Universidade Federal de Goiás
Instituto de Matemática e Estatística

Emerson Ferreira de Melo

Sobre Anéis de Lie Admitindo Automorfismos de Ordens Finitas e Álgebras de Lie Quase Nilpotentes

Goiânia
2011

sibi
sistema de bibliotecas ufg

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: [x] **Dissertação** [ ] **Tese**

2. Identificação da Tese ou Dissertação

Autor (a): Emerson Ferreira de Melo
E-mail: emersonferreirademelo@gmail.com
Seu e-mail pode ser disponibilizado na página? [x]Sim [ ] Não

Vínculo empregatício do autor
Agência de fomento: Conselho Nacional de Desenvolvimento Científico e Tecnológico Sigla: CNPq
País: Brasil UF: GO CNPJ:
Título: Sobre Anéis de Lie Admitindo Automorfismos de Ordem Finita e Álgebras de Lie Quase Nilpotentes

Palavras-chave: Anéis de Lie, Álgebras de Lie, Automorfismos, Quase Nilpotência
Título em outra língua: On Lie Rings Admitting Automorphisms of Finite Order and Lie Algebras Almost Nilpotent

Palavras-chave em outra língua: Lie Rings, Lie Algebras, Automorphisms, Almost Nilpotency

Área de concentração: Álgebra
Data defesa: (dd/mm/aaaa) 28/02/2011
Programa de Pós-Graduação: Mestrado em Matemática
Orientador (a): Jhone Caldeira Silva
E-mail:
Co-orientador (a):*
E-mail:

3. Informações de acesso ao documento:
Liberação para disponibilização?[1] [x] total [ ] parcial

Em caso de disponibilização parcial, assinale as permissões:
[ ] Capítulos. Especifique:
[ ] Outras restrições:
Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.
O Sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

Emerson Ferreira de Melo Data: / /
Assinatura do (a) autor (a)

[1] Em caso de restrição, esta poderá ser mantida por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Todo resumo e metadados ficarão sempre disponibilizados.

EMERSON FERREIRA DE MELO

Sobre Anéis de Lie Admitindo Automorfismos de Ordens Finitas e Álgebras de Lie Quase Nilpotentes

Dissertação apresentada ao Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de concentração: Álgebra.

Orientador: Prof. Dr. Jhone Caldeira Silva

Goiânia
2011

Dados Internacionais de Catalogação na Publicação na (CIP)
GPT/BC/UFG

Melo, Emerson Ferreira de.
M528s Sobre Anéis de Lie admitindo automorfismos de ordens finitas e álgebras de Lie Quase Nilpotente [manuscrito] / Emerson Ferreira de Melo. - 2011.
xv, 88 f.

Orientador: Prof. Dr. Jhone Caldeira Silva.
Dissertação (Mestrado) – Universidade Federal de Goiás, Instituto de Matemática e Estatística, 2011.
Bibliografia.

1. Anéis de Lie 2. Álgebras de Lie 3. Automorfismos 4. Quase Nilpotente I. Título.

CDU:512.55

EMERSON FERREIRA DE MELO

Sobre Anéis de Lie Admitindo Automorfismos de Ordens Finitas e Álgebras de Lie Quase Nilpotentes

Dissertação defendida no Programa de Pós-Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás como requisito parcial para obtenção do título de Mestre em Matemática, aprovada no dia 28 de fevereiro de 2011, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Jhone Caldeira Silva
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Profa. Dra. Marinês Guerreiro
Departamento de Matemática-UFV

Profa. Dra. Aline de Souza Lima
Instituto de Matemática e Estatística-UFG

Emerson Ferreira de Melo

Graduou-se em Matemática pela UEG - Universidade Estadual de Goiás.

Aos amigos Rogério Santana, Marcos Pavani, Carlos Eduardo, Jair, Airton, Edson, pelo incentivo.

Agradecimentos

Agradeço a Deus, por me permitir desfrutar desta fase única da vida, que é o mestrado.

A minha família, que apesar de não ter ideia do que eu estudo, valorizam meu esforço e dedicação.

Ao meu amigo Rogério Alves, pelo convite para fazer o curso de verão em 2008, o que me despertou o interesse pela matemática.

Aos amigos, Welder, Sílvio, Agenor e João Luís, os quais me ajudaram com as primeiras demonstrações matemáticas.

Aos amigos de Rio Verde, Edson e Airton, pois sei que sempre posso contar com eles.

Aos amigos do mestrado, Alex, Alfredo, Benedito, Bruno, Caíke, Carlos, Danillo, Diogo, Douglas, Edwin, Fernando, Flávio, Kaye, Lívio, Lucimeire, Márcio, Gabriel, Mayer, Sérgio, Silvana, Rosane, Thársis, Ubirajara, Hugo, pela convivência e ajuda nas listas de exercícios.

A minha namorada Lidiane, pela companheirismo.

Ao meu orientador, professor Jhone Caldeira Silva, pela sugestão do tema e ensinamentos.

Finalmente, agradeço à CNPQ pelo suporte financeiro.

Vai ter com a formiga, ó preguiçoso; olha para os seus caminhos, e sê sábio. Pois ela, não tendo chefe, nem guarda, nem dominador, prepara no verão o seu pão; na sega ajunta o seu mantimento.

Provérbios de Salomão,
Pv. 6:6-11.

Resumo

Melo, Emerson Ferreira de. **Sobre Anéis de Lie Admitindo Automorfismos de Ordens Finitas e Álgebras de Lie Quase Nilpotentes**. Goiânia, 2011. 88p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Nesta dissertação apresentamos um estudo sobre anéis e álgebras de Lie admitindo um automorfismo de ordem finita, com ênfase em questões sobre nilpotência. Demonstramos resultados importantes desta teoria, como por exemplo o Teorema de Higman, Kreknin e Kostrikin. Além disso, considere L uma álgebra de Lie de dimensão finita sobre um corpo algebricamente fechado de característica 0. Suponha que L admita uma álgebra de derivações nilpotente D com n pesos em L, e seja m a dimensão da componente nula de Fitting com respeito a D. Então L é quase nilpotente, ou seja, L contém uma subálgebra N de codimensão $\{m,n\}$-limitada e classe de nilpotência n-limitada. Se $m = 0$, então L é nilpotente de classe limitada por uma função de n. Este teorema foi publicado por E. I. Khukhro e P. Shumyatsky num artigo intitulado "Lie Algebras with almost constant-free derivations".

Palavras–chave

Anéis de Lie, Álgebras de Lie, Automorfismos, Quase Nilpotência

Abstract

Melo, Emerson Ferreira de. **On Lie Rings Admitting Automorphisms of Finite Order and Lie Algebras almost Nilpotent**. Goiânia, 2011. 88p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

In this work we present a study on Lie rings and algebras admitting an automorphism of finite order. We emphasize questions on nilpotency. We prove important results of this theory, for example the Higman, Kreknin and Kostrikin's Theorem. Furthermore, let L be a finite dimensional Lie algebra over an algebraically closed field of characteristic 0. Suppose that L admits a nilpotent Lie algebra D with n weights in L, and let m be the dimension of the Fitting null component with respect to D. Then L is almost nilpotent, namely, L contains a nilpotent subalgebra N of $\{m,n\}$-bounded codimension and of n-bounded nilpotency class. If $m = 0$, then L is nilpotent of bounded class by a function of n. This theorem was published by E. I. Khukhro and P. Shumyatsky in the paper entitled " Lie Algebras with Almost Constant-Free Derivations".

Keywords

Lie Rings, Lie Algebras, Automorphisms, Almost Nilpotency

Sumário

Introdução

As álgebras de Lie têm sido aporte teórico fundamental para descobertas científicas relevantes e consiste de uma teoria que muito se fortaleceu no século passado, tendo contribuído com importantes trabalhos de reconhecimento internacional.

Alguns resultados sobre álgebras de Lie podem ser obtidos mediante o estudo de anéis de Lie. Considerando A um anel de Lie, definimos o conjunto dos pontos fixos de um automorfismo φ em A por $C_A(\varphi) = \{a \in A \ : \ a^\varphi = a\}$, que é um subanel de A. O automorfismo φ é dito *regular* quando $C_A(\varphi) = 0$ e *quase regular* quando $C_A(\varphi)$ é finito.

Encontrar hipóteses sobre as quais uma álgebra de Lie (ou anel de Lie) é nilpotente é um dos problemas estudados na atualidade. Nesse sentido, temos o Teorema de Higman-Kreknin-Kostrikin, o qual afirma que se um anel de Lie A (ou uma álgebra de Lie) admite um automorfismo regular φ de ordem prima p, então ele é nilpotente. Uma generalização deste resultado devido a Khukhro [9] afirma que se o subanel (ou a subálgebra) dos pontos fixos é finito, digamos $|C_A(\varphi)| = q$ (ou tem dimensão finita no caso de álgebra de Lie), então o anel é *quase nilpotente* no seguinte sentido: existe um subanel nilpotente, cuja classe de nilpotência é limitada por uma função dependendo somente de p e o índice (ou codimensão) é limitado por uma função dependendo somente de p e q.

Resultados semelhantes podem ser obtidos sem admitir a existência de um automorfismo regular. Nesse caso, uma alternativa, conforme veremos, é obter uma decomposição de uma álgebra de Lie em seus espaços de peso relativos a uma álgebra de derivações D.

Em [18] J. C. Silva apresenta um estudo sobre álgebras de Lie de derivações que não admitem constantes não triviais. Especificamente, o principal resultado em [18] afirma que se uma álgebra de Lie de dimensão finita sobre um corpo de característica 0 admite uma álgebra de derivações nilpotente D livre de constantes (isto é, $x^\delta = 0$ para todo $\delta \in D$ implica $x = 0$), então L é nilpotente.

Nosso objetivo aqui é apresentar um estudo um pouco mais geral. Abordamos resultados correlatos e apresentamos uma demonstração para o resultado principal de [12], devido a E. I. Khukhro e P. Shumyatsky que afirma que se uma álgebra de Lie L de dimensão finita sobre um corpo algebricamente de característica 0 admite uma álgebra de derivações nilpotente D quase livre de contantes, ou seja, a dimensão da componente nula de Fitting é finita, então L é quase nilpotente no seguinte sentido: se m é a dimensão da componente nula de Fitting com respeito a D e D admite n pesos em L, então L contém uma subálgebra N de codimensão limitada por uma função dependendo somente de m e n, e a classe de nilpotência de N é limitada em termos somente de n.

Observe que isto melhora o resultado principal de [18], pois para $m = 0$ encontramos um limite superior para a classe de nilpotência de L em termos do número de pesos de D.

No desenrolar das discussões, necessitamos conceitos fundamentais, propriedades básicas e alguns resultados mais elaborados da Teoria de Anéis de Lie. Utilizamos certas graduações em álgebras de Lie e decomposições em espaços de peso. Além disso, um importante ingrediente para as demonstrações apresentadas no Capítulo 3 é um método consistindo de sucessivas "remodelagens" de comutadores, conhecida como Transformação HKK.

Grande parte dos resultados são essencialmente sobre álgebras de Lie $\mathbb{Z}_p$-graduadas onde p é um primo e a componente L_0 possui dimensão finita. As técnicas empregadas nas demonstrações dos resultados principais são técnicas combinatórias que podem ser encontradas em [9]. Adicionalmente, técnicas de Álgebra Linear são empregadas, visto que em muitos resultados faz-se necessário obter decomposições em soma (direta) cujos fatores têm certas propriedades requeridas.

No primeiro capítulo introduzimos resultados básicos da Teoria de Grupos, anéis de Lie, álgebras de Lie e produto tensorial. Alguns destes resultados são bem conhecidos e por isso omitimos as respectivas demonstrações. Por outro lado, também apresentamos resultados e conceitos não tão conhecidos, como por exemplo, o conceito de *peso* de uma álgebra de Lie. Finalizamos o capítulo apresentando alguns resultados sobre o anel de Lie $L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$, obtido a partir do produto tensorial de um anel de Lie L e do anel $\mathbb{Z}[\omega]$, onde ω é uma raiz da unidade.

O segundo capítulo é dedicado ao estudo de anéis de Lie que admitem um automorfismo regular. O principal objetivo do capítulo é demonstrar que se um anel de Lie admite um automorfismo regular de ordem prima p, então ele é nilpotente de classe de nilpotência limitada por um número $h(p)$.

No terceiro capítulo é demonstrado que se um anel de Lie A admite um automorfismo φ de ordem prima p tal que $|C_A(\varphi)| = q$, então ele possui um subanel nilpotente de classe de nilpotência limitada por uma função dependendo de p e índice limitado por uma função dependendo de p e q.

Finalmente, o quarto capítulo é dedicado ao resultado principal desta dissertação. Seu conteúdo consiste em demonstrar o teorema principal do artigo publicado por E. I. Khukhro e P. Shumyatsky [12] sobre álgebras de Lie admitindo álgebra de derivações quase livre de constantes. Para isso, utilizamos na maior parte da demonstração resultados apresentados no segundo e terceiro capítulos, adaptados para álgebras de Lie $\mathbb{Z}_p$-graduadas.

A fim de mostrar um pouco da evolução do estudo de álgebras de Lie via automorfismos e complementar as discussões dos capítulos anteriores, no quarto capítulo fazemos alguns comentários finais e neles apresentamos a conjectura de Higman, resultados sobre álgebras de Lie quase solúveis e sobre grupos nilpotentes admitindo automorfismos de ordens primas.

CAPÍTULO 1

Preliminares

Neste capítulo apresentamos algumas definições e demonstramos alguns resultados relacionados à Teoria de Grupos, Anéis, Álgebras de Lie e Produto Tensorial, os quais fazem parte do aparato teórico necessário às discussões deste trabalho.

1.1 Teoria de Grupos

Dado um grupo G, denotamos por 1 seu elemento neutro e, quando não houver risco de confusão, também denotamos por 1 o seu subgrupo trivial.

Seja X um subconjunto de um grupo G. Denotamos por $\langle X \rangle$ o subgrupo de G gerado por X. No caso particular em que X gera todo grupo G, escrevemos $G = \langle X \rangle$.

Lema 1.1 *Seja G um grupo abeliano sem torção (isto é, apenas o elemento neutro possui ordem finita) tal que $G = \langle g_1, g_2, \ldots, g_n \rangle$, onde os g_i são geradores livres. Então dado um número primo p existe um subgrupo H de G tal que o índice de H em G é p, e o subgrupo H não contém nenhum dos geradores, ou seja, $g_1, g_2, \ldots, g_n \notin H$.*

Daremos um exemplo para ilustrar o lema acima. Como G é abeliano, usaremos a notação aditiva. A ideia principal é mudar os geradores de G de forma conveniente. Apenas para ilustrar a ideia da demonstração do caso geral, consideraremos $G = \langle g_1, g_2, g_3 \rangle$. Agora considere $\overline{g}_1 = g_1 + g_2 + g_3$, $\overline{g}_2 = 3g_2 + 2g_3$ e $\overline{g}_3 = g_2 + g_3$. Então $\overline{g}_1 - \overline{g}_3 = g_1$, $3\overline{g}_3 - \overline{g}_2 = g_3$ e $\overline{g}_2 - 2\overline{g}_3 = g_2$ e, assim, $G = \langle \overline{g}_1, \overline{g}_2, \overline{g}_3 \rangle$.

Claramente, para qualquer número primo p, o subgrupo $H = \langle \overline{g}_1, \overline{g}_2, p \cdot \overline{g}_3 \rangle$ possui índice p em G. Sendo assim, nosso objetivo é mostrar que, para qualquer p, o sistema

$$\begin{cases} a_1 \cdot \overline{g}_1 + a_2 \cdot \overline{g}_2 + a_3 \cdot (p \cdot \overline{g}_3) = g_1 \\ a_4 \cdot \overline{g}_1 + a_5 \cdot \overline{g}_2 + a_6 \cdot (p \cdot \overline{g}_3) = g_2 \\ a_7 \cdot \overline{g}_1 + a_8 \cdot \overline{g}_2 + a_9 \cdot (p \cdot \overline{g}_3) = g_3 \end{cases}$$

não tem solução $a_i \in \mathbb{Z}$, para $i = 1, \ldots, 9$. Equivalentemente, queremos mostrar que, para qualquer p, o sistema

$$\begin{cases} a_1 g_1 + (a_1 + 3a_2 + pa_3)g_2 + (a_1 + 2a_2 + a_3 p)g_3 = g_1 \\ a_4 g_1 + (a_4 + 3a_5 + pa_6)g_2 + (a_4 + 2a_5 + a_6 p)g_3 = g_2 \\ a_7 g_1 + (a_7 + 3a_8 + pa_9)g_2 + (a_7 + 2a_8 + a_9 p)g_3 = g_3 \end{cases}$$

não tem solução, ou ainda, os sistemas

$$\begin{cases} a_1 = 1 \\ a_1 + 3a_2 + pa_3 = 0 \\ a_1 + 2a_2 + pa_3 = 0 \end{cases} \text{(i)}\,, \quad \begin{cases} a_4 = 0 \\ a_4 + 3a_5 + pa_6 = 1 \\ a_4 + 2a_5 + pa_6 = 0 \end{cases} \text{(ii)} \quad \text{e} \quad \begin{cases} a_7 = 0 \\ a_7 + 3a_8 + pa_9 = 0 \\ a_4 + 2a_8 + pa_9 = 1 \end{cases} \text{(iii)}$$

não têm soluções.

Para qualquer p, os sistemas (i), (ii) e (iii) não possuem solução inteira. No caso geral onde $G = \langle g_1, g_2, \ldots, g_n \rangle$, podemos considerar

$$\begin{aligned} \overline{g}_1 &= g_1 + g_{n-1} + g_n, \\ \overline{g}_2 &= g_2 + g_{n-1} + g_n, \\ &\vdots \\ \overline{g}_{n-1} &= 3g_{n-1} + 2g_n, \\ \overline{g}_n &= g_{n-1} + g_n \end{aligned}$$

e $H = \langle \overline{g}_1, \overline{g}_2, \ldots, p \cdot \overline{g}_n \rangle$, sendo assim, provar que H não contém os geradores de G se resume em provar que os sistemas (i), (ii) e (iii) não possuem solução para qualquer p. Mas, isto já foi verificado.

O lema acima garante que dado p existe um subgrupo H de índice p tal que H não contém os geradores de G. Porém, obviamente não garante que H não contenha combinações lineares dos geradores. Para garantir que o subgrupo H descrito acima não contém uma determinada combinação linear, precisamos restringir o número primo p. Por exemplo, se considerarmos, como no exemplo acima, $G = \langle \overline{g}_1, \overline{g}_2, \overline{g}_3 \rangle$ (onde $\overline{g}_1 = g_1 + g_2 + g_3$, $\overline{g}_2 = 3g_2 + 2g_3$ e $\overline{g}_3 = g_2 + g_3$) e exigirmos que $H = \langle \overline{g}_1, \overline{g}_2, p \cdot \overline{g}_3 \rangle$ além de não conter os geradores de G também não contenha $g_1 + g_2$, precisaremos que não apenas os sistemas (i), (ii) e (iii), mas também o sistema

$$\begin{cases} b_1 = 1 \\ b_1 + 3b_2 + pb_3 = 1 \\ b_1 + 2b_2 + pb_3 = 0 \end{cases} \text{(iv)}$$

não tenha solução, ou seja, p deve ser diferente de 3.

Observação 1.2 *A discussão acima sobre a restrição do número p terá uma aplicação importante no Capítulo 4, onde consideraremos g_i os pesos de uma álgebra de Lie.*

Teorema 1.3 *Seja G um grupo. Se H e K são subgrupos de G, ambos de índice finito, então o subgrupo $H \cap K$ também tem índice finito.*

Demonstração. Primeiro vamos provar que, para todo $a \in G$, temos $(H \cap K)a = Ha \cap Ka$. Como $(H \cap K)a \subseteq Ha$ e $(H \cap K)a \subseteq Ka$, temos $(H \cap K)a \subseteq Ha \cap Ka$.

Dado $x \in Ha \cap Ka$, temos $x = ha = ka$, com $h \in H$, $k \in K$, logo $h = k \in (H \cap K)$. Consequentemente, $x \in (H \cap K)a$ e temos $Ha \cap Ka \subseteq (H \cap K)a$.

Sendo assim, como a quantidade de classes Ha e Ka são finitas, temos que as possíveis interseções $Ha \cap Ka$ também o são. Portanto, $[G : H \cap K]$ é finito.

$\square$

Corolário 1.4 *Seja V um espaço vetorial sobre um corpo F. Se H e K são subespaços de V, ambos de codimensão finita, então o subespaço $H \cap K$ também tem codimensão finita.*

Dado um grupo G, definimos o **comutador** de dois elementos $x, y \in G$, por $[x,y] = x^{-1}y^{-1}xy$ e definimos, por indução, o comutador de r elementos $x_1, x_2, \ldots, x_r \in G$ por $[x_1, x_2, \ldots, x_r] = [[x_1, x_2, \ldots, x_{r-1}], x_r]$, onde $[x_1] = x_1$.

Dado um conjunto X, definimos por recorrência o **peso** de um comutador em X. Primeiro definimos como comutadores de peso 1 os elementos de X, e agora, se c_1 e c_2 são comutadores de pesos r_1 e r_2 respectivamente, então $[c_1, c_2]$ é um comutador de peso $r_1 + r_2$ em X. O comutador $[x_1, x_2, \ldots, x_r] = [[x_1, x_2, \ldots, x_{r-1}], x_r]$, onde cada entrada é um comutador de peso 1, é chamado de *comutador simples de peso r*.

Dados dois subconjuntos A e B de um grupo G, definimos o subgrupo $[A, B]$ como

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

De forma análoga à definição de comutador de r elementos, dados $X_1, X_2, \ldots, X_r$ subconjuntos de G, definimos $[X_1, X_2, \ldots, X_r]$ como sendo o subgrupo de G gerado por todos comutadores da forma $[x_1, x_2, \ldots, x_r]$, onde $x_i \in X_i$.

Definição 1.5 *A **série derivada** de um grupo G é definida por:*

$$\begin{array}{rcl} G^{(0)} & = & G; \\ G^{(1)} & = & [G,G]; \\ & \vdots & \\ G^{(n)} & = & [G^{(n-1)},G^{(n-1)}]. \end{array}$$

Um grupo é dito solúvel de comprimento derivado n quando n é o menor número natural tal que $G^{(n)}=1$.

Dizemos que um elemento $z \in G$ pertence ao centro de um grupo G, denotado por $Z(G)$, quando $[z,g]=1$ para todo $g \in G$.

Definição 1.6 *A **série central inferior** de um grupo G é dada por:*

$$\begin{array}{rcl} \gamma_1(G) & = & G; \\ \gamma_2(G) & = & [G,G]; \\ & \vdots & \\ \gamma_{s+1}(G) & = & [\gamma_s(G),G]. \end{array}$$

Dizemos que um grupo é nilpotente de classe c quando c é o menor número natural tal que $\gamma_{c+1}(G)=1$.

Observamos que $\gamma_{c+1}(G)$ é gerado por todos os comutadores simples de peso $c+1$ nos elementos de G. De posse da definição de grupo nilpotente, temos as seguintes equivalências, cuja demonstração pode ser encontrada em [3].

Teorema 1.7 *Dado um grupo G, as seguintes afirmações são equivalentes:*

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

(ii) $[g_1,g_2,\ldots,g_{c+1}]=1$*, para todo $g_i \in G$;*

Corolário 1.8 *Um grupo G é nilpotente de classe $c>1$ se, e somente se, $G/Z(G)$ é nilpotente de classe $c-1$.*

Teorema 1.9 *Se um grupo G é gerado por um subconjunto X, então G é nilpotente de classe $\leq c$ se, e somente se, todo comutador de peso $c+1$ com entradas em X é igual a 1.*

Demonstração. Note que se G é nilpotente de classe c, então pelo Teorema 1.7, todo comutador de peso $c+1$ é igual a 1. Em particular, comutadores com entradas em X são iguais a 1.

Para demonstrar a recíproca, usaremos indução sobre c. Se $c = 1$, então por hipótese todos os geradores de G comutam, consequentemente G é abeliano, logo é nilpotente de classe igual a 1. Seja $c > 1$. Como $[x_1,\ldots,x_c,x] = 1$, para todo $x \in X$, ou seja, o comutador $[x_1,\ldots,x_c]$ comuta com todos os geradores de G e consequentemente com todos os elementos de G, segue que $[x_1,\ldots,x_c] \in Z(G)$, para todos $x_i \in X$. Pela hipótese de indução, $G/Z(G)$ é nilpotente de classe $\leq c-1$, pois o grupo quociente $G/Z(G)$ é gerado pelas classes laterais dos elementos de X. Portanto, pelo Corolário 1.8, G é nilpotente de classe $\leq c$.

