Arthur Campos

Bases de Gröbner

Uberlândia-MG

Dezembro, 2018

Arthur Campos

Bases de Gröbner

Trabalho apresentado à Faculdade de Matemática, como parte dos requisitos para obtenção do título de LICENCIADO EM MATEMÁTICA

Universidade Federal de Uberlândia – UFU

Faculdade de Matemática

Orientador: Prof. Dr. Cícero Carvalho

Uberlândia-MG

Dezembro, 2018

Arthur Campos

Bases de Gröbner

Trabalho apresentado à Faculdade de Matemática, como parte dos requisitos para obtenção do título de LICENCIADO EM MATEMÁTICA

Trabalho aprovado. Uberlândia-MG, 20 de dezembro de 2018:

Prof. Dr. Cícero Carvalho
Orientador

Prof. Dr. Victor Gonzalo L. Neumann

Prof. Dr. Neiton Pereira da Silva

Uberlândia-MG
Dezembro, 2018

Agradecimentos

Agradeço ao meu orientador Cícero Carvalho por ter me dado a honra de trabalhar com ele este ano, aos meus pais pelo apoio incondicional nos momentos em que me desanimei e pelo exemplo de determinação e força que são em minha vida. Agradeço também ao meu amigo João Paulo Guardieiro por me escutar e me ajudar nas demonstrações feitas neste trabalho, e aos professores Victor Gonzalo e Neiton Pereira por aceitarem o convite à banca.

"If I have seen further it is by
standing on the shoulders of giants.
(Isaac Newton)

Sumário

1 Introdução

Seja K um corpo e denote por $K[\boldsymbol{X}]$ o anel de polinômios $K[X_1, \ldots, X_n]$. O produto $aX_1^{\alpha_1} \cdots X_n^{\alpha_n}$, onde $a \in K^*$ e $\alpha_1, \ldots, \alpha_n$ são inteiros não negativos é chamado de termo, enquanto $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ é chamado de monômio. Às vezes o monômio $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ será denotado por $\boldsymbol{X}^{\boldsymbol{\alpha}}$ onde $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ e $\mathbb{N}_0$ é o conjunto dos inteiros não negativos. Denotamos $\mathcal{M}$ o conjunto dos monômios de $K[\boldsymbol{X}]$. Dado um polinômio $f \in K[\boldsymbol{X}]$ dizemos que um monômio M aparece em f se o coeficiente de M em f é não nulo.

Neste capítulo, falaremos sobre o método de bases de Gröbner, que irá nos permitir resolver problemas de ideais polinomiais por meio de um algoritmo. Este método é também usado em vários sistemas de álgebra computacional para estudar ideais polinomiais específicos que surgem em aplicações. Neste capítulo e no próximo, vamos nos concentrar nestes dois problemas:

a. Todo ideal $I \subset K[\boldsymbol{X}]$ tem um conjunto gerador finito? Em outras palavras, nós podemos escrever $I = \langle f_1, \ldots, f_s \rangle$ para algum $f_i \in K[\boldsymbol{X}]$?

b. Dado $f \in K[\boldsymbol{X}]$ e um ideal $I = \langle f_1, \ldots, f_s \rangle$, determine se $f \in I$.

Para começar nosso estudo de bases de Gröbner, vamos considerar alguns casos especiais em que sabemos técnicas algoritmicas para resolver os problemas dados acima.

Exemplo 1.1. Quando $n = 1$, sabemos dizer se um ideal $I \subset K[\boldsymbol{X}]$ tem um conjunto gerador finito. Nomeadamente, dado um ideal $I \subset K[X]$, nós sabemos que $I = \langle g \rangle$ para algum $g \in K[X]$. Então, ideais tem uma simples descrição neste caso.

Também vimos que dado $f \in K[X]$, para saber se $f \in I = \langle g \rangle$, dividimos g por f:

$$f = q \cdot g + r,$$

onde $q, r \in K[X]$ e $r = 0$ ou grau(r) <grau(g). Então nós provamos que $f \in I$ se e somente se $r = 0$. Logo, temos um teste algoritmo para saber se um polinômio está num ideal para o caso $n = 1$.

Exemplo 1.2. Agora, seja n (o número de variáveis) arbitrário, e considere o problema de resolver um sistema de equações polinomiais:

$$\begin{aligned} a_{11}X_1 + \cdots a_{1n}X_n + b_1 &= 0 \\ &\vdots \\ a_{m1}X_1 + \cdots + a_{mn}X_n + b_m &= 0. \end{aligned} \tag{1.1}$$

onde cada polinômio é linear.

Por exemplo, considere o sistema

$$\begin{aligned} 2X_1 + 3X_2 - X_3 &= 0 \\ X_1 + X_2 - 1 &= 0 \\ X_1 + X_3 - 3 &= 0 \end{aligned} \tag{1.2}$$

Cuja matriz do sistema na forma escalonada é representada por :

$$\begin{pmatrix} 2 & 3 & -1 & 0 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

A forma desta matriz mostra que X_3 é uma variável livre e chamando $X_3 = t$ (qualquer elemento de K), temos

$$\begin{aligned} X_1 &= -T + 3, \\ X_2 &= T - 2, \\ X_3 &= T. \end{aligned}$$

Essas são as equações paramétricas para uma linha L em K^3. O sistema de equações original mostra L como uma variedade afim.

2 Ordenando monômios em mais de uma variável

Definição 2.1. Uma **ordem monomial** é uma relação $>$ sobre o conjunto $\mathcal{M}$ de monômios $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ satisfazendo:

(i) $>$ é uma ordem total sobre $\mathcal{M}$.

(ii) Se $X_1^{\alpha_1} \dots X_n^{\alpha_n} > X_1^{\beta_1} \dots X_n^{\beta_n}$ e $X_1^{\gamma_1} \dots X_n^{\gamma_n} \in K[\boldsymbol{X}]$ então $X_1^{\alpha_1} \dots X_n^{\alpha_n} \cdot X_1^{\gamma_1} \dots X_n^{\gamma_n} > X_1^{\beta_1} \dots X_n^{\beta_n} \cdot X_1^{\gamma_1} \dots X_n^{\gamma_n}$.

(iii) $>$ é uma boa ordenação sobre $\mathcal{M}$. Isto significa que todo subconjunto não vazio de $\mathcal{M}$ tem um menor elemento sob $>$.

O seguinte lema irá nos ajudar a entender em que o item (iii) significa.

Lema 2.2. *Uma relação de ordem $>$ sobre $\mathcal{M}$ é uma boa ordenação se e somente se toda sequência estritamente decrescente em $\mathcal{M}$,*

$$X_1^{\alpha_{1,1}} \dots X_n^{\alpha_{n,1}} > X_1^{\alpha_{1,2}} \dots X_n^{\alpha_{n,2}} > X_1^{\alpha_{1,3}} \dots X_n^{\alpha_n,3} > \dots$$

eventualmente termina.

Demonstração. Provemos pela contrapositiva,

($\Rightarrow$) Dado uma sequência infinita então $\{ X_1^{\alpha_{1,1}} \dots X_n^{\alpha_{n,1}}, X_1^{\alpha_{1,2}} \dots X_n^{\alpha_{n,2}}, X_1^{\alpha_{1,3}} \dots X_n^{\alpha_n,3}, \dots\}$ é um subconjunto não vazio de $\mathcal{M}$ com nenhum elemento mínimo, logo $>$ não é uma boa ordenação.

($\Leftarrow$) Se $>$ não é uma boa ordenação, então algum conjunto não vazio $S \subset \mathcal{M}$ não tem um menor elemento. Agora, pegue $X_1^{\alpha_{1,1}} \dots X_n^{\alpha_{n,1}} \in S$. Como $X_1^{\alpha_{1,1}} \dots X_n^{\alpha_{n,1}}$ não é o elemento mínimo, existe $X_1^{\alpha_{1,2}} \dots X_n^{\alpha_{n,2}}$ tal que $X_1^{\alpha_{1,1}} \dots X_n^{\alpha_{n,1}} > X_1^{\alpha_{1,2}} \dots X_n^{\alpha_{n,2}}$ em S. Agora, $X_1^{\alpha_{1,2}} \dots X_n^{\alpha_{n,2}}$ não é o menor elemento de S, assim existe um $X_1^{\alpha_{1,3}} \dots X_n^{\alpha_{n,3}}$ tal que $X_1^{\alpha_{1,2}} \dots X_n^{\alpha_{n,2}} > X_1^{\alpha_{1,3}} \dots X_n^{\alpha_{n,3}}$ em S. Continuando desta maneira, encontramos uma sequência estritamente decrescente que não termina. □

Definição 2.3. (**Ordem Lexicográfica**). Dados dois monômios $\prod_{i=1}^n X_i^{\alpha_i}$ e $\prod_{i=1}^n X_i^{\beta_i}$ dizemos que:

$$\prod_{i=1}^{n} X_i^{\alpha_i} >_{lex} \prod_{i=1}^{n} X_i^{\beta_i}$$

se existe $i \in 1, ...n$ tal que $\alpha_i > \beta_i$ e $\alpha_j = \beta_j$ para todo $j < i$

Proposição 2.4. *A ordem lexicográfica sobre $\mathcal{M}$ é uma ordem monomial.*

Demonstração.

- Que $>_{lex}$ é uma ordem total segue diretamente da definição porque dados dois monômios é sempre possível comparar os expoentes deles.

