Bases de Gröbner

Peterson Pereira de Oliveira

DISSERTAÇÃO APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO TÍTULO DE MESTRE
EM
MATEMÁTICA

Área de Concentração: **Álgebra**
Orientadora: **Profa. Dra. Gladys Chalom de Oliveira**

Durante a elaboração deste trabalho, o autor recebeu apoio financeiro do CNPq.

São Paulo
2002

BASES DE GRÖBNER

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Peterson Pereira de Oliveira e aprovada pela comissão julgadora.

São Paulo, 17 de setembro de 2002.

Banca Examinadora:

- Profa. Dra. Gladys Chalom de Oliveira (orientadora) (IME-USP)
- Prof. Dr. Eduardo Nascimento Marcos (IME-USP)
- Prof. Dr. Arnaldo Mandel (IME-USP)

Resumo

Neste trabalho, estudamos a Teoria das Bases de Gröbner para álgebras não comutativas. Além disso, vimos que uma $\mathcal{K}$-álgebra com unidade, que possui a teoria das bases de Gröbner, é isomorfa a um quociente de Álgebra de Caminhos. Definimos a álgebra estendida por laços, que é uma generalização para o caso não comutativo do processo de homogeneização. Expomos aqui o resultado principal: *Seja F um subconjunto de uma álgebra de caminhos Λ e seja $\mathcal{G} \subset \Lambda'$ homogêneo, onde Λ' é a álgebra Λ estendida por laços. Se $\mathcal{G}$ é uma base de Gröbner para $\langle F^* \rangle$, então $\mathcal{G}_*$ é uma base de Gröbner para $\langle F \rangle$.*

Abstract

In this work, we study Gröbner Bases Theory to non commutative algebras. Moreover, we see that a $\mathcal{K}$-algebra with unity and with Gröbner bases theory is isomorphic to a quocient of path algebras. We define algebra extended by loops, as a generalization of the homogenization process to non commutative case. Here, we present the main result: *Let F be a subset of the path algebra Λ and let $\mathcal{G} \subset \Lambda'$ be homogeneous, where Λ' is the algebra Λ extended by loops. If $\mathcal{G}$ is a Gröbner basis to $\langle F^* \rangle$, then $\mathcal{G}_*$ is a Gröbner basis to $\langle F \rangle$.*

Aos meus queridos pais,
Elifas e Zilma.

Introdução

Nesse trabalho apresentamos um pouco sobre a teoria das *Bases de Gröbner* apresentadas em [7], [9] e [10], tendo feito um estudo detalhado desses artigos. Como estamos interessados em estudar essa teoria no caso não comutativo, surgiu, em discussão (com o autor de [9] e [10]) a idéia de generalizar o processo de *homogeneização* do caso comutativo (veja [3], cap.10) para o caso não comutativo.

Começamos aqui com a teoria para espaços vetoriais (Capítulo 2) e estendemos esses resultados para $\mathcal{K}$-álgebras, após ter introduzido o conceito de *ordem admissível*. Nos procedimentos *Algoritmo da Divisão* e *Construção de Bases de Gröbner*, ambos para o caso não comutativo, descritos em [9], houve a necessidade de se fazer algumas correções para que fornecessem o resultado esperado.

Ainda no Capítulo 2 (seção 5), temos alguns resultados que mostram em que situações podemos garantir a existência de uma base de Gröbner finita.

Na seção *Por que Álgebras de Caminhos?* (seção 3.1), podemos ver a importância dessas álgebras no estudo das bases de Gröbner (veja [7] e [9]). Nesta seção, temos um dos principais resultados do trabalho: *uma $\mathcal{K}$-álgebra com unidade que possui a teoria de base de Gröbner, ou seja, possui uma $\mathcal{K}$-base multiplicativa com uma ordem admissível nessa base, é isomorfa ao quociente de uma álgebra de caminhos.*

Uma questão que ainda está aberta é: *quais são as condições necessárias*

e suficientes sobre um ideal I, para que o quociente $\mathcal{K}\mathcal{Q}/I$ tenha a teoria de bases de Gröbner?, sabemos apenas que se o ideal for *2-nomial*, isto é, se puder ser gerado por elementos da forma $p, q - r$, com p, q, r pertencentes a $\mathcal{K}$-base de $\mathcal{K}\mathcal{Q}$, então o quociente $\mathcal{K}\mathcal{Q}/I$ possui uma base multiplicativa, o que não implica em ter uma ordem admissível nessa base. Os resultados apresentados até este momento podem ser encontrados em [7], [9] e [10].

Na seção 3.2, temos a generalização dos resultados encontrados em [3] (cap.10) para álgebras de caminhos, $\mathcal{K}\mathcal{Q}/I$.

Sumário

Capítulo 1

Preliminares

Antes de iniciarmos as definições e resultados sobre a Teoria de Bases de Gröbner, veremos alguns conceitos básicos para um entendimento melhor dessa teoria (tais conceitos podem ser encontrados com mais detalhes em [1] e [2]).

1.1 Categorias e Funtores

Uma categoria $\mathcal{C}$ consiste de uma classe de *objetos*, Obj $\mathcal{C}$, e para cada par ordenado de objetos, (A, B), tem-se o conjunto de *morfismos*, $\mathcal{C}(A, B)$ (eventualmente vazio), tais que, se $(A, B) \neq (C, D)$, então $\mathcal{C}(A, B) \cap \mathcal{C}(C, D) = \varnothing$ e uma aplicação $\mathcal{C}(A, B) \times \mathcal{C}(B, C) \to \mathcal{C}(A, C)$, denotada por $(f, g) \mapsto gf$, satisfazendo os seguintes axiomas:

(1) Para cada objeto A, existe um *morfismo identidade* $1_A \in \mathcal{C}(A, A)$ tal que $f1_A = f$ para todo $f \in \mathcal{C}(A, B)$ e $1_A g = g$ para todo $g \in \mathcal{C}(C, A)$;

(2) Se A, B, C, D são objetos da categoria $\mathcal{C}$ com $\alpha \in \mathcal{C}(A, B), \beta \in \mathcal{C}(B, C)$, $\gamma \in \mathcal{C}(C, D)$, então $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (propriedade associativa)

Em uma categoria $\mathcal{C}$, um morfismo $f \in \mathcal{C}(A, B)$ é chamado de isomorfismo se existe $g \in \mathcal{C}(B, A)$ tal que $fg = 1_B$ e $gf = 1_A$. Quando existe um isomorfismo $f \in \mathcal{C}(A, B)$ diz-se que A é isomorfo a B e denota-se $A \cong B$.

Um morfismo $f \in \mathcal{C}(A, B)$ é chamado monomorfismo em $\mathcal{C}$ (respectivamente epimorfismo) se quaisquer que sejam $g_1, g_2 \in \mathcal{C}(C, A)$ (respectivamente $\in \mathcal{C}(A, C)$), sempre que $fg_1 = fg_2$ (respectivamente $g_1 f = g_2 f$) implicar $g_1 = g_2$.

Dizemos que X é um objeto zero de uma categoria $\mathcal{C}$ se para qualquer objeto $Y \in \mathrm{Obj}\,\mathcal{C}$, não vazio, tem-se: $\mathcal{C}(X, Y)$ e $\mathcal{C}(Y, X)$ são conjuntos unitários, este objeto é único a menos de isomorfismo e vamos denotá-lo por 0.

Seja $\mathcal{C}$ uma categoria e A, B objetos em $\mathcal{C}$. Um objeto P na categoria $\mathcal{C}$ é dito *projetivo* se para qualquer epimorfismo $g : A \to B$ e morfismo $h : P \to B$, existe um morfismo $s : P \to A$ tal que $g\,s = h$.

1.2 Anéis e Módulos

1.2.1 Anéis

Um anel R é um conjunto não vazio munido de duas operações binárias, chamadas adição (+) e multiplicação (.), tais que:

(1) R é um grupo abeliano com relação à adição, isto é, $(R, +)$ é um grupo abeliano.

(2) R é um semigrupo com relação à multiplicação, isto é, $(R, .)$ é um semigrupo.

(3) A operação de multiplicação é distributiva sobre a adição, ou seja, para todo $z, x, y \in R$, temos $z(x + y) = zx + zy$ e $(z + x)y = zy + xy$.

(4) R contém unidade, isto é, existe $1 \in R$ tal que $1.x = x.1 = x$ para todo $x \in R$.

Seja S um subconjunto de um anel R. Dizemos que S é um subanel se S é fechado com relação à adição e à multiplicação e se contém a unidade de R. Um ideal à esquerda (respectivamente à direita) é um subconjunto I de R com as seguintes propriedades:

$\forall\, i, j \in I$ tem-se $i + j \in I$;

$\forall\, r \in R$ e $\forall\, i \in I$ tem-se $ri \in I$ (respectivamente $ir \in I$).

Chamamos de ideal bilateral de R ao ideal que é simultaneamente ideal à esquerda e à direita.

Sejam R e S anéis. Uma transformação $f : R \to S$ é um homomorfismo de anéis com unidade quando f preserva adição, multiplicação e unidade. Em outras palavras, f satisfaz as condições:

- $f(x + y) = f(x) + f(y)$
- $f(x.y) = f(x).f(y)$
- $f(1_R) = 1_S$

A composição de homomorfismos de anéis é também um homomorfismo de anel. Chamamos de endomorfismos aos homomorfismos que vão de um anel em si mesmo. Um isomorfismo entre os anéis R e S, de acordo com a definição dada na página 5, é um homorfismo que é bijetivo. Neste caso, costumamos dizer que R e S são isomorfos como anéis.

Um divisor de zero à esquerda (respectivamente à direita) é um elemento $r \in R$ para o qual existe $s \in R\backslash\{0\}$ tal que $r.s = 0$ (respectivamente $s.r = 0$). E um elemento invertível à esquerda (respectivamente à direita) em R é um elemento $r \in R$ para o qual existe $s \in R$ tal que $r.s = 1$ (respectivamente $s.r = 1$). Um anel em que todos os elementos não nulos são invertíveis à esquerda e à direita é chamado de anel com divisão.

1.2.2 Módulos

Seja R um anel. Um R-módulo à esquerda é um grupo abeliano M, que denotaremos aditivamente, sobre o qual existe uma ação linear de R, isto é, existe uma transformação $(-,-) : R \times M \to M$, denotada por $(r,m) = rm$, que satisfaz:

(1) $(r+s)m = rm + sm$

(2) $r(m+n) = rm + rn$

(3) $(r.s)m = r(sm)$

(4) $1.m = m$

para todos $r, s \in R$ e $m, n \in M$.

Seja R um anel. Considere as aplicações $\lambda, \rho : R \times R \to R$ definidas por: $\lambda(a,x) = ax$ e $\rho(a,x) = xa$. R munido de sua operação aditiva e a multiplicação determinada por λ (respectivamente ρ) é um R-módulo à esquerda (respectivamente à direita) o qual denotaremos por ${}_RR$ (respectivamente R_R).

Sejam M e N R-módulos. Uma aplicação $f : M \to N$ é um homomorfismo de R-módulos se preserva a operação de soma e a ação de R, ou seja, se satisfaz as condições:

(1) $f(m+n) = f(m) + f(n)\ \forall\, m, n \in M$

(2) $f(rm) = rf(m)\ \forall\, m \in M$ e $r \in R$

Neste caso também dizemos que f é R-linear.

Observe que a composição de dois homomorfismos de R-modulos é novamente um homomorfismo de R-módulos.

O anel dos endomorfismos de um módulo M é o anel dos homomorfismos de módulo em si mesmo.

Um isomorfismo de módulo é um homomorfismo de módulos $f : M \to N$, que é bijetivo. Neste caso dizemos que M e N são isomorfos.

Um subconjunto N de M é um submódulo de M, se N é um subgrupo aditivo de M e $rn \in N$ para todo $r \in R$ e $n \in N$. (Os submódulos de ${}_RR$ são os ideais à esquerda de R)

Seja $f : M \to N$ um homomorfismo de R-módulos. Definem-se o núcleo e a imagem de f da seguinte forma:

- Núcleo de $f := Ker(f) = \{m \in M : f(m) = 0\}$
- Imagem de $f := Im(f) = \{n \in N : f(m) = n \text{ para algum } m \in M\}$

É de imediata verificação que $Ker(f)$ e $Im(f)$ são submódulos de M e N, respectivamente.

Na categoria de módulos sobre um anel R, a definição dada na seção 1.1 para monomorfismos (respectivamente epimorfismos) pode ser dada da seguinte forma: um morfismo de R-módulos $f : M \to N$ é um monomorfismo (epimorfismo) se $Ker(f) = \{0\}$, ou seja, se for injetor (respectivamente $Im(f) = N$, ou seja, se for sobrejetor).

Uma sequência de morfismos

$$\cdots \xrightarrow{f_3} M_2 \xrightarrow{f_2} M_1 \xrightarrow{f_1} M_0 \xrightarrow{f_0} M \longrightarrow 0$$

é *exata* quando $Im(f_i) = Ker(f_{i-1})$, para todo $i > 0$ e f_0 for sobrejetor. Quando os módulos M_i são projetivos, dizemos que a sequência exata é uma resolução projetiva de M. Note que, nesse caso, $M \cong M_0/Im(f_1)$. Como todo módulo é imagem homomórfica de um módulo livre, a resolução projetiva sempre existe. Para mais detalhes veja [4].