□

1.2 Automorfismos de Grupos

Apresentaremos agora alguns resultados sobre automorfismos de grupos, cujas demonstrações podem ser encontradas em [9] e [10].

Admitiremos sem demonstrar dois resultados da Álgebra Linear, os quais também podem ser encontrados em [9] e [10]. O primeiro é o Teorema da Forma Normal de Jordan e o segundo garante um limite para os blocos de Jordan de uma matriz sobre certas condições.

Teorema 1.10 (Teorema da Forma Normal de Jordan) *Seja φ uma transformação linear de um espaço vetorial V de dimensão finita sobre um corpo F. Se todos os autovalores de φ pertencem a F, então V tem uma base na qual a matriz de φ está na forma normal de Jordan, isto é, sua matriz pode ser escrita na forma de blocos diagonais $diag(J_1,\ldots,J_s)$, onde os blocos de Jordan J_i são da forma*

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

onde os λ_i são autovalores de φ (não necessariamente distintos).

Teorema 1.11 *Seja p um número primo e φ um elemento de ordem p^k em um grupo de transformações lineares de um espaço vetorial V sobre um corpo F de característica p. Então todos os autovalores de φ são iguais a 1 e V tem uma F-base na qual a matriz de φ na forma normal de Jordan possui todos seus blocos de tamanho no máximo $p^k \times p^k$, e existe pelo menos um bloco de tamanho exatamente $p^k \times p^k$.*

Definimos o conjunto dos pontos fixos de um automorfismo φ de G por $C_G(\varphi) = \{g \in G \ : \ g^\varphi = g\}$, que é um subgrupo de G. O automorfismo φ é dito **regular** quando $C_G(\varphi) = 1$.

O próximo teorema será utilizado várias vezes ao longo deste trabalho, com o intuito de mostrar que certos p-grupos admitindo automorfismos de ordem p^i são triviais, por não possuírem pontos fixos.

Lema 1.12 *Seja p um número primo. Se φ é um automorfismo de ordem p^k de um p-grupo abeliano não trivial G, então $C_G(\varphi) \neq 1$.*

Demonstração. Considere o subgrupo não trivial de G

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

que pode ser considerado como um espaço vetorial sobre o corpo $\mathbb{Z}_p$ e cuja restrição de φ em V é uma transformação linear.

Pelo Teorema 1.11, φ possui todos seus autovalores iguais a 1. Portanto, os autovetores não triviais de φ associados ao autovalor 1 são elementos não triviais que pertencem a $C_G(\varphi)$.

□

Definimos o **posto** de um grupo abeliano G como sendo o número minimal de geradores que G possa admitir.

Lema 1.13 *Seja G um p-grupo abeliano finito. Se o subgrupo*

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

de G possui posto r (ou, como espaço vetorial, possui dimensão r), então G também possui posto r. Na verdade, o posto de G é igual ao posto de V.

Demonstração. Seja s o posto de G. Como G é um grupo abeliano finito, usando o Teorema fundamental dos grupos abelianos finitamente gerados, temos que o posto de G é maior ou igual ao posto de V e $G = \langle g_1 \rangle \oplus \cdots \oplus \langle g_s \rangle$, onde $|\langle g_i \rangle| = p^{k_i} \geq p$.

Por outro lado, $H = \langle p^{k_1 - 1} \cdot g_1 \rangle \oplus \cdots \oplus \langle p^{k_s - 1} \cdot g_s \rangle$ é um subgrupo de V e tem posto s, logo $s \leq r$.

□

Lema 1.14 *Seja p um número primo e seja φ um automorfismo de ordem p^k de um p-grupo abeliano G, onde $|C_G(\varphi)| = p^n$. Então o posto de G é no máximo $p^k n$.*

Demonstração. Assumimos primeiro que G possui posto finito e demonstramos que seu posto é no máximo $p^k n$.

Considere o subgrupo $V = \langle g \in G : g^p = 1 \rangle$ como um espaço vetorial sobre $\mathbb{Z}_p$ e φ como uma transformação linear de V. Pelo Teorema 1.11, todos os autovalores de φ são iguais a 1 e V possui uma $\mathbb{Z}_p$-base na qual a matriz de φ na forma normal de Jordan possui blocos

$$J_i = \begin{pmatrix} 1 & 1 & & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}$$

de tamanho no máximo $p^k \times p^k$.

Calculando os pontos fixos de cada bloco,

$$\begin{pmatrix} 1 & 1 & & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_2 + x_3 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix},$$

temos, necessariamente, $x_2 = x_3 = \cdots = x_r = 0$. Sendo assim, o subconjunto desta base correspondente a cada bloco contém um único autovetor pertencente a $C_V(\varphi)$ e podemos ver que os autovetores correspondentes a diferentes blocos são linearmente independentes.

Assim, a dimensão do subespaço de V gerado por seus pontos fixos, ou seja $d = \dim C_V(\varphi)$, é igual ao número de blocos l. Por outro lado, o posto de V, ou melhor, a dimensão de V, é igual à soma da dimensão dos blocos e consequentemente é no máximo $p^k l$. Finalmente, observando a desigualdade

$$p^d = |C_V(\varphi)| \leq |C_G(\varphi)| \leq p^n,$$

concluímos que $l = d \leq n$. Agora, pelo Lema 1.13, o posto de V, e consequentemente o posto de G, é no máximo $p^k n$.

Agora, para concluir a demonstração, precisamos mostrar que de fato o posto de G é finito. Nas hipóteses do teorema, suponha que G não tenha posto finito. Então podemos encontrar um subgrupo H de G o qual tem posto finito e maior que $p^k n$.

Como H é um p-grupo abeliano e de posto finito, temos que H é finito. Logo pelo Lema 1.13, o subgrupo

$$V_H = \langle h \in H : h^p = 1 \rangle,$$

visto como espaço vetorial sobre $\mathbb{Z}_p$, possui dimensão maior que $p^k n$.

Assim, pelo Lema 1.11, a matriz de φ deve possuir mais que n blocos, visto que cada um possui tamanho no máximo $p^k \times p^k$. Como cada bloco possui um único vetor de $C_{V_H}(\varphi)$, deveríamos ter mais que n autovetores de $C_{V_H}(\varphi)$ na base de V_H. Como cada autovetor corresponde a um subespaço, teríamos $|C_{V_H}(\varphi)| > p^n$. Portanto, necessariamente o posto de G é finito.

$\square$

1.3 Anéis de Lie

Definição 1.15 *Um **anel de Lie** A é um anel não associativo e identidade, cuja multiplicação, a qual é usualmente denotada por colchetes $[\ ,\ ]$, satisfaz os seguintes axiomas:*

(L_1) $[a,a] = 0$, *para todo* $a \in A$;

(L_2) $[[a,b],c] + [[b,c],a] + [[c,a],b] = 0$, *para todos* $a,b,c \in A$.

O axioma (L_2) é conhecido como *Identidade de Jacobi* e o produto $[a,b]$ é usualmente chamado de **comutador** de a e b.

Tendo em vista a definição de anel, temos que as seguintes propriedades são satisfeitas:

(i) $[a_1 + a_2, b] = [a_1, b] + [a_2, b]$, para todos $a_1, a_2, b \in A$;

(ii) $[a, b_1 + b_2] = [a, b_1] + [a, b_2]$, para todos $a, b_1, b_2 \in A$.

Utilizando as propriedades (i), (ii) e o axioma (L_1), podemos obter a propriedade de anticomutatividade:

(iii) $[a,b] = -[b,a]$, para todos $a, b \in A$.

Dado um anel de Lie A, dizemos que um subconjunto B de A é um *subanel de Lie*, se B é um subgrupo aditivo de A e a operação produto é fechada em B. Em outras palavras, se B é um anel de Lie contido em A. Dizemos que um subanel I é um *ideal* de A

se dado $b \in I$ temos $[a,b] \in I$, para todos $a \in A$.

De maneira análoga ao que foi feito para grupos, vamos definir, por indução, o *comutador de r elementos* $x_1, x_2, \ldots, x_r$ como $[x_1, x_2, \ldots, x_r] = [[x_1, \ldots, x_{r-1}], x_r]$. O conceito de *comutador simples de peso r* em elementos de um anel de Lie A é o mesmo utilizado para grupos.

Chamamos de *segmento inicial de peso t* de um comutador simples (digamos de peso r), o subcomutador formado pelos t primeiros elementos (da esquerda para direita), por exemplo,

$$[x_1, x_2, \ldots, x_r] = [\underbrace{[x_1, x_2, \ldots, x_t]}_{\text{segmento inicial}}, \ldots, x_r].$$

Dados dois ideais H e K de um anel de Lie A, conseguimos um novo ideal $[H,K]$ de A, definindo $[H,K]$ como o subgrupo aditivo

$$\langle [h,k] : h \in H \text{ e } k \in K \rangle.$$

Definimos a seguir duas séries de ideais de um anel de Lie A, que são análogas às séries derivada e central inferior de um grupo G.

Definição 1.16 *A **série derivada** de um anel de Lie A é definida como:*

$$\begin{array}{rcl} A^{(0)} & = & A; \\ A^{(1)} & = & [A,A]; \\ & \vdots & \\ A^{(n)} & = & [A^{(n-1)}, A^{(n-1)}]. \end{array}$$

Um anel de Lie é dito solúvel de comprimento derivado n quando n é o menor número natural tal que $A^{(n)} = 0$.

Definição 1.17 *Definimos a **série central inferior** de um anel de Lie A do seguinte modo:*

$$\begin{array}{rcl} \gamma_1(A) & = & A; \\ \gamma_2(A) & = & [A,A]; \\ & \vdots & \\ \gamma_{s+1}(A) & = & [\gamma_s(A), A]. \end{array}$$

Dizemos que um anel de Lie é nilpotente de classe c quando c é o menor número natural tal que $\gamma_{c+1}(A) = 0$.

Dizemos que um elemento $z \in A$ pertence ao centro de um anel de Lie A, denotado por $Z(A)$, quando $[z,a] = 0$, para todo $a \in A$.

Enunciamos agora versões dos Teoremas 1.7 e 1.9 para anéis de Lie. As demonstrações são análogas às de Teoria de Grupos.

Teorema 1.18 *Dado um anel de Lie A, as seguintes afirmações são equivalentes:*

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

(ii) $[x_1, x_2, \ldots, x_{c+1}] = 0$*, para todos* $x_1, x_2, \ldots, x_{c+1} \in A$*;*

Corolário 1.19 *Um anel de Lie A é nilpotente de classe* $c > 1$ *se, e somente se,* $A/Z(A)$ *é nilpotente de classe* $c-1$*.*

Teorema 1.20 *Se um anel de Lie A é gerado por um subconjunto X, então A é nilpotente de classe* $\leq c$ *se, e somente se, todo comutador de peso* $c+1$ *com entradas em X é igual a 0.*

Lema 1.21 *Seja A um anel de Lie. Denotamos por nA o subanel gerado por todos os elementos da forma* $n \cdot a = \underbrace{a + a + \cdots + a}_{n}$ *, onde* $a \in A$*. Então* $(nA)^{(s)} = n^{2^s} A^{(s)}$ *e* $\gamma_k(nA) = n^k \gamma_k(A)$*.*

Demonstração. Provaremos apenas para a série central inferior, o caso para a série derivada é análogo. Temos que $\gamma_k(nA)$ é o ideal gerado por todos comutadores da forma

$$[n \cdot a_1, n \cdot a_2, \ldots, n \cdot a_k] = [\underbrace{a_1 + \cdots + a_1}_{n \text{ vezes}}, \underbrace{a_2 + \cdots + a_2}_{n \text{ vezes}}, \ldots, \underbrace{a_k + \cdots + a_k}_{n \text{ vezes}}],$$

onde $a_i \in A$. Portanto, usando a propriedade distributiva, segue o resultado.

$\square$

Demonstramos a seguir dois resultados combinatoriais, cujas demonstrações são essencialmente repetidas aplicações da Identidade de Jacobi e da propriedade de anticomutatividade.

Lema 1.22 *Seja A um anel de Lie. Dado um comutador* $[a, x_1, \ldots, x_i \ldots, x_j, \ldots, x_k]$*, onde* $a \in \gamma_k(A')$*, temos*

$$[a, x_1, \ldots, x_i \ldots, x_j, \ldots, x_k] \equiv [a, x_1, \ldots, x_j \ldots, x_i, \ldots, x_k] \ (mod\ \gamma_{k+1}(A')),$$

para todos $i, j = 1, \ldots, k$*.*

Demonstração. Utilizando a Identidade de Jacobi e a propriedade de anticomutatividade, temos a seguinte igualdade

$$[a,x_1,x_2] = [a,x_2,x_1] + [a,[x_1,x_2]]. \tag{1-1}$$

Claramente o comutador $[a,[x_1,x_2]]$ pertence a $\gamma_{k+1}(A'))$, ou seja,

$$[a,x_1,x_2] = [a,x_2,x_1] \ (mod \ \gamma_{k+1}(A')).$$

Aplicando sucessivas vezes a igualdade (1-1) e lembrando que $\gamma_s(A')$ é um ideal para todo s, conseguimos o resultado desejado.

□

Lema 1.23 *Seja A um anel de Lie. Podemos escrever o comutador $[x_1,\dots,x_i,\dots,x_k]$ como uma combinação linear de comutadores da forma $[x_i,\dots]$, ou seja, o comutador $[x_1,\dots,x_i,\dots,x_k]$ pode ser escrito como uma combinação linear de comutadores cuja primeira entrada é x_i.*

Exemplo 1.24 *Apenas para exemplificar, utilizaremos a igualdade (1-1) para escrever o comutador $[x_1,x_2,x_3]$ como combinação linear de comutadores com a primeira entrada igual a x_3.*

$$\begin{aligned}
[x_1,x_2,x_3] &= [x_1,x_3,x_2] + [x_1,[x_2,x_3]] \\
&= -[x_3,x_1,x_2] - [[x_2,x_3],x_1] \\
&= -[x_3,x_1,x_2] + [x_3,x_2,x_1].
\end{aligned}$$

O caso geral decorre de sucessivas aplicações da igualdade (1-1) e da propriedade de anticomutatividade.

Dado um elemento $a \in A$, definimos o centralizador de a em A como sendo o subanel

$$C_A(a) = \{x \in A : [x,a] = 0\}.$$

Analogamente, dado um subconjunto H de A, definimos

$$C_A(H) = \{x \in A : [x,h] = 0, \text{ para todo } \ h \in H\}.$$

Lema 1.25 *Para todo elemento a de um anel de Lie arbitrário A, existe uma bijeção entre o conjunto dos comutadores da forma $\{[x,a] : x \in A\}$ e o conjunto das classes laterais (à direita) do centralizador $C_A(a)$.*

Demonstração. Afirmamos que a aplicação que associa cada classe $C_A(a)+x$ ao elemento $[x,a]$ satisfaz o desejado. Esta aplicação está bem definida, uma vez que outro representante x' da classe $C_A(a)+x$ satisfaz $x'=c+x$ para algum $c\in C_A(a)$, logo

$$[x',a]=[c+x,a]=[c,a]+[x,a]=[x,a].$$

Mostremos que a aplicação é injetiva. Se $[x,a]=[y,a]$, então

$$[x-y,a]=[x,a]-[y,a]=[x,a]-[x,a]=0,$$

o que significa que $x-y\in C_A(a)$. A sobrejetividade é imediata.

□

Usaremos a expressão *r-limitada* para indicar que existe uma função $f=f(r)$, dependendo somente de r, que limita superiormente certo valor ou propriedade. Por exemplo, dizemos que um anel de Lie A é nilpotente de classe r-limitada, quando existe uma função $f=f(r)$, dependendo apenas de r tal que sua classe de nilpotência não é maior que $f(r)$.

Analogamente, usaremos a notação $\{r_1,\dots,r_k\}$*-limitada* para indicar que certo valor é limitado superiormente por uma função $f=f(r_1,\dots,r_k)$, dependendo apenas de $r_1,\dots,r_k$.

Teorema 1.26 *Seja A um anel de Lie arbitrário com $\gamma_k(A)$ finito de ordem n. Então A possui um subanel nilpotente de classe no máximo k cujo índice é $\{k,n\}$-limitado.*

Demonstração. Vamos mostrar que o subgrupo $C_A(\gamma_k(A))$ satisfaz o desejado. Primeiro vamos mostrar que $|A:C_A(\gamma_k(A))|$ é $\{k,n\}$-limitado.

Como $\gamma_k(A)$ é finito de ordem n, então existem $x_1,x_2,\dots,x_n\in\gamma_k(A)$ tais que $\gamma_k(A)=\langle x_1,x_2,\dots,x_n\rangle$. Para cada $x_i\in\gamma_k(A)$, o conjunto $\{[\ell,x_i]:\ell\in A\}$ tem cardinalidade menor que n, pois $[\ell,x_i]\in\gamma_k(A)$.

Assim, pelo Lema 1.25, temos $|A:C_A(x_i)|\leq n$. Logo da igualdade

$$C_A(\gamma_k(A))=\bigcap_{i=1}^{n}C_A(x_i)$$

segue que $|A:C_A(\gamma_k(A))|$ é $\{k,n\}$-limitada.

Agora devemos mostrar que $C_A(\gamma_k(A))$ é nilpotente de classe no máximo k. Para isto, é suficiente provar que $[c_1,c_2,\dots,c_{k+1}]=0$, para todos $c_1,c_2,\dots,c_{k+1}\in C_A(\gamma_k(A))$.

Mas isto segue do fato que $[c_1,c_2,\ldots,c_k] \in \gamma_k(A)$ e $c_{k+1} \in C_A(\gamma_k(A))$. $\square$

Anéis de Lie Livres

O conceito de anel de Lie livre será utilizado na demonstração de resultados importantes deste trabalho, com o intuito de facilitar alguns cálculos, porém, não faremos aqui um estudo detalhado deste tema, apenas discutiremos fatos necessários para o entendimento das técnicas que utilizaremos. Uma discussão mais profunda sobre este tema pode ser encontrada no Capítulo 1 de [9].

O conceito de anel de Lie livre é na verdade uma analogia ao conceito de grupo livre e, da mesma forma que um grupo livre, o anel de Lie livre possui uma "propriedade universal", a qual afirma que toda função de seus geradores em um anel de Lie qualquer pode ser estendida de forma única para um homomorfismo.

Dizemos que um anel de Lie A é gerado pelo conjunto X, e denotamos $A = \langle X \rangle$ quando $A = \sum_i A_i$, onde A_i é a componente homogênea de A de peso i, isto é, A_i é o subgrupo aditivo gerado por todos os comutadores de peso i em elementos de X. Analogamente, se $A = \langle x_1, x_2, \ldots \rangle$, então $A = \sum A_{i_1,i_2,\ldots}$, onde $A_{i_1,i_2,\ldots}$ é a componente multihomogênea de peso i_1 em x_1, de peso i_2 em x_2 etc, isto é, $A_{i_1,i_2,\ldots}$ é o subgrupo aditivo de A gerado por todos comutadores em elementos $x_1, x_2, \ldots$ de peso i_1 em x_1, de peso i_2 em x_2 etc.

Um ideal ou um subgrupo aditivo I de um anel de Lie $A = \langle X \rangle$ é dito **homogêneo** (multihomogêneo) com respeito ao conjunto de geradores X se

$$I = \bigoplus I \cap A_i \quad (I = \bigoplus I \cap A_{i_1,i_2,\ldots}).$$

As interseções $I \cap A_i$ $(I \cap A_{i_1,i_2,\ldots})$ são chamadas de componentes homogêneas de peso i (multihomogênea de multipeso $(i_1, i_2, \ldots)$) do ideal (ou subgrupo aditivo) homogêneo (multihomogêneo) I.

Definição 1.27 *Um anel de Lie F é dito livre sobre um conjunto X se F pode ser decomposto como soma direta $F = \bigoplus F_i$ de suas componentes homogêneas. Os elementos do conjunto X são chamados de **geradores livres** de F.*

Dado um conjunto X podemos encontrar um anel de Lie $F(X)$ livre em X. A grosso modo, o anel de Lie $F(X)$ é construído do seguinte modo: primeiro definimos o produto como sendo a concatenação de colchetes e, para todo inteiro positivo i, construímos as componentes homogêneas F_i de peso i em elementos de X. Agora consideramos

$F(X)$ como o conjunto de todas as combinações lineares finitas de elementos das componentes homogêneas F_i, identificando duas combinações lineares se uma pode ser obtida da outra por meio da Identidade de Jacobi, anticomutatividade e distribuitividade.

Agora, dado um anel de Lie A e uma função $\lambda : X \longrightarrow A$ podemos definir um homomorfismo $\Lambda : F(X) \longrightarrow A$ tal que $\Lambda(x) = \lambda(x)$, para todo $x \in X$, fazendo:

$$\Lambda(\sum_J [x_{j_1}, \ldots, x_{j_k}]) = \sum_J [\lambda(x_{j_1}), \ldots, \lambda(x_{j_k})], \text{ para todos } x_{j_1}, \ldots, x_{j_k} \in X.$$

A unicidade é de verificação imediata.

Analogamente, seja A um anel de Lie, o ideal de A gerado pelo conjunto X é denotado por ${}_{id}\langle X\rangle$. O grupo aditivo de ${}_{id}\langle X\rangle$ é gerado pelos comutadores simples da forma $[\ldots[[x,a_1],a_2],\ldots,a_k]$, onde $x \in X$, $a_i \in A$ e $k \geq 0$.

Definição 1.28 *Seja G um grupo abeliano. Um anel de Lie A tem uma G-graduação, ou é dito G-graduado, se cada elemento $g \in G$ corresponde a um subgrupo A_g do grupo aditivo de A tal que*

(i) $A = \sum_{g \in G} A_g$;

(ii) $[A_a, A_b] \subseteq A_{a+b}$, *para todos* $a, b \in G$.

O conceito de anel de Lie G-graduado será amplamente usado neste trabalho. Um exemplo importante será dado na próxima seção, a qual trata de álgebras de Lie.

1.4 Álgebras de Lie

Definição 1.29 *Um espaço vetorial L sobre um corpo F, com uma operação $L \times L \longrightarrow L$, onde o par (x,y) é levado em $[x,y]$, é chamado uma* ***álgebra de Lie*** *sobre F se os seguintes axiomas são satisfeitos:*

(L_1) *A operação produto é bilinear, isto é, para todos $x, x_1, x_2, y, y_1, y_2 \in L$ e $\alpha \in F$*
$[x_1 + x_2, y] = [x_1, y] + [x_2, y]$,
$[x, y_1 + y_2] = [x, y_1] + [x, y_2]$,
$\alpha[x,y] = [\alpha x, y] = [x, \alpha y]$;

(L_2) $[x,x] = 0$, *para todo* $x \in L$;

(L_3) $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$, *para todos* $x, y, z \in L$.

Uma álgebra de Lie pode ser considerada como um anel de Lie onde seu grupo aditivo é na verdade um espaço vetorial. Sendo assim, os resultados e definições sobre anéis de Lie estudados na seção anterior se estendem naturalmente para álgebras de Lie.

É interessante também observar que alguns resultados sobre anéis de Lie finitos valem automaticamente para álgebras de Lie de dimensão finita, uma vez que $\alpha[x,y] = [\alpha x, y] = [x, \alpha y]$. Por exemplo, o Teorema 1.26, pode ser enunciado para álgebras de Lie do seguinte modo:

Teorema 1.30 *Suponha que L é uma álgebra de Lie arbitrária com $\gamma_k(L)$ de dimensão finita n. Então L possui uma subálgebra nilpotente de classe no máximo k, cuja codimensão é $\{k,n\}$-limitada.*

Dado um espaço vetorial V, podemos definir uma álgebra de Lie no espaço vetorial das transformações lineares de V, usualmente denotado por $EndV$, utilizando como produto uma nova operação. Por exemplo, dados $x, y \in EndV$ definimos o produto de Lie (ou comutador) $[x,y] = xy - yx$, onde as operações no lado direto são as usuais (composição e subtração de transformações lineares de V). Apenas para diferenciar chamaremos de $gl(V)$ o espaço vetorial $EndV$ com este novo produto.

Como o grupo aditivo de uma álgebra de Lie L é um espaço vetorial, também podemos definir sobre suas transformações lineares o produto de Lie, ou seja, dada uma álgebra de Lie L, podemos definir, usando o produto de Lie, uma nova álgebra de Lie em suas transformações lineares, denotada por $gl(L)$.