- Se $\prod_{i=1}^{n} X_i^{\alpha_i} >_{lex} \prod_{i=1}^{n} X_i^{\beta_i}$, então existe $i \in 1, ...n$ tal que $\alpha_i > \beta_i$ e $\alpha_j = \beta_j$ para todo $j < i$, $\prod_{i=1}^{n} X_i^{\alpha_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i} = \prod_{i=1}^{n} X_i^{\alpha_i+\gamma_i}$ e $\prod_{i=1}^{n} X_i^{\beta_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i} = \prod_{i=1}^{n} X_i^{\beta_i+\gamma_i}$. Então, em $(\alpha+\gamma)-(\beta+\gamma) = \alpha-\beta$ existe $i \in 1, ...n$ tal que $\alpha_i > \beta_i$ e $\alpha_j = \beta_j$ para todo $j < i$. Assim $\prod_{i=1}^{n} X_i^{\alpha_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i} > \prod_{i=1}^{n} X_i^{\beta_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i}$.

- Suponha que $>_{lex}$ não é uma boa ordenação. Então pelo Lema 2.2 existe uma sequência infinita estritamente decrescente $X_1^{\alpha_{1,1}} \dots X_n^{\alpha_{n,1}} > X_1^{\alpha_{1,2}} \dots X_n^{\alpha_{n,2}} > X_1^{\alpha_{1,3}} \dots X_n^{\alpha_{n,3}} > \dots$ de elementos de $\mathcal{M}$. Considere as primeiras entradas de $X_1^{\alpha_{1,i}} \dots X_n^{\alpha_{n,i}} \in \mathcal{M}$. Pela definição de ordem lexicográfica, estas primeiras entradas formam uma sequência não crescente de inteiros não negativos. Como o conjunto dos inteiros não negativos é bem ordenado, as primeiras entradas de $X_1^{\alpha_{1,i}} \dots X_n^{\alpha_{n,i}}$ devem estabilizar em algum momento. Isto é, existe um k tal que as primeiras componentes de $X_1^{\alpha_{1,i}} \dots X_n^{\alpha_{n,i}}$ com $i \geq k$ são iguais. Começando de $X_1^{\alpha_{1,k}} \dots X_n^{\alpha_{n,k}}$, a segunda e subsequentes entradas continuam tendo uma ordem lexicográfica. As segundas entradas de $X_1^{\alpha_{1,k}} \dots X_n^{\alpha_{n,k}}$, $X_1^{\alpha_{1,k+1}} \dots X_n^{\alpha_{n,k+1}}, \dots$ formam uma sequência não crescente. Pela mesma razão de antes, as segundas entradas também estabilizam. Continuando dessa mesma maneira, para algum l, $X_1^{\alpha_{1,l}} \dots X_n^{\alpha_{n,l}}$, $X_1^{\alpha_{1,l+1}} \dots X_n^{\alpha_{n,l+1}} \dots$ são iguais. Isto contradiz o fato de $X_1^{\alpha_{1,l}} \dots X_n^{\alpha_{n,l}} >_{lex} X_1^{\alpha_{1,l+1}} \dots X_n^{\alpha_{n,l+1}}$

□

Definição 2.5. Ordem Lexicográfica Graduada. Seja $\prod_{i=1}^{n} X_i^{\alpha_i}$ e $\prod_{i=1}^{n} X_i^{\beta_i} \in \mathcal{M}$. Dizemos que $\prod_{i=1}^{n} X_i^{\alpha_i} >_{grlex} \prod_{i=1}^{n} X_i^{\beta_i}$ se

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ ou } |\alpha| = |\beta| \text{ e } \prod_{i=1}^{n} X_i^{\alpha_i} >_{lex} \prod_{i=1}^{n} X_i^{\beta_i}.$$

Definição 2.6. Ordem Lexicográfica Graduada Reversa. Seja $\prod_{i=1}^{n} X_i^{\alpha_i}$ e $\prod_{i=1}^{n} X_i^{\beta_i} \in \mathcal{M}$. Dizemos que $\prod_{i=1}^{n} X_i^{\alpha_i} >_{grevlex} \prod_{i=1}^{n} X_i^{\beta_i}$ se

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ ou } |\alpha| = |\beta| \text{ e existe } i \in 1, ...n \text{ tal que } \alpha_i < \beta_i \text{ e } \alpha_j = \beta_j \text{ para todo } j > i$$

Exemplo 2.7. $X^5YZ >_{grlex} X^4YZ^2$, pois ambos os monômios tem grau total 7 e $X^5YZ >_{lex} X^4YZ^2$. Neste caso, também temos que $X^5YZ >_{grevlex} X^4YZ^2$, pois a variável Z em X^5YZ é menor que a variável Z em X^4YZ^2.

Definição 2.8. Seja $f = \sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} \boldsymbol{X}^{\boldsymbol{\alpha}}$ um polinômio não nulo em $K[\boldsymbol{X}]$ e $>$ uma ordem monomial.

- O **multigrau** de f é

  $multigrau(f) = \boldsymbol{\alpha}$ tal que $\boldsymbol{X}^{\boldsymbol{\alpha}}$ é o maior dos monômios de f com respeito a ordem $>$.

- O **coeficiente líder** de f é

$$LC(f) = a_{multigrau(f)} \in K.$$

- O **monômio líder** de f é

$$LM(f) = \boldsymbol{X}^{multigrau(f)}, \text{ (com coeficiente 1).}$$

- O **termo líder** de f é

$$LT(f) = LC(f) \cdot LM(f).$$

Definição 2.9. Seja $>$ uma ordem monomial em $\mathcal{M}$ e sejam $\boldsymbol{\alpha}$ e $\boldsymbol{\beta}$ duas n-uplas cujas entradas são inteiros não negativos. Escrevemos $\boldsymbol{\alpha} > \boldsymbol{\beta}$ se $\boldsymbol{X}^{\boldsymbol{\alpha}} > \boldsymbol{X}^{\boldsymbol{\beta}}$.

Exemplo 2.10. Seja $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2$ e considere a ordem lexicográfica. Assim:

$$\begin{gathered} multigrau(f) = (3,0,0), \\ LC(f) = -5, \\ LM(f) = X^3, \\ LT(f) = -5X^3. \end{gathered}$$

Lema 2.11. *Seja $f, g \in K[\boldsymbol{X}]$ polinômios não nulos. Então:*

- *(i) $multigrau(f \cdot g) = multigrau(f) + multigrau(g)$.*
- *(ii) Se $f + g \neq 0$, então $multigrau(f + g) \leq max(multigrau(f), multigrau(g))$. Se, além disso, $multigrau(f) \neq multigrau(g)$, então igualdade ocorre.*

Demonstração. (i) Por definição o multigrau de $f \cdot g$ é o expoente do termo líder de $f \cdot g$. É claro que o termo líder de $f \cdot g$ é igual ao termo líder de f vezes o termo líder g. Seja $a_{\boldsymbol{\alpha}}\boldsymbol{X}^{\alpha}$ o termo líder de f onde $\boldsymbol{\alpha}$ é o multigrau de f e $b_{\boldsymbol{\beta}}\boldsymbol{X}^{\beta}$ o termo líder de g onde $\boldsymbol{\beta}$ é o multigrau de g. Assim $a_{\boldsymbol{\alpha}}\boldsymbol{X}^{\alpha} \cdot b_{\boldsymbol{\beta}}\boldsymbol{X}^{\beta} = a_{\boldsymbol{\alpha}}b_{\boldsymbol{\beta}}\boldsymbol{X}^{\alpha+\beta}$ onde o multigrau da multiplicação é $(\boldsymbol{\alpha} + \boldsymbol{\beta})$. Assim multigrau$(f \cdot g)$ = multigrau(f)+ multigrau(g).

(ii) Se $f+g \neq 0$, afirmamos que o multigrau de $f+g$ é menor ou igual que o máximo dos multigraus de f e g pois como estamos somando dois polinômios o multigrau da soma obviamente não pode ser aumentado, isto poderia acontecer se fizéssemos a multiplicação de f e g, porém com a soma isto é impossível. O que pode acontecer é que nessa soma

alguns termos de f e g se cancelem, inclusive os termos líderes, fazendo com que o multigrau da soma seja menor que o máximo dos multigraus. Porém como não podemos garantir que isto ocorra sempre, segue que multigrau$(f+g) \leq$ max(multigrau(f),multigrau(g)).

Se multigrau$(f) \neq$ multigrau(g) então suponha que o multigrau de f é maior que o multigrau de g, assim não existe a possibilidade do termo líder de f ser cancelado por nenhum termo de g, logo o multigrau$(f+g) =$ máx(multigrau(f),multigrau(g)).

