente nilpotente.*

Seja w uma palavra e seja $w(G)$ o subgrupo verbal de G gerado pelos valores de w. Nosso principal interesse é discutir as seguintes questões (introduzidas em [47]), que generalizam o Problema Restrito de Burnside:

Problema 2.2.7. *Sejam $n \geq 1$ e w uma palavra. Será que a classe de todos os grupos G satisfazendo a identidade $w^n \equiv 1$ e tendo $w(G)$ localmente finito é uma variedade?*

Problema 2.2.8. *Sejam $n \geq 1$ e w uma palavra. Será que a classe de todos os grupos G satisfazendo a identidade $w^n \equiv 1$ e tendo $w(G)$ localmente nilpotente é uma variedade?*

Sabemos que a solução do Problema Restrito de Burnside garante que a resposta para os Problemas 2.2.7 e 2.2.8 é afirmativa se $w = x$. Na verdade, é simples mostrar que a resposta é afirmativa sempre que w é uma palavra não-comutador, conforme demonstramos no Lema 2.2.9 a seguir. Desta forma, esses problemas se referem essencialmente a palavras comutadores. Não sabemos se eles são equivalentes ou não. Aqui apresentamos resultados referentes a várias outras palavras.

A palavra w é chamada de *comutador* se a soma dos expoentes de cada variável envolvida em w é igual a zero.

Lema 2.2.9. *Se w é uma palavra não-comutador, então os Problemas 2.2.7 e 2.2.8 têm respostas positivas.*

Demonstração. De fato, suponhamos que $w(x_1, x_2, \ldots, x_m)$ é uma palavra não-comutador e que a soma dos expoentes da variável x_i, $1 \leq i \leq m$, é $r \neq 0$. Consideremos um grupo G satisfazendo a identidade $w^n \equiv 1$ e substituamos todas as variáveis, exceto x_i, pela unidade de G e a variável x_i por um elemento arbitrário $g \in G$. Facilmente vemos que g^r é um w-valor, para todo $g \in G$. Portanto, G satisfaz a identidade $x^{nr} \equiv 1$, isto é, G tem expoente finito. Agora resta observar que as Afirmações 2.2.2 e 2.2.5 implicam em respostas positivas para os Problemas 2.2.7 e 2.2.8, respectivamente. ■

Primeiramente listamos alguns resultados relacionados ao Problema 2.2.8. Em [46] Shumyatsky considerou o caso em que $w = [x_1, x_2, \ldots, x_k]$ (a palavra central inferior) e provou o teorema:

Teorema 2.2.10. *Sejam k e n inteiros positivos. A classe de todos os grupos G satisfazendo a identidade $[x_1, x_2, \ldots, x_k]^n \equiv 1$ e tendo $\gamma_k(G)$ localmente nilpotente é uma variedade.*

Para citarmos outros resultados, apresentamos algumas breves definições.

Definição 2.2.11. *Uma palavra w é chamada de <u>comutador multilinear de peso k</u> se ela tem a forma de um monômio de Lie multilinear em exatamente k variáveis independentes.*

Exemplos particulares de comutadores multilineares são as palavras derivadas, definidas pelas equações

$$\delta_0(x) = x,$$

$$\delta_k(x_1, \ldots, x_{2^k}) = [\delta_{k-1}(x_1, \ldots, x_{2^{k-1}}), \delta_{k-1}(x_{2^{k-1}+1} \ldots, x_{2^k})],$$

e as palavras centrais inferiores, definidas por

$$\gamma_1(x) = x,$$

$$\gamma_{k+1}(x_1, \ldots, x_{k+1}) = [\gamma_k(x_1, \ldots, x_k), x_{k+1}].$$

Se um grupo G possui uma série normal de comprimento finito cujos quocientes são localmente nilpotentes, então utilizemos por ora $h(G)$ para indicar o número minimal h com a propriedade de que G possui uma tal série normal de comprimento h. O número h é chamado de *altura de Hirsch-Plotkin de* G. Agora, para h e n inteiros positivos e w uma palavra, denotemos por $\mathfrak{X}(w, n, h)$ a classe de todos os grupos G tais que $h(w(G)) \leq h$ e G satisfaz a identidade $w^n \equiv 1$. O resultado seguinte foi obtido em [47].

Teorema 2.2.12. *Seja w um comutador multilinear. Para quaisquer inteiros positivos h e n, a classe $\mathfrak{X}(w, n, h)$ é uma variedade.*

Assim, podemos observar relativo sucesso no caso em que consideramos a hipótese de nilpotência local. Isto se dá devido ao fato de que os resultados Lie-teóricos de Zelmanov constituem uma ferramenta bastante eficiente quando aplicados a grupos nilpotentes. Por outro lado, o caso geral apresenta maiores dificuldades de solução. Sendo assim, para obtermos resultados satisfatórios relacionados ao Problema 2.2.7, faz-se necessário considerar hipóteses adicionais sobre n ou w. Uma dificuldade significativa é que não sabemos se a teoria de Hall-Higman pode ser aplicada com sucesso neste caso. Vejamos maiores detalhes.

É conhecido que a altura de Fitting de um grupo solúvel finito de expoente n é n-limitada (uma demonstração pode ser encontrada em [41, Lema 2.5]). Entretanto, uma questão em aberto é se a altura de Fitting de um grupo solúvel finito satisfazendo a identidade $[x, y]^n \equiv 1$ é limitada em função de n. Neste sentido, usando a teoria clássica de Hall-Higman, Shumyatsky mostrou em [48, Corolário 3.3] o seguinte resultado:

Teorema 2.2.13. *Seja G um grupo solúvel finito satisfazendo a identidade $([x_1, x_2][x_3, x_4])^n \equiv 1$, onde n é um inteiro positivo que não possui divisores da forma p^2q^2, para primos distintos p e q. Seja h o número de divisores positivos de n, contando multiplicidades. Então a altura de Fitting de G não excede $3h$.*

Este fato foi importante na demonstração do teorema a seguir.

Teorema 2.2.14 ([48])**.** *Seja n um inteiro positivo que não possui divisores da forma p^2q^2, para primos distintos p e q. Então a classe de todos os grupos G satisfazendo a identidade $([x_1, x_2][x_3, x_4])^n \equiv 1$ e tendo G' localmente finito é uma variedade.*

Assim, ao invés de considerar a identidade $[x, y]^n \equiv 1$, os resultados apresentados em [48] envolvem a identidade $([x_1, x_2][x_3, x_4])^n \equiv 1$, que a princípio pode parecer estranha. Observamos que o subgrupo verbal gerado pelos valores da palavra $[x, y]$ é idêntico ao subgrupo verbal gerado pelos valores da palavra $[x_1, x_2][x_3, x_4]$. Por esta razão, o tratamento de identidades deste tipo aparece como uma etapa natural na discussão dos problemas de interesse. Em particular, em [49] Shumyatsky mostrou o

Teorema 2.2.15. *Para quaisquer inteiros positivos k e n existe um inteiro positivo $t = t(k, n)$, dependendo apenas de k e n, tal que a classe de todos os grupos G tendo $\gamma_k(G)$ localmente finito e satisfazendo a propriedade de que todo produto de t comutadores da forma $[x_1, x_2, \ldots, x_k]$ tem ordem dividindo n é uma variedade.*

A demonstração desse fato envolve as seguintes ferramentas: a classificação dos grupos simples finitos, a teoria de Hall-Higman e os resultados Lie-teóricos de Zelmanov. Outro resultado chave na demonstração é o Teorema de Segal [40], que afirma que o grupo derivado de um grupo prosolúvel finitamente gerado é fechado.

O teorema a seguir melhora consideravelmente o Teorema 2.2.15. Ele foi apresentado em [51] e no Capítulo 4 apresentamos uma discussão detalhada de sua demonstração.

Teorema 4.0.1. *Seja w um comutador multilinear. Para qualquer inteiro positivo n existe um inteiro positivo $\mu = \mu(n)$, dependendo apenas de n, tal que a classe de todos os grupos G tendo o subgrupo verbal $w(G)$ localmente finito e satisfazendo a propriedade de que todo produto de μ w-valores em G tem ordem dividindo n é uma variedade.*

Observamos que o Teorema 4.0.1 melhora o Teorema 2.2.15 de duas formas:

(i) primeiramente, o novo resultado é provado para qualquer comutador multilinear (o resultado anterior refere-se apenas à palavras do tipo $[x_1, x_2, \ldots, x_k]$);

(ii) além disso, μ depende apenas de n (no resultado anterior, t depende de n e da palavra w).

Estas conquistas foram possíveis devido a uma conveniente aplicação do Teorema de Segal.

Descrevemos, assim, os resultados mais revelantes quando consideradas palavras que são comutadores multilineares. De outro lado, entendemos que o estudo mais relevante de comutadores não multilineares é certamente o caso das palavras de Engel. Estas são definidas indutivamente pelas equações:

$$[x, {}_0 y] = x,$$
$$[x, {}_k y] = [[x, {}_{k-1} y], y].$$

Seja G um grupo. Um elemento x é chamado *k-Engel* (à esquerda) se $[g, {}_k x] = 1$ para todo $g \in G$. O grupo G é dito *k-Engel* se todos os seus elementos são k-Engel. Uma questão ainda em aberto é se um grupo k-Engel é localmente nilpotente. Usando as técnicas apresentas por Zelmanov na solução do Problema Restrito de Burnside, Wilson mostrou que a resposta é positiva no caso em que G é residualmente finito [56, 1991]. Um pouco mais tarde, em 1998, Burns e Medvedev demonstraram o seguinte resultado:

Teorema 5.2.1. *Existem funções $c(k)$ e $e(k)$, dependendo apenas de k, tais que se G é um grupo k-Engel residualmente finito, então G é uma extensão de um grupo de expoente dividindo $e(k)$ por um grupo nilpotente de classe no máximo $c(k)$.*

Utilizando o Teorema 5.2.1, Shumyatsky demonstrou:

Teorema 2.2.16 ([50]). *Sejam n uma potência de primo e k um inteiro positivo. Existe um inteiro positivo $t = t(n,k)$, dependendo apenas de n e k, tal que a classe de todos os grupos G satisfazendo a identidade $([x_1, {}_k y_1] \cdots [x_t, {}_k y_t])^n \equiv 1$ e tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito é uma variedade.*

O próximo resultado estende o Teorema 2.2.16 para o caso em que n não é mais assumido como sendo uma potência de primo e sim um inteiro positivo qualquer. Isto foi provado em [52] e dedicamos o Capítulo 5 à discussão de sua demonstração.

Teorema 5.0.1. *Sejam n e k inteiros positivos. Existe um inteiro positivo $\lambda = \lambda(n,k)$, dependendo apenas de n e k, tal que a classe de todos os grupos G satisfazendo a identidade $([x_1, {}_k y_1] \cdots [x_\lambda, {}_k y_\lambda])^n \equiv 1$ e tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito é uma variedade.*

Ao contrário do Teorema 4.0.1 que trata dos comutadores multilineares, no caso em que lidamos com as palavras de Engel não somos capazes de demonstrar que a função λ pode ser escolhida sem depender do parâmetro k. Para entender a principal dificuldade, podemos analisar as ferramentas Lie-teóricas empregadas na solução do Problema Restrito de Burnside. Um resultado de Zelmanov [61] afirma que se L é uma álgebra de Lie gerada por um número finito de elementos satisfazendo a propriedade de que todos os produtos envolvendo estes geradores são ad-nilpotentes e se L satisfaz uma identidade polinomial, então L é nilpotente. Para que sejamos capazes de aplicar este resultado, necessitamos considerar uma situação em que o grupo G possui geradores $g_1, g_2, \ldots, g_m$ tais que todos os comutadores em $g_1, g_2, \ldots, g_m$ possuem ordens limitadas. Um fato importante é que algumas palavras w possuem a seguinte propriedade: se x e y são w-valores, então $[x, y]$ também é um w-valor, isto é, para algumas palavras w o conjunto de w-valores é fechado em relação a comutadores. Por exemplo, as palavras δ_k e γ_k satisfazem essa condição. Também existem situações em que é possível reduzir o problema para o caso em que o conjunto de w-valores é fechado em relação a comutadores. Entretanto, as palavras de Engel não permitem tal tratamento e aí está a dificuldade em problemas que as envolvem.

2.3 O Problema Restrito de Burnside para Grupos Residualmente Finitos

Podemos ainda discutir certas generalizações do Problema Restrito de Burnside focadas na Afirmação 2.2.3. A questão a seguir talvez seja a melhor motivação para os resultados que apresentamos neste sentido. Ela foi introduzida por Mazurov em [23, Problema 13.34].

Problema 2.3.1. *Seja G um grupo satisfazendo a identidade $[x, y]^n \equiv 1$. Será que G' é periódico?*

A resposta para esta questão é negativa. Em [4] Deryabina e Kozhevnikov mostraram que existem contra-exemplos quando n é um inteiro ímpar suficientemente grande. Os métodos utilizados por eles baseiam-se nas técnicas de Olshanskii [35] (tais técnicas envolvem métodos geométricos aplicados à teoria combinatória de grupos). Em contrapartida, G' é periódico se $n = 2$ (neste caso, G' tem expoente 4) [28] ou se $n = 3$ [10, 30]. Ainda em contraste com os resultados de Deryabina e Kozhevnikov, no caso em que G é um grupo residualmente finito, Shumyatsky apresentou o seguinte resultado.

Teorema 2.3.2. *Sejam $q = p^s$ uma potência de primo e G um grupo residualmente finito satisfazendo $[x, y]^q = 1$, para todos $x, y \in G$. Então G' é localmente finito.*

O Teorema 2.3.2 foi demonstrado em [42] utilizando as técnicas desenvolvidas por Zelmanov em sua solução para o Problema Restrito de Burnside. Isto porque trata-se de problemas de naturezas semelhantes.

Outro resultado neste sentido foi obtido como corolário do Teorema 2.2.14:

Corolário 2.3.3 ([48])**.** *Seja G um grupo residualmente finito satisfazendo a identidade $([x_1, x_2][x_3, x_4])^n \equiv 1$, onde n é um inteiro positivo que não possui divisores da forma p^2q^2, para primos distintos p e q. Então G' é localmente finito.*

Desta forma, naturalmente estamos também interessados em estudar o seguinte problema, proposto em [44].

Problema 2.3.4. *Sejam n um inteiro positivo e w uma palavra. Suponhamos que G é um grupo residualmente finito tal que todo w-valor tem ordem dividindo n. Será que o subgrupo verbal $w(G)$ é localmente finito?*

Observamos que no caso em que $w = x$, o Problema 2.3.4 é exatamente o Problema Restrito de Burnside. Também é fácil verificar que a resposta é positiva para palavras não-comutadores. Algumas outras respostas positivas para o Problema 2.3.4 foram obtidas de maneira direta como corolários de resultados sobre variedades anteriormente mencionados. Uma delas foi mencionada no Corolário 2.3.3 e, por exemplo, outra pode ser deduzida do Teorema 2.2.15:

Corolário 2.3.5 ([49]). *Sejam k e n inteiros positivos e seja t como no Teorema 2.2.15. Suponhamos que G é um grupo residualmente finito satisfazendo a propriedade de que todo produto de t comutadores da forma $[x_1, x_2, \ldots, x_k]$ tem ordem dividindo n. Então $\gamma_k(G)$ é localmente finito.*

Observamos que o corolário não é válido se a hipótese de finitude residual for retirada. Basta recordar o resultado de Deryabina e Kozhevnikov citado anteriormente.

No Capítulo 6 apresentamos respostas positivas para o Problema 2.3.4, obtidas como corolários dos Teoremas 4.0.1 e 5.0.1, respectivamente, a saber:

Corolário 6.0.1. *Sejam n inteiro positivo e $\mu = \mu(n)$ como no Teorema 4.0.1. Se w é um comutador multilinear e G é um grupo residualmente finito satisfazendo a propriedade de que todo produto de μ w-valores tem ordem dividindo n, então o subgrupo verbal $w(G)$ é localmente finito.*

Corolário 6.0.2. *Sejam n e k inteiros positivos e $\lambda = \lambda(n, k)$ como no Teorema 5.0.1. Suponhamos que G é um grupo residualmente finito satisfazendo a identidade $([x_1, {}_k y_1] \cdots [x_\lambda, {}_k y_\lambda])^n \equiv 1$. Então o subgrupo verbal correspondente à k-ésima palavra de Engel é localmente finito.*

Enfatizamos que os Corolários 6.0.1 e 6.0.2 não afirmam que os subgrupos verbais em questão têm expoente n. De fato, de acordo com Kleiman [22, demonstração do Teorema 3], sendo q uma potência do primo p, se $q \geq p^2$, existe um grupo finito G satisfazendo a identidade $([x_1, y_1] \cdots [x_m, y_m])^q \equiv 1$, para algum inteiro positivo m tal que G' tem expoente no mínimo pq. Não é conhecido ainda se, sob as hipóteses do Corolário 6.0.2, o subgrupo verbal correspondente à k-ésima palavra de Engel tem expoente finito.

Ainda não sabemos dizer se o Problema 2.3.4 é ou não equivalente ao Problema 2.2.7. Somos capazes de demonstrar que uma resposta positiva para o Problema 2.2.7 implica em uma resposta positiva para o Problema 2.3.4 (conforme mostramos no Capítulo 6).

Capítulo 3

Métodos Lineares em Grupos Nilpotentes

Os anéis de Lie constituem uma importante ferramenta na Teoria dos Grupos. Métodos que associam anéis de Lie a p-grupos apareceram por volta dos anos 30 do século passado no contexto do Problema Restrito de Burnside. Devido às grandes contribuições de Higman, Khukhro, Kostrikin e Zelmanov neste sentido, tais métodos vêm sendo considerados com bastante frequência em problemas correlatos.

Em [61] Zelmanov obteve resposta positiva para o Problema Restrito de Burnside a partir do seguinte resultado:

Teorema 3.0.6 ([61], III(0.4)). *Seja L uma álgebra de Lie gerada pelos elementos $a_1, a_2, \ldots, a_m$. Suponhamos que L satisfaz uma identidade polinomial f e que cada monômio em $a_1, a_2, \ldots, a_m$ é ad-nilpotente. Então L é nilpotente.*

Resultados interessantes em Teoria dos Grupos são obtidos como corolários deste teorema.

De acordo com o Problema Restrito de Burnside, a ordem de qualquer grupo finito m-gerado de expoente n é $\{m, n\}$-limitada. Neste trabalho aparecem alguns resultados que, em certo sentido, são generalizações desse fato. Para isso, faz-se necessário aplicar técnicas Lie-teóricas no mesmo sentido que Zelmanov utilizou em sua solução do Problema Restrito de Burnside.

Dedicamos este capítulo à apresentação de alguns métodos lineares em grupos nilpotentes. O foco principal é descrever a construção da álgebra de Lie associada a um p-grupo finito e apresentar alguns fatos relacionados com as ideias desenvolvidas por Zelmanov. Também aparecem resultados importantes devidos a Lazard, Khukhro e Shumyatsky.

