Katiucy Freire de Oliveira, Jhone Caldeira

Instituto de Matemática e Estatística, Universidade Federal de Goiás, CEP 74001-970 - Goiânia, Goiás.

katiucyfreire16@hotmail.com, jhone@mat.ufg.br

Um Estudo sobre Grupos Nilpotentes e Anéis de Lie Associados

PALAVRAS-CHAVE: Grupos, Nilpotência, Anéis de Lie, Automorfismos.

1 INTRODUÇÃO

O estudo de grupos nilpotentes e automorfismos permitem uma abordagem bastante interessante de parte da teoria algébrica e está diretamente relacionado com importantes problemas de interesse da comunidade científica matemática. Muitos problemas na Teoria dos Grupos podem ser tratados com a teoria dos grupos nilpotentes e seus automorfismos. Além disso, a importancia da teoria das álgebras de Lie está ligada às discussões sobre grupos nilpotentes e seus automorfismos. Então, neste trabalho, faremos um estudo sobre grupos nilpotentes, tratando os principais elementos básicos desta teoria, bem como estudaremos elementos da teoria dos anéis de Lie e discutiremos a construção de anéis de Lie associados a grupos.

2 OBJETIVOS

O objetivo deste trabalho é apresentar um breve estudo introdutório da Teoria dos Grupos Nilpotentes e da Teoria dos Anéis de Lie. Estudando as propriedades especiais de anéis sobre grupos nilpotentes e construir anéis de Lie associados a grupos nilpotentes.

3 DEFINIÇÕES PRELIMINARES e GRUPOS NILPOTENTES

Nesta seção apresentaremos alguns conceitos e resultados necessários para o entendimento das discussões futuras.

Seja K um anel comutativo. Um grupo aditivo M é dito ser um K-módulo quando admite a multiplicação por elementos de K, isto é, $K \times M \to M$, e ainda satisfaz os seguintes axiomas:

$1a = a; 1 \in K;$

$(\alpha + \beta)a = \alpha a + \beta a;$

$(\alpha\beta)a = \alpha(\beta a), \forall \alpha, \beta \in K$ e $a \in M$.

Observamos que todo grupo abeliano pode ser considerado naturalmente como um $\mathbb{Z}-$módulo.

Definição 3.1. Os elementos $m_1, m_2, \ldots, m_s$ geram o $K-$módulo M se cada elemento $m \in M$ pode ser expresso na forma:

$$m = \sum k_i m_i, \text{ com } k_i \in K.$$

Então $m_1, m_2, \dots, m_s$ são os *geradores do* $K-$*módulo*.

Definição 3.2. Seja M um conjunto de geradores de um grupo. Dizemos que G é livremente gerado por M, ou um grupo livre em M, se existe apenas as relações triviais entre os elementos de M.

É imediato o seguinte corolário:

Corolário 3.2.1. Todo grupo G é um quociente de um grupo livre, isto é, todo $K-$módulo $s-$gerado tem uma imagem homomórfica de $K-$módulo livre $s-$gerado:

$$e_1K \oplus e_2K \oplus \cdots \oplus e_sK.$$

O grupo abeliano $e_iK = \{e_i|k \in K\}$ é isomorfo a K, para todo $1 \leq i \leq s$.

Definição 3.3. Sejam A e B dois $K-$módulos. Seu produto tensorial $A \otimes_k B$ é definido como o módulo quociente de $K-$módulo livre com $a \otimes b$ geradores livres, $a \in A$ e $b \in B$, do submódulo gerado de todos os elementos de forma que:

$$\begin{gathered} k(a_0 \otimes b_0) = ka_0 \otimes b_0, ka_0 \otimes b_0 = a_0 \otimes kb_0, \\ a_0 \otimes (b_1 + b_2) = a_0 \otimes b_1 + a_0 \otimes b_2, \\ (a_1 + a_2) \otimes b_0 = a_1 \otimes b_0 + a_2 \otimes b_0, \\ \forall k \in K, a_i \in A \text{ e } b_i \in B; i = 0, 1, 2. \end{gathered}$$

Se os elementos $a_1, \dots, a_s$ geram um $K-$módulo A e os elementos $b_1, \dots, b_r$ geram um $K-$módulo B, então os sr elementos $a_i \otimes b_j$, $i = 1, \dots, s; j = 1, \dots, r$, geram o $K-$módulo $A \otimes_k B$.

E se os $K-$módulos $M = \oplus M_i$ e $N = \oplus N_j$ são decompostos em somas diretas de $K-$módulos M_i e M_j, então o produto tensorial $M \otimes_k N$ é decomposto em somas diretas:

$$M \otimes_k N = \oplus(M_i \otimes N_j) \text{ de } K-\text{módulos } M_i \otimes_k N_j.$$

Definição 3.4. Para cada $n \geq 1$ e $n \in \mathbb{N}$, as $n-$ésimas raízes da unidade são os números complexos Z que satisfazem a equação $Z^n = 1$, ou seja, é uma raiz do polinômio $X^n - 1$:

$$1, \omega, \omega^2, \dots, \omega^{n-1}.$$

Assim podemos dizer que uma $n-$ésima raiz primitiva da unidade satisfaz:

$$Z^k \neq 1; k = 1, 2, \dots, n-1,$$

ou seja, quando ela não é também uma raiz $m-$ésima da unidade para $m \leq n$.