□

3 Algoritmo da divisão em mais de uma variável

Começamos esta seção enunciando o algoritmo da divisão em $K[\boldsymbol{X}]$;

Teorema 3.1. ***(Algoritmo da Divisão em*** $K[\boldsymbol{X}]$***).*** *Fixe uma ordem monomial $>$ em $K[\boldsymbol{X}]$, e seja $F = (f_1, \ldots, f_s)$ uma s-upla ordenada de polinômios em $K[\boldsymbol{X}]$. Então todo $f \in K[\boldsymbol{X}]$ pode ser escrito como*

$$f = a_1 f_1 + \ldots + a_s f_s + r.$$

onde $a_i, r \in K[\boldsymbol{X}]$, ou $r = 0$ ou r é uma combinação linear, com coeficientes em K, de monômios, nos quais nenhum é divisível por qualquer $LT(f_1), \ldots, LT(f_s)$. Chamamos r de resto da divisão de f por F. Além disso, se $a_i f_i \geq 0$, então

$$multigrau(f) \geq multigrau(a_i f_i).$$

Neste trabalho não iremos demonstrar o algoritmo, pois a demonstração é muito técnica, porém vamos descrever o algoritmo e dar alguns exemplos mostrando sua utilização. A ideia é basicamente a mesma do caso de quando dividimos dois polinômios em uma variável: usaremos os termos líderes de $f_1, \ldots, f_s$ para cancelar o termo líder de f e dos polinômios subsequentes que aparecerão nos passos da divisão. A novidade aqui é que às vezes o termo líder dos polinômios subsequentes não são múltiplos de qualquer um dos $LT(f_1), \ldots, LT(f_s)$, então nós os movemos diretamente para o resto e prosseguimos com o algoritmo. É claro que isto é um processo finito pois análogo ao caso de uma variável, o monômio líder dos polinômios subsequentes é sempre menor (com relação a ordem monomial) que o do polinômio anterior, isso nos leva a uma sequência estritamente decrescente em $\mathcal{M}$, que sabemos pelo Lema 2.2 sempre ter um fim.

Exemplo 3.2. Primeiramente, dividiremos $f = X^2Y + XY^2 + Y^2$ por $f_1 = XY - 1$ e $f_2 = Y^2 - 1$ usando a ordem lexicográfica com $X > Y$. Iremos empregar o mesmo esquema feito pela divisão de polinômios em uma variável, a diferença é que agora existem mais divisores e quocientes. O termo líder de f_1 é XY e o termo líder de f_2 é Y^2, como o termo líder de f_1 é o único que divide o termo líder de f que é igual a X^2Y, começaremos a divisão de f por f_1. Temos que $LT(f) = X^2Y = LT(f_1)X$ então escrevemos $f = Xf_1 + (f - Xf_1)$ ou seja $f = Xf_1 + (XY^2 + X + Y^2)$. Aplicamos o processo agora ao resto intermediário $XY^2 + X + Y^2$. Temos que o termo líder desse polinômio é XY^2 (e observe que $XY^2 < LT(f) = X^2Y$), além disso XY^2 é múltiplo de $LT(f_1) = XY$. Como $XY^2 = LT(f_1)Y$ escrevemos $XY^2 + X + Y^2 = Yf_1 + (X + Y^2 + Y)$ e portanto

$f = Xf_1 + Yf_1 + (X + Y^2 + Y) = (X + Y)f_1 + (X + Y^2 + Y)$. Note que agora o termo líder do resto intermediário que é igual a X, que não é múltiplo nem de $LT(f_1) = XY$ nem de $LT(f_2) = Y^2$. Entretanto $X + Y^2 + Y$ não é o resto final da divisão pois o termo líder de f_2 divide Y^2. Assim, vamos mover X para o resto, escrevemos $f = (X + Y)f_1 + (Y^2 + Y) + X$ e vamos dividir $Y^2 + Y$ por f_1 e f_2. Temos que termo líder de $Y^2 + Y$ é Y^2 e além disso $Y^2 = LT(f_2) \cdot 1$, logo escrevemos $X^2Y + XY^2 + Y^2 = (X + Y)f_1 + 1 \cdot f_2 + (Y + 1) + X$. Agora o termo líder do resto intermediário que é igual a Y não é múltiplo do termo líder de f_2 nem do termo líder de f_1, assim vamos mover Y para o resto e escrevemos $f = (X + Y)f_1 + 1 \cdot f_2 + (1) + X + Y$. O termo líder do resto intermediário que é igual a 1 não é múltiplo de nenhum dos termos líderes de f_1 e f_2 ,assim também movemos 1 para o resto. Agora, como o resto intermediário é 0 finalizamos o processo.

$$\text{Portanto } f = X^2Y + XY^2 + Y^2 = (X + Y) \cdot (XY - 1) + 1(Y^2 - 1) + X + Y + 1$$

Uma boa propriedade do algoritmo da divisão em $K[X]$ é a maneira que ele resolve o problema de um polinômio pertencer ou não a um ideal. Conseguimos algo similar para mais variáveis? Um Corolário do Teorema 3.1 simples de ver é que se feita a divisão de f por $F = (f_1 \dots f_s)$ e obtido $r = 0$, temos

$$f = a_1 f_1 + \dots a_s f_s,$$

de modo que $f \in \langle f_1 \dots f_s \rangle$. Então $r = 0$ é uma condição suficiente para um polinômio f pertencer a um dado ideal. Entretanto, $r = 0$ não é uma condição necessária para f pertencer ao ideal. Veremos isso no exemplo abaixo:

Exemplo 3.3. Seja $f_1 = XY + 1, f_2 = Y^2 - 1 \in K[X, Y]$ com a ordem lexicográfica. Dividindo $f = XY^2 - X$ por $F = (f_1, f_2)$ o resultado é

$$XY^2 - X = Y \cdot (XY + 1) + 0 \cdot (Y^2 - 1) + (-X - Y).$$

Com $F = (f_2, f_1)$, entretanto, temos

$$XY^2 - X = X \cdot (Y^2 - 1) + 0(XY + 1) + 0.$$

A segunda divisão mostra que $f \in \langle f_1, f_2 \rangle$. Então mesmo na primeira divisão o resto dando diferente de 0, f ainda assim pertence a $\langle f_1, f_2 \rangle$.

4 Ideais monomiais e Lema de Dickson

Definição 4.1. Um ideal $I \subset K[\boldsymbol{X}]$ é um **ideal monomial** se existe um conjunto de monômios que geram I.

Um exemplo de um ideal monomial é dado por $I = \langle X^4Y^2, X^3Y^4, X^2Y^5 \rangle \subset K[X, Y]$.

Lema 4.2. *Seja $I = \langle \boldsymbol{X}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in A \rangle$ um ideal monomial. Então um monômio $\boldsymbol{X}^{\boldsymbol{\beta}}$ pertence a I se e somente se $\boldsymbol{X}^{\boldsymbol{\beta}}$ é múltiplo de $\boldsymbol{X}^{\boldsymbol{\alpha}}$ para algum $\boldsymbol{\alpha} \in A$.*

Demonstração. ($\Rightarrow$) Se $\boldsymbol{X}^{\boldsymbol{\beta}} \in I$ então $\boldsymbol{X}^{\boldsymbol{\beta}} = \sum_{i=1}^{n} \boldsymbol{X}^{\boldsymbol{\alpha_i}} h_i$. Assim $\boldsymbol{X}^{\boldsymbol{\beta}}$ é um monômio que certamente aparece em algum dos polinômios $\boldsymbol{X}^{\boldsymbol{\alpha_i}} h_i$, para $i = 1, \ldots, n$, e portanto é múltiplo de $\boldsymbol{X}^{\boldsymbol{\alpha_i}}$ para algum $i = 1, \ldots, n$.

($\Leftarrow$) Se $\boldsymbol{X}^{\boldsymbol{\beta}}$ é um múltiplo de $\boldsymbol{X}^{\boldsymbol{\alpha}}$ para algum $\alpha \in A$, então $\boldsymbol{X}^{\boldsymbol{\beta}} \in I$ pela definição de ideal.

□

Lema 4.3. *Seja I um ideal monomial, e seja $f \in K[\boldsymbol{X}]$. Então as seguintes afirmações são equivalentes:*

- *$f \in I$.*
- *Todo termo de f pertence a I*
- *f é uma K-combinação linear de monômios em I.*

Demonstração. $(i) \Rightarrow (iii)$ Considere $I = \langle m_1, \ldots m_s \rangle$. Como $f \in I, f = \sum_{i=1}^{s} m_i h_i$ e podemos expandir cada h_i como K-combinações lineares de monômios. Assim aplicando a distributiva dos m_i's o resultado segue.

As implicações $(iii) \Rightarrow (ii) \Rightarrow (i)$ são triviais. □

Corolário 4.4. *Dois ideais monomiais I e J são iguais se e somente se eles contém os mesmos monômios.*

Demonstração. ($\Rightarrow$) Trivial

($\Leftarrow$)Se os ideais contém os mesmos monômios, sabemos pelo item (iii) do Lema 4.3 que todo $f \in I$ é uma K-combinação linear de monômios em I, mas esses monômios

também estão em J, então f uma K-combinação linear de monômios em J, logo $f \in J$. Fazendo essa mesma análise para um polinômio qualquer $g \in J$ chegamos que $f \in I$. Como todo polinômio do ideal I pertence ao ideal J e todo polinômio do ideal J pertence ao ideal I concluímos que $I = J$ □

Lema 4.5 (Dickson)**.** *Seja I um ideal monomial de $K[\boldsymbol{X}]$, então existe um conjunto finito de monômios que geram I.*

Demonstração. Usaremos indução sobre o número de variáveis. O caso de uma variável é imediato uma vez que em $K[X]$ todo ideal é principal, ou seja, $I = \langle f \rangle$ com $f \in K[X]$. Assim dado um monômio $m \in I$ temos que $m = h \cdot f$ para algum $h \in K[X]$. Pela igualdade de polinômios, segue que f (e h) deve ser um monômio.

