Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre Centralizadores de Automorfismos Coprimos em Grupos Finitos

por

Aline de Souza Lima

Brasília

2009

Agradecimentos

A Deus, pelo dom da vida, pelo conhecimento e por me permitir mais essa conquista.

A minha mãe, Maria Abadia, pelo apoio e pelo exemplo de luta e serenidade.

A minha irmã, Joselaine, pela compreensão e amizade.

Aos meus amigos do Departamento de Matemática da UNB, pelos momentos de alegria, companheirismo e trocas de conhecimento. De forma especial ao Evander que esteve sempre pronto para ouvir e ajudar.

Ao meu amigo Jhone que esteve presente em minha vida durante os últimos seis anos e meio, compartilhando todos os momentos de alegrias e tristezas.

Aos meus amigos da República Fernando, Jhone, Jorge, Ricardo e Sandra, que durante quatro anos fizeram o papel de família.

Ao meu orientador professor Pavel Shumyatsky, pela escolha do tema e pela ajuda na construção do meu conhecimento; por sua paciência para com minhas limitações e seu estímulo em meus momentos de cansaço.

Aos professores, Aline Pinto, Antonio Tamarozzi, Pavel Zalesski e Sheila Chagas, pelas correções e sugestões que contribuiram para a versão final deste trabalho.

Aos professores do Departamento de Matemática da UNB e a todos os funcionários, pela prestatividade e paciência que sempre demonstraram.

Ao CNPq/Capes, pelo suporte financeiro.

$\cdots$ *Pedi e lhe será dado; buscai, e achareis; batei, e lhe será aberto.* Lucas 11,9.

Resumo

Seja p um número primo. Seja A um p-grupo abeliano elementar agindo sobre um $p^{'}$-grupo finito G. Neste trabalho realizamos um estudo da influência dos centralizadores dos automorfismos em A sobre a estrutura de G .

Nesse sentido demonstramos que se A tem ordem p^{n+1} e assumindo que existe um inteiro positivo m tal que

$$[C_G(a)^{(d)}, \underbrace{C_G(b)^{(d)}, \cdots, C_G(b)^{(d)}}_{m}] = 1,$$

para todos $a, b \in A^{\#}$, onde $2^d \leq n$, então $G^{(d)}$ é nilpotente de classe $\{p, d, m\}$-limitada. Ainda, assumindo que existe um inteiro positivo m tal que

$$[\gamma_n(C_G(a)), \underbrace{\gamma_n(C_G(b)), \cdots, \gamma_n(C_G(b))}_{m}] = 1,$$

para todos $a, b \in A^{\#}$, então $\gamma_n(G)$ é nilpotente de classe $\{p, n, m\}$-limitada.

Outro resultado é, se A tem ordem p^2 e assumindo que o subgrupo $\langle C_G(a), C_G(b)\rangle$ satisfaz uma lei positiva de grau n para todos $a, b \in A^{\#}$, então G satisfaz uma lei positiva de grau limitado por uma função dependendo somente de n e p.

Abstract

Let p be a prime number. Let A be an elementary abelian p-group acting on a finite p'-group G. In this work we study the influence of the centralizers of the automorphisms in A on the structure of G.

We show that if A has order p^{n+1} and if there exists a positive integer m such that

$$[C_G(a)^{(d)}, \underbrace{C_G(b)^{(d)}, \cdots, C_G(b)^{(d)}}_{m}] = 1$$

for all $a, b \in A^{\#}$, where $2^d \leq n$, then $G^{(d)}$ is nilpotent of $\{p, d, m\}$-bounded class. We also show that if there exists a positive integer m such that

$$[\gamma_n(C_G(a)), \underbrace{\gamma_n(C_G(b)), \cdots, \gamma_n(C_G(b))}_{m}] = 1$$

for all $a, b \in A^{\#}$, then $\gamma_n(G)$ is nilpotent of $\{p, n, m\}$-bounded class.

Another result is that if A has order p^2 and the subgroup $\langle C_G(a), C_G(b)\rangle$ satisfies a positive law of degree n for all $a, b \in A^{\#}$, then G satisfies a positive law of degree bounded by a function depending only on n and p.

Sumário

Introdução

Seja G um grupo finito e α um automorfismo de G. Denotamos o centralizador de α em G, ou subgrupo de pontos fixos, por $C_G(\alpha) = \{x \in G | x^\alpha = x\}$. Se $C_G(\alpha) = 1$ dizemos que α é livre de pontos fixos e se a ordem de α é coprima com a ordem de G, então α é um automorfismo coprimo de G. É bem conhecido que a estrutura de um grupo finito está intimamente relacionada com os subgrupos de pontos fixos de automorfismos do grupo. Vários autores obtiveram resultados interessantes a partir desta relação. A melhor e mais conhecida ilustração da influência do subgrupo de pontos fixos na estrutura de um grupo é que se G admite um automorfismo livre de pontos fixos de ordem prima, então G é nilpotente (Thompson, [30]), e a classe de nilpotência de G é limitada por uma função dependendo somente da ordem do automorfismo (Higman, [9]).

Seja A um p-grupo abeliano elementar não cíclico agindo sobre um p'-grupo finito G. Temos então o subgrupo de pontos fixos $C_G(A) = \{x \in G | x^a = x \textit{ para todo } a \in A\}$ de A em G. Ward, [34] e [35], mostrou que se a ordem de A é maior ou igual que p^3, e se $C_G(a)$ é nilpotente para qualquer $a \in A^\#$, onde $A^\#$ denota o conjunto dos elementos de A diferentes da identidade, então G é nilpotente. Ainda, que se a ordem de A é maior ou igual que p^4, e se o subgrupo derivado $C_G(a)'$ de $C_G(a)$ é nilpotente para todo $a \in A^\#$, então o subgrupo derivado G' de G é nilpotente. Sob as mesmas hipóteses Shumyatsky [25], mostrou que se $C_G(a)$ é nilpotente de classe c (respectivamente $C_G(a)'$ é nilpotente de classe c) para todo $a \in A^\#$, então a classe de nilpotência de G (respectivamente de G') é limitada por uma função dependendo somente de p e c.

Se um grupo G possui automorfismos coprimos podemos estudar as propriedades satisfeitas pelos centralizadores desses automorfismos e averiguar se as mesmas são satisfeitas pelo grupo G, pois em algumas situações o grupo é gerado por esses centralizadores. Seja G um grupo admitindo uma ação de um grupo A. Se A é abeliano não cíclico e a ordem de A é coprima com a ordem de G, então

$$G = \left\langle C_G(a) | a \in A^{\#} \right\rangle .$$

A demonstração desse fato pode ser encontrado em [6, 6.2.1].

Uma condição suficiente para que um p'-grupo finito G seja nilpotente com classe de nilpotência limitada foi obtida por Shumyatsky [26]: sejam p um primo e A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo G e suponha que existe um inteiro positivo m tal que

$$[C_G(a), \underbrace{C_G(b), \cdots, C_G(b)}_{m}] = 1,$$

para quaisquer $a, b \in A^{\#}$. O autor mostrou que a classe de nilpotência de G é limitada por uma função dependendo somente de p e m. Como consequência imediata deste resultado, o autor obteve que se existe um inteiro positivo m tal que $\langle C_G(a), C_G(b) \rangle$, o subgrupo de G gerado por $C_G(a)$ e $C_G(b)$, é nilpotente de classe no máximo c para todos $a, b \in A^{\#}$, então G é nilpotente de classe limitada por uma função dependendo somente de p e m.

O estudo de comutadores de elementos de um grupo G que sobre certas condições garanta a nilpotência de G não é nova. Relembramos aqui idéias bem conhecidas e muito utilizadas no trato com grupos finitos que é a definição de grupo de Engel. Um grupo G é um *grupo de Engel* se para cada par ordenado (x, y) de elementos em G existe um inteiro positivo $n(x, y)$ tal que

$$[y, \underbrace{x, \cdots, x}_{n}] = 1.$$

Se o inteiro $n = n(x, y)$ pode ser escolhido independentemente de x e y, dizemos que G é um *grupo n-Engel*. Agora o resultado de Zorn [33] , diz que um grupo de Engel finito é nilpotente. Logo, a idéia de trabalhar com comutadores dos subgrupos de pontos fixos dos automorfismos coprimos de um grupo G parece muito natural, já que os subgrupos de pontos fixos geram todo o grupo.

Usaremos em todo o trabalho a notação $\{a, b, c, \cdots\}$-limitada sempre que existir uma função limitante dependendo apenas dos parâmetros $a, b, c, \cdots$.

Um dos objetivos deste trabalho, o qual desenvolvemos ao longo do capítulo 3, é mostrar uma generalização do resultado de Shumyatsky [26]. Podemos enunciar tal generalização na forma dos seguintes teoremas.

Teorema 1. *Sejam p um primo, n, d inteiros positivos tais que $2^d \leq n$. Seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre um p'-grupo finito G. Assuma que existe um inteiro positivo m tal que $[C_G(a)^{(d)}, \underbrace{C_G(b)^{(d)}, \cdots, C_G(b)^{(d)}}_{m}] = 1$, para todos $a, b \in A^{\#}$. Então, $G^{(d)}$ é nilpotente de classe $\{p, d, m\}$-limitada.*

Teorema 2. *Sejam p um primo e n um inteiro positivo. Seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre um p'-grupo finito G. Assuma que existe um inteiro positivo m tal que $[\gamma_n(C_G(a)), \underbrace{\gamma_n(C_G(b)), \cdots, \gamma_n(C_G(b))}_{m}] = 1$, para todos $a, b \in A^{\#}$. Então, $\gamma_n(G)$ é nilpotente de classe $\{p, n, m\}$-limitada.*

Mais um exemplo da influência dos centralizadores de automorfismos de ordem coprima de um grupo G na estrutura de G é dado por Khukhro e Shumyatsky [13]: sejam p é um primo, e um inteiro positivo e A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G, assuma que o expoente do $C_G(a)$ divide e para todo $a \in A^{\#}$. Então, o expoente de G é limitado por uma função dependendo somente de e e p. Lembramos que um grupo G tem *expoente* n, se $x^n = 1$ para todo $x \in G$. Denotamos o expoente de um grupo G por $exp(G)$. Mais tarde, Guralnick e Shumyatsky [7] mostraram que se

A tem ordem p^3 e o expoente do subgrupo derivado $C_G(a)'$ divide e para todo $a \in A^{\#}$, então o expoente de G' é limitado por uma função que depende de e e p somente.

Tratamos também a situação onde os subgrupos de pontos fixos satisfazem uma lei positiva. Seja F o grupo livre sobre $X = \{x_1, x_2, \cdots\}$. Uma palavra positiva em X é qualquer elemento não trivial de F não envolvendo os inversos dos x_i. Uma lei positiva de um grupo G é uma identidade não trivial da forma $u \equiv v$, onde u, v são palavras positivas em F, válida para toda substituição $X \to G$. O máximo dos comprimentos de u e v é chamado de grau da lei $u \equiv v$. Um exemplo fácil de lei positiva é $x^e \equiv 1$, onde $e \leq 1$ é um inteiro positivo. Assim, grupos de expoente finito, e em particular grupos finitos, satisfazem uma lei positiva. Outro exemplo é dado por grupos abelianos que satisfazem a lei positiva $xy \equiv yx$. Agora, se $G/Z(G)$ satisfaz a lei $\alpha \equiv \beta$, então G satisfaz $\alpha\beta \equiv \beta\alpha$. Logo, por indução na classe de nilpotência, segue que todo grupo nilpotente de classe c satisfaz uma lei positiva. Malcev [18] mostrou que um grupo que é uma extensão de um grupo nilpotente por um grupo de expoente finito satisfaz uma lei positiva. Mais precisamente, ele exibiu uma lei positiva de duas variáveis $M_c(x, y)$ e de grau 2^c satisfeita em todos os grupos nilpotentes de classe c, conhecida como *lei de Malcev*. Além disso, se G é uma extensão de um grupo nilpotente de classe c por um grupo de expoente e, então G satisfaz a lei positiva $M_c(x^e, y^e)$.

Ol'shanskii e Storozhev [19] deram uma resposta negativa para a recíproca do resultado de Malcev, ou seja, nem todo grupo satisfazendo uma lei positiva é necessariamente a extensão de um grupo nilpotente por um grupo de expoente finito. Mas em contraste com essa resposta negativa, Burns, Macedonska e Medvedev [2] responderam de forma positiva a recíproca do resultado de Malcev para uma grande classe de grupos, incluindo todos os solúveis e os residualmente finitos. Em particular, eles mostraram que existe funções $c(n)$ e $e(n)$ dependendo somente de n, tal que qualquer grupo finito satisfazendo uma lei positiva de grau n é uma extensão de um grupo nilpotente de classse no máximo $c(n)$ por um grupo de expoente dividindo $e(n)$.

Neste contexto, de grupos satisfazendo uma lei positiva, apresentamos mais um exemplo da influência dos subgrupos de pontos fixos na estrutura do grupo G. Seja A um p-grupo abeliano elementar agindo sobre um p'-grupo finito G. Shumyatsky [24] mostrou que se a ordem de A é p^3 e supondo que $C_G(a)$ satisfaz uma lei positiva de grau n, para todo $a \in A^{\#}$, então G satisfaz uma lei positiva de grau limitado por uma função dependendo somente de p e n. Salientamos que este resultado não é válido se o grupo A tem ordem p^2. De fato, pode-se exibir um exemplo de [15]. Seja q um primo impar e denote por t o maior divisor impar de $q-1$. Seja G_k o grupo formado pelas matrises

$$M = \begin{pmatrix} u+qa & qb \\ qc & v+qd \end{pmatrix}$$

de determinante 1, onde a, b, c, d, u, v estão no anel de residuos módulo q^{k+1} e $uv = u^t = 1$ módulo q. Então, G_k tem comprimento derivado m ou $m+1$, onde m é o menor inteiro tal que $2^m \geq k+1$. Sejam α_k e β_k automorfismos de G_k tal que para qualquer

$$M = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in G_k$$

temos que

$$M^{\alpha_k} = (M^{-1})^T \quad \text{e} \quad \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}^{\beta_k} = \begin{pmatrix} a_1 & -a_2 \\ -a_3 & a_4 \end{pmatrix}.$$

É fácil checar que $V_k = \langle \alpha_k, \beta_k \rangle$ é o grupo de Klein agindo sobre G_k livre de pontos fixos. Além disso, o centralizador em G_k de qualquer $\alpha_k \in V_k^{\#}$ é cíclico, logo satisfaz a lei positiva $xy \equiv yx$, e G_k pode ser gerado por 3 elementos. Assim, não existe uma lei positiva que é satisfeita em todos os grupos G_k.

Sob as mesmas hipóteses, Shumyatsky [23] mostrou que esta propriedade vale para o subgrupo derivado G' de G, isto é, se A tem ordem p^4 e $C_G(a)'$ satisfaz uma lei positiva de grau n para todo $a \in A^{\#}$, então G' satisfaz uma lei positiva de grau limitado por uma função dependendo somente de n e p.

Nosso objetivo aqui é mostrar que diminuindo uma unidade do posto de A no resultado original e assumindo que os subgrupos $\langle C_G(a), C_G(b)\rangle$ satisfazem uma lei positiva, para todos $a, b \in A^{\#}$, então G satisfaz uma lei positiva. Tal resultado está demonstrado no quarto capítulo deste trabalho e formalmente pode ser enunciado da seguinte forma.

Teorema 3. *Seja p um primo. Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G. Assuma que $\langle C_G(a), C_G(b)\rangle$ satisfaz uma lei positiva de grau n para todos $a, b \in A^{\#}$. Então, G satisfaz uma lei positiva de grau limitado por uma função dependendo somente de n e p.*

Uma ferramenta efetiva que se mostra de grande ajuda no estudo dos problemas propostos neste trabalho é a teoria de álgebras de Lie. As construções associando à um grupo um anel de Lie foram introduzidas nos anos 30 no contexto do Problema Restrito de Burnside. Neste trabalho, no segundo capítulo, exibimos duas formas distintas e usuais de associar um anel de Lie a um grupo. A primeira delas consiste em tomar a soma direta dos quocientes dos termos da série central inferior de G, que se torna um anel de Lie. Na segunda se utiliza a série de *Jennings-Lazard-Zassenhaus* e se obtem uma álgebra de Lie sobre o corpo com p elementos $\mathbb{F}_p$, onde p é um primo. No segundo capítulo citamos alguns dos principais resultados da teoria de álgebras de Lie que utilizamos no decorrer do trabalho.

Para um melhor esclarecimento das técnicas que utilizamos e entendimento do trabalho que fizemos, a partir dos objetivos propostos anteriormente neste texto, dividimos este trabalho em quatro capítulos. No primeiro capítulo exibimos resultados básicos da teoria de grupos. Alguns destes resultados são bem conhecidos e por este motivo dispensamos as respectivas demonstrações. Por outro lado, também apresentamos certos resultados não tão conhecidos e na medida do possível incluímos suas demonstraçoes como meio de compreendê-los melhor. O segundo capítulo é totalmente dedicado a apresentar resultados sobre álgebras de Lie que são relevantes para a solução dos problemas propostos neste

trabalho como também exibir as técnicas que já vem sendo desenvolvidas a bastante tempo por vários autores e que são cruciais como ferramentas no desenvolvimento tanto da própria teoria de álgebras de Lie como na teoria de grupos como vemos nesste trabalho. No terceiro capítulo desenvolvemos a demonstração dos Teoremas 1 e 2 e no quarto e último capítulo apresentamos a demonstração do Teorema 3.

Capítulo 1

Resultados Preliminares

Na primeira seção deste capítulo preliminar apresentamos algumas definições importantes e já bem conhecidas da teoria de grupos como a definição de grupo solúvel e grupo nilpotente, além de alguns resultados básicos envolvendo comutadores e a série central inferior de um grupo G. Na segunda seção apresentamos o conceito de subgrupo de Fitting generalizado de um grupo, junto com alguns resultados que caracterizam tais subgrupos. A definição de grupo de automorfismos coprimos de um dado grupo G e as relações de tais automorfismos com a estrutura de G podem ser encontradas na terceira seção deste capítulo e sem dúvida desempenham um papel essencial em todos os resultados apresentados neste trabalho. Finalizamos este capítulo com duas pequenas seções, uma sobre p-grupos regulares e p-grupos potentes e a última sobre o dual de um grupo abeliano, com definições e resultados que se fazem úteis no decorrer deste trabalho principalmente no quarto capítulo.

1.1 Resultados Gerais Sobre Grupos

Seja G um grupo e $x_1, x_2, \cdots$ elementos de G. O comutador de x_i e x_j é definido por:

$$[x_i, x_j] = x_i^{-1} x_j^{-1} x_i x_j.$$

De forma mais geral, um comutador simples de peso $n \geq 2$ é definido recursivamente para $x_1, x_2, \cdots, x_n$ elementos arbitrários de G por

$$[x_1, \cdots, x_n] = [[x_1, \cdots, x_{n-1}], x_n],$$

onde por convenção $[x_1] = x_1$. Para simplificar a notação usualmente se escreve

$$[x,_n y] = [x, \underbrace{y, \cdots, y}_{n}].$$

Em particular o *Grupo derivado* G' de G é definido como

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

Tomando repetidamente subgrupos derivados, obtemos a *série Derivada* de G, uma sequência decrescente de subgrupos totalmente invariantes, ou seja, invariante por todos endomorfismos de G

$$G = G^{(0)} \geq G' \geq G^{(2)} \geq \cdots ,$$

onde $G^{(n+1)} = (G^{(n)})'$. Temos que cada quociente $G^{(n)}/G^{(n+1)}$ é abeliano.

Outra importante sequência decrescente de subgrupos de um grupo G, é a *série central inferior* de G

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots ,$$

definida por $\gamma_{n+1}(G) = [\gamma_n(G), G]$. Cada $\gamma_n(G)$ é totalmente invariante em G e ainda $\gamma_n(G)/\gamma_{n+1}(G)$ está no centro de $G/\gamma_{n+1}(G)$.

Já a *série central superior* de um grupo G

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

definida por $Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G))$, é uma sequência crescente de subgrupos

característicos de G, isto é, invariantes por todos automorfismos de G, mas não necessariamente totalmente invariantes em G. Denotamos $Z_1(G) = Z(G)$ que é chamado o *centro* de G.

Lema 1.1.1 (Lema dos Três Subgrupos)**.** *Sejam x, y, z elementos de um grupo G e H, K, L subconjuntos de G. Então, temos que*

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

(ii) Se $[H, K, L] = 1$ *e* $[K, L, H] = 1$*, então* $[L, H, K] = 1$*.*

Demonstração: Temos a seguinte igualdade

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

Faça $a = xzx^{-1}yx$, $b = yxy^{-1}zy$ e $c = zyz^{-1}xz$. Note que b e c são obtidos de a por uma permutação cíclica dos elementos x, y, z. Além disso, $[x, y^{-1}, z]^y = a^{-1}b$. Segue também por permutações cíclicas de x, y, z que $[y, z^{-1}, x]^z = b^{-1}c$ e $[z, x^{-1}, y]^x = c^{-1}a$. Como $(a^{-1}b)(b^{-1}c)(c^{-1}a) = 1$, concluímos o item (i).

Suponha agora que $[H, K, L] = [K, L, H] = 1$. Então, para todos $x \in H$, $y \in K$ e $z \in L$, temos $[x, y^{-1}, z] = [y, z^{-1}, x] = 1$. Logo, pelo item (i), temos $[z, x^{-1}, y] = 1$. Mas $[L, H, K]$ é gerado pelo conjunto de todos os comutadores da forma $[z, x^{-1}, y]$, portanto, $[L, H, K] = 1$. ■

Outro resultado sobre propriedades elementares de comutadores de subgrupos é o seguinte lema, cuja demonstração pode ser encontrada em [6].

Lema 1.1.2. *Sejam H, K e L subgrupos de um grupo G. Então, temos que*

1. *$[H, K]$ é um subgrupo normal de $\langle H, K\rangle$;*
2. *Se H, K e L são subgrupos normais de G, então $[HK, L] = [H, L][K, L]$.*

Lema 1.1.3. *Em qualquer grupo G temos que $[\gamma_i(G), \gamma_j(G)] \subseteq \gamma_{i+j}(G)$.*

Demonstração: Podemos assumir sem perda de generalidade que $\gamma_{i+j}(G) = 1$. Para facilitar a notação faremos $\gamma_k = \gamma_k(G)$, $k = 1, 2, \cdots$.

Usamos indução sobre j. Se $j = 1$ temos por definição $[\gamma_i, \gamma_1] = \gamma_{i+1}$. Assuma $j \geq 2$. Pela hipótese de indução, temos que

$$[\gamma_i, \gamma_{j-1}, \gamma_1] \subseteq [\gamma_{i+j-1}, \gamma_1] \subseteq \gamma_{i+j} = 1 \quad e \quad [\gamma_1, \gamma_i, \gamma_{j-1}] \subseteq [\gamma_{i+1}, \gamma_{j-1}] \subseteq \gamma_{i+j} = 1.$$

Assim, pelo Lema dos Três Subgrupos, $[\gamma_{j-1}, \gamma_1, \gamma_i] = 1$. Portanto, $[\gamma_i(G), \gamma_j(G)] = 1$ como queríamos. ■

Lema 1.1.4. *Seja G um grupo e k um inteiro positivo. Então*

(i) $\gamma_k(G)$ contém todos os comutadores de peso $\geq k$ em G;

(ii) $\gamma_k(G)$ é gerado pelos comutadores simples de peso $\geq k$ em G;

(iii) Se $G = \langle M \rangle$, então $\gamma_k(G)$ é gerado pelos comutadores simples de peso $\geq k$ em M;

(iv) $G^{(k)} \subseteq \gamma_{2^k}(G)$.

Demonstração: Para simplificar a notação faremos $\gamma_i = \gamma_i(G)$, $i = 1, 2, \cdots$.

(i) Vamos usar indução sobre k. Para $k = 1$, $\gamma_1(G) = G$, e a afirmação é verdadeira. Suponha agora que $k \geq 2$ e $r \geq k$. Considere um comutador c de peso r. Então $c = [c_1, c_2]$, onde c_1, c_2 são comutadores de peso r_1 e r_2 respectivamente com $r_1 + r_2 = r$. Pela hipótese de indução $c_1 \in \gamma_{r_1}$ e $c_2 \in \gamma_{r_2}$. Portanto,

$$c = [c_1, c_2] \in [\gamma_{r_1}, \gamma_{r_2}] \subseteq \gamma_{r_1+r_2} = \gamma_r \subseteq \gamma_k.$$

(ii) Denotando por N_k o subgrupo gerado por todos os comutadores simples de peso k e observando que $[x_1, x_2, \cdots, x_k]^y = [x_1^y, x_2^y, \cdots, x_k^y]$, vemos que N_k é normal em G. Pelo que vimos anteriormente, $N_k \subseteq \gamma_k$, logo basta mostrar que $\gamma_k \subseteq N_k$. Novamente usamos indução sobre k. Se $k = 1$ a afirmação é verdadeira. Suponha agora que $k \geq 2$. Então $N_{k-1} \subseteq \gamma_{k-1}$. Note que

$$N_{k-1}/N_k \subseteq Z(G/N_k),$$

o que implica que $[N_{k-1}, G] \subseteq N_k$. Mas $[N_{k-1}, G] = [\gamma_{k-1}, G] = \gamma_k$. Portanto, $\gamma_k \subseteq N_k$ como queríamos.