Definição 1.31 *Seja L uma álgebra de Lie. Por uma derivação de L entendemos uma aplicação linear $\delta : L \longrightarrow L$ satisfazendo a relação*

$$\delta([x,y]) = [x, \delta(y)] + [\delta(x), y], \quad \textit{para todos } x, y \in L.$$

Lema 1.32 *A coleção de todas as derivações de L, denotada por $Der\ L$, é um subespaço vetorial de $gl(L)$.*

Demonstração. Considere a álgebra de Lie L sobre um corpo F. Sejam $\delta_1, \delta_2 \in Der\ L$ e $\alpha \in F$. Sabemos que $\alpha\delta_1 + \delta_2$ é também uma transformação linear e

$$\begin{aligned}
(\alpha\delta_1 + \delta_2)(xy) &= \alpha\delta_1(xy) + \delta_2(xy) \\
&= \alpha x\delta_1(y) + \alpha\delta_1(x)y + x\delta_2(y) + \delta_2(x)y \\
&= x(\alpha\delta_1(y) + \delta_2(y)) + (\alpha\delta_1(x) + \delta_2(x))y \\
&= x(\alpha\delta_1 + \delta_2)(y) + (\alpha\delta_1 + \delta_2)(x)y, \text{ para todos } x, y \in L.
\end{aligned}$$

Portanto, $\alpha\delta_1 + \delta 2 \in Der\ L$.

□

Lema 1.33 *O produto de Lie (comutador) de duas derivações de L é também uma derivação de L.*

Demonstração. Sejam δ_1, $\delta_2 \in Der\ L$. Mostremos que $[\delta_1, \delta_2] \in Der\ L$. Para isso, basta observar a igualdade:

$$\begin{aligned}
[\delta_1,\delta_2](xy) &= \delta_1\delta_2(xy) - \delta_2\delta_1(xy) \\
&= \delta_1(x\delta_2(y) + \delta_2(x)y) - \delta_2(x\delta_1(y) + \delta_1(x)y) \\
&= \delta_1(x\delta_2(y)) + \delta_1(\delta_2(x)y) - \delta_2(x\delta_1(y)) - \delta_2(\delta_1(x)y) \\
&= x\delta_1\delta_2(y) + \delta_1(x)\delta_2(y) + \delta_2(x)\delta_1(y) + \delta_1\delta_2(x)y \\
&- x\delta_2\delta_1(y) - \delta_2(x)\delta_1(y) - \delta_1(x)\delta_2(y) - \delta_2\delta_1(x)y \\
&= x(\delta_1\delta_2(y) - \delta_2\delta_1(y)) + (\delta_1\delta_2(x) - \delta_2\delta_1(x))y \\
&= x[\delta_1,\delta_2](y) + [\delta_1,\delta_2](x)y, \text{ para todos } x,y \in L.
\end{aligned}$$

□

Conforme os dois lemas anteriores , temos que $Der\ L$ é uma subálgebra de Lie de $gl(L)$.

Exemplo 1.34 *Seja L uma álgebra de Lie. Se $x \in L$, a aplicação que leva $y \in L$ em $[x,y]$ é um endomorfismo de L, o qual denotaremos por* **adx**. *Escrevemos adx(y)=$[x,y]$. Claramente, adx é uma transformação linear. Por outro lado, usando a Identidade de Jacobi obtemos a seguinte igualdade*

$$[x,[y,z]] = [[x,y],z] + [y,[x,z]], \ \textit{para todos} \ x,y,z \in L,$$

ou seja,

$$adx([y,z]) = [adx(y),z] + [y,adx(z)].$$

Portanto, $adx \in Der\ L$.

Lema 1.35 *A aplicação $ad : L \longrightarrow gl(L)$ definida por $ad(x) = adx$ é um homomorfismo.*

A aplicação $L \longrightarrow Der\ L$ que leva x em adx é conhecida como a **representação adjunta** de L.

Definição 1.36 *Seja L uma álgebra de Lie. Dizemos que $x \in L$ é ad-nilpotente se adx é um endomorfismo nilpotente, ou seja, existe um inteiro positivo m tal que $(adx)^m(y) = 0$, para todo $y \in L$.*

Observação 1.37 *Se L é nilpotente, então todos os seus elementos são ad-nilpotentes.*

A recíproca da observação anterior é conhecida como *Teorema de Engel*.

Teorema 1.38 (Teorema de Engel) *Seja L uma álgebra de Lie de dimensão finita. L é nilpotente se, e somente se, todos os elementos de L são ad-nilpotentes.*

Demonstração. Usaremos sem demonstrar o Teorema 1.5.1 de [18], o qual afirma que se todos elementos de L são ad-nilpotentes e $L \neq 0$, então $Z(L) \neq 0$.

Precisamos mostrar que se todos os elementos de L são ad-nilpotentes, então L é nilpotente. Demonstraremos usando indução sobre a dimensão de L.

Se dimensão de L é igual a 1, então L é uma álgebra de Lie comutativa, ou seja, $[x,y] = 0$ para todos $x,y \in L$, uma vez que todos elementos são múltiplos de algum gerador de L.

Agora suponha que a dimensão de L é maior que 1. Usamos o fato que $Z(L) \neq 0$ para concluir que a dimensão de $L/Z(L)$ é menor que a dimensão de L. Logo, por hipótese de indução, temos que $L/Z(L)$ é nilpotente (observe que os elementos de $L/Z(L)$ também são ad-nilpotentes). Portanto, pelo Corolário 1.19, L é nilpotente.

$\square$

1.5 Espaços de Peso

Dada uma álgebra de Lie nilpotente L admitindo uma álgebra de derivações nilpotente, estamos interessados em decompô-la como soma direta de subespaços invariantes sob suas derivações. Para isso, é preciso introduzir a noção de peso e espaços de peso de uma álgebra de Lie. Omitiremos algumas demonstrações que o leitor pode encontrar em [18].

Em certo sentido, a decomposição de uma álgebra de Lie em espaços de peso é uma generalização do Teorema da Decomposição Primária usualmente estudado em Álgebra Linear, cuja demonstração pode ser encontrada em [5]. A principal diferença é que na decomposição em espaços de peso encontramos subespaços invariantes sob um conjunto de transformações lineares e não sob apenas uma.

Teorema 1.39 (Teorema da Decomposição Primária) *Seja T um operador linear sobre o espaço vetorial V de dimensão finita sobre o corpo F. Seja p o polinômio minimal de T, tal que*

$$p = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k},$$

onde os p_i são polinômios distintos, irredutíveis e unitários sobre F e os r_i são inteiros positivos. Seja W_i o núcleo de $p_i(T)^{r_i}$, $i = 1, \ldots, k$. Então

(i) $V = W_1 \oplus \cdots \oplus W_k$;

(ii) *Cada W_i é invariante sob T;*

(iii) *Se T_i é o operador induzido sobre W_i por T, então o polinômio minimal de T_i é $p_i^{r_i}$.*

Lema 1.40 *Sejam T e S transformações lineares em um espaço vetorial V de dimensão finita satisfazendo $[\ldots,[[S,\underbrace{T]T],\ldots,T]}_{n} = 0$, para algum n, (aqui $[\ ,\ ]$ é o produto de Lie). Sejam p um polinômio e*

$$V_{pT} = \{v \in V : p(T)^m(v) = 0, \;\; para\ algum\ m\}.$$

Então V_{pT} é invariante sob S.

De posse dos resultados acima, podemos demonstrar o seguinte:

Teorema 1.41 *Seja L uma álgebra de Lie nilpotente de transformações lineares em um espaço vetorial V de dimensão finita. Então podemos decompor*

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r,$$

onde os subespaços V_i, $i = 1, 2, \ldots, r$, são invariantes sob L e o polinômio minimal da restrição de cada $T \in L$ sobre V_i é uma potência de um polinômio irredutível.

Demonstração. Se o polinômio minimal de cada $T \in L$ é uma potência de um polinômio irredutivel, não há o que demonstrar. Caso contrário, pelo Teorema da Decomposição Primária, para cada $T \in L$ temos a seguinte decomposição:

$$V = V_{p_1T} \oplus V_{p_2T} \oplus \cdots \oplus V_{p_kT},$$

onde p_i, $i = 1, 2, \ldots, k$, são polinômios irredutíveis, $V_{p_iT} \neq 0$, $k > 1$ e existe m, tal que $(p_i(T))^m(V_{p_iT}) = 0$, para cada i.

Como L é nilpotente, pelo Teorema de Engel (1.38), todos os elementos de L são ad-nilpotentes. Logo vale o Lema 1.40, ou seja, dado $S \in L$, temos $S(V_{p_iT}) \subseteq V_{p_iT}$.

Se o polinômio minimal da restrição de cada $S \in L$ a V_{p_iT} é uma potência de polinômio irredutivel, o teorema está demonstrado. Caso contrário, temos, para cada $S \in L$, a seguinte decomposição

$$V_{p_iT} = V_{p_{i_1}S} \oplus V_{p_{i_2}S} \oplus \cdots \oplus V_{p_{i_t}S},$$

onde p_{i_j} é um polinômio irredutível, $V_{p_{i_j}S} \neq 0$, $t > 1$, e existe r tal que $(p_{i_j}(S))^r(V_{p_{i_j}T}) = 0$.

Novamente pelo Lema 1.40, os subespaços $V_{p_{i_j}T}$ são invariantes sob os elementos de L. Portanto, usando indução sobre a dimensão de V, temos o resultado desejado.

$\square$

Definição 1.42 *Seja L uma álgebra de Lie de transformações lineares em um espaço vetorial V sobre um corpo algebricamente fechado F. Então a aplicação $\alpha : T \longmapsto \alpha(T)$ de L no corpo base F é chamada um peso se existe um vetor não-nulo $v \in V$ tal que $(T - \alpha(T)I)^m(v) = 0$, para todo $T \in L$ e algum m (dependendo de v e T).*

O conjunto de vetores satisfazendo esta condição, juntamente com o vetor nulo, é um subespaço V_α, chamado **espaço de peso** de V correspondente ao peso α. Os escalares $\alpha(T)$ são chamados *valores de peso*.

Observe que os valores de peso são os autovalores dos elementos da álgebra.

Exemplo 1.43 *Considere L a álgebra de Lie do Teorema 1.41 sobre um corpo algebricamente fechado. O espaço vetorial V pode ser decomposto como*

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r,$$

onde para cada $T \in L$ e cada $i = 1, 2, \ldots, r$, podemos associar o escalar $\alpha_i(T)$ tal que $(\lambda - \alpha_i(T))^k$ é o polinômio minimal de T restrita ao subespaço V_i. Então, a aplicação $\alpha_i : T \longmapsto \alpha_i(T)$ de L em F é claramente um peso e ainda temos $V_{\alpha_i} = V_i$, $i = 1, 2, \ldots, r$.

Lema 1.44 (Fitting) *Seja T uma transformação linear em um espaço vetorial V de dimensão finita. Então V pode ser decomposto como $V = V_{0T} \oplus V_{1T}$, onde V_{0T} e V_{1T} são invariantes sob T, a transformação induzida em V_{0T} é nilpotente e a transformação induzida em V_{1T} é um isomorfismo. Ainda,*

$$V_{1T} = \bigcap_{i=1}^{\infty} T^i(V) \ \text{ e } \ V_{0T} = \{v \in V : T^i(v) = 0, \ \text{para algum } i\}.$$

Demonstração. Temos $V \supseteq T(V) \supseteq T^2(V) \supseteq \cdots$. Portanto existe um inteiro positivo r tal que $T^r(V) = T^{r+1}(V) = \cdots$. Assim, $T^r(V) = \bigcap_{i=1}^{\infty} T^i(V)$. Vamos denotar $T^r(V) = V_{1T}$.

Seja $B_i = \{v \in V : T^i(v) = 0\}$. Então, $B_1 \subseteq B_2 \subseteq \cdots$, e existe um inteiro positivo s tal que $B_s = B_{s+1} = \cdots$. Temos $B_s = \{v \in V : T^i(v) = 0 \ \text{ para algum } i\}$. Denote $B_s = V_{0T}$.

Tome $t = max(r, s)$. Então $V_{0T} = B_t$ e $V_{1T} = T^t(V)$. Seja $x \in V$. Temos $T^t(x) = T^{2t}(y)$, para algum $y \in V$, pois $T^t(V) = T^{2t}(V)$.

Podemos escrever $x = (x - T^t(y)) + T^t(y)$. Temos $T^t(y) \in V_{1T}$, enquanto $T^t(x - T^t(y)) = T^t(x) - T^{2t}(y) = 0$, donde $x - T^t(y) \in V_{0T}$. Portanto, segue $V = V_{0T} + V_{1T}$.

Agora, tome $v \in V_{0T} \cap V_{1T}$. Como $v \in V_{1T}$, então $v = T^t(w)$, para algum $w \in V$. Por outro lado, $v \in V_{0T}$ nos dá $T^t(v) = 0$. Com isso, $T^{2t}(w) = T^t(T^t(w)) = T^t(v) = 0$. Isto implica $w \in V_{0T} = B_t$ e $T^t(w) = 0$. Logo, $v = 0$ e $V_{0T} \cap V_{1T} = 0$, donde $V = V_{0T} \oplus V_{1T}$.

Como $V_{0T} = B_t$, temos $T^t = 0$ em V_{0T}, mostrando que T restrita a V_{0T} é nilpotente. Ainda, $V_{1T} = T^t(V) = T^{t+1}(V) = T(V_{1T})$ e temos que T é sobrejetiva em V_{1T}. Logo, T restrita a V_{1T} é um isomorfismo.

$\square$

O subespaço V_{0T} no Lema de Fitting é chamado **componente nula de Fitting** de V relativa a T.

Definição 1.45 *Dada uma álgebra de Lie de transformações lineares L, definimos a Componente Nula de Fitting de V relativa a L como o subespaço*

$$V_0 = \{v \in V : T^i(v) = 0, \ \textit{para todo } T \in L \textit{ e algum } i \textit{ (dependendo de } T \textit{ e } v)\}.$$

Observação 1.46 *Se a Componente Nula de Fitting relativa a L é diferente de zero, então a função nula é um peso de L.*

Suponhamos F um corpo de característica zero, L a álgebra de Lie da Definição 1.42 e seja α um peso. Conforme as discussões anteriores, para cada $v_\alpha \in V_\alpha$, temos que $(T - \alpha(T)I)^m(v_\alpha) = 0$, para algum m dependendo de T. Isto implica que o único autovalor da restrição de T em V_α é $\alpha(T)$.

Temos também que em V_α existe um vetor não nulo v tal que $T(v) = \alpha(T)v$, para todo $T \in L$. Como dados T e S pertencentes a L, temos $T + S \in L$, então $(T + S)(v) = \alpha(T + S)v$.

Por outro lado, $(T + S)(v) = T(v) + S(v) = \alpha(T)v + \alpha(S)v = (\alpha(T) + \alpha(S))v$. Logo $\alpha(T + S) = \alpha(T) + \alpha(S)$.

Do mesmo modo, se $k \in F$, temos $(kT)(v) = \alpha(kT)(v)$ e $k(T(v)) = k(\alpha(T)v)$, logo $\alpha(kT) = k(\alpha(T))$.

Portanto, os pesos de uma álgebra de Lie são funcionais lineares.

Lembrando que o subgrupo aditivo de uma álgebra de Lie L é um espaço vetorial, podemos enunciar o seguinte teorema.

Teorema 1.47 *Seja D uma álgebra de derivações de uma álgebra de Lie L de dimensão finita. Se D é nilpotente, então*

$$L = \bigoplus_{\alpha} L_\alpha,$$

onde os L_α são os espaços de peso, relativos a D.

Demonstração. A demonstração é imediata usando o Teorema 1.41 e o Exemplo 1.43, uma vez que D é uma álgebra de Lie de transformações lineares nilpotente.

□

Lema 1.48 *Seja δ uma derivação em uma álgebra de Lie L e seja F o corpo base de L. Se $\alpha,\beta \in F$ e $x,y \in L$, então*

$$(\delta-(\alpha+\beta)I)^m([x,y]) = \sum_{n=0}^{m} \binom{m}{n} [(\delta-\alpha I)^n(x),(\delta-\beta I)^{m-n}(y)],$$

para todo m inteiro positivo.

Usaremos o lema acima para demonstrar o próximo resultado, sua demonstração pode ser encontrada em [18].

Proposição 1.49 *Seja D uma álgebra de derivações de uma álgebra de Lie L de dimensão finita. Suponha D nilpotente e considere $L = \bigoplus_{\alpha} L_\alpha$ a decomposição de L em espaços de peso relativa a D. Sejam L_α e L_β espaços de peso determinados por D correspondentes aos pesos α e β, respectivamente. Então,*

$$\begin{cases} [L_\alpha, L_\beta] \subseteq L_{\alpha+\beta}, & \text{se } \alpha+\beta \text{ é um peso} \\ [L_\alpha, L_\beta] = 0, & \text{se } \alpha+\beta \text{ não é um peso} \end{cases}.$$

Demonstração. Consideremos $\delta \in D$ e sejam $x \in L_\alpha$, $y \in L_\beta$ tais que $(\delta-\alpha(\delta)I)^r(x) = 0$ e $(\delta-\beta(\delta)I)^s(y) = 0$, onde r e s são inteiros positivos. Por simplicidade, escreveremos α para $\alpha(\delta)$ e β para $\beta(\delta)$.

Devemos mostrar que existe um inteiro positivo m tal que

$$(\delta-(\alpha+\beta)I)^m([x,y]) = 0$$

quando $\alpha+\beta$ é um peso.

Pelo lema anterior, temos

$$(\delta-(\alpha+\beta)I)^m([x,y]) = \sum_{n=0}^{m} \binom{m}{n} [(\delta-\alpha I)^n(x),(\delta-\beta I)^{m-n}(y)].$$

Portanto, basta tomar m maior que $r+s$ para que o lado direto da igualdade seja zero. Por outro lado, se $\alpha+\beta$ não é um peso, devemos ter $L_{\alpha+\beta} = 0$.

□

Observação 1.50 *Dada uma álgebra de derivações D nilpotente de uma álgebra de Lie L de dimensão finita, temos que os pesos α de L relativos a D são funcionais lineares, ou seja, $\alpha \in D^*$, onde D^* é o espaço dual de D.*

Seja A o grupo aditivo de D^* gerado pelos pesos de L. Definindo $L_b = 0$, se $b \in D^*$ e b não é um peso, temos que vale $[L_a, L_b] \subseteq L_{a+b}$, para todo $a, b \in D^*$. Portanto, como A é um grupo abeliano, o Teorema 1.47 junto com a Proposição 1.49 garante que L é uma álgebra de Lie A-graduada.

1.6 Módulos e Produto Tensorial

Para os nossos objetivos, um R-módulo M (o qual daremos a definição rigorosa a seguir) pode ser considerado como uma generalização do conceito de espaço vetorial, onde ao invés de exigirmos que os escalares pertençam a um corpo F exigimos apenas que pertençam a um anel R. Diante disso, dado um automorfismo φ de um R-módulo M é natural investigarmos propriedades de M estudando subgrupos M_i de M com a seguinte propriedade: para todo $x \in M_i$ existe $r_i \in R$ tal que $x^\varphi = r_i \cdot x$. Os subgrupos M_i são os análogos dos autoespaços e os r_i dos autovalores de uma transformação linear.

Pretendemos extrair resultados sobre um anel de Lie L que admite um automorfismo de ordem n via um R-módulo $\widetilde{L}$, onde R é um anel conveniente. Faremos isto usando propriedades dos subgrupos de $\widetilde{L}$ de mesma natureza dos M_i descritos acima. A construção de $\widetilde{L}$ se dará por meio do produto tensorial entre L e o anel $\mathbb{Z}[\omega]$ (que será definido adiante). As discussões sobre módulos e produto tensorial tratadas aqui podem ser encontradas em [2] e [9].

<u>***R*-Módulos**</u>

Definição 1.51 *Seja R um anel (não necessariamente abeliano e com unidade). Um R-módulo à esquerda (ou um módulo à esquerda sobre R) é um conjunto M que satisfaz os seguintes axiomas:*

(i) *M possui uma operação binária $(M, +)$ em relação a qual M é um grupo abeliano;*

(ii) *Existe uma ação de R em M (isto é, $R \times M \longrightarrow M$) tal que $(r, m) \mapsto rm$, para todo $r \in R$ e para todo $m \in M$, a qual satisfaz:*

  (a) *$(r+s)m = rm + sm$, para todo $r, s \in R$, $m \in M$;*

  (b) *$(rs)m = r(sm)$, para todo $r, s \in R$, $m \in M$;*

(c) *$r(m+n) = rm + rn$, para todo $r \in R$, $m,n \in M$.*

Se o anel R tem unidade impomos um axioma adicional:

(d) *$1m = m$, para todo $m \in M$.*

Definição 1.52 *Seja R um anel e seja M um R-módulo à esquerda. Um R-submódulo à esquerda de M é um subgrupo N de M o qual é fechado sob a ação dos elementos do anel, isto é, $rn \in N$, para todo $r \in R$, $n \in N$.*

Analogamente podemos definir um R-módulo e R-submódulo à direita. Neste trabalho R representa um anel abeliano e usaremos apenas o termo R-módulo M para indicar que M é um módulo à esquerda e à direita com $rm = mr$.

O próximo exemplo mostra que um grupo abeliano pode ser considerado naturalmente como um $\mathbb{Z}$-módulo.

Exemplo 1.53 *Seja A um grupo abeliano e escreva a operação de A como $+$. Podemos considerar A como um $\mathbb{Z}$-módulo definindo a ação de $\mathbb{Z}$ da seguinte forma: para todo $n \in \mathbb{Z}$ e $a \in A$ definimos*

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{\text{(n cópias de a)}}, \ se\ n > 0 \\ 0, \ se\ n = 0 \\ \underbrace{-a - a - \cdots - a}_{\text{(n cópias de -a)}}, \ se\ n < 0 \end{cases} .$$

Lembrando que o grupo aditivo de um anel de Lie L é abeliano, concluímos que L pode ser considerado como um $\mathbb{Z}$-módulo.

Definição 1.54 *Sejam M e N R-módulos. Uma aplicação φ é um homomorfismo de R-módulo (ou apenas homomorfismo, quando não houver risco de confusão) se*

$$\varphi(rx + y) = r\varphi(x) + \varphi(y),$$

para todos $x, y \in M$ e todo $r \in R$.

Os R-módulos M e N são ditos *isomorfos* quando φ é um isomorfismo, ou seja, quando φ é um homomorfismo injetivo e sobrejetivo.

Definição 1.55 *Dizemos que um R-módulo F é* ***livre*** *sobre o subconjunto A de F se para todo elemento não nulo $x \in F$, existem elementos únicos e não nulos $r_1, r_2, \ldots, r_n \in R$ e $a_1, a_2, \ldots, a_n \in A$ tais que $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, para algum inteiro positivo n. Neste caso dizemos que A é um conjunto de geradores livres de F.*

Na verdade, existe um teorema cuja demonstração pode ser encontrada em [2], o qual garante que dado um conjunto A, existe um R-módulo livre $F(A)$, que satisfaz a seguinte propriedade: se M é algum R-módulo e φ é uma função $\varphi : A \longrightarrow M$, então existe um único homomorfismo $\phi : F(A) \longrightarrow M$ tal que $\phi(a) = \varphi(a)$, para todo $a \in A$. Os elementos do R-módulo $F(A)$ são na verdade todas as combinações lineares da forma $r_1a_1 + r_2a_2 + \cdots + r_na_n$, onde $r_1, r_2, \ldots, r_n \in R$ e $a_1, a_2, \ldots, a_n \in A$, para algum inteiro positivo n.

Produto Tensorial

Suponha que R seja um subanel de um anel S. Dado um R-módulo M é natural perguntar se M pode ser considerado como um S-módulo ou ainda se existe um S-módulo que contenha uma cópia isomorfa de M. O produto tensorial que será definido a seguir permite em certos casos definir um S-módulo que contenha uma cópia isomorfa de M. Este será o nosso objetivo agora, construir um R-módulo $\widetilde{L}$ (R conveniente) que contenha uma cópia isomorfa de um anel de Lie L admitindo um automorfismo de ordem finita.

Sejam A e B dois R-módulos. O **produto tensorial** $A \otimes_R B$ é definido como o grupo quociente do R-módulo livre gerado pelos geradores livres $a \otimes b, a \in A, b \in B$, pelo R-submódulo gerado por todos elementos da forma

$$\begin{gathered} r(a \otimes b) - ra \otimes b, \;\; ra \otimes b - a \otimes rb, \\ a \otimes (b_1 + b_2) - (a \otimes b_1 + a \otimes b_2), \\ (a_1 + a_2) \otimes b - (a_1 \otimes b + a_2 \otimes b), \end{gathered}$$

onde $r \in R; a, a_1, a_2 \in A; b, b_1, b_2 \in B$.

