Universidade de São Paulo
Instituto de Matemática e Estatística
Departamento de Ciência da Computação

MAC-5701 – **Relatório de Estudo**

Alexey Antônio Villas Bôas, orientado
Profa. Dra. Alegria Gladys C. de Oliveira, orientadora

São Paulo, 25 de junho de 2002

Resumo

Este documento apresenta um resumo do trabalho realizado na matéria `MAC-5701`, contendo resultados apresentados em [2], [3] e [4]. Este trabalho foi criado a partir do estudo destes artigos e de apresentações semanais de seu conteúdo, o que sedimentou o aprendizado do aluno e levantou novas discussões sobre os tópicos em questão. Assistiram a estas apresentações a Profa. Dra. Alegria Gladys C. de Oliveira e o aluno de mestrado Peterson Pereira de Oliveira. Parte do conteúdo estudado durante o semestre (e presente neste trabalho) foi apresentado no Colóquio de Representações de Álgebras do IME-USP.

O trabalho tem o propósito de apresentar uma introdução à Teoria de Bases de Gröbner, explorando inicialmente aspectos relacionados a espaços vetoriais e ao anel de polinômios. Em seguida, o exemplo mais geral de álgebras é estudado e fornece-se uma justificativa do largo uso de Álgebras de Caminhos no estudo de Bases de Gröbner (mostrando que na realidade se trata de um exemplo universal). Finalmente, são apresentados algoritmos e processos computacionais relacionados com a Teoria de Bases de Gröbner.

Sumário

Capítulo 1

Preliminares

Este capítulo contém algumas definições e resultados que serão utilizados ao longo de todo o texto.

1.1 Álgebras, Monóides e Semigrupos

Nesta seção introduzimos algumas definições largamente utilizadas ao longo do texto. Primeiramente vejamos o conceito de **monóide**.

Definição 1.1.1 *(Monóide) Um* ***monóide*** *é uma tripla* $(M, ., 1)$*, onde* M *é um conjunto não vazio, . é uma operação binária associativa em* M *e 1 é um elemento de* M *tal que*

$$1.a = a = a.1$$

para todo $a \in M$*.*

Além de monóides, utilizaremos ao longo do texto o conceito de semigrupo. Um **semigrupo** é um monóide sem a hipótese de existência do elemento 1, isto é, ele consiste de um conjunto não vazio com uma operação binária associativa nesse conjunto.

Em seguida vejamos o conceito de **álgebra associativa**. Esse conceito é obtido combinando o de um anel com o de um espaço vetorial, como nos mostra a definição 1.1.2.

Definição 1.1.2 *(Álgebra Associativa) Uma* ***álgebra associativa*** *(sobre um corpo* K*) é um par consistindo de um anel* $(A, +, ., 0, 1)$ *e um espaço vetorial* A *sobre* K *tais que o conjunto* A*, a adição e o 0 são os mesmos no anel e no espaço vetorial e*

$$a(xy) = (ax)y = x(ay)$$

para $a \in K$*,* $x, y, \in A$*.*

Ao longo deste texto, todas as álgebra que tratarmos serão álgebras associativas sobre um corpo K, e as denominaremos apenas por "álgebras" ou "K-álgebras".

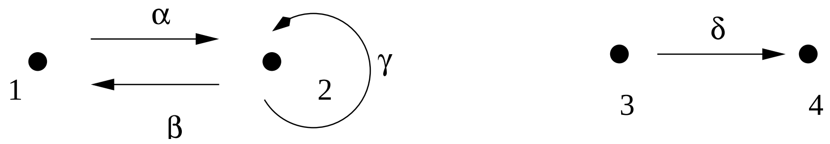
1.2 Carcazes

Nesta parte apresentaremos o conceito de álgebras de caminhos. Muitas das idéias aqui mostradas foram extraídas de [1].

Vejamos primeiro a definição de **carcaz**:

Definição 1.2.1 *Um **carcaz** Γ é dado por dois conjuntos, Γ_0, Γ_1, e um par de funções $s, e : \Gamma_0 \longrightarrow \Gamma_1$. Os elementos de Γ_0 são chamados de **vértices**, enquanto os de Γ_1 de **flechas**. Dada uma flecha $\alpha \in \Gamma_1$, $s(\alpha)$ é o **vértice inicial** de α e $e(\alpha)$ é o **vértice final** de α.*

Podemos representar carcazes de uma forma gráfica:



No exemplo acima, temos $\Gamma_0 = \{1, 2, 3, 4\}$ e $\Gamma_1 = \{\alpha, \beta, \gamma\}$. Temos ainda que $s(\alpha) = e(\beta) = 1$, $s(\beta) = e(\alpha) = s(\gamma) = e(\gamma) = 2$, $s(\delta) = 3$ e $e(\delta) = 4$.

Um **caminho** γ em $\Gamma = (\Gamma_0, \Gamma_1, s, e)$ é descrito da seguinte forma: $\gamma = \alpha_1\alpha_2 \cdots \alpha_n$, onde $1 \leq i \leq n-1, e(\alpha_i) = s(\alpha_{i+1})$. O número de flechas nesse caminho γ será denotado por $l(\gamma)$ e chamado de **comprimento de** γ (no exemplo $l(\gamma) = n$). Por convenção um caminho de comprimento zero (também chamado **caminho trivial**) é um caminho sem flechas, associado a um vértice $\alpha \in \Gamma_0$.

Dado um caminho $\gamma = \alpha_1\alpha_2 \cdots \alpha_n$ denotaremos por $s(\gamma) = s(\alpha_1)$ e por $e(\gamma) = e(\alpha_n)$. No caso em que γ não é um caminho trivial e $s(\gamma) = e(\gamma)$, diremos que γ é um **circuito orientado**.

1.3 Álgebras de Caminhos

Seja K um corpo. Seja ainda $\Gamma = (\Gamma_0, \Gamma_1, s, e)$ um carcaz finito, isto é, onde os conjuntos Γ_0 e Γ_1 são finitos. A partir de K e Γ definiremos uma álgebra $K\Gamma$. Primeiramente, consideremos $\mathcal{B}$ o conjunto de todos os caminhos. Note que os vértices também estão incluídos em $\mathcal{B}$ através dos caminhos de comprimento zero (triviais). Considere $K\Gamma$ como sendo o K-espaço vetorial com base $\mathcal{B}$. Para transformarmos $K\Gamma$ numa álgebra, precisamos definir uma multiplicação em $\mathcal{B}$. O produto em $\mathcal{B}$ será definido por concatenação da seguinte forma. Sejam $\alpha, \beta \in \mathcal{B}$ então

$$\alpha\beta = \begin{cases} \text{o caminho } \alpha\beta, \text{ se } e(\alpha) = s(\beta). \\ 0, \text{ caso contrário.} \end{cases}$$

Estendendo por linearidade essa multiplicação a todos os elementos, temos uma estrutura de álgebra bem definida em $K\Gamma$. A álgebra $K\Gamma$ definida como acima é chamada de **álgebra de caminhos**.

1.4 Ordens

Ao longo de todo o texto trabalharemos com uma boa ordem na base $\mathcal{B}$ definida na seção anterior.

Definição 1.4.1 ***(Boa Ordem)*** *Um conjunto não vazio parcialmente ordenado X é dito **bem-ordenado** se todo subconjunto não vazio de X tem um menor elemento.*

Note que como conseqüência toda boa-ordem é uma ordem total.

São exemplos de boas ordens (em uma álgebra de caminhos):

1. A ordem de comprimento-lexicografia (à esquerda).

Basta ordenar os vértices e flechas arbitrariamente, contanto que os vértices sejam menores que as flechas. Então se $p = b_1 \cdots b_r$ e $q = b'_1 \cdots b'_j$ $(b_i, b'_k \in \mathcal{B})$ são caminhos de comprimento maior ou igual a 1, definimos $p < q$ se $l(p) < l(q)$ ou, se $l(p) = l(q)$, existe $1 \leq i \leq r$ tal que $b_k = b'_k, 1 \leq k < i$ e $b_i < b'_i$.

2. A ordem de peso-lexicografia (à esquerda).

   Seja W uma função peso definida da seguinte forma: $W : \Gamma_1 \longrightarrow \{1, 2, 3, \ldots\}$. Seja ainda $W : \mathcal{B} \longrightarrow \{1, 2, 3, \ldots\}$ sua extensão natural; isto é, $W(v) = 0$ se v é um vértice e se $a_i \in \Gamma_1$ defina $W(a_1 \cdots a_r) = \sum_{i=1}^{r} W(a_i)$. Em seguida ordene os vértices e flechas, de forma que os vértices sejam menores que as flechas. Ordene as flechas de forma que se $W(a) < W(b)$ então $a < b$. Por fim, defina que $p < q$ se $W(p) < W(q)$ e se $W(p) = W(q)$, utilize a ordem de comprimento-lexicografia.