1.3 Álgebras

Seja R um anel comutativo. Uma R-álgebra A é um R-módulo munido de uma operação de multiplicação $(.)$, que satisfaz:

(1) $(A, .)$ é um semigrupo.

(2) A operação de multiplicação é distributiva sobre a adição de A vista como R-módulo.

Além disso, R age centralmente em A, ou seja,

$$r(ab) = (ra)b = a(rb)$$

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

Se a R-álgebra A possui unidade, dizemos que a R-álgebra A é uma álgebra com unidade e temos o seguinte homomorfismo de anéis:

$$\begin{array}{rcl} \varepsilon : R & \longrightarrow & A \\ r & \longmapsto & \varepsilon(r) = r1 \end{array}$$

Quando R é um corpo, uma base para a R-álgebra A, é uma base para A vista como módulo, ou seja, como R espaço vetorial. Se A admite uma R-base finita, dizemos que A tem dimensão finita sobre R.

Sejam A e B R-álgebras. Uma transformação $f : A \to B$ é um homomorfismo de R-álgebras se satisfaz:

(1) $f(a + b) = f(a) + f(b)\ \forall\, a, b \in A$

(2) $f(xa) = xf(a)\ \forall\, a \in A, \forall\, x \in R$

(3) $f(ab) = f(a)f(b)\ \forall\, a, b \in A$

(4) Se A e B são álgebras com unidade, então $f(1_A) = 1_B$.

Um homomorfismo de R-álgebras que for sobrejetor e injetor é um isomorfismo de R-álgebras, neste caso dizemos que A e B são álgebras isomorfas e escreveremos $A \cong B$. Relembramos também que aqui, nesta categoria, os homomorfismos injetores são monomorfismos e os sobrejetores são epimorfismos.

1.3.1 Álgebras de Caminhos

Nos exemplos que serão dados neste trabalho, utilizaremos apenas as álgebras de caminhos. Esse uso não é de forma nenhuma uma coincidência. Mais adiante, veremos que as álgebras de caminhos são inevitáveis no estudo da teoria de bases de Gröbner.

Agora vamos introduzir as noções de quiver e de álgebra de caminhos. Um quiver é um sistema $\mathcal{Q}(\mathcal{Q}_0, \mathcal{Q}_1, o, t)$, onde $\mathcal{Q}_0$ é um conjunto (cujos elementos são chamados de vértices), $\mathcal{Q}_1$ é um conjunto (cujos elementos são chamados de flechas), e cada uma das aplicações $o, t : \mathcal{Q}_1 \to \mathcal{Q}_0$ associa a cada flecha um vértice. Se $\alpha \in \mathcal{Q}_1$, $o(\alpha)$ é chamado de origem de α e $t(\alpha)$ é chamado de término de α. Um quiver é dito finito se ambos os conjuntos $\mathcal{Q}_0$ e $\mathcal{Q}_1$ são finitos.

Neste trabalho assumiremos que todo quiver $\mathcal{Q}$ é finito.

Definição. 1.1 *Um caminho γ de comprimento n, $n > 0$, no quiver $\mathcal{Q}$ é uma sequência de flechas $\gamma = \alpha_1 ... \alpha_n$ tal que $t(\alpha_i) = o(\alpha_{i+1})$ para todo $i = 1, \cdots, n-1$ (isto é, $\alpha_i \in \mathcal{Q}_1$ para todo $i \in \{1, \cdots, n\}$). A cada vértice $i \in \mathcal{Q}_0$ associamos também um caminho, chamado caminho trivial ou de comprimento nulo, denotado por e_i.*

Definição. 1.2 *Dado um caminho não trivial $\gamma = \alpha_1 ... \alpha_n$ definimos $o(\gamma) = o(\alpha_1)$ e $t(\gamma) = t(\alpha_n)$. No caso em que $o(\gamma) = t(\gamma)$ dizemos que γ é um circuito orientado.*

Definição. 1.3 *Dados $i, j \in \mathcal{Q}_0$ dizemos que i e j estão unidos por aresta se existe $\alpha \in \mathcal{Q}_1$ tal que $o(\alpha) = i$ e $t(\alpha) = j$ ou $o(\alpha) = j$ e $t(\alpha) = i$. Um quiver é conexo quando para quaisquer dois vértices i e j em $\mathcal{Q}_0$ a seguinte condição é verificada:*

- *Sempre que $i \neq j$ existe uma sequência de vértices $i = l_1, \cdots, l_n = j$ tais que l_k e l_{k+1} estão unidos por aresta, para todo $k \in \{1, \cdots, n-1\}$.*

Seja $\mathcal{K}$ um corpo. Consideremos $\mathcal{KQ}$ o $\mathcal{K}$-espaço vetorial tendo como base o conjunto de todos os caminhos de $\mathcal{Q}$. É importante notarmos que $\mathcal{KQ}$ tem estrutura de $\mathcal{K}$-álgebra, quando definimos a operação de multiplicação (.) de caminhos da seguinte forma:

$$\alpha.\beta = \begin{cases} 0 & \text{se } o(\beta) \neq t(\alpha) \\ \alpha\beta & \text{se } o(\beta) = t(\alpha) \end{cases}$$

Definição. 1.4 *Sejam $\mathcal{K}$ um corpo e $\mathcal{Q}$ um quiver. Denotamos por J o ideal de $\mathcal{KQ}$ gerado por todas as flechas de $\mathcal{Q}_1$. Dizemos que um ideal X de $\mathcal{KQ}$ é admissível quando satisfaz:*

- $X \subset J^2$
- $J^n \subset X$ *para algum* $n \in \mathbb{N}$

Uma relação em $\mathcal{Q}$ é uma combinação linear de caminhos de comprimento maior ou igual a dois com mesma origem e mesmo término.

Um importante resultado com relação a estes conceitos é a proposição abaixo cuja demonstração pode ser encontrada em [1].

Proposição 1.5 *Seja I um ideal admissível da $\mathcal{K}$-álgebra $\mathcal{KQ}$. Então existe um conjunto finito de relações $\rho_1, \cdots, \rho_t$, $t \in \mathbb{N}$ tal que $I = \langle \rho_1, \cdots, \rho_t \rangle$.* ∎

Definição. 1.6 *Seja $\rho = \{\rho_1, \cdots, \rho_t\}$ um conjunto de relações em $\mathcal{KQ}$. Dizemos que $(\mathcal{Q}, \rho)$ é um quiver com relações e a $\mathcal{K}$-álgebra quociente de $\mathcal{KQ}$ pelo ideal $\langle \rho \rangle$ é chamada algebra de caminhos de $(\mathcal{Q}, \rho)$ sobre o corpo $\mathcal{K}$, que denotaremos simplesmente por $\mathcal{KQ}/\langle \rho \rangle$.*

Lembramos que uma álgebra A é básica quando ${}_AA = P_1 \coprod \cdots \coprod P_s$, onde P_i é A-módulo projetivo indecomponível e $P_i \ncong P_j$ sempre que $i \neq j$ para todo $i, j \in \{1, \cdots, s\}$. O próximo resultado nos mostra como as álgebras de caminhos são importantes, e podemos encontrar sua demonstração em [1].

Proposição 1.7 *(Teorema de Gabriel) Seja $\mathcal{K}$ um corpo algebricamente fechado, e Λ uma $\mathcal{K}$-álgebra conexa, básica e de dimensão finita. Então existe um quiver $\mathcal{Q}$ e um conjunto de relações ρ, tal que $\langle\rho\rangle$ seja um ideal admissível de $\mathcal{K}\mathcal{Q}$, de modo que Λ é isomorfo à álgebra de caminhos $\mathcal{K}\mathcal{Q}/\langle\rho\rangle$.*

∎

O quiver $\mathcal{Q}$ associado à Λ recebe o nome de quiver ordinário de Λ.

Seja Λ uma $\mathcal{K}$-álgebra de dimensão finita, indecomponível e básica, e seja $E = \{e_1, \cdots, e_n\}$ um sistema completo de idempotentes ortogonais e primitivos de Λ. A determinação do quiver ordinário de Λ é realizada tomando um conjunto (de vértices) em bijeção com E, e estipulando que entre os vértices i e j existem exatamente $dim_{\mathcal{K}}[e_j(rad\Lambda/rad^2\Lambda)e_i]$ flechas.

Seja $\mathcal{Q}$ um quiver. Uma representação de $\mathcal{Q}$ é dado pelo sistema

$$V = ((V_i)_{i\in\mathcal{Q}_0}, (f_\alpha)_{\alpha\in\mathcal{Q}_1}),$$

onde para cada $i \in \mathcal{Q}_0$, V_i é um $\mathcal{K}$-espaço vetorial (não necessariamente de dimensão finita) e f_α é uma transformação $\mathcal{K}$-linear de $V_{o(\alpha)}$ para $V_{t(\alpha)}$. Dado um caminho não trivial $\gamma = \alpha_1 ... \alpha_s$, $s \in \mathbb{N}$, de i a j em $\mathcal{Q}$, podemos definir $V(\gamma)$ como a transformação linear de V_i para V_j dada pela composta $f_{\alpha_s} \cdots f_{\alpha_1}$ e estendendo esta definição para uma combinação linear de caminhos.

Dizemos que uma representação V satisfaz uma relação r se $V(r) = 0$, e dizemos que V satisfaz um sistema de relações ρ se V satisfizer cada relação $r \in \rho$. Uma representação de um quiver com relações $(\mathcal{Q}, \rho)$ é uma representação de $\mathcal{Q}$ que satisfaz as relações de ρ.

Definição. 1.8 *Sejam $V = ((V_i)_{i\in\mathcal{Q}_0}, (f_\alpha)_{\alpha\in\mathcal{Q}_1})$ e $W = ((W_i)_{i\in\mathcal{Q}_0}, (g_\alpha)_{\alpha\in\mathcal{Q}_1})$ duas representações de $\mathcal{Q}$, um morfismo $\phi : V \to W$ é uma família de transformações $\mathcal{K}$-lineares $\phi = (\phi_i)_{i\in\mathcal{Q}_0}$ tal que, para cada $\alpha \in \mathcal{Q}_1$, o seguinte*

diagrama comuta:

$$\begin{array}{ccc} V_{o(\alpha)} & \xrightarrow{f_\alpha} & V_{t(\alpha)} \\ {\scriptstyle \phi_{o(\alpha)}}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \phi_{t(\alpha)}} \\ W_{o(\alpha)} & \xrightarrow{g_\alpha} & W_{t(\alpha)} \end{array}$$

A composição de morfismos é definida coordenada a coordenada. Desta forma, fica definida a *categoria das representações* de $(\mathcal{Q}, \rho)$.

Dada uma $\mathcal{K}$-álgebra Λ de dimensão finita, indecomponível, básica, e sendo $\mathcal{K}$ algebricamente fechado, pelo teorema de Gabriel Λ, é isomorfa a uma álgebra de caminhos da forma $\mathcal{K}\mathcal{Q}/\langle\rho\rangle$, nestas condições, a categoria construida da forma acima e a categoria dos módulos à direita, que são finitamente gerados sobre a álgebra Λ, são equivalentes.

1.4 Ordem

A escolha de uma boa ordem é fundamental para o estudo da teoria das bases de Gröbner. Mas antes, precisamos de alguns conceitos básicos a respeito de *ordem.*

Definição. 1.9 *Uma ordem parcial em um conjunto não vazio X é uma relação transitiva, antissimétrica e reflexiva em X, que denotaremos por $\leq$ e escreveremos $x \leq y$, com $x, y \in X$ para indicar que o par ordenado (x, y) pertence a ordem.*

Diremos ainda que um conjunto X é *parcialmente ordenado* se existe uma ordem parcial em X.

Dado um conjunto X, parcialmente ordenado por $\leq$, pode ocorrer que para todo $x, y \in X$, $x \leq y$ ou $y \leq x$. Neste caso, dizemos que $\leq$ é uma *ordem total* em X e que X é *totalmente ordenado.* Chamaremos aqui um conjunto totalmente ordenado de *cadeia.*

Utilizaremos ainda a seguinte notação:

i) $x \geq y$ se $y \leq x$;

ii) $x < y$ se $x \leq y$ e $x \neq y$;

iii) $x > y$ se $y \leq x$ e $x \neq y$.

Definição. 1.10 *Seja X um conjunto parcialmente ordenado. Um elemento $a \in X$ é dito mínimo se $a \leq x$ para todo $x \in X$.*

Temos ainda que $a \in X$ é dito minimal se $x \leq a$ implica $x = a$ para todo $x \in X$.

Por fim, diremos que $a \in X$ é limitante inferior de um subconjunto E de X se $a \leq x$ para qualquer $x \in E$.

Definição. 1.11 *Dizemos que $\leq$ é uma boa ordem em X, se é uma ordem total em X e todo subconjunto não vazio possui um elemento minimal.*

O próximo resultado é fundamental para o restante do trabalho.

Teorema 1.12 *Seja X um conjunto. Então $\leq$ é uma boa ordem em X se e somente se $\leq$ é uma ordem total e para cada cadeia descendente de elementos de X, $b_1 \geq b_2 \geq \cdots$ existe algum $N \in \mathbb{N}^*$ tal que $b_N = b_{N+1} = \cdots$.*

∎

Capítulo 2

Bases de Gröbner

As bases de Gröbner, que aparecem inicialmente no trabalho de Buchberger, em 1965, tem como idéia principal o de providenciar um método sistemático de construir um conjunto de geradores para ideais de um anel (de polinômios) e decidir se determinado polinômio pertence ou não a esse ideal. Esse método é particularmente interessante do ponto de vista computacional. As definições e resultados dadas nesse capítulo podem ser encontrados em [9] e [10].

