

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

VICTOR HUGO LÓPEZ SOLÍS

O Lema do Diamante de Bergman e Aplicações

Goiânia
2012

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: **Dissertação** **Tese**

2. Identificação da Tese ou Dissertação

Autor (a):	VICTOR HUGO LÓPEZ SOLÍS		
E-mail:	Victorhugomath@hotmail.com		
Seu e-mail pode ser disponibilizado na página?	<input checked="" type="checkbox"/> Sim	<input type="checkbox"/> Não	
Vínculo empregatício do autor	SEM VINCULO		
Agência de fomento:		Sigla:	CAPES
País:	BRASIL	UF:	CNPJ:
Título:	O LEMA DO DIAMANTE DE BERGMAN E APLICAÇÕES.		
Palavras-chave:	Grafos orientados, Módulos, Álgebras associativas, Álgebras de Lie, Álgebra P_n .		
Título em outra língua:	THE LEMMA OF BERGMAN'S DIAMOND AND APPLICATIONS.		
Palavras-chave em outra língua:	Oriented graphs, Modules, Associative algebras, Lie algebras, Algebra P_n .		
Área de concentração:	ALGEBRA.		
Data defesa: (dd/mm/aaaa)	19/03/2012.		
Programa de Pós-Graduação:	MESTRADO EM MATEMÁTICA		
Orientador (a):	Dra. Shirlei Serconeck.		
E-mail:	shirleik@terra.com.br		
Co-orientador (a):*			
E-mail:			

*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento SIM NÃO¹

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.

Victor Hugo López Solís

Assinatura do (a) autor (a)

Data: 12 / 12 / 2012

¹ Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

VICTOR HUGO LÓPEZ SOLÍS

O Lema do Diamante de Bergman e Aplicações

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.

Orientadora: Profa. Dra. Shirlei Serconek

Goiânia
2012

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

L9251 López Solís, Victor Hugo.
O lema do Diamante de Bergman e Aplicações
[manuscrito] / Victor Hugo López Solís. - 2012.
61 f.
Orientadora: Prof^a. Dr^a. Shirlei Serconek.
Dissertação (Mestrado) – Universidade Federal de Goiás,
Instituto de Matemática e Estatística, 2012.
Bibliografia.

1. Álgebras Associativas. 2. Lie, Álgebras de. I. Título.

CDU: 512.554.3

VÍCTOR HUGO LÓPEZ SOLÍS

O LEMA DO DIAMANTE DE BERGMAN E APLICAÇÕES

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 19 de março de 2012, pela Banca Examinadora constituída pelos professores:



Profa. Dra. Shirlei Serconek
Instituto de Matemática e Estatística-UFG
Presidente da Banca



Profa. Dra. Rosemary Miguel Pires
Instituto de Ciências Exatas-UFF



Profa. Dra. Ivonildes Ribeiro Martins
Instituto de Matemática e Estatística-UFG

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador(a).

Victor Hugo López Solís

Graduou-se em Matemática na UNASAM-Universidad Nacional Santiago Antunez de Mayolo no Perú.

Aos meus pais, **Victor e Hermelinda** e, a meus irmãos **Johnny e Jesús** com todo o amor e carinho.

Agradecimentos

Agradeço primeiramente e acima de tudo a Deus, pela oportunidade e pela perseverança que me deu ao longo do desenvolvimento deste trabalho.

Gostaria de aproveitar esta oportunidade para agradecer a quem contribuiu, de alguma forma ou de outra, para a realização desta dissertação.

A minha orientadora e amiga Shirlei Serconek pela paciência e pela dedicação em me orientar por todo o período em que desenvolvi este trabalho.

Obrigado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás pelo apoio e a amizade que de alguma maneira fizeram sentirnos como em casa.

Obrigado a todos os amigos e colegas que eu conheci no dia a dia na universidade, em especial a meus amigos do mestrado. Pelo que compartilhamos: refeições, cafés, jogos,... coisas que tornam a vida valer a pena.

Finalmente, quero agradecer a CAPES pelo apoio financeiro.

A verdade vos libertará.

Jesus, em João 8,32.

Resumo

López Solís, Victor Hugo. **O Lema do Diamante de Bergman e Aplicações.** Goiânia, 2012. 61p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

O nosso trabalho tem como objetivo principal, estabelecer condições para obter uma forma canônica para os elementos de um anel, semigrupo ou estrutura algébrica similar. Isto é obtido através do resultado principal, o Teorema 3.10 (O Lema do Diamante de Bergman), com aplicações.

Palavras-chave

Grafos orientados, Módulos, Álgebras associativas, Álgebras de Lie, Álgebra P_n .

Abstract

López Solís, Victor Hugo. **The Lemma of Bergman's Diamond and Applications**. Goiânia, 2012. 61p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Our work has as main objective, to establish conditions for a canonical form for elements of a ring, semigroup or algebraic structure similar. This result is obtained through the main Theorem 3.10 (The Lemma of Bergman's Diamond) with applications.

Keywords

Oriented graphs, Modules, Associative algebras, Lie algebras, Algebra P_n .

Sumário

Introdução	9
1 Conjuntos Parcialmente Ordenados e Grafos Orientados	11
1.1 Conjuntos Parcialmente Ordenados	11
1.2 Grafos Orientados	13
2 Módulos, Álgebras e Álgebras de Lie	15
2.1 Módulos	15
2.2 Álgebras	19
2.3 Álgebras de Lie	24
2.3.1 Álgebras Universais Envelopantes	26
3 O Lema do Diamante de Bergman	31
3.1 O Teorema Principal: Bases para k -Álgebras Associativas	31
3.2 Aplicação: Um Problema sobre Idempotentes	37
3.3 Aplicação: O Teorema de Poincaré-Birkhoff-Witt	41
3.4 Aplicação: Como Tirar Proveito das Identidades	43
4 A Álgebra P_n	51
4.1 As Álgebras $ch(P_n)$	55
4.2 PGC-Álgebras	57
Referências Bibliográficas	61

Introdução

Os principais resultados neste trabalho são "*triviais*", segundo Bergman [1]. Mas, o que é trivial, quando descrito em forma abstrata pode estar longe de ser claro no contexto de uma situação complicada onde ela é necessária. Portanto, vale a pena estabelecer formulações explícitas e provas desses resultados.

Estaremos preocupados com as condições que devem ser verificadas para estabelecer uma forma canônica para os elementos de um anel, semigrupo ou estrutura algébrica similar.

Suponha que L é uma álgebra associativa com elemento identidade 1 sobre um anel comutativo k , e que temos uma apresentação de L por uma família X de geradores e uma família S de relações. Suponha que cada relação $\sigma \in S$ foi escrita na forma $W_\sigma = f_\sigma$, onde W_σ é um monômio (um produto de elementos de X) e f_σ é uma combinação k -linear de monômios, e que desejamos usar essas relações como instruções para "reduzir" expressões r para elementos de L . Isto é, se quaisquer dos monômios que aparecem na expressão r contêm um dos W_σ como uma subpalavra, substituímos f_σ por essa subpalavra, e iteramos esse processo até quando seja possível. A dificuldade é que este processo não está em geral bem definido. Em cada etapa devemos escolher que redução aplicar e a qual subpalavra dos monômios. Sobre quais hipóteses podemos mostrar: (i') que tal processo produzirá que cada expressão tenha uma única forma irreduzível? e (ii') podemos concluir então que darão uma forma canônica para os elementos de L ?

Existe um resultado muito geral sobre isto, dado por Newman, muitas vezes chamado de "Lema do Diamante." Seja G um grafo orientado. Aqui os vértices de G podem ser expressões para os elementos de algum objeto algébrico e as arestas etapas de redução indo de uma expressão a outra "melhor", onde um número suficiente de reduções é dado de forma que a relação de equivalência que eles geram corresponda igualdade no objeto. Suponha que

- (i) *O grafo orientado G satisfaz condições de cadeia descendente. Isto é, todos os caminhos positivamente orientados em G terminam; e*
- (ii) *Quando duas arestas, e e e' procedem de um vértice a de G , existem caminhos positivamente orientados p e p' em G saindo dos pontos finais b e b' dessas arestas a um vértice comum c (condição do "Diamante".) Então cada componente*

conexa C de G tem um único vértice minimal m_C . Isto significa que cada caminho positivamente orientado maximal que começa em um ponto de C terminará em m_C ; em outras palavras, as reduções dadas produziram formas canônicas únicas para os elementos do objeto algébrico original.

Nosso resultado principal, o Teorema 3.10 (O Lema do Diamante de Bergman), é um análogo e um fortalecimento das observações feitas acima para o caso dos anéis associativos com processos de redução da forma esboçada anteriormente. É auto-suficiente e não segue a formulação grafo-teórico de Newman. O fortalecimento está no resultado de que os análogos das condições (i) e (ii) necessitam apenas ser verificados para monômios, e o fato de que (ii) só precisa ser verificado para "monômios não triviais ambigualmente redutíveis". Ou seja, basta verificar, para cada monômio que pode ser escrito como ABC com $AB = W_\sigma$, $BC = W_\tau$ ($\sigma, \tau \in S$, $B \neq 1$) ou $ABC = W_\sigma$, $B = W_\tau$ ($\sigma \neq \tau \in S$) tal que as duas expressões que se reduzem a ABC (no primeiro caso, $f_\sigma C$ e Af_τ ; no segundo f_σ e $Af_\tau C$) podem ser reduzidas a um valor comum.

Uma melhoria adicional obtida, útil em muitas aplicações, é que, no análogo de (ii), os caminhos p e p' não precisam ser estritamente e positivamente orientados, mas devem apenas ficar "abaixo" do elemento original ABC , com respeito à ordem parcial sob monômios introduzida em conexão com (i). Veja (condição (a')) do Teorema 3.10). Na Seção 3.4 também mostramos como tirar proveito das identidades para simplificar a verificação da condição do "Diamante".

Como uma primeira aplicação do Teorema 3.10 obtemos a seção 3.2 onde consideramos um problema sobre idempotentes. Estudamos o anel gerado por um conjunto de elementos idempotentes e obtemos uma base para esse anel.

Na seção 3.3 apresentamos uma das aplicações mais importantes de nosso trabalho, o Teorema clássico de Poincaré-Birkhoff-Witt (PBW) que é resolvido de maneira elegante usando o Teorema 3.10.

No Capítulo 4 consideramos a álgebra P_n . Estudamos uma classe de álgebras de quocientes da álgebra Q_n correspondente a grafos de n vértices. As álgebras Q_n de todas as pseudo-raízes de um polinômio genérico não comutativo foram introduzidas e estudadas por Gelfand et al.,[2]. Especializamos para um tipo de grafo particular, o grafo P_n de n vértices. Na Seção 4.1 estudamos as álgebras $ch(P_n)$, e usamos o Teorema 3.10 para encontrar uma base PBW para essa álgebra. Para fazer isso, na Seção 4.2 estudamos as álgebras PGC-álgebras.

Conjuntos Parcialmente Ordenados e Grafos Orientados

Neste capítulo, definiremos conjuntos parcialmente ordenados e condições de cadeias. Definimos grafos orientados e damos as definições de caminhos maximais e de caminhos maximais positivamente orientados.

1.1 Conjuntos Parcialmente Ordenados

Definição 1.1 Um conjunto parcialmente ordenado é um par (A, \preceq) , onde A é um conjunto juntamente com uma relação \preceq definida sobre A que satisfaz as seguintes condições, para todo $a, b, c \in A$

- (i) *Reflexividade*: $a \preceq a$;
- (ii) *Antissimetria*: Se $a \preceq b$ e $b \preceq a$, então $a = b$;
- (iii) *Transitividade*: Se $a \preceq b$ e $b \preceq c$, então $a \preceq c$.

Os elementos $a, b \in A$ são **comparáveis**, se $a \preceq b$ ou $b \preceq a$. No entanto, dois elementos de um conjunto parcialmente ordenado não precisam ser comparáveis. Um conjunto parcialmente ordenado A onde quaisquer dois elementos são comparáveis é dito **totalmente ordenado**.

Exemplo 1.2 Seja A o conjunto de todos os subconjuntos de $\{1, 2, 3, 4, 5\}$. Defina

$$C \preceq D \text{ se, e somente se } C \subset D.$$

Então A é parcialmente ordenado, mas não é totalmente ordenado pois,

$$\{1, 2\} \text{ e } \{3, 4\} \text{ não são comparáveis.}$$

Seja (A, \preceq) um conjunto parcialmente ordenado. Um elemento $c \in A$ é **maximal** em A se para cada $a \in A$ que é comparável a c , $a \preceq c$; em outras palavras, para todo $a \in A$, $c \preceq a$ implica $c = a$. Observe que se c é maximal, não necessariamente se tem $a \preceq c$ para todo $a \in A$ (pode existir $a \in A$ que não é comparável a c). Além disso, um conjunto dado pode ter muitos elementos maximais ou nenhum (por exemplo, \mathbb{Z} com a ordem usual). Uma **cota superior** de um subconjunto não vazio B de A é um elemento $d \in A$ tal que $b \preceq d$ para cada $b \in B$. Um subconjunto não vazio B de A que é totalmente ordenado por \preceq é chamado uma **cadeia** em A .

Exemplo 1.3 O conjunto S de todos os pontos (x, y) no plano real com $y \leq 0$ é um conjunto parcialmente ordenado, com a ordem

$$(x_1, y_1) \preceq (x_2, y_2) \text{ se, e somente se } x_1 = x_2 \text{ e } y_1 \leq y_2.$$

S têm um número infinito de elementos maximais.

Definição 1.4 Um conjunto parcialmente ordenado A satisfaz a **condição de cadeia ascendente (CCA)** se dada qualquer sequência de elementos comparáveis de A

$$a_1 \preceq a_2 \preceq a_3 \preceq \dots$$

existe um inteiro positivo n tal que

$$a_n = a_{n+1} = a_{n+2} = \dots.$$

Analogamente, A satisfaz a **condição de cadeia descendente (CCD)** se para cada sequência de elementos comparáveis de A

$$a_1 \succeq a_2 \succeq a_3 \succeq \dots$$

existe um inteiro positivo n tal que $a_n = a_{n+1} = a_{n+2} = \dots$.

Exemplo 1.5 O anel \mathbb{Z} satisfaz a condição de cadeia ascendente (CCA) para ideais, mas não satisfaz a condição de cadeia descendente (CCD), pois para a cadeia

$$\mathbb{Z} \supseteq (2) \supseteq (2^2) \supseteq (2^3) \supseteq \dots$$

não existe um inteiro n tal que $(2^n) = (2^{n+1}) = (2^{n+2}) = \dots$.

Exemplo 1.6 Seja $\mathfrak{F}(\mathbb{R})$ o conjunto de todas as funções $f: \mathbb{R} \rightarrow \mathbb{R}$. $\mathfrak{F}(\mathbb{R})$ é um anel com as definições

$$f + g : a \rightarrow f(a) + g(a) \text{ e } fg : a \rightarrow f(a)g(a).$$

Observamos que para cada inteiro positivo n ,

$$I_n = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f(x) = 0 \quad \forall x \geq n\}$$

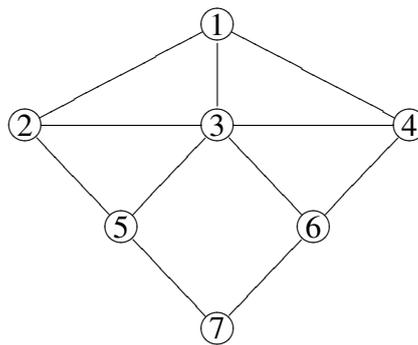
é um ideal de $\mathfrak{F}(\mathbb{R})$ e $I_n \subset I_{n+1}$ para todo n . Portanto, $\mathfrak{F}(\mathbb{R})$ não satisfaz a condição de cadeia ascendente (CCA).

1.2 Grafos Orientados

Definição 1.7 Um *grafo* G é um par ordenado de conjuntos disjuntos (V, E) . O conjunto V é o conjunto de *vértices* e E é o conjunto de *arestas*.

Se $e = \{u, v\}$ é uma aresta então dizemos que os vértices u e v são os pontos extremos de e . Um vértice e uma aresta são **incidentes** se o vértice é um dos extremos da aresta. Dois vértices u e v são **adjacentes** se $\{u, v\}$ é uma aresta.

Exemplo 1.8 O grafo $G = (V, E)$,



onde $V = \{1, 2, 3, 4, 5, 6, 7\}$ e $E = \{12, 13, 14, 23, 25, 35, 36, 43, 46, 57, 67\}$.