Seja F um corpo. Quando se constrói uma extensão de um corpo, se busca um conjunto maior no qual as operações soma e produto sigam funcionando bem e além disso possamos resolver equações polinomiais. Denotamos $F[\omega]$ o corpo obtido a partir de F pela adjunção do elemento ω ao corpo F, onde ω não pertence a F. Isso nos leva à seguinte proposição:

Proposição 3.5. Seja ω uma $n-$ésima raiz primitiva da unidade. Se A é um subgrupo de um grupo abeliano B, então:

$$(A \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]) \cap B \otimes 1 = A \otimes 1,$$

onde $\mathbb{Z}$ é o conjunto dos números inteiros.

Demonstração. Se ω é uma raiz $n-$ésima primitiva da unidade, então uma base para $\mathbb{Z}[\omega]$ sobre $\mathbb{Z}$ será $b = \{1, a, a^2, \ldots, a^{f(n)-1}\}$, onde $f(n)$ é a função de Euler. Logo $\mathbb{Z}[\omega] = \mathbb{Z} \oplus_{\mathbb{Z}} \mathbb{Z}\omega \oplus_{\mathbb{Z}} \mathbb{Z}\omega^2 \oplus_{\mathbb{Z}} \cdots \oplus_{\mathbb{Z}} \mathbb{Z}\omega^{f(n)-1}$. Agora olhemos separadamente os elementos da interseção:

$$\begin{gathered} A \oplus_{\mathbb{Z}} \mathbb{Z}[\omega] = A \otimes_{\mathbb{Z}} \mathbb{Z} \oplus A \otimes_{\mathbb{Z}} \mathbb{Z}\omega \oplus \cdots \oplus A \otimes_{\mathbb{Z}} \mathbb{Z}\omega^{f(n)-1}, \\ B \oplus_{\mathbb{Z}} \mathbb{Z}[\omega] = B \otimes_{\mathbb{Z}} \mathbb{Z} \oplus B \otimes_{\mathbb{Z}} \mathbb{Z}\omega \oplus \cdots \oplus B \otimes_{\mathbb{Z}} \mathbb{Z}\omega^{f(n)-1}, \\ B \oplus 1 = \{b \otimes_{\mathbb{Z}} 1; b \in B\}. \end{gathered}$$

Como A é um subgrupo de B, então A está em B, logo $A \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$ está imerso naturalmente em $B \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$. Portanto,

$$(A \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]) \cap B \otimes 1 = A \otimes 1.$$

$\square$

3.1 Grupos Solúveis e Nilpotentes

Nesta seção apresentamos fatos sobre comutadores e grupos solúveis, exibindo algumas propriedades relacionadas a eles. Também definimos grupos nilpotentes e séries centrais de um grupo.

Definição 3.6. Se G é um grupo e $x, y \in G$, então o comutador entre x e y, $[x, y]$, é o elemento

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

Definimos comutador de peso $n \geq 2$ recursivamente da seguinte forma. Sejam $x_1, x_2, \ldots, x_n, y \in G$ então,

$$\begin{gathered} [x_1] = x_1 \\ \vdots \\ [x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]. \end{gathered}$$

Notação: $[x\ ,\ _n y] = [x, \underbrace{y, \ldots, y}_{n}]$.

Proposição 3.6.1. Sejam $x, y, z, t \in G$. Temos que:
I) $ab = ba[a, b], a^b = a[a, b]$;
II) $[x, y] = [y, x]^{-1}$;
III) $[x, y] = 1$, se $xy = yx$;
IV) $[x, y]^z = [x^z, y^z]$;
V) $[xy, z] = [x, z]^y[y, z] = [x, z][[x, z], y][y, z]$;
VI) $[x, y]z = z[x^z, y^z]$;
VII) $[x, y, z] = [x, y]^{-1}[x, y]^z$;
VII) (Identidade de Hall-Witt) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$.

Definição 3.6.2. O subgrupo comutador $[M, N]$ dos subconjuntos arbitrários M e N de um grupo é definido por:

$$[M, N] = \langle [m, n]; m \in M \text{ e } n \in N \rangle,$$

ou seja, é o conjunto de todos os produtos finitos de comutadores do tipo $[m, n]$ ou inversos destes.

Definição 3.7. Definimos a série derivada de um grupo G por:

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(n)} \supset \cdots,$$

onde $G^{(n)}$ é dito o $n-$ésimo grupo derivado de G, e os membros da série derivada de G são dados por

$$\begin{gathered} G' = G^{(1)} = [G, G] \\ G'' = G^{(2)} = [G', G'] \\ \vdots \\ G^{(s+1)} = [G^{(s)}, G^{(s)}], \end{gathered}$$

onde G' é chamado subgrupo derivado de G.

Definição 3.8. A cadeia de subgrupos $1 \leq K_1 \leq K_2 \leq \cdots \leq K_n = G$ é dito ser uma série de G de comprimento n. A série é dita subnormal quando satisfaz a condição:

$$K_i \trianglelefteq K_{i+1}, \forall\, i.$$

E é dita normal quando satisfaz a condição

$$K_i \trianglelefteq G, \forall\, i.$$

O grupo quociente $\frac{K_{i+1}}{K_i}$ de uma série subnormal é também chamado quociente ou fator.