2.1 Bases de Gröbner Lineares

Nesta seção vamos considerar somente espaços vetoriais. As idéias introduzidas aqui servirão de base para o restante do trabalho. E trataremos de algumas propriedades das bases de Gröbner nesse caso.

Seja $\mathcal{K}$ um corpo e V um $\mathcal{K}$-espaço vetorial. Fixemos, para V, uma base $\mathcal{B} = \{b_i\}_{i\in\mathcal{I}}$, onde $\mathcal{I}$ é um conjunto de índices.

Como $\mathcal{B}$ é uma base de V, então para cada $v \in V$, existe uma família $(\lambda_i)_{i\in\mathcal{I}}$ tal que $v = \sum_{i\in\mathcal{I}} \lambda_i b_i$, onde $\lambda_i = 0$, exceto para um número finito de índices.

Se $v = \sum_{i \in \mathcal{I}} \lambda_i b_i$, dizemos que b_i *ocorre em* v se $\lambda_i \neq 0$.

Definição. 2.1 *Se $\mathcal{B} = \{b_i\}_{i \in \mathcal{I}}$ é uma base do espaço vetorial V, com uma boa ordem $>$ em $\mathcal{B}$, e se $v = \sum_{i \in \mathcal{I}} \lambda_i b_i$ é não nulo, dizemos que b_i é o maior elemento de v se b_i ocorre em v e $b_i \geq b_j$ para todo b_j ocorrendo em v. Denotaremos o maior elemento b_i de v por $Tip(v)$ e o seu coeficiente λ_i por $CTip(v)$.*

O conjunto dos elementos $b_i \in \mathcal{B}$ tais que b_i ocorre em v é dito suporte de v, denotado por supp*(v).*

Se X é um subconjunto de V, definimos por

(i) $Tip(X) = \{b \in \mathcal{B} : b = Tip(x)$ para algum $0 \neq x \in X\}$

(ii) $NonTip(X) = \mathcal{B} \setminus Tip(X)$

Assim, ambos, $Tip(X)$ e $NonTip(X)$ são subconjuntos de $\mathcal{B}$ e dependem da escolha da boa ordem de $\mathcal{B}$.

Denotamos por $Span(X)$ o espaço vetorial gerado pelo conjunto X.

O próximo resultado será bastante usado ao longo do trabalho.

Teorema 2.2 *Seja V um espaço vetorial sobre o corpo $\mathcal{K}$, com base $\mathcal{B}$. Seja $>$ uma boa ordem em $\mathcal{B}$. Suponha que W é subespaço de V, então*

$$V = W \oplus Span(NonTip(W)).$$

Prova. Seja $W' = Span(NonTip(W))$. Primeiramente vamos mostrar que $W \cap W' = \{0\}$.

Seja $x \in W' \setminus \{0\}$. Se $x \in W$, então $Tip(x) \in Tip(W)$. No entanto, $Tip(x) \in NonTip(W)$ pois $x \in W'$, e assim obteríamos uma contradição.

Agora, mostraremos que $V = W + W'$. Aqui usaremos o fato da boa ordenação em $\mathcal{B}$.

Seja $v \in V$ tal que $Tip(v)$ é minimal com respeito a propriedade de $v \notin W + W'$, mostraremos que isso nos levará a uma contradição.

Considere $Tip(v) = b$ e $\alpha = CTip(v)$. Note que $Tip(v - \alpha b) < tip(v)$. Assim $w + w' = v - \alpha b \in W + W'$, pela condição de minimalidade, com $w \in W$ e $w' \in W'$.

Se $b \in NonTip(W)$, teremos $w' + \alpha b \in W'$ e assim,

$$v = w + (w' + \alpha b)$$

o que não pode acontecer.

Por outro lado, se $b \in Tip(W)$, então existe $z \in W$ tal que $Tip(z) = b$, seja $\beta = CTip(z)$. Então $Tip(v - (\alpha/\beta)z) < Tip(v)$. Novamente, pela condição de minimalidade, temos que $v - (\alpha/\beta)z = w + w'$ com $w \in W$ e $w' \in W'$.

Logo, temos uma contradição, pois

$$v = (w + (\alpha/\beta)z) + w' \in W + W'$$

∎

Do teorema 2.2 podemos ver que todo vetor não nulo $v \in V$ pode ser escrito de forma única como $w_v + N(v)$, onde $N(v) \in Span(NonTip(W))$ e $w_v \in W$.

Definição. 2.3 *Chamamos $N(v)$ a forma normal de v.*

Seja W um subespaço de V. A seguir, temos a definição de uma base de Gröbner linear para W.

Definição. 2.4 *Dizemos que um conjunto de vetores $\mathcal{G} \subset W$ é uma base de Gröbner linear para W com respeito a boa ordem $>$ se*

$$Span(Tip(W)) = Span(Tip(\mathcal{G})).$$

Se $\mathcal{G}$ é uma base de Gröbner linear para W, então $Span(\mathcal{G}) = W$.

Pois, como $\mathcal{G} \subset W$, $Span(\mathcal{G}) \subset W$. Suponha por absurdo que $W \not\subset Span(\mathcal{G})$, assim tome $w \in W \setminus Span(\mathcal{G})$ com $Tip(w)$ minimal.

Como $Span(Tip(W)) = Span(Tip(\mathcal{G}))$, existe $g \in \mathcal{G}$ tal que $Tip(w) = Tip(g)$. Dessa forma, $w' = w - (CTip(w)/CTip(g))g \in Span(\mathcal{G})$, pois $Tip(w') < Tip(w)$. Logo $w = w' + (CTip(w)/CTip(g))g \in Span(\mathcal{G})$, que é um absurdo. Portanto, $Span(\mathcal{G}) = W$.

Definição. 2.5 *Seja W um subespaço de V. Dizemos que um subconjunto $\mathcal{G}$ de W é uma base de Gröbner linear reduzida para W (com respeito a $>$) se:*

(i) $\mathcal{G}$ é uma base de Gröbner linear para W;

(ii) Se $g \in \mathcal{G}$, então $CTip(g) = 1$;

(iii) Se g e g' são elementos distintos de $\mathcal{G}$, então $Tip(g) \neq Tip(g')$;

(iv) Se $g \in \mathcal{G}$, então $g - Tip(g) \in Span(NonTip(W))$.

Para garantir a existência de uma base de Gröbner linear reduzida temos o seguinte resultado:

Proposição 2.6 *Seja V um espaço vetorial e $>$ uma boa ordem na base $\mathcal{B}$ de V. Seja W um subespaço de V. Então existe uma única base de Gröbner linear reduzida para W.*

Prova. Seja $\mathcal{T} = Tip(W)$ e defina $\mathcal{G} = \{t - N(t) : t \in \mathcal{T}\}$. Pelo teorema 2.2, $t - N(t) \in W$. Agora, $Tip(t - N(t)) = t$ porque nenhum elemento ocorrendo em $N(t)$ pode ser Tip de um elemento em W. Logo $\mathcal{G}$ é uma base de Gröbner linear para W.

Ainda observando que para $g = t - N(t) \in \mathcal{G}$, $Tip(g) = t$, temos de forma direta as demais propriedades de uma base de Gröbner linear reduzida. ∎

2.2 Bases de Gröbner para $\mathcal{K}$-Álgebras

Agora, voltamos a nossa atenção para $\mathcal{K}$-álgebras, não necessariamente com unidade. Seja Λ uma $\mathcal{K}$-álgebra e seja $\mathcal{B}$ uma $\mathcal{K}$-base de Λ. Assumimos que, para todo $b, b' \in \mathcal{B}$ temos $bb' \in \mathcal{B}$ ou $bb' = 0$. Tal $\mathcal{K}$-base é dita *base multiplicativa* de Λ.

Não queremos uma ordem arbitrária em $\mathcal{B}$, queremos uma ordem que preserve a estrutura multiplicativa de $\mathcal{B}$.

Definição. 2.7 *Dizemos que uma boa ordem em $\mathcal{B}$ é admissível, se satisfaz as seguintes condições, para todo $p, q, r, s \in \mathcal{B}$:*

(i) Se $p < q$ então $pr < qr$, se ambos são não nulos;

(ii) Se $p < q$ então $sp < sq$, se ambos são não nulos;

(iii) Se $p = sqr$ então $p \geq q$.

Como exemplo de uma $\mathcal{K}$-álgebra que possui uma $\mathcal{K}$-base multiplicativa com ordem admissível são as álgebras de caminhos $\mathcal{KQ}$, tendo como base $\mathcal{B}$ o conjunto de todos os caminhos em $\mathcal{Q}$, incluindo os vértices, e a ordem é a *comprimento-lexicográfica*, isto é, dado às flechas e aos vértices uma ordenação arbitrária (ou seja, uma lexicografia), com os vértices menores que as flechas. Se p e q são caminhos de comprimento maiores que 1, dizemos que $p < q$ se o comprimento de p for menor que o comprimento de q ou se $p = p_1 p_2 \cdots p_r$ e $q = q_1 q_2 \cdots q_r$, com p_i, q_j caminhos de comprimento 1 em $\mathcal{B}$, e para algum $1 \leq i \leq r$, $p_j = q_j$ se $j < i$ e $p_i < q_i$.

Dizemos que uma $\mathcal{K}$-álgebra Λ possui a *teoria de bases de Gröbner* se Λ possui uma base multiplicativa $\mathcal{B}$ com ordem admissível $>$ nessa base. A partir desse ponto, assumimos que a $\mathcal{K}$-álgebra Λ possui a teoria de bases de Gröbner. Seja I um ideal bilateral em Λ.

Definição. 2.8 *Dizemos que um conjunto $\mathcal{G} \subset I$ é uma base de Gröbner para I com respeito à ordem $>$, se*

$$\langle Tip(\mathcal{G}) \rangle = \langle Tip(I) \rangle$$

como ideais bilaterais.

Uma observação a se fazer é que aqui também é válido o teorema 2.2, ou seja, como espaços vetoriais

$$\Lambda = I \oplus Span(NonTip(I))$$

Em particular, todo $r \in \Lambda$ não nulo, pode ser escrito de forma única como $r = i_r + N(r)$, onde $i_r \in I$, e $N(r) \in Span(NonTip(I))$. $N(r)$ é também chamado de *forma normal de* r.

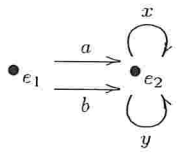
Definição. 2.9 *Sejam $b_1, b_2 \in X \subset \Lambda$, dizemos que b_1 divide b_2 (em X) se existem $c, d \in X$ tais que $b_2 = b_1 d$, $b_2 = c b_1$ ou $b_2 = c b_1 d$.*

Proposição 2.10 *Se uma base multiplicativa $\mathcal{B}$ de uma $\mathcal{K}$-álgebra Λ admite uma ordem admissível, então toda sequência infinita de $\mathcal{B}$, $b_1, b_2, \cdots$, tal que b_{i+1} divide b_i para todo $i \geq 1$ estabiliza, isto é, existe $N \in \mathbb{N}$ tal que $b_N = b_{N+k}$, para todo $k \in \mathbb{N}$.*

Prova. Por definição, como b_{i+1} divide b_i, então existem $c_i, d_i \in \mathcal{B}$, tais que $b_i = c_i b_{i+1} d_i$, para $i \geq 1$. Daí, $b_i \geq b_{i+1}$, ou seja, obtem-se uma cadeia descendente. Como a ordem dada é uma boa ordem, o resultado segue da proposição 1.12. ∎

Este resultado mostra que nem toda base multiplicativa possue uma ordem admissível. Como mostra o próximo exemplo:

Exemplo. Seja $\mathcal{Q}$ o seguinte quiver:



Seja o ideal $I =< ax^n - b, a - by^m : m, n \in \mathbb{N}^* >$. Uma base multiplicativa $\mathcal{B}$ de $\Lambda = \mathcal{K}\mathcal{Q}$ é o conjunto de todos os caminhos de $\mathcal{Q}$. Note que, em Λ/I, temos $\overline{ax^n} = \overline{by^m x^n} = \overline{b}$ e $\overline{by^m} = \overline{ax^n y^m} = \overline{a}$ para todo $n, m \in \mathbb{N}$, assim podemos considerar em Λ/I a seguinte base

$$\overline{\mathcal{B}} = \mathcal{B} \setminus \{bx^n, ay^m, ax^n, by^m, ax^n y^m, by^m x^n : m, n \in \mathbb{N}^*\}.$$

Note que $\overline{\mathcal{B}}$ contém uma base de $\mathcal{K}\langle x, y\rangle$. Note também que, $\overline{a}\,\overline{x} = \overline{b}$ o que implica em dizer que $\overline{a}$ divide $\overline{b}$. Por outro lado, $\overline{b}\,\overline{y} = \overline{a}$, logo, $\overline{b}$ divide $\overline{a}$. Assim, temos uma sequência descendente infinita $\overline{a}, \overline{b}, \overline{a}, \overline{b}, \cdots$ que não estabiliza, portanto $\overline{\mathcal{B}}$ não possui uma ordem admissível.

Dada uma base $\mathcal{B}$, chamaremos de *monômios* seus elementos. Diremos que um ideal I em Λ é um *ideal monomial* se ele pode ser gerado por elementos de $\mathcal{B}$.