Outro exemplo que podemos tomar é a ordem de grau e lexicografia, para o anel de polinômios $K[x_1, \ldots, x_n]$:

1. Basta ordenar as variáveis arbitrariamente (desde que elas sejam maiores que o 1). Suponha, sem perda de generalidade que $1 < x_1 < \cdots < x_n$. Então, se $p = x_1^{f_1} x_2^{f_2} \cdots x_n^{f_n}$ e $q = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ definimos $p < q$ se

   $\sum_{i=1}^{n} f_i < \sum_{i=1}^{n} e_i$ ou
   $\sum_{i=1}^{n} f_i = \sum_{i=1}^{n} e_i$ e existe $1 \leq j \leq n$ tal que $f_i = e_i$ para $i < j$ e $f_j < e_j$.

Capítulo 2

Introdução a Bases de Gröbner

2.1 Bases de Gröbner Lineares

Iniciamos com uma lista de definições que serão utilizadas ao longo desta seção. Assume-se que K é um corpo e $V = K^n$ um espaço vetorial (de dimensão finita) sobre K. Seja $\mathcal{B} = \{b_1, \dots b_n\}$ base de V. Ordenamos os elementos de $\mathcal{B}$ da seguinte forma:

$$b_n < b_{n-1} < \cdots < b_2 < b_1 \text{ (chamada de ordem reversa (\textit{reverse order}))}$$

Chamaremos essa boa ordem de $\leq$.

Seja $v \in V$. Então, v se escreve de forma única como $v = \sum_{i=1}^{n} \alpha_i b_i$ com $b_i \in \mathcal{B}$.

Definição 2.1.1 *(**Tip**) Seja $v \in V$ e $v = \sum_{i=1}^{n} \alpha_i b_i$ com $b_i \in \mathcal{B}$. Dizemos que b_i **ocorre** em v se $\alpha_i \neq 0$. Dizemos ainda que*

$$supp(v) = \{b_i \in B \mid \alpha_i \neq 0\}$$

$Tip(v)$ é o elemento maximal de $supp(v)$.

Seja ainda $X \subseteq V$ um subconjunto. $Tip(X)$ é o conjunto de todos os elementos b de $\mathcal{B}$ tais que existe $x \in X$ com $Tip(x) = b$. Além disso, $B \setminus Tip(X) = Nontip(X)$.

Definição 2.1.2 *(**Sharp**) Um vetor $x \in X \subseteq V$ é **sharp em** X se as seguintes condições são satisfeitas:*

- *O coeficiente de $Tip(x)$ (denotado por $CTip(x)$) é 1*
- *$supp(x) \setminus \{Tip(x)\} \subseteq Nontip(X)$.*

$$Sharp(X) = \{x \in X \mid x \text{ é sharp em } X\}$$

Note que $Sharp(X)$ é unicamente determinado pela base $\mathcal{B}$ e sua ordem (ressalta-se aqui a importância da ordem escolhida) e pelo conjunto X. No que segue, iremos provar que $Sharp(W)$ é uma base de W, se W é um subespaço não nulo de V.

Lema 2.1.1 *Seja $W \subseteq V$ subespaço. Sejam $x, y \in Sharp(W)$ Então, $Tip(x) = Tip(y) \Leftrightarrow x = y$*

Prova. ($\Leftarrow$) Trivial

($\Rightarrow$)

Sejam $x, y \in Sharp(W)$ com $x \neq y$. Então,

$$x = Tip(x) + \sum_{\beta_i \in Nontip(W)} \alpha_i \beta_i$$

$$y = Tip(x) + \sum_{\gamma_i \in Nontip(W)} \delta_i \gamma_i$$

Como W é subespaço, $x - y \in W$. Mas,

$$x - y = \sum_{\beta_i \in Nontip(W)} \alpha_i \beta_i - \sum_{\gamma_i \in Nontip(W)} \delta_i \gamma_i$$

Mas então, como x e y são sharps, $supp(x-y) \subseteq Nontip(W)$ e, em particular, $Tip(x-y) \in Nontip(W)$. Mas, conforme visto antes, $x - y \in W$, o que nos leva a uma contradição. $\square$

Lema 2.1.2 *$Sharp(W)$ é linearmente independente.*

Prova. Precisamos provar que

$$\sum_{x_i \in Sharp(W)} \alpha_i x_i = 0$$

implica $\alpha_i = 0$, para todo i. (Nota-se que, pelo Lema anterior, podemos ter no máximo um vetor sharp com um dado tip. Assim, como V é de dimensão finita, $Sharp(W)$ é finito.)

Mas, pelo lema anterior, cada tip aparece uma única vez na soma acima (se os vetores sharp são diferentes, seus tips são diferentes). Com isso, como os vetores são sharp, nenhum tip pode aparecer no suporte de outro elemento sharp.

Assim, a soma acima pode ser reescrita como

$$\sum_{x_i \in Sharp(W)} \alpha_i Tip(x_i) + \text{ NonTips}$$

Assim, como cada $Tip(x)$ aparece uma única vez, ele não pode ser anulado por outro elemento e $\alpha_i = 0$, para todo i. $\square$

Introduzimos uma notação antes de apresentar o próximo resultado.

Definição 2.1.3 *Seja $X \subseteq V$ subconjunto e $x \in Sharp(X)$. Se $w \in V$, então denotamos por $< w, x >$ o coeficiente de $Tip(x)$ na expansão de w como combinação linear de elementos de $\mathcal{B}$.*

Lema 2.1.3 *Seja W subespaço de V. Então, para cada elemento $b \in Tip(W)$, existe $x \in Sharp(W)$ tal que $Tip(x) = b$.*

Prova. Suponha que a afirmação não é verdadeira. Então existe um conjunto C não vazio de elementos de W tal que os tips dos elementos de C não são tip de nenhum vetor sharp. Tomemos $v \in C$ com tip minimal entre os tips dos elementos de C. Por hipótese, v não é sharp. Então, existem $b_1, b_2, \ldots, b_n \in supp(v)$ tal que $b_i \in Tip(W)$, para $1 \leq i \leq n$, com cada b_i menor que $Tip(v)$ e $supp(v) \setminus \{b_1, b_2, \ldots, b_n, Tip(v)\} \subseteq Nontip(W)$ (esses são todos os tips de W que ocorrem em v diferentes de $Tip(v)$). Pela minimalidade de v, temos que existem vetores sharp $s_1, \ldots, s_n$ cujos tips são $b_1, \ldots, b_n$, respectivamente. Tomamos então

$$s = v - \sum_{i=1}^{n} < v, s_i > s_i$$

Então s é sharp e $Tip(s) = Tip(v)$, uma contradição. $\square$

Com isso, enunciamos o próximo resultado.

Teorema 2.1.4 *Seja V um espaço vetorial de dimensão finita com uma base bem ordenada $\mathcal{B}$ e W subespaço de V. Então $Sharp(W)$ é uma base para W.*

Prova. Seja $u \in W$. Pelo Lema acima

$$v = u - \sum_{x \in Sharp(W)} < u, x > x \in Nontip(W)$$

Mas, como W é subespaço vetorial, $v \in W$, logo $v = 0$. Com isso, u se escreve como combinação linear de elementos de $Sharp(W)$. Conforme visto anteriormente $Sharp(W)$ é linearmente independente e, portanto, uma base. $\square$

Em seguida, mostramos duas aplicações da teoria vista até este ponto para dois resultados já bem conhecidos.

Operadores Lineares. As idéias vistas até agora nos fornecem uma prova simples para o fato de que se V é um espaço vetorial de dimensão finita, T um operador linear em V diagonalizável e W um subespaço T-invariante de V, então $T\mid_W$ é diagonalizável.

Primeiramente seja $\mathcal{B} = \{b_1, b_2, \ldots, b_3\}$ uma base bem ordenada[1] de autovetores de V (ela existe, pois T é diagonalizável). Procuraremos uma base de autovetores para W. Mas, se $x \in Sharp(W)$:

$$x = Tip(x) + \sum_{b_i \in Nontip(W)} \alpha_i b_i$$

Mas como $\mathcal{B}$ é uma base de autovetores, temos:

$$T(x) = T(Tip(x)) + T(\sum_{b_i \in Nontip(W)} \alpha_i b_i) = \lambda Tip(x) + \sum_{b_i \in Nontip(W)} \lambda_i \alpha_i b_i$$

Temos dois casos:

1. $\lambda = 0$

[1] Aqui, como $\mathcal{B}$ é finita, existe uma boa ordem para $\mathcal{B}$ (qualquer conjunto finito pode ser bem ordenado). Para o resultado mostrado aqui, podemos tomar qualquer boa ordem nessa base (por exemplo: $b_1 < b_2 < \cdots < b_n$).

Neste caso, suponha que $T(x) \neq 0$. Mas, como $\lambda = 0$,

$$T(x) = \sum_{b_i \in Nontip(W)} \lambda_i \alpha_i b_i$$

e $Tip(T(x)) \in Nontip(W)$. Mas W é T-invariante, logo $T(x) \in W$, o que nos leva a uma contradição. Portanto, $T(x) = 0$ e x é autovetor.