Equivalentemente podemos considerar o produto tensorial como o conjunto de todas as somas

$$\left\{ \sum r_{a,b} a \otimes b : a \in A, b \in B \right\}$$

onde identificamos os elementos

$$\begin{gathered} r(a \otimes b) = ra \otimes b = a \otimes rb, \\ a \otimes (b_1 + b_2) = (a \otimes b_1 + a \otimes b_2), \\ (a_1 + a_2) \otimes b = (a_1 \otimes b + a_2 \otimes b). \end{gathered}$$

Neste trabalho, usaremos apenas um exemplo de produto tensorial e alguns conceitos básicos desta teoria. Maiores detalhes sobre este assunto podem ser encontrados em [2] e [9].

Dada uma raiz n-ésima da unidade ω, podemos construir o anel

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

onde $\phi(n)$ é a Função de Euler. A soma e o produto são os usuais de números complexos.

Seja L um anel de Lie. Como $\mathbb{Z}[\omega]$ e L são $\mathbb{Z}$-módulos, podemos definir o produto tensorial $L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$ que denotaremos apenas por $L \otimes \mathbb{Z}[\omega]$.

De fato, $L \otimes \mathbb{Z}[\omega]$ é um $\mathbb{Z}[\omega]$-módulo, definindo o produto

$$k \cdot a \otimes b = a \otimes k \cdot b,$$

para todo $k \in \mathbb{Z}[\omega]$ e $a \otimes b \in L \otimes \mathbb{Z}[\omega]$.

Também podemos considerar $L \otimes \mathbb{Z}[\omega]$ como um anel de Lie, definindo o produto como

$$[a_1 \otimes b_1, a_2 \otimes b_2] = [a_1, a_2] \otimes b_1 b_2. \tag{1-2}$$

O anel de Lie L, pode ser imerso em $L \otimes \mathbb{Z}[\omega]$ pela aplicação $a \longmapsto a \otimes 1$.

Dado um automorfismo φ de ordem finita n de um anel de Lie L, podemos considerar φ como um automorfismo de $L \otimes \mathbb{Z}[\omega]$ fazendo φ agir de forma trivial em $\mathbb{Z}[\omega]$, ou seja, $(a \otimes b)^{\varphi} = a^{\varphi} \otimes b$, para todo $a \otimes b \in L \otimes \mathbb{Z}[\omega]$.

Lema 1.56 *Considerando $\widetilde{L} = L \otimes \mathbb{Z}[\omega]$ o anel de Lie definido acima e φ um automorfismo de ordem finita n do anel de Lie L agindo em $\widetilde{L}$ da forma descrita anteriormente, temos as seguintes propriedades:*

(i) $C_{\widetilde{L}}(\varphi) = C_L(\varphi) \otimes \mathbb{Z}[\omega]$;

(ii) $\widetilde{L}^{(s)} = L^{(s)} \otimes \mathbb{Z}[\omega]$;

(iii) $\gamma_s(p\widetilde{L}) = \gamma_s(pL) \otimes \mathbb{Z}[\omega]$.

Demonstração. Demonstração do item (i). A inclusão $C_L(\varphi) \otimes \mathbb{Z}[\omega] \subseteq C_{\widetilde{L}}(\varphi)$ é imediata. Para demonstrar a inclusão contrária observe que

$$\widetilde{L} = \bigoplus_{i=0}^{\phi(n)-1} L \otimes \mathbb{Z}\omega^i.$$

Sendo assim, é suficiente demonstrar que $C_{\widetilde{L}}(\varphi) \cap L \otimes \mathbb{Z}\omega^i = C_L(\varphi) \otimes \mathbb{Z}\omega^i$, onde $i = 0, \ldots, \phi(n) - 1$. Por outro lado, $C_{\widetilde{L}}(\varphi) \cap L \otimes 1 = C_L(\varphi) \otimes 1$, o que implica

$$C_{\widetilde{L}}(\varphi) \cap L \otimes \mathbb{Z} = C_L(\varphi) \otimes \mathbb{Z},$$

pois $L \otimes \mathbb{Z} = L \otimes 1$, uma vez que $\ell \otimes m = m\ell \otimes 1$, para todo $\ell \in L$ e todo $m \in \mathbb{Z}$. Na verdade, temos $L \otimes \mathbb{Z}\omega^i = L \otimes \omega^i$, pelo mesmo argumento.

Diante disso, dado $\widetilde{\ell} \in C_{\widetilde{L}}(\varphi) \cap L \otimes \mathbb{Z}\omega^i$ podemos considerar $\widetilde{\ell} = \ell \otimes \omega^i$, para algum $\ell \in L$. Mas

$$\omega^{n-i}\widetilde{\ell} = \ell \otimes 1 \in C_{\widetilde{L}}(\varphi),$$

que implica $\ell \in C_L(\varphi)$. Portanto, $\ell \otimes \omega^i \in C_L(\varphi) \otimes \mathbb{Z}\omega^i$ e consequentemente $C_{\widetilde{L}}(\varphi) \cap L \otimes \mathbb{Z}\omega^i = C_L(\varphi) \otimes \mathbb{Z}\omega^i$, para todo $i = 0, \ldots, \phi(n) - 1$.

Demonstração do item (ii). Usando a definição do produto em $\widetilde{L}$ e lembrando que o anel $\mathbb{Z}[\omega]$ possui identidade multiplicativa, é fácil verificar a igualdade

$$\widetilde{L}^{(1)} = L^{(1)} \otimes_{\mathbb{Z}} \mathbb{Z}[\omega],$$

uma vez que $\widetilde{L}^{(1)} = [\widetilde{L}, \widetilde{L}]$ é o ideal gerado pelo conjunto $\{[x, y] : x, y \in \widetilde{L}\}$.

Portanto, como $\widetilde{L}^{(s)} = [\widetilde{L}^{(s-1)}, \widetilde{L}^{(s-1)}]$, o resultado segue por indução sobre s.

Demonstração do item (iii). A demonstração é análoga ao item (ii), uma vez que, $\gamma_2(p\widetilde{L}) = (\widetilde{pL})^{(1)}$ e lembrando que $\gamma_s(p\widetilde{L}) = [\gamma_{s-1}(p\widetilde{L}), \widetilde{L}]$.

$\square$

CAPÍTULO 2

Automorfismos de Anéis de Lie

O objetivo principal deste capítulo é demonstrar um teorema devido a Higman, Kreknin e Kostrikin encontrado em [9], o qual afirma que se um anel de Lie admite um automorfismo regular de ordem prima p, então ele é nilpotente e sua classe de nilpotência é limitada por um número $h(p)$.

O roteiro para a demonstração consta basicamente de duas etapas: a primeira delas consiste em demonstrar o resultado para o caso em que o anel de Lie é solúvel, e a segunda etapa demonstrar que um anel de Lie é solúvel quando admite um automorfismo regular de ordem p.

A técnica utilizada permitirá enunciar outra versão do teorema, conhecida como versão combinatorial. Essa nova versão será de grande importância para extrair resultados sobre automorfismos quase regulares, que é o tema do próximo capítulo.

Dado um automorfismo φ de um anel de Lie L, frequentemente usaremos o tensor $\widetilde{L} = L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$, onde podemos assumir que φ age de forma natural em $\widetilde{L}$, do seguinte modo, $(\ell \otimes b)^{\varphi} = \ell^{\varphi} \otimes b$, para todo $\ell \in L$ e $b \in \mathbb{Z}[\omega]$.

2.1 Automorfismos Regulares de Anéis de Lie Solúveis

O resultado a ser alcançado afirma que se φ é um automorfismo de ordem prima p de um anel de Lie L, então, para todo número natural $s \geq 1$, temos

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

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

Por outro lado, conforme mostramos no Capítulo 1, dados um anel de Lie L e $\varphi \in AutL$, o produto tensorial $\widetilde{L} = L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$ também é um anel de Lie e valem as seguintes igualdades:

(i) ${}_{id}\langle C_{\widetilde{L}}(\varphi)\rangle = {}_{id}\langle C_L(\varphi)\rangle \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$;

(ii) $\widetilde{L}^{(s)} = L^{(s)} \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$;

(iii) $\gamma_s(p\widetilde{L}) = \gamma_s(pL) \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$.

Portanto, se

$$\gamma_{f+1}(p\widetilde{L}) \subseteq {}_{id}\langle C_{\widetilde{L}}(\varphi)\rangle + \widetilde{L}^{(s)},$$

então

$$\gamma_{f+1}(pL)\otimes 1 = \gamma_{f+1}(p\widetilde{L}) \cap L\otimes 1 \subseteq$$
$$\subseteq \left({}_{id}\langle C_{\widetilde{L}}(\varphi)\rangle + \widetilde{L}^{(s)}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[\omega] \cap L\otimes 1 = \left({}_{id}\langle C_L(\varphi)\rangle + L^{(s)}\right)\otimes 1,$$

ou seja, podemos supor sem perda de generalidade que $L = \widetilde{L}$.

As definições a seguir são fundamentais às técnicas aplicadas aos resultados principais.

Definição 2.1 *O subgrupo aditivo do anel de Lie L dado por*

$$^{i}L = \{\ell \in L :\ \ell^{\varphi} = \omega^{i}\ell\}$$

*é chamado φ-**componente** de L com respeito a ω^i. Os elementos de uma φ-componente são chamados φ-**homogêneos**.*

Definição 2.2 *Dado um automorfismo φ de ordem n de um anel de Lie L. Um ideal I de L é dito φ-**homogêneo** se $I = \sum_{i=0}^{n-1} I \cap {}^{i}L$.*

Lema 2.3 *Seja L um anel de Lie e φ um automorfismo de ordem n. Então:*

(i) $nL \subseteq {}^{0}L + {}^{1}L + \cdots + {}^{n-1}L$.

(ii) *Se $\ell_0 + \ell_1 + \cdots + \ell_{n-1} = 0$, onde $\ell_i \in {}^{i}L$, então $n\ell_j = 0$, para todo $j = 0, 1, \ldots, n-1$.*

(iii) *Se o grupo aditivo de L não tem n-torção, (ou seja, para algum $\ell \in L$ a igualdade $n\ell = 0$ implica $\ell = 0$), então a soma das φ-componentes é direta.*

Demonstração. Demonstração do item (i). Para cada $a \in L$ e cada $i = 0,1,\ldots,n-1$, definimos ${}^{i}a = \sum_{s=0}^{n-1} \omega^{-is} a^{\varphi^s}$. Temos que ${}^{i}a \in {}^{i}L$. De fato,

$$\begin{aligned} ({}^{i}a)^{\varphi} &= \left(\sum_{s=0}^{n-1} \omega^{-is} \cdot a^{\varphi^s} \right)^{\varphi} &&= \sum_{s=0}^{n-1} \omega^{-is} \cdot a^{\varphi^{s+1}} = \\ &= \omega^{i} \cdot \sum_{s=0}^{n-1} \omega^{-i(s+1)} \cdot a^{\varphi^{s+1}} &&= \omega^{i} \cdot \sum_{r=0}^{n-1} \omega^{-ir} \cdot a^{\varphi^{r}} = \omega^{i} \cdot {}^{i}a, \end{aligned} \tag{2-1}$$

onde fazemos $r = s+1$. Por outro lado,

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

pois, para $s = 0$, temos $\sum_{i=0}^{n-1} \omega^{0} = n$ e, para $s \neq 0 \ (mod\ n)$, temos $\sum_{i=0}^{n-1} \omega^{is} = 0$, uma vez que

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

ou seja,

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

Como $\omega^{s} \neq 1$, temos que $\sum_{i=0}^{n-1} \omega^{is} = 0$.

Demonstração do item (ii). Aplicando φ^{k}, $\quad k = 0,1,\ldots,n-1$, em $\sum_{i=0}^{n-1} \ell_i = 0$, temos:

$$\begin{array}{ccccccccc} \ell_0 & + & \ell_1 & + & \ell_2 & + & \ldots & + & \ell_{n-1} = 0 \\ \ell_0 & + & \omega^{1} \cdot \ell_1 & + & \omega^{2} \cdot \ell_2 & + & \ldots & + & \omega^{n-1} \cdot \ell_{n-1} = 0 \\ \ell_0 & + & \omega^{2} \cdot \ell_1 & + & \omega^{4} \cdot \ell_2 & + & \ldots & + & \omega^{2(n-1)} \cdot \ell_{n-1} = 0 \\ \vdots & & \vdots & & & & \vdots & & \\ \ell_0 & + & \omega^{n-1} \cdot \ell_1 & + & \omega^{2(n-1)} \cdot \ell_2 & + & \ldots & + & \omega^{(n-1)(n-1)} \cdot \ell_{n-1} = 0. \end{array}$$

Para mostrar que $n \cdot \ell_i = 0$, para algum i, multiplicamos cada uma dessas equações por uma potência de ω apropriada para fazer o coeficiente de ℓ_i igual a 1 e então somamos todas as n equações. Observando a soma destas equações, vemos que o coeficiente de cada ℓ_i é exatamente $\sum_{k=0}^{n-1} \omega^{ik}$. Então torná-lo igual a 1 é o mesmo que multiplicá-lo por potências apropriadas de forma a torná-lo $\sum_{k=0}^{n-1} \omega^{ik} \cdot \omega^{-ik}$. Com isso, fazemos com que o coeficiente de ℓ_j $(j \neq i)$ seja $\sum_{k=0}^{n-1} \omega^{(j-i)k}$, o qual é igual 0 conforme demonstramos no final do item (i).

Demonstração do item (iii). Como L não tem n-torção, se tivermos

$$\ell_0 + \ell_1 + \cdots + \ell_{n-1} = a_0 + a_1 + \cdots + a_{n-1},$$

onde $\ell_i, a_i \in {}^iL$, então

$$(\ell_1 - a_1) + \cdots + (\ell_{n-1} - a_{n-1}) = 0$$

e, pelo item (ii), temos $n(\ell_j - a_j) = 0$, para todo $j = 0, 1, \ldots, n-1$. Portanto $\ell_j = a_j$.

$\square$

Lema 2.4 *Para todos i e j, temos*

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

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

Demonstração. Para $a \in {}^iL$ e $b \in {}^jL$, temos

$$[a, b]^{\varphi} = [a^{\varphi}, b^{\varphi}] = [\omega^i \cdot a, \omega^j \cdot b] = \omega^{i+j} \cdot [a, b]$$

e, assim, $[a, b] \in {}^{i+j}L$, como desejado.

$\square$

Dado um automorfismo φ de ordem n de um anel de Lie L, usando o Lema 2.4 e observando que a φ-componente ${}^0L$ é o subanel dos pontos fixos de φ, concluímos que o grupo aditivo do ideal ${}_{id}\langle C_L(\varphi)\rangle$ é gerado pelos comutadores simples que possuem um subcomutador $[{}^{i_1}x_1, \ldots, {}^{i_r}x_r]$, onde ${}^{i_j}x_j \in {}^{i_j}L$ e $i_1 + \cdots + i_r \equiv 0$ $(mod\ n)$.

Lema 2.5 *Seja p um número primo e sejam $i_1, \ldots, i_k$ elementos não nulos de $\mathbb{Z}_p$ (não necessariamente distintos). Seja M o conjunto*

$$M = \left\{ \sum_{s \in S} i_s : S \subseteq \{1, 2, \ldots, k\} \right\}$$

onde, por definição, a soma é 0 *para* $S = \emptyset$. *Então ou* $M = \mathbb{Z}_p$ *ou* $| M | \geq k+1$.

Demonstração. A demonstração será feita por indução sobre k. Denotaremos por $M(s)$ o conjunto de todas as somas envolvendo $\{i_1, \ldots, i_s\}$. Para $k = 1$, temos $|M(1)| = |\{0, i_1\}| = 2$, pois $i_1 \neq 0$.

Como $M(k) \subseteq M(k+1)$, se $M(k) = \mathbb{Z}_p$ então $M(k+1) = \mathbb{Z}_p$. Sendo assim basta provar o caso em que $|M(k)| \geq k+1$. Para isto suponha que alguma soma $\sigma + i_{k+1}$, onde $\sigma \in M(k)$, não pertence a $M(k)$. Então

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

Por outro lado, se toda soma $\sigma + i_{k+1}$ pertence a $M(k)$, então, por recorrência e tomando $\sigma = 0$, temos $i_{k+1},\ 2i_{k+1},\ 3i_{k+1}, \ldots,\ (p-1)i_{k+1} \in M(k)$. Como $0, i_{k+1},\ 2i_{k+1},\ 3i_{k+1}, \ldots, (p-1)i_{k+1}$ são distintos (pois $\mathbb{Z}_p$ não possui subgrupos próprios e $i_1 \neq 0$), temos que $|M(k)| = |M(k+1)| = p$, ou seja $M(k+1) = \mathbb{Z}_p$.

$\square$

Mostraremos um resultado para o subanel $H = {}^0L + {}^1L + \cdots + {}^{p-1}L$ que afirma que para todo número natural s temos

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

onde $f = f(p,s)$.

Deveremos ser capazes de observar na demonstração deste resultado dois fatos:

1. Está sendo demonstrado um resultado mais geral, no qual H é considerado um anel de Lie $\mathbb{Z}_p$-graduado.

2. Como H contém pL, temos que o resultado também é valido para o subanel pL.

Estes fatos mais gerais que acabamos de comentar, permitirão enunciar a versão combinatorial do Teorema HKK [1].

Proposição 2.6 *Considere* $H = {}^0L + {}^1L + \cdots + {}^{p-1}L$. *Para todo número natural* $s \geq 1$, *temos*

(i) $[\gamma_n(H'), \underbrace{H, H, \ldots, H}_{p-1}] \subseteq \gamma_{n+1}(H') +_{id} \langle {}^0L \rangle$, $n \geq 1$;

[1]Como é conhecido o Corolário 2.16 devido à Higman, Kreknin e Kostrikin.

(ii) $\gamma_{(p-1)n+2}(H) \subseteq \gamma_{n+1}(H^{'}) +_{id} \langle {}^{0}L \rangle$, *$n \geq 0$;*

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

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

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

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

Assim, basta mostrar que

$$[{}^{i_0}c, {}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{p-1}}y_{p-1}] \in \gamma_{n+1}(H') +_{id} \langle {}^{0}L \rangle$$

para todo elemento φ-homogêneo ${}^{i_0}c \in \gamma_n(H') \cap {}^{i_0}L$ e ${}^{i_k}y \in {}^{i_k}L$.

Podemos assumir $i_r \neq 0$, para todo $r = 0, 1, \ldots, p-1$, pois, se $i_r = 0$ para algum r, teremos $[{}^{i_0}c, {}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{p-1}}y_{p-1}] \in {}_{id}\langle {}^{0}L \rangle$. Note também que, pelo Lema 1.22, toda permutação de elementos ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{p-1}}y_{p-1}$ não altera o comutador módulo o subgrupo $\gamma_{n+1}(H')$.

Pelo Lema 2.5, podemos arranjar os $p-1$ índices $i_1, i_2, \ldots, i_{p-1}$ de modo a obter qualquer elemento de $\mathbb{Z}_p$. Em particular podemos obter $-i_0$, ou seja, podemos escrever o comutador $[{}^{i_0}c, {}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{p-1}}y_{p-1}]$ como a soma de um comutador com segmento inicial em ${}^{0}L$ (consequentemente pertencendo à ${}_{id}\langle {}^{0}L \rangle$) e outros em $\gamma_{n+1}(H')$.

Demonstração do item (ii). A demonstração será feita por indução sobre n. Para $n = 0$, temos $\gamma_2(H) = [H, H] = \gamma_1(H')$ e para $n > 0$:

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

Agora, pela hipótese de indução e pelo item (i), temos:

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

conforme desejado.

Demonstração do item (iii). A demonstração será feita por indução sobre s. Para $s = 1$, temos $\gamma_2(H) = H'$ e, para $s > 1$, usando $\frac{(p-1)^s-1}{p-2} = (p-1)\frac{(p-1)^{s-1}-1}{p-2} + 1$ e o item (ii), temos:

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

Agora, usando a hipótese de indução no anel de Lie solúvel H', concluímos que

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

conforme desejado.

□

Teorema 2.7 *Se φ é um automorfismo regular de ordem prima p de um anel de Lie L, então, para todo número natural $s \geq 1$, temos*

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

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

Demonstração. A demonstração segue pela aplicação do item (iii) da Proposição 2.6, mediante as seguintes observações:

$$pL \subseteq H = {}^0L + {}^1L + \cdots + {}^{p-1}L \;\text{ e }\; H^{(s)} \subseteq L^{(s)}.$$

□

Teorema 2.8 (Kreknin, Kostrikin) *Se um anel de Lie L é solúvel de comprimento derivado s e admite um automorfismo regular φ de ordem prima p, então L é nilpotente e sua classe de nilpotência é no máximo* $\frac{(p-1)^s-1}{p-2}$.

Demonstração. Por hipótese, ${}^0L = 0$ e $L^{(s)} = 0$. Com isso, aplicando o Teorema 2.7 e o Lema 1.21, temos

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

Em particular isso implica que o grupo aditivo de $\gamma_{f(p,s)+1}(L)$ (que é abeliano) é um p-grupo, o qual é φ-invariante. Pelo Lema 1.12, se o grupo aditivo de $\gamma_{f(p,s)+1}(L)$, ou seja, se $\gamma_{f(p,s)+1}(L)$ não for igual a 0, o automorfismo φ deveria ter um ponto fixo não trivial, contrariando a hipótese. Portanto $\gamma_{f(p,s)+1}(L) = 0$, conforme desejado.

□

Anunciamos agora uma versão combinatorial do teorema anterior.

Teorema 2.9 *Sejam p um primo, s um número natural e seja $f = f(p,s) = \frac{(p-1)^s-1}{p-2}$. Se ${}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_{f+1}}y_{f+1}$ são alguns elementos de um anel de Lie com índices superiores arbitrários $i_1, i_2, \dots, i_{f+1} \in \mathbb{Z}$, então o comutador simples*

$$[{}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_{f+1}}y_{f+1}]$$

pode ser representado como uma combinação linear de comutadores, cada qual possuindo o mesmo conjunto de entradas ${}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_{f+1}}y_{f+1}$. Além disso, para cada comutador dessa combinação linear ou o comutador pertence a $L^{(s)}$ ou o comutador contém um subcomutador com seus índices superiores somando 0 módulo p.

Demonstração. Seja ω uma raiz p-ésima da unidade e seja F um anel de Lie livre sobre $\mathbb{Z}[\omega]$ com geradores livres ${}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_{f+1}}y_{f+1}$. Para cada $i = 1, 2, \dots, p-1$, denotamos por ${}^{i}F$ o subgrupo aditivo de F gerado por todos os comutadores nos geradores livres ${}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_{f+1}}y_{f+1}$, tais que a soma dos índices superiores de suas entradas é igual i módulo p.

Note que o grupo aditivo do ideal ${}_{id}\langle {}^{0}F \rangle$ é gerado por todos os comutadores nos elementos ${}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_{f+1}}y_{f+1}$ que possuem subcomutadores com índices superiores somando zero módulo p.

Definimos um automorfismo φ de ordem p de F colocando $\ell^{\varphi} = \omega^{i}\ell$, para todo $\ell \in {}^{i}F$, $i = 0, 1, \dots, p-1$, e estendendo a ação de φ para a soma $F = \sum_i {}^{i}F$ por linearidade.

Desta definição, temos que os subgrupos aditivos ${}^{i}F$ são as φ-componentes. Como o grupo aditivo F não possui torção, pelo item (iii) do Lema 2.3, temos

$$F = {}^{0}F \oplus {}^{1}F \oplus \dots \oplus {}^{p-1}F.$$

Pela Proposição 2.6, item (iii) (onde $H = F$), segue que:

$$[{}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_{f+1}}y_{f+1}] \in F^{(s)} + {}_{id}\langle {}^{0}F \rangle.$$

Como os ideais $F^{(s)}$ e ${}_{id}\langle {}^{0}F \rangle$ são multihomogêneos com respeito aos geradores livres ${}^{i_s}y_s$, então o resultado é verdadeiro para F. Agora, conforme discussão do Capítulo 1 sobre anéis de Lie livres, podemos definir uma bijeção (identidade) entre os geradores

${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{f+1}}y_{f+1}$ de F e os respectivos elementos de L e, em seguida, estender para um homomorfismo de F em L provando o resultado para L.

