Universidade de Brasília

Centralizadores em grupos de torção residualmente finitos

Um estudo via Métodos de Lie

Mateus Figueiredo de Souza

Orientadora: Profª. Dr.ª Cristina Acciarri

Brasília, 20 de Fevereiro de 2020

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Centralizadores em grupos de torção residualmente finitos
Um estudo via métodos de Lie

por

Mateus Figueiredo de Souza*

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

MESTRE EM MATEMÁTICA

Brasília, 20 de fevereiro de 2020.

Comissão Examinadora:

Profa. Dra. Cristina Acciarri - MAT/UnB (Orientadora)

Prof. Dr. Emerson Ferreira de Melo – MAT/UnB (Membro)

Prof. Dr. Jhone Caldeira Silva – UFG (Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação.

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

Fc

Figueiredo de Souza, Mateus
Centralizadores em grupos de torção residualmente finitos - Um estudo via Métodos de Lie / Mateus Figueiredo de Souza; orientador Cristina Acciarri. -- Brasília, 2020.
106 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2020.

1. Centralizadores. 2. Grupos de Torção. 3. Métodos de Lie. I. Acciarri, Cristina, orient. II. Título.

Agradecimentos

A Deus por ter me dado coragem de vir de tão longe tentar a vida em Brasília e por ter me dado forças para suportar as adversidades naturais da vida de um estudante de Mestrado.

À minha mãe, dona Raimunda Figueiredo, por todas as mensagens de confiança e por sempre me motivar lembrando-me de seu desejo de morar na praia. Ao meu pai, seu Raimundo Nonato, que deu o primeiro passo na minha educação conseguindo, com muita luta, uma vaga no Colégio Acreano. Ainda, agradeço aos meus irmãos Alcemira, Alcimara e Tiago por ter sido meu alicerce, ter me incentivado e acreditado em mim.

À minha orientadora, professora Cristina Acciarri, pelas orientações, pelos diversos ensinamentos e conselhos que levarei para a vida. Agradeço acima de tudo por ter me motivado em todos os meus constantes momentos de melancolia, pelos elogios e críticas, e por ter acreditado em mim quando nem mesmo eu o fazia.

Aos membros da banca, professores Emerson Ferreira e Jhone Caldeira pelos elogios e pelos conselhos para melhoria deste trabalho.

À minha companheira Maria Gabriela que há muito tempo tem sido meu porto seguro. Sem seu apoio, carinho, amor e paciência eu não teria concluído este Mestrado.

À Maria Edna, a melhor sub-amiga que uma pessoa pode ter. Você se tornou minha melhor amiga, mesmo que tenha ganhado isto com uma aposta. Agradeço por ter ouvido meu choro até instantes antes da apresentação.

Ao meu amigo João Pedro por diversas vezes ter compartilhado horas de conversas sobre Matemática. Sua ajuda na disciplina de Análise foi crucial para o entendimento de diversas noções e suas ideias, sempre precisas, me ajudaram a entender alguns passos de determinadas provas expostas neste trabalho.

Aos meus amigos Junio e Deivid pelo apoio com o LaTex e ao Geovane pelas conversas e caminhadas pela UnB.

Aos meus amigos Adler, Claudia, Gabriel, Murilo, Rosalina, Paulo, Tharles, Vítor, Rodolfo e Rômulo por me proporcionarem diversos momentos de descontração.

Agradeço ao Márcio e à Raquel pela hospitalidade quando recém-chegado a Brasília, pelos passeios que fizemos quando ainda morava na Asa Sul, e principalmente, pelas boas risadas que compartilhamos.

Faço um agradecimento especial ao professor Sérgio Brazil pelo incentivo e por ter sido meu pai na Universidade Federal do Acre. Ainda, aos professores Wenden Charles e José Ronaldo pelas cartas de recomendação para chegar à UnB.

Agradeço também aos professores que participaram da minha formação como mestre, Jiazheng Zhou, Tarcísio Castro, Irina Sviridova, Daniele Nantes, Alex Carrazedo e, principalmente, Aline Pinto.

Finalmente, agradeço ao CNPq pelo apoio financeiro que foi crucial para minha permanência em Brasília.

Resumo

Construções dadas por N. Gupta e S.N. Sidki em [6] mostram que um grupo de torção residualmente finito não necessariamente é localmente finito. Um questionamento natural, portanto, é o seguinte: Sob quais condições pode-se concluir que um grupo de torção residualmente finito é localmente finito?

Os trabalhos de V.P. Shunkov [32] e B. Hartley [8, 9] evidenciam que uma ferramenta próspera no estudo de grupos de torção é impor condições sobre centralizadores. Shunkov prova, por exemplo, que se G é um grupo de torção possuindo uma involução g tal que $C_G(g)$ é finito, então G é localmente finito.

Utilizando Métodos de Lie, A. Shalev prova no artigo *Centralizers in residually finite torsion groups* [28], referência principal deste trabalho, que se G é um grupo de torção residualmente finito, sem 2–elementos, que é agido por um 2–grupo finito Q de modo que $C_G(Q)$ é solúvel ou têm expoente finito, então G é localmente finito. Na classe dos grupos residualmente–(finito nilpotente), A. Shalev obtém em [28] o seguinte resultado mais forte: se G é um grupo de torção residualmente–(finito nilpotente), sem 2–elementos, que é agido por um 2–grupo finito Q de modo que $C_G(Q)$ satisfaz uma identidade não trivial de grupo, então G é localmente finito. A. Shalev ainda generaliza em [28] o resultado de Shunkov provando que se G é um grupo de torção residualmente finito possuindo um 2–subgrupo finito Q tal que $C_G(Q)$ é finito, então G é localmente finito.

Palavras-chave: Centralizadores, Grupos de Torção, Métodos de Lie.

Abstract

Examples given by N. Gupta and S.N. Sidki in [6] show that a residually finite torsion group is not necessarily locally finite. A natural question, therefore, is: Under which conditions is it possible to conclude that a residually finite torsion group is locally finite?

The works of V.P. Shunkov [32] and B. Hartley [8, 9] show that a thriving tool in the study of torsion groups is to impose conditions on the centralizers. Shunkov proves, for instance, that if G is a torsion group admitting an involution g such that $C_G(g)$ is finite, then G is locally finite.

Using Lie Methods, A. Shalev proves in the article *Centralizers in residually finite torsion groups* [28], main reference of this dissertation, that if G is a residually finite torsion group, with no 2–elements, acted by a finite 2–group Q such that $C_G(Q)$ is soluble or has finite exponent, then G is locally finite. For the class of residually–(finite nilpotent) groups, A. Shalev obtains in [28] the next stronger result: if G is a residually–(finite nilpotent) group, with no 2–elements, acted by a finite 2–group Q such that $C_G(Q)$ satisfies a non trivial group identity, then G is locally finite. A. Shalev further generalizes in [28] Shunkov's result, proving that if G is a residually finite torsion group that has a finite 2–subgroup Q such that $C_G(Q)$ is finite, then G is locally finite.

Keywords: Centralizers, Torsion Groups, Lie Methods.

Conteúdo

Introdução **1**

1 Noções preliminares **5**
1.1 Ações de grupos 5
1.1.1 Noções gerais de ações de grupos 5
1.1.2 Ações via automorfismos 7
1.2 Grupos nilpotentes 11
1.3 Grupos solúveis 17

2 Álgebras de Lie **23**
2.1 Módulos e álgebras 23
2.2 N_p–séries e o anel de Lie associado 29
2.3 Identidades polinomiais 38

3 Os resultados de Zelmanov e Bahturin–Zaicev **45**
3.1 Propriedades residuais 45
3.2 O Teorema de Zelmanov 51
3.3 Sobre identidades em álgebras de Lie graduadas 55

4 Resultados principais **65**
4.1 Grupos localmente finitos 66
4.2 Restrição aos grupos de torção residualmente–(finito nilpotente) 67
4.3 Limite na altura de Fitting em função do expoente 76
4.4 O Teorema Principal de A. Shalev 83

Bibliografia **91**

Lista de Símbolos **95**

Introdução

Um grupo G é dito de torção se todo elemento de G tem ordem finita. E G é dito ser localmente finito se todo subgrupo finitamente gerado de G é finito. O Problema Geral de Burnside é o seguinte questionamento: É verdade que todo grupo de torção é localmente finito? Dizemos que G tem expoente finito se os elementos de G têm ordens finitas limitadas por um número inteiro positivo n. Assim, uma versão mais restrita do problema anterior é a seguinte: É verdade que todo grupo de expoente finito é localmente finito? Tal problema ficou conhecido como Problema de Burnside. O Problema Geral de Burnside recebeu resposta negativa em 1964 dada por E.S. Golod em [3]. Já o Problema de Burnside recebeu resposta negativa em 1968 dadas por P.S. Novikov e S.I. Adian em [21–23].

Permita-nos denotar por $\mathcal{C}$ uma classe de grupos finitos fechadas para subgrupos, imagens epimórficas e produtos diretos finitos. Um grupo G é chamado residualmente–$\mathcal{C}$ se todo elemento não trivial de G possui uma imagem não trivial em um grupo na classe $\mathcal{C}$. Nosso interesse particular neste trabalho é quando $\mathcal{C}$ denota a classe dos grupos finitos, neste caso um grupo residualmente–$\mathcal{C}$ é chamado residualmente finito. Uma outra resposta negativa ao Problema Geral de Burnside foi dada por N. Gupta e S.N. Sidki em [6], onde os autores construíram, para cada primo ímpar p, um p–grupo infinito 2–gerado e residualmente finito. Portanto, um questionamento natural é o seguinte: Sob quais condições pode-se concluir que um grupo de torção residualmente finito é localmente finito?

Sejam G e Q dois grupos e suponha que Q age em G. Vários resultados foram obtidos entre os anos 60 e 80 do século passado que mostram como impor condições sobre o subgrupo dos pontos fixos $C_G(Q)$ nos retorna informações sobre o grupo G. Por exemplo, se G e Q são solúveis de ordens finitas e coprimas, J.G. Thompson prova em [33] que a altura de Fitting de G é limitada superiormente por uma função da altura de Fitting de $C_G(Q)$ e do número de primos dividindo a ordem de Q. Posteriormente, em [32], V.P. Shunkov mostra que se G é grupo de torção e G possui uma involução g cujo centralizador $C_G(g)$ é finito, então G é localmente finito. Tal resultado foi estendido por N.R. Rocco e P. Shumyatsky em [24], onde provam que se G é um grupo de torção residualmente finito que possui um 2–elemento g tal que $C_G(g)$ é finito, então G é localmente finito. Ainda neste contexto, B. Hartley prova em [8] que se G

é grupo de torção e possui um automorfismo involutivo φ tal que $|C_G(\varphi)| = n < \infty$, então G possui um subgrupo normal H tal que $H' \leq C_G(\varphi)$ e $[G:H]$ é limitado superiormente por uma função de n.

Os trabalhos de V.P. Shunkov e B. Hartley evidenciam que um caminho próspero no estudo de grupos de torção é o de impor condições sobre centralizadores. Neste sentido, no artigo *Centralizers in residually finite torsion groups* [28], principal referência deste trabalho, A. Shalev prova o seguinte resultado.

Teorema A. *Seja G um grupo de torção residualmente finito e sem 2–elementos. Suponha que Q seja um 2–grupo finito agindo em G de modo que $C_G(Q)$ seja solúvel ou possua expoente finito. Nestas condições, G é localmente finito.*

A ideia principal para provar o Teorema A é notar que podemos assumir que G é finitamente gerado e, neste último caso, mostrar que todo fator finito de G é solúvel de altura de Fitting limitada por um inteiro positivo fixo m. Para fazer isto, iremos utilizar um resultado de A. Turull, melhorando o resultado de J.G. Thompson anteriormente citado e um resultado devido a A. Shalev, também provado em [28], limitando a altura de Fitting de um grupo finito solúvel em função de seu expoente.

Seja G um grupo arbitrário. Dizemos que G satisfaz uma identidade não trivial de grupo se existe um elemento não trivial $w = w(x_1,\ldots,x_n)$ no grupo livremente gerado por $x_1,\ldots,x_n$ de modo que para todos $g_1,\ldots,g_n \in G$ vale $w(g_1,\ldots,g_n) = 1$. Na classe dos grupos residualmente–(finito nilpotente), A. Shalev obtém uma versão mais forte do Teorema A.

Teorema B. *Seja G um grupo de torção residualmente–(finito nilpotente) e sem 2–elementos. Suponha que Q seja um 2–grupo finito agindo em G de modo que $C_G(Q)$ satisfaça uma identidade não trivial de grupo. Nestas condições, G é localmente finito.*

Nas condições do Teorema B, assumindo que G é finitamente gerado, mostra-se que G é produto direto de p–subgrupos maximais e residualmente um p–grupo finito, $p \neq 2$, o que reduz a prova ao caso em que G é residualmente–p, $p \neq 2$. Neste caso particular, quando G é residualmente–p, uma das técnicas essenciais utilizadas na demonstração é a técnica de Métodos de Lie, que consiste em traduzir à linguagem de álgebras de Lie um problema sobre o grupo G, demonstrar resultados sobre álgebras de Lie, e então retornar estes resultados à linguagem de Teoria de Grupos e deduzir consequências sobre a estrutura do grupo G.

Ainda motivado pelos resultados de V.P. Shunkov, N.R. Rocco e P. Shumyatsky, A. Shalev também prova em [28] o seguinte resultado, como um corolário imediato do Teorema A.

Corolário A. *Seja G um grupo de torção residualmente finito. Se G possui um 2–subgrupo finito Q tal que $C_G(Q)$ é finito, então G é localmente finito.*

Finalizamos estas notas iniciais observando que este trabalho está divido em 4 capítulos. No primeiro capítulo nos dispomos a expor as ferramentas fundamentais sobre Teoria de Grupos a serem utilizadas ao longo do trabalho. Iremos neste capítulo, essencialmente, obter resultados fundamentais sobre ações de grupos, grupos nilpotentes e grupos solúveis.

No capítulo seguinte, iremos construir as noções essenciais sobre álgebras de Lie que serão comumente utilizadas nos capítulos posteriores. Noções como N_p–séries e o anel de Lie associado serão construídas neste capítulo, além do conceito de identidades em álgebras e PI–álgebras.

No terceiro capítulo deste trabalho, nos devotamos a provar dois resultados essenciais para a utilização de Métodos de Lie na demonstração do Teorema B. O primeiro deles, provado em [37] por E.I. Zelmanov, afirma que se G é um grupo de torção finitamente gerado e residualmente–p e o anel de Lie associado a G construído no Capítulo 2 satisfaz uma identidade polinomial, então G é finito. Para a prova deste resultado iremos utilizar um resultado obtido por E.I. Zelmanov em [36], onde Zelmanov prova que se L é uma álgebra de Lie sobre um corpo F, de característica positiva p, satisfazendo uma identidade polinomial, sob convenientes suposições adicionais, pode-se concluir que L é nilpotente. Observamos que este último resultado é o principal teorema provado por Zelmanov em [36], resultado este que foi essencial para dar uma solução positiva ao Problema Restrito de Burnside. Posteriormente, iremos provar um resultado estabelecido em [1] por Y.A. Bahturin e M.V. Zaicev sobre álgebras de Lie graduadas.

No capítulo final deste trabalho, iremos inicialmente expor os resultados básicos sobre grupos localmente finitos que serão utilizados na demonstração do Teorema A. Posteriormente, iremos demonstrar o Teorema B. A seção seguinte se devota a estabelecer um resultado A. Shalev, limitando a altura de Fitting de um grupo solúvel G em função de seu expoente. Concluimos o trabalho dando a demonstração do Teorema A e Corolário A.

Capítulo 1

Noções preliminares

Neste capítulo expomos noções básicas e resultados preliminares que necessitaremos ao longo deste trabalho. Resultados como Teoremas de Isomorfismo, Teoremas de Sylow e Teorema da Correspondência são assumidos conhecidos. As principais referências bibliográficas utilizadas neste capítulo são os livros de H.E. Rose [26], I.M. Isaacs [13] e H. Kurzweiel e B. Stellmacher [19]. Quando X, Y forem conjuntos e $f : X \longrightarrow Y$ uma função utilizaremos a notação exponencial x^f para denotar a imagem do elemento $x \in X$ pela função f. Ainda, quando G for um grupo finito e $g \in G$, $|G|$ denota a ordem de G e pomos $|g| = |\langle g \rangle|$.

1.1 Ações de grupos

1.1.1 Noções gerais de ações de grupos

Em toda esta subseção, G denota um grupo arbitrário.

Definição 1.1. Dizemos que G age no conjunto não vazio X se para cada $g \in G$ e $x \in X$ existe um elemento bem definido $x^g \in X$ de modo que para cada $g, h \in G$ e $x \in X$ valem

(i) $x^1 = x$;

(ii) $x^{gh} = (x^g)^h$.

Da definição acima, se G age no conjunto não vazio X, a aplicação que associa o elemento $x \in X$ ao elemento x^g é uma bijeção de X. Mais do que isto, a aplicação

$$\begin{aligned} \rho : G &\longrightarrow Sym(X) \\ g &\longmapsto \quad g^\rho : X \longrightarrow X \\ & \qquad\quad x \longmapsto x^g \end{aligned}$$

é um homomorfismo de grupos, onde $Sym(X)$ denota o grupo das permutações do conjunto X. O conjunto $K = \{g \in G;\ x^g = x\ \forall\ x \in X\}$ é chamado o núcleo da ação. Usamos esta nomenclatura pois K coincide com o núcleo de ρ.

Reciprocamente, se $\rho : G \longrightarrow Sym(X)$ é um homomorfismo, $x^g := x^{g^\rho}$ define uma ação de G em X. Vemos, pois, que uma ação de G em X determina e é determinada por um homomorfismo de G em $Sym(X)$.

Lema 1.2. *Suponha que G age no conjunto não vazio X e seja $N \trianglelefteq G$ um subgrupo contido no núcleo da ação. Então, a ação de G em X induz uma ação de G/N em X.*

Demonstração. Sejam $x \in X$ e $g,h \in G$. Se $Ng = Nh$, então $gh^{-1} \in N$. Por hipótese, N está contido no núcleo da ação e portanto $x^{gh^{-1}} = x$, isso é, $x^g = x^h$. Finalmente, dados $Ng, Nh \in G/N$ e $x \in X$ fica bem definido o elemento $x^{Ng} := x^g$ e vale $x^{N1} = x^1 = x$ e $x^{NgNh} = x^{Ngh} = x^{gh} = (x^g)^h = (x^{Ng})^{Nh}$. Isso é, G/N age em X. □

Suponha que G age no conjunto não vazio X. Definimos uma relação $\sim$ em X do seguinte modo: dados $x, y \in X$, $x \sim y$ se existe $g \in G$ tal que $x^g = y$. Observe que a relação $\sim$ é relação de equivalência em X. A classe de equivalência de $x \in X$ é chamada a órbita de x e é denotada por $\mathcal{O}_G(x)$. Ainda, se $x \in X$, definimos o estabilizador de x em G como sendo o subgrupo $stab_G(x) := \{g \in G; x^g = x\}$. O seguinte teorema relaciona estes dois últimos conjuntos, sua prova pode ser encontrada em [26, pág. 95, Teorema 5.7].

Teorema 1.3 (da Órbita-Estabilizador)**.** *Para todo $x \in X$ existe uma bijeção entre os conjuntos $\mathcal{O}_G(x)$ e o conjunto das classes laterais à direita de $stab_G(x)$.*

Seja p um primo. Um elemento $g \in G$ é chamado um p–elemento se $|g|$ é alguma potência de p. Assim, G é chamado um p–grupo se todo elemento em G é um p–elemento. Em particular, pelo Teorema de Cauchy, G é um p–grupo finito se, e somente se, $|G|$ é uma potência de p.

Lembramos que para cada $x, g \in G$ o conjugado de x por g é o elemento $x^g = g^{-1}xg$.

Lema 1.4. *([26, pág.105, Lema 5.21]) Se G é um p–grupo finito, p um primo, então $Z(P) \neq 1$.*

Seja G um grupo arbitrário e $S(G)$ o conjunto formado por todos os subgrupos de G. Para todo $g \in G$, a função $I_g : G \longrightarrow G$ definida por $x \mapsto x^g = g^{-1}xg$ é automorfismo de G. Dado $H \in S(G)$, definindo $H^g = g^{-1}Hg = I_g(H)$, vemos que G age por conjugação em $S(G)$. O estabilizador $stab_G(H)$ do elemento $H \in S(G)$ é chamado o normalizador de H em G e é denotado por $N_G(H)$. Este subgrupo é o menor subgrupo de G no qual H é normal. Agora, a órbita de H é o conjunto formado pelos seus conjugados. Então, se G é finito, pelo Teorema 1.3 o número de conjugados de H em G é igual a $[G : N_G(H)]$. Finalmente, definindo $C_G(H) := \{g \in G; gh = hg\ \forall\ h \in H\}$, o centralizador de H em G, temos que $C_G(H) \trianglelefteq N_G(H)$.

Dizemos que o grupo G age transitivamente no conjunto X se para todos $x, y \in X$ existe $g \in G$ de modo que $x^g = y$. Um dos principais resultados sobre ações transitivas é demonstrado a seguir.

Teorema 1.5 (Argumento de Frattini)**.** *Suponha que G age no conjunto não vazio X e G possui um subgrupo normal N agindo transitivamente em X. Nestas condições, para todo $x \in X$, $G = stab_G(x)N$.*

Demonstração. Seja $x \in X$ um elemento arbitrário e $g \in G$. Como N age transitivamente em X, existe $n \in N$ de modo que $x^g = x^n$. Segue que $gn^{-1} \in stab_G(x)$, isso é, $g \in stab_G(x)N$. A arbitrariedade da escolha de $g \in G$ mostra que $G \leq stab_G(x)N$ e o resultado está demonstrado. □

Corolário 1.6. *([19, pág. 66, Teorema 3.2.7]) Suponha que G é finito e seja $N \trianglelefteq G$. Sejam p um primo e P um p–subgrupo de Sylow de N. Então, $G = N_G(P)N$.*

1.1.2 Ações via automorfismos

Sejam A um grupo e suponha que A age no conjunto subjacente ao grupo G. Então sabemos que esta ação determina e é determinada por um homomorfismo $\rho : A \longrightarrow Sym(G)$. Como G é grupo, $Aut(G) \leq Sym(G)$. Dizemos, então, que A age via automorfismos no grupo G se $Im(\rho) \leq Aut(G)$. Isso é, A age via automorfismos no grupo G se A age no conjunto G e a aplicação $a^\rho : G \longrightarrow G$ definida por $g \mapsto g^a$ é um homomorfismo de G.

Durante esta subseção, assuma que A é um grupo agindo no grupo G, $B \leq A$, $H \leq G$ e $\rho : A \longrightarrow Aut(G)$ é o homomorfismo determinado pela ação de A no grupo G. Nestas condições, para qualquer subconjunto X de G e $a \in A$, X^a denota a imagem de X pelo automorfismo a^ρ de G. A seguir fixamos algumas notações.

Definição 1.7. Pomos por definição as seguintes:

(i) $N_B(H) = \{b \in B; H^b = H\}$;

(ii) $C_B(H) = \{b \in B; h^b = h,\ \forall h \in H\}$;

(iii) $C_H(b) = \{h \in H; h^b = h\}$ para todo $b \in B$;

(iv) $C_H(B) = \bigcap_{b \in B} C_H(b)$;

(v) $g^{-a} := (g^{-1})^a$ para todos $g \in G$ e $a \in A$;

(vi) $[g,a] := g^{-1}g^a$ e $[a,g] := g^{-a}g$, para todos $g \in G$ e $a \in A$.

Note que $N_B(H), C_B(H) \leq B$, $C_H(a), C_H(B) \leq H$ e $C_A(G)$ é o núcleo da ação de A no grupo G. O subgrupo $C_G(A) = \{g \in G; g^a = g,\ \forall a \in A\}$ é chamado o centralizador de A em G e é de particular interesse neste trabalho. Ainda, H é chamado A–invariante se $N_A(H) = A$ o que ocorre se, e somente se, para todo $h \in H$ e $a \in A$, $h^a \in H$.

Lema 1.8. *Seja N um subgrupo normal A–invariante de G. Então, a ação de A em G induz a uma ação de G em G/N.*

Demonstração. Sejam $g, h \in G$ e suponha que $gN = hN$. Temos que $g^{-1}h \in N$ e, portanto, para todo $a \in A$, temos que $(g^{-1}h)^a = g^{-a}h^a \in N$, isso é, $h^aN = g^aN$. Segue que $(gN)^a := g^aN$ define uma ação de A em G/N. □

Suponha que $N \trianglelefteq G$, $G = HN$ e $N \cap H = 1$. Neste caso, dizemos que G é produto semi-direto interno de N por H, H é chamado um complemento para N em G e escrevemos $G = N \rtimes H$. Neste caso, todo elemento de $g \in G$ pode ser escrito de modo único na forma hn onde $h \in H$ e $n \in N$. Ainda, desde que $N \trianglelefteq G$, para todo $h \in H$, a aplicação $n \mapsto n^h$ é um automorfismo de N e, portanto, H age em N por conjugação. Note ainda que dados $h_1, h_2 \in H$ e $g_1, g_2 \in N$, vale $h_1g_1h_2g_2 = h_1h_2h_2^{-1}g_1h_2g_2 = h_1h_2g_1^{h_2}g_2$.

Por sua vez, considere o conjunto $A \times G = \{(a,g); a \in A, g \in G\}$. Lembramos que A age em G via automorfismos e a ação é determinada pelo homomorfismo $\rho : A \longrightarrow Aut(G)$. Defina $(a,g) \cdot (b,h) := (ab, g^bh)$, para cada $(a,g), (b,h) \in A \times G$. É possível conferir que $A \times G$ com a multiplicação assim definida é um grupo, o qual denotamos por $G \rtimes_\rho A$, chamado o produto semi-direto externo de G por A com relação ao homomorfismo ρ. Se $a \in A$ e $g \in G$, note que $(a,1)^{-1}(1,g)(a,1) = (a^{-1},1)(1,g)(a,1) = (a^{-1},g)(a,1) = (1,g^a)$, o que mostra que a ação de A em G é por conjugação. Em tempo, $A \times 1$ e $1 \times G$ são subgrupos de $G \rtimes_\rho A$ isomorfos a A e G, respectivamente, e $1 \times G \trianglelefteq G \rtimes_\rho A$. Como $(A \times 1) \cap (1 \times G) = 1$, $(A \times 1)(1 \times G) = G \rtimes_\rho A$ e $1 \times G \trianglelefteq G \rtimes_\rho A$, o grupo $G \rtimes_\rho A$ é produto semidireto interno de $1 \times G$ por $A \times 1$. Identificando $A \times 1$ com A e $1 \times G$ com G, podemos observar $G \rtimes_\rho A$ como um produto semidireto interno de G por A.

Dizemos que A age coprimamente em G se A e G são grupos finitos de ordens relativamente primas. Nosso interesse particular em ações coprimas é no estudo de centralizadores, mas, antes de expormos alguns resultados nesse sentido, enunciamos um importante resultado conhecido como Teorema de Schur–Zassenhaus. Uma prova deste resultado pode ser encontrada em [13, pág. 79, Teorema 3.8]

Teorema 1.9 (de Schur–Zassenhaus)**.** *Suponha que G é um grupo finito e $N \trianglelefteq G$ é tal que $|N|$ e $[G:N]$ são relativamente primos. Então existe um subgrupo H de G tal que $G = N \rtimes H$. Mais do que isto, quaisquer dois complementos para N em G são conjugados em G.*

Lema 1.10. *Suponha que a ação de A em G é coprima e seja H um subgrupo A–invariante de G. Seja $g \in G$ um elemento tal que $(Hg)^a = Hg$ para todo $a \in A$. Então, existe $c \in C_G(A)$ tal que $Hg = Hc$.*

Demonstração. Para cada $a \in A$ temos que $g^a g^{-1} \in H$. Trabalhando no produto semidireto $G \rtimes_\rho A$, temos que $[a, g^{-1}] \in H$ para todo $a \in A$. Isso mostra que $A^{g^{-1}} \leq AH$. Dado que $H \trianglelefteq AH$ e $|H|$ e $[AH : H]$ são relativamente primos, pelo Teorema 1.9, A e $A^{g^{-1}}$ são conjugados em AH e existe $a \in A$ e $h \in H$ de modo que $A^{g^{-1}} = A^{ah} = A^h$. Logo, $A^{g^{-1}h^{-1}} = A$ e, portanto, $hg \in N_{G \rtimes_\rho A}(A)$. Pondo $c = hg$, $c \in N_{G \rtimes_\rho A}(A) \cap Hg$ e $\langle [a,c];\ a \in A \rangle = \langle c^{-a} c;\ a \in A \rangle \leq A \cap G = 1$, isso é, $c \in C_G(A)$. □

No que segue, expomos o principal resultado no nosso estudo de ações coprimas.

Teorema 1.11. *Seja A um grupo finito agindo no grupo finito G e suponha que A e G possuem ordens coprimas. Seja N um subgrupo normal A–invariante de G. Nessas condições*

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

Demonstração. Claramente temos que $C_G(A)N/N \leq C_{G/N}(A)$. Reciprocamente, se $Ng \in C_{G/N}(A)$, para todo $a \in A$ vale que $(Ng)^a = Ng$. Pelo Lema 1.10, existe $c \in C_G(A)$ tal que $Ng = Nc \in C_G(A)N/N$. Logo $C_{G/N}(A) \leq C_G(A)N/N$ e o resultado está demonstrado. □

O grupo G é chamado de torção, ou periódico, se todo elemento em G tem ordem finita. Note que subgrupos, grupos quocientes e produtos diretos finitos de grupos de torção são, também, de torção. A seguinte versão do Teorema 1.11 foi provada em [24] por N.R. Rocco e P. Shumyatsky.

Teorema 1.12. *Suponha que A é um 2–grupo finito agindo num grupo de torção G. Suponha que G não possui 2–elementos. Então, para qualquer subgrupo normal A–invariante N de G, temos que*

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

Demonstração. Inicialmente, todo elemento em G tem ordem ímpar. Logo, para todo $x \in G$ existe um único elemento $y \in \langle x \rangle$ tal que $y^2 = x$. Permita-nos escrever $y = x^{\frac{1}{2}}$ e, definindo $x^{-\frac{1}{2}} = y^{-1}$, note que $x^{-\frac{1}{2}} = (x^{-1})^{\frac{1}{2}}$. Como $x^{\frac{1}{2}} \in \langle x \rangle$, para todo $\varphi \in Aut(G)$ vale que $(x^{\frac{1}{2}})^\varphi \in \langle x^\varphi \rangle$. Ainda, $(x^{\frac{1}{2}})^\varphi (x^{\frac{1}{2}})^\varphi = (x^{\frac{1}{2}} x^{\frac{1}{2}})^\varphi = x^\varphi$. Segue-se que $(x^{\frac{1}{2}})^\varphi = (x^\varphi)^{\frac{1}{2}}$. Analogamente verifica-se

que $(x^{-\frac{1}{2}})^{\varphi} = (x^{-\varphi})^{\frac{1}{2}}$. Assumindo adicionalmente que φ tem ordem 2, temos que

$$\begin{aligned}(x(x^{-\varphi}x)^{-\frac{1}{2}})^{\varphi} &= x^{\varphi}((x^{-\varphi}x)^{-\varphi})^{\frac{1}{2}} = x^{\varphi}(x^{-\varphi}x)^{\frac{1}{2}} = x^{\varphi}(x^{-\varphi}x)^{\frac{1}{2}}(x^{-\varphi}x)^{\frac{1}{2}}(x^{-\varphi}x)^{-\frac{1}{2}} \\ &= x^{\varphi}x^{-\varphi}x(x^{-\varphi}x)^{-\frac{1}{2}} = x(x^{-\varphi}x)^{-\frac{1}{2}}.\end{aligned}$$

Isso é, $x(x^{-\varphi}x)^{-\frac{1}{2}} \in C_G(\varphi)$.

A prova é por indução em $|A|$. Note antes que nosso trabalho se resume a verificar que $C_{G/N}(A) \leq C_G(A)N/N$ pois claramente $C_G(A)N/N \leq C_{G/N}(A)$. Suponha inicialmente que $|A| = 2$ e seja $A = \langle\varphi\rangle$. Seja $xN \in C_{G/N}(A)$ um elemento fixado. Temos que $x^{-\varphi}x \in N$. Portanto, desde que φ tem ordem 2 e $x = x(x^{-\varphi}x)^{-\frac{1}{2}}(x^{-\varphi}x)^{\frac{1}{2}}$, temos das considerações do último parágrafo que $xN = x(x^{-\varphi}x)^{-\frac{1}{2}}(x^{-\varphi}x)^{\frac{1}{2}}N = x(x^{-\varphi}x)^{-\frac{1}{2}}N \in C_G(\varphi)N/N = C_G(A)N/N$.

Podemos, então, supor que $|A| \geqslant 4$ e o resultado vale para 2–grupos finitos com ordem estritamente menor que $|A|$. Pelo Lema 1.4, podemos escolher um elemento $\varphi \in Z(A)$ de ordem 2. Seja $H = C_G(\varphi)$. Para cada $h \in H$ e $a \in A$, note que $(h^a)^{\varphi} = h^{a\varphi} = h^{\varphi a} = (h^{\varphi})^a = h^a$, isso é, H é subgrupo A–invariante de G. Do fato que N é A–invariante, concluimos que $H \cap N$ é A–invariante e, portanto, A age em $H/(H \cap N)$. Em tempo, se K é o núcleo da ação de A em H, $\varphi \in K$ e $|A/K| < |A|$. Por hipótese de indução, temos que

$$C_{H/(H\cap N)}(A/K) = C_H(A/K)(H \cap N)/(H \cap N).$$

Desde que $C_{H/(H\cap N)}(A/K) = C_{H/(H\cap N)}(A)$ e $C_H(A/K) = C_H(A) = C_G(A)$, temos que

$$C_{H/(H\cap N)}(A) = C_G(A)(H \cap N)/(H \cap N).$$

Seja por sua vez $xN \in C_{G/N}(A)$. Então temos que $x^{-\varphi}x \in N$ e $x = x(x^{-\varphi}x)^{-\frac{1}{2}}(x^{-\varphi}x)^{\frac{1}{2}}$. Desde que φ tem ordem 2, $x(x^{-\varphi}x)^{-\frac{1}{2}} \in H$ e então para todo $a \in A$ concluímos que

$$(x(x^{-\varphi}x)^{-\frac{1}{2}})^{-a}x(x^{-\varphi}x)^{-\frac{1}{2}} \in H.$$

Para todo $a \in A$ ainda obtemos que $x^aN = (x(x^{-\varphi}x)^{-\frac{1}{2}})^aN = xN = x(x^{-\varphi}x)^{-\frac{1}{2}}N$, isso é, $(x(x^{-\varphi}x)^{-\frac{1}{2}})^{-a}x(x^{-\varphi}x)^{-\frac{1}{2}} \in N$. Vemos, pois, que $x(x^{-\varphi}x)^{-\frac{1}{2}}(H \cap N) \in C_{H/(H\cap N)}(A)$. Então existem $c \in C_G(A)$ e $d \in H \cap N$ tais que $x(x^{-\varphi}x)^{-\frac{1}{2}} = cd$ e então $xN = x(x^{-\varphi}x)^{-\frac{1}{2}}(x^{-\varphi}x)^{\frac{1}{2}}N = cdN = cN \in C_G(A)N/N$. A arbitrariedade da escolha de $xN \in C_{G/N}(A)$ estabelece que $C_{G/N}(A) \leq C_G(A)N/N$ e o resultado está demonstrado. □

Terminamos esta seção com o próximo resultado, também obtido em [24] por Rocco e Shumyatsky. Este é um primeiro resultado que mostra como impor condições em centralizadores de grupos de torção nos retornam informações sobre o grupo.