2. $\lambda \neq 0 \Rightarrow T(x)/\lambda \in Sharp(W)$. Logo, $T(x)$ é um vetor sharp com o mesmo tip de x e, portanto $T(x)/\lambda = x$ e x é autovetor.

Com isso, $Sharp(W)$ nos fornece a base de autovetores procurada.

Eliminação de Gauss. A aplicação seguinte da teoria de Bases de Gröbner diz respeito à forma linha escalonada de uma matriz. Sejam $x_1, x_2, \ldots x_r \in K^n$ e seja

$$M = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{bmatrix}$$

Seja M^* a forma linha escalonada de M:

$$M^* = \begin{bmatrix} x_1^* \\ x_2^* \\ \vdots \\ x_r^* \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ & & \vdots & \\ 0 & 0 & \ldots & 1 \\ 0 & 0 & \ldots & 0 \\ & & \vdots & \\ 0 & 0 & \ldots & 0 \end{bmatrix}$$

Tomamos a ordem reversa (*reverse order*) vista no início desta seção. Com essa ordem, $x_k^*, x_{k-1}^*, \cdots, x_2^*, x_1^*$ (com $k \leq r$) são sharps no espaço gerado por $x_1, \ldots, x_r$. Além disso, eles são todos os sharps. Isso pode ser visto pelo fato de que a eliminação de Gauss utilizada para obter a forma matriz escalonada não altera o espaço linha da matriz. Assim, se existe um vetor sharp que não aparece em M^*, ele é gerado pelos sharps de M^*, mas um conjunto de vetores sharp não pode gerar outro sharp que não esteja neste conjunto (o tip dele simplesmente não aparece na união dos suportes do outros vetores).

Com isso, a eliminação de Gauss fornece um algoritmo para encontrar os vetores sharp do espaço gerado por $x_1, \ldots, x_n$. Além disso, como o conjunto dos vetores sharp é único, a forma matriz escalonada é única. Por fim, temos que, se $x \in span(x_1, \ldots, x_n)$, $x = \sum_{i=1}^{k} < x, x_i^* > x_i^*$. Essa fórmula lembra a de uma base ortonormal.

2.2 Anéis

Seja K um corpo e $R = K[x_1, \ldots, x_n]$ o anel comutativo dos polinômios sobre K e considere R como espaço vetorial sobre K. Sua base $\mathcal{B}$ consiste de todos os monômios e o 1. Note que o monóide $\mathcal{B}$ possui a propriedade cancelativa. De fato, se $a, b, c \in \mathcal{B}$ e $a \neq 0$, temos:

$$ab = ac \overset{\text{operação de adição no anel}}{\Rightarrow} ab - ac = 0 \Rightarrow a(b-c) = 0 \overset{\text{R é domínio}}{\Rightarrow} b - c = 0$$

Ordenando as variáveis: $1 < x_1 < x_2 < \cdots < x_n$, $\mathcal{B}$ pode ser totalmente ordenada utilizando a ordem de grau e lexicografia. Note que, neste exemplo, temos também outra ordem parcial sobre $\mathcal{B}$: divisibilidade. Sua definição segue.

Definição 2.2.1 ***(Divisão)*** *Sejam $b_1 = x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ e $b_2 = x_1^{f_1}x_2^{f_2}\cdots x_n^{f_n}$ elementos de $\mathcal{B}$. Dizemos que b_1* ***divide*** *b_2 se $e_1 \leq f_1, e_2 \leq f_2, \ldots, e_n \leq f_n$.*

É bastante conhecida a prova de que a divisibilidade não possui anticadeias (seqüencias infinitas de elementos incomparáveis).

Fixemos agora a base $\mathcal{B}$ com a ordem de grau e lexicografia e seja I um ideal não nulo de R.

Definição 2.2.2 ***(Base de Gröbner)*** *Sejam R, $\mathcal{B}$ e I como acima. Um conjunto finito de polinômios $G = \{z_1, \ldots, z_m\} \subseteq I$ é uma* ***Base de Gröbner*** *(também chamado de* ***Conjunto Gerador de Gröbner****) para I se*

$$\langle Tip(G) \rangle = \langle Tip(I) \rangle,$$

ou seja, para cada $v \in I$, existe $g \in G$ tal que $Tip(g) \mid Tip(v)$.

Proposição 2.2.1 *Seja I um ideal de R, como acima. Então uma base de Gröbner G para I gera I como ideal bilateral.*

> **Prova.** Suponha que não. Então existe $v \in I$ tal que $v \notin \langle G \rangle$. Dada a boa ordem em $\mathcal{B}$ podemos tomar v com tip minimal tal que isso ocorra. Mas, por definição de base de Gröbner, existe $g \in G$ tal que $Tip(g) \mid Tip(v)$, ou seja $Tip(v) = hTip(g)$, para algum $h \in R$. Então $v - hg \in I$ e tem tip menor que v. Logo $v - hg \in \langle G \rangle$ e $v \in \langle G \rangle$, uma contradição. □

Definição 2.2.3 ***(Minsharp)*** *$MinSharp(I)$ denota o conjunto dos vetores sharp em I cujo tip é minimal em $Tip(I)$ com relação à divisão. Além disso denotamos:*

$$MinTip(I) = Tip(MinSharp(I))$$

Proposição 2.2.2 *Sejam R e I como acima. Então $Nontip(I)$ é o conjunto de monômios mônicos que não são divisíveis por elementos de $MinTip(I)$.*

Por outro lado, $MinTip(I)$ é o conjunto de monômios que não estão em $Nontip(I)$ e cujos divisores próprios pertencem todos a $Nontip(I)$.

> **Prova.** A prova do teorema acima se baseia unicamente na inspeção cuidadosa dos definições de $MinTip(I)$ e $Nontip(I)$.
>
> Para a primeira parte, provaremos as duas inclusões de conjuntos. Primeiro, suponha $v \in Nontip(I)$ divisível por um elemento $g \in MinTip(I)$. Pelo Lema anterior, existe um vetor sharp s cujo tip é g. Logo, tomando um múltiplo de s, teremos que v é tip de um vetor em I, um absurdo. A inclusão reversa vem da definição de $MinTip(I)$. Se um elemento não é divisível por nenhum monômio de $MinTip(I)$, então ele não pode pertencer a $Tip(I)$, por definição.

Para a segunda parte, basta notar primeiramente que um vetor em $MinTip(I)$ não pode estar em $Nontip(I)$ (um monômio não pode ser ao mesmo tempo tip de um elemento em I e não ser tip de nenhum elemento de I). Além disso, se um elemento de $MinTip(I)$ tem um divisor próprio, pela minimalidade deste conjunto (com relação à divisão), este divisor não pode ser tip de nenhum elemento de I. $\square$

2.2.1 Exemplo

Seja $R = K[x, y]$ (com K um corpo de característica zero) e $\mathcal{B}$ o monóide ordenado utilizando a ordem de grau e lexicografia, com $x < y$. Segue um exemplo, para o ideal $I = \langle xy^2 - x^2, x^2y - y^2 \rangle$:

$$MinSharp(I) = \{xy^2 - x^2, x^2y - y^2, y^3 - x^3, x^4 - y^2\}$$

($MinSharp(I)$ pode ser calculado algoritmicamente)

$$MinTip(I) = \{xy^2, x^2y, y^3, x^4\}$$

$$Nontip(I) = \{1, x, x^2, x^3, y, y^2, xy\}$$

Proposição 2.2.3

$$R = I \oplus span(Nontip(I))$$

Prova. Primeiramente mostramos que se $f \in R$, $f = f_1 + f_2$ com $f_1 \in I$ e $f_2 \in span(Nontip(I))$. Se $supp(f) \subseteq Nontip(I)$, $f_1 = 0$, $f_2 = f$ e não há o que mostrar. Suponha que existe $b \in supp(f)$ com $b \in Tip(I)$. Por outro lado, pelo Lema anterior, existe um vetor sharp (em I) s com $Tip(s) = b$. Aqui cabem duas observações:

1. $s \in I$, pela definição de vetor sharp.
2. $f - s$ tem tip menor que f.