Uma exposição completa dos tópicos abordados aqui pode ser encontrada em [13], [14], [20] e [43].

3.1 Propriedades Imediatas de p-Grupos Regulares

Dado um p-grupo finito G, definimos, para todo $i \geq 0$, os seguintes subgrupos:

$$\Omega_i(G) = \left\langle x \in G / x^{p^i} = 1 \right\rangle \quad \text{e} \quad \mho_i(G) = G^{p^i} = \left\langle x^{p^i} / x \in G \right\rangle.$$

Ambos $\Omega_i(G)$ e $\mho_i(G)$ são subgrupos característicos de G.

Uma observação importante é que as igualdades

$$\Omega_i(G) = \left\{ x \in G / x^{p^i} = 1 \right\} \quad \text{e} \quad \mho_i(G) = \left\{ x^{p^i} / x \in G \right\}$$

não são válidas para qualquer p-grupo finito. Por exemplo,

$$\Omega_1(D_{2^m}) = \left\langle x \in D_{2^m} / x^2 = 1 \right\rangle = D_{2^m},$$

mas nem todo elemento de D_{2^m} tem ordem 2.

Isto motiva a definição:

Definição 3.1.1. *Seja G um p-grupo finito. Dizemos que G é um p-grupo regular se*

$$x^p y^p \equiv (xy)^p \mod \mho_1\left(\langle x, y \rangle'\right), \text{ para todos } x, y \in G.$$

Equivalentemente, se

$$\gamma_p\left(\langle x, y \rangle\right) \leq \mho_1\left(\langle x, y \rangle'\right).$$

Lema 3.1.2 (Propriedades Imediatas de um p-Grupo Regular)**.**

(a) *Se G é um p-grupo finito tal que a classe de nilpotência de G é menor do que p, então G é regular.*

(b) *Se G é um p-grupo regular, então para todo $i \geq 1$,*

$$\Omega_i(G) = \left\{ x \in G / x^{p^i} = 1 \right\} \quad e \quad \mho_i(G) = \left\{ x^{p^i} / x \in G \right\}.$$

3.2 Álgebras de Lie Associadas a p-Grupos

Entendemos por *anel de Lie* R um anel não associativo sem unidade cuja multiplicação é denotada por $[x, y]$ e satisfaz as seguintes propriedades:

(i) $[x, x] = 0$, para todo $x \in R$ (anticomutatividade);

(ii) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$, para todos $x, y, z \in R$ (Identidade de Jacobi).

Consideremos agora um anel A comutativo com unidade e seja L um A-módulo. Suponhamos que esteja definida em L uma multiplicação em que o produto dos elementos $x, y \in L$ é indicado por $[x, y]$.

Definição 3.2.1. *Dizemos que L é uma álgebra de Lie sobre A se para quaisquer $x, y, z \in L$ e quaisquer $a, b \in A$ as seguintes propriedades são satisfeitas:*

(i) $[ax + by, z] = a[x, z] + b[y, z]$;

(ii) $[x, ay + bz] = a[x, y] + b[x, z]$;

(iii) $[x, x] = 0$ (*anticomutatividade*);

(iv) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ (*Identidade de Jacobi*).

Observamos que, no sentido das definições anteriores, qualquer anel de Lie pode ser visto naturalmente como uma álgebra de Lie sobre $\mathbb{Z}$.

Neste contexto de anéis e álgebras de Lie, a multiplicação denotada por $[\ ,\ ]$ é conhecida como *comutador de Lie*.

Certas aplicações lineares são relevantes na Teoria das Álgebras de Lie, destacando-se dentre elas as derivações. Se L é uma álgebra de Lie, então qualquer aplicação linear $\delta : L \longrightarrow L$ satisfazendo a condição

$$\delta\left([x,y]\right) = [x, \delta\left(y\right)] + [\delta\left(x\right), y],$$

para todos $x, y \in L$, é dita uma *derivação* de L.

Um exemplo interessante é a aplicação definida por $y \longmapsto [x, y]$, para um elemento fixado $x \in L$. Denotamos esta aplicação por adx (*operador adjunto* definido por x) e escrevemos $adx(y) = [x, y]$. É fácil ver que ad$x$ é uma derivação para qualquer $x \in L$.[1]

Seja L uma álgebra de Lie sobre um corpo $\mathbb{F}$. Sejam n, m inteiros positivos e $x, y, x_1, x_2, \ldots, x_m \in L$. Definimos indutivamente

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

e

$$[x, {}_0 y] = x, \quad [x, {}_n y] = [[x, {}_{n-1} y], y].$$

As noções de série central inferior e série derivada são definidas para álgebras de Lie com os mesmos significados que definimos para grupos e, assim, as noções de álgebras de Lie nilpotentes e solúveis surgem de maneira natural.

Definição 3.2.2. *Um elemento $a \in L$ é chamado ad-nilpotente se existe um inteiro positivo n tal que $[x, {}_n a] = 0$, para todo $x \in L$. Se n é o menor inteiro positivo com esta propriedade, dizemos que a é ad-nilpotente de índice n.*

Observamos que um elemento de L é dito ad-nilpotente de índice n se o correspondente operador adjunto da álgebra de Lie L é nilpotente de índice n.

Definição 3.2.3. *Uma série de grupos*

$$G = G_1 \geq G_2 \geq \cdots$$

é chamada N-série se satisfaz a propriedade $[G_i, G_j] \leq G_{i+j}$, para todos i, j.

[1] Desta forma, podemos definir uma representação de L, dada pela aplicação $x \longmapsto adx$. Esta é conhecida como *representação adjunta de L*.

É fácil ver que uma N-série é central, ou seja, vale que $G_i/G_{i+1} \leq Z(G/G_{i+1})$ para todo i.

Definição 3.2.4. *Dizemos que uma N-série é uma $\underline{N_p\text{-série}}$ quando satisfeita a condição*

$$G_i^p \leq G_{pi}$$

para todo i, onde p é um primo fixado.

Utilizando generalizações de construções apresentadas por Magnus [29] e Zassenhaus [58], Lazard [26] apresentou um método onde, dado um grupo G, é possível associar um anel de Lie $L(G)$ a qualquer N-série de G. Além disso, discutiu propriedades especiais que podem ser obtidas quando consideramos uma N_p-série de G, caso em que $L(G)$ pode ser visto como uma álgebra de Lie. Aqui descrevemos brevemente a construção de um anel de Lie associado a uma N-série e as propriedades obtidas quando olhamos para $L(G)$ como sendo uma álgebra de Lie (ou seja, quando se trata de uma N_p-série).

Dada uma N-série de G, consideremos $L(G)$ como sendo a soma direta dos grupos abelianos $L_i = G_i/G_{i+1}$ (usando notação aditiva). A operação de comutação em G, $(x, y) \longmapsto [x, y]$, induz uma operação binária (que também denotamos por [,]) em $L(G)$. Para os elementos homogêneos $xG_{i+1} \in L_i$ e $yG_{j+1} \in L_j$, definimos

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

e estendemos (por linearidade) para elementos arbitrários de $L(G)$.

Lema 3.2.5. *A operação binária definida anteriormente está bem definida e $L(G)$ munido das operações $+$ e [,] é um anel de Lie.*

O procedimento discutido pode ser realizado considerando-se qualquer N-série de G. No caso em que todos os quocientes G_i/G_{i+1} de uma N-série têm expoentes p, p primo, $L(G)$ pode ser visto como uma álgebra de Lie sobre $\mathbb{F}_p$, o corpo com p elementos. Isto sempre ocorre quando tomamos uma N_p-série.

Desejamos estudar o caso particular em que consideramos uma N_p-série de G e a álgebra de Lie associada $L(G)$. É possível observar relações profundas existentes entre G e $L(G)$. Para um elemento arbitrário $x \in G_i \backslash G_{i+1}$, denotamos por $\widetilde{x}$ o elemento associado $xG_{i+1} \in L(G)$. O resultado seguinte é devido a Lazard e pode ser encontrado em [26, p. 131].

Lema 3.2.6. *Para qualquer $x \in G$, temos que $(ad\widetilde{x})^p = ad(\widetilde{x^p})$. Consequentemente, se $x^n = 1$, então $\widetilde{x}$ é ad-nilpotente de índice no máximo n.*

Definição 3.2.7. *Seja $\mathcal{L}$ a álgebra de Lie livre sobre $\mathbb{F}$ com uma quantidade enumerável de geradores livres, digamos $x_1, x_2, \ldots$, e seja $f = f(x_1, x_2, \ldots, x_n)$ um elemento não-nulo de $\mathcal{L}$. Dizemos que uma álgebra de Lie L satisfaz a identidade polinomial $f \equiv 0$ se $f(a_1, a_2, \ldots, a_n) = 0$ para quaisquer $a_1, a_2, \ldots, a_n \in L$. Neste caso, dizemos que L é uma álgebra de Lie com identidade polinomial ou uma <u>PI-álgebra de Lie</u>.*

É conhecido que qualquer lei de grupo que vale em G implica certa identidade polinomial na álgebra de Lie associada $L(G)$. Em [57], Wilson e Zelmanov apresentaram um algoritmo efetivo para escrever explicitamente a identidade polinomial da álgebra de Lie quando a lei de grupo é conhecida. O algoritmo apresentado refere-se à situações bastante gerais, sendo significativamente eficiente. Entretanto, nas argumentações de nossos novos resultados não se faz necessário explicitar as identidades polinomiais referentes às leis de grupo consideradas. Nos embasamos apenas na existência de tais identidades polinomiais, como afirma a proposição a seguir.

Proposição 3.2.8. *Seja G um grupo satisfazendo uma identidade $w \equiv 1$. Então existe um polinômio de Lie não-nulo f sobre $\mathbb{F}_p$ cuja forma depende apenas de p e w tal que a álgebra de Lie associada $L(G)$ satisfaz a identidade $f \equiv 0$.*

Para ilustrar a afirmação da proposição anterior, apresentamos um caso particular.

Proposição 3.2.9 (Higman, [12])**.** *Sejam n uma potência de primo e G um grupo tais que $x^n = 1$, para todo $x \in G$. Então para qualquer N_p-série de G, a álgebra de Lie associada $L(G)$ satisfaz a identidade*

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

Finalizamos esta seção com a definição de monômio em elementos de uma álgebra de Lie. Se X é qualquer subconjunto de L, por um *monômio* em elementos de X entendemos qualquer elemento de L que pode ser obtido por meio de repetidas operações de comutadores de Lie com um sistema arbitrário de colchetes envolvendo os elementos de X. Em particular, os elementos de X são vistos como monômios cujo sistema de colchetes é vazio.

3.3 A Série de Jennings-Lazard-Zassenhaus

Em linhas gerais, é possível construir várias N_p-séries de um grupo G e existem diferentes caminhos para se associar a G uma álgebra de Lie. Estamos particularmente interessados em definir uma N_p-série conhecida por série de Jennings-Lazard-Zassenhaus, cuja relevância é bem conhecida por suas aplicações em resultados Lie-teóricos na Teoria dos Grupos. E é exatamente para este tipo de série que aplicaremos os resultados discutidos na seção anterior.

Relembramos aqui a "Fórmula de Coleção" (veja, por exemplo, [14, p. 239]).

Lema 3.3.1. *Seja G um grupo.*

(a) *Se $x, y \in G$, então*

$$(xy)^{p^n} \equiv x^{p^n} y^{p^n} \mod \gamma_2(G)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(G)^{p^{n-r}}, \quad \textit{para todo } n \geq 1.$$

(b) *Se $x, y \in G$, $H \leq G$ e $x, [x, y] \in H$, então*

$$\left[x^{p^n}, y\right] \equiv [x, y]^{p^n} \mod \gamma_2(H)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(H)^{p^{n-r}}, \quad \textit{para todo } n \geq 1.$$

Demonstração.

(a) Denotemos $R = \gamma_2(G)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(G)^{p^{n-r}}$. Pela Fórmula de Compilação de P. Hall (Lema 1.1.9), existem $g_i \in \gamma_i(G)$, $i = 2, \ldots, p^n$, tais que

$$x^n y^n = (xy)^n g_2^{\binom{p^n}{2}} g_3^{\binom{p^n}{3}} \dots g_{p^n},$$

para todo $n \geq 1$.

Se $\mathrm{mdc}(i,p) = 1$, então $\binom{p^n}{i}$ é um número divisível por p^n e, para $i > 1$, $g_i^{\binom{p^n}{i}} \in \gamma_2(G)^{p^n} \leq R$. Agora, se $i = p^r j$, onde $r \geq 1$ e $\mathrm{mdc}(p,j) = 1$, então $\binom{p^n}{i}$ é um número divisível por p^{n-r} e $i \geq p^r$. Assim, $g_i^{\binom{p^n}{i}} \in \gamma_{p^r}(G)^{p^{n-r}} \leq R$. Portanto,

$$x^{p^n} y^{p^n} \equiv (xy)^{p^n} \mod R.$$

(b) Por (a), temos

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

Mas

$$(x\,[x,y])^{p^n} = (x^y)^{p^n} = \left(x^{p^n}\right)^y = x^{p^n}\left[x^{p^n}, y\right]$$

e, assim, a propriedade está demonstrada. ■

Lema 3.3.2. *Se $n \geq 0$, então $\left[\gamma_i(G)^{p^n}, \gamma_j(G)\right] \leq \prod_{r=0}^{n} \gamma_{j+ip^r}(G)^{p^{n-r}}$, para todos $i, j \geq 1$.*

Demonstração. O caso $n = 0$ é óbvio. Denotemos $R = \prod_{r=0}^{n} \gamma_{j+ip^r}(G)^{p^{n-r}}$. Como $R \lhd G$, é suficiente mostrar que $\left[x^{p^n}, y\right] \in R$ para quaisquer $x \in \gamma_i(G)$, $y \in \gamma_j(G)$. Pelo Lema 3.3.1-(b), para todo $n \geq 1$,

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

onde $H = \langle x, [x,y] \rangle$.

Agora, segue do Lema 1.1.8 que $\gamma_2(H)$ é o fecho normal de $[x,y,x]$ em H. Assim, $\gamma_2(H) \leq \gamma_{2i+j}(G)$. Como $H \leq \gamma_i(G)$, temos $\gamma_m(H) \leq \gamma_{mi+j}(G)$, para todo

$m \geq 2$. Desta forma, $\gamma_{p^r}(H)^{p^{n-r}} \leq \gamma_{p^r i+j}(G)^{p^{n-r}} \leq R$, para $r = 1, \ldots, n$. Além disso, $\gamma_2(H)^{p^n} \leq \gamma_{i+j}(G)^{p^n} \leq R$ e $[x, y]^{p^n} \in \gamma_{i+j}(G)^{p^n} \leq R$. Portanto, $\left[x^{p^n}, y\right] \in R$, como desejado. ■

Apresentamos a seguir uma série de subgrupos de G definida a partir dos termos da série central inferior de G cujos quocientes são todos p-grupos abelianos elementares.

Definição 3.3.3. *Para qualquer inteiro positivo i, definimos*

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

Os subgrupos D_i são característicos em G e formam uma série $G = D_1 \geq D_2 \geq \cdots$ para o grupo G. [2]

Proposição 3.3.4. *A série $\{D_i\}$ é uma N_p-série.*

A proposição anterior é consequência imediata dos Lemas 3.3.5 e 3.3.6 a seguir.

Lema 3.3.5. *Sejam G um grupo, $i \geq 1, j \geq 1, h \geq 0$ e $R = \prod_{r=0}^{h} \gamma_{i+jp^r}(G)^{p^{h-r}}$. Se $x \in \gamma_i(G)$ e $n \geq 2$, então*

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

Demonstração. Argumentaremos por indução sobre n. Se $n = 2$, então pelo Lema 1.1.8-(c) temos

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

Como $\langle x, R\rangle \leq \gamma_i(G)$, segue que $\gamma_2(\langle x, R\rangle) \leq [R, \gamma_i(G)]$.

[2] Observamos que é possível ter $D_{i-1} = D_i > D_{i+1}$. Se G é abeliano, então $D_i = G^{p^k}$, onde k é o menor inteiro positivo tal que $p^k \geq i$ e, assim, $D_i = G^{p^k}$ sempre que $p^{k-1} < i < p^k$. No caso em que G é um grupo de expoente p, temos $D_i = \gamma_i(G)$ para todo i.

Para $n > 2$, temos
$$\gamma_n(\langle x, R\rangle) \leq [\gamma_{n-1}(\langle x, R\rangle), \gamma_i(G)].$$

Usando a definição de R para o caso $n = 2$ e a hipótese de indução quando $n > 2$, obtemos, para $n \geq 2$,

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

Agora, utilizando o Lema 1.1.2 e o Lema 3.3.2, segue que

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

onde $i + p^s in - p^s i \geq in$. ■

Lema 3.3.6. *Sejam G um grupo, $i \geq 1, j \geq 1, h \geq 0$ e $k \geq 0$. Então*

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

Demonstração. Suponhamos $x \in \gamma_i(G)$ e $y \in \gamma_j(G)$. Sejam $z = [x, y^{p^h}]$ e $H = \langle x, z\rangle$. Pelo Lema 3.3.1-(b), segue que

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

Para $n = 1, \ldots, p^k$, definimos

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

Pelo Lema 3.3.2, segue que $z \in H_1$. Assim, $H \leq \langle x, H_1 \rangle$. Pelo Lema 3.3.5, temos $\gamma_n(H) \leq H_n$. Logo,

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

Agora, denotemos $R = D_{ip^k+jp^h}(G)$. Se $m + h - r \geq k$, então pela Definição 3.3.3, segue que $\gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq R$. Desta forma, se $s = \max\{m+h-k+1, \ \ 0\}$, então

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

Portanto,

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

pois $ip^k + jp^{s+k-m} \geq ip^k + jp^h$.

Assim, $[x^{p^k}, y^{p^h}] \in R$ e $x^{p^k}R$ comuta com $y^{p^h}R$. Segue que cada elemento de $\gamma_i(G)^{p^k}R/R$ comuta com cada elemento de $\gamma_j(G)^{p^h}R/R$ e, finalmente,

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

■

Estamos prontos para demonstrar a Proposição 3.3.4.

Demonstração.

(i) A série $\{D_i\}$ é uma N-série, ou seja, para m, n inteiros positivos, temos

$$[D_m, D_n] \leq D_{m+n}.$$

Essa propriedade é consequência direta da Definição 3.3.3 e do Lema 3.3.6.