Agora suponhamos que o teorema seja válido para ideais em anéis de polinômios com $n-1$ variáveis, com $n \geq 2$. Seja I um ideal monomial de $K[\boldsymbol{X}]$ e escolha um monômio $f_1 \in I$ de tal forma que $f_1 = g_1 \cdot X_n^{\alpha_1}$, onde $g_1 \in \mathcal{M}_{n-1}$ e $\alpha_1 \in \mathbb{N}$ é o menor possível. Se $I = \langle f_1 \rangle$ então o lema está demonstrado. Caso contrário, escolha um monômio $f_2 = g_2 \cdot X_n^{\alpha_2} \in I \backslash \langle f_1 \rangle$ onde $g_2 \in \mathcal{M}_{n-1}$ e α_2 é mínimo. Observe que pelo processo de escolha, necessariamente $\alpha_2 \geq \alpha_1$. Se $I = \langle f_1, f_2 \rangle$ então provamos o lema. Caso contrário continuamos o processo. Vamos supor que este procedimento continua indefinidamente, ou seja, que possamos obter uma sequência infinita de monômios $f_1, f_2, \ldots \in I$ tal que $f_i = g_i \cdot X_n^{\alpha_i} \in I \setminus \langle f_1, \ldots, f_{i-1} \rangle$ com $g_i \in \mathcal{M}_{n-1}, \alpha_i \in \mathbb{N}$ o menor possível e $\alpha_i \geq \alpha_{i-1}$ para todo $i > 1$.

Por hipótese de indução, temos que o ideal J de $K[X_1, \ldots X_{n-1}]$ dado por $J = \langle \{g_i \,|\, i = 1, \ldots \text{ e } g_i \in \mathcal{M}_{n-1}\} \rangle$ é finitamente gerado, ou seja, existem $m_1, \ldots, m_r \in \mathcal{M}_{n-1}$ tais que $J = \langle m_1, \ldots, m_r \rangle$. Dado g_i como acima, temos $g_i \in \langle m_1, \ldots, m_r \rangle$, ou seja, existe um $p \in \mathcal{M}_{n-1}$ de modo que $g_i = p \cdot m_j$ para algum $j \in 1, \ldots, r$.

Por outro lado $m_j \in J$, então existe um monômio $q \in \mathcal{M}_{n-1}$ tal que $m_j = q \cdot g_k$ para algum g_k como descrito acima. Deste modo, temos que $g_i = p \cdot q \cdot g_k$.

Se $i = k$, então $p \cdot q = 1$, ou seja, $p = \alpha \in K \setminus \{0\}$ e $g_i = \alpha \cdot m_j$. Como a sequência $g_1, g_2, \ldots \in \mathcal{M}_{n-1}$ é infinita não podemos ter este caso indefinidamente, ou seja, existem índices $i \neq k$ tais que $g_k \mid g_i$, digamos $g_i = m \cdot g_k$ com $m \in \mathcal{M}_{n-1}$. Sem perda de generalidade podemos supor $i > k$. Deste modo,

$$f_i = g_i \cdot X_n^{\alpha_i} = m \cdot g_k \cdot X_n^{\alpha_i - \alpha_k} \cdot X_n^{\alpha_k} = m \cdot X_n^{\alpha_i - \alpha_k} \cdot f_k$$

e $f_i \in \langle f_k \rangle \subset \langle f_1, \ldots, f_k \rangle$, contrariando a escolha de f_i.

Segue assim, que existe um índice $s \in \mathbb{N}_*$ tal que $I = \langle f_1, \ldots, f_s \rangle$, ou seja, I é finitamente gerado por monômios. □

Corolário 4.6. *Seja $>$ uma relação de ordem sobre $\mathbb{Z}_{\geq 0}^n$ satisfazendo:*

- $>$ *é uma ordem total sobre* $\mathbb{Z}^n_{\geq 0}$.
- *Se* $\boldsymbol{\alpha} > \boldsymbol{\beta}$ *e* $\boldsymbol{\gamma} \in \mathbb{Z}^n_{\geq 0}$, *então* $\boldsymbol{\alpha} + \boldsymbol{\gamma} > \boldsymbol{\beta} + \boldsymbol{\gamma}$.

Então $>$ *é bem ordenado se e somente se* $\boldsymbol{\alpha} \geq 0$ *para todo* $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geq 0}$

Demonstração. ($\Rightarrow$) Assumindo que $>$ é uma boa ordenação, seja α_0 o menor elemento de $\mathbb{Z}^n_{\geq 0}$, precisamos mostrar que $\alpha_0 \geq 0$. Pela contrapositiva, se $0 > \alpha_0$, então pela hipótese (ii), podemos somar α_0 de ambos os lados, assim obtemos $\alpha_0 > 2\alpha_0$, que é impossível pois α_0 é o menor elemento de $\mathbb{Z}^n_{\geq 0}$

($\Leftarrow$) Seja $A \subset \mathbb{Z}^n_{\geq 0}$ um conjunto não vazio. Como $I = \langle \boldsymbol{X}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in A \rangle$ é um ideal monomial, o Lema de Dickson nos dá $\boldsymbol{\alpha(1)}, \ldots, \boldsymbol{\alpha(s)} \in A$ de modo que $I = \langle \boldsymbol{X}^{\boldsymbol{\alpha(1)}}, \ldots, \boldsymbol{X}^{\boldsymbol{\alpha(s)}} \rangle$. Como $>$ é uma relação de ordem total sobre $\mathbb{Z}^n_{\geq 0}$ podemos assumir que $\boldsymbol{\alpha(1)} < \ldots \boldsymbol{\alpha(s)}$. Afirmamos que $\boldsymbol{\alpha(1)}$ é o menor elemento de A. Para provar isso, tome $\boldsymbol{\alpha} \in A$. Então $\boldsymbol{X}^{\boldsymbol{\alpha}} \in I = \langle \boldsymbol{X}^{\boldsymbol{\alpha(1)}}, \ldots, \boldsymbol{X}^{\boldsymbol{\alpha(s)}} \rangle$, de modo que pelo Lema 4.2, $\boldsymbol{X}^{\boldsymbol{\alpha}}$ é divisível por algum $\boldsymbol{X}^{\boldsymbol{\alpha(i)}}$. Isto nos mostra que $\boldsymbol{\alpha} = \boldsymbol{\alpha i} + \boldsymbol{\gamma}$ para algum $\boldsymbol{\gamma} \in \mathbb{Z}^n_{\geq 0}$. Então $\boldsymbol{\gamma} \geq 0$ e hipótese (ii) implicam que

$$\boldsymbol{\alpha} = \boldsymbol{\alpha(i)} + \boldsymbol{\gamma} \geq \boldsymbol{\alpha(i)} + 0 = \boldsymbol{\alpha(i)} \geq \boldsymbol{\alpha(1)}.$$

Então, $\boldsymbol{\alpha(1)}$ é o menor elemento de A. □

5 Teorema da base de Hilbert e bases de Gröbner

Nesta seção saberemos responder se todo ideal $I \subset K[\boldsymbol{X}]$ tem um conjunto gerador finito. Esta discussão nos levará a bases de ideais com "boas" propriedades relativas ao algoritmo da divisão. A ideia chave que usaremos é que uma vez escolhida a ordem monomial, cada $f \in K[\boldsymbol{X}]$ tem um único termo líder. Então, para qualquer ideal I, podemos definir o ideal de termos líderes, da seguinte forma.

Definição 5.1. Seja $I \subset K[\boldsymbol{X}]$ um ideal diferente de $\{0\}$.

- Denotamos por $LT(I)$ o conjunto de termos líderes de I. Então,

$$LT(I) = \{c\boldsymbol{X}^{\boldsymbol{\alpha}} : \text{existe } f \in I \text{ com } LT(f) = c\boldsymbol{X}^{\boldsymbol{\alpha}}\}.$$

- Denotamos por $\langle LT(I)\rangle$ o ideal gerado pelos elementos de $LT(I)$.

Proposição 5.2. *Seja $I \subset K[\boldsymbol{X}]$ um ideal.*

- *(i) $\langle LT(I)\rangle$ é um ideal monomial.*
- *(ii) Existem $g_1, \ldots, g_t \in I$ tais que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.*

Demonstração. (i) Os monômios líderes dos elementos de $I - \{0\}$ geram o ideal monomial $\langle LM(g) : g \in I - \{0\}\rangle$. Os monômios líderes de g e os termos líderes de g diferem apenas por uma constante, assim temos que $\langle LT(g) : g \in I - \{0\}\rangle = \langle LM(g) : g \in I - \{0\}\rangle$. Como o elemento $0 \in I$ não tem termo líder temos que $\langle LT(g) : g \in I - \{0\}\rangle = \langle LT(I)\rangle$. Assim $\langle LT(I)\rangle$ é um ideal monomial. □

Demonstração. (ii) Como $\langle LT(I)\rangle$ é um ideal monomial, o Lema de Dickson nos diz que existe um conjunto finito de monômios $\{g_1, g_2, \ldots g_t\}$ onde $\langle LT(I)\rangle = \langle g_1, \ldots, g_t\rangle$. Como o termo líder de g_i é o próprio g_i para $i \in \{1, \ldots t\}$ temos que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$ □

Agora usando a Proposição 5.2 e o algoritmo da divisão podemos provar a existência de um conjunto gerador finito para todo ideal polinomial, respondendo assim o problema de descrição de um ideal. Seja $I \subset K[\boldsymbol{X}]$ um ideal e considere o ideal associado $\langle LT(I)\rangle$ como definido no início da seção. Como sempre, selecionamos uma ordem monomial particular para usar no algoritmo da divisão e computar termos líderes.