Podemos subtrair vetores sharp de f sucessivamente, enquanto o suporte do vetor resultante contiver elementos de $Tip(I)$. Como o tip do vetor resultante após uma subtração é sempre menor, esse processo deve parar (pela boa ordem em $\mathcal{B}$) e, ao final teremos

$$f' = f - s_1 - s_2 - \cdots - s_n \in span(Nontip(I))$$

com $s_1, s_2, \ldots, s_n$ sharps. Mas então

$$f = s_1 - s_2 - \cdots - s_n + f' \in I + span(Nontip(I))$$

Por fim, mostramos que $I \cap span(Nontip(I)) = \emptyset$. De fato, seja $g \in I \cap span(Nontip(I))$. Então $Tip(g) \in Tip(I)$ e $Tip(g) \in Nontip(I)$, uma contradição. $\square$

Proposição 2.2.4 *Sejam R e I como acima. Então*

$$R/I \simeq span(Nontip(I))$$

(como espaço vetorial)

Prova. Seja

$$T: \begin{array}{l} span(Nontip(I)) \longrightarrow R/I \\ x \mapsto \overline{x} \end{array}$$

Mostraremos que T é linear e bijetora. Mas, se $x, y \in R$ e $\lambda \in K$, temos

$$T(x+y) = \overline{x+y} = \overline{x} + \overline{y} = T(x) + T(y)$$

$$T(\lambda x) = \overline{\lambda x} = \overline{\lambda}\overline{x} = \overline{\lambda} T(x)$$

Mostraremos agora que T é bijetora. Seja $x \in Ker(T)$. Então

$$T(x) = 0 \Rightarrow x \in I \overset{x \in span(Nontip(I))}{\Rightarrow} x = 0$$

Seja $\overline{x} \in R/I$. Como $x \in R$, temos que $x = x_1 + x_2$, com $x_1 \in I$ e $x_2 \in span(Nontip(I))$. Logo, $x - x_2 \in I$ e $T(x_2) = \overline{x_2} = \overline{x}$. □

No exemplo, R/I tem dimensão 7.

No restante deste capítulo, apresentamos o conceito de ordem monoidal. Esse conceito é bastante parecido com o de ordem admissível (apresentado no Capítulo 4).

Definição 2.2.4 ***(Ideal de Ordem)*** *Seja Y um conjunto e $\leq$ uma ordem parcial em Y. Dizemos que $X \subseteq Y$ é um* ***ideal de ordem*** *de Y se $x \in X$ e $y \geq x$ implica $y \in X$.*

Lema 2.2.5 *[6] As seguintes condições em um conjunto parcialmente ordenado Y são equivalentes:*

1. *A Condição de Cadeia Ascendente vale para ideais de ordem de Y.*
2. *Toda seqüência infinita de elementos de Y tem uma subseqüência ascendente infinita.*
3. *Toda seqüência infinita de elementos de Y tem uma subseqüência ascendente de comprimento dois.*
4. *Não existe em Y uma seqüência estritamente descendente infinita ou uma anticadeia infinita.*

Definição 2.2.5 ***(Ordem monoidal)*** *Seja $\mathcal{B}$ um monóide com uma boa ordem $\leq$. Dizemos que $\leq$ é* ***monoidal*** *se*

- $1 \leq a, \forall a \in \mathcal{B}$
- *Para cada $b, c \in \mathcal{B}$, $b \leq c \Rightarrow bd \leq cd$ e $db \leq dc, \forall d \in \mathcal{B}$*

Lema 2.2.6 *Seja M um monóide que satisfaz a propriedade cancelativa (dos dois lados) e $\leq$ uma ordem monoidal total em M. Então*

1. *Para todo $a, b \in M$, se a divide b então $a \leq b$.*
2. *Se a divisibilidade à esquerda é uma boa ordem parcial (em M), então $\leq$ é uma boa ordem.*

Prova. (1)

Sejam a, b como no enunciado do Lema. $b = ac$. Como $\leq$ é monoidal, temos que

$$1 \leq c \overset{\leq \text{ é monoidal}}{\Rightarrow} a \leq ac = b$$

(2) Como visto anteriormente, divisão não tem anticadeias. Logo, se tomamos uma seqüência infinita de elementos de M, existem a, b nesta seqüência tais que $a \mid b$. Logo, por (1), $a \leq b$ e temos as condições do ítem 3 do Lema 2.2.5 satisfeitas. $\square$

Capítulo 3

Bases de Gröbner em Álgebras de Caminhos

Este capítulo apresenta generalizações do que foi visto até aqui para o caso de Álgebras de Caminhos. Inicialmente destaca-se algumas propriedades das Álgebras de Caminhos (também presentes no anel de polinômios e na álgebra livre) e apresenta-se resultados para qualquer álgebra que possua essas propriedades. Alguns resultados interessantes particulares para álgebras finitamente geradas também são apresentados e, por fim, mostra-se uma justificativa para o uso de Álgebras de Caminhos em Teoria de Bases de Gröbner.

3.1 Anéis e Álgebras de Caminhos

Bases de Gröbner Lineares em K-álgebras Primeiramente, mostramos a generalização de resultados centrais de Bases de Gröbner lineares já vistos para o caso de dimensão finita. Assuma V um espaço vetorial com uma base $\mathcal{B}$ com uma boa ordem $\leq$. Seja ainda $Fin(\mathcal{B})$ a coleção de todos os subconjuntos finitos de $\mathcal{B}$. A boa ordem em $\mathcal{B}$ induz uma boa ordem em $Fin(\mathcal{B})$ (também chamada de $\leq$), da seguinte forma:

Sejam $C, D \in Fin(\mathcal{B})$. $C \leq D$ se:

1. $C = \emptyset$ ou
2. $C \neq \emptyset$ e $Tip(C) \leq Tip(D)$ ou
3. $C \neq \emptyset$ e $Tip(C) = Tip(D)$ e $C \setminus Tip(C) \leq D \setminus Tip(D)$

Lema 3.1.1 *$(Fin(\mathcal{B}), \leq)$ é um conjunto bem ordenado.*

Nota-se que com a ordem $\leq$ em $Fin(\mathcal{B})$ tem-se uma boa-ordem nos elementos de V (pois o suporte de um elemento de V é um elemento de $Fin(\mathcal{B})$).

Lema 3.1.2 *Sejam $v, w \in V$ e $Tip(w) \in supp(v)$. Seja λ o único escalar tal que $\lambda = \beta/\alpha$, onde β é o coeficiente de $Tip(w)$ em v e α o coeficiente de $Tip(w)$ em w. Então $v - \lambda w < v$.*

Segue uma generalização do Teorema 2.2.4.

Teorema 3.1.3 *Seja V um espaço vetorial e W um subespaço de V. Então*

$$V = W \oplus span(Nontip(W)).$$

Note o leitor que, com esse teorema, podemos escrever todo vetor $v \in V$ **de forma única** como $v = w_v + N(v)$, com $w_v \in W$ e $N(v) \in span(Nontip(W))$. Chamaremos $N(v)$ de **forma normal de** v (módulo W).

Álgebras Seja $K\Gamma$ a álgebra de caminhos construída a partir de um carcaz Γ com conjunto de vértices $\Gamma_0 = \{v_1, \ldots, v_n\}$ e de flechas $\Gamma_1 = \{a_1, \ldots, a_k\}$. Sua base $\mathcal{B}$ consiste de todos os caminhos em Γ. Tomamos ainda a ordem de comprimento e lexicografia em $\mathcal{B}$ (denotada por $\leq$), ordenando os vértices e as flechas da seguinte forma: $v_1 < \cdots < v_n < a_1 < \cdots < a_k$.

Dizemos ainda que para $b_1, b_2 \in \mathcal{B}$, b_1 **divide** b_2 (denotado por $b_1 \mid b_2$) se existem $u, v \in \mathcal{B}$ tais que $b_2 = ub_1v$. A base $\mathcal{B}$ aqui apresentada satisfaz algumas propriedades importantes para o Teoria de Bases de Gröbner. Em seguida destacamos 5 delas:

(M1) $\mathcal{B} \cup \{0\}$ é fechado para multiplicação

(M2) A divisão é reflexiva em $\mathcal{B}$.

(M3) Para cada $b \in \mathcal{B}$, $\{a \text{ tal que } a \mid b\}$ é finito.

(M4) Sejam $b_1, b_2, u, v \in \mathcal{B}$. Se nenhum dos produtos for zero, então:

$$b_1 < b_2 \Rightarrow ub_1v < ub_2v$$

(M5) Sejam $b_1, b_2 \in B$. Então $b_1 \mid b_2 \Rightarrow b_1 \leq b_2$.

Nota-se que as bases já discutidas do anel comutativo de polinômios e da álgebra livre também satisfazem essas propriedades.

Lema 3.1.4 *Divisão é uma ordem parcial.*
Para cada $b \in \mathcal{B}$, $\{(u, w, v) \in \mathcal{B}^3 \mid b = uwv\}$ é finito.

Prova. A prova da primeira parte segue por (M2) e (M5).

Para a segunda parte, basta notar que u, w e v dividem b e aplicar (M3). Isso pode ser visto da seguinte forma. Por (M2), existem $b_1, b_2, b_3, b_4 \in \mathcal{B}$ tais que $u = b_1ub_2$ e $v = b_3vb_4$. Assim, $b = b_1ub_2wb_3vb_4$ e u, w e v dividem b. Por M3 só existe um número finito de tais elementos. □

No que segue R será uma álgebra com uma base $\mathcal{B}$ bem ordenada satisfazendo M1 a M5 e I um ideal de R.