$\square$

2.2 Automorfismos Regulares de Anéis de Lie

Nesta seção demonstramos que se φ é um automorfismo de ordem n de um anel de Lie L, então $(nL)^{(f)} \subseteq {}_{id}\langle {}^0L\rangle$, onde $f = f(n) = 2^{n-1} - 1$. Agora, se demostrarmos para $\widetilde{L}$ temos

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

Assim, podemos assumir sem perda de generalidade que $L = \widetilde{L}$.

Ao contrário do que foi feito na seção anterior, primeiro demonstraremos o resultado na sua forma combinatorial.

Lema 2.10 *Suponha que a, b e c sejam números naturais tais que $1 \leq a, b, c \leq n-1$. Se $a + b \equiv c (mod\ n)$, então ou ambos $a > c$ e $b > c$ ou ambos $a < c$ e $b < c$.*

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

$\square$

Proposição 2.11 *Suponha que ω seja uma raiz n-ésima da unidade e que o anel de Lie H sobre $\mathbb{Z}[\omega]$ admita um automorfismo φ de ordem n, onde H é decomposto em soma direta de φ-componentes do seguinte modo:*

$$H = {}^0H \oplus {}^1H \oplus {}^2H \oplus \cdots \oplus {}^{n-1}H.$$

Então, para todo $k = 1, 2, \ldots, n-1$,

(i) $H^{(2^{k-1})} \cap {}^kH \subseteq \langle {}^{k+1}H, {}^{k+2}H, \ldots, {}^{n-1}H\rangle + {}_{id}\langle {}^0H\rangle$;

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

(iii) $H^{(2^{n-1}-1)} \subseteq {}_{id}\langle {}^0H\rangle$.

Demonstração. Demonstramos os ítens (i) e (ii) simultaneamente por indução sobre k.

Para $k=1$. Demonstração do item (i). Temos

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

Logo $H' \cap {}^1H$ é gerado por todos comutadores $[x,y]$ onde $x \in {}^iH$, $y \in {}^jH$ e $i+j \equiv 1\ (mod\ n)$. Se i ou j é igual a 0, temos $[x,y] \in {}_{id}\langle {}^0H\rangle$. Se ambos são maiores que 0, pelo Lema 2.10, ambos são maiores que 1 e assim $[x,y] \in \langle {}^2H, {}^3H, \ldots, {}^{n-1}H\rangle$.

Item (ii). Temos $H' = \bigoplus_{i=0}^{n-1} H' \cap {}^i H$ e do fato ${}^iH \subseteq \langle {}^2H, {}^3H, \ldots, {}^{n-1}H\rangle + {}_{id}\langle {}^0H\rangle$, para $i = 0,2,3,\ldots,n-1$, junto com o item (i), temos $H' \cap {}^iH \subseteq \langle {}^2H, {}^3H, \ldots, {}^{n-1}H\rangle + {}_{id}\langle {}^0H\rangle$, para todo i. Portanto, $H' \subseteq \langle {}^2H, {}^3H, \ldots, {}^{n-1}H\rangle + {}_{id}\langle {}^0H\rangle$.

Para $k>1$, provamos (i) primeiramente usando a hipótese de indução de (i) e (ii). O subanel $H^{(2^{k-1})} \cap {}^kH$ é gerado por todos comutadores $[x,y]$, onde $x \in H^{(2^{k-1}-1)} \cap {}^iH$, $y \in H^{(2^{k-1}-1)} \cap {}^jH$ e $i+j \equiv k\ (mod\ n)$. Se algum i,j é igual 0, então $[x,y] \in {}_{id}\langle {}^0H\rangle$. Se ambos são maiores que 0, então pelo Lema 2.10 ou ambos são maiores que k ou ambos são menores que k. No primeiro caso é imediato.

Já no segundo caso, aplicamos (ii) ao subanel $H^{(2^{k-1}-1)}$ o qual contém x e y:

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

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

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

Por repetidas aplicações da identidade de Jacobi $[a,[b,c]] = [a,b,c] - [a,c,b]$, todo comutador $[x,[u_1,u_2,\ldots,u_q]]$ pode ser expresso como combinação linear de comutadores simples da forma

$$[x,u_{\pi(1)},\ldots,u_{\pi(q)}], \ \ \text{onde} \ \ \pi \in S_q.$$

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

$$[x, v_1, v_2, \ldots, v_q], \;\; v_s \in {}^{j_s}H, \;\; j_s \geq k, \;\; \sum_{s=1}^{q} j_s \equiv j \;\; (mod\ n),$$

onde é satisfeito

$$i + j_1 + j_2 + \cdots + j_q \equiv k \;\; (mod\ n), \;\; \text{pois} \;\; i + j \equiv k \;\; (mod\ n).$$

Se tivermos $j_q = k$, então

$$i + j_1 + j_2 + \cdots + j_{q-1} \equiv 0 \;\; (mod\ n),$$

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

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

Se, no entanto, $j_q > k$, então claramente

$$i + j_1 + j_2 + \cdots + j_{q-1} \equiv t \not\equiv 0 \;\; (mod\ n)$$

e, pelo Lema 2.10, temos $t > k$. Assim,

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

Logo, em todos os casos, os comutadores $[x, v_1, v_2, \ldots, v_q]$ estão contidos em

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

Portanto, este subanel também contém $[x, y]$, como desejado.

Agora vamos provar o item (ii) usando a hipótese de indução para $k-1$ no anel de Lie $H^{(2^{k-1})}$:

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

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

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

como desejado.

A demonstração do item (iii) segue de (ii) colocando $k = n-1$.

$\square$

Antes de enunciar o próximo teorema, vamos relembrar a identidade para variedades solúveis, definidas pelas identidades

$$\delta_0(x) = x, \quad \delta_1 = [x_1, x_2], \quad \ldots, \quad \delta_{k+1} = [\delta_k(x_1, \ldots, x_{2^k}), \delta_k(x_{2^k+1}, \ldots, x_{2^{k+1}})].$$

Teorema 2.12 *Sejam n um número natural e $f(n) = 2^{2^{n-1}-1}$. Se ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{f(n)}}y_{f(n)}$ são alguns elementos de um anel de Lie arbitrário com índices superiores arbitrários $i_1, i_2, \ldots, i_{f(n)} \in \mathbb{Z}$, então o comutador*

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

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

Demonstração. A demonstração é análoga à demonstração do Teorema 2.9.

Seja ω uma raiz p-ésima da unidade e seja F um anel de Lie livre sobre $\mathbb{Z}[\omega]$ com geradores livres ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{f(n)}}y_{f(n)}$. Para cada $i = 1, 2, \ldots, n-1$, denotamos por ${}^{i}F$ o subgrupo aditivo de F gerado por todos os comutadores nos geradores livres ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{f(n)}}y_{f(n)}$, tais que a soma dos índices superiores de suas entradas é igual a i módulo n.

Note que o grupo aditivo do ideal ${}_{id}\langle {}^{0}F \rangle$ é gerado por todos os comutadores nos elementos ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{f(n)}}y_{f(n)}$ que possuem subcomutadores com índices superiores somando zero módulo n.

Definimos um automorfismo φ de F de ordem n colocando $\ell^{\varphi} = \omega^{i}\ell$, para todo $\ell \in {}^{i}F$, $i = 0, 1, \ldots, n-1$, e estendendo a ação de φ para a soma $F = \sum_i {}^{i}F$ por linearidade. Desta forma os subgrupos aditivos ${}^{i}F$ são as φ-componentes. Como o grupo aditivo F não possui torção, pelo item (iii) do Lema 2.3, temos

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

Pela Proposição 2.11, item (iii), segue que

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

$\square$

Teorema 2.13 *Se φ é um automorfismo de ordem finita n de um anel de Lie L, então*

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

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

Demonstração. Temos, pelo Lema 2.3, $nL \subseteq {}^0L + {}^2L + \cdots + {}^{n-1}L$ e, portanto, pelo Teorema 2.12, temos

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

$\square$

Corolário 2.14 *Suponha que o anel de Lie L admita um automorfismo regular de ordem finita n.*

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

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

Demonstração. Demonstração do item (i). Pelo Teorema 2.13, temos

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

Portanto,

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

e, juntamente com fato de L não possuir n-torção, obtemos $n^{2^{2^{n-1}-2}} L^{2^{n-1}-1} = 0$. Procedendo do mesmo modo, temos $L^{2^{n-1}-1} = 0$.

Demonstração do item (ii). Se $n = p$ é primo, o fato de $L^{2^{n-1}-1} \neq 0$ implica em $L^{2^{n-1}-1}$ ser um p-grupo abeliano não trivial. Logo, pelo Lema 1.12, φ possui um ponto fixo não trivial. Portanto, necessariamente $L^{2^{n-1}-1} = 0$.

$\square$

O teorema a seguir nos permite obter um limite superior em função de n para o comprimento derivado de um anel de Lie admitindo um automorfismo regular de ordem n.

Teorema 2.15 (Kreknin) *Se um anel de Lie L admite um automorfismo regular de ordem finita n, então L é solúvel e seu comprimento derivado não é maior que* $2^n - 2$.

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

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

Note que T é um ideal φ-invariante. Pelo Teorema 2.13,

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

onde $f(n) = 2^{2^{n-1}-1}$. Assim, $L^{(2^{n-1}-1)} \subseteq T$. Logo é suficiente provar que $T^{(2^{n-1}-1)} = 0$, uma vez que

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

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

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

onde $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ é a decomposição de n como um produto de potências de primos. Note que estes subgrupos de Sylow são subanéis φ-invariantes e $[x_i, x_j] = 0$ sempre que $x_i \in T_{p_i}$ e $x_j \in T_{p_j}$, com $i \neq j$. Então é suficiente provar que cada subanel T_{p_i} é solúvel de comprimento derivado no máximo $2^{n-1} - 1$.

Temos $n = p^k s$, $p \in \{p_1, p_2, \dots, p_r\}$ e $(p, s) = 1$. Podemos obter a seguinte decomposição $\langle\varphi\rangle = \langle\varphi\rangle_p \otimes \langle\varphi\rangle_{p'}$ onde $|\langle\varphi\rangle_p| = |\langle\varphi^s\rangle| = p^k$ e $|\langle\varphi\rangle_{p'}| = |\langle\varphi^{p^k}\rangle| = s$. Então $C_{T_p}(\varphi^{p^k}) = 0$, pois se $C_{T_p}(\varphi^{p^k}) = A \neq 0$, temos $C_A(\varphi^s) \neq 0$, uma vez que $|\langle\varphi^s\rangle| = p^k$ e A é φ^s-invariante (veja Lema 1.12). Logo $C_{T_p}(\varphi^{p^k}) \cap C_{T_p}(\varphi^s) = C_{T_p}(\varphi) \neq 0$, o que é uma contradição. Portanto, $C_{T_p}(\varphi^{p^k}) = 0$.

Assim T_p admite um automorfismo regular φ^{p^k} de ordem coprima com todos os elementos de seu grupo aditivo, logo pelo item (i) do Corolário 2.14, T_p é solúvel de comprimento derivado $\leq 2^{n-1} - 1$.

$\square$

Agora estamos prontos para obter um limite superior em função de p da classe de nilpotência de um anel de Lie admitindo um automorfismo regular de ordem prima p.

Corolário 2.16 (Higman, Kreknin e Kostrikin) *Se um anel de Lie admite um automorfismo regular de ordem prima p, então ele é nilpotente e sua classe de nilpotência é limitada por algum número $h(p)$, o qual depende somente de p e é no máximo $\frac{(p-1)^{2^{p-1}-1}-1}{p-2}$.*

Demonstração. Dado um anel de Lie L que admite um automorfismo de ordem prima p, temos pelo item (ii) do Corolário 2.14 que L é solúvel de comprimento derivado $\leq 2^{p-1}-1$ e, portanto, pelo Teorema 2.8, temos que L é nilpotente de classe no máximo $\frac{(p-1)^{2^{p-1}-1}-1}{p-2}$, conforme desejado. □

O corolário acima será chamado ao longo do texto de *Teorema HKK*. A função $h(p)$ do Teorema HKK é conhecida como *Função de Higman*.

Podemos também formular uma versão combinatorial do corolário acima, conhecida como versão combinatorial do Teorema HKK.

Corolário 2.17 *Para todo número primo p existe um número natural $h(p)$, dependendo somente de p e sendo no máximo $\frac{(p-1)^{2^{p-1}-1}-1}{p-2}$ tal que se ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{h(p)+1}}y_{h(p)+1}$ são alguns elementos de um anel de Lie arbitrário com índices superiores arbitrários $i_1, i_2, \ldots, i_{h(p)+1} \in \mathbb{Z}$, então o comutador simples*

$$[{}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{h(p)+1}}y_{h(p)+1}]$$

pode ser representado como uma combinação linear de comutadores, cada qual com o mesmo conjunto de entradas ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{h(p)+1}}y_{h(p)+1}$ e contendo um subcomutador com índices superiores com soma zero módulo p.

Demonstração. A demonstração pode ser obtida do Corolário 2.16 construindo um anel de Lie livre F, como foi feito nos Teoremas 2.9 e 2.12.

O Teorema 2.9 garante que

$$[{}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{h(p)+1}}y_{h(p)+1}] \in H^{(2^{p-1}-1)} + {}_{id}\langle {}^{0}F \rangle$$

e o Teorema 2.12 garante que

$$H^{(2^{p-1}-1)} \subseteq {}_{id}\langle {}^{0}F \rangle.$$

□

Usando a identidade de Jacobi $[a,[b,c]] = [a,b,c] - [a,c,b]$, podemos expressar todo comutador como uma combinação linear de comutadores simples, cada um com o mesmo conjunto de entradas. Isto permite "fortalecer" a conclusão do Corolário 2.17 no seguinte sentido:

Corolário 2.18 *Para todo número primo p existe um número natural $h(p)$, dependendo somente de p e sendo no máximo $\frac{(p-1)^{2^{p-1}-1}-1}{p-2}$ tal que se ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{h(p)+1}}y_{h(p)+1}$ são alguns elementos de um anel de Lie arbitrário com índices superiores arbitrários $i_1, i_2, \ldots, i_{h(p)+1} \in \mathbb{Z}$, então o comutador simples*

$$[{}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{h(p)+1}}y_{h(p)+1}]$$

pode ser representado como uma combinação linear de comutadores simples, cada qual com o mesmo conjunto de entradas ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_{h(p)+1}}y_{h(p)+1}$ e contendo um subcomutador com índices superiores com soma zero módulo p.

2.3 Automorfismos Semisimples

Nesta seção demonstramos algumas generalizações dos resultados obtidos nas duas seções anteriores. Suas demonstrações também podem ser encontradas em [11] e [17].

Um automorfismo φ de ordem n de um anel de Lie é dito semisimples se o subgrupo aditivo da sua extensão $\widetilde{L} = L \otimes \mathbb{Z}[\omega]$ é decomposto em soma direta

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

onde ${}^{i}\widetilde{L} = \{\ell \in \widetilde{L} : \ell^{\varphi} = \omega^{i}\ell\}$. Em outras palavras, o anel de Lie $\widetilde{L}$ é escrito como soma direta de suas φ componentes.

Chamaremos ω^i de autovalor de φ, mesmo que ${}^{i}L = 0$.

Por motivos já mencionados, consideraremos $L = \widetilde{L}$. O resultado principal desta seção é uma generalização do Teorema HKK.

Teorema 2.19 *Suponha que um anel de Lie L admite um automorfismo semisimples φ de ordem prima, com exatamente d autovalores distintos com φ-componentes não nulas e todos estes autovalores diferentes de 1 (isto é, o automorfismo é regular). Então o anel de Lie L é nilpotente de classe no máximo $\frac{d^{2^{d-1}-1}-1}{d-1}$.*

Os passos para sua demonstração são num certo sentido os mesmos da demonstração do Teorema HKK. Primeiro generalizaremos o Teorema 2.8 e em seguida o Teorema 2.15.

Teorema 2.20 *Suponha que um anel de Lie L admite um automorfismo semisimples φ de ordem prima, com exatamente d autovalores distintos com φ-componentes não nulas e todos estes autovalores diferentes de 1. Então*

(i) $[\gamma_k([L,L]),\underbrace{L,\ldots,L}_{d}] \subseteq \gamma_{k+1}([L,L])$, *para todo inteiro positivo k;*

(ii) $\gamma_{dk+2}(L) \subseteq \gamma_{k+1}([L,L])$, *para todo inteiro positivo k;*

(iii) $\gamma_{f(d,n)+1}(L) \subseteq L^{(n)}$, *para todo inteiro positivo n. Aqui* $f(d,n) = \dfrac{d^n-1}{d-1}$.

Demonstração. Provaremos apenas o item (i), as demonstrações dos demais são análogas às demonstrações dos itens (ii) e (iii) do Teorema 2.6, apenas trocando $p-1$ por d.

Demonstração do item (i). Por hipótese temos que

$$L = \bigoplus_{i=0}^{p-1} {}^{i}L$$

e também ${}^{i}L \neq 0$ somente para d valores distintos de i. Sejam $i_1,\ldots,i_d$ todos estes valores.

Lembrando que L' e $\gamma_k(L')$ são ideais de L e são φ-homogêneos, ou seja,

$$L' = \sum_{i=0}^{p-1} L' \cap {}^{i}L \ \text{ e } \ \gamma_k(L') = \sum_{i=0}^{p-1} \gamma_k(L') \cap {}^{i}L,$$

precisamos provar apenas que

$$[{}^{i_0}c, {}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_d}y_d] \equiv 0 \ (mod\ \gamma_{k+1}([L,L])), \tag{2-3}$$

para todo ${}^{i_0}c \in {}^{i_0}L \cap \gamma_k([L,L])$ e ${}^{i_s}y_s \in {}^{i_s}L$, onde $i_s \in \{i_1,\ldots,i_d\}$.

Pelo Lema 1.22 podemos permutar os elementos ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_d}y_d$ sem alterar a congruência módulo $\gamma_{k+1}([L,L])$ e pelo Lema 2.5, podemos obter no mínimo $d+1$ elementos de $\mathbb{Z}_p$ somando combinações dos índices $i_s \in \{i_1,\ldots,i_d\}$ do comutador (2-3).

Portanto, podemos permutar os elementos ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_d}y_d$ de forma conveniente, conseguindo um comutador com segmento inicial cuja soma de seus índices superiores não pertença a $\{i_1,\ldots,i_d\}$, ou seja, permutando os elementos ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_d}y_d$ conseguimos um comutador que pertence a uma φ-componente que é nula.

$\square$

A seguir, limitamos superiormente por um valor que depende somente de d o comprimento derivado de um anel de Lie admitindo um automorfismo semisimples com exatamente d autovalores distintos com φ-componentes não nulas e todos estes autovalores diferentes de 1.

Teorema 2.21 *Suponha que um anel de Lie L admite um automorfismo semisimples φ de ordem prima, com exatamente d autovalores distintos com φ-componentes não nulas e todos estes autovalores diferentes de 1. Então L é solúvel e seu comprimento derivado é no máximo* $2^d - 1$.

Demonstração. Como L admite um automorfismo semisimples de ordem prima p, temos que

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

Pelo item (ii) da Proposição 2.11, temos

$$L^{(2^k-1)} \subseteq \langle {}^{k+1}L, {}^{k+2}L, \ldots, {}^{p-1}L \rangle + {}_{id}\langle {}^{0}L \rangle, \quad k = 1,2,\ldots,p-1. \tag{2-4}$$

Por outro lado, podemos fazer uma reordenação dos índices de modo que as primeiras φ-componentes sejam aquelas não nulas,

$$L = \underbrace{{}^{1}L \oplus \cdots \oplus {}^{d}L}_{\text{não nulas}} \oplus \cdots \oplus {}^{p-1}L.$$

Sendo assim, pela propriedade (2-4) temos

$$L^{(2^d-1)} = 0,$$

uma vez que as φ-componentes ${}^{i}L$ são iguais a zero, para $d < i \leq p-1$, e ${}^{0}L = 0$, por hipótese.

$\square$

Agora, aplicando os Teoremas 2.20 e 2.21 provamos o Teorema 2.19.

Os resultados demonstrados acima, assim como o Teorema HKK, possuem suas versões combinatoriais para álgebras de Lie. Estas versões nos permitirão obter generalizações dos resultados sobre automorfismos quase regulares e serão usadas de forma decisiva na demonstração do resultado principal do Capítulo 4.

Teorema 2.22 *Existe uma função $g(n)$ com a seguinte propriedade. Seja p um primo e suponha que*

$$L = \bigoplus_{i=0}^{p-1} L_i$$

é uma álgebra de Lie $\mathbb{Z}_p$-graduada sobre algum corpo. Se $L_0 = 0$ e existem exatamente n componentes não triviais entre os L_i, então L é nilpotente de classe no máximo $g(n)$.

Demonstração. Na demonstração do Teorema 2.19 (na qual usamos os Teoremas 2.20 e 2.21) usamos o fato do anel de Lie admitir um automorfismo semisimples para definir uma $\mathbb{Z}_p$-graduação sobre ele, e o fato de possuir apenas d autovalores distintos com φ-componentes não nulas e todos estes autovalores diferentes de 1 para garantir que $L_0 = 0$ e existem exatamente d componentes não triviais entre os L_i.

Portanto, lembrando que uma álgebra de Lie é um exemplo de anel de Lie e tomando $g(n) = \frac{n^{2^{n-1}-1}-1}{n-1}$, segue o resultado como desejado.

□

Teorema 2.23 *Seja p um primo e suponha que*

$$L = \bigoplus_{i=0}^{p-1} L_i$$

é uma álgebra de Lie $\mathbb{Z}_p$-graduada sobre algum corpo. Se existem no máximo n componentes não triviais entre os L_i, então todo comutador de peso no mínimo $g(n)+1$ em elementos $y_i \in L_i$ pode ser representado como uma combinação linear de comutadores simples, tendo as mesmas entradas e segmento inicial em L_0 (isto é, tendo um segmento inicial cuja soma dos índices é zero módulo p).

Demonstração. Conforme discutido na demonstração do teorema anterior, podemos usar o item (iii) do Teorema 2.20 e a propriedade (2-4) para garantir que

$$\gamma_{g(n)+1}(L) \subseteq {}_{id}\langle {}^0L \rangle, \quad \text{onde } g(n) = \frac{n^{2^{n-1}-1}-1}{n-1}.$$

Como ${}_{id}\langle {}^0L \rangle$ é um ideal multihomogêneo, segue o resultado desejado.

□

CAPÍTULO 3

Automorfismos Quase Regulares

Dado um automorfismo φ de ordem prima p de um anel de Lie L, se $C_L(\varphi)$ é finito, digamos $|C_L(\varphi)| = q$, estamos interessados em garantir a existência de um subanel de L cujo índice é limitado por uma função dependendo somente de p e q, de tal modo que seja nilpotente de classe limitada por uma função dependendo somente de p.

Para isso, será necessário apresentar técnicas bastantes particulares e engenhosas, introduzidas por E. I. Khukhro em [9]. O maquinário baseia-se em diversas operações realizadas sobre comutadores de modo que seja possível obter objetos que se anulem.

Definição 3.1 *Dado um anel de Lie L, dizemos que um automorfismo φ de L é quase regular se $C_L(\varphi)$ é finito.*

Inicialmente provaremos resultados mais gerais sobre anéis de Lie $\mathbb{Z}_p$-graduados e em seguida construiremos os chamados centralizadores generalizados, os quais serão o ponto de partida para a construção de um subanel com as propriedades desejadas.

O próximo resultado, é uma consequência natural do Teorema HKK. Na verdade, sua demonstração consiste em aplicar o Teorema HKK em sua versão combinatorial (Corolário 2.18) várias vezes em um comutador, com intuito de conseguir subcomutadores com características desejadas.

