Bases de Gröbner

Augusto Duarte Pena

Neste trabalho, abordaremos as propriedades básicas das Bases de Gröbner. Temos como objetivo mostrar aplicações interessantes das Bases de Gröbner e fornecer um método prático (um algoritmo) que permita encontrá-las. Utilizaremos exemplos para melhor compreensão durante o texto.

1 História

Sob a orientação de Wolfgang Gröbner, a teoria de Bases de Gröbner foi desenvolvida por Bruno Buchberger, seu aluno de doutorado, durante a década de 1960. O problema principal da tese de Bruno era determinar um método para encontrar uma base para $K[x_1, \ldots, x_n]/I$ como um K-espaço vetorial. Veremos a diante que um dos maiores problemas para se trabalhar com polinômios em $K[x_1, \ldots, x_n]$ é que o algoritmo da divisão não comporta como no caso com apenas uma variável. Quando lidamos com polinômios em uma única variável, a divisão euclidiana tem unicamente determinados o quociente e o resto. No caso de várias variáveis, a ordenação das variáveis, assim como a ordenação da divisão tem um impacto na divisão.

Assim, a teoria desenvolvida busca então circunvir tais problemas e obter alguns paralelos com o caso em uma única variável.

2 Bases de Gröbner

2.1 Ordem monomial em $K[x_1, \ldots, x_n]$

Começaremos definindo como se dá a ordem em polinômios em várias variáveis e algumas de suas propriedades.

Definição 2.1. *Uma **ordem monomial** em $K[x_1, \ldots, x_n]$ é uma relação $>$ em $\mathbb{Z}^n_{\geq 0}$, ou equivalentemente, uma relação no conjunto de monômios $\{x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}\}$, satisfazendo:*

i. $>$ *é uma ordem total em* $\mathbb{Z}^n_{\geq 0}$*;*

ii. Se $\alpha > \beta$ *e* $\gamma \in \mathbb{Z}^n_{\geq 0}$*, então* $\alpha + \gamma > \beta + \gamma$*;*

iii. $>$ *é uma boa ordem em* $\mathbb{Z}^n_{\geq 0}$*, isto é, todo subconjunto não vazio de* $\mathbb{Z}^n_{\geq 0}$ *possui um menor elemento com respeito a* $>$*.*

Lema 2.2. *Uma relação de ordem total $>$ em $\mathbb{Z}^n_{\geq 0}$ é uma boa ordem se, e somente se, toda sequência estritamente decrescente em $\mathbb{Z}^n_{\geq 0}$*

$$\alpha_1 > \alpha_2 > \alpha_3 > \cdots$$

eventualmente termina.

Demonstração. Suponha que exista uma sequência infinitamente decrescente em $\mathbb{Z}^n_{\geq 0}$, então a sequência $\{\alpha_1, \alpha_2, \alpha_3, \ldots\}$ é um subconjunto não vazio de $\mathbb{Z}^n_{\geq 0}$ que não possui menor elemento, o que é uma contradição.

Reciprocamente, suponha por absurdo que $>$ não é uma boa ordem, então existe algum subconjunto não vazio $S \subset \mathbb{Z}^n_{\geq 0}$ que não possui menor elemento. Tome $\alpha_1 \in S$. Como a_1 não é o menor elemento podemos encontrar $\alpha_1 > \alpha_2$ em S. Mas α_2 ainda não é o menor elemento,

podemos encontrar $\alpha_2 > \alpha_3$ em S. Seguindo este raciocínio obtemos uma sequência infinitamente decrescente

$$\alpha_1 > \alpha_2 > \alpha_3 \cdots .$$

□

Definição 2.3 (Ordem Lexicográfica). *Sejam $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha >_{lex} \beta$ se na diferença de vetores $\alpha - \beta \in \mathbb{Z}^n$, a coordenada não nula mais a esquerda é positiva. Escrevemos $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.*

Proposição 2.4. *A ordem lexicográfica em $\mathbb{Z}^n_{\geq 0}$ é uma ordem monomial.*

Demonstração.

i. A ordem lexicográfica $>_{\text{lex}}$ é uma ordem total pela definição e pelo fato da ordem numérica usual em $\mathbb{Z}^n_{\geq 0}$ ser uma ordem total.

ii. Se $\alpha >_{\text{lex}} \beta$ então temos que a entrada não negativa mais a esquerda em $\alpha - \beta$, digamos $\alpha_k - \beta_k$, é positiva. Como $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ e $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$, então em $(\alpha+\gamma)-(\beta+\gamma) = \alpha-\beta$, a entrada não negativa mais a esquerda é também $\alpha_k - \beta_k > 0$.