Segue o conceito de redução. Ele é que nos permite encontrar a forma normal de um elemento, dada uma Base de Gröbner. Um algoritmo para isso será apresentado no capítulo 4.

Definição 3.1.1 ***(Redução simples de anel)***
Seja R uma álgebra e $a \in R$. Uma ***redução simples de anel*** *ρ para a é denotada por uma 4-tupla (λ, u, f, v), onde $\lambda \in K^*$, $u, v \in \mathcal{B}$ e $f \in R$. Além disso, as seguintes condições são satisfeitas:*

- $u\,Tip(f)v \in supp(a)$
- $u\,Tip(f)v \notin supp(a - \lambda ufv)$

Neste caso, dizemos que $\rho(a) = a - \lambda ufv$ é a redução de a por ρ. Uma **redução de álgebra** para a é uma seqüência de reduções simples para a. Denotamos essa redução por $\rho_1\rho_2\cdots\rho_q(a)$, onde $\rho_q(a)$ é uma redução simples para a e ρ_i é uma redução para $\rho_{i+1}\cdots\rho_q(a)$ para $i = q-1,\ldots,1$. Se cada ρ_i é dado por $(\lambda_i,\, u_i,\, f_i,\, v_i)$ e cada $f_i \in S \subseteq R$, dizemos que a redução é sobre S.

Teorema 3.1.5 *Seja G uma Base de Gröbner para um ideal I de R. Então, cada elemento de R pode ser reduzido sobre G para sua forma normal (modulo I).*

A próxima questão diz respeito a como decidir se um conjunto gerador de um ideal é uma Base de Gröbner para esse ideal. Essa questão será tratada no contexto de Álgebras de Caminhos na seção 4.2.

3.2 Álgebras Finitamente Geradas

Continuaremos com a notação anterior: R é uma álgebra com uma base $\mathcal{B}$ que satisfaz as Propriedades M1–M5.

Lema 3.2.1 *Seja S um semigrupo finitamente gerado e T um subconjunto não vazio de S, tal que $ST \subseteq T$. Se $S \setminus T$ é finito, então existe um conjunto finito $W \subseteq T$ tal que $T = W \cup SW$.*

Prova. Seja V um conjunto gerador finito para S. Se $s \in S$ seja $l(a)$ o menor comprimento de um produto de geradores que é igual a a. Seja ainda $N = max\{l(z) \mid z \notin T\}$ e $W = \{b \in T \mid l(b) \leq N+1\}$ – note que para que N esteja bem definido precisamos ter $S \setminus T$ finito. Como N e V são finitos, W é finito (pois só é possível um número finito de combinações de finitos geradores com um comprimento máximo).

Falta mostrar que $T = W \cup SW$. Por um lado, $W \cup SW \subseteq T$, pois:

$W \subseteq T$ por construção de W. Além disso, como $ST \subseteq T$, $SW \subseteq T$.

Precisamos agora mostrar que $T \subseteq W \cup SW$. Assuma, por absurdo que isso não é verdade. Nesse caso, existe $x \in T \setminus W \cup SW$. Seja tal x, de modo que $l(x) = l$ seja minimal com respeito a $x \notin W \cup SW$. Assim, temos que $x = x_1x_2\cdots x_l$ e $l > N+1$, uma vez que x não pertence a W. Tomamos, então $x_2\cdots x_l \in T$, pois $l(x_2\cdots x_l) > N$. Pela hipótese de indução, temos ainda que $x_2\cdots x_l \in W \cup SW$.

Mas, $S(W \cup SW) = SW$. Assim, como $x_2\cdots x_l \in W \cup SW$, $x = x_1x_2\cdots x_l \in S(W \cup SW) = SW \Rightarrow x \in W \cup SW$, uma contradição. □

Teorema 3.2.2 *Assuma que R é uma álgebra finitamente gerada (como álgebra) com uma base bem ordenada $\mathcal{B}$ satisfazendo as propriedades M1 a M5 e I um ideal não nulo de R. Se R/I tem dimensão finita, então I possui uma Base de Gröbner finita.*

Prova. Como R é finitamente gerada, podemos ver facilmente que $\mathcal{B}$ é finitamente gerado como semigrupo. Estão seja:

$$T = \{0\} \cup \{b \in \mathcal{B} \mid b = Tip(g) \text{ para algum } g \in I\}$$

Mas, pela propriedade M4 temos que se $g \in I$ e $u, v \in \mathcal{B}$ então $Tip(ugv) = uTip(g)v$, se $uTip(g)v \neq 0$. Com isso, temos que $BTB \subseteq T$. Logo, por M2, $BT \subseteq T$. Além disso, $B \setminus T = Nontip(I)$, que, como a álgebra tem dimensão finita, é um conjunto finito (pelo

Teorema 3.1.3). Logo, pelo Lema acima, existe $W \subseteq T$ finito tal que $T = W \cup BW \cup \{0\}$. Por outro lado, por M2, temos que $W \subseteq BWB$ e $BW \subseteq BWB$ e por M4 $BWB \subseteq T = W \cup BW \cup \{0\}$ e temos que

$$T = BWB \cup \{0\}$$

Tomemos então $f \in MinSharp(I)$. Então $Tip(f) \in T$ e existe $w \in W$ que divide f. Mas, pela definição de $MinSharp(I)$, $w = Tip(f)$. Logo, o fato de W ser finito faz com que $MinSharp(I)$ seja finito. □

Suponha agora que C é um ideal de semigrupo de $\mathcal{B} \cup \{0\}$ (Isto significa que $0 \in C$ e $BCB \subseteq C$). Então KC, o espaço linear gerado por C, é um ideal bilateral de R tal que $Nontip(KC) = \mathcal{B} \backslash C$. Temos a seguinte seqüência de espaços vetoriais.

$$0 \longrightarrow KC \longrightarrow R \underset{\nu}{\overset{\pi}{\underset{\longleftarrow}{\longrightarrow}}} R/KC \longrightarrow 0$$

Seja $\pi : R \longrightarrow R/KC$ a projeção canônica de R em R/KC.

Lema 3.2.3 *Sejam $b_1, b_2 \in \mathcal{B}$ com $b_1 \notin C$. Então $\pi(b_1) \neq \pi(b_2)$.*

Prova. Sejam b_1, b_2 como nas hipóteses do Lema. Suponha que $\pi(b_1) = \pi(b_2)$. Então $b_1 + KC = b_2 + KC$ e $b_1 - b_2 \in KC$. Mas como KC é o espaço linear gerado por C e $b_1, b_2 \in \mathcal{B}$, temos, que $b_1 \in KC$ e $b_2 \in KC$, um absurdo. □

Com isso, seja $\nu : R/KC \longrightarrow R$ a transformação linear que leva um elemento de $\pi(B \setminus C)$ em sua pré-imagem em R (por π) e leva o 0 no 0. Essa transformação está bem definida e $\pi\nu = 1_{R/KC}$. Temos ainda que $\pi(B \setminus C)$ (com a boa ordem de B restrita a $B \setminus C$) é uma base de R/KC satisfazendo as propriedades M1 a M5.

Lema 3.2.4 *Seja $f \in R$ tal que $supp(f) \subseteq B \setminus C$. Então $\nu\pi(f) = f$.*

Prova. Seja $f \in R$, como nas hipóteses do Lema. Então f se escreve como $f = \sum_{i=0}^{n} \alpha_i b_i$, com $\alpha_i \in K$ e $b_i \in B \setminus C$. Com isso, temos:

$$\nu(\pi(f)) = \nu(\sum_{i=0}^{n} \alpha_i \pi(b_i)) = \sum_{i=0}^{n} \alpha_i \nu(\pi(b_i))$$

Mas, como $\pi(b_i) \in \pi(B \setminus C)$, pela definição de ν, $\nu(\pi(b_i)) = b_i$. E com isso, temos o resultado procurado. □

Lema 3.2.5 *Seja $f \in B \setminus C$ e seja $v \in \pi(B \setminus C)$ com $v \mid \pi(f)$. Então $\nu(v) \mid f$.*

Prova.

$v \mid \pi(f) \Rightarrow \exists u, h \in \pi(B \backslash C)$ tais que $uvh = \pi(f)$. Então $\nu(uvh) = \nu(\pi(f)) \Rightarrow \nu(u)\nu(v)\nu(h) = f$ e temos o resultado procurado. □

Teorema 3.2.6 *Seja C um ideal de semigrupo de $\mathcal{B} \cup \{0\}$. Se I é um ideal de R tal que $C \subseteq I$ então:*

$$MinSharp(I) = \nu(MinSharp(\pi I)) \cup (C \cap MinSharp(I))$$

Prova. Primeiro mostraremos que $MinSharp(I)$ está incluído na união. Para tanto, suponha que $f \in MinSharp(I)$. Temos dois casos:

- $Tip(f) \in C$
  Neste caso, $f \in C$, pois vetores em $MinSharp(I)$ são sharp. Assim, como $C \subseteq I$, $Tip(f) \in I$ e $f = Tip(f) \in C$ (pelo Lema 2.1.1).
- $Tip(f) \notin C$
  Neste caso nenhum elemento de C aparece no suporte de f, pois f é sharp e todo elemento de C é tip de algum elemento de I (já que $C \subseteq I$). Então, temos que $\nu\pi(f) = f$.
  Para mostrar que $f \in \nu(MinSharp(\pi I))$, basta mostrar que $\pi(f) \in MinSharp(\pi(I))$. Mas pelo Lema anterior, vemos que isso ocorre.