Definição 1.9 Se $G = (V, E)$ e $H = (W, F)$ são grafos tais que $W \subset V$ e $F \subset E$, então H é um *subgrafo* de G .

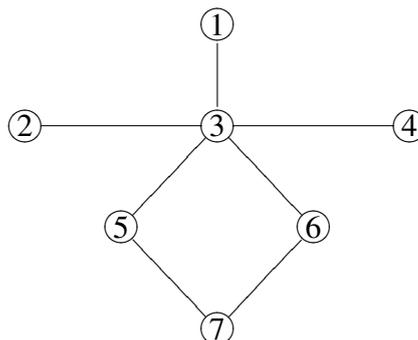
Definição 1.10 Um *caminho* em um grafo G é simplesmente um subgrafo de G , que tem a forma

$$V = \{v_1, v_2, \dots, v_n\}, \quad E = \{v_1v_2, v_2v_3, \dots, v_{n-1}v_n\}.$$

Definição 1.11 Um grafo $G = (V, E)$ é **conexo** se para cada par $\{u, v\}$ de vértices distintos existe um caminho de u a v .

Definição 1.12 Seja $G = (V, E)$ um grafo. Dizemos que um *subgrafo conexo* $H = (W, F)$ de $G = (V, E)$ é **maximal** se $W = V$

Exemplo 1.13 O grafo $H = (W, F)$,

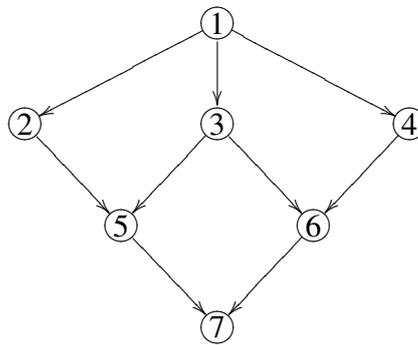


onde $W = \{1, 2, 3, 4, 5, 6, 7\}$ e $E = \{13, 23, 35, 36, 43, 57, 67\}$ é um subgrafo conexo maximal de $G = (V, E)$.

Vamos definir o grafo mais importante para nosso trabalho subsequente na seguinte definição.

Definição 1.14 Um **grafo orientado** (ou **digrafo**) é um grafo G cujas arestas têm direção e são chamados **arcos**.

Exemplo 1.15 O grafo G ,



onde $V = \{1, 2, 3, 4, 5, 6, 7\}$ e $E = \{12, 13, 14, 25, 35, 36, 46, 57, 67\}$.

As flechas sobre os arcos são usadas para codificar a informação direcional: um arco do vértice u ao vértice v indica que a gente pode mover-se de u para v , mas não de v para u . Se temos escolhido uma orientação em um grafo G como no exemplo anterior, dizemos que o grafo G é **positivamente orientado**.

Módulos, Álgebras e Álgebras de Lie

Vamos primeiro introduzir a definição de k -módulo, onde k é um anel (associativo) comutativo com elemento identidade 1. Formalmente, os módulos sobre um anel são uma generalização de grupos abelianos (que são módulos sobre \mathbb{Z}). Quando k é um corpo, um k -módulo é um "espaço vetorial sobre k "; isto é, na definição de espaço vetorial, permitimos que os escalares estejam em um corpo.

2.1 Módulos

Definição 2.1 *Seja k um anel comutativo com elemento identidade 1. Um k -módulo unitário é um grupo abeliano (aditivo) M com uma **multiplicação escalar** $k \times M$, denotada por*

$$(r, m) \mapsto rm,$$

tais que os seguintes axiomas sejam verdadeiros para todo $m, m' \in M$ e todo $r, r' \in k$:

- (i) $r(m + m') = rm + rm'$;
- (ii) $(r + r')m = rm + r'm$;
- (iii) $(rr')m = r(r'm)$;
- (iv) $1m = m$.

Exemplo 2.2 *Cada espaço vetorial sobre um corpo k é um k -módulo unitário.*

Exemplo 2.3 *Cada grupo abeliano aditivo é um \mathbb{Z} -módulo unitário.*

Exemplo 2.4 *Se k é um anel comutativo, então $\mathbb{M}at_n(k)$ o grupo abeliano aditivo de todas as matrizes $n \times n$ com entradas em k é um k -módulo.*

Exemplo 2.5 *Seja V é um espaço vetorial de dimensão finita sobre um corpo k , e $T : V \rightarrow V$ uma transformação k -linear. O espaço vetorial V é um $k[x]$ -módulo unitário com a multiplicação escalar*

$$k[x] \times V \longrightarrow V$$

definida por: Se $f(x) = \sum_{i=0}^m c_i x^i$ é um elemento de $k[x]$ e $v \in V$, então

$$\begin{aligned} f(x)v &= \left(\sum_{i=0}^m c_i x^i \right) v = \sum_{i=0}^m c_i T^i v \\ &= c_0 v + c_1 T v + c_2 T^2 v + \dots, \end{aligned}$$

onde T^0 é a aplicação identidade 1_V . Denotamos V olhado como um $k[x]$ -módulo unitário por V^T .

Aqui temos um caso especial desta construção. Consideremos $A \in \mathbb{M}at_n(k)$ e $T : k^n \longrightarrow k^n$ a transformação linear dada por $T(w) = Aw$. O espaço vetorial k^n é um $k[x]$ -módulo unitário se definimos a multiplicação escalar

$$k[x] \times k^n \longrightarrow k^n$$

como segue-se: Se $f(x) = \sum_{i=0}^m c_i x^i$ e $w \in k^n$, então

$$\begin{aligned} f(x)w &= \left(\sum_{i=0}^m c_i x^i \right) w = \sum_{i=0}^m c_i A^i w \\ &= c_0 I w + c_1 A w + c_2 A^2 w + \dots, \end{aligned}$$

onde $A^0 = I$ é a matriz identidade. Mostramos que $(k^n)^T = (k^n)^A$.

Ambos k -módulos têm os mesmos elementos (chamados, todos de n -uplas), e a multiplicação escalar coincide em ambos: Em $(k^n)^T$, temos $xw = T(w)$; em $(k^n)^A$, temos $xw = Aw$; eles coincidem porque $T(w) = Aw$.

Definição 2.6 Se k é um anel comutativo e, M e N são k -módulos, então a função $f : M \longrightarrow N$ é um **k -homomorfismo** se, para todo $m, m' \in M$ e todo $r \in k$, têm-se

(i) $f(m + m') = f(m) + f(m')$;

(ii) $f(rm) = rf(m)$.

Se um k -homomorfismo é uma bijeção, então é chamado um **k -isomorfismo**. Os k -módulos M e N são chamados **isomorfos**, denotado por $M \cong N$, se existe um k -isomorfismo $f : M \longrightarrow N$.

Observe que a composta de k -homomorfismos é um k -homomorfismo e, se f é um k -isomorfismo, então sua inversa f^{-1} é também um k -isomorfismo.

Exemplo 2.7 Pelo exemplo 2.3, os \mathbb{Z} -módulos são grupos abelianos. Então cada homomorfismo de grupos abelianos é um homomorfismo de \mathbb{Z} -módulos.

Exemplo 2.8 Seja V um espaço vetorial sobre um corpo k , e $T : V \rightarrow V$ uma transformação linear, $\{v_1, \dots, v_n\}$ uma base para V e A a matriz de T relativa a essa base. Mostramos que os $k[x]$ -módulos V^T e $(k^n)^A$ são isomorfos.

Definamos

$$\varphi : V \rightarrow k^n$$

por $\varphi(v_i) = e_i$, onde $\{e_1, \dots, e_n\}$ é a base canônica de k^n ; a transformação φ é um isomorfismo de k -espaços vetoriais. Primeiro mostraremos que φ é um $k[x]$ -homomorfismo. Para isso é suficiente provarmos que $\varphi(f(x)v) = f(x)\varphi(v)$ para todo $f(x) \in k[x]$ e todo $v \in V$. Então

$$\begin{aligned} \varphi(xv_i) &= \varphi(T(v_i)) \\ &= \varphi(\sum a_{ji}v_j) = \sum a_{ji}\varphi(v_j) = \sum a_{ji}e_j, \end{aligned}$$

que é a i -ésima coluna de A . Por outro lado,

$$x\varphi(v_i) = A\varphi(v_i) = Ae_i,$$

que é também a i -ésima coluna de A . Segue-se que $\varphi(xv) = x\varphi(v)$ para todo $v \in V$, e podemos facilmente provar, por indução sobre o grau de f , que

$$\varphi(f(x)v) = f(x)\varphi(v)$$

para todo $f(x) \in k[x]$ e todo $v \in V$.

Definição 2.9 Se M e N são k -módulos, então

$$\text{Hom}_k(M, N) = \{f : M \rightarrow N \mid f \text{ é um } k\text{-homomorfismo}\}.$$

$\text{Hom}_k(M, N)$ é um grupo abeliano aditivo: Se $f, g \in \text{Hom}_k(M, N)$, então define $f + g : M \rightarrow N$ por

$$f + g : m \mapsto f(m) + g(m).$$

Proposição 2.10 Se M e N são k -módulos, onde k é um anel comutativo, então $\text{Hom}_k(M, N)$ é um k -módulo, com a multiplicação escalar dada por

$$rf : m \mapsto f(rm).$$

Demonstração. A verificação dos axiomas na definição de k -módulo é simples, mas apresentamos a prova de

$$(rr')f = r(r'f)$$

porque ele usa a comutatividade de k .

Se $m \in M$, então $(rr')f : m \mapsto f(rr'm)$. Por outro lado, $r(r'f) : m \mapsto (r'f)(rm) = f(r'rm)$. Como k é comutativo, $rr' = r'r$, e portanto $(rr')f = r(r'f)$. \square

Além disso, existem as leis distributivas: Se $p : M' \rightarrow M$ e $q : N \rightarrow N'$, então $(f+g)p = fp + gp$ e $q(f+g) = qf + qg$ para todo $f, g \in \text{Hom}_k(M, N)$.

Definição 2.11 Se M é um k -módulo, então um **submódulo** N de M , denotado por $N \subseteq M$, é um subgrupo aditivo N de M fechado com a multiplicação escalar: $rn \in N$ se $n \in N$ e $r \in k$; isto é,

$$kN \subseteq N.$$

Definição 2.12 Se M é um k -módulo, então um k -homomorfismo $f : M \rightarrow M$ é chamado um **k -endomorfismo** de M . O anel dos **endomorfismos** de M , denotado por $\text{End}_k(M)$, é o conjunto de todos os k -endomorfismos de M . Como um k -módulo, $\text{End}_k(M) = \text{Hom}_k(M, M)$.

Definição 2.13 Um k -módulo M é um **k -módulo livre** se M é isomorfo a uma soma direta de cópias de k : isto é, se existe um conjunto de índices I tal que

$$M = \sum_{i \in I} \bigoplus k_i,$$

onde $k_i = \langle b_i \rangle \cong k$ para todo i . Chamamos $B = \{b_i \mid i \in I\}$ uma **base** de M .

Exemplo 2.14 Um \mathbb{Z} -módulo livre é um grupo abeliano livre. Cada anel comutativo k , quando é considerado como um k -módulo, é um k -módulo livre.

Proposição 2.15 Sejam M um k -módulo livre, e $B = \{b_i \mid i \in I\}$ uma base para M . Se N é um k -módulo e $\gamma : B \rightarrow N$ uma função, então existe um único k -homomorfismo de módulos

$$\tilde{\gamma} : M \rightarrow N$$

com $\tilde{\gamma}(b_i) = \gamma(b_i)$ para todo $i \in I$.

$$\begin{array}{ccc} & M & \\ & \uparrow & \searrow \tilde{\gamma} \\ B & \xrightarrow{\gamma} & N \end{array}$$

Demonstração. Cada elemento $m \in M$ tem uma única expressão da forma

$$m = \sum_{i \in I} r_i b_i,$$

onde $r_i \in k$ e quase todos $r_i = 0$. Defina $\tilde{\gamma}: M \rightarrow N$ por

$$\tilde{\gamma}(m) = \sum_{i \in I} r_i \gamma(b_i).$$

□

2.2 Álgebras

Nesta seção introduzimos a definição de k -álgebras, onde k é um anel (associativo) comutativo com elemento identidade 1.

Definição 2.16 *Se k é um anel comutativo, então um anel A é uma k -álgebra se A é um k -módulo unitário com uma operação bilinear*

$$\cdot : A \times A \rightarrow A$$

chamada **produto**, que satisfaz

$$r(a \cdot b) = (ra) \cdot b = a \cdot (rb)$$

para todo $a, b, c \in A$ e $r \in k$.

Ao longo de nosso trabalho denotaremos o produto de $a, b \in A$ simplesmente por ab , salvo indicação contrária.

Exemplo 2.17 *Se k é um anel comutativo com elemento identidade 1, então $\text{Mat}_n(k)$ é uma k -álgebra, onde o produto é o produto usual de matrizes.*

Definição 2.18 *Sejam M e S k -álgebras, um k -homomorfismo de anéis $f: M \rightarrow S$ é chamado um **homomorfismo de k -álgebras** se*

$$f(ra) = rf(a)$$

para todo $a \in M$ e $r \in k$; isto é, f é também um homomorfismo de k -módulos.

Exemplo 2.19 *Seja $A = \mathbb{C}[x]$, então A é uma \mathbb{C} -álgebra, onde o produto é o produto usual de polinômios, e $\varphi: A \rightarrow A$, dado por*

$$\varphi: \sum_j c_j x^j \mapsto \sum_j c_j (x-1)^j$$

é um homomorfismo de \mathbb{C} -álgebras. Por outro lado, a função $\theta: A \rightarrow A$, definida por

$$\theta: \sum_j c_j x^j \mapsto \sum_j \bar{c}_j (x-1)^j$$

(onde \bar{c} é o complexo conjugado de c), é um homomorfismo de \mathbb{C} -módulos mas não é um homomorfismo de \mathbb{C} -álgebras. Por exemplo, $\theta(ix) = -i(x-1)$ enquanto $i\theta(x) = i(x-1)$. No entanto, $\mathbb{C}[x]$ é também uma \mathbb{R} -álgebra, e θ é um homomorfismo de \mathbb{R} -álgebras.

Definição 2.20 Uma k -álgebra A é **associativa** se o produto definido em A é associativo, isto é, $(ab)c = a(bc)$ para todo $a, b, c \in A$.

Exemplo 2.21 Do exemplo 2.17 temos que a k -álgebra $\text{Mat}_n(k)$ é uma k -álgebra associativa, pois o produto de matrizes é associativo.

Definição 2.22 Uma k -álgebra A é uma **k -álgebra graduada** se existem k -submódulos A_p , para $p \geq 0$, tais que

$$(i) \quad A = \sum_{p \geq 0} \bigoplus A_p;$$

(ii) Para todo $p, q \geq 0$, se $x \in A_p$ e $y \in A_q$, então $xy \in A_{p+q}$; isto é,

$$A_p A_q \subseteq A_{p+q}.$$

Um elemento $x \in A_p$ é chamado **homogêneo de grau p** .

Exemplo 2.23 O anel polinomial $A = k[x]$ é uma k -álgebra graduada se definimos

$$A_p = \{rx^p \mid r \in k\}.$$

Os elementos homogêneos de grau p são os monômios de grau p .

Exemplo 2.24 O anel polinomial $A = k[x_1, x_2, \dots, x_n]$ é uma k -álgebra graduada se definimos

$$A_p = \{rx_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} \mid r \in k \text{ e } \sum e_i = p\};$$

isto é, A_p consiste de todos os monômios de grau total p .

Definição 2.25 Uma k -álgebra A é uma **k -álgebra filtrada** se para cada inteiro $p \geq 0$ existe um k -submódulo $A^{(p)}$ tais que

$$(i) \quad A^{(p)} \subseteq A^{(q)} \text{ se } p \leq q;$$

$$(ii) \quad \bigcup A^{(p)} = A;$$

$$(iii) \quad A^{(p)} A^{(q)} \subseteq A^{(p+q)}.$$

Observação 2.26 Se A é uma k -álgebra graduada, estabelecendo $A^{(p)} = \sum_{s \leq p} \bigoplus A_s$ obtemos uma filtração de A , e A torna-se uma k -álgebra filtrada.