(ii) A série $\{D_i\}$ é uma N_p-série, ou seja, para m, n inteiros positivos, temos

$$D_n^p \leq D_{pn}.$$

De fato, por **(i)**, temos $\gamma_p(D_n) \leq D_{pn}$ e, assim, pelo Lema 3.1.2-(a), D_n/D_{pn} é regular. Mas o quociente D_n/D_{pn} é gerado por elementos de ordem p, pois se $ip^k \geq n$ e $x \in \gamma_i(G)$, temos $(x^{p^k})^p \in D_{ip^{k+1}} \leq D_{pn}$. Portanto, pelo Lema 3.1.2-(b), $(D_n/D_{pn})^p = 1$ e, assim, $D_n^p \leq D_{pn}$. ■

Associando uma Álgebra de Lie a um Grupo

A série $\{D_i\}$ é chamada de *série central p-dimensional* de G e é conhecida como sendo a *série de Jennings-Lazard-Zassenhaus*. Os quocientes $L_i = D_i/D_{i+1}$ são todos abelianos elementares, portanto podem ser vistos como espaços vetoriais sobre $\mathbb{F}_p$. Em conformidade com os procedimentos anteriormente descritos, podemos associar a G uma álgebra de Lie dada por

$$L(G) = \bigoplus L_i$$

sobre $\mathbb{F}_p$, correspondente à série central p-dimensional.

Observamos que $L(G)$ tem estrutura de uma álgebra de Lie restrita (p-álgebra de Lie)[3] , porém trataremos $L(G)$ apenas como uma álgebra de Lie. Esta álgebra particular desempenha papel fundamental nas discussões Lie-teóricas em resultados do "tipo Zelmanov", inclusive nos novos resultados que apresentamos.

Denotemos por $L_p(G)$ a subálgebra de $L(G)$ gerada por D_1/D_2. No caso em que G é finitamente gerado, a nilpotência de $L_p(G)$ produz um forte impacto sobre a estrutura de G. Fixemos um número positivo c e suponhamos que G é gerado por $a_1, a_2, \ldots, a_m$. Seja $\rho_1, \rho_2, \ldots, \rho_s$ a lista de todos os comutadores simples em $a_1, a_2, \ldots, a_m$ de peso no máximo c. Claramente, s é um número $\{c, m\}$-limitado. A proposição a seguir pode ser encontrada implicitamente em [61] e a demonstração que apresentamos se encontra em [43, Proposição 2.11].

[3] Uma álgebra de Lie L definida sobre um corpo de característica prima p é dita *restrita* se existe uma aplicação $[p] : L \longrightarrow L$ satisfazendo

(i) $(ada)^p = ad\left(a^{[p]}\right)$, para todo $a \in L$;

(ii) Para todo $\alpha \in \mathbb{F}_p$ e $a \in L$, $(\alpha a)^{[p]} = \alpha^p a^{[p]}$;

(iii) Para todos $a, b \in L$, $(a+b)^{[p]} = a^{[p]} + b^{[p]} + \sum_{i=1}^{p-1} \varphi_i(a,b)$, onde $\varphi_i(a,b)$ são determinados da seguinte maneira:

$$(ad\,(a \otimes x + b \otimes 1))^{p-1}\,(a \otimes 1) = \sum_{i=1}^{p-1} i\varphi_i(a,b) \otimes x^{i-1} \quad \text{em} \quad L \otimes_{\mathbb{F}_p} \mathbb{F}_p\,[x].$$

Proposição 3.3.7. *Seja G um grupo gerado por m elementos $a_1, a_2, \ldots, a_m$. Suponhamos que $L_p(G)$ é nilpotente de classe c. Se $\rho_1, \rho_2, \ldots, \rho_s$ é a lista de todos os comutadores simples em $a_1, a_2, \ldots, a_m$ de peso no máximo c, então, para todo inteiro positivo i, o grupo G pode ser escrito como um produto*

$$G = \langle \rho_1 \rangle \langle \rho_2 \rangle \cdots \langle \rho_s \rangle D_{i+1}$$

de subgrupos cíclicos gerados por $\rho_1, \rho_2, \ldots, \rho_s$ e D_{i+1}. Em particular, se todo ρ_j tem ordem finita, então

$$G = \langle \rho_1 \rangle \langle \rho_2 \rangle \cdots \langle \rho_s \rangle .$$

Demonstração. Primeiramente observamos que, para todo inteiro positivo i, D_i é um subgrupo gerado por D_{i+1} e pelos elementos da forma $[b_1, b_2, \ldots, b_j]^{p^k}$, onde $jp^k \geq i$ e $b_1, b_2, \ldots, b_j \in \{a_1, a_2, \ldots, a_m\}$. Este fato é consequência da Fórmula de Coleção (Lema 3.3.1) e de propriedades elementares de comutadores.

Para demonstrar a proposição, usaremos indução sobre i. O caso $i = 0$ é trivial e, assim, podemos supor que $i \geq 1$ e que

$$G = \langle \rho_1 \rangle \langle \rho_2 \rangle \cdots \langle \rho_s \rangle D_i.$$

Segue que qualquer elemento $x \in G$ pode ser escrito na forma

$$x = \rho_1^{\alpha_1} \rho_2^{\alpha_2} \ldots \rho_s^{\alpha_s} y, \tag{3.1}$$

onde $y \in D_i$. Sem perda de generalidade, podemos assumir que $D_{i+1} = 1$.

Para $y \in D_i$, podemos escrever

$$y = (\sigma_1^{p^{k_1}})^{\beta_1} (\sigma_2^{p^{k_2}})^{\beta_2} \ldots (\sigma_r^{p^{k_r}})^{\beta_r}, \tag{3.2}$$

onde cada σ_n é da forma $[b_1, b_2, \ldots, b_j]$, com $jp^{k_n} \geq i$ e $b_1, b_2, \ldots, b_j \in \{a_1, a_2, \ldots, a_m\}$.

Denotemos por $\widetilde{a}_n$ o elemento $a_n D_2 \in L_p(G)$, $n = 1, 2, \ldots, m$. Por hipótese, $L_p(G)$ é nilpotente de classe c e isto significa que $[\widetilde{b}_1, \widetilde{b}_2, \ldots, \widetilde{b}_{c+1}] = 0$ para quaisquer $b_1, b_2, \ldots, b_{c+1} \in \{a_1, a_2, \ldots, a_m\}$. Isto implica que $[b_1, b_2, \ldots, b_{c+1}] \in D_{c+2}$ para quaisquer $b_1, b_2, \ldots, b_{c+1} \in \{a_1, a_2, \ldots, a_m\}$ e que $\gamma_{c+1}(G) \leq D_{c+2}$. Pela

Proposição 3.3.4, para qualquer $d \geq c+1$ é válido que $\gamma_d(G) \leq D_{d+1}$, pois $\gamma_d(G) = [\gamma_{d-1}(G), G] \leq [D_d, G] \leq D_{d+1}$.

Agora, se σ_n é da forma $[b_1, b_2, \ldots, b_j]$, com $j \geq c+1$, então

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

Dito isso, podemos assumir que cada σ_n é da forma $[b_1, b_2, \ldots, b_j]$ com $j \leq c$. Nesse caso, σ_n está contido na lista $\rho_1, \rho_2, \ldots \rho_s$. Resta agora notar que, pela Proposição 3.3.4, $\sigma_n^{p^{kn}} \in Z(G)$. Comparando (3.1) e (3.2), concluímos que

$$x \in \langle \rho_1 \rangle \langle \rho_2 \rangle \cdots \langle \rho_s \rangle ,$$

como desejado. ∎

Tendo em vista a Proposição 3.3.7, é de suma importância conhecer um critério que dê condições para que uma álgebra de Lie seja nilpotente de classe limitada. O próximo resultado foi provado em [24, Corolário do Teorema 4] de maneira imediata a partir do Teorema 3.0.6.

Teorema 3.3.8. *Seja L uma álgebra de Lie sobre $\mathbb{F}_p$ gerada por m elementos $a_1, a_2, \ldots, a_m$. Suponhamos que L satisfaz uma identidade $f \equiv 0$ e que cada monômio nos geradores $a_1, a_2, \ldots, a_m$ é ad-nilpotente de índice no máximo n. Então L é nilpotente de classe $\{f, n, m, \mathbb{F}_p\}$-limitada.*

Demonstração. Consideremos F_m a álgebra de Lie sobre $\mathbb{F}_p$ livre m-gerada com geradores livres $f_1, f_2, \ldots, f_m$. Seja I o ideal de F_m gerado por todos os f-valores sobre os elementos de F_m e por todos os elementos da forma $[g, {}_n x]$, onde $g \in F_m$ e x é qualquer monômio nos elementos f_i, $i = 1, 2, \ldots, m$. Assim, F/I satisfaz as hipóteses do Teorema 3.0.6 e, portanto, é nilpotente de classe $c = c(f, m, n, \mathbb{F}_p)$. Por outro lado, qualquer álgebra de Lie satisfazendo as hipóteses do Teorema 3.0.6 e satisfazendo a condição de que todo monômio nos geradores é ad-nilpotente de índice no máximo n é uma imagem de F/I sob o homomorfismo induzido pela aplicação $f_i \longmapsto a_i$, $i = 1, 2, \ldots, m$. Desta forma, concluímos que L é nilpotente de classe no máximo c. ∎

Capítulo 4

O Problema Restrito de Burnside para Comutadores Multilineares

O objetivo principal deste capítulo é demonstrar o resultado a seguir.

Teorema 4.0.1. *Seja w um comutador multilinear. Para qualquer inteiro positivo n existe um inteiro positivo $\mu = \mu(n)$, dependendo apenas de n, tal que a classe de todos os grupos G tendo o subgrupo verbal $w(G)$ localmente finito e satisfazendo a propriedade de que todo produto de μ w-valores em G tem ordem dividindo n é uma variedade.*

A solução do Problema Restrito de Burnside por Zelmanov [59, 60] ofereceu grandes contribuições ao desenvolvimento da Teoria dos Grupos. Com a utilização dos métodos envolvidos, outros problemas vêm sendo resolvidos de maneira efetiva. A partir das técnicas de Zelmanov, certas generalizações do Problema Restrito de Burnside podem ser discutidas e algumas variedades de grupos interessantes têm sido descobertas, conforme comentamos na Seção 2.2.

Relembramos que nossas discussões centrais estão baseadas em fatos relacionados aos Problemas 2.2.7 e 2.2.8. Antes de apresentarmos as argumentações que levam à demonstração do Teorema 4.0.1, façamos uma reflexão sobre o Problema 2.2.7.

Seja w uma palavra e consideremos a classe $\mathfrak{X}$ de todos os grupos G satisfazendo a identidade $w^n \equiv 1$ e tendo $w(G)$ localmente finito. Então, para demonstrar que $\mathfrak{X}$ é uma variedade, pelo Teorema de Birkhoff (1.3.8), devemos mostrar que $\mathfrak{X}$ é fechada com respeito a subgrupos, quocientes e produtos cartesianos de seus membros. Observamos que é fácil ver que a classe $\mathfrak{X}$ é fechada em relação a subgrupos e quocientes. Desta forma, precisamos discutir resultados que nos permitam concluir que $\mathfrak{X}$ também é fechada em relação a produtos cartesianos. É exatamente este o foco central das discussões que passamos a apresentar no presente capítulo e no Capítulo 5, onde abordaremos o caso das palavras de Engel.

4.1 Limitando a Altura de Fitting de um Grupo Solúvel Finito

Relembramos que o subgrupo de Fitting $F(G)$ de um grupo G é o produto de todos os subgrupos normais nilpotentes de G. Denotamos por $F_i(G)$ o i-ésimo termo da série de Fitting de G e por $h(G)$ a altura de Fitting de G. Sabemos que se G é um grupo solúvel finito, então a série de Fitting possui comprimento finito. Também é conhecido que no caso em que G é finito, $F(G)$ contém todos os subgrupos subnormais nilpotentes de G (Lema 1.1.11-(b)).

Nesta seção discutimos alguns resultados relacionados com a altura de Fitting de um grupo solúvel finito. Eles são necessários para a demonstração do Teorema 4.0.1. O ponto chave é combinar o Teorema de Segal (que afirma que o grupo derivado de um grupo prosolúvel finitamente gerado é fechado [40]) com outras ferramentas.

Definição 4.1.1. *Seja G um grupo. Um elemento $x \in G$ é dito um elemento de Engel (à esquerda) se existe um inteiro positivo n tal que $[y, {}_n x] = 1$, para todo $y \in G$.*

Necessitamos do lema a seguir, que pode ser encontrado em [13, Teorema III.6.15].

Lema 4.1.2. *Todo elemento de Engel de um grupo finito G está contido em $F(G)$.*

Definição 4.1.3. *Seja G um grupo. Um elemento $x \in G$ é chamado* <u>δ_k-comutador</u> *se existem $x_1, \ldots, x_{2^k} \in G$ tais que $x = \delta_k(x_1, \ldots, x_{2^k})$.*

Usaremos de maneira natural o fato de que inversos e conjugados de δ_k-comutadores são novamente δ_k-comutadores.

O importante teorema a seguir foi demonstrado em [40].

Teorema 4.1.4 (Segal)**.** *Se G é um grupo solúvel finito gerado por m elementos $y_1, y_2, \ldots, y_m$, então todo elemento de G' pode ser escrito como um produto de um número m-limitado de comutadores da forma $[a, b]$, onde $a \in G$, $b \in \{y_1, y_2, \ldots, y_m\}$.*

Em [32] Nikolov e Segal generalizaram o teorema anterior desconsiderando a hipótese de G ser solúvel. Do Teorema 4.1.4, deduzimos o lema:

Lema 4.1.5. *Seja l um inteiro positivo. Seja G um grupo solúvel finito gerado por m elementos $g_1, g_2, \ldots, g_m$ tais que a ordem de cada g_i divide l. Então todo elemento de G pode ser escrito como um produto de um número $\{m, l\}$-limitado, $f = f(m, l)$, de conjugados de g_i.*

Demonstração. Pelo Teorema 4.1.4, todo elemento de G' pode ser escrito como um produto de r comutadores $[a_i, b_i]$, onde r é um número m-limitado, $a_i \in G$ e $b_i \in \{g_1, g_2, \ldots, g_m\}$. Agora, se $x \in G'$, podemos escrever

$$\begin{aligned} x = [a_1, b_1][a_2, b_2] \cdots [a_r, b_r] &= b_1^{-a_1} b_1 b_2^{-a_2} b_2 \cdots b_r^{-a_r} b_r \\ &= b_1^{(l-1)a_1} b_1 b_2^{(l-1)a_2} b_2 \cdots b_r^{(l-1)a_r} b_r. \end{aligned}$$

Assim, x é um produto de no máximo rl conjugados de g_i. Como G/G' é gerado por elementos de ordens dividindo l e a ordem de G/G' é no máximo m^l, segue que cada elemento de G é um produto de no máximo $f = rl + m^l$ conjugados dos g_i. ■

Nas discussões que seguem no restante deste capítulo, usaremos $f(m,l)$ para denotar o número $\{m,l\}$-limitado no mesmo sentido do Lema 4.1.5. Também usaremos a notação de produtos à esquerda para os colchetes

$$[x_1, x_2, x_3, \ldots, x_n] = [\ldots[[x_1, x_2], x_3], \ldots, x_n],$$

para todos $x_1, x_2, x_3, \ldots, x_n \in G$.

Lema 4.1.6. *Sejam G um grupo, d um δ_k-comutador e $x \in G$. Então $[x, \underbrace{d, \ldots, d}_{k}]$ é um δ_k-comutador.*

Demonstração. Notemos que d pode ser visto com um δ_i-comutador para cada $i \leq k$. Claramente, $[x,d]$ é um δ_1-comutador. Usando indução sobre k, podemos assumir que $k \geq 1$ e que $[x, \underbrace{d, \ldots, d}_{k-1}]$ é um δ_{k-1}-comutador. Então $[x, \underbrace{d, \ldots, d}_{k}] = [[x, \underbrace{d, \ldots, d}_{k-1}], d]$ é um δ_k-comutador, como queríamos demonstrar. ■

Lema 4.1.7. *Seja G um grupo solúvel finito tal que $h(G) = 2$. Seja $x \in G$ e suponhamos que o subgrupo $\langle x, F(G)\rangle$ é nilpotente. Então $x \in F(G)$.*

Demonstração. Denotemos $F = F(G)$. Como G/F é nilpotente, temos que $\langle x, F\rangle$ é subnormal. Assim, $\langle x, F\rangle$ é um subgrupo subnormal nilpotente de G. Portanto, pelo Lema 1.1.11-(b), segue que $x \in F$. ■

O próximo resultado é fundamental para a demonstração do Teorema 4.0.1. É uma das principais ideias da contribuição que este trabalho representa. Ele nos permite limitar a altura de Fitting de um grupo solúvel finito satisfazendo certa identidade.

Lema 4.1.8. *Seja G um grupo solúvel finito. Suponhamos que a altura de Fitting de $G^{(k)}$ é h. Então é possível escolher h δ_k-comutadores em G, digamos $d_1, d_2, \ldots, d_h$, tais que o subgrupo $\langle d_1, d_2, \ldots, d_h\rangle$ tem altura de Fitting exatamente h.*

Demonstração. Denotemos $F_i(G^{(k)})$ por F_i, $1 \leq i \leq h$. Se $h = 1$, então o lema é óbvio. Assim, assumimos que $h \geq 2$. Como $F_h = G^{(k)}$, existe um δ_k-comutador d_1 tal que $d_1 \notin F_{h-1}$. Já que a altura de Fitting de $G^{(k)}/F_{h-2}$ é igual a 2, pelo Lema 4.1.7

segue que o subgrupo $\langle d_1, F_{h-1}\rangle / F_{h-2}$ não é nilpotente. Desta forma, de acordo com o Lema 4.1.2, a imagem de d_1 em $\langle d_1, F_{h-1}\rangle / F_{h-2}$ não pode ser um elemento de Engel. Logo existe $x_1 \in F_{h-1}$ tal que $[x_1, \underbrace{d_1, \ldots, d_1}_{i}] \notin F_{h-2}$, para qualquer inteiro positivo i. Definamos $d_2 = [x_1, \underbrace{d_1, \ldots, d_1}_{k}]$. Pelo Lema 4.1.6 segue que d_2 é um δ_k-comutador. Além disso, $d_2 \in F_{h-1} \backslash F_{h-2}$.

Analogamente, como o subgrupo $\langle d_2, F_{h-2}\rangle / F_{h-3}$ não é nilpotente, existe $x_2 \in F_{h-2}$ tal que $[x_2, \underbrace{d_2, \ldots, d_2}_{i}] \notin F_{h-3}$, para qualquer inteiro positivo i. Definamos $d_3 = [x_2, \underbrace{d_2, \ldots, d_2}_{k}]$. Notemos que d_3 é um δ_k-comutador e que $d_3 \in F_{h-2} \backslash F_{h-3}$.

Continuando com este processo, temos que existe $x_{r-1} \in F_{h-(r-1)}$ tal que podemos escolher um δ_k-comutador d_r definido por $d_r = [x_{r-1}, \underbrace{d_{r-1}, \ldots, d_{r-1}}_{k}]$, onde $1 \leq r \leq h$ e $d_r \in F_{h-(r-1)} \backslash F_{h-r}$.