Teorema 5.3. *(Teorema da Base de Hilbert) Todo ideal $I \subset K[\boldsymbol{X}]$ tem um conjunto gerador finito. Isto é, $I = \langle g_1, \ldots, g_t \rangle$ para algum $g_1, \ldots, g_t \in I$.*

Demonstração. Se $I = \{0\}$, tomamos $\{0\}$ como nosso conjunto gerador que certamente é finito. Se I contem algum polinômio não nulo, então um conjuntor gerador $g_1, \ldots, g_t$ para I pode ser construído como seguinte.

Pela Proposição 5.2, existem $g_1, \ldots, g_t \in I$ tais que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Afirmamos que $I = \langle g_1, \ldots, g_t \rangle$.

É claro que $\langle g_1, \ldots, g_t \rangle \subset I$ pois cada $g_i \in I$. Reciprocamente, seja $f \in I$ um polinômio qualquer. Se aplicarmos o algoritmo da divisão na divisão de f por $g_1, \ldots, g_t$, então conseguimos uma expressão da forma

$$f = a_1 g_1 + \ldots + a_t g_t + r$$

onde nenhum dos termos de r é divisível por qualquer termo líder de g_i onde $i \in \{1, \ldots, t\}$. Afirmamos que $r = 0$. Para ver isso, note que

$$r = f - a_1 g_1 - \ldots - a_t g_t \in I.$$

pois $f \in I$ e como $g_1, \ldots, g_t \in I$ a combinação linear deles também pertence a I.

Se $r \neq 0$, então o termo líder de r pertence a $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ e pelo Lema 4.2 segue que o termo líder de r deve ser divisível por algum termo líder de g_i com $i \in \{1, \ldots, t\}$. Isto contradiz o significado de resto, assim r deve ser zero. Então

$$f = a_1 g_1 + \ldots + a_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle,$$

mostrando que $I \subset \langle g_1, \ldots, g_t \rangle$. □

Além de responder o problema da descrição de um ideal, as bases $\{g_1, \ldots, g_t\}$ usadas na prova do Teorema acima tem a propriedade especial que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Nem todas as bases de um ideal se comportam dessa maneira. A essas bases "especiais" daremos o seguinte nome.

Definição 5.4. Fixada uma ordem monomial. Um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal I é dito **Bases de Gröbner** se

$$\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle.$$

Lema 5.5. *Equivalentemente, um conjunto $\{g_1, \ldots, g_t\} \subset I$ é uma base de Gröbner de I se e somente se o termo líder de qualquer elemento de I é divisível por algum termo líder de g_i com $i \in \{1, \ldots, t\}$.*

Corolário 5.6. *Fixada uma ordem monomial. Então todo ideal $I \subset K[\boldsymbol{X}]$ diferente de $\{0\}$ tem uma base de Gröbner. Além disso, qualquer base de Gröbner para um ideal I é uma base de I.*

Demonstração. Dado um ideal não nulo, o conjunto $G = \{g_1, \ldots, g_t\}$ construído na prova do Teorema 5.3 é uma base de Gröbner por definição. Agora, para provar a segunda afirmação, note que se $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$, então pelo Teorema 5.3 sabemos que $I = \langle g_1, \ldots, g_t\rangle$, de modo que G é uma base para I. □

Teorema 5.7. *(Condição de Cadeia Ascendente) Seja $I_1 \subset I_2 \subset I_3 \subset \ldots$ uma cadeia ascendente de ideais em $K[\boldsymbol{X}]$. Então existe um $N \geq 1$ tal que $I_N = I_{N+1} = I_{N+2} = \cdots$.*

Demonstração. Dado uma cadeia ascendente $I_1 \subset I_2 \subset I_3 \subset \ldots$, considere o conjunto $I = \cup_{i=1}^{\infty} I_i$. Iniciamos a demonstração mostrando que I também é um ideal em $K[\boldsymbol{X}]$. Sabemos que $0 \in I$ pois $0 \in I_i$ para todo i. Agora, se $f, g \in I$ então pela definição de I, $f \in I_i$ e $g \in I_j$ para algum i e j (possivelmente diferentes). Entretanto, como os ideais I_i formam uma cadeia ascendente, se considerarmos que $i \leq j$, então ambos f e g estão em I_j. Como I_j é um ideal, a soma $f + g \in I_j$, e consequentemente $f + g \in I$. Logo I é um ideal.

Pelo Teorema da Base de Hilbert, o ideal I deve ter um conjunto gerador finito, isto é $I = \langle f_1, \ldots, f_s\rangle$. Porém cada um dos geradores está contido em algum dos I_j isto é $f_i \in I_{j_i}$ para algum $j_i, i = i, \ldots, s$. Tome N o máximo do j_i. Então pela definição de cadeia ascendente $f_i \in I_N$ para todo i. Então temos

$$I = \langle f_1, \ldots, f_s\rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I.$$

Como resultado a cadeia ascendente se estabiliza em I_N e todos os ideais subsequentes na cadeia são iguais. □

Definição 5.8. Seja K um corpo, e sejam $f_1, \ldots, f_s$ polinômios em $K[\boldsymbol{X}]$. Então definimos

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0 \text{ para todo } 1 \leq i \leq s\}$$

Chamamos $V(f_1, \ldots, f_s)$ a **variedade afim** definida por $f_1, \ldots, f_s$.

Definição 5.9. Seja $I \subset K[\boldsymbol{X}]$ um ideal. Denotemos por $V(I)$ o conjunto

$$V(I) = \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0 \text{ para todo } i\}.$$

Embora um ideal não nulo I sempre contenha infinitos polinômios, o conjunto $V(I)$ pode ser definido por um conjunto finito de equações polinomiais.

Proposição 5.10. *$V(I)$ é uma variedade afim. Em particular, se $I = \langle f_1, \ldots, f_s \rangle$, então $V(I) = V(f_1, \ldots, f_s)$.*

Demonstração. Pelo Teorema da Base de Hilbert, $I = \langle f_1, \ldots, f_s \rangle$ para algum conjunto gerador finito. Afirmamos que $V(I) = V(f_1, \ldots, f_s)$. Primeiro, como $f_i \in I$, se $f(a_1, \ldots, a_n) = 0$ para todo $f \in I$, então $f_i(a_1, \ldots, a_n) = 0$, então $V(I) \subset V(f_1, \ldots, f_s)$. Por outro lado, seja $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$ e seja $f \in I$. Como $I = \langle f_1, \ldots, f_s \rangle$, podemos escrever

$$f = \sum_{i=1}^{s} h_i f_i$$

para algum $h_i \in K[\boldsymbol{X}]$. Então

$$\begin{gathered} f(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) = \\ = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0. \end{gathered}$$

Logo, $V(f_1, \ldots, f_s) \subset V(I)$ e consequentemente, eles são iguais. □

6 Propriedades das bases de Gröbner

Como visto na seção anterior, todo ideal não nulo $I \subset K[\boldsymbol{X}]$ tem uma base de Gröbner. Nesta seção, estudaremos as propriedades desta base e aprenderemos a detectar quando uma base dada é uma base de Gröbner. Começaremos provando que o resto é unicamente determinado quando dividimos por uma base de Gröbner.

Proposição 6.1. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subset K[\boldsymbol{X}]$ e seja $f \in K[\boldsymbol{X}]$. Então há um único $r \in K[\boldsymbol{X}]$ com as seguintes propriedades:*

- *(i) Nenhum termo de r é múltiplo de qualquer $LT(g_1), \ldots, LT(g_t)$.*
- *(ii) Há um $g \in I$ tal que $f = g + r$.*

  Em particular, r é o resto da divisão de f por G independente de como os elementos de G estão listados no algoritmo da divisão.

Demonstração. O algoritmo da divisão nos dá que $f = a_1g_1 + \ldots + a_tg_t + r$, onde r satisfaz (i). Além disso definindo $g = a_1g_1 + \ldots + a_tg_t$ temos $g \in I$ e $f = g + r$ satisfazendo (ii). Isto prova a existência de r. Para provar a unicidade, suponha que $f = g + r = g' + r'$. Então $r - r' = g' - g \in I$, tal que se $r \neq r'$, então $LT(r - r') \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Pelo Lema 4.2, segue que o termo líder de $(r - r')$ é múltiplo de algum termo líder de g_i. Isto é impossível pois nenhum termo de r e r' é múltiplo de algum termo líder de g_i com $i = 1, \ldots t$. Então $r - r'$ deve ser zero, assim $r = r'$ e a unicidade está provada. □

Corolário 6.2. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subset K[\boldsymbol{X}]$ e $f \in K[\boldsymbol{X}]$. Então $f \in I$ se e somente se o resto da divisão de f por G é zero.*

Demonstração. Seja $f \in I$ e seja $f = \sum_{i=1}^{s} q_ig_i + r$ a divisão de f por $(g_1, \ldots, g_s)$. Então $r = f - \sum_{i=1}^{s} q_ig_i \in I$ e assim temos que ter $r = 0$, caso contrário r seria um polinômio não nulo em I cujo termo líder não é múltiplo de $LT(g_i)$ para todo $i = 1, \ldots, s$, contrariando o fato que $g_1, \ldots, g_r$ é uma base de Gröbner para I. A outra implicação é óbvia. □

Definição 6.3. Escreveremos $\overline{f}^F$ para o resto da divisão de f pela ordenada $s - upla$ $F = (f_1, \ldots, f_s)$. Se F é uma base de Gröbner para $(f_1, \ldots, f_s)$, então podemos enxergar F como um conjunto (sem qualquer ordem particular) pela Proposição 6.1.