Uma noção importante associada a uma álgebra filtrada A é a **álgebra graduada associada** $G(A) = \bar{A}$. Obtém-se esta álgebra, formando o módulo

$$(\alpha) \quad \bar{A} = G(A) = \sum_{p \geq 0} \bigoplus G(A_p), \quad \text{onde } G(A_p) = A^{(p)} / A^{(p-1)},$$

com $A^{(-1)} = 0$. A multiplicação em $G(A)$ está definida por

$$(\beta) \quad (a_p + A^{(p-1)})(a_q + A^{(q-1)}) = a_p a_q + A^{(p+q-1)}$$

se $a_p \in A^{(p)}$, $a_q \in A^{(q)}$. Esta multiplicação está bem definida. De fato, se $a_p \equiv b_p \pmod{A^{(p-1)}}$ e $a_q \equiv b_q \pmod{A^{(q-1)}}$, então

$$a_p a_q \equiv b_p b_q \pmod{A^{(p+q-1)}}.$$

Portanto (β) está bem definida para um elemento de $G(A_p)$ e um elemento de $G(A_q)$ com resultado em $G(A_{p+q})$ e é estendida pela adição para $G(A)$. Isto dá uma álgebra graduada $G(A)$ com $G(A_p)$ como o submódulo de elementos homogêneos de grau p .

Vamos construir a **álgebra tensorial** sobre um k -módulo M . Quando M é um k -módulo livre com base X , a álgebra tensorial também será uma k -álgebra livre com base X ; isto é, ela será o anel polinomial sobre k com variáveis em X que não comutam.

Definição 2.27 Seja k um anel comutativo, e M um k -módulo. Defina

$$T^0(M) = k, \\ T^1(M) = M, \dots, T^p(M) = M \otimes_k \cdots \otimes_k M \quad (p \text{ vezes}) \text{ se } p \geq 2.$$

Proposição 2.28 Se M é um k -módulo. Então existe uma k -álgebra graduada

$$T(M) = \sum_{p \geq 0} T^p(M)$$

com a ação de $r \in k$ sobre $T^p(M)$ dada por

$$r(x_1 \otimes \cdots \otimes x_p) = (rx_1) \otimes x_2 \otimes \cdots \otimes x_p = (x_1 \otimes \cdots \otimes x_p)r,$$

com a multiplicação

$$(x_1 \otimes \cdots \otimes x_p)(y_1 \otimes \cdots \otimes y_q) = x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q \in M^{p+q}$$

Demonstração. A multiplicação é associativa porque não se precisa dos parênteses para descrever os geradores $m_1 \otimes \cdots \otimes m_p$ de $T^p(M)$. As leis distributivas são verdadeiras porque a multiplicação é k -bilinear. Finalmente, $1 \in k = T^0(M)$ é a identidade, cada elemento de k comuta com cada elemento de $T(M)$, e naturalmente

$$T^p(M)T^q(M) \subseteq T^{p+q}(M).$$

Portanto, $T(M)$ é uma álgebra graduada. \square

Definição 2.29 *Se k é um anel comutativo e M é um k -módulo. Então $T(M)$ é chamada a álgebra tensorial sobre M .*

Denotamos a categoria dos k -módulos à esquerda por ${}_k\mathbf{Mod}$ e por $\mathbf{Gr}_k\mathbf{Alg}$ a categoria das k -álgebras graduadas. Para um estudo mais detalhado de categorias e funtores veja [10].

Proposição 2.30 *A álgebra tensorial define um functor $T : {}_k\mathbf{Mod} \rightarrow \mathbf{Gr}_k\mathbf{Alg}$. Além disso, T preserva sobrejeções.*

Demonstração. Veja [10], pág. 723. \square

Vamos generalizar a noção de módulo livre para álgebra livre.

Definição 2.31 *Se X é um subconjunto de uma k -álgebra F , então F é uma k -álgebra livre com base X se, para cada k -álgebra A e cada função $\varphi : X \rightarrow A$, existe um único homomorfismo de k -álgebras $\tilde{\varphi}$ com*

$$\tilde{\varphi}(x) = \varphi(x)$$

para todo $x \in X$. Em outras palavras, o seguinte diagrama comuta, onde $i : X \rightarrow F$ é a inclusão.

$$\begin{array}{ccc} F & & \\ \uparrow i & \searrow \tilde{\varphi} & \\ X & \xrightarrow{\varphi} & A \end{array}$$

Na seguinte proposição, afirmamos que a k -álgebra graduada $T(M)$ é uma k -álgebra livre.

Proposição 2.32 *Se M é um k -módulo livre com base X , onde k é um anel comutativo, então $T(M)$ é uma k -álgebra livre com base X .*

Demonstração. Consideremos o diagrama

$$\begin{array}{ccc} T(M) & & \\ \uparrow j & \searrow T(\tilde{\varphi}) & \\ M & & T(A) \\ \uparrow i & \searrow \tilde{\varphi} & \downarrow \mu \\ X & \xrightarrow{\varphi} & A \end{array}$$

onde $i : X \rightarrow M$ e $j : M \rightarrow T(M)$ são inclusões, e A é uma k -álgebra. Sabe-se que A como um k -módulo gera um k -homomorfismo de módulos $\tilde{\varphi} : M \rightarrow A$, pois M é uma k -módulo livre com base X . Aplicando o functor T obtemos um homomorfismo de k -álgebras

$$T(\tilde{\varphi}) : T(M) \rightarrow T(A).$$

Para a existência de um homomorfismo de k -álgebras $T(M) \rightarrow A$, é suficiente definir um homomorfismo de k -álgebras $\mu : T(A) \rightarrow A$ tal que a composição $\mu \circ T(\tilde{\varphi})$ seja um homomorfismo de k -álgebras. Para cada p , considere o diagrama

$$\begin{array}{ccc} A \times \cdots \times A & \xrightarrow{h_p} & T^p(A) \\ & \searrow m_p & \downarrow \mu_p \\ & & A \end{array}$$

onde $h_p : (a_1, \dots, a_p) \mapsto a_1 \otimes \cdots \otimes a_p$ e $m_p : (a_1, \dots, a_p) \mapsto a_1 \cdots a_p$, onde $a_1 \cdots a_p$ é o produto dos elementos a_1, \dots, a_p na k -álgebra A . Como, m_p é k -multilinear, induz um k -homomorfismo μ_p que faz o diagrama comutativo. Defina

$$\mu : T(A) \rightarrow A$$

por $\mu = \sum_p \mu_p$. Para verificar que μ é multiplicativo, é suficiente mostrar

$$\mu_{p+q}((a_1 \otimes \cdots \otimes a_p)(a'_1 \otimes \cdots \otimes a'_q)) = \mu_p(a_1 \otimes \cdots \otimes a_p)\mu_q(a'_1 \otimes \cdots \otimes a'_q).$$

Mas essa equação segue da lei associativa em A :

$$(a_1 \cdots a_p)(a'_1 \cdots a'_q) = a_1 \cdots a_p a'_1 \cdots a'_q.$$

Finalmente, a unicidade desse homomorfismo de k -álgebras segue do fato de que M gera a $T(M)$ como uma k -álgebra. \square

Definição 2.33 Se k é um anel comutativo e M é um k -módulo livre com base X , então $T(M)$ é chamado o anel dos polinômios sobre k nas **variáveis não comutativas** X , e é denotado por $k \langle X \rangle$.

Se M é um k -módulo livre com base X , então cada elemento u de $T(M)$ tem a única expressão

$$u = \sum_{\substack{p \geq 0 \\ i_1, \dots, i_p}} r_{i_1, \dots, i_p} x_{i_1} \otimes \cdots \otimes x_{i_p}$$

onde $r_{i_1, \dots, i_p} \in k$ e $x_{i_j} \in X$.

Definição 2.34 Uma *apresentação* de uma k -álgebra A é a escolha de um sistema de geradores de X e um conjunto S de homomorfismos de k -álgebras

$$\varphi : A \longrightarrow A.$$

Uma apresentação que usaremos mais adiante é da álgebra associativa livre $k \langle X \rangle$.

2.3 Álgebras de Lie

As álgebras de Lie surgem "de maneira natural" como módulos de aplicações lineares dotados de uma nova operação que é em geral não é associativa. É possível descrever esse tipo de sistema abstrato com poucos axiomas.

Definição 2.35 Seja k um anel comutativo. Uma *k -álgebra de Lie* é um k -módulo L , com uma operação $L \times L \longrightarrow L$, denotada por $(x, y) \mapsto [x, y]$ e chamada o *colchete* ou *comutador* de x e y que satisfaz os seguintes axiomas:

- (i) A operação colchete é bilinear.
- (ii) $[x, x] = 0$ para todo $x \in L$.
- (iii) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ para todo $x, y, z \in L$

O axioma (iii) é chamado a **identidade de Jacobi**.

Como o colchete de Lie $[,]$ é bilinear, temos

$$0 = [x + y, x + y] = [x, x] + [x, y] + [y, x] + [y, y] = [x, y] + [y, x].$$

Portanto os axiomas (i) e (ii) implicam

$$(ii') \quad [x, y] = -[y, x] \text{ para todo } x, y \in L.$$

Inversamente, se $\text{car } k \neq 2$, é claro que (ii') implica (ii).

Exemplo 2.36 Seja k um anel comutativo e A uma k -álgebra associativa. Defina o colchete de Lie como

$$[x, y] = xy - yx$$

para todo $x, y \in A$. Afirmamos que A é uma álgebra de Lie.

De fato, considere $x, y, z \in A$ e $r \in k$, então

- (i) a operação $[,]$ é bilinear,

$$\begin{aligned} [x+y, z] &= (x+y)z - z(x+y) = xz + yz - zx - zy \\ &= (xz - zx) + (yz - zy) = [x, z] + [y, z] \end{aligned}$$

(análogo na outra coordenada) e também

$$\begin{aligned} r[x, y] &= r(xy - yx) = r(xy) - r(yx) \\ &= (rx)y - y(rx) \text{ pois } A \text{ é uma } k\text{-álgebra} \\ &= [rx, y] \end{aligned}$$

e analogamente $r[x, y] = [x, ry]$, assim $r[x, y] = [rx, y] = [x, ry]$

(ii) $[x, x] = xx - xx = 0$

(iii) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = (x(yz - zy) - (yz - zy)x) + (y(zx - xz) - (zx - xz)y) + (z(xy - yx) - (xy - yx)z) = 0,$

na última igualdade temos usado a associatividade da álgebra.

A álgebra de Lie obtida nesta forma é chamada **a álgebra de Lie** da álgebra associativa A . Denotamos esta álgebra de Lie por A_L .

Aqui temos um exemplo particular do exemplo anterior.

Exemplo 2.37 Suponha que L é um k -módulo de dimensão finita. A k -álgebra associativa $\text{End}_k(L)$ de todos os k -endomorfismos de L é uma k -álgebra de Lie, definindo o colchete de Lie $[\cdot, \cdot]$ por

$$[x, y] = x \circ y - y \circ x$$

para todo $x, y \in \text{End}_k(L)$, onde \circ denota a composição de aplicações. A fim de distinguir esta nova estrutura algébrica da antiga associativa, escrevemos $\mathfrak{gl}(L)$ para $\text{End}_k(L)$ visto como álgebra de Lie e é chamada a **álgebra linear geral**.

Definição 2.38 Sejam L e L' duas k -álgebras de Lie. Uma aplicação linear $\varphi : L \rightarrow L'$ é um **homomorfismo de k -álgebras de Lie** se

$$\varphi([x, y]) = [\varphi(x), \varphi(y)]$$

para todo $x, y \in L$. Além disso, φ é um isomorfismo se for um homomorfismo invertível. Neste caso φ é chamado um **isomorfismo de k -álgebras de Lie**. Duas k -álgebras de Lie L, L' são **isomorfas**, denotada por $L \cong L'$, se existe um isomorfismo de k -álgebras de Lie.

Similarmente, é natural a noção de subálgebra de Lie de L .

Definição 2.39 Um k -submódulo K de L é chamado uma **subálgebra** de L se $[x, y] \in K$ para todo $x, y \in K$; isto é

$$[K, K] \subseteq K$$

em particular, K é uma álgebra de Lie relativa às operações herdadas de L .

Definição 2.40 Um k -submódulo I de uma k -álgebra de Lie L é chamado um **ideal** de L se para todo $x \in L, y \in I$ temos que $[x, y] \in I$; isto é

$$[L, I] \subseteq I.$$

Observação 2.41 Os ideais fazem na teoria de álgebras de Lie, o papel dos subgrupos normais na teoria de grupos e dos ideais bilaterais na teoria de anéis.

A construção de uma **álgebra quociente** L/I (I um ideal de L) é formalmente igual à construção de um anel quociente. Como módulo, L/I é o módulo quociente, seu colchete de Lie é definido por

$$[x+I, y+I] = [x, y] + I.$$

Essa operação está bem definida, pois se $x+I = x'+I, y+I = y'+I$, então temos $x' = x+u$ ($u \in I$), $y' = y+v$ ($v \in I$) de onde

$$[x', y'] = [x, y] + ([u, y] + [x, v] + [u, v]),$$

e portanto $[x', y'] + I = [x, y] + I$, pois os termos entre parênteses estão em I .

Definição 2.42 Uma **representação** de uma k -álgebra de Lie L é um k -homomorfismo $\varphi : L \rightarrow \mathfrak{gl}(M)$, onde M é um k -módulo.

2.3.1 Álgebras Universais Envelopantes

Nesta subseção vamos estabelecer o conceito da **álgebra universal envelopante** $k[L]$ de uma álgebra de Lie L , onde k é um anel comutativo. A função principal de $k[L]$ é reduzir a teoria das representações de L a representações da álgebra associativa $k[L]$. Uma propriedade importante de $k[L]$ é que L é isomorfa a uma subálgebra de $(k[L])_L$.

Definição 2.43 Seja L uma álgebra de Lie. Um par $(k[L], i)$, onde $k[L]$ é uma álgebra associativa com elemento identidade 1 e $i : L \rightarrow k[L]$ é um homomorfismo de álgebras de Lie, é dito **álgebra universal envelopante** de L se dada qualquer álgebra associativa A com elemento identidade 1 e um homomorfismo de álgebras de Lie

$$\varphi : L \rightarrow A_L,$$

existe um único homomorfismo (de álgebras associativas)

$$\tilde{\varphi} : k[L] \longrightarrow A \text{ (com } \tilde{\varphi}(1) = 1)$$

tal que $\varphi = \tilde{\varphi} \circ i$; isto é, o diagrama é comutativo.

$$\begin{array}{ccc} k[L] & & \\ \uparrow i & \searrow \tilde{\varphi} & \\ L & \xrightarrow{\varphi} & A \end{array}$$

Assim, dada qualquer representação $\varphi : L \longrightarrow gl(L)$ existirá um único homomorfismo de k -álgebras associativas $\tilde{\varphi} : k[L] \longrightarrow gl(L)$ que fará comutar o diagrama:

$$\begin{array}{ccc} k[L] & & \\ \uparrow i & \searrow \tilde{\varphi} & \\ L & \xrightarrow{\varphi} & gl(L) \end{array}$$

Daremos a seguir propriedades importantes de $(k[L], i)$.

Teorema 2.44 1. Sejam $(k[L], i)$, $(k[L]', i')$ álgebras universais envelopantes de L . Então existe um único isomorfismo $j : k[L] \longrightarrow k[L]'$ tal que $i' = j \circ i$.

2. $k[L]$ é gerada $i(L)$ como álgebra associativa.

3. Sejam L_1, L_2 álgebras de Lie com suas respectivas $(k[L_1], i_1)$, $(k[L_2], i_2)$ álgebras universais envelopantes, e seja θ um homomorfismo de L_1 em L_2 . Então, existe um único homomorfismo θ' de $k[L_1]$ em $k[L_2]$ tal que $i_2 \circ \theta = \theta' \circ i_1$, isto é, temos um diagrama comutativo:

$$\begin{array}{ccc} L_1 & \xrightarrow{\theta} & L_2 \\ \downarrow i_1 & & \downarrow i_2 \\ k[L_1] & \xrightarrow{\theta'} & k[L_2] \end{array}$$

4. Sejam I um ideal de L e J o ideal de $k[L]$ gerado por $i(I)$. Se $l \in L$, então $j : l + I \mapsto i(l) + J$ é um homomorfismo de álgebras de Lie de L/I em $(k[L]/J)_L$, e $(k[L]/J, j)$ é a álgebra universal envelopante de L/I .

Demonstração.