Com isso mostramos que $MinSharp(I)$ está incluído na união.

A inclusão reversa segue do fato de que, como C é um ideal de semigrupo, se $b \in \mathcal{B} \setminus C$ e $b' \mid b$ então $b' \in \mathcal{B} \setminus C$. Com isso, se $v \in MinSharp(\pi(I))$ então $\nu(v) \in MinSharp(I)$. □

Com isso, se R é uma álgebra de caminhos, podemos definir $C(N)$ como sendo o ideal de semigrupo que consiste de todos os caminhos de comprimento maior ou igual a N. Seja ainda I um ideal de R que contém $C(N)$. Se tomamos a seguinte seqüência de espaços vetoriais:

$$0 \longrightarrow KC(N+1) \longrightarrow R \underset{\nu_{N+1}}{\overset{\pi_{N+1}}{\rightleftarrows}} R/KC(N+1) \longrightarrow 0$$

temos, pelo Teorema acima que

$$MinSharp(I) = \nu_{N+1}(MinSharp(\pi_{N+1} I)) \cup (C(N+1) \cap MinSharp(I))$$

Porém, como todo caminho de comprimento $N+1$ é divisível por um caminho de comprimento N (para $N \geq 1$), temos que $C(N+1) \cap MinSharp(I) = \emptyset$ e $MinSharp(I) = \nu_{N+1}(MinSharp(\pi_{N+1} I))$. Ou seja, ao calcular $MinSharp(I)$, toda vez que um caminho de comprimento maior ou igual a $N+1$ aparecer no suporte de um elemento, podemos substituí-lo por 0.

3.3 Carcazes

Nesta parte da discussão mostraremos que uma álgebra de caminhos pode ser vista como um exemplo universal, contendo as propriedades apresentadas no parágrafo anterior. Nesta seção, olhamos para as Propriedades M1 a M5 como axiomas e mostramos que é possível construir um carcaz a partir de qualquer álgebra que apresente essas propriedades. O resultado principal a ser demonstrado nesta seção é o Teorema 3.3.9

Primeiramente, assuma que S é um semigrupo com 0 e seja $\mathcal{B} = S \setminus 0$ um conjunto bem ordenado com as propriedades M1 a M5.

Lema 3.3.1 *Se $a = uv \in \mathcal{B}$ então $u \mid a$ e $v \mid a$.*

Prova. Pela propriedade M2 a divisão é reflexiva, logo podemos encontrar $b, c \in \mathcal{B}$ tais que $u = buc$. Logo, $a = bucv$ e $u \mid a$. Utilizando o mesmo argumento concluímos que $v \mid a$. $\square$

Definição 3.3.1 ***(Origem e Término)*** *Seja $a \in \mathcal{B}$. Definiremos então* ***origem de a*** *como:*

$$o(a) = \{r \in \mathcal{B} \mid a = ras \text{ para algum } s \in \mathcal{B}\}$$

Diremos ainda que o ***término de a*** *é:*

$$t(a) = \{s \in \mathcal{B} \mid a = ras \text{ para algum } r \in \mathcal{B}\}$$

Lema 3.3.2 *$o(a)$ e $t(a)$ são ambos semigrupos finitos em $\mathcal{B}$.*

Prova. Mostramos aqui o argumento para $o(a)$. O caso para $t(a)$ é análogo. Primeiramente note que $o(a)$ é não vazio pela reflexividade da divisão (Propriedade M2). Mostremos então é um semigrupo.

Para tanto, sejam $r_1, r_2 \in o(a)$. Então existem $s_1, s_2 \in t(a)$ tais que $r_1 a s_1 = a$ e $r_2 a s_2 = a$. Mas tomando, $r_1 r_2 a s_2 s_1 = r_1 a s_1 = a$. Logo $r_1 r_2 \in o(a)$, o que mostra que $o(a)$ é um semigrupo.

Para provar que é finito, basta notar que cada $r \in o(a)$ está no conjunto dos divisores de a e, pelo Lema 3.3.1 e pela Propriedade M3, esses conjunto é finito. $\square$

Teorema 3.3.3 *$o(a)$ e $t(a)$ consistem ambos de um único idempotente.*

Prova. Mostraremos aqui o argumento para $o(a)$. O caso para $t(a)$ é análogo.

Sejam $u, v, w \in o(a)$. Queremos mostrar que $v = uvw$. Naturalmente $v \mid uvw$, logo $v \leq uvw$. Suponhamos, por contradição, que $v < uvw$. Então, pela Propriedade M4, temos que $v < uvw \Rightarrow uvw < u^2vw^2 < \cdots$. Como $o(a) \subseteq \mathcal{B}, 0 \notin o(a)$. Pelo Lema 3.3.2 temos que $o(a)$ é finito e, portanto, $v = uvw$. Mostramos ainda algumas conclusões:

- $u = u^3$:

  Obviamente $u \mid u^3$. Logo $u \leq u^3$. Se $u < u^3$, temos que $u < u^3 \Rightarrow u^3 < u^5 < \cdots$. Mas só temos finitos casos, logo $u = u^3$.

- $u = u^2$:

  $u \mid u^2uu \Rightarrow u = u^2uu$ (pelo mesmo argumento acima) $\Rightarrow u = u^3u \Rightarrow u = uu \Rightarrow u = u^2$

- $u = v$:

  Por um lado, $v \mid vuu \Rightarrow u = vuu \Rightarrow u = vu$.
  Por outro lado, $v \mid vvu \Rightarrow v = v^2u \Rightarrow v = vu$.

Logo, $v = u\ \forall u, v \in o(a)$. $\square$

Note apenas que se $e \in \mathcal{B}$ é um idempotente, então $e = o(e) = t(e)$, pois $e = eee$. Relacionaremos agora os idempotentes entre si.

Teorema 3.3.4 *Sejam e e f dois idempotentes distintos em $\mathcal{B}$. Então $ef = 0$.*

Prova. Suponho que $e \neq f$ e $ef \neq 0$. Logo, ou $e < f$ ou $f < e$. Se $e < f$, temos que $ef < f^2$ (pela Propriedade M4) $\Rightarrow e^2f < ef^2 \Rightarrow ef < ef$, um absurdo. O caso $f < e$ segue de modo análogo. □

Lema 3.3.5 *Seja $e \in \mathcal{B}$ um idempotente. Se $x \in \mathcal{B}$ e $ex \neq 0$ então $e = o(x)$. Se $xe \neq 0$ então $e = t(x)$.*

Prova. Podemos escrever $x = axb$, onde $a = o(x)$ e $b = t(x)$. Como $ex \neq 0$, temos que $ea \neq 0$. Logo pelo Teorema 3.3.4 e e a não podem ser idempotentes distintos. Mas como eles são idempotentes, $e = a = o(x)$. O caso para $t(x)$ é análogo. □

Teorema 3.3.6 *Se $e \in \mathcal{B}$ é um idempotente, então seu único divisor é ele mesmo.*

Prova. Por contradição, suponha que $e = uv$. Mostraremos que $e = u = v$:

> $veu = v(uv)u = v(uv)^3u = (vuvu)(vuvu) = (vuvu)^2 = vuvu$. Se chamamos $vuvu = f$, então f é um idempotente.

Como $fv \neq 0$ e $uf \neq 0$, temos que $f = o(v) = t(u) \Rightarrow v = fvr$ e $u = quf$, para algum $r, q \in \mathcal{B}$.

Logo, $e = uv = quffvr \overset{\text{f é idempotente}}{=} qufvr \Rightarrow f \mid e$. Mas $e \mid f \Rightarrow e = f = uev$. Então, $u = o(e)$ e $v = t(e)$. Mas, como e é idempotente, $e = o(e) = t(e) = u = v$. □

Definição 3.3.2 ***(Elemento Irredutível)*** *Dizemos que um elemento não idempotente $f \in \mathcal{B}$ é **irredutível**, se seus únicos divisores são $f, o(f)$ e $t(f)$.*

Lema 3.3.7 *$o(u)u = u$ e $ut(u) = u$.*

Prova. Apresentamos a prova para $o(u)$.

$$o(u)u = o(u)(o(u)ut(u)) = o(u)o(u)ut(u) = o(u)ut(u) = u$$

□

Teorema 3.3.8 *Todo elemento não idempotente de $\mathcal{B}$ é um produto de elementos irredutíveis.*

Prova. Por contradição, considere u minimal tal que u não é produto de irredutíveis e nem idempotente. Logo, ele também não pode ser irredutível e $u = awb$, onde w não é irredutível e $w \notin \{o(u), t(u), u\}$. Pelo Lema 3.3.1, temos que $a \mid u$, $w \mid u$ e $b \mid u$. Portanto $a \leq u, w \leq u$ e $b \leq u$.