Agora, seja $H = \langle d_1, d_2, \ldots, d_h\rangle$. Resta mostrar que o subgrupo H possui altura de Fitting exatamente h. De fato, temos que $d_h \in F(H)$. Além disso, observamos que $d_{h-1} \in F_2(H)$ mas $d_{h-1} \notin F(H)$ (em caso contrário, existiria um inteiro positivo j tal que $[d_h, \underbrace{d_{h-1}, \ldots, d_{h-1}}_{j}] = 1$). De forma mais geral, temos que $d_{h-r} \in F_{r+1}(H)$ mas $d_{h-r} \notin F_r(H)$, onde $0 \leq r \leq h-1$. Portanto, H tem altura de Fitting h, como desejado. ■

Notação. Fixemos um inteiro positivo k. Utilizamos o símbolo w_j para denotar a palavra que é o produto de j δ_k-comutadores, cada um deles com entradas independentes. Assim, por exemplo, o símbolo w_2 denota a palavra $\delta_k(x_1, \ldots, x_{2^k})\delta_k(y_1, \ldots, y_{2^k})$.

É fácil ver que se um elemento de um grupo G é um w_i-valor, então é também um w_j-valor para qualquer $i \leq j$. Desta forma, para qualquer $i \leq j$, a identidade $w_j^n \equiv 1$ implica a identidade $w_i^n \equiv 1$ em G.

Um bem-conhecido corolário da Teoria de Hall-Higman afirma que a altura de Fitting de qualquer grupo solúvel finito de expoente n é limitada pelo número de divisores de n, contando multiplicidades. Denotaremos este número por $h(n)$. Uma demonstração para este fato pode ser encontrada em [41, Lema 2.5].

Isso nos permite demonstrar o lema a seguir.

Lema 4.1.9. *Sejam j e n inteiros positivos satisfazendo a propriedade $j \geq f(h(n)+1,n)$. Seja G um grupo solúvel finito satisfazendo a identidade $w_j^n \equiv 1$. Então $h(G^{(k)}) \leq h(n)$.*

Demonstração. Suponhamos o lema falso. Escrevamos $h = h(n)$. Pelo Lema 4.1.8, podemos escolher $h+1$ δ_k-comutadores $d_1, d_2, \ldots, d_{h+1}$ em G tais que o subgrupo $H = \langle d_1, d_2, \ldots, d_{h+1} \rangle$ tem altura de Fitting no máximo $h+1$. Pelo Lema 4.1.5, qualquer elemento de H pode ser escrito como um produto de no máximo $f(h(n)+1,n)$ conjugados dos d_i. Por hipótese, qualquer produto deste tipo tem ordem dividindo n. Assim, H possui expoente n e, portanto, como observamos anteriormente, $h(H) \leq h$. Mas isto é uma contradição e o lema está demonstrado. ∎

Corolário 4.1.10. *Sob as mesmas hipóteses do Lema 4.1.9, temos que $h(G) \leq h(n) + k$.*

Demonstração. Basta notar que a altura de Fitting de $G/G^{(k)}$ satisfaz a propriedade $h(G/G^{(k)}) \leq k$. ∎

4.2 O Caso dos δ_k-Comutadores

Nesta seção demonstramos o Teorema 4.0.1 no caso particular em que w é um δ_k-comutador. O caso geral será obtido como consequência deste resultado. Necessitamos do conceito de grupo monolítico, introduzido por Hall e Higman ([11]).

Definição 4.2.1. *Um grupo G é dito monolítico se possui um único subgrupo normal minimal que é simples não abeliano.*

Recordamos que um subgrupo normal minimal de um grupo finito é simples ou é o produto direto de subgrupos simples isomorfos (uma demonstração para este fato pode ser encontrada em [38]).

Proposição 4.2.2. *Sejam j, j_1 e n inteiros positivos tais que $j \geq j_1 n + 1$ e seja G um grupo finito satisfazendo a identidade $w_j^n \equiv 1$. Suponhamos que G não possui subgrupos solúveis normais não triviais. Então G possui um subgrupo normal L tal que L é residualmente monolítico e G/L pertence residualmente à classe dos grupos finitos satisfazendo uma identidade $w_{j_1}^{n/p} \equiv 1$, para algum primo p divisor de n.*

Demonstração. Consideremos M um subgrupo normal minimal de G. Então $M \cong S_1 \times S_2 \times \cdots \times S_r$, onde $S_1, S_2, \ldots, S_r$ são grupos simples isomorfos (observamos que r pode ser igual a 1). O grupo G age sobre M permutando os fatores simples e, assim, obtemos uma representação de G por permutações do conjunto $\{S_1, S_2, \ldots, S_r\}$. Seja L_M o núcleo desta representação.

Como S_1 não é solúvel, podemos escolher um elemento não trivial $b \in S_1$ da forma w_1 (conforme a notação introduzida na Página 63). Seja p um divisor primo da ordem de b. Queremos mostrar que a identidade $w_{j_1}^{n/p} \equiv 1$ é satisfeita em G/L_M. Suponhamos que isto é falso. Seja $q = p^\alpha$ a maior potência de p que divide n. Como estamos supondo que a identidade $w_{j_1}^{n/p} \equiv 1$ não é satisfeita em G/L_M, temos que a identidade $w_{j_1}^{n/q} \equiv 1$ também não é satisfeita em G/L_M e, portanto, existe um elemento $a \in G$ da forma w_{j_1} tal que q divide a ordem de a módulo L_M. Escrevamos $n = n_1 q$ e $a_1 = a^{n_1}$. Desta forma, a_1 é um elemento da forma $w_{j_1 n_1}$ cuja ordem é q. Logo a_1 permuta regularmente alguns q fatores do conjunto $\{S_1, S_2, \ldots, S_r\}$. Sem perda de generalidade, suponhamos que S_1 é um desses fatores. Podemos escrever

$$\begin{aligned}
(ba_1)^q &= \underbrace{(ba_1)(ba_1)\cdots(ba_1)}_{q} \\
&= (ba_1)\left(ba_1^{-1}a_1a_1\right)\left(ba_1^{-1}a_1^{-1}a_1a_1a_1\right)\cdots(ba_1) \\
&= bb^{a_1^{-1}}b^{a_1^{-2}}\cdots b^{a_1}.
\end{aligned}$$

Como $b \in S_1$, cada um dos elementos $b^{a_1^{-i}}$ pertence a um diferente subgrupo S_i e, assim, o produto $bb^{a_1^{-1}}b^{a_1^{-2}}\cdots b^{a_1}$ possui a mesma ordem de b. Logo $(ba_1)^q$ tem ordem divisível por p e, como $q = p^\alpha$, o elemento ba_1 tem ordem divisível por $p^{\alpha+1}$. Ainda, sendo ba_1 da forma $w_{j_1 n_1 + 1}$, podemos vê-lo como sendo da forma w_j e, por isso, sua ordem deve dividir n. Isto contradiz nossa escolha maximal de p^α. Portanto, a identidade $w_{j_1}^{n/p} \equiv 1$ é satisfeita em G/L_M.

Agora consideremos L a interseção de todos os subgrupos L_M, onde M percorre o conjunto dos subgrupos normais minimais de G. Sabemos pelo Teorema de Remak (1.2.2) que G/L é isomorfo a um produto subcartesiano dos grupos G/L_M. A discussão anterior nos dá que G/L pertence residualmente à classe dos grupos finitos satisfazendo a identidade $w_{j_1}^{n/p} \equiv 1$. Assim, a demonstração estará completa uma vez provado que L é residualmente monolítico.

Se T é o produto dos subgrupos normais minimais de G, segue que T é o produto de grupos simples $S_1, S_2, \ldots, S_t$ que comutam dois a dois e L é a interseção dos normalizadores dos grupos S_i. A expressão de T como um produto dos S_i é única a menos da ordem dos fatores e um automorfismo de T apenas permuta os subgrupos S_i. Como G não possui subgrupos solúveis normais não triviais, temos $C_G(T) = 1$ e, portanto, sendo G isomorfo a algum subgrupo do grupo dos automorfismos de T, qualquer elemento de L induz um automorfismo não trivial de algum dos S_i.

Seja ρ_i o homomorfismo natural de L no grupo dos automorfismos de S_i. Verifiquemos que a imagem de ρ_i é um subgrupo monolítico. Sabemos que $\rho_i(L) \cong L/C_L(S_i)$. Temos que $\rho_i(S_i)$ é subgrupo normal minimal simples de $\rho_i(L)$ e ainda $C_{\rho_i(L)}(\rho_i(S_i)) = 1$, ou seja, $\rho_i(S_i)$ é não abeliano. De fato, se $\rho_i(x) \in C_{\rho_i(L)}(\rho_i(S_i))$, então $[xC_L(S_i), S_iC_L(S_i)] \leq C_L(S_i)$, o que é equivalente a $[x, S_i] \leq C_L(S_i)$. Segue que $[x, S_i] \leq C_L(S_i) \cap S_i = 1$. Logo $x \in C_L(S_i)$. Além disso, não existe outro subgrupo normal minimal em $\rho_i(L)$. Suponhamos que K é um subgrupo normal minimal em $\rho_i(L)$. Então $[K, \rho_i(S_i)] \leq K \cap \rho_i(S_i) = 1$, o que é um absurdo pois $C_{\rho_i(L)}(\rho_i(S_i)) = 1$. Portanto, $\rho_i(L)$ é monolítico.

Agora, para concluir que L é residualmente monolítico, basta observar que $\bigcap\limits_i ker \rho_i = \bigcap\limits_i C_L(S_i) = 1$ e que L é isomorfo a um produto subcartesiano dos $L/C_L(S_i)$ (de acordo com o Teorema 1.2.4). $\blacksquare$

<u>**Escolha de $\mu(x)$**</u>

Agora estamos aptos a escolher uma função $\mu(x)$ definida para qualquer inteiro positivo x e satisfazendo as seguintes propriedades:

1. $\mu(x) \geq f(h(x)+1, x)$, para todo x;

2. $\mu(x) \geq x \cdot \mu(y) + 1$, para todos x, y tais que y é um divisor próprio de x.

Uma função com tais propriedades pode ser construída utilizando indução sobre x. Com efeito, definamos $\mu(1) = f(1,1)$. Agora suponhamos que $\mu(x)$ está definida para todo $x \leq n-1$. Seja M o máximo entre $f(h(n)+1, n)$ e $n \cdot \mu(y) + 1$, onde y varia no conjunto de todos os divisores próprios de n. Por indução, todos os elementos sobre os quais escolhemos o máximo já estão definidos. Façamos $\mu(n) = M$. Desta forma, estabelecemos a existência de uma função com as propriedades desejadas.

A proposição a seguir é obtida utilizando as técnicas Lie-teóricas desenvolvidas por Zelmanov na solução do Problema Restrito de Burnside. Denotamos por $O_{p'}(G)$ o produto de todos os p'-subgrupos normais de G, onde p' é um número primo diferente de p.

Proposição 4.2.3. *Sejam m, n e l inteiros positivos e $\mu = \mu(n)$. Seja G um grupo nilpotente finito satisfazendo a identidade $w_\mu^n \equiv 1$. Suponhamos que G pode ser gerado por m elementos $g_1, g_2, \ldots, g_m$, tais que a ordem de cada g_i e de cada comutador da forma $[g, x]$, onde $g \in \{g_1, g_2, \ldots, g_m\}$ e $x \in G$, divide l. Então a ordem de G é $\{k, m, n, l\}$-limitada.*

Demonstração. Como G é um grupo nilpotente finito, é claro que qualquer primo que divide a ordem de G é um divisor de l. Assim, é suficiente limitar a ordem do p-subgrupo de Sylow de G para qualquer primo p. Logo podemos passar ao quociente $G/O_{p'}(G)$ e supor que G é um p-grupo e n é uma potência de p.

Suponhamos, primeiramente, G solúvel de comprimento derivado $j \leq k$. Se G é abeliano, é fácil ver que $|G|$ é $\{k, m, n, l\}$-limitada, pois G é um grupo m-gerado cujos geradores têm ordens dividindo l. Argumentando por indução sobre j, vamos assumir que $\left|G : G^{(j-1)}\right|$ é $\{k, m, n, l\}$-limitado.

Suponhamos, por ora, que $G^{(j-1)}$ é central. Neste caso, $|G : Z(G)|$ é $\{k,m,n,l\}$-limitado e o Teorema de Schur (1.5.3) garante que $|G'|$ também é $\{k,m,n,l\}$-limitada. Passando ao quociente G/G', temos que este é um grupo abeliano que pode ser gerado por m elementos, cada um de ordem dividindo l. Logo $|G/G'|$ é $\{k,m,n,l\}$-limitada e, portanto, o mesmo vale para $|G|$.

Agora vejamos o que ocorre no caso em que $G^{(j-1)}$ não é central. Consideremos o subgrupo

$$A = \left\langle \left[g_1, G^{(j-1)}\right], \left[g_2, G^{(j-1)}\right], \ldots, \left[g_m, G^{(j-1)}\right] \right\rangle.$$

Como cada g_i normaliza A, para todo $1 \leq i \leq m$, segue que A é normal em G. Passando ao quociente G/A, temos que a imagem de $G^{(j-1)}$ é central e, aplicando a argumentação do parágrafo anterior, obtemos que A tem índice $\{k,m,n,l\}$-limitado em G. Pela Observação 1.4.3, o número de geradores de A depende apenas de m e do índice de A em G e, portanto, é $\{k,m,n,l\}$-limitado. Como A é abeliano e, por hipótese, cada comutador da forma $[g,x]$, com $g \in \{g_1, g_2, \ldots, g_m\}$ e $x \in G$ tem ordem dividindo l, segue que A é um grupo de expoente l. Assim, pela solução positiva do Problema Restrito de Burnside, temos que $|A|$ e, consequentemente, $|G|$ é $\{k,m,n,l\}$-limitada.

Finalmente, consideremos o caso geral, ou seja, abandonemos a hipótese de que G é solúvel de comprimento derivado no máximo k. Aplicando as discussões anteriores ao quociente $G/G^{(k)}$ (que é solúvel de comprimento derivado k), obtemos que $\left|G : G^{(k)}\right|$ é $\{k,m,n,l\}$-limitado. Logo resta mostrar que $\left|G^{(k)}\right|$ é $\{k,m,n,l\}$-limitada. Seja r o número minimal de geradores de $G^{(k)}$. Pela Observação 1.4.3, r é $\{k,m,n,l\}$-limitado. Um bem-conhecido corolário do Teorema da Base de Burnside (Corolário 1.6.2) diz que se um p-grupo é r-gerado, então qualquer conjunto gerador deste grupo contém um conjunto gerador com exatamente r elementos. Pela Observação 1.1.7, $G^{(k)}$ é gerado pelos δ_k-comutadores cujas entradas são elementos de G. Assim, $G^{(k)}$ pode ser gerado por r δ_k-comutadores, digamos, $d_1, d_2, \ldots, d_r$.

A identidade $w_\mu^n \equiv 1$ nos dá que a ordem de cada d_i divide n. Além disso, como $[d_i, d_j]$ é novamente um δ_k-comutador, segue que qualquer comutador em $d_1, d_2, \ldots, d_r$ tem ordem dividindo n. Sabemos que a identidade $\delta_k^n \equiv 1$ vale em $G^{(k)}$ (isto porque vale a identidade $w_\mu^n \equiv 1$). Desta forma, pelo Lema 3.2.8, existe um polinômio de Lie não-nulo

f sobre $\mathbb{F}_p$, cuja forma depende apenas de k e n, tal que a álgebra $L_p(G^{(k)})$ satisfaz a identidade $f \equiv 0$ (conforme as discussões da Seção 3.3).

Consideremos um monômio de Lie arbitrário σ nos geradores $\widetilde{d_1}$, $\widetilde{d_2}$, $\ldots$, $\widetilde{d_r}$ de $L_p(G^{(k)})$ e seja ρ o comutador de grupo em $d_1, d_2, \ldots, d_r$ com o mesmo sistema de colchetes que σ. A definição de $L_p(G^{(k)})$ nos dá ou $\sigma = 0$ ou $\sigma = \widetilde{\rho}$. Como $\rho^n = 1$, o Lema 3.2.6 implica que σ é ad-nilpotente de índice no máximo n. O Teorema 3.3.8 nos diz que $L_p(G^{(k)})$ é nilpotente de classe dependendo apenas de k, m e n. Combinando isto com o Lema 3.3.7, concluímos que existe um número $\{k, m, n\}$-limitado s tal que $G^{(k)}$ pode ser escrito como um produto de no máximo s subgrupos cíclicos, cada um de ordem no máximo n. Portanto, $G^{(k)}$ tem ordem no máximo n^s, como queríamos demonstrar. ■

Na sequência, apresentamos uma proposição com considerações análogas àquelas da Proposição 4.2.3, porém não mais assumimos G nilpotente. Na demonstração utilizamos o resultado a seguir, devido a Jones.

Teorema 4.2.4 ([16])**.** *Qualquer família infinita de grupos simples finitos gera a variedade de todos os grupos.*

Nas discussões que seguem, $\pi(G)$ denota o conjunto de todos os números primos divisores de $|G|$.

Proposição 4.2.5. *Sejam m, n, l inteiros positivos e $\mu = \mu(n)$. Seja G um grupo finito satisfazendo a identidade $w_\mu^n \equiv 1$. Suponhamos que G pode ser gerado por m elementos $g_1, g_2, \ldots, g_m$, tais que a ordem de cada g_i e de cada comutador das formas $[g, x]$ e $[g, x, y]$, onde $g \in \{g_1, g_2, \ldots, g_m\}$, $x, y \in G$, divide l. Então a ordem de G é $\{k, m, n, l\}$-limitada.*

Demonstração. Se $n = 1$, então a identidade $w_\mu \equiv 1$ implica a identidade $w_1 \equiv 1$ em G. Assim, G é solúvel de comprimento derivado no máximo k. Se G é abeliano, é fácil ver que $|G|$ é $\{k, m, n, l\}$-limitada, uma vez que G é m-gerado e seus geradores têm ordens dividindo l. Argumentando agora por indução sobre o comprimento derivado $j \leq k$ de G, suponhamos que $\left|G : G^{(j-1)}\right|$ é $\{k, m, n, l\}$-limitado.

Vamos assumir, por ora, que $G^{(j-1)}$ é central. Neste caso, $G/Z(G)$ tem ordem $\{k, m, n, l\}$-limitada e, pelo Teorema de Schur, G' também tem ordem $\{k, m, n, l\}$-limitada. Passando ao quociente G/G', temos que este é um grupo abeliano que pode ser gerado por

m elementos, cada um de ordem dividindo l. Logo, $|G/G'|$ é $\{k,m,n,l\}$-limitada e, consequentemente, $|G|$ é $\{k,m,n,l\}$-limitada.