Teorema 1.13. *Suponha que A é um 2–grupo finito agindo no grupo de torção G. Se $C_G(A)$ não possui 2–elementos, então G não possui 2–elementos.*

Demonstração. Argumentamos por indução em $|A|$. Se $|A| = 2$, seja $A = \langle \varphi \rangle$. Se G possui um 2–elemento, podemos tomar uma involução $g \in G$. Note que $(gg^{\varphi})^{\varphi} = g^{\varphi}g = (gg^{\varphi})^{-1}$. Desde que G é grupo de torção, $|gg^{\varphi}| < \infty$. Se $|gg^{\varphi}| = 2n$, $n \geqslant 1$, temos que $|(gg^{\varphi})^n| = 2$ e $((gg^{\varphi})^n)^{\varphi} = ((gg^{\varphi})^{\varphi})^n = ((gg^{\varphi})^{-1})^n = ((gg^{\varphi})^n)^{-1} = (gg^{\varphi})^n$. Assim, $(gg^{\varphi})^n$ é uma involução em $C_G(\varphi) = C_G(A)$. Podemos então supor que $|gg^{\varphi}| = 2n+1$, $n \geqslant 0$. Então, $(g^{\varphi}g)^{n+1}g$ é uma involução e $((g^{\varphi}g)^{n+1}g)^{\varphi} = ((g^{\varphi}g)^{n+1})^{-1}g^{\varphi} = (g^{\varphi}(g^{\varphi}g)^{n+1})^{-1} = (g(g^{\varphi}g)^n)^{-1} = (g^{\varphi}g)^{n+1}g$. Isso é, $(g^{\varphi}g)^{n+1}g$ é uma involução em $C_G(A)$.

Podemos então supor que $|A| \geqslant 4$ e que o resultado vale para 2–grupos finitos com ordens estritamente menores a $|A|$. Pelo Lema 1.4 podemos tomar φ um elemento de ordem 2 em $Z(A)$. Se G possui um 2–elemento, o parágrafo anterior mostra que $H = C_G(\varphi)$ possui um 2–elemento. Como φ está no núcleo K da ação de A em H, temos que A/K é um 2–grupo finito agindo em H e tal que $|A/K| < |A|$. Por indução, temos que $C_H(A/K)$ possui um 2–elemento. Finalmente o resultado segue pois $C_H(A/K) = C_G(A)$. □

1.2 Grupos nilpotentes

Nesta seção temos por objetivo expor as noções essenciais que precisaremos sobre grupos nilpotentes.

Lembramos que para todo grupo G e elementos $x, y \in G$, o comutador de x e y é definido como sendo o elemento $[x,y] = x^{-1}y^{-1}xy$. Assim, para todos subconjuntos X e Y de G fica definido o conjunto $[X,Y] = \langle [x,y]; x \in X, y \in Y \rangle$. O subgrupo $G' \coloneqq [G,G]$ é chamado o subgrupo derivado de G. Pode-se verificar que para todo subgrupo normal N de G, G/N é abeliano se, e somente se, $G' \leq N$.

Seja X um conjunto não vazio. Definimos comutadores no conjunto X (como expressões formais) indutivamente pelo seu peso. Se $x \in X$, então x é um comutador de peso 1. Se c_1, c_2 são comutadores em X de pesos $r_1, r_2 \geqslant 1$, respectivamente, então $[c_1, c_2]$ é comutador de peso $r_1 + r_2$. Indutivamente, temos definido comutador de qualquer peso em X. Os comutadores simples de peso $n \geqslant 1$ em X são definidos indutivamente pelas regras $[x_1] = x_1$ e, para todo $n \geqslant 2$, $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$.

O seguinte resultado é uma coleção de várias propriedades de comutadores válidas em qualquer grupo. Propriedades estas que podem ser verificadas manualmente. Lembramos que um subgrupo H de um grupo G é dito ser característico em G, o que denotamos por H *char* G, se para todo automorfismo φ de G, $H^{\varphi} \subseteq H$.

Teorema 1.14. *Sejam G um grupo e $x,y,z \in G$.*

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

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

(iii) $[xy,z] = [x,z]^y[y,z]$ *e* $[x,yz] = [x,z][x,y]^z$;

(iv) $[x^{-1},y] = [y,x]^{x^{-1}}$ *e* $[x,y^{-1}] = [y,x]^{y^{-1}}$;

(v) $[x,y,z]^{y^{-1}}[y,z,x]^{z^{-1}}[z,x,y]^{x^{-1}} = 1$ *(Identidade de Hall–Witt);*

(vi) Se $H,K \leq G$, então $[H,K] \trianglelefteq \langle H,K\rangle$ e $[H,K] = [K,H]$;

(vii) Se H,K,L são subgrupos normais de G, então [HK,L]=[H,L][K,L];

(ix) Para todo grupo G_1 e homomorfismo $\varphi : G \longrightarrow G_1$, vale $([x,y])^{\varphi} = [x^{\varphi},y^{\varphi}]$. Em particular, $G'charG$.

Sejam G um grupo e $X_1,\ldots,X_n \subseteq G$. Definimos indutivamente $[X_1] = X_1$ e

$$[X_1,\ldots,X_{n-1},X_n] = [[X_1,\ldots,X_{n-1}],X_n].$$

O seguinte resultado é conhecido como Lema dos Três Subgrupos, sua prova pode ser encontrada em [4, pág. 19, Teorema 2.3].

Lema 1.15. *Sejam H,K,L subgrupos de um grupo G e $N \trianglelefteq G$. Então se $[H,K,L],[K,L,H] \leq N$, temos que $[L,H,K] \leq N$.*

Por uma série de um grupo G entendemos uma cadeia de subgrupos

$$1 = K_0 \leq K_1 \leq \cdots \leq K_n = G.$$

A série é chamada normal se $K_i \trianglelefteq G$ para todo $i = 0,\ldots,n$. Neste último caso, cada grupo K_{i+1}/K_i é chamado um fator da série.

Uma série de subgrupos normais $1 = K_0 \leq K_1 \leq \cdots \leq K_n = G$ de um grupo G é chamada central se $K_{i+1}/K_i \leq Z(G/K_i)$ para todo $i = 0,\ldots,n-1$.

Lema 1.16. *Sejam G um grupo e $H,K \trianglelefteq G$ com $H \leq K$. Então $K/H \leq Z(G/H)$ se, e somente se, $[G,K] \leq H$.*

Lembramos que um grupo G é chamado nilpotente se possui uma série central. Note que, por definição, todo grupo abeliano é nilpotente, nesse sentido, nilpotência pode ser observada como uma generalização de abelianidade.

O seguinte resultado determina algumas propriedades básicas de grupos nilpotentes, sua prova pode ser encontrada em [26, pág. 213, Teorema 10.6].

Teorema 1.17. *Se G é um grupo nilpotente, então todos subgrupos e grupos quocientes de G são nilpotentes. Se G e Q são grupos nilpotentes, então $G \times Q$ é grupo nilpotente. Finalmente, para cada primo p e p–grupo finito G, G é nilpotente.*

Definição 1.18. Seja G um grupo. Defina $\gamma_1(G) = G$ e para todo $n > 1$, defina indutivamente $\gamma_n(G) = [\gamma_{n-1}(G), G]$. Ainda, defina $Z_0(G) = 1$ e para todo $n \geqslant 0$ defina indutivamente $Z_{n+1}(G)$ pela regra $Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G))$. As cadeias de subgrupos $G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \cdots$ e $1 = Z_0(G) \leq Z_1(G) \leq \cdots$ são chamadas, respectivamente, de série central inferior e série central superior do grupo G.

Lema 1.19. *Sejam G um grupo e $G = K_1 \geq K_2 \geq \cdots \geq K_n \geq \cdots$ uma cadeia de subgrupos normais de G com a propriedade de que $[K_n, G] \leq K_{n+1}$ para todo $i \geqslant 1$. Então, $\gamma_n(G) \leq K_n$ para todo $n \geqslant 1$.*

Demonstração. Argumentamos por indução em n, com resultado claro se $n = 1$. Se $n > 1$ e $\gamma_{n-1}(G) \leq K_{n-1}$, então temos que $\gamma_n(G) = [\gamma_{n-1}(G), G] \leq [K_{n-1}, G] \leq K_n$. □

O Lema 1.19 mostra que se G é um grupo nilpotente, a série central inferior de G é uma série central de G de menor comprimento. Neste caso, o menor n tal que $\gamma_{n+1}(G) = 1$ é chamado a classe de nilpotência de G.

Teorema 1.20. *Sejam G um grupo e $\gamma_n(G)$ o n–ésimo termo da série central inferior de G. Vale as seguintes:*

(i) Para todos inteiros positivos n, m temos que $[\gamma_n(G), \gamma_m(G)] \leq \gamma_{n+m}(G)$;

(ii) $\gamma_n(G)$ contém todos os comutadores em G de peso $\geqslant n$;

(iii) $\gamma_n(G) = \langle [g_1, \ldots, g_n];\ g_1, \ldots, g_n \in G \rangle$.

Demonstração. Argumentamos por indução em m para provar o item (i). Se $m = 1$, veja que $[\gamma_n(G), \gamma_1(G)] = [\gamma_n(G), G] = \gamma_{n+1}(G)$. Podemos, portanto, supor $m > 1$ e que o resultado vale para $m - 1$. Assim, temos que $[G, \gamma_n(G), \gamma_{m-1}(G)] = [\gamma_{n+1}(G), \gamma_{m-1}(G)] \leq \gamma_{n+m}(G)$ e $[\gamma_n(G), \gamma_{m-1}(G), G] \leq [\gamma_{n+m-1}(G), G] = \gamma_{n+m}(G)$.

Pelo Lema 1.15 temos que

$$[\gamma_n(G),\gamma_m(G)] = [\gamma_n(G),[\gamma_{m-1}(G),G]] = [[\gamma_{m-1}(G),G],\gamma_n(G)] \leq \gamma_{n+m}(G)$$

e o item (i) está verificado.

Para provar o item (ii), argumentamos por indução em n. Se $n = 1$ o resultado é imediato. Se $n > 1$ e c é comutador em G de peso maior ou igual a n, podemos escrever $c = [c_1, c_2]$ onde c_1 e c_2 são comutadores de peso r_1, r_2, respectivamente, e $r_1 + r_2 \geqslant n$. Por indução, temos que $c_1 \in \gamma_{r_1}(G)$ e $c_2 \in \gamma_{r_2}(G)$. Pelo item (i), temos que $c = [c_1, c_2] \in [\gamma_{r_1}(G), \gamma_{r_2}(G)] \leq \gamma_{r_1+r_2}(G) \leq \gamma_n(G)$. Isto prova o item (ii).

Para todo inteiro positivo n , defina $K_n = \langle [g_1,\ldots,g_n]; g_i \in G\rangle$. Dado que para todos $g_1,\ldots,g_n,g \in G$ vale que $[g_1,\ldots,g_n]^g = [g_1^g,\ldots,g_n^g]$, $K_n \trianglelefteq G$ e, pelo item (ii), $K_n \leq \gamma_n(G)$. Provamos a inclusão contrária por indução em n. O caso $n = 1$ é óbvio. Se $n > 1$, por hipótese de indução, temos que $\gamma_{n-1}(G) \leq K_{n-1}$. Para cada $g_1,\ldots,g_n \in G$, note que $[g_1,\ldots,g_{n-1}]g_n = g_n[g_1,\ldots,g_{n-1}][[g_1,\ldots,g_{n-1}],g_n]$, isso é, $[g_1,\ldots,g_{n-1}]g_nK_n = g_n[g_1,\ldots,g_{n-1}]K_n$. Isso mostra que $K_{n-1}/K_n \leq Z(G/K_n)$. Lema 1.16 estabelece que $[G,K_{n-1}] \leq K_n$ e então $\gamma_n(G) = [\gamma_{n-1}(G),G] \leq [K_{n-1},G] \leq K_n$. O item (iii) está verificado. □

O seguinte resultado verifica que no caso de grupos nilpotentes, as séries centrais inferior e superior têm o mesmo comprimento. Sua prova pode ser encontrada em [26, pág. 211, Teorema 10.4]

Teorema 1.21. *Seja G um grupo arbitrário. Se $Z_n(G) = G$, então $\gamma_{n+1}(G) = 1$ e*

$$\gamma_{r+1}(G) \leq Z_{s-r}(G)$$

para todo $r = 0,\ldots,n$. Reciprocamente, se $\gamma_{n+1}(G) = 1$, então $Z_n(G) = G$ e a igualdade acima ainda vale.

O resultado anterior mostra que se um grupo G é nilpotente, então existe n tal que $Z_n(G) = G$. Portanto, se um grupo G é não trivial e $Z(G)$ é trivial, então G não é nilpotente. Em particular, o grupo $D_3 = \langle r,s;\ r^3 = s^2 = 1,\ sr = r^2s\rangle$ é não nilpotente, dado que possui centro trivial.

O seguinte resultado estabelece condições equivalentes para que um grupo finito G seja nilpotente, sua prova pode ser encontrada em [26, pág. 216, Teorema 10.9].

Teorema 1.22. *Para todo grupo finito G, são equivalentes:*

(i) G possui uma série central;

(ii) Existe $n \geqslant 0$ de modo que $\gamma_{n+1}(G) = 1$;

(iii) *Existe $n \geqslant 0$ de modo que $Z_n(G) = G$;*

(iv) *Se $H < G$, então $H < N_G(H)$;*

(v) *Todo subgrupo maximal de G é normal em G;*

(vi) *Todos os subgrupos de Sylow de G são normais em G;*

(vii) *G é produto direto de seus subgrupos de Sylow;*

(viii) *Se $g,h \in G$ são quaisquer elementos de ordens coprimas, então g e h comutam.*

Dado um grupo G, a intersecção de todos os subgrupos maximais de G é chamado o subgrupo de Frattini de G, denotado por $\Phi(G)$. No caso em que G não possui subgrupos maximais, definimos $\Phi(G) = G$. De qualquer modo, vemos que $\Phi(G)$ é subgrupo característico de G.

Teorema 1.23. *Seja G um grupo finito. Então $\Phi(G)$ é nilpotente.*

Demonstração. Seja H um subgrupo arbitrário de G. Se $H < G$, então existe K um subgrupo maximal de G contendo H. Por definição, $\Phi(G) \leq K$ e daí $H\Phi(G) \leq K < G$. Em outras palavras, se H é subgrupo de G tal que $G = H\Phi(G)$, então $H = G$. Seja P um subgrupo de Sylow de $\Phi(G)$. Pelo Corolário 1.6 do Argumento de Frattini, temos que $G = N_G(P)\Phi(G)$ e portanto $N_G(P) = G$, isso é, $P \trianglelefteq G$. Em particular $P \trianglelefteq \Phi(G)$ e o resultado segue do Teorema 1.22. □

O seguinte teorema mostra que $\Phi(G)$ é muito útil para concluir nilpotência em G quando G é grupo finito. Sua prova pode ser encontrada em [26, pág. 219, Teoremas 10.16 e 10.17].

Teorema 1.24. *Seja G um grupo finito. Então G é nilpotente se, e somente se, $G/\Phi(G)$ é nilpotente. Ainda, G é nilpotente se, e somente se, $G' \leq \Phi(G)$.*

Teorema 1.25. *Seja G um grupo finito e $\varphi \in Aut(G)$ um automorfismo de ordem coprima com $|G|$. Se o automorfismo induzido por φ em $G/\Phi(G)$ é trivial, então $\varphi = 1$.*

Demonstração. Pelo Teorema 1.11, temos que $G/\Phi(G) = C_{G/\Phi(G)}(\varphi) = C_G(\varphi)\Phi(G)/\Phi(G)$. Isso é, $G = C_G(\varphi)\Phi(G)$. Pela prova do Teorema 1.23, vemos que $C_G(\varphi) = G$, logo $\varphi = 1$. □

Um p–grupo G é chamado abeliano elementar se G é abeliano e $|g| = p$ para todo elemento não trivial $g \in G$. Seja G um p–grupo abeliano elementar. Definindo $g + h := gh$ e $\alpha g := g^\alpha$, onde $g,h \in G$ e $\alpha \in \mathbb{F}_p$, vemos que G pode ser observado como espaço vetorial sobre o corpo finito com p elementos $\mathbb{F}_p$.

O seguinte resultado é conhecido como Teorema de Bases de Burnside. Uma prova pode ser encontrada em [25, pág. 140, 5.3.2]. A seguir G^p é o subgrupo gerado pelas p–ésimas potências do grupo G, ou seja, $G^p = \langle g^p;\ g \in G \rangle$.

Teorema 1.26 (de Bases de Burnside)**.** *Seja G um p–grupo finito. Então $\Phi(G) = G'G^p$ e $\Phi(G)$ é o menor subgrupo normal de G cujo quociente é um p–grupo abeliano elementar. Ainda, se $[G : \Phi(G)] = p^r$, todo conjunto de geradores de G possui um subconjunto de r elementos que também gera G.*

Se G é um grupo arbitrário e $H, K \trianglelefteq G$ são subgrupos nilpotentes, é natural se perguntar se HK é nilpotente. Isto é estabelecido no próximo resultado.

Teorema 1.27 (H. Fitting)**.** *Sejam G um grupo arbitrário e H, K dois subgrupos normais nilpotentes de G, de classes r e s, respectivamente. Então HK é nilpotente de classe no máximo $r+s$.*

Demonstração. Basta-nos mostrar que $\gamma_{r+s+1}(HK) = 1$. Pelo Teorema 1.14, temos que $\gamma_2(HK) = [HK, HK] = [H,H][H,K][K,H][K,K]$. Indutivamente, vemos que $\gamma_n(HK)$ é produto de subgrupos da forma $[H_1, \ldots, H_n]$ onde $H_i \in \{H, K\}$ para todo $i = 1, \ldots, n$. Tomando $n = r+s+1$, em todo subgrupo da forma $[H_1, \ldots, H_n]$, onde $H_i \in \{H, K\}$, H ocorre pelo menos $r+1$ vezes ou K ocorre pelo menos $s+1$ vezes. Logo, $\gamma_{r+s+1}(HK) \leq \gamma_{r+1}(H)\gamma_{s+1}(K) = 1$. □

O Teorema 1.27 mostra que em todo grupo finito G o produto de todos os subgrupos normais nilpotentes é, ainda, um subgrupo normal nilpotente de G, denotado por $F(G)$, chamado o subgrupo de Fitting de G, em homenagem a H. Fitting. Claramente, $F(G)$ é subgrupo característico de G.

Sejam G um grupo finito e p um primo. Se $P_1, \ldots, P_n$ são todos os p–subgrupos de Sylow de G, definimos $O_p(G) = \cap_{i=1}^n P_i$. O subgrupo $O_p(G)$ é um subgrupo característico de G, chamado o p–radical de G. Observamos que $O_p(G)$ é um p–subgrupo normal de G e contém todos os p–subgrupos normais de G.

Teorema 1.28. *Sejam G um grupo finito e $p_1, \ldots, p_n$ todos os primos distintos dividindo a ordem de G. Então*

$$F(G) = \prod_{i=1}^{n} O_{p_i}(G).$$

Demonstração. Seja $N = \prod_{i=1}^{n} O_{p_i}(G)$. Então pelos Teoremas 1.17 e 1.27 temos que N é subgrupo normal nilpotente de G. Portanto, $N \leq F(G)$. Reciprocamente, como $F(G)$ é nilpotente,

pelo Teorema 1.22 temos que $F(G)$ é produto direto de seus subgrupos de Sylow os quais, sendo característicos em $F(G)$, são característicos em G. Em particular, se P é um p–subgrupo de Sylow de $F(G)$, então $P \trianglelefteq G$ e $P \leq O_p(G)$. Isto mostra que $F(G) \leq N$. □

1.3 Grupos solúveis

Um grupo G é chamado solúvel se possui uma série normal $1 = N_0 \leq N_1 \leq \cdots \leq N_k = G$ da qual todo fator é um grupo abeliano. Uma tal série é chamada uma série solúvel para G. Note que imediatamente da definição concluímos que todos os grupos nilpotentes são solúveis. Neste sentido, solubilidade pode ser entendida como uma generalização de nilpotência.

Decorre da definição que se G é um grupo solúvel, então todo subgrupo e grupo quociente de G é, também, solúvel. Um fato ainda trivial é que se um grupo G possui um subgrupo normal K tal que ambos K e G/K são solúveis, então G é solúvel. Isto estabelece uma diferença entre a classe dos grupos nilpotentes e a classe dos grupos solúveis. Considere $D_3 = \langle r, s;\ r^3 = s^2 = 1 \text{ e } sr = r^2 s\rangle$. Então, $1 < \langle r\rangle < D_3$ é série solúvel de D_3, isso é, D_3 é grupo solúvel não-nilpotente.

Lema 1.29. *Seja G um grupo finito solúvel não trivial. Existe um subgrupo normal K de G tal que $[G : K]$ é um número primo.*

O seguinte resultado, obtido por W. Feit e J.G. Thompson em [2], é possivelmente um dos maiores resultados da Teoria de Grupos Finitos Solúveis.

Teorema 1.30. *Seja G um grupo finito de ordem ímpar. Então G é solúvel.*

Lema 1.31. *([26, pág. 235, Teorema 11.1]) Seja G um grupo finito solúvel e K um subgrupo normal minimal de G. Então, K é um p–grupo abeliano elementar para algum primo p.*

Seja G um grupo arbitrário. Definimos os subgrupos $G^{(n)}$ de G indutivamente pelas regras $G^{(0)} = G$ e para todo $n \geqslant 1$, $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$. Note que $G^{(1)} = G' = \gamma_2(G)$ é o subgrupo derivado de G. Por isto, para todo $n \geqslant 0$, $G^{(n)}$ é chamado o n–ésimo subgrupo derivado de G.

Se G é qualquer grupo e $N \trianglelefteq G$, sabemos que G/N é abeliano se, e somente se, $G' \leq N$. Indução em n mostra que para toda cadeia $G = K_0 \geq K_1 \geq \cdots \geq K_n \geq \cdots$ da qual cada grupo K_n/K_{n+1} é abeliano, vale que $G^{(n)} \leq K_n$, para todo $n \geqslant 0$. Em particular, G é solúvel se, e somente se, $G^{(n)} = 1$ para algum $n \geqslant 0$. Assim, se G é solúvel, podemos definir o comprimento derivado $d(G)$ como sendo o menor inteiro não negativo n tal que $G^{(n)} = 1$.

Definição 1.32. Seja G um grupo arbitrário. Uma série $1 = K_0 \leq \cdots \leq K_n = G$ de subgrupos normais de G é chamada uma série de Fitting se, para todo $i = 0, \ldots, n-1$, K_{i+1}/K_i é um grupo nilpotente.

Note que, desde que grupos abelianos são nilpotentes, grupos solúveis possuem séries de Fitting.

Definição 1.33. Seja G um grupo solúvel. O menor inteiro não negativo n tal que G possui uma série de Fitting $1 = K_0 \leq \cdots \leq K_n = G$ é chamado a altura de Fitting de G e é denotado por $h(G)$.

Lema 1.34. *Sejam G um grupo solúvel, $H \leq G$ e $K \trianglelefteq G$. Então, $h(H), h(G/K) \leqslant h(G)$.*

Demonstração. Seja $1 = K_0 \leq \cdots \leq K_n = G$ uma série de Fitting de G. Então $1 = (K_0 \cap H) \leq \cdots \leq (K_n \cap H) = H$ e $1 = K_0K/K \leq \cdots \leq K_nK/K = G/K$ são séries de Fitting de H e G/K. De fato, para todo $i = 0, \ldots, n-1$ vale que $(K_{i+1} \cap H)/(K_i \cap H) = (K_{i+1} \cap H)/(K_{i+1} \cap H) \cap K_i \cong (K_{i+1} \cap H)K_i/K_i \leq K_{i+1}/K_i$ é nilpotente. Ainda, para cada $i = 0, \ldots, n-1$, seja $\varphi_i : K_{i+1} \longrightarrow K_{i+1}K/K_iK$ definida por $g \mapsto gK_iK$ para todo $g \in K_{i+1}$. Então, φ_i é homomorfismo sobrejetor de núcleo $K_i(K_{i+1} \cap K)$. Logo, $K_{i+1}/K_i(K_{i+1} \cap K) \cong K_{i+1}K/K_iK$. Segue-se que

$$\begin{aligned}(K_{i+1}K/K)/(K_iK/K) &\cong K_{i+1}K/K_iK \cong K_{i+1}/K_i(K_{i+1} \cap K) \\ &\cong (K_{i+1}/K_i)/(K_i(K_{i+1} \cap K)/K_i)\end{aligned}$$

é nilpotente, para todo $i = 0, \ldots, n-1$. □

Lema 1.35. *Sejam G e H dois grupos solúveis. Então $h(G \times H) = max\{h(G), h(H)\}$.*

Demonstração. Sejam $r = h(G)$ e $s = h(H)$. Então, sejam $1 = K_0 \leq K_1 \leq \cdots \leq K_r = G$ e $1 = H_0 \leq H_1 \leq \cdots \leq H_s = H$ séries de Fitting de G e H, respectivamente. Suponha sem perda de generalidade que $r \geqslant s$. Temos que

$$1 = (K_0 \times H_0) \leq K_1 \times H_0 \leq \cdots \leq K_{r-s} \times H_0 \leq K_{r-s+1} \times H_1 \leq \cdots \leq K_r \times H_s = G \times H$$

é série de Fitting de $G \times H$ desde que para quaisquer grupos A, B e subgrupos normais $C \trianglelefteq A$ e $D \trianglelefteq B$ vale que $(C \times D) \trianglelefteq (A \times B)$ e $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$. Deste modo, temos que $h(G \times H) \leqslant r = max\{h(G), h(H)\}$. Por outro lado, $G \cong G \times 1 \leq G \times H$ e, portanto, pelo Lema 1.34, temos que $r = h(G) \leqslant h(G \times H)$. O resultado está demonstrado. □

Seja G um grupo finito solúvel. Definimos o n–ésimo subgrupo de Fitting de G indutivamente pelas regras $F_0(G) = 1$ e para todo $n \geqslant 0$, $F_{n+1}(G)/F_n(G) = F(G/F_n(G))$. A cadeia $1 = F_0(G) \leq F_1(G) = F(G) \leq \cdots \leq F_k(G) \leq \cdots$ é formada por subgrupos característicos em G da qual todo fator é um grupo finito nilpotente, chamada a série de Fitting superior de G.

Lema 1.36. *Seja G um grupo finito solúvel. Então $h(G)$ é o menor n tal que $F_n(G) = G$. Se $G \neq 1$, então $h(G) = h(G/F(G)) + 1$.*

Demonstração. Seja $1 = K_0 \leq K_1 \leq \cdots \leq K_n = G$ uma série de Fitting de G. Afirmamos que $K_i \leq F_i(G)$ para todo $i = 0, \ldots, n$. De fato, o resultado é claro para $i = 0$. Se $i \geqslant 1$ suponha que nossa afirmação está demonstrada para $i-1$. Então, $K_{i-1} \leq F_{i-1}(G)$ e, portanto, temos que $(K_i/K_{i-1})/(K_i \cap F_{i-1}(G)/K_{i-1}) \cong K_i/(K_i \cap F_{i-1}(G))$. Desde que K_i/K_{i-1} é grupo nilpotente, temos que $K_iF_{i-1}(G)/F_{i-1}(G) \cong K_i/(K_i \cap F_{i-1}(G))$ é subgrupo normal nilpotente de $G/F_{i-1}(G)$. Logo, temos que $K_iF_{i-1}(G)/F_{i-1}(G) \leq F(G/F_{i-1}(G))$, isso é, $K_i \leq F_i(G)$. Nossa afirmação está verificada. Finalmente, se $h(G) = n$, as considerações anteriores mostram que $F_n(G) = G$. Como $F_k(G) = G$ para $k < n$ contraria a minimalidade da escolha de n, temos que $h(G)$ é o menor n tal que $F_n(G) = G$.

Supondo que $G \neq 1$, então $h(G) \geqslant 1$. Seja $n = h(G/F(G))$. Se $h(G) \leqslant n$, tomemos uma série de Fitting $1 = K_0 \leq K_1 \leq \cdots \leq K_n = G$ de G. Então, desde que $K_1 \leq F(G)$, $1 \leq K_2F(G)/F(G) \leq \cdots \leq K_nF(G)/F(G) = G/F(G)$ é uma série de Fitting de $G/F(G)$. Logo, $h(G/F(G)) \leqslant n-1$, uma contradição. □

No que segue, terminaremos nossa seção de grupos solúveis generalizando-se a própria noção de solubilidade e considerando alguns resultados obtidos por P. Hall e G. Higman em [7]. A partir de agora, nesta seção, seja $\pi \subseteq \mathbb{P}$ onde $\mathbb{P}$ denota o conjunto dos números primos. Definimos $\pi' = \mathbb{P} \setminus \pi$.

Um grupo finito G é chamado π–grupo se π contém o conjunto dos primos dividindo a ordem de G (note que esta definição é equivalente à de p–grupos finitos no caso em que $\pi = \{p\}$, p um primo). Definimos $\pi(G) := \{p \in \mathbb{P};\ p \text{ divide } |G|\}$ e $\pi(g) = \pi(\langle g \rangle)$ para todo $g \in G$.

Definição 1.37. Um grupo G é chamado π–separável se G possui uma série de subgrupos normais $1 = K_0 \leq K_1 \leq \cdots \leq K_n = G$ da qual todo fator é π–grupo ou π'–grupo. No caso em que cada π–fator é solúvel, dizemos que G é π–solúvel.

Note que subgrupos, grupos quocientes e produtos diretos finitos de grupos finitos π–separáveis são, ainda, π–separáveis. Um caso de particular interesse é quando $\pi = \{p\}$ onde p é um número primo. Neste caso, um grupo π–separável é chamado p–separável e um grupo π–solúvel é chamado p–solúvel. Contudo, desde que p–grupos finitos são nilpotentes, logo solúveis, temos que as noções de p–separabilidade e p–solubilidade são equivalentes.

Seja G um grupo finito solúvel. Então, podemos tomar $1 = F_0(G) \leq F(G) \leq \cdots \leq F_h(G) = G$ a série de Fitting superior de G. Todo fator desta série é nilpotente, logo produto direto de seus subgrupos de Sylow. Portanto, utilizando o Teorema da Correspondência, podemos refinar a série de Fitting superior de G à forma $1 = K_0 \leq K_1 \leq \cdots \leq K_n = G$ onde K_{i+1}/K_i é p–grupo para algum primo p, para todo $i = 0, \ldots, n-1$. Em resumo, grupos finitos solúveis

são π–solúveis. A recíproca é também válida: Um grupo G finito é solúvel se for π–solúvel para qualquer conjunto de primos π.

Sejam G um grupo finito e H e K dois π–subgrupos normais do grupo G. Então, dado que $|HK|$ divide $|H||K|$, HK é π–subgrupo normal de G. Consequentemente, o produto de todos os π–subgrupos normais de G, denotado por $O_\pi(G)$, é o maior π–subgrupo normal de G e, por isso, $O_\pi(G)charG$. Analogamente obtém-se $O_{\pi'}(G)$, o maior π'–subgrupo normal de G.

Sendo $\pi_1,\ldots,\pi_n,\ldots$ uma sequência de conjuntos de primos, definimos indutivamente $O_{\pi_1,\ldots,\pi_n}(G)$ pela regra $O_{\pi_1,\ldots,\pi_n}(G)/O_{\pi_1,\ldots,\pi_{n-1}}(G) = O_{\pi_n}(G/O_{\pi_1,\ldots,\pi_{n-1}}(G))$, para todo $n \geqslant 2$. No caso particular em que $\pi_{2n-1} = \pi'$ e $\pi_{2n} = \pi$, para todo $n \geqslant 1$, chegamos à série $1 \leq O_{\pi'}(G) \leq O_{\pi',\pi}(G) \leq O_{\pi',\pi,\pi'}(G) \leq \cdots$, chamada a π–série superior de G. No caso ainda mais particular em que $\pi = \{p\}$, p um primo, obtemos a série $1 \leq O_{p'}(G) \leq O_{p',p}(G) \leq O_{p',p,p'}(G) \leq \cdots$ chamada a p–série superior de G.

Seja G um grupo finito π–separável. Então, G possui uma série de subgrupos normais $1 = K_0 \leq K_1 \leq \ldots \leq K_n = G$ da qual todo fator é π–grupo ou π'–grupo. Suponha sem perda de generalidade que K_1 é π'–grupo e que K_i/K_{i-1} é π'-grupo se, e somente se, K_{i+1}/K_i é π–grupo para todo $i \geqslant 1$. Por simplicidade, permita-nos escrever H_n para denotar o n–ésimo termo da π–série superior de G. Afirmamos que $K_{2n-1} \leq H_{2n-1}$ e $K_{2n} \leq H_{2n}$ para todo $n \geqslant 1$. Provamos isto por indução. Desde que K_1 é π'–subgrupo normal de G, temos que $K_1 \leq H_1 = O_{\pi'}(G)$. Suponha, então, que $n \geqslant 1$ e $K_{2n-1} \leq H_{2n-1}$. Temos que K_{2n}/K_{2n-1} é π–grupo e portanto, $K_{2n}H_{2n-1}/H_{2n-1} \cong K_{2n}/(K_{2n} \cap H_{2n-1})$ é π–subgrupo normal de G/H_{2n-1}. Isso mostra que $(K_{2n}H_{2n-1})/H_{2n-1} \leq O_\pi(G/H_{2n-1}) = H_{2n}/H_{2n-1}$, isso é $K_{2n} \leq H_{2n}$. Analogamente, como K_{2n+1}/K_{2n} é π'–grupo, temos que $K_{2n+1}H_{2n}/H_{2n} \cong K_{2n+1}/(K_{2n+1} \cap H_{2n})$ é π'–subgrupo normal de G/H_{2n}. Segue-se que $K_{2n+1} \leq H_{2n+1}$. Nossa afirmação está verificada. Um resultado análogo pode ser obtido supondo que K_1 é π–grupo.

O último parágrafo estabelece que a π–série superior do grupo finito π–separável G sempre alcança o grupo G e é a série com menor número de π–fatores, este número é chamado o π–comprimento de G, denotado por $l_\pi(G)$. No caso em que $\pi = \{p\}$, p um primo, denotamos $l_\pi(G) = l_p(G)$ e o chamamos de p–comprimento de G. Análogo aos resultados considerados anteriormente sobre altura de Fitting, expomos a seguir resultados básicos sobre o p–comprimento de grupos finitos p–solúveis. A prova pode ser encontrada em [11, pág. 689, Lema 6.4].

Lema 1.38. *Sejam G e Q dois grupos finitos p–solúveis, p um número primo. Sejam $H \leq G$ e $K \trianglelefteq G$. Valem as seguintes:*

(i) $l_p(G/K), l_p(H) \leqslant l_p(G)$;

(ii) $l_p(G \times Q) = max\{l_p(G), l_p(Q)\}$.

No que segue, estabelecemos alguns dos principais resultados que serão utilizados nesta dissertação para estabelecer limite no p–comprimento de grupos finitos p–solúveis.

Teorema 1.39. *Seja G um grupo finito π–separável. Então*

$$C_{G/O_{\pi'}(G)}(O_{\pi',\pi}(G)/O_{\pi'}(G)) \leq O_{\pi',\pi}(G)/O_{\pi'}(G).$$

Demonstração. Suponha inicialmente que $O_{\pi'}(G) = 1$. Seja $C = C_G(O_\pi(G))$ e assim defina $B = C \cap O_\pi(G)$. Desde que $O_\pi(G)$ é característico em G, também o são ambos B e C. Desejamos mostrar que $B = C$. Suponha por absurdo que $B < C$. Então C/B é grupo finito π–separável não trivial e podemos tomar subgrupo característico K/B não trivial que é π–grupo ou π'–grupo. Por um lado, temos que $B \leq O_\pi(G)$ e portanto B é π–subgrupo de G. Por outro lado, temos que K/B é característico em C/B, que por sua vez é normal em G/B. Segue-se que $K/B \trianglelefteq G/B$, isso é, $K \trianglelefteq G$. Ora, se K/B é π–grupo, temos que K é π–grupo. Como K é normal em G, temos que $K \leq O_\pi(G)$ e, então, $K \leq C \cap O_\pi(G) = B$, uma contradição. Podemos, então, supor que K/B é π'–grupo. Pelo Teorema 1.9, existe $H \leq K$ tal que $K = H \rtimes B$. Ora, desde que $B \leq O_\pi(G)$, temos que $H \leq K \leq C \leq C_G(B)$, isso é, $H \trianglelefteq K$. Finalmente, H sendo π'–subgrupo normal de K, H é característico em K e normal em G. Isso mostra que $H \leq O_{\pi'}(G) = 1$ e $K = B$, uma nova contradição. Estas considerações estabelecem o caso particular em que $O_{\pi'}(G) = 1$.

Podemos, então, supor que G é qualquer grupo finito π–separável. Então, $G/O_{\pi'}(G)$ é π–separável e $O_{\pi'}(G/O_{\pi'}(G)) = 1$. O último parágrafo estabelece o resultado desejado. □

Sejam p um primo e G um grupo finito. Sabemos que $O_{p'}(G)$ e $O_{p',p}(G)$ são subgrupos característicos de G. Portanto, definindo $A \leq G$ pela regra $A/O_{p'}(G) = \Phi(O_{p',p}(G)/O_{p'}(G))$, temos que A é, também, um subgrupo característico de G. Concluímos então que G age no grupo $O_{p',p}(G)/A$ e podemos considerar $C_G(O_{p',p}(G)/A)$, o núcleo desta ação.