Proposição 2.11 *Seja Λ uma $\mathcal{K}$-álgebra com base multiplicativa $\mathcal{B}$ que admite uma ordem admissível $>$. Se I é um ideal monomial em Λ, então I tem um único conjunto gerador monomial minimal, em relação à divisão.*

Prova. Seja A o conjunto de todos os monômios em I. Seja

$$M = \{p \in A : \text{se } q \in A \text{ divide } p, \text{ então } q = p\}$$

Pela proposição anterior temos que M é não vazio.

Seja $\mathcal{C}$ um conjunto de monômios que geram I. Se $b \in \mathcal{C}$, então, para algum $m \in M$, m divide b. Assim, $\mathcal{C} \subset \langle M\rangle$. Logo, $I \subset \langle M\rangle$.

Agora, seja M' um outro conjunto de monômios geradores de I, então todo $m \in M$ é divisível por algum $m' \in M'$. Mas, pela definição de M, $m' = m$. Logo, $M \subset M'$. ∎

Note que o conjunto minimal de geradores M não depende de qualquer ordem admissível particular. A existência de uma ordem admissível é necessária apenas para mostrar que M é não vazio.

Observe ainda que para todo ideal I de Λ, se $\mathcal{G}$ é uma base de Gröbner de I, então $Tip(\mathcal{G})$ contém o conjunto gerador monomial minimal de $\langle Tip(I)\rangle$.

Seja $\mathcal{T}$ o conjunto gerador monomial minimal de $\langle Tip(I)\rangle$ (dada uma ordem admissível $>$).

Definição. 2.12 *A base de Gröbner reduzida para I, com respeito à ordem $>$ é*

$$\mathcal{G} = \{t - N(t) : t \in \mathcal{T}\}$$

Proposição 2.13 *Seja $>$ uma ordem admissível na base multiplicativa $\mathcal{B}$ da $\mathcal{K}$-álgebra Λ. Sejam I um ideal em Λ e $\mathcal{G}$ uma base de Gröbner reduzida para I. Então:*

(i) $\mathcal{G}$ é uma base de Gröbner de I;

(ii) Se $g \in \mathcal{G}$, então $CTip(g) = 1$;

(iii) Se $g \in \mathcal{G}$, então $g - Tip(g) \in Span(NonTip(I))$;

(iv) $Tip(\mathcal{G})$ é o conjunto gerador monomial minimal para $\langle Tip(I)\rangle$ ∎

2.3 Algoritmo da Divisão

Nesta seção, fixamos um corpo $\mathcal{K}$, uma $\mathcal{K}$-álgebra Λ com base multiplicativa $\mathcal{B}$ e uma ordem admissível $>$ nessa base.

Dados $x, y \in \Lambda$, temos visto como podemos dividir y por x em Λ, definição 2.9. Apresentamos agora o *algoritmo da divisão*, onde mostraremos como dividir um elemento $y \in \Lambda$ por um dado conjunto X. Enfatizamos aqui que a ordenação no conjunto X afeta no resultado do algoritmo da divisão, como veremos mais tarde.

Seja $X = \{x_1, \cdots, x_n\}$ um conjunto ordenado de elementos de Λ e $y \in \Lambda$.

O algoritmo nos fornecerá inteiros não negativos $m_1, m_2, \cdots, m_n$ e elementos $u_{ij}, v_{ij} \in \Lambda$ $1 \leq i \leq n$ e $1 \leq j \leq m_i$ tais que:

(i) $y = \sum_{i=1}^{n}(\sum_{j=1}^{m_i} u_{ij}x_iv_{ij}) + r$;

(ii) $Tip(y) \geq Tip(u_{ij}x_iv_{ij})$ $\forall i, j$;

(iii) Para cada $b \in \mathcal{B}$ tal que b ocorra em r, $Tip(x_i)$ não divide b, $1 \leq i \leq n$.

Chamaremos r de *resto da divisão* de y por X e denotaremos por $y \Rightarrow_X r$.

Apresentamos abaixo o algoritmo em pseudo-código:

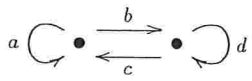
O Algoritmo da Divisão

INPUT: $x_1, \cdots, x_n$ (ordenado), y
OUTPUT: $m_1, \cdots, m_n, u_{ij}, v_{ij}, r$
INICIALIZE: $m_1 := 0, \cdots, m_n := 0, r := 0, z := y$,
INÍCIO:
ENQUANTO $(z \neq 0)$ FAÇA
  PARA $(i = 1)$ ATÉ n FAÇA
    SE $Tip(z) = uTip(x_i)v$ para $u, v \in \mathcal{B}$ ENTÃO
      $m_i := m_i + 1$
      $u_{im_i} := v$
      $z := z - [Ctip(z)/Ctip(x_i)]ux_iv$
      VÁ PARA INÍCIO

$$r := r + Ctip(z)Tip(z)$$
$$z := z - Ctip(z)Tip(z)$$

Antes de prosseguirmos, veremos um exemplo em que a ordem do conjunto X dada inicialmente influi no resto r obtido através do algoritmo da divisão:

Exemplo. Seja $\mathcal{Q}$ o quiver



Seja a álgebra de caminhos $\mathcal{KQ}$ com base multiplicativa $\mathcal{B}$, formada por todos os possíveis caminhos do quiver, com a ordem comprimento-lexicográfica, onde a lexicografia é dada por $a < b < c < d$.

Tomemos $X = \{f_1 = cab - ab, f_2 = abdc - dc\}$ e $y = bcabdc$.

Iniciando o algoritmo, vemos que $z = bcabdc = bTip(f_1)dc$.

Assim, $u_{11} = b, v_{11} = dc$ e $z := bcabdc - u_{11}f_1v_{11} = -babdc$. Agora, como $z = bTip(f_2)$, $u_{12} := b$ e $z := -babdc - [CTip(z)]u_{12}f_2 = bdc$.

Note que, nem $Tip(f_1)$, nem $Tip(f_2)$ divide $Tip(z) = bdc$, logo o resto $r = bdc$, e agora z toma o valor zero, parando assim o algoritmo, retornando:

$$bcabdc = bf_1dc + bf_2 - bdc.$$

No entanto, se invertermos a ordenação em X, ou seja, se iniciarmos o algoritmo tomando primeiramente o elemento f_2, veremos que o algoritmo nos retornará

$$bcabdc = bcf_2,$$

pois $(bc)(dc) = 0$. Note que o resto nesse caso é $r = 0$.

Como podemos perceber, a ordem influencia no resto da divisão. No entanto, se X for uma base de Gröbner, então o resto da divisão independe da ordenação em X, como podemos ver no próximo resultado.

Proposição 2.14 *Seja $\mathcal{G}$ uma base de Gröbner de um ideal I de Λ. Seja $y \in \Lambda$ e assuma que $X = \{g \in \mathcal{G} : Tip(g) \leq Tip(y)\}$ seja finito. Se $y \Rightarrow_X r$, então r independe da ordem dos elementos de X. Na verdade $r = N(y)$.*

Prova. Considere $y \Rightarrow_X r$. Então, como $Tip(r) \leq Tip(y)$, temos que para cada $g \in \mathcal{G}$, $Tip(g)$ não divide nenhum elemento da base ocorrendo em r.

Assim $r \in Span(Nontip(I))$. Agora, $y = \sum_i \sum_j u_{ij} g_i v_{ij} + r$. Mas, pelo teorema 2.2, $y = i_y + N(y)$ com $i_y \in I$ e $N(y) \in Span(Nontip(I))$, únicos.

Assim, como $\sum_i \sum_j u_{ij} g_i v_{ij} \in I$, temos $r \in Span(Nontip(I))$, e portanto $r = N(y)$. ∎

Corolário 2.15 *Se $\mathcal{G}$ é uma base de Gröbner de um ideal I em Λ tal que para cada $b \in \mathcal{B}$ exista somente um número finito de elementos $g \in \mathcal{G}$ com $Tip(g) \leq b$, então existe um algoritmo para encontrar a forma normal de elementos de Λ.*

∎

Note que agora temos também um método para encontrar a base de Gröbner reduzida uma vez encontrada uma base de Gröbner com um número finito de termos com um dado Tip. Note que, com essa hipótese, não é necessário que a base de Gröbner seja finita. Pois, para cada $x \in \Lambda$, temos apenas um número finito de elementos $g \in \mathcal{G}$ tais que $Tip(g) \leq Tip(x)$. Viabilizando assim o uso do algoritmo da divisão.

Este é um algoritmo, isto é, o processo termina, se $I_{MON} = \langle Tip(I) \rangle$ tem um conjunto de monômios gerador finito.

O método procede da seguinte forma:

(i) Dada uma base de Gröbner $\mathcal{G}$ tal que somente um número finito de termos possui um dado Tip.

(ii) Encontre o conjunto gerador monomial minimal $\mathcal{T}$ de I_{MON}.

(iii) Para cada $t \in \mathcal{T}$, usando o algoritmo da divisão, calcule $t \Rightarrow_G N(t)$.

(iv) A base de Gröbner reduzida é $\{t - N(t) : t \in \mathcal{T}\}$.

2.4 Relações de Sobreposição

Definição. 2.16 *Sejam $f, g \in \Lambda$ e suponha que existam $b, c \in \mathcal{B}$ tais que:*

(i) $Tip(f)c = bTip(g)$

(ii) $Tip(f)$ não divide b e $Tip(g)$ não divide c.

Então a relação de sobreposição de f e g por b e c é dada por:

$$o(f, g, b, c) = (1/CTip(f))fc - (1/CTip(g))bg$$

Exemplo. Seja a álgebra livre $\mathcal{K}\langle x, y, z\rangle$, com $\mathcal{K}$-base gerada por $1, x, y, z$ e ordem comprimento lexicográfica (que é uma ordem admissível), onde a lexicografia é dada por $1 < x < y < z$.

Sejam $f = zxyyz - xyz$ e $g = xyx - xy$. Como $Tip(f) = zxyyx$ e $Tip(g) = xyx$, note que

$$Tip(f)yx = zxyyTip(g)$$

e $Tip(f)$ não divide $zxyy$ e $Tip(g)$ não divide yx. Portanto, temos aqui uma relação de sobreposição

$$\begin{aligned} o(f, g, zxyy, yx) &= fyx - zxyyg = (zxyyx - xyz)yx - zxyy(xyx - xy) \\ &= zxyyxyx - xyzyx - zxyyxyx + zxyyxy \\ &= zxyyxy - xyzyx \end{aligned}$$

Temos ainda que, $Tip(g)yx = xyTip(g)$ e que $Tip(g)$ não divide xy e não divide yx, assim temos aqui mais uma relação de sobreposição de g sobre ele mesmo:

$$\begin{aligned} o(g,g,xy,yx) &= gyx - xyg = (xyx - xy)yx - xy(xyx - xy) \\ &= xyxyx - xyyx - xyxyx + xyxy \\ &= -xyyx + xyxy \end{aligned}$$

Note que $Tip(o(f,g,b,c)) < Tip(f)c = bTip(g)$.

Suponha que $X = \{x_1, \cdots, x_n\} \subset \Lambda$. Seja I o ideal gerado por X.
Se $Tip(x_i) = uTip(x_j)v$ para algum $u, v \in \mathcal{B}$, então fazendo

$$X' = \{x_1, \cdots, x_{i-1}, x_i - [CTip(x_i)/CTip(x_j)]ux_jv, x_{i+1}, \cdots, x_n\}$$

temos que X' é também gerador de I.

Continuando o processo, obtemos um conjunto finito Y gerador de I tal que $Tip(y_i)$ não divide $Tip(y_j)$, para $y_i, y_j \in Y$ com $i \neq j$.

Este é um processo finito pela boa ordem assumida. Assim podemos assumir que não há divisões de $Tip's$ em um conjunto gerador de um ideal.

Definição. 2.17 *Dizemos que um conjunto de elementos X é Tip reduzido se para elementos distintos $x, y \in X$, $Tip(x)$ não divide $Tip(y)$.*

Definição. 2.18 *Dizemos que um elemento $f = \sum_{i=1}^{n} \alpha_i b_i$, com $b_i \in \mathcal{B}$ e $\alpha_i \in \mathcal{K} \setminus \{0\}$ para $1 \leq i \leq n$ é (à esquerda) uniforme se para cada $c \in \mathcal{B}$, ou $cb_i = 0$ para $1 \leq i \leq n$, ou $cb_i \neq 0$ para $1 \leq i \leq n$.*

Se um dado conjunto possui apenas elementos uniformes dizemos então que esse conjunto é uniforme.

Definição. 2.19 *Seja Λ uma $\mathcal{K}$-álgebra com base multiplicativa $\mathcal{B}$ e uma ordem admissível $>$ em $\mathcal{B}$. Seja $\mathcal{C}$ o conjunto formado pelos elementos indecomponíveis de $\mathcal{B}$. Para todo $b \in \mathcal{B}$ definimos o comprimento de b, $\ell(b)$, como sendo o menor inteiro n tal que $b = c_1c_2 \cdots c_n$, onde $c_i \in \mathcal{C}$ com $1 \leq i \leq n$.*

Cabe observar que o conjunto $\mathcal{C}$ pode ser infinito, no entanto, $\ell(b)$ é sempre finito, pois se $b = c_1c_2c_3c_3\cdots$, teríamos uma sequência infinita, $b, c_2c_3c_4\cdots, c_3c_4\cdots, \cdots$, com $b \geq c_2c_3c_4\cdots \geq c_3c_4\cdots \geq \cdots$, contradizendo a hipótese da boa ordenação em $\mathcal{B}$.