Definição 3.9. Um grupo G diz-se solúvel se admite uma série subnormal

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

onde cada subgrupo G_{i-1} é normal em G_i e o grupo quociente $\frac{G_i}{G_{i-1}}, 1 \leq i \leq n$, é abeliano.

Exemplo 3.9. Todo grupo abeliano é solúvel.

Lema 3.10. Seja H um subgrupo normal de um grupo G. Então, o grupo quociente G/H é abeliano se, e somente se, $G^{(1)} \subset H$.

Teorema 3.11. Um grupo G é solúvel se e somente se sua série derivada termina; isto é, se existe um inteiro positivo n tal que $G^{(n)} = \{1\}$.

Demonstração. Vamos assumir inicialmente que existe um inteiro positivo n tal que $G^{(n)} = \{1\}$. Então, obviamente,

$$G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(n)} = \{1\}$$

é uma série subnormal abeliana para G. Reciprocamente, suponhamos que G contém uma série subnormal abeliana

$$G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}.$$

Como todo quociente $\frac{G_i}{G_{i-1}}, 0 \leq i \leq n-1$, é abeliano, segue do Lema 3.10. e de um argumento de indução que $G^{(i)} \subset G_i, 1 \leq i \leq n$. Logo, temos em particular que $G^{(n)} = \{1\}$.

□

Temos dois resultados:

I) Subgrupos e grupos quocientes de grupos solúveis são solúveis. Valendo também a recíproca deste resultado.

II) Seja H um subgrupo normal de um grupo G. Se ambos H e G/H são solúveis, então G é solúvel.

Agora podemos estudar uma classe de grupos que, de certa forma está entre a classe do grupo abelianos e a classe dos grupos solúveis.

Definição 3.12. Um grupo G diz-se nilpotente se ele contém uma série de subgrupos

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

tal que cada subgrupo G_{i-1} é normal em G e cada quociente $\frac{G_i}{G_{i-1}}$ está contido no centro de $\frac{G}{G_{i-1}}, 1 \leq i \leq n$. Uma tal série de subgrupos de G diz-se uma série central de G.

Exemplo 3.12. Todo grupo abeliano é nilpotente.

Definição 3.12.1. Denotaremos por $\gamma_i(G)$ os membros da série central inferior de G:

$$\gamma_1(G) = G,\ \ \gamma_2(G) = [\gamma_1(G), G],\ \ \ldots\ ,\ \ \gamma_{s+1}(G) = [\gamma_s, G].$$

Dessa forma

$$G = \gamma_1(G) \supset \gamma_2(G) \supset \cdots \supset \gamma_{s+1}(G).$$

Definição 3.12.2. Sendo $Z(G) = \{z \in G; zg = gz\ \forall g \in G\}$ o centro de G, que é um subgrupo normal de G, denotaremos por $\zeta_i(G)$ os membros a série central superior de G, onde $\zeta_0(G) = 1, \zeta_1(G) = Z(G)$ e indutivamente $\zeta_i(G)$ como sendo o único subgrupo de G tal que $\frac{\zeta_i(G)}{\zeta_{i-1}} = Z(G/\zeta_{i-1}(G))$. Esse subgrupo chama-se $i-$ésimo centro de G.

$$1 = \zeta_0(G) \subset \zeta_1(G) \subset \cdots \subset \zeta_n(G) \subset \cdots$$

Teorema 3.13. Seja G um grupo. São equivalentes:

I) G é nilpotente.

II) Existe um inteiro positivo m tal que $\zeta_m(G) = G$.

III) Existe um inteiro positivo n tal que $\gamma_n(G) = 1$.

Proposição 3.14 Subgrupos e produtos diretos finitos de grupos nilpotentes são também nilpotentes.

4 ANÉIS DE LIE ASSOCIADOS

Aqui apresentamos a construção padrão do anel de Lie associado a um grupo G, com base na menor série central de G. Ainda, provaremos a nilpotência de grupos solúveis de expoente primo, como ilustração das vantagens de usar anéis de Lie que são objetos mais lineares do que grupos. Ainda trataremos dos anéis de Lie de um grupo de expoente primo. Por fim, apresentaremos teoremas sobre a nilpotência de anéis de Lie solúveis satisfazendo as condições de Engel.

Começamos definindo anéis de Lie e apresentando algumas de suas propriedades.

4.1 Anéis de Lie

Um anel de Lie é um anel não associativo sem identidade, cuja multiplicação, que é usualmente denotada por $[a, b]$, satifaz os seguintes axiomas:
I) $[a, a] = 0$;
II) $[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$. (Identidade de Jacobi)
Ou seja, um anel de Lie não é comutativo e satisfaz a Identidade de Jacobi.

Observações.

- A partir da identidade Jacobiana não é difícil deduzir que, se I e J são ideais de um anel de Lie, então o subgrupo aditivo gerado pelo conjunto dos comutadores $\{[a, b] | a \in I, b \in J\}$ é também um ideal do anel de Lie. Este é denotado por $[I, J]$.