Já no caso em que $G^{(j-1)}$ não é central, consideremos o subgrupo

$$A = \left\langle \left[g_1, G^{(j-1)}\right], \left[g_2, G^{(j-1)}\right], \dots, \left[g_m, G^{(j-1)}\right] \right\rangle.$$

Como cada g_i normaliza A, para todo $1 \leq i \leq m$, temos que A é normal em G. Passando ao quociente G/A, temos que a imagem de $G^{(j-1)}$ é central e, aplicando a argumentação do parágrafo anterior, obtemos que A tem índice $\{k,m,n,l\}$-limitado em G. Pela Observação 1.4.3, A pode ser gerado por um número $\{k,m,n,l\}$-limitado de elementos. Como A é abeliano e, por hipótese, cada comutador da forma $[g,x]$, com $g \in \{g_1, g_2, \dots, g_m\}$ e $x \in G$ tem ordem dividindo l, segue que A é um grupo de expoente l. Desta forma, a solução do Problema Restrito de Burnside nos dá que $|A|$ e, portanto, $|G|$ é $\{k,m,n,l\}$-limitada.

Agora apliquemos indução sobre n. O caso $n = 1$ está demonstrado por meio das discussões anteriores. Suponhamos $n \geq 2$ e que a proposição é verdadeira para grupos satisfazendo uma identidade $w_{\mu(n/p)}^{n/p} \equiv 1$, para algum primo p divisor de n. Em outras palavras, a hipótese de indução é que existe um número N_0, $\{k,m,n,l\}$-limitado, tal que se G é um grupo finito satisfazendo uma identidade $w_{\mu(n/p)}^{n/p} \equiv 1$, gerado por m elementos $g_1, g_2, \dots, g_m$, onde cada g_i e todos os comutadores das formas $[g,x]$ e $[g,x,y]$, com $g \in \{g_1, g_2, \dots, g_m\}$ e $x, y \in G$, têm ordens dividindo l, então $|G| \leq N_0$.

Primeiramente, suponhamos que G não possui subgrupos solúveis normais não triviais. Como $\mu(n) \geq n \cdot \mu(n/p) + 1$, a Proposição 4.2.2 nos dá que G possui um subgrupo normal L tal que L é residualmente monolítico e G/L pertence residualmente à classe dos grupos finitos satisfazendo uma identidade $w_{\mu(n/p)}^{n/p} \equiv 1$, para algum primo p divisor de n. Pela hipótese de indução, segue que G/L é residualmente de ordem no máximo N_0. Assim, G/L é isomorfo a um produto subcartesiano de grupos cujas ordens são no máximo N_0. Sendo G/L um grupo m-gerado, pelos Teoremas 1.3.2 e 1.3.3, o número de subgrupos normais distintos de índice no máximo N_0 em G/L é $\{m, N_0\}$-limitado. Logo $|G/L|$ é $\{k,m,n,l\}$-limitada. Em particular, segue que L pode ser gerado por r elementos, onde r é um número $\{k,m,n,l\}$-limitado.

Do Teorema 4.2.4 segue que, salvo isomorfismos, existe apenas um número finito de grupos monolíticos satisfazendo a identidade $w_\mu^n \equiv 1$. Seja $N_1 = N_1(n,\mu)$ o máximo das ordens destes grupos. Então L é residualmente de ordem no máximo N_1. Agora, sendo L um grupo r-gerado, sabemos que o número de subgrupos normais distintos de índice no máximo N_1 em L é $\{r, N_1\}$-limitado (Teoremas 1.3.2 e 1.3.3). Portanto L tem ordem $\{k, m, n, l\}$-limitada e, consequentemente, a ordem de G é $\{k, m, n, l\}$-limitada.

Agora vejamos o que ocorre se retiramos a hipótese de G não possuir subgrupos solúveis normais não triviais. Seja S o produto de todos os subgrupos solúveis normais de G. A discussão anterior nos dá que G/S tem ordem $\{k, m, n, l\}$-limitada. Como $\mu(n) \geq f(h(n)+1, n)$, o Corolário 4.1.10 implica que a altura de Fitting $h(S)$ é $\{k, m, n, l\}$-limitada. Seja $F = F(G) = F(S)$ o subgrupo de Fitting de G e passemos ao quociente G/F. Este satisfaz as hipóteses da proposição e é tal que $h(S/F) < h(S)$. Por indução sobre $h(S)$, obtemos que $|G : F|$ é $\{k, m, n, l\}$-limitado.

Por um momento, vamos supor que F seja central. Neste caso, $|G : Z(G)|$ é $\{k, m, n, l\}$-limitado e, pelo Teorema de Schur, $|G'|$ é $\{k, m, n, l\}$-limitada. Como G pode ser gerado por m elementos, todos de ordens dividindo l, segue que $|G|$ é $\{k, m, n, l\}$-limitada.

Se F não é central, consideremos o subgrupo

$$N = \langle [g_1, F], [g_2, F], \ldots, [g_m, F] \rangle.$$

Como cada g_i normaliza N, para todo $1 \leq i \leq m$, segue que N é normal em G. Passando ao quociente G/N, temos que a imagem de F é central e, aplicando a discussão do parágrafo anterior, obtemos que $|G : N|$ é $\{k, m, n, l\}$-limitado. Resta limitar $|N|$.

Sabemos que N pode ser gerado por um número $\{k, m, n, l\}$-limitado de elementos. Seja s o número minimal de geradores de N. Como N é nilpotente, $\pi(N)$ consiste dos primos divisores de l. Assim, é suficiente limitar a ordem do p-subgrupo de Sylow de N, para todo primo $p \in \pi(N)$. Seja P o p-subgrupo de Sylow de N e escrevamos $N = P \times O_{p'}(N)$. Se $y_1, y_2, \ldots$ é a lista de todos os elementos da forma $[g_i, y]$, onde $1 \leq i \leq m$ e $y \in F$, denotemos por $b_1, b_2, \ldots$ as correspondentes projeções dos y_j em P. Segue que $P = \langle b_1, b_2, \ldots \rangle$. Como P é um p-grupo finito s-gerado, o Corolário 1.6.2 (Teorema da Base de Burnside) garante que P é na verdade gerado por s elementos na lista $b_1, b_2, \ldots$. Por hipótese, a ordem de cada um destes divide l. Observamos que cada comutador da forma $[b_i, z]$ também tem ordem dividindo l. Pela Proposição 4.2.3, segue que P tem ordem $\{k, m, n, l\}$-limitada. Assim, a demonstração está completa. ■

Agora estamos prontos para demonstrar o Teorema 4.0.1 no caso em que w é um δ_k-comutador.

Teorema 4.2.6. *Sejam n um inteiro positivo e $\mu = \mu(n)$. Seja $\mathfrak{X}$ a classe de todos os grupos G tais que $G^{(k)}$ é localmente finito e satisfazendo a propriedade de que qualquer w_μ-valor em G tem ordem dividindo n. Então $\mathfrak{X}$ é uma variedade.*

Demonstração. É fácil ver que a classe $\mathfrak{X}$ é fechada em relação a subgrupos e quocientes de seus membros. Pelo Teorema de Birkhoff, resta mostrar que se D é um produto cartesiano de grupos em $\mathfrak{X}$, então $D \in \mathfrak{X}$. Observamos que a identidade $w_\mu^n \equiv 1$ é satisfeita em D e, assim, é suficiente mostrar que $D^{(k)}$ é localmente finito. Para isto, mostraremos que qualquer subconjunto finito de $D^{(k)}$ gera um subgrupo finito.

Seja T um subconjunto finito qualquer de $D^{(k)}$. Claramente, existem δ_k-comutadores $h_1, h_2, \ldots, h_m \in D$ tais que $T \leq \langle h_1, h_2, \ldots, h_m \rangle = H$. Assim, é suficiente verificar que o subgrupo H é finito. É fácil ver que a identidade $w_\mu^n \equiv 1$ nos dá que a ordem de cada h_i divide n, para todo $1 \leq i \leq m$. Além disso, se $h \in \{h_1, h_2, \ldots, h_m\}$ e $x, y \in H$, então cada comutador da forma $[h, x] = h^{-1}h^x$ é um produto de dois δ_k-comutadores e cada comutador da forma $[h, x, y] = (h^{-1}h^x)^{-1}(h^{-1}h^x)^y$ é um produto de quatro δ_k-comutadores. Uma vez que da escolha de μ temos $\mu(n) \geq 4$, para todo $n \geq 2$, a identidade $w_\mu^n \equiv 1$ implica que a ordem de cada um desses comutadores divide n.

Notando que $D^{(k)}$ é isomorfo a um produto subcartesiano de grupos localmente finitos, temos $D^{(k)}$ residualmente localmente finito. Se Q é qualquer quociente localmente finito de $D^{(k)}$, pela Proposição 4.2.5 segue que a imagem de H em Q é finita e tem ordem $\{k, m, n\}$-limitada. Na verdade, segue que a ordem da imagem de H em Q não depende de Q. Portanto H é finito, como desejado. ■

A versão particular do Teorema 4.0.1 quando consideramos δ_k-comutadores é consequência imediata do teorema anterior. Assim, temos demonstrado o

Teorema 4.2.7. *Seja n um inteiro positivo. Existe um inteiro positivo $\mu = \mu(n)$, dependendo apenas de n, tal que a classe de todos os grupos G com $G^{(k)}$ localmente finito e satisfazendo a propriedade de que qualquer produto de μ δ_k-comutadores em G tem ordem dividindo n é uma variedade.*

4.3 O Caso dos Comutadores Multilineares

Seja k um inteiro positivo. Nesta seção denotamos por w um comutador multilinear de peso k. Os lemas a seguir foram apresentados em [44] e são importantes para a demonstração do caso geral.

Lema 4.3.1. *Seja G um grupo. Todo δ_k-comutador em G é um w-valor.*

Demonstração. O caso $k = 1$ é óbvio e, assim, podemos supor que $k \geq 2$ e usar indução sobre k.

Escrevamos $w = [w_1, w_2]$, onde w_1 e w_2 são comutadores multilineares de pesos k_1 e k_2, respectivamente, com $k_1 + k_2 = k$ e as variáveis envolvidas em uma das palavras w_1, w_2 não ocorrem na outra. Seja $k_0 = \text{máx}\{k_1, k_2\}$. Pela hipótese de indução, todo δ_{k_0}-comutador em G é um w_1-valor bem como um w_2-valor. Sabendo que $w = [w_1, w_2]$, segue que o conjunto de todos os w-valores contém o conjunto dos elementos da forma $[x, y]$, onde x e y são tomados independentemente no conjunto dos δ_{k_0}-comutadores. Assim, qualquer comutador de δ_{k_0}-comutadores representa um w-valor, ou seja, qualquer δ_{k_0+1}-comutador é um w-valor. Desta forma, resta observar que vale $k_0 + 1 \leq k$ e a demonstração está concluída. ■

O próximo lema utiliza o conceito de subcomutador de peso $s \leq k$ de w. Definimos subcomutador utilizando indução reversa sobre s, conforme descrevemos.

Definição 4.3.2. *O único subcomutador de peso k de w é o próprio w. Agora, se $s \leq k-1$, dizemos que um comutador multilinear v de peso s é um <u>subcomutador</u> de w se, e somente se, existe um subcomutador u de w de peso maior do que s e um comutador multilinear v_1 tal que ou $u = [v, v_1]$ ou $u = [v_1, v]$.*

Observamos que se v é um subcomutador de w, então claramente temos $w(G) \leq v(G)$, para qualquer grupo G.

Lema 4.3.3. *Sejam w um comutador multilinear e G um grupo solúvel no qual todo w-valor tem ordem finita. Então o subgrupo verbal $w(G)$ é localmente finito.*

Demonstração. Seja G um contra-exemplo cujo comprimento derivado é o menor possível. Seja T o último termo não trivial da série derivada de G. Passando ao quociente sobre o subgrupo gerado por todos os subgrupos normais localmente finitos de G, podemos assumir que G não possui subgrupos normais localmente finitos não triviais.

Como T é abeliano, segue que não há w-valores contidos em $T \setminus \{1\}$. Seja $s = s(w, G)$ o menor número tal que qualquer subcomutador de peso s de w não possui valores em $T \setminus \{1\}$. Claramente $s \geq 2$, pois $T \neq 1$. Podemos escolher um subcomutador $v = [v_1, v_2]$ de peso maior do que ou igual a s tal que ambos v_1 e v_2 são subcomutadores de peso menor do que s, pelo menos um deles assumindo valor não trivial em $T \setminus \{1\}$. Seja H_i o subgrupo de T gerado pelos v_i-valores contidos em T, $i = 1, 2$. Pela escolha de v, pelo menos um destes subgrupos é não trivial. Como v não possui w-valores em $T \setminus \{1\}$, segue que $[H_1, v_2(G)] \leq T$ e $[H_2, v_1(G)] \leq T$ e, assim, temos que $H_1 \leq C_G(v_2(G))$ e $H_2 \leq C_G(v_1(G))$. Observando que $w(G) \leq u(G)$, para qualquer subcomutador u de w, concluímos que H_1 e H_2 centralizam o subgrupo verbal $w(G)$. Portanto, ambos os subcomutadores v_1 e v_2 não possuem valores não triviais contidos na imagem de T em $G/C_G(w(G))$.

A discussão anterior mostra que $s(w, G/C_G(w(G))) \leq s - 1$. Usando indução sobre $s(w, G)$, segue que $w(G)/Z(w(G))$ (a imagem de $w(G)$ em $G/C_G(w(G))$) é localmente finito. Pelo Corolário 1.5.5, o grupo derivado de $w(G)$ é localmente finito. Como o quociente de $w(G)$ por seu derivado é abeliano e, por hipótese, gerado por elementos de ordens finitas, segue que é localmente finito. Agora, o Teorema 1.5.6 garante que $w(G)$ também é localmente finito, como desejado. ■

É chegado o momento de demonstrar o Teorema 4.0.1. Observamos que, pelo Lema 4.3.1, toda palavra que é o produto de μ δ_k-comutadores é também um produto de μ w-valores. Nas discussões abaixo, $\mu(n)$ é usado no mesmo sentido do Teorema 4.2.6.

Teorema 4.3.4. *Sejam w um comutador multilinear e n um inteiro positivo. Seja $\mathfrak{X}$ a classe de todos os grupos G tendo $w(G)$ localmente finito e satisfazendo a propriedade de que qualquer produto de μ w-valores em G tem ordem dividindo n. Então $\mathfrak{X}$ é uma variedade.*

Demonstração. É fácil ver que a classe $\mathfrak{X}$ é fechada em relação a subgrupos e quocientes de seus membros. Portanto, resta mostrar que se D é um produto cartesiano de grupos em $\mathfrak{X}$, então $D \in \mathfrak{X}$. Sabemos que D satisfaz a propriedade de que qualquer produto de μ w-valores em D tem ordem dividindo n e, assim, é suficiente mostrar que $w(D)$ é localmente finito.

Suponhamos que w possui peso k. Se $G \in \mathfrak{X}$, pelo Lema 4.3.1 temos $G^{(k)} \leq w(G)$ e, assim, $G^{(k)}$ é localmente finito. Pelo Teorema 4.2.6, a classe dos grupos G onde $G^{(k)}$ é localmente finito e satisfazendo a propriedade de que todo produto de μ δ_k-comutadores em G tem ordem dividindo n é uma variedade. Assim, segue que D pertence a esta variedade e, portanto, $D^{(k)}$ é localmente finito. Passemos ao quociente $D/D^{(k)}$, que é solúvel de comprimento derivado k e tem a propriedade de que qualquer w-valor tem ordem dividindo n. Aplicando o Lema 4.3.3 a este quociente, temos que $w(D/D^{(k)})$ é localmente finito. Para concluir que $w(D)$ é localmente finito, basta notar que $w(D/D^{(k)}) \cong w(D)/w(D) \cap D^{(k)}$ e aplicar o Teorema 1.5.6. A demonstração está concluída. ∎

O Teorema 4.0.1 é consequência imediata do teorema anterior e, assim, alcançamos parte de nossos objetivos com esta tese.

Capítulo 5

O Problema Restrito de Burnside para Palavras de Engel

O objetivo principal deste capítulo é demonstrar o resultado a seguir.

Teorema 5.0.1. *Sejam n e k inteiros positivos. Existe um inteiro positivo $\lambda = \lambda(n,k)$, dependendo apenas de n e k, tal que a classe de todos os grupos G satisfazendo a identidade $([x_1, {}_k y_1] \cdots [x_\lambda, {}_k y_\lambda])^n \equiv 1$ e tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito é uma variedade.*

Seguimos interessados em estudar certas generalizações para a Afirmação 2.2.2 que, conforme mencionamos, é equivalente ao Problema Restrito de Burnside. Mais especificamente, desejamos discutir mais uma resposta afirmativa para o Problema 2.2.7.

No capítulo anterior abordamos esse problema para um produto de determinada quantidade de comutadores multilineares. Passamos agora a discutir o caso em que consideramos palavras de Engel.

Relembramos que em [50], Shumyatsky apresentou o seguinte resultado:

Teorema 2.2.16. *Sejam q uma potência de primo e k um inteiro positivo. Existe um inteiro positivo $t = t(q,k)$, dependendo apenas de q e k, tal que a classe de todos os grupos G satisfazendo a identidade $([x_1, {}_k y_1] \cdots [x_t, {}_k y_t])^q \equiv 1$ e tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito é uma variedade.*

O ponto chave para a demonstração do Teorema 2.2.16 é a proposição abaixo, cuja demonstração usa técnicas Lie-teóricas no mesmo sentido que Zelmanov utilizou na solução do Problema Restrito de Burnside. Observamos que ela generaliza o Problema Restrito de Burnside em certo sentido.

Proposição 5.0.2 ([50]). *Existe um inteiro positivo $t = t(q,k)$ com a seguinte propriedade. Sejam l um inteiro positivo e G um grupo finito gerado por m elementos $a_1, a_2, \ldots, a_m$, cada um de ordem dividindo l. Suponhamos que G satisfaz a identidade $([x_1, {}_k y_1] \cdots [x_t, {}_k y_t])^q \equiv 1$, onde q é uma potência de primo. Então a ordem de G é $\{k, m, q, l\}$-limitada.*

O Teorema 5.0.1 representa uma melhoria do Teorema 2.2.16 no sentido de que n não é mais assumido como sendo uma potência de primo, ou seja, considera n um inteiro positivo qualquer.

Novamente a demonstração envolve as seguintes ferramentas: a classificação dos grupos simples finitos, a teoria de Hall-Higman, os resultados Lie-teóricos de Zelmanov e o Teorema de Segal ([40]). Os primeiros resultados obtidos são bastante semelhantes àqueles descritos no Capítulo 4.

5.1 Limitando a Altura de Fitting de um Grupo Solúvel Finito

Como anteriormente, $F(G)$ denota o subgrupo de Fitting de um grupo G, $F_i(G)$ denota o i-ésimo termo da série de Fitting de G e $h(G)$ a altura de Fitting de G.

Mais uma vez necessitamos de alguns fatos relacionados com a altura de Fitting de um grupo solúvel finito satisfazendo uma identidade específica. Estes seguem do Teorema de Segal combinado com outras técnicas.

Iniciamos esta seção com algumas definições.