Podemos notar ainda que, o comprimento de um elemento depende da escolha da base multiplicativa $\mathcal{B}$. O resultado abaixo, descrito em [10], é uma versão do *Lema do Diamante* (veja [5], [7]) e será muito importante para a construção de uma base de Gröbner mais adiante.

Teorema 2.20 *Seja Λ uma $\mathcal{K}$-álgebra com base multiplicativa $\mathcal{B}$ e ordem admissível $>$. Suponha que $\mathcal{G}$ é um conjunto uniforme, Tip reduzido de Λ. Suponha que para toda relação de sobreposição*

$$o(g_1, g_2, p, q) \Rightarrow_{\mathcal{G}} 0$$

com $g_1, g_2 \in \mathcal{G}$. Então $\mathcal{G}$ é uma base de Gröbner para $\langle\mathcal{G}\rangle$.

Prova. Assuma que $\mathcal{G}$ tem a propriedade de que toda relação de sobreposição tem resto zero sobre a divisão por $\mathcal{G}$. Seja $x \in \langle\mathcal{G}\rangle$ e assuma que $Tip(x)$ não é divisível pelo Tip de nenhum elemento de $\mathcal{G}$, veremos que isto nos levará a uma contradição. Sem perda de generalidade, vamos assumir que x é uniforme. Como $\mathcal{G}$ é um conjunto gerador de $\langle\mathcal{G}\rangle$, podemos escrever:

$$x = \sum_{i,j} \alpha_{ij} p_{ij} g_i q_{ij} \qquad (*)$$

onde $g_i \in \mathcal{G}$, $p_{ij}, q_{ij} \in \mathcal{B}$ e $\alpha_{ij} \in \mathcal{K}$. Considere todas as formas de se escrever x. Seja $\overline{p}$ o maior elemento (com respeito à ordem dada) da base $\mathcal{B}$ ocorrendo do lado direito de $(*)$. Como estamos assumindo que $Tip(x)$ não é divisível pelo Tip de nenhum elemento de $\mathcal{G}$, temos pela uniformidade de x que $\overline{p}$ é maior que $Tip(x)$ na ordem $>$. Logo, os $\overline{p}$'s se cancelam.

Considerando todas formas de escrever x como em $(*)$, escolhemos aquela em que $\overline{p}$ seja o menor possível e tenha o menor número de ocorrências do lado direito de $(*)$.

Como $\overline{p}$ não ocorre do lado esquerdo de $(*)$, ele deve aparecer em pelo menos dois somandos do lado direito de $(*)$. Logo, existem i, j, i', j' tais que

$$\overline{p} = p_{ij}Tip(g_i)q_{ij} = p_{i'j'}Tip(g_{i'})q_{i'j'} .$$

Para simplificar a notação escreveremos $p = p_{ij}$, $g = g_i$, $q = q_{ij}$, $p' = p_{i'j'}$, $g' = g_{i'}$ e $q' = q_{i'j'}$.

Caso 1: $\ell(p) < \ell(p')$.

Caso 1.1: $\ell(q) < \ell(q')$. Então $Tip(g')$ é divisível por $Tip(g)$ e assim $Tip(g)$ divide $Tip(g')$ contradizendo a hipótese de Tip redução.

Caso 1.2: $\ell(q) \geq \ell(q')$. Consideremos duas possibilidades:

Caso 1.2.1: $\ell(p') \geq \ell(pTip(g))$.

Então não existe relação de sobreposição entre $Tip(g)$ e $Tip(g')$ em $\overline{p}$.

Pela escolha dos comprimentos, segue que existe um caminho q'' tal que $\overline{p} = pTip(g)q''Tip(g')q'$.

Agora, se $g = \sum \alpha_r p_r + \alpha Tip(g)$ e $g' = \sum \beta_s {p'}_s + \beta Tip(g')$, então:

$$\begin{aligned} pgq &= pgq''(1/\beta)g'q' - pgq''(1/\beta)(g' - Tip(g'))q' \\ &= (\alpha/\beta)pTip(g)q''g'q' + \sum(\alpha_r/\beta)pp_rq''g'q' - \sum(\beta_s/\beta)pgq''{p'}_sq' . \end{aligned}$$

Logo, escrito pgq desta forma, podemos combinar seu Tip com o Tip de $p'g'q'$ e assim, diminue o número de ocorrências de $\overline{p}$, que contradiz a minimalidade assumida.

Caso 1.2.2: $\ell(p') < \ell(pTip(g))$

Então existe uma relação de sobreposição de $Tip(g)$ e $Tip(g')$ em $\overline{p}$. Digamos $Tip(g)r = sTip(g')$. Logo, $\overline{p} = pTip(g)rq' = psTip(g')q'$. Então

$$pgq = CTip(g)p\, o(g, g', s, r)q' + (CTip(g)/CTip(g'))p'g'q' .$$

Como $o(g, g', s, r) \Rightarrow_{\mathcal{G}} 0$, então

$$o(g, g', s, r) = \sum_{i=1}^{n} \sum_{j=1}^{m_i} u_{ij} g_i v_{ij} ,$$

onde $Tip(u_{ij}g_iv_{ij})$ é menor que $Tip(g)r = sTip(g')$, para todo i, j.

Desse modo,

$$pgq + p'g'q' = pgrq' - \left(\frac{CTip(g)}{CTip(g')}\right) psg'q' + \left(\frac{CTip(g)}{CTip(g')}\right) p'g'q' + p'g'q' .$$

De acordo com as relações assumidas acima, temos que $\overline{p}$ ocorre em $pgrq'$, $psg'q'$ e $p'g'q'$, que contradiz a minimalidade assumida.

Caso 2: $\ell(p) = \ell(p')$

Então $Tip(g)$ divide $Tip(g')$, ou vice-versa, que contradiz a hipótese de Tip reduzido em $\mathcal{G}$.

Caso 3: $\ell(p) > \ell(p')$

Como no Caso 1. ∎

Uma aplicação desse último resultado está no próximo algoritmo, que é o análogo não comutativo do algoritmo de Buchberger [6] para construção de bases de Gröbner.

Dado $I = \langle f_1, \cdots, f_n \rangle$, $f_i \in \Lambda$, uniformes, para todo $1 \leq i \leq n$ e Tip reduzidos, o algoritmo produz uma sequência, possivelmente infinita, de elementos Tip reduzidos e uniformes. Além disso, a sequência $\mathcal{G}$ obtida, é um conjunto gerador de I onde toda relação de sobreposição se reduz a zero sobre $\mathcal{G}$. Portanto, pelo teorema anterior, $\mathcal{G}$ é uma base de Gröbner para I. Apresentamos abaixo o algoritmo em pseudo-código.

Construção de base de Gröbner

INPUT: $f_1, \cdots, f_n$

OUTPUT: $g_1, g_2, g_3, \cdots$

PARA $i = 1$ ATÉ n FAÇA

  $g_i := f_i$

$\mathcal{G} := \{g_1, \cdots, g_n\}$

Count $:= n$

FAÇA

$\mathcal{H} := \mathcal{G}$

PARA *cada par de elementos* $h, k \in \mathcal{H}$ *e*

cada relação de sobreposição de h, k FAÇA

SE $o(h,k,p,q) \Rightarrow_{\mathcal{H}} r$ E $r \neq 0$ FAÇA

Count := Count + 1

$g_{\text{Count}} = r$

$\mathcal{G} := \mathcal{G} \cup \{g_{\text{Count}}\}$

ENQUANTO $Tip(g_i) = uTip(g_j)v$, com $i \neq j$ e $u, v \in \mathcal{B}$

FAÇA

$g_i := g_i - ug_jv$

ENQUANTO $(\mathcal{H} \neq \mathcal{G})$

Lema 2.21 *Utilizando a notação usada no algoritmo. Se* $b \in \mathcal{B}$ *é um gerador monomial minimal de* I_{MON}*, então para algum* m *inteiro,* $Tip(g_m) = b$▮

Proposição 2.22 *Se* I_{MON} *tem um conjunto finito de geradores monomiais, então o algoritmo acima termina em um número finito de passos e fornece uma base de Gröbner finita.*

Prova. Seja $\mathcal{T} = \{t_1, \cdots, t_s\}$ o conjunto gerador monomial minimal de I_{MON}.

Assim, pelo lema anterior, $\mathcal{T} \subset \{Tip(g_1), \cdots, Tip(g_N)\}$, para N suficientemente grande. Logo $Tip(\{g_1, \cdots, g_N\})$ gera I_{MON} sendo portanto uma base de Gröbner para I.

Como toda relação de sobreposição está em I, $o(g_i, g_j, p, q) \Rightarrow_{\{g_1, \cdots, g_N\}} 0$. Logo o algoritmo termina em um número finito de passos. ▮

Exemplo. Nem todo ideal I possui uma base de Gröbner finita, mesmo que I seja finitamente gerado, como podemos ver abaixo:

Seja $\mathcal{Q}$ o quiver:

Seja $I = \langle f = xyx - xy \rangle$ ideal bilateral em $\mathcal{K}\mathcal{Q}$, cuja $\mathcal{K}$-base é o conjunto de todos os caminhos de $\mathcal{Q}$ e a ordem é o comprimento lexicográfica, com a lexicografia dada por $1 < x < y$.

Seja $\mathcal{G}_0 = \{f\}$. Note que, $o_1 = o(f, f, xy, yx) = xy^2x + xyxy$ e fazendo a divisão por $\mathcal{G}_0$, temos que $o_1 \Rightarrow_{\mathcal{G}_0} g_1 = -xy^2x + xy^2$ e $Tip(f)$ não divide $Tip(g_1)$. Calculamos então $o_2 = o(f, g_1, xy, y^2x) = -xy^3x + xyxy^2$, fazendo a divisão por $\mathcal{G}_1 = \mathcal{G}_0 \cup \{g_1\}$, obtemos $o_2 \Rightarrow_{\mathcal{G}_1} g_2 = -xy^3x + xy^3$, e observe que nem $Tip(f) = xyx$ e nem $Tip(g_1) = xy^2x$ dividem $Tip(g_2) = xy^3x$, acrescentamos então g_2 a $\mathcal{G}_1$, fazendo $\mathcal{G}_2 = \mathcal{G}_1 \cup \{g_2\}$. Continuando o processo, temos que $o_n = o(f, g_{n-1}, xy, y^nx) \Rightarrow_{\mathcal{G}_{n-1}} g_n = -xy^{n+1}x + xy^{n+1}$, sendo que nenhum dos Tip's anteriores divide $Tip(g_n)$. Podemos concluir então que, se utilizarmos o processo de construção de bases de Gröbner descrito acima encontraremos em $\mathcal{G}$ o conjunto de elementos cujo Tip's são da forma xy^nx, com $n \in \mathbb{N}$, e teremos portanto uma base de Gröbner infinita, pois para cada elemento em $Tip(\mathcal{G})$ temos um elemento em $\mathcal{G}$.

2.5 $\mathcal{K}$-álgebras de Dimensão Finita

Nesta seção voltaremos nossa atenção para as $\mathcal{K}$-álgebras de dimensão finita da forma Λ/I, onde Λ é uma $\mathcal{K}$-álgebra finitamente gerada, com uma base multiplicativa e uma ordem admissível nessa base, e I é um ideal bilateral de Λ. O que mais podemos dizer a respeito dessas álgebras?

Antes, lembremos que $I_{MON} = \langle Tip(I) \rangle$.

Lema 2.23 *Seja Λ uma $\mathcal{K}$-álgebra finitamente gerada e $\mathcal{B}$ uma $\mathcal{K}$-base multiplicativa de Λ. Então $\mathcal{B} \cup \{0\}$ é finitamente gerada como semigrupo.*

Prova. Seja $X = \{x_1, x_2, \cdots, x_n\}$ um conjunto gerador de Λ como $\mathcal{K}$-álgebra. Para cada $x_i \in X$, $1 \leq i \leq n$, temos $x_i = \sum_j \alpha_{ij} b_{ij}$, com $b_{ij} \in \mathcal{B}$ e $\alpha_{ij} \in \mathcal{K}$. Seja $\overline{\mathcal{B}} = \bigcup_{i=1}^{n} supp(x_i)$, é fácil ver que $\overline{\mathcal{B}}$ é finito.

$\overline{\mathcal{B}}$ gera $\mathcal{B} \cup \{0\}$ como semigrupo. Suponha, por contradição, que $\overline{\mathcal{B}}$ não gera $\mathcal{B} \cup \{0\}$ como semigrupo, daí existe $b \in \mathcal{B}$ tal que b não pode ser escrito como produto de elementos de $\overline{\mathcal{B}}$. Como X é gerador de Λ, temos

$$\begin{aligned} b &= \sum_i \beta_i x_{i_1}^{t_{i_1}} x_{i_2}^{t_{i_2}} \cdots x_{i_{r_i}}^{t_{i_{r_i}}} \\ &= \sum_i \beta_i (\sum_{j_1} \alpha_{i_1 j_1} b_{i_1 j_1})^{t_{i_1}} (\sum_{j_2} \alpha_{i_2 j_2} b_{i_2 j_2})^{t_{i_2}} \cdots (\sum_{j_{r_i}} \alpha_{i_{r_i} j_{r_i}} b_{i_{r_i} j_{r_i}})^{t_{i_{r_i}}} \end{aligned}$$

Note que, do lado direito da equação temos uma combinação linear de produtos de elementos de $\overline{\mathcal{B}}$, que por sua vez são elementos de $\mathcal{B} \cup \{0\}$.