1. Sejam $(k[L], i)$ e $(k[L]', i')$ duas álgebras universais envelopantes de L . No diagrama comutativo

$$\begin{array}{ccc} k[L] & & \\ \uparrow i & \searrow j & \\ L & \xrightarrow{i'} & k[L]' \end{array}$$

temos que, das propriedades universais de $k[L]$ e $k[L]'$ seguem respectivamente, que existem únicos $j : k[L] \rightarrow k[L]'$ tal que $i' = j \circ i$ e $j' : k[L]' \rightarrow k[L]$ tal que $i = j' \circ i'$. Mostraremos que j é um isomorfismo com inversa j' . Considere o diagrama comutativo

$$\begin{array}{ccc} & k[L]' & \\ & \uparrow & \searrow j \circ j' \\ L & \xrightarrow{i'} & k[L]' \end{array}$$

e como $k[L]'$ tem a propriedade universal e $id_{k[L]'}$ faz comutar o diagrama, segue da unicidade que $j \circ j' = id_{k[L]'}$. Reciprocamente, $j' \circ j = id_{k[L]}$. Portanto, j é um isomorfismo com inversa j' e $k[L] \cong k[L]'$.

2. Sejam K a subálgebra associativa de $k[L]$ gerada por $i(L)$ e ι a inclusão de K em $k[L]$. Seja $i' : k[L] \rightarrow K$ o único homomorfismo de álgebras associativas tal que $i = i' \circ i$. Logo, $\iota \circ i' : k[L] \rightarrow k[L]$ e o diagrama comutará

$$\begin{array}{ccccc} & k[L] & & & \\ & \uparrow & \searrow i' & \searrow \iota \circ i' & \\ L & \xrightarrow{i} & K & \xrightarrow{\iota} & k[L] \end{array}$$

Considerando o diagrama comutativo,

$$\begin{array}{ccc} & k[L] & \\ & \uparrow & \searrow \iota \circ i' \\ L & \xrightarrow{\iota \circ i} & k[L] \end{array}$$

e pela unicidade da extensão de $\iota \circ i$ temos que $\iota \circ i' = id_{k[L]}$. Portanto ι é um isomorfismo com inverso i' e $K = k[L]$.

3. Sejam L_1 e L_2 duas álgebras de Lie com $(k[L_1], i_1)$ e $(k[L_2], i_2)$ suas respectivas álgebras universais envelopantes, e

$$\theta : L_1 \rightarrow L_2$$

um homomorfismo de álgebras de Lie. Assim,

$$i_2 \circ \theta : L_1 \rightarrow (k[L_2])_L$$

é um homomorfismo de álgebras de Lie e daí existe um único homomorfismo de álgebras associativas $\theta' : k[L_1] \longrightarrow k[L_2]$ tal que $\theta' \circ i_1 = i_2 \circ \theta$.

$$\begin{array}{ccc} L_1 & \xrightarrow{\theta} & L_2 \\ \downarrow i_1 & \searrow i_2 \circ \theta & \downarrow i_2 \\ k[L_1] & \xrightarrow{\theta'} & k[L_2] \end{array} .$$

4. Para mostrar que j é um homomorfismo de álgebras de Lie, basta considerar o homomorfismo de álgebras de Lie

$$\varphi : L \longrightarrow (k[L]/J)_L$$

tal que $l \mapsto i(l) + J$, para todo $l \in L$ e observar que $i(I) \subseteq J$, então $\varphi(I) = 0$, induzindo assim o homomorfismo j de álgebras de Lie.

Seja A uma álgebra associativa qualquer e

$$\theta : L/I \longrightarrow A_L$$

um homomorfismo de álgebras de Lie.

Considerando a projeção canônica $\pi : L \longrightarrow L/I$ temos que $\theta \circ \pi : L \longrightarrow A_L$ é homomorfismo de álgebras de Lie (pois é composta de homomorfismos), e pela propriedade universal de $k[L]$ segue que existe um homomorfismo de álgebras associativas

$$(\theta \circ \pi)' : k[L] \longrightarrow A$$

tal que $\theta \circ \pi = (\theta \circ \pi)' \circ i$.

Temos assim $I \subseteq \text{Ker}(\theta \circ \pi)$ e daí $J \subseteq \text{Ker}(\theta \circ \pi)'$, o que induz o homomorfismo de álgebras associativas

$$\theta' : k[L]/J \longrightarrow A,$$

onde $u + J \mapsto (\theta \circ \pi)'(u)$ para todo $u \in k[L]$ e temos que

$$\theta(l + I) = (\theta \circ \pi)(l) = (\theta \circ \pi)' \circ i(l)$$

e também

$$\theta' \circ j(l + I) = \theta'(i(l) + J) = (\theta \circ \pi)' \circ i(l) = \theta(l + I),$$

daí $\theta' \circ j = \theta$.

Precisamos mostrar que θ' é único. Mas isto segue do item (2) deste teorema observando o fato que $\theta'(l + I) = i(l) + J$ para todo $l + I \in L/I$, ou seja, $j(L/I)$ gera $k[L]/J$ como k -álgebra associativa.

□

Temos do item (1) do teorema anterior a unicidade da álgebra universal. A existência de um par adequado $(k[L], i)$ não é difícil estabelecer como se mostra na seguinte:

Observação 2.45 *Seja $T(L)$ a álgebra tensorial sobre L (ver definição 2.29), e J o ideal bilateral em $T(L)$ gerado por todos os elementos*

$$a \otimes b - b \otimes a - [a, b] \quad (a, b \in L).$$

Defina $k[L] = T(L)/J$, e considere-se o homomorfismo canônico $\pi : T(L) \rightarrow k[L]$.

Afirmamos que $(k[L], i)$ é a álgebra universal envelopante de L , onde

$$i : L \rightarrow k[L]$$

é a restrição de π a L . Consideremos

$$j : L \rightarrow A_L$$

como na definição 2.43, onde A é uma álgebra associativa com elemento identidade 1. Da propriedade universal de $T(L)$ segue que existe um homomorfismo de álgebras associativas

$$\phi' : T(L) \rightarrow A$$

que estende j e leva 1 em 1. A propriedade

$$j([a, b]) = [j(a), j(b)] = j(a)j(b) - j(b)j(a) \text{ para } a, b \in L,$$

de j força todos os $a \otimes b - b \otimes a - [a, b]$ estarem em $\text{Ker } \phi'$, assim ϕ' induz um homomorfismo $\phi : k[L] \rightarrow A$ tal que $\phi \circ i = j$.

$$\begin{array}{ccc} k[L] & & \\ \uparrow i & \searrow \phi & \\ L & \xrightarrow{j} & A \end{array}$$

A unicidade de ϕ segue do fato de que, 1 e $\text{Im}(i)$ juntos geram $k[L]$.

O Lema do Diamante de Bergman

3.1 O Teorema Principal: Bases para k -Álgebras Associativas

Seja k um anel (associativo) comutativo com elemento identidade 1, X um conjunto, $\langle X \rangle$ o semigrupo livre com elemento identidade 1 sobre X , e $k \langle X \rangle$ a k -álgebra associativa livre sobre X .

Começaremos com algumas definições dadas em [1].

Definição 3.1 *Seja S um conjunto de pares da forma $\sigma = (W_\sigma, f_\sigma)$, onde $W_\sigma \in \langle X \rangle$ e $f_\sigma \in k \langle X \rangle$. Para qualquer $\sigma \in S$ e $A, B \in \langle X \rangle$, $r_{A\sigma B}$ denota o endomorfismo de k -módulos de $k \langle X \rangle$ que fixa todos os elementos de $\langle X \rangle$ com exceção de $AW_\sigma B$, e que envia este elemento para $Af_\sigma B$. S é chamado um **sistema de redução** e as aplicações*

$$r_{A\sigma B} : k \langle X \rangle \longrightarrow k \langle X \rangle$$

são chamadas de **reduções**.

Definição 3.2 *Dizemos que uma redução $r_{A\sigma B}$ atua **trivialmente** sobre um elemento $a \in k \langle X \rangle$ se o coeficiente de $AW_\sigma B$ em a é zero, e diremos que a é **irreduzível** (em S) se cada redução é trivial sobre a , isto é, se a não envolve nenhum dos monômios $AW_\sigma B$. O k -submódulo de todos os elementos irreduzíveis de $k \langle X \rangle$ será denotado por $k \langle X \rangle_{irr}$. Uma sequência finita de reduções r_1, \dots, r_n ($r_i = r_{A_i \sigma_i B_i}$) será chamada **final** sobre $a \in k \langle X \rangle$ se*

$$(r_n \circ \dots \circ r_1)(a) \in k \langle X \rangle_{irr}.$$

Definição 3.3 *Um elemento a de $k \langle X \rangle$ será chamado de **redução finita** se para cada sequência infinita r_1, r_2, \dots de reduções, r_i atua trivialmente sobre $(r_{i-1} \circ \dots \circ r_1)(a)$ para todo i suficientemente grande.*

Se a é de redução finita, então qualquer sequência maximal de reduções r_i , tal que cada r_i atua não trivialmente sobre $(r_{i-1} \circ \dots \circ r_1)(a)$, será finita, e portanto uma sequência final.

Segue-se de sua definição que os elementos de redução finita formam um k -submódulo de $k \langle X \rangle$.

Definição 3.4 Dizemos que $a \in k \langle X \rangle$ é de **redução única** se é de redução finita e suas imagens com respeito a todas as sequências de reduções finais é a mesma. Esse valor comum será denotado por $r_S(a)$.

O lema seguinte irá lidar com as dificuldades na prova de nosso teorema principal, que resultará da união possível e cancelamento de termos após uma redução de uma soma ou produto.

Lema 3.5

- (i) O conjunto de elementos de redução única de $k \langle X \rangle$ forma um k -submódulo, e r_S é uma aplicação k -linear deste submódulo em $k \langle X \rangle_{irr}$.
- (ii) Suponha que $a, b, c \in k \langle X \rangle$ são de tal forma que para todos os monômios A, B, C com coeficientes não nulos em a, b, c , respectivamente, o produto ABC é de redução única. (Em particular, isto implica que abc é de redução única.) Seja r qualquer composição finita de reduções. Então, $ar(b)c$ é de redução única, e

$$r_S(ar(b)c) = r_S(abc).$$

Demonstração.

- (i) Suponha que $a, b \in k \langle X \rangle$ são de redução única e $\alpha \in k$. Sabemos que $\alpha a + b$ é de redução finita. Seja r qualquer composição de reduções finais sobre esse elemento, então

$$r(\alpha a + b) = r_S(\alpha a + b).$$

Como a é de redução única podemos encontrar uma composição finita de reduções r' tal que

$$r'r(a) = r_S(a),$$

e similarmente existe uma composição finita de reduções r'' tal que

$$r''r'r(b) = r_S(b).$$

Como $r(\alpha a + b)$ é irredutível, temos

$$r(\alpha a + b) = r''r'r(\alpha a + b) = \alpha r''r'r(a) + r''r'r(b) = \alpha r_S(a) + r_S(b),$$

segundo-se nossa afirmação.

- (ii) De (i) e a forma como (ii) está formulado, claramente é suficiente provar (ii) no caso em que a, b, c são os monômios A, B, C , e r é uma única redução $r_{D\sigma E}$. Mas neste caso

$$Ar_{D\sigma E}(B)C = r_{AD\sigma EC}(ABC),$$

é a imagem de ABC com respeito a uma redução, portanto é de redução única se ABC também for, com a mesma forma reduzida.

□

Definição 3.6 Chamemos a uma 5-upla (σ, τ, A, B, C) com $\sigma, \tau \in S$ e $A, B, C \in \langle X \rangle \setminus \{1\}$, tal que

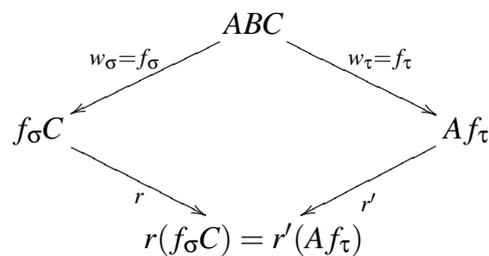
$$W_\sigma = AB, \quad W_\tau = BC,$$

uma **ambiguidade de sobreposição** de S . Dizemos que a ambiguidade de sobreposição (σ, τ, A, B, C) é **resolúvel**, se existem composições de reduções, r e r' , tais que

$$r(f_\sigma C) = r'(Af_\tau)$$

(a condição do diamante sobre os resultados das duas formas indicadas para reduzir ABC).

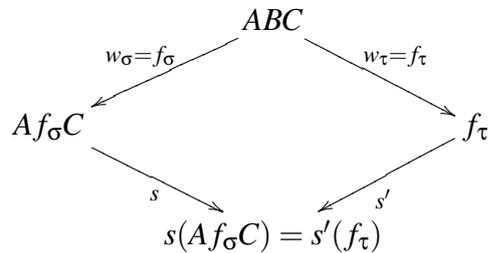
O diagrama a seguir ilustra o definido



Definição 3.7 Uma 5-upla (σ, τ, A, B, C) com $\sigma \neq \tau \in S$ e $A, B, C \in \langle X \rangle$ será uma **ambiguidade de inclusão** se

$$W_\sigma = B, \quad W_\tau = ABC;$$

e tal ambiguidade será **resolúvel** se $Af_\sigma C$ e f_τ podem ser reduzidas a uma expressão comum.



Definição 3.8 Por uma **ordem parcial de semigrupo** sobre $\langle X \rangle$ entendemos uma ordem parcial " \leq ", tal que

$$B < B' \Rightarrow ABC < AB'C \quad (A, B, B', C \in \langle X \rangle),$$

e será chamada **compatível** com S se para todo $\sigma \in S$, f_σ é uma combinação linear de monômios $\langle W_\sigma$.

Denotamos por I o ideal bilateral de $k \langle X \rangle$ gerado pelos elementos $W_\sigma - f_\sigma$ ($\sigma \in S$). Como um k -módulo, I é gerado pelos produtos $A(W_\sigma - f_\sigma)B$.

Definição 3.9 Se \leq é uma ordem parcial sobre $\langle X \rangle$ compatível com o sistema de redução S , e A é qualquer elemento de $\langle X \rangle$, I_A denotará o submódulo de $k \langle X \rangle$ gerado por todos os elementos $B(W_\sigma - f_\sigma)C$ tal que $BW_\sigma C < A$. Dizemos que a ambiguidade de sobreposição (σ, τ, A, B, C) é **resolúvel relativo a \leq** se

$$f_\sigma C - Af_\tau \in I_{ABC}$$

(ou para a ambiguidade de inclusão, se $Af_\sigma C - f_\tau \in I_{ABC}$). Qualquer ambiguidade resolúvel é resolúvel relativa a \leq .

Teorema 3.10 (O Lema do Diamante de Bergman) Seja S um sistema de redução para a álgebra associativa livre $k \langle X \rangle$ (um subconjunto de $\langle X \rangle \times k \langle X \rangle$), e \leq uma ordem parcial de semigrupo sobre $\langle X \rangle$, compatível com S , e satisfazendo a CCD. Então as seguintes condições são equivalentes:

- (a) Todas as ambiguidades de S são resolúveis;
- (a') Todas as ambiguidades de S são resolúveis relativo a \leq ;
- (b) Todos os elementos de $k \langle X \rangle$ são de redução única com relação a S ;
- (c) Um conjunto de representantes em $k \langle X \rangle$ para os elementos da álgebra

$$R = k \langle X \rangle / I$$

determinado pelos geradores X e as relações $W_\sigma = f_\sigma$ ($\sigma \in S$) é dado pelo k -submódulo $k \langle X \rangle_{irr}$ gerado pelos monômios S -irredutíveis de $\langle X \rangle$.

Quando essas condições são verdadeiras, R pode ser identificado com o k -módulo $k \langle X \rangle_{irr}$, que é uma k -álgebra com a multiplicação $a.b = r_S(ab)$.

Demonstração. Observamos facilmente de nossa hipótese geral, por indução com relação à ordenação parcial \leq com a condição de cadeia descendente, que cada elemento de $\langle X \rangle$, e portanto cada elemento de $k \langle X \rangle$, é de redução finita.

Para mostrarmos que (b) \Leftrightarrow (c), primeiro note que (c) implica dizer que

$$k \langle X \rangle = k \langle X \rangle_{irr} \oplus I.$$

Assumindo (b), observamos que

$$r_S : k \langle X \rangle \longrightarrow k \langle X \rangle_{irr}$$

é uma projeção sobrejetiva, pois todos os elementos de $k \langle X \rangle$ são de redução única; seu núcleo está contido em I porque cada redução altera um elemento por um membro de I , e contém I porque para todo A, B, σ ,

$$r_S(A(W_\sigma - f_\sigma)B) = r_S(AW_\sigma B) - r_S(Af_\sigma B) = 0$$

pelo lema 3.5(i). Então

$$k \langle X \rangle / \text{Ker}(r_S) \cong \text{Im}(r_S).$$

Logo $k \langle X \rangle / I \cong k \langle X \rangle_{irr}$ provando (c). Reciprocamente, assumamos (c) e suponhamos que $a \in k \langle X \rangle$ pode ser reduzido tanto a $b, b' \in k \langle X \rangle_{irr}$. Então

$$a = b + I \text{ e } a = b' + I,$$

logo $b - b' \in I$, e $b - b' \in k \langle X \rangle_{irr}$ pois $k \langle X \rangle_{irr}$ é um k -submódulo de $k \langle X \rangle$. Portanto

$$b - b' \in k \langle X \rangle_{irr} \cap I = \{0\},$$

assim $b = b'$, provando (b).