Definição 5.1.1. *Seja G um grupo.*

(a) *Um elemento $x \in G$ é dito elemento k-Engel (à esquerda) se $[y, {}_k x] = 1$, para todo $y \in G$.*

(b) *Um elemento $g \in G$ é chamado valor k-Engel se existem $x, y \in G$ tais que $g = [x, {}_k y]$.*

(c) *O grupo G é dito grupo k-Engel se $[y, {}_k x] = 1$, para todos $x, y \in G$ (ou seja, se todos os seus elementos são k-Engel).*

(d) *Se para todos $x, y \in G$ existe k, dependendo de x e y, tal que $[x, {}_k y] = 1$, então G é dito um grupo de Engel.*

Observamos que é fácil ver que grupos k-Engel são grupos de Engel. Comentamos anteriormente que uma questão de interesse é saber se um grupo k-Engel é localmente nilpotente. Este fato ainda é desconhecido. Em [56] Wilson mostrou que a resposta é positiva se G é residualmente finito. A origem dos grupos de Engel se deu com o desenvolvimento da Teoria das Álgebras de Lie. Apresentamos a seguir um resultado clássico para grupos de Engel finitos, que é o análogo para o Teorema de Engel para álgebras de Lie de dimensão finita. Pode ser encontrado em [37, Teorema XII.3.4].

Teorema 5.1.2 (Teorema de Zorn)**.** *Um grupo de Engel finito é nilpotente.*

Relembramos o seguinte resultado devido a Segal [40].

Teorema 5.1.3. *Se G é um grupo solúvel finito gerado por m elementos $y_1, y_2, \ldots, y_m$, então todo elemento de G' pode ser escrito como um produto de um número m-limitado de comutadores da forma $[a, b]$, onde $a \in G$, $b \in \{y_1, y_2, \ldots, y_m\}$.*

Usando este fato, obtemos o lema a seguir, cuja demonstração é repetida aqui para auxiliar o leitor na visualização da construção de $\lambda(n, k)$.

Lema 5.1.4. *Seja l um inteiro positivo. Seja G um grupo solúvel finito gerado por m elementos $g_1, g_2, \ldots, g_m$ tais que a ordem de cada g_i divide l. Então todo elemento de G pode ser escrito como um produto de um número $\{m, l\}$-limitado, $f = f(m, l)$, de conjugados de g_i.*

Demonstração. Pelo Teorema 5.1.3, todo elemento de G' pode ser escrito como um produto de r comutadores $[b_i, a_i]$, onde r é um número m-limitado, $b_i \in G$ e $a_i \in \{g_1, g_2, \ldots, g_m\}$. Seja $f = rl + m^l$. Se $x \in G'$, podemos escrever

$$\begin{aligned} x = [b_1, a_1][b_2, a_2] \cdots [b_r, a_r] &= (a_1^{-1})^{b_1} a_1 (a_2^{-1})^{b_2} a_2 \cdots (a_r^{-1})^{b_r} a_r \\ &= a_1^{(l-1)b_1} a_1 a_2^{(l-1)b_2} a_2 \cdots a_r^{(l-1)b_r} a_r. \end{aligned}$$

Assim, x é um produto de no máximo rl conjugados de g_i. Como G/G' é gerado por elementos de ordens dividindo l e a ordem de G/G' é no máximo m^l, segue que cada elemento de G é um produto de no máximo f conjugados dos g_i. ■

No restante deste capítulo, usaremos $f(m, l)$ para denotar o número $\{m, l\}$-limitado no mesmo sentido do Lema 5.1.4 e manteremos a notação de produtos à esquerda para colchetes.

Lema 5.1.5. *Seja G um grupo solúvel finito. Suponhamos que a altura de Fitting do subgrupo verbal de G correspondente à k-ésima palavra de Engel é h. Então é possível escolher h valores k-Engel de G, digamos $v_1, v_2, \ldots, v_h$, tais que o subgrupo $\langle v_1, v_2, \ldots, v_h \rangle$ tem altura de Fitting exatamente h.*

Demonstração. Seja R o subgrupo verbal de G correspondente à k-ésima palavra de Engel. Denotemos $F_i(R)$ por F_i, $1 \leq i \leq h$. Se $h = 1$, então o lema é óbvio. Assim, assumimos $h \geq 2$. Como $F_h = R$, existe um valor k-Engel v_1 tal que $v_1 \notin F_{h-1}$. Já que a altura de Fitting de R/F_{h-2} é igual a 2, pelo Lema 4.1.7, o subgrupo $\langle v_1, F_{h-1} \rangle / F_{h-2}$ não é nilpotente. Desta forma, de acordo com o Lema 4.1.2, a imagem de v_1 em $\langle v_1, F_{h-1} \rangle / F_{h-2}$ não pode ser um elemento de Engel. Logo existe $x_1 \in F_{h-1}$ tal que $[x_1, {}_i v_1] \notin F_{h-2}$, para qualquer inteiro positivo i. Definamos $v_2 = [x_1, {}_k v_1]$. Notemos que v_2 é um valor k-Engel e, além disso, $v_2 \in F_{h-1} \backslash F_{h-2}$.

Analogamente, como o subgrupo $\langle v_2, F_{h-2} \rangle / F_{h-3}$ não é nilpotente, existe $x_2 \in F_{h-2}$ tal que $[x_2, {}_i v_2] \notin F_{h-3}$, para qualquer inteiro positivo i. Definamos $v_3 = [x_2, {}_k v_2]$. Temos que v_3 é um valor k-Engel e $v_3 \in F_{h-2} \backslash F_{h-3}$.

Continuando com este processo, temos que existe $x_{r-1} \in F_{h-(r-1)}$ tal que podemos escolher um valor k-Engel v_r definido por $v_r = [x_{r-1}, {}_k v_{r-1}]$, onde $1 \leq r \leq h$ e $v_r \in F_{h-(r-1)} \backslash F_{h-r}$.

Agora, seja $H = \langle v_1, v_2, \ldots, v_h \rangle$. Resta mostrar que o subgrupo H possui altura de Fitting exatamente h. De fato, temos $v_h \in F(H)$. Além disso, observamos que $v_{h-1} \in F_2(H)$ mas $v_{h-1} \notin F(H)$ (em caso contrário, existiria um inteiro positivo j tal que $[v_h, {}_j v_{h-1}] = 1$). Em geral, temos $v_{h-r} \in F_{r+1}(H)$ mas $v_{h-r} \notin F_r(H)$, onde $0 \leq r \leq h-1$. Portanto, H tem altura de Fitting h e o lema está demonstrado. ■

Notação. Fixemos um inteiro positivo k. Utilizamos o símbolo u_j para denotar a palavra que é o produto de j valores k-Engel. Assim, por exemplo, o símbolo u_2 denota a palavra $[x_1, {}_k y_1]\, [x_2, {}_k y_2]$.

Claramente, se um elemento de um grupo G é um u_i-valor, então é também um u_j-valor em G, para qualquer $i \leq j$. Desta forma, para qualquer $i \leq j$, a identidade $u_j^n \equiv 1$ implica a identidade $u_i^n \equiv 1$ em G. Também é fácil ver que a identidade $u_j^n \equiv 1$ implica que todo valor k-Engel tem ordem dividindo n e este fato será utilizado nas argumentações posteriores sem muitos comentários.

Novamente aplicaremos um corolário da Teoria de Hall-Higman que afirma que a altura de Fitting de qualquer grupo solúvel finito de expoente n é limitada pelo número de divisores de n, contando multiplicidades. Este número será denotado por $h(n)$.

Lema 5.1.6. *Sejam j e n inteiros positivos satisfazendo a propriedade $j \geq f(h(n)+1, n)$. Seja G um grupo solúvel finito satisfazendo a identidade $u_j^n \equiv 1$. Então a altura de Fitting do subgrupo verbal de G correspondente à k-ésima palavra de Engel é no máximo $h(n)$.*

Demonstração. Suponhamos o lema falso. Escrevamos $h = h(n)$. Pelo Lema 5.1.5, podemos escolher $h+1$ valores k-Engel $v_1, v_2, \ldots, v_{h+1}$ em G tais que o subgrupo $H = \langle v_1, v_2, \ldots, v_{h+1} \rangle$ tem altura de Fitting no máximo $h+1$. Pelo Lema 5.1.4, qualquer elemento de H pode ser escrito como um produto de no máximo $f(h(n)+1, n)$ conjugados dos v_i. Como conjugados de valores k-Engel são novamente valores k-Engel, por hipótese, qualquer produto deste tipo tem ordem dividindo n. Assim, H possui expoente n e, portanto, $h(H) \leq h$. Mas isto é uma contradição e a demonstração está concluída. ■

Corolário 5.1.7. *Sob as mesmas hipóteses do Lema 5.1.6, temos* $h(G) \leq h(n) + 1$.

Demonstração. Se R é o subgrupo verbal de G correspondente à k-ésima palavra de Engel, então pelo lema anterior $h(R) \leq h(n)$. O quociente G/R é um grupo de Engel finito. Pelo Teorema de Zorn (Teorema 5.1.2), temos que G/R é nilpotente. Portanto, $h(G) \leq h(n) + 1$. ■

5.2 O Caso das Potências de Primos

Dedicamos esta seção a fatos relacionados ao Teorema 2.2.16 que são úteis para a obtenção do Teorema 5.0.1. Não introduzimos resultados inéditos. O foco principal aqui é apresentar uma demonstração da Proposição 5.0.2 para que seja entendida a relação entre as funções $t = t(q, k)$ e $\lambda = \lambda(n, k)$. No decorrer das presentes discussões, q denota uma potência de um primo p.

O teorema a seguir foi demonstrado por Burns e Medvedev [3] e tem papel fundamental para a obtenção do Teorema 2.2.16.

Teorema 5.2.1. *Existem funções* $c(k)$ *e* $e(k)$*, dependendo apenas de* k*, com a propriedade seguinte. Seja* G *um grupo* k*-Engel finito. Então* G *é uma extensão de um grupo de expoente dividindo* $e(k)$ *por um grupo nilpotente de classe no máximo* $c(k)$*.*

Em algumas discussões aqui, por questões de praticidade, fixado um número inteiro k, escreveremos e e c para indicar $e(k)$ e $c(k)$, respectivamente, como no Teorema 5.2.1.

Agora apresentamos um lema que nos ajuda a reduzir o Teorema 2.2.16 para certas questões sobre p-grupos finitos.

Lema 5.2.2. *Seja* q *uma potência de um número primo* p*. Seja* G *um grupo finito no qual todos os valores* k*-Engel têm ordens dividindo* q*. Então o subgrupo verbal de* G *correspondente à* k*-ésima palavra de Engel é um* p*-grupo.*

Demonstração. Suponhamos o resultado falso e seja G um contra-exemplo de ordem minimal. Claramente G não possui p-subgrupos normais não triviais. Seja r um primo divisor de $|G|$, $r \neq p$, e suponhamos que G possui um r-subgrupo R tal que o quociente $N_G(R)/C_G(R)$ contém um elemento z de ordem co-prima com r. Assim, z pode ser visto como um automorfismo não trivial de R e, portanto, $[R,_k z] \neq 1$ (segundo o Teorema 5.3.6 de [7] [4]). Por outro lado, por hipótese, $[R,_k z]$ deve conter p-elementos, o que é uma contradição. Desta forma, $N_G(R)/C_G(R)$ é um r-grupo, para qualquer r-subgrupo R de G. Portanto, de acordo com Teorema 7.4.5 de [7], G admite um r-complemento normal K [5] . Usando indução sobre $|G|$, temos que o subgrupo verbal de K correspondente à k-ésima palavra de Engel é um p-grupo. Como G não possui p-subgrupos normais não triviais, segue que K é um grupo de Engel. Assim, K é nilpotente, segundo o Teorema de Zorn. Novamente pelo fato de G não possuir p-subgrupos normais não triviais, segue que K é um p'-grupo. Então G é um p'-grupo, o que é uma contradição. ■

A proposição a seguir nos permite visualizar o número $t = t(q,k)$ e é essencial para demonstrarmos a Proposição 5.0.2.

Proposição 5.2.3. *Existe um número $t = t(q,k)$, dependendo apenas de q e k, com a propriedade seguinte. Se G é um p-grupo finito gerado por $2c$ elementos, cada um de ordem dividindo eq e, se G satisfaz a identidade $u_t^q \equiv 1$, então $\gamma_{c+1}(G)$ tem expoente dividindo eq.*

Demonstração. Seja G um p-grupo finito gerado por $2c$ elementos, cada um de ordem dividindo eq. Seja R o subgrupo verbal de G correspondente à k-ésima palavra de Engel. O quociente G/R é um grupo k-Engel e, pelo Teorema de Burns-Medvedev (Teorema 5.2.1), R está contido em um subgrupo normal S de G tal que G/S é nilpotente de classe no máximo c e S/R é um grupo de expoente dividindo e. Como as ordens dos geradores de G são limitadas, segue que G/S tem ordem $\{q,k\}$-limitada. Portanto, o número minimal de geradores de S/R é $\{q,k\}$-limitado (Observação 1.4.3). Pela solução do Problema Restrito de Burnside, concluímos que S/R tem ordem $\{q,k\}$-limitada.

[4] O Teorema 5.3.6 de [7] afirma que se A é um p'-grupo de automorfismos do p-grupo P, então $[P,A,A] = [P,A]$.

[5] A primeira parte do Teorema 7.4.5 de [7] afirma que um grupo G possui um p-complemento normal se, e somente se, $N_G(H)/C_G(H)$ é um p-grupo, para todo p-subgrupo não trivial H de G.

Seja r o número minimal de geradores de R. Logo r é $\{q,k\}$-limitado. Pelo Corolário 1.6.2, podemos escolher um conjunto gerador de R formado por r valores k-Engel, digamos $b_1,\ldots,b_r$. O Lema 1.23 de [5] afirma que qualquer elemento de R' pode ser escrito na forma $[x_1,b_1]\cdots[x_r,b_r]$, para adequados $x_1,\ldots,x_r \in R$. Façamos $t = q^r + qr$ e suponhamos que G satisfaz a identidade $u_t^q \equiv 1$. Como cada um dos comutadores $[x_i,b_i]$ é um produto de um valor k-Engel e do inverso de um valor k-Engel e como um inverso de um valor k-Engel é uma $(n-1)$-ésima potência de um valor k-Engel, segue que qualquer elemento de R' é o produto de no máximo qr valores k-Engel. Agora, R/R' é gerado por valores k-Engel e tem ordem no máximo q^r. Assim, qualquer elemento de R é o produto de no máximo t valores k-Engel. Em particular, o expoente de R é no máximo q e, portanto, o expoente de S é no máximo eq. Resta observar que $\gamma_{c+1}(G) \leq S$. A demonstração está concluída. ■

Agora estamos prontos para demonstrar a Proposição 5.0.2. A argumentação envolve as técnicas Lie-teóricas desenvolvidas por Zelmanov. Por esta razão, faremos uso dos resultados descritos no Capítulo 3.

Demonstração da Proposição 5.0.2. Seja R o subgrupo verbal de G correspondente à k-ésima palavra de Engel. Então, pelo Teorema 5.2.1, G/R é uma extensão de um grupo de expoente dividindo e por um grupo nilpotente de classe no máximo c. A solução positiva do Problema Restrito de Burnside garante que G/R tem ordem $\{k,m,l\}$-limitada. Portanto, é suficiente mostrar que a ordem de R é $\{k,q,m,l\}$-limitada. Pelo Lema 5.2.2, R é um p-grupo. Agora, a Proposição 5.2.3 diz que se $x_1,\ldots,x_{2c} \in R$ são quaisquer elementos de ordens dividindo eq, então $\gamma_{c+1}(\langle x_1,\ldots,x_{2c}\rangle)$ tem expoente dividindo eq. Seja

$$S = \{[x_1,\ldots,x_r] \,:\, c+1 \leq r \leq 2c;\ x_1,\ldots,x_r \in R,\ x_1^{eq} = \cdots = x_r^{eq} = 1\}.$$

É fácil ver que S consiste de elementos de ordens dividindo eq. Mostremos que $[x,y] \in S$ sempre que $x,y \in S$. De fato, suponhamos $x = [x_1,\ldots,x_r]$. Se $r \leq 2c-1$, então escrevemos $[x,y] = [x_1,\ldots,x_r,y]$ e, claramente, este último pertence a S. Se $r = 2c$, fazendo $z = [x_1,\ldots,x_{c+1}]$, escrevemos $[x,y] = [z,x_{c+2},\ldots,x_{2c},y]$. Desta forma, o comutador tem peso $c+1$ com todas as entradas possuindo ordens dividindo eq. Assim, em ambos os casos, $[x, y] \in S$.

Seja $T = \langle S \rangle$ o subgrupo de R gerado pelo conjunto S. Como R é gerado por elementos de ordens dividindo q, segue que $\gamma_{c+1}(R) \leq T$. Sabemos que o índice de R em G é $\{k, q, m, l\}$-limitado. Portanto, o número minimal de geradores de R também é $\{k, q, m, l\}$-limitado. A demonstração da proposição estará completa uma vez provado que a ordem de T é $\{k, q, m, l\}$-limitada.

Se s é o número minimal de geradores de T, então s é $\{k, q, m, l\}$-limitado. Aplicando o Corolário 1.6.2, temos, na verdade, que T é gerado por s elementos, digamos $a_1, a_2, \ldots, a_s$, pertencentes a S.

Já que a identidade $[x,_k y]^q \equiv 1$ vale em T, segue do Lema 3.2.8 que existe um polinômio de Lie não-nulo f sobre $\mathbb{F}_p$, cuja forma depende apenas de k e q, tal que a álgebra $L_p(T)$ satisfaz a identidade $f \equiv 0$ (usando as notações da Seção 3.3).

Consideremos, agora, um monômio de Lie arbitrário σ nos geradores $\widetilde{a}_1, \widetilde{a}_2, \ldots, \widetilde{a}_s$ de $L_p(T)$ e seja ρ o comutador de grupo em $a_1, a_2, \ldots, a_s$ possuindo o mesmo sistema de colchetes que σ. A definição de $L_p(T)$ nos dá ou $\sigma = 0$ ou $\sigma = \widetilde{\rho}$. Como $\rho^{eq} = 1$, o Lema 3.2.6 implica que σ é ad-nilpotente de índice no máximo eq. Pelo Teorema 3.3.8, $L_p(T)$ é nilpotente de classe dependendo apenas de s, k e q. Combinando isto com o Lema 3.3.7, concluímos que existe um número $\{p, k, m, l\}$-limitado d tal que T pode ser escrito como um produto de no máximo d subgrupos cíclicos, cada um de ordem no máximo eq. Portanto, T possui ordem no máximo $e^d q^d$, como desejado. ∎

O Teorema 2.2.16 é obtido como consequência da Proposição 5.0.2. A argumentação é análoga ao que fizemos no Capítulo 4, na demonstração do Teorema 4.2.6. Não apresentaremos aqui a demonstração do Teorema 2.2.16 porque não o aplicamos diretamente para a obtenção do Teorema 5.0.1. É exatamente a Proposição 5.0.2 que nos interessa.