(iii) Como vimos no item anterior $\gamma_k(G) = \langle [x_1, x_2, \cdots, x_k]/x_i \in G \rangle$. Mas cada x_i pode ser escrito como um produto de elementos de M e seus inversos, pois M gera G. Agora usando propriedades de comutadores, $[ab, c] = [a, c]^b[b, c] = [a, c][a, c, b][b, c]$ e $[a, bc] = [a, c][a, b]^c = [a, c][a, b][a, b, c]$, obtemos o resultado desejado.

(iv) Usamos indução sobre k. Se $k = 1$ não há nada que fazer. Suponha que $k \geq 1$ e que $G^{(k-1)} \subseteq \gamma_{2^{k-1}}(G)$. Pela definição de $G^{(k)}$ e pelo Lema 1.1.3, temos que

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \subseteq [\gamma_{2^{k-1}}, \gamma_{2^{k-1}}] \subseteq \gamma_{2^k}.$$

■

Definição 1.1.5. *Um grupo G é dito* solúvel *se existe um número k tal que $G^{(k)} = 1$. O menor número k tal que essa propriedade seja satisfeita é chamado de* comprimento derivado *de G e é denotado por $dl(G)$.*

Uma série de subgrupos de um grupo G, $1 = H_1 \leq H_2 \leq \cdots \leq H_n = G$, é *subnormal* em G se H_i é normal em H_{i+1}, para todo $i = 1, \cdots, n$.

Definição 1.1.6. *Dizemos que um grupo G é* nilpotente *se G possui uma série subnormal*

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

tal que $G_{i+1}/G_i \leq Z(G/G_i)$ para $i = 0, 1, 2, \cdots, n-1$.

Para qualquer grupo G as seguintes afirmações são equivalentes:

(a) $\gamma_{c+1}(G) = 1$;

(b) $Z_c(G) = G$;

(c) para quaisquer $c+1$ elementos $x_1, \cdots, x_{c+1}$ de G, temos que $[x_1, \cdots, x_{c+1}] = 1$.

Um grupo satisfazendo um dos itens acima é nilpotente. O menor número c tal que $\gamma_{c+1}(G) = 1$ é chamado de *classe de nilpotência* de G e é denotado por $cl(G)$.

Pelas afirmações citadas acima, obtemos imediatamente que se G é um grupo nilpotente com classe de nilpotência no máximo $2^k - 1$, então G é solúvel e $dl(G) \leq k$.

Outro fato importante sobre a classe dos grupos nilpotentes é que ela é fechada para subgrupos, imagens homomórficas e produtos diretos finitos de grupos nilpotentes. Além disso, se fixamos um número c, a classe dos grupos nilpotentes de classe de nilpotência menor ou igual a c é uma variedade.

Um importante resultado chamado de Critério de Ph. Hall [8] diz o seguinte

Teorema 1.1.7. *Seja G um grupo e N um subgrupo normal de G. Suponha que N e G/N' são nilpotentes, então G é nilpotente de classe limitada em termos das classes de N e de G/N'.*

Lema 1.1.8. *Seja G um grupo que possui um subgrupo normal nilpotente N de classe c e de índice finito. Suponha que G tem um subgrupo normal H tal que $[G : N] = [H : H \cap N]$. Então, G/H é nilpotente de classe no máximo c.*

Demonstração. É claro que $G = HN$ e o resultado segue. □

Definição 1.1.9. *Um grupo finito G é chamado* p-grupo *se sua ordem é uma potência do número primo p.*

Temos que todo p-grupo finito é nilpotente. Na verdade, um dos resultados mais clássicos da teoria de grupos nilpotentes é que um grupo finito G é nilpotente se, e somente se, G é o produto direto de seus subgrupos de Sylow. Outro resultado muito conhecido é o seguinte.

Teorema 1.1.10 (Fitting)**.** *Sejam G um grupo qualquer e A, B subgrupos normais nilpotentes de G com $cl(A) = c_1$ e $cl(B) = c_2$. Então, o subgrupo AB também é nilpotente de classe no máximo $c_1 + c_2$.*

Demonstração: Sem perda de generalidade podemos considerar $G = AB$. Ponha $c = c_1 + c_2$. Vamos usar indução sobre c e vamos assumir que $cl(G) = 0$ se, e somente se, $G = 1$. Como A e B são subgrupos normais de G, $Z(A)$ e $Z(B)$ também são normais em G. Pela hipótese de indução $G/Z(A)$ é nilpotente de classe no máximo $c - 1$. Logo, $\gamma_{c-1}(G) \subseteq Z(A)$. Analogamente obtemos que $\gamma_{c-1}(G) \subseteq Z(B)$. Com isso $\gamma_{c-1}(G) \subseteq Z(A) \cap Z(B)$. Portanto $\gamma_{c-1}(G) \subseteq Z(G)$ e o resultado segue. ■

Definição 1.1.11. *O subgrupo de um grupo G gerado por todos os subgrupos normais nilpotentes de G é um subgrupo nolmal nilpotente de G. É chamado de* subgrupo de Fitting *de G e denotado por $F(G)$.*

$F(G)$ é na verdade o único subgrupo normal nilpotente maximal de G. Para um dado grupo G, $F(G)$ pode ser trivial. No entanto isso nunca acontece no caso em que G é solúvel pois neste caso um subgrupo normal minimal de tal grupo é sempre abeliano e portanto nilpotente. De fato, num grupo solúvel acontece o seguinte fato cuja demonstração pode ser encontrada em [6, 6.1.3].

Lema 1.1.12. *Se G é um grupo solúvel, então $C_G(F(G)) \subseteq F(G)$.*

Definição 1.1.13. *Se G é um grupo, o* subgrupo de Frattini *de G é definido como a interseção de todos os subgrupos maximais de G e denotado por $\Phi(G)$.*

Se G não possui subgrupos maximais, então $\Phi(G) = G$. Uma observação importante é que o subgrupo de Frattini de um grupo G também pode ser visto como o conjunto dos elementos não geradores de G, ou seja, se $x \in \Phi(G)$ e $M \subseteq G$ é tal que $\langle x, M\rangle = G$, então $\langle M\rangle = G$.

O próximo resultado nos mostra uma importante relação entre o subgrupo de Fitting e o subgrupo de Fratini de um grupo G e sua demostração pode ser encontrada em [6, 6.1.6].

Lema 1.1.14. *Seja G um grupo. Faça $F = F(G)$ e $\Phi = \Phi(G)$. Então, temos que*

(i) $[F, F] \subseteq \Phi \subseteq F$;

(ii) $F/\Phi = F(G/\Phi)$.

Um conceito não tão conhecido na literatura é o do subgrupo de Fitting generalizado de um grupo G. Na próxima seção apresentamos a definição de tal subgrupo e algumas propriedades que utilizamos no decorrer do trabalho.

1.2 Subgrupo de Fitting Generalizado

O *socle* de um grupo G é o subgrupo gerado por todos os subgrupos normais minimais de G. Como o produto de subgrupos normais de um grupo é um subgrupo podemos trocar a palavra gerado por produto. Assim, o socle de um grupo é o produto de seus subgrupos normais minimais.

Definição 1.2.1. *Sejam X um grupo e $F(X)$ o subgrupo de Fitting de X. Definimos*

$$F^*(X) = socle(F(X)C_X(F(X)) \ mod \ F(X)).$$

Defina $E(X)$ como o último termo da série derivada de $F^*(X)$.

É fácil ver que $F(X)C_X(F(X))/F(X)$ não tem subgrupos normais solúveis. Podemos escolher um p-grupo $P \leq C_X(F(X))$ tal que $PC_X(F(X))/F(X)$ é normal minimal em $X/F(X)$ e então $PF(X)$ é um subgrupo normal nilpotente de X. Assim $F(X)C_X(F(X))/F(X)$ não tem subgrupos normais solúveis e ainda o socle do quociente $F(X)C_X(F(X))/F(X)$ é um produto direto de grupos simples não abelianos. É fácil ver que $F^*(X) = F(X)E(X)$ e que $C_X(F^*(X)) \leq F^*(X)$. Essa é na verdade a propriedade mais importante do grupo $F^*(X)$ - sendo fácil mostrá-la quando X é solúvel - verificamos tais propriedades no seguinte lema.

Lema 1.2.2. *Sejam $F^*(X)$ e $E(X)$ como na definição acima, então*

(i) $F^*(X) = F(X)E(X)$;

(ii) $[F(X), E(X)] = 1$;

(iii) $C_X(F^*(X)) \leq F^*(X)$.

Demonstração: Observamos que o item (i) já foi discutido nos parágrafo acima, logo resta mostrar os outros dois itens (ii) e (iii). Note que $F(X)C_X(F(X))/C_X(F(X))$ sendo uma imagem homomórfica de um grupo nilpotente é solúvel. Assim,

$$E(X) = (F^*(X))^\infty \leq (F(X)C_X(F(X))^\infty \leq C_X(F(X))$$

e o item (ii) segue.

Agora suponha que $C_X(F^*(X)) \not\leq F^*(X)$. Então,

$$C_X(F^*(X))F(X)/F(X) \trianglelefteq C_X(F(X))F(X)/F(X)$$

e $C_X(F^*(X)) \cap F^*(X) = Z(F^*(X)) \leq F(X)$. Assim,

$$C_X(F^*(X))F(X)/F(X) \cap F^*(X)/F(X) = 1.$$

Vimos anteriormente que existe um subgrupo subnormal de $F(X)C_X(F(X))/F(X)$ que anula $F^*(X)/F(X)$, o que é impossível pela definição de $F^*(X)$. O que completa a demonstração. ■

Pelo item (ii) do lema anterior temos que $F(X) \cap E(X) \leq Z(E(X))$. Também observamos que $E(X)/(F(X) \cap E(X)) \equiv F^*(X)/F(X)$ é um produto de grupos simples não abelianos. Assim, $Z(E(X)) = F(X) \cap E(X)$. Agora $E(X)/Z(E(X))$ é um produto direto de grupos simples não abelianos $S_i/Z(E(X))$, $1 \leq i \leq n$. Defina $E_i = (S_i)^\infty$. Os grupos E_i são quasisimples - ou seja, $E_i/Z(E_i)$ é um grupo simples não abeliano. Eles são chamados de componentes de X. Vamos frequêntemente escrever $\overline{E_i}$ para $E_i/Z(E_i)$.

Lema 1.2.3. *Nas condições acima, temos que*

(i) $[E_i, E_j] = 1$ *se* $i \neq j$*;*

(ii) $E(X) = E_1 \cdots E_n$*.*

Demonstração: $[E_i, E_j] \leq Z(E(X))$ pois $E(X)/Z(E(X))$ é um produto direto dos grupos $E_iZ(E(X))/Z(E(X))$. Assim, $[E_i, E_j, E_i] = 1$ se $i \neq j$. Segue pelo Lema dos Três Subgrupos que $[E_i, E_i, E_j] = 1$. Como E_i é perfeito temos $[E_i, E_j] = 1$ se $i \neq j$. Agora, claramente, $E(X) = E_1 \cdots E_nZ(E(X))$. Portanto,

$$E(X) = E(X)' = (E_1 \cdots E_n)' = E_1 \cdots E_n.$$

Isso completa a demonstração. ■

A próxima seção mostra a intrínseca relação entre automorfismos coprimos de um dado grupo G e a estrutura de G.

1.3 Automorfismos Coprimos

Um *automorfismo coprimo* φ de um grupo G é um automorfismo cuja ordem é coprima com a ordem do grupo, isto é, $(|G|, |\varphi|) = 1$.

Sejam G um grupo finito, φ um automorfismo de G. Relembramos que

$$C_G(\varphi) = \{x \in g / x^{\varphi} = x\}$$

é o conjunto de todos os pontos fixos de φ. Observamos que $C_G(\varphi)$ é um subrupo de G. Dizemos que φ é *livre de pontos fixos* se $C_G(\varphi) = 1$.

Se N é qualquer subgrupo φ-invariante de G, então φ induz uma aplicação $\overline{\varphi}$ do conjunto das classes laterais a esquerda de N sobre si mesma da seguinte forma

$$\overline{\varphi} : xN \to x^{\varphi}N.$$

Se N for um subgrupo normal de G, então $\overline{\varphi}$ é um automorfismo do grupo quociente G/N. Por abuso de notação usamos o mesmo símbolo φ para denotar o automorfismo induzido. E temos o seguinte resultado, cuja demonstração pode ser encontrada em [6].

Lema 1.3.1. *Seja G um grupo finito adimitindo um automorfismo coprimo φ. Seja N um subgrupo normal φ-invariante de G. Então, $C_{G/N}(\varphi) = C_G(\varphi)N/N$.*

Teorema 1.3.2. *Sejam P um p-grupo e Q um q-grupo abeliano não cíclico de automorfismos de P, com p e q primos distintos. Então,*

$$P = \prod_{x \in Q^{\#}} C_P(x).$$

Em Particular, P é gerado pelos subgrupos $C_P(x)$ para x em $Q^{\#}$.

Demonstração: O símbolo $Q^{\#}$ denota o conjunto de elementos não nulos de Q.

Suponha que P é p-grupo abeliano elementar. Podemos considerar P como um espaço vetorial sobre $\mathbb{Z}_p$ e ver P como um Q-módulo. Como $p \neq q$, pelo Teorema de Maschke ([6, 3.3.1]), P é um Q-módulo completamente redutível. Então

$$P = P_1 \oplus P_2 \oplus \cdots \oplus P_n,$$

onde P_i é um Q-submódulo irredutível de P para $1 \leq i \leq n$. Como Q é abeliano Q/Q_i é cíclico, onde Q_i denota o núcleo da representação de Q em P_i. Mas como Q é não cíclico segue que $Q_i \neq 1$ para todo $1 \leq i \leq n$. Escolhendo x_i em $Q_i^{\#}$ temos que $P_i \subseteq C_P(x_i)$, portanto

$$P = \sum_{i=1}^{n} C_P(x_i) \subseteq \sum_{x \in Q^{\#}} C_P(x).$$

Revertendo para a notação multiplicativa o resultado segue para o caso onde P é p-grupo abeliano elementar.

Agora seja P um p-grupo qualquer. Vamos usar indução sobre a ordem de P. Fazendo $Z = \Omega_1(Z(P)) = \langle x \in Z(P) | x^p = 1 \rangle$ temos, pelo parágrafo anterior, que $Z_j = C_Z(x_j) \neq 1$ para algum j. Mas então o teorema vale em $\overline{P} = P/Z_j$ por indução. Pelo Lema 1.3.1 concluímos que $P = Z_j \prod_{i=1}^{n} C_P(x_i)$. Mas Z_j está contido em $C_P(x_j)$ e está no centro de P, portanto $\prod_{i=1}^{n} C_P(x_i)$, como queríamos. ■

Se π é um conjunto de primos, um subgrupo H de G será chamado um *S_π-subgrupo* de G se H é um π-grupo e $|G : H|$ não é divisível por nenhum primo em π. Tal subgrupo é também chamado de *subgrupo de Hall* de G. Quando $\pi = \{p\}$, H é simplesmente um p-subgrupo de Sylow de G, que designamos por S_p-subgrupo. Denotamos por $\pi(G)$ o conjunto dos primos que dividem a ordem de G.

Pelo Teorema de Sylow, G possui um S_p-subgrupo para todo $p \in \pi(G)$ e ainda quaisquer dois S_p-subgrupos são conjugados em G. Para um conjunto arbitrário de primos π um grupo G pode possuir ou não um S_π-subgrupo e, se o grupo possui tal subgrupo,

pode ser verdade ou não que qualquer dois deles são conjugados em G. O Teorema de Schur-Zassenhaus nos dá uma condição suficiente para a existencia e conjugação de S_π-subgrupos em G (na verdade $S_{\pi'}$-subgrupo na notação do teorema).

Se H é um S_π-subgrupo de G e suponha que H possui um complemento K em G, então $|K| = |G : H|$ e $|G : K| = |H|$, o que implica que K é um $S_{\pi'}$-subgrupo de G. Inversamente, se G possui um S_π-subgrupo H e um $S_{\pi'}$-subgrupo K, então $G = HK$ com $H \cap K = 1$, assim cada um é complemento do outro.

Podemos então enunciar o Teorema de Schur-Zassenhaus, o qual não será demonstrado aqui, mas uma demonstração pode ser encontrada em [6, 6.2.1].

Teorema 1.3.3 (Schur-Zassenhaus)**.** *Seja H um S_π-subgrupo normal de G. Então*

(i) G possui um $S_{\pi'}$-subgrupo K que é um complemento de H em G.

(ii) Se H ou G/H é solúvel, então quaisquer dois $S_{\pi'}$-subgrupos de G são conjugados em G.

Note que no segundo item do teorema acima H ou G/H tem ordem impar, logo pelo Teorema de Feit-Thompson, H ou G/H é solúvel. Assim, na hipótese do item (ii) pode-se omitir a solubilidade do subgrupo.

O Teorema de Schur-Zassenhaus tem a seguinte importante consequência, que também não será demonstrada aqui mas pode ser encontrada em [6].

Teorema 1.3.4. *Seja A um grupo de automorfismos coprimos de um grupo finito G, isto é, $(|G|, |A|) = 1$. Então*

(i) A deixa invariante algum S_p-subgrupo de G.

(ii) Quaisquer dois S_p-subgrupo A-invariantes de G são conjugados por um elemento de $C_G(A)$.

(iii) Se H é um p-subgrupo A-invariante de G, então H está contido em um S_p-subgrupo A-invariante de G.

(iv) Se P é um S_p-subgrupo A-invariante de G, então $C_P(A)$ é um S_p-subgrupo de $C_G(A)$.

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

Teorema 1.3.5. *Se A é um π'-grupo abeliano não cíclico de automorfismos de um π-grupo G. Então*

$$G = \left\langle C_G(\alpha) | \alpha \in A^{\#} \right\rangle.$$

Demonstração: Como A é não cíclico algum S_q-subgrupo Q de A é não cíclico. Agora Q deixa invariante um S_p-subgrupo P de G para cada p em $\pi(G)$. Além disso, pelo Teorema 1.3.2, $P = \left\langle C_P(\alpha) | \alpha \in Q^{\#} \right\rangle$. Como G é gerado por um conjunto de S_p-subgrupos com p percorrendo todo $\pi(G)$, o resultado segue. ■

A demonstração do próximo lema segue do Teorema 1.3.2 e do Teorema 1.3.5.

Lema 1.3.6. *Sejam p um primo e A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G. Sejam $A_1, A_2, \cdots, A_{p+1}$ os subgrupos maximais de A. Se H é um subgrupo A-invariante de G temos que $H = \langle C_H(A_1), \cdots, C_H(A_{p+1}) \rangle$. Além disso, se H é nilpotente, então $H = \prod_i C_H(A_i)$.*

Lema 1.3.7. *Sejam p um primo e A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G. Sejam $A_1, A_2, \cdots, A_{p+1}$ os subgrupos maximais de A. Seja m o máximo das ordens dos $C_G(A_i)$, onde $1 \leq i \leq p+1$. Então, a ordem de G é $\{m, p\}$-limitada.*

Demonstração: Seja q um primo que divide a ordem de G. Pelo Lema 1.3.4, A normaliza algum q-subgrupo de Sylow Q de G. Já pelo Lema 1.3.6, $Q = \prod_i C_Q(A_i)$. Logo,

$|Q| \leq m^{p+1}$. Note que isso mostra que qualquer primo divisor da ordem de G é $\{m,p\}$-limitado. Portanto a ordem de G é $\{m,p\}$-limitada. ■

Lema 1.3.8. *Sejam p um primo e A um p-grupo abeliano elementar de ordem p^k, $k \geq 3$, agindo sobre um p'-grupo finito G. Sejam $A_1, A_2, \cdots, A_s$ os subgrupos maximais de A, então*

$$G' = \langle [C_G(A_i), C_G(A_j)] | 1 \leq i, j \leq s \rangle.$$

Demonstração: Pelo Lema 1.3.6, $G = \langle C_G(A_i) | 1 \leq i \leq s \rangle$. Agora considere o subgrupo $R = \langle [C_G(A_i), C_G(A_j)] | 1 \leq i, j \leq s \rangle$. Temos que R é A-invariante e assim $R = \langle C_R(A_1), \cdots, C_R(A_s) \rangle$. Para mostrar que R é normal é suficiente mostrar que y^x pertence a R para qualquer $y \in C_R(A_i)$ e $x \in C_G(A_j)$. Observamos que $y^x = y^x y^{-1} y$ e tanto $y^x y^{-1}$ como y pertencem a R. Portanto, $y^x \in R$ e R é normal.

Como G/R é abeliano, concluímos que $R = G'$. ■

O Próximo resultado é devido à Glauberman [5].

Teorema 1.3.9. *Sejam p um primo e A um p-grupo abeliano elementar de ordem $\geq p^3$ agindo sobre um p'-grupo finito G. Suponha que $C_G(a)$ é solúvel, para todo $a \in A^{\#}$, então G é solúvel.*

Relembrando a segunda seção deste capítulo, sobre subgrupo de Fitting generalizado, e a definição de $E(G)$ estamos aptos à demonstrar o importante lema devido a Robert M. Guralnick.

Lema 1.3.10. *Seja A um grupo não cíclico de ordem p^2 agindo sobre um p'-grupo finito N que é um produto direto de grupos simples. Então, $N = \langle E(C_N(a)); a \in A \rangle$.*

Demonstração: Não existe perda em assumir que A age transitivamente sobre os fatores simples de N. Seja t o número de fatores simples de N, e seja L um desses fatores

simples. Suponha primeiramente que $t = 1$. Vamos usar o fato que se B é um grupo de automorfismos coprimos de um grupo simples finito, então B é cíclico - é onde usamos a classificação dos grupos simples (veja [7]). No caso $t = 1$ algum elemento não trivial $a \in A$ centraliza N. Então, $N = E(C_N(a))$ e não temos nada que mostrar.

Se $t = p$, então algum elemento não trivial de A normaliza cada fator e $p^2 - p$ elementos de A permuta os fatores. Escolha geradores a e b de A entre os elementos que não normalizam algum desses fatores. Então, $C_N(a)$ e $C_N(b)$ são distintos subgrupos diagonais de N. Estes são simples e portanto $C_N(a) = E(C_N(a))$ e $C_N(b) = E(C_N(b))$. O subgrupo $\langle E(C_N(a)), E(C_N(b))\rangle$ é A-invariante e, como p é primo, só pode ser N.

Agora, se $t = p^2$, então A permuta os fatores regularmente e $E(C_N(a))$ é um produto de p cópias de L, onde cada fator é um subgrupo diagonal de uma órbita de a. É fácil ver que, como essas órbitas são distintas para geradores a, b de A, dois desses geram um subgrupo A-invariante de N contendo L. Esse subgrupo é necessariamente todo o N pois A permuta os fatores regularmente. ■

1.4 p-Grupos Regulares e p-Grupos Potentes

Um dos objetivos desta seção é apresentar as principais propriedades de p-grupos regulares que serão requisitados no segundo capítulo deste trabalho no momento de definir o anel de Lie associado a um grupo G sobre $\mathbb{F}_p$. Além dos p-grupos regulares também se faz necessário falar algo sobre p-grupos potentes. p-grupos potentes possuem propriedades lineares muito boas, das quais se destaca como uma ferramenta importante neste trabalho a seguinte: se um p-grupo potente G é gerado por elementos de expoente p^e, onde e é um inteiro positivo, então o expoente de G também é p^e. Assim, outro dos objetivos desta seção é mostrar que essa propriedade realmente vale. Esta e outras propriedades interessantes dos p-grupos potentes podem ser encontradas nas notas de Dixon, du Sautoy,

Mann e Segal, *Analytic pro-p Groups* [3].

Definição 1.4.1. *Seja G um p-grupo finito. Para todo $i \geq 0$, definimos*

$$\Omega_i(G) = \left\langle x \in G | x^{p^i} = 1 \right\rangle,$$

e

$$\mho_i(G) = G^{p^i} = \left\langle x^{p^i} | x \in G \right\rangle.$$

Observamos que os subgrupos $\Omega_i(G)$ e $\mho_i(G)$ são característicos em G.

Desde que $G/\Phi(G)$ é p-grupo abeliano elementar temos que $x^p \in \Phi(G)$, para todo $x \in G$. Assim $\mho_i(G) = G^p \leq \Phi(G)$. Consequêntemente, se G é um p-grupo, $\Phi(G)$ é o menor subgrupo de G com quociente abeliano elementar.

Observamos que no caso de p-grupos o expoente de G é simplesmente a ordem máxima dos elementos de G. Se $exp(G) = p^e$, então $x^{p^e} = 1$, para todo $x \in G$. Desta forma $\Omega_e(G) = \langle x \in G | x^{p^e} = 1 \rangle = G$ e podemos considerar uma série ascendente

$$1 = \Omega_0(G) \leq \Omega_1(G) \leq \cdots \leq \Omega_{e-1}(G) \leq \Omega_e(G) = G,$$

que chamamos de Ω-série de G. Similarmente, temos que $\mho_e(G) = \langle x^{p^e} | x \in G \rangle = 1$ e a seguinte série descendente

$$G = \mho_0(G) \geq \mho_1(G) \geq \cdots \geq \mho_{e-1}(G) \geq \mho_e(G) = 1,$$

que chamamos de $\mho$-série de G. A $\mho$-série é estritamente decrescente. Logo, a $\mho$-série de um p-grupo finito de expoente p^e, tem exatamente e passos.