- Se A e B são subconjuntos de um anel de Lie, então $A + B$ é denotado por: $A + B = \{a + b | a \in A \text{ e } b \in B\}$. Assim, se A e B são subanéis, então $A + B$ também é um subanel, e se A e B são ideais, então $A + B$ é também um ideal.

- Os teoremas de homomorfismos de anéis de Lie são análogos aos teoremas de homomorfismos de grupos.

- Se L_1 e L_2 são R-álgebras de Lie, um homomorfismo de Lie é um homomorfismo de $R-$módulos $\varphi : L_1 \longrightarrow L_2$ tal que $([a, b])\varphi = [(a)\varphi, (b)\varphi]$,para todo $a, b \in L_1$. Um isomorfismo de Lie entre L_1 e L_2 é um homomorfismo de Lie bijetor e um automorfismo de Lie é um isomorfismo de Lie de uma álgebra de Lie em si mesma.

- Se $L = \langle X \rangle$ é um anel de Lie gerado pelo conjunto X, então $L = \sum_i L_i$, onde L_i é a componente homogênea de L de peso i, que é o subgrupo aditivo gerado por todos os comutadores de peso i em elementos de X.

Definição 4.1.1. Os membros da série central inferior, $\gamma_i(L)$, do anel de Lie L são definidos por indução, como seguinte:

$$\gamma_1(L) = L, \ \ldots, \ \gamma_{s+1}(L) = [\gamma_s(L), L]$$

(às vezes são denotados também por $L^i = \gamma_i(L)$).

Definição 4.1.2. Os membros da série derivada são também definidos por indução:

$$L' = \gamma_2(L) = L^2, \ \ L'' = L^{(2)} = [L', L'], \ \ldots, \ L^{(s+1)} = [L^{(s)}, L(s)].$$

É fácil ver que $L^{(s)} \subseteq \gamma_{2^s}(L)$, para todo $s \in \mathbb{N}$.

É fácil ver também que, se $L = \langle X \rangle$, então $\gamma_k(L) = \sum_{i=k}^{\infty} L_i$, onde L_i são as componentes homogêneas do anel de Lie L de peso i.

4.2 Resultados Análogos a Teoremas sobre Grupos

Podemos definir anéis de Lie nilpotentes usando o seguinte teorema.

Teorema 4.2.1. As seguintes condições são equivalentes para um anel de Lie L:
a) $\gamma_{c+1}(L) = 0$;
b) L tem uma série central de comprimento c

$$L = L_1 \geq L_2 \geq \cdots \geq L_c \geq L_{c+1} = 0,$$

isto é, de tal forma que $[L_i, L] \leq L_{i+1} \forall \ i = 1, 2, \ldots, c$.
c) O anel de Lie L satisfaz a identidade

$$[x_1, x_2, \ldots, x_{c+1}] = 0.$$

Antes de enuciar a Definição 4.2.2. e os teoremas que a seguem, comentamos fatos sobre grupos definidos por identidades. Isto nos dará uma ilustração dessa definição e dos teoremas seguintes. Lembremos que as definições para anéis de Lie são análogas às de grupos.

Seja G um grupo. Sabemos que G é abeliano se, e somente se, $[x, y] = 1$, para todos $x, y \in G$. Assim, grupos abelianos são definidos pela identidade $[x, y] = 1$. A identidade $[\ldots[[x_1, x_2], x_3], \ldots, x_{c+1}] = 1$ define a variedade dos grupos nilpotentes de classe no máximo c, e a identidade $\delta_k = 1$ de 2^k variáveis, onde δ_k é definida recursivamente por $\delta_0(x) = [x], \delta_1 = [x_1, x_2], \delta_{k+1} = [\delta_k(x_1, \ldots, x_{2^k}), \delta_k(x_{2^k+1}, \ldots, x_{2^{k+1}})]$, define a variedade dos grupos solúveis de comprimento derivado k. Outra maneira de definir estas classes de grupos é em termos da existência de uma série de subgrupos normais com fatores centrais ou abelianos, respectivamente.

Analisemos a solubilidade e como se comporta esse grupo:

$$
\begin{array}{ll}
\delta_0(x) = x & 2^0 \text{ variáveis} \\
\delta_1(x_1, x_2) = [x_1, x_2] = [\delta_0(x_1), \delta_0(x_2)] & 2^1 \text{ variáveis} \\
\delta_2(x_1, x_2, x_3, x_4) = [\delta_1(x_1, x_2), \delta_1(x_3, x_4)] = [[x_1, x_2], [x_3, x_4]] & 2^2 \text{ variáveis} \\
\vdots & \vdots \\
\delta_n(x_1, \ldots, x_{2^n}) = [\delta_{n-1}(x_1, \ldots, x_{2^{n-1}}), \delta_{n-1}(x_{2^{n-1}+1}, \ldots, x_{2^n})] & 2^n \text{ variáveis.}
\end{array}
$$

Temos então que G é solúvel de comprimento derivado n se, e somente se,

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

para todos os elementos em G.