Por exemplo, com $F = (X^2Y - Y^2, X^4Y^2 - Y^2) \subset K[X, Y]$, usando a ordem lexicográfica, temos

$$\overline{X^5Y}^F = XY^3$$

pois o algoritmo da divisão nos dá que

$$X^5Y = (X^3 + XY)(X^2 - Y^2) + 0 \cdot (X^4Y^2 - Y^2) + XY^3.$$

Definição 6.4. Seja $f, g \in K[\boldsymbol{X}]$ polinômios não nulos.

- (i) Se $multigrau(f) = \alpha$ e $multigrau(g) = \beta$, então defina $\gamma = (\gamma_1, \ldots, \gamma_n)$, onde $\gamma_i = max(\alpha_i, \beta_i)$ para cada i. Chamamos X^γ o **mínimo múltiplo comum** dos monômios líderes de f e g e escrevemos $X^\gamma = LCM(LM(f), LM(g))$.
- (ii) O **S-polinômio** de f e g é a combinação

$$S(f, g) = \frac{X^\gamma}{LT(f)} \cdot f - \frac{X^\gamma}{LT(g)} \cdot g.$$

Por exemplo, seja $f = X^3Y^2 - X^2Y^3 + X$ e $g = 3X^4Y + Y^2$ em $\mathbb{R}[X, Y]$ com a ordem lexicográfica graduada. Então $\gamma = (4, 2)$ e

$$S(f, g) = \frac{X^4Y^2}{X^3Y^2} \cdot f - \frac{X^4Y^2}{3X^4Y} \cdot g$$
$$X \cdot f - \frac{1}{3} \cdot Y \cdot g = -X^3Y^3 + X^2 - \frac{1}{3}Y^3$$

Lema 6.5. *Suponha que temos um somatório $\sum_{i=1}^s c_i f_i$, onde $c_i \in K$ e o $multigrau(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ para todo i. Se $multigrau(\sum_{i=1}^s c_i f_i) < \delta$, então $\sum_{i=1}^s c_i f_i$ é uma combinação linear, com coeficientes em K, de S-polinômios $S(f_j, f_k)$ para $1 \leq j, k \leq s$. Além disso, cada $S(f_j, f_k)$ tem $multigrau < \delta$.*

Demonstração. Para todo $i \in \{1, \ldots, s\}$ chamamos d_i o coeficiente líder de f_i, de modo que $c_i d_i$ é o coeficiente líder de $c_i f_i$; como todos os termos da forma $c_i f_i$ tem multigrau δ e a soma $\sum_{i=1}^s c_i f_i$ tem multigrau menor que δ, segue facilmente que $\sum_{i=1}^s c_i d_i = 0$. Defina $p_i = \dfrac{f_i}{d_i}$ e note que p_i tem coeficiente líder 1, com $i \in \{1, \ldots, s\}$. Considere a soma telescópica

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \ldots$$
$$+(c_1 d_1 + \ldots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \ldots + c_s d_s) p_s$$

.

Pela hipótese, o termo líder de f_i é $d_i \boldsymbol{X}^\delta$, para todo $i \in \{1, \ldots, s\}$ o que implica que o mínimo múltiplo comum do termo líder de f_j e do termo líder de f_m é $\boldsymbol{X}^\delta$, onde $j, m \in \{1, \ldots, s\}$, então

$$S(f_j, f_m) = \frac{\boldsymbol{X}^\delta}{LT(f_j)} f_j - \frac{\boldsymbol{X}^\delta}{LT(f_m)} f_m = \frac{\boldsymbol{X}^\delta}{d_j \boldsymbol{X}^\delta} f_j - \frac{\boldsymbol{X}^\delta}{d_m \boldsymbol{X}^\delta} f_m = p_j - p_m. \qquad (6.1)$$

Usando esta equação e $\sum_{i=1}^{s} c_i d_i = 0$, a soma telescopia acima se torna

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \ldots + (c_1 d_1 + \ldots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s),$$

que é uma soma da forma desejada. Para todo $j \in \{ 1, \ldots, m\}$ distintos, p_j e p_m tem multigrau δ e coeficiente líder 1 e a diferença $p_j - p_m$ tem multigrau menor que δ, pela equação (6.1), o mesmo é verdade para $S(f_j, f_m)$, provando assim o lema. □

Usando S-polinômios e o Lema 6.5, podemos agora provar o critério de Buchberger que diz quando uma base de um ideal é uma base de Gröbner.

Teorema 6.6. *(Critério de Buchberger) Seja I um ideal polinomial. Então uma base $G = \{g_1, \ldots, g_t\}$ para I é uma base de Gröbner para I se e somente se para todos os pares $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por G (listado em alguma ordem) é zero.*

Demonstração. Se G é uma base de Gröbner, então como $S(g_i, g_j) \in I$, o resto da divisão de G é zero pelo Corolário 6.2. Reciprocamente, seja $f \in I$ um polinômio não nulo. Devemos mostrar que se todos os S-polinômios tem resto zero na divisão por G, então $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$. Dado $f \in I = (g_1, \ldots, g_t)$, existem polinômios $h_i \in K[\boldsymbol{X}]$ tais que

$$f = \sum_{i=1}^{t} h_i g_i \tag{6.2}$$

Pelo Lema 2.11 segue que

$$multigrau(f) \leq max(multigrau(h_i g_i)). \tag{6.3}$$

Se a igualdade não ocorre, então algum cancelamento ocorre sobre os termos líderes de 6.2. Dado uma expressão 6.2 para f, seja $m(i) = \text{multigrau}(h_i g_i)$, onde $i \in \{1, \ldots, t\}$ e defina $\delta = \max(m(1), \ldots, m(t))$. Então a desigualdade 6.3 se torna

$$\text{multigrau}(f) \leq \delta$$

Agora considere todas as maneiras possíveis que f pode ser escrito da forma 6.2. Para cada expressão, pegamos um diferente δ. Como uma ordem monomial é uma boa ordenação, podemos selecionar uma expressão da forma 6.2 tal que δ é minimal. Mostraremos que uma vez que este δ é escolhido, temos que $\text{multigrau}(f) = \delta$. Então a igualdade ocorre em 6.3, assim $\text{multigrau}(f) = \text{multigrau}(h_i g_i)$ para algum i e seguirá que o termo líder de f é divisível pelo termo líder de g_i. Isto mostrará que $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$, que é o que queremos provar. Resta mostrar que o $\text{multigrau}(f) = \delta$. Provemos isto por

contradição. A igualdade pode falhar somente quando multigrau$(f) < \delta$. Para isolar os termos do multigrau δ, vamos escrever f da seguinte maneira:

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} LT(h_i)g_i + \sum_{m(i)=\delta} (h_i - LT(h_i))g_i + \sum_{m(i)<\delta} h_i g_i \quad (6.4)$$

Todos os monômios que aparecem na segunda e terceira soma do lado direito da igualdade tem multigrau menor que δ. Então como supomos que o multigrau$(f) < \delta$ temos que a primeira soma também tem multigrau menor que δ. Seja o termo líder de h_i igual a $c_i \boldsymbol{X}^{\alpha(i)}$. Então a primeira soma $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{m(i)=\delta} c_i \boldsymbol{X}^{\alpha(i)} g_i$ tem exatamente a forma descrita do Lema 6.5 com $f_i = \boldsymbol{X}^{\alpha(i)} g_i$. Então o Lema 6.5 implica que esta soma é uma combinação linear de S-polinômios $S(\boldsymbol{X}^{\alpha(j)} g_j, \boldsymbol{X}^{\alpha(k)} g_k)$. Entretanto,

$$S(\boldsymbol{X}^{\alpha(j)} g_j, \boldsymbol{X}^{\alpha(k)} g_k) = \frac{\boldsymbol{X}^{\delta}}{\boldsymbol{X}^{\alpha(j)} LT(g_j)} \boldsymbol{X}^{\alpha(j)}(g_j) - \frac{\boldsymbol{X}^{\delta}}{\boldsymbol{X}^{\alpha(k)} LT(g_k)} \boldsymbol{X}^{\alpha(k)} = \boldsymbol{X}^{\delta - \gamma_{jk}} S(g_j, g_k).$$

onde $\boldsymbol{X}^{\gamma_{jk}} = LCM(LM(g_j), LM(g_k))$. Então existem constantes $c_{jk} \in K$ tais que

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk} \boldsymbol{X}^{\delta - \gamma jk} S(g_j, g_k) \quad (6.5)$$

O próximo passo é usar nossa hipótese que o resto da divisão de $S(g_j, g_k)$ por $g_1, \ldots g_t$ é zero. Usando o algoritmo da divisão, isto significa que cada S-polinômio pode ser escrito da forma

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \quad (6.6)$$

onde $a_{ijk} \in K[\boldsymbol{X}]$. O algoritmo da divisão nos diz que

$$multigrau(a_{ijk} g_i) \leq multigrau(S(g_j, g_k)) \quad (6.7)$$

para todo i, j, k. Intuitivamente, isto nos diz que quando o resto é zero, podemos encontrar uma expressão para $S(g_j, g_k)$ em termos de G onde nem todo os termos líderes cancelam. Para explorar isso, multiplique a expressão de $S(g_j, g_k)$ por $\boldsymbol{X}^{\delta - \gamma jk}$ para obter

$$\boldsymbol{X}^{\delta - \gamma jk} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i,$$

onde $b_{ijk} = \boldsymbol{X}^{\delta - \gamma jk} a_{ijk}$. Então 6.7 e o Lema 6.5 implicam que

$$multigrau(b_{ijk} g_i) < multigrau(\boldsymbol{X}^{\delta - \gamma jk} S(g_j, g_k)) < \delta \quad (6.8)$$