Teorema 1.4.2. *Seja G um p-grupo abeliano finito. Para todo $i \geq 0$ vale as seguintes afirmações*

(i) $\Omega_i(G) = \left\{ x \in G | x^{p^i} = 1 \right\}$;

(ii) $\mho_i(G) = \left\{x^{p^i} | x \in G\right\}$;

(iii) $|G : \Omega_i(G)| = |\mho_i(G)|$ *(consequêntemente* $|G : \mho_i(G)| = |\Omega_i(G)|$*).*

Demonstração: Considere o homomorfismo

$$\begin{array}{rccc} \varphi & : & G & \longrightarrow & G \\ & & x & \longmapsto & x^{p^i} \end{array}$$

Como G é abeliano, temos que $\Omega_i(G)$ é o núcleo de φ e $\mho_i(G)$ a imagem. Assim os itens (i) e (ii) são satisfeitos. Já o item (iii) segue diretamente do primeiro teorema do isomorfismo. ■

Uma observação importante é que nenhum dos itens do teorema acima valem para p-grupos em geral.

Teorema 1.4.3 (A Fórmula de Compilação de Phillip Hall)**.** *Sejam G um grupo e $x, y \in G$. Então, existem elementos $c_i = c_i(x, y) \in \gamma_i(\langle x, y\rangle)$ tais que*

$$x^n y^n \equiv (xy)^n \; c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \cdots c_n,$$

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

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

A Fórmula de Compilação de Phillip Hall é especialmente significativa quando G tem expoente primo p, desde que p divide $\binom{p}{i}$ para todo $1 \leq i \leq p-1$. Consequêntemente, podemos escrever

$$x^p y^p = (xy)^p z c_p, \text{ onde } z \in \mho_1(\langle x, y\rangle').$$

Definição 1.4.4. *Seja G um p-grupo finito. Dizemos que G é um* p-grupo regular *se*

$$x^p y^p = (xy)^p (mod\ \mho_1(\langle x, y\rangle')),\ \textit{para todos } x, y \in G.$$

Equivalentemente, se $c_p = c_p(x,y) \in \mho_1(\langle x,y\rangle')$*, ou seja, se* $\gamma_1(\langle x,y\rangle) \leq \mho_1(\langle x,y\rangle')$.

A condição na definição de p-grupo regular é local pois somente envolve o subgrupo gerado pelos elementos x e y. Assim, todo subgrupo e quociente de p-grupos regulares são também p-grupos regulares. Em contrapartida, a regularidade não é mantida quando tomamos o produto direto. É claro que todo p-grupo abeliano e todo grupo de expoente p é regular.

Lema 1.4.5. *Seja* G *um* p*-grupo regular e sejam* $x, y \in G$*.* $x^p = y^p$ *se, e somente se,* $(x^{-1}y)^p = 1$.

Demonstração: Usamos indução sobre a ordem de G. Seja $H = \langle x,y\rangle$. Como G é regular, podemos escrever $x^{-p}y^p = (x^{-1}y)^p z$, para algum $z \in \mho_1(H')$. Portanto, para mostrar a equivalência reclamada no lema é suficiente mostrar que $\mho_1(H') = 1$ sempre que $x^p = y^p$ ou $(x^{-1}y)^p = 1$.

Se H é abeliano $\mho_1(H') = 1$ e o resultado segue. Podemos supor então que H é não abeliano. Suponha primeiramente que $x^p = y^p$. Logo $[y, x^p] = 1$ e dai $x^p = (x^p)^y = (x^y)^p$. Desde que H não é cíclico, existe um subgrupo maximal M de H contendo x. Temos que $M \trianglelefteq H$ pois H é p-grupo, então $x^y \in M$. Por indução temos que $[x,y]^p = (x^{-1}y)^p = 1$. Agora, $H' = \left\langle [x,y]^h | h \in H \right\rangle$ e a ordem de $[x,y]^h$ divide p. Por indução o lema vale em H' e em particular o produto de dois elementos de H' de ordem dividindo p também tem ordem dividindo p. Assim, $\mho_1(H') = \langle x^p | x \in H'\rangle = 1$.

Assuma agora que $(x^{-1}y)^p = 1$. Conjugando por x^{-1} obtemos $(yx^{-1})^p = 1$. O parágrafo acima nos dá que $[x^{-1}, y] = 1$. Desde que $H = \langle x,y\rangle = \langle x^{-1}, y\rangle$, temos que $H' = \left\langle [x^{-1},y]^h | h \in H \right\rangle$. Consequêntemente, $\mho_1(H') = 1$. ■

Para p-grupos regulares vale o mesmo resultado que para p-grupos abelianos finitos visto no Teorema 1.4.2.

Teorema 1.4.6. *Seja G um p-grupo regular. Então, para todo $i \geq 1$ vale as seguintes afirmações*

(i) Para todos $x, y \in G$, temos que $x^{p^i} = y^{p^i}$ se, e somente se, $(x^{-1}y)^{p^i} = 1$;

(ii) $\Omega_i(G) = \left\{x \in G | x^{p^i} = 1\right\}$;

(iii) $\mho_i(G) = \left\{x^{p^i} | x \in G\right\}$;

(iv) $|G : \Omega_i(G)| = |\mho_i(G)|$ *(consequêntemente* $|G : \mho_i(G)| = |\Omega_i(G)|$*).*

Note que se o item (i) realiza-se para um valor particular de i, então o conjunto $A = \left\{x \in G | x^{p^i} = 1\right\}$ é um subgrupo de G e consequêntemente coincide com $\Omega_i(G)$. Portanto, o item (i) implica no item (ii). A demonstração do item (i) segue por indução sobre i utilizando o Lema 1.4.6. Já o item (iii) segue por indução sobre a ordem de G partindo do Teorema 1.4.2.

Definição 1.4.7. *Um subgrupo N de um p-grupo finito G é dito* potentemente imerso *em G, se $N^p \geq [N, G]$ para $p \neq 2$ (ou $N^4 \geq [N, G]$ para $p = 2$) e denotamos por $Np.i.G$.*

Algumas observações importantes podem ser feitas sobre tais subgrupos. A primeira é que $[N, N] \leq N^2$ é sempre verdade pois N/N^2 tem expoente 2, portanto é abeliano. Outro fato importante é que se $Np.i.G$, então N é normal em G. Ainda mais, se $Np.i.G$, $N/N^p \leq Z(G/N^p)$.

Seja $\varphi : G \longrightarrow G_1$ um homomorfismo qualquer do grupo G para o grupo G_1. Temos que $N\varphi \leq G_1$ e

$$[N\varphi, G\varphi] = [N, G]\varphi \leq N^p\varphi = (N\varphi)^p.$$

Portanto, $N\varphi$ é potentemente imerso em $G\varphi$. Em particular qualquer quociente de G é potentemente imerso.

Lema 1.4.8. *Seja G um p-grupo finito e sejam N, M subgrupos potentemente imersos em G. Então, $[M, N]$, M^p e MN são potentemente imersos em G. Ainda, seja $H \leq G$*

tal que N é normal em G, $N \leq H$ não é potentemente imerso em H, então existe um subgrupo normal J de G tal que

- *se p é impar,*

$$N^p[N,H,H] \leq J < N^p[N,H] \quad e \quad |N^p[N,H] : J| = p;$$

- *se $p = 2$,*

$$N^4[N,H]^2[N,H,H] \leq J < N^4[N,H] \quad e \quad |N^4[N,H] : J| = 2.$$

Definição 1.4.9. *Um p-grupo finito G é dito* potente *se, e somente se, G é potentemente imerso em si mesmo, ou seja, $G^p \geq [G,G]$ para $p \neq 2$ (ou $G^4 \geq [G,G]$ para $p = 2$).*

Outra caracterização desses grupos no caso p impar é a seguinte: se p é impar, G é potente se, e somente se, $G^p = \Phi(G) = \mho_1(G)$.

Novamente observamos que $[G,G] \leq G^2$ é sempre verdade, e se H é um subgrupo potentemente imerso em G, então H é potente.

Corolário 1.4.10. *Se G é um p-grupo potente, então $[G,G]$, G^p, $\Phi(G)$, $G^{(k)}$, $\gamma_k(G)$ para todo $k \in \mathbb{N}$, são potentemente imersos em G.*

Lema 1.4.11. *Se G é um p-grupo potente, então*

(i) $G^{p^i} = \mho_i(G) = \{x^{p^i} | x \in G\}$, para todo $i \in \mathbb{N}$. Em particular $(G^{p^i})^{p^j} = G^{p^{i+j}}$, para todos $i, j \in \mathbb{N}$;

(ii) G^{p^i} é potentemente imerso em G, para todo $i \in \mathbb{N}$;

(iii) Os G^{p^i} formam uma série central de G. Se $exp(G) = p^e$, então G é nilpotente de classe menor ou igual a e.

Seja G um p-grupo finito e faça

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

Para simplificar a notação escrevemos $G_i = P_i(G)$.

Lema 1.4.12. *Seja G um p-grupo potente. Então*

1. *Para cada i, G_i é potentemente imerso em G e $G_{i+1} = G_i^p = \Phi(G_i)$;*

2. *Para cada i, a aplicação $x \mapsto x^p$ induz um homomorfismo de G_i/G_{i+1} para G_{i+1}/G_{i+2}.*

Demonstração: Como $G = G_1$ é potente, temos que G_1 é potentemente imerso em G. Suponhe que G_i é potentemente imerso em G para algum $i \geq 1$. Então, $G_{i+1} = G_i^p[G_i, G] = G_i^p$ e pelo Lema 1.4.8, G_{i+1} é pottemente imerso em G. Como $G_i^p \leq \Phi(G_i) = G_i^p[G_i, G_i] \leq G_{i+1}$ segue que $G_{i+1} = \Phi(G_i)$. E o item (i) segue por indução.

Pelo item (i) temos que G_i é potente e ainda que $G_{i+1} = P_2(G_i)$ e $G_{i+2} = P_3(G_i)$. Assim, mudando a notação, podemos assumir que $i = 1$, e então substituindo G por G/G_3, podemos assumir que $G_3 = 1$. Então, $[G, G] \leq G_2 \leq Z(G)$, assim para $x, y \in G$ temos

$$(xy)^p = x^p y^p [y, x]^{p(p-1)/2}.$$

Se p é impar então $p \backslash (p(p-1)/2)$, assim

$$[y, x]^{p(p-1)/2} \in G_2^p = G_3 = 1.$$

Se $p = 2$ então $[G, G] \leq G^4 \leq G_3 = 1$. Assim, em ambos os casos temos $(xy)^p = x^p y^p$. Como $G_2^p = G_3 = 1$ e $G^p = G_2$, segue que $x \mapsto x^p$ induz um homomorfismo de G/G_2 em G_2/G_3, o que completa a demonstração. ■

Teorema 1.4.13. *Seja $G = \langle a_1, a_2, \cdots, a_r \rangle$ um p-grupo potente. Então, $G^p = \langle a_1^p, a_2^p, \cdots, a_r^p \rangle$.*

Demonstração: Seja $\theta : G/G_2 \to G_2/G_3$ o homomorfismo dado no Lema anterior. Então, G_2/G_3 é gerado por $\{(a_1 G_2)\theta, \cdots, (a_d G_2)\theta\}$, assim $G_2 = \langle a_1^p, a_2^p, \cdots, a_d^p \rangle G_3$. Como $G_3 = \Phi(G_2)$ e $G_2 = G^p$, o resultado segue pelo Lema 1.4.12. ■

Proposiçao 1.4.14. *Se $G = \langle a_1, a_2, \cdots, a_d \rangle$ é um p-grupo potente, então $G = \langle a_1 \rangle \cdots \langle a_d \rangle$, isto é, G é o produto de seus subgrupos ciclicos $\langle a_i \rangle$.*

O *posto* de um grupo G é o menor inteiro r tal que todo subgrupo de G pode ser gerado por r elementos. Denotamos por $rk(G)$ o posto de um grupo G. Para um p-grupo finito G, denotamos por $d(G)$ a menor cardinalidade de um conjunto de geradores de G. Assim, $d(G)$ é também a dimensão de $G/\Phi(G)$ como um espaço vetorial sobre $\mathbb{F}_p$. Se G é um p-grupo potente e H um subgrupo de G, então mostramos no próximo teorema que $d(H) \leq d(G)$. Consequêntemente, como o posto de um grupo finito G é definido por $rk(G) = sup\{d(H)|H \leq G\}$, se G é um p-grupo potente, então $rk(G) = d(G)$.

Teorema 1.4.15. *Se G é um p-grupo potente e H é um subgrupo de G, então $d(H) \leq d(G)$.*

Demonstração: Usamos indução sobre a ordem G. Seja $d = d(G)$ e seja $m = d(G_2)$. Pelo item (i) do Lema 1.4.12, G_2 é potente, assim pela hipótese de indução podemos supor que o subgrupo $K = H \cap G_2$ satisfaz $d(K) \leq m$.

Agora, pelo item (ii) do Lema 1.4.12a aplicação $\pi : G/G_2 \to G_2/G_3$ dada por $x \mapsto x^p$ é um epimorfismo, e $dim(ker\pi) = d - m$ (onde dim é a dimensão como um $\mathbb{F}_p$ espaço vetorial). Logo, $dim(ker\pi \cap HG_2/G_2) \leq d - m$, onde

$$dim((HG_2/G_2)\pi) \geq dim(HG_2/G_2) - (d - m) = m - (d - e)$$

onde $e = dim(HG_2/G_2)$. Sejam $h_1, \cdots, h_e$ elementos de H tais que $HG_2 = \langle h_1, \cdots, h_e \rangle G_2$. Como $\Phi(K) \leq K^p \leq G_3$, o subspaço de $K/\Phi(K)$ gerado pelos $h_1^p, \cdots, h_e^p$ tem dimensão no mínimo $dim((HG_2/G_2)\pi) \geq m - (d - e)$. Como $d(K) \geq m$, podemos encontrar $d - e$ elementos $y_1, \cdots, y_{d-e}$ de K tal que

$$K = \langle h_1^p, \cdots, h_e^p, y_1, \cdots, y_{d-e} \rangle \Phi(K).$$

Então, $K = \langle h_1^p, \cdots, h_e^p, y_1, \cdots, y_{d-e}\rangle$ e assim

$$H = H \cap \langle h_1, \cdots, h_e\rangle G_2 = \langle h_1, \cdots, h_e\rangle K = \langle h_1^p, \cdots, h_e^p, y_1, \cdots, y_{d-e}\rangle.$$

Portanto, $d(H) \leq d$ como queríamos. ■

Definição 1.4.16. *Para um p-grupo finito G e um inteiro positivo r, $V(G,r)$ denota a intersecçao dos núcleos de todos os homomorfismos de G sobre $GL_r(\mathbb{F}_p)$.*

Relembrando que $GL_r(\mathbb{F}_p)$ denota o grupo das matrizes $r \times r$ inversíveis com entradas em $\mathbb{F}_p$ e $U_r(\mathbb{F}_p)$ o grupo de matrizes triangulares $r \times r$ com entradas em $\mathbb{F}_p$.

Como a imagem de qualquer homomorfismo de um p-grupo G sobre $GL_r(\mathbb{F}_p)$ é um p-grupo, e todo p-subgrupo de $GL_r(\mathbb{F}_p)$ é conjugado de um subgrupo do menor grupo unitriangular $U_r(\mathbb{F}_p)$, podemos definir $V(G,r)$ como a intersecção dos núcleos de todos os homomorfismos de G sobre $U_r(\mathbb{F}_p)$. Note que um elemento $g \in G$ pertence a $V(G,r)$ se, e somente se, g age trivialmente em toda representaçao linear de G sobre qualquer $\mathbb{F}_p$-espaço vetorial de dimensão no máximo r.

Para $r \in \mathbb{N}$, definimos o inteiro $\lambda(r)$ por

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

Lema 1.4.17. *(i) O grupo $U_r(\mathbb{F}_p)$ tem uma série, de comprimento $\lambda(r)$, de subgrupos normais, cujos fatores são abelianos elementares;*

(ii) Se G é um p-grupo finito, então $G/V(G,r)$ tem uma série com as propriedades acima.

Demonstração: O item (ii) segue diretamente do item (i), pois $G/V(G,r)$ é isomorfo a um subgrupo do produto direto de cópias finitas de $U_r(\mathbb{F}_p)$. Para mostrar o item (i),

note que o resultado é trivia se $r = 1$. Se $r \geq 2$, ponha $s = [r/2]$. Então os elementos de $U_r(\mathbb{F}_p)$ tem a forma

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

com $A \in U_s(\mathbb{F}_p)$ e $C \in U_{r-s}(\mathbb{F}_p)$. A aplicação que leva x para (A, C) é um homomorfismo de $U_r(\mathbb{F}_p)$ em $U_s(\mathbb{F}_p) \times U_{r-s}(\mathbb{F}_p)$ e o núcleo, é fácil ver que, é um p-grupo abeliano elementar. ■

Proposiçao 1.4.18. *Seja G um p-grupo finito e r um inteiro positivo. Ponha $V = V(G, r)$ e seja $W = V$ se p é impar, $W = V^2$ se $p = 2$. Se $N \lhd G$, $d(N) \leq r$, e $N \leq W$, então N é potentemente imerso em W.*

Demonstração: Usamos indução sobre a ordem de N. Primeiramente, suponha que p é impar e que $[N, V] \not\leq N^p$. Em vista do Lema 1.4.10, podemos assumir que $N^p = 1$ e $|[N, V]| = p$. Como G é um p-grupo, existe $M \lhd G$ com $[N, V] \leq M < N$ e $|N : M| = p$. Como $N/[N, V]$ é abeliano elementar, temos $d(M/[N, V]) = d(N/[N, V]) - 1 \leq r - 1$; como $[N, V]$ é cíclico, segue que $d(M) \leq r$. Portanto,, pela hipótese de indução, $[M, V] \leq M^p = 1$. Assim, M é central em N, e como N/M é cíclico segue que N é abeliano. Então, N é um $\mathbb{F}_p$-espaço vetorial de dimensão no máximo r, logo a ação conjugação de V em N será trivial. Assim, $[N, V] = 1$, em contradição com a afirmação inicial.

Agora suponha que $p = 2$. Como no parágrafo anterior, reduzimos ao caso onde $N^4 = 1$ e $|[N, W]| = 2$. Como qualquer produto de quadrados em N é congruente a um quadrado modulo $[N, W]$, segue que $(N^2)^2 = 1$. Também, se $a, b \in N$ então

$$[a^2, b] = [a, b]^2 \in [N, W]^2 = 1,$$

e $N^2 \leq Z(N)$. Agora, N/N^2 é um $\mathbb{F}_{\not p}$-espaço vetorial de dimensãoo no máximo r, logo

$[N, V] \leq N^2$. Portanto, para $a \in N$ e $v \in V$ temos

$$\begin{array}{rcl} (a^2)^v & = & (a^v)^2 \quad = \quad (ba)^2 \quad \text{com} \quad b \in N^2 \\ & = & a^2. \end{array}$$

Assim, $[N^2, V] = 1$. Portanto, $[N, V, V] = 1$ e então

$$[N, W] = [N, V^2] \leq [N, V]^2 [N, V, V] = 1,$$

contrariando a afirmação inicial. ■

Observamos que na demonstraçao da Proposição 1.4.18, a definição de $V(G, r)$ foi usada somente para representaçõoes lineares de G resultantes da ação por conjugação de G sobre seções abelianas elementar de G. Portanto, o resultado também é válido se substituirmos V, na proposição, pelo subgrupo

$$V^* = \bigcap C_G(A/B),$$

onde (A, B) percorre todos os pares de subgrupos normais de G com $B < A$ e A/B abeliano elementar de posto no máximo r.

Teorema 1.4.19. *Seja G um p-grupo finito de posto r. Então, G tem um subgrupo potente característico de índice no máximo $p^{r\lambda(r)}$ se p é impar e $p^{r+r\lambda(r)}$ se $p = 2$.*

Demonstração: Ponha $V = V(G, r)$. Pelo Lema 1.4.17, existe uma série de subgrupos normais de G para V, de comprimento no máximo $\lambda(r)$, com cada fator abeliano elementar. Como G tem posto r, cada fator tem ordem no máximo p^r, assim $|G : V| \leq p^{r\lambda(r)}$. Se p é impar, a proposição 1.4.18 mostra que V é potente. Se $p = 2$, sabemos pela Proposição 1.4.18 que V^2 é potente; e como $|V/V^2| \leq 2^2$ temos $|G : V^2| \leq p^{r+r\lambda(r)}$. Isso completa a demonstração. ■

Lema 1.4.20. *Seja G um grupo de expoente primo p e posto r. Então $|G| \leq p^s$, onde $s = s(r)$ é um número dependendo somente de r.*

Demonstração: Pelo Teorema 1.4.19, temos um subgrupo potente característico N de G de índice no máxima $p^{\mu(r)}$, onde $\mu(r)$ é um número dependendo somente de r. O Corolário 1.4.17 mostra que N é o produto de no máximo r subgrupos cíclicos. Portanto, N tem ordem no máximo p^r e o resultado segue. ■

1.5 O Dual de um Grupo Abeliano

Seja G um grupo abeliano com a operação aditiva. Definimos um *caracter* de G como um homomorfismo de G no grupo multiplicativo dos números complexos, $\chi : G \to \mathbb{C}^*$, tal que $\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$ para todos $g_1, g_2 \in G$, $\chi(0) = 1$ e $\chi(g)^k = \chi(kg)$, para todo $g \in G$. Dados dois caracteres χ_1 e χ_2 de G, seja $\chi_1\chi_2 : G \to \mathbb{C}^*$ o caracter produto, definido por $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. Os caracteres de G formam um grupo

$$\hat{G} = Hom(G, \mathbb{C}^*),$$

chamado o *grupo caracter* ou *dual* de G. Por exemplo, se $G = C_n$ é cíclico de ordem n, com gerador s, e $\chi : C_n \to \mathbb{C}^*$ é um caracter, então $\omega = \chi(s)$ satisfaz a equação $\omega^n = 1$, e inversamente, toda função $\chi(s^i) = \omega^i$, onde ω é uma n-ésima raiz da unidade, é um caracter de C_n. Ainda, a aplicação $\chi \to \chi(s)$ é um homomorfismo de $\hat{G}$ para $\mathbb{C}^\times$. Em particular, escolhendo para $\chi(s)$ uma n-ésima raiz primitiva da unidade, obtemos um gerador para $\hat{C_n}$, de ordem n, vemos assim que $\hat{C_n} \cong U_n$, onde U_n é o grupo das n-ésimas raizes da unidade em $\mathbb{C}^\times$. Isso mostra que $\hat{C_n}$ é cíclico de ordem n.

Seja $T = \mathbb{R}/\mathbb{Z}$. Observamos que T, o grupo aditivo dos números reais módulo $\mathbb{Z}$, é isomorfo ao grupo multiplicativo dos números complexos de módulo 1, via a aplicação $x \to e^{(2\pi ix)}$. Como T é divisível, pois é o quociente de um grupo divisível, ele é um $\mathbb{Z}$-

módulo injetivo e segue que o funtor $A \mapsto \hat{A} = Hom_{\mathbb{Z}}(A, T)$ é exato, então para qualquer subgrupo B de A temos a sequência exata

$$0 \to \hat{A/B} \to \hat{A} \to \hat{B} \to 0.$$

Usando este fato fica fácil obter o seguinte teorema

Teorema 1.5.1. *Todo grupo abeliano finito é isomorfo a seu próprio dual.*

Demonstração: Para o caso onde A é cíclico provamos anteriormente. Em geral podemos escrever $A = A_1 \times \cdots \times A_r$, onde cada A_i é cíclico, pelo teorema da base para grupos abelianos.

Temos que

$$Hom(B \times C, T) \cong Hom(B, T) \times Hom(C, T),$$

isto é $B \times C \cong \hat{B} \times \hat{C}$. Por indução segue que $\hat{A} = \hat{A_1} \times \cdots \times \hat{A_r}$ e obtemos que $\hat{A} \cong A_i$, portanto $\hat{A} \cong A$, como queríamos. ■

Capítulo 2

Algumas Ferramentas da Teoria de Álgebras de Lie

O principal objetivo deste trabalho é estudar como certas restrições sobre centralizadores de automorfismos coprimos de um dado grupo G resulta em propriedades específicas satisfeitas no grupo G. Todavia, como mencionado na introdução deste trabalho, a teoria de álgebras de Lie se apresenta como uma ferramenta efetiva para o desenvolvimento dos problemas inicialmente propostos. Assim, dedicamos este capítulo na apresentação de tal ferramenta. Primeiramente mostramos algumas propriedades gerais que valem em qualquer álgebra de Lie além de alguns conceitos, como de solubilidade e nilpotência, que são similares à teoria de grupos. Na segunda seção, apresentamos alguns resultados clássicos sobre identidades polinomiais em álgebras de Lie, onde não exporemos as demonstrações pois fugiria aos objetivos deste trabalho. Já na terceira seção mostramos os seguintes resultados, que são equivalentes aos Teoremas 1 e 2 citados na introdução deste trabalho cuja formulação foi feita para grupos e agora os formulamos para álgebras de Lie.