Teorema 1.40. *Sejam p um primo e G um grupo finito p–solúvel. Seja $A \leq G$ definido por $A/O_{p'}(G) = \Phi(O_{p',p}(G)/O_{p'}(G))$. Então,*

$$C_G(O_{p',p}(G)/A) = O_{p',p}(G).$$

Demonstração. Suponha inicialmente que $O_{p'}(G) = 1$. Assim, $A = \Phi(O_p(G))$. Pelo Teorema 1.26, $O_p(G)/A$ é um p–grupo abeliano elementar, logo, $O_p(G) \leq C_G(O_p(G)/A)$. Suponha que $O_p(G) < C = C_G(O_p(G)/A)$. Dado que $C \trianglelefteq G$, temos que C não é p–subgrupo de G e podemos tomar elemento $c \in C \setminus O_p(G)$ de ordem coprima com p. O automorfismo $\alpha : O_p(G) \longrightarrow O_p(G)$ dado por $x \mapsto x^c = c^{-1}xc$ tem ordem coprima com p e induz um automorfismo trivial em $O_p(G)/A$. Pelo Teorema 1.25 temos que $\alpha = 1$ e portanto $c \in C_G(O_p(G))$. Mas, pelo Teorema

1.39, $C_G(O_p(G)) \leq O_p(G)$ desde que G é p–solúvel e $O_{p'}(G) = 1$. Segue-se que $c = 1$, uma contradição.

Podemos assumir finalmente que G é qualquer grupo finito p–solúvel. Então $G/O_{p'}(G)$ é grupo finito p–solúvel tal que $O_{p'}(G/O_{p'}(G)) = 1$. Seja $A/O_{p'}(G) = \Phi(O_p(G/O_{p'}(G)) = \Phi(O_{p',p}(G)/O_{p'}(G))$. Pelas considerações anteriores temos que

$$C_{G/O_{p'}(G)}(O_{p',p}(G)/A) = O_{p',p}(G)/O_{p'}(G)$$

o que, por sua vez, resulta em $C_G(O_{p',p}(G)/A) = O_{p',p}(G)$. □

Seja G um grupo finito p–solúvel, p um primo. Pelo Teorema 1.40, temos que $O_{p',p}(G)$ é o núcleo da ação de G em $O_{p',p}(G)/A$. Pelo Teorema 1.26 podemos observar $V = O_{p',p}(G)/A$ como espaço vetorial sobre $\mathbb{F}_p$. Portanto, $G/O_{p',p}(G)$ é isomorfo a um grupo de automorfismos lineares de V.

Teorema 1.41. *Sejam G um grupo finito, $A, B \trianglelefteq G$ e $B \leq A$. Suponha que A/B é um p–grupo abeliano elementar, o qual observamos como espaço vetorial sobre $\mathbb{F}_p$, e seja $\rho : G \longrightarrow Aut_{\mathbb{F}_p}(A/B)$ o homomorfismo determinado pela ação de G em A/B.*

(i) Se $a \in A$ e $x_1, \ldots, x_n \in G$, então

$$(aB)(\rho(x_1) - 1) \cdots (\rho(x_n) - 1) = [a, x_1, \ldots, x_n]B.$$

(ii) Para cada $a \in A$, $x \in G$ e $n \in \mathbb{N}^*$, vale

$$x^{-n}(xa)^n B = (aB)(1 + \rho(x) + \cdots + \rho(x)^{n-1}).$$

Demonstração. Nas condições do item (i), temos que

$$(aB)(\rho(x_1) - 1) = a^{x_1}B - aB = -aB + a^{x_1}B = a^{-1}a^{x_1}B = [a, x]B.$$

Utilizando raciocínio análogo, o resultado segue por indução em n. Com respeito ao item (ii), temos que

$$\begin{aligned}(aB)(1 + \rho(x) + \cdots + \rho(x)^{n-1}) &= aB + a^x B + \cdots + a^{x^{n-1}} B = a^{x^{n-1}} B + \cdots + a^x B + aB \\ &= (x^{-n} \underbrace{xaxa \cdots xa}_{n})B = x^{-n}(xa)^n B.\end{aligned}$$

□

Capítulo 2

Álgebras de Lie

Neste capítulo, temos por objetivo estabelecer as noções principais sobre álgebras e álgebras de Lie satisfazendo identidades polinomiais que serão de maior utilidade nesta dissertação, bem como expor a construção de um anel de Lie associado a um grupo G.

2.1 Módulos e álgebras

Nesta seção nos dispomos a estabelecer as principais noções sobre álgebras e álgebras de Lie que serão utilizadas neste trabalho.

Por um anel entendemos um conjunto R munido de duas operações $+$ e $\cdot$, chamadas respectivamente de adição e multiplicação, de modo que

(i) $(R,+)$ é grupo abeliano;

(ii) Para todos $x,y,z \in R$ valem $x(y+z) = xy+xz$ e $(x+y)z = xz+yz$.

Se a multiplicação no anel R é associativa (respec., comutativa) dizemos que R é anel associativo (respec., comutativo). Ainda, se o anel R possui elemento neutro com relação à multiplicação, dizemos que R é anel unitário. Vamos assumir conhecidas as noções básicas da Teoria de Anéis, a saber, definições de subanéis, ideiais, Teoremas de Homomorfismo e Correspondência, etc.

Exemplo 2.1. Os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos clássicos de anéis associativos, comutativos e unitários. Se R é qualquer anel associativo e n é um inteiro positivo, o conjunto $M_{n\times n}(R)$ das matrizes $n \times n$ sobre R é um anel associativo com adição e multiplicação usuais de matrizes.

Exemplo 2.2. Considere $\mathbb{R}^3 = \{(x_1,x_2,x_3); x_1,x_2,x_3 \in \mathbb{R}\}$. Defina "+" em $\mathbb{R}^3$ componente-a-componente e defina $\cdot : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ como segue:

$$(x_1,x_2,x_3)\cdot(y_1,y_2,y_3) = (x_2y_3 - y_2x_3, -x_1y_3 + y_1x_3, x_1y_2 - y_1x_2).$$

Então, $(\mathbb{R}^3,+,\cdot)$ é um anel satisfazendo as seguintes condições;

- $u \cdot u = 0$ para todo $u \in \mathbb{R}^3$;
- $(u \cdot v)\cdot w + (v \cdot w)\cdot u + (w \cdot u)\cdot v = 0$ para todos $u,v,w \in \mathbb{R}^3$.

Definição 2.3. Um anel R é chamado anel de Lie se satisfaz as seguintes condições:

(i) Lei anticomutativa: $xx = 0$ para todo $x \in R$;

(ii) Identidade de Jacobi: $(xy)z + (yz)x + (zx)y = 0$ para todos $x,y,z \in R$.

O primeiro item na definição acima recebe este nome pois para cada x,y em um anel de Lie R vale $(x+y)(x+y) = xx + xy + yx + yy = xy + yx = 0$, isso é, $xy = -yx$. O segundo item recebe esse nome em homenagem ao matemático alemão C.J.J. Jacobi.

Definição 2.4. Seja R um anel associativo comutativo e com unidade. Um grupo abeliano aditivo $(M,+)$ é chamado um R–módulo à esquerda se para cada $\alpha \in R$ e $m \in M$ existe um elemento bem definido $\alpha m \in M$ de modo que para todos $\alpha,\alpha_1,\alpha_2 \in R$ e $m,m_1,m_2 \in M$ valem:

(i) $(\alpha_1 + \alpha_2)m = \alpha_1 m + \alpha_2 m$;

(ii) $\alpha(m_1 + m_2) = \alpha m_1 + \alpha m_2$;

(iii) $(\alpha_1\alpha_2)m = \alpha_1(\alpha_2 m)$;

(iv) $1m = m$.

Note-se que a definição acima de módulos é uma generalização da definição de espaços vetoriais sobre corpos. Assim, por exemplo, um submódulo do R–módulo à esquerda M é um subgrupo de M fechado com relação à multiplicação por escalar, o R–submódulo gerado por um subconjunto S de M é o menor dos R–submódulos de M contendo S e uma função $\varphi : M \longrightarrow M'$ entre os R–módulos à esquerda M e M' é chamada um homomorfismo de R–módulos se $(\alpha m_1 + m_2)^\varphi = \alpha m_1^\varphi + m_2^\varphi$ para todos $\alpha \in R$ e $m_1,m_2 \in M$.

Definição 2.5. Seja R um anel associativo comutativo e com unidade. Um R–módulo M é chamado livremente gerado pelo conjunto X se M é gerado por X e para todo módulo M' e função $f : X \longrightarrow M'$ existe um único homomorfismo de R–módulos $\varphi : M \longrightarrow M'$ tal que $\varphi|_X = f$.

Note que $\emptyset$ gera livremente o R–módulo trivial. Dado um conjunto não vazio X, podemos considerar o conjunto M das R–combinações lineares finitas formais de elementos em X. Definindo adição em M de modo natural, temos que M é R–módulo livremente gerado por X.

Definição 2.6. Seja R um anel associativo comutativo e com unidade. Sejam A,B dois R–módulos e M o R–módulo livremente gerado pelo conjunto $A \times B$. Em M, nós consideramos N, o R–submódulo gerado por todas as expressões da forma

- $\alpha(a,b) - (\alpha a, b)$, $(\alpha a, b) - (a, \alpha b)$;
- $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$, $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$,

onde $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$ e $\alpha \in R$. O R–módulo quociente $A \otimes B := M/N$ é chamado o produto tensorial de A e B. Para cada $a \in A$, $b \in B$ identificando $a \otimes b = (a,b) + N$, temos que os elementos de $A \otimes B$ são da forma $\sum_{i,j} a_i \otimes b_j$, pois os elementos $a \otimes b$ geram $A \otimes B$ e neste R–módulo vale $\alpha(a \otimes b) = (\alpha a) \otimes b = a \otimes (\alpha b)$.

Definição 2.7. Sejam R um anel associativo comutativo com unidade e A, B, C três R–módulos. Uma função $f : A \times B \longrightarrow C$ é chamada bilinear se para todos $a, a' \in A, b, b' \in B$ e $\alpha \in R$ vale $f(\alpha a + a', b) = \alpha f(a,b) + f(a',b)$ e $f(a, \alpha b + b') = \alpha f(a,b) + f(a,b')$.

Lema 2.8. *Sejam R, A, B, C como na definição anterior. Então, para toda função bilinear $f : A \times B \longrightarrow C$ existe um único homomorfismo de R–módulos $f^* : A \otimes B \longrightarrow C$ tal que $f^* \varphi = f$ onde $\varphi : A \times B \longrightarrow A \otimes B$ é a função que leva (a,b) em $a \otimes b$.*

Demonstração. Nas condições acima, sejam M e N como na Definição 2.6. Então, existe um único homomorfismo $\psi : M \longrightarrow C$ que estende a função f. A saber, ψ leva $\sum \alpha_{ab}(a,b)$ em $\sum \alpha_{ab} f(a,b)$. Desde f é bilinear, temos que $N \subseteq Ker(\psi)$ e então

$$\begin{aligned} \overline{\psi} : M/N = A \otimes B &\longrightarrow C \\ \sum \alpha_{ab}(a,b) + N &\longmapsto \sum \alpha_{ab} f(a,b) \end{aligned}$$

é um homomorfismo bem definido de R–módulos. Então note que para cada $(a,b) \in A \times B$ vale que $f(a,b) = \overline{\psi}(a \otimes b) = \overline{\psi}(\varphi(a,b)) = (\overline{\psi}\varphi)(a,b)$. O resultado segue tomando $\overline{\psi} = f^*$. □

Definição 2.9. Seja R um anel associativo comutativo e unitário. Um anel $(L, +, \cdot)$ que é ao mesmo tempo um R–módulo à esquerda é chamado uma R–álgebra, ou uma álgebra sobre R, se para todos $\alpha \in R$ e $l_1, l_2 \in L$ vale $\alpha(l_1 l_2) = (\alpha l_1) l_2 = l_1 (\alpha l_2)$.

Se $(L, +, \cdot)$ é anel associativo, dizemos que a R–álgebra L é associativa e caso $(L, +, \cdot)$ seja anel de Lie, dizemos que a álgebra é uma R–álgebra de Lie.

Exemplo 2.10. Para cada anel associativo comutativo e com unidade R e inteiro positivo n, o anel associativo $M_{n\times n}(R)$ é uma álgebra associativa e unitária sobre o anel R com multiplicação escalar usual. Ainda, o anel no Exemplo 2.2 é uma álgebra de Lie sobre o corpo dos números reais com multiplicação escalar usual.

Na Teoria de Álgebras de Lie é bastante comum o uso de colchetes para denotar a operação de multiplicação. A partir de então, adotamos esta convenção. O seguinte exemplo fornece uma vasta classe de álgebras de Lie.

Exemplo 2.11. Sejam R um anel associativo comutativo e com unidade e A uma R–álgebra associativa. Defina $[\ ,\ ]: A\times A \longrightarrow A$ por $[a,b]=ab-ba$ para todo $a,b\in A$. Então, para todos $a,b,c\in A$ vale

- $[[a,b],c]=[ab-ba,c]=abc-bac-cab+cba$;
- $[[b,c],a]=[bc-cb,a]=bca-cba-abc+acb$;
- $[[c,a],b]=[ca-ac,b]=cab-acb-bca+bac$.

Por isso segue que

$$\begin{aligned}[[a,b],c]+[[b,c],a]+[[c,a],b] &= (abc-bac-cab+cba)+(bca-cba-abc+acb)\\ &+ (cab-acb-bca+bac)=0.\end{aligned}$$

Como $[a,a]=0$ para todo $a\in A$ e as demais propriedades da definição de R–álgebra de Lie seguem do fato que $(A,+,\cdot)$ é uma R–álgebra associativa, temos que $(A,+,[\ ,\ ])$ é uma R–álgebra de Lie, chamada a álgebra de Lie associada à álgebra associativa $(A,+,\cdot)$.

Definição 2.12. Sejam R um anel associativo comutativo e unitário e L_1, L_2 duas R–álgebras. Uma aplicação $\varphi: L_1 \longrightarrow L_2$ é chamada um homomorfismo de R–álgebras se

(i) φ é homomorfismo de R–módulos;

(ii) Para todos $l,m\in L_1$ vale $(lm)^{\varphi}=l^{\varphi}m^{\varphi}$.

Definição 2.13. Sejam R um anel associativo comutativo e com unidade e L uma R–álgebra. Para cada $U,V\subseteq L$, defina

$$UV={}_{+}\langle uv; u\in U, v\in V\rangle.$$

Assim, um R–submódulo U de L é chamado uma R–subálgebra de L se $UU\subseteq U$. Ainda, U é chamado um ideal de L se $UL+LU\subseteq U$. No caso particular em que L é uma R–álgebra de Lie,

a anticomutatividade de L mostra que $[U,L] = [L,U]$ e por isso U é ideal de L se, e somente se, $[U,L] \subseteq L$. Mais do que isto, se U e V são ideais de L, segue da identidade de Jacobi que $[U,V]$ é ideal de L.

A prova do seguinte resultado pode ser encontrada em [12, pág. 324, Teorema 8.13]

Lema 2.14. *Sejam R um anel associativo comutativo unitário e L uma R–álgebra de Lie. Seja R^* um anel associativo comutativo unitário contendo R e tal que $1_R = 1_{R^*}$. Nestas condições, R^* pode ser observado como R–módulo e então podemos considerar $L^* = L \otimes_R R^*$. Defina*

(a) $[\ ,\ ] : L^* \times L^* \longrightarrow L^*, \quad \left[\sum l_i \otimes \alpha_i, \sum z_j \otimes \beta_j\right] = \sum [l_i, z_j] \otimes (\alpha_i \beta_j)$;

(b) $\cdot : R^* \times L^* \longrightarrow L^*, \quad \alpha\left(\sum l_i \otimes \alpha_i\right) = \sum l_i \otimes \alpha\alpha_i$.

Assim, valem as seguintes:

(i) *L^* com a multiplicação escalar e colchete acima definidos é uma R^*–álgebra de Lie;*

(ii) *Se φ é um automorfismo de L, a aplicação $\varphi^* : L^* \longrightarrow L^*$ definida por $\varphi^*\left(\sum l_i \otimes \alpha_i\right) = \sum l_i^{\varphi} \otimes \alpha_i$ é um automorfismo de L^*;*

(iii) *Se R^* é um R–módulo livre, para todos U e V submódulos de L, $U \otimes R^*$ é R^*–submódulo de L^*, $[U,V] \otimes R^* = [U \otimes R^*, V \otimes R^*]$ e se I é ideal de L, então $I \otimes R^*$ é ideal de L^*;*

(iv) *Dado um automorfismo φ de L, seja φ^* como definido no item (ii). Então, para todo R–submódulo U de L contendo todos os elementos invariantes por φ, $U \otimes R^*$ contém todos os elementos de L^* invariantes por φ^*.*

Dado um subconjunto X de uma R–álgebra de Lie L, podemos falar sobre o R–submódulo gerado por X, da R–subálgebra $\langle X \rangle$ de L gerada por X e do ideal $id(X)$ de L gerado por X, este último sendo o menor ideal de L contendo X.

Lema 2.15. *Seja $\emptyset \neq X$ um subconjunto da R–álgebra de Lie L. Então*

(i) $\langle X \rangle = {}_+\langle [l_1, \ldots, l_n];\ n > 0,\ l_1, \ldots, l_n \in X \rangle$;

(ii) *Assuma $L = \langle Y \rangle$. Então,*

$$id(X) = {}_+\langle [l, l_1, \ldots, l_n]; l \in X,\ n \geqslant 0,\ l_1, \ldots, l_n \in Y \rangle.$$

Demonstração. Façamos a prova de (i), a prova do item (ii) é análoga. Permita-nos definir $T = {}_+\langle [l_1, \ldots, l_n];\ n > 0,\ l_1, \ldots, l_n \in X \rangle$. Por definição, $\langle X \rangle = \cap S$ onde $X \subseteq S$ e S é subálgebra

de L. Se S é uma subálgebra de L contendo X, então, para todos $l_1,\dots,l_n \in X$ vale que $[l_1,\dots,l_n] \in S$, logo $T \subseteq S$. Por outro lado, pela identidade de Jacobi, vale que

$$[x,[y,z]] = -[y,z,x] = [x,y,z] + [z,x,y].$$

Vemos, portanto, que para todos $n,m \geqslant 1$ e elementos $l_1,\dots,l_n,y_1,\dots,y_m \in X$, o comutador $[[l_1,\dots,l_n],[y_1,\dots,y_m]]$ pode ser escrito como combinação linear de comutadores simples de peso $m+n$ com entradas em X. Então, T é uma subálgebra de L. Dado que $X \subseteq T$, temos que $\langle X \rangle \subseteq T$. Portanto, T é a menor subálgebra de L contendo X. □

Definição 2.16. Seja L uma álgebra de Lie sobre R. Defina $\gamma_1(L) = L$ e para todo $n > 1$ defina indutivamente $\gamma_n(L) = [\gamma_{n-1}(L), L]$.

Note que por indução sobre n, é possível ver que $L = \gamma_1(L) \supseteq \gamma_2(L) \supseteq \cdots \supseteq \gamma_n(L) \supseteq \cdots$ é uma série de ideais da R–álgebra de Lie L, chamada a série central inferior de L.

Teorema 2.17. *Sejam R um anel associativo comutativo e unitário e L uma álgebra de Lie sobre R. Então valem as seguintes:*

(i) $[\gamma_n(L), \gamma_m(L)] \subseteq \gamma_{n+m}(L)$ *para todos* $n,m > 0$*;*

(ii) $\gamma_n(L)$ *contém todos os comutadores de peso maior ou igual a n;*

(iii) $\gamma_n(L)$ *é gerado pelos comutadores simples de peso n.*

Demonstração. Note que se $U,V,W \subseteq L$, então $[[U,V],W] \subseteq [[V,W],U] + [[W,U,V]]$, o que decorre imediatamente de identidade de Jacobi. Provamos o item (i) por indução em m, com caso óbvio se $m = 1$. Se $m > 1$ e o resultado vale para $m-1$, temos que

$$\begin{aligned} [\gamma_n(L), \gamma_m(L)] &= [\gamma_n(L), [\gamma_{m-1}(L), L]] = [[\gamma_{m-1}(L), L], \gamma_n(L)] \\ &\subseteq [[L, \gamma_n(L)], \gamma_{m-1}(L)] + [[\gamma_n(L), \gamma_{m-1}(L)], L] \subseteq \gamma_{n+m}(L). \end{aligned}$$

O item (i) está, portanto, verificado. O item (ii) decorre imediatamente do item (i), utilizando raciocínio igual à prova do item (ii) do Teorema 1.20. Finalmente, o item (iii) decorre de uma indução em n. □

Definição 2.18. Seja L uma álgebra de Lie sobre R. L é chamada nilpotente se existe inteiro não negativo n tal que $\gamma_{n+1}(L) = 0$. Neste caso, o menor número n tal que $\gamma_{n+1}(L) = 0$ é chamado a classe de nilpotência de L. O seguinte resultado é uma consequência imediata do Teorema 2.17.

Teorema 2.19. *Seja L uma R–álgebra de Lie. São equivalentes:*

(i) $\gamma_{c+1}(L) = 0$;

(ii) *L possui uma série de ideais $L = L_1 \supseteq L_2 \supseteq \cdots \supseteq L_c \supseteq L_{c+1} = 0$ tal que $[L_i, L] \subseteq L_{i+1}$ para todo $i = 1, \ldots, c$;*

(iii) *Para todos $l_1, \ldots, l_{c+1} \in L$ vale $[l_1, \ldots, l_{c+1}] = 0$.*

Se L é uma R–álgebra de Lie, para todo ideal I de L o R–módulo quociente L/I se torna uma álgebra de Lie com o colchete definido por $[x+I, y+I] = [x,y]+I$, para todos $x, y \in L$.

Teorema 2.20. *Seja L uma R–álgebra de Lie. Então para todo ideal I de L valem:*

(i) *L/I é nilpotente de classe no máximo c se, e somente se, $\gamma_{c+1}(L) \subseteq I$;*

(ii) *L/I é nilpotente de classe no máximo c se L é nilpotente de classe no máximo c.*

Demonstração. As duas afirmações decorrem imediatamente do fato, por exemplo obtido por indução em n, que $\gamma_n(L/I) = (\gamma_n(L)+I)/I$. □

2.2 N_p–séries e o anel de Lie associado

Durante toda esta seção, p denota um primo fixado.

Definição 2.21. Uma filtração de um grupo G é uma cadeia de subgrupos $G = K_1 \geq K_2 \geq \cdots \geq K_i \geq \cdots$ tal que para todos $i, j \geqslant 1$ vale que $[K_i, K_j] \leq K_{i+j}$. Assim, uma N_p–série de G é definida como sendo uma filtração $G = K_1 \geq K_2 \geq \cdots \geq K_i \geq \cdots$ tal que para todo $i \geqslant 1$ vale $K_i^p \leq K_{pi}$.

Seja, então, G um grupo e seja $G = K_1 \geq K_2 \geq \cdots \geq K_i \geq \cdots$ uma N_p–série de G. Por definição de N_p–série, para cada $i \geqslant 1$ vale que o grupo K_i/K_{i+1} é um p–grupo abeliano elementar e, portanto, pelo Teorema 1.26, pode ser observado como espaço vetorial sobre o corpo $\mathbb{F}_p$. Vamos definir estrutura de álgebra de Lie no espaço soma $L(G) = \bigoplus_{i \geqslant 1} K_i/K_{i+1}$.

Definimos um colchete de Lie $[\ ,\ ]$ em $L(G)$ do seguinte modo: Sendo $i, j \geqslant 1$, para cada $gK_{i+1} \in K_i/K_{i+1}$ e $hK_{j+1} \in K_j/K_{j+1}$ defina

$$[gK_{i+1}, hK_{j+1}] \coloneqq [g,h]K_{i+j+1} \in K_{i+j}/K_{i+j+1}.$$

Se $gK_{i+1} = g'K_{i+1}$ e $hK_{j+1} = h'K_{j+1}$ existem $d_i \in K_{i+1}$ e $d_j \in K_{j+1}$ tais que $g = g'd_i$ e $h = h'd_j$. Disto, segue-se que

$$[gK_{i+1}, hK_{j+1}] = [g,h]K_{i+j+1} = [g'd_i, h'd_j]K_{i+j+1} = [g', h'd_j]^{d_i}[d_i, h'd_j]K_{i+j+1}.$$

Por um lado temos que

$$[d_i, h'd_j] \in [K_{i+1}, K_j] \leq K_{i+j+1}.$$

Por outro lado, $[g', d_j] \in [K_i, K_{j+1}] \leq K_{i+j+1}$, $[g', h', d_j] \in [K_i, K_j, K_{j+1}] \leq K_{i+j+1}$ e $[g', h'd_j, d_i] \in [K_i, K_j, K_i] \leq K_{i+j+1}$. Portanto, vemos que

$$\begin{aligned} [g', h'd_j]^{d_i}K_{i+j+1} &= [g', h'd_j][g', h'd_j, d_i]K_{i+j+1} \\ &= [g', d_j][g', h'][g', h', d_j][g', h'd_j, d_i]K_{i+j+1} \\ &= [g', h']K_{i+j+1}. \end{aligned}$$

Segue-se que

$$[gK_{i+1}, hK_{j+1}] = [g', h'd_j]^{d_i}[d_i, h'd_j]K_{i+j+1} = [g', h']K_{i+j+1} = [g'K_{i+1}, h'K_{j+1}].$$

Estas considerações verificam que o colchete $[\ ,\ ]$ não depende da escolha de representantes. Estendendo-o por linearidade em $L(G)$, vamos mostrar que $(L(G), +, [\ ,\ ])$ é uma álgebra de Lie sobre $\mathbb{F}_p$. Por definição de $L(G)$, já sabemos que $L(G)$ é um espaço vetorial sobre $\mathbb{F}_p$. Vamos mostrar aqui que o colchete acima definido satisfaz a identidade de Jacobi. As propriedades de bilinearidade e anticomutatividade podem ser verificadas manualmente mas suas provas serão omitidas.

Sejam $x \in K_i$, $y \in K_j$ e $z \in K_s$. Pela identidade de Hall–Witt, Teorema 1.14, temos que

$$[x,y,z]^{y^{-1}}[y,z,x]^{z^{-1}}[z,x,y]^{x^{-1}} = 1.$$

Segue-se que em $L(G)$ vale

$$\begin{aligned} &[x,y,z]^{y^{-1}}[y,z,x]^{z^{-1}}[z,x,y]^{x^{-1}}K_{i+j+s+1} = \\ &[x,y,z][x,y,z,y^{-1}][y,z,x][y,z,x,z^{-1}][z,x,y][z,x,y,x^{-1}]K_{i+j+s+1} = \\ &[x,y,z][y,z,x][z,x,y]K_{i+j+s+1} = 0. \end{aligned}$$

Isso é, em $L(G)$ vale

$$[xK_{i+1},\, yK_{j+1},\, zK_{s+1}] + [yK_{j+1},\, zK_{s+1},\, xK_{i+1}] + [zK_{s+1},\, xK_{i+1},\, yK_{j+1}] = 0.$$

Desde que $[\ ,\ ]$ foi estendido por linearidade em $L(G)$, temos que $[\ ,\ ]$ satisfaz a identidade de Jacobi em L. Pelas nossas considerações iniciais $(L(G), +, [\ ,\ ])$ é uma álgebra de Lie sobre o corpo $\mathbb{F}_p$.

As considerações anteriores mostram como a partir de um grupo G podemos construir uma álgebra de Lie sobre o corpo $\mathbb{F}_p$. O anel $L(G)$ construído a partir de uma N_p–série de G é chamado o anel de Lie de G associado à N_p–série de G.

Definição 2.22. Sejam R um anel associativo, comutativo e com unidade e L uma R–álgebra de Lie. Para cada $l \in L$, definimos $ad_l : L \longrightarrow L$ por $ad_l(z) = [z, l]$ para todos $l \in L$. Assim, um elemento $l \in L$ é chamado ad–nilpotente se existe $n \geqslant 1$ tal que $ad_l^n = 0$. Isto é, se $[z, \underbrace{l, \ldots, l}_{n}] = 0$ para todo $z \in L$.

O seguinte resultado é provado em [20, pág. 131, Corolário 6.8] por M.P. Lazard.

Teorema 2.23. *Seja G um grupo e $G = K_1 \geq \cdots \geq K_n \geq \cdots$ uma N_p–série de G. Dado $x \in K_i \setminus K_{i+1}$, seja $x^* = xK_{i+1}$. Então, $ad_{x^*}^p = ad_{(x^p)^*}$. Em particular, se x tem ordem finita, então x^* é ad–nilpotente.*

No que segue, iremos construir uma N_p–série para qualquer grupo G, chamada a série de Jennings–Lazard–Zassenhaus de G. Esta série será utilizada nos próximos capítulos e nas provas de alguns dos principais resultados deste trabalho.

Sejam G um grupo e m um inteiro positivo. Definimos $G^m = \langle g^m;\ g \in G \rangle$. Note que G^m é subgrupo característico de G e para todo $N \trianglelefteq G$ vale $(G/N)^m = G^m N/N$. Finalmente notamos que para todos inteiros positivos n, m vale $G^{mn} \leq (G^m)^n$.

Lembramos que nesta seção estamos assumindo que p é um primo fixado.

Definição 2.24. Para cada grupo G e $n \geqslant 1$ defina

$$D_n(G) = \prod_{jp^k \geqslant n} \gamma_j(G)^{p^k}.$$

Note que para cada grupo G vale $D_1(G) = G$ e $D_2(G) = G^p[G,G]$. Em particular, se G é p–grupo finito, então $D_2(G) = \Phi(G)$ onde $\Phi(G)$ denota o subgrupo de Frattini de G. Note ainda que para cada $n \geq 1$, $D_n(G)$ é um subgrupo característico de G, logo, $G = D_1(G) \geq D_2(G) \geq \cdots \geq D_n(G) \geq \cdots$ é uma cadeia de subgrupos característicos de G, chamada a série de Jennings–Lazard–Zassenhaus de G associada ao primo fixado p.

Lema 2.25. *Seja G um grupo e $N \trianglelefteq G$. Então $D_m(G/N) = D_m(G)N/N$ para todo inteiro positivo m.*

Demonstração. Pelo Teorema 1.20, para todo inteiro positivo j vale

$$\gamma_j(G/N) = \langle [g_1N,\ldots,g_jN];\ g_1,\ldots,g_j \in G\rangle = \langle [g_1,\ldots,g_j]N;\ g_1,\ldots,g_j \in G\rangle = \gamma_j(G)N/N.$$

Analogamente, verifica-se que para todo inteiro positivo i vale $\gamma_j(G/N)^i = \gamma_j(G)^iN/N$. O resultado segue da definição de $D_m(G/N)$. □

Para cada inteiro positivo n, seja n^* o menor inteiro positivo k tal que $kp \geqslant n$. Nossa intenção é provar o seguinte resultado.

Teorema 2.26. *Se G é um grupo arbitrário, então a série de Jennings–Lazard–Zassenhaus de G associada ao primo p é uma N_p–série de G. Mais do que isto, valem as seguintes:*

(i) $D_n(G) = [D_{n-1}(G), G]D_{n^*}(G)^p,\ \forall n \geqslant 2$;

(ii) Se G possui um N_p–série $G = K_1 \geq K_2 \geq \cdots \geq K_i \geq \cdots$, então para cada $n \geqslant 1$ vale $D_n(G) \leq K_n$.

Para a prova deste teorema precisamos de alguns resultados iniciais, os quais serão provados a seguir. A prova do próximo resultado, contudo, pode ser encontrada em [11, cap. III, pág. 317].

Teorema 2.27 (Identidade de Hall–Petrescu)**.** *Seja G um grupo e $x,y \in G$. Para cada $n \geqslant 2$, existem $c_i \in \gamma_i(\langle x,y\rangle)$, $i = 2,\ldots,n$, tais que*

$$x^ny^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \ldots c_n.$$

Lema 2.28. *Para todo grupo G e $x,y \in G$ valem:*

(i) $x^{p^n}y^{p^n} \equiv (xy)^{p^n}\left(mod\,\gamma_2(G)^{p^n}\prod_{r=1}^{n}\gamma_{p^r}(G)^{p^{n-r}}\right)$, *para todo $n \geqslant 1$;*

(ii) Para todo $H \leq G$ tal que $x,[x,y] \in H$ e $n \geqslant 1$ vale

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

Demonstração. Para a prova do item (i), defina $N = \gamma_2(G)^{p^n}\prod_{r=1}^{n}\gamma_{p^r}(G)^{p^{n-r}}$. Pelo Teorema 2.27, temos que $x^{p^n}y^{p^n} = (xy)^{p^n}c_2^{\binom{p^n}{2}}\ldots c_{p^n}$ onde, para cada $j = 2,\ldots,p^n$, $c_j \in \gamma_j(\langle x,y\rangle)$. Seja

$j = 2, \ldots, p^n$ fixado e permita-nos escrever $v_p(l)$ para denotar o expoente da maior potência de p dividindo o inteiro positivo l. Note que para todos os inteiros positivos a, b vale $v_p(ab) = v_p(a) + v_p(b)$. Escrevendo $j = p^r t$ onde t é coprimo com p, temos que

$$\binom{p^n}{j} = \frac{p^n}{j}\binom{p^n - 1}{j-1} = \frac{p^{n-r}}{t}\binom{p^n - 1}{j-1}.$$

Isto mostra que

$$t\binom{p^n}{j} = p^{n-r}\binom{p^n - 1}{j-1}.$$

Portanto, temos que $v_p\left(\binom{p^n}{j}\right) \geqslant n - r$. Isto é, se j é coprimo com p, temos que p^n divide $\binom{p^n}{j}$. Logo, obtemos que $c_j^{\binom{p^n}{j}} \in \gamma_2(G)^{p^n} \leq N$. Por outro lado, se $r \geqslant 1$, vemos que p^{n-r} divide $\binom{p^n}{j}$ e como $j = p^r t$ obtemos $c_j^{\binom{p^n}{j}} \in \gamma_j(G)^{p^{n-r}} \leq \gamma_{p^r}(G)^{p^{n-r}} \leq N$.

Portanto, temos que

$$x^{p^n} y^{p^n} = (xy)^{p^n} c_2^{\binom{p^n}{2}} \ldots c_{p^n} \equiv (xy)^{p^n} (mod N).$$

Isto prova o item (i) do lema. Para a prova do item (ii), note que $x^{p^n}[x^{p^n}, y] = (x^{p^n})^y = (x^y)^{p^n} = (x[x,y])^{p^n}$. Pelo item (i), para cada $n \geqslant 1$, sendo $H = \langle x, [x,y] \rangle$, temos que

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

O resultado segue. □

Lema 2.29. *Para todo $i, j \geqslant 1$, $k \geqslant 0$ e G um grupo arbitrário, vale*

$$[\gamma_j(G)^{p^k}, \gamma_i(G)] \leq \prod_{r=0}^{k} \gamma_{i+jp^r}(G)^{p^{k-r}}.$$

Demonstração. Seja $N = \prod_{r=0}^{k} \gamma_{i+jp^r}(G)^{p^{k-r}}$. Então, $N \trianglelefteq G$ e obtemos o resultado mostrando que $[x^{p^k}, y] \in N$ para todos $x \in \gamma_j(G)$ e $y \in \gamma_i(G)$. Sejam, portanto, $x \in \gamma_j(G)$ e $y \in \gamma_i(G)$ elementos fixados. Se $k = 0$ o resultado vale pelo Teorema 1.20, por isso supomos $k > 1$.

Definindo $H = \langle x, [x,y] \rangle$, o Lema 2.28 mostra que

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

Por outro lado, temos que $[x,y]^{p^k} \in \gamma_{j+i}(G)^{p^k} \leq N$. Pela equação anterior, obtemos o resultado verificando que $\gamma_2(H)^{p^k} \prod_{r=1}^{k} \gamma_{p^r}(H)^{p^{k-r}} \leq N$.