E verificamos também a sua nilpotência:

$$
\begin{array}{l}
\gamma_1(x) = x \\
\gamma_2(x_1, x_2) = [\gamma_1(x_1), \gamma_1(x_2)] = [x_1, x_2] \\
\gamma_3(x_1, x_2, x_3) = [\gamma_2(x_1, x_2), x_3] = [[x_1, x_2], x_3] \\
\vdots \\
\gamma_{n+1}(x_1, x_2, \ldots, x_{n+1}) = [\gamma_n(x_1, x_2, \ldots, x_n), x_{n+1}].
\end{array}
$$

Então G é nilpotente de classe n se, e somente se

$$\gamma_{n+1}(x_1, x_2, \ldots, x_{n+1}) = [\gamma_n(x_1, x_2, \ldots, x_n), x_{n+1}] = 1,$$

para todos os elementos em G.

Com isso, podemos apresentar a seguinte definição:

Definição 4.2.2. Um anel de Lie L satisfazendo o teorema acima é dito nilpotente, e o menor número natural c com a propriedade indicada, é chamado classe de nilpotência de L.

Quando dizemos que um anel de Lie é nilpotente de classe c estamos querendo dizer que ele é nilpotente de classe $\leq c$. E ainda percebemos que para saber se um anel de Lie é nilpotente basta verificar se seus geradores são nilpotentes.

Teorema 4.2.3. Se um anel de Lie é gerado por um subconjunto M, então ele é nilpotente de classe $\leq c$, se, e somente se, todo comutador de peso $c + 1$ nos elementos de M é igual a 0.

Proposição 4.2.4. Suponha L um anel de Lie arbritário e k um inteiro positivo. Então:
a) o ideal $\gamma_k(L)$ contém todos os comutadores de peso $\geq k$ nos elementos de L.
b) o subgrupo aditivo $\gamma_k(L)$ é gerado pelos comutadores simples de peso k nos elementos de L.
c) se $L = \langle M \rangle$, então o subgrupo aditivo $\gamma_k(L)$ é gerado pelos comutadores simples de peso $\geq k$ nos elementos de M. É também gerado pelos comutadores básicos de peso $\geq k$ em elementos de M. Em particular, se L é finitamente gerado, então para cada $k \in \mathbb{N}$, o subgrupo aditivo $\frac{\gamma_k(L)}{\gamma_{k+1}(L)}$ é também finitamente gerado, por um número $(k, s)-$limitado de geradores.

Teorema 4.2.5. As seguintes condições são equivalentes para um anel de Lie L.
a) $L^{(s)} = 0$;
b) L tem uma série de ideais de comprimento s com fatores abelianos

$$L = L_0 \trianglelefteq L_1 \trianglelefteq \cdots \trianglelefteq L_{s-1} \trianglelefteq L_s = 0,$$

tal que $[L_i, L_i] \leq L_{i+1}$, para todo $i = 0, 1, \ldots, s - 1$.
c) L satisfaz a identidade

$$\delta_s(x_1, x_2, \ldots, x_{2^s}) = 0.$$

Um anel de Lie satisfazendo essas condições é dito ser solúvel e o menor número s com a propriedade indicada, é chamado comprimento derivado de L. Podemos chamá-lo de "índice de solubilidade".

Muitas vezes é dito que um anel de Lie é solúvel de comprimento derivado s, significando que é solúvel de comprimento derivado $\leq s$.

Observe, que o análogo do Teorema 4.2.3 não se aplica a solubilidade, pois existem exemplos de anéis de Lie $G = \langle M \rangle$ com $\delta_k(m_1, m_2, \ldots, m_{2^k}) = 1$, para certos $m_1, m_2, \ldots, m_{2^k} \in M$ que, entretanto, não são solúveis de comprimento derivado k.

4.3 Construindo um Anel de Lie Associado a um Grupo

Primeiramente daremos a definição de anel de Lie associado, que é definido em termos da série central inferior de um grupo. Seja G um grupo. Vamos colocar $\gamma_k = \gamma_k(G), k \in \mathbb{N}$, nos casos em que há somente um ambiente de grupo G de modo que não haja perigo de confusão.

Definição 4.3.1. O grupo aditivo do anel associativo $L(G)$ de um grupo G é a soma direta

$$L(G) = \bigoplus_{k=1}^{\infty} \frac{\gamma_k}{\gamma_{k+1}},$$

escrevendo os grupos abelianos $\frac{\gamma_k}{\gamma_{k+1}}$ aditivamente.

Para cada $k \in \mathbb{N}$, o fator dessa soma direta é dito componente homogênea de $L(G)$ de peso k. Os elementos das componentes homogêneas $\frac{\gamma_k}{\gamma_{k+1}}$ de peso k do anel de Lie $L(G)$ são chamados elementos homogêneos de $L(G)$ de peso k. A multiplicação em G é definida pelos elementos homogêneos por

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

onde $a + \gamma_{i+1}$ e $b + \gamma_{j+1}$ são as imagens dos elementos $a \in \gamma_i$ e $b \in \gamma_j$ nos grupos quociente $\frac{\gamma_i}{\gamma_{i+1}}$ e $\frac{\gamma_j}{\gamma_{j+1}}$, respectivamente. Logo $[a, b] + \gamma_{i+j+1}$ são as imagens do grupo comutador $[a, b]$ no grupo quociente $\frac{\gamma_{i+j}}{\gamma_{i+j+1}}$. Então a multiplicação é estendida para $L(G)$ por linearidade. Isto define uma estrutura de anel de Lie em $L(G)$.