Teorema 2.3.8. *Sejam p um primo, n, d inteiros positivos tais que $2^d \leq n$. Seja L uma álgebra de Lie tal que $pL = L$ e seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre L por automorfismos. Assuma que existe um inteiro positivo m tal que $[C_L(a)^{(d)}, \underbrace{C_L(b)^{(d)}, \cdots, C_L(b)^{(d)}}_{m}] = 0$, para quaisquer $a, b \in A^{\#}$. Então, $L^{(d)}$ é nilpotente de classe $\{p, d, m\}$-limitada.*

Teorema 2.3.9. *Sejam p um primo e n um inteiro positivo. Seja L uma álgebra de Lie tal que $pL = L$ e seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre L por automorfismos. Assuma que existe um inteiro positivo m de tal forma que $[\gamma_n(C_L(a)), \underbrace{\gamma_n(C_L(b)), \cdots, \gamma_n(C_L(b))}_{m}] = 0$, para quaisquer $a, b \in A^{\#}$. Então, $\gamma_n(L)$ é nilpotente de classe $\{p, n, m\}$-limitada.*

E finalmente, na última seção deste capítulo, mostramos o elo de ligação entre a teoria de álgebras de Lie e a teoria de grupos com duas maneiras distintas de associar um anel de Lie a um grupo.

2.1 Álgebras de Lie

Seja L um R-Módulo, onde R denota um anel comutativo com unidade. Suponhamos que L é munido com uma operação $L \times L \longrightarrow L$ denotada por $(a, b) \mapsto [a, b]$. O R-módulo L é dito uma *R-álgebra de Lie*, ou uma álgebra de Lie sobre R, se a operação satisfaz as seguintes condições, para todos $a, b, c \in L$, $r, s \in R$,

1. $[a, a] = 0$;
2. $[ra + sb, c] = r[a, c] + s[b, c]$;
3. $[a, rb + sc] = r[a, b] + s[a, c]$;
4. $[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$, (Identidade de Jacobi).

Pelo item (1), temos que $[a+b, a+b] = 0$, para todos $a, b \in L$, o que implica que em qualquer álgebra de Lie $[x, y] = -[y, x]$. Assim, o produto de Lie é uma aplicação R-bilinear antisimétrica.

Sejam $a_1, a_2, \cdots, a_n$ elementos de uma R-álgebra de Lie L. Então, o produto $[a_1, a_2, \cdots, a_n]$ de n fatores é definido recursivamente, para $n \geq 2$ por

$$[a_1, a_2, \cdots, a_n] = [[a_1, a_2, \cdots, a_{n-1}], a_n].$$

Uma observação importante e que será usada no decorrer deste trabalho é que uma álgebra de Lie sobre o anel dos inteiros $\mathbb{Z}$ é simplesmente chamada de *anel de Lie*.

Sejam U, V e W R-submódulos de uma R-álgebra de Lie L. Definimos $[U, V]$ como sendo o R-submódulo de L, gerado por todos os produtos $[u, v]$, $u \in U, v \in V$

$$[U, V] = \langle [u, v] | u \in U, v \in V \rangle .$$

Escrevemos a soma $U + V$ da forma,

$$U + V = \{u + v | u \in U, v \in V\} .$$

Assim, $U + V$ é um R-submódulo de L e valem,

$$U + V = V + U \text{ e } (U + V) + W = U + (V + W).$$

Um R-módulo I de L é dito um *ideal* da R-álgebra de Lie L, $I \lhd_R L$, se $[I, L] \subseteq I$, ou equivalentemente, $[L, I] \subseteq I$.

Se L_1 e L_2 são R-álgebras de Lie, um *homomorfismo* (de Lie) de L_1 em L_2 é um homomorfismo de R-módulos

$$\theta : L_1 \to L_2 \text{ tal que } [a, b]\theta = [a\theta, b\theta],$$

para todos $a, b \in L_1$. O *núcleo* de θ, $Ker\ \theta = \{a \in L_1 | a\theta = 0\}$, é um ideal de L_1.

Seja I um ideal da R-álgebra de Lie L. Então, o R-módulo L/I tem estrutura de álgebra de Lie com multiplicação

$$[a + I, b + I] = [a, b] + I.$$

A aplicação quociente $\pi : L \to L/I$, definida por $a\pi = a + I$, para todo $a \in L$, é um homomorfismo (de Lie) sobrejetor, chamado homomorfismo canônico onde o núcleo de π é I.

A interseção de qualquer família de ideais de L ainda é um ideal de L e a soma de dois ideais de L também é um ideal de L. Se X é um subconjunto de L, o ideal gerado por X é a interseção de todos os ideais de L que contém X.

Um R-submódulo M de L é uma *R-subálgebra* de Lie, $M \leq_R L$, se $[M, M] \subseteq M$. A interseção de qualquer família de R-subálgebras de Lie de uma R-álgebra de Lie é uma R-subálgebra de Lie. Se X é um subconjunto de L, a interseção de todas as R-subálgebras de L que contém X é a R-subálgebra de L gerada por X.

Muitas das definições na teoria de álgebras de Lie são análogas as de grupo, é claro levando em consideração a operação de multiplicação definida aqui. Para economizar notação escrevemos álgebra de Lie para denotar uma R-álgebra de Lie.

Seja X um subconjunto de um álgebra de Lie L. O *centralizador* de X em L é definido por

$$C_L(X) = \{y \in L | [X, y] = 0\}.$$

Utilizando a Identidade de Jacobi verifica-se que $C_L(X)$ é uma subálgebra de L. A subálgebra $C_L(L)$ de L é chamada de *centro* de L e é denotada por $Z(L)$. Já o *normalizador* em L deve ser tomado sob uma subálgebra X e é definido por

$$N_L(X) = \{y \in L | [X, y] \subseteq X\}.$$

Da mesma forma temos que $N_L(X)$ é uma subálgebra de L.

Também como em grupos, podemos definir as séries centrais superior, inferior e série derivada de uma álgebra de Lie.

A *série central superior* de uma álgebra de Lie L,

$$0 = Z_0(L) \subseteq Z_1(L) \subseteq Z_2(L) \subseteq \cdots \subseteq Z_i \subseteq \cdots,$$

é definida por $Z_{i+1}(L) = \{x \in L | [L, x] \subseteq Z_i(L)\}$, para $i = 0, 1, \cdots$. A série

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

com $\gamma_{i+1}(L) = [\gamma_i(L), L]$, para todo $i = 1, 2, \cdots$, é a *série central inferior* de L. Já a *série Derivada* de uma álgebra de Lie L é a série

$$L = L^{(0)} \supseteq L' \supseteq L^{(2)} \supseteq \cdots \supseteq L^{(i)} \supseteq \cdots$$

onde $L^{(i+1)} = (L^{(i)})'$, para todo $i = 1, 2, \cdots$.

Por analogia a teoria de grupos defini-se comutadores de peso maiores ou iguais a 1. Seja M um subconjunto de uma álgebra de Lie L, um comutador de peso 1 em elementos de M é exatamente os elementos de M. Agora, assuma que a definição de comutadores de peso $\leq w-1$ em elementos de M já é conhecida. Então, os comutadores de peso w são as expressões da forma $[c_1, c_2]$, onde c_1 e c_2 são comutadores de peso w_1 e w_2 respectivamente, com $w_1 + w_2 = w$.

Com toda essa similaridade entre álgebra de Lie e grupos, é natural pensar nos conceitos de solubilidade e nilpotência para álgebras de Lie.

Definição 2.1.1. *Uma álgebra de Lie L é dita* solúvel *se existe um inteiro d tal que $L^{(d)} = 0$. O menor inteiro d tal que a igualdade ocorre é chamado de* comprimento derivado*, ou grau de solubilidade, de L.*

Novamente, se L é solúvel então qualquer subálgebra e álgebra quociente também o são.

Definição 2.1.2. *Uma álgebra de Lie L é dita* nilpotente *se existe um inteiro $n \geq 1$ tal que $\gamma_{n+1}(L) = 0$. O menor inteiro n tal que a igualdade vale é chamado de* classe de nilpotência *de L denotado por $cl(L)$.*

Também é análogo à teoria de grupos a verificação de que, L é nilpotente de classe menor ou igual que c se, e somente se, $[x_1, x_2, \cdots, x_{c+1}] = 0$ vale para todos os elementos de L. Se a classe de nilpotência de L é no máximo c, então, qualquer subálgebra de L ou álgebras quocientes são nilpotentes de classe no máximo c. Observanmos que L/I é nilpotente de classe no máximo c, onde I é um ideal de L se, e somente se, $\gamma_{c+1}(L) \subseteq I$.

Como para grupos, temos que $L^{(n)} \subseteq \gamma_{2^n}(L)$. Logo, uma álgebra de Lie nilpotente é solúvel e a classe de nilpotencia limita o comprimento derivado de L.

Definição 2.1.3. *Seja G um grupo abeliano. Um anel de Lie L tem uma* G-graduação *ou é* G-graduado*, se para cada elemento $g \in G$ corresponde um subgrupo L_g do grupo aditivo de L tal que*

1. $L = \oplus_{g \in G} L_g$;
2. $[L_x, L_y] \leq L_{x+y}$, *para quisquer* $x, y \in G$.

Qualquer elemento de L_g chama-se *homogêneo*. Observamos que a condição 1 da definição acima nos diz que todo elemento de L é uma soma finita de elementos homogêneos que são unicamente determinados. Se

$$x = x_0 + x_1 + \cdots + x_l$$

é a decomposição de um elemento $x \in L$, então os elementos x_i chamam-se *componentes homogêneas* de x.

Seja φ um automorfismo de ordem n da álgebra de Lie L. Suponhamos que o anel base R de L possui uma n-ésima raiz primitiva da unidade w. Podemos considerar para cada $i = 0, 1, \cdots, n-1$ o seguinte subconjunto

$$L_i = \left\{x \in L | x^{\varphi} = w^i x\right\}.$$

Na verdade L_i pode ser definido para todo inteiro positivo i, obedecido a regra $L_i = L_j$ se, e somente se, $i \equiv j (mod\ n)$.

É imediato que cada L_i é um submódulo de L, em particular, observamos que L_0 consiste exatamente de $C_L(\varphi)$. A importância destes submódulos de L fica evidenciada por suas funções de autoespaço que destacamos a seguir. Denotamos por nL o submódulo de L dado por $\{nx, x \in L\}$ e lembramos que uma álgebra de Lie é dita não ter n-torção se $nx = 0$ para $x \in L$ for possível somente se $x = 0$.

Proposiçao 2.1.4. *Nos termos descritos acima, temos que*

(i) $[L_i, L_j] \leq L_{i+j}$, *para todos* $i, j \geq 0$;

(ii) $L_0 + L_1 + \cdots + L_{n-1}$ *é uma subálgebra* φ*-invariante de* L *e* $nL \leq L_0 + L_1 + \cdots + L_{n-1}$;

(iii) Se L *não tem* n*-torção a soma* $L_0 + L_1 + \cdots + L_{n-1}$ *é direta.*

Suponhamos agora que o anel base R da álgebra de Lie L não possua uma n-ésima raiz primitiva da unidade. Podemos considerar $R[\omega]$ a menor extenção de R que admite uma citada raiz ω. Considere o $R[\omega]$-módulo estendido $L^* = L \otimes_R R[\omega]$. Cálculos rotineiros mostram que L^*, com respeito às operações

$$[l_1 \otimes r_1, l_2 \otimes r_2] = [l_1, l_2] \otimes r_1 r_2, \quad l_i \in L, \quad r_i \in R[\omega],$$

$$r(l_1 \otimes r_1) = l_1 \otimes r r_1, \quad l_1 \in L, \quad r, r_1 \in R[\omega],$$

torna-se uma $R[\omega]$-álgebra de Lie.

Pela definição é fácil ver que L^* tem estrutura semelhante a de L. Além disso, para quaisquer inteiros $k \geq 0$ e $m \geq 1$, temos que $(L^*)^{(k)} = L^k \otimes_R R[\omega]$ e $\gamma_m(L^*) = \gamma_m(L) \otimes_R R[\omega]$. Em particular, se L for solúvel então L^* é solúvel com o mesmo comprimento derivado e, se L for nilpotente, então L^* é nilpotente de mesma classe de nilpotencia.

Pode-se definir um automorfismo φ^* de L^* correspondente ao automorfismo φ de L, pondo $\varphi^* = \varphi \otimes 1$, ou seja, $(x \otimes r)^{\varphi} = x^{\varphi} \otimes r$, para todos $x \in L$ e $r \in R[\omega]$. Logo, $|\varphi^*| = |\varphi|$ e as propriedades da ação de φ em L podem ser transferidas à L^* pois

$$C_{L^*}(\varphi^*) = C_L(\varphi) \otimes_R R[\omega].$$

Essencialmente, o que observamos acima é que não há perda de generalidade em se assumir que o anel base de uma álgebra de Lie contenha uma n-ésima raiz primitiva da unidade, quando o propósito for estudar as consequências da ação de um automorfismo de ordem n sobre a sua estrutura.

2.2 Identidades Polinomiais para Álgebras de Lie

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

Denote por F a álgebra de Lie sobre R com geradores livres enumeráveis $x_1, x_2, x_3, \cdots$. Seja $f = f(x_1, x_2, \cdots, x_n)$ um elemento de F diferente de zero. A álgebra de Lie L satisfaz a identidade $f \equiv 0$ se $f(a_1, a_2, \cdots, a_n) = 0$ para quaisquer $a_1, a_2, \cdots, a_n \in L$. Neste caso dizemos que L é *PI*. Um resultado bem conhecido de Zel'manov diz que se a álgebra de Lie L é finitamente gerada e é PI e além disso que qualquer comutador em seus geradores é ad-nilpotente, então, L é nilpotente [[32], $III(0.4)$]. Usando esse resultado e alguns argumentos de rotina universal, podemos deduzir o próximo teorema.

Teorema 2.2.1. *Seja L uma álgebra de Lie sobre um corpo R gerada por $a_1, a_2, \cdots, a_m$. Assuma que L satisfaz uma identidade $f \equiv 0$ e que cada comutador nos geradores $a_1, a_2, \cdots, a_m$ é ad-nilpotente de índice no máximo n. Então, L é nilpotente de classe $\{f, n, m, R\}$-limitada.*

Demonstração: Considere a R-álgebra livre m-gerada F_m com geradores $f_1, \cdots, f_m$ e seja T o ideal de F_m gerado por todos os valores de f nos elementos de F_m e por todos os elementos da forma $[g,_n c]$, onde $g \in F_m$ e c é um comutador arbitrário nos f_i. Então, o quociente F/T satisfaz as hipótese do resultado de Zel'manov citado no parágrafo anterior e portanto é nilpotente de classe $u = u(m, n, f, R)$. Temos que L é uma imagem de F/T pelo homomorfismo induzido pela aplicação $f_i \to a_i$. Portanto, L é nilpotente de classe no máximo u. ■

Um importante critério para uma álgebra de Lie ser PI é o seguinte

Teorema 2.2.2 (Bahturin-Linchenko-Zaicev)**.** *Seja L uma álgebra de Lie sobre um corpo R. Assuma que um grupo finito A age sobre L por automorfismos tal que $C_L(A)$, a subálgebra formada pelos elementos fixos, é PI. Assuma ainda que a característica de R é zero ou prima com a ordem de A. Então, L é PI.*

Esse teorema foi primeiro demonstrado para o caso onde A é solúvel por Bahturin e Zaicev [1] e mais tarde estendido para o caso geral por Linchenko [17].

Corolário 2.2.3 ([27])**.** *Seja F a álgebra de Lie livre de posto enumerável sobre R. Denote por F^* o conjunto dos elementos diferentes de zero de F. Para qualquer grupo finito A existe uma aplicação*

$$\phi : F^* \to F^*$$

tal que se L e A são como no Teorema 2.2.2, e se $C_L(A)$ satisfaz uma identidade $f \equiv 0$, então, L satisfaz a identidade $\phi(f) \equiv 0$.

2.3 Condições de Nilpotência para Álgebras de Lie

Um teorema bem conhecido de Kreknin [10], diz que se um anel de Lie L admite um automorfismo livre de pontos fixos de ordem finita n, então L é solúvel de comprimento derivado no máximo $2^n - 2$. Para o desenvolvimento de nosso trabalho requeremos a seguinte extensão deste resultado, sua demonstração pode ser encontrada em [14].

Teorema 2.3.1. *Seja L um anel de Lie admitindo um automorfismo a de ordem finita n tal que $[L, \underbrace{C_L(a), \cdots, C_L(a)}_{t}] = 0$. Assuma que $nL = L$. Então, L é solúvel com comprimento derivado no máximo $(t+1)^{n-1} + log_2 t$.*

Lema 2.3.2. *Seja $t \geq 1$. Seja L uma álgebra de Lie, e K uma subálgebra nilpotente de classe c. Assuma que K é gerada pelos subespaços $X_1, \cdots, X_m$ tal que para qualquer espaço-comutador Y em $X_1, \cdots, X_m$ temos $[L, \underbrace{Y, \cdots, Y}_{t}] = 0$. Então, existe um número u, $\{c, m, t\} - limitado$, tal que $[L, \underbrace{K, \cdots, K}_{u}] = 0$.*

Demonstração: Usamos indução sobre c. Temos que K' é gerado por comutadores de peso ≥ 2 em $X_1, \cdots, X_m$ e o número de tais espaços é $\{c, m\}$-limitado. Pela hipótese de indução existe um número $\{c, m, t\}$-limitado u_1 tal que $[L, \underbrace{K', \cdots, K'}_{u_1}] = 0$.

Seja $r = m(t-1)+1$ e considere o espaço-comutador M da forma $M = [L, Y_1, \cdots, Y_r]$, onde $Y_1, \cdots, Y_r \in \{X_1, \cdots, X_m\}$. Logo, para uma permutação π dos símbolos $1, 2, \cdots, m$ temos que $M \leq [L, Y_{\pi(1)}, \cdots, Y_{\pi(r)}] + [L, K']$. O número r é grande o suficiente para assegurar que algum X_i ocorre na lista $Y_1, \cdots, Y_r$ no mínimo t vezes. Assim, como $[L, \underbrace{X_i, \cdots, X_i}_{t}] = 0$, obtemos que $M \leq [L, K']$.

Agora faça $u = u_1 r$. Usando o fato que $K = K' + \sum X_j$ e $M \leq [L, K']$ para qualquer escolha de $Y_1, \cdots, Y_r \in \{X_1, \cdots, X_m\}$, concluímos que

$$[L, \underbrace{K, \cdots, K}_{u}] \leq [L, \underbrace{K', \cdots, K'}_{u_1}] = 0.$$

■

Um caso particular do Lema 2.3.2, que nos ajudará a deduzir que certos elementos de L são ad-nilpotentes, é o seguinte lema de Khukhro e Shumyatsky [13].

Lema 2.3.3. *Suponha que L é uma álgebra de Lie, H uma subálgebra de L gerada por r elementos $h_1, h_2, \cdots, h_r$ tal que todos os comutadores nos h_i são ad-nilpotentes em L de índice t. Se H é nilpotente de classe u, então para algum número v, $\{r,t,u\}$-limitado, temos que $[L, \underbrace{H, \cdots, H}_{v}] = 0$.*

A partir deste momento vamos estudar a seguinte situação.

Hipótese A. *Sejam ω uma p-ésima raíz primitiva da unidade e L uma álgebra de Lie sobre $\mathbb{Z}[\omega]$ tal que $L = pL$. Seja A um p-grupo abeliano elementar de ordem p^k agindo por automorfismos sobre L, e seja $\hat{A}$ o grupo dual de A.*

Para qualquer $\alpha \in \hat{A}$ temos o seguinte conjunto:

$$L_\alpha = \{x \in L |\ x^a = \alpha(a)x,\ \textit{para cada } a\ \in A\}.$$

Como A é finito, pelo Teorema 1.5.1, temos que A e $\hat{A}$ são isomorfos. Agora, L se decompõe como soma direta de autoespaços comuns para todos $a \in A^\#$. Logo $L = \oplus_\alpha L_\alpha$, onde $\alpha \in \hat{A}$. Além disso é fácil ver que $[L_\alpha, L_\beta] \leq L_{\alpha\beta}$, para todos $\alpha, \beta \in \hat{A}$. Realmente, para quaisquer $x \in L_\alpha$ e $y \in L_\beta$ temos $[x,y]^a = [x^a, y^a] = [\alpha(a)x, \beta(a)y] = \alpha\beta(a)[x,y]$ para todo $a \in A^\#$.

Para qualquer inteiro positivo n e quaisquer $\alpha_1, \alpha_2, \cdots, \alpha_{2^n} \in \hat{A}$ definimos indutivamente:

$$\gamma(\alpha_1) = L_{\alpha_1},\ \cdots,\ \gamma(\alpha_1, \alpha_2, \cdots, \alpha_n) = [\gamma(\alpha_1, \alpha_2, \cdots, \alpha_{n-1}), L_{\alpha_n}],\ \text{e}$$

$$\delta(\alpha_1) = L_{\alpha_1},\ \cdots,\ \delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^n}) = [\delta(\alpha_1, \cdots, \alpha_{2^{n-1}}), \delta(\alpha_{2^{n-1}+1}, \cdots, \alpha_{2^n})].$$

Como usualmente, $\gamma_n(L)$ e $L^{(n)}$ denota o n-ésimo termo da série central inferior e o n-ésimo termo da série derivada de L, respectivamente.

Lema 2.3.4. *Sob a* Hipótese A, *temos que* $\gamma_n(L) = \sum \gamma(\alpha_1, \alpha_2, \cdots, \alpha_n)$ *e também* $L^{(n)} = \sum \delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^n})$, *onde* $\alpha_1, \alpha_2, \cdots, \alpha_{2^n}$ *percorrem independentemente todo* $\hat{A}$.

Demonstração: Ponha $Q = \sum \gamma(\alpha_1, \cdots, \alpha_n)$. Para qualquer $\beta \in \hat{A}$ temos que,

$$[\gamma(\alpha_1, \cdots, \alpha_n), L_\beta] \leq \gamma(\alpha_1\alpha_2, \alpha_3, \cdots, \alpha_n, \beta) \leq Q.$$

O que mostra que Q é normalizado por L_β para todo $\beta \in \hat{A}$, e portanto é um ideal de L, visto que $L = \bigoplus_\beta L_\beta$, $\beta \in \hat{A}$.

Temos que L/Q é nilpotente de classe no máximo $n-1$ e assim $\gamma_n(L) \leq Q$. Como a inclusão $Q \leq \gamma_n(L)$ é óbvia, concluímos que $\gamma_n(L) = \sum \gamma(\alpha_1, \alpha_2, \cdots, \alpha_n)$.

Para provar a outra igualdade, ponha $R_n = \sum \delta(\alpha_1, \cdots, \alpha_{2^n})$ e, agindo por indução sobre n, assuma que $R_{n-1} = L^{(n-1)}$. Vamos mostrar que $R_n = R'_{n-1}$.

Para quaisquer $\beta_1, \cdots, \beta_{2^{n-1}} \in \hat{A}$ temos que,

$$[\delta(\alpha_1, \cdots, \alpha_{2^n}), \delta(\beta_1, \cdots, \beta_{2^{n-1}})] \leq R_n.$$

O que implica que $\delta(\beta_1, \cdots, \beta_{2^{n-1}})$ normaliza R_n.

Portanto, R_n é um ideal em R_{n-1} e segue que $R_n = R'_{n-1}$. ■

Corolário 2.3.5. *Assuma a* Hipótese A. *Então, para qualquer* $\beta \in \hat{A}$, *temos que* $L_\beta \cap \gamma_n(L) = \sum \gamma(\alpha_1, \alpha_2, \cdots, \alpha_n)$, *onde* $\alpha_1, \alpha_2, \cdots, \alpha_n$ *satisfazem a condição que* $\alpha_1\ \alpha_2 \cdots \alpha_n = \beta$. *Similarmente,* $L_\beta \cap L^{(n)} = \sum \delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^n})$, *onde* $\alpha_1\alpha_2 \cdots \alpha_{2^n} = \beta$.

O próximo lema pode ser encontrado em [25].

Lema 2.3.6. *Assuma a* Hipótese A *com* $k \geq 2$. *Suponha que existe um inteiro* u *tal que* $[L, {}_u C_L(a)] = 0$, *para todo* $a \in A^{\#}$. *Então,* L *é nilpotente de classe* $\{p, u\}$*-limitada.*

Demonstração: Pelo Teorema 2.3.1, temos que L é solúvel de comprimento derivado $\{p,u\}$-limitado d. Vamos usar indução sobre d. Aplicando a hipótese de indução em L', assumimos que L' é nilpotente de casse e, $\{p,u\}$-limitada.

Seja B qualquer subgrupo de A de ordem p^2. Sejam $B_1,\cdots,B_{p+1}$ os subgrupos cíclicos de B e considere $C_i = C_L(B_i)$, $1 \leq i \leq p+1$. Então, $L = \sum C_i$.