Sabemos que $\gamma_2(H) = \langle [z_1, \ldots, z_s];\ s \geqslant 2, z_1, \ldots, z_s \in \{x, [x,y]\} \rangle$. Assim, como $x \in \gamma_j(G)$ e $y \in \gamma_i(G)$, temos que $\gamma_2(H) \leq \gamma_{i+2j}(G) \leq \gamma_{i+j}(G)$. Segue que $\gamma_2(H)^{p^k} \leq \gamma_{i+j}(G)^{p^k} \leq N$. Ainda, dado que $H = \langle x, [x,y] \rangle \leq \gamma_j(G)$ e $\gamma_2(H) \leq \gamma_{i+2j}(G)$, temos por indução em r que para todo $r \geqslant 2$ vale $\gamma_r(H) \leq \gamma_{i+jr}(G)$. Em particular, para todo $r = 1, \ldots, k$ vale $\gamma_{p^r}(H) \leq \gamma_{i+jp^r}(G)$ e, portanto, $\gamma_{p^r}(H)^{p^{k-r}} \leq \gamma_{i+jp^r}(G)^{p^{k-r}} \leq N$. Nossas considerações iniciais estabelecem o resultado. □

Lema 2.30. *Suponha que $i, j \geqslant 1$ e $k \geqslant 0$. Sejam G um grupo arbitrário e $R = \prod_{r=0}^{k} \gamma_{i+jp^r}(G)^{p^{k-r}}$. Para todo $x \in \gamma_i(G)$ e $n \geqslant 2$ vale que*

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

Demonstração. Provamos o resultado por indução em $n \geqslant 2$.

Note que $\gamma_2(\langle x,R \rangle) = [R, \langle x,R \rangle]$. De fato, se $x_1, x_2 \in \langle x \rangle$ e $r_1, r_2 \in R$, temos que $[x_1 r_1, x_2 r_2]$ $= [x_1, x_2 r_2]^{r_1} [r_1, x_2 r_2] = [x_1, r_2]^{r_1} [r_1, x_2 r_2]$. Desde que $R \trianglelefteq G$, temos que $R \trianglelefteq \langle x,R \rangle = \langle x \rangle R$. Segue-se que $[R, \langle x,R \rangle] \trianglelefteq \langle x,R \rangle$ e $[x_1, r_2]^{r_1} [r_1, x_2 r_2] \in [R, \langle x,R \rangle]$. Logo, $\gamma_2(\langle x,R \rangle) \leq [R, \langle x,R \rangle]$. Ora, $x \in \gamma_i(G)$ e $R \leq \gamma_i(G)$ e portanto

$$\begin{aligned}
\gamma_2(\langle x,R \rangle) &\leq [R, \gamma_i(G)] = \Big[\prod_{r=0}^{k} \gamma_{i+jp^r}(G)^{p^{k-r}}, \gamma_i(G) \Big] = \prod_{r=0}^{k} [\gamma_{i+jp^r}(G)^{p^{k-r}}, \gamma_i(G)] \\
&\leq \prod_{r=0}^{k} \prod_{m=0}^{h-r} \gamma_{i+(i+jp^r)p^m}(G)^{p^{k-r-m}} = \prod_{r=0}^{k} \prod_{m=0}^{h-r} \gamma_{i(1+p^m)+jp^{r+m}}(G)^{p^{k-(r+m)}} \\
&\leq \prod_{0 \leqslant r+m \leqslant k} \gamma_{2i+jp^{r+m}}(G)^{p^{k-(r+m)}} \leq \prod_{t=0}^{k} \gamma_{2i+jp^t}(G)^{p^{k-t}}.
\end{aligned}$$

Finalmente, suponha $n > 2$ e que o resultado vale para todo $s \leqslant n-1$.

$$\begin{aligned}
\gamma_n(\langle x,R\rangle) &= [\gamma_{n-1}(\langle x,R\rangle),\langle x,R\rangle] \leq [\gamma_{n-1}(\langle x,R\rangle),\gamma_i(G)] \leq \Big[\prod_{r=0}^{k}\gamma_{i(n-1)+jp^r}(G)^{p^{k-r}},\gamma_i(G)\Big] \\
&= \prod_{r=0}^{k}[\gamma_{i(n-1)+jp^r}(G)^{p^{k-r}},\gamma_i(G)] \leq \prod_{r=0}^{k}\prod_{m=0}^{k-r}\gamma_{i+(i(n-1)+jp^r)p^m}(G)^{p^{k-r-m}} \\
&= \prod_{r=0}^{k}\prod_{m=0}^{k-r}\gamma_{i(1+(n-1)p^m)+jp^{r+m}}(G)^{p^{k-(r+m)}} \leq \prod_{0\leqslant r+m\leqslant k}\gamma_{in+jp^{r+m}}(G)^{p^{k-(r+m)}} \\
&\leq \prod_{t=0}^{k}\gamma_{in+jp^t}(G)^{p^{k-t}}.
\end{aligned}$$

Vemos pois que o resultado vale também para n. O resultado está provado. □

Lema 2.31. *Se $i,j \geqslant 1$ e $h,k \geqslant 0$, então*

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

Demonstração. Pelo Lema 2.29 podemos supor $k > 0$. Sejam $x \in \gamma_i(G)$ e $y \in \gamma_j(G)$ e considere $H = \langle x,[x,y^{p^h}]\rangle$. Pelo Lema 2.28 item (ii), temos que

$$[x^{p^k},y^{p^h}] \equiv [x,y^{p^h}]^{p^k}\Big(mod\,\gamma_2(H)^{p^k}\prod_{m=1}^{k}\gamma_{p^m}(H)^{p^{k-m}}\Big). \tag{2.1}$$

Para cada $n = 1,\ldots,p^k$ defina

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

Então, $H_1 = \prod_{r=0}^{h}\gamma_{i+jp^r}(G)^{p^{h-r}}$. Pelo Lema 2.29, temos que $[x,y^{p^h}] \in H_1$ e por isso temos que

$$H = \langle x,[x,y^{p^h}]\rangle \leq \langle x,H_1\rangle. \tag{2.2}$$

Segue pelo Lema 2.30 que para todo $n \geqslant 2$

$$\gamma_n(H) \leq \prod_{r=0}^{h}\gamma_{ni+jp^r}(G)^{p^{h-r}} = H_n. \tag{2.3}$$

Temos, pois, que $\gamma_2(H) \leq H_2 \leq H_1$ e por isso

$$\gamma_2(H)^{p^k} \prod_{m=1}^{k} \gamma_{p^m}(H)^{p^{k-m}} \leq H_1^{p^k} \prod_{m=1}^{k} H_{p^m}^{p^{k-m}} = \prod_{m=0}^{k} H_{p^m}^{p^{k-m}}. \tag{2.4}$$

Por outro lado, como $[x, y^{p^h}] \in H_1$, temos que $[x, y^{p^h}]^{p^k} \in H_1^{p^k}$. Segue de (2.1) e (2.4) que

$$[x^{p^k}, y^{p^h}] \in \prod_{m=0}^{k} H_{p^m}^{p^{k-m}}. \tag{2.5}$$

Sejam $m \in \{0, \ldots, k\}$ e $r \in \{0, \ldots, h\}$. Então, $m+h-r \geqslant k$ se, e somente se, $m+h-k \geqslant r$, isso é, se e somente se $m+h-k+1 > r$. Por outro lado, se $m+h-r \geqslant k$, temos por definição de $D_t(G)$, $t \geqslant 1$, que $\gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq D_{ip^k+jp^h}(G)$. Logo, sendo $s = max(m+h-k+1, 0)$, temos que

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

Segue que

$$H_{p^m}^{p^{k-m}} \leq D_{ip^k+jp^h}(G)\gamma_{ip^m+jp^s}(G)^{p^{k-m}} \leqslant D_{ip^k+jp^h}(G) \tag{2.6}$$

pois $ip^k + jp^{s+k-m} \geqslant ip^k + jp^h$. Finalmente, segue de (2.5) e (2.6) que

$$[x^{p^k}, y^{p^h}] \in \prod_{m=0}^{k} H_{p^m}^{p^{k-m}} \leq D_{ip^k+jp^h}(G). \tag{2.7}$$

Vemos pois que $x^{p^k} D_{ip^k+jp^h}(G)$ comuta com $y^{p^h} D_{ip^k+jp^h}(G)$ em $G/D_{ip^k+jp^h}(G)$. Isto é, cada elemento de $\gamma_i(G)^{p^k} D_{ip^k+jp^h}(G)$ comuta com cada elemento de $\gamma_j(G)^{p^h} D_{ip^k+jp^h}(G)$. Portanto,

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

O resultado está, portanto, demonstrado. □

A prova do seguinte resultado pode ser encontrada em [25, pág. 159, Teorema 6.1.1] e [25, pág. 164, Teorema 6.1.8].

Lema 2.32 (Lema de Schreier)**.** *Seja G um grupo finitamente gerado e H um subgrupo de G de índice finito. Então H é finitamente gerado.*

Para expormos a prova do Teorema 2.26, necessitamos ainda um resultado sobre grupos nilpotentes.

Teorema 2.33. *Seja G um grupo finitamente gerado e suponha que $g^s = 1$ para todo $g \in G$. Se G é nilpotente, então G é finito.*

Demonstração. Argumentamos por indução na classe de nilpotência de G. Se $cl(G) = 1$ nada temos que fazer. Suponha que $cl(G) \geqslant 2$ e $G = \langle g_1, \ldots, g_m \rangle$. Então, dado que $G/\gamma_2(G)$ é abeliano, todo elemento em $G/\gamma_2(G)$ é da forma $g_1^{r_1} \ldots g_m^{r_m} \gamma_2(G)$ onde $0 \leqslant r_1, \ldots, r_m \leqslant s$. Isto mostra que $|G/\gamma_2(G)| \leqslant s^m$. Em particular, pelo Lema 2.32, temos que $\gamma_2(G)$ é finitamente gerado. Por indução, temos que $\gamma_2(G)$ é finito e então G é finito. □

Estamos, pois, em condições de verificar que a série de Jennings–Lazard–Zassenhaus de um grupo G é, de fato, uma N_p–série.

Demonstração do Teorema 2.26. Seja G um grupo e $D_i(G)$ o i–ésimo termo da série de Jennings–Lazard–Zassenhaus de G associada ao primo p. Vamos verificar que dados $n, m \geqslant 1$ vale

$$[D_n(G), D_m(G)] \leq D_{n+m}(G),\ D_n(G)^p \leq D_{pn}(G) \tag{2.8}$$

Sejam fixados $n, m \geqslant 1$. Pelo Lema 2.31, temos que

$$\begin{aligned} [D_n(G), D_m(G)] &= \Big[\prod_{ip^k \geqslant n} \gamma_i(G)^{p^k}, \prod_{jp^h \geqslant m} \gamma_j(G)^{p^h} \Big] = \prod_{ip^k \geqslant n} \prod_{jp^h \geqslant m} [\gamma_i(G)^{p^k}, \gamma_j(G)^{p^h}] \\ &\leq \prod_{ip^k \geqslant n} \prod_{jp^h \geqslant m} D_{ip^k + jp^h}(G) \leq D_{n+m}(G). \end{aligned}$$

Isto mostra a primeira relação em (2.8).

Para provar a segunda relação em (2.8), vamos reduzir a prova ao caso em que G é um p–grupo finito. Inicialmente, dados $x \in D_n(G)$ e $y \in D_m(G)$, podemos tomar um subgrupo H de G finitamente gerado e tal que $x \in D_n(H)$ e $y \in D_m(H)$. Logo, podemos assumir que G é finitamente gerado. Se o resultado vale para p–grupos finitos, considere $G/D_{pn}(G)$. Note que para cada $g \in G$ vale que $g^{p^k} \in D_{pn}(G)$ para algum inteiro fixo k. Logo, todo elemento em $G/D_{pn}(G)$ tem ordem dividindo p^k. Ainda, $G/D_{pn}(G)$ é finitamente gerado e nilpotente pois $\gamma_{pn}(G) \leq D_{pn}(G)$. Pelo Teorema 2.33, vemos que $G/D_{pn}(G)$ é um p–grupo finito. Como o resultado vale para p–grupos finitos, vemos pelo Lema 2.25 que

$$(D_n(G/D_{pn}(G))^p = (D_n(G)/D_{pn}(G))^p = D_n(G)^p D_{pn}(G)/D_{pn}(G) \leq D_{pn}(G)/D_{pn}(G),$$

isto é, $D_n(G)^p \leq D_{pn}(G)$.

Finalmente, assumindo que G é um p–grupo finito, temos que $\gamma_p(D_n(G)/D_{pn}(G)) = 1$ o que mostra que $D_n(G)/D_{pn}(G)$ é regular. Mais do que isto, se $g \in \gamma_j(G)$ e $jp^k \geqslant n$, temos que $g^{p^{k+1}} \in \gamma_j(G)^{p^{k+1}} \leq D_{pn}(G)$. Isto é, $D_n(G)/D_{pn}(G)$ é gerado por elementos de ordem p. Isto mostra que $(D_n(G)/D_{pn}(G))^p = 1$ e $D_n(G)^p \leq D_{pn}(G)$. Portanto, concluímos que a série de Jennings–Lazard–Zassenhaus de um grupo G é uma N_p–série de G. Resta-nos demonstrar os itens (i) e (ii) do Teorema 2.26.

Seja G um grupo e $D_i(G)$ o i–ésimo termo da série de Jennings–Lazard–Zassenhaus de G associada ao primo p. Dado $n \geqslant 2$, desde que a série $G = D_1(G) \geq \cdots \geq D_i(G) \geq \cdots$ é uma N_p–série de G, temos que $[D_{n-1}(G), G]D_{n^*}(G)^p \leq D_n(G)$. Suponha que $ip^k \geqslant n$. Se $k = 0$, $i \geqslant n$ e temos que $\gamma_i(G)^{p^k} = \gamma_i(G) \leq \gamma_n(G) = [\gamma_{n-1}(G), G] \leq [D_{n-1}(G), G]$. Ainda, se $k > 0$, temos que $ip^{k-1} \geqslant n^*$ e, portanto, $\gamma_i(G)^{p^k} \leq (\gamma_i(G)^{p^{k-1}})^p \leq D_{ip^{k-1}}(G)^p \leq D_{n^*}(G)^p$. Em qualquer caso vemos que $\gamma_i(G)^{p^k} \leq [D_{n-1}(G), G]D_{n^*}(G)^p$. Portanto, $D_n(G) \leq [D_{n-1}(G), G]D_{n^*}(G)^p$ e o item (i) está verificado. Finalmente, suponha que $G = K_1 \geq \cdots \geq K_i \geq \cdots$ é qualquer N_p–série de G. Se $n \geqslant 2$ e $D_{n-1}(G) \leq K_{n-1}$, temos que $D_n(G) = [D_{n-1}(G), G]D_{n^*}(G)^p \leq [K_{n-1}, G]K_{n^*}^p \leq K_n$. O item (ii), portanto, segue por indução em n. □

Seja G um grupo arbitrário. Pelo Teorema 2.26, a série de Jennings–Lazard–Zassenhaus de G associada ao primo p é uma N_p–série de G. Pelas considerações iniciais desta seção, sabemos que $L(G) = \bigoplus_{n \geqslant 1} D_n(G)/D_{n+1}(G)$ possui uma estrutura de $\mathbb{F}_p$–álgebra de Lie. Nosso interesse particular com a álgebra $L(G)$ é mais específico na subálgebra de $L(G)$ gerada por $D_1(G)/D_2(G)$. Tal subálgebra será denotada por $L_p(G)$ e será utilizada na demonstração de alguns dos principais resultados deste trabalho.

2.3 Identidades polinomiais

Nesta seção temos como objetivo principal a expor as noções essenciais da teoria de álgebras satisfazendo identidades polinomiais.

Seja X um conjunto não vazio. Definimos um monômio não associativo de grau 1 em X como sendo um elemento de X. Supondo definidos os monômios não associativos de grau k em X para todo $k = 1, \ldots, n-1$, $n > 1$, definimos os monômios não associativos de grau n em X como sendo uma expressão da forma $(u)(v)$ onde u é monômio não associativo de grau $i < n$ e v é monômio não associativo de grau $n - i$ em X. Indutivamente, definimos os monômios não associativos de grau n para todo inteiro positivo n.

Exemplo 2.34. Se X é um conjunto arbitrário, os monômios não associativos de graus 3 e 4, por exemplo são da forma $(xy)z, x(yz)$ e $((xy)z)w, (x(yz))w, (xy)(zw), x((yz)w), x(y(zw))$, respectivamente, onde $x, y, z, w \in X$.

Dado X um conjunto não vazio, podemos considerar o conjunto $\Gamma(X)$ dos monômios não associativos sobre X munido com a operação de justa-posição. Se $w \in \Gamma(X)$, escrevemos $w = w(x_1, \ldots, x_n)$ para descrever o fato que $x_1, \ldots, x_n$ são os únicos elementos de X ocorrendo em w.

Definição 2.35. Seja R um anel associativo comutativo e com unidade e $\mathcal{C}$ uma classe de R–álgebras. Uma R–álgebra L da classe $\mathcal{C}$ é chamada livre nesta classe, livremente gerada (como álgebra) por um conjunto $X \subseteq L$, se $L = \langle X \rangle$ e para toda R–álgebra L_1 e função $f : X \longrightarrow L_1$ existe um único homomorfismo $\varphi : L \longrightarrow L_1$ tal que $\varphi|_X = f$.

Teorema 2.36. *Se R é um anel associativo comutativo e com unidade, para todo conjunto X, existe uma R–álgebra livre na classe de todas as R–álgebras e livremente gerada por X.*

Demonstração. Se $X = \emptyset$, a R–álgebra trivial é livre na classe de todas as R–álgebras e é por definição livremente gerada pelo X. Então suponha $X \neq \emptyset$ e seja $R(X)$ o R–módulo livremente gerado por $\Gamma(X)$. Um elemento em $R(X)$ é chamado um polinômio não associativo em X. Assim, um elemento em $R(X)$ é da forma $\sum_{u \in \Gamma(X)} \alpha_u u$ onde $\alpha_u \neq 0$ somente para um número finito de $u \in \Gamma(X)$. Em $R(X)$ definimos:

(i) Multiplicação: $\big(\sum_{u \in \Gamma(X)} \alpha_u u\big)\big(\sum_{v \in \Gamma(X)} \beta_v v\big) = \sum_{u,v \in \Gamma(X)} (\alpha_u \beta_v) uv$;

(ii) Multiplicação escalar: $r\big(\sum_{u \in \Gamma(X)} \alpha_u u\big) = \sum_{u \in \Gamma(X)} r\alpha_u u$.

É fácil ver que $R(X)$ com as operações acima definidas se torna uma R–álgebra não associativa gerada pelo conjunto X.

Seja, agora, L uma R–álgebra e $f : X \longrightarrow L$ uma função. Para todo monômio não associativo u de grau 1 em X defina $u^\varphi = u^f$. Supondo $n > 1$ e que foram definidos $v^\varphi \in L$ para todos monômios não associativos v de grau menor que n, para todo monômio não associativo de grau n, digamos $u = (v)(w)$ onde v e w são de grau menor que n, podemos definir $u^\varphi = (v)^\varphi (w)^\varphi$. Estendendo por linearidade a função φ definida em $\Gamma(X)$ e tomando valores em L, obtemos um homomorfismo de $R(X)$ em L estendendo f. A unicidade é imediata e concluímos. □

Sejam R um anel associativo comutativo e unitário e $R(X)$ a R–álgebra livre não associativa livremente gerada por X. Seja $f \in R(X)$ um elemento arbitrário. Então, existem $v_1, \ldots, v_m \in$

$\Gamma(X)$ e $\alpha_1,\ldots,\alpha_m \in R$ tais que $f = \alpha_1 v_1 + \cdots + \alpha_m v_m$. Se $x_1,\ldots,x_n$ são todas as variáveis ocorrendo nos monômios $v_1,\ldots,v_m$, escrevemos $f = f(x_1,\ldots,x_n)$. Ainda, para cada R–álgebra L é bem definido o elemento $f = f(l_1,\ldots,l_n) \in L$ obtido trocando-se a variável x_i por $l_i \in L$, $i = 1,\ldots,n$.

Definição 2.37. Sejam R um anel associativo comutativo e unitário e L uma R–álgebra. Sejam $R(X)$ a R–álgebra livre não associativa livremente gerada por X e $f(x_1,\ldots,x_n), g(x_1,\ldots,x_n) \in R(X)$. A fórmula

$$f(x_1,\ldots,x_n) \equiv g(x_1,\ldots,x_n) \tag{2.9}$$

é chamada uma identidade. A identidade (2.9) é satisfeita em L se para todos $l_1,\ldots,l_n \in L$ vale $f(l_1,\ldots,l_n) = g(l_1,\ldots,l_n)$.

Em nosso trabalho, identidades da forma $f(x_1,\ldots,x_n) \equiv 0$ são de particular interesse, por isto provamos a seguinte caracterização.

Lema 2.38. *Sejam R um anel associativo comutativo e unitário e L uma R–álgebra arbitrária. Então $f(x_1,\ldots,x_n) \equiv 0$ é uma identidade satisfeita em L se, e somente se, $f^\varphi = 0$ para todo homomorfismo $\varphi : R(X) \longrightarrow L$.*

Demonstração. Sejam R, L e f como no enunciado. Se $f(x_1,\ldots,x_n) \equiv 0$ é satifeita em L, então para todo homomorfismo $\varphi : R(X) \longrightarrow L$ vale $f^\varphi = (f(x_1,\ldots,x_n))^\varphi = f(x_1^\varphi,\ldots,x_n^\varphi) = 0$. Reciprocamente, suponha que f é anulado por todos os homomorfismos de R–álgebras de $R(X)$ em L. Sejam $l_1,\ldots,l_n \in L$ escolhidos arbitrariamente e $f : X \longrightarrow L$ a função que leva x_i em l_i, $i = 1,\ldots,n$ e x em 0 para todos os demais $x \in X$. Então, f estende-se de modo único a um homomorfismo φ de $R(X)$ em L e vale que $f(x_1,\ldots,x_n)^\varphi = f(x_1^\varphi,\ldots,x_n^\varphi) = f(l_1,\ldots,l_n) = 0$. Isso é, $f(x_1,\ldots,x_n) \equiv 0$ é identidade satisfeita em L. □

Como uma consequência imediata do Lema 2.38, temos o seguinte.

Lema 2.39. *Sejam R um anel associativo comutativo e unitário e L uma R–álgebra arbitrária. Então $T(L) = \{f \in R(X); f \equiv 0$ é satifeita em $L\}$ é um ideal de $R(X)$, chamado o ideal das identidades polinomiais de L em $R(X)$.*

Definição 2.40. Seja $\mathcal{C}$ uma classe de R–álgebras. Dizemos que a identidade $f(x_1,\ldots,x_n) \equiv 0$ é uma identidade não trivial na R–álgebra L de $\mathcal{C}$ se tal identidade é satisfeita em L mas existe uma R–álgebra L' na classe $\mathcal{C}$ que não satisfaz esta identidade. Neste caso, dizemos que L é uma álgebra da classe $\mathcal{C}$ satisfazendo uma identidade polinomial.

Exemplo 2.41. Seja $\mathcal{C}$ a classe das R–álgebras de Lie. O centro de uma R–álgebra de Lie L é o conjunto $Z(L) = \{z \in L;\ [z,l] = 0\ \forall\ l \in L\}$. Note que $Z(L)$ é um ideal de L; L é chamada abeliana se $Z(L) = L$. Neste caso, $f(x,y) = xy \equiv 0$ é uma identidade não trivial satisfeita em L. Ainda, se L é uma R–álgebra de Lie nilpotente, de classe c por exemplo, então $f(x_1,\ldots,x_{c+1}) = x_1 \ldots x_{c+1} \equiv 0$ é uma identidade em L, vide Teorema 2.19.

A seguir damos um exemplo de cunho mais geral.

Exemplo 2.42. Seja $\mathcal{C}$ a classe de todas as $\mathbb{F}$–álgebras, $\mathbb{F}$ um corpo. Seja L uma $\mathbb{F}$–álgebra de dimensão estritamente menor que n. Provamos a seguir que L satisfaz a seguinte identidade não trivial

$$f = f(x_1,\ldots,x_n) = \sum_{\sigma\in S_n} sign(\sigma) x_{\sigma(1)} \ldots x_{\sigma(n)} \equiv 0. \tag{2.10}$$

Seja σ um elemento arbitrário do grupo simétrico S_n. Pondo $m_\sigma(x_1,\ldots,x_n) = x_{\sigma(1)} \ldots x_{\sigma(n)}$, temos que para cada $\alpha \in S_n$ vale $m_\sigma(x_{\alpha(1)},\ldots,x_{\alpha(n)}) = x_{\alpha\sigma(1)} \ldots x_{\alpha\sigma(n)} = m_{\alpha\sigma}(x_1,\ldots,x_n)$. Por exemplo se $n = 4$, $\sigma = (12)(34)$ e $\alpha = (1234)$, então $m_\sigma(x_1,\ldots,x_4) = x_2x_1x_4x_3$ e por isso $m_\sigma(x_{\alpha(1)},\ldots,x_{\alpha(4)}) = m_\sigma(x_2,x_3,x_4,x_1) = x_3x_2x_1x_4 = x_{\alpha\sigma(1)} \ldots x_{\alpha\sigma(4)} = m_{\alpha\sigma}(x_1,\ldots,x_4)$. Segue-se que para todo $\alpha \in S_n$ vale

$$\begin{aligned}
f(x_{\alpha(1)},\ldots,x_{\alpha(n)}) &= \sum_{\sigma\in S_n} sign(\sigma) m_\sigma(x_{\alpha(1)},\ldots,x_{\alpha(n)}) \\
&= \sum_{\sigma\in S_n} sign(\alpha)sign(\alpha)sign(\sigma) m_{\alpha\sigma}(x_1,\ldots,x_n) \\
&= sign(\alpha) \sum_{\sigma\in S_n} sign(\alpha)sign(\sigma) m_{\alpha\sigma}(x_1,\ldots,x_n) \\
&= sign(\alpha) \sum_{\sigma\in S_n} sign(\alpha\sigma) m_{\alpha\sigma}(x_1,\ldots,x_n) \\
&= sign(\alpha) \sum_{\beta\in S_n} sign(\beta) m_\beta(x_1,\ldots,x_n) \\
&= sign(\alpha) f(x_1,\ldots,x_n).
\end{aligned}$$

Portanto, se $1 \leqslant i \neq j \leqslant n$, tomando $\alpha = (ij) \in S_n$ temos que

$$f(x_{\alpha(1)},\ldots,x_{\alpha(n)}) = -f(x_1,\ldots,x_n).$$

Da igualdade acima, se substituirmos as variáveis x_i e x_j pela mesma variável y, obtemos um polinômio sendo igual ao seu oposto, isso é, obtemos o polinômio nulo.

Seja $\{e_1,\ldots,e_k\}$ uma base de L. Por hipótese, temos que $n > k$. Como f é linear em cada uma de suas entradas, temos que os valores que f assume em L são combinações lineares de

valores da forma $f(l_1,\ldots,l_n)$ onde $l_1,\ldots,l_n \in \{e_1,\ldots,e_k\}$. Contudo, escolhendo $l_1,\ldots,l_n \in \{e_1,\ldots,e_n\}$, algum e_i é tomado pelo menos 2 vezes e, portanto, o resultado obtido é zero como estabelece o último parágrafo. Portanto, f é identicamente nulo em L.

Finalmente, seja $M_{n\times n}(\mathbb{F})$ a $\mathbb{F}$–álgebra associativa das matrizes $n\times n$ sobre $\mathbb{F}$. Sendo E_{uv} a (u,v)–ésima matriz elementar, sabemos que $E_{uv}E_{st} = E_{ut}$ se $v = s$ e $E_{uv}E_{st} = 0$ se $v \neq s$. Por isso, $f(E_{11},\ldots,E_{(n-1)n}) = E_{1n} \neq 0$. Nossa afirmação está verificada.

Definição 2.43. Seja X um conjunto não vazio e $\Gamma(X)$ o monoide dos monômios sobre X. Dadas $x_1,\ldots,x_n \in X$, podemos considerar o subconjunto de $\Gamma(X)$ que consiste dos monômios com entradas exclusivamente em $S = \{x_1,\ldots,x_n\} \subseteq X$. Para cada monômio w com entradas em S está associada uma n–upla $\alpha = (m_1,\ldots,m_n)$ onde, para cada $i = 1,\ldots,n$, m_i é o número de ocorrências de x_i em w. O número m_i é chamado o grau de w com relação à variável x_i e α é chamado o multigrau de w.

Definição 2.44. Seja X um conjunto não vazio e $R(X)$ a R–álgebra livre não associativa livremente gerada por X. Um polinômio $f = f(x_1,\ldots,x_n) \in R(X)$ é chamado homogêneo com relação à variável x_i se f é uma combinação linear de monômios com mesmo grau com relação à variável x_i. Neste caso, o grau de um monômio de f com relação a x_i é chamado o grau de f com relação a x_i. Ainda, f é chamado multi-homogêneo se f é combinação linear de monômios cada um dos quais associados ao mesmo multigrau. Finalmente, f é dita multilinear se f é multi-homogêneo e cada monômio de f tem multigrau $\underbrace{(1,1,\ldots,1)}_{n}$.

Por exemplo, o multigrau do monômio $w = w(x_1,x_2,x_3) = (x_1x_2)((x_1x_3)x_2)$ é $(2,2,1)$. O polinômio $f(x_1,x_2,x_3) = (x_2(x_1x_2))x_3 + x_2(x_1(x_3x_2))$ é multihomogêneo não linear e o polinômio $f(x_1,\ldots,x_4) = (x_1x_2)(x_3x_4) + ((x_1x_3)x_4)x_2$ é multilinear.

Se $f(x_1,\ldots,x_n) \equiv 0$ é uma identidade satisfeita na R–álgebra L e o polinômio f é multilinear, dizemos que a identidade é multilinear. Em vários sentidos, pode ser mais interessante trabalhar com identidades multilineares. Logo, um importante resultado é que toda identidade tem "consequências" multilineares. Isso é provado a seguir.

Teorema 2.45. *Sejam R um anel associativo comutativo e unitário e L uma R–álgebra. Suponha que a identidade $f(x_1,\ldots,x_n) \equiv 0$ seja satisfeita em L. Então, a partir de f podemos obter uma identidade multilinear satisfeita em L.*

Demonstração. Seja $f(x_1,\ldots,x_n) \equiv 0$ uma identidade satisfeita na R–álgebra L. Escreva

$$f = f_0 + f_1 + \cdots + f_t, \tag{2.11}$$

onde para cada $i = 0,\ldots,t$, f_i é polinômio homogêneo de grau i em x_1. Se $f_0 \neq 0$, então o número de variáveis ocorrendo em f_0 é estritamente menor que n. Escolhendo-se $l_2,\ldots,l_n \in L$,

temos que $f(0,l_2,\ldots,l_n) = f_0(l_2,\ldots,l_n) = 0$. Isso é, $f_0 \equiv 0$ é satisfeita em L. Por indução no número de variáveis, obtemos que f_0 tem consequência multilinear. Podemos, então, supor que $f_0 = 0$. Se $t = 1$, f é linear em x_1 e podemos considerar outras variáveis. Se $t > 1$, considere f como sendo um polinômio em x_1 e tome $g(y,z,x_2,\ldots,x_n) = f(x+y) - f(y) - f(z)$. Note que o número total de ocorrências de y ou z em qualquer monômio de g é igual a t e o número de ocorrências de y e z em qualquer destes é no máximo $t-1$. Por definição de g, vemos que $g(a,b,l_2,\ldots,l_n) = 0$ para todos $a,b,l_2,\ldots,l_n \in L$. Isso é $g(y,z,x_2,\ldots,x_n) \equiv 0$ é satisfeita em L. Repetidas aplicações deste processo reduz o número de variáveis ocorrendo um número máximo de vezes. Logo, em um número finito de passos obtemos uma identidade multilinear satisfeita em L. □

Para encerrar este capítulo, tecemos mais um comentário. Sejam R um anel associativo comutativo e unitário, $X = \{x_1,\ldots,x_n,\ldots\}$ um conjunto enumerável de variáveis e $R(X)$ a R–álgebra livre na classe de todas as R–álgebras, livremente gerada por X, definida no Teorema 2.36. Seja I o ideal de $R(X)$ gerado pelo conjunto $\{ff,\ (fg)h+(gh)f+(hf)g;\ f,g,h \in R(X)\}$. Então, a R–álgebra quociente $R(X)/I$ é uma R–álgebra de Lie gerada por X (identificando x com $x+I$). Mais do que isto, se L é uma R–álgebra de Lie, seja $f : X \longrightarrow L$ uma função arbitrária. Existe um único homomorfismo $\varphi : R(X) \longrightarrow L$ estendendo a função f. Por definição de I, vemos que I está contido no núcleo de φ e, portanto, $\overline{\varphi} : R(X)/I \longrightarrow L$ definida por $f+I \mapsto f^{\varphi}$ é um homomorfismo bem definido de R–álgebras de Lie estendendo a função $x+I \mapsto x^f$. Isto mostra que $R(X)/I$ é uma R–álgebra de Lie livre na classe de todas as R–álgebras de Lie, livremente gerada por X. Notamos ainda que uma R–álgebra de Lie L satisfaz uma identidade não trivial na classe de todas as R–álgebras de Lie se, e somente se, existe um elemento $f = f(x_1,\ldots,x_n)$ não trivial de $R(X)/I$ tal que $f(l_1,\ldots,l_n) = 0$ para todos $l_1,\ldots,l_n \in L$.

Capítulo 3

Os resultados de Zelmanov e Bahturin–Zaicev

Neste capítulo, iremos introduzir as noções e obter alguns resultados básicos sobre grupos residualmente–$\mathcal{C}$, onde $\mathcal{C}$ denota uma classe de grupos finitos fechada para subgrupos, imagens epimórficas e produtos diretos finitos. Nossa atenção particular, inicialmente, será no caso em que $\mathcal{C}$ for a classe dos p–grupos finitos. Neste caso um grupo residualmente–$\mathcal{C}$ será chamado residualmente–p. Se G é um grupo arbitrário, pelo Teorema 2.26, sabemos que dado um primo p, a série de Jennings–Lazard–Zassenhaus de G associada a p é uma N_p–série de G e, portanto, $L(G) = \bigoplus_{i\geqslant 1} D_i(G)/D_{i+1}(G)$ admite uma estrutura de $\mathbb{F}_p$–álgebra de Lie. Temos como objetivo principal neste capítulo demonstrar um resultado, obtido em [37] por E.I. Zelmanov, onde é mostrado que se G é um grupo de torção finitamente gerado e residualmente–p e a subálgebra $L_p(G) = \langle D_1(G)/D_2(G)\rangle$ da álgebra de Jennings–Lazard–Zassenhaus de G associada ao primo p satisfaz uma identidade polinomial não trivial, então G é finito. Após isto, para que possamos utilizar tal resultado de E.I. Zelmanov no capítulo final deste trabalho, iremos demonstrar um resultado obtido em [1] por Y.A. Bahturin e M.V. Zaicev, onde é provado que se L é uma álgebra de Lie sobre um corpo $\mathbb{F}$ agida por um grupo finito solúvel G de modo que $|G|$ não é divisível pela característica de $\mathbb{F}$ e a subálgebra $C_L(G)$ dos pontos fixos satisfaz uma identidade polinomial não trivial, então L também satisfaz uma identidade polinomial não trivial.

3.1 Propriedades residuais

Em toda esta seção, $\mathcal{C}$ denota uma classe de grupos finitos que é fechada para subgrupos, imagens epimórficas e produtos diretos finitos. Um grupo G é chamado residualmente–$\mathcal{C}$ se para todo elemento não trivial g em G existem $Q = Q_g$ em $\mathcal{C}$ e um homomorfismo $\varphi = \varphi_g : G \longrightarrow Q$

tal que $g^{\varphi} \neq 1$. Note que todo grupo G na classe $\mathcal{C}$ é claramente residualmente–$\mathcal{C}$ pois para cada elemento não trivial $g \in G$ basta-nos tomar $Q_g = G$ e $\varphi_g = id(G)$, este último sendo o automorfismo idêntico de G.

Se o grupo G está na classe $\mathcal{C}$, permita-nos escrever $G \in \mathcal{C}$. O seguinte teorema estabelece uma condição necessária e suficiente para que um grupo G seja residualmente–$\mathcal{C}$.

Teorema 3.1. *Para um grupo arbitrário G, são equivalentes:*

(i) *G é residualmente–$\mathcal{C}$;*

(ii) $\bigcap\{N \trianglelefteq G; G/N \in \mathcal{C}\} = 1$.

Demonstração. Suponha inicialmente que G é residualmente–$\mathcal{C}$. Então, dado $1 \neq g \in G$, existem um grupo $Q = Q_g$ na classe $\mathcal{C}$ e um homomorfismo $\varphi = \varphi_g : G \longrightarrow Q$ tal que $g^{\varphi} \neq 1$. Desde que $\mathcal{C}$ é fechada para subgrupos e $G/ker(\varphi) \cong Im(\varphi)$, temos que $ker(\varphi) \in \{N \trianglelefteq G; G/N \in \mathcal{C}\}$. Em outras palavras, $ker(\varphi)$ é um subgrupo normal de G que não contém g e cujo grupo quociente está em $\mathcal{C}$. Pela arbitrariedade da escolha de $1 \neq g \in G$, temos que $\bigcap\{N \trianglelefteq G; G/N \in \mathcal{C}\} = 1$.