Teorema 4.3.2. Se G é nilpotente de classe c, então $L(G)$ é um anel de Lie e também é nilpotente de classe c, e se G é finito, então $|L(G)| = |G|$. Se G é solúvel de comprimento derivado s, então $L(G)$ também é solúvel de comprimento derivado $\leq s$. Além disso, cada automorfismo φ do grupo G induz um automorfismo do anel de Lie $L(G)$ por sua ação sobre os grupos quocientes $\frac{\gamma_i}{\gamma_{i+1}}$ e se G é finito e a ordem da φ é coprima a ordem de G, então φ atua em $L(G)$ e $\left|C_{L(G)}(\varphi)\right| = |C_G(\varphi)|$.

Demonstração. Se $a' + \gamma_{i+1} = a + \gamma_{i+1} \in \frac{\gamma_i}{\gamma_{i+1}}$ e $b' + \gamma_{j+1} = b + \gamma_{j+1} \in \frac{\gamma_j}{\gamma_{j+1}}$, então $a' = ag_1$, onde $g_1 \in \gamma_{i+1}$ e $b' = bg_2$, onde $g_2 \in \gamma_{j+1}$ e assim

$$[a', b'] = [ag_1, ag_2] \equiv [a, b](\mathrm{mod} \gamma_{i+j+1}),$$

pois $\underbrace{[\gamma_i, \gamma_{j+1}]}_{\leq \gamma_{i+j+1}} | \underbrace{[\gamma_{i+1}, \gamma_j]}_{\leq \gamma_{i+1+j}} \leq \gamma_{i+j+1}$.

A não comutatividade e a identidade de Jacobi são multilineares e, portanto, é suficiente confirmá-las para elementos homogêneos. Sejam $\bar{a} = a + \gamma_{i+1} \in \frac{\gamma_i}{\gamma_{i+1}}$, $\bar{b} = b + \gamma_{j+1} \in \frac{\gamma_j}{\gamma_{j+1}}$ e $\bar{c} = c + \gamma_{k+1} \in \frac{\gamma_k}{\gamma_{k+1}}$. Então

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

pois $[a, b] = [b, a]^{-1}$. Também temos

$$[\bar{a}, \bar{b}, \bar{c}] + [\bar{b}, \bar{c}, \bar{a}] + [\bar{c}, \bar{a}, \bar{b}] = [a, b, c] + [b, c, a] + [c, a, b] + \gamma_{i+j+k+1} = 0,$$

por causa da identidade de Witt para grupos

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

e $[a, b^{-1}, c]^b = [a, b^{-1}, c][[a, b^{-1}, c], b] \equiv [a, b^{-1}, c] \equiv [[a, b]^{-1}, c] \equiv [a, b, c]^{-1}(\mathrm{mod} \gamma_{i+j+k+1})$.

Analogamente, fazemos para $[b, c^{-1}, a]^c$ e $[c, a^{-1}, b]^a$.

Portanto, temos que $L(G)$ é um anel de Lie.

Para continuarmos a demonstração consideremos o seguinte resultado:

Lema 4.3.3. No anel de Lie associado a um a grupo arbitrário G, vale para qualquer k:

a) $\frac{\gamma_k}{\gamma_{k+1}} = \left\langle [a_1, a_2 \dots, a_k] | a_i \in \frac{\gamma_1}{\gamma_2} \right\rangle$;

b) $\gamma_k(L(G)) = \bigoplus_{i=k}^{\infty} \frac{\gamma_i}{\gamma_{i+1}}$.

Demonstração.

a) Temos que γ_k/γ_{k+1} é gerado pelas imagens dos comutadores $[g_1, g_2, \dots, g_k]$ de peso k em elementos de $g_i \in G$. Usando a definição de multiplicação de anéis de Lie associados, podemos provar que a imagem de comutador de peso k é igual do comutador $[\overline{g}_1, \overline{g}_2, \dots, \overline{g}_k]$ no anel de Lie , onde $\overline{g}_1$ é imagem em γ_1/γ_2. Assim passando para notação aditiva, temos $\gamma_k/\gamma_{k+1} = + \langle [\overline{g}_1, \overline{g}_2, \dots, \overline{g}_k] | \overline{g}_i \in \gamma_1/\gamma_2 \rangle$, o que comprova a afirmação a).

Como $[\overline{g}_1, \overline{g}_2, \dots, \overline{g}_k] \in \gamma_k(L(G))$, resulta de a) que $\gamma_k(L(G)) \supseteq \bigoplus_{i=k}^{\infty} \gamma_i/\gamma_{i+1}$; a inclusão inversa resulta do fato de que $[\gamma_m, \gamma_n] \leq \gamma_{m+n}$. Assim, o lema está provado. $\square$

O fato de que $|G| = |L(G)|$, se G é um grupo nilpotente finito, segue a partir das equações

$$|G| = \prod_{i=1}^{c} |\gamma_i/\gamma_{i+1}| \quad \text{e} \quad |L(G)| = \prod_{i=1}^{c} |\gamma_i/\gamma_{i+1}|,$$

onde c é a classe de nilpotência.

Se o grupo G satisfaz a identidade de solubilidade

$$\delta_s(x_1, x_2, \dots, x_{2^s}) = 1,$$

então, pela definição de multiplicação no anel de Lie associado, a mesma identidade está satisfeita com os elementos homogêneos de $L(G)$, e, como essa identidade é multilinear, ela está satisfeita por $L(G)$ mesmo.