5.3 O Caso Geral

Agora dedicamos nossa atenção a outro resultado central nesta tese. Vamos demonstrar uma generalização do Problema Restrito de Burnside envolvendo palavras de Engel onde não mais nos restringiremos a produtos de valores de Engel com ordens dividindo uma potência de primo. A demonstração do Teorema 5.0.1 passa por uma etapa bastante semelhante ao que descrevemos na seção anterior. Mais precisamente, iremos demonstrar um generalização para a Proposição 5.0.2.

Proposição 5.3.1. *Sejam j, j_1 e n inteiros positivos tais que $j \geq j_1 n + 1$ e seja G um grupo finito satisfazendo a identidade $u_j^n \equiv 1$. Suponhamos que G não possui subgrupos solúveis normais não triviais. Então G possui um subgrupo normal L tal que L é residualmente monolítico e G/L pertence residualmente à classe dos grupos finitos satisfazendo uma identidade $u_{j_1}^{n/p} \equiv 1$, para algum primo p divisor de n.*

Demonstração. Consideremos M um subgrupo normal minimal de G. Então $M \cong S_1 \times S_2 \times \cdots \times S_r$, onde $S_1, S_2, \ldots, S_r$ são grupos simples isomorfos. O grupo G age sobre M permutando os fatores simples e, assim, obtemos uma representação de G por permutações do conjunto $\{S_1, S_2, \ldots, S_r\}$. Seja L_M o núcleo desta representação.

Como S_1 não é solúvel, podemos escolher um elemento não trivial $b \in S_1$ da forma u_1 (conforme a notação introduzida na Página 80). Isto porque se todos os elementos da forma u_1 fossem triviais, S_1 seria um grupo k-Engel finito e, assim, pelo Teorema de Zorn, seria nilpotente.

Seja p um divisor primo da ordem de b. Queremos mostrar que a identidade $u_{j_1}^{n/p} \equiv 1$ é satisfeita em G/L_M. Suponhamos que isto é falso. Seja $q = p^\alpha$ a maior potência de p que divide n. Como estamos supondo que a identidade $u_{j_1}^{n/p} \equiv 1$ não é satisfeita em G/L_M, temos que a identidade $u_{j_1}^{n/q} \equiv 1$ também não é satisfeita em G/L_M e, portanto, existe um elemento $a \in G$ da forma u_{j_1} tal que q divide a ordem de a módulo L_M. Escrevamos $n = n_1 q$ e $a_1 = a^{n_1}$. Desta forma, a_1 é um elemento da forma $u_{j_1 n_1}$ cuja ordem é q. Logo, a_1 permuta regularmente alguns q fatores do conjunto $\{S_1, S_2, \ldots, S_r\}$. Sem perda de generalidade, suponhamos que S_1 é um desses fatores. Escrevamos

$$\begin{aligned}(ba_1)^q &= \underbrace{(ba_1)(ba_1)\cdots(ba_1)}_{q}\\ &= (ba_1)\left(ba_1^{-1}a_1a_1\right)\left(ba_1^{-1}a_1^{-1}a_1a_1a_1\right)\cdots(ba_1)\\ &= bb^{a_1^{-1}}b^{a_1^{-2}}\cdots b^{a_1}.\end{aligned}$$

Como $b \in S_1$, cada um dos elementos $b^{a_1^{-i}}$ pertence a um diferente subgrupo S_i e, assim, o produto $bb^{a_1^{-1}}b^{a_1^{-2}}\cdots b^{a_1}$ possui a mesma ordem de b. Logo $(ba_1)^q$ tem ordem divisível por p e, como $q = p^\alpha$, o elemento ba_1 tem ordem divisível por $p^{\alpha+1}$. Ainda, sendo ba_1 da forma $u_{j_1n_1+1}$, podemos vê-lo como sendo da forma u_j e por isso sua ordem deve dividir n. Isto contradiz nossa escolha maximal de p^α. Portanto, a identidade $u_{j_1}^{n/p} \equiv 1$ é satisfeita em G/L_M.

Agora consideremos L a interseção de todos os subgrupos L_M, onde M percorre o conjunto dos subgrupos normais minimais de G. Sabemos pelo Teorema de Remak que G/L é isomorfo a um produto subcartesiano dos grupos G/L_M. A discussão anterior nos dá que G/L pertence residualmente à classe dos grupos finitos satisfazendo a identidade $u_{j_1}^{n/p} \equiv 1$. Assim, a demonstração estará completa uma vez provado que L é residualmente monolítico.

Se T é o produto dos subgrupos normais minimais de G, então T é o produto de grupos simples $S_1, S_2, \ldots, S_r$ que comutam dois a dois e L é a interseção dos normalizadores dos grupos S_i. A expressão de T como um produto dos S_i é única a menos da ordem dos fatores e um automorfismo de T apenas permuta os subgrupos S_i. Como G não possui subgrupos solúveis normais não triviais, temos $C_G(T) = 1$ e, portanto, sendo G isomorfo a algum subgrupo do grupo dos automorfismos de T, qualquer elemento de L induz um automorfismo não trivial de algum dos S_i.

Seja ρ_i o homomorfismo natural de L no grupo dos automorfismos de S_i. Como mostrado na demonstração da Proposição 4.2.2, a imagem de ρ_i é um subgrupo monolítico e a interseção dos núcleos de todos os ρ_i é trivial. Portanto, L é residualmente monolítico. ■

<u>Escolha de $\lambda(x, y)$</u>

Seja $t = t(x, y)$ com o mesmo sentido da Proposição 5.0.2. Agora vamos escolher uma função $\lambda(x, y)$ definida para quaisquer inteiros positivos x, y e satisfazendo as seguintes propriedades:

1. $\lambda(x, y) \geq f(h(x) + 1, x)$ para todos x, y;

2. $\lambda(x, y) \geq t(x, y)$ sempre que x é uma potência de primo;

3. $\lambda(x, y) \geq x \cdot \lambda(z, y) + 1$ para todos x, y, z tais que z é um divisor próprio de x.

Uma função com tais propriedades pode ser construída utilizando indução sobre x. De fato, fixemos um inteiro positivo y e definamos $\lambda(1, y)$ como sendo o máximo entre os números $f(1, 1)$ e $t(1, y)$. Agora suponhamos que $\lambda(x, y)$ está definida para todo $x \leq n-1$. Se n é uma potência de primo, então coloquemos $\lambda(n, y) = t(n, y)$. Caso contrário, seja M o máximo entre $f(h(n) + 1, n)$ e $n \cdot \lambda(z, y) + 1$, onde z varia no conjunto de todos os divisores próprios de n. Por indução, todos os elementos sobre os quais escolhemos o máximo já estão definidos e, neste caso, coloquemos $\lambda(n, y) = M$. Como isto pode ser feito claramente para qualquer y, estabelecemos a existência de uma função com as propriedades desejadas. No momento conveniente, mostraremos que esta escolha satisfaz as hipóteses do Teorema 5.0.1.

A seguir, generalizamos a Proposição 5.0.2 em certo sentido. Para isto, necessitamos do lema:

Lema 5.3.2. *Sejam m, c e l inteiros positivos. Se G é um grupo finito, nilpotente de classe no máximo c, gerado por m-elementos $g_1, g_2, \ldots, g_m$, onde a ordem de cada g_i divide l, então a ordem de G é $\{m, c, l\}$-limitada.*

Demonstração. Como $g_i^l = 1$, para todo $1 \leq i \leq m$, temos $|\langle g_i \rangle| = l_i$, onde l_i divide l. Denotemos por N_i o fecho normal de g_i em G. Logo $G = N_1 \times N_2 \times \cdots \times N_m$ e, assim, $|G|$ divide $|N_1||N_2| \cdots |N_m|$.

Utilizando indução sobre c, mostremos que $|N_i|$ divide $l_i^{\alpha_i}$ para algum inteiro positivo α_i. Primeiramente, se G é abeliano, segue que $N_i = \langle g_i \rangle$ e, assim, $|N_i| = l_i \leq l$, para todo $1 \leq i \leq m$. Logo $|G| \leq l^m$.

Podemos assumir $c \geq 2$. Neste caso, para todo $1 \leq i \leq m$, temos $N_i \leq \langle g_i, G' \rangle$ e, assim, a classe de nilpotência de N_i é no máximo $c - 1$. Por indução, existem inteiros positivos α_i, dependendo de c, tais que $|N_i|$ divide $l_i^{\alpha_i}$, para todo $1 \leq i \leq m$.

Seja $\alpha = \text{máx}\ \{\alpha_i : 1 \leq i \leq m\}$. Isto implica que $|N_i| \leq l^\alpha$, para todo $1 \leq i \leq m$ e, assim, $|G| \leq l^{\alpha m}$. Portanto, $|G|$ é $\{m, c, l\}$-limitada. ■

Proposição 5.3.3. *Sejam m, n e l inteiros positivos e $\lambda = \lambda(n, k)$. Seja G um grupo finito satisfazendo a identidade $u_\lambda^n \equiv 1$. Suponhamos que G pode ser gerado por m elementos $g_1, g_2, \ldots, g_m$ tais que a ordem de cada g_i e de cada comutador da forma $[g, x]$, onde $g \in \{g_1, g_2, \ldots, g_m\}$ e $x \in G$, divide l. Então a ordem de G é $\{k, m, n, l\}$-limitada.*

Demonstração. Se $n = 1$, então G é um grupo k-Engel. Pelo Teorema 5.2.1, existem c e e, dependendo apenas de k, com a propriedade de que G possui um subgrupo normal N tal que N é de expoente dividindo e e G/N é um grupo nilpotente de classe no máximo c. Pelo Lema 5.3.2, segue que G/N tem ordem $\{k, m, n, l\}$-limitada.

Sabemos que o número minimal de geradores de N é limitado em termos de m e $|G : N|$. Da solução do Problema Restrito de Burnside, segue que $|N|$ e, consequentemente, $|G|$ é $\{k, m, n, l\}$-limitada.

Agora apliquemos indução sobre n. O caso $n = 1$ está demonstrado no parágrafo anterior. Podemos assumir que $n \geq 2$ e que a proposição é verdadeira para grupos satisfazendo uma identidade $u_{\lambda(n/p,k)}^{n/p} \equiv 1$, para algum primo p divisor de n. Em outras palavras, a hipótese de indução é que existe um número N_0, $\{k, m, n, l\}$-limitado, tal que se G é um grupo finito satisfazendo uma identidade $u_{\lambda(n/p,k)}^{n/p} \equiv 1$, gerado por m elementos $g_1, g_2, \ldots, g_m$, onde cada g_i e todos os comutadores da forma $[g, x]$ têm ordens dividindo l, então $|G| \leq N_0$.

Primeiramente, suponhamos que G não possui subgrupos solúveis normais não triviais. Como $\lambda(n,k) \geq n \cdot \lambda(n/p,k) + 1$, pela Proposição 5.3.1, G possui um subgrupo normal L tal que L é residualmente monolítico e G/L pertence residualmente à classe dos grupos finitos satisfazendo uma identidade $u_{\lambda(n/p,k)}^{n/p} \equiv 1$, para algum primo p divisor de n. Pela hipótese de indução, G/L é residualmente de ordem no máximo N_0. Assim, G/L é isomorfo a um produto subcartesiano de grupos cujas ordens são no máximo N_0. Sendo G/L um grupo m-gerado, pelos Teoremas 1.3.2 e 1.3.3, o número de subgrupos normais distintos de índice no máximo N_0 em G/L é $\{m, N_0\}$-limitado. Logo, $|G/L|$ é $\{k,m,n,l\}$-limitada. Em particular, pela Observação 1.4.3, L pode ser gerado por r elementos, onde r é um número $\{k,m,n,l\}$-limitado.

Do Teorema 4.2.4 segue que, salvo isomorfismos, existe apenas um número finito de grupos monolíticos satisfazendo a identidade $u_\lambda^n \equiv 1$. Seja $N_1 = N_1(n,\lambda)$ o máximo das ordens destes grupos. Então L é residualmente de ordem no máximo N_1. Agora, sendo L um grupo r-gerado, sabemos que o número de subgrupos normais distintos de índice no máximo N_1 em L é $\{r, N_1\}$-limitado. Portanto, a ordem de L e, consequentemente, a ordem de G é $\{k,m,n,l\}$-limitada.

Vejamos agora o que ocorre quando retiramos a hipótese de G não possuir subgrupos solúveis normais não triviais. Seja S o produto de todos os subgrupos solúveis normais de G. A discussão anterior nos dá que G/S tem ordem $\{k,m,n,l\}$-limitada. Como $\lambda(n,k) \geq f(h(n)+1,n)$, o Corolário 5.1.7 nos dá que a altura de Fitting $h(S)$ é $\{k,m,n,l\}$-limitada. Seja $F = F(G)$ o subgrupo de Fitting de G e passemos ao quociente G/F. Este satisfaz as hipóteses da proposição e é tal que $h(S/F) < h(S)$. Por indução sobre $h(S)$, obtemos que F tem índice $\{k,m,n,l\}$-limitado em G.

Suponhamos F central. Neste caso, $|G:Z(G)|$ é $\{k,m,n,l\}$-limitado e, pelo Teorema de Schur, $|G'|$ é $\{k,m,n,l\}$-limitada. Como G pode ser gerado por m elementos, todos de ordens dividindo l, segue que $|G|$ é $\{k,m,n,l\}$-limitada.

No caso em que F não é central, consideremos o subgrupo

$$N = \langle [g_1, F], [g_2, F], \ldots, [g_m, F] \rangle.$$

Como cada g_i normaliza N, para todo $1 \leq i \leq m$, segue que N é normal em G. Aplicando os resultados do parágrafo anterior ao quociente G/N, segue que $|G : N|$ é $\{k, m, n, l\}$-limitado. Resta mostrar que $|N|$ e, portanto, $|G|$, é $\{k, m, n, l\}$-limitada.

Sabemos que N pode ser gerado por um número $\{k, m, n, l\}$-limitado de elementos. Seja s o número minimal de geradores de N. Como N é nilpotente, $\pi(N)$ consiste dos primos divisores de l. Assim, é suficiente limitar a ordem do p-subgrupo de Sylow de N, para todo primo $p \in \pi(N)$.

Seja P o p-subgrupo de Sylow de N e escrevamos $N = P \times O_{p'}(N)$. Se $y_1, y_2, \ldots$ é a lista de todos os elementos da forma $[g_i, y]$, onde $1 \leq i \leq m$ e $y \in F$, denotemos por $b_1, b_2, \ldots$ as correspondentes projeções dos y_j em P. Daí $P = \langle b_1, b_2, \ldots \rangle$. Como P é um p-grupo finito s-gerado, o Corolário 1.6.2 garante que P é na verdade gerado por s elementos na lista $b_1, b_2, \ldots$. Por hipótese, a ordem de cada um destes divide l. Seja q a maior potência de p que divide n. Como $\lambda(n, k) \geq t(q, k)$, pela Proposição 5.0.2 concluímos que P tem ordem $\{k, m, n, l\}$-limitada e a demonstração está completa. ■

É chegado o momento de demonstrar o Teorema 5.0.1.

Teorema 5.3.4. *Sejam n um inteiro positivo e $\lambda = \lambda(n, k)$. Seja $\mathfrak{X}$ a classe de todos os grupos tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito e satisfazendo a propriedade de que qualquer u_λ-valor tem ordem dividindo n. Então $\mathfrak{X}$ é uma variedade.*

Demonstração. É fácil verificar que a classe $\mathfrak{X}$ é fechada em relação a subgrupos e quocientes de seus membros. Resta mostrar que se D é um produto cartesiano de grupos em $\mathfrak{X}$, então $D \in \mathfrak{X}$. É óbvio que a identidade $u_\lambda^n \equiv 1$ é satisfeita em D e, assim, é suficiente mostrar que se R é o subgrupo verbal de D correspondente à k-ésima palavra de Engel, então R é localmente finito. Para isto, mostraremos que qualquer subconjunto finito de R gera um subgrupo finito.

Seja S um subconjunto finito qualquer de R. Claramente, existem valores k-Engel $h_1, h_2, \ldots, h_m \in D$ tais que $S \leq \langle h_1, h_2, \ldots, h_m \rangle = H$. Assim, é suficiente verificar que o subgrupo H é finito. É fácil ver que a identidade $u_\lambda^n \equiv 1$ implica que a ordem de cada h_i divide n, para todo $1 \leq i \leq m$. Além disso, se $h \in \{h_1, h_2, \ldots, h_m\}$ e $x \in H$, então cada comutador da forma $[h, x]$ é um produto de n valores k-Engel. Uma vez que da escolha de λ temos $\lambda(n, k) \geq n$, para todo $n \geq 2$, a identidade $u_\lambda^n \equiv 1$ implica que a ordem de cada um desses comutadores divide n.

Notando que R é isomorfo a um produto subcartesiano de grupos localmente finitos, temos R residualmente localmente finito. Se Q é qualquer quociente localmente finito de R, então pela Proposição 5.3.3, a ordem da imagem de H em Q é finita e $\{k, m, n\}$-limitada. Na verdade, a ordem da imagem de H em Q não depende de Q. Portanto H é finito, como desejado. ■

O Teorema 5.0.1 é obtido como consequência imediata do teorema anterior. Assim, alcançamos outro objetivo deste trabalho.

Capítulo 6

Corolários para Grupos Residualmente Finitos

Neste capítulo apresentamos alguns resultados sobre grupos residualmente finitos relacionados a generalizações do Problema Restrito de Burnside. Precisamente, vamos demonstrar um corolário imediato do Teorema 4.0.1 e outro do Teorema 5.0.1, a saber:

Corolário 6.0.1. *Sejam n inteiro positivo e $\mu = \mu(n)$ como no Teorema 4.0.1. Se w é um comutador multilinear e G é um grupo residualmente finito satisfazendo a propriedade de que todo produto de μ w-valores tem ordem dividindo n, então o subgrupo verbal $w(G)$ é localmente finito.*

Corolário 6.0.2. *Sejam n e k inteiros positivos e $\lambda = \lambda(n, k)$ como no Teorema 5.0.1. Suponhamos que G é um grupo residualmente finito satisfazendo a identidade $([x_1, {}_k y_1] \cdots [x_\lambda, {}_k y_\lambda])^n \equiv 1$. Então o subgrupo verbal correspondente à k-ésima palavra de Engel é localmente finito.*

Sabemos que o Problema Restrito de Burnside é equivalente à afirmação de que todo grupo residualmente finito de expoente n é localmente finito. Por outro lado, é bem conhecido que um grupo residualmente finito periódico não é necessariamente localmente finito. Exemplos podem ser encontrados em trabalhos de Aleshin [2], Golod [6], Grigorchuk [8], Gupta [9] e Sushchansky [54].

Os Corolários 6.0.1 e 6.0.2 são formulações particulares para o Problema 2.3.4, o qual discutimos na Seção 2.3 e reescrevemos abaixo.