Seja $r = (u-1)(p+1)+1$. Se $Z = Z(L')$, temos que $[Z,X,Y] = [Z,Y,X]$ para quaisquer subconjuntos X, Y de L. Com este fato obtemos que

$$[Z,_r L] = \sum [Z,_{u_1} C_1,\cdots,_{u_{p+1}} C_{p+1}],$$

onde $u_1 + u_2 + \cdots + u_{p+1} = r$.

O número r é grande o suficiente para certificarmos que $u_i \geq u$ para algum i. Consequentemente $[Z,_{u_1} C_1,\cdots,_{u_{p+1}} C_{p+1}] = 0$, pois $[L,_u C_i] = 0$, para todo i. Assim, $[Z,_r L] = 0$. Então, $Z \leq Z_r(L)$, onde Z_r é o r-ésimo termo da série central superior de L.

Aplicando este argumento repetidamente para $L/Z, L/Z_2(L')$ e assim por diante, concluímos que $Z_e(L') \leq Z_{er}(L)$. Como L é nilpotente de classe e, $L' \leq Z_{er}(L)$. Portanto, L é nilpotente de classe no máximo $er+1$. ■

Começamos nosso propósito nesta seção que é o de demonstrar os Teoremas 2.3.9 e 2.3.8, mencionados na introdução deste capítulo, com o caso $n = 2$.

Proposiçao 2.3.7. *Sejam p um primo e L uma álgebra de Lie tal que $pL = L$. Seja A um p-grupo abeliano elementar de ordem p^3 agindo sobre L por automorfismos. Assuma que existe um inteiro positivo m tal que $[C_L(a)', \underbrace{C_L(b)',\cdots,C_L(b)'}_{m}] = 0$, para quaisquer $a, b \in A^{\#}$. Então, L' é nilpotente de classe $\{p,m\}$-limitada.*

Demonstração: Temos que para todos $\alpha_1, \alpha_2, \beta_1, \beta_2$ pertencentes a $\hat{A}$, existem $a, b \in A^{\#}$ tal que $L_{\alpha_1}, L_{\alpha_2} \leq C_L(a)$ e $L_{\beta_1}, L_{\beta_2} \leq C_L(b)$. Logo, $[L_{\alpha_1}, L_{\alpha_2}] \leq C_L(a)'$ e $[L_{\beta_1}, L_{\beta_2}] \leq C_L(b)'$.

Do fato de $[C_L(a)', \underbrace{C_L(b)', \cdots, C_L(b)'}_{m}] = 0$, para quaisquer $a, b \in A^{\#}$, temos que

$$[[L_{\alpha_1}, L_{\alpha_2}], \underbrace{[L_{\beta_1}, L_{\beta_2}], \cdots, [L_{\beta_1}, L_{\beta_2}]}_{m}] = 0.$$

Então, $[L', \underbrace{[L_{\beta_1}, L_{\beta_2}], \cdots, [L_{\beta_1}, L_{\beta_2}]}_{m}] = 0$, pois $L' = \sum[L_\alpha, L_\beta]$, $\alpha, \beta \in \hat{A}$.

Pelo corolário 2.3.5, $C_{L'}(a) = \sum[L_\alpha, L_\beta]$, onde $\alpha\beta(a) = 1$. Mas pelo que vimos no parágrafo precedente $L_\alpha, L_\beta \leq C_L(c)$ para algum c, não nulo, pertencente a A. Logo $[L_\alpha, L_\beta] \leq C_L(c)'$ e, portanto, $[L',_m [L_\alpha, L_\beta]] = 0$.

Fazendo $K = C_{L'}(a)$ e usando o Lema 2.3.2, com subespaços da forma $[L_\alpha, L_\beta] \leq C_{L'}(a)$ no lugar de X_i, temos que existe um número inteiro u, $\{m, p\}$-limitado, tal que $[L', \underbrace{K, \cdots, K}_{u}] = 0$. Portanto, pelo Lema 2.3.6, L' é nilpotente de classe $\{m, p\}$-limitada. ■

Passamos agora aos casos gerais.

Teorema 2.3.8. *Sejam p um primo, n e d inteiros positivos tais que $2^d \leq n$. Seja L uma álgebra de Lie tal que $pL = L$ e seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre L por automorfismos. Assuma que existe um inteiro positivo m tal que $[C_L(a)^{(d)}, \underbrace{C_L(b)^{(d)}, \cdots, C_L(b)^{(d)}}_{m}] = 0$, para quaisquer $a, b \in A^{\#}$. Então, $L^{(d)}$ é nilpotente de classe $\{p, d, m\}$-limitada.*

Demonstração: Para todos $\alpha_1, \alpha_2, \cdots, \alpha_{2^d}, \beta_1, \beta_2, \cdots, \beta_{2^d}$ em $\hat{A}$, existem $a, b \in A^{\#}$ tais que $L_{\alpha_1}, \cdots, L_{\alpha_{2^d}} \subseteq C_L(a)$ e $L_{\beta_1}, \cdots, L_{\beta_{2^d}} \subseteq C_L(b)$. Logo

$$\delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^d}) \subseteq C_L(a)^{(d)} \text{ e } \delta(\beta_1, \beta_2, \cdots, \beta_{2^d}) \subseteq C_L(b)^{(d)}.$$

Por hipótese, $[\delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^d}), \underbrace{\delta(\beta_1, \beta_2, \cdots, \beta_{2^d}), \cdots, \delta(\beta_1, \beta_2, \cdots, \beta_{2^d})}_{m}] = 0$, e como

$L^{(d)} = \sum \delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^d})$, $\alpha_1, \alpha_2, \cdots, \alpha_{2^d} \in \hat{A}$, obtemos que

$$[L^{(d)}, \underbrace{\delta(\beta_1, \beta_2, \cdots, \beta_{2^d}), \cdots, \delta(\beta_1, \beta_2, \cdots, \beta_{2^d})}_{m}] = 0.$$

Observamos que $C_L(a)^{(d)} \subseteq C_{L^{(d)}}(a)$ e $C_L(b)^{(d)} \subseteq C_{L^{(d)}}(b)$. Agora, pelo corolário 2.3.5,

$$C_{L^{(d)}}(a) = \sum \delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^d}),$$

onde $\alpha_1\alpha_2 \cdots \alpha_{2^d}(a) = 1$.

Pelo que vimos anteriormente $\delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^d}) \subseteq C_L(c)^{(d)}$, para algum $c \in A^{\#}$.

Fazendo $K = C_{L^{(d)}}(a)$ e usando o Lema 2.3.2, com $\delta(\alpha_1, \alpha_2, \cdots, \alpha_{2^d})$ no lugar de X_i, temos que existe um número inteiro u, $\{m, d, p\}$-limitado, tal que $[L^{(d)}, {}_u K] = 0$. Portanto, pelo Lema 2.3.6, $L^{(d)}$ é nilpotente de classe $\{m, u\}$-limitada. ■

Teorema 2.3.9. *Sejam p um primo e n um inteiro positivo. Seja L uma álgebra de Lie tal que $pL = L$ e seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre L por automorfismos. Assuma que existe um inteiro positivo m de tal forma que $[\gamma_n(C_L(a)), \underbrace{\gamma_n(C_L(b)), \cdots, \gamma_n(C_L(b))}_{m}] = 0$, para quaisquer $a, b \in A^{\#}$. Então, $\gamma_n(L)$ é nilpotente de classe $\{p, n, m\}$-limitada.*

Demonstração: Para todos $\alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_n$ em $\hat{A}$, existem $a, b \in A^{\#}$ tal que $L_{\alpha_1}, \cdots, L_{\alpha_n} \subseteq C_L(a)$ e $L_{\beta_1}, \cdots, L_{\beta_n} \subseteq C_L(b)$. Com isso observamos que

$$\gamma(\alpha_1, \cdots, \alpha_n) \subseteq \gamma_n(C_L(a)) \quad \text{e} \quad \gamma(\beta_1, \cdots, \beta_n) \subseteq \gamma_n(C_L(b)).$$

Como por hipótese $[\gamma_n(C_L(a)), \underbrace{\gamma_n(C_L(b)), \cdots, \gamma_n(C_L(b))}_{m}] = 0$, para todos $a, b \in A^{\#}$, então,

$$[\gamma(\alpha_1, \cdots, \alpha_n), \underbrace{\gamma(\beta_1, \cdots, \beta_n), \cdots, \gamma(\beta_1, \cdots, \beta_n)}_{m}] = 0.$$

O que implica que

$$[\gamma_n(L), \underbrace{\gamma(\beta_1, \cdots, \beta_n), \cdots, \gamma(\beta_1, \cdots, \beta_n)}_{m}] = 0,$$

pois $\gamma_n(L) = \sum \gamma(\alpha_1, \cdots, \alpha_n)$, onde $\alpha_1, \cdots, \alpha_n \in \hat{A}$.

Pelo Corolário 2.3.5

$$C_{\gamma_n(L)}(a) = \sum \gamma(\alpha_1, \cdots, \alpha_n),$$

onde $\alpha_1 \cdots \alpha_n(a) = 1$. Pondo $K = C_{\gamma_n(L)}(a)$ e considerando $\gamma(\alpha_1, \cdots, \alpha_n)$ no lugar de X_i no Lema 2.3.2, concluímos que existe um número inteiro u, $\{m, n, p\}$-limitado, tal que $[\gamma_n(L),_u K] = 0$.

Portanto, pelo Lema 2.3.6, $\gamma_n(L)$ é nilpotente de classe $\{p, u\}$-limitada. ■

2.4 O Anel de Lie Associado a um Grupo

Existem muitas maneiras de obter um anel de Lie associado a um grupo G. Nesta seção apresentamos duas formas distintas de construir um anel de Lie a partir de um dado grupo G, tais construções são as chaves que ligam o que vimos nas seções anteriores deste capítulo com a solução dos problemas propostos inicialmente para grupos. A primeira construção consiste em tomar a soma direta dos quocientes dos termos da série central inferior de G, que com a soma e a multiplicação por colchetes é um anel de Lie. Já na segunda construção utilizamos a conhecida série de Jennings-Lazard-Zassenhaus e obtemos um anel de Lie sobre o corpo com p elementos $\mathbb{F}_p$, onde p é primo.

Associando um anel de Lie a grupos nilpotentes

Dado um grupo G, consideramos a série central inferior de G,

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \cdots .$$

Para cada $i \geq 1$, o quociente $\gamma_i(G)/\gamma_{i+1}(G)$ é um grupo abeliano, de fato pode ser visto como um $\mathbb{Z}$-módulo. Vamos denotar este $\mathbb{Z}$-módulo por $L_i(G)$ e usar a notação aditiva. Para simplificar, usamos γ_i no lugar de $\gamma_i(G)$.

A soma direta

$$L(G) = \bigoplus_{i=0}^{\infty} L_i(G)$$

é abeliana e o somando $L_i(G) = \gamma_i/\gamma_{i+1}$ é chamado *componente homogênea* de $L(G)$. Define-se uma multiplicação $[,]$ entre as componentes homogeneas de $L(G)$ da seguinte forma: dados $a \in \gamma_i$ e $b \in \gamma_j$ arbitrários, temos

$$[a\gamma_{i+1}, b\gamma_{j+1}] = [a, b]\gamma_{i+j+1},$$

onde $[a, b]$ é o comutador de a e b no grupo G. Pode-se mostrar que esta operação está bem definida e que, por $\mathbb{Z}$-linearidade, pode ser estendida a todo $L(G)$.

Primeiramente, observamos alguns fatos sobre a operação definida acima

1. Desde que $[\gamma_s(G), \gamma_t(G)] \leq \gamma_{s+t}(G)$, temos que para $x \in \gamma_i(G)$, $y \in \gamma_j(G)$, o comutador $[x, y] \in \gamma_{i+j}(G)$. Assim podemos tomar a imagem de $[x, y]$ em $\gamma_{i+j}(G)/\gamma_{i+j+1}(G)$.

   Por outro lado, se $x'\gamma_{i+1} = x\gamma_{i+1}$ e $y'\gamma_{j+1} = y\gamma_{j+1}$, temos que $x' = xu$, para algum $u \in \gamma_{i+1}$ e $y' = yv$, para algum $v \in \gamma_{j+1}$. Logo,

$$\begin{aligned} [x', y']\gamma_{i+j+1} &= [xu, yv]\gamma_{i+j+1} = [x, yv][x, yv, u][u, yv]\gamma_{i+j+1} = [x, yv]\gamma_{i+j+1} \\ &= [x, v][x, y][x, y, v]\gamma_{i+j+1} = [x, y]\gamma_{i+j+1}. \end{aligned}$$

Assim, a multiplicação $[,]$ está bem definida.

2. Sejam $x_1\gamma_{i+1}, x_2\gamma_{i+1} \in \gamma_i/\gamma_{i+1}$ e $y\gamma_{j+1} \in \gamma_j/\gamma_{j+1}$. Por definição:

$$\begin{aligned}[x_1\gamma_{i+1} + x_2\gamma_{i+1}, y\gamma_{j+1}] &= [x_1x_2\gamma_{i+1}, y\gamma_{j+1}] = [x_1x_2, y]\gamma_{i+j+1} = [x_1, y][x_1, y, x_2][x_2, y]\gamma_{i+j+1} \\ &= [x_1, y][x_2, y]\gamma_{i+j+1} = [x_1, y]\gamma_{i+j+1} + [x_2, y]\gamma_{i+j+1} \\ &= [x_1\gamma_{i+1}, y\gamma_{j+1}] + [x_2\gamma_{i+1}, y\gamma_{j+1}].\end{aligned}$$

A lei $[x\gamma_{i+1}, y_1\gamma_{j+1} + y_2\gamma_{j+1}] = [x\gamma_{i+1}, y_1\gamma_{j+1}] + [x\gamma_{i+1}, y_2\gamma_{j+1}]$ é verificada similarmente.

3. Temos que $x^{-1}\gamma_{i+1} = -(x\gamma_{i+1})$. E ainda $[x^n, y]\gamma_{i+j+1} = [x, y^n]\gamma_{i+j+1} = n[x\gamma_{i+1}, y\gamma_{j+1}]$.

4. A observação no item (2) mostra que a operação $[,]$ restrita a $L_i \times L_j$ é bilinear.

Com essas observações em mãos, é suficiente verificar os itens (1) e (4) da definição de álgebra de Lie, para mostrar que $L(G)$ é um anel de Lie.

De fato, dados $a, b \in L(G)$, temos $a = a_1 + a_2 + \cdots + a_s$ e $b = b_1 + b_2 + \cdots + b_t$, com $s, t \geq 1$ e $a_i, b_i \in L_i = \gamma_i/\gamma_{i+1}$. Assim, $[a, b] = \sum_{i,j}[a_i, b_j]$, onde $a_i = x_i\gamma_{i+1}$ e $b_i = y_i\gamma_{i+1}$.

Portanto, basta verificar os itens restantes para elementos homogêneos.

Pondo $a_i = x\gamma_{i+1}(G)$, temos

$$[a_i, a_i] = [x\gamma_{i+1}(G), x\gamma_{i+1}(G)] = [x, x]\gamma_{2^i+1}(G) = \gamma_{2^i+1}(G) = 0,$$

e ainda,

$$[a_i, a_j] + [a_j + a_i] = [x, y]\gamma_{i+j+1} + [y, x]\gamma_{i+j+1} = [x, y][y, x]\gamma_{i+j+1} = \gamma_{i+j+1} = 0.$$

Portanto, $[a, a] = 0$, para todo $a \in L(G)$.

Agora, para mostrar que a Identidade de Jacobi vale, sejam $a_i = x\gamma_{i+1}$, $b_j = y\gamma_{j+1}$ e $c_k = z\gamma_{k+1}$. Vamos utilizar propriedades de comutadores de um grupo G, a saber

$a^b = a[a,b]$ e $ab = ba[a,b]$ e a Identidade de Witt $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a = 1$, para $a,b,c \in G$.

Pela identidade de Witt,

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

Logo,

$$\begin{aligned} 0 &= [x,y^{-1},z]\gamma_{i+j+k+1} + [y,z^{-1},x]\gamma_{i+j+k+1} + [z,x^{-1},y]\gamma_{i+j+k+1} \\ &= [[x,y^{-1}]\gamma_{i+j+1}, z\gamma_{k+1}] + [[y,z^{-1}]\gamma_{j+k+1}, x\gamma_{i+1}] + [[z,x^{-1}]\gamma_{k+i+1}, y\gamma_{j+1}] \\ &= [x\gamma_{i+1}, y^{-1}\gamma_{j+1}, z\gamma_{k+1}] + [y\gamma_{j+1}, z^{-1}\gamma_{k+1}, x\gamma_{i+1}] + [z\gamma_{k+1}, x^{-1}\gamma_{i+1}, y\gamma_{j+1}] \\ &= [x\gamma_{i+1}, -y\gamma_{j+1}, z\gamma_{k+1}] + [y\gamma_{j+1}, -z\gamma_{k+1}, x\gamma_{i+1}] + [z\gamma_{k+1}, -x\gamma_{i+1}, y\gamma_{j+1}] \\ &= -[a_i,b_j,c_k] - [b_j,c_k,a_i] - [c_k,a_i,b_j]. \end{aligned}$$

Portanto, $[a_i,b_j,c_k] + [b_j,c_k,a_i] + [c_k,a_i,b_j] = 0$ e, consequêntemente, para todos a,b,c pertencentes a $L(G)$, temos que $[a,b,c] + [b,c,a] + [c,a,b] = 0$.

Com todas essas observações mostramos que $L(G)$ é um anel de Lie com as operações $+$ e $[,]$.

O anel $L(G)$ é conhecido como o anel de Lie associado ao grupo G. A rigor este não é o único anel de Lie que pode ser associado a um grupo, como veremos mais adiante neste trabalho, embora seja o mais comumente usado nas aplicações no trato com grupos nilpotentes.

Uma das principais aplicações para o método do anel de Lie está no trabalho com grupos nilpotentes que consiste em mostrar algumas propriedades para $L(G)$ e tentar obter daí informações sobre o grupo G. Evidentemente, o anel de Lie associado a um grupo

pode ser construído independentemente da nilpotência de G. Entretanto, sua utilização efetiva se dá precisamente em grupos nilpotentes. Tal relação entre um grupo e o anel de Lie associado que definimos acima pode ser vista nos dois seguintes lemas.

Lema 2.4.1. *Seja $L(G)$ o anel de Lie associado ao grupo G, e seja k um inteiro positivo qualquer. Então,*

(i) Para todo $a_j\gamma_2 \in L_1 = G/\gamma_2$ temos que $[a_1\gamma_2, \cdots, a_k\gamma_2] = [a_1, \cdots, a_k]\gamma_{k+1}$;

(ii) $L_k = \langle [a_1\gamma_2, \cdots, a_k\gamma_2]/a_i \in G\rangle$, isto é, $L_k = \langle [\underbrace{L_1, \cdots, L_1}_{k}]\rangle$;

(iii) $L(G) = \langle L_1\rangle$;

(iv) $L(G)^k = \underset{s\geq k}{\oplus} L_s$.

Demonstração: Para mostrar o item (i) basta observarmos que

$$\begin{aligned}[a_1\gamma_2, a_2\gamma_2, \cdots, a_k\gamma_2] &= [[a_1, a_2]\gamma_3, a_3\gamma_2, \cdots, a_k\gamma_2] = [[a_1, a_2, a_3]\gamma_4, a_4\gamma_2, \cdots, a_k\gamma_2] = \\ &= \cdots = [a_1, \cdots, a_k]\gamma_{k+1}.\end{aligned}$$

Sabemos que $\gamma_k(G)$ é gerado por todos os comutadores simples de peso $\geq k$. Logo,

$$L_k = \gamma_k(G)/\gamma_{k+1}(G) = \langle [x_1, \cdots, x_k]\gamma_{k+1} | x_i \in G\rangle\,.$$

Agora, como visto no item anterior $[x_1\gamma_2, x_2\gamma_2, \cdots, x_k\gamma_2] = [x_1, x_2, \cdots, x_k]\gamma_{k+1}$, e o item (ii) segue. Desde que $L(G) = \overset{\infty}{\underset{i=1}{\oplus}} L_i$, segue do item (ii) que $L(G) = \langle L_1\rangle$. Para finalizar, temos que $[L_r, L_s] \leq L_{r+s}$. Deste modo segue que

$$L(G)^k = [\underbrace{L(G), L(G), \cdots, L(G)}_{k}] \leq \underset{i\geq k}{\oplus} L_i.$$

Por outro lado, $L_i = [\underbrace{L_1, L_1, \cdots, L_1}_{i}] \leq L(G)^i \leq L(G)^k$, $i \geq k$. Portanto, $L(G)^k = \underset{s\geq k}{\oplus} L_s$.

■

Lema 2.4.2. *Seja G um grupo nilpotente e seja $L(G)$ o anel de Lie associado a G. Então*

(i) *$L(G)$ é nilpotente e $cl(L(G)) = cl(G)$;*

(ii) *Se G é um grupo finito, então $|G| = |L(G)|$;*

(iii) *Para todo automorfismo φ de G, a ação de φ sobre os quocientes $L_i = \gamma_i(G)/\gamma_{i+1}(G)$ induz por linearidade um automorfismo de $L(G)$.*

Demonstração: Pelo Lema 2.4.1, $L(G)^k = \bigoplus_{s\geq k} L_s$, para todo inteiro positivo k. Se $\gamma_{c+1}(G) = 1$ temos que $L(G)^{c+1} = \bigoplus_{s\geq c+1} L_s = 0$, pois $L_s = \gamma_s(G)/\gamma_{s+1}(G) = 0$, para todo $s \geq c+1$. Por outro lado, se $L(G)^{c+1} = 0$, então, $L_{c+1} = \gamma_{c+1}(G)/\gamma_{c+2}(G) = 0$. Como G é nilpotente, suponha que $cl(G) = c$, logo $\gamma_{c+1}(G) = 1$ e o item (i) segue.

Suponha que $cl(G) = c$, logo $\gamma_{c+1}(G) = 1$. Então, $L(G) = \bigoplus_{i=1}^{c} L_i = \bigoplus_{i=1}^{c} \gamma_i/\gamma_{i+1}$. Portanto, pelo Teorema de Lagrange, $|L(G)| = \prod_{i=1}^{c} |\gamma_i/\gamma_{i+1}| = |G|$, e obtemos o item (ii).

Desde que cada $\gamma_i(G)$ é característico em G, temos que se $\varphi \in Aut(G)$, então φ induz um automorfismo $\overline{\varphi}_i$ em cada $L_i = \gamma_i/\gamma_{i+1}$ dado por

$$(x\gamma_{i+1})\overline{\varphi}_i = x\varphi\gamma_{i+1}.$$

Se $a = a_1 + a_2 + \cdots + a_k \in L(G)$, com $a_i \in L_i$, definamos $a\overline{\varphi} = a_1\overline{\varphi}_1 + a_2\overline{\varphi}_2 + \cdots + a_k\overline{\varphi}_k$.

Observamos que a aplicação $\overline{\varphi}$ é um automorfismo do grupo aditivo $L(G) = \bigoplus_{i=1}^{\infty} L_i$, logo φ induz um automorfismo dos somandos diretos $(\overline{\varphi}_i)$.

Desde que $\overline{\varphi}$ é estendido para a soma por linearidade como a multiplicação, basta mostrar que $\overline{\varphi}$ preserva o produto de Lie para elementos dos somandos.

Pondo $a_i = x\gamma_{i+1}$ e $b_j = y\gamma_{j+1}$, temos

$$\begin{aligned}[a_i, b_j]\overline{\varphi} &= [x\gamma_{i+1}, y\gamma_{j+1}]\overline{\varphi} = ([x,y]\gamma_{i+j+1})\overline{\varphi} = [x,y]\varphi\gamma_{i+j+1} \\ &= [x\varphi, y\varphi]\gamma_{i+j+1} = [x\varphi\gamma_{i+1}, y\varphi\gamma_{j+1}] = [(x\gamma_{i+1})\overline{\varphi}, (y\gamma_{j+1})\overline{\varphi}] \\ &= [a_i\overline{\varphi}, b_j\overline{\varphi}]\end{aligned}$$

e assim, concluímos a demonstração. ■

Se φ é um automorfismo de ordem n do grupo G, então φ induz um automorfismo em $L(G)$, que para simplificar a notação denotamos também como φ, de ordem dividindo n. Além disso, se G é finito e ordem de φ é coprima com a ordem de G, então

$$C_{L(G)}(\varphi) = \oplus_i C_{\gamma_i}(\varphi)\gamma_{i+1}/\gamma_{i+1}.$$

Em particular, se φ age livre de pontos fixos em um grupo nilpotente G, então o mesmo ocorre com o automorfismo induzido sobre $L(G)$.

Uma observação interessante é que ao contrário da classe de nilpotência, o comprimento derivado de $L(G)$ pode não coincidir com o de G, porém, pode-se provar que este não é maior do que o de G.