Se $\varphi \in \mathrm{Aut}G$, para elementos homogêneos $\bar{a} = a + \gamma_{i+1} \in \frac{\gamma_i}{\gamma_{i+1}}$ e $\bar{b} = b + \gamma_{j+1} \in \frac{\gamma_j}{\gamma_{j+1}}$, temos

$$[\bar{a}, \bar{b}]^\varphi = [a, b]^\varphi + \gamma_{i+j+1} = [a^\varphi + \gamma_{i+1}, b^\varphi + \gamma_{j+1} = [\bar{a}^\varphi, \bar{b}^\varphi].$$

Então, por definição, estendemos a ação do automorfismo φ em $L(G)$ para um grupo abeliano γ_i/γ_{i+1}, por linearidade, $x = (x_1+\gamma_2)+(x_2+\gamma_3)+(x_3+\gamma_4)+\cdots \Rightarrow x^\varphi = (x_1+\gamma_2)^\varphi+(x_2+\gamma_3)^\varphi = (x_3+\gamma_4)^\varphi+\cdots$

Logo, para $l_1 = \sum_s l_{1s}, l_2 = \sum_s l_{2s}$, onde $l_{is} \in \gamma_s/\gamma_{s+1}, i = 1, 2, s \in \mathbb{N}$, temos

$[l_1, l_2]^\varphi = \left[\sum_s l_{1s}, \sum_r l_{2r}\right]^\varphi = \left(\sum_{s,r} [l_{1s}, l_{2r}]\right)^\varphi = \sum_{s,r} [l_{1s}, l_{2r}]^\varphi = \sum_{s,r} [l_{1s}^\varphi, l_{2r}^\varphi] = [\sum_s l_{1s}^\varphi, \sum_r l_2 r^\varphi] = [l_1^\varphi, l_2^\varphi]$.

Isso significa que φ realmente é um automorfismo do anel de Lie $L(G)$.

No caso em que G é um grupo nilpotente finito, a fidelidade de um automorfismo induzido da ordem de G decorre de:

"Seja G um grupo finito , φ um automorfismo de G tal que $(|G|, |C_G(\varphi)|) = 1$. Se φ centraliza todos os fatores de alguma série subnormal de G

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq K_2 \trianglelefteq \cdots \trianglelefteq K_s = G,$$

então $\varphi = 1$."

Agora, uma vez que um automorfismo age trivialmente sobre $L(G)$ se, e somente se, ele centraliza todos os fatores da série central inferior de G, com a mesma hipótese, decorre de: "Seja G um grupo finito, φ um automorfismo de G, e N um sugrupo normal $\varphi-$invariante de G do qual a ordem é coprima com a ordem de φ, $(|N|, |\varphi|) = 1$. Então $C_{G/N}(\varphi) = C_G(\varphi)N/N$." que $\left|C_{G(G)}(\varphi)\right| = |C_G(\varphi)|$, o que completa a demonstração do teorema.

$\square$

Uma observação a se fazer é que em contraste com a classe de nilpotência, o comprimento derivado do anel Lie associado $L(G)$ pode ser menor do que o comprimento derivado do grupo G, mesmo que o grupo G seja nilpotente.

O próximo corolário segue do Lema 4.3.3.

Corolário 4.3.4. Para qualquer grupo G, o anel de Lie associado $L(G)$ é gerado pela sua componente homogênea γ_1/γ_2 de peso 1. Se o grupo G é gerado por um conjunto M, então o anel de Lie $L(G)$ é gerado pelas imagens dos elementos de M no grupo quociente γ_1/γ_2.

Embora o anel de Lie associado possa ser construído a partir de um grupo arbitrário, é claro que ele reflete apenas as propriedades do grupo fator $G/\bigcap_{i=1}^{\infty}\gamma_i(G)$, pois, claramente, $L(G) \cong L(G/\bigcap_{i=1}^{\infty}\gamma_i(G))$.

4.4 O Anel de Lie de um Grupo de Expoente Primo

Aqui a situação é mais natural do que no caso de grupos de expoente composto p^k, uma vez que a identidade (p-1)-Engel é, de fato, multilinear.

Lemma 4.4.1 As duas condições seguintes são equivalentes para alguma álgebra de Lie L sobre um corpo de característica $p > 0$:

a) $[x, \underbrace{y, y, \ldots, y}_{p-1}] = 0$ para $x, y \in L$;

b) $\sum_{\pi \in \mathbb{S}_{p-1}} [x, y_{\pi(1)}, y_{\pi(2)}, \ldots, y_{\pi(p-1)}] = 0$, para $x, y_1, y_2, \ldots, y_{p-1} \in L$.

Demonstração.
b) $\Rightarrow$ a) Colocando $y_1 = y_2 = \cdots = y_{p-1}$ na afirmação em b), temos

$$(p-1)! \times [x, \underbrace{y, y, \ldots, y}_{p-1}] = 0.$$

Como $(p-1)! \neq 0$, segue que $[x, \underbrace{y, y, \ldots, y}_{p-1}] = 0$.

a) $\Rightarrow$ b) Substituindo $y = y_1 + y_2 + \cdots + y_{p-1}$ em a), vemos que a multihomogeneidade das componentes de peso 1 em cada variável $x, y_1, y_2, \ldots, y_{p-1}$ da equação resultante coincide com o lado esquerdo de b).