Entre os elementos a, b, w há pelo menos um que não é irredutível. Além disso, pelo menos um deles não é produto de irredutíveis, pois se fosse, o escreveríamos como esse produto e u seria produto de irredutíveis. Mas, como u é minimal com respeito a não ser produto de irredutíveis, temos que um deles (a, b ou w) é igual a u. Por hipótese, $w \neq u$. Logo $a = u$ ou $b = u$. Suponha que $a = u$.

Nesse caso, $u = uwb \overset{\text{Lema 3.3.7}}{=} o(u)u(wb)$. Então $t(u) = wb$, pelo Teorema 3.3.3. Além disso, como $w \mid t(u)$, pelo Teorema 3.3.6 w $= t(u)$, uma contradição. Procedemos do mesmo modo para o caso em que $b = u$. □

Com os teoremas que provamos construímos um carcaz $\Gamma(\mathrm{S})$ cujos vértices são os idempotentes não nulos de S e cujas flechas são seus elementos irredutíveis. O vértice inicial e o vértice final de cada flecha são determinados pela sua origem e por seu término, respectivamente. Como a origem e o término de cada elemento de S consiste de um único idempotente, conseguimos associar a cada flecha um vértice de origem e um de término. Cada membro de $S \setminus \{0\}$ pode ser identificado com pelo menos um caminho, pelo Teorema 3.3.8.

Seja ainda $\Gamma(S)^*$ o semigrupo com zero construído a partir de $\Gamma(S)$. Então $\Gamma(S)^*$ pode diferir de S, pois dois caminhos distintos em $\Gamma(\mathrm{S})$ podem representar o mesmo elemento em S (o Teorema 3.3.8 não nos garante unicidade) ou um caminho em $\Gamma(\mathrm{S})$ pode representar zero em S. De todo modo, temos o seguinte resultado.

Teorema 3.3.9 *Seja S um semigrupo com zero que satisfaz as propriedades M1–M5. Então existe um carcaz $\Gamma(S)$ e um homomorfismo de semigrupo $\pi : \Gamma(S)^* \to S$ (que leva o 0 no 0) tal que a imagem inversa de um idempotente (ou irredutível) consiste de um único idempotente (resp. irredutível).*

Pelo Teorema 3.3.8 π é sobrejetora.

Teorema 3.3.10 *Com a notação do Teorema 3.3.9, se $s \in S$ é não nulo, então $\pi^{-1}(s)$ é finito.*

Prova. Suponha que isso não é verdade. Então escolha $0 \neq s \in S$ minimal com respeito a $\pi^{-1}(s)$ ser infinito. Defina:

$$A = \{x \in \Gamma(S)^* \mid \exists y \in \pi^{-1}(s) \text{ com } x \mid y \text{ e } x \neq y\}$$

Suponhamos então que A é infinito. Nesse caso, s não é irredutível, pois pelo Teorema 3.3.9 a imagem inversa de um irredutível é um único irredutível.

Temos, ainda que se $y \in \pi^{-1}(s)$, y não pode ser irredutível, pela fidelidade de π a elementos irredutíveis. Logo, podemos escrever $y = x_1x_2x_3$, com $x_1, x_2, x_3 \in A$. Portanto, se A é finito, $\pi^{-1}(s)$ também o é. Em seguida mostraremos que A não pode ser infinito.

Primeiramente, mostramos que $A \cap \pi^{-1}(s) = \emptyset$.

> Suponha que z está na intersecção. Então, como $z \in A$, $\exists y \in \pi^{-1}(s)$ tal que $z \neq y$ e $z \mid y$. Assim, $y = uzv$ e $s = \pi(u)\pi(z)\pi(v) \overset{z\in\pi^{-1}(s)}{=} \pi(z)$, o que mostra que $\pi(u) = o(s)$ e $\pi(v) = t(s)$, pelo Lema 3.3.5. Mas, pela fidelidade de π a idempotentes, u e v são idempotentes em $\Gamma(S)^*$. Logo, $uzv = z$ e $y = z$, uma contradição.

Assim, para cada $x \in A$, temos que $\pi(x) \mid s$ e $\pi(x) \neq s$. Mas, pela Propriedade M3 s tem apenas finitos divisores. Logo, $\pi(A)$ é um conjunto finito de membros não nulos de S, cada um menor que s. Com isso, pela minimalidade de s, A é finito. □

Os resultados apresentados nos mostram que as álgebras de caminhos surgem de uma maneira natural ao se estudar Bases de Gröbner. Um resultado mais geral (porém não apresentado aqui), nos mostra que elas de fato representam um exemplo universal no estudo dessa teoria. Detalhes desse resultado podem ser encontrados em [5].

Capítulo 4

Construção de Bases de Gröbner e Formas Normais

Neste capítulo discutiremos um algoritmo que possibilita encontrar formas normais dada um Base de Gröbner e um processo de construção de Bases de Gröbner a partir de um conjunto gerador. Nesta seção modificaremos ligeiramente as hipóteses sobre a álgebra em questão, deixando de exigir as propriedades M1 a M5 em favor de outras. Mas essa modificação não implicará nenhuma perda de generalidade, uma vez que as Álgebras de Caminhos satisfazem ambas as hipóteses e consistem um exemplo universal, conforme comentado anteriormente. Na realidade, a notação utilizada nos trabalhos envolvendo Bases de Gröbner não comutativas tem se mostrado bastante heterogênea, mas a notação apresentada neste capítulo é a que vêm sido utilizada nos trabalhos mais recentes dentre os estudados.

Ao longo deste capítulo, seja K um corpo, R uma K-álgebra finitamente gerada e $\mathcal{B}$ uma $K-$base de R.

Definição 4.0.3 ***(Base Multiplicativa)*** *Seja K um corpo, R uma K-álgebra e $\mathcal{B}$ uma $K-$base de R. $\mathcal{B}$ é dita* ***multiplicativa*** *se para todo $b, b' \in \mathcal{B}$, $bb' \in \mathcal{B}$ ou $bb' = 0$.*

Definimos em seguida como deve ser a ordem $\leq$ em $\mathcal{B}$.

Definição 4.0.4 ***(Ordem Admissível)*** *Dizemos que uma boa ordem em $\mathcal{B}$ é* ***admissível*** *se satisfaz as seguintes condições, para $p, q, r, s \in \mathcal{B}$:*

1. *Se $p < q$, então $pr < qr$, se ambos os produtos são não nulos.*

2. *Se $p < q$, então $sp < sq$, se ambos os produtos são não nulos.*

3. *Se $p = qr$ então, $p \geq q$ e $p \geq r$.*

No restante deste capítulo, assumimos que $\mathcal{B}$ é uma base multiplicativa e fixamos uma ordem admissível $\leq$ em $\mathcal{B}$.

4.1 Formas Normais e o Algoritmo da Divisão

Nesta seção apresentamos o **Algoritmo da Divisão**, que nos mostra como "dividir" um elemento de R por um subconjunto de R. Mais formalmente, o algoritmo recebe como entrada um subconjunto **ordenado** de elementos $X = \{x_1, x_2, \ldots, x_n\}$ de R e um elemento $y \in R$. Ele devolve inteiros não negativos $m_1, \ldots, m_n$, elementos $u_{i,j}$, $v_{i,j} \in B$, com $1 \leq i \leq n$ e $1 \leq j \leq m_i$ e $r \in R$ tais que:

1. $y = \sum_{i=1}^{n} \sum_{j=1}^{m_i} (u_{i,j} x_i v_{i,j}) + r$.

2. $Tip(y) \geq Tip(u_{i,j} x_i v_{i,j})$ para todo i, j.

3. Para todo $b \in supp(r)$, $Tip(x_i)$ não divide b, para $1 \leq i \leq n$.

Note que $Tip(r) \leq Tip(y)$.

Chamaremos aqui r de **resto** da divisão de y por X e denotaremos por $y \Rightarrow_X r$. Segue o algoritmo em pseudocódigo.

```
DIVISAO(y, X = {x_1, ..., x_n})
z ← y
enquanto z ≠ 0
    faça dividi ← falso
         i ← 1
         enquanto i ≤ n
             faça se existem u, v ∈ B tais que
                       Tip(z) = u Tip(x_i) v
                    então m_i ← m_i + 1
                          u_{i,m_i} ← (CTip(z)/CTip(x_i))u
                          v_{i,m_i} ← v
                          z ← z − (CTip(z)/CTip(x_i)) u x_i v
                          dividi ← verdadeiro
                    senão i ← i + 1

         se dividi = falso
            então r ← r + CTip(z) Tip(z)
                  z ← z − CTip(z) Tip(z)
```

Frisa-se que se X é um conjunto qualquer a ordem dos elementos de X pode alterar o valor do resto fornecido pelo algoritmo. Entretanto isso não ocorre se X for uma Base de Gröbner, como nos mostra o seguinte resultado.