Como b não é produto de elementos de $\overline{\mathcal{B}}$, então b não aparece do lado direito da equação. Assim, temos que b é uma combinação linear de elementos de $\mathcal{B} \setminus \{b\}$, uma contradição, pois $\mathcal{B}$ é uma base.

Portanto, $\overline{\mathcal{B}}$ gera $\mathcal{B} \cup \{0\}$ como semigrupo. ∎

Proposição 2.24 *Seja Λ uma $\mathcal{K}$-álgebra finitamente gerada com base multiplicativa $\mathcal{B}$ e ordem admissível $>$ nessa base. Suponha que I é um ideal tal que $dim_{\mathcal{K}}(\Lambda/I) = N$. Então I_{MON} tem um conjunto finito de geradores monomiais.*

Prova. Como Λ/I é isomorfo a $Span(NonTip(I))$, como espaço vetorial, segue que $NonTip(I)$ é um conjunto finito, pois é uma $\mathcal{K}$-base de $Span(NonTip(I))$.

Como Λ é finitamente gerada como $\mathcal{K}$-álgebra, temos que $\mathcal{B} \cup \{0\}$ é finitamente gerado como semigrupo (lema acima). Seja $X = \{b_1, \cdots, b_k\}$ gerador de $\mathcal{B} \cup \{0\}$, como semigrupo. Mostraremos que

$$\mathcal{D} = (\{bc : b \in X \text{ e } c \in NonTip(I)\} \cap Tip(I)) \cup (X \cap Tip(I))$$

contém o conjunto gerador de I_{MON}.

Suponha que t pertence ao conjunto gerador monomial minimal de I_{MON}. Se $t \in X$, nada temos a fazer. Suponha que $t \notin X$, então $t = b_{i_1} b_{i_2} \cdots b_{i_s}$, com $b_{i_j} \in X$ para todo $1 \leq j \leq s$. Pela minimalidade de t, temos que $b_{i_2} \cdots b_{i_s} \notin Tip(I)$. Logo $b_{i_2} \cdots b_{i_s} \in NonTip(I)$.

Portanto, fazendo $c = b_{i_2} \cdots b_{i_s}$, temos que $t = b_{i_1} c$. Como queríamos. ∎

Corolário 2.25 *Seja Λ uma $\mathcal{K}$-álgebra finitamente gerada com base multiplicativa $\mathcal{B}$ e uma ordem admissível $>$ em $\mathcal{B}$. Suponha que I é um ideal de Λ gerado por elementos uniformes e Λ/I de dimensão finita.*

Então I tem uma base de Gröbner finita uniforme com respeito a $>$ e pode ser calculado em um número finito de passos pelo algoritmo anterior.

∎

Capítulo 3

Bases de Gröbner e Álgebra de Caminhos

3.1 Por que Álgebras de Caminhos?

Nesta seção vamos ver um pouco mais sobre a relação entre as álgebras que admitem uma base multiplicativa com uma ordem admissível e as álgebras de caminhos.

E também por que o uso dessas álgebras é necessário para se estudar a teoria de bases de Gröbner. Na verdade, veremos que toda álgebra com unidade que admite uma base multiplicativa com uma ordem admissível é quociente de uma álgebra de caminhos. Os resultados encontrados nessa seção foram demonstrados por Green em [10].

Ainda aqui, $\mathcal{K}$ será um corpo e Λ uma $\mathcal{K}$-álgebra com uma base multiplicativa $\mathcal{B}$ e uma ordem admissível $>$ em $\mathcal{B}$.

Seja I um ideal de Λ gerado por elementos da forma $b, b_1 - b_2$, onde $b, b_1, b_2 \in \mathcal{B}$, tal ideal é denominado um *ideal 2-nomial.*

Para relembrar, seja X um conjunto. Se uma relação $\sim$ em X satisfaz:

(1) $x \sim x$, para todo $x \in X$.

(2) Se $x \sim y$, então $y \sim x$, para todo $x, y \in X$.

(3) Se $x \sim y$ e $y \sim z$, então $x \sim z$, para todo $x, y, z \in X$.

dizemos que $\sim$ é uma relação de equivalência.

Proposição 3.1 *Existe uma correspondência biunívoca entre o conjunto de relações de equivalência em $\mathcal{B} \cup \{0\}$ e ideais 2-nomiais.*

Prova. Seja $\sim$ uma relação de equivalência em $\mathcal{B} \cup \{0\}$. Definimos $I_\sim$ o ideal gerado por $b_1 - b_2$ se $b_1 \sim b_2$ e b se $b \sim 0$.

Por outro lado se I é um ideal 2-nomial, seja $\sim_I$ a relação de equivalência dada por

(i) $b_1 \sim_I b_2$ se $b_1 - b_2 \in I$

(ii) $b \sim_I 0$ se $b \in I$

∎

Chamamos a relação de equivalência $\sim$ em $\mathcal{B} \cup \{0\}$ correspondente a I por *relação associada* (a I).

Lema 3.2 *Seja I um ideal 2-nomial em Λ com relação associada $\sim_I$. Então $\sum_{i=1}^{r} \alpha_i b_i \in I$, com $\alpha_i \in \mathcal{K}$ e $b_i \in \mathcal{B}$, se, e somente se, para cada classe $[b]$ de $\sim_I$ temos $\sum_{b_i \in [b]} \alpha_i b_i \in I$.*

Prova. Considere $\sum_{i=1}^{r} \alpha_i b_i \in \Lambda$. Se para cada classe de equivalência $[b]$ a soma $\sum_{b_i \in [b]} \alpha_i b_i \in I$ é claro que $\sum_{i=1}^{r} \alpha_i b_i \in I$.

Suponha que $x = \sum_{i=1}^{r} \alpha_i b_i \in I$. Então $x = \sum_{j=1}^{s} \beta_j (b_j - b'_j) + \sum_{l=1}^{t} \gamma_l b_l$ com $b_j - b'_j, b_l \in I$.Podemos reescrever x como sendo:

$$\begin{aligned} x &= \sum_{i=1}^{r} \alpha_i b_i \\ &= \sum_{j=1}^{s} \beta_j b_j + \sum_{j=1}^{s} -\beta_j b'_j + \sum_{l=1}^{t} \gamma_l b_l \end{aligned}$$

Fixamos então uma classe $[b]$ e vemos que

$$\sum_{b_i \in [b]} \alpha_i b_i = \sum_{b_j, b'_j \in [b]} \beta_j (b_j - b'_j) + \sum_{b_l \in [b]} \gamma_l b_l.$$

O resultado segue a partir dessa observação. ∎

Teorema 3.3 *Suponha que S é uma $\mathcal{K}$-álgebra com base multiplicativa $\mathcal{C}$. Seja I ideal em S e $\pi : S \to S/I$ a projeção canônica.*

Seja $\mathcal{B}$ o conjunto dos elementos não nulos de $\pi(\mathcal{C})$. $\mathcal{B}$ é uma base multiplicativa de S/I se e somente se I é um ideal 2-nomial.

Prova. Primeiramente vamos mostar que se I é um ideal 2-nomial, então $\mathcal{B}$ é uma base multiplicativa.

Sejam $\pi(c_1), \pi(c_2) \in \pi(\mathcal{C})$. Então $\pi(c_1)\pi(c_2) = \pi(c_1 c_2) \in \pi(\mathcal{C})$ e $\pi(\mathcal{C}) = \mathcal{B} \cup \{0\}$.

Agora precisamos mostrar que $\mathcal{B}$ é uma $\mathcal{K}$-base de S/I, para isso é suficiente mostrar que os elementos de $\mathcal{B}$ são linearmente independentes.

Seja $\sum_{i=1}^{n} \alpha_i \pi(c_i) = 0$ com $\pi(c_i) \neq 0$ e distintos. Daí, $\sum_{i=1}^{n} \alpha_i c_i \in I$. Seja $\sim$ a relação em $\mathcal{C} \cup \{0\}$ associada a I.

Pelo lema 3.2, para cada classe de equivalência $[c]$, temos $\sum_{c_i \in [c]} \alpha_i c_i \in I$.

Se $c_i \in [c]$, então $\pi(c_i) = \pi(c)$. Logo os $c'_i s$ estão em diferentes classes de equivalência, pois $\pi(c_i)$ são distintos. Assim $\alpha_i c_i \in I$ e concluimos que ou

$c_i \in I$, o que não pode acontecer, pois estamos supondo $\pi(c_i) \neq 0$, ou $c_i \notin I$, o que implica em $\alpha_i = 0$.

Portanto $\mathcal{B}$ é uma base multiplicativa de S/I.

Agora vamos mostrar que se $\mathcal{B}$ é uma base multiplicativa de S/I, então I é um ideal 2-nomial.

Definimos a relação $\sim$ em $\mathcal{C} \cup \{0\}$ por $c \sim c'$ se $\pi(c) = \pi(c')$. É fácil ver que o ideal 2-nomial correspondente a $\sim$ (pela proposição 3.1) é I. E isto completa a prova. ∎

A partir desse ponto assumiremos que Λ é uma $\mathcal{K}$-álgebra com unidade, mas não que $1 \in \mathcal{B}$, a menos que este seja o único idempotente. Assim, $1 = \sum_{i=1}^{n} \alpha_i b_i$, com $\alpha_i \in \mathcal{K} \setminus \{0\}$ e b_i distintos em $\mathcal{B}$.

Lema 3.4 *O conjunto $\{b_1, \cdots, b_n\}$ é um conjunto de idempotentes ortogonais e cada $\alpha = 1$.*

Prova. Suponha que $b_i b_j \neq 0$ com $i \neq j$. Então $b_i b_j = b \in \mathcal{B}$. Assuma que $b \neq b_i$ (o caso em que $b \neq b_j$ é análogo). Então

$$b_i = b_i \cdot 1 = \sum_{j=1}^{n} \alpha_j b_i b_j.$$

Assim, existe algum $l \neq j$ tal que $b_i b_l = b$, pois $b = b_i b_j$ deve ser cancelado por algum $b_i b_l$. Agora, ou $b_l > b_j$ ou $b_j > b_l$, mas em nenhum caso podemos ter $b_i b_l = b_i b_j = b$, pela ordem assumida. Portanto se $i \neq j$ tem-se $b_i b_j = 0$.

Logo $b_i = \alpha b_i b_i = \alpha b_i$ e portanto $\alpha = 1$. ∎

Proposição 3.5 *Se b_i e b_j são elementos distintos de $\{b_1, \cdots, b_n\}$, então para todo $b \in \mathcal{B}$, $b_i b = b_j b$ implica $b_i b = b_j b = 0$ e $b b_i = b b_j$ implica $b b_i = b b_j = 0$.*

Prova. Pelo Lema acima, b_i e b_j são idempotentes ortogonais, logo $b_i = b_i b_i$ e $b_i b_j = b_j b_i = 0$. Assim,

$$b_i b = b_j b \Longrightarrow b_i b = b_i b_i b = b_i b_j b = 0$$

e

$$b b_i = b b_j \Longrightarrow b b_i = b b_i b_i = b b_j b_i = 0$$

∎

Como podemos observar, o conjunto de idempotentes $\{b_1, \cdots, b_n\}$ tais que $1 = \sum_{i=1}^{n} b_i$ são elementos muito especiais de $\mathcal{B}$. Para distinguí-los, escreveremos $1 = \sum_{i=1}^{n} v_i$ com b_i substituidos pelos v_i.

Proposição 3.6 *Se $b \in \mathcal{B}$ então existem únicos i, j tais que $v_i b = b$ e $b v_j = b$. Se $k \neq i$, então $v_k b = 0$. Se $k \neq j$, então $b v_k = 0$.*

Prova. Como $b = b \cdot 1 = \sum_{i=1}^{n} b v_i$, concluimos que $b v_j = b$ para algum j. Mas se $k \neq j$, como $v_j v_k = 0$, $b v_k = 0$. De forma análoga se mostra a segunda parte do resultado. ∎

Se $b \in \mathcal{B}$, definimos v_i como sendo a *origem de* b, $o(b) = v_i$, se $v_i b = b$. Da mesma forma, definimos v_j por *término de* b, $t(b) = v_j$, se $b v_j = b$.

O próximo resultado mostra que os $v_i's$ tem a propriedade de minimalidade com respeito à ordem $>$.

Lema 3.7 *Se $b \in \mathcal{B}$ tal que $o(b) = v$ ou $t(b) = v$, então $b \geq v$.*

Prova. Suponha que $o(b) = v$, assim $vb = b$, como v é idempotente, temos $vvb = b$, no entanto a ordem que estamos assumindo é admissível, segue que $b \geq v$. ∎

Corolário 3.8 *Se $b \in \mathcal{B} \setminus \{v_1, \cdots, v_n\}$, então $b^2 \neq b$.*

Prova. Se $b^2 = 0$ nada temos a fazer. Suponha que $b^2 \neq 0$, então $o(b) = t(b) = v$, pelo lema acima temos que $v < b$, utilizando a propriedade da ordem ser admissível, temos $b = bv < bb$. ∎

Lema 3.9 *O conjunto $\mathcal{Q}_0 = \{v_1, \cdots, v_n\}$ é um conjunto completo de idempotentes primitivos ortogonais para Λ.*

Prova. Já temos visto que $\mathcal{Q}_0$ é um conjunto completo de idempotentes ortogonais, falta apenas mostar que ele é um conjunto primitivo.