Reciprocamente, suponha que $\bigcap\{N \trianglelefteq G; G/N \in \mathcal{C}\} = 1$. Então, para cada $1 \neq g \in G$ existe $N = N_g \trianglelefteq G$ tal que $G/N \in \mathcal{C}$ e $g \notin N$. Tomando $\varphi : G \longrightarrow G/N$ como sendo o homomorfismo canônico, vemos que g^{φ} é não trivial em G/N. Por definição, temos que G é residualmente–$\mathcal{C}$. □

O Teorema 3.1 mostra que na intenção de provar que um grupo G é residualmente–$\mathcal{C}$, às vezes, é conveniente trabalhar com a família de subgrupos normais definidas no seu enunciado. Assim, para cada grupo G iremos denotar por $\tau_{\mathcal{C}}(G)$ o conjunto $\{N \trianglelefteq G;\ G/N \in \mathcal{C}\}$.

Ao definirmos uma nova classe de grupos, no nosso caso, a classe dos grupos residualmente–$\mathcal{C}$, denotada por $r\mathcal{C}$, é natural desejar saber se esta classe é também fechada para subgrupos, imagens epimórficas e produtos diretos finitos. Desejamos responder estes três questionamentos no caso $r\mathcal{C}$ e trabalhamos neste sentido nos próximos parágrafos. O fechamento de $r\mathcal{C}$ para subgrupos é estabelecido a seguir.

Lema 3.2. *Se um grupo G é residualmente–$\mathcal{C}$, então H também o é para todo $H \leqslant G$.*

Demonstração. Sejam H um subgrupo arbitrário de G e $N \in \tau_{\mathcal{C}}(G)$. Então, $H \cap N \trianglelefteq H$ e, como $G/N \in \mathcal{C}$ e $H/H \cap N$ é isormofo a $HN/N \leqslant G/N$, temos que $H \cap N \in \tau_{\mathcal{C}}(H)$. Daí, segue-se que

$$\bigcap_{K \in \tau_{\mathcal{C}}(H)} K \subseteq \bigcap_{N \in \tau_{\mathcal{C}}(G)} (H \cap N).$$

Pelo Teorema 3.1, esta última intersecção deve ser trivial e portanto

$$\bigcap_{K\in\tau_{\mathcal{C}}(H)} K = 1.$$

Novamente pelo Teorema 3.1, temos que H é residualmente–$\mathcal{C}$. □

Iremos, agora, definir a classe dos grupos livres.

Definição 3.3. Sejam F um grupo e $X \subseteq F$. F é dito ser livre de base X se para toda função $f : X \longrightarrow G$, onde G é um grupo arbitrário, existe um único homomorfismo $\varphi : F \longrightarrow G$ tal que $\varphi|_X = f$. Dizemos que F é livre se existe um subconjunto X de F tal que F é livre com base X.

Note que por definição o grupo trivial é livre com base $X = \emptyset$ e que $(\mathbb{Z}, +)$ é livre com base $1 \in \mathbb{Z}$. A seguir mostramos como a partir de qualquer conjunto não vazio X é sempre possível construir um grupo F tendo X como um conjunto de geradores livres.

Seja X um conjunto arbitrário e não vazio. Definimos X^{-1} como sendo o conjunto das expressões formais x^{-1}, $x \in X$ e assim pomos $X^{\pm 1} := X \cup X^{-1}$. Por uma palavra em X de comprimento $n \geqslant 0$ entendemos uma justaposição de n elementos em $X^{\pm 1}$. Se $n = 0$ obtemos a palavra vazia, a qual denotamos por 1. Definimos igualdade de duas palavras em X do seguinte modo: se $u = x_1^{e_1} \dots x_n^{e_n}$ e $v = y_1^{d_1} \dots y_m^{d_m}$ são duas palavras em X, $n, m \geqslant 1$, então $u = v$ se e somente se $n = m$, $x_i = y_i$ e $e_i = d_i$ para todo $i = 1, \dots, n$.

Se $u = x_1^{e_1} \dots x_n^{e_n}$ é uma palavra em X, definimos uma subpalavra de X como sendo a palavra vazia ou uma palavra da forma $u = x_r^{e_r} \dots x_s^{e_s}$ onde $1 \leqslant r \leqslant s \leqslant n$. Ainda, definimos o inverso de u como sendo $u^{-1} = x_n^{-e_n} \dots x_1^{-e_1}$. Note então que $(u^{-1})^{-1} = u$.

Seja u uma palavra em X. Uma operação elementar é ou uma inserção ou um cancelamento em u de uma subpalavra da forma xx^{-1} onde $x \in X$. Por exemplo, se $u = xyy^{-1}z$, $x, y, z \in X$, então uma operação elementar é a troca de u por $w = aa^{-1}xyy^{-1}z$ onde $a \in X$. Outra operação elementar é o cancelamento da subpalavra yy^{-1} de u, obtendo-se portanto $w = xz$. Se w é qualquer palavra em X, escrevemos $w \longrightarrow w'$ para denotar que a palavra w' pode ser obtida de w por uma redução elementar.

Se u e v são duas palavras em X, dizemos que u e w são equivalentes, o que denotamos por $u \sim v$, se existem palavras $u = v_1, \dots, v_n = v$ tais que $u = v_1 \longrightarrow \cdots \longrightarrow v_n = v$. Claramente, $\sim$ é relação de equivalência em $W(X)$, onde $W(X)$ é o conjunto das palavras em X, e denotamos por $[u]$ a classe de equivalência da palavra u em X.

Lembramos que um semigrupo é qualquer conjunto munido de uma operação associativa e um monóide é um semigrupo com unidade. Se M_1, M_2 são quaisquer monóides e $f : M_1 \longrightarrow M_2$ é uma função, f é dita ser homomorfismo de monóides se para todos $g_1, g_2 \in M_1$ vale $(g_1 g_2)^f = g_1^f g_2^f$ e $1_{M_1}^f = 1_{M_2}$.

A prova do seguinte resultado pode ser encontrada em [27, pág. 300, Lema 5.70].

Lema 3.4. *Seja X um conjunto não vazio e $W(X)$ o conjunto das palavras em X. Então, $W(X)$ é um monóide com a operação de concatenação. Se $u,u',v,v' \in W(X)$ e $u \sim u'$ e $v \sim v'$, então $uv \sim u'v'$. Ainda, se G é um grupo arbitrário e $f : X \longrightarrow G$ é uma função, então a função $\psi : W(X) \longrightarrow G$ definida por $\psi(1_{W(X)}) = 1_G$ e $\psi : (x_1^{e_1} \dots x_n^{e_n}) \mapsto f(x_1)^{e_1} \dots f(x_n)^{e_n}$ é um homomorfismo de monóides tal que se u,u' são duas palavras em X e $u \sim u'$, então $\psi(u) = \psi(u')$.*

Uma palavra u em X é dita ser reduzida se u não possui uma subpalavra da forma xx^{-1} onde $x \in X^{\pm 1}$. Note que 1 é uma palavra reduzida. A prova do seguinte resultado pode ser encontrada em [27, pág. 301, Prop. 5.71].

Lema 3.5. *Seja X um conjunto não vazio e $W(X)$ o conjunto das palavras em X. Então, todo elemento em $W(X)$ é equivalente a uma única palavra reduzida.*

Teorema 3.6. *Seja X um conjunto não vazio e $F = \{[u]; u \in W(X)\}$. Então, F é um grupo com a operação $[u][v] = [uv]$ e F é livre com base X.*

Demonstração. Pelo Lema 3.4, temos que $[\cdot]$ é uma operação bem definida em F. Claramente $[1]$ é elemento neutro para $[\cdot]$ e para todo $[u] \in F$, $[u][u^{-1}] = [u^{-1}][u] = [1]$. Ainda, se $[u],[v],[w] \in F$, temos que $([u][v])[w] = [uv][w] = [(uv)w] = [u(vw)] = [u]([v][w])$. Portanto, F é um grupo. Ainda, se $w = x_1^{e_1} \dots x_n^{e_n}$ é uma palavra em X, então $[w] = [x_1]^{e_1} \dots [x_n]^{e_n}$ o que mostra que F é gerado por X, onde identificamos X com o conjunto $\{[x]; x \in X\}$. Notamos que pelo Lema 3.5, para todo $[u] \in F$, existe uma única palavra reduzida w tal que $[u] = [w]$. Se $f : X \longrightarrow G$ é uma função arbitrária, onde G é um grupo, defina $\varphi : F \longrightarrow G$ por $[x_1]^{e_1} \dots [x_n]^{e_n} \mapsto f(x_1)^{e_1} \dots f(x_n)^{e_n}$, onde $w = x_1^{e_1} \dots x_n^{e_n}$ é palavra reduzida em X. Pelo Lema 3.5, φ é bem definida, estende f e se w é uma palavra reduzida em X, $\varphi([w]) = \psi(w)$, onde ψ é a função definida no Lema 3.4. Sejam u,v,w palavras reduzidas em X e suponha que $uv \sim w$. Por um lado, desde que w é reduzida temos que $\varphi([u][v]) = \varphi([uv]) = \varphi([w]) = \psi(w)$. Por outro lado, desde que u e v são reduzidas, temos que $\varphi([u])\varphi([v]) = \psi(u)\psi(v) = \psi(uv)$. Pelo Lema 3.4 obtemos que $\varphi([u])\varphi([v]) = \psi(uv) = \psi(w) = \varphi([u][v])$. Isto mostra que φ é um homomorfismo e o resultado está verificado. □

Seja X um conjunto não vazio e F o grupo livre com base X construído no Teorema 3.6. Vimos que todo elemento de F é a classe de uma palavra reduzida em X. Assim, podemos observar os elementos de F como palavras reduzidas em X e, fazendo isto, a operação de F é a concatenação seguida de redução.

Sejam X_1 e X_2 dois conjuntos e $f : X_1 \longrightarrow X_2$ uma bijeção. Sejam F_1 e F_2 os grupos com base X_1 e X_2, respectivamente, construídos na prova do Teorema 3.6. Nós podemos observar f tendo

F_2 como contra-domínio e então existe um único homomorfismo $\varphi_1 : F_1 \longrightarrow F_2$ estendendo f. Analogamente, existe um único homomorfismo $\varphi_2 : F_2 \longrightarrow F_1$ estendendo f^{-1}. É fácil ver que $\varphi_2 = (\varphi_1)^{-1}$ e portanto F_1 e F_2 são isomorfos. Então, se $X_1 = X = X_2$, temos que todos os grupos livres com base X são mutuamente isomorfos. Em particular, todo grupo livre com base X é gerado por X.

No que segue, provamos que todo grupo livre é residualmente–p para qualquer primo p. Pelo Teorema 3.6, obtemos portanto uma vasta classe de grupos residualmente–p.

Teorema 3.7. *Sejam F um grupo livre e p um número primo. Então F é residualmente–p.*

Demonstração. Suponha que F é livre com base $\emptyset \neq X \subseteq F$. Então, todo elemento de F é uma palavra reduzida em X. Assim, se $1 \neq w \in F$, existem inteiros $r, q, i_1, \ldots, i_r, m_1, \ldots, m_r$ e $x_{i_1}, \ldots, x_{i_r} \in X$ de modo que $1 \leqslant q \leqslant r$, $\{i_1, \ldots, i_r\} = \{1, \ldots, q\}$ e $x_{i_u} \neq x_{i_{u+1}}$ para todos $u = 1, \ldots, r-1$ e $w = x_{i_1}^{m_1} \ldots x_{i_r}^{m_r}$.

Escolha n um inteiro positivo suficientemente grande de modo que $p^n \nmid m_1 \ldots m_r$ e seja R o anel das matrizes $(r+1) \times (r+1)$ sobre $\mathbb{Z}_{p^n}$. Considere G como sendo o conjunto das matrizes superiores de R cujos elementos na diagonal principal são iguais a 1. Então, como tais matrizes têm determinante 1, G é grupo com a multiplicação de R. Mais do que isto, $|G| = p^{\frac{nr(r+1)}{2}}$ e G é um p–grupo finito.

Pela arbitrariedade da escolha de $1 \neq w \in F$, o resultado estará verificado se encontrarmos um homomorfismo $\varphi = \varphi_w : F \longrightarrow G$ tal que $w^\varphi \neq 1$.

Para cada $1 \leqslant u, v \leqslant r+1$, seja $E_{uv} = [a_{ij}]$ a matriz de R dada por $a_{ij} = 0$ se $(i, j) \neq (u, v)$ e $a_{ij} = 1$ se $(i, j) = (u, v)$. Então sabemos que dados $1 \leqslant u, v, s, t \leqslant r+1$ vale que $E_{uv}E_{st} = E_{ut}$ se $v = s$ e $E_{uv}E_{st} = 0$ se $v \neq s$.

Seja $1 \leqslant j \leqslant q$ fixado. Se $i_u = i_v = j$, temos que $u \neq v+1$ e $v \neq u+1$. Assim, temos que $(1 + E_{u(u+1)})(1 + E_{v(v+1)}) = 1 + E_{u(u+1)} + E_{v(v+1)} = (1 + E_{v(v+1)})(1 + E_{u(u+1)})$. Portanto, fica bem definido o elemento

$$g_j = \prod_{i_u = j} (1 + E_{u(u+1)}).$$

Note que para cada $l \in \mathbb{Z}$ vale

$$g_j^l = 1 + l \sum_{i_u = j} E_{u(u+1)}.$$

Considere $g = g_{i_1}^{m_1} \ldots g_{i_r}^{m_r}$. Dado que $g_j \in G$ para cada $j = 1, \ldots, q$, temos que g é um elemento do grupo G.

Ainda, como

$$g = g_{i_1}^{m_1} \dots g_{i_r}^{m_r} = \Big(1 + m_1 \sum_{i_u = i_1} E_{u(u+1)}\Big) \dots \Big(1 + m_r \sum_{i_u = i_r} E_{u(u+1)}\Big),$$

na expansão de g ocorre o termo $E_{1(r+1)}$ com coeficiente $m_1 \dots m_r$, que é não trivial em $\mathbb{Z}_{p^n}$. Isto mostra que $g \neq 1_G$.

Seja $f : X \longrightarrow G$ a função definida do seguinte modo: $x_{i_u}^f = g_{i_u}$ para todo $u = 1, \dots, r$ e $x^f = 1$ para todos os demais x em X. Então, existe um único homomorfismo $\varphi : F \longrightarrow G$ que estende a função f. Finalmente, temos que $w^\varphi = (x_{i_1}^{m_1} \dots x_{i_r}^{m_r})^\varphi = g_{i_1}^{m_1} \dots g_{i_r}^{m_r} = g \neq 1_G$. O resultado está, portanto, verificado. □

Se G é um grupo arbitrário, podemos considerar F o grupo livremente gerado pelos elementos de G. Tomando a função identidade de G, obtemos um único homomorfismo de F em G que estende tal função. Este homomorfismo deve ser sobrejetor e, sendo assim, G é quociente de F. Isto mostra que todo grupo é quociente de algum grupo livre.

Suponha que $\mathcal{C}$ seja a classe dos grupos finitos. Um grupo residualmente–$\mathcal{C}$ é chamado residualmente finito. As considerações do último parágrafo e a existência de grupos infinitos simples mostram que a classe dos grupos residualmente finitos não é fechada para imagens epimórficas. Um exemplo de grupo infinito simples é obtido por G. Higman em [10]. Neste artigo, G. Higman constrói um grupo finitamente gerado G que não possui subgrupos normais próprios de índice finito. Mais especificamente, G é um grupo gerado por elementos a, b, c, d e valem em G as seguintes relações $a^{-1}ba = b^2$, $b^{-1}cb = c^2$, $c^{-1}dc = d^2, d^{-1}ad = a^2$. Como todo grupo finitamente gerado possui pelo menos um subgrupo normal maximal, a partir de G podemos obter um grupo infinito, finitamente gerado e simples.

Seja $\mathcal{C}'$ uma classe de grupos finitos fechada para subgrupos, imagens epimórficas e produtos diretos finitos. Suponha que todo grupo na classe $\mathcal{C}$ é também um grupo na classe $\mathcal{C}'$. Então um grupo residualmente–$\mathcal{C}$ é também residualmente–$\mathcal{C}'$. Ora, desde que todo p–grupo finito, p um primo, é nilpotente e todo grupo nilpotente é solúvel, temos que a classe dos grupos residualmente–$\mathcal{C}$ não é fechada para imagens epimórficas sendo $\mathcal{C}$ a classe dos p–grupos finitos, a classe dos grupos finitos nilpotentes ou a classe dos grupos finitos solúveis. Para finalizar esta seção, respondemos afirmativamente nossa última pergunta.

Teorema 3.8. *A classe r$\mathcal{C}$ é fechada para produtos diretos finitos.*

Demonstração. Sejam $G_1, \dots, G_m$ grupos residualmente–$\mathcal{C}$. Se $g = (g_1, \dots, g_m) \in G := G_1 \times \cdots \times G_m$ é um elemento não trivial, existe $i \in \{1, \dots, m\}$ tal que $g_i \neq 1_{G_i}$. Desde que G_i é residualmente–$\mathcal{C}$, existe $N_i = N_{g_i} \trianglelefteq G_i$ de modo que $g_i \notin N_i$ e $G_i/N_i \in \mathcal{C}$. Segue-se que $g \notin K := G_1 \times \cdots \times G_{i-1} \times N_i \times \cdots \times G_m$ e $G_1 \times \cdots \times G_i \times \cdots G_n/K \cong G_i/N_i \in \mathcal{C}$. □

3.2 O Teorema de Zelmanov

Em toda esta seção, p denota um primo fixado e $\mathcal{C}_p$ denota a classe dos p–grupos finitos.

Um grupo G que é residualmente–p pode, naturalmente, não ser um p–grupo (vide a classe dos grupos livres). Isto não ocorre, entretanto, se G for de torção, como estabelece o próximo resultado.

Lema 3.9. *Se G é um grupo de torção residualmente–p, então G é um p–grupo.*

Demonstração. Suponha que G não é um p–grupo. Então, existe $1 \neq g \in G$ que não é um p–elemento. Como G é de torção, g tem ordem finita e, assim, podemos supor sem perda de generalidade que $|g| = q$, q um primo diferente de p. Seja $N \in \tau_{\mathcal{C}_p}(G)$, então G/N é um p–grupo finito e por isso $g \in N$. Pela arbitrariedade de escolha de $N \in \tau_{\mathcal{C}_p}(G)$ e o fato de ser G um grupo residualmente–p, temos que $g = 1$, uma contradição. □

Seja G um grupo de torção e suponha que as ordens dos elementos de G são limitadas por um inteiro positivo n. Neste caso dizemos que G têm expoente finito e o mínimo múltiplo comum das ordens dos elementos de G é chamado o expoente de G, que é denotado por $exp(G)$. Note que claramente todo grupo finito G tem expoente finito. Mais do que isto, $exp(G)$ é o produto dos expoentes dos subgrupos de Sylow de G.

Lembramos que para cada inteiro positivo i e para todo grupo G, $D_i(G)$ denota o i–ésimo termo da série de Jennings–Lazard–Zassenhaus de G associado ao primo p. O seguinte resultado nos mostra uma propriedade particular de grupos residualmente–p.

Lema 3.10. *Seja G um grupo residualmente–p. Então, $D_\infty(G) := \bigcap_{i \geqslant 1} D_i(G) = 1$.*

Demonstração. Seja G um grupo arbitrário e $N \trianglelefteq G$. Pelo Lema 2.25, sabemos que $D_i(G/N) = D_i(G)N/N$ para todo inteiro positivo i.

Suponha, então, que G é residualmente–p e seja $N \in \tau_{\mathcal{C}_p}(G)$. Temos que G/N é um p–grupo finito e, pelo Teorema 1.17 obtemos que G/N é um grupo nilpotente. Assim, se c e p^e denotam, respectivamente, a classe de nilpotência e o expoente de G/N, temos que $D_{cp^e}(G/N) = 1$. Segue que $D_{cp^e}(G) \leqslant N$ e, em particular, $D_\infty(G) \leqslant N$. Pela arbitrariedade da escolha de $N \in \tau_{\mathcal{C}_p}(G)$ e o fato de G ser residualmente–p, obtemos que $D_\infty(G) = 1$. □

O Lema 3.10 mostra que a série de Jennings–Lazard–Zassenhaus, associada ao primo p, de um grupo residualmente–p é muito útil no seguinte sentido: Seja G um grupo residualmente–p e suponha que desejemos provar que, sobre algumas suposições a mais convenientes, G é finito. Uma ideia, então, é mostrar que nas condições impostas a ordem dos quocientes $|G/D_i(G)|$, i um número inteiro positivo, é limitada superiormente por uma função que não

depende de i. Neste caso, deve existir i tal que $D_i(G) = D_{i+k}(G)$ para todo inteiro positivo k e, consequentemente, $D_i(G) = D_\infty(G)$. Pelo lema anterior, concluímos que $D_i(G) = 1$ e G é finito. Dadas estas observações, provamos o seguinte resultado.

Teorema 3.11. *([31, Proposição 2.11]) Seja G um grupo gerado pelos elementos $g_1, \ldots, g_m$ e tal que a álgebra $L_p(G)$ é nilpotente de classe no máximo c. Seja $\rho_1, \ldots, \rho_s$ a lista de todos os comutadores simples de peso menor ou igual a c com entradas em $\{g_1, \ldots, g_m\}$. Então, para qualquer inteiro não negativo i, G pode ser escrito como produto*

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

dos subgrupos cíclicos gerados por $\rho_1, \ldots, \rho_s$ e o subgrupo $D_{i+1}(G)$.

Demonstração. Primeiramente, como $G = \langle g_1, \ldots, g_m \rangle$, para cada inteiro não negativo i pode-se verificar, utilizando as identidades do Teorema 1.14 e do Lema 2.28, que $D_i(G) = \langle [b_1, \ldots, b_j]^{p^k}, D_{i+1}(G);\ jp^k \geqslant i,\ b_1, \ldots, b_j \in \{g_1, \ldots, g_m\} \rangle$.

A prova é por indução em i. Assumindo que $i \geqslant 0$ e $G = \langle \rho_1 \rangle \cdots \langle \rho_s \rangle D_{i+1}(G)$, iremos provar que $G = \langle \rho_1 \rangle \cdots \langle \rho_s \rangle D_{i+2}(G)$.

Desde que $L_p(G)$ é nilpotente de classe no máximo c, pelo Lema 2.19, sabemos que $\gamma_{c+1}(L_p(G)) = 0$ e todo comutador simples de peso maior ou igual a $c+1$, em $L_p(G)$, é trivial. Em particular, dados $b_1, \ldots, b_{c+1} \in G$, em $L_p(G)$ vale $[b_1 D_2(G), \ldots, b_{c+1} D_2(G)] = [b_1, \ldots, b_{c+1}] D_{c+2}(G) = 0$, isso é, $[b_1, \ldots, b_{c+1}] \in D_{c+2}(G)$. Pelo Teorema 1.20, obtemos que $\gamma_{c+1}(G) \leq D_{c+2}(G)$. Mais do que isto, para todo $d \geqslant c+1$, temos que $\gamma_d(G) \leq D_{d+1}(G)$.

Por hipótese, temos que $G = \langle \rho_1 \rangle \cdots \langle \rho_s \rangle D_{i+1}(G)$. Então, dado $g \in G$, podemos escrever

$$g = \rho_1^{\alpha_1} \ldots \rho_s^{\alpha_s} z$$

onde cada $\alpha_r \in \mathbb{Z}$ e $z \in D_{i+1}(G)$. Por outro lado, pelas considerações iniciais, podemos escrever

$$z = (w_1^{p^{k_1}})^{\beta_1} \ldots (w_l^{p^{k_l}})^{\beta_l} y$$

onde cada $\beta_n \in \mathbb{Z}$ e cada w_n é um comutador simples, com entradas em $\{g_1, \ldots, g_m\}$, de peso j_n e $j_n p^{k_n} \geqslant i+1$ e $y \in D_{i+2}$. Seja $n \in \{1, \ldots, l\}$. Se $j_n \leqslant c$ temos que $w_n \in \{\rho_1, \ldots, \rho_s\}$. Por outro lado, se $j_n \geqslant c+1$ obtemos que $w_n^{p^{k_n}} \in \gamma_{j_n}(G)^{p^{k_n}} \leq D_{j_n+1}(G)^{p^{k_n}} \leq D_{(j_n+1)p^{k_n}}(G) \leq D_{i+2}(G)$.

Finalmente, desde que $g = \rho_1^{\alpha_1} \ldots \rho_s^{\alpha_s} z = \rho_1^{\alpha_1} \ldots \rho_s^{\alpha_s} (w_1^{p^{k_1}})^{\beta_1} \ldots (w_l^{p^{k_l}})^{\beta_l} y$, resta-nos observar que $D_{i+1}(G)/D_{i+2}(G)$ é subgrupo do centro de $D_i(G)/D_{i+2}(G)$. Portanto,

$$g \in \langle \rho_1 \rangle \cdots \langle \rho_s \rangle D_{i+2}(G)$$

e o resultado está verificado. □

O seguinte teorema é o conteúdo principal da celebrada solução dada por E. Zelmanov em 1989 ao Problema Restrito de Burnside, solução esta que o fez receber uma medalha Fields em 1994. O Problema Restrito de Burnside é o questionamento se é verdade que todo grupo finito gerado por n elementos e de expoente m tem ordem limitada superiormente por uma função de m e n. Pela densidade deste resultado, não podemos dar uma demonstração completa nesta dissertação. Contudo, daremos em linhas gerais a ideia de sua prova.

Teorema 3.12. *Seja L uma álgebra de Lie sobre um corpo $\mathbb{F}$ de característica $p > 0$ gerada pelos elementos $l_1, \ldots, l_n$. Assuma que*

1. *todo comutador em $l_1, \ldots, l_n$ é ad–nilpotente;*

2. *L satisfaz uma identidade polinomial.*

Nessas condições, L é nilpotente.

Seja L uma álgebra de Lie sobre um corpo $\mathbb{F}$ de característica positiva p. Suponha que L é gerada pelos elementos $l_1, \ldots, l_n$, todo comutador nestes elementos é ad–nilpotente e que L satisfaz uma identidade polinomial não trivial. Então, podemos assumir que L satisfaz uma identidade multilinear. Seja K a $\mathbb{F}$–álgebra gerada pelos elementos $e_1, e_2, \ldots$, e com as relações $e_i^2 = 0$ e $e_i e_j = e_j e_i$ para todos $i, j \in \mathbb{N}^*$. Desde que L satisfaz uma identidade multilinear, temos que $\overline{L} = L \otimes_{\mathbb{F}} \mathbb{K}$ satisfaz uma identidade multilinear.

Seja F um corpo infinito de característica p e suponha que $\mathbb{F} \subseteq F$. Desde que $\overline{L}$ satisfaz uma identidade multilinear, temos que $\overline{L} \otimes_{\mathbb{F}} F$ também satisfaz uma identidade multilinear. Estas considerações mostram que podemos assumir que $\mathbb{F}$ é um corpo infinito.

Seja A uma qualquer álgebra de Lie. Um elemento $a \in A$ é dito um elemento *sanduíche* se para todos $x, y \in A$ vale $[x,a,a] = 0 = [x,a,y,a]$. Ainda, A é dita ser localmente nilpotente se toda subálgebra finitamente gerada de A é nilpotente. O seguinte teorema foi provado em [16] por A.I. Kostrikin e E.I. Zelmanov.

Teorema 3.13. *Seja A uma álgebra de Lie sobre um corpo de característica p. Se A é gerada por uma família de elementos sanduíches, então A é localmente nilpotente.*

Ainda, o seguinte resultado foi provado em [15] por A.I. Kostrikin.

Teorema 3.14. *Seja A uma álgebra de Lie satisfazendo uma identidade polinomial. Então, A possui um único ideal maximal localmente nilpotente, denotado por $Loc(A)$. Mais do que isto, $A/Loc(A)$ não possui nenhum ideal localmente nilpotente não nulo.*

Os Teoremas 3.13 e 3.14 sugerem o seguinte esboço de prova para o Teorema 3.12: Desde que L satisfaz uma identidade polinomial, temos pelo Teorema 3.14 que L possui um único ideal maximal localmente nilpotente, a saber $Loc(L)$, e $L/Loc(L)$ não possui qualquer ideal não nulo localmente nilpotente. Note que $L/Loc(L)$ satisfaz as mesmas condições de L no Teorema 3.12. Se $Loc(L) = L$, desde que L é finitamente gerada, obtemos que L é nilpotente. Podemos então assumir que $Loc(L) \neq L$. Neste caso, desde que $L/Loc(L)$ não possui ideais não nulos localmente nilpotentes, podemos assumir que $Loc(L) = 0$ e L não possui ideais não nulos localmente nilpotentes.

Suponha que seja possível encontrar um polinômio $f = f(x_1, \ldots, x_r)$ não identicamente nulo em L e tal que para todos $l_1, \ldots, l_r \in L$, $f(l_1, \ldots, l_r)$ é um elemento sanduíche. Desde que $\mathbb{F}$ é infinito, o subespaço I de L gerado pelo conjunto $f(L) = \{f(l_1, \ldots, l_r);\ l_1, \ldots, l_r \in L\}$ é um ideal de L. Contudo, pelo Teorema 3.13, temos que I é localmente nilpotente, uma contradição.

Dadas essas considerações, podemos enfim provar o principal resultado desta seção.

Teorema 3.15. *([37, pág. 572, Teorema 1.6]) Seja G um grupo de torção finitamente gerado e residualmente–p. Então se $L_p(G)$ satisfaz uma identidade polinomial, G é finito.*

Demonstração. Seja G um grupo de torção gerado pelos elementos $g_1, \ldots, g_m$. Suponha que G é residualmente–p e que $L_p(G)$ satisfaz uma identidade polinomial. Pelo Lema 3.9, temos que G é p–grupo. Seja $w = w(x_1, \ldots, x_n)$ um comutador de grupo no grupo livremente gerado por $X := \{x_1, \ldots, x_n\}$ e $\overline{w}$ o correspondente comutador de Lie na álgebra de Lie livremente gerada por X. Se $h_1, \ldots, h_n \in G$ então $w(h_1, \ldots, h_n)$ tem ordem finita. Para cada $i = 1, \ldots, n$ denotando por $\overline{h_i}$ o elemento $h_i D_2 \in L_p(G)$, pelo Teorema 2.23, temos que $\overline{w}(\overline{h_1}, \ldots, \overline{h_n})$ é ad–nilpotente.

Desde que $L_p(G)$ por definição é a subálgebra de $L(G) = \bigoplus_{i \geqslant 1} D_i(G)/D_{i+1}(G)$ gerada por $D_1(G)/D_2(G)$ e $G = \langle g_1, \ldots, g_m \rangle$, temos que $L_p(G) = \langle g_1 D_2(G), \ldots, g_m D_2(G) \rangle$ é finitamente gerada por elementos nos quais todo comutador é ad–nilpotente. Assim, $L_p(G)$ satisfaz as condições do Teorema 3.12 e, portanto, é nilpotente.

Pelo Teorema 3.11, sendo c a classe de nilpotência de $L_p(G)$, temos que para todo $i \geqslant 1$ vale

$$G = \langle \rho_1 \rangle \cdots \langle \rho_s \rangle D_i(G) \tag{3.1}$$

onde $\rho_1, \ldots, \rho_s$ são todos os comutadores simples de peso menor ou igual a c com entradas no conjunto $\{g_1, \ldots, g_m\}$.

Se $l \geqslant 2$ é arbitrário, o número de comutadores simples de peso exatamente l com entradas no conjunto $\{g_1, \ldots, g_m\}$ é $(m-1)m^{l-1}$. Segue-se que, para todo $l \geqslant 1$, o número de comutadores simples com entradas em $\{g_1, \ldots, g_m\}$ de peso no máximo l é $m + (m-1)m + (m-1)m^2 + \cdots + (m-1)m^{l-1} = m^l$. Isto mostra que $s = m^c$.

Como G é grupo de torção, podemos considerar k como sendo a maior ordem de um elemento no conjunto $\{\rho_1,\ldots,\rho_s\}$. Assim, pela igualdade em (3.1), para todo inteiro positivo i vale

$$|G/D_i(G)| \leqslant k^{m^c}. \tag{3.2}$$

Da desigualdade em (3.2), temos que existe $i_0 \in \mathbb{N}$ tal que $D_{i_0}(G) = D_{i_0+n}(G)$ para todo natural n e, em particular, temos que $D_{i_0}(G) = D_\infty(G)$.

Como G é residualmente–p, pelo Lema 3.10 temos que $D_\infty(G) = 1$. A desigualdade em (3.2) e o fato que $D_{i_0}(G) = D_\infty(G)$ implica que $|G| \leqslant k^{m^c}$, isso é, G é finito. O teorema está demonstrado. □

3.3 Sobre identidades em álgebras de Lie graduadas

Sejam G um grupo e L uma álgebra de Lie sobre um anel associativo comutativo e unitário R. Dizemos que G age em L via automorfismos de R–álgebras de Lie se para cada $g \in G$ e $l \in L$ existe um elemento bem determinado $l^g \in L$ de modo que para todos $g,h \in G$ e $l \in L$ vale $l^{gh} = (l^g)^h$ e a aplicação $l \mapsto l^g$ é um homomorfismo de R–álgebras de Lie de L. Neste caso, o conjunto $C_L(G) := \{l \in L; l^g = l \ \forall\ g \in G\}$ é chamado o centralizador de G em L. Note que $C_L(G)$ é uma R–subálgebra de Lie de L.

Nesta seção temos por objetivo provar o seguinte resultado fundamental provado em [1] por Y.A. Bahturin e M.V. Zaicev.

Teorema 3.16. *Sejam $\mathbb{F}$ um corpo arbitrário e L uma álgebra de Lie sobre $\mathbb{F}$. Suponha que L seja agida por um grupo finito solúvel G e que a característica de $\mathbb{F}$ não divida a ordem de G. Nestas condições, se a subálgebra dos pontos fixos $C_L(G)$ satisfaz uma identidade polinomial, então L também satisfaz uma identidade polinomial.*

Observamos que satisfazer uma identidade polinomial é uma condição essencial para que possamos utilizar o Teorema 3.15. O Teorema 3.16 é, portanto, crucial aos nossos objetivos pois nos fornece uma condição suficiente para que uma álgebra de Lie satisfaça uma identidade polinomial.

Definição 3.17. Sejam S um semigrupo com unidade e R um anel associativo comutativo e com unidade. Uma álgebra A sobre R é chamada S–graduada se para cada elemento g no semigrupo S existe um R–submódulo de A, denotado por A_g, de modo que para todos $g,h \in S$ vale $A_gA_h \subseteq A_{gh}$ e

$$A = \sum_{g\in S} A_g.$$

Neste caso, para cada $g \in S$, A_g é chamado uma componente homogênea de A.

Note que, na definição acima, como S tem unidade, o R–submódulo A_1 é subálgebra de A. Sejam S um semigrupo com unidade, R um anel comutativo com unidade e A uma R–álgebra S–graduada. Um elemento arbitrário não nulo no R–submódulo A_g, $g \in S$, é chamado um elemento homogêneo de grau g. Nós dizemos que A tem S–graduação finita se existe um número finito de elementos g em S tais que $A_g \neq 0$. Assim, A tem graduação finita se, e somente se, existe um subconjunto finito H de S tal que sempre que $A_g \neq 0$ temos que $g \in H$. Neste último caso podemos supor sem perda de generalidade que $1 \in H$. De fato, se $1 \notin H$, basta-nos considerar $H' = H \cup \{1\}$.

A seguir, damos dois exemplos de álgebras graduadas.

Exemplo 3.18. Considere $S = \mathbb{N}$ o semigrupo aditivo dos inteiros não negativos e R um anel associativo comutativo e com unidade. Sejam s um inteiro positivo e $A := R[x_1, \ldots, x_s]$ o anel dos polinômios em s variáveis $\{x_1, \ldots, x_s\}$ comutativas e associativas sobre R. Então, sabemos que A é uma R–álgebra. Dado $n \geqslant 1$, dizemos que um monômio $x_1^{\alpha_1} \ldots x_s^{\alpha_s}$ é de grau n se $\alpha_1 + \cdots + \alpha_s = n$. Seja $n \in \mathbb{N}$. Se $n = 0$, então pomos $A_n = 0$ e, se $n \neq 0$, A_n denota o R–submódulo de A gerado pelos monômios de grau n. Ora, se $n, m \neq 0$ e f, g são dois monômios em A de graus n e m, respectivamente, então temos que fg é um monômio de grau $n+m$. Segue-se que A é a soma dos R–submódulos A_n com $n \in \mathbb{N}$ e para todos $n, m \in \mathbb{N}$ vale $A_n A_m \subseteq A_{n+m}$. Isto mostra que A é uma R–álgebra $\mathbb{N}$–graduada.