O comentário final na afirmação do teorema é claro, e as implicações (b) \Rightarrow (a) \Rightarrow (a') são imediatas. Resta provar (a') \Rightarrow (b).

Assumamos (a'). Será suficiente provar que todos os monômios $D \in \langle X \rangle$ são de redução única, pois os elementos de redução única de $k \langle X \rangle$ formam um submódulo. Vamos assumir por indução que todos os monômios $\langle D \rangle$ são de redução única. Assim, o domínio de r_S inclui o submódulo gerado por todos esses monômios, portanto o núcleo de r_S contém I_D . Devemos mostrar que dadas quaisquer duas reduções $r_{L\sigma M'}$ e $r_{L'\tau M}$ agindo não trivialmente sobre D (e, conseqüentemente levando D a uma combinação linear de monômios $\langle D \rangle$) temos

$$r_S(r_{L\sigma M'}(D)) = r_S(r_{L'\tau M}(D)).$$

Existem três casos de acordo com as localizações relativas das subpalavras W_σ e W_τ no monômio D . Podemos assumir sem perda de generalidade que

$$\text{comprimento}(L) \leq \text{comprimento}(L'),$$

isto é, que a cópia indicada de W_σ em D não começa depois da copia indicada de W_τ .

Caso 1 . As subpalavras W_σ e W_τ se sobrepõem em D , mas nenhuma contém a outra. Então $D = LABCM$, onde (σ, τ, A, B, C) é uma ambiguidade de sobreposição de S , e

$$r_{L\sigma M'}(D) - r_{L'\tau M}(D) = L(f_\sigma C - Af_\tau)M.$$

Por (a'), $f_\sigma C - Af_\tau \in I_{ABC}$. Assim $L(f_\sigma C - Af_\tau)M \in I_{LABCM} = I_D$ que é eliminado por r_S . Portanto

$$r_S(r_{L\sigma M'}(D)) - r_S(r_{L'\tau M}(D)) = 0,$$

como queríamos.

Caso 2 . Uma das subpalavras W_σ , W_τ de D está contida na outra. Esse caso é tratado como no caso anterior usando a resolubilidade das ambiguidades de inclusão relativas a \leq .

De fato, se $D = LABCM$, onde (σ, τ, A, B, C) é uma ambiguidade de inclusão de S , e

$$r_{L'\sigma M'}(D) - r_{L\tau M}(D) = L(Af_\sigma C - f_\tau)M.$$

Por (a'), $Af_\sigma C - f_\tau \in I_{ABC}$. Logo $L(Af_\sigma C - f_\tau)M \in I_{LABCM} = I_D$, como $I_D \subseteq \text{Ker}(r_S)$ obtemos $r_S(r_{L'\sigma M'}(D)) - r_S(r_{L\tau M}(D)) = 0$, como queríamos.

Caso 3 . Se W_σ e W_τ são subpalavras disjuntas de D . Então $D = LW_\sigma N W_\tau M$, e devemos provar que os elementos $Lf_\sigma N W_\tau M$ e $LW_\sigma N f_\tau M$ são iguais. Mas o Lema 3.5(ii) mostra que cada um deles é igual a $r_S(Lf_\sigma N f_\tau M)$.

□

Alguém poderia perguntar: Se um sistema de redução S têm ambiguidades não resolúveis, será possível fazer com que o procedimento de redução esteja bem definido mediante a restrição de nosso processo de redução por algumas regras adicionais que especificam qual é a redução a aplicar sempre que houver uma escolha? Isso daria um

processo bem definido, mas não uma forma canônica. Duas expressões irreduzíveis para um elemento que poderia ter sido reduzido no âmbito do processo não restrito ainda serão distintas expressões irreduzíveis para o mesmo elemento de L . Veremos na próxima seção que a maneira de lidar com as ambiguidades não resolúveis não é restringir mas de aumentar nosso processo de redução.

Neste trabalho estamos interessados principalmente nas formas canônicas, mas o seguinte Corolário pode ser de uso para outros fins, veja [1].

Corolário 3.11 *Seja $k \langle X \rangle$ uma álgebra associativa livre, $e \leq$ uma ordem parcial de semigrupo de $\langle X \rangle$ com condições de cadeia descendente. Se S é um sistema de reduções sobre $k \langle X \rangle$ compatível com \leq e sem ambiguidades, então o conjunto de reduções $W_\sigma = f_\sigma(\sigma \in S)$ da k -álgebra é independente. Mais geralmente, se $S_1 \subseteq S_2$ são sistemas de reduções, tal que S_2 é compatível com \leq e todas suas ambiguidades são resolúveis, e se S_2 contem algum σ tal que W_σ é irreduzível com respeito a S_1 , então, a inclusão dos ideais associados a esse sistema, $I_1 \subset I_2$, é estrita.*

3.2 Aplicação: Um Problema sobre Idempotentes

Consideremos o seguinte problema:

Seja R um anel no qual, se $x + x = 0$ ou $x + x + x = 0$, segue-se que $x = 0$. Suponhamos que a, b, c e $a + b + c$ são todos idempotentes em R . Segue-se que $ab = 0$?

Evidentemente devemos estudar o anel R definido pelos geradores a, b, c e reduções:

$$a^2 = a, \quad (3-1)$$

$$b^2 = b, \quad (3-2)$$

$$c^2 = c, \quad (3-3)$$

$$(a + b + c)^2 = a + b + c. \quad (3-4)$$

Podemos usar as três primeiras relações para eliminar monômios que contêm as sequências aa, bb, cc de todas as expressões em R . Se em (3-4) expandimos o lado esquerdo, e simplificando o resultado usando (3-1), (3-2) e (3-3),

$$\begin{aligned} (a + b + c)(a + b + c) &= a + b + c \\ a^2 + ab + ac + ba + b^2 + bc + ca + cb + c^2 &= a + b + c \\ a + ab + ac + ba + b + bc + ca + cb + c &= a + b + c \\ ab + ac + ba + bc + ca + cb &= 0 \end{aligned}$$

obtemos

$$ba = -ab - bc - cb - ac - ca \quad (3-5)$$

Se (3-1) – (3-3) e (3-5) são usados como fórmulas de reduções, isto dará formas canônicas únicas para os elementos de R ? Há cinco sequências ambigualmente redutíveis:

$$aaa, bbb, ccc; baa, bba.$$

A resolubilidade das três primeiras ambiguidades é imediata. Mas, nos últimos dois casos, se reduzimos o monômio em questão nas duas formas possíveis, igualamos as expressões resultantes e completamos as reduções obtemos uma equação não trivial.

De fato, estudamos primeiro baa : Reduzimos a expressão baa aplicando (3-5), de modo que obtemos

$$\begin{aligned} & (-ab - bc - cb - ac - ca)a \\ &= -aba - bca - cba - aca - caa. \end{aligned}$$

Usamos as reduções anteriores para reduzir mais a expressão acima

$$\begin{aligned} & -a(-ab - bc - cb - ac - ca) - bca - c(-ab - bc - cb - ac - ca) - aca - ca \\ &= aab + abc + acb + aac + aca - bca + cab + cbc + ccb + cac + cca - aca - ca \\ &= ab + abc + acb + ac - bca + cab + cbc + cb + cac + ca - ca \\ &= ab + abc + acb + ac - bca + cab + cbc + cb + cac \end{aligned}$$

No entanto, se reduzimos a expressão baa , aplicando (3-1), obtemos $ba = -ab - bc - cb - ac - ca$. Portanto, igualando as duas expressões resultantes, temos

$$ab + abc + acb + ac - bca + cab + cbc + cb + cac = -ab - bc - cb - ac - ca.$$

Isolando um termo cuidadosamente escolhido, vem:

$$bca = abc + acb + cab + cac + cbc + 2ab + 2ac + 2cb + bc + ca.$$

Agora estudamos a expressão bba : Reduzimos-lho primeiro aplicando (3-5), de modo que obtemos

$$\begin{aligned} & b(-ab - bc - cb - ac - ca) \\ &= -bab - bbc - bcb - bac - bca. \end{aligned}$$

Usamos as reduções anteriores para reduzir mais a expressão acima

$$\begin{aligned}
& -(-ab - bc - cb - ac - ca)b - bc - bcb - (-ab - bc - cb - ac - ca)c - bca \\
& = abb + bcb + cbb + acb + cab - bc - bcb + abc + bcc + cbc + acc + cac - bca \\
& = ab + bcb + cb + acb + cab - bc - bcb + abc + bc + cbc + ac + cac - bca \\
& = ab + cb + acb + cab + abc + cbc + ac + cac - bca
\end{aligned}$$

No entanto, se reduzimos a expressão bba , aplicando (3-2), obtemos $ba = -ab - bc - cb - ac - ca$. Portanto, igualando as duas expressões resultantes, temos

$$ab + cb + acb + cab + abc + cbc + ac + cac - bca = -ab - bc - cb - ac - ca.$$

Isolando de novo um termo cuidadosamente escolhido,

$$bca = abc + acb + cab + cac + cbc + 2ab + 2ac + 2cb + bc + ca.$$

Portanto observamos que nas reduções das expressões baa e bba obtemos o mesmo resultado, isto é

$$bca = abc + acb + cab + cac + cbc + 2ab + 2ac + 2cb + bc + ca. \quad (3-6)$$

Se isto é adicionado a nossa lista de regras de redução, então baa e bba se reduzem a expressões únicas. Porém duas novas ambiguidades foram criadas: $bbca$ e $bcaa$. Mas quando analisamos cada uma dessas na mesma forma (uma página completa de cálculos) todos os termos se cancelam.

De fato, para nossa comodidade mostraremos o processo de redução só da expressão $bbca$: Primeiro aplicamos (3-6), de modo que obtemos

$$\begin{aligned}
& b(abc + acb + cab + cac + cbc + 2ab + 2ac + 2cb + bc + ca) \\
& = babc + bacb + bcab + bcac + bcbc + 2bab + 2bac + 2bcb + bbc + bca.
\end{aligned}$$

Para reduzir mais a expressão acima usamos as reduções anteriores

$$babc + bacb + bcab + bcac + bcbc + 2bab + 2bac + 2bcb + bc + bca.$$

Por outro lado, se reduzimos a expressão $bbca$, aplicando (3-2), obtemos bca . Igualando as duas expressões anteriores

$$babc + bacb + bcab + bcac + bcbc + 2bab + 2bac + 2bcb + bc + bca = bca$$

obtemos

$$babc + bacb + bcab + bcac + bcbc + 2bab + 2bac + 2bcb + bc = 0.$$

Assim,

$$(-ab - bc - cb - ac - ca)bc + (-ab - bc - cb - ac - ca)cb + (abc + acb + cab + cac + cbc + 2ab + 2ac + 2cb + bc + ca)b + (abc + acb + cab + cac + cbc + 2ab + 2ac + 2cb + bc + ca)c + bcbc + 2(-ab - bc - cb - ac - ca)b + 2(-ab - bc - cb - ac - ca)c + 2bcb + bc = 0$$

$$\begin{aligned} & -abbc - bc bc - cb bc - acbc - cabc - abcb - bccb - cbcb - ac cb - cacb + abcb + \\ & acbb + cabb + cacb + cbc b + 2abb + 2acb + 2cbb + bcb + cab + abcc + acbc + cabc + \\ & cacc + cbcc + 2abc + 2acc + 2cbc + bcc + cac + bcbc - 2abb - 2bcb - 2cbb - 2acb - \\ & 2cab - 2abc - 2bcc - 2cbc - 2acc - 2cac + 2bcb + bc = 0 \end{aligned}$$

$$\begin{aligned} & -abc - bc bc - cbc - acbc - cabc - abcb - bccb - cbcb - acb - cacb + abcb + acb + \\ & cab + cacb + cbc b + 2ab + 2acb + 2cb + bcb + cab + abc + acbc + cabc + cac + cbc + \\ & 2abc + 2ac + 2cbc + bc + cac + bcbc - 2ab - 2bcb - 2cb - 2acb - 2cab - 2abc - 2bc - \\ & 2cbc - 2ac - 2cac + 2bcb + bc = 0 \end{aligned}$$

$$0 = 0$$

Fazendo o mesmo procedimento anterior com a expressão $bcaa$, obtemos a última igualdade. Aceitando esse resultado, concluímos que não será necessário adicionar mais fórmulas a nossa lista.

Os monômios irredutíveis neste sistema de redução são essas palavras em a, b e c no qual nenhuma letra acontece duas vezes na sequência, e as sequências ba e bca nunca acontecem; isto é, b nunca ocorre (imediatamente ou a uma distância) à esquerda de a .

Para observar que esse procedimento eventualmente termina para cada elemento, note que em cada uma das equações (3-1)-(3-3), (3-5) e (3-6), o lado direito é uma combinação linear de termos que são de comprimento menor que o lado esquerdo, ou têm o mesmo comprimento, poucas ocorrências de b à esquerda de a , e nenhuma ocorrência total de b ou a . Disto segue-se que o mesmo será verdadeiro para as equações obtidas aplicando uma dessas reduções a uma subpalavra de alguma palavra mais longa. (A observação sobre o total de ocorrências de b e a é necessária para essa dedução. se falharam, isto é, se o lado direito de (3-6) tem o termo aca , então reduzindo $bcbca$, o número de ocorrências de b à esquerda de a não pode diminuir). Em linguagem formal, então, a ordem parcial de monômios que faz $U < V$ se U tem comprimento menor que V , ou se tem mesmo comprimento mas com um número menor de b 's à esquerda dos a 's e U não pode conter mais a 's ou b 's que V , é uma ordem parcial de semigrupo que satisfaz DCC e é compatível com nossos sistemas de reduções (3-1)-(3-3), (3-5) e (3-6). Pelo Teorema 3.10 todas as ambiguidades desse sistema são resolúveis. Portanto, concluímos que as palavras irredutíveis formarão uma \mathbb{Z} -base para R . Em particular, 2 e 3 não são divisores de zero em R , e $ab \neq 0$ pois é um elemento da base do anel R assim, a questão original é respondida de forma negativa.

3.3 Aplicação: O Teorema de Poincaré-Birkhoff-Witt

Seja k um anel comutativo e L uma álgebra de Lie que é livre como um k -módulo, sobre uma base X . Formamos a k -álgebra associativa livre $k \langle X \rangle$ como na Definição 2.33, e identificamos L como o k -submódulo de $k \langle X \rangle$ gerado por X de acordo à Proposição 2.32. Assim, temos o colchete de Lie $[\cdot, \cdot]$ operando sobre esse submódulo de $k \langle X \rangle$.

Denotamos por $k[L]$, $k \langle X \rangle / J$, onde J é o ideal bilateral gerado por todos os elementos

$$ab - ba - [a, b] \quad (a, b \in L)$$

com o produto indicando o produto tensorial. Dado $a \in L$ vamos escrever a' para a imagem de a em $k[L]$. Sabemos que $k[L]$ é a álgebra universal envelopante de L .

Escolhemos uma ordem total \preceq sobre X . Observe que pela k -bilinearidade do colchete de Lie de L , o ideal I será gerado pelos elementos

$$xy - yx - [x, y]$$

com $x, y \in X$. Além disso, pela antissimetria do colchete, tais elementos com $x \prec y$ de fato geram o ideal todo.

Teorema 3.12 (*Poincaré-Birkhoff-Witt (PBW)*) *A álgebra universal envelopante $k[L]$ é livre como um k -módulo, sobre a base que consiste de todos os produtos $x'y' \dots z'$ com $x, y, \dots, z \in X$ e $x \preceq y \preceq \dots \preceq z$.*

Demonstração. Seja S o sistema de redução sobre $k \langle X \rangle$ que consiste de todos os pares

$$\sigma_{xy} = (yx, xy - [x, y])$$

para todo $y \succ x$ em X . Assim, o ideal gerado pelas diferenças $W_\sigma - f_\sigma$ ($\sigma \in S$) é precisamente J , e as imagens em $k[L]$ das palavras irredutíveis com respeito a S são precisamente a base requerida.