Proposição 3.2 *Para todos m e n, existe uma função $f = f(m,n,p)$, dependendo apenas de m,n,p, tal que todo comutador simples de peso f em elementos ${}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_f}x_f$ de um anel de Lie arbitrário com índices $i_s \neq 0 \pmod{p}$ é igual a uma combinação linear de comutadores, cada um tendo o mesmo conjunto de entradas $X = \{{}^{i_s}x_s \,:\, 1 \leq s \leq f\}$ e cada um contendo ou um subcomutador da forma*

$$[{}^{k_1}w_1, {}^{k_2}w_2, \ldots, {}^{k_t}w_t], \quad {}^{k_i}w_i \in X, \tag{3-1}$$

o qual tem m segmentos iniciais com índices superiores somando 0 *módulo* p*:*

$$k_1 + k_2 + \cdots + k_{r_i} \equiv 0 \ (mod\ p), \quad i = 1, 2, \ldots, m,$$
$$1 < r_1 < r_2 < \cdots < r_m = t,$$

ou contendo um subcomutador da forma

$$[{}^{k_0}w, c_1, c_2, \ldots, c_n], \tag{3-2}$$

onde ${}^{k_0}w \in X$ *e cada um dos n comutadores* c_i *é simples e tem a forma*

$$[{}^{k_1}u_1, {}^{k_2}u_2, \ldots, {}^{k_s}u_s], \quad {}^{k_j}u_j \in X,$$

com índices superiores somando 0 *módulo* p*, isto é,*

$$k_1 + k_2 + \cdots + k_s \equiv 0 \ (mod\ p).$$

Observação: *podemos considerar* $f(m,n,p) = 1 + \sum_{i=1}^{m-1} (h(p)+1)^{i+1} \cdot n^i$*, onde* $h(p)$ *é a função de Higman.*

Antes de demonstrar a Proposição 3.2, é necessário definir e demonstrar alguns resultados técnicos. Considere $X = \{{}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_f}x_f\}$ o conjunto dos geradores livres de um anel de Lie livre, o qual denotaremos por L.

Definindo uma Graduação em L

Definimos sobre L a $\mathbb{Z}_p$-graduação

$$L = L_0 \oplus L_1 \oplus L_2 \oplus \cdots \oplus L_{p-1},$$

onde para cada s o subgrupo aditivo L_s é gerado por todos comutadores nos geradores ${}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_f}x_f$ tendo índices superiores somando s módulo p.

Transformação HKK

Descreveremos a seguir um procedimento, que chamaremos de Transformação HKK, afim de “transformar” um comutador em uma combinação linear de outros comutadores, onde cada membro desta combinação linear possui propriedades desejadas.

Recordamos que pelo Teorema HKK, dados elementos ${}^{j_i}a_i \in L_{j_i}$, $i = 1, 2, \ldots, h+1$, o comutador simples

$$[{}^{j_1}a_1, {}^{j_2}a_2, \ldots, {}^{j_{h+1}}a_{h+1}]$$

de peso $h+1$ é igual a uma combinação linear de comutadores com mesmo conjunto de entradas e um segmento inicial em L_0, ou seja, um segmento inicial tendo o mesmo conjunto de entradas e soma dos índices superiores igual a zero módulo p.

Assim, o segmento inicial de peso $h+1$ do comutador

$$[{}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_f}x_f] \tag{3-3}$$

é igual a uma combinação linear de comutadores com entradas em X e com segmento inicial em L_0. Em outras palavras, o comutador (3-3) é uma combinação linear de comutadores da forma

$$[{}^{k_1}x_{i_1}, {}^{k_2}x_{i_2}, \ldots, {}^{k_r}x_{i_r}, {}^{k_{r+1}}x_{i_{r+1}}, \ldots], \;\; r \leq h+1, \quad k_1 + k_2 + \cdots + k_r \equiv 0 \; (mod \;\, p),$$

onde ${}^{k_j}x_{i_j} \in X$.

Para cada comutador desta combinação linear colocamos

$${}^{k_{r+1}}y_1 = -[{}^{k_1}x_{i_1}, {}^{k_2}x_{i_2}, \ldots, {}^{k_r}x_{i_r}, {}^{k_{r+1}}x_{i_{r+1}}]$$

(claramente ${}^{k_{r+1}}y_1 \in L_{k_{r+1}}$) e denotamos

$${}^{k_{r+s}}y_s = {}^{k_{r+s}}x_{i_{r+s}} \text{ para } s \geq 2.$$

Note que ${}^{k_{r+1}}y_1 = [{}^{k_{r+1}}x_{i_{r+1}}, c_0]$, onde

$$c_0 = [{}^{k_1}x_{i_1}, {}^{k_2}x_{i_2}, \ldots, {}^{k_r}x_{i_r}] \in L_0.$$

Assim, concluímos que o comutador simples (3-3) é igual a uma combinação linear de comutadores simples da forma

$$[{}^{k_{r+1}}y_1, {}^{k_{r+2}}y_2, \ldots], \tag{3-4}$$

cujos pesos de cada um não são menores que $f - h$.

Para f suficientemente grande, temos $f - h \geq h+2$ e podemos aplicar o mesmo procedimento para os comutadores da forma (3-4) obtidos acima, substituindo seus segmentos iniciais de peso $h+1$ por suas expressões como uma combinação linear de comutadores simples com mesmas entradas ${}^{k_{r+1}}y_1, {}^{k_{r+2}}y_2, \ldots$ e com segmentos iniciais em L_0.

Essa transformação pode ser executada várias vezes se f for suficientemente grande. Com as mudanças de variáveis, temos que o peso do comutador diminui no máximo $h+1$ em cada passo.

Vamos imaginar que a transformação mencionada acima tenha sido executada várias vezes no comutador (3-3). Afirmamos que o comutador resultante pode ser considerado como uma combinação linear de comutadores da forma

$$[{}^{i_1}y_1, {}^{i_2}y_2, \ldots {}^{i_r}y_r], \tag{3-5}$$

onde para cada s os elementos ${}^{i_s}y_s$ têm a forma

$${}^{i_s}y_s = [{}^{i_s}x, c_1, c_2, \ldots, c_k], \quad k \geq 0, \tag{3-6}$$

onde ${}^{i_s}x$ denota um elemento de X, e cada $c_i \in L_0$ também tem a forma (3-5), com $r \leq h+1$ e $i_1 + i_2 + \cdots + i_r \equiv 0 \ (mod\ p)$.

Para demonstrar a afirmação acima, faremos apenas uma ilustração, onde o somatório indica uma combinação linear e, por simplicidade, omitimos os índices superiores:

$$\begin{array}{rcll}
[{}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_f}x_f] & = & \sum_j \alpha_j [[c_1, x_{i_{r+1}}], x_{i_{r+2}}, \ldots] & \text{(fazendo a mudança de variável)} \\
& = & \sum_j \alpha_j [y_1, \ \ y_2, \ldots] & \text{(executando a transformação)} \\
& = & \sum_j \alpha_j [[c_2, y_{j_{r+1}}], y_{j_{r+2}}, \ldots] & \text{(fazendo a mudança de variável)} \\
& = & \sum_j \alpha_j [z_1, \ \ z_2, \ldots] & \text{(executando a transformação)} \\
& \vdots & \quad \vdots &
\end{array}$$

onde $\alpha = \pm 1$ e cada $c_i \in L_0$ depende das primeiras (da esquerda) $h+1$ entradas do comutador anterior.

Devemos observar que poderemos ter elementos do tipo $c_i \in L_0$ “dentro” de outros elementos do tipo $c_j \in L_0$. Isso ocorrerá por exemplo quando o elemento

$y_1 = -[c_1, x_{i_{r+1}}]$ da ilustração acima estiver contido em c_2. Outro caso interessante é quando $y_{j_{r+1}} = y_1$, pois nesse caso teremos $z_1 = [x, c_1, c_2]$.

A definição de altura de um comutador da forma (3-5), a qual daremos a seguir, pode parecer um pouco abstrata no primeiro momento, porém a altura de tal comutador pode ser considerada como a quantidade de elementos $c_i \in L_0$ que ocorrem (ou são gerados) durante o processo de formação do comutador (3-5), por meio de repetidas aplicações da Transformação HKK no comutador (3-3).

Definição 3.3 *Definimos a altura do comutador (3-5) por indução como sendo a soma das alturas dos elementos* ${}^{i_s}y_s$ *(*$s = 1, 2, \ldots, r$*), sendo a altura de um elemento da forma (3-6) igual à soma de* k *com a soma das alturas dos elementos* $c_1, c_2, \ldots, c_k$ *(os quais também possuem a forma do comutador (3-5)) . Quando* $k = 0$*, a altura de um elemento* ${}^{i_s}y_s = {}^{i_s}x$ *da forma (3-6) é tomada como sendo* 0.

Por exemplo, a altura do comutador (3-3) é igual a 0 e a altura do comutador (3-4) é 1, uma vez que a altura do elemento ${}^{k_{r+1}}y_1$ é 1, a altura do elemento c_0 é 0, e a altura dos elementos ${}^{k_{r+s}}y_s,\ \ s \geq 2$, são todas iguais a 0.

Definiremos a seguir de forma precisa a Transformação HKK, a qual na verdade consiste dos procedimentos descritos acima que, em um certo sentido, possibilitam diminuir o peso de um comutador em no máximo $h+1$ unidades e aumentar sua altura em 1 unidade.

Definição 3.4 *A* ***Transformação HKK*** *do comutador (3-5) consiste em:*

a) Representar o comutador (3-5) como combinação linear de comutadores simples com mesmas entradas ${}^{i_1}y_1, {}^{i_2}y_2, \ldots, {}^{i_r}y_r$ e com um segmento inicial de peso no máximo $h+1$ pertencendo a L_0, ou seja, comutadores da forma

$$[c, {}^{k_{w+1}}y_{i_{w+1}}, {}^{k_{w+2}}y_{i_{w+2}}, \ldots, {}^{k_r}y_{i_r}], \tag{3-7}$$

onde

$$c = [{}^{k_1}y_{i_1}, {}^{k_2}y_{i_2}, \ldots, {}^{k_w}y_{i_w}],\ \ w \leq h+1,\ \ k_1 + k_2 + \cdots + k_w \equiv 0 \ \ (mod \ \ p). \tag{3-8}$$

b) Mudar a notação

$${}^{k_{w+1}}z_1 = -[c, {}^{k_{w+1}}y_{i_{w+1}}],\ \ {}^{k_{w+s}}z_s = {}^{k_{w+s}}y_{i_{w+s}} \ \text{ para } s \geq 2.$$

Dizemos que o comutador resultante da forma

$$[{}^{k_{w+1}}z_1, {}^{k_{w+2}}z_2, \dots, {}^{k_r}z_{r-w}] \tag{3-9}$$

é obtido de (3-5) por meio da Transformação HKK.

Lema 3.5 *Todo comutador da forma (3-9), obtido de um comutador (3-5) por meio de uma aplicação da Transformação HKK, é também um comutador da forma (3-5), e sua altura é exatamente uma unidade maior.*

Demonstração. Claramente os elementos ${}^{k_{w+s}}z_s = {}^{k_{w+s}}y_{i_{w+s}}$ para $s \geq 2$ têm a forma (3-6). Para $s = 1$, substituímos em ${}^{k_{w+1}}z_1 = [{}^{k_{w+1}}y_{i_{w+1}}, c]$ a expressão de ${}^{k_{w+1}}y_{i_{w+1}}$ dada por (3-6):

$${}^{k_{w+1}}z_1 = [{}^{k_{w+1}}y_{i_{w+1}}, c] = [{}^{i_s}x, c_1, c_2, \dots, c_k, c].$$

Note que cada c_i tem a forma (3-5), com $r \leq h+1$, por definição e c é também da forma (3-5), com $r \leq h+1$ por (3-8). Consequentemente, ${}^{k_{w+1}}z_1$ tem a forma (3-6) e o comutador (3-9) tem a forma (3-5).

Calculando a altura do comutador (3-9), vemos que a única diferença entre esta e a altura de (3-5) é a ocorrência adicional de um elemento $c \in L_0$ em ${}^{k_{w+1}}z_1$.

□

Voltando à demonstração da Proposição 3.2. Conforme a discussão sobre anéis de Lie livres do Capítulo 1, temos que é suficiente prová-la para o anel de Lie L construído acima, uma vez que podemos criar uma bijeção entre os geradores de L e os respectivos elementos de um anel de Lie arbitrário e ainda pelo fato de a componente L_0 de L ser formada por todos os comutadores com soma dos índices superiores iguais a 0. Vamos provar antes o seguinte lema.

Lema 3.6 *Se um comutador da forma (3-5) tem peso $r \leq h+1$ e altura no mínimo $f_1(m,n,p) = \sum_{i=1}^{m-1} (h(p)+1)^i \cdot n^i$, então ele é igual a uma combinação linear de comutadores, cada um contendo: ou um subcomutador da forma (3-1) ou um subcomutador da forma (3-2) da conclusão da Proposição 3.2.*

Demonstração. Construiremos o grafo de ocorrência de subcomutadores $c \in L_0$ nos comutadores (3-5). Seus vértices serão particionados em diferentes níveis e cada nível será particionado em subconjuntos. Os vértices de nível 1 são os elementos c_i da expressão (3-6) para todo elemento ${}^{i_s}y_s$ ocorrendo no comutador (3-5) em consideração.

Esses vértices de nível 1 são particionados em subconjuntos com respeito aos elementos ${}^{i_s}y_s$, onde dizemos que eles pertencem a um mesmo subconjunto se ocorrem na mesma expressão (3-6).

Todo elemento c_i de nível 1 também tem a forma (3-5) por definição e, pela fórmula (3-6), eles contêm outros elementos de L_0, que são os vértices de nível 2 conectados com os respectivos vértices de nível 1. Os vértices de nível 2 são particionados em grupos do mesmo modo, e assim por diante.

Apenas para uma ilustração de como é construído o grafo descrito acima, considere $[{}^{i_1}y_1, {}^{i_2}y_2]$ um comutador da forma (3-5), onde:

(i) ${}^{i_1}y_1 = [x, c_1, c_2]$ e ${}^{i_2}y_2 = [x, \overline{c}_1, \overline{c}_2, \overline{c}_3]$,

(ii) $c_1 = [a_1, a_2]$, com $a_1 = [x, c_1(a), c_2(a)]$ e $a_2 = [x, \overline{c}_1(a), \overline{c}_2(a)]$
$c_2 = [b_1, b_2]$, com $b_1 = [x, c_1(b), c_2(b)]$ e $b_2 = [x, \overline{c}_1(b)]$

(iii) $\overline{c}_1 = [d_1, d_2]$, com $d_1 = [x, c_1(d), c_2(d)]$ e $d_2 = [x, \overline{c}_1(d), \overline{c}_2(d)]$
$\overline{c}_2 = e_1$, com $e_1 = [x, c_1(e), c_2(e)]$
$\overline{c}_3 = [f_1, f_2]$, com $f_1 = [x, c_1(f), c_2(f)]$, e $f_2 = [x, \overline{c}_1(f), \overline{c}_2(f)]$.

Eis os grafos:

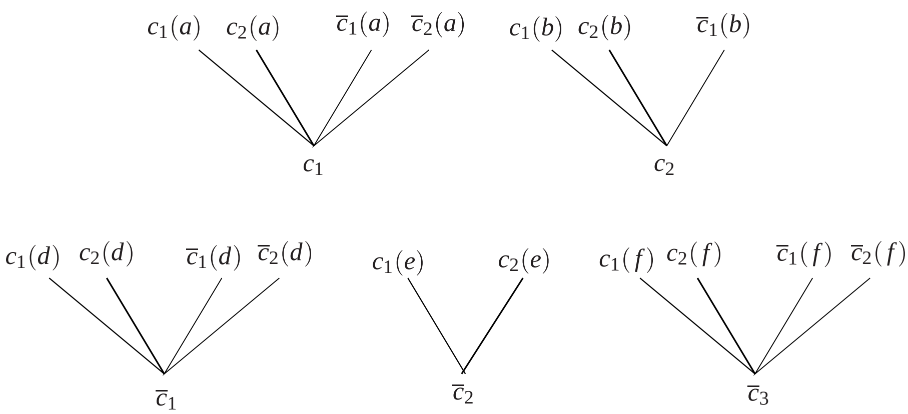

Figura 3.1: *Grafo*

Observe que o número de vértices deste grafo é igual à altura do comutador original (3-5). Notemos também que cada vértice é conectado com os vértices do próximo nível de no máximo $h+1$ subconjuntos, e o nível 1 também é formado por no máximo $h+1$ subconjuntos, uma vez que o comutador (3-5) tem peso $r \leq h+1$ pela hipótese do lema.

Mostremos primeiro que: ou o número de níveis é no mínimo m, ou no mínimo um dos grupos em algum nível contém número de vértices no mínimo n. De fato, suponhamos que o número de níveis é menor que m e que todos os grupos tenham menos que n vértices. Então no nível 1 existem menos que $(h+1)\cdot n$ vértices, dado que existem no máximo $h+1$ grupos neste nível. Assim, no nível 2 existem menos que $(h+1)^2\cdot n^2$ vértices, pois cada vértice de nível 1 é conectado com vértices de nível 2 de no máximo $h+1$ grupos, cada um contendo menos que n vértices, e assim por diante. Isto permite estabelecer por indução que no nível i existem menos que $(h+1)^i\cdot n^i$ vértices, ou seja, o número total de vértices será menor que

$$\sum_{i=1}^{m-1}(h(p)+1)^i\cdot n^i = f_1(m,n,p),$$

o que contradiz a hipótese do lema.

Mas se algum grupo de algum nível tem no mínimo n vértices, então o comutador (3-5) possui um subcomutador da forma (3-2). E se o número de níveis é no mínimo m, então existe uma cadeia de subcomutadores de L_0 de comprimento m. Utilizando a identidade de Jacobi $[a,[b,c]]=[a,b,c]-[a,c,b]$, transformamos essa cadeia em uma combinação linear de comutadores simples (nos elementos de $X=\{{}^{i_s}x_s\}$) em L_0. Com isso, obtemos uma combinação linear onde cada comutador contém um subcomutador da forma (3-1) da Proposição 3.2.

$\square$

Segue uma breve ilustração dos argumentos acima:

<u>Caso 1</u>: Apenas para ilustração, suponhamos que no nível 2 exista um grupo com n vértices e que este grupo corresponda ao elemento c_2, e que c_2 corresponda a ${}^{i_2}y_2$. Logo teremos o seguinte comutador:

$$\begin{aligned}[{}^{i_1}y_1,{}^{i_2}y_2,\ldots,{}^{i_r}y_r] &= [{}^{i_1}y_1,[{}^{i_2}x,c_1,c_2,\ldots,c_k],\ldots,{}^{i_r}y_r] = \\ &= [{}^{i_1}y_1,[{}^{i_2}x,c_1,[{}^{i_1}y(c_2)_1,{}^{i_2}y(c_2)_2,\ldots,{}^{i_r}y(c_2)_r],\ldots,c_k],\ldots,{}^{i_r}y_r] = \\ &= [{}^{i_1}y_1,[{}^{i_2}x,c_1,[{}^{i_1}y(c_2)_1,\underbrace{[{}^{i_2}x(c_2),c'_1,c'_2,\ldots,c'_n]}_{\text{subcomutador desejado}},\ldots,{}^{i_r}y(c_2)_r],\ldots,c_k],\ldots,{}^{i_r}y_r],\end{aligned}$$

o qual possui um subcomutador da forma (3-2).

<u>Caso 2</u>: Apenas para ilustração, suponhamos que o número de níveis seja $m=2$. Logo existe uma cadeia de subcomutadores de L_0 com comprimento 2. Considerando a

mesma cadeia do Caso 1 acima trocando n por $q < n$, temos:

$$
\begin{gathered}
[{}^{i_1}y_1, [{}^{i_2}x, c_1, [{}^{i_1}y(c_2)_1, [{}^{i_2}x(c_2), c'_1, c'_2, \ldots, c'_q], \ldots, {}^{i_r}y(c_2)_r], \ldots, c_k], \ldots {}^{i_r}y_r] = \\
-[{}^{i_1}y_1, [{}^{i_2}x, c_1, [[{}^{i_2}x(c_2), c'_1, c'_2, \ldots, c'_q], {}^{i_1}y(c_2)_1, \ldots, {}^{i_r}y(c_2)_r], \ldots, c_k], \ldots {}^{i_r}y_r] = \\
-[{}^{i_1}y_1, [{}^{i_2}x, c_1, [{}^{i_2}x(c_2), c'_1, c'_2, \ldots, c'_q, {}^{i_1}y(c_2)_1, \ldots, {}^{i_r}y(c_2)_r], \ldots, c_k], \ldots {}^{i_r}y_r] = \\
[{}^{i_1}y_1, [{}^{i_2}x, c_1, \underbrace{[\underbrace{c'_1}_{\in {}^0L}, {}^{i_2}x(c_2), c'_2, \ldots, c'_q, {}^{i_1}y(c_2)_1, \ldots, {}^{i_r}y(c_2)_r], \ldots, c_k]}_{\in {}^0L}, \ldots {}^{i_r}y_r],
\end{gathered}
$$

ou seja, após escrevermos as entradas com elementos de X obtemos dois segmentos iniciais com índices somando 0 módulo p.

Agora finalizaremos a demonstração da Proposição 3.2.

Para provar a Proposição 3.2 aplicamos a Transformação HKK no comutador (3-3), em seguida aplicamos novamente nos comutadores da forma (3-5) resultantes, e assim por diante. Fazemos este processo $f_1(m,n,p)$ vezes. Note que o comutador (3-3) pode ser considerado como um comutador da forma (3-5) cuja altura é exatamente 0. Em cada passo, o peso de cada comutador da forma (3-9) é menor que o peso do comutador (3-5) do qual foi obtido por meio da Transformação HKK, por não mais que $h+1$. Consequentemente, se o peso inicial é no mínimo $f(m,n,p) = (h+1)\cdot f_1(m,n,p)+1$, então é possível aplicar a Transformação HKK $f_1(m,n,p)$ vezes. Se a combinação linear resultante contém comutadores da forma (3-5) de peso maior que $h+1$, então aplicamos a Transformação HKK nestes até conseguirmos uma combinação linear de comutadores da forma (3-5) de peso $r \leq h+1$.

Como o comutador (3-3) é também um comutador da forma (3-5) de altura 0, temos após a transformação descrita acima, que ele será expresso conforme o Lema 3.5 como uma combinação linear de comutadores da forma (3-5) de peso no máximo $h+1$, e altura no mínimo $f_1(m,n,p)$. A aplicação do Lema 3.6 completa a prova da proposição.

$\square$

Automorfismos Quase Regulares

O próximo teorema afirma que se um anel de Lie L tal que $L = pL$ admite um automorfismo φ de ordem prima p e número de pontos fixos igual a $|C_L(\varphi)| = q$, então L possui um subanel de índice $\{p,q\}$-limitado, o qual é nilpotente de classe p-limitada.

A demonstração para o anel $L = pL$ consiste em construir, de forma especial, um subanel $M(p)$ onde os comutadores das formas (3-1) e (3-2) são iguais a 0.

Teorema 3.7 *Seja φ um automorfismo de ordem prima p de um anel de Lie (álgebra) L tal que $L = pL$. Se o número de pontos fixos de φ em L é finito e igual a $|C_L(\varphi)| = q$ (a dimensão da subálgebra $C_L(\varphi)$ é finita e igual a q), então L possui um subanel (subálgebra) de índice $\{p,q\}$-limitado (codimensão $\{p,q\}$-limitada), o qual é nilpotente de classe p-limitada.*

Seja $\widetilde{L} = L \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$, onde ω é uma raiz p-ésima da unidade, e definimos a ação natural de φ sobre $\widetilde{L}$, conforme feito no capítulo anterior. Temos $C_{\widetilde{L}}(\varphi) = C_L(\varphi) \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$ e, consequentemente, $|C_{\widetilde{L}}(\varphi)| = |C_L(\varphi)|^{p-1} = q^{p-1}$.

Portanto, se provarmos que o Teorema 3.7 vale para $\widetilde{L}$, teremos provado a existência de um subanel $\widetilde{L}_1$ de $\widetilde{L}$, o qual possui índice $\{p, q^{p-1}\}$-limitado e é nilpotente de classe p-limitada. Assim, identificando L com o subanel $L \otimes_{\mathbb{Z}} 1$ de $\widetilde{L}$, temos que $L \cap \widetilde{L}_1$ é um subanel de índice $\{p,q\}$-limitado em L e é nilpotente de classe p-limitada. Logo assumiremos, sem perda de generalidade, $L = \widetilde{L}$.

Definição 3.8 *Um padrão de um comutador em elementos φ-homogêneos ${}^{i_s}x_s \in {}^{i_s}L$ é definido como uma estrutura de colchetes junto com um arranjo de índices superiores. O comutador será chamado de valor do padrão nos elementos ${}^{i_s}x_s \in {}^{i_s}L$.*

Por exemplo,

$$[[{}^1a, {}^3b, {}^4c], [{}^2d, {}^5e]] \quad \text{e} \quad [[{}^1x, {}^3y, {}^4z], [{}^2u, {}^5v]] \tag{3-10}$$

são valores do mesmo padrão

$$[[{}^1*, {}^3*, {}^4*], [{}^2*, {}^5*]].$$

Para todo conjunto ordenado (de comprimento arbitrário k)

$$\bar{x} = ({}^{i_1}x_1, {}^{i_2}x_2, \dots, {}^{i_k}x_k)$$

de elementos φ-homogêneos ${}^{i_s}x_s \in {}^{i_s}L$, escolhemos $j \leq p-1$ tal que

$$j + i_1 + i_2 + \cdots + i_k \equiv 0 \ (mod\ p)$$

e definimos o homomorfismo

$$\vartheta_{\overline{x}}:\ {}^{j}y \longmapsto [{}^{j}y, {}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_k}x_k],\ \ {}^{j}y \in {}^{j}L,$$

do subgrupo aditivo ${}^{j}L$ em ${}^{0}L$.