Assim, temos o sistema de equações

$$\sum_{k=0}^{p-1} i^k M^k = 0; i = 0, 1, 2, \ldots, p-1,$$

onde M_k é a soma de todos os elementos homogêneos nos quais y_1 ocorre em k entradas. Após a demonstração apresentaremos um exemplo, a saber, para $p = 3$.

Para o sistema dado, (i^k) é a sua matriz dos coeficientes e entendemos M_k como sendo as incógnitas. A matriz (i^k) é da forma

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & \ldots & 0 \\ 1 & 2 & 2^2 & \ldots & 2^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (p-1) & (p-1)^2 & \ldots & (p-1)^{p-1} \end{pmatrix},$$

que tem determinante de Vandermonde, sendo não nulo. Portanto, temos um sistema linear homogêneo cuja solução é única. Portanto, $M_k = 0$, para todo $k = 0, 1, \ldots, p-1$, como queríamos. Assim, o lema está demonstrado.

□

Exemplo 4.4.1 Vejamos o caso $p = 3$. Temos:

O item a) nos dá $[x, y, y] = 0$, para todos $x, y \in L$.

Assim,

- $i = 0 \Rightarrow y = 0 \cdot y_1 + y_2$

$0^0 \cdot [x, y_2, y_2]$, onde não há ocorrência de y_1.

- $i = 1 \Rightarrow y = y_1 + y_2$

$$[x, y_1 + y_2, y_1 + y_2] = 1^2 \cdot \underbrace{[x, y_1, y_1]}_{\in M_2} + 1^1 \cdot \underbrace{[x, y_1, y_2]}_{\in M_1} + 1^1 \cdot \underbrace{[x, y_2, y_1]}_{\in M_1} + 1^0 \cdot \underbrace{[x, y_2, y_2]}_{\in M_0}.$$

- $i = 2 \Rightarrow y = 2 \cdot y_1 + y_2$

$$[x, 2y_1 + y_2, 2y_1 + y_2] = [x, 2y_1, 2y_1] + [x, 2y_1, y_2] + [x, y_2, 2y_1] + [x, y_2, y_2] =$$

$$2^2 \cdot \underbrace{[x, y_1, y_1]}_{\in M_2} + 2^1 \cdot \underbrace{[x, y_1, y_2]}_{\in M_1} + 2^1 \cdot \underbrace{[x, y_2, y_1]}_{\in M_1} + 2^0 \cdot \underbrace{[x, y_2, y_2]}_{\in M_0}.$$

Teorema 4.4.2. O anel de Lie associado $L(P)$ de qualquer grupo P de expoente primo p satisfaz as identidades

$$pa = 0 \;\; e \;\; [a, \underbrace{b, b, \ldots, b}_{p-1}] = 0.$$

Teorema 4.4.3. Se uma álgebra de Lie L solúvel de comprimento derivado s sobre um corpo de característica p satisfaz a $n-$ésima condição de Engel, que é

$$[x, \underbrace{y, y, \ldots, y}_{n}] = 0,$$

para todos $x, y \in L$, e quer $p = 0$ ou $n < p$, então L é nilpotente de classe no máximo $\frac{(n+1)^s - 1}{n}$.

Corolário 4.4.3. Todo grupo solúvel G de comprimento derivado s de expoente primo p é nilpotente e sua classe de nilpotência é no máximo $\frac{p^s - 1}{p-1}$.

5 REFERÊNCIAS BIBLIOGRÁFICAS

[Gor] D. Gorenstein, **Finite Groups**, Harper & Row, New York, 1968.

[Her] I. N. Herstein, **Topics in algebra**. 2.ed., New York, J. Wiley & Sons, 1995.

[Hig] G. Higman , **Groups and Lie rings having automorphisms without non-trivial fixed points**, J. London Math. Soc., **32** (1957), $321 - 334$.

[Hof] K. Hoffman, R. Kunze, **Álgebra linear**. 2.ed., Rio de Janeiro, Livros Técnicos e Científicos, 1979.

[Khu1] E. I. Khukhro, **Nilpotent Groups and their Automorphisms**, Walter de Gruyter & Co., Berlin, 1993.

[Khu2] E. I. Khukhro, **p-Automorphisms of finite p-groups**, Cambridge Univ. Press, Lecture Note Series **246** (1998).

[MHal] M. Hall Jr., **The Theory of Groups**, Macmillan, New York, 1959.

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

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

[San] L. A. B. San Martin, **Álgebras de Lie**. Campinas, Editora da Unicamp, 1999.

[Shu1] P. Shumyatsky, **On the nilpotency class of Lie rings with fixed-point-free automorphisms**, Turk. J. Math., **29** (2005), 65-74.

[Sil1] J. C. Silva, **Álgebras de Lie de Derivações Livres de Constantes**, Dissertação de Mestrado, Universidade de Brasília, 2004.

[Sil2] J. C. Silva, **Variedades de Grupos e Generalizações Verbais para o Problema Restrito de Burnside**, Tese de Doutorado, Universidade de Brasília, 2009.