Exemplo 3.19. Sejam S um semigrupo e R um anel associativo comutativo e com unidade. Para cada $g \in S$ nós consideramos um conjunto enumerável $Z_g := \{z_1^g, z_2^g, \ldots, z_i^g, \ldots\}$. Então, considere Z a união de todos os conjuntos Z_g com $g \in S$ e $R(Z)$ a R–álgebra livre não associativa gerada por Z, definida no Capítulo 3. Vamos mostrar que $R(Z)$ admite uma S–graduação.

Para cada $g \in S$ e todo número inteiro positivo i escrevemos $|z_i^g| = g$. Assim, se $w = z_{i_1}^{g_1} \ldots z_{i_n}^{g_n}$ é um monômio em Z de tamanho $n \geqslant 1$, definimos $|w| = |z_{i_1}^{g_1}| \ldots |z_{i_n}^{g_n}| = g_1 \ldots g_n \in S$. Então, para cada $g \in S$, seja $R(Z)_g = {}_+\langle w;\ w \text{ é monômio em } Z \text{ e } |w| = g \rangle$.

Desde que a cada monômio em $R(Z)$ foi associado um "peso", temos que

$$R(Z) = \sum_{g \in S} R(Z)_g.$$

Mais do que isto, se w_1 e w_2 são dois monômios em Z, é fácil ver que $|w_1 w_2| = |w_1| \cdot |w_2|$. Assim, para quaisquer elementos g e h em S vale $R(Z)_g R(Z)_h \subseteq R(Z)_{gh}$. Concluimos, assim, que $R(Z)$ é S–graduada.

A partir de agora, nesta seção, denotaremos por S um semigrupo arbitrário com unidade e $\mathbb{F}$ um corpo, também, arbitrário. Ainda, denotaremos por $F(Z)$ a $\mathbb{F}$–álgebra livre gerada por Z definida no Exemplo 3.19.

Definição 3.20. Sejam A uma $\mathbb{F}$–álgebra S–graduada e $f = f(z_{i_1}^{g_1}, \ldots, z_{i_n}^{g_n}) \in F(Z)$. Dizemos que o polinômio f é dito uma identidade graduada em A se

$$f(a_1, \ldots, a_n) = 0$$

para todos $a_1, \ldots, a_n \in A$ tais que $a_r \in A_{g_r}$, $r = 1, \ldots, n$.

Definição 3.21. Sejam A e B duas $\mathbb{F}$–álgebras S–graduadas. Um homomorfismo $\varphi : A \longrightarrow B$ é chamado S–graduado se para cada $g \in S$ vale $A_g^{\varphi} \subseteq B_g$. Assim, podemos definir para toda $\mathbb{F}$–álgebra S–graduada A o conjunto

$$T^G(A) = \{f \in F(Z);\ f^{\varphi} = 0 \text{ para todo homomorfismo } S\text{–graduado } \varphi : F(Z) \longrightarrow A\}.$$

Dada A uma $\mathbb{F}$–álgebra S–graduada, o próximo lema nos diz que $T^S(A)$ é um ideal de $F(Z)$ e também caracteriza $T^S(A)$ como o conjunto das identidades graduadas de A.

Lema 3.22. *Seja A uma $\mathbb{F}$–álgebra S–graduada. Então, $T^S(A)$ é um ideal de $F(Z)$ e um elemento $f \in F(Z)$ é uma identidade graduada em A se, e somente se, $f \in T^S(A)$.*

Demonstração. A primeira afirmação sobre $T^S(A)$ decorre imediatamente da definição de $T^S(A)$ e de homomorfismos de álgebras. Então, provamos a segunda afirmação.

Suponha, inicialmente, que $f = f(z_{i_1}^{g_1}, \ldots, z_{i_n}^{g_n})$ seja uma identidade graduada em A. Consideremos um homomorfismo S–graduado φ de $F(Z)$ em A. Então temos que $(z_{i_r}^{g_r})^{\varphi} \in A_{g_r}$ com $r = 1, \ldots, n$. Segue que

$$f^{\varphi} = f((z_{i_1}^{g_1})^{\varphi}, \ldots, (z_{i_n}^{g_n})^{\varphi}) = 0.$$

Portanto, a arbitrariedade da escolha do homomorfismo S–graduado $\varphi : F(Z) \longrightarrow A$ mostra que $f \in T^S(A)$.

Reciprocamente, suponha que $f = f(z_{i_1}^{g_1}, \ldots, z_{i_n}^{g_n})$ seja anulado por todos os homomorfismos S–graduados $\varphi : F(Z) \longrightarrow A$. Sejam $a_1, \ldots, a_n \in A$ e suponha que $a_r \in A_{g_r}$ com $r = 1, \ldots, n$. Definimos a função $\overline{\varphi} : Z \longrightarrow A$ como segue: para todo $r = 1, \ldots, n$ pomos $(z_{i_r}^{g_r})^{\overline{\varphi}} = a_r$ e $z^{\overline{\varphi}} = 0$ para todos os demais z em Z. Então, $\overline{\varphi}$ estende-se de modo único a um homomorfismo $\varphi : F(Z) \longrightarrow A$ que satisfaz $\varphi|_Z = \overline{\varphi}$. Desde que A é S–graduada, pela definição de $\overline{\varphi}$ temos que φ é S–graduado. Segue por hipótese que $f^{\varphi} = 0$, isso é, $f(a_1, \ldots, a_n) = 0$. Da arbitrariedade da escolha de $a_r \in A_{g_r}$, $r = 1, \ldots, n$, temos que f é identidade graduada em A. □

Suponha agora que H seja um subconjunto finito de S. Então, para cada inteiro positivo i, defina

$$x_i = \sum_{g \in H} z_i^g.$$

Definindo $X = \{x_i;\ i \geqslant 1\}$, podemos considerar $F(X)$ a subálgebra de $F(Z)$ gerada pelo conjunto X. Pelo seguinte teorema provado em [17] por A. G. Kurosh, temos que $F(X)$ é álgebra livre.

Teorema 3.23 (A. G. Kurosh)**.** *Seja $\mathbb{F}$ um corpo e A uma álgebra não associativa livre sobre $\mathbb{F}$. Então, toda subálgebra de A é livre não associativa sobre $\mathbb{F}$.*

Seja n um inteiro positivo fixo. Então, escrevemos V_n para denotar o subespaço de $F(X)$ gerado por todos os produtos da forma $(x_{\sigma(1)} \dots x_{\sigma(n)})$, sendo considerados todos os possíveis rearranjamentos de parênteses, onde σ varia arbitrariamente no grupo simétrico S_n. Ainda, para cada $g = (g_1, \dots, g_n)$, onde $g_1, \dots, g_n \in H$, denotamos por V_n^g o subespaço de $F(Z)$ gerado por todos os produtos da forma

$$(z_{\sigma(1)}^{g_{\sigma(1)}} \cdots z_{\sigma(n)}^{g_{\sigma(n)}}),$$

onde novamente estamos considerando todos os possíveis rearranjamentos de parênteses e σ varia arbitrariamente no grupo S_n. Finalmente, definimos

$$V_n^S := \bigoplus_{g \in H^n} V_n^g.$$

Seja A uma $\mathbb{F}$–álgebra S–graduada e suponha que

$$A = \sum_{h \in H} A_h.$$

Ainda, seja $T(A)$ o ideal das identidades polinomiais de A em $F(X)$, introduzido no Capítulo 2. Definimos para cada $n \geqslant 1$

$$c_n(A) = dim\Big(\frac{V_n}{V_n \cap T(A)}\Big) \text{ e } c_n^S(A) = dim\Big(\frac{V_n^S}{V_n^S \cap T^S(A)}\Big).$$

Lema 3.24. *Nas condições anteriores vale $c_n(A) \leqslant c_n^S(A)$ para todo $n \geqslant 1$.*

Demonstração. Seja $n \geqslant 1$ fixado. Nós, inicialmente, afirmamos que $V_n \subseteq V_n^S$. Como H é finito, seja $H = \{h_1, \dots, h_s\}$. Assim, temos que $x_i = z_i^{h_1} + \cdots + z_i^{h_s}$ para todo $i \geqslant 1$. Sejam

$1 \leqslant i, j \leqslant n$. Note que

$$x_i x_j = (z_i^{h_1} + \cdots + z_i^{h_s})(z_j^{h_1} + \cdots + z_j^{h_s}) = \sum_{u,v=1}^{s} z_i^{h_u} z_j^{h_v}. \tag{3.3}$$

Seja $\sigma \in S_n$ um elemento arbitrário e $(x_{\sigma(1)} \ldots x_{\sigma(n)})$ um produto com ordenamento de parênteses arbitrário mas fixado. De (3.3), temos que $(x_{\sigma(1)} \ldots x_{\sigma(n)})$ se decompõe numa soma de produtos da forma

$$(z_{\sigma(1)}^{g_{\sigma(1)}} \cdots z_{\sigma(n)}^{g_{\sigma(n)}}),$$

com estrutura de parêntesis exatamente igual à sua. Portanto, $(x_{\sigma(1)} \ldots x_{\sigma(n)}) \in V_n^S$ e, por definição de V_n, concluímos que $V_n \subseteq V_n^S$.

Ainda, mostremos que $T(A) \subseteq T^S(A)$. Seja $f \in T(A)$ e suponha, sem perda de generalidade, que $f = f(x_1, \ldots, x_m)$. Assim, para todo homomorfismo graduado $\varphi : F(Z) \longrightarrow A$ temos que

$$\begin{aligned} f^\varphi &= (f(x_1, \ldots, x_m))^\varphi = f(x_1^\varphi, \ldots, x_m^\varphi) \\ &= f((z_1^{h_1})^\varphi + \cdots + (z_1^{h_s})^\varphi, \ldots, (z_m^{h_1})^\varphi + \cdots + (z_m^{h_s})^\varphi) = 0, \end{aligned}$$

desde que $\varphi|_{F(X)} : F(X) \longrightarrow A$ é um homomorfismo. Temos pelo Lema 3.22 que $f \in T^S(A)$. A arbitrariedade da escolha de $f \in T(A)$ mostra, enfim, que $T(A) \subseteq T^S(A)$.

Ainda, afirmamos que $V_n \cap T(A) = V_n \cap T^S(A)$. De fato, seja $f \in V_n \cap T^S(A)$. Então, podemos escrever $f = f(x_1, \ldots, x_n)$ e para cada homomorfismo S–graduado $\varphi : F(Z) \longrightarrow A$ vale que $f^\varphi = 0$, desde que $f \in T^S(A)$. Como A é S–graduada e

$$A = \sum_{h \in H} A_h,$$

para cada $a_1, \ldots, a_n \in A$, podemos escrever

$$a_i = \sum_{j=1}^{s} a_i^{h_j},\ i = 1, \ldots, n$$

onde $a_i^{h_j} \in A_{h_j}$ para todo $j = 1, \ldots, s$. Definimos uma função $\overline{\varphi} : Z \longrightarrow A$ como segue: $(z_i^{h_j})^{\overline{\varphi}} = a_i^{h_j}$ com $i = 1, \ldots, n$ e $j = 1, \ldots, s$ e $z^{\overline{\varphi}} = 0$ para todos os demais $z \in Z$. Então, $\overline{\varphi}$ estende-se de modo único a um homomorfismo $\varphi : F(Z) \longrightarrow A$ que é, por definição de $\overline{\varphi}$, S–graduado e portanto $f^\varphi = f(a_1^{h_1} + \cdots + a_1^{h_s}, \ldots, a_n^{h_1} + \cdots + a_n^{h_s}) = f(a_1, \ldots, a_n) = 0$. Pela arbitrariedade da escolha de $a_1, \ldots, a_n \in A$, temos que $f \in T(A)$ e assim $V_n \cap T^S(A) \subseteq V_n \cap T(A)$. Como $T(A) \subseteq T^S(A)$, temos que $V_n \cap T(A) \subseteq V_n \cap T^S(A)$, isto mostra nossa última afirmação.

Das considerações acima, concluímos que

$$\begin{aligned} V_n/V_n\cap T(A) &= V_n/V_n\cap T^S(A) = V_n/V_n^S\cap V_n\cap T^S(A) \\ &\cong V_n+(V_n^S\cap T^S(A))/(V_n^S\cap T^S(A)) \subseteq V_n^S/V_n^S\cap T^S(A). \end{aligned}$$

Disto concluímos que $c_n(A)\leqslant c_n^S(A)$ e o lema está demonstrado. □

Para que possamos demonstrar o principal resultado provado em [1] por Y.A. Bahturin e M.V. Zaicev, iremos utilizar o próximo resultado cuja prova por ser muito técnica será omitida aqui, mas pode ser encontrada em [1, Lema 4]. No que segue, para qualquer grupo G, $G^{\#}$ denota o conjunto dos elementos não triviais de G.

Lema 3.25. *Seja A uma álgebra de Lie sobre o corpo $\mathbb{F}$ finitamente graduada por um grupo G. Suponha que a componente unitária A_1, que é subálgebra de A, satisfaz uma identidade polinomial não trivial da forma*

$$x_0x_1\ldots x_{d-1} \equiv \sum_{\sigma\in(S_{d-1})^{\#}} \alpha_\sigma x_0x_{\sigma(1)}\ldots x_{\sigma(d-1)} \tag{3.4}$$

onde cada produto acima é normalizado à esquerda e $\alpha_\sigma\in\mathbb{F}$ para todo $\sigma\in(S_{d-1})^{\#}$. Então, para todo número positivo b e n suficientemente grande, vale

$$c_n^G(A) < \frac{n!}{b^n}.$$

Podemos, então, demonstrar o principal teorema obtido em [1] por Y.A. Bahturin e M.V. Zaicev. A saber, o seguinte resultado.

Teorema 3.26. *Seja $A=\sum_{g\in G} A_g$ uma álgebra de Lie sobre o corpo $\mathbb{F}$ finitamente graduada por um grupo G. Se a componente homogênea A_1 satisfaz uma identidade não trivial como em (3.4), então também A satisfaz uma identidade não trivial como em (3.4).*

Demonstração. Tome $b=1$. Pelo Lema 3.25, para n suficientemente grande, temos que

$$c_n^G(A) < n!.$$

Segue pelo Lema 3.24 que $c_n(A)<n!$. Considerando V o subespaço de V_n gerado pelos produtos normados à esquerda $x_{\sigma(1)}\ldots x_{\sigma(n)}$, onde σ varia sobre o grupo simétrico S_n, temos que $dim(V)=n!$. Por outro lado, desde que

$$V/(V\cap T(A)) = V/(V\cap(V_n\cap T(A))) \cong V+(V_n\cap T(A))/(V_n\cap T(A)) \subseteq V_n/V_n\cap T(A),$$

temos que $dim(V/V\cap T(A)) < n!$. Concluímos portanto que $V\cap T(A)\neq 0$ e A satisfaz uma identidade não trivial como em (3.4). □

Antes de provarmos o resultado principal desta seção, precisamos de mais um resultado sobre automorfismos de álgebras de Lie.

Teorema 3.27. *Sejam $\mathbb{F}$ um corpo e L uma álgebra de Lie sobre $\mathbb{F}$. Seja φ um automorfismo de L de ordem n e ω uma n–ésima raiz primitiva da unidade. Considere $L^* = L\otimes\mathbb{F}[\omega]$ com estrutura de álgebra de Lie sobre $\mathbb{F}[\omega]$ e permita-nos escrever $\varphi = \varphi\otimes 1$. Para cada $i = 0,\ldots,n-1$, defina ${}^iL^* = \{l\in L^*; l^\varphi = \omega^i l\}$. Então valem as seguintes afirmações:*

(i) Para cada $i = 0,\ldots,n-1$, ${}^iL^*$ é um $\mathbb{F}[\omega]$–subespaço φ–invariante de L^*;

(ii) $[{}^iL^*, {}^jL^*] \subseteq {}^{i+j(modn)}L^*$ para todos $i, j = 0,\ldots,n-1$;

(iii) $H := {}^0L^* + \cdots + {}^{(n-1)}L^*$ é $\mathbb{F}[\omega]$–subálgebra φ–invariante de L^* e $nL^*\subseteq H$;

(iv) Se $char(\mathbb{F})\nmid n$, H é soma direta dos subespaços ${}^iL^*$, $i = 0,\ldots,n-1$, e $L^* = H$.

Demonstração.

(i) Seja $i\in\{0,\ldots,n-1\}$ fixado. Claramente, $0\in {}^iL^*$. Se $l_1, l_2\in {}^iL^*$ e $\lambda\in\mathbb{F}[\omega]$, temos que

$$(\lambda l_1 + l_2)^\varphi = \lambda l_1^\varphi + l_2^\varphi = \lambda\omega^i l_1 + \omega^i l_2 = \omega^i(\lambda l_1 + l_2).$$

Isto mostra que ${}^iL^*$ é um subespaço de L^*. A φ–invariância é devida ao fato de φ ser transformação linear de L^*.

(ii) Sejam $i, j\in\{0,\ldots,n-1\}$ fixados. Considere $l_i\in {}^iL^*$ e $l_j\in {}^jL^*$. Temos que

$$[l_i, l_j]^\varphi = [l_i^\varphi, l_j^\varphi] = [\omega^i l_i, \omega^j l_j] = \omega^{i+j}[l_i, l_j].$$

Isto mostra que $[l_i, l_j]\in {}^{i+j(modn)}L^*$. A arbitrariedade da escolha de $l_i\in {}^iL^*$ e $l_j\in {}^jL^*$ e a definição de $[{}^iL^*, {}^jL^*]$ mostram que $[{}^iL^*, {}^jL^*]\subseteq {}^{i+j(modn)}L^*$.

(iii) Sejam $h_1, h_2\in H$. Então, podemos escrever $h_1 = l_0^1 + \cdots + l_{n-1}^1$ e $h_2 = l_0^2 + \cdots + l_{n-1}^2$ onde $l_i^k\in {}^iL^*$, $k = 1,2$ e $i = 0,\ldots,n-1$. Pelo item anterior obtemos que

$$[h_1, h_2] = \left[\sum_{i=0}^{n-1} l_i^1, \sum_{j=0}^{n-1} l_j^2\right] = \sum_{i,j=0}^{n-1}[l_i^1, l_j^2]\in {}^0L^* + \cdots + {}^{(n-1)}L^* = H.$$

Isto mostra que H é $\mathbb{F}[\omega]$–subálgebra de L^*. Desde que H é soma de $\mathbb{F}[\omega]$–subespaços φ–invariantes, concluímos então que H é $\mathbb{F}[\omega]$–subálgebra φ–invariante. Vamos, agora, mostrar que $nL \subseteq H$.

Seja $l \in L^*$ um elemento fixado. Para todo $i \in \{0,\ldots,n-1\}$ defina

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

Note que para cada $i \in \{0,\ldots,n-1\}$ vale

$$\begin{aligned} l_i^{\varphi} &= \left(\sum_{s=0}^{n-1} \omega^{-is} l^{\varphi^s}\right)^{\varphi} = \sum_{s=0}^{n-1} \omega^{-is} l^{\varphi^{s+1}} = \sum_{s=0}^{n-1} \omega^{i}\omega^{-i}\omega^{-is} l^{\varphi^{s+1}} \qquad (3.5)\\ &= \omega^i \sum_{s=0}^{n-1} \omega^{-i(s+1)} l^{\varphi^{s+1}}. \qquad (3.6) \end{aligned}$$

Fazendo $t = s+1$ em (3.5), temos que

$$l_i^{\varphi} = \omega^i \sum_{s=0}^{n-1} \omega^{-i(s+1)} l^{\varphi^{s+1}} = \omega^i \sum_{t=1}^{n} \omega^{-it} l^{\varphi^t} = \omega^i l_i.$$

Isto é, $l_i \in {}^iL^*$ para cada $i = \{0,\ldots,n-1\}$. Note que

$$\begin{aligned} \sum_{i=0}^{n-1} l_i &= \sum_{i=0}^{n-1}\left(\sum_{s=0}^{n-1} \omega^{-is} l^{\varphi^s}\right) = \sum_{s=0}^{n-1}\left(\sum_{i=0}^{n-1} \omega^{-is} l^{\varphi^s}\right)\\ &= \sum_{s=0}^{n-1} (1+\omega^{-s}+\omega^{-2s}+\cdots+\omega^{-(n-1)s}) l^{\varphi^s}. \end{aligned}$$

Agora, se $s \neq 0$, vale que ω^{-s} é raiz de $1+x+\cdots+x^{n-1}$. Portanto, vemos que

$$\sum_{i=0}^{n-1} l_i = nl.$$

Obtemos finalmente que $nL^* \subseteq H$.

(iv) Suponha que $l_i \in {}^iL^*$, $i \in \{0,\ldots,n-1\}$, e que $l_0+\cdots+l_{n-1}=0$. Assim, para todo $k = 0,\ldots,n-1$, aplicando φ^k na igualdade $l_0+\cdots+l_{n-1}=0$, obtemos as seguintes

igualdades

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

Seja $i \in \{0,\ldots,n-1\}$ fixado e $k \in \{1,\ldots,n\}$, note que o coeficiente de l_i na k–ésima igualdade é $\omega^{i(k-1)}$. Multiplicando a k–ésima igualdade por $\omega^{-i(k-1)}$, o coeficiente resultante de l_i na nova igualdade será igual a 1. Por outro lado, se $i \neq j \in \{1,\ldots,n\}$, o coeficiente resultante de l_j na k–ésima equação será $\omega^{(j-i)(k-1)}$. Agora, se $i \neq j \in \{1,\ldots,n\}$, temos que ω^{j-i} é raiz de $1 + x + \cdots + x^{n-1}$ e, portanto

$$\sum_{k=1}^{n} (\omega^{j-i})^{k-1} = 0.$$

Logo, somando as n equações resultantes da multiplicação da k–ésima equação por $\omega^{-i(k-1)}$, vemos que $nl_i = 0$, para todo $i = 0,\ldots,n-1$.

Se $l_0 + \cdots + l_{n-1} = a_1 + \cdots + a_{n-1}$ e $l_i, a_i \in {}^iL^*$, $i = 0,\ldots,n-1$, temos que que $(l_0 - a_0) + \cdots + (l_{n-1} - a_{n-1}) = 0$. Pelas considerações anteriores temos que $n(l_i - a_i) = 0$ para todo $i = 0,\ldots,n-1$. Supondo aditivamente que $char(\mathbb{F}) \nmid n$, para todo tal i vale $l_i = a_i$. Isto mostra que H é soma direta dos subespaços ${}^iL^*$ com $i = 0,\ldots,n-1$. Finalmente, como $char(\mathbb{F}) \nmid n$, temos que $l = n(n^{-1}l)$ para todo $l \in L^*$. Segue do item (iii) que $L^* = nL^* = H$.

□

Estamos, finalmente, em condições de demonstrar o principal resultado desta seção.

Demonstração do Teorema 3.16. Suponha que $\mathbb{F}$ seja um corpo e L seja uma álgebra de Lie sobre o corpo $\mathbb{F}$. Suponha que o grupo finito solúvel G aja em L por automorfismos de álgebras de Lie e que $char(\mathbb{F}) \nmid |G|$. Suponha, ainda, que a subálgebra dos pontos fixos $C_L(G) = \{l \in L;\ l^g = l,\ \forall g \in G\}$ satisfaz uma identidade polinomial.

Pelo Teorema 2.45, sabemos que toda identidade polinomial tem consequência multilinear. Portanto, podemos assumir que $C_L(G)$ satisfaz uma identidade da forma

$$f = \sum_{\sigma \in S_n} \alpha_\sigma x_0 x_{\sigma(1)} \cdots x_{\sigma(n)}$$

onde para cada $\sigma \in S_n$, $\alpha_\sigma \in \mathbb{F}$. Isso é, $C_L(G)$ satisfaz uma identidade como em (3.4). Provamos o resultado por indução em $|G|$.

Suponha inicialmente que $|G| = p$, p um primo, e seja g um gerador de G. Se $\mathbb{F}$ é algebricamente fechado, desde que $char(\mathbb{F}) \nmid p$, temos que o polinômio $x^p - 1$ possui em $\mathbb{F}$ exatamente p raízes distintas e, portanto, g é diagonalizável. Se ω denota uma p–ésima raiz primitiva da unidade, então $1, \omega, \ldots, \omega^{p-1}$ são todas as p–ésimas raízes da unidade e desde que $\mathbb{F}$ é algebricamente fechado, temos que $\mathbb{F} = \mathbb{F}[\omega]$. Para todo $i = 0, \ldots, p-1$ defina ${}^iL : \{l \in L; l^g = \omega^i l\}$. Pelo Teorema 3.27, temos que

$$L = {}^0L + \cdots + {}^{p-1}L. \tag{3.7}$$

Além disso, a decomposição em (3.7) determina uma G–graduação finita em L com relação à qual a álgebra unitária, no caso ${}^0L = C_L(G)$, satisfaz uma identidade polinomial como em 3.4. Pelo Teorema 3.26, temos que L satisfaz uma identidade polinomial não trivial.

Podemos, então, supor que $\mathbb{F}$ não é algebricamente fechado. Neste caso, considere $\overline{\mathbb{F}}$ o fecho algébrico de $\mathbb{F}$ e $L^* = L \otimes \overline{\mathbb{F}}$ com estrutura de álgebra de Lie sobre $\overline{\mathbb{F}}$. Desde que $C_L(G)$ satisfaz uma identidade multilinear como em (3.4), temos que $C_{L^*}(G)$ satisfaz a identidade multilinear. Pelo argumento utilizado no caso algebricamente fechado, temos que L^* satisfaz uma identidade polinomial com coeficientes em $\overline{\mathbb{F}}$. Como $\overline{\mathbb{F}}$ é espaço vetorial sobre $\mathbb{F}$, podemos decompor os coeficientes da identidade satisfeita em L^* numa base de $\overline{\mathbb{F}}$ sobre $\mathbb{F}$. Assim, a $\mathbb{F}$–álgebra L^* satisfaz uma identidade polinomial com coeficientes em $\mathbb{F}$ e o mesmo ocorre para sua subálgebra L.

Finalmente, podemos supor que $|G|$ não é prima. Lembrando que G é solúvel, tomemos H um subgrupo normal próprio de G e consideremos $C_L(H)$ a subálgebra dos pontos fixos dos automorfismos induzidos pelos elementos de H. Sendo H um subgrupo normal de G, para todos $g \in G$ e $h \in H$ existe $h' \in H$ tal que $gh = h'g$. Portanto, se $l \in C_L(H)$, temos que $(l^g)^h = l^{gh} = l^{h'g} = (l^{h'})^g = l^g$. Segue-se que $C_L(H)$ é G–invariante e, então, agida por G. Como H está contido no núcleo da ação de G em $C_L(H)$, temos que G/H age via automorfismos de álgebras de Lie em $C_L(H)$. Ora, G/H é grupo solúvel com ordem estritamente menor que $|G|$ e $C_{C_L(H)}(G/H) = C_L(G)$ satisfaz identidade como em (3.4). Por hipótese de indução obtemos que $C_L(H)$ satisfaz uma identidade polinomial. Logo, como H é próprio em G e $char(\mathbb{F}) \nmid |H|$, usando uma vez mais indução, obtemos que L satisfaz uma identidade polinomial não trivial, o que completa a demonstração.

□

Capítulo 4

Resultados principais

Lembramos que um grupo G é dito ser localmente finito se todo subgrupo finitamente gerado de G é finito. Note que todo grupo localmente finito G é de torção. O Problema Geral de Burnside é o seguinte questionamento: É verdade que todo grupo de torção é localmente finito? Note que grupos de torção não necessariamente possuem expoente finito, podemos considerar por exemplo o grupo das raízes complexas da unidade. Assim, uma versão do Problema Geral de Burnside é a seguinte, conhecida como Problema de Burnside: É verdade que todo grupo de expoente finito é localmente finito? Ambos os problemas receberam respostas negativas dadas por E. Golod em [3] e P.S. Novikov e S.I Adian em [21–23].

N. Gupta e S.N. Sidki construíram em [6], para cada primo ímpar p, um p–grupo infinito 2–gerado que é residualmente finito. Lembramos que um grupo G é dito ser residualmente finito se todo elemento não trivial de G possui uma imagem não trivial em um grupo finito. Em particular, um grupo de torção residualmente finito não necessariamente é localmente finito. É, portanto, natural desejar descobrir sob quais hipóteses um grupo de torção residualmente finito é localmente finito.

Em [8], B. Hartley prova que se G é um grupo de torção possuindo um automorfismo involutivo φ tal que $|C_G(\varphi)| = n < \infty$, então G possui um subgrupo normal K tal que $[G : K]$ é limitado por uma função de n e $K' \leq C_G(\varphi)$. Mais do que isto, G possui um subgrupo normal nilpotente de índice n–limitado e classe de nilpotência no máximo 2.

Em [32], V. P. Shunkov prova que se G é um grupo de torção que possui uma involução g cujo centralizador $C_G(g)$ é finito, então G é localmente finito. Posteriormente, em [30], P. Shumyatsky estende o resultado de Shunkov mostrando que todo grupo de torção residualmente finito possuindo um 4–subgrupo cujo centralizador é finito deve ser, necessariamente, localmente finito.

Os dois últimos parágrafos mostram que um caminho para conclusão de finitude local em grupos de torção residualmente finitos é supor condições sobre centralizadores. Nesse sentido, A. Shalev prova em [28, Teorema 1.1] o seguinte resultado, objeto principal deste trabalho.

Teorema 4.1. *Seja G um grupo de torção residualmente finito e sem 2–elementos. Suponha que Q seja um 2–grupo finito agindo em G de modo que $C_G(Q)$ seja solúvel ou possua expoente finito. Nestas condições, G é localmente finito.*

Como um corolário imediato do resultado acima, A. Shalev prova em [28, Corolário 1.2] a seguinte generalização dos resultados anteriormente citados de V.P. Shunkov e P. Shumyatsky.

Corolário 4.2. *Seja G um grupo de torção residualmente finito. Se G possui um 2–subgrupo finito Q tal que $C_G(Q)$ é finito, então G é localmente finito.*

Para a prova destes resultados, iremos expor na primeira seção deste capítulo noções essenciais sobre grupos localmente finitos.

Na segunda seção deste capítulo utilizaremos a série de Jennings–Lazard–Zassenhaus para demonstrar o Teorema 4.1 no caso em que G é grupo residualmente–(finito nilpotente). Neste caso, contudo, a suposição de $C_G(Q)$ ser solúvel ou de expoente finito será trocada por uma hipótese mais geral. Neste ponto, utilizaremos os resultados de E.I. Zelmanov e Y.U Bahturin e M.V. Zaicev descritos no Capítulo 3.

Posteriormente, na terceira seção do capítulo, utilizando alguns resultados obtidos em [7] por P. Hall e G. Higman com relação ao p–comprimento de grupos p–solúveis, provaremos um resultado de A. Shalev, também obtido em [28, Lema 2.5], limitando a altura de Fitting de grupos finitos solúveis em termo de seus expoentes.

Finalmente, iremos concluir este trabalho na quarta seção deste capítulo onde iremos demonstrar ambos o Teorema 4.1 e o Corolário 4.2.

4.1 Grupos localmente finitos

Seja G um grupo localmente finito. Afirmamos que todo grupo quociente de G é também localmente finito. De fato, dado N um subgrupo normal arbitrário de G, suponha que X seja um conjunto finito de elementos em G/N. Então, existem $g_1,\dots,g_r \in G$ tais que $X = \{g_1N,\dots,g_rN\}$ e, portanto, $\langle X\rangle = \langle g_1,\dots,g_r\rangle N/N$. Desde que G é localmente finito, temos que $\langle g_1,\dots,g_r\rangle$ é finito e disto segue que $\langle X\rangle$ é finito. Como $X \in G/N$ foi escolhido arbitrariamente, temos que G/N é localmente finito.

Por sua vez, sejam G um grupo e N um subgrupo normal de G tal que ambos N e G/N são localmente finitos. Sejam $g_1,\dots,g_r \in G$ escolhidos arbitrariamente e $H = \langle g_1,\dots,g_r\rangle$.

Desde que G/N é localmente finito e HN/N é subgrupo finitamente gerado de G/N, temos que $H/(H\cap N)\cong HN/N$ é finito. Isso é, $[H:H\cap N]<\infty$. Pelo Lema 2.32, temos que $H\cap N$ é subgrupo finitamente gerado de H. Contudo, $H\cap N\leq N$ e N é localmente finito. Concluímos portanto que $H\cap N$ é finito. Finalmente, $[H:H\cap N]<\infty$ e $H\cap N$ finito mostra que H é finito. Em suma, acabamos de provar o seguinte resultado.

Lema 4.3. *Seja G um grupo. Suponha que existe um subgrupo normal N de G tal que ambos N e G/N sejam localmente finitos. Nessas condições, G é localmente finito.*

Corolário 4.4. *Sejam G e H dois grupos arbitrários. Então, $G\times H$ é localmente finito se, e somente se, G e H são localmente finitos.*

Demonstração. Se $G\times H$ é localmente finito, o fato que G e H são isomorfos a $G\times 1$ e $1\times H$, respectivamente, mostra que G e H são localmente finitos. Reciprocamente, se G e H são locamente finitos, dado que $(G\times H)/(G\times 1)\cong H$ e $G\times 1\cong G$, temos que a finitude local de $G\times H$ é garantida pelo Lema 4.3. □

O seguinte resultado enfraquece a condição do Lema 4.3.

Lema 4.5. *Um grupo G é localmente finito se, e somente se, G possui uma série de subgrupos normais $G=G_0\trianglerighteq G_1\trianglerighteq\cdots\trianglerighteq G_k=1$ da qual todo fator é localmente finito.*

Demonstração. Seja G um grupo que possui uma série $G=G_0\trianglerighteq G_1\trianglerighteq\cdots\trianglerighteq G_k=1$ da qual todo fator é localmente finito. Verificamos a finitude local de G por indução em k. Se $k=1$, não há nada a provar. Se $k>1$, por hipótese de indução, G_1 é localmente finito. Desde que G/G_1 é localmente finito, segue do Lema 4.3 que G é localmente finito.

A recíproca é imediata e o resultado está demonstrado. □

4.2 Restrição aos grupos de torção residualmente–(finito nilpotente)

Lembramos que um grupo G é dito ser residualmente–(finito nilpotente) se para todo $1\neq g\in G$ existem um grupo finito nilpotente N e um homomorfismo $\varphi: G\longrightarrow N$ tal que $g^{\varphi}\neq 1$.

Nosso interesse principal nesta seção é provar o seguinte resultado estabelecido em [28] por A. Shalev.

Teorema 4.6 (A. Shalev)**.** *Seja G um grupo de torção residualmente–(finito nilpotente) e sem 2–elementos. Suponha que Q seja um 2–grupo finito agindo em G de modo que $C_G(Q)$ satisfaça uma identidade não trivial de grupo. Nestas condições, G é localmente finito.*

Dizemos que uma identidade $w = 1$ não trivial de grupo é satisfeita no grupo G se existem variáveis $x_1, \ldots, x_n$ e $w = w(x_1, \ldots, x_n)$ um elemento não trivial do grupo livremente gerado pelo conjunto $X = \{x_1, \ldots, x_n\}$ tal que para todos $g_1, \ldots, g_n \in G$ vale $w(g_1, \ldots, g_n) = 1$. Para a prova do Teorema 4.6 iremos inicialmente fazer algumas considerações sobre grupos residualmente–(finito nilpotente).

Nesta seção, permita-nos escrever $\mathcal{C}_{f.n.}$ para denotar a classe dos grupos finitos nilpotentes e $\mathcal{C}_p$ para denotar a classe dos p–grupos finitos, p um primo. Lembramos, então, que para cada classe de grupos finitos $\mathcal{C}$ fechada para subgrupos, imagens epimórficas e produtos diretos finitos e para cada grupo G, $\tau_{\mathcal{C}}(G)$ denota a família dos subgrupos normais N de G tais que G/N está na classe $\mathcal{C}$.