Suponha, por absurdo, que $\mathcal{Q}_0$ não é um conjunto primitivo.

Seja $v_i = x + y$ para algum $i \in \{1, \cdots, n\}$, onde x e y são idempotentes ortogonais não nulos.

Agora, $x = \sum \alpha_j v_j + \sum \beta_l b_l$, com $\alpha, \beta \in \mathcal{K}$ e $b_l \in \mathcal{B}$.

Como $v_i = v_i x v_i + v_i y v_i$, vemos que $\alpha_j = 0$ se $i \neq j$ e que se $\beta_l \neq 0$, então $o(b_l) = v_i = t(b_l)$. Logo,

$$x = \alpha_i v_i + \sum \beta_l b_l$$

e

$$y = (1 - \alpha_i) v_i - \sum \beta_l b_l$$

Como $xy = 0$ e $b_l b_j \neq v_i$, concluimos que $\alpha_i(1 - \alpha_i) = 0$.

Daí, podemos assumir que $\alpha_i = 1$. Seja b o menor b_l ocorrendo em $\sum \beta_l b_l$.

Novamente usando que $xy = 0$, $v_i b = b$ e que b é menor que todos os produtos $b_l b_k$ não nulos, vemos que em xy não se pode cancelar $v_i b$. Logo, todos os $\beta_l = 0$. E isto completa a prova. ∎

Definição. 3.10 *Seja $\mathcal{Q}_1 = \{b \in (\mathcal{B} \setminus \mathcal{Q}_0) : b$ não pode ser escrito como produto $b_1 b_2$ com $b_1, b_2 \in \mathcal{B} \setminus \mathcal{Q}_0\}$, ou seja, $\mathcal{Q}_1$ é o conjunto dos elementos indecomponíveis de $\mathcal{B}$.*

Proposição 3.11 *Seja Λ uma $\mathcal{K}$-álgebra com base multiplicativa $\mathcal{B}$ e uma ordem admissível $>$ em $\mathcal{B}$. Se $\mathcal{Q}_0$ e $\mathcal{Q}_1$ são os únicos subconjuntos de $\mathcal{B}$ definidos por $1 = \sum_{v \in \mathcal{Q}_0} v$ e $\mathcal{Q}_1$ são os elementos indecomponíveis de $\mathcal{B} \setminus \mathcal{Q}_0$, então todo $b \in \mathcal{B} \setminus \mathcal{Q}_0$ é produto $b_1 \dots b_r$ com $b_i \in \mathcal{Q}_1$. Em particular, $\mathcal{Q}_0 \cup \mathcal{Q}_1$ gera a base multiplicativa $\mathcal{B}$, como semigrupo.*

Prova. Seja $b \in \mathcal{B} \setminus \mathcal{Q}_0$, se $b \in \mathcal{Q}_1$ nada temos que fazer. Suponha que $b \notin \mathcal{Q}_0 \cup \mathcal{Q}_1$, então $b = b_1 b_2$ para algum $b_1, b_2 \in \mathcal{B} \setminus \mathcal{Q}_0$. Como $b = o(b_1) b_1 b_2$ e $b = b_1 b_2 t(b_2)$, vemos que $b > b_1$ e $b > b_2$, pela ordem assumida.

Se $b_1, b_2 \in \mathcal{Q}_1$ terminamos aqui a demonstração. Se não, continuamos o processo obtendo $b_i = b_{i_1} \dots b_{i_n}$, com $b_{i_j} \in \mathcal{B} \setminus \mathcal{Q}_0$.

Como a ordem $>$ é total, temos uma cadeia descendente $b > b_{i_{s_1}} > \cdots$. Mas $>$ é uma boa ordem, logo esse processo estabiliza (teorema 1.12), isto é, cada b_{i_j} é um produto finito de elementos de $\mathcal{Q}_0 \cup \mathcal{Q}_1$, terminando assim a prova. ∎

Agora, seja $\mathcal{Q}$ o quiver com conjunto de vértices $\mathcal{Q}_0$ e conjunto de flechas $\mathcal{Q}_1$, isto é, se $b \in \mathcal{Q}_1$, o vemos como sendo uma flecha de origem $o(b)$ e término $t(b)$. Chamamos $\mathcal{Q}$ o quiver associado a $\mathcal{B}$.

Teorema 3.12 *Seja Λ uma $\mathcal{K}$-álgebra com uma base multiplicativa $\mathcal{B}$ e uma ordem admissível $>$ em $\mathcal{B}$. Seja $\mathcal{Q}$ o quiver associado a $\mathcal{B}$. Então existe um epimorfismo de $\mathcal{K}$-álgebras*

$$\varphi : \mathcal{K}\mathcal{Q} \to \Lambda$$

tal que:

(i) Se p é um caminho em $\mathcal{Q}$, então $\varphi(p) \in \mathcal{B} \cup \{0\}$.

(ii) Se $b \in \mathcal{B}$, então existe um caminho $p \in \mathcal{Q}$ tal que $\varphi(p) = b$.

(iii) O núcleo de φ é um ideal 2-nomial.

Prova. Seja Λ uma $\mathcal{K}$-álgebra com uma base multiplicativa $\mathcal{B}$ e ordem admissível $>$ nessa base. Temos visto que existem únicos subconjuntos $\mathcal{Q}_0$ e $\mathcal{Q}_1$ de $\mathcal{B}$. Além disso, pelo lema 3.9, $\mathcal{Q}_0$ é um conjunto completo de idempotentes primitivos ortogonais. Seja $\mathcal{Q}$ o quiver associado a Λ.

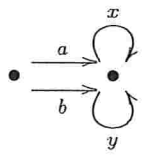
Definimos o homomorfismo de álgebras $\varphi : \mathcal{K}\mathcal{Q} \to \Lambda$, enviando os vértices v de $\mathcal{Q}$ ao seu correspondente em $\mathcal{Q}_0 \subset \mathcal{B}$ e as flechas de $\mathcal{Q}$ no elemento correspondente em $\mathcal{Q}_1 \subset \mathcal{B}$. Por construção, caminhos de $\mathcal{Q}$ são enviados a elementos de $\mathcal{B} \cup \{0\}$ e pela proposição 3.11, temos que φ é sobrejetiva.

Note que a imagem da base multiplicativa dos caminhos de $\mathcal{Q}$ pela φ é $\mathcal{B} \cup \{0\}$. Assim, pelo teorema 3.3, concluimos que o núcleo de φ é um ideal 2-nomial de $\mathcal{Q}$, completando assim a prova. ∎

Sabemos que dada uma $\mathcal{K}$-álgebra Λ com uma base $\mathcal{B}$ multiplicativa e uma ordem admissível $>$ em $\mathcal{B}$, existe um quiver $\mathcal{Q}$ tal que $\Lambda = \mathcal{K}\mathcal{Q}/I$, onde I é um ideal 2-nomial. Surge então a seguinte pergunta: *quais as condições necessárias e suficientes sobre o ideal 2-nomial I, para o quociente de álgebra de caminhos $\mathcal{K}\mathcal{Q}/I$ tenha uma base $\mathcal{B}$ multiplicativa com uma ordem admissível $>$?*

O que se sabe até agora é que a afirmativa não vale em geral para todos os ideais 2-nomiais, como podemos ver no exemplo abaixo:

Exemplo. Seja $\mathcal{Q}$ o seguinte quiver:



Seja o ideal 2-nomial $I =< ax^n - b, a - by^m : m, n \in \mathbb{N}^* >$. Considere em $\Lambda = \mathcal{K}\mathcal{Q}$ a $\mathcal{K}$-base formada por todos os caminhos de $\mathcal{Q}$. Para Λ/I definimos a seguinte $\mathcal{K}$-base $\overline{\mathcal{B}} = \mathcal{B} \setminus \{bx^n, ay^m, ax^n, by^m, ax^n y^m, by^m x^n : m, n \in \mathbb{N}^*\}$.

Suponha que $\overline{\mathcal{B}}$ tenha uma ordem admissível e que $a > b$. Como $x < xy$,

multiplicamos pela esquerda por a, e obtemos a seguinte relação:

$$\begin{aligned} a(x) &< a(xy) \\ b &< (ax)y \\ b &< by \\ b &< a \end{aligned}$$

O que não poderia acontecer em tal ordem.

A opção que nos resta é $a < b$, no entanto se tomarmos a relação $y < xy$ e multiplicarmos pela esquerda por a chegaremos ao absurdo de que $b < a$. Portanto, para este quociente é impossível se definir uma ordem admissível.

3.2 Homogeneização

Em [3] é apresentado o processo de homogeneização para o caso comutativo, no anel de polinômios com n variáveis.

Sabendo que o anel de polinômios em n variáveis comutativas é um caso particular das álgebras de caminhos e que toda álgebra com unidade com a teoria de bases de Gröbner é isomorfa ao quociente de uma álgebra de caminhos, teorema 3.12, veio-nos a pergunta se o mesmo processo, e também quais os resultados, podia-se aplicar às álgebras de caminhos. Nesta seção procuramos responder a esta pergunta com a versão, do caso não comutativo, para as álgebras de caminhos $\mathcal{K}\mathcal{Q}/I$, onde I é um ideal bilateral de $\mathcal{K}\mathcal{Q}$.

Sejam $\mathcal{K}$ um corpo e Q um quiver finito. Seja $\Lambda = \mathcal{K}Q/I$ a álgebra de caminhos associada a Q e I um ideal bilateral de $\mathcal{K}Q$. Considere em Λ uma base multiplicativa $\mathcal{B}$ e $>$ uma ordem admissível em $\mathcal{B}$.

Definimos então $\tilde{Q}$ acrescentando a Q um laço em cada vértice e a partir daí a $\mathcal{K}$-álgebra $\Lambda' = \mathcal{K}\tilde{Q}/\tilde{I}$, onde $\tilde{I} = \langle I, \alpha Z - Z\alpha \rangle$ como ideal bilateral de $\mathcal{K}\tilde{Q}$, $\alpha \in \mathcal{Q}_1$ e $Z = \sum_{i \in |Q_0|} l_i$, aqui l_i representa cada um dos novos laços acrescidos a Q. Chamaremos Λ' *a álgebra extendida por laços* de Λ.

Tomamos para Λ' a seguinte base $\tilde{\mathcal{B}} = \{Z^n b : b \in \mathcal{B} \ e \ n \geq 0\}$.

Tanto Λ quanto Λ' são finitamente geradas como $\mathcal{K}$-álgebras, logo $\mathcal{B}$ e $\tilde{\mathcal{B}}$ são finitamente gerados como semigrupos.

Assim, fixemos para $\mathcal{B}$ um conjunto gerador minimal U, como semigrupo. Para $\tilde{\mathcal{B}}$, tomemos $\tilde{U} = U \cup \{l_i : i \in |\mathcal{Q}_0|\}$.

Definimos por $\ell(b)$ o *comprimento* de $b \in \mathcal{B}$ (respectivamente $\tilde{\mathcal{B}}$) o menor $n \in \mathbb{N}$ tal que $b = b_1 b_2 \cdots b_n$ com $b_i \in U$ (respectivamente $\tilde{U}$). Em $f \in \Lambda$ (Λ'), definimos o *comprimento* de f por $\ell(f) = \max\{\ell(b) : b \in \mathcal{B}(\tilde{\mathcal{B}}) \ ocorra \ em \ f\}$. Diremos que um elemento $f = \sum_{i=1}^{n} \lambda_i b_i$, com $\lambda_i \in \mathcal{K}$ e $b_i \in \mathcal{B}\,(\tilde{\mathcal{B}})$, é *homogêneo* se $\ell(f) = \ell(b_i)$ para todo $1 \leq i \leq n$.

Um ideal I é *homogêneo* se pode ser gerado por elementos homogêneos.

Definimos em $\tilde{\mathcal{B}}$ a ordem

$$e_i \prec l_j \prec b, \text{ para todo } i, j \in |\mathcal{Q}_0| \text{ e } b \in \mathcal{B} \text{ e}$$

$$Z^n b_1 \prec Z^m b_2 \text{ se : } \begin{cases} \text{se } b_1 < b_2 \text{ em } \mathcal{B} \text{ ou} \\ \text{se } b_1 = b_2 \text{ em } \mathcal{B} \text{ e } n < m \end{cases}$$

Vamos mostrar que a ordem acima é de fato uma ordem admissível. Sejam $Z^n b_1, Z^m b_2, Z^r b_3, Z^s b_4 \in \tilde{\mathcal{B}}$, então:

(1) se $Z^n b_1 \prec Z^m b_2$ e $Z^n b_1 Z^r b_3$ e $Z^m b_2 Z^r b_3$ são não nulos, temos que, se $b_1 < b_2$ então $b_1 b_3 < b_2 b_3$. Agora, se $b_1 = b_2$, $n < m$ e portanto $b_1 b_3 = b_2 b_3$ e $n + r < m + r$. Assim, $Z^n b_1 Z^r b_3 \prec Z^m b_2 Z^r b_3$.

(2) da mesma forma, se $Z^n b_1 \prec Z^m b_2$, então $Z^r b_3 Z^n b_1 \prec Z^r b_3 Z^m b_2$, se os produtos são não nulos.

(3) se $Z^n b_1 = Z^m b_2 Z^r b_3 Z^s b_4 = Z^{m+r+s} b_2 b_3 b_4$, temos que $r \leq n$ e $b_3 \leq b_1$ logo $Z_r b_3 \preceq Z^n b_1$.

Portanto a ordem $\prec$ definida acima é uma ordem admissível.