Para mostrar que esse sistema de reduções deve terminar, definimos o **índice de ordenação** de um elemento $x_1 \cdots x_n \in \langle X \rangle$ como o número de pares (i, j) tal que $i < j$ mas $x_i \succ x_j$. (Por exemplo, 0 se $x_1 \preceq \dots \preceq x_n$, $n(n-1)/2$ se $x_1 \succ \dots \succ x_n$). Ordenamos parcialmente $\langle X \rangle$ tomando $A \leq B$ se A é de comprimento menor ou igual que o de B , ou se A é uma permutação dos termos de B mas tem menor ou igual índice de ordenação. Então é simples verificar que \leq é uma ordem parcial de semigrupo em $\langle X \rangle$, compatível com S , e satisfazendo CCD.

De fato, de nossa definição temos que \leq é uma ordem parcial. Se $B < B'$, isto é, B tem comprimento menor que B' , ou tem um menor índice de ordenação, então $AB < AB'$ já que $A \leq A$ e portanto $ABC < AB'C$ pois também $C \leq C$. Assim, mostramos que \leq é uma ordem parcial de semigrupo sobre $\langle X \rangle$. Seja $\sigma \in S$, isto é,

$$\sigma = \sigma_{xy} \text{ para } y \succ x.$$

Como

$$xy < W_\sigma = yx, \quad [x, y] < W_\sigma = yx$$

e $f_\sigma = xy - [x, y]$, temos claramente que \leq é compatível com S . Observe que para qualquer $a, b \in L$,

$$ab - ba - [a, b] \in I_C \text{ para qualquer } C \in \langle X \rangle \text{ de comprimento } > 2. \quad (3-7)$$

As ambiguidades de S são claramente e precisamente as 5-uplas $(\sigma_{xy}, \sigma_{yz}, z, y, x)$ com $z \succ y \succ x \in X$. Para resolver uma ambiguidade relativa a \leq devemos estudar o elemento zyx ,

$$\begin{aligned} r_{1\sigma_{zy}x}(zyx) - r_{z\sigma_{yx}1}(zyx) &= (yz - [y, z])x - z(xy - [x, y]) \\ &= (yzx - [y, z]x) - (zxy - z[x, y]) \end{aligned}$$

Para reduzir mais o termo yzx , aplicamos $r_{y\sigma_{zx}1}$. Similarmente, para zxy aplicamos $r_{1\sigma_{zx}y}$. De modo que obtemos

$$\begin{aligned} &(y(xz - [x, z]) - [y, z]x) - ((xz - [x, z])y - z[x, y]) \\ &= (yxz - y[x, z] - [y, z]x) - (xzy - [x, z]y - z[x, y]). \end{aligned}$$

Da mesma forma, para reduzir yxz , aplicamos $r_{1\sigma_{yx}z}$. Similarmente, para tratar com xzy , aplicamos $r_{x\sigma_{zy}1}$. Assim

$$\begin{aligned} &((xy - [x, y])z - y[x, z] - [y, z]x) - (x(yz - [y, z]) - [x, z]y - z[x, y]) \\ &= (xyz - [x, y]z - y[x, z] - [y, z]x) - (xyz - x[y, z] - [x, z]y - z[x, y]) \\ &= (x[y, z] - [y, z]x) - (y[x, z] - [x, z]y) + (z[x, y] - [x, y]z) \\ &= (x[y, z] - [y, z]x) + (y[z, x] - [z, x]y) + (z[x, y] - [x, y]z) \end{aligned}$$

Na última igualdade, usamos a antissimetria do colchete de Lie. Além disso, de (3-7) obtemos que a última igualdade é igual a $([x, [y, z]] + [y, [z, x]] + [z, [x, y]])$ módulo I_{zyx} , isto é,

$$\begin{aligned} &([x, [y, z]] + [y, [z, x]] + [z, [x, y]]) \text{ mod } I_{zyx} \\ &= 0 \text{ mod } I_{zyx}, \end{aligned}$$

pela identidade de Jacobi em L .

Então,

$$r_{1\sigma_{zy}x}(zyx) - r_{z\sigma_{yx}1}(zyx) = 0 \text{ mod } I_{zyx}$$

$$r_{1\sigma_{zy}x}(zyx) = r_{z\sigma_{yx}1}(zyx) \text{ mod } I_{zyx}.$$

Assim, nossas ambiguidades são resolúveis relativas a \leq . Portanto, pelo teorema 3.10, $k[L]$ tem a base indicada. \square

Observação 3.13 *Observamos que para um corpo k e L, L' álgebras de Lie sobre k , é uma questão em aberta:*

$$\text{Se } k[L] \cong k[L'] \text{ implica } L \cong L'.$$

3.4 Aplicação: Como Tirar Proveito das Identidades

Suponha-se dadas $z \succ y \succ x$ como na prova do Teorema 3.12. A identidade de Jacobi para comutadores em $k \langle X \rangle$ diz que

$$[x, [y, z]]_{k \langle X \rangle} + [y, [z, x]]_{k \langle X \rangle} + [z, [x, y]]_{k \langle X \rangle} = 0. \quad (3-8)$$

Observamos que aplicando reduções de S a termos apropriados, podemos reduzir o lado esquerdo de (3.8), primeiro a

$$[x, [y, z]]_{k \langle X \rangle} + [y, [z, x]]_{k \langle X \rangle} + [z, [x, y]]_{k \langle X \rangle},$$

e finalmente a

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0,$$

que é zero pela identidade de Jacobi em L . Agora, observe que se os termos do lado esquerdo de (3-8) são expandidos, o monômio zyx aparece exatamente duas vezes, no primeiro termo e no terceiro (com sinal oposto), e que nas reduções que fizemos, $r_{1\sigma_{zyx}}$ age no primeiro termo, e $r_{z\sigma_{yx1}}$ age no segundo. Além disso, todas as outras reduções que fizemos no lado esquerdo de (3-8) afetam monômios $\prec zyx$ sob a ordem parcial do Teorema 3.12. Portanto, alterado o valor por membros de I_{zyx} . Como começamos e terminamos com 0, podemos concluir que

$$r_{1\sigma_{zyx}}(zyx) - r_{z\sigma_{yx1}}(zyx) \in I_{zyx},$$

como queríamos.

O seguinte Lema estabelece o princípio geral acima.

Lema 3.14 *Suponha que S é um sistema de reduções sobre a álgebra livre $k \langle X \rangle$ e \leq uma ordem parcial de semigrupo sobre $\langle X \rangle$ compatível com S . Seja*

$$(\sigma, \tau, A, B, C) \quad (3-9)$$

uma ambiguidade de sobreposição (respectivamente uma ambiguidade de inclusão) de S e suponha

$$f_1 + \dots + f_n = 0 \quad (3-10)$$

é uma equação em $k \langle X \rangle$, tal que somente dois de seus termos, digamos f_i e f_j , envolvem o monômio ABC com coeficiente não nulo, e neles seus coeficientes são unidades de k . Então a ambiguidade (3-9) é resolúvel relativo a \leq se, e somente se

$$f_1 + \dots + r_{1\sigma C}(f_i) + \dots + r_{A\tau 1}(f_j) + \dots + f_n \in I_{ABC}. \quad (3-11)$$

(ou uma fórmula análoga no caso de uma ambiguidade de inclusão).

Demonstração. Segue-se diretamente do Teorema 3.12. \square

Uma advertência na aplicação do Lema acima é certificar-se de que não só reduções subsequentes, mas também reduções realizadas "junto com" o anterior, só afetam monômios $\langle ABC \rangle$, sob a nossa ordem parcial. Quando resumimos os cálculos acima, no próximo corolário, esta advertência toma a forma das hipóteses $zyx > yxz$, $zyx > xzy$, $zyx > xzy$.

Corolário 3.15 *Suponha que x, y, z são elementos de X , tais que $zyx > yxz$ e $zyx > xzy$ sob a nossa ordem parcial, e suponha que S contém as reduções*

$$\sigma = (zy, yz - a), \quad \tau = (yx, xy - b),$$

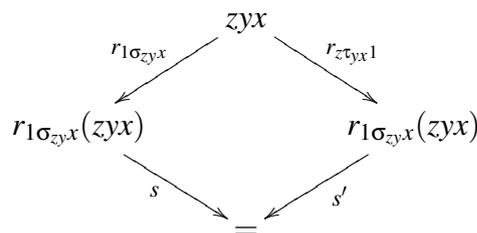
para $a, b \in k \langle X \rangle$. Então a ambiguidade (σ, τ, z, y, x) é resolúvel relativo a \leq se, e somente se, nosso sistema de reduções respeita a identidade de Jacobi

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$$

no sentido de que

$$[x, a] + [y, [z, x]] + [z, b] \in I_{zyx}.$$

Demonstração. Temos o diamante que mostra o processo de redução



onde s e s' são composições de reduções.

Para estudar a ambiguidade (σ, τ, z, y, x) relativa a \leq devemos estudar o elemento zyx .

$$\begin{aligned} r_{1\sigma_{zy}x}(zyx) - r_{1\sigma_{zy}x}(zyx) &= (yz - a)x - z(xy - b) \\ &= (yzx - ax) - (zxy - zb). \end{aligned}$$

Como

$$[x, [y, z]] = xyz - xzy - yzx + zyx,$$

para reduzir mais o termo xzy , aplicamos $r_{x\sigma_{zy}1}$. Similarmente, para reduzir zyx , aplicamos $r_{1\sigma_{zy}x}$. De modo que obtemos

$$\begin{aligned} xyz - x(yz - a) - yzx + (yz - a)x \\ = xyz - xyz + xa - yzx + yzx - ax \\ = xa - ax = [x, a]. \end{aligned}$$

Analogamente,

$$[y, [z, x]] = yzx - yxz - zxy + xzy.$$

Reduzimos o termo yxz , aplicando $r_{1\tau_{yxz}}$. Similarmente, para reduzir xzy , aplicamos $r_{x\sigma_{zy}1}$. Assim

$$\begin{aligned} yzx - (xy - b)y - zxy + x(yz - a) \\ = yzx - xyz + by - zxy + xyz - xa \\ = (bz - zxy) + (yzx - xa). \end{aligned}$$

Da mesma maneira,

$$[z, [x, y]] = zxy - zyx - xyz + yxz$$

para reduzir a expressão zyx , aplicamos $r_{z\tau_{yx}1}$, e para yxz , aplicamos $r_{1\tau_{yxz}}$. De modo que obtemos

$$\begin{aligned} zxy - z(xy - b) - xyz + (xy - b)z \\ = zxy - zxy + zb - xyz + xyz - bz \\ = zb - bz = [z, b]. \end{aligned}$$

Portanto,

$$\begin{aligned} [x, [y, z]] + [y, [z, x]] + [z, [x, y]] &= [x, a] + [y, [z, x]] + [z, b] \\ = (xa - ax) + (bz - zxy) + (yzx - xa) + (zb - bz) &= (yzx - ax) - (zxy - zb) \\ = r_{1\sigma_{zy}x}(zyx) - r_{1\sigma_{zy}x}(zyx), \end{aligned}$$

isto é,

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = r_{1\sigma_{zyx}}(zyx) - r_{1\sigma_{zyx}}(zyx).$$

Do Lema 3.14, a ambiguidade (σ, τ, z, y, x) é resolúvel relativa a \leq se, e somente se

$$\begin{aligned} r_{1\sigma_{zyx}}(zyx) - r_{1\sigma_{zyx}}(zyx) &\in I_{zyx}, \text{ isto é,} \\ r_{1\sigma_{zyx}}(zyx) &= r_{1\sigma_{zyx}}(zyx) \pmod{I_{zyx}}. \end{aligned}$$

Obtemos então

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0 \pmod{I_{zyx}}$$

no sentido de que

$$[x, a] + [y, [z, x]] + [z, b] \in I_{zyx}.$$

□

Lembremos que para um elemento x de uma álgebra associativa R , $adx : R_L \rightarrow R_L$ é definida pela aplicação $y \mapsto [x, y] = xy - yx$.

Corolário 3.16 *Suponha que $\text{car}(k) = p > 0$, isto é, que k é uma \mathbb{Z}_p -álgebra comutativa. Suponha que x, y são elementos de X tais que $yx > xy$ (respectivamente $xy > yx$) e suponha que S contém os elementos*

$$\sigma = (yx, xy - a) \text{ (resp. } (xy, yx + a)), \tau = (x^p, b).$$

Então a ambiguidade $(\sigma, \tau, y, x, x^{p-1})$ (resp. $(\tau, \sigma, x^{p-1}, x, y)$) é resolúvel relativa a \leq se, e somente se, nosso sistema de redução respeita a identidade

$$(adx)^p(y) = (adx^p)(y)$$

com

$$(adx)^{p-1}(a) - (adb)(y) \in I_{yx^p} \text{ (resp. } I_{x^p y}).$$

Demonstração. Temos o diamante que mostra o processo de redução

$$\begin{array}{ccc} & yx^p & \\ r_{1\sigma_{yx,x^{p-1}}} \swarrow & & \searrow r_{y\tau,x^{p-1}} \\ r_{1\sigma_{yx,x^{p-1}}}(yx^p) & & r_{y\tau,x^{p-1}}(yx^p) \\ & \searrow s & \swarrow s' \\ & = & \end{array}$$

onde s e s' são composições de reduções.

Para estudar a ambiguidade $(\sigma, \tau, y, x, x^{p-1})$ relativa a \leq devemos estudar o elemento yx^p ,

$$\begin{aligned}
& r_{1\sigma_{yx}x^{p-1}}(yx^p) - r_{y\tau_{xp}1}(yx^p) \\
&= r_{1\sigma_{yx}x^{p-1}}(yxx^{p-1}) - r_{y\tau_{xp}1}(yx^p) \\
&= (xy - a)x^{p-1} - yb.
\end{aligned}$$

Mas

$$(adx)^p(y) = \sum_{i=0}^p (-1)^i \binom{p}{i} x^{p-i} y x^i = x^p y - y x^p \quad (\text{pois } \text{car}(k) = p).$$

Então para reduzir mais o termo yx^p , aplicamos $r_{1\sigma_{yx}x^{p-1}}$. Similarmente, para reduzir $x^p y$, aplicamos $r_{y\tau_{xp}1}$. De modo que

$$by - (xy - a)x^{p-1}.$$

Da mesma maneira,

$$\begin{aligned}
(adx^p)(y) &= [x^p, y] \\
&= x^p y - y x^p.
\end{aligned}$$

Reduzimos o termo $x^p y$, aplicando $r_{y\tau_{xp}1}$. Da mesma forma, para reduzir yx^p , aplicamos $r_{1\sigma_{yx}x^{p-1}}$. Assim,

$$by - yb = [b, y].$$

Por outro lado,

$$\begin{aligned}
(adx^p)(y) - (adx)^p(y) &= [x^p, y] - (adx)^{p-1}([x, y]) \\
&= x^p y - y x^p - \sum_{i=0}^{p-1} (-1)^i \binom{p-1}{i} x^{(p-1)-i} (xy - yx) x^i.
\end{aligned}$$

Para reduzir $x^p y$ e yx^p usamos as reduções $r_{y\tau_{xp}1}$ e $r_{1\sigma_{yx}x^{p-1}}$. Similarmente, para reduzir a expressão yx , aplicamos $r_{1\sigma_{yx}}$. Então

$$\begin{aligned}
by - yb - \sum_{i=0}^{p-1} (-1)^i \binom{p-1}{i} x^{(p-1)-i} a x^i \\
= [b, y] - (adx)^{p-1}(a) = (adb)(y) - (adx)^{p-1}(a).
\end{aligned}$$

Portanto,

$$\begin{aligned}
(adb)(y) - (adx)^{p-1}(a) &= (adx^p)(y) - (adx)^p(y) = (by - yb) - (by - (xy - a)x^{p-1}) \\
&= (xy - a)x^{p-1} - yb = r_{y\tau_{xp}1}(yx^p) - r_{1\sigma_{yx}x^{p-1}}(yx^p).
\end{aligned}$$

Do Lema 3.14, a ambiguidade $(\sigma, \tau, y, x, x^{p-1})$ é resolúvel relativa a \leq se, e somente se

$$r_{y\tau_{xp}1}(yx^p) - r_{1\sigma_{yx}x^{p-1}}(yx^p) \in I_{yx^p},$$

isto é,

$$r_{y\tau_x^p 1}(yx^p) = r_{1\sigma_{yx}x^{p-1}}(yx^p) \bmod I_{yx^p}.$$

Assim

$$(adx)^p(y) = (adx^p)(y) \bmod I_{yx^p}$$

no sentido que

$$(adx)^{p-1}(a) - (adb)(y) \in I_{yx^p}$$

□

Corolário 3.17 *Suponha que x é um elemento de X e n um inteiro positivo tal que S contém o elemento*

$$\sigma = (x^n, a).$$

Então todas as ambiguidades $(\sigma, \sigma, x^i, x^{n-i}, x^i)$ são resolúveis relativas a \leq se, e somente se, nosso sistema de redução respeita a identidade

$$[x^n, x] = 0$$

significando

$$[a, x] \in I_{x^{n+1}}.$$

Demonstração. Temos o diamante que mostra o processo de redução

$$\begin{array}{ccc}
 & x^{n+1} & \\
 r_{1\sigma_{yx}x} \swarrow & & \searrow r_{x\sigma_{xn}1} \\
 r_{1\sigma_{xn}x}(x^{n+1}) & & r_{x\sigma_{xn}1}(x^{n+1}) \\
 s \searrow & & \swarrow s' \\
 & = &
 \end{array}$$

onde s e s' são composições de reduções.