Lema 4.7. *Seja G um grupo de torção residualmente–(finito nilpotente). Se $g, h \in G$ possuem ordens coprimas então g e h comutam.*

Demonstração. Dado $N \in \tau_{\mathcal{C}_{f.n}}(G)$, G/N é grupo finito nilpotente. Desde que g e h possuem ordens coprimas, $gN, hN \in G/N$ possuem ordens coprimas. Pelo Teorema 1.22, temos que gN e hN comutam, isso é, $[g,h] \in N$. Pela arbitrariedade da escolha de $N \in \tau_{\mathcal{C}_{f.n}}(G)$ e o fato de G ser residualmente–(finito nilpotente), o Teorema 3.1 mostra que $[g,h] = 1$. □

O seguinte resultado estabelece que grupos de torção finitamente gerados residualmente–(finito nilpotente) são produtos diretos de p–subgrupos maximais e residualmente–p, p um primo. Uma vantagem de ter esse resultado é que todas as propriedades mantidas por produtos diretos e verificadas em grupos de torção residualmente–p são diretamente estendidas aos grupos de torção finitamente gerados e residualmente–(finito nilpotente).

Lema 4.8. *Seja G um grupo de torção finitamente gerado e residualmente–(finito nilpotente). Então, G é produto direto de um número finito de p–subgrupos maximais que são característicos e residualmente–p, com p primo.*

Demonstração. Seja p um primo arbitrário. Para cada $N \in \tau_{\mathcal{C}_{f.n.}}(G)$, G/N é um grupo finito nilpotente e, pelo Teorema 1.22, possui um único p–subgrupo de Sylow, normal em G/N. Assim, pelo Teorema da Correspondência, existe um único subgrupo normal em G, o qual denotamos por $P(N)$, que contém N e cuja imagem em G/N é o seu p–subgrupo de Sylow. Afirmamos que

$$K(p) = \bigcap_{N \in \tau_{\mathcal{C}_{f.n.}}(G)} P(N)$$

é um p–subgrupo de G contendo todos os p–subgrupos de G.

Suponha, por absurdo, que $K(p)$ não seja um p–grupo. Então, existe um elemento $1 \neq g \in K(p)$ que não é um p–elemento. Desde que G é de torção, g tem ordem finita e podemos supor que g tem ordem coprima com p. Qualquer que seja $N \in \tau_{\mathcal{C}_{f.n.}}(G)$, por definição de $K(p)$, temos que a imagem de g em G/N é um p–elemento. Assim, desde que a ordem de g é coprima com p, temos que $g \in N$. Pela arbitrariedade da escolha de $N \in \tau_{\mathcal{C}_{f.n.}}(G)$ e o Teorema 3.1, temos que $g = 1$, uma contradição. Portanto, $K(p)$ é um p–subgrupo de G, como afirmado.

Suponha, agora, que Q seja um p–subgrupo arbitrário de G. Para cada $N \in \tau_{\mathcal{C}_{f.n.}}(G)$, temos que QN/N é um p–subgrupo de G/N. Disto, segue-se que $QN \leq P(N)$ e $Q \leq P(N)$. Como $N \in \tau_{\mathcal{C}_{f.n.}}(G)$ foi escolhido arbitrariamente, temos que

$$Q \leq \bigcap_{N \in \tau_{\mathcal{C}_{f.n.}}(G)} P(N) = K(p),$$

mostrando que $K(p)$ é o maior p–subgrupo de G. Em particular, dado que automorfismos preservam as ordens dos elementos, temos que $K(p)$ é um subgrupo característico de G.

Do fato que G é residualmente–(finito nilpotente) e pelo Teorema 3.1, vemos que

$$\bigcap_{N \in \tau_{\mathcal{C}_{f.n.}}(G)} (K(p) \cap N) = 1. \tag{4.1}$$

Por outro lado, se $N \in \tau_{\mathcal{C}_{f.n.}}(G)$, temos que $K(p)N/N$ é um p–grupo finito. Isso mostra que

$$\tau(K(p)) \coloneqq \{K(p) \cap N; N \in \tau_{\mathcal{C}_{f.n.}}(G)\} \subseteq \tau_{\mathcal{C}_p}(K(p)). \tag{4.2}$$

Por (4.1), (4.2) e o Teorema 3.1, temos que $K(p)$ é residualmente–p.

Resta-nos mostrar que $K(p)$ é não trivial somente para um número finito de primos p e que G é produto direto dos $K(p)$.

Por hipótese, temos que G é finitamente gerado, digamos por $a_1, \ldots, a_m$. Desde que G é de torção, para cada $i = 1, \ldots, m$ podemos considerar $\pi(a_i) = \{p_{i1}, \ldots, p_{ir_i}\}$, o conjunto dos primos dividindo $|a_i|$. Assim, fixado $i = 1, \ldots, m$, existem $g_{ij} \in K(p_{ij})$, $j = 1, \ldots, r_i$, de modo que $a_i = g_{i1} \ldots g_{ir_i}$. Dado que $G = \langle a_1, \ldots, a_m \rangle$, temos que $G = \langle g_{ij};\ i = 1, \ldots, m,\ j = 1, \ldots, r_i \rangle$. Pelo Lema 4.7, se $a, b \in G$ possuem ordens coprimas, temos que $|ab| = |a||b|$. Obtemos então que $K(p) \neq 1$ se, e somente se, $p \in \pi \coloneqq \{p_{11}, \ldots, p_{1r_1}, \ldots, p_{m1}, \ldots, p_{mr_m}\}$.

Seja $g \in G$ um elemento arbitrário. Pelas considerações anteriores podemos tomar primos $p_1, \ldots, p_r \in \pi$, distintos dois a dois, e $g_i \in K(p_i)$, $i = 1, \ldots, r$, de modo que $g = g_1 \ldots g_r$. Suponha que para cada $i = 1, \ldots, r$ existe $g_i' \in K(p_i)$ tais que $g = g_1' \ldots g_r'$. Dado $N \in \tau_{\mathcal{C}_{f.n.}}(G)$,

vale que

$$gN = (g_1 \dots g_r)N = (g_1N) \dots (g_rN) = (g'_1 \dots g'_r)N = (g'_1N) \dots (g'_rN).$$

Desde que G/N é finito e nilpotente, pelo Teorema 1.22, G/N é produto direto de seus subgrupos de Sylow. Segue-se que $g_iN = g'_iN$ para todo $i = 1, \dots, r$, isso é, $g_i^{-1}g'_i \in N$. Assim, pela arbitrariedade da escolha de $N \in \tau_{\mathcal{C}_{f.n.}}(G)$ e o Teorema 3.1, temos que $g_i = g'_i$ para todo $i = 1, \dots, r$.

Finalmente, verificamos que todo elemento em G é escrito de modo único como um produto de elementos nos grupos $K(p)$, p um primo. Desde que $K(p) \neq 1$ somente para um número finito de primos p, o resultado está verificado. □

Sejam G um grupo satisfazendo uma identidade não trivial de grupo e $D_n(G)$ o n–ésimo termo da série de Jennings–Lazard–Zassenhaus associada ao primo p introduzida no Capítulo 2, Definição 2.24. Do fato que G satisfaz uma identidade não trivial de grupo, é natural conjecturar que alguma consequência seja obtida na $\mathbb{F}_p$–álgebra de Lie $L(G) = \bigoplus_{n \geqslant 1} D_n(G)/D_{n+1}(G)$ a partir da identidade não trivial satisfeita em G. Isto é estabelecido no que segue. Antes disto, generalizamos a definição de identidade de grupo.

Definição 4.9. Sejam G um grupo, H um subgrupo de G e $a_1, \dots, a_n \in G$. Dizemos que uma identidade não trivial w é satisfeita nas classes $a_1H, \dots, a_nH$ se existe um elemento não trivial $w = w(x_1, \dots, x_n)$ no grupo livremente gerado pelo conjunto $X = \{x_1, \dots, x_n\}$ tal que para todos $h_1, \dots, h_n \in H$ vale $w(a_1h_1, \dots, a_nh_n) = 1$.

Note que se um grupo G satisfaz uma identidade não trivial de grupo, então tal identidade será satisfeita nas classes $a_1G, \dots, a_nG$ para todos $a_1, \dots, a_n \in G$. Assim, o seguinte resultado, provado em [35, Teorema 1] por J.S. Wilson e E.I. Zelmanov, mostra que se G é um grupo satisfazendo uma identidade não trivial de grupo, a $\mathbb{F}_p$–álgebra de Lie associada à série de Jennings–Lazard–Zassenhaus de G satisfaz uma identidade polinomial não trivial.

Teorema 4.10 (Wilson–Zelmanov)**.** *Sejam G um grupo e H um subgrupo de G de índice finito. Sejam $a_1, \dots, a_n \in G$ e suponha que uma identidade não trivial $w = w(x_1, \dots, x_n)$ é satisfeita nas classes $a_1H, \dots, a_nH$. Então, para cada primo p, a $\mathbb{F}_p$–álgebra de Lie $L_p(G)$ associada à série de Jennings–Lazard–Zassenhaus de G satisfaz uma identidade polinomial não trivial.*

Demonstração. Para cada grupo Q, deixe-nos denotar por $\delta(q)$ o grau de $q \in Q$ com relação à série de Jennings–Lazard–Zassenhaus associada ao primo p. Isto é, $\delta(q) = \infty$ se $q \in D_\infty(Q)$ e se $q \notin D_\infty(Q)$, $\delta(q)$ é o inteiro positivo i tal que $q \in D_i(Q) \setminus D_{i+1}(Q)$.

Sejam F o grupo livremente gerado por $x_1,\dots,x_n$ e p um primo fixado. Pelo Lema 3.7 temos que F é residualmente–p. Por outro lado, pelo Lema 3.10 temos que $D_\infty(F)=1$. Assim, $\delta(w)=m<\infty$. Podemos supor $m>1$ e, trocando w por $[w,x_i]$, se necessário, podemos supor que m é coprimo com p. Assim, se j,k são inteiros não negativos tais que $jp^k=m$, temos que $j=m$ e $k=0$. A definição de $D_m(F)$ mostra que $D_m(F)=\gamma_m(F)D_{m+1}(F)$. Por outro lado, $\gamma_{m+1}(F)\leq D_{m+1}(F)$. Segue-se que existem $r\geqslant 1$, $\alpha_1,\dots,\alpha_r$ comutadores simples de peso exatamente m com entradas em $x_1,\dots,x_n$ e $1\leqslant k_1,\dots,k_r<p$ tais que

$$w=\alpha_1^{k_1}\dots\alpha_r^{k_r}w'$$

onde w' tem grau pelo menos $m+1$.

Para cada $i=1,\dots,n$ seja d_i o número de ocorrências da variável x_i em α_1. Dado que α_1 é comutador simples de peso m com entradas em $x_1,\dots,x_n$, temos que $m=\sum_{i=1}^{n}d_i$.

Dadas novas variáveis $z_1,\dots,z_m$, seja $Y=\{x_1,\dots,x_n,z_1,\dots,z_m\}$ e F_1 o grupo livremente gerado pelo conjunto Y. Em F_1, considere o elemento

$$w_1=w(x_1z_1\dots z_{d_1},x_2z_{d_1+1}\dots z_{d_1+d_2},\dots,x_nz_{d_1+d_2+\dots+d_{n-1}+1}\dots z_m).$$

Então, w_1 tem grau m com relação à série de Jennings–Lazard–Zassenhaus de F_1 e podemos escrever

$$w_1=\beta_1\cdots\beta_q \tag{4.3}$$

onde cada β_i é comutador de peso no mínimo m com entradas em Y. Por definição de w_1 e o fato de que comutadores de peso m são lineares em suas entradas módulo o grupo gerado pelos comutadores de peso $m+1$, numa escrita como acima para w_1, pelo menos algum β_i tem peso exatamente m e contém cada uma das variáveis $z_1,\dots,z_m$.

Sabemos que em qualquer grupo A vale a igualdade $ab=ba[a,b]$. Utilizando isto, em (4.3) podemos levar à esquerda, na ordem em que aparecem, todos os comutadores β_i não contendo a variável z_1, pagando-se um preço de acrescentar novos comutadores, até mais complexos, mas todos os acrescentados contendo a variável z_1. Então, no produto de comutadores contendo z_1 , levamos à esquerda, na ordem em que aparecem, os comutadores não contendo z_2. Fazendo isto ordenadamente de 1 até m, escrevemos $w_1=\sigma_1\dots\sigma_m\sigma_{m+1}$ onde, para cada $i=1,\dots,m$, σ_i é um produto de comutadores não contendo a variável z_i mas contendo a variável z_j para todo $j<i$, e σ_{m+1} é um produto de comutadores cada um dos quais contendo todas as variáveis $z_1,\dots,z_m$.

Sejam $h_1,\dots,h_m \in H$. Então, desde que a lei $w=1$ é satisfeita nas classes $a_1H,\dots,a_nH$, temos que

$$w_1(a_1,\dots,a_n,h_1,\dots,h_m) = w(a_1h_1\dots h_{d_1},\dots,a_nh_{(d_1+\dots+d_{n-1}+1)}\dots h_m) = 1.$$

Defina, para cada $i=2,\dots,m+1$, $w_i = \sigma_i\dots\sigma_{m+1}$ e suponha que dado $1 \leqslant i \leqslant m$ vale

$$w_i(a_1,\dots,a_n,h_1,\dots,h_m) = 1, \text{ para todo } h_1,\dots,h_m \in H.$$

Desde que w_{i+1} é produto de comutadores envolvendo a variável z_i, tomando $h_1,\dots,h_m \in H$ com a única condição que $h_i = 1$, obtemos que

$$\sigma_i(a_1,\dots,a_n,h_1,\dots,1,\dots,h_m) = 1,$$

isto porque $w_i = \sigma_i w_{i+1}$ e $w_{i+1}(a_1,\dots,a_n,h_1,\dots,1,\dots,h_m) = 1$. Por outro lado, σ_i é produto de comutadores não envolvendo a variável z_i e por isso para cada $h_1,\dots,h_m \in H$ temos que

$$\sigma_i(a_1,\dots,a_n,h_1,\dots,h_m) = 1.$$

Finalmente, concluímos que

$$w_i(a_1,\dots,a_n,h_1,\dots,h_m) = 1 = w_{i+1}(a_1,\dots,a_n,h_1,\dots,h_m).$$

Por indução, vemos que para cada $h_1,\dots,h_m \in H$ vale

$$w_{m+1}(a_1,\dots,a_n,h_1,\dots,h_m) = 1.$$

Por definição, $w_{m+1} = \sigma_{m+1}$ é produto de comutadores de peso maior ou igual a m nos quais aparecem todas as variáveis $z_1,\dots,z_m$. Portanto, como F_1 é livremente gerado por Y e pelo Lema 1.20, nós podemos escrever $w_{m+1} = uv$ onde u é um produto de comutadores simples de peso exatamente m com entradas em $z_1,\dots,z_m$ e v é produto de comutadores de peso pelo menos $m+1$ contendo cada uma das variáveis $z_1,\dots,z_m$ e, possivelmente, alguma variável x_i, $1 \leqslant i \leqslant n$. Então, $u \neq 1$ e para cada $h_1,\dots,h_m \in H$ vale

$$u(h_1,\dots,h_m) = v(a_1,\dots,a_n,h_1,\dots,h_m)^{-1}. \tag{4.4}$$

Seja $D_i = D_i(G)$ o i–ésimo termo da série de Jennnings–Lazard–Zassenhaus de G associada ao primo p. Para cada $g \in G$ lembramos que $\delta(g)$ denota o grau de g com relação e esta série.

Pela igualdade em (4.4), temos que para cada $h_1,\ldots,h_m \in H$ vale

$$\delta(u(h_1,\ldots,h_m)) \geqslant 1+\sum_{i=1}^{m}\delta(h_i). \tag{4.5}$$

Por outro lado, sejam $k_1,\ldots,k_m \in G$ e suponha que possamos escrever $k_i = h_i c_i$ onde $\delta(c_i) \geqslant 1+\delta(k_i)$ para cada $i=1,\ldots,m$. Desde que u é um produto de comutadores de peso exatamente m com entradas no conjunto $z_1,\ldots,z_m$, podemos escrever $u(k_1c_1^{-1},\ldots,k_mc_m^{-1})$ na forma g_1g_2 onde $g_1,g_2 \in G$, g_1 é um produto de comutadores de peso m com entradas no conjunto $k_1,\ldots,k_m$ e g_2 é um produto de comutadores de peso maior ou igual a m, os comutadores de peso m contendo pelo menos um dos elementos c_i. Assim, temos que

$$\delta(g_2) \geqslant 1+\sum_{i=1}^{m}\delta(k_i). \tag{4.6}$$

Por outro lado, $k_ic_i^{-1} \in H$ para cada $i=1,\ldots,m$. Segue de (4.5) que

$$\delta(u(k_1c_1^{-1},\ldots,k_mc_m^{-1})) \geqslant 1+\sum_{i=1}^{m}\delta(k_ic_i^{-1}) = 1+\sum_{i=1}^{m}\delta(k_i) \tag{4.7}$$

pois para todos $a,b \in G$ vale $\delta(ab) = min\{\delta(a),\delta(b)\}$. Das desigualdades em (4.6) e (4.7), temos que

$$\delta(u(k_1,\ldots,k_m)) \geqslant 1+\sum_{i=1}^{m}\delta(k_i).$$

Agora, desde que $[G:H]<\infty$, a série $G \geq HD_2 \geq HD_3 \geq \ldots \geq HD_t \geq \ldots$ deve estacionar, isso é, existe um inteiro positivo t tal que para todo $l \geqslant t$ vale $D_t \leq HD_l$. Sejam $g_{11},\ldots,g_{1t},\ldots,g_{m1},\ldots,g_{mt}$ elementos arbitrários de G e, para cada $i=1,\ldots,m$, defina $k_i = [g_{i1},\ldots,g_{it}]$. Desde que $\{D_i; i \geqslant 1\}$ é uma N_p–série, temos que

$$k_i = [g_{i1},\ldots,g_{it}] \in \left[D_{\delta(g_{i1})},\ldots,D_{\delta(g_{it})}\right] \leq D_{\sum_{j=1}^{t}\delta(g_{ij})}, i=1,\ldots,m.$$

Isso é, $\delta(k_i) \geqslant \sum_{j=1}^{t}\delta(g_{ij})$, $i=1,\ldots,m$. Por outro lado, para cada $i=1,\ldots,m$ vale que $[g_{i1},\ldots,g_{it}] \in D_t \leq HD_l$ para todo $l \geqslant t$. Segue-se que

$$\delta(u([g_{11},\ldots,g_{1t}],\ldots,[g_{m1},\ldots,g_{mt})) \geqslant 1+\sum_{i=1}^{m}\delta(k_i) \geqslant 1+\sum_{i,j}\delta(g_{ij}). \tag{4.8}$$

Finalmente, escreva $u = [z_{\lambda_1}, \ldots, z_{\lambda_m}] \ldots [z_{\mu_1}, \ldots, z_{\mu_m}]$ e considere o elemento correspondente

$$f_1(z_1, \ldots, z_m) = [z_{\lambda_1}, \ldots, z_{\lambda_m}] + \cdots + [z_{\mu_1}, \ldots, z_{\mu_m}]$$

na álgebra de Lie sobre $\mathbb{F}_p$ livremente gerada por $z_1, \ldots, z_m$. Então, escolhendo novas variáveis $x_{11}, \ldots, x_{1t}, \ldots, x_{m1}, \ldots, x_{mt}$, podemos considerar o elemento

$$f = f_1([x_{11}, \ldots, x_{1t}], \ldots, [x_{m1}, \ldots, x_{mt}])$$

na $\mathbb{F}_p$–álgebra de Lie livremente gerada por $\{x_{11}, \ldots, x_{mt}\}$. Para cada $i = 1, \ldots, m$ e $j = 1, \ldots, t$, seja g_{ij} um elemento arbitrário de G. Então, se $\overline{g}_{ij}$ denota a imagem de g_{ij} em $D_{\delta(g_{ij})}/D_{\delta(g_{ij})+1}$, de (4.8) segue que:

$$\begin{aligned} f(\overline{g}_{11}, \ldots, \overline{g}_{1t}, \ldots, \overline{g}_{m1}, \ldots, \overline{g}_{mt}) &= f_1([\overline{g}_{11}, \ldots, \overline{g}_{1t}], \ldots, [\overline{g}_{m1}, \ldots, \overline{g}_{mt}]) \\ &= u([g_{11}, \ldots, g_{1t}], \ldots, [g_{m1}, \ldots, g_{mt}]) D_{1+\sum_{i,j} \delta(g_{ij})} \\ &= 0. \end{aligned}$$

Isto mostra que $f = 0$ em $L_p(G)$ e, portanto, $L_p(G)$ satisfaz uma identidade polinomial. □

Note que na prova do Teorema 4.10, a única propriedade utilizada da série de Jennings–Lazard–Zassenhaus do grupo G associada ao primo p é que para todos inteiros positivos n e m vale $[D_n(G), D_m(G)] \leq D_{n+m}(G)$. Contudo, tal propriedade é também válida em qualquer N_p–série de G e portanto o resultado é obtido para qualquer N_p–série de G.

Podemos, então, provar o Teorema 4.6.

Demonstração do Teorema 4.6. Seja G um grupo de torção residualmente–(finito nilpotente), sem 2–elementos, agido por um 2–grupo finito Q. Suponha que $C_G(Q)$ satisfaça uma identidade não trivial de grupo. Nessas condições, vamos mostrar que G é localmente finito.

Seja $X = \{x_1, \ldots, x_n\} \subseteq G$ um conjunto fixado. Desde que Q é finito, temos que $X^Q := \{x_i^q; i = 1, \ldots, n \text{ e } q \in Q\}$ é um conjunto finito e $\langle X \rangle \leq \langle X^Q \rangle$. Por outro lado, vemos que $\langle X^Q \rangle$ é um subgrupo Q–invariante de G e $C_{\langle X^Q \rangle}(Q) \leq C_G(Q)$. Estas condições mostram que podemos assumir, sem perda de generalidade, que G é finitamente gerado.

Adicionalmente, se G é finitamente gerado, o Lema 4.8 mostra que G é produto direto de p–subgrupos maximais característicos e residualmente–p, $p \neq 2$ desde que G não possui 2–elementos.

Das considerações anteriores e pelo Corolário 4.4 temos que o Teorema 4.6 estará demonstrado se o verificarmos no caso particular em que G é residualmente–p, $p \neq 2$.

Seja, então, G um grupo de torção residualmente–p, $p \neq 2$, agido por um 2–grupo finito Q de modo que $C_G(Q)$ satisfaz uma identidade não trivial de grupo. Assuma que G é finitamente gerado e vamos mostrar que G é finito.

Seja $D_i = D_i(G)$ o i–ésimo termo da série de Jennings–Lazard–Zassenhaus de G, associada ao primo p. Então, sabemos que

$$L(G) = \bigoplus_{i\geq 1} D_i/D_{i+1}$$

tem estrutura de álgebra de Lie sobre o corpo $\mathbb{F}_p$.

Como cada subgrupo D_i é característico em G, temos que Q age via automorfismos em cada D_i e, pelo mesmo motivo, Q age via automorfismos em cada fator D_i/D_{i+1}. Observando cada fator anterior como espaço vetorial sobre o corpo $\mathbb{F}_p$, vemos que Q age em cada fator D_i/D_{i+1} via automorfismos lineares. Segue-se que a ação de Q em G induz uma ação via automorfismos lineares de Q no espaço vetorial $L(G)$. Por definição de $[\cdot,\cdot]$ em $L(G)$, temos que a ação de Q em G induz uma ação via automorfismos de álgebras de Lie de Q em $L(G)$.

Seja $l \in C_{L(G)}(Q)$. Então, existem $r \in \mathbb{N}^*$ e $l_i \in D_i/D_{i+1}$ tais que $l = \sum_{i=1}^{r} l_i$ e vale, para todo $q \in Q$, que

$$l^q = (\sum_{i=1}^{r} l_i)^q = \sum_{i=1}^{r} l_i^q = l = \sum_{i=1}^{r} l_i.$$

Assim, temos que

$$C_{L(G)}(Q) = \bigoplus_{i\geq 1} C_{D_i/D_{i+1}}(Q).$$

Ora, desde que Q é 2–grupo finito e D_i/D_{i+1} é grupo de torção sem 2 torção, vale pelo Teorema 1.12 que

$$C_{D_i/D_{i+1}}(Q) = C_{D_i}(Q)D_{i+1}/D_{i+1} = (C_G(Q) \cap D_i)D_{i+1}/D_{i+1}.$$

Assim, temos que

$$C_{L(G)}(Q) = \bigoplus_{i\geq 1} C_{D_i/D_{i+1}}(Q) = \bigoplus_{i\geq 1} (C_G(Q) \cap D_i)D_{i+1}/D_{i+1}.$$

Por outro lado, temos que $\{C_G(Q) \cap D_i; i \geq 1\}$ define uma N_p–série de $C_G(Q)$. Como $C_Q(G)$ satisfaz uma identidade não trivial de grupo, pelo Teorema 4.10, temos que

$$\begin{aligned}\bigoplus_{i\geq 1}(C_G(Q)\cap D_i)/(C_G(Q)\cap D_{i+1}) &= \bigoplus_{i\geq 1}(C_G(Q)\cap D_i)/(C_G(Q)\cap D_i)\cap D_{i+1}\\ &\cong \bigoplus_{i\geq 1}((C_G(Q)\cap D_i)D_{i+1}/D_{i+1}\\ &\cong C_{L(G)}(Q)\end{aligned}$$

satisfaz uma identidade polinomial não trivial. Desde que $p = char(\mathbb{F}_p) \nmid |Q|$ e Q é grupo finito solúvel, temos pelo Teorema 3.16, que $L(G)$ é uma álgebra de Lie satisfazendo uma identidade polinomial não trivial. Portanto, a subálgebra $L_p(G)$ satisfaz uma identidade polinomial.

Em resumo, G é grupo de torção finitamente gerado, residualmente–p, e $L_p(G)$ satisfaz uma identidade polinomial. Segue do Teorema 3.15 que G é finito. Isso conclui a prova do resultado. □

4.3 Limite na altura de Fitting em função do expoente

Nesta seção, nos dispomos a provar um resultado de A. Shalev [28, Lema 2.5] limitando a altura de Fitting de grupos finitos solúveis em termos de seus expoentes. Neste propósito, fazemos algumas considerações e provamos alguns resultados preliminares.

Em [7], P. Hall e G. Higman estabeleceram um limite ao p–comprimento de grupos finitos p–solúveis em termos do expoente de um subgrupo de Sylow. Nós iremos provar este resultado nas páginas seguintes. Antes precisamos da seguinte definição.

Definição 4.11. Seja p um primo. Se existe um inteiro não negativo m tal que $p = 2^{2^m}+1$, então p é chamado um primo de Fermat (em homenagem a Pierre de Fermat). Por outro lado, se existe um inteiro positivo n tal que $p = 2^n - 1$, então dizemos que p é um primo de Mersenne (em homenagem a Marin Mersenne).

Os seguintes dois resultados são alguns dos principais resultados provados em [7] por P. Hall e G. Higman. Suas provas podem ser encontradas, por exemplo, em [12, pág. 426, , Teorema 2.9] e [12, pág. 440, Teorema 3.9], respectivamente.

Teorema 4.12 (Teorema B de Hall–Higman)**.** *Seja K um corpo de característica positiva p e V um espaço vetorial de dimensão finita sobre o corpo K. Seja G um grupo finito p–solúvel de automorfismos lineares de V tal que $O_p(G) = 1$. Se g é um elemento de G de ordem p^n, então o polinômio minimal de g é $(t-1)^r$ onde $r \leqslant p^n$. Se $r < p^n$, existem inteiros $n_0 \leqslant n$ para os quais $p^{n_0} - 1$ é potência de um primo q e os q–subgrupos de Sylow de G são não-abelianos. Mais do que isto, se n_0 é o menor tal inteiro, então $r \geqslant p^{n-n_0}(p^{n_0}-1)$.*

Lembramos que para cada grupo finito G e primo p, $O_p(G)$ denota a intersecção de todos os p–subgrupos de Sylow de G.

Teorema 4.13. *Seja K um corpo de característica positiva p e V um espaço vetorial de dimensão finita sobre o corpo K. Seja G um grupo finito p–solúvel de automorfismos lineares de V e suponha que $O_p(G) = 1$. Suponha que g e h sejam elementos de um p–subgrupo de Sylow de G tais que $g^{p^{m-1}}$ e $h^{p^{m-1}}$ não comutam. Então, ou $(g-1)^{p^m-1} \neq 0$ ou $(h-1)^{p^m-1} \neq 0$.*

Na intenção de utilizar os Teoremas 4.12 e 4.13 no estudo de p–comprimento de grupos finitos p–solúveis, se faz conveniente estudar soluções da equação $p^a = q^b + 1$, onde p e q são números primos e a e b são inteiros positivos. Isto é feito no próximo resultado.

Lema 4.14. *([12, pág. 424, Lema 2.7]) Sejam p,q números primos e a,b inteiros positivos. Suponha que $p^a = q^b + 1$. Então, vale uma das seguintes:*

(i) $p = 2$, $b = 1$, *a é primo e* $q = 2^a - 1$ *é um primo de Mersenne;*

(ii) $q = 2$, $a = 1$, $b = 2^m$ *e* $p = 2^{2^m} + 1$ *é um primo de Fermat;*

(iii) $p^a = 9$ *e* $q^b = 8$.

Demonstração. Claramente, $p = 2$ ou $q = 2$.

Se $p = 2$, então $a > 1$. Se $b = 2c$, então $q^{2c} - 1 = 2^a - 2 = 2(2^{a-1} - 1) \not\equiv 0(mod 4)$. Por outro lado, desde que q é ímpar, temos que $q^{2c} - 1$ é múltiplo de 4, uma contradição. Vemos, portanto, que b é ímpar. Se $b > 1$, considere $f(x) = x^{b-1} - x^{b-2} + \cdots + 1$ no anel $\mathbb{F}_2[x]$. Como q é ímpar, temos que $f(\overline{q}) = \overline{1} = \overline{q}$. Desde que $2^a = (q+1)(q^{b-1} - q^{b-2} + \cdots + 1)$, vemos que $q + 1 = 2^d$ para algum inteiro d e temos o seguinte absurdo:

$$2^{a-d} = q^{b-1} - q^{b-2} + \cdots + 1 \equiv 1(mod 2).$$

Então, temos que $b = 1$. Finalmente, se $a = ef$ e vale que e e f são maiores que 1, então $q = 2^a - 1 = 2^{ef} - 1 = (2^e - 1)(2^{e(f-1)} + 2^{e(f-2)} + \cdots + 1)$, um absurdo desde que q é primo. Concluímos, portanto, que a é número primo e que estamos no caso (i).

Supomos, então, que $q = 2$. Desse modo $p^a = 2^b + 1$.

Se $a > 1$ escrevemos

$$2^b = p^a - 1 = (p-1)(p^{a-1} + p^{a-2} + \cdots + p + 1).$$

Disto obtemos que $p - 1 = 2^c$ e $p^{a-1} + p^{a-2} + \cdots + 1 = 2^{b-c} > 1$ para algum c. Considerando o polinômio $f(x) = x^{a-1} + x^{a-2} + \cdots + 1$ em $\mathbb{F}_2[x]$, temos que $f(\overline{p}) = \overline{a}$. Das considerações

anteriores vemos que $a \equiv 2^{b-c} \equiv 0(mod 2)$, isso é, a é número par. Escrevendo $a = 2d$, temos que $2^b = p^{2d} - 1 = (p^d - 1)(p^d + 1)$. Segue-se que $p^d + 1 = 2^e$ e $p^d - 1 = 2^f$ para convenientes e e f. Claramente $f = 1$, $e = 2$ e por isso obtemos $p^d = 3$, isso é, $p^a = 9$ e $2^b = 8$, ou seja, estamos no caso (iii).

Finalmente, se $a = 1$, $p = 2^b + 1$ e resta-nos mostrar que $b = 2^m$. Se $b = 2^c d$, d um ímpar, temos que

$$p = 2^{2^c d} + 1 = (2^{2^c} + 1)(2^{(d-1)2^c} - \cdots + 1).$$

Por isso vemos que $b = 2^c$ e $p = 2^{2^c} + 1$ é primo de Fermat, como indicado no item (ii).

A demonstração está completa. □

Sejam G um grupo finito e p um primo fixados. Denote por $p^{e_p(G)}$ o expoente de um p–subgrupo de Sylow P de G. Dado que subgrupos de Sylow em grupos finitos são conjugados, logo isomorfos, temos que $e_p(G)$ independe da escolha de $P \in S_p(G)$, onde $S_p(G)$ denota o conjunto dos p–subgrupos de Sylow de G. Mais do que isto, $e_p(G)$ é um invariante numérico no sentido que se G é isomorfo ao grupo G', então $e_p(G') = e_p(G)$. Em tempo, é fácil ver que se $H \leq G$ e $N \trianglelefteq G$, então ambos $e_p(H)$ e $e_p(G/N)$ são menores ou iguais a $e_p(G)$.

Definição 4.15. Sejam G um grupo finito e p um número primo. Seja P um p–subgrupo de Sylow de G. Lembramos que, por definição, $P = 1$ se p não divide a ordem de G. Para cada $n \geqslant 0$ defina $\mu_{2n}(P) := \langle x^{p^n}; x \in P \rangle$ e para cada $n \geqslant 1$ defina

$$\mu_{2n-1}(P) := \langle [x^{p^{n-1}}, y^{p^{n-1}}], z^{p^n}; x, y, z \in P \rangle.$$

Assim, temos a seguinte cadeia de subgrupos de P

$$P = \mu_0(P) \geq \mu_1(P) \geq \mu_2(P) \geq \cdots \geq \mu_i(P) \geq \cdots.$$

Como $\mu_{2e_p(G)}(P) = \langle x^{p^{e_p(G)}}; x \in P \rangle = 1$, a cadeia acima sempre alcança o grupo trivial em G. No caso particular em que p divide a ordem de G, note que $\mu_{2(e_p(G)-1)}(P) \neq 1$, então, o menor número m tal que $\mu_m(P) = 1$ é $2e_p(G) - 1$ ou $2e_p(G)$. Em qualquer caso, denotando por $e_p^*(G)$ o menor inteiro não negativo m tal que $\mu_m(P) = 1$, temos que

$$e_p(G) = \lfloor \frac{1 + e_p^*(G)}{2} \rfloor$$

onde "$\lfloor \cdot \rfloor$" denota a função maior inteiro. Note que $e_p^*(G)$ é também um invariante numérico pois subgrupos de Sylow de G são conjugados.

Teorema 4.16. *([12, pág. 405, Lema 4.2]) Seja G um grupo finito p–solúvel tal que p divide a ordem de G. Então, vale:*

(i) $e_p(G/O_{p',p}(G)) \leqslant e_p(G) - 1$ *se vale uma das seguintes condições:*

- *(a)* *p é impar e não é primo de Fermat;*
- *(b)* *p é primo de Fermat e os 2–subgrupos de Sylow de G são abelianos;*
- *(c)* *$p = 2$ e os q–subgrupos de Sylow de G são abelianos para todos primo de Mersenne q.*

(ii) *Se $p \geqslant 3$, então $e_p^*(G/O_{p',p}(G)) \leqslant e_p^*(G) - 1$.*

Demonstração. Seja P um subgrupo de Sylow de G e escreva

$$A/O_{p'}(G) = \Phi(O_{p',p}(G)/O_{p'}(G)).$$

Desse modo, sabemos que $V = O_{p',p}(G)/A$ pode ser visto como espaço vetorial sobre $\mathbb{F}_p$. Considerando a ação natural de G em V, pelo Teorema 1.40 o núcleo da ação é $C_G(O_{p',p}(G)/A) = O_{p',p}(G)$ e, por isso, temos que $G/O_{p',p}(G)$ é isomorfo a um grupo de automorfismos lineares de V e, como sabemos, $O_p(G/O_{p',p}(G)) = 1$. Seja $\rho : G \longrightarrow Aut_{\mathbb{F}_p}(V)$ o homomorfismo determinado pela ação de G em V. Se $y \in P \cap O_{p',p}(G)$, $x \in P$ e

$$(yA)(\rho(x) - 1)^{p^n - 1} \neq 1,$$

afirmamos que $x^{p^n} \neq 1$ ou $(xy)^{p^n} \neq 1$. Inicialmente, dado que $\mathbb{F}_p$ é um corpo de característica p, em $\mathbb{F}_p[X]$ temos que $(x-1)^p = \sum_{i=0}^{p} \binom{p}{i} (-1)^i x^{p-i} = x^p - 1$. Por indução em n obtemos que $(x-1)^{p^n} = x^{p^n} - 1$ para todo $n \geqslant 1$. Por outro lado, $(x-1)^{p^n} = (x-1)^{p^n - 1}(x-1)$ e, portanto, $(x-1)^{p^n-1} = 1 + x + \cdots + x^{p^n-1}$, para todo $n \geqslant 1$. Pelo item (ii) do Teorema 1.41, temos que

$$x^{-p^n}(xy)^{p^n}A = (yA)(1 + \rho(x) + \cdots + \rho(x)^{p^n-1}) = (yA)(\rho(x) - 1)^{p^n-1} \neq 1.$$

Ainda, se $y \in P \cap O_{p',p}(G)$, $x \in P$ e

$$(yA)(\rho(x) - 1)^{2p^n - 1} \neq 1,$$

então $[(xy)^{p^n}, x^{p^n}] \neq 1$. De fato, se $v = (yA)(\rho(x) - 1)^{p^n - 1}$, pelo item (ii) do Teorema 1.41 temos que

$$v = (yA)(1 + \cdots + \rho(x)^{p^n-1}) = x^{-p^n}(xy)^{p^n}A.$$

Segue pelo item (i) do Teorema 1.41 que

$$1 \neq v(\rho(x)-1)^{p^n} = v(\rho(x^{p^n})-1) = [x^{-p^n}(xy)^{p^n}, x^{p^n}]A = [(xy)^{p^n}, x^{p^n}]A.$$

Para a prova do item (i) do Teorema 4.16, seja $n = e_p(G/O_{p',p}(G))$. Desde que P é um p–subgrupo de Sylow de G, vemos que $PO_{p',p}(G)/O_{p',p}(G)$ é um p–subgrupo de Sylow de $G/O_{p',p}(G)$ e existe $x \in P$ de modo que $|xO_{p',p}(G)| = p^n = |\rho(x)|$.