Como $|{}^{0}L| = q$, temos o seguinte resultado.

Lema 3.9 *Para todo $\overline{x}$, temos $|{}^{j}L : Ker\ \vartheta_{\overline{x}}| \leq q$.*

Iniciamos agora a construção de certos conjuntos que chamaremos de **centralizadores generalizados** de níveis $1, \ldots, h+1$, que será feita por indução. Primeiro definimos ${}^{j}K(1) = {}^{j}L$, para todo $j \neq 0$. Para cada elemento $c \in {}^{0}L$ que pode ser representado como valor de algum padrão de peso no máximo $N = f(h+1, h, p)$ nos elementos ${}^{i_s}x_s \in {}^{i_s}L$ para $i_s \neq 0$, fixamos uma tal apresentação para cada possível padrão de peso menor ou igual a N. Os elementos φ-homogêneos ${}^{i_s}x_s$, que ocorrem em todas estas apresentações, são chamados de representantes de nível 1, onde o nível é indicado por parênteses ${}^{i_s}x_s(1)$.

Temos que o número total de representantes de nível 1 é $\{p, q\}$-limitado, pois o número de todos os padrões de peso no máximo $N = f(h+1, h, p)$ é p-limitado e o número de elementos $c \in^{0} L$ é no máximo q.

Agora construimos os centralizadores generalizados ${}^{j}K(2)$ de nível 2, colocando, para cada $j = 1, 2, \ldots, p-1$,

$${}^{j}K(2) = \bigcap_{\overline{x}} Ker\ \vartheta_{\overline{x}}\ ,$$

onde $\overline{x} = ({}^{i_1}x_1(1), {}^{i_2}x_2(1), \ldots, {}^{i_k}x_k(1))$ percorre todos os conjuntos ordenados de comprimento $k \leq N$ de representantes de nível 1 (temos que $i_1, \ldots, i_k$ devem satisfazer $j + i_1 + i_2 + \cdots + i_k \equiv 0\ (mod\ p)$, de acordo com a definição do homomorfismo $\vartheta_{\overline{x}}$).

Como o número destes conjuntos ordenados é claramente $\{p, q\}$-limitado, e o índice de cada subgrupo $Ker\ \vartheta_{\overline{x}}$ em ${}^{j}L$ é no máximo q pelo Lema 3.9, segue que o índice do subgrupo ${}^{j}K(2)$ em ${}^{j}L$ é também $\{p, q\}$-limitado, lembrando que o índice de uma interseção de subgrupos é menor ou igual ao produto dos índices dos subgrupos.

Podemos notar que os elementos ${}^{j}y \in {}^{j}K(2)$ possuem a seguinte propriedade de centralizadores com respeito aos representantes de nível 1:

$$[{}^{j}y, {}^{i_1}x_1(1), {}^{i_2}x_2(1), \ldots, {}^{i_k}x_k(1)] = 0,$$

sempre que $j+i_1+i_2+\cdots+i_k \equiv 0 \ (mod\ p)$ e $k \leq N$.

Agora procedemos por indução. Suponha que, para $t < h+1$ e para cada $j = 1,2,\ldots,p-1$, já tenham sido construídos centralizadores de níveis $\leq t$ que são subgrupos aditivos de ${}^{j}L$,

$$ {}^{j}K(1) \geq {}^{j}K(2) \geq \cdots \geq {}^{j}K(t) $$

de índices $\{p,q\}$-limitados em ${}^{j}L$ e que tenham sido fixados representantes ${}^{i_s}x_s(\varepsilon_s) \in {}^{i_s}L$, para $i_s \neq 0$ de níveis $\varepsilon_s \leq t$, cujo número total é $\{p,q\}$-limitado. Suponha também que, para todo $s \leq t$, os elementos ${}^{j}y \in {}^{j}K(s)$ possuem a seguinte propriedade de centralizadores com respeito aos representantes de níveis menores que s:

$$ \begin{gathered} [{}^{j}y, {}^{i_1}x_1(\varepsilon_1), {}^{i_2}x_2(\varepsilon_2), \ldots, {}^{i_k}x_k(\varepsilon_k)] = 0, \\ \text{sempre que } {}^{j}y \in {}^{j}K(s), \ \ k \leq N, \\ \varepsilon_j < s \ (j = 1,2,\ldots,k) \ \text{ e } \ j+i_1+i_2+\cdots+i_k \equiv 0 \ (mod\ p). \end{gathered} \tag{3-11} $$

Agora para $j = 1,2,\ldots,p-1$, definimos

$$ {}^{j}K(t+1) = \bigcap_{\overline{x}} Ker\ \vartheta_{\overline{x}} \ , $$

onde $\overline{x} = ({}^{i_1}x_1(\varepsilon_1), {}^{i_2}x_2(\varepsilon_2), \ldots, {}^{i_k}x_k(\varepsilon_k))$ percorre todos os conjuntos ordenados de comprimento $k \leq N$ de representantes de níveis $\varepsilon_u \leq t$ (temos $j+i_1+i_2+\cdots+i_k \equiv 0 \ (mod\ p)$, de acordo com a definição do homomorfismo $\vartheta_{\overline{x}}$).

Novamente, como o número destes conjuntos ordenados é claramente $\{p,q\}$-limitado e o índice de cada subgrupo $Ker\ \vartheta_{\overline{x}}$ em ${}^{j}L$ é no máximo q, pelo Lema 3.9, temos que o índice do subgrupo ${}^{j}K(t+1)$ em ${}^{j}L$ é também $\{p,q\}$-limitado. E ainda temos ${}^{j}K(t+1) \leq {}^{j}K(t)$.

Para todo elemento $c \in {}^{0}L$, o qual pode ser representado como um valor de algum padrão de peso no máximo N nos elementos ${}^{i_s}x_s \in {}^{i_s}K(t+1)$, para $i_s \neq 0$, fixamos uma tal apresentação para cada possível padrão de peso no máximo N. Os elementos φ-homogêneos ${}^{i_s}x_s$, que ocorrem em todas estas apresentações, são chamados de representantes de nível $t+1$, onde o nível é indicado por parênteses ${}^{i_s}x_s(t+1)$. É claro que o total de representantes de nível $(t+1)$ é também $\{p,q\}$-limitado.

Assim terminamos a definição dos centralizadores generalizados ${}^{j}K(1), {}^{j}K(2), \ldots, {}^{j}K(h+1)$, $j = 1,2,\ldots,p-1$.

O próximo passo é demonstrar que o subanel

$$M(p) = \langle {}^1K(h+1), {}^2K(h+1), \dots, {}^{p-1}K(h+1) \rangle$$

possui índice $\{p,q\}$-limitado em pL e é nilpotente de classe p-limitada.

Como $pL \subseteq {}^0L + \cdots + {}^{p-1}L$, e $[{}^jL : {}^jK(h+1)]$ é $\{p,q\}$-limitado para todo $j = 1, \dots, p-1$, segue que $[{}^jL : M(p)]$ também é $\{p,q\}$-limitado, uma vez que $[{}^jL : M(p)] \leq [{}^jL : {}^jK(h+1)]$, pois ${}^jK(h+1) \subseteq M(p)$. Portanto, podemos concluir que $[{}^0L + \cdots + {}^{p-1}L : M(p)]$ e, consequentemente, $[pL : M(p)]$ é $\{p,q\}$-limitado.

Para mostrar que o subanel

$$M(p) = \langle {}^1K(h+1), {}^2K(h+1), \dots, {}^{p-1}K(h+1) \rangle$$

é nilpotente de classe menor que $N = f(h+1, h, p)$, onde f é a função da Proposição 3.2, é suficiente mostrar que todo comutador simples de peso N da forma

$$[{}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_N}y_N], \quad {}^{i_s}y_s \in {}^{i_s}K(h+1), \tag{3-12}$$

onde cada entrada percorre os geradores deste subanel, é igual a 0.

Pela Proposição 3.2, basta mostrar que comutadores da forma (3-1) e (3-2), os quais são obtidos aplicando a Proposição 3.2 ao comutador (3-12) com $m = h+1$ e $n = h$, são iguais a 0.

Vamos considerar primeiro os comutadores da forma (3-2), ou seja, comutadores da forma

$$[{}^jy, c_1, c_2, \dots, c_h], \tag{3-13}$$

onde ${}^jy \in {}^jK(h+1)$ e cada $c_i \in {}^0L$ é um comutador cujas entradas são representantes de nível $h+1$.

Assim, como ${}^iK(h+1) \subseteq {}^iK(s)$, para todo $s \leq h+1$, temos que cada representante de nível $h+1$ usado para representar os comutadores $c_i \in {}^0L$, os quais são valores de um padrão de peso menor que N, também pode ser considerado como representante de nível $s = 1, 2, \dots, h$.

Com isso, usando que $[a,[b,c]] = [a,b,c] - [a,c,b]$, podemos expandir o comutador (3-13) como uma combinação linear de comutadores da forma

$$[{}^{j}y, {}^{i_1}x(1), \ldots, {}^{i_k}x(1), {}^{i_{k+1}}x(2), \ldots, {}^{i_l}x(2), \ldots, {}^{i_{t+1}}x(h), \ldots, {}^{i_u}x(h)],$$
$${}^{j}y \in {}^{j}K(h+1). \tag{3-14}$$

Por simplicidade, omitimos os índices inferiores, pois para o que segue é importante apenas que os representantes estejam em ordem cresceste de nível.

Para as discussões que seguem, faz-se necessário apresentar o conceito de quaserepresentante.

Definição 3.10 *Um quaserepresentante de nível s é um comutador em representantes, o qual contém somente um representante de nível s, e os níveis dos demais representantes são menores que s.*

Note que um representante pode ser considerado como um quaserepresentante de mesmo nível.

Lema 3.11 *Todo comutador da forma (3-14) é igual a uma combinação linear de comutadores da forma*

$$[{}^{j}y, {}^{v_1}\widehat{x}(1), {}^{v_2}\widehat{x}(2), \ldots, {}^{v_h}\widehat{x}(h), {}^{v_{h+1}}\widehat{x}(\varepsilon_{h+1}), \ldots], \tag{3-15}$$

cujas entradas do segmento inicial após ${}^{j}y \in {}^{j}K(h+1)$ são compostas por quaserepresentantes, sendo um de cada nível dentre $1, 2, \ldots, h$, em ordem crescente de nível.

Demonstração. Vamos aplicar ao comutador (3-14) uma sequência de processos, de maneira que, a cada passo, um comutador da forma (3-14) será igual a uma combinação linear de comutadores da forma

$$[{}^{j}y, {}^{v_1}\widehat{x}(1), {}^{v_2}\widehat{x}(2), \ldots, {}^{v_s}\widehat{x}(s), {}^{v_{s+1}}\widehat{x}(\varepsilon_{s+1}), \ldots], \tag{3-16}$$

com ${}^{j}y$ na primeira entrada e quaserepresentantes tendo a seguinte propriedade: à esquerda do primeiro quaserepresentante (primeiro da esquerda) de algum nível existem apenas ${}^{j}y$ e quaserepresentantes de níveis menores. Em particular, o comutador (3-14) é também um comutador da forma (3-16).

No comutador (3-16) a parte colecionada é o maior segmento inicial da forma

$$[{}^{j}y, {}^{v_1}\widehat{x}(1), {}^{v_2}\widehat{x}(2), \ldots, {}^{v_s}\widehat{x}(s)], \quad s \geq 1,$$

o qual contém a partir da segunda entrada à direita de ${}^{j}y$ um quaserepresentante de cada nível $1,2,\ldots,s$ em ordem crescente de nível.

Agora transportamos o primeiro representante de nível $s+1$ da parte não colecionada para o final da parte colecionada usando a igualdade

$$[\ldots,b,\widehat{x}(s+1),\ldots] = [\ldots,\widehat{x}(s+1),b,\ldots] + [\ldots,[b,\widehat{x}(s+1)],\ldots],$$

onde as reticências significam as partes inalteradas.

Note que realmente existe um quaserepresentante de nível $s+1$ à direita da parte colecionada, uma vez que o comutador (3-14) contém representantes de todos os níveis menores ou iguais a h. Observe ainda que o subcomutador $[b,\widehat{x}(s+1)]$ pode ser considerado como um quaserepresentante de nível $s+1$, pois o nível de b é menor que $s+1$.

Podemos dizer que de certo modo o procedimento descrito acima é transportar o primeiro representante de cada nível no comutador (3-14) para a esquerda até conseguirmos a ordenação desejada. E neste processo são acumulados quaserepresentantes de mesmo nível do representante que está sendo transportado.

Como não aparece quaserepresentantes de níveis maiores que h nas etapas deste processo, então após um número finito de passos o processo será encerrado, donde temos o resultado desejado.

$\square$

Lema 3.12 *Se* ${}^{i_1}\widehat{x}_1(\varepsilon_1), {}^{i_2}\widehat{x}_2(\varepsilon_2), \ldots, {}^{i_k}\widehat{x}_k(\varepsilon_k)$ *são quaserepresentantes de níveis* $\varepsilon_u < s$ $(u = 1,2,\ldots,k)$ *com peso no máximo* $h+1$ *e um elemento* ${}^{j}y$ *ou pertence a* ${}^{j}K(s)$ *ou é um quaserepresentante de nível s, então*

$$[{}^{j}y, {}^{i_1}\widehat{x}_1(\varepsilon_1), {}^{i_2}\widehat{x}_2(\varepsilon_2), \ldots, {}^{i_k}\widehat{x}_k(\varepsilon_k)] = 0, \tag{3-17}$$

sempre que $j+i_1+i_2+\cdots+i_k \equiv 0 \ (mod\ p)$ *e* $k \leq N$.

Demonstração. Escrevemos cada um dos quaserepresentantes ${}^{i_u}\widehat{x}_u(\varepsilon_u)$ como um comutador em representantes de níveis menores que s e usando $[a,[b,c]] = [a,b,c] - [a,c,b]$ expandimos os colchetes internos no comutador (3-17) e obtemos a um comutador envolvendo esses representantes e ${}^{j}y$.

Se ${}^{j}y \in {}^{j}K(s)$, então o comutador de (3-17) é igual a uma combinação linear de comutadores da forma (4-5), os quais são iguais a 0.

Se ${}^{j}y$ é um quaserepresentante de nível s, então o elemento ${}^{j}y$, visto como um comutador em representantes, é igual a uma combinação linear de comutadores simples em representantes, os quais começam com o único representante de nível s, que pertence a ${}^{j}K(s)$ por definição. Sendo assim, novamente o comutador (3-17) é igual a uma combinação linear de comutadores da forma (4-5), os quais são todos iguais a 0.

$\square$

Recapitulando...

Agora, após toda esta discussão sobre comutadores, representantes e quaserepresentantes, vamos recapitular o que desejamos demonstrar: queremos demonstrar que o subanel

$$M(p) = \langle {}^{1}K(h+1), {}^{2}K(h+1), \ldots, {}^{p-1}K(h+1) \rangle$$

é nilpotente de classe menor que $N = f(h+1, h, p)$. Faremos isto mostrando que todo comutador da forma (3-12) é igual a 0. No entanto, aplicando a Proposição 3.2 ao comutador (3-12), vemos que ele será escrito como uma combinação linear de comutadores, os quais possuem subcomutadores da forma (3-1) ou (3-2). Por isso, é suficiente demonstrar que os comutadores das formas (3-1) ou (3-2), são iguais a 0.

Primeiramente vamos demonstrar que os comutadores da forma (3-2), obtidos pela aplicação da Proposição 3.2 ao comutador (3-12), são iguais a 0, ou seja, comutadores da forma

$$[{}^{j}y, c_1, c_2, \ldots, c_h], \tag{3-18}$$

onde ${}^{j}y \in {}^{j}K(h+1)$ e cada $c_i \in {}^{0}L$ é um comutador cujas entradas são representantes de nível $h+1$, são iguais a 0.

Demonstração. Pelo Teorema HKK (2.16), o segmento inicial do comutador (3-15) de peso $h+1$

$$[{}^{j}y, {}^{v_1}\widehat{x}(1), {}^{v_2}\widehat{x}(2), \ldots, {}^{v_h}\widehat{x}(h)]$$

é igual a uma combinação linear de comutadores simples nas mesmas entradas ${}^{j}y, {}^{v_1}\widehat{x}(1), {}^{v_2}\widehat{x}(2), \ldots, {}^{v_h}\widehat{x}(h)$ com segmento inicial em ${}^{0}L$. Se tal segmento inicial contém ${}^{j}y$, então podemos escrevê-lo como uma combinação linear de comutadores simples começando com ${}^{j}y$, os quais são nulos, pelo Lema (3.12). Se tal segmento inicial não contém ${}^{j}y$, então ele deve conter exatamente um quaserepresentante ${}^{v_s}\widehat{x}(s)$ de nível máximo s. Logo podemos escrever tal segmento inicial como combinação linear de comutadores simples com as mesmas entradas e começando com ${}^{v_s}\widehat{x}(s)$ e, mais uma vez pelo Lema (3.12), temos que o comutador (3-15) é igual 0.

Finalmente, usando o Lema (3.11), concluímos que todo comutador da forma (3-14) e, consequentemente, todo comutador da forma (3-18), é igual a 0.

□

Agora, para completar a demonstração de que o subanel

$$M(p) = \langle {}^1K(h+1), {}^2K(h+1), \ldots, {}^{p-1}K(h+1) \rangle$$

é nilpotente de classe menor que $N = f(h+1, h, p)$, consideremos o caso onde temos um comutador da forma (3-1)

$$[{}^{k_1}w_1, {}^{k_2}w_2, \ldots, {}^{k_t}w_t], \quad {}^{k_i}w_i \in X \tag{3-19}$$

da Proposição 3.2, com $m = h+1$ e $n = h$, obtido do comutador (3-12). Pela escolha, o comutador (3-19) tem $h+1$ segmentos iniciais distintos com índices superiores somando zero módulo p

$$\begin{gathered} k_1 + k_2 + \cdots + k_{r_i} \equiv 0 \pmod{p}, \quad i = 1, 2, \ldots, h+1, \\ 1 < r_1 < r_2 < \cdots < r_{h+1} = t. \end{gathered}$$

Como o comutador (3-19) pertence a ${}^0L$ e possui como entradas representantes de nível $h+1$, podemos escrevê-lo como valor do mesmo padrão

$$[{}^{k_1}x(h+1), {}^{k_2}x(h+1), \ldots, {}^{k_t}x(h+1)]. \tag{3-20}$$

Isto nos permitirá obter comutadores numa forma tal que o Lema 3.12 é aplicável.

Agora escrevemos o segmento inicial de comprimento r_h do comutador (3-20) (o qual também pertence a ${}^0L$) como um valor do mesmo padrão em representantes de nível h. Em seguida, escrevemos o segmento de comprimento r_{h-1} como um valor do mesmo padrão em representantes de nível $h-1$, e assim por diante. Logo podemos escrever o comutador (3-19) como um comutador da forma

$$[{}^{k_1}x(1), \ldots, {}^{k_r}x(1), {}^{k_{r+1}}x(2) \ldots, {}^{k_s}x(2), \ldots, {}^{k_{u+1}}x(h+1), \ldots, {}^{k_t}x(h+1)]. \tag{3-21}$$

Este último tem uma propriedade desejada, como segue:

Lema 3.13 *Todo comutador da forma (3-21) é igual a uma combinação linear de comutadores da forma*

$$[{}^{\nu_1}\widehat{x}(1), {}^{\nu_2}\widehat{x}(2), \ldots, {}^{\nu_{h+1}}\widehat{x}(h+1), {}^{\nu_{h+2}}\widehat{x}(\varepsilon_{h+2}), \ldots] \tag{3-22}$$

cujo segmento inicial contém um quaserepresentante de cada nível $1, 2, \ldots, h+1$ *em ordem crescente de nível.*

A demonstração do lema acima é análoga à prova do Lema 3.11, a única diferença é que devemos colecionar segmentos iniciais da forma

$$[{}^{\nu_1}\widehat{x}(1), {}^{\nu_2}\widehat{x}(2), \ldots, {}^{\nu_s}\widehat{x}(s)], \quad s \geq 1.$$

De modo semelhante à demonstração do fato que o comutador (3-15) é 0, mostraremos que todo comutador da forma (3-22) também é 0. Para isto, utilizamos o Teorema HKK para mostrar que seu segmento inicial de peso $h+1$ é uma combinação linear de comutadores nas mesmas entradas ${}^{\nu_1}\widehat{x}(1), {}^{\nu_2}\widehat{x}(2), \ldots, {}^{\nu_{h+1}}\widehat{x}(h+1)$ e com segmento inicial em ${}^{0}L$, ou seja, com índices superiores somando 0 módulo p. Mais uma vez temos exatamente um quaserepresentante ${}^{\nu_s}\widehat{x}(s)$ de nível máximo s. Assim, escrevendo tal segmento inicial como combinação linear de comutadores simples nas mesmas entradas e começando com ${}^{\nu_s}\widehat{x}(s)$, temos pelo Lema (3.12) que todo comutador da forma (3-22) é 0.

Consequentemente, pelo Lema 3.13, todo comutador da forma (3-21), e portanto comutadores da forma (3-19), são iguais a 0.

Portanto, concluímos que o subanel

$$L_1 = \langle {}^{1}K(h+1), {}^{2}K(h+1), \ldots, {}^{p-1}K(h+1) \rangle$$

é nilpotente de classe menor que $N = f(h+1, h, p)$, e como já havíamos demonstrado, temos que L_1 possui índice $\{p,q\}$-limitado em $L = pL$.

Neste capítulo o principal resultado obtido afirma que um anel Lie $L = pL$ admitindo um automorfismo φ de ordem prima com número de pontos fixos igual a $|C_L(\varphi)| = q$, possui um subanel de índice $\{p,q\}$-limitado e classe de nilpotência p-limitada.

Com um olhar atento na demonstração do resultado principal, percebemos que tal demonstração pode ser adaptada de forma natural para um anel de Lie L com uma $\mathbb{Z}_p$-graduação.

Isto será essencial para provar que se $L = \bigoplus_{i=0}^{p-1} L_i$ é uma álgebra de Lie $\mathbb{Z}_p$-graduada sobre algum corpo, com L_0 de dimensão finita, digamos $\dim L_0 = m$ e tal que existem n componentes não triviais entre os L_i, então L contém uma subálgebra com classe de nilpotência limitada em termos somente de n e de codimensão finita limitada em termos de m e n, como veremos no Capítulo 4.

CAPÍTULO 4

Álgebras de Lie Quase Nilpotentes

Neste capítulo apresentamos um resultado devido a E. I. Khukhro e P. Shumyatsky [12], o qual afirma que uma álgebra de Lie L de dimensão finita sobre um corpo algebricamente fechado de característica 0 admitindo uma álgebra de derivações nilpotente D com n pesos em L e componente nula de Fitting de dimensão m, possui uma subálgebra N de codimensão $\{m,n\}$-limitada e classe de nilpotência n-limitada.

Suponha que uma álgebra de Lie L admite uma álgebra de derivações nilpotente possuindo n pesos e componente nula de Fitting de dimensão m. Neste caso, dizemos que L é *quase nilpontente* se L contém uma subálgebra N de codimensão limitada por uma função dependendo de m e n e a classe de nilpotência limitada em termos somente de n.

Definição 4.1 *Se D é uma álgebra de derivações de L, chamamos de* ***subálgebra constante*** *(em relação a D) a subálgebra formada pelos elementos x tais que $x^{\delta} = 0$, para todo $\delta \in D$. Dizemos que D é quase livre de constantes se a dimensão da subálgebra constante possui dimensão finita.*

Observação 4.2 *Dada uma álgebra de derivações D de um anel de Lie L, conforme a definição de componente nula de Fitting (ver 1.45), temos que a subálgebra constante (em relação a D) está contida na componente nula de Fitting (relativa a D).*

O próximo teorema afirma que se uma álgebra de Lie L de dimensão finita sobre um corpo algebricamente fechado de característica 0 admite uma álgebra de derivações nilpotente D quase livre de constantes, então L é quase nilpotente.