Se substituirmos a expressão acima por $\boldsymbol{X}^{\delta-\gamma jk}S(g_j, g_k)$ em 6.5, obtemos uma equação

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk}\boldsymbol{X}^{\delta-\gamma jk}S(g_j, g_k) = \sum_{j,k} c_{jk}(\sum_i b_{ijk}g_i) = \sum_i \tilde{h}_i g_i \tag{6.9}$$

que por 6.8 tem a propriedade de que para todo i,

$$multigrau(\tilde{h}_i g_i) < \delta$$

Substituindo $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_i \tilde{h}_i g_i$ na equação 6.4 obtemos uma expressão de f como uma combinação de polinômios $g_i's$ onde todos os termos tem multigrau menor que δ. Isto contradiz a minimalidade de δ e completa a prova do teorema. □

Como um exemplo de aplicação do Teorema acima, considere o ideal $I = \langle Y - X^2, Z - X^3\rangle$ do cubo torcido no $\mathbb{R}^3$. Afirmamos que $G = \{Y - X^2, Z - X^3\}$ é uma base de Gröbner para a ordem lexicográfica com $Y > Z > X$. Para provar isto, considere o S-polinômio

$$S(Y - X^2, Z - X^3) = \frac{YZ}{Y}(Y - X^2) - \frac{YZ}{Z}(Z - X^3) = -ZX^2 + YX^3.$$

Usando o algoritmo da divisão, temos que

$$-ZX^2 + YX^3 = X^3 \cdot (Y - X^2) + (-X^2) \cdot (Z - X^3) + 0,$$

de modo que $\overline{S(Y - X^2, Z - X^3)}^G = 0$. Então, pelo Teorema 6.6, G é uma base de Gröbner para I.

7 Algoritmo de Buchberger

No Corolário 5.6, nós vimos que todo ideal em $K[\boldsymbol{X}]$ diferente de 0 tem uma base de Gröbner. Infelizmente, a prova dada não nos mostrou como produzir esta base, então podemos nos perguntar: Dado um ideal $I \subset K[\boldsymbol{X}]$, como construir uma base de Gröbner para I?

Teorema 7.1. *(Algortimo de Buchberger) Seja $I = \langle f_1, \ldots, f_s \rangle \neq 0$ um ideal polinomial. Então uma base de Gröbner para I pode ser construída em um número finito de passos pelo seguinte algoritmo:*
INPUT: $F = (f_1, \ldots, f_s)$
OUTPUT: Uma base de Gröbner $G = (g_1, \ldots, g_t)$ *para* I, *com* $F \subset G$
$G := F$

REPETIR

$$G' := G$$
$$\textit{PARA cada par } \{p, q\}, p \neq q \textit{ em } G' \textit{ FAÇA}$$
$$S := \overline{S(p,q)}^{G'}$$
$$\textit{SE } S \neq 0 \textit{ ENTÃO } G := G' \cup \{S\}$$

ATÉ $G = G'$

Demonstração. Começaremos a demonstração com algumas notações usadas. Se $G = \{g_1, \ldots, g_t\}$ então $\langle G \rangle$ e $\langle LT(G) \rangle$ irão denotar os seguintes ideais:

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle$$
$$\langle LT(G) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Voltando a prova do teorema, vamos mostrar que $G \subset I$ permanece em todos os estágios do algoritmo. Isto é verdade inicialmente e quanto mais "aumentarmos" G, faremos isto adicionando o resto $S = \overline{S(p,q)}^{G'}$ para $p, q \in G$. Portanto, se $G \subset I$, então p, q e consequentemente $S(p,q)$ estão em I e como estamos dividindo por $G' \subset I$ temos que $G \cup \{S\} \subset I$. Note que G contém a base dada F de I de modo que G é atualmente uma base de I.
O algoritmo termina quando $G = G'$, que significa que $S = \overline{S(p,q)}^{G'} = 0$ para todo $p, q \in G$. Então G é uma base de Gröbner de $\langle G \rangle = I$ pelo Teorema 6.6.
Resta provar que o algoritmo termina. Precisamos considerar o que acontece depois de cada passo através do laço principal. O conjunto G consiste de G' (o antigo G) junto com

os restos não nulos dos $S-$polinômios de elementos de G'. Então

$$\langle LT(G')\rangle \subset \langle LT(G)\rangle \tag{7.1}$$

como $G' \subset G$. Além do mais, se $G' \neq G$, afirmamos que $\langle LT(G')\rangle$ é estritamente menor que $\langle LT(G)\rangle$. Para ver isto,suponha que um resto não nulo r de um S-polinômio foi adicionado a G. Como r é o resto da divisão por $G', LT(r)$ não é divisível pelos termos líderes de elementos de G' e então $LT(r) \notin \langle LT(G')\rangle$. Ainda $LT(r) \in \langle LT(G)\rangle$, que prova nossa afirmação.
Por 7.1, os ideais $\langle LT(G')\rangle$ das sucessivas interações do laço formam uma cadeia ascendente de ideais em $K[\boldsymbol{X}]$. Então o Teorema 5.7 implica que depois de um número finito de interações a cadeia irá se estabilizar, de modo que $\langle LT(G')\rangle = \langle LT(G)\rangle$ deve acontecer eventualmente. Pelo parágrafo anterior, isto implica que $G' = G$, de modo que o algoritmo termina depois de um número finito de passos.

□

Note que uma vez que o resto $\overline{S(p,q)}^{G'} = 0$, este resto continuará sendo zero mesmo se adicionarmos mais elementos ao conjunto gerador G'. Então, não há necessidade de computar esses restos nos passos subsequentes através do laço principal. De fato, se adicionarmos novos geradores f_j um de cada vez, os únicos restos que necessitam serem checados são $\overline{S(f_i,f_j)}^{G'}$, onde $i \leq j-1$.
As bases de Gröbner computadas usando o algoritmo acima são geralmente maiores que o necessário. Podemos eliminar alguns geradores não necessários usando o seguinte lema.

Lema 7.2. *Seja G uma base de Gröbner para o ideal polinomial I. Seja $p \in G$ um polinômio tal que $LT(p) \in \langle LT(G-\{p\})\rangle$. Então $G-\{p\}$ é também uma base de Gröbner para I.*

Demonstração. Sabemos que $\langle LT(G)\rangle = \langle LT(I)\rangle$. Se $LT(p) \in \langle LT(G-\{p\})\rangle$, então temos que $\langle LT(G-\{p\})\rangle = \langle LT(G)\rangle$. Pela definição, segue que $G-\{p\}$ é também uma base de Gröbner para I. □

Ajustando as constantes de modo que todos os coeficientes líderes sejam iguais a 1 e removendo qualquer p com $LT(p) \in \langle LT(G-\{p\})\rangle$ de G, chegamos a mais uma definição.

Definição 7.3. Uma **base de Gröbner minimal** para um ideal polinomial I é uma base de Gröbner G para I tal que:

- $(i) LC(p) = 1$ para todo $p \in G$.
- (ii) Para todo $p \in G, LT(p) \notin \langle LT(G-\{p\})\rangle$.

Podemos construir uma base de Gröbner minimal para um ideal não nulo aplicando o algoritmo de Buchberger e então usando o Lema 7.2 para eliminar qualquer gerador desnecessário que talvez foi incluído. Para ilustrar este procedimento, considere o ideal I cuja base de Gröbner é dada por

$$\begin{aligned} f_1 &= X^3 - 2XY, \\ f_2 &= X^2Y - 2Y^2 + X, \\ f_3 &= -X^2, \\ f_4 &= -2XY, \\ f_5 &= -2Y^2 + X. \end{aligned}$$

Como alguns dos coeficientes líderes são diferentes de 1, o primeiro estágio é multiplicar os geradores por constantes adequadas para satisfazer o item (i) da definição de base de Gröbner minimal. Depois disso note que temos $LT(f_1) = X^3 = -X \cdot LT(f_3)$ e similarmente temos $LT(f_2) = X^2Y = -\frac{1}{2}X \cdot LT(f_4)$, assim pelo Lema 7.2 podemos dispensar f_1 e f_2. Como não há mais casos onde o termo líder de um gerador divide o termo líder de um outro gerador, concluímos que

$$\tilde{f}_3 = X^2, \tilde{f}_4 = XY, \tilde{f}_5 = Y^2 - \frac{1}{2}X$$

é uma base de Gröbner minimal para I.
Infelizmente, um ideal pode ter mais de uma base de Gröbner minimal. Por exemplo para o ideal I considerado acima, é fácil ver que

$$f'_3 = X^2 + aXY, \tilde{f}_4 = XY, \tilde{f}_5 = Y^2 - \frac{1}{2}X \tag{7.2}$$

é também uma base de Gröbner minimal, onde $a \in K$ é uma constante qualquer. Então, podemos produzir infinitas bases de Gröbner minimais (assumindo que K é infinito). Felizmente, podemos destacar uma base de Gröbner minimal que é melhor que as outras.

Definição 7.4. Uma **base de Gröbner reduzida** para um ideal polinomial I é uma base de Gröbner G para I tal que:

- $(i) LC(p) = 1$ para todo $p \in G$.
- (ii) Para todo $p \in G$, nenhum monômio de p pertence a $\langle LT(G - \{p\})\rangle$.

Note que para a base de Gröbner dada em 7.2, somente quando $a = 0$ temos que ela é reduzida.
Em geral, uma base de Gröbner reduzida tem a seguinte propriedade.