Afirmamos que não existe inteiro positivo n_0 tal que $p^{n_0}-1$ seja potência de um primo q e os q–subgrupos de Sylow de G sejam não–abelianos. De fato, se existem inteiros positivos n_0, b e um primo q tal que $p^{n_0}-1 = q^b$, então pelo Lema 4.14, temos que valem uma das seguintes

(a) $p = 2$, $b = 1$, n_0 é primo de $q = 2^{n_0}-1$ é primo de Mersenne;

(b) $q = 2$, $n_0 = 1$, $b = 2^m$ e $p = 2^{2^m}+1$ é primo de Fermat;

(c) $p^{n_0} = 9$ e $q^b = 8$.

As condições do teorema, portanto, verificam nossa afirmação. Pelo Teorema 4.12, o polinômio minimal de $\rho(x)$ é $(t-1)^{p^n}$. Desde que $O_{p',p}(G) \trianglelefteq G$, temos que $P \cap O_{p',p}(G)$ é p–subgrupo de Sylow de $O_{p',p}(G)$ e consequentemente $(P \cap O_{p',p}(G))A/A$ é o p–subgrupo de Sylow de $O_{p',p}(G)/A$. Ora, desde que $O_{p',p}(G)/A$ é um p–grupo, $(P \cap O_{p',p}(G))A/A = O_{p',p}(G)/A$, isso, é $(P \cap O_{p',p}(G))A = O_{p',p}(G)$. Deste modo, existe $y \in P \cap O_{p',p}(G)$ tal que

$$(yA)(\rho(x)-1)^{p^n-1} \neq 1.$$

Pelas nossas considerações iniciais, vemos que $x^{p^n} \neq 1$ ou $(xy)^{p^n} \neq 1$. Isso é, $e_p(G) > n$, o que conclui a prova do item (i).

Para a prova do item (ii), suponha que $p \geqslant 3$. Vamos mostrar que $e_p^*(G/O_{p',p}(G)) \leqslant e_p^*(G)-1$.

Suponha inicialmente que $e_p^*(G/O_{p',p}(G)) = 2n$. Desde que p divide a ordem de G, temos que $e_p(G) \geqslant 1$ e então $e_p^*(G) \geqslant 1$. O resultado segue se $2n = 0$. Nós podemos, então, supor que $2n > 0$. Sabemos que $PO_{p',p}(G)/O_{p',p}(G)$ é p–subgrupo de Sylow de $G/O_{p',p}(G)$. Logo, desde que $\mu_{2n-1}(G/O_{p',p}(G)) \neq 1$, existem $x_1, x_2 \in P$ tais que $[x_1^{p^{n-1}}, x_2^{p^{n-1}}]O_{p',p}(G) \neq 1$. Portanto, $\rho(x_1)^{p^{n-1}}$ e $\rho(x_2)^{p^{n-1}}$ não comutam. Pelo Teorema 4.13, temos que $(\rho(x_1)-1)^{p^n-1} \neq 0$ ou que $(\rho(x_2)-1)^{p^n-1} \neq 0$. Escreva x para o elemento satisfazendo a diferença anterior. Então, desde que $O_{p',p}(G) = (P \cap O_{p',p}(G))A$, existe $y \in P \cap O_{p',p}(G)$ tal que

$$(yA)(\rho(x)-1)^{p^n-1} \neq 0.$$

Pelas considerações iniciais, vemos que $x^{p^n} \neq 1$ ou $(xy)^{p^n} \neq 1$. Isso é, $\mu_{2n}(P) \neq 1$ e $e_p^*(G) > 2n$. Finalmente, podemos supor que $e_p^*(G/O_{p',p}(G)) = 2n+1$. Neste caso, $e_p(G/O_{p',p}(G)) = n+1$ e existe $x \in P$ tal que $|xO_{p',p}(G)| = |\rho(x)| = p^{n+1}$. Pelo Teorema 4.12, o polinômio minimal de $\rho(x)$ é $(t-1)^{p^r}$ com $r \leqslant p^{n+1}$. Mas, mais do que isto, vale $r \geqslant p^{n+1} - p^n$.

Como $p \geqslant 3$, mostra-se por indução que $p^m \geqslant 3p^{m-1}$ para todo inteiro positivo m. Então, temos que $r \geqslant p^{n+1} - p^n \geqslant 2p^n > 2p^n - 1$. Por isso, existe $y \in P \cap O_{p',p}(G)$ tal que

$$(yA)(\rho(x) - 1)^{2p^n - 1} \neq 1.$$

Pelas considerações iniciais, vemos que $[(xy)p^n, x^{p^n}] \neq 1$. Isso mostra que $\mu_{2n+1}(P) \neq 1$ e por isso $e_p^*(G) > 2n+1 = e_p^*(G/O_{p',p}(G))$. □

Teorema 4.17. *([12, pág. 451, Teorema 4.3]) Suponha que G seja um grupo finito p–solúvel, p um primo. Sejam $l_p = l_p(G)$ o p–comprimento de G e $p^{e_p(G)}$ o expoente de um p–subgrupo de Sylow de G. Então, valem as seguintes.*

(i) $l_p \leqslant e_p(G)$ se for satisfeita uma das seguintes condições:

- *(a) p é impar e não é primo de Fermat;*
- *(b) p é primo de Fermat e os 2–subgrupos de Sylow de G são abelianos;*
- *(c) $p = 2$ e os q–subgrupos de Sylow de G são abelianos para todos primo de Mersenne q.*

(ii) Se p é primo de Fermat, então $l_p \leqslant 2e_p(G)$.

Demonstração. Façamos nossa prova de (i) por indução em l_p. Se $l_p \leqslant 1$, nada temos a fazer. Se $l_p > 1$, o p–comprimento de $\overline{G} = G/O_{p',p}(G)$ é $l_p - 1$. Por indução, temos que $l_p - 1 \leqslant e_p(\overline{G})$. Por outro lado, pelas condições $(a) - (c)$ e o Teorema 4.16, temos que $e_p(\overline{G}) \leqslant e_p(G) - 1$. Logo, temos que $l_p \leqslant e_p(G)$ e (i) está verificado.

Para a prova de (ii), usamos indução em l_p para verificar que $l_p \leqslant e_p^*(G)$. Se $l_p \leqslant 1$, nada temos a fazer. Se $l_p > 1$, então por indução temos que $l_p - 1 \leqslant e_p^*(G/O_{p',p}(G)) \leqslant e_p^*(G) - 1$, isso é, $l_p \leq e_p^*(G)$. Nossa afirmação está verificada. Finalmente, temos que $l_p \leqslant e_p^*(G) \leqslant 2e_p(G)$. □

Note que o Teorema 4.17 não estabelece um limite no 2–comprimento de um grupo finito 2–solúvel arbitrário. Este resultado foi estabelecido em [5] por F. Gross no caso particular de grupos solúveis. Em [5], F. Gross mostra que o 2–comprimento de um grupo finito solúvel G de ordem par é no máximo $2e_2(G) - 1$. Deste modo, pelo Teorema 4.17, para cada grupo finito solúvel G e primo p vale que $l_p(G) \leqslant 2e_p(G)$. Em outras palavras, o p–comprimento

de um grupo finito solúvel G é limitado superiormente por uma função do expoente de um p–subgrupo de Sylow de G.

Podemos, portanto, demonstrar o principal resultado desta seção. No que segue, lembramos que para cada grupo finito solúvel G, $F(G)$ denota o subgrupo de Fitting de G e $h(G)$ denota a altura de Fitting de G.

Teorema 4.18 (A. Shalev)**.** *A altura de Fitting de um grupo finito solúvel de expoente $n = p_1^{e_1} \dots p_n^{e_n}$ é limitada superiormente por uma função de n.*

Demonstração. Seja G um grupo finito solúvel e defina

$$b(G) = \prod_{p \in \mathbb{P}} (l_p(G) + 1).$$

Vamos mostrar por indução em $|G|$ que

$$h(G) < b(G). \tag{4.9}$$

Note que tal desigualdade já vale na classe dos grupos finitos nilpotentes.

Suponha que $|G| > 1$ e $h(Q) < b(Q)$ para todo grupo finito solúvel Q com $|Q| < |G|$. Suponha inicialmente que G possui dois subgrupos normais minimais distintos H e K. Então, $H \cap K = 1$ e G é isomorfo a um subgrupo do grupo $(G/H) \times (G/K)$. Pelos Lemas 1.34 e 1.35, vemos que

$$h(G) \leqslant h((G/H) \times (G/K)) = \max\{h(G/H), h(G/K)\}. \tag{4.10}$$

Por outro lado, por hipótese de indução temos que

$$\max\{h(G/H), h(G/K)\} < \max\{b(G/H), b(G/K)\}. \tag{4.11}$$

Pelo Lema 1.38, temos que $b(G/H), b(G/K) \leqslant b(G)$. Segue-se que $h(G) < b(G)$.

Podemos, portanto, assumir que G possui um único subgrupo normal minimal. Neste caso, desde que G é solúvel, pelo Lema 1.31, tal subgrupo é um p–grupo abeliano elementar para algum primo p e, mais do que isto, $O_q(G) = 1$ para cada primo q diferente de p. Deste modo, temos que $O_{p'}(G) = 1$ e $O_{p',p}(G) = O_p(G) = F(G)$. Desde que $F(G) \neq 1$, por hipótese de indução, temos que $h(G/F(G)) < b(G/F(G))$, isso é,

$$h(G/F(G)) < \prod_{q \in \mathbb{P}} (l_q(G/F(G)) + 1). \tag{4.12}$$

Desde que p divide a ordem de G e $F(G) = O_{p',p}(G)$, temos que $l_p(G/F(G)) = l_p(G) - 1$. Segue-se que

$$\prod_{q\in\mathbb{P}}(l_q(G/F(G))+1) < \prod_{q\in\mathbb{P}}(l_q(G)+1) = b(G). \tag{4.13}$$

Finalmente pelo Lema 1.36 temos que $h(G) = h(G/F(G)) + 1$. Segue das desigualdades em (4.12) e (4.13) que $h(G) = h(G/F(G)) + 1 \leqslant b(G/F(G)) < b(G)$. Nossa afirmação está verificada.

Se G é um grupo finito solúvel, verificamos que

$$h(G) < \prod_{p\in\mathbb{P}}(l_p(G)+1).$$

Assim, pelo Teorema 4.17 e o comentário antes do Teorema 4.18, temos que

$$h(G) < \prod_{p\in\mathbb{P}}(l_p(G)+1) \leqslant \prod_{p\in\mathbb{P}}(2e_p(G)+1). \tag{4.14}$$

Finalmente desde que, para cada grupo finito G, o expoente de G é o produto dos expoentes de seus subgrupos de Sylow, (4.14) mostra que a altura de Fitting de um grupo finito solúvel de expoente n é limitada superiormente por uma função de n. □

4.4 O Teorema Principal de A. Shalev

Na seção final deste trabalho temos como objetivo demonstrar o Teorema 4.1, obtido em [28, Teorema 1.1] por A. Shalev, que diz o seguinte: se um grupo de torção residualmente–finito G, sem 2–elementos, é agido por um 2–grupo finito Q de modo que $C_G(Q)$ é solúvel ou de expoente finito, então G é localmente finito. Para isto, inicialmente demonstramos um resultado de A. Turull sobre altura de Fitting de grupos finitos solúveis e posteriormente demonstramos um resultado sobre grupos residualmente–(finito solúveis).

Para cada grupo finito G, seja $|G| = p_1 \dots p_n$, com $p_1, \dots, p_n$ primos não necessariamente distintos. Definimos $k(G) = n$, isto é, $k(G)$ é o número de primos dividindo a ordem de G, contando-se as multiplicidades.

Em 1964, no artigo *Automorphisms of Solvable Groups*, J.G. Thompson iniciou o estudo de relações entre a altura de Fitting de um grupo finito solúvel G, agido coprimamente por um grupo finito Q, com a altura de Fitting do centralizador $C_G(Q)$. Mais especificamente, J.G. Thompson provou o seguinte resultado cuja prova pode ser encontrada em [33].

Teorema 4.19 (Thompson)**.** *Seja G um grupo finito solúvel agido por um grupo finito solúvel Q e suponha que $(|Q|,|G|)=1$. Então, $h(G)\leqslant 5^{k(Q)}h(C_G(Q))$.*

Posteriormente em [18], H. Kurzweil melhorou o resultado de Thompson na seguinte versão.

Teorema 4.20 (Kurzweil)**.** *Seja G um grupo finito solúvel agido coprimamente por um grupo finito solúvel Q. Então, $h(G)\leqslant 4k(Q)+h(C_G(Q))$.*

Finalmente em 1984, no artigo *Fitting Height of Groups and of Fixed Points*, A. Turull melhorou o resultado de Kurzweil obtendo, como prova em seu artigo, o melhor resultado possível, que enunciamos a seguir.

Teorema 4.21 (A. Turull)**.** *Seja G um grupo finito solúvel agido por um grupo finito solúvel Q e suponha que $(|Q|,|G|)=1$. Nestas condições, $h(G)\leqslant 2k(Q)+h(C_G(Q))$.*

Sendo o Resultado de Turull o melhor possível, fazemos sobre ele algumas considerações.

Para a prova do Teorema 4.21, A. Turull utilizou a ferramenta de torres de grupos que vamos descrever a seguir.

Sejam Q e G dois grupos finitos e suponha que Q age em G. Uma Q–torre de G de altura $h\geqslant 1$ é uma sequência $(P_i)_{i=1,\ldots,h}$ de subgrupos Q–invariantes de G para a qual valem as seguintes condições:

(i) P_i é p_i–grupo, p_i um primo, para cada $i=1,\ldots,h$.

(ii) $P_i\leq N_G(P_j)$ sempre que $1\leqslant i<j\leqslant h$.

(iii) Os grupos definidos pelas regras

  (a) $P_h'=P_h$

  (b) $P_i'=P_i/C_{P_i}(P_{i+1}'), i=1,\ldots h-1,$

  são não triviais.

(iv) $p_i\neq p_{i+1}$ para cada $i=1,\ldots,h-1$.

O Teorema 4.21 decorre dos seguintes resultados, cujas provas podem ser encontradas em [34, Lemas 1.5, 1.9 e Teorema 3.1], respectivamente.

Teorema 4.22. *Sejam Q e G dois grupos finitos, Q agindo em G, e $(P_i)_{i=1,\ldots,h}$ uma sequência de subgrupos Q–invariantes satisfazendo as condições $(i)-(iii)$ da definição de Q–torre. Nestas condições, para qualquer função crescente $f:\{1,\ldots,h_1\}\longrightarrow\{1,\ldots,h\}$, definindo-se $P_i^1=P_{f(i)}$ para cada $i=1,\ldots,h_1$, temos que $(P_i^1)_{i=1,\ldots,h_1}$ satisfaz as condições $(i)-(iii)$ da definição de Q–torre.*

Teorema 4.23. *Seja G um grupo finito solúvel e Q um grupo finito agindo em G tal que $(|Q|,|G|)=1$. Então, a altura de Fitting de G é a maior altura de uma Q–torre $(P_i)_{i=1,\ldots,h}$ de G.*

Teorema 4.24. *Seja Q um p–grupo de ordem prima agindo no grupo finito G tal que p não divide $|G|$. Seja $(P_i)_{i=1,\ldots,h}$ uma Q–torre de G e assuma que Q centraliza P_k (possivelmente com $k=0$ e $P_k=1$). Então, existe um $j\geqslant k$ de modo que $(C_{P_i}(Q))_{i=1,\ldots,j-1,j+1,\ldots,h}$ satisfaz as condições $(i)-(iii)$ da definição de Q–torre. Se $2\nmid|P_k|$, então podemos tomar $j>k$.*

Vamos mostrar como destes últimos resultados podemos provar o Teorema 4.21.

Sejam Q e G dois grupos finitos solúveis de ordens coprimas e suponha que Q age em G. Vamos provar por indução em $|Q|$ que vale $h(G)\leqslant 2k(Q)+h(C_G(Q))$. Suponha inicialmente que $|Q|$ não é número primo. Desde que Q é grupo finito solúvel, pelo Lema 1.29, podemos escolher $N\trianglelefteq Q$ de modo que $|Q/N|$ é um número primo p. Por indução, temos que $h(G)\leqslant 2k(N)+h(C_G(N))$. Por outro lado, desde que $N\trianglelefteq Q$, a ação de Q em G induz uma ação de Q/N em $C_G(N)$. Novamente por indução, temos que $h(C_G(N))\leqslant 2k(Q/N)+h(C_{C_G(N)}(Q/N))=2+h(C_G(Q))$, pois $C_{C_G(N)}(Q/N)=C_G(Q)$ e $|Q/N|$ é número primo. Disto, segue-se que

$$h(G)\leqslant 2k(N)+h(C_G(N))\leqslant 2k(N)+2+h(C_G(Q))=2k(Q)+h(C_G(Q)).$$

Podemos, portanto, supor que Q é um grupo de ordem prima agindo no grupo finito solúvel G tal que $(|Q|,|G|)=1$. Pelo Teorema 4.23, $h(G)$ é a maior altura de uma Q–torre de G. Se $h=h(G)$ é a altura de Fitting de G, podemos tomar $(P_i)_{i=1,\ldots,h}$ uma Q–torre de G. Pelo Teorema 4.24, existe um $j\geqslant 0$ de modo que $(C_{P_i}(Q))_{i=1,\ldots,j-1,j+1,\ldots,h}$ satisfaz as condições $(i.)$–$(iii.)$ da definição de Q–torre. Pelo Teorema 4.22, a partir desta sequência podemos obter uma Q–torre de $C_G(Q)$. Novamente pelo Teorema 4.23, temos que $h(C_G(Q))\geqslant h(G)-2$, isso é, $h(G)\leqslant 2+h(C_G(Q))$. Desde que $k(Q)=1$, Teorema 4.21 está demonstrado.

Anterior à prova do Teorema 4.1, mostramos mais um único resultado sobre grupos residualmente–(finito solúvel). Lembramos que um grupo G é residualmente–(finito solúvel) se para todo $1\neq g\in G$ existem um grupo finito solúvel F e um homomorfismo $\varphi: G\longrightarrow F$ de modo que $g^{\varphi}\neq 1$.

Lema 4.25. *Sejam h um inteiro positivo e G um grupo finitamente gerado e residualmente–(finito solúvel). Suponha que todo fator finito de G é solúvel com altura de Fitting no máximo h. Então, existe uma série de subgrupos característicos*

$$G=G_1\geq G_2\geq\cdots\geq G_h\geq G_{h+1}=1$$

tal que G_i/G_{i+1} é residualmente–(finito nilpotente) para todo $i=1,\ldots,h$.

Demonstração. Desde que G é finitamente gerado, podemos utilizar um resultado de M. Hall [14] que afirma que todo grupo finitamente gerado possui somente um número finito de subgrupos com um mesmo índice finito fixado. Portanto, se A é um subgrupo normal de índice finito em G, temos que $\{A^{\varphi};\ \varphi \in Aut(G)\}$ é um conjunto finito. Segue-se que $A' = \bigcap_{\varphi \in Aut(G)} A^{\varphi}$ é um subgrupo característico de índice finito em G contido em A.

Vamos provar este resultado por indução em h. Se $h = 1$, G é residualmente–(finito nilpotente) e o resultado segue. Se $h > 1$, seja H a intersecção de todos os subgrupos normais N de índice finito de G tais que $h(G/N) \leqslant h-1$. Então, $H \trianglelefteq G$. Dado que o subgrupo $\cap\{N/H;\ N \trianglelefteq G, [G:N] < \infty \text{ e } h(G/N) \leqslant h-1\}$ é trivial em G/H, o Teorema 3.1 mostra que G/H é residualmente–(finito solúvel). Mais do que isto, por definição de H, todo fator finito de G/H é solúvel com altura de Fitting no máximo $h-1$. Por indução, podemos tomar uma série

$$1_{G/H} = (H/H) = G_h/H \leq G_{h-1}/H \leq \cdots \leq G_1/H = G/H$$

de subgrupos característicos de G/H, tal que todo fator da série é residualmente–(finito nilpotente).

Seja K a intersecção dos subgrupos característicos N de índice finito em G tais que $h(G/N) \leq h-1$. Claramente $H \leq K$. Seja M um subgrupo normal de índice finito em G tal que $h(G/M) \leqslant h-1$. Desde que G é finitamente gerado, pelas considerações iniciais temos que M contém um subgrupo N, característico e de índice finito em G, e tal que $h(G/N) = h(G/M) \leqslant h-1$. Por definição temos que $K \leq N \leq M$. Isso mostra que $K \leq H$, isso é, $H = K$ e H é subgrupo característico de G. Portanto, temos que

$$1 = G_{h+1} \leq H = G_h \leq \cdots \leq G_1 = G \tag{4.15}$$

é uma série de subgrupos característicos de G. Desde que para todo $i = 1, \ldots, h-1$ vale que G_i/G_{i+1} é grupo residualmente–(finito nilpotente), o resultado estará verificado se mostrarmos que H é residualmente–(finito nilpotente).

Seja $1 \neq g \in H$. Desde que G é residualmente–(finito solúvel) podemos tomar $S \trianglelefteq G$ de índice finito e tal que $g \notin S$. Agora, $g \notin S$ mostra que $h(G/S) = h$. Podemos então tomar uma série

$$1_{G/S} = S/S \leq S_h/S \leq \cdots \leq S_1/S = G/S$$

de subgrupos normais de G/S tal que todo fator da série é um grupo finito nilpotente. Note que $h(G/S_h) \leqslant h-1$ e então $H \leq S_h$. Dado que $H/(H \cap S) \cong HS/S \leq S_h/S$, temos que $H/(H \cap S)$ é grupo finito nilpotente. Como $g \notin H \cap S$, obtemos um subgrupo normal de H não contendo g

e cujo grupo quociente obtido é finito e nilpotente. A arbitrariedade da escolha de $1 \neq g \in H$ mostra que H é residualmente–(finito nilpotente). □

Estamos prontos para demonstrar o Teorema 4.1.

Demonstração do Teorema 4.1. Seja G um grupo de torção, sem 2–elementos, sendo agido por um 2–grupo finito Q de modo que $C_G(Q)$ é solúvel ou de expoente finito. Iremos provar que G é localmente finito. Sejam $x_1,\ldots,x_n \in G$ elementos arbitrários. Pondo $X = \{x_1,\ldots,x_n\}$, temos que $X^Q := \{x_i^q; i = 1,\ldots,n \text{ e } q \in Q\}$ é finito, desde que Q é 2–grupo finito. Ainda, $\langle X\rangle \leq \langle X^Q\rangle$. Agora, $\langle X^Q\rangle$ é Q–invariante e $C_{\langle X^Q\rangle}(Q) = \langle X^Q\rangle \cap C_G(Q)$ é solúvel ou de expoente finito. Portanto podemos supor, sem perda de generalidade, que G é finitamente gerado.

Suponha inicialmente que $C_G(Q)$ é solúvel. Seja $N \trianglelefteq G$ um subgrupo Q–invariante de índice finito. Desde que G não possui 2–elementos, temos que G/N é grupo finito de ordem ímpar. Pelo Teorema 1.30, temos que G/N é solúvel. Pelo Teorema 1.12, temos que $C_{G/N}(Q) = C_G(Q)N/N$ e, portanto, $h(C_{G/N}(Q)) \leqslant h(C_G(Q))$. Segue do Teorema 4.21 que

$$h(G/N) \leqslant 2k(Q) + h(C_{G/N}(Q)) \leqslant 2k(Q) + h(C_G(Q)). \tag{4.16}$$

Por um lado vemos que a altura de Fitting de qualquer fator finito de G por um subgrupo normal Q–invariante N de G é limitada por uma função que não depende da escolha de N.

Por outro lado, desde que G é finitamente gerado, todo subgrupo normal de índice finito em G contém um subgrupo característico de índice finito em G.

As considerações anteriores mostram que todo quociente finito de G é solúvel com altura de Fitting limitada superiormente por $m = 2k(Q) + h(C_G(Q)$. Pelo Lema 4.25 podemos tomar uma série de subgrupos característicos

$$G = G_1 \geq G_2 \geq \cdots \geq G_m \geq G_{m+1} = 1$$

da qual todo fator é residualmente–(finito nilpotente). Ora, para cada $i = 1,\ldots,m$, Q age no grupo G_i/G_{i+1} e pelo Lema 1.12 temos que

$$C_{G_i/G_{i+1}}(Q) = C_{G_i}(Q)G_{i+1}/G_{i+1} = (C_G(Q) \cap G_i)G_{i+1}/G_{i+1}$$

é solúvel. Pelo Teorema 4.6, temos que G_i/G_{i+1} é localmente finito para cada $i = 1,\ldots,m$. O Lema 4.5 então mostra que G é localmente finito. Isto conclui o caso da demonstração em que $C_G(Q)$ é solúvel.

Podemos, então, assumir que $C_G(Q)$ é de expoente finito. Seja $N \trianglelefteq G$ um subgrupo Q–invariante de índice finito em G. Novamente pelo Teorema 1.30 temos que G/N é solúvel e,

pelo Teorema 1.12, temos que $C_{G/N}(Q) = C_G(Q)N/N$. Em particular, $C_{G/N}(Q)$ tem expoente dividindo $exp(C_G(Q))$. Escrevendo $exp(C_G(Q)) = p_1^{e_1} \dots p_r^{e_r}$, temos pelo Teorema 4.18 que

$$h(C_{G/N}(Q)) = h(C_G(Q)N/N) \leqslant \prod_{i=1}^{r}(2e_i + 1).$$

Novamente pelo Teorema 4.21, temos que

$$h(G/N) \leqslant 2k(Q) + h(C_{G/N}(Q)) \leqslant 2k(Q) + \prod_{i=1}^{r}(2e_i + 1).$$

Isso é, a altura de Fitting de todo quociente finito de G por um subgrupo normal Q–invariante N é limitada por uma função que não depende da escolha de N. O resultado segue exatamente como no caso onde $C_G(Q)$ é solúvel. □

Na introdução ao Capítulo 4, vimos que V.P. Shunkov prova em [32] que se G é um grupo de torção possuindo uma involução cujo centralizador é finito, então G é localmente finito. Ainda, vimos que P. Shumyatsky prova em [30] que se G é um grupo de torção residualmente finito possuindo um 4–subgrupo cujo centralizador é finito, então, G é localmente finito. Iremos finalmente, expor a prova do Corolário 4.2, generalizando os resultados de V.P. Shunkov e P. Shumyatsky.

Demonstração do Corolário 4.2. Seja G um grupo de torção residualmente finito possuindo um 2–subgrupo finito Q cujo centralizador $C_G(Q)$ é finito. Como $C_G(Q)$ é finito e G é residualmente finito, existe um subgrupo normal $N \trianglelefteq G$ de índice finito tal que $C_G(Q) \cap N = 1$. Desde que $N \trianglelefteq G$, temos que Q age em N e por hipótese temos que $C_N(Q) = N \cap C_G(Q) = 1$. Pelo Teorema 1.13, N não possui 2–elementos. Portanto, pelo Teorema 4.1, podemos concluir que N é localmente finito. Posto que ambos N e G/N são localmente finitos, pelo Lema 4.3 concluímos que G é localmente finito. □

O trabalho de A. Shalev evidencia que para a conclusão de que um grupo de torção residualmente finito G seja localmente finito, um caminho próspero a ser seguido é o de impor condições em centralizadores. Por exemplo, sendo G e Q como nas condições do Teorema 4.1, pode-se provar que G é localmente finito se assumirmos que $C_G(Q)$ satisfaz uma condição de Engel ou, utilizando o Lema 1.34 e o Teorema 4.18, se assumirmos que $C_G(Q)$ possui uma cadeia finita de subgrupos normais tal que todo fator da série é solúvel ou de expoente finito.

Ainda, observamos que variações do Teorema 4.1 podem ser obtidas encontrando-se resultados que limitem a altura de Fitting de grupos finitos solúveis.

Se A é qualquer grupo finito, denotamos por $q(A)$ o maior primo dividindo a ordem de A. Seguindo as ideias de Shalev, P. Shumyatsky prova em [29] uma generalização do Teorema 4.1, que expomos a seguir.

Teorema 4.26 (P. Shumyatsky)**.** *Seja A um grupo finito solúvel agindo num grupo de torção residualmente finito G. Suponha que todo elemento de G tem ordem coprima com $|A|$ e $C_G(A)$ é solúvel ou tem expoente finito. Nestas condições, se todo subgrupo $(q(A)-1)$–gerado de G é finito e solúvel, temos que G é localmente finito.*

Observe que nas condições do Teorema 4.26, se $q(A) = 2$, então A é 2–grupo finito e por isso obtemos o Teorema 4.1.

Finalmente observamos que P. Shumyatsky ainda obtém em [29] a seguinte generalização do Corolário 4.2.

Corolário 4.27 (P. Shumyatsky)**.** *Sejam G um grupo residualmente finito e q um primo. Suponha que todo subgrupo 2–gerado de G é finito e que G possui um q–subgrupo finito Q tal que $C_G(Q)$ é finito. Nestas condições, G é localmente finito.*

Bibliografia

[1] Y.A. Bahturin and M.V. Zaicev. Identities of graded algebras. *J. Algebra*, 205:1 – 12, 1998.

[2] W. Feit and J.G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.

[3] E.S. Golod. On nil-algebras and finitely approximable *p*–groups. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:273 – 276, 1964.

[4] D. Gorenstein. *Finite groups*. Chelsea Publishing Company, New York, 1980.

[5] F. Gross. The 2-length of a finite solvable group. *Pacific J. Math*, 15:1221–1237, 1965.

[6] N. Gupta and S.N. Sidki. On the Burnside Problem for periodic groups. *Math. Z.*, 182:385–388, 1983.

[7] P. Hall and G. Higman. On the p-length of p-soluble groups and reduction theorems for Burnside's Problem. *Proc. Lond. Math. Soc.*, s3-6:1–42, 1956.

[8] B. Hartley. Centralizers in locally finite groups. In O.H. Kegel, F. Menegazzo, and G. Zacher, editors, *Group Theory: Proceedings of a Conference held at Brixen/Bressanone*, volume 1281, pages 36–51. Springer, 1987.

[9] B. Hartley. A general Brauer-Fowler theorem and centralizers in locally finite groups. *Pacific J. Math.*, 152:101 – 117, 1992.

[10] G. Higman. A finitely generated infinite simple group. *J. Lond. Math. Soc.*, s1-26:61–64, 1951.

[11] B. Huppert. *Endliche Gruppen I*. Springer, Berlin, 1967.

[12] B. Huppert and N. Blackburn. *Finite Groups II*. Springer, Berlin, 1 edition, 1982.

[13] I.M. Isaacs. *Finite Group Theory*. American Mathematical Society, 2008.

[14] M. Hall Jr. A topology for free groups and related groups. *Ann. of Math.*, 52:127–139, 1950.

[15] A.I. Kostrikin. Lie rings satisfying an Engel condition. *Dokl. Akad. Nauk SSSR*, 108:580–582, 1956.

[16] A.I. Kostrikin and E.I. Zelmanov. A theorem on sandwich algebras. *Tr. Mat. Inst. Steklova*, 183:106–111, 1990.

[17] A.G. Kurosh. Non-associative free algebras and free products of algebras. *Mat. Sb.*, 20:239–262, 1947.

[18] H. Kurzweil. p-Automorphismen von auflösbaren p'-gruppen. *Math. Z.*, 120:326–354, 1971.

[19] H. Kurzweil and B. Stellmacher. *The Theory of Finite Groups: An Introduction*. Springer, New York, 2004.

[20] M.P. Lazard. Sur les groups nilpotents et les anneaux de lie. *Ann. Sci. Éc. Norm. Supér.*, 71:101–190, 1954.

[21] P.S. Novikov and S.I. Adian. Infinite periodic groups I. *Math. USSR Izv*, 2:209–236, 1968.

[22] P.S. Novikov and S.I. Adian. Infinite periodic groups II. *Math. USSR Izv*, 2:241–479, 1968.

[23] P.S. Novikov and S.I. Adian. Infinite periodic groups III. *Math. USSR Izv*, 2(3):665–685, 1968.

[24] N.R. Rocco and P. Shumyatsky. On periodic groups having almost regular 2-elements. *Proc. Edinb. Math. Soc. (2)*, 41:385 – 391, 1998.

[25] D.J.S. Robinson. *A Course in the Theory of Groups*. Springer, New York, 2 edition, 1996.

[26] H.E. Rose. *A Course on Finite Groups*. Springer, London, 2009.

[27] J.J. Rotman. *Advanced Modern Algebra*. Prentice Hall, Kent, 2002.

[28] A. Shalev. Centralizers in residually finite torsion groups. *Proc. Amer. Math. Soc.*, 126:3495 – 4399, 1998.

[29] P. Shumyatsky. Centralizers in groups with finiteness conditions. *J. Group Theory*, 1:275–282, 1998.

[30] P. Shumyatsky. On groups having a four-subgroup with finite centralizer. *Q. J. Math.*, 49:491–499, 1998.

[31] P. Shumyatsky. Applications of lie ring methods to group theory. In R. Costa, A. Grishkov, H. Guzzo Jr., and L.A. Peresi, editors, *Nonassociative algebras and its applications, in: Lecture Notes in Pure and Appl. Math.*, volume 211, pages 373–395. CRC Press, New York, 2000.

[32] V.P. Shunkov. On periodic groups having an almost regular involution. *Algebra Logic*, 11:260–272, 1972.

[33] J.G. Thompson. Automorphisms of solvable groups. *J. Algebra*, 1:259 – 267, 1964.

[34] A. Turull. Fitting height of groups and of fixed points. *J. Algebra*, 86:555 – 566, 1984.

[35] J.S. Wilson and E.I. Zelmanov. Identities for lie algebras of pro-p groups. *J. Pure Appl. Algebra*, 81:103 – 109, 1992.

[36] E.I. Zelmanov. Solution of the Restricted Burnside Problem for groups of odd exponent. *Math. USSR Izv*, 36:41 – 60, 1991.

[37] E.I. Zelmanov. Lie ring methods in the theory of nilpotent groups. In *Groups '93*, pages 567–585, Galway-St Andrews, 1995. London Math. Soc. Lecture Note Series 212.

Lista de Símbolos

Símbolo	Significado
$F(G)$	Subgrupo de Fitting do grupo finito G
$\Phi(G)$	Subgrupo de Frattini do grupo G
$O_p(G)$	O produto de todos os p–subgrupos normais de um grupo finito G
$D_n(G)$	O n–ésimo termo da série de Jennings–Lazard–Zassenhaus de um grupo G
$\gamma_n(G)$	O n–ésimo termo da série central inferior do grupo G
$S_p(G)$	O conjunto dos p–subgrupos de Sylow do grupo finito G
$h(G)$	Altura de Fitting do grupo solúvel G
$l_p(G)$	O p–comprimento do grupo finito p–solúvel G
$e_p(G)$	O inteiro k tal que p^k é o expoente de um p–subgrupo de Sylow do grupo finito G
$\delta(g)$	O peso do elemento g com respeito à série de Jennings–Lazard–Zassenhaus do grupo G
G^m	O subgrupo gerado pelas m–ésimas potências dos elementos do grupo G
$L_p(G)$	A álgebra gerada pelo primeiro fator da série de Jennings–Lazard–Zassenhaus do grupo G