A série de Jennings-Lazard-Zassenhaus e a Álgebra de Lie Correspondente

Lema 2.4.3. *Seja G um grupo e $G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots$ a série central inferior de G. Temos que,*

(i) Se x, y são elementos de G, então para $n \geq 1$,

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

(ii) Se x, y são elementos de G e H é um subgrupo de G tal que x e $[x, y]$ pertencem a H, então para $n \geq 1$,

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

Demonstração: Seja $R = \gamma_2(G)^{p^n} \prod_{r=1}^{n} \gamma_{p^r}(G)^{p^{n-r}}$. Pela Fórmula de Compilação de Phillip Hall (Teorema 1.4.3), existe um elemento $c_i \in \gamma_i(G)$, com $i = 2, \cdots, p^n$, de tal forma que $x^{p^n} y^{p^n} = (xy)^{p^n} c_2^{\binom{p^n}{2}} \cdots c_{p^n}$. Se $(i, p) = 1$, então $\binom{p^n}{i}$ é divisível por p^n, e para $i > 1$, $c_i^{\binom{p^n}{i}} \in \gamma_2(G)^{p^n} \leq R$. Agora, se $i = p^r j$, com $r \geq 1$ e $(p, j) = 1$, então $c_i^{\binom{p^n}{i}}$ é divisível por p^{n-r} e $i \geq p^r$. Assim, $c_i^{\binom{p^n}{i}} \in \gamma_{p^r}(G)^{p^{n-r}} \leq R$. Portanto, $x^{p^n} y^{p^n} \equiv (xy)^{p^n} mod\ R$ e o item (i) segue.

Consequentemente,

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

Mas $(x[x, y])^{p^n} = (x^y)^{p^n} = (x^{p^n})^y = x^{p^n}[x^{p^n}, y]$, e o resultado segue. ■

Lema 2.4.4. *Se $n \geq 0$, $[\gamma_i(G)^{p^n}, \gamma_j(G)] \leq \prod_{r=0}^{n} \gamma_{j+ip^r}(G)^{p^{n-r}}$.*

Demonstração: Seja $R = \gamma_{j+ip^r}(G)^{p^{n-r}}$. Como R é normal em G, é suficiente mostrar que $[x^{p^n}, y] \in R$ para quaisquer $x \in \gamma_i(G)$, $y \in \gamma_j(G)$. Pelo item (ii) do Lemma 2.4.3,

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

onde $H = \langle x, [x, y] \rangle$. Então, $\gamma_2(H)$ é o fêcho normal de $[x, y, x]$ em H. Assim, temos que $\gamma_2(H) \leq \gamma_{2i+j}(G)$. Como $H \leq \gamma_i(G)$, segue que $\gamma_m(H) \leq \gamma_{mi+j}(G)$ para todo $m \geq 2$. Logo $\gamma_{p^r}(H)^{p^{n-r}} \leq \gamma_{p^r i+j}(G)^{p^{n-r}} \leq R$, para $r = 1, \cdots, n$. Também temos que $\gamma_2(H)^{p^n} \leq \gamma_{i+j}(G)^{p^n} \leq R$ e $[x, y]^{p^n} \in \gamma_{i+1}(G)^{p^n} \leq R$. Portanto, $[x^{p^n}, y] \in R$, como

queríamos. ■

Definição 2.4.5. *Para quaisquer inteiro positivo n e primo p, faça*

$$D_n(G) = \prod_{ip^k \geq n} \gamma_i(G)^{p^k}.$$

$D_n(G)$ é um subgrupo característico de G, e temos a seguinte série

$$G = D_1(G) \geq D_2(G) \geq \cdots \geq D_n(G) \geq \cdots .$$

Note que é possível que $D_{n-1}(G) = D_n(G) \leq D_{n+1}(G)$. Se G for um grupo abeliano, então $D_n(G) = G^{p^k}$, onde k é o menor inteiro tal que $p^k \geq n$. Assim, $D_n(G) = G^{p^k}$ se $p^{k-1} < n \leq p^k$.

Se G for um p-grupo finito então, $D_n(G) = \Phi(G)$ é o subgrupo de Frattini de G. Agora, se G é um grupo de expoente p então, $D_n(G) = \gamma_n(G)$, para todo n.

A série $D_n(G)$ é central em G e para mostrar isso precisamos dos seguintes lemas.

Lema 2.4.6. *Suponha que $i \geq 1$, $j \geq 1$ e $h \geq 0$. Seja $R = \prod_{r=0}^{h} \gamma_{i+jp^r}(G)^{p^{h-r}}$. Se $x \in \gamma_i(G)$ e $n \geq 2$, então $\gamma_n(\langle x, R\rangle) \leq \prod_{r=0}^{h} \gamma_{in+jp^r}(G)^{p^{h-r}}$.*

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

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

Aplicando o Lema 1.1.2 e o Lema 2.4.4, temos que

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

pois $i + p^s in - p^s i \geq in$. E o lema segue. ■

Lema 2.4.7. *Seja $i \geq 1$, $j \geq 1$, $h \geq 0$ e $k \geq 0$, então $[\gamma_i(G)^{p^k}, \gamma_j(G)^{p^h}] \leq D_{ip^k+jp^h}(G)$.*

Demonstração: Suponha que $x \in \gamma_i(G)$ e $y \in \gamma_j(G)$. Sejam $z = [x, y^{p^h}]$ e $H = \langle x, z\rangle$. Pelo Lema 2.4.3 item (ii),

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

Para $n = 1, \cdots, p^k$, defina $H_n = \prod_{r=0}^{h}\gamma_{in+jp^r}(G)^{p^{h-r}}$. Pelo Lema 2.4.4, $z \in H_1$. Assim $H \leq \langle x, H_1\rangle$ e, pelo Lema 2.4.6, $\gamma_n(H) \leq H_n$. Portanto,

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

Faça $R = D_{ip^k+jp^h}(G)$. Se $m+h-r \geq k$, então, pela definição de D_i, $\gamma_{ip^m+jp^r}(G)^{p^{h-r}} \leq R$. Assim, se $s = max(m + h - k + 1, 0)$ então

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

Portanto,

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

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

Logo $[x^{p^k}, y^{p^h}] \in R$ e $(x^{p^k})R$ comuta com $(y^{p^h})R$. Portanto, cada elemento de $\gamma_i(G)^{p^k}R/R$ comuta com cada elemento de $\gamma_j(G)^{p^h}R/R$, e $[\gamma_i(G)^{p^k}, \gamma_j(G)^{p^h}] \leq R$. ■

Teorema 2.4.8. *Sejam $\{D_i\}$ a série definida em 2.4.5 e p um primo, então*

(i) $[D_m(G), D_n(G)] \leq D_{n+m}(G)$;

(ii) $D_n(G)^p \leq D_{p^n}(G)$;

(iii) Para $n > 1$, $D_n(G) = [D_{n-1}(G), G]D_m(G)^p$, onde m é o menor inteiro tal que $pm \geq n$.

Demonstração: O item (i) segue imediatamente da definição de $\{D_i\}$ e do Lema 2.4.7. Logo restam os dois últimos itens.

Pelo item (i) temos que $\gamma_p(D_n(G)) \leq \gamma_{pn}(G)$, assim $D_n(G)/D_{pn}(G)$ é regular (veja a seção 4 do primeiro capítulo deste trabalho). Mas $D_n(G)/D_{pn}(G)$ é gerado por elementos de ordem p pois se $ip^k \geq n$ e $x \in \gamma_i(G)$ então, $(x^{p^k})^p \in D_{ip^{k+1}}(G) \leq D_{pn}(G)$. Portanto, pelo Teorema 1.4.8, $(D_n(G)/D_{pn}(G))^p = 1$ e ainda $D_n(G)^p \leq D_{pn}(G)$. E o item (ii) está provado.

Pelos itens (i) e (ii), $[D_{n-1}(G), G]D_m(G)^p \leq D_n(G)$. Suponha que $ip^k \geq n$. Se $k = 0$,

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

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

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

Portanto, $\gamma_i(G)^{p^k} \leq [D_{n-1}(G), G]D_m(G)^p$ em qualquer caso, e a afirmação segue da definição de $\{D_i\}$. ■

Corolário 2.4.9. *Suponha que $G = R_1 \geq R_2 \geq \cdots$ é uma série do grupo G tal que $R_n \trianglelefteq G$, $[R_n, G] \leq R_{n+1}$ e $R_n^p \leq R_{np}$ para todo $n \geq 1$. Então, $R_n \geq D_n(G)$ para todo $n \geq 1$.*

Demonstração: Segue do Teorema 2.4.8 item (iii) por indução sobre n. ■

Com isso demonstramos que a série $D_n(G)$ é central em G. A série $D_n(G)$ é chamada *Série de Jennings-Lazard-Zassenhaus.*

Definição 2.4.10. *Seja p um número primo arbitrário mas fixo. Seja G um grupo. Uma série de subgrupos*

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

é uma N-série *se satisfaz $[G_i, G_j] \leq G_{i+j}$ para todos i, j. Toda N-série é central (i.e. $G_i/G_{i+1} \leq Z(G/Gi+1)$ para todo i). Uma N-série é uma* N_p-série *se $G_i^p \leq G_{pi}$ para todo i.*

Podemos associar um anel de Lie $L^*(G)$ a qualquer N_p-serie $(*)$ de um grupo G da seguinte forma

Dado uma N_p-série $(*)$, seja $L^*(G) = \oplus L_i^*$, onde $L_i^* = G_i/G_{i+1}$, escrito aditivamente. A comutação em G induz uma operação binária $[,]$ em L. Para elementos homogêneos $xG_{i+1} \in L_i^*$ e $yG_{j+1} \in L_j^*$ a operação é definida por

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

e estendida para elementos arbitrários de $L^*(G)$ por linearidade. É fácil checar que essa operação está bem definida e que $L^*(G)$ com as operações $+$ e $[,]$ é um anel de Lie sobre $\mathbb{F}_p$. Como fizemos as contas no caso anterior do anel de Lie associado a grupos nilpotentes e os cálculos são praticamente os mesmos, não os explicitaremos aqui.

Para qualquer $x \in G_i/G_{i+1}$ denotamos x^* como o elemento xG_{i+1} de $L^*(G)$.

Lema 2.4.11 (Lazard [16]). *Se $(*)$ é uma N_p-série então $(adx^*)^p = ad(x^p)^*$ para qualquer $x \in G$. Consequentemente, se x tem ordem finita t, então x^* é ad-nilpotente de índice no máximo t.*

Seja Fr o grupo Livre com geradores livres $x_1, x_2, \cdots$, e escolha um elemento não trivial $w = w(x_1, x_2, \cdots, x_s)$ em Fr. Dizemos que o grupo G satisfaz a identidade $w \equiv 1$ se $w(g_1, g_2, \cdots, g_s) = 1$ para quaisquer elementos $g_1, g_2, \cdots, g_s$ em G.

A seguinte proposição pode ser extraída da demonstração do Teorema 1 no artigo de Wilson e Zel'manov [31].

Proposiçao 2.4.12. *Seja G um grupo satisfazendo uma identidade $w \equiv 1$. Então, existe um polinômio de Lie f sobre $\mathbb{F}_p$ multilinear, diferente de zero, dependendo somente de p e w tal que para qualquer N_p-série $(*)$ de G a algebra $L^*(G)$ satisfaz a identidade $f \equiv 0$.*

De fato, Wilsom e Zelmanov [31], descreveram um algorítmo efetivo para escrever f explicitamente para qualquer p e w. Mas não vamos precisar desse algorítmo nesse trabalho.

Um grupo G pode ter muitas N_p-séries, mas podemos observar pelo Teorema 2.4.8 que a série Jennings-Lazard-Zassenhaus $\{D_i\}$, definida anteriormente, é uma N_p-série.

Associamos a G a álgebra de Lie $DL(G)$ sobre $\mathbb{F}_p$ correspondente a série de Jennings-Lazard-Zassenhaus, ou seja, $DL(G) = \oplus L_i$ com $L_i = D_j/D_{j+1}$, onde $D_i = D_i(G)$. Se A age sobre o grupo G, A induz um grupo de automorfismo de todo quociente D_j/D_{j+1}. Essa ação estende-se para a soma direta $\oplus D_j/D_{j+1}$. Assim, A pode ser visto como um grupo agindo sobre a subálgebra $L_p(G) = \langle L_1 \rangle$ de $DL(G)$ gerada por L_1, como automorfismo de álgebras de Lie.

Proposiçao 2.4.13. *Seja G um grupo gerado pelos elementos $a_1, a_2, \cdots, a_m$, e assuma que $L_p(G)$ é nilpotente de classe no máximo c. Seja $\rho_1, \rho_2, \cdots, \rho_s$ a lista de todos os*

comutadores simples nos geradores $a_1, a_2, \cdots, a_m$ *de peso* $\leq c$. *Então, para qualquer inteiro não negativo* i *o grupo* G *pode ser escrito como um produto*

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

dos subgrupos cíclicos gerados por $\rho_1, \rho_2, \cdots, \rho_s$ *e* D_{i+1}.

Demonstração: Primeiramente observamos que para qualquer inteiro i o subgrupo D_i é gerado por D_{i+1} e elementos da forma $[b_1, \cdots, b_j]^{p^k}$, onde $jp^k \geq i$ e $b_1, \cdots, b_j \in \{a_1, a_2, \cdots, a_m\}$. Essa observação pode ser demonstrada usando o Lema 2.4.3 e a Identidade de Witt.

Para demonstrar a proposição usamos indução sobre i. O caso $i = 0$ é trivial. Assuma que $i \geq 1$ e

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

Então, qualquer elemento $x \in G$ pode ser escrito na forma

$$x = \rho_1^{\alpha_1}\rho_2^{\alpha_2}\cdots\rho_s^{\alpha_s} y,$$

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

Pela observação feita no primeiro parágrafo podemos escrever

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

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

Denote $a_l D_2 \in L_p(G)$ por $\bar{a_l}$, $l = 1, \cdots, m$. Por hipótese $L_p(G)$ é nilpotente de classe c, logo $[\bar{b_1}, \cdots, \bar{b_{c+1}}] = 0$ para quaisquer $b_1, \cdots, b_{c+1} \in \{a_1, a_2, \cdots, a_m\}$. Isso implica que $[b_1, \cdots, b_{c+1}] \in D_{c+2}$ para quaisquer $b_1, \cdots, b_{c+1} \in \{a_1, a_2, \cdots, a_m\}$ e $\gamma_{c+1} \leq D_{c+2}$. Então, como $\{D_i\}$ é uma N_p-série, para qualquer $d \geq c+1$ temos $\gamma_d \leq D_{d+1}$.

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

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

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

Novamente, pelo fato de $\{D_i\}$ ser uma N_p-série, temos que $\sigma_n^{p^{k_n}} \in Z(G)$. Agora, comparando a maneira que escrevemos x e y, obtemos que

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

como queríamos. ■

Lema 2.4.14. *Suponha que G é um p-grupo finito d-gerado tal que a álgebra de Lie $L_p(G)$ é nilpotente de classe c. Então, G tem um subgrupo potente característico de índice $\{p, c, d\}$-limitado.*

Demonstração: Sejam $\rho_1, \rho_2, \cdots, \rho_s$ todos os comutadores simples de peso $\geq c$ nos geradores de G. Aqui s é um número $\{c, d\}$-limitado. Como G é um p-grupo finito e a classe de nilpotência de $L_p(G)$ é c, pela proposição anterior, temos que todo elemento $g \in G$ pode ser escrito da forma $g = \rho_1^{k^1}, \rho_2^{k^2}, \cdots, \rho_s^{k^s}$. Portanto, $|G/G^{p^m}| \leq p^{sm}$ para qualquer inteiro positivo m. Seja V a interseção dos núcleos de todos os homomorfismos de P em $GL_s(\mathbb{F}_p)$. Faça $W = V$ se $p \neq 2$, ou $W = V^2$ se $p = 2$. O expoente do p-subgrupo de Sylow de $GL_s(\mathbb{F}_p)$ é um número $\{p, s\}$-limitado. Então, $G^{p^a} \leq W$ para algum número $\{p, s\}$-limitado a que também é $\{p, c, d\}$-limitado pois s é $\{c, d\}$-limitado. Existe um número, $u \geq a$ $\{p, c, d\}$-limitado, tal que $|G^{p^u}/G^{p^{u+r}}| \leq p^s$, por outro lado a desigualdade $|G/G^{p^m}| \leq p^{sm}$ será falsa para algum m. Então, $G^{p^u} \leq G^{p^a} \leq W$, e G^{p^u} é um grupo potente. O índice de G^{p^u} é no máximo p^{us} e portanto é $\{p, c, d\}$-limitado. ■

O seguinte resultado foi obtido por Riley [20] e pode ser deduzido facilmente utilizando o Lema 2.4.14 em conjunto com o Teorema 1.4.15.

Lema 2.4.15. *Suponha que G é um p-grupo finito d-gerado tal que a álgebra de Lie $L_p(G)$ é nilpotente de classe c. Então, o posto de G é $\{p, c, d\}$-limitado.*

Seja H um subgrupo de um grupo G, denotamos por $L(G, H)$ o subconjunto de $DL(G)$ gerado pelos elementos homogêneos da forma hD_{j+1}, onde $h \in D_j \cap H$. Temos que $L(G, H)$ é uma subálgebra de $DL(G)$. Além disso, $L(G, H)$ é isomorfa a álgebra de Lie associada com a N_p-série $\{H_i\}$ de H com $H_i = D_i \cap H$. Da mesma forma, temos ainda que $L_p(G, H) = L_p(G) \cap L(G, H)$. Pelo Lema 1.3.1, se G é um grupo finito e se A é de ordem coprima com G, então $L_p(G, C_G(A)) = C_{L_p(G)}(A))$.

Lema 2.4.16. *Suponha que qualquer comutador de Lie em elementos homogêneos $x_1, x_2, \cdots, x_r$ de $DL(G)$ é ad-nilpotente de índice no máximo t. Seja $K = \langle x_1, x_2, \cdots, x_r \rangle$ e assuma que $K \leq L(G, H)$ para algum subgrupo H de G satisfazendo a identidade $w \equiv 1$. Então para algum número u, $\{r, t, w, p\}$-limitado, temos que $[DL(G), \underbrace{K, \cdots, K}_{u}] = 0$.*

Demonstração: Em vista do Lema 2.3.3 é suficiente mostrar que K tem classe de nilpotencia $\{r, t, w, p\}$-limitada. Sabemos pela Proposição 2.4.12 que K satisfaz certa identidade polinomial multilinear dependendo somente de w. Assim o Teorema 2.2.1 mostra que K tem classe de nilpotência $\{r, t, w, p\}$-limitada. ■

Capítulo 3

Limitando a Classe de Nilpotência em Grupos Finitos

Nosso objetivo nesse capítulo, como mencionamos na introdução deste trabalho, é demonstrar os seguintes resultados:

Teorema 1. *Sejam p um primo, n, d inteiros positivos tais que $2^d \leq n$. Seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre um p'-grupo finito G. Assuma que existe um inteiro positivo m tal que $[C_G(a)^{(d)}, \underbrace{C_G(b)^{(d)}, \cdots, C_G(b)^{(d)}}_{m}] = 1$, para todos $a, b \in A^{\#}$. Então, $G^{(d)}$ é nilpotente de classe $\{p, d, m\}$-limitada.*

Teorema 2. *Sejam p um primo e n um inteiro positivo. Seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre um p'-grupo finito G. Assuma que existe um inteiro positivo m tal que $[\gamma_n(C_G(a)), \underbrace{\gamma_n(C_G(b)), \cdots, \gamma_n(C_G(b))}_{m}] = 1$, para todos $a, b \in A^{\#}$. Então, $\gamma_n(G)$ é nilpotente de classe $\{p, n, m\}$-limitada.*

De certa forma o maior esforço no sentido de demonstrar os Teoremas 1 e 2 foi feito na terceira seção do capítulo anterior com a formulação e solução destes problemas para álgebras de Lie, pois o primeiro passo que damos é associar um anel de Lie a série central inferior dos subgrupos $\gamma_n(G)$ e $G^{(d)}$ de G e assim verificar que valem as hipóteses dos

Teoremas 2.3.9 e 2.3.8 para estes anéis de Lie associados. Constatamos então que estes anéis de Lie associados aos subgrupos $G^{(d)}$ e $\gamma_n(G)$ tem classes de nilpotência $\{p,d,m\}$-limitada e $\{p,n,m\}$-limitada respectivamente. Consequentemente, pela finitude de G, concluímos que tanto G^d quanto $\gamma_n(G)$ tem classe $\{p,d,m\}$-limitada e $\{p,n,m\}$-limitada respectivamente.

3.1 Caso Geral

Para qualquer inteiro positivo j e para quaisquer subgrupos $H_1,\cdots,H_{2^j}$ de um grupo G, definimos indutivamente

$$\delta(H_1)=H_1,\ \cdots,\ \delta(H_1,\cdots,H_{2^j})=[\delta(H_1,\cdots,H_{2^{j-1}}),\delta(H_{2^{j-1}+1},\cdots,H_{2^j})].$$

Em particular, se H é um subgrupo de um grupo G, então $H^{(j)}=\delta(\underbrace{H,\cdots,H}_{2^j})$.

Lema 3.1.1. *Sejam p um primo e k um inteiro positivo com $k\geq 3$. Seja A um p-grupo abeliano elementar de ordem p^k agindo sobre um p'-grupo finito G. Sejam $A_1,A_2,\cdots,A_s$ os subgrupos maximais de A, então para n tal que $2^n\leq k-1$ temos que*

$$G^{(n)}=\langle\delta(C_G(A_{i_1}),\cdots,C_G(A_{i_{2^n}}))|1\leq i_1,i_2,\cdots,i_{2^n}\leq s\rangle\,,$$

e para n tal que $n\leq k-1$ temos que

$$\gamma_n(G)=\langle[C_G(A_{i_1}),C_G(A_{i_2}),\cdots,C_G(A_{i_n})]|1\leq i_1,\cdots,i_n\leq s\rangle\,.$$

Demonstração: Considere o subgrupo

$$R_l=\left\langle\delta(C_G(A_{i_1}),\cdots,C_G(A_{i_{2^l}}))|1\leq i_1,i_2,\cdots,i_{2^l}\leq s\right\rangle,$$

onde $2^l\leq k-1$. É fácil ver que $R_l\leq G^{(l)}$, para mostrar a outra inclusão usamos indução sobre l. Para $l=1$ temos, pelo Lema 1.3.8, $R_1=G'=\langle[C_G(A_{i_1}),C_G(A_{i_2})]|1\leq i_1,i_2\leq s\rangle$.

Como hipótese de indução temos que $R_{l-1} = G^{(l-1)}$. Vamos mostrar que $R'_{l-1} \leq R_l$. Para quaisquer $C_G(A_{j_1}), \cdots, C_G(A_{j_{2^l}}) \leq G$, temos que

$$[\delta(C_G(A_{i_1}), \cdots, C_G(A_{i_{2^l}})), \delta(C_G(A_{j_1}), \cdots, C_G(A_{j_{2^{l-1}}}))] \leq R_l.$$

O que implica que R_l é normal em R_{l-1}, e ainda o quociente R_{l-1}/R_l é abeliano. Portanto, $R'_{l-1} \leq R_l$ como queríamos.

Agora, dado $m \leq k-1$, considere o subgrupo

$$S_m = \langle [C_G(A_{i_1}), C_G(A_{i_2}), \cdots, C_G(A_{i_m})] | 1 \leq i_1, \cdots, i_m \leq s \rangle .$$

Usamos indução sobre m. Se $m = 2$, pelo Lema 1.3.8, temos que $S_2 = \gamma_2(G) = G'$. Considere então o subgrupo S_{m-1} para $m \geq 3$. Temos que para quaisquer subgrupos $C_G(A_j), C_G(A_{i_1}), C_G(A_{i_2}), \cdots, C_G(A_{i_m})$ de G,

$$[[C_G(A_{i_1}), \cdots, C_G(A_{i_{m-1}})], C_G(A_j)] \leq S_m,$$

isto é, $[S_{m-1}, C_G(A_j)] \leq S_m$ para todo j. Portanto, como G é gerado pelos $C_G(A_j)$, temos que $S_m = \gamma_m(G)$. ■

Lema 3.1.2. *Assuma as hipóteses do Teorema 1. Então, $G^{(d)}$ é nilpotente.*

Demonstração: Assuma que G é um contraexemplo cuja ordem é a menor possível. Como cada $C_G(a)$ é solúvel, para todo $a \in A^{\#}$ segue, por Glauberman (Teorema 1.3.9), que G é solúvel. Por hipótese, temos que a d-ésima derivada do subgrupo G' de G, isto é $G^{(d+1)}$, é nilpotente. Temos ainda que $G^{(d+1)}$ é abeliano. De fato, se $G^{(d+1)}$ não é abeliano, $G^{(d)}/G^{(d+2)}$ é nilpotente pela hipótese de indução e assim, pelo Critério de Ph. Hall (Teorema 1.1.7), $G^{(d)}$ é nilpotente, uma contradição. Portanto, $G^{(d+1)}$ é abeliano.