Proposição 7.5. *Seja $I \neq 0$ um ideal polinomial. Então, para uma ordem monomial dada, I tem uma única base de Gröbner reduzida.*

Demonstração. Seja G uma base de Gröbner minimal para I. Dizemos que $g \in G$ é **reduzido para** G desde que nenhum monômio de g esteja em $\langle LT(G - \{g\})\rangle$. Nosso objetivo é modificar G até que todos os seus elementos estejam reduzidos. Uma primeira observação é que se g é reduzido para G, então g é reduzido também para qualquer outra base de Gröbner minimal de I que contenha g e tem o mesmo conjunto de termos líderes. Isto segue porque a definição de reduzido só envolve os termos líderes.
Agora, dado $g \in G$, seja $g' = \overline{g}^{G-\{g\}}$ e defina $G' = (G - \{g\}) \cup g'$. Afirmamos que G' é uma base de Gröbner minimal para I. Para ver isto, primeiramente note que $LT(g') = LT(g)$, pois quando dividimos g por $G - \{g\}, LT(g)$ vai para o resto pois não é divisível por qualquer elemento de $LT(G - \{g\})$. Isto mostra que $\langle LT(G')\rangle = \langle LT(G)\rangle$. Como G' está claramente contido em I, vemos que G' é uma base de Gröbner e a minimalidade segue. Finalmente, note que g' é reduzida para G' por construção.
Agora, tome os elementos de G e aplique o processo acima até que todos esses elementos estejam reduzidos. A base de Gröbner talvez mude a cada processo que fizermos mas nossa observação anterior mostrou que uma vez que um elemento é reduzido para G, ele continua reduzido para qualquer outra base de Gröbner minimal de I que contenha G, uma vez que nunca mudamos os termos líderes. Assim, terminamos com uma base de Gröbner reduzida.
Finalmente, para provar a unicidade, suponha que G e $\tilde{G}$ são bases de Gröbner reduzidas para I. Então em particular, G e $\tilde{G}$ são bases de Gröbner minimais, e por definição de base de Gröbner $\langle LT(G)\rangle = \langle LT(I)\rangle = \langle LT(\tilde{G})\rangle$. Tome m, termo líder qualquer de G, ele pode ser escrito como

$$m = a_1\tilde{m}_1 + \ldots + a_n\tilde{m}_n$$

onde $\tilde{m}_i \in LT(\tilde{G})$ com $i \in \{1, \ldots, n\}$. Por definição de base de Gröbner minimal, o coeficiente líder de m é 1 e os coeficientes líderes de cada $\tilde{m}_i$ com $i \in \{1, \ldots, n\}$ são 1, assim é fácil ver que $m = \tilde{m}_i$, para algum $\tilde{m}_i$. Portanto $LT(G) \subset LT(\tilde{G})$.
A outra implicação é análoga e assim concluímos que $LT(G) = LT(\tilde{G})$.
Então, dado $g \in G$, existe $\tilde{g} \in \tilde{G}$ tal que $LT(g) = LT(\tilde{g})$. Se mostrarmos que $g = \tilde{g}$, seguirá que $G = \tilde{G}$, e a unicidade estará provada.
Para mostrar que g é igual a $\tilde{g}$, vamos olhar para a diferença entre g e $\tilde{g}$. Esta diferença está em I e como G é uma base de Gröbner, segue que $\overline{g - \tilde{g}}^G = 0$. Mas também sabemos que o termo líder de g é igual ao termo líder de $\tilde{g}$. Então, estes termos se cancelam na diferença entre g e $\tilde{g}$ e o restante dos termos não são divisíveis por nenhum dos termos líderes de G pois G é base de Gröbner reduzida. Isto mostra que $\overline{g - \tilde{g}}^G = g - \tilde{g}$, e então $g - \tilde{g} = 0$.

□

8 Melhorias no algoritmo de Buchberger

Ao projetar softwares matemáticos, deve-se prestar atenção não apenas se os algoritmos empregados estão corretos, mas também à sua eficiência. Nesta seção, discutiremos algumas melhorias no algoritmo básico de Buchberger para calcular as bases de Gröbner que podem acelerar bastante os cálculos. Algumas versões dessas melhorias foram incorporadas à maioria dos sistemas de álgebra computacional que oferecem pacotes de base de Gröbner. A primeira classe de modificações que consideraremos diz respeito ao Teorema 6.6 que afirma que uma base de um ideal G é uma base de Gröbner desde que $\overline{S(f,g)}^{G} = 0$ para todo $f, g \in G$. Se voltarmos ao capítulo anterior, veremos que esse critério é a força motriz por trás do algoritmo de Buchberger. Portanto, uma boa maneira de melhorar a eficiência do algoritmo seria mostrar que menos S-polinômios $S(f,g)$ precisam ser considerados. Fazendo exemplos a mão, as divisões polinomiais envolvidas são a parte que mais gastam tempo. Então, qualquer redução no número de divisões que precisam ser realizadas é bom. Para identificar S-polinômios que podem ser ignorados no Teorema 6.6, primeiro precisamos dar uma visão mais geral do que significa ter resto zero. A definição é a seguinte.

Definição 8.1. Fixada uma ordem monomial e seja $G = \{g_1, \ldots, g_s\} \subset K[\boldsymbol{X}]$. Dado $f \in K[\boldsymbol{X}]$, dizemos que f **reduz a zero módulo G**, escrito

$$f \to_G 0,$$

se f pode ser escrito na forma

$$f = a_1 g_1 + \cdots + a_t g_t,$$

tal que sempre que $a_i g_i \neq 0$, temos que

$$multigrau(f) \geq multigrau(a_i g_i).$$

Lema 8.2. *Seja $G = (g_1, \ldots, g_s)$ um conjunto ordenado de elementos de $K[\boldsymbol{X}]$ e fixe $f \in K[\boldsymbol{X}]$. Então $\overline{f}^{G} = 0$ implica $f \to_G 0$, embora o contrário seja falso em geral.*

Demonstração. Se $\overline{f}^{G} = 0$, então o algoritmo da divisão implica

$$f = a_1 g_1 + \cdots + a_t g_t + 0,$$

e também pelo algoritmo da divisão, sempre que $a_i g_i \neq 0$, temos que

$$multigrau(f) \geq multigrau(a_i g_i)$$

Isto mostra que $f \to_G 0$, . Para ver que o contrário pode falhar, considere o Exemplo 3.3. Se dividirmos $f = XY^2 - X$ por $G = (XY + 1, Y^2 - 1)$ o algoritmo da divisão nos dá

$$XY^2 - X = Y \cdot (XY + 1) + 0 \cdot (Y^2 - 1) + (-X - Y),$$

de modo que $\overline{f}^G = -X - Y \neq 0$. Porém ainda podemos escrever

$$XY^2 - X = 0 \cdot (XY + 1) + X(Y^2 - 1),$$

e como

$$multigrau(XY^2 - X) \geq multigrau(X \cdot (Y^2 - 1))$$

(de fato, eles são iguais), disto segue que $f \to_G 0$. □

Teorema 8.3. *Uma base $G = \{g_1, \ldots, g_s\}$ para um ideal I é uma base de Gröbner se e somente se $S(g_i, g_j) \to_G 0$, para todo $i \neq j$.*

Demonstração. No Teorema 6.6, provamos este resultado sobre as hipóteses que $\overline{S(g_i, g_j)}^G = 0$ para todo $i \neq j$. Mas se analisarmos a prova, veremos que tudo que usamos foi

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i,$$

onde

$$multigrau(S(g_j, g_k)) \geq multigrau(a_{ijk} g_i)$$

[Veja 6.6 e 6.7]. Isto é exatamente o que $S(g_i, g_j) \to_G 0$, significa, e o teorema segue □

Proposição 8.4. *Dado um conjunto finito $G \subset K[\boldsymbol{X}]$, suponha que temos $f, g \in G$ tal que*

$$LCM(LM(f), LM(g)) = LM(f) \cdot LM(g).$$

Isto significa que os monômios líderes de f e g são relativamente primos. Então

$$S(f, g) \to_G 0.$$

Demonstração. Por simplicidade, assumimos que f, g foram multiplicados por constantes apropriadas para fazer $LC(f) = LC(g) = 1$. Escrevemos $f = LM(f) + p, g = LM(g) + q$. Então, como $LCM(LM(f), LM(g)) = LM(f) \cdot LM(g)$, temos

$$\begin{aligned} S(f,g) &= LM(g) \cdot f - LM(f) \cdot g \\ &= (g - q) \cdot f - (f - p) \cdot g \\ &= g \cdot f - q \cdot f - f \cdot g + p \cdot g \\ &= p \cdot g - q \cdot f \end{aligned} \tag{8.1}$$

Afirmamos que

$$multigrau(S(f,g)) = max(multigrau(p \cdot g), multigrau(q \cdot f)) \tag{8.2}$$

Note que 8.1 e 8.2 implicam $S(f,g) \to_G 0$ pois $f, g \in G$. Para provar 8.2, observe que nos últimos polinômios de 8.1, os monômios líderes de $p \cdot g$ e $q \cdot f$ são distintos e então, não podem se cancelar. Se os monômios fossem o mesmo, teríamos

$$LM(p) \cdot LM(g) = LM(q) \cdot LM(f).$$

Assim o monômio líder de g dividiria o monômio líder de q, pois os monômios líderes de f e g são relativamente primos. O que é um absurdo pois o monômio líder de g é maior que o monômio líder de q. □

Referências

[1] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Third ed., Springer, New York, 2007.