Teorema 4.3 *Seja L uma álgebra de Lie de dimensão finita sobre um corpo algebricamente fechado de característica 0. Suponha que L admita uma álgebra de derivações nilpotente D com n pesos em L e seja m a dimensão da componente nula de Fitting com respeito a D. Então L é quase nilpotente, ou seja, L contém uma subálgebra N de codimensão $\{m,n\}$-limitada e classe de nilpotência n-limitada. Se $m = 0$, então L é nilpotente de classe limitada por uma função dependendo somente de n.*

Pelo Teorema 1.47, podemos escrever

$$L = L_0 \oplus L_{\alpha_1} \oplus \cdots \oplus L_{\alpha_{n-1}},$$

onde os α_i são os pesos relativos a D e, pela Proposição 1.49, temos $[L_\alpha, L_\beta] \subseteq L_{\alpha+\beta}$, onde consideramos $\alpha+\beta = 0$, se $\alpha+\beta$ não for peso de L. Aqui L_0 representa a componente relativa ao peso $\alpha = 0$, que é a componente nula de Fitting.

Conforme demonstrado no Capítulo 1, os pesos de L pertencem a D^* (espaço dual de D). Seja A o subgrupo aditivo de D^* gerado pelos pesos, podemos naturalmente considerar L como uma álgebra de Lie A-graduada.

Por outro lado, L possui n pesos, donde podemos escrever

$$A = \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle.$$

Lembrando que a soma de pesos pode ser um peso, ou seja, é possível ocorrer $\alpha_i + \alpha_j = \alpha_k$, utilizamos o Lema 1.1 junto com a Observação 1.2 para encontrar um subgrupo B de A com índice primo p o qual não contém os pesos diferentes de 0.

Identificamos o grupo quociente A/B com $\mathbb{Z}_p$. Assim, induzimos em L uma $\mathbb{Z}_p$-graduação, onde as novas componentes L_i são as somas de todas as antigas componentes L_α, onde α percorre todos os pesos iguais a i módulo B.

Como os pesos não triviais não estão em B, a componente L_0 contém apenas o peso $\alpha = 0$. Ou seja, a dimensão de L_0 permanece a mesma, isto é, a dimensão de L_0 é igual a m.

Portanto, é suficiente demonstrar o seguinte teorema.

Teorema 4.4 *Seja p um primo e suponha que $L = \bigoplus_{i=0}^{p-1} L_i$ é uma álgebra de Lie $\mathbb{Z}_p$-graduada sobre algum corpo. Se L_0 tem dimensão finita, digamos $\dim L_0 = m$ e existem n componentes não triviais entre os L_i, então L é quase nilpotente, ou seja, L contém uma subálgebra N de codimensão $\{m,n\}$-limitada e classe de nilpotência n-limitada. Se $L_0 = 0$, então L é nilpotente de classe limitada em termos de n.*

É interessante observar que a classe de nilpotência e a codimensão não dependem do número primo p.

Na verdade, a demonstração do Teorema 4.4 perpassa integralmente as discussões do Capítulo 3. Basta usar a função $g(n)$ do Teorema 2.23, ao invés da função de Higman $h(p)$.

Faremos apenas os passos da demonstração.

Proposição 4.5 *Seja p um primo arbitrário e suponha que*

$$L = \bigoplus_{i=0}^{p-1} L_i$$

é uma álgebra de Lie $\mathbb{Z}_p$-graduada sobre algum corpo tal que existem exatamente n componentes não triviais entre os L_i. Para todos s e t inteiros positivos, existe uma função $f = f(s,t,n)$ com a seguinte propriedade. Todo comutador simples de peso f em elementos ${}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_f}x_f$, onde ${}^{i_j}x_j \in L_{i_j}$ é igual a uma combinação linear de comutadores, cada um tendo o mesmo conjunto de entradas $X = \{{}^{i_j}x_j \ : \ 1 \leq j \leq f\}$ e cada um contendo ou um subcomutador da forma

$$[{}^{k_1}w_1, {}^{k_2}w_2, \ldots, {}^{k_m}w_m], \quad {}^{k_i}w_i \in X, \tag{4-1}$$

o qual tem s segmentos iniciais com índices superiores somando 0 módulo p:

$$k_1 + k_2 + \cdots + k_{r_i} \equiv 0 \ (mod\ p), \quad i = 1, 2, \ldots, s$$
$$1 < r_1 < r_2 < \cdots < r_s = m,$$

ou contendo um subcomutador da forma

$$[{}^{k_0}w, c_1, c_2, \ldots, c_t], \tag{4-2}$$

onde ${}^{k_0}w \in X$ e cada um dos t comutadores c_i é simples e tem a forma

$$[{}^{k_1}u_1, {}^{k_2}u_2, \ldots, {}^{k_m}u_m], \quad {}^{k_j}u_j \in X,$$

com índices superiores somando 0 módulo p:

$$k_1 + k_2 + \cdots + k_m \equiv 0 \ (mod\ p).$$

Observação: *Podemos considerar $f(s,t,n) = 1 + \sum_{i=1}^{s-1} (g(n)+1)^{i+1} \cdot n^i$, onde $g(n)$ é a função do Teorema 2.23.*

Demonstração. Observe que se $n = p$, este teorema é exatamente a Proposição 3.2. Caso contrário, a demonstração segue os mesmos passos. Primeiro, adaptamos a Transformação HKK definida no capítulo anterior. Nesta nova transformação, usamos $g(n)$ ao invés do número $h(p)$ para construir (ou gerar) os elementos $c_i \in L_0$.

Conforme o Teorema 2.23, podemos escrever o segmento inicial de peso $g(n)+1$ do comutador

$$[{}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_f}x_f] \tag{4-3}$$

como uma combinação linear de comutadores simples com entradas em X e segmento inicial em L_0, ou seja, uma combinação linear de comutadores da forma

$$[{}^{k_1}x_{i_1}, {}^{k_2}x_{i_2}, \ldots, {}^{k_r}x_{i_r}, {}^{k_{r+1}}x_{i_{r+1}}, \ldots], \text{ com } r \leq g(n)+1, \quad k_1+k_2+\cdots+k_r \equiv 0 \ (mod\ p),$$

onde ${}^{k_j}x_{i_j} \in X$.

Como na Transformação HKK, para cada comutador desta combinação linear colocamos

$${}^{k_{r+1}}y_1 = -[{}^{k_1}x_{i_1}, {}^{k_2}x_{i_2}, \ldots, {}^{k_r}x_{i_r}, {}^{k_{r+1}}x_{i_{r+1}}]$$

(claramente ${}^{k_{r+1}}y_1 \in L_{k_{r+1}}$) e denotamos

$${}^{k_{r+s}}y_s = {}^{k_{r+s}}x_{i_{r+s}} \text{ para } s \geq 2.$$

Assim, concluímos que o comutador (4-3) é igual a uma combinação linear de comutadores simples da forma

$$[{}^{k_{r+1}}y_1, {}^{k_{r+2}}y_2, \ldots]. \tag{4-4}$$

Do mesmo modo que procedemos na demonstração da Proposição 3.2, executamos o mesmo procedimento várias vezes até conseguirmos um comutador de peso no máximo $g(n)+1$ e altura no mínimo $\sum_{i=1}^{m-1}(g(p)+1)^i \cdot n^i$. Portanto, o resultado segue conforme o desejado.

$\square$

Centralizadores Generalizados

Agora, precisamos construir centralizadores generalizados de nível $g(n)+1$. Para todo conjunto ordenado (de comprimento arbitrário k)

$$\overline{x} = ({}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_k}x_k)$$

de elementos ${}^{i_s}x_s \in L_{i_s}$, escolhemos $j \leq p-1$ tal que

$$j+i_1+i_2+\cdots+i_k \equiv 0 \ (mod \ p)$$

e definimos o homomorfismo

$$\vartheta_{\overline{x}}: \ {}^{j}y \longmapsto [{}^{j}y, {}^{i_1}x_1, {}^{i_2}x_2, \ldots, {}^{i_k}x_k], \ \ {}^{j}y \in L_j,$$

do subgrupo aditivo L_j em L_0.

Como $|L_0| = m$, temos o seguinte resultado.

Lema 4.6 *Para todo $\overline{x}$ como descrito acima, a codimensão $Ker \ \vartheta_{\overline{x}}$ em L_j é no máximo m.*

Definimos $K_j(1) = L_j$, para todo $j \neq 0$. Consideramos todos os padrões (conforme a Definição 3.8) em elementos das componentes L_i com $i \neq 0$, de peso no máximo $N(n) = f(g(n)+1, g(n), n)$, e que produzam algum elemento de L_0. Para cada padrão considerado, escolhemos uma base do subespaço de L_0 gerado por todos os seus valores. Os elementos que formam os valores que pertencem a alguma base são chamados de representantes de nível 1 e são denotados por ${}^{i_s}x_s(1)$. O total de representantes de nível 1 é $\{m,n\}$-limitado, pois $dimL_0 = m$ e existe somente uma quantidade n-limitada de padrões de peso no máximo $N(n)$.

Suponha que, para $t < g(n)+1$ e para cada $j = 1,2,\ldots,p-1$, já tenham sido construídos centralizadores de níveis $\leq t$, que são subgrupos aditivos de L_j,

$$K_j(1) \geq K_j(2) \geq \cdots \geq K_j(t)$$

de codimensões $\{m,n\}$-limitadas em L_j e que tenham sido fixados representantes ${}^{i_s}x_s(\varepsilon_s) \in L_{i_s}$ para $i_s \neq 0$ de níveis $\varepsilon_s \leq t$, cujo número total é $\{m,n\}$-limitado. Suponha também que, para todo $s \leq t$, os elementos ${}^{j}y \in K_j(s)$ possuam a seguinte propriedade de centralizadores com respeito aos representantes de níveis menores que s:

$$\begin{gathered}[{}^{j}y, {}^{i_1}x_1(\varepsilon_1), {}^{i_2}x_2(\varepsilon_2), \ldots, {}^{i_k}x_k(\varepsilon_k)] = 0, \ \text{sempre que} \ \ {}^{j}y \in K_j(s), \ \ k \leq N, \\ \varepsilon_j < s (j = 1,2,\ldots,k) \ e \ j+i_1+i_2+\cdots+i_k \equiv 0 \ (mod \ p). \end{gathered} \tag{4-5}$$

Agora para $j = 1,2,\ldots,p-1$, definimos

$$K_j(t+1) = \bigcap_{\overline{x}} Ker \ \vartheta_{\overline{x}} \ ,$$

onde $\overline{x} = ({}^{i_1}x_1(\varepsilon_1), {}^{i_2}x_2(\varepsilon_2), \dots, {}^{i_k}x_k(\varepsilon_k))$ percorre todos os conjuntos ordenados de comprimento $k \leq N(n)$ de representantes de níveis $\varepsilon_u \leq t$ (temos $j + i_1 + i_2 + \cdots + i_k \equiv 0 \ (mod\ p)$, de acordo com a definição do homomorfismo $\vartheta_{\overline{x}}$).

Como o número destes conjuntos ordenados é claramente $\{m,n\}$-limitado e a codimensão de cada subgrupo $Ker\ \vartheta_{\overline{x}}$ em L_j é no máximo m, temos que o índice do subgrupo $K_j(t+1)$ em L_j é também $\{m,n\}$-limitado. E ainda temos $K_j(t+1) \leq K_j(t)$.

Para cada padrão de peso no máximo $N(n)$, com todos os índices superiores diferentes de zero e somando 0 módulo p, consideramos o subespaço de L_0 gerado por todos os seus valores em elementos de $L_j(t)$. Fixamos uma base para o subespaço, a qual consiste de alguns dos valores do padrão. Os elementos de $L_j(t)$ que formam os valores que pertencem a alguma base são chamados de representantes de nível t e denotamos por ${}^{i_s}x_s(t+1)$. Claramente, o número de representantes de nível t é $\{m,n\}$-limitada.

Como apenas n das componentes L_i são não triviais, então existem no máximo n subespaços não triviais entre os $K_i(g(n)+1)$.

Obtendo a Subálgebra Nilpotente Desejada

Afirmamos que a subálgebra gerada por todos os centralizadores generalizados de nível $g(n)+1$,

$$M(n) = \langle K_1(g(n)+1), \dots, K_{p-1}(g(n)+1) \rangle, \tag{4-6}$$

é a subálgebra nilpotente desejada. A prova de que $M(n)$ é nilpotente de classe menor que $f(g(n)+1, g(n), n)$ segue os mesmos passos da demonstração do Capítulo 3 de que o subanel

$$M(p) = \langle {}^1K(h+1), {}^2K(h+1), \dots, {}^{p-1}K(h+1) \rangle$$

é nilpotente de classe menor que $N = f(h+1, h, p)$, a saber:

1) Verifica-se, via Lema 1.20, que é suficiente mostrar que todo comutador simples de peso $N(n)$ da forma

$$[{}^{i_1}y_1, {}^{i_2}y_2, \dots, {}^{i_{N(n)}}y_{N(n)}], \quad {}^{i_s}y_s \in K_{i_s}(h+1), \tag{4-7}$$

onde cada entrada percorre os geradores de $M(n)$, é igual a 0;

2) Demonstra-se que os subcomutadores da forma (4-1), como estabelecido pelo Teorema 4.5 aplicado ao comutador (4-7), são iguais a 0;

3) Demonstra-se que os subcomutadores da forma (4-2), como estabelecido pelo Teorema 4.5 aplicado ao comutador (4-7), são iguais a 0.

Demonstração. As demonstrações dos passos (1), (2) e (3), são idênticas às feitas no Capítulo 3 para o subanel $M(p)$, por isso não refaremos aqui.

Agora precisamos demonstrar que a subálgebra $M(n)$ possui codimensão $\{m,n\}$-limitada. Como $K_j(g(n)+1)$ é a interseção finita de subespaços de codimensão finita em L_j (veja Lema 4.6), pelo Corolário 1.4 a codimensão de $K_j(g(n)+1)$ em L_j é $\{m,n\}$-limitada. Assim, a codimensão de $M(n)$ em L_j é $\{m,n\}$-limitada, para $j=1,\dots,p-1$, pois $L_j(g(n)+1)\subseteq M(n)$. Portanto, como $L=\bigoplus_{i=0}^{p-1} L_i$ e apenas n das componentes são não triviais, segue que $M(n)$ tem codimensão finita em L.

Assim, concluímos a demonstração do Teorema 4.4.

□

Como no Teorema 4.3 consideramos a subálgebra constante diferente de 0, podemos enunciá-lo em uma forma onde D é uma subálgebra de L. Isto é mais conveniente para mostrar um resultado similar para álgebras de Lie localmente finitas com dimensão infinita.

Considerar D uma subálgebra de L significa que todos elementos de D são da forma adx, ou seja, todo elemento $\delta\in D$ é na verdade uma aplicação que leva $y\in L$ em $[x,y]$, para algum $x\in L$ fixado. Portanto, podemos identificar δ com $x\in L$. Desta forma obtemos o

Teorema 4.7 *Seja L uma álgebra de Lie localmente finita sobre um corpo algebricamente fechado de característica* 0. *Suponha que L contém uma subálgebra nilpotente D com n pesos em L tal que a componente nula de Fitting com respeito a D é de dimensão finita m. Então L contém uma subálgebra N de codimensão finita limitada por uma função de m e n e a classe de nilpotência de N é limitada por uma função dependendo somente de n.*

Demonstração. Primeiramente precisamos demonstrar que $L=\sum_{\alpha} L_\alpha$, onde os L_α são os espaços de pesos de L, relativos a D.

Como por hipótese D é nilpotente, temos que D está contido na componente nula de Fitting, pois, dado $x \in D$, existe i tal que,

$$[\underbrace{x, \ldots, x}_{i}, y] = 0,$$

para todo $y \in D$. Assim, D possui dimensão finita.

Agora, dado $v \in L$, a subálgebra $S = \langle D, v \rangle$ é finitamente gerada, pois D é finitamente gerado. Logo S tem dimensão finita. Sendo assim, o Teorema 1.47 garante que $S = \sum_{\beta} S_{\beta}$, onde os S_{β} são os espaços de peso de S, relativos a D. Por outro lado, pela definição de espaço de peso, dado $x \in D$ e $u \in S_{\beta} \neq 0$ temos $(x - \beta(x)I)^m(u) = 0$, para algum m (dependendo de u e x). Então u pertence à algum espaço de peso L_{α}, ou seja, existe L_{α} tal que $L_{\alpha} \supseteq S_{\beta}$.

Portando, $v \in \sum_{\alpha} L_{\alpha}$ e consequentemente $L = \sum_{\alpha} L_{\alpha}$, ou melhor, L é A-graduada, onde A é o subgrupo de D^*, gerado por todos os pesos. Como na demonstração do Teorema 4.3, temos que é suficiente demonstrar o Teorema 4.4.

$\square$

4.0.1 Comentários Finais

É interessante analisar a evolução do estudo sobre automorfismos de álgebras de Lie e comparar os Teoremas 4.3 e 4.7 com alguns resultados já existentes, em particular os resultados obtidos nos Capítulos 2 e 3 (os quais naturalmente valem para álgebras de Lie).

Seja L uma álgebra de Lie de dimensão finita admitindo um automorfismo regular φ de ordem n. Em 1955 Borel e Mostow [1] provaram que L é solúvel.

Agora seja L uma álgebra de Lie não necessariamente de dimensão finita. Suponha que L admite um automorfismo regular de ordem n. Higman [4] provou, em 1957, que se n é um número primo, então L é nilpotente de classe limitada em termos de n. Para n um número natural qualquer, Kreknin [13] provou, em 1963, que L é solúvel de comprimento derivado limitado em termos de n.

Agora seja φ quase regular, isto é, a subálgebra L gerada pelos pontos fixos possui dimensão finita igual a m. Para n um número primo, Khukhro [8] demonstrou, em 1992, que L é quase nilpotente (é o resultado discutido no Capítulo 3) e, para n um número natural qualquer, Makarenko e Khukhro [14] provaram, em 2004, que L é quase solúvel (a definição de quase solúvel é análoga à definição de quase nilpotente, basta trocar o termo nilpotente por solúvel).

Finalmente temos o resultado principal do Capítulo 4, provado em 2006 por Khukhro e Shumyatsky [12], cuja demonstração usa o fato de que a prova proposta por Khukhro [8] para o caso de um automorfismo quase regular de ordem prima pode ser generalizada para álgebras de Lie $\mathbb{Z}_p$-graduadas.

Conjectura de Higman

O limite superior para função de Higman $h(p)$ apresentado nos Corolários 2.16, 2.17 e 2.18 é muito maior que os valores de $h(p)$ previstos pela Conjectura de Higman, a qual afirma que $h(p) = \frac{p^2-1}{4}$, para $p > 2$ e $h(2) = 1$.

Em [4], Higman construiu exemplos mostrando que $h(p) \geq \frac{p^2-1}{4}$, para $p > 2$. Neste mesmo trabalho, Higman mostrou que $h(5) = 6$ e, em [6], Hughes mostrou que $h(7) = 12$.

A demonstração que $h(2) = 1$ e $h(3) = 2$ é bastante simples. Para provar o caso onde $p = 2$, devemos considerar, em um anel de Lie $\mathbb{Z}_2$-graduado $L = {}^0L + {}^1L$, apenas os comutadores de peso 2 em elementos de ${}^1L$, os quais claramente pertencem a ${}^0L$. Para provar o caso $p = 3$, somente temos que considerar, em um anel de Lie $\mathbb{Z}_3$-graduado $L = {}^0L + {}^1L + {}^2L$, comutadores $[a,b,c]$ de peso 3 em elementos a,b,c, ou de ${}^1L$ ou de ${}^2L$. Se $a,b,c \in {}^1L$, então $[a,b,c] \in {}^0L$. Nos outros casos, podemos assumir $a \in {}^1L$. Sendo assim, se $b \in {}^2L$, temos $[a,b] \in {}^0L$, o que implica $[a,b,c] \in {}_{id}\langle {}^0L \rangle$. Se $b \in {}^1L$ e $c \in {}^2L$, aplicando a Identidade de Jacobi, temos

$$[a,b,c] = [a,c,b] + [a,[b,c]] \in {}_{id}\langle {}^0L \rangle,$$

uma vez que, $[a,c]$ e $[b,c]$ pertencem a ${}^0L$.

Álgebras de Lie Quase Solúveis

O teorema principal do trabalho de Makarenko e Khukhro [14] sobre álgebras de Lie quase solúveis é:

Teorema 4.8 *Se uma álgebra de Lie L admite um automorfismo φ de ordem n cuja subálgebra dos pontos fixos possui dimensão finita igual a m, então L possui um ideal de* *comprimento derivado limitado por uma função somente de n e de codimensão limitada por uma função de m e n.*

Assim como vários resultados apresentados aqui, este também possui sua versão para álgebras de Lie $\mathbb{Z}_n$-graduadas.

Teorema 4.9 *Seja $L = L_0 \oplus L_1 \oplus \cdots \oplus L_{n-1}$ uma álgebra de Lie $\mathbb{Z}_n$-graduada. Se a componente L_0 tem dimensão finita igual m, então L possui um ideal solúvel de comprimento derivado limitado por uma função somente de n e de codimensão limitada por uma função de m e n.*

As técnicas usadas nas demonstrações dos teoremas acima são semelhantes às apresentadas no Capítulo 3. A principal diferença é que em um anel de Lie $L = \langle X \rangle$ não basta verificar a identidade de variedades solúveis apenas nos geradores.

Grupos Nilpotentes Admitindo Automorfismos de Ordens Primas

Usando o Teorema HKK podemos obter uma cota superior para a classe de nilpotência de um grupo nilpotente admitindo um automorfismo regular de ordem prima p.

Teorema 4.10 (Higman) *Se um grupo nilpotente G admite um automorfismo regular φ de ordem prima p, então a classe de nilpotência de G é no máximo $h(p)$, onde $h(p)$ é a função de Higman.*

A demonstração deste resultado é obtida via o anel de Lie associado ao grupo G

$$L(G) = \bigoplus_{k=1}^{\infty} \gamma_k(G)/\gamma_{k+1}(G)$$

e pode ser encontrada em [9]. No mesmo sentido, temos um resultado sobre p-grupos admitindo um automorfismo quase regular.

Teorema 4.11 *Se um p-grupo nilpotente P admite um automorfismo φ de ordem prima p com exatamente p^m pontos fixos, então P possui um subgrupo de índice $\{p,m\}$-limitado e nilpotente de classe no máximo h(p), onde h(p) é a função de Higman.*

Referências Bibliográficas

[1] BOREL, A; MOSTOW, G. **On semi-simple automorphisms of Lie Algebras**. Ann. Math. 61, 389-405, 1955.

[2] DUMMIT, D. S; FOOTE, R. M. **Abstract algebra**. University of Vermont, 1999.

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

[4] HIGMAN, G. **Groups e rings which have automorphisms without non-trivial fixed elements**. J. London. Math. Soc. 32, 321-334, 1957.

[5] HOFFMAN, K; KUNZE, R. **Álgebra Linear**. Livros Técnicos e Científicos 2ed., 1971.

[6] HUGHES, I. **Groups with fixed-point-free automorphisms**. Math. Rep. Acad. Sci. Canada 7, 61-66, 1985.

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

[8] KHUKHRO, E. I. **Groups and Lie rings admitting an almost regular automorphisms of prime order**. English Trasl. in Math. USSR Sb. 71, 51-63, 1992.

[9] KHUKHRO, E. I. **Nilpotent groups and their automorphisms**. Walter de Gruyter & Co., Berlin, 1993.

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

[11] KHUKHRO, E. I. **Finite groups of bounded rank with an almost regular Automorphism of Prime Order**. Siberian J. Math. Vol 43, 955-962, 2002.

[12] KHUKHRO, E. I; SHUMYATSKY, P. **Lie Algebras with almost constant-free derivations**. Elsevier, J. Algebra 306, 544-551, 2006.

[13] KREKNIN, V. A. **The solubility of Lie algebras with regular automorphisms of finite period**. English Trasl. in Math. USSR Doklady 4, 683-685, 1963.

[14] MAKARENKO, N. Y; KHUKHRO, E. **Almost solubility of Lie algebras with almost regular automorphisms**. J. Algebra 277, 370-407, 2004.

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

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

[17] SHALEV, A. **Automorphisms of finite groups of bounded rank**. Israel J. Math. Soc. 82, 395-404, 1993.

[18] SILVA, J. C. **Álgebras de Lie de Derivações Livres de Constantes**. Dissertação de Mestrado: Brasília, UnB, 2004.