Sejam $A_1, \cdots, A_s$ os subgrupos maximais de A. Pelo Lema 3.1.1, temos que $G^{(d+1)}$ é gerado pelos $\delta(C_{G'}(A_{i_1}), \cdots, C_{G'}(A_{i_{2^d}}))$ com $1 \leq i_1, i_2, \cdots, i_{2^d} \leq s$. Para $A_{k_1}, \cdots, A_{k_{2^d}}$ seja $R = \delta(C_G(A_{k_1}), \cdots, C_G(A_{k_{2^d}}))$. Como a ordem de A é p^{n+1} e $2^d \leq n$, existe $a \in A^{\#}$ tal que os centralizadores $C_G(A_{k_1}), \cdots, C_G(A_{k_{2^d}})$ estão todos contidos em $C_G(a)$ e portanto $\delta(C_G(A_{k_1}), \cdots, C_G(A_{k_{2^d}})) \subseteq C_G(a)^{(d)}$. Então, temos que

$$[G^{(d+1)}, \underbrace{R, \cdots, R}_{m}] = [\prod_i \delta(C_{G'}(A_{i_1}), \cdots, C_{G'}(A_{i_{2^d}})), \underbrace{R, \cdots, R}_{m}] =$$

$$= \prod_i [\delta(C_{G'}(A_{i_1}), \cdots, C_{G'}(A_{i_{2^d}})), \underbrace{R, \cdots, R}_{m}] = 1.$$

Assim, $G^{(d+1)}R$ é nilpotente. Consequêntemente, $G^{(d+1)}R$ é um subgrupo subnormal nilpotente de G. Segue que $R \subseteq F(G)$. Portanto, como tomamos R arbitrariamente e $G^{(d)}$ é gerado pelos $\delta(C_G(A_{i_1}), \cdots, C_G(A_{i_{2^d}}))$ com $1 \leq i_1, i_2, \cdots, i_{2^d} \leq s$, temos que $G^{(d)}$ é nilpotente. ■

Agora podemos demonstrar o Teorema 1.

Teorema 1. *Sejam p um primo, n, d inteiros positivos tais que $2^d \leq n$. Seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre um p'-grupo finito G. Assuma que existe um inteiro positivo m tal que $[C_G(a)^{(d)}, \underbrace{C_G(b)^{(d)}, \cdots, C_G(b)^{(d)}}_{m}] = 1$, para todos $a, b \in A^{\#}$. Então, $G^{(d)}$ é nilpotente de classe $\{p, d, m\}$-limitada.*

Demonstração: Seja $L(G^{(d)})$ o anel de Lie associado ao grupo $G^{(d)}$ e considere o produto tensorial $L = L(G^{(d)}) \otimes \mathbb{Z}[w]$, onde w é uma p-ésima raiz primitiva da unidade. Temos que L é uma álgebra de Lie sobre $\mathbb{Z}[w]$ e A age sobre L. Como G é um grupo finito e mostramos que $G^{(d)}$ é nilpotente, para mostrar que a classe de nilpotência de $G^{(d)}$ é $\{p, d, m\}$-limitada é suficiente mostrar que $L(G^{(d)})$ tem classe $\{p, d, m\}$-limitada. Para tanto, dividimos a demonstração em duas partes. A primeira consiste em, utilizar o Lema

2.3.8 para demonstrar que $L^{(d)}$ tem classe $\{p, d, m\}$-limitada. Em um segundo momento, utilizamos indução para mostrar que L tem classe $\{p, d, m\}$-limitada, e concluimos então, que $L(G^{(d)})$ é nilpotente de classe $\{p, d, m\}$-limitada.

Para facilitar a notação utilizamos γ_i no lugar de $\gamma_i(G^{(d)})$.

Se $a \in A^{\#}$, temos que $C_L(a) = \oplus\, C_{\gamma_i}(a)\gamma_{i+1}/\gamma_{i+1}$ e pelo Lema 3.1.1

$$C_L(a)^{(d)} = \sum \delta(C_{\gamma_{i_1}}(a), C_{\gamma_{i_2}}(a), \cdots, C_{\gamma_{i_{2^d}}}(a))\gamma_{i_1+i_2+\cdots+i_{2^d}+1}/\gamma_{i_1+i_2+\cdots+i_{2^d}+1}.$$

Logo,

$$[C_L(a)^{(d)}, \underbrace{C_L(b)^{(d)}, \cdots, C_L(b)^{(d)}}_{m}] = \sum [T, Y_1, \cdots, Y_m],$$

onde T e Y_k são da seguinte forma.

$T = \delta(C_{\gamma_{i_1}}(a), C_{\gamma_{i_2}}(a), \cdots, C_{\gamma_{i_{2^d}}}(a))\gamma_{i_1+i_2+\cdots+i_d+1}/\gamma_{i_1+i_2+\cdots+i_d}$ e

$Y_k = \delta(C_{\gamma_{j_{1_k}}}(b), C_{\gamma_{j_{2_k}}}(b), \cdots, C_{\gamma_{j_{2^d_k}}}(b))\gamma_{j_{1_k}+j_{2_k}+\cdots+j_{2^d_k}+1}/\gamma_{j_{1_k}+j_{2_k}+\cdots+j_{2^d_k}+1}.$

Por hipótese, $[C_G(a)^{(d)}, \underbrace{C_G(b)^{(d)}, \cdots, C_G(b)^{(d)}}_{m}] = 1$. Então, $[T, Y_1, \cdots, Y_m] = 0$ e, portanto,

$$[C_L(a)^{(d)}, \underbrace{C_L(b)^{(d)}, \cdots, C_L(b)^{(d)}}_{m}] = 0.$$

Concluímos, pelo Lema 2.3.8, que $L^{(d)}$ é nilpotente de classe $\{p, d, m\}$-limitada.

O objetivo agora é mostrar que L é nilpotente de classe $\{p, d, m\}$-limitada.

Sejam $A_1, \cdots, A_s$ os subgrupos maximais de A. Pelo Lema 3.1.1 temos que

$$G^{(d)} = \left\langle \delta(C_G(A_{i_1}), \cdots, C_G(A_{i_{2^d}})) | 1 \leq i_1, i_2, \cdots, i_{2^d} \leq s \text{ e } 2^d \leq n \right\rangle.$$

Sejam $X_1, \cdots, X_t$ as imagens dos subgrupos da forma $\delta(C_G(A_{j_1}), \cdots, C_G(A_{j_{2^d}}))$ em $G^{(d)}/G^{(d+1)}$. Logo, L é gerado pelos conjuntos $X_1, \cdots, X_t$.

Como a ordem de A é p^{n+1} e $2^d \leq n$, para quaisquer $i_1, \cdots, i_{2^d}, j_1, \cdots, j_{2^d} \leq s$ existem $a, b \in A^{\#}$ tais que os centralizadores $C_G(A_{i_1}), \cdots, C_G(A_{i_{2^d}})$ estão todos contidos em $C_G(a)$

e $C_G(A_{j_1}), \cdots, C_G(A_{j_{2^d}})$ estão todos contidos em $C_G(b)$. Por hipótese, temos que

$$[\delta(C_G(A_{i_1}), \cdots, C_G(A_{i_{2^d}})), \underbrace{\delta(C_G(A_{j_1}), \cdots, C_G(A_{j_{2^d}})), \cdots, \delta(C_G(A_{j_1}), \cdots, C_G(A_{j_{2^d}}))}_{m}] = 1,$$

logo

$$[C_{G^{(d)}}(A_k), \underbrace{\delta(C_G(A_{j_1}), \cdots, C_G(A_{j_{2^d}})), \cdots, \delta(C_G(A_{j_1}), \cdots, C_G(A_{j_{2^d}}))}_{m}] = 1.$$

Agora, se X_l é a imagem de $\delta(C_G(A_{j_1}), \cdots, C_G(A_{j_{2^d}}))$ em $G^{(d)}/G^{(d+1)}$, segue que $[C_L(A_k), \underbrace{X_l, \cdots, X_l}_{m}] = 0$, portanto $[L, \underbrace{X_l, \cdots, X_l}_{m}] = 0$ pois $L = \sum_k C_L(A_k)$.

Faça $Z = Z(L^{(d)})$. Temos que $[Z, X, Y] = [Z, Y, X]$ para quaisquer subconjuntos $X, Y \subseteq L^{(d-1)}$.

Ponha $r = (m-1)t + 1$. Como L é gerado pelos conjuntos $X_1, \cdots, X_t$, então $L^{(d-1)}$ é gerado por $\delta(X_{i_1}, X_{i_2}, \cdots, X_{i_{2^{d-1}}})$, com $1 \leq i_1, \cdots, i_{2^{d-1}} \leq t$. Levando em conta estes fatos, temos que

$$[Z, {}_r\, L^{(d-1)}] = \sum [Z, {}_{u_1}\, \delta_1(X^1_{i_1}, X^1_{i_2}, \cdots, X^1_{i_{2^{d-1}}}), \cdots, {}_{u_t}\, \delta_t(X^t_{i_1}, X^t_{i_2}, \cdots, X^t_{i_{2^{d-1}}})],$$

onde $u_1 + \cdots + u_t = r$.

O número r é suficientemente grande para que $u_j \geq m$ para algum j. Afirmamos que

$$[Z, {}_{u_1}\, \delta_1(X^1_{i_1}, X^1_{i_2}, \cdots, X^1_{i_{2^{d-1}}}), \cdots, {}_{u_t}\, \delta_t(X^t_{i_1}, X^t_{i_2}, \cdots, X^t_{i_{2^{d-1}}})] = 0.$$

De fato, temos que $\delta_k(X^k_{i_1}, X^k_{i_2}, \cdots, X^k_{i_{2^{d-1}}}) \subset X_j$, para algum $j \in \{1, 2, \cdots, t\}$ e ainda $[L, \underbrace{X_j, \cdots, X_j}_{m}] = 0$, o que conclui nossa afirmação. Logo, $[Z, \underbrace{L^{(d-1)}, \cdots, L^{(d-1)}}_{r}] = 0$ e $Z \leq Z_r(L^{(d-1)})$, onde Z_r é o r-ésimo termo da série central superior de $L^{(d-1)}$.

Aplicando este argumento repetidamente para $L^{(d-1)}/Z$, $L^{(d-1)}/Z_2(L^{(d)}), \cdots$ e assim por diante, concluimos que $L^{(d)} \leq Z_{er}(L^{(d-1)})$.

Portanto, $L^{(d-1)}$ é nilpotente de classe no máximo $er+1$.

Por indução, concluímos que $L^{(d-2)}, L^{(d-3)}, \cdots, L$, são nilpotentes de classe $\{p,d,m\}$-limitada. ■

Seguindo os mesmos passos da demonstração do Lema 3.1.2 temos o seguinte resultado.

Lema 3.1.3. *Assuma as hipótese do Teorema 2. Então, $\gamma_n(G)$ é nilpotente.*

A demonstração de que $\gamma_n(G)$ é nilpotente é idêntica a que fizemos na demonstração do Lema 3.1.2 para $G^{(d)}$ e por esta razão a omitimos. Nos resta então mostrar que, sob as hipóteses do Teorema 2, a classe de nilpotência de $\gamma_n(G)$ é $\{p,n,m\}$-limitada e essa demonstração segue os mesmos passos da demonstração do Teorema 1.

Teorema 2. *Sejam p um primo e n um inteiro positivo. Seja A um p-grupo abeliano elementar de ordem p^{n+1} agindo sobre um p'-grupo finito G. Assuma que existe um inteiro positivo m tal que $[\gamma_n(C_G(a)), \underbrace{\gamma_n(C_G(b)), \cdots, \gamma_n(C_G(b))}_{m}] = 1$, para todos $a, b \in A^{\#}$. Então, $\gamma_n(G)$ é nilpotente de classe $\{p,n,m\}$-limitada.*

Demonstração: Seja $L(\gamma_n(G))$ o anel de Lie associado ao grupo $\gamma_n(G)$. Faça $L = L(\gamma_n(G)) \otimes \mathbb{Z}[w]$, onde w é uma p-ésima raiz primitiva da unidade. L é uma álgebra de Lie sobre $\mathbb{Z}[w]$ e A age sobre L. Temos que L é nilpotente pois $\gamma_n(G)$ o é, logo é suficiente mostrar que $L(\gamma_n(G))$ tem classe $\{p,n,m\}$-limitada. Novamente, dividimos a demonstração em duas parte. A primeira consiste em utilizar o Lema 2.3.9 para demonstrar que $\gamma_n(L)$ tem classe $\{p,n,m\}$-limitada. Em seguida, utilizamos recursividade para mostrar que L tem classe $\{p,n,m\}$-limitada, concluindo então, que $L(\gamma_n(G))$ é nilpotente com classe $\{p,n,m\}$-limitada.

Para facilitar a notação utilizamos γ_i no lugar de $\gamma_i(\gamma_n(G))$.

Se $a \in A^{\#}$, temos que $C_L(a) = \oplus\, C_{\gamma_i}(a)\gamma_{i+1}/\gamma_{i+1}$ e pelo Lema 3.1.1

$$\gamma_n(C_L(a)) = \sum [C_{\gamma_{i_1}}(a), C_{\gamma_{i_2}}(a), \cdots, C_{\gamma_{i_n}}(a)]\gamma_{i_1+i_2+\cdots+i_n+1}/\gamma_{i_1+i_2+\cdots+i_n+1},$$

onde $[C_{\gamma_{i_1}}(a), C_{\gamma_{i_2}}(a), \cdots, C_{\gamma_{i_n}}(a)] = B \leq \gamma_n(C_G(a))$.

Então,

$$[\gamma_n(C_L(a)), \underbrace{\gamma_n(C_L(b)), \cdots, \gamma_n(C_L(b))}_{m}] = \sum [T, Y_1, \ldots, Y_m],$$

onde $T = B\gamma_{i_1+i_2+\cdots+i_n+1}/\gamma_{i_1+i_2+\cdots+i_n+1}$ e $Y_k = D_k\gamma_{j_{1_k}+j_{2_k}+\cdots+j_{n_k}+1}/\gamma_{j_{1_k}+j_{2_k}+\cdots+j_{n_k}+1}$, com $D_k \leq \gamma_n(C_G(b))$.

Por hipótese, $[\gamma_n(C_G(a)), \underbrace{\gamma_n(C_G(b)), \cdots, \gamma_n(C_G(b))}_{m}] = 1$, então $[T, Y_1, \ldots, Y_m] = 0$. Portanto,

$$[\gamma_n(C_L(a)), \underbrace{\gamma_n(C_L(b)), \cdots, \gamma_n(C_L(b))}_{m}] = 0.$$

Concluímos, pelo Lema 2.3.9, que $\gamma_n(L)$ é nilpotente de classe e, $\{p, n, m\}$-limitada, e a primeira parte da demonstração está concluída.

O objetivo agora é mostrar que L é nilpotente de classe $\{p, n, m\}$-limitada.

Sejam $A_1, \cdots, A_s$ os subgrupos maximais de A. Pelo Lema 3.1.1,

$$\gamma_n(G) = \langle [C_G(A_{i_1}), C_G(A_{i_2}), \cdots, C_G(A_{i_n})] | 1 \leq i_1, \cdots, i_n \leq s \rangle .$$

Sejam $X_1, \cdots, X_t$ as imagens dos subgrupos da forma $[C_G(A_{i_1}), C_G(A_{i_2}), \cdots, C_G(A_{i_n})]$ em $\gamma_n(G)/(\gamma_n(G))'$. Logo, L é gerado pelos conjuntos $X_1, \cdots, X_t$.

Como a ordem de A é p^{n+1}, para quaisquer $i_1, \cdots, i_n, j_1, \cdots, j_n \leq s$ existem $a, b \in A^{\#}$ tais que os centralizadores $C_G(A_{i_1}), \cdots, C_G(A_{i_n})$ estão todos contidos em $C_G(a)$ e $C_G(A_{j_1}), \cdots, C_G(A_{j_n})$ estão todos contidos em $C_G(b)$. Por hipótese, temos que

$$[[C_G(A_{i_1}), \cdots, C_G(A_{i_n})], \underbrace{[C_G(A_{j_1}), \cdots, C_G(A_{j_n})], \cdots, [C_G(A_{j_1}), \cdots, C_G(A_{j_n})]}_{m}] = 1,$$

logo, $[C_{\gamma_n(G)}(A_k), \underbrace{[C_G(A_{j_1}), \cdots, C_G(A_{j_n})], \cdots, [C_G(A_{j_1}), \cdots, C_G(A_{j_n})]}_{m}] = 1.$

Agora, se X_l é a imagem de $[C_G(A_{j_1}), \cdots, C_G(A_{j_n})]$ em $\gamma_n(G)/(\gamma_n(G))'$, segue que $[C_L(A_k), \underbrace{X_l, \cdots, X_l}_{m}] = 0$. Portanto $[L, \underbrace{X_l, \cdots, X_l}_{m}] = 0$ pois $L = \sum_k C_L(A_k)$.

Faça $Z = Z(\gamma_n(L))$. Logo, temos que $[Z, X, Y] = [Z, Y, X]$ para quaisquer subconjuntos $X, Y \subseteq \gamma_{n-1}(L)$.

Ponha $r = (m-1)t + 1$. Como L é gerado pelos conjuntos $X_1, \cdots, X_t$, segue que $\gamma_{n-1}(L)$ é gerado por $[X_{i_1}, \cdots, X_{i_{n-1}}]$ para $1 \leq i_1, \cdots, i_{n-1} \leq t$. Levando em conta estes fatos, podemos escrever

$$[Z, _r\, \gamma_{n-1}(L)] = \sum [Z, _{u_1}\, [X^1_{i_1}, \cdots, X^1_{i_{(n-1)}}], \cdots, _{u_t}\, [X^t_{i_1}, \cdots, X^t_{i_{(n-1)}}]],$$

onde $u_1 + \cdots + u_t = r$.

O número r é suficientemente grande para que $u_j \geq m$ para algum j. Afirmamos que

$$[Z, _{u_1}\, [X^1_{i_1}, \cdots, X^1_{i_{(n-1)}}], \cdots, _{u_t}\, [X^t_{i_1}, \cdots, X^t_{i_{(n-1)}}]] = 0.$$

De fato, $[X^k_{i_1}, \cdots, X^k_{i_{(n-1)}}] \subset X_j$ para algum $j \in \{1, 2, \cdots, t\}$ e, como visto anteriormente, $[L, \underbrace{X_j, \cdots, X_j}_{m}] = 0$ o que conclui nossa afirmação. Então, temos que $[Z, \underbrace{\gamma_{n-1}(L), \cdots, \gamma_{n-1}(L)}_{r}] = 0$ e $Z \leq Z_r(\gamma_{n-1}(L))$, onde Z_r é o r-ésimo termo da série central superior de $\gamma_{n-1}(L)$.

Aplicando este argumento repetidamente para $\gamma_{n-1}(L)/Z$, $\gamma_{n-1}(L)/Z_2(\gamma_n(L)), \cdots$ e assim por diante, concluímos que $\gamma_n(L) \leq Z_{er}(\gamma_{n-1}(L))$.

Portanto, $\gamma_{n-1}(L)$ é nilpotente de classe no máximo $er + 1$.

Por indução, concluímos que $\gamma_{n-2}(L), \gamma_{n-3}(L), \cdots, \gamma_1(L) = L$, são nilpotentes de classe $\{p, n, m\}$-limitada. ■

Capítulo 4

Grupos que Satisfazem uma lei positiva

Vimos, tanto na introdução deste trabalho quanto no capítulo anterior, que impondo certas restrições sobre os centralizadores de automorfismos coprimos de um dado grupo G obtemos propriedades específicas satisfeitas em todo o G. E uma pergunta natural que surge é em quais situações tal fenômeno ocorre. Neste capítulo estudamos outro caso particular deste fenômeno. Como forma de refrescar nossas idéias relembramos rapidamente o que significa um grupo satisfazer uma lei positiva.

Seja F o grupo livre sobre $X = \{x_1, x_2, \cdots\}$. Uma palavra positiva em X é qualquer elemento não trivial de F não envolvendo os inversos dos x_i. Uma lei positiva de um grupo G é uma identidade não trivial da forma $u \equiv v$, onde u, v são palavras positivas em F, válida para toda substituição $X \to G$. O máximo dos comprimentos de u e v é chamado de grau da lei $u \equiv v$. Sejam p um número primo e e um inteiro positivo, seja A um p-grupo abeliano elementar agindo sobre um p'-grupo finito G, Shumyatsky [24] mostrou que se a ordem de A é p^3 e assumindo que $C_G(a)$ satisfaz uma lei positiva de grau n, para todo $a \in A^{\#}$, então G satisfaz uma lei positiva de grau limitado por uma função dependendo somente de p e n. O autor utilizou o resultado de Burns, Macedonska e Medvedev [2], onde eles mostraram que existe funções $c(n)$ e $e(n)$ dependendo somente

de n, tal que qualquer grupo finito satisfazendo uma lei positiva de grau n é uma extensão de um grupo nilpotente de classse no máximo $c(n)$ por um grupo de expoente dividindo $e(n)$, além é claro da teoria de álgebras de Lie apresentada no segundo capítulo deste trabalho. Nosso principal objetivo aqui é mostrar o seguinte teorema

Teorema 3. *Seja p um primo. Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G. Assuma que $\langle C_G(a), C_G(b)\rangle$ satisfaz uma lei positiva de grau n para todos $a, b \in A^{\#}$. Então, G satisfaz uma lei positiva de grau limitado por uma função dependendo somente de n e p.*

4.1 Redução ao Caso de p-Grupos

Sejam p um primo e e um inteiro positivo. Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um $p^{'}$-grupo finito G. Suponha que para quaisquer elementos $a, b \in A^{\#}$ o subgrupo $\langle C_G(a), C_G(b)\rangle$ possui um subgrupo normal nilpotente, digamos N_{ab}, de classe no máximo c cujo quociente $\langle C_G(a), C_G(b)\rangle / N_{ab}$ tem expoente e. Dado $a \in A^{\#}$. Faça $N_a = (\cap_{b\in A^{\#}} N_{ab}) \cap C_G(a)$. Note que N_a é nilpotente de classe no máximo c e que o quociente $C_G(a)/N_a$ tem expoente dividindo e. De fato, temos que o quociente $\langle C_G(a), C_G(b)\rangle / N_{ab}$ tem expoente e, para todo $b \in A^{\#}$, e $C_G(a)/N_a$ pode ser imerso no produto cartesiano finito de quocientes da forma $\langle C_G(a), C_G(b_i)\rangle / N_{ab_i}$, com $b_i \in A^{\#}$. Como cada um destes quocientes tem expoente e, segue que $C_G(a)/N_a$ tem expoente e, para todo $b \in A^{\#}$. Além disso, temos que $N_a \subseteq F(\langle N_a, C_G(b)\rangle)$, para todo $b \in A^{\#}$.

Lema 4.1.1. *Sob as hipóteses acima temos que $N_a \leq F(G)$.*

Demonstração: Seja x um elemento arbitrário de N_a. Então, para qualquer $b \in A^{\#}$ temos $x \in F(\langle N_a, C_G(b)\rangle)$. Precisamos mostrar que $x \in F(G)$. Seja G um contraexemplo de menor ordem. Suponha primeiramente que G é solúvel. Então, $x \in F_2(G)$. Faça $F = F(G)$, como $F(G/\Phi(G)) = F/\Phi(G)$, Lema 1.1.14, podemos supor que F é abeliano.

Pelo Lema 1.3.6, $F = \prod_{a \in A^{\#}} C_F(a)$. Como $x \in F(\langle N_a, C_G(b)\rangle)$ para qualquer $b \in A^{\#}$, existe um inteiro positivo n tal que $[C_F(b), \underbrace{x, \cdots, x}_{n}] = 1$ para qualquer $b \in A^{\#}$. Segue que $[F, \underbrace{x, \cdots, x}_{n}] = 1$, e consequêntemente $\langle x, F(G)\rangle$ é um subgrupo subnormal nilpotente de G. Portanto, $x \in F$, uma contradição. Como x é arbitrário em N_a, o resultado segue.

Agora consideramos o caso onde G não é solúvel. Seja M um subgrupo normal minimal A-invariante de G. Por indução $MN_a/M \leq F(G/M)$. Se $F(G) \neq 1$, podemos assumir que $M \leq F(G)$. Então, MN_a é um grupo solúvel satisfazendo as hipóteses do lema, logo $N_a \leq F(MN_a)$, o que é uma contradição. Assim podemos assumir que $F(G) = 1$ e que M é um produto direto de grupos simples.

Tomando qualquer elemento $x \in N_a$ considere o subgrupo $M\left\langle x^A\right\rangle$. Note que este subgrupo satisfaz a hipótese do Lema e, pela hipótese de indução, $G = M\left\langle x^A\right\rangle$. Como $x \in F(\langle N_a, C_G(b)\rangle)$, para todo $b \in A^{\#}$, então x centraliza $E(C_G(b))$, para todo $b \in A^{\#}$ (ver Lema 1.2.2 do primeiro capítulo). Agora, pelo Lema 1.3.10, $M = \left\langle E(C_M(b)) | b \in A^{\#}\right\rangle$. Portanto, $x \in Z(G)$, uma contradição pois $Z(G) \subseteq F(G) = 1$. ■

Um caso semelhante ao do Teorema 3 e já citado na introdução deste trabalho foi obtido por Khukhro e Shumyatsky [13], onde os autores trabalharam com o expoente de um grupo e mostraram o seguinte resultado.

Teorema 4.1.2. *Sejam p um primo e e um inteiro positivo. Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G. Assuma que o expoente de $C_G(a)$ divide e para todo $a \in A^{\#}$. Então, o expoente de G é $\{e, p\}$-limitado.*

Combinando o Lema 4.1.1 e o Teorema 4.1.2 deduzimos o seguinte Lema.