Para estudar a ambiguidade $(\sigma, \sigma, x^i, x^{n-i}, x^i)$ relativa a \leq devemos estudar o elemento x^{n+1} ,

$$\begin{aligned}
 r_{1\sigma_{yx}x}(x^{n+1}) - r_{x\sigma_{xn}1}(x^{n+1}) &= r_{1\sigma_{yx}x}(x^n x) - r_{x\sigma_{xn}1}(x x^n) \\
 &= ax - xa \\
 &= [a, x].
 \end{aligned}$$

Pela definição do colchete de Lie,

$$[x^n, x] = x^n x - x x^n.$$

Para reduzir a expressão $x^n x$, aplicamos $r_{1\sigma_{x^n}x}$. Similarmente, para reduzir $x x^n$, aplicamos $r_{x\sigma_{x^n}1}$. De modo que

$$ax - xa = [a, x].$$

Portanto,

$$[x^n, x] = [a, x] = r_{1\sigma_{x^n}x}(x^{n+1}) - r_{x\sigma_{x^n}1}(x^{n+1}).$$

Do Lema 3.14, a ambiguidade $(\sigma, \sigma, x^i, x^{n-i}, x^i)$ é resolúvel relativa a \leq se, e somente se

$$r_{1\sigma_{x^n}x}(x^{n+1}) - r_{x\sigma_{x^n}1}(x^{n+1}) \in I_{x^{n+1}},$$

isto é,

$$r_{1\sigma_{x^n}x}(x^{n+1}) = r_{x\sigma_{x^n}1}(x^{n+1}) \pmod{I_{x^{n+1}}}.$$

Segue que

$$[x^n, x] = 0 \pmod{I_{x^{n+1}}}$$

ou seja,

$$[a, x] \in I_{x^{n+1}}.$$

□

Podemos agora estabelecer o resultado análogo ao Teorema de Poincaré-Birkhoff-Witt, para álgebras de Lie de característica p .

Exemplo 3.18 *Demonstrar o análogo do Teorema de Poincaré-Birkhoff-Witt para álgebras de Lie de característica p [7; Cap 5, lema 4].*

No seguinte Corolário, as famílias de elementos $((x_{gh}), \dots, ((v_{hj}))$ devem ser olhadas como as entradas das matrizes x, y, z, u, v .

Corolário 3.19 *Suponha que p, m, n, q são inteiros positivos, e que X contém os elementos x_{gh}, y_{hi}, z_{ij} ($g \leq p, h \leq m, i \leq n, j \leq q$). Suponha que $u \leq m$ é um inteiro positivo tal que $x_{gu}y_{ui} > x_{gh}y_{hi}$ para todo $h \neq u$, e $v \leq n$ um inteiro positivo tal que $y_{hv}z_{vj} > y_{hi}z_{ij}$ para todo $i \neq v$, e que S contém as reduções*

$$\sigma_{gi} = \{x_{gu}y_{ui}, -\sum_{h \neq u} x_{gh}y_{hi} + u_{gi}\} \quad (g \leq p, i \leq n),$$

$$\tau_{hj} = \{y_{hv}z_{vj}, -\sum_{i \neq v} y_{hi}z_{ij} + v_{hj}\} \quad (h \leq m, j \leq q).$$

onde $u_{gi}, v_{hj} \in k \langle X \rangle$. (Esse sistema de reduções apresenta relações matriciais $xy = u$, $yz = v$, com a u -ésima, respectivamente a v -ésima entrada do produto de matrizes tomadas como a palavra a ser reduzida.)

Então as pq ambiguidades $(\sigma_{gv}, \tau_{uj}, x_{gu}, y_{uv}, z_{vj})$ ($g \leq p, j \leq q$) são resolúveis relativas a \leq se, e somente se, o sistema de reduções S respeita a identidade da associatividade para a multiplicação de matrizes

$$(xy)z = x(yz),$$

isto é

$$uz - xv \in ((I_{x_{gu}y_{uv}z_{vj}})).$$

Demonstração. A demonstração é análoga às provas dos Corolários acima. □

Observação 3.20 Se no Lema 3.14 adicionamos as hipóteses de que todos os monômios $\langle ABC$ são de redução única, então as hipóteses de que os dois coeficientes não nulos de ABC em (3.10) sejam unidades podem ser enfraquecidas para não sejam divisores de zero em k . Quando todos os monômios $\langle ABC$ são de redução única, I_{ABC} pode ser caracterizada como o $\text{Ker}(r_S | \text{Span dos monômios } \langle ABC)$. Assim se escrevemos $-\alpha$ e $-\alpha$ para os dois coeficientes de ABC em (3.10), então (3.11), implica que $\alpha(f_\sigma C - Af_\tau) \in I_{ABC}$, de onde $\alpha r_S(f_\sigma C - Af_\tau) = 0$. Então $r_S(f_\sigma C - Af_\tau) = 0$, e a ambiguidade dada é resolúvel.

A Álgebra P_n

Seja $p(x) = x^n - a_{n-1}x^{n-1} + a_{n-2}x^{n-2} - \dots + (-1)^n a_0$ um polinômio com coeficientes em uma álgebra de divisão. Gelfand e Retakh, [4], estudaram as relações entre os coeficientes a_i e um conjunto genérico $\{x_1, \dots, x_n\}$ de soluções de $p(x) = 0$. Para qualquer ordenação (i_1, \dots, i_n) de $\{1, \dots, n\}$ podemos construir pseudo-raízes y_k , $k \in [n] = \{1, \dots, n\}$, (certas funções racionais em x_{i_1}, \dots, x_{i_n}) que dão uma decomposição

$$p(t) = (t - y_n) \cdots (t - y_2)(t - y_1),$$

onde t é uma variável central.

Exemplo 4.1 *A álgebra Q_2 . Seja R um anel associativo com elemento identidade 1 e $P(t) = t^2 + a_1t + a_2$, onde t é uma variável central, com raízes x_1 e x_2 de modo que a diferença $x_1 - x_2$ é invertível em R . Então*

$$\begin{aligned} x_1^2 + a_1x_1 + a_2 &= 0 \\ x_2^2 + a_1x_2 + a_2 &= 0, \end{aligned}$$

de onde obtemos

$$x_1^2 - x_2^2 + a_1(x_1 - x_2) = 0.$$

Somando e subtraindo x_1x_2 , temos

$$x_1(x_1 - x_2) + (x_1 - x_2)x_2 + a_1(x_1 - x_2) = 0.$$

Multiplicando por $(x_1 - x_2)^{-1}$,

$$x_1 + (x_1 - x_2)x_2(x_1 - x_2)^{-1} + a_1 = 0,$$

o que implica

$$a_1 = -x_1 - x_1x_2, \quad x_1x_2 = (x_1 - x_2)x_2(x_1 - x_2)^{-1}.$$

Daí, $x_1^2 + (-x_1 - x_1x_2)x_1 + a_2 = 0$ e $x_1^2 - x_1^2 - x_1x_2x_1 + a_2 = 0$. Assim,

$$a_2 = x_1x_2x_1.$$

Portanto, $P(t) = t^2 + (-x_1 - x_{12})t + x_{12}x_1$,

$$\begin{aligned} P(t) &= t^2 - x_1t - x_{12}t + x_{12}x_1 \\ &= (t - x_1)t - x_{12}(t - x_1) \\ &= t(t - x_1) - x_{12}(t - x_1) = (t - x_{12})(t - x_1). \end{aligned}$$

Assim,

$$P(t) = (t - x_{12})(t - x_1).$$

Se por outro lado, fizermos

$$x_2^2 - x_1^2 + a_1(x_2 - x_1) = 0,$$

obtemos

$$x_2(x_2 - x_1) + (x_2 - x_1)x_1 + a_1(x_2 - x_1) = 0.$$

Então,

$$a_1 = -x_2 - x_{21}, \quad x_{21} = (x_2 - x_1)x_1(x_2 - x_1)^{-1}.$$

Daí, $a_2 = x_{21}x_2$. Portanto

$$P(t) = (t - x_{21})(t - x_2).$$

Então a igualdade

$$(t - x_{12})(t - x_1) = (t - x_{21})(t - x_2),$$

fornece as relações

$$\begin{aligned} x_{12} + x_1 &= x_{21} + x_2 \\ x_{12}x_1 &= x_{21}x_2 \end{aligned}$$

Gelfand et al., [3], introduziram a álgebra Q_n de todas as pseudo-raízes de um polinômio genérico não comutativo, determinaram uma base para essa álgebra e encontraram muitas apresentações dessas álgebras incluindo a seguinte:

Teorema 4.2 *As álgebras Q_n têm uma apresentação por geradores $u(A)$, $\emptyset \neq A \subseteq [n] = \{1, 2, \dots, n\}$ e relações*

$$\sum_{C, D \subseteq A} [u(C \cup i), u(D \cup j)] = \left(\sum_{E \subseteq A} u(E \cup i \cup j) \right) \sum_{F \subseteq A} (u(F \cup i) - u(F \cup j)),$$

para todo $A \subseteq [n]$, $i, j \in [n] \setminus A$, $i \neq j$.

Algumas vezes escrevemos $u(i)$ para $u(\{i\})$ e $u(i, j)$ para $u(\{i, j\})$ com $i \neq j \in [n]$.

Exemplo 4.3 Quando $n = 2$, a restrição $A \subseteq [n]$ e $i, j \in [n] \setminus A$ implicam $A = \emptyset$. Portanto Q_2 têm uma apresentação dada pelos geradores $u(1)$, $u(2)$ e $u(1,2)$, e a única relação

$$[u(1), u(2)] = u(1,2)(u(1) - u(2)).$$

Gelfand et al.,[3] estudaram uma classe de álgebras de quocientes de Q_n correspondentes a grafos de n vértices. Seja G um grafo com o conjunto de vértices $[n] = \{1, 2, \dots, n\}$ e um conjunto de arestas E que são elementos de $P([n])$ com cardinalidade 2 (portanto G não tem laços ou arestas múltiplas). Então podemos considerar a álgebra quociente $Q_n(G)$ obtida pelo acréscimo de relações adicionais $u(\{i, j\}) = 0$ se $\{i, j\} \notin E$ para Q_n . O seguinte teorema dá uma apresentação da álgebra $Q_n(G)$.

Teorema 4.4 Seja G um grafo com n vértices e conjunto de arestas E . Então a álgebra $Q_n(G)$ é gerada pelos elementos $u(i)$, $i \in [n]$ e $u(i, j)$, $\{i, j\} \in E$, com as seguintes relações (supondo $u(i, j) = 0$ se $\{i, j\} \notin E$):

- (i) $[u(i), u(j)] = u(i, j)(u(i) - u(j))$, $i \neq j$ e $i, j \in [n]$;
- (ii) $[u(i, k), u(j, k)] + [u(i, k), u(j)] + [u(i), u(j, k)] = u(i, j)(u(i, k) - u(j, k))$, para distintos $i, j, k \in [n]$;
- (iii) $[u(i, j), u(k, l)] = 0$, para distintos $i, j, k, l \in [n]$.

Demonstração. Veja [3], pág. 5. □

Exemplo 4.5 Se G é um grafo com n vértices e nenhuma aresta, então obtemos somente relações da forma

$$0 = [u(i), u(j)] = u(i)u(j) - u(j)u(i) \text{ (pois } u(i, j) = 0 \text{ para todo } \{i, j\} \notin E).$$

$Q_n(G)$ é isomorfo à álgebra dos polinômios comutativos em n variáveis.

Exemplo 4.6 A álgebra $Q_n(G)$ correspondente ao grafo



é apresentada pelos geradores v_1 , v_2 e $e_{1,2}$, e uma única relação

$$[v_1, v_2] + e_{1,2}(v_2 - v_1) = 0.$$

Nos referimos aos elementos $u(i)$, $i \in [n]$ como vértices e $u(i, j)$, $\{i, j\} \in E$, como arestas. Também identificamos os vértices do grafo com os correspondentes geradores da álgebra. Algumas vezes nos referiremos à álgebra $Q_n(G)$ para um grafo específico G , como a álgebra G . Usando essa terminologia, a seguinte proposição é imediata de (i) e (iii).

Proposição 4.7 *Os vértices de G comutam se, e somente se, eles não estão conectados por uma aresta. Arestas não adjacentes em G comutam.*

É difícil achar uma maneira de reduzir a relação (ii). Para isso, fixemos distintos $i, j, k \in [n]$. Sejam $V = \text{Span}\{u(i), u(j), u(k), u(i, j), u(j, k), u(i, k)\}$ e $v_{i,j,k} = [u(i, k), u(j, k)] + [u(i, k), u(j)] + [u(i), u(j, k)] - u(i, j)(u(i, k) - u(j, k))$. Considere a ação natural de S_3 sobre $T(V)$ definindo

$$\sigma u(i) = u(\sigma(i)) \text{ e } \sigma u(i, j) = u(\sigma(i), \sigma(j))$$

e estendendo linearmente.

Proposição 4.8 *A órbita de $v_{i,j,k}$ sobre a ação de S_3 gera um espaço de dimensão 2 em $T(V)$.*

Demonstração. Consideremos as transposições

$$\mu = \begin{pmatrix} i & j & k \\ j & i & k \end{pmatrix} \text{ e } \tau = \begin{pmatrix} i & j & k \\ k & j & i \end{pmatrix}.$$

Como estas permutações geram S_3 , será suficiente mostrar que a ação de τ e μ leva o Span de $v_{i,j,k}$ e $v_{k,j,i}$ sobre ele mesmo. Como esse espaço é claramente fixado por τ , precisamos só considerar μ . Como μ leva a $v_{i,j,k}$ sobre $-v_{i,j,k}$ e $v_{k,j,i}$ sobre $v_{k,j,i} - v_{i,j,k}$, obtemos o resultado. □

Dizemos que G é um **triângulo livre** se $\{i, j\}, \{j, k\} \in E$ implica que $\{i, k\} \notin E$ para qualquer $i, j, k \in [n]$. Neste caso a relação (ii) é reduzida um pouco mais.

Proposição 4.9 *Se G é um grafo triangular livre. Então (ii) é equivalente a*

(ii') *$u(i)$ comuta com $u(j, k)$ quando $\{i, j\}, \{i, k\} \notin E$ e*

(ii'') *$[u(i), u(j, k)] + u(i, j)u(j, k) = [u(k), u(i, j)] + u(j, k)u(i, j) = 0$ quando $\{i, j\}, \{j, k\} \in E$, $\{i, k\} \notin E$ para distintos $i, j, k \in [n]$.*

Demonstração. Sabemos da Proposição 4.8 acima que podemos substituir a relação (ii) por $v_{i,j,k}$ e $v_{k,j,i}$. Na situação em que $\{i, j\}, \{i, k\} \notin E$, $v_{i,j,k}$, vem a ser $[u(i), u(i, k)]$ e $v_{k,j,i}$ torna-se ser zero pois $u(i, j)$ e $u(i, k)$ são zero. Isto nos dá a relação (ii').

Em (ii'), $u(i, k) = 0$, assim, $v_{i,j,k} = [u(i), u(j, k)] + u(i, j)u(j, k)$ e $v_{k,j,i} = [u(k), u(i, j)] + u(j, k)u(i, j)$. \square

Vamos especializar para um particular grafo triangular livre, o grafo P_n de n vértices. Este grafo tem vértices $[n]$ e arestas $\{k, k+1\}$ para $k \in [n-1]$.



Referiremos aos elementos da álgebra P_n , usando v_i para $u(i)$ e e_{ij} para $u(i, j)$. Aplicando os fatos sobre as relações (i), (ii) e (iii) obtemos.