Problema 2.3.4. *Sejam n um inteiro positivo e w uma palavra. Suponhamos que G é um grupo residualmente finito tal que todo w-valor tem ordem dividindo n. Será que o subgrupo verbal $w(G)$ é localmente finito?*

Vimos que para $w = x$, o Problema 2.3.4 é exatamente o Problema Restrito de Burnside e que algumas respostas positivas foram obtidas, por exemplo, em [42], [48] e [49], utilizando as técnicas Lie-teóricas desenvolvidas por Zelmanov. As discussões sobre variedades de grupos e o Problema 2.3.4 são problemas de naturezas semelhantes e resultados para o Problema 2.3.4 podem ser obtidos como consequências daqueles resultados obtidos para variedades. É exatamente essa ideia que utilizaremos para demonstrar os Corolários 6.0.1 e 6.0.2.

Demonstração do Corolário 6.0.1. Sejam w um comutador multilinear, n um inteiro positivo e $\mu = \mu(n)$ como no Teorema 4.0.1. Seja $\mathfrak{X}$ a classe de todos os grupos tais que o subgrupo verbal correspondente à palavra w é localmente finito e tem a propriedade de que todo produto de μ w-valores tem ordem dividindo n.

Qualquer quociente finito de G pertence a $\mathfrak{X}$. Sendo G residualmente finito, G é isomorfo a um produto subcartesiano de quocientes finitos que pertencem a $\mathfrak{X}$ e, assim, G pertence residualmente a $\mathfrak{X}$. Sabemos, pelo Teorema 4.0.1, que $\mathfrak{X}$ é uma variedade e, além disso, é claro que se um grupo pertence residualmente a certa variedade, então ele pertence a tal variedade (de acordo com a Proposição 1.3.6). Portanto, $G \in \mathfrak{X}$ e, consequentemente, $w(G)$ é localmente finito. ∎

Demonstração do Corolário 6.0.2. Sejam n e k inteiros positivos, u uma k-ésima palavra de Engel e $\lambda = \lambda(n, k)$ como no Teorema 5.0.1. Seja $\mathfrak{X}$ a classe de todos os grupos satisfazendo a propriedade de que qualquer produto de λ u-valores tem ordem dividindo n e tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito.

Qualquer quociente finito de G pertence a $\mathfrak{X}$. Como G é residualmente finito, G é isomorfo a um produto subcartesiano de quocientes finitos que pertencem a $\mathfrak{X}$. Segue que G pertence residualmente a $\mathfrak{X}$. Pelo Teorema 5.0.1, $\mathfrak{X}$ é uma variedade e, assim, $G \in \mathfrak{X}$. Portanto, o subgrupo verbal de G correspondente à k-ésima palavra de Engel é localmente finito. ■

Observamos que as demonstrações são completamente análogas. Na verdade, são exemplos do lema que apresentamos a seguir, que afirma que uma resposta positiva para o Problema 2.2.7 implica em uma resposta positiva para o Problema 2.3.4. Já é mais complicado decidir se a recíproca é verdadeira. Ainda não sabemos dizer se os Problemas 2.2.7 e 2.3.4 são equivalentes.

Lema 6.0.5. *Se o Problema 2.2.7 tem resposta positiva, então o Problema 2.3.4 também tem.*

Demonstração. De fato, seja $\mathfrak{X}$ a classe de todos os grupos G satisfazendo a identidade $w^n \equiv 1$ e tendo o subgrupo verbal $w(G)$ localmente finito. Suponhamos que $\mathfrak{X}$ é uma variedade. Seja H um grupo residualmente finito satisfazendo a identidade $w^n \equiv 1$. Então H pertence residualmente a $\mathfrak{X}$. Como $\mathfrak{X}$ é uma variedade, segue que $H \in \mathfrak{X}$ e, portanto, $w(H)$ é localmente finito. ■

Ainda enfatizamos que o Corolário 6.0.1 não afirma que o subgrupo verbal $w(G)$ correspondente ao comutador multilinear w tem expoente n e que o Corolário 6.0.2 não afirma que o subgrupo verbal correspondente à k-ésima palavra de Engel tem expoente n. Relembramos que estas questões são de certo modo relacionadas ao resultado de Kleiman, apresentado ao final da Seção 2.3.

Considerações Finais

Com as discussões anteriores finalizamos a apresentação de nossas principais contribuições no intuito de estender o Problema Restrito de Burnside. Certamente ainda há outras questões a serem discutidas no sentido do Problema Restrito de Burnside Generalizado. Desta forma, encerramos este trabalho registrando alguns fatos que merecem reflexões futuras.

1. Os resultados que apresentamos por meio dos Teoremas 4.0.1 e 5.0.1 trazem as hipóteses de que determinados produtos de valores da palavra em questão têm ordens dividindo n. Sabemos que o subgrupo verbal gerado por esses produtos é o mesmo subgrupo verbal gerado simplesmente pelos valores da palavra. Desta forma, podemos nos perguntar se os seguintes resultados são válidos:

(a) *Seja w um comutador multilinear. Se n é um inteiro positivo, será que a classe de todos os grupos G satisfazendo a condição de que todo w-valor tem ordem dividindo n e tendo o subgrupo verbal $w(G)$ localmente finito é uma variedade?*

(b) *Sejam n e k inteiros positivos. Será que a classe de todos os grupos G satisfazendo a identidade $[x,_k y]^n \equiv 1$ e tendo o subgrupo verbal correspondente à k-ésima palavra de Engel localmente finito é uma variedade?*

Até o presente momento não sabemos como demonstrar estas formulações. Uma dificuldade significativa é que não sabemos se a teoria de Hall-Higman pode ser aplicada com sucesso nestes casos. Vimos que é conhecido que a altura de Fitting de um grupo solúvel finito de expoente n é n-limitada. Entretanto, uma questão em aberto é se a altura de Fitting de um grupo solúvel finito satisfazendo a identidade $[x,y]^n \equiv 1$ é limitada em função de n.

2. Vimos que os Corolários 6.0.1 e 6.0.2 não afirmam que os subgrupos verbais em questão têm expoente n. Desta forma, fica a pergunta:

Será que existe um grupo G satisfazendo as hipóteses do Corolário 6.0.1 (respectivamente, do Corolário 6.0.2) tal que o subgrupo verbal $w(G)$ (respectivamente, o subgrupo verbal correspondente à k-ésima palavra de Engel) tem expoente infinito?

3. O Problema 2.2.7 é equivalente ao Problema 2.3.4? Se enunciarmos generalizações para cada uma das equivalências do Problema Restrito de Burnside (ver Seção 2.1), então quais equivalências podem ser obtidas?

4. Em [43, Teorema 3.2] Shumyatsky mostrou o seguinte resultado:

Teorema. *Sejam k e n inteiros positivos e seja G um grupo residualmente finito tal que $[x_1, x_2, \ldots, x_k]$ é n-Engel, para todos $x_1, x_2, \ldots, x_k \in G$. Então $\gamma_k(G)$ é localmente nilpotente.*

Assim, outra questão natural é a investigação de palavras que satisfaçam a mesma propriedade, ou seja, uma questão em aberto é saber para quais palavras $w = w(x_1, x_2, \ldots, x_m)$ o problema abaixo tem resposta positiva.

Problema. *Seja n um inteiro positivo. Seja G um grupo residualmente finito satisfazendo a identidade $[x, {}_n w] \equiv 1$. Será que o subgrupo verbal $w(G)$ é localmente nilpotente?*

Referências Bibliográficas

[1] S. I. ADIAN, *The Burnside problem and identities in groups*, Izdat. "Nauka", Moscow, (1975), 335 pp.

[2] S. V. ALESHIN, *Finite automata and the Burnside problem for periodic groups*, Math. Notes **11** (1972), 199 – 203.

[3] R. G. BURNS, Y. MEDVEDEV, *A note on Engel groups and local nilpotence*, J. Austral. Math. Soc. (Series A) **64** (1998), 92-100.

[4] G. S. DERYABINA, P. A. KOZHEVNIKOV, *The derived subgroup of a group with commutators of bounded order can be non-periodic*, Comm. Algebra (9) **27** (1999), 4525 – 4530.

[5] J. D. DIXON, M. P. F. du SAUTOY, A. MANN, D. SEGAL, *Analytic pro-p Groups*, London Math. Soc. Lecture Note Series, Cambridge Univ. Press **157** (1991).

[6] E. S. GOLOD, *On nil-algebras and finitely approximable p-groups*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 273 – 276.

[7] D. GORENSTEIN, *Finite Groups*, Harper & Row, New York, 1968.

[8] R. I. GRIGORCHUK, *On the Burnside problem for periodic groups*, Funct. Anal. Appl. **14** (1980), 53 – 54.

[9] N. D. GUPTA, *Periodicity of the commutator subgroup of a certain group*, Notices AMS, **14** (1967), 703.

[10] N. GUPTA, S. SIDKI, *On the Burnside problem for periodic groups*, Math. Z. **182** (1983), 385 – 388.

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

[12] G. HIGMAN, *Lie rings methods in the theory of finite nilpotent groups*, in: Proc. Intern. Congr. Math. Edinburgh-1958, Cambridge Univ. Press (1960), 307 – 312.

[13] B. HUPPERT, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[14] B. HUPPERT, N. BLACKBURN, *Finite Groups II*, Springer-Verlag, Berlin, 1982.

[15] S. V. IVANOV, *On the Burnside problem on periodic groups*, Bull. Amer. Math. Soc. (N.S.) **27** (1992), n. 2, 257 – 260.

[16] G. A. JONES, *Varieties and simple groups*, J. Austral. Math. Soc. **17** (1974), 163 – 173.

[17] M. HALL JR., *Solution of the Burnside problem for exponent six*, Illinois J. Math. **2** (1958), 764 – 786.

[18] M. HALL JR., *The Theory of Groups*, Macmillan, New York, 1959.

[19] M. I. KARGAPOLOV, Ju. I. MERZLJAKOV, *Fundamentals of the Theory of Groups*, Springer-Verlag, New York, 1979.

[20] E. I. KHUKHRO, *Nilpotent Groups and their Automorphisms*, Walter de Gruyter & Co., Berlin, 1993.

[21] E. I. KHUKHRO, *p-Automorphisms of finite p-groups*, Cambridge Univ. Press, Lecture Note Series **246** (1998).

[22] Ju. G. KLEIMAN, *On a basis of the product of varieties of groups*, II. Math. USSR Izvestija **8** (1974), 481 – 489.

[23] E. I. KHUKHRO, V. D. MAZUROV (eds), *Unsolved problems in group theory.* The Kourovka notebook. Thirteenth augmented edition. Edited by V. D. Mazurov and E. I. Khukhro. Russian Academy of Sciences Siberian Division, Institute of Mathematics, Novosibirsk, 1995.

[24] E. I. KHUKHRO, P. SHUMYATSKY, *Bounding the exponent of a finite group with automorphisms*, J. Algebra **212** (1999), 363 – 374.

[25] A. I. KOSTRIKIN, *On the Burnside Problem*, Izv. Akad. Nauk SSSR Ser. Mat. **23** (1959), 3 – 34.

[26] M. LAZARD, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. École Norm. Sup. **71** (1954), 101 – 190.

[27] I. G. LYSIONOK, *Infinite Burnside groups of even period*, Izv. Ross. Akad. Nauk Ser. Mat. **60** (1996), 3 – 224.

[28] I. D. MACDONALD, *On certain varieties of groups*, Math. Z. **76** (1961), 270 – 282.

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

[30] N. S. MENDELSOHN, *Some examples of man-machine interaction in the solution of mathematical problems*, in: Computational problems in abstract algebra (Proc. Conf., Oxford, 1967), Pergamon, Oxford, (1970), 217 – 222.

[31] H. NEWMANN, *Varieties of Groups*, Springer-Verlag, Berlin, 1967.

[32] N. NIKOLOV, D. SEGAL, *On finitely generated profinite groups. I: Strong completeness and uniform bounds*, Ann. of Math. (2) **165** (2007), 171-238.

[33] P. S. NOVIKOV, S. I. ADIAN, *Infinite periodic groups* I, II, III, Izv. Akad. Nauk SSSR Ser. Mat. **32** (1968) $212 - 244, 251 - 524, 709 - 731$.

[34] A. Yu. OLSHANSKII, *On a geometric method in the combinatorial group theory*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), 415 – 424, PWN, Warsaw, (1984).

[35] A. Yu. OLSHANSKII, *Geometry of defining relations in groups*, Math. Appl. (Soviet Ser.) **70** (1991).

[36] D. J. S. ROBINSON, *Finiteness Conditions and Generalized Soluble Groups, Part 1*, Springer-Verlag, Berlin, 1972.

[37] D. J. S. ROBINSON, *A Course in the Theory of Groups*, 2.ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996.

[38] J. J. ROTMAN, *An Introduction to the Theory of Groups*, 4.ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[39] I. N. SANOV, *Solution of Burnside's problem for exponent 4*, Leningrad State Univ. Annals (Uchenye Zapiski), Math. Ser. **10** (1940), 166 – 170.

[40] D. SEGAL, *Closed subgroups of profinite groups*, Proc. London Math. Soc. (3) **81** (2000), 29 – 54.

[41] A. SHALEV, *Centralizers in residually finite torsion groups*, Proc. Amer. Math. Soc. **126** (1998), 3495 – 3499.

[42] P. SHUMYATSKY, *On groups with commutators of bounded order*, Proc. Amer. Math. Soc. **127** (1999), 2583 – 2586.

[43] P. SHUMYATSKY, *Applications of Lie ring methods to group theory*, in: Nonassociative algebra and its applications (R. Costa, A. Grishkov, H. Guzzo Jr. and L. A. Peresi, eds), Marcel Dekker (2000), 373 – 395.

[44] P. SHUMYATSKY, *Verbal subgroups of residually finite groups*, Quart. J. Math. (Oxford) **51** (2000), 523 – 528.

[45] P. SHUMYATSKY, *Verbal generalizations of the Restricted Burnside Problem*, in: 16th School of Algebra, Part II (Portuguese) (Brasilia, 2000), Mat. Contemp. SBM **21** (2001), 239 – 254.

[46] P. SHUMYATSKY, *A (locally nilpotent)-by-nilpotent variety of groups*, Math. Proc. Camb. Phil. Soc. **132** (2002), 193 – 196.

[47] P. SHUMYATSKY, *On varieties arising from the solution of the Restricted Burnside Problem*, J. Pure Appl. Alg. **171** (2002), 67 – 74.

[48] P. SHUMYATSKY, *Commutators in residually finite groups*, Monatsh. Math. **137** (2002), 157 – 165.

[49] P. SHUMYATSKY, *A variety of groups*, Math. Proc. Camb. Phil. Soc. **138** (2005), 21 – 26.

[50] P. SHUMYATSKY, *Engel values in residually finite groups*, Monatsh. Math., **152** (2007), 169-175.

[51] P. SHUMYATSKY, J. C. SILVA, *The Restricted Burnside Problem for Multilinear Commutators*, Math. Proc. Camb. Phil. Soc., 2008.

[52] P. SHUMYATSKY, J. C. SILVA, *Engel Words and the Restricted Burnside Problem*, Monatsh. Math., 2008.

[53] P. SHUMYATSKY, J. C. SILVA, *Varieties of Groups and the Restricted Burnside Problem*, Ischia Group Theory 2008, World Scientific, 2008.

[54] V. I. SUSHCHANSKY, *Periodic p-elements of permutations and the general Burnside problem*, Dokl. Akad. Nauk SSSR **247** (1979), 447 – 461.

[55] A. TURULL, *Fitting height of groups and of fixed points*, J. Algebra **86** (1984), 555 – 566.

[56] J. S. WILSON, *Two-generator conditions for residually finite groups*, Bull. London Math. Soc. **23** (1991), 239 – 248.

[57] J. S. WILSON, E. ZELMANOV, *Identities for Lie algebras of pro-p groups*, J. Pure. Appl. Algebra **81** (1992), 103 – 109.

[58] H. ZASSENHAUS, *Ein Verfahren, jeder endlischen Gruppe einen Lie-Ring mit der Charakteristiki p zuzuordnen*, Abh. Math. Seminar Hans. Univ. Hamburg **13** (1940), 200 – 207.

[59] E. ZELMANOV, *The solution of the Restricted Burnside Problem for groups of odd exponent*. Math. USSR Izvestija **36** (1991), $41 - 60$.

[60] E. ZELMANOV, *The solution of the Restricted Burnside Problem for 2-groups*, Math. Sb. **182** (1991), $568 - 592$.

[61] E. ZELMANOV, *Nil rings and periodic groups*, The Korean Math. Soc. Lecture Notes in Math., Seoul, (1992).

[62] E. ZELMANOV, *Lie ring methods in the theory of nilpotent groups*, in: C. M. Campbell et al. (Eds.), Proceedings of Groups'93, St. Andrews, London Math. Soc. Lecture Note Series, Vol. 212, Cambridge University Press, Cambridge, (1995), $567 - 585$.

Índice Remissivo

álgebra de Lie, 47
    p-álgebra de Lie, 56
    PI, 50

altura
    de Fitting, 20, 62, 64, 79, 80
    de Hirsch-Plotkin, 38
anel de Lie, 47, 49

comutador, 17, 37
    δ_k-comutador, 61
    de Lie, 47
    multilinear, 37

derivação, 48

elemento
    k-Engel, 40, 78
    ad-nilpotente, 48, 50
    de Engel, 60

Fórmula de Coleção, 51
Fórmula de Compilação de P. Hall, 20

grupo
    k-Engel, 40, 78
    m-gerado, 26
    p-grupo regular, 46
    de Engel, 78
    derivado, 17
    finitamente gerado, 26
    livre, 22, 23
    localmente $\mathfrak{X}$, 29
    monolítico, 64
    nilpotente, 18, 19
    residualmente $\mathfrak{X}$, 22, 24
    solúvel, 18, 19

Homomorfismo Transfer, 28

identidade, 24
    de Jacobi, 47

monômio, 51

operador adjunto, 48

palavra, 24
    central inferior, 38
    derivada, 38
Problema de Burnside, 31
    Problema Restrito de Burnside, 33
produto
    cartesiano, 21
    subcartesiano, 21

série
    N-série, 48

N_p-série, 49
abeliana, 18
central p-dimensional, 56
central inferior, 18
de Fitting, 20
de Jennings-Lazard-Zassenhaus, 51, 56
derivada, 18
subcomutador, 73
subgrupo
de Frattini, 30
de Fitting, 20
verbal, 24

Teorema
da Base de Burnside, 30
de Birkhoff, 25
de Remak, 21
de Schmidt, 29
de Schur, 28
de Segal, 61, 78
de Zorn, 78
transversal, 26

valor, 24
k-Engel, 78
u_j-valor, 80
w_j-valor, 63
variedade, 24, 72, 75, 90

Deus sempre nos dá a saída para nossos problemas e nossas angústias. Confiemos n'Ele sem duvidar!