Lema 4.1.3. *Sejam p um primo e e um inteiro positivo. Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G. Assuma que o expoente do quociente $\langle C_G(a), C_G(b)\rangle / F(\langle C_G(a), C_G(b)\rangle)$ divide e para todos $a, b \in A^{\#}$. Então, o expoente do quociente $G/F(G)$ é $\{e, p\}$-limitado.*

Demonstração: Seja N_a como no lema anterior. Logo, $N_a \leq F(G)$ e $C_G(a)/N_a$ tem expoente $\{e,p\}$-limitado. Portanto, a imagem de $C_G(a)$ no quociente $G/F(G)$ tem expoente $\{e,p\}$-limitado, para todo $a \in A^{\#}$. Logo, pelo Teorema 4.1.2, $G/F(G)$ tem expoente $\{e,p\}$-limitado. ■

Lema 4.1.4. *Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G solúvel de comprimento derivado no máximo d. Assuma que $\langle C_G(a), C_G(b)\rangle$ tem um subgrupo nilpotente de classe no máximo c e índice k, para todos $a, b \in A^{\#}$. Então, G tem um subgrupo nilpotente característico cuja classe e o índice são ambos $\{c,k,d,p\}$-limitados.*

Demonstração: Sem perda de generalidade podemos assumir que, para todos $a, b \in A^{\#}$, o subgrupo $\langle C_G(a), C_G(b)\rangle$ tem um subgrupo nilpotente característico de classe no máximo c e índice no máximo k. Sejam $A_1, A_2, \cdots, A_{p+1}$ os subgrupos maximais de A e faça $G_i = C_G(A_i)$ para $i = 1, \cdots, p+1$. Escolha $a \in A^{\#}$. Para qualquer $b \in A^{\#}$ denote por N_{ab} algum subgrupo nilpotente característico de classe no máximo c e índice no máximo k de $\langle C_G(a), C_G(b)\rangle$. Faça $N_a = (\cap_{b\in A^{\#}} N_{ab}) \cap C_G(a)$. Podemos assumir sem perda de generalidade que $a \in A_1$ e então o índice de N_a em G_1 é $\{p,k\}$-limitado. Temos uma importante propriedade dos subgrupos N_a: se M é um subgrupo normal abeliano A-invariante de G, então MN_a é nilpotente de classe no máximo $c+1$. De fato, pelo Lema 1.3.6, $M = \prod M_j$, onde $M_j = G_j \cap M$. Portanto, para mostrar que MN_a é nilpotente de classe no máximo $c+1$ é suficiente mostrar que $\langle M_j, N_a\rangle$ é nilpotente de classe no máximo $c+1$, para todo $j = 1, \cdots, p+1$. Mas, N_a está contido em um subgrupo nilpotente característico de classe no máximo c de $\langle C_G(a), C_G(b)\rangle$ enquanto M_j está contido em um subgrupo normal abeliano de $\langle C_G(a), C_G(b)\rangle$. Segue, portanto, que $\langle M_j, N_a\rangle$ é nilpotente de classe no máximo $c+1$, como queríamos.

Agora, suponha que H é um subgrupo normal nilpotente de classe u A-invariante de G.

Então, HN_a é nilpotente de classe no máximo $c\frac{u(u+1)}{2}+u$. De fato, sabemos do parágrafo anterior que HN_a/H' é nilpotente de classe no máximo $\leq c+1$. Portanto, pelo Teorema de Hall [8], HN_a é nilpotente de classe no máximo $c\frac{u(u+1)}{2}+u$. Estamos agora prontos para demonstrar o lema usando indução sobre d. Suponha por indução que $G^{'}$ tem um subgrupo nilpotente característico tal que a classe e o índice são $\{c,k,d,p\}$-limitados. Agora, faça $L_0 = G^{'}$ e $L_j = L_{j-1}G_j$ para $j = 1,\cdots,p+1$. Pelo Lema 1.3.6, $L_{p+1} = G$. Usamos indução sobre j para mostrar que L_j tem um subgrupo nilpotente característico com a propriedade requerida para todo j. Assuma que o lema vale para L_{j-1} e seja Q um subgrupo nilpotente característico de L_{j-1} cuja classe u e o índice t são ambos limitados em termos de p,c,d e k somente. Considere o subgrupo QN_a de L_j. Pode-se facilmente checar que o índice de QN_a em L_j é no máximo kt e vimos acima que QN_a é nilpotente de classe $\{c,u\}$-limitada. Assim, o fecho normal de QN_a em L_j é um subgrupo característico com a propriedade requerida e a demonstração está completa. ■

O próximo Teorema foi demonstrado por Shumyatsky [26] e consiste de um caso particular ao que propomos mostrar neste capítulo, onde o autor utilizou técnicas parecidas com as que utilizamos no terceiro capítulo deste trabalho.

Teorema 4.1.5. *Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um $p^{'}$-grupo finito G. Assuma que $\langle C_G(a), C_G(b)\rangle$ é nilpotente de classe no máximo c, para todos $a,b \in A^{\#}$. Então, G é nilpotente de classe limitada por uma função dependendo somente de p e c.*

Lema 4.1.6. *Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um $p^{'}$-grupo finito G. Assuma que $\langle C_G(a), C_G(b)\rangle$ tem um subgrupo nilpotente de classe no máximo c e índice k, para todos $a,b \in A^{\#}$. Então, G tem um subgrupo normal nilpotente cuja classe e o índice são $\{c,k,p\}$-limitados.*

Demonstração: Sejam $A_1, A_2, \cdots, A_{p+1}$ os subgrupos maximais de A. Logo, combi-

nando o Lema 4.1.3 com o Lema 1.3.4 (v), temos que no quociente $G/F(G)$ o subgrupo $\langle C_G(A_i), C_G(A_j)\rangle$ tem ordem $\{k,p\}$-limitada, para todos $1 \leq i,j \leq p+1$. Logo, pelo Lema 4.1.3, $G/F(G)$ tem ordem $\{k,p\}$-limitada. Assim é suficiente mostrar o lema para o caso onde G é nilpotente. Pegue $a \in A^{\#}$. Para qualquer subgrupo H, A-invariante de G e $b \in A^{\#}$ defina o parâmetro $j_b(H)$ como o menor inteiro positivo j tal que $\langle C_H(a), C_H(b)\rangle$ tem um subgrupo normal nilpotente de classe no máximo c e índice no máximo j. Faça $\lambda(H) = \sum_{b\in A^{\#}} j_b(H)$. É claro que $\lambda(G)$ é $\{k,p\}$-limitado. Usamos indução sobre $\lambda(G)$. O caso $\lambda(G) = p^2 - 1$ (o menor valor possível para $\lambda(G)$ - ocorre se, e somente se, $\langle C_G(a), C_G(b)\rangle$ é nilpotente de classe c para qualquer $a, b \in A^{\#}$) segue imediatamente do Teorema 4.1.5. Assuma, por indução, que se H é um subgrupo A-invariante de G tal que $\lambda(H) \leq \lambda(G)$, então H tem um subgrupo normal nilpotente cuja a classe e o índice são $\{c,k,p\}$-limitados. Seja $f = f(c,p)$ a função que limita a classe do grupo no Teorema 4.1.5. Denote por R o $(f+2)$-termo da série central inferior de G. Suponha que $k(R) = k(G)$. Logo, usando o Lema 1.1.8 é fácil checar que neste caso $\left\langle C_{G/R}(a), C_{G/R}(b)\right\rangle$ é nilpotente de classe no máximo c, para todos $a, b \in A^{\#}$, e novamente pelo Teorema 4.1.5, G/R é nilpotente de classe f. Como $R = \gamma_{f+2}(G)$, concluímos que $R = 1$ e o resultado segue.

Assuma agora que $\lambda(R) \leq \lambda(G)$. Então, pela hipótese de indução, R tem um subgrupo normal nilpotente cuja classe e o índice são $\{c,k,p\}$-limitados e, consequentemente, o comprimento derivado de G é $\{c,k,p\}$-limitados. E o teorema segue do Lema 4.1.4. ■

No próximo resultado consideramos um q-grupo finitamente gerado G. Supondo que o subgrupo $\langle C_G(a), C_G(b)\rangle$ de G é uma extensão de um grupo nilpotente de classe no máximo c por um grupo de expoente e, para todos $a, b \in A^{\#}$, onde A, como nos resultados anteriores, é um p-grupo abeliano elementar de ordem p^2 agindo sobre G, concluímos que o posto de G é limitado por uma função que depende de c, e, m e p. Tal resultado é a chave para provarmos o Teorema 3 e em sua demonstração utilizamos a teoria de álgebra

Lie, mais precisamente a associação da álgebra de Lie correspondente a série de Jennings-Lazard-Zassenhaus ao grupo G. Os detalhes dessa associação de uma álgebra de Lie a um grupo pode ser visto no segundo capítulo deste trabalho.

Proposiçao 4.1.7. *Sejam p e q primos distintos. Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre o q-grupo finito m-gerado G. Assuma que $\langle C_G(a), C_G(b)\rangle$ é uma extenção de um grupo nilpotente de classe no máximo c por um grupo de expoente e, para todos $a, b \in A^{\#}$. Então, o posto de G é $\{c, e, m, p\}$-limitado.*

Demonstração: Primeiramente, note que se $q > e$, então o subgrupo $\langle C_G(a), C_G(b)\rangle$ é nilpotente de classe no máximo c, para todos $a, b \in A^{\#}$, e pelo Teorema 4.1.5, G é nilpotente de classe $\{c, p\}$-limitada. Assim, podemos assumir que $q \leq e$ e e é uma potência de q. Relembrando a quarta seção do segundo capítulo deste trabalho, onde associamos um anel de Lie a um grupo finito pela série de Jennings-Lazard-Zassenhaus correspondente. Ponha $D_j = D_j(G)$, $L = L_q(G)$ e $L_j = L \cap D_j/D_{j+1}$. Logo $L = \oplus L_j$. Podemos ver A como um grupo agindo sobre L. Sejam $A_1, A_2, \cdots, A_{p+1}$ os subgrupos maximais distintos de A e para quisquer i, j faça $L_{ij} = C_{L_j}(A_i)$. Como $G = \prod_{a\in A^{\#}} C_G(a)$, para qualquer j, temos

$$L_j = \sum_{1\leq i\leq p+1} L_{ij}.$$

Pelo Lema 1.3.1, para qualquer $l \in L_{ij}$ existe $x \in D_j \cap C_G(A_i)$ tal que $l = xD_{j+1}$. Sabemos que para qualquer $k = 1, \cdots, p+1$ o subgrupo $\langle C_G(A_i), C_G(A_k)\rangle$ é uma extensão de um grupo nilpotente de classe no máximo c por um grupo de expoente dividindo e. Portanto,

$$[C_G(A_i), \underbrace{x^e, \ldots, x^e}_{c}] = 1.$$

Como $L = \sum_k C_L(A_k)$, segue que a transformação linear de L induzida por comutação com o elemento correspondente a x^e é nilpotente de índice no máximo c. Combinando

esse fato com o Lema de Lazard 2.4.11, temos que

$$\text{qualquer elemento em } L_{ij} \text{ é ad-nilpotente de índice no máximo } ce. \tag{4.1}$$

O problema é que não podemos afirmar que o produto de Lie desses elementos está novamente em algum L_{ij}. Para superar esse problema extendemos o corpo base de L por uma p-ésima raiz primitiva da unidade ω, formando a álgebra de Lie $\overline{L} = L \otimes \mathbb{F}_q[\omega]$. É natural identificar L com a $\mathbb{F}_q$-subalgebra $L \otimes 1$ de $\overline{L}$. Observamos que se um elemento $x \in L$ é ad-nilpotente de índice m, temos que, o "mesmo"elemento $x \otimes 1$ é ad-nilpotente em $\overline{L}$ de mesmo índice. A idéia é provar que $\overline{L}$ é nilpotente de classe $\{p, n\}$-limitada e consequentemente L também o será.

Ponha $\overline{L_j} = L_j \otimes \mathbb{F}_q[\omega]$. Então, $\overline{L} = \langle \overline{L_1} \rangle$, pois $L = \langle L_1 \rangle$, e $\overline{L}$ é a soma direta dos componentes homogêneos $\overline{L_j}$. Como o $\mathbb{F}_q$-espaço L_1 é m-dimencional o $\mathbb{F}_q[\omega]$-espaço $\overline{L_1}$ também o é. O grupo A age naturalmente sobre $\overline{L}$ e temos que $\overline{L_{ij}} = C_{\overline{L_j}}(A_i)$, onde $\overline{L_{ij}} = L_{ij} \otimes \mathbb{F}_q[\omega]$. O que devemos mostrar agora é que

$$\text{qualquer elemento } y \in \overline{L_{ij}} \text{ é ad-nilpotente de índice } \{p, n\} - \text{limitado.} \tag{4.2}$$

De fato, como $y \in \overline{L_{ij}} = L_{ij} \otimes \mathbb{F}_q[\omega]$, podemos escrever y da forma

$$y = x_0 + \omega x_1 + \omega^2 x_2 + \cdots + \omega^{p-2} x_{p-2}$$

para alguns $x_0, x_1, \cdots, x_{p-2} \in L_{ij}$, os quais são todos ad-nilpotentes de índice no máximo ce por (4.1). Considere $H = \langle x_0, \omega x_1, \omega^2 x_2, \cdots, \omega^{p-2} x_{p-2} \rangle$. Note que $H \subseteq C_{\overline{L}}(A_i)$, pois $x_0, x_1, \cdots, x_{p-2} \in C_{\overline{L}}(A_i)$. Um comutador de peso k nos $\omega^s x_s$ tem a forma $\omega^t x$ para algum $x \in L_{is}$, onde $s = kj$. Como, por (4.1), x é ad-nilpotente de índice no máximo ce, então $\omega^t x$ também o é.

Combinando a Proposição 2.4.1 com o fato de $L_q(G, C_G(A_i)) = C_{L_q(G)}(A_i)$, concluímos que $C_L(A_i)$ satisfaz uma identidade polinomial multilinear de grau $\{c, e\}$-limitado. Como

essa identidade é multilinear, também é satisfeita em $C_{\overline{L}}(A_i) = C_L(A_i) \otimes \mathbb{F}_q[\omega]$. Como consequência do fato de $H \subseteq C_{\overline{L}}(A_i)$ essa identidade é satisfeita em H. Agora, pelo Teorema 2.2.1, H é nilpotente de classe $\{p, c, e\}$-limitada. E o Lema 2.3.3 diz que para algum número v, $\{p, c, e\}$-limitado, $[L, \underbrace{H, \cdots, H}_{v}] = 0$.

Assim, obtemos (4.2).

Como A é abeliano e agora o corpo base contém todas as raizes para A, todo $\overline{L}_j$ se decompoêm em soma direta de autoespaços comuns para A. Em particular, o espaço $\overline{L}_1$ é gerado por no máximo m autovetores comuns para A. Portanto, $\overline{L}$ é gerada por m autovetores comuns para A de $\overline{L}_1$. Todo autoespaço comum está contido no centralizador $C_{\overline{L}}(A_i)$, para algum $1 \leq i \leq p+1$, pois A é não cíclico. Note que qualquer comutador nesses autovetores comuns é novamente um autovetor comum. Portanto, se $l_1, \cdots, l_m \in \overline{L}_1$ são autovetores comuns para A, gerando $\overline{L}$, então qualquer comutador nesses geradores pertence a algum $\overline{L}_{ij}$, e portanto, é ad-nilpotente de índice $\{p, c, e\}$-limitado.

Sabemos que uma identidade polinomial $f \equiv 0$ é satisfeita em $C_{\overline{L}}(A_i) = C_L(A_i) \otimes \mathbb{F}_q[\omega]$. Pelo Corolário 2.2.3, $\overline{L}$ satisfaz alguma identidade $\phi(f) \equiv 0$ que depende somente de c, e e p. Agora o Teorema 2.2.1 diz que $\overline{L}$ (por conseguinte L) é nilpotente de classe $\{p, c, e\}$-limitada. Portanto, pelo Lema 2.4.15, o teorema segue. ■

Finalmente passamos à demonstração do Teorema 3.

Teorema 3. *Seja p um primo. Seja A um p-grupo abeliano elementar de ordem p^2 agindo sobre um p'-grupo finito G. Assuma que $\langle C_G(a), C_G(b)\rangle$ satisfaz uma lei positiva de grau n, para todos $a, b \in A^{\#}$. Então, G satisfaz uma lei positiva de grau $\{n, p\}$-limitado.*

Demonstração: De acordo com o Teorema de Burns, Macedonska e Madvedev, existem números c e e que dependem somente de n tal que, para quaisquer $a, b \in A^{\#}$ o subgrupo $\langle C_G(a), C_G(b)\rangle$ é uma extensão de um grupo nilpotente de classe no máximo c por um grupo cujo expoente divide e. Agora, o Lema 4.1.3 nos diz que o expoente do quociente

$G/F(G)$ é $\{e,p\}$-limitado. Vamos denotar este expoente por ϵ. Seja $\{q_1,\cdots,q_t\}$ o conjunto dos primos que dividem a ordem de $F(G)$. Vamos assumir que $q_1,\cdots,q_r$ dividem e mas que $q_{r+1},\cdots,q_t$ não dividem e. Seja S_i o q_i-subgrupo de Sylow de $F(G)$ e escreva $S = S_{r+1}\times\cdots\times S_t$. Logo, para quaisquer $a,b\in A^{\#}$, o subgrupo $\langle C_S(a), C_S(b)\rangle$ é nilpotente de classe no máximo c. Assim, pelo Teorema 4.1.5, S é nilpotente de classe $\{c,p\}$-limitada.

Sejam g,h elementos arbitrários de S_i para algum $i\leq r$, ou de S. Seja H um subgrupo normal minimal A-invariante de G contendo g e h. Como $H=\prod_{a\in A^{\#}} C_H(a)$, temos que H é gerado por no máximo $2p^2$ elementos. Pela Proposição 4.1.7, e o fato de S ser nilpotente de classe $\{c,p\}$-limitada, segue que o posto de H é $\{n,p\}$-limitado. Agora, para quaisquer $a,b\in A^{\#}$, o subgrupo $\langle C_H(a), C_H(b)\rangle$ é uma extensão de um grupo nilpotente de classe no máximo c por um grupo de expoente dividindo e e, ao mesmo tempo, $\langle C_H(a), C_H(b)\rangle$ tem posto $\{n,p\}$-limitado, para quaisquer $a,b\in A^{\#}$. Segue que $\langle C_H(a), C_H(b)\rangle$ tem um subgrupo de classe no máximo c e índice $\{n,p\}$-limitado [veja Lema 1.4.19]. Aplicando o Lema 4.1.6, concluímos que H tem um subgrupo nilpotente cuja classe e o índice são ambos $\{n,p\}$-limitados. Denotemos por k o maior destes limitantes.

Sejam x,y elementos arbitrários de G. Mostramos acima que qualquer subgrupo de Sylow de $\left\langle x^{k\epsilon}, y^{k\epsilon}\right\rangle$ tem classe $\{n,p\}$-limitada, onde ϵ é o expoente $\{n,p\}$-limitado do quociente $G/F(G)$. Então, $\left\langle x^{k\epsilon}, y^{k\epsilon}\right\rangle$ tem classe $\{n,p\}$-limitada. Seja v o máximo das classes dos subgrupos $\left\langle x^{k\epsilon}, y^{k\epsilon}\right\rangle$, onde x e y percorrem todo G. Portanto, G satisfaz a lei de Malcev sobre duas variáveis $M_v(x^{k\epsilon}, y^{k\epsilon})$ cujo grau é $\{n,p\}$-limitado. E a demonstração está completa. ■

Referências Bibliográficas

[1] BAHTURIN, Yu. A., ZAICEV, M. V., *Identities of Graded Algebras*. J. Algebra, (2005), 1 – 12.

[2] BURNS, R. G., MACEDONSKA, O., MEDVEDEV, Yu., *Groups Satisfying Semigroup Laws, and Nilpotent-by-Burnside Varieties*. J. Algebra, **195** (1997), 510 – 525.

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

[4] GAGEN, T. M., *Topics in Finite Groups*. Cambridge University Press, London Math. Soc. Lecture Note Series, **16** (1976).

[5] GLAUBERMAN, G., *On Solvable Signalizer Functors in Finite Groups*. Proc. London Math. Soc. (3) **33** (1976), no. 1, 1 – 27.

[6] GORENSTEIN, D., *Finite Groups*. New York, Evanston, London : Harper and Row, (1968).

[7] GURALNICK, R., SHUMYATSKY P., *Derived Subgroups of Fixed Points*. Israel J. Math. **126**(2001), 345 – 362.

[8] HALL, P., *Some Sufficient Conditions for a Group to be Nilpotent*. Illinois J. Math., **2** (1958), 787 – 801.

[9] HIGMAN, G., *Groups and Lie Rings Having Automorphisms Without Non-trivial Fixed Points*. J. London Math. Soc., **32** (1957), 321 – 334.

[10] KREKNIN, V. A., *Solvability of Lie Algebras With a Regular Automorphisms of Finite Period*. Soviet Math. Dokl. **4** (1963), 683 – 685.

[11] KHUKHRO, E. I., *p-Automorphisms of Finite p-Groups*. London Mathematical Society : Cambridge University Press, (1997).

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

[13] KHUKHRO, E. I., SHUMYATSKY, P., *Bounding the Exponent of a Finite Group With Automorphisms*. J. Algebra, **212** (1999), 363 − 374.

[14] KHUKHRO, E. I., SHUMYATSKY, P., *On Fixed Points of Automorphisms of Lie Rings end Locally Finite Groups*. Algebra and Logic **34** (1995), 395 − 405.

[15] KOVACS, L. G., WALL, G. E., *Involutory Automorphisms of Groups of Odd Order and their Fixed Point Groups*. Nagoya Math. J., **27** (1966), 113 − 120.

[16] LAZARD, M., *Sur les Groupes Nilpotents et les Anneaux de Lie*. Ann. Sci. École Norm. Supr., **71** (1954), 101 − 190.

[17] LINCHENCO, V., *Identities of Lie Algebras With Actions of Hopf Algebras*. Comm. Algebra, **25** (1997), 3179 − 3187.

[18] MALCEV, A. I., *Nilpotent Semigroups*. Uchen. Zap. Ivanovsk. Ped. Inst., **4** (1953), 107 − 111.

[19] OLSHANSKI, A. Yu., STOROZHEV, A., *A Group Variety Defined by a Semigroup Law*. J. Austral Math. Soc. Ser. . A, **60** (1996), 255 − 259.

[20] RILEY, D. M., *Analytic Pro-p Groups and their Graded Groups Rings*. J. Pure Appl. Algebra, **90** (1993), 69 − 76.

[21] ROBINSOM, D. J. S., *A course in the Theory of Groups*, Springer - Verlag Berlin Heidelberg, New York, (1985).

[22] ROTMAN, J. J., *An Introduction to Theory of Groups*, Allyn e Bacon Inc., (1965).

[23] SHUMYATSKY, P., *Positive Laws in Derived Subgroups of Fixed Points*, The Quarterly Journal of Math., to appear.

[24] SHUMYATSKY, P., *Positive Laws in Fixed Points*. Trans. Amer. Math. Soc. **356** (2004), no. 5, 2081 − 2091.

[25] SHUMYATSKY, P., *Finite Groups and the Fixed Points of Coprime Automorphisms*. Proc. Am. Math. Soc., **129**(**12**) (2001), 3479 − 3484.

[26] SHUMYATSKY, P., *On Locally Finite Groups and the Centralizers of Automorphisms*. Bollettino U.M.I., **4** − **B**(**8**) (2001), 731 − 736.

[27] SHUMYATSKY, P., *Exponent of a Finite Group With an Involutory Automorphism*. J. Group Theory **2**(1999), no. 4, 367 − 372.

[28] SHUMYATSKY, P., *Involutory Automorphisms of Finite Groups and their Centralizers*. Arch. Math. (Basel), **71** (1998), 425 − 432.

[29] SHUMYATSKY, P., *On Periodic Soluble Groups and the Fixed Point Groups of Operators*. Comm. Algebra **20**(**10**) (1992).

[30] THOMPSON, J. G., *Finite Groups With Fixed-point-free Automorphisms of Prime order*. Proc. Nat. Acad. Sci. U.S.A., **45** (1959), 578 − 581.

[31] WILSON, J. S., ZELMANOV, E., *Identities for Lie Algebras of Pro-p Grupos*. J. Pure Appl. Algebra, **81** (1992), 103 − 109.

[32] ZELMANOV, E., *Nil Rings and Periodic Groups*. The Korean Math. Soc. Lecture Notes in Math.,Seoul, (1992).

[33] ZORN, M., *Nilpotency of Finite Groups*. Bull. Amer. Math. Soc., **42** (1936), 485 − 486.

[34] WARD, J. N., *On Finite Groups Admitting Automorphisms With Nilpotent Fixed-Point Group*. Bull. Austral. Math. Soc., **5** (1971), 281 − 282.

[35] WARD, J. N., *On Finite Soluble Groups and the Fixed-Point Group of Automorphisms*. Bull. Austral. Math. Soc., **5** (1971), 375 − 378.