Proposição 4.10 *A álgebra P_n gerada pelo grafo P_n é apresentada pelos geradores $v_1, v_2, \dots, v_n, e_{12}, e_{23}, \dots, e_{(n-1)n}$ e relações*

$$[v_i, v_j] = 0 \text{ para } i > j, i, j \in [n],$$

$$[v_i, v_{i+1}] + e_{i,i+1}(v_{i+1} - v_i) = 0 \text{ para } i \in [n-1],$$

$$[e_{i,i+1}, e_{j,j+1}] = 0 \text{ para } j > i+1, i, j \in [n-1],$$

$$[v_i, e_{j,j+1}] = 0 \text{ se } j > i+1 \text{ ou } j < i-2, j \in [n-1], i \in [n],$$

$$[v_i, e_{i+1,i+2}] + e_{i,i+1}e_{i+1,i+2} = 0 \text{ para } i \in [n-2],$$

$$[v_{i+2}, e_{i,i+1}] + e_{i+1,i+2}e_{i,i+1} = 0 \text{ para } i \in [n-2].$$

4.1 As Álgebras $ch(P_n)$

Seja V o *Span* dos geradores de P_n . Definimos uma filtração de $T(V)$.

Proposição 4.11 *Tomemos $G^{(0)} = k$. Então definindo*

$$G^{(i)} = \text{Span}\{u(A_1)u(A_2)\cdots u(A_s) \mid \sum_{l=1}^s (3 - |A_l|) \leq i\}$$

para $i \geq 1$ temos uma filtração de $T(V)$.

Demonstração. Para mostrar que $i \leq j$ implica $G^{(i)} \subseteq G^{(j)}$ observe que, se $\sum_{l=1}^s (3 - |A_l|) \leq i$ então $\sum_{l=1}^s (3 - |A_l|) \leq j$. Para mostrar $\bigcup G^{(i)} = T(V)$ observe que cada monômio $u(A_1)u(A_2)\cdots u(A_s)$ em $T(V)$ está em $G^{(i)}$ para $i = \sum_{l=1}^s (3 - |A_l|)$. Finalmente, para mostrar que

$$G^{(i)}G^{(j)} \subseteq G^{(i+j)}$$

mostraremos que o produto de um monômio em $G^{(i)}$ e um monômio em $G^{(j)}$ está contido em G^{i+j} e então estendemos linearmente. Suponha que

$$u(u(A_1)u(A_2)\dots u(A_s)) \in G^{(i)} \quad \text{e}$$

$$u(B_1)u(A_2)\dots u(B_j) \in G^{(j)}.$$

Então o produto destes dois monômios é

$$u(A_1)u(A_2)\dots u(A_s)u(A_{s+1})u(A_{s+2})\dots u(A_{s+j})$$

onde $A_{s+i} = B_i$. Então $\sum_{l=1}^{s+j} (3 - |A_l|) = (\sum_{l=1}^s (3 - |A_l|)) + (\sum_{l=1}^j (3 - |B_l|)) \leq i + j \quad \square$

Exemplo 4.12 Com esta filtração, $G^{(1)}$ é o espaço de todos os $u(i, j)$, desde que $(3 - |\{i, j\}|) = 1$, e assim o monômio só pode ter comprimento 1. Como $u(i)$ teve $(3 - |\{i\}|) = 2$ obtemos que $G^{(2)}$ contém todas as combinações de monômios das formas $u(i)$, $u(i, j)$ e $u(i, j)u(k, l)$.

Esta filtração de $T(V)$ induz uma filtração na álgebra P_n e, portanto, podemos considerar a álgebra graduada associada $G(P_n)$. Se eliminarmos os termos não comutativos nas relações dadas na Proposição 4.10, essas relações serão todas verdadeiras em $G(P_n)$. Consideramos a álgebra dada por essas relações eliminadas, que chamamos $ch(P_n)$.

Definição 4.13 A álgebra $ch(P_n)$ é apresentada pelos geradores $v_1, v_2, \dots, v_n, e_{12}, e_{23}, \dots, e_{(n-1)n}$ e relações

$$[v_i, v_j] = 0 \quad \text{para } j > i + 1, i, j \in [n],$$

$$[v_i, v_j] = 0 \quad \text{para } i \in [n - 1],$$

$$[e_{i,i+1}, e_{j,j+1}] = 0 \quad \text{para } j > i + 1, i, j \in [n - 1],$$

$$[v_i, e_{j,j+1}] = 0 \quad \text{se } j > i + 1 \text{ ou } j < i - 2, j \in [n - 1], i \in [n],$$

$$[v_i, e_{i+1,i+2}] = 0 \quad \text{para } i \in [n - 2],$$

$$[v_{i+2}, e_{i,i+1}] = 0 \quad \text{para } i \in [n - 2].$$

Nossa intenção é usar o Teorema 3.10 para encontrar uma base PBW para $ch(P_n)$. Antes de aplicar o Lema do Diamante de Bergman a $ch(P_n)$, devemos provar alguns resultados mais gerais sobre álgebras, cujas relações são comutadores de geradores.

4.2 PGC-Álgebras

Definição 4.14 *Suponha que uma álgebra A tem uma apresentação pelos geradores $\{a_1, a_2, \dots, a_n\}$ e um conjunto de relações S , onde cada relação em S é da forma $[a_i, a_j] = 0$ para $i, j \in [n]$. Então, dizemos que A é uma PGC-álgebra.*

Se A é uma PGC-álgebra sobre n geradores, então para um ideal I em A , $A/I = S_n$ é a álgebra comutativa livre sobre n geradores. No entanto, nem todas as álgebras são PGC como mostra o exemplo seguinte.

Exemplo 4.15 *A álgebra A apresentada pelos geradores a, b e a relação $[ab, a] = 0$ não é PGC.*

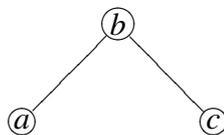
Exemplo 4.16 *A álgebra A apresentada pelos geradores a, b, c e a relação $[a, b] = 0$ é PGC.*

Exemplo 4.17 *Tanto a álgebra comutativa e a álgebra livre sobre n geradores são PGC.*

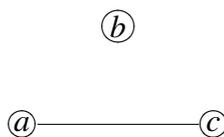
A estrutura de uma PGC-álgebra está inteiramente baseada sobre os pares de geradores que comutam. Podemos então descrever essa álgebra usando um grafo onde cada vértice é um gerador e existe uma aresta entre dois vértices se os geradores comutam.

Definição 4.18 *Seja A uma PGC-álgebra sobre os geradores $\{a_1, a_2, \dots, a_n\}$. O grafo comutador $G_C(A)$ de A é o grafo com vértices $\{a_1, a_2, \dots, a_n\}$ e arestas dadas pela regra, e_{a_i, a_j} é uma aresta se, e somente se $[a_i, a_j] = 0$. Muitas vezes também consideramos o complemento deste grafo, $\overline{G_C(A)}$, chamado o grafo não comutador de A onde existe uma aresta entre dois geradores somente quando eles não comutarem.*

Exemplo 4.19 *Um exemplo simples de uma PGC-álgebra é a álgebra apresentada pelos geradores $\{a, b, c\}$ e as relações $ab - ba = bc - cb = 0$. O grafo $G_C(A)$ é mostrado aqui:*



O grafo não comutador $\overline{G_C(A)}$ é



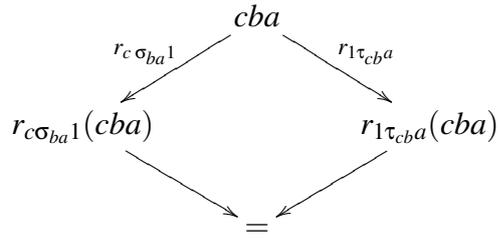
O Teorema 3.10 dá um método para determinar uma base para tal álgebra. Se, no exemplo acima, escolhermos um monômio ordenado primeiro pelo comprimento e depois lexicograficamente com $c > b > a$ obtemos as seguintes reduções:

$$\begin{aligned} cb &\longmapsto bc \\ ba &\longmapsto ab, \end{aligned}$$

isto é; as reduções

$$\sigma = (ba, ab) \text{ e } \tau = (cb, bc)$$

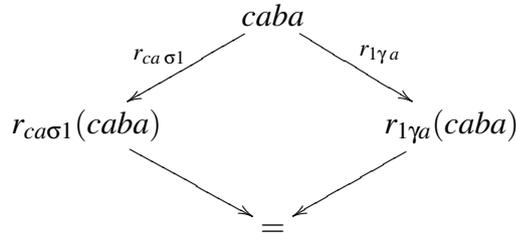
Isso dá uma ambiguidade, ou seja cba , que devemos resolver.



de onde

$$\begin{aligned} r_{c\sigma_{ba}1}(cba) &= r_{1\tau_{cba}}(cba) \\ r_{c\sigma_{ba}1}(c(ba)) &= r_{1\tau_{cba}}((cb)a) \\ cab &= bca. \end{aligned}$$

que dá a nova redução $\gamma = (cab, bca)$ e uma nova ambiguidade para resolver, $caba$.



logo

$$\begin{aligned} r_{ca\sigma 1}(caba) &= r_{1\gamma a}(caba) \\ r_{ca\sigma 1}(ca(ba)) &= r_{1\gamma a}((cab)a) \\ caab &= bcaa \end{aligned}$$

que dá a nova redução $(caab, bcaa)$ e a nova ambiguidade $caaba$.

Podemos mostrar indutivamente pela adjunção das reduções $(caa\dots ab, bcaa\dots a)$ que todas as ambiguidades são resolúveis, e eliminamos a seguinte lista de palavras: $cb, ba, cab, caab, caaab, caa\dots ab, \dots$. Uma base para a álgebra consiste no conjunto de todos os monômios que não contenham uma dessas palavras. Esta base não é PBW pois nossas ambiguidades de relações de grau 2 não foram resolúveis (sem a adição de relações de maior grau).

Exemplo 4.20 *Vamos olhar a mesma álgebra aplicando o Lema do Diamante de Bergman com uma ordenação monomial diferente. Primeiro vamos ordenar pelo comprimento e depois lexicograficamente com $b > a > c$. De modo que obtemos as reduções:*

$$ba \longmapsto ab$$

$$bc \longmapsto cb.$$

Elas não têm ambiguidades, e uma base para a álgebra consiste de todos os monômios que não contêm ba ou bc . Esta base é PBW pois todas as ambiguidades são resolúveis.

Estamos interessados nos casos em que todas as ambiguidades de grau 3 sejam resolúveis, para obter uma base PBW. Para nos ajudar a continuar na busca de tais exemplos vamos precisar a seguinte definição.

Definição 4.21 *Se G é um grafo com n vértices, então uma **ordenação de vértices** de G é uma aplicação sobrejetiva dos vértices de G sobre $[n]$.*

Proposição 4.22 *Seja A uma PGC-álgebra com grafo comutador $G_C(A)$. Suponha que existe uma ordenação de vértices de $G_C(A)$. Assim, para quaisquer três vértices a, b e c se $\{a, c\} \notin E$, $\{a, b\}, \{b, c\} \in E$, assim nem $a < b < c$ ou $c < b < a$ acontece. Então existe uma ordem monomial tal que todas as ambiguidades de grau 3 são resolúveis com o Lema do Diamante de Bergman e portanto a álgebra tem uma base PBW.*

Proposição 4.23 *Seja A uma PGC-álgebra com grafo não comutador $\overline{G_C(A)}$. Suponha que existe uma ordenação de vértices de $\overline{G_C(A)}$. Assim, para quaisquer três vértices a, b e c se $\{a, c\} \in E$, $\{a, b\}, \{b, c\} \notin E$, assim nem $a < b < c$ ou $c < b < a$ acontece. Então existe uma ordem monomial tal que todas as ambiguidades de grau 3 são resolúveis com o Lema do Diamante de Bergman e portanto a álgebra tem uma base PBW.*

Demonstração. Como as duas afirmações são equivalentes, provaremos somente a primeira. Ordenamos os monômios primeiro pelo comprimento e depois estendendo lexicograficamente a ordenação dos vértices. É suficiente mostrar que, dados três vértices distintos a, b e c , todas as ambiguidades que envolvem os geradores se resolvem. Primeiro observe que, se nenhum dos geradores a, b e c comutam uns com os outros, então não pode haver ambiguidade. O mesmo vale se houver apenas um par que comuta.

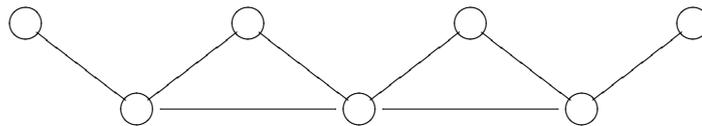
Se os três comutam uns com os outros, então temos uma ambiguidade que pode ser resolvida.

Finalmente, considere o caso onde $\{a, c\} \notin E$, $\{a, b\}, \{b, c\} \in E$. As únicas ambiguidades que poderiam surgir viriam dos monômios abc ou cba . No entanto, como b não está entre c e a na ordenação, não é possível que ambos cb e ba sejam reduções (e similarmente ab e bc). Portanto, não há ambiguidade a resolver. \square

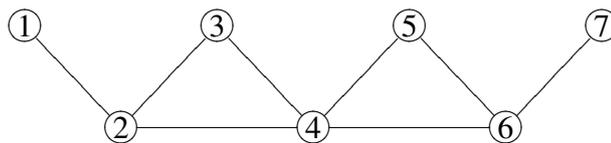
Exemplo 4.24 O grafo P_4 têm 3 arestas e 4 vértices:



A álgebra $ch(P_4)$ é PGC assim, podemos tomar o grafo não comutador. No grafo não comutador de $ch(P_4)$ temos que representar cada gerador com um vértice: isto significa, um vértice para cada vértice em P_4 e um vértice para cada aresta em P_4 . O que temos é (temos conectado geradores que não comutam)



Precisamos renomear o grafo acima de tal maneira que possamos satisfazer os requerimentos da Proposição 4.23. A seguinte designação faz o trabalho:



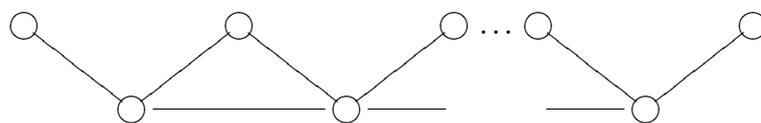
Com este ordenamento dos vértices temos mostrado que todas as ambiguidades da álgebra são resolúveis. Portanto a álgebra $ch(P_4)$ tem uma base PBW.

No entanto, essa técnica pode claramente ser estendida para P_n .

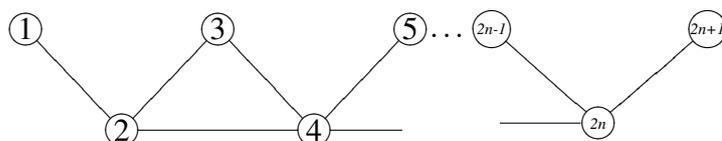
Exemplo 4.25 Do grafo P_n



podemos formar o grafo não comutador:



Usando a Proposição 4.23 e a ordenação mostrada aqui



temos que todas as ambiguidades da álgebra são resolúveis. Portanto a álgebra $ch(P_n)$ tem uma base PBW.

Referências Bibliográficas

- [1] BERGMAN, G. M. **The diamond lemma for ring theory**. *Advances in Mathematics*, 29(2):178–218, 1978.
- [2] BOLLOBÁS, B. **Graph Theory**. Springer-Verlag, New York, 1979.
- [3] GELFAND, I; GELFAND, S; RETAKH, V. **Noncommutative algebras associated to complexes and graphs**. *Selecta Math.(N.S.)*, 7(4):525–531, 2000.
- [4] GELFAND, I; RETAKH, V. **Noncommutative Vieta theorem and symmetric functions**. *Gelfand Math. Sem. Boston: Birkhäuser*, 5(2):93–100, 1996.
- [5] HUMPHREYS, J. E. **Introduction to Lie Algebras and Representation Theory**. Springer-Verlag, New York, 1972.
- [6] HUNGERFORD, T. W. **Algebra**. Springer-Verlag, New York, 1974.
- [7] JACOBSON, N. **Lie Algebras**. Dover Publications, Inc., New York, 1962.
- [8] KNAPP, A. W. **Lie Groups Beyond an Introduction**. Birkhäuser, Boston, 1996.
- [9] NACIN, D. **The algebra P_n is Koszul**. *Communications in Algebra*, 35(8):1291–1306, 2007.
- [10] ROTMAN, J. J. **Advanced Modern Algebra**. Prentice Hall, New York, 2002.