Proposição 4.1.1 *Seja G uma base de Gröbner para um ideal I de R, tal que G possua um número finito de elementos com um dado tip. Seja $y \in R$ e seja $X = \{g_1, \ldots, g_n\} = \{g \in G \mid Tip(g) \leq Tip(y)\}$. Se $y \Rightarrow_X r$, então r é independente da ordem dos elementos de X. Na realidade, $r = N(y)$.*

Prova. Seja $y \Rightarrow_X r$. Como $Tip(r) \leq Tip(y)$, vemos que $Tip(r)$ não é divisível por nenhum elemento de $Tip(G)$. Com isso, $r \in span(Nontip(I))$. Mas $y = \sum_{i=1}^{n} \sum_{j=1}^{m_i} (u_{i,j} g_i v_{i,j}) + r$, com $r \in span(Nontip(I))$ e $u_{i,j} g_i v_{i,j} \in I$, para cada i, j. Assim, pelo Teorema 3.1.3, $r = N(y)$. □

Corolário 4.1.2 *Seja G uma base de Gröbner com as mesmas propriedades da Proposição. Então, dado $v \in R$, existe um algoritmo para calcular $N(v)$.*

4.2 Construção de Bases de Gröbner

Ao longo desta seção, seja I um ideal de R. Antes de apresentarmos o processo de construção de uma Base de Gröbner para I a partir de um conjunto gerador de I, precisamos de algumas definições.

Definição 4.2.1 ***(Tip-redução)*** *Seja $X \subseteq R$. Dizemos que X é **tip-reduzido** se para $x, y \in X$ com $x \neq y$, $Tip(x)$ não divide $Tip(y)$.*

Seja $X = \{x_1, \ldots, x_n\}$ e sejam $1 \leq i, j \leq n$ tais que $Tip(x_i) = u\,Tip(x_j)v$ para algum $u, v \in \mathcal{B}$. Então, se tomamos

$$X' = \{x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_n\}$$

com $x_i' = x_i - (CTip(x_i)/CTip(x_j))ux_jv$, nota-se que $\langle X \rangle = \langle X' \rangle$.

Definição 4.2.2 ***(Uniformidade)*** *Um elemento $v \in R$, onde $v = \sum_{i=1}^{m} \alpha_i b_i$, com $\alpha \in K^*$ e $b_i \in \mathcal{B}$ é* ***uniforme*** *se para cada $c \in \mathcal{B}$,*

$cb_i = 0$ *para todo* $1 \leq i \leq m$ *ou* $cb_i \neq 0$ *para todo* $1 \leq i \leq m$.

Em uma álgebra de caminhos um elemento é uniforme se todos os elementos de seu suporte começam no mesmo vértice e todos eles terminam no mesmo vértice.

Nota-se ainda que todo elemento f de R pode ser escrito como uma soma de elementos uniformes $f = f_1 + f_2 + \cdots + f_n$. Neste caso, dizemos que f_i, $1 \leq i \leq n$ são as **projeções uniformes** de f.

Proposição 4.2.1 *Seja R uma álgebra de caminhos e I um ideal de R. Se $f = f_1 + f_2 + \cdots + f_n \in I$, onde cada f_i é um elemento uniforme, então $f_i \in I$, para cada i e I pode ser gerado por elementos uniformes.*

Prova. Seja $f \in I$ como no enunciado do Proposição. Seja ainda $\{e_\alpha \mid \alpha \in \mathcal{A}\}$ o conjunto de vértices vistos como idempotentes em R. Então $\sum_{\alpha,\beta \in \mathcal{A}} e_\alpha f e_\beta$ é a decomposição de f em suas projeções uniformes. Assim, como cada parcela da soma pertence a I, temos o resultado procurado. $\square$

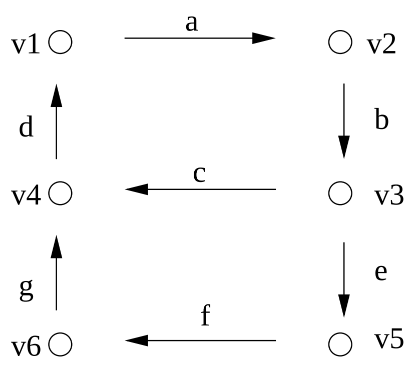
Definição 4.2.3 ***(Relação de Sobreposição)*** *Sejam $f, g \in R$ e suponha elementos $b, c \in \mathcal{B}$ tais que:*

1. $Tip(f)c = b\,Tip(g)$
2. $Tip(f)$ *não divide* b *e* $Tip(g)$ *não divide* c

A ***relação de sobreposição*** *de f e g por b e c é*

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

Para ilustrar o conceito de relação de sobreposição, tomemos o seguinte exemplo, onde $R = K\Gamma$ e Γ é o carcaz abaixo:



Seja ainda $v_1 < v_2 \cdots < v_6 < a < b \cdots < g$ e sejam $p = abcdabcd - abefgd$ e $q = cdabcda - efgda$. Então:

$$o(p, q, abcdab, abcda) = p(abcda) - (abcdab)q \neq 0$$
$$o(p, q, ab, a) = p(a) - (ab)q = 0$$
$$o(q, q, cdab, bcda) = q(bcda) - (cdab)q \neq 0$$

Com isso, podemos apresentar o seguinte Teorema, que é a base para o processo de construção de Bases de Gröbner.

Teorema 4.2.2 *Seja R uma K-álgebra com base multiplicativa $\mathcal{B}$ com uma ordem admissível $\leq$. Seja $G \subseteq R$ tal que*

1. *G é um conjunto de elementos uniformes*
2. *G é um conjunto tip-reduzido*
3. *Para cada relação de sobreposição*
$$o(g_1, g_2, a, b) \Rightarrow_G 0$$
com $g_1, g_2 \in G$,

Então G é uma Base de Gröbner para $\langle G \rangle$.

Como nos mostra a Proposição 4.2.1 e o comentário seguindo a definição 4.2.1, as hipóteses 1 e 2 do Teorema não consistem nenhuma perda de generalidade.

O processo de construção de Bases de Gröbner recebe como entrada um conjunto $\{f_1, \ldots, f_n\}$ de elementos uniformes e tip-reduzidos e devolve um conjunto G (possivelmente infinito) de forma que G é uma Base de Gröbner para $I = \langle f_1, \ldots, f_n \rangle$.

BG($f_1, \ldots, f_n$)
para $i \leftarrow 1$ **até** n
    faça $g_i \leftarrow f_i$
$G \leftarrow \{g_1, g_2, \ldots, g_n\}$
$Count \leftarrow n$
repita
        $H \leftarrow G$
        para cada relação de sobreposição $o(h, k, a, b)$
         com $h, k \in H$
            faça se $o(h, k, a, b) \Rightarrow_H r \neq 0$
                então $Count \leftarrow Count + 1$
                    $g_{Count} \leftarrow r$
                    $G \leftarrow G \cup \{g_{Count}\}$
                    enquanto $Tip(g_i) = u\,Tip(g_j)$
                    , com $i \neq j$ e $u, v \in \mathcal{B}$
                        faça $g_i \leftarrow g_i -$
                            $(CTip(g_i)/CTip(g_j))ug_jv$

    até $H = G$

Infelizmente não temos garantias de que esse processo pára para qualquer entrada. Mas pode ser provado que se o ideal tiver um conjunto monomial gerador finito, o processo pára em um número finito de passos.

Referências Bibliográficas

[1] F. U. Coelho, (1992) *Uma Introdução à Teoria de Representações de Álgebras.* XII Escola de Álgebra.

[2] D. Farkas e E. Green, *Do Subspaces Have Distinguished bases?*, Rocky Mountain Journal of Mathematics, Volume 22 Number 4, Fall 1992, 1295-1302.

[3] D. Farkas, C. Feustel e E. Green, *Synergy in the Theories of Gröbner Bases and Path Algebras*, Canadian Journal of Mathematics, Vol 45 (4), 1993, 727-739.

[4] E. L. Green, (1999) *Noncommutative Gröbner Bases and Projective Resolutions.* In Michler and Schneider, eds, *Proceedings of the Euroconference Computational Methods for Representations of Groups and Algebras*, Essen, 1997, volume 173 of Progress in Mathematics, pp. 29-60. Basel, Birkhäuser Verlag.

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

[6] G. Higman, (1952) *Ordering by Divisibility in Abstract Algebras.* Proc. London Math. Soc (3) 2 (1952), 326-336.

[7] N. Jacobson, *Basic Algebra 1.* W. H. Freeman and Company, 1985.