Definição. 3.13 *Para $f = \sum_{i=1}^{m} \lambda_i b_i \in \Lambda$, definimos o homogeneizado de f em Λ' por $f^* = \sum_{i=1}^{m} \lambda_i Z^{\ell(f)-\ell(b_i)} b_i$.*

Note que, para todo $f \in \Lambda$, o homogeneizado de f é homogêneo.

Lema 3.14 *Para todo $f, g \in \Lambda$, temos $Z^k (fg)^* = f^* g^*$, onde $k = \ell(f) + \ell(g) - \ell(fg)$.*

Prova. Sejam $f = \sum_{i=1}^{n} \lambda_i b_i$ e $g = \sum_{j=1}^{m} \beta_j b_j$, com $\lambda_i, \beta_j \in \Lambda$ e $b_i, b_j \in B$. Como $\ell(f) + \ell(g) \geq \ell(fg)$, tomamos $k = \ell(f) + \ell(g) - \ell(fg)$. Daí,

$$\begin{aligned}
f^* g^* &= (\sum_{i=1}^{n} \lambda_i b_i)^* (\sum_{j=1}^{m} \beta_j b_j)^* \\
&= (\sum_{i=1}^{n} \lambda_i Z^{\ell(f)-\ell(b_i)} b_i)(\sum_{j=1}^{m} \beta_j Z^{\ell(g)-\ell(b_j)} b_j) \\
&= \sum_{i,j} \lambda_i \beta_j Z^{(\ell(f)+\ell(g))-(\ell(b_i)+\ell(b_j))} b_i b_j \\
&= \sum_{i,j} \lambda_i \beta_j Z^{\ell(fg)-\ell(b_i b_j)} Z^k b_i b_j \\
&= Z^k (\sum_{i,j} \lambda_i \beta_j b_i b_j)^* \\
&= Z^k ((\sum_{i=1}^{n} \lambda_i b_i)(\sum_{j=1}^{m} \beta_j b_j))^* \\
&= Z^k (fg)^*
\end{aligned}$$

∎

Definimos agora a seguinte aplicação entre as álgebras Λ' e Λ:

$$\varphi : \Lambda' \to \Lambda$$

que a cada elemento $Z^n b \in \tilde{\mathcal{B}}$ associa o elemento $b \in \mathcal{B}$, para todo $n \in \mathbb{N}$. Note que, para cada $b \in \mathcal{B}$, existe $Zb \in \tilde{\mathcal{B}}$ tal que $\varphi(Zb) = b$. Dessa forma, temos que φ estendida por linearidade a toda Λ' é de fato um epimorfismo de álgebras. Note que $\varphi(\sum_{i=1}^{n} Z^{k_i} e_i) = 1$, para todo $k_i \in \mathbb{N}$ e que $ker(\varphi) = \langle Z - 1 \rangle$.

Para simplificar a notação, usaremos $g_* = \varphi(g)$ para todo $g \in \Lambda'$.

Lema 3.15 *Para todo $f \in \Lambda$ temos $(f^*)_* = f$.*

Prova. Seja $f = \sum_{i=1}^{n} \lambda_i b_i$, com $\lambda_i \in \Lambda$ e $b_i \in \mathcal{B}$. Note que

$$\begin{aligned}
(f^*)_* &= (\sum_{i=1}^{n} \lambda_i Z^{\ell(f)-\ell(b_i)} b_i)_* \\
&= \sum_{i=1}^{n} (\lambda_i Z^{\ell(f)-\ell(b_i)} b_i)_* \\
&= \sum_{i=1}^{n} \lambda_i (Z^{\ell(f)-\ell(b_i)}))_* (b_i)_* \\
&= \sum_{i=1}^{n} \lambda_i b_i \\
&= f
\end{aligned}$$

∎

Lema 3.16 *Seja $g \in \Lambda'$ homogêneo de comprimento d e seja $d' = \ell(g_*)$. Então $d' \leq d$ e $g = Z^{d-d'}(g_*)^*$.*

Prova. A desigualdade $d' \leq d$ é imediata da definição de g_*. Seja $m \in supp_{\tilde{\mathcal{B}}}(g)$, $m = tZ^i$, com $t \in \mathcal{B}$. Assim o monômio $m_* \in supp_{\mathcal{B}}(g_*)$ correspon-

dente a m é t. Como $\ell(t) = d - i$ o monômio em $supp((g_*)^*)$ correspondente a m_* é $tZ^{d'-(d-i)}$. Logo $Z^{d-d'}(g_*)^* = g$. ∎

Definição. 3.17 *Sejam $F \subset \Lambda$ e $\mathcal{G} \subset \Lambda'$, definimos por*

$$F^* = \{f^* : f \in F\}$$

$$\mathcal{G}_* = \{g_* : g \in \mathcal{G}\}$$

Lema 3.18 *Seja $f \in \Lambda$. Então $\ell(f) = \ell(f^*)$.*

Prova. Considere $f = \sum_{i=1}^{m} \lambda_i b_i$ com $\lambda_i \in \mathcal{K}$ e $b_i \in \mathcal{B}$, base de Λ, $1 \leq i \leq m$.

Por definição temos que $f^* = \sum_{i=1}^{m} \lambda_i Z^{l(f)-l(b_i)} b_i$. Para todo somando de f^* temos:

$$\ell(Z^{\ell(f)-\ell(b_i)}b_i) = \ell(Z^{\ell(f)-\ell(b_i)}) + \ell(b_i) = (\ell(f) - \ell(b_i)) + \ell(b_i) = \ell(f)$$

Logo, $\ell(f^*) = \max\{\ell(Z^{\ell(f)-\ell(b_i)}b_i) : 1 \leq i \leq m\} = \ell(f)$ ∎

Lema 3.19 *Seja $F = \{f_i\}_{i\in\mathcal{I}}$ um subconjunto de Λ, não necessariamente finito, e $f = \sum_{i=1}^{m} r_i f_i s_i \in \langle F \rangle$. Se $d = \max\{\ell(r_i f_i s_i) : 1 \leq i \leq m\}$ e $d' = \ell(f)$. Então $Z^{d-d'} f^* \in \langle F^* \rangle$.*

Prova. Pelo Lema 3.18, temos que $d = \max\{\ell((r_i f_i s_i)^*) : 1 \leq i \leq m\}$. Tome $k_i = \ell(r_i) + \ell(f_i) + \ell(s_i) - \ell(r_i f_i s_i)$, $1 \leq i \leq m$.

Seja $\overline{f} = \sum_{i=1}^{m} Z^{d-\ell(r_i f_i s_i)} Z^{k_i} (r_i f_i s_i)^* = \sum_{i=1}^{m} (Z^{d-\ell(r_i f_i s_i)} r_i)^* f_i^* s_i^*$, pelo lema 3.14. Logo, $\overline{f} \in \langle F^* \rangle$ e é homogêneo (por construção) com $d'' = \ell(\overline{f}) \leq d$.

Além disso, usando o lema 3.14 e o lema 3.15, temos

$$\begin{aligned}\overline{f}_* &= \sum_{i=1}^{m}(Z^{d-\ell(r_i f_i s-i)}Z^{k_i}(r_i f_i s_i)^*)_* \\ &= \sum_{i=1}^{m}(Z^{d-\ell(r_i f_i s_i)})_*(r_i^*)_*(f_i^*)_*(s_i^*)_* \\ &= \sum_{i=1}^{m} r_i f_i s_i = f\end{aligned}$$

Usando o Lema 3.16, podemos concluir que

$$\overline{f} = Z^{d''-d'}(\overline{f}_*)^* = Z^{d''-d'}f^*$$

Como $d'' \leq d$, finalmente temos:

$$Z^{d-d'}f^* = Z^{d-d''}Z^{d''-d'}f^* = Z^{d-d''}\overline{f} \in \langle F^* \rangle$$

∎

Lema 3.20 *Seja F um subconjunto de Λ. Então $(\langle F^* \rangle)_* = \langle F \rangle$.*

Prova. Seja $f \in \langle F \rangle$. Pelo Lema 3.19, $Z^k f^* \in \langle F^* \rangle$, para algum $k \in \mathbb{N}$, e assim

$$f = (f^*)_* = (Z^k f^*)_* \in (\langle F^* \rangle)_*$$

Por outro lado, se $g \in \langle F^* \rangle$, digamos $g = \sum_{i=1}^{m} r_i (f_i)^* s_i$ com $f_i \in F$ e $r_i, s_i \in \Lambda'$ para $1 \leq i \leq m$, temos

$$\begin{aligned}g_* &= (\sum_{i=1}^{m} r_i (f_i)^* s_i)_* \\ &= \sum_{i=1}^{m}(r_i)_*[(f_i)^*]_*(s_i)_* \\ &= \sum_{i=1}^{m}(r_i)_* f_i (s_i)_*\end{aligned}$$

Logo, $g_* \in \langle F \rangle$. ∎

Teorema 3.21 *Seja F um subconjunto de Λ e seja $\mathcal{G} \subset \Lambda'$ homogêneo. Se $\mathcal{G}$ é uma base de Gröbner para $\langle F^* \rangle$, então $\mathcal{G}_*$ é uma base de Gröbner de $\langle F \rangle$.*

Prova. Suponha que $\mathcal{G}$ é uma base de Gröbner para $\langle F^* \rangle$. Vamos recorrer à definição de base de Gröbner.

Como $\mathcal{G}_* \subset \langle F \rangle$, então $\langle Tip(\mathcal{G}_*) \rangle \subseteq \langle Tip(\langle F \rangle) \rangle$, resta-nos verificar que $\langle Tip(\langle F \rangle) \rangle \subseteq \langle Tip(\mathcal{G}_*) \rangle$, ou seja, dado $f \in \langle F \rangle$ existe $g_* \in \mathcal{G}_*$ tal que $Tip(g_*)$ divide $Tip(f)$.

Seja $f \in \langle F \rangle$, podemos escrever $f = \sum_{i=1}^{m} \lambda_i b_i$, onde $\lambda_i \in \mathcal{K}$ e $b_i \in \mathcal{B}$ para $1 \leq i \leq m$.

Sem perda de generalidade, suponha que $Tip(f) = b_1$. Note que $\ell(b_1) = \ell(f)$, daí

$$f^* = \lambda_1 b_1 + \sum_{i=2}^{m} \lambda_i Z^{\ell(f)-\ell(b_i)} b_i$$

segue então pela ordem que $Tip(f^*) = b_1 = Tip(f)$.

Pelo lema 3.19, existe $k \in \mathbb{N}$ tal que $h = Z^k f^* \in \langle F^* \rangle$. Pela observação acima, $Tip(h) = Z^k Tip(f)$.

Como $\mathcal{G}$ é uma base de Gröbner para $\langle F^* \rangle$, existe $g \in \mathcal{G}$ tal que $Tip(h) = Z^{k_r} r Tip(g) Z^{k_s} s$, para algum $Z^{k_r} r, Z^{k_s} s \in \tilde{\mathcal{B}}$. $Tip(g) \in \tilde{\mathcal{B}}$, logo $Tip(g) = Z^{k_g} b$ para algum $b \in \mathcal{B}$ e $k_g \in \mathbb{N}$.

Daí, $Tip(h) = Z^k b_1 = Z^{k_r} r Tip(g) Z^{k_s} s = Z^{k_r} r Z^{k_g} b Z^{k_s} s = Z^{k_r + k_g + k_s} rbs$.

Por hipótese g é homogêneo, assim $Tip(g) = Z^{k_g} b$ é tal que, para todo $Z^t b_t \neq Tip(g)$ ocorrendo em g, temos que ou $k_g < t$ o que implica em $b > b_t$ e assim $Tip(g_*) = b$. Logo $Tip(f) = r Tip(g_*) s$, e assim $\mathcal{G}_*$ é uma base de Gröbner para $\langle F \rangle$. ∎

Referências Bibliográficas

[1] Assem, I., Simsom, D., Skowronski, A., *Representation Theory of Finite Dimensional Algebras*, preprint.

[2] Auslander, M., Reiten, I., Smalø, S., *Representation Theory of Artin Algebras*, vol 36 of Cambridge Studies in Advanced Mathematics, Cambridge University Press.

[3] Becker, T., Weispfenning, V., *Gröbner Bases, A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics, Springer-Verlag. 1993.

[4] Benson, B. J., *Representations and Cohomology*, Cambridge University Press. 1991.

[5] Bergman, G. M., *The Diamond Lemma for ring theory*, Adv. in Math. 29, 1978, 178-218.

[6] Buchberger, *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Ideal*, Ph.D. Thesis, University of Innsbruck, 1965.

[7] Farkas, D. R., Feustel, C. D., Green, E. L., *Synergy in the Theories of Gröbner Bases and Path Algebras*, Can. J. Math., 45, 1993, 727-739.

[8] Feustel, C. D., Green, E. L., Kirkman, E., Kuzmanovich, J., *Constructing Projective Resolutions*, Comm. in Alg., 21, 1993, 1869-1887

[9] Green, E. L., *Multiplicative Bases, Gröbner Bases, and Right Gröbner Bases*, J. Symbolic Computation, 29, 2000, n.4-5, 601-623.

[10] Green, E. L., *Noncommutative Gröbner Bases and Projectives Resolutions*, In Michler and Schneider, eds, Proceedings of the Euroconference Computational Methods for Representations of Groups and Algebras, Essen, 1997, vol. 173 of Progress in Mathematics, 29-60. Basel, Bikhaüser Verlag.