iii. Suponha que $>_{\text{lex}}$ não é uma boa ordem, então pelo Lema (2.2) temos que existe uma sequência infinitamente decrescente

$$\alpha_1 >_{\text{lex}} \alpha_2 >_{\text{lex}} \alpha_3 >_{\text{lex}} \cdots$$

de $\mathbb{Z}^n_{\geq 0}$. Tome a primeira coordenada dos elementos $\alpha_i \in \mathbb{Z}^n_{\geq 0}$. Pela definição de ordem lexicográfica, as primeiras coordenadas formam uma sequência não crescente de inteiros não negativos. Como os números naturais são bem ordenados, esta sequência deve eventualmente "estabilizar", isto é, a partir de um certo k natural toda coordenada de a_i com $i \geq k$ é igual.
A partir de a_k as segundas e seguintes coordenadas de $a_k, a_{k+1}, \ldots$ formam uma sequência não crescente e pelo mesmo argumento eventualmente "estabilizam". Seguindo este raciocínio temos que para algum l, todos os $\alpha_l, \alpha_{l+1}, \ldots$ são iguais, o que contradiz $\alpha >_{\text{lex}} \alpha_{l+1}$.

□

Definição 2.5 (Ordem Lexicográfica Graduada). *Sejam $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha >_{grlex} \beta$ se*

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

Proposição 2.6. *A ordem lexicográfica graduada em $\mathbb{Z}^n_{\geq 0}$ é uma ordem monomial.*

Demonstração. Ver [1, p. 58] □

Definição 2.7 (Ordem Lexicográfica Graduada Reversa). *Sejam $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha >_{grevlex} \beta$ se*

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i, \quad \textit{ou} \quad |\alpha| = |\beta|,$$

e a coordenada não nula mais a direita de $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ é negativa.

Proposição 2.8. *A ordem lexicográfica graduada reversa em $\mathbb{Z}^n_{\geq 0}$ é uma ordem monomial.*

Demonstração. Ver [1, p. 58] □

Observação 2.9. *Com o uso do Corolário* (2.25) *podemos demonstrar todas as ordens monomiais citadas acimas são boas ordens mais facilmente.*

Exemplo 2.10. *Considere o polinômio* $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in \mathbb{R}[x, y, z]$. *Reordenando os termos de maneira decrescente de acordo com cada ordem, temos:*

- *Com respeito a ordem lexicográfica:* $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$.
- *Com respeito a ordem lexicográfica graduada:* $f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$.
- *Com respeito a ordem lexicográfica graduada reversa:* $f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$.

As definições a seguir são simplesmente as generalizações esperadas para polinômios em várias variáveis.

Definição 2.11. *Seja* $f = \sum_\alpha a_\alpha x^\alpha$ *um polinômio não nulo em* $K[x_1, \ldots, x_n]$ *e seja* $>$ *uma ordem monomial.*

i. O ***multigrau*** *de* f *é*
$$multigrau(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0)$$

ii. O ***coeficiente líder*** *de* f *é*
$$CL(f) = a_{multigrau(f)} \in K$$

iii. O ***monômio líder*** *de* f *é*
$$ML(f) = x^{multigrau(f)}$$
(com coeficiente 1*)*

iv. O ***termo líder*** *de* f *é*
$$TL(f) = CL(f) \cdot ML(f).$$

Exemplo 2.12. *Tomando o polinômio do exemplo anterior com a ordem lexicográfica, temos*
$$multigrau(f) = (3, 0, 0), CL(f) = -5, ML(f) = x^3, \text{ e } TL(f) = -5x^3.$$

Lema 2.13. *Sejam* $f, g \in K[x_1, \ldots, x_n]$ *polinômios não nulos. Então:*

i. $multigrau(fg) = multigrau(f) + multigrau(g)$

ii. Se $f + g \neq 0$, *então* $multigrau(f + g) \leq \max(multigrau(f), multigrau(g))$.

Ainda, se $multigrau(f) \neq multigrau(g)$, *então a igualdade ocorre.*

Demonstração.

i. Sejam f e g polinômios não nulos em $K[x_1, \ldots, x_n]$. Tome A e B subconjuntos não vazios de $\mathbb{Z}^n_{\geq 0}$ e escreva
$$\begin{aligned} f &= h_{\alpha_1}x^{\alpha_1} + \sum_{\alpha \in A - \{\alpha_1\}} h_\alpha x^\alpha, \quad \text{onde } multigrau(f) = \alpha_1 \\ g &= k_{\beta_1}x^{\beta_1} + \sum_{\beta \in B - \{\beta_1\}} h_\beta x^\beta, \quad \text{onde } multigrau(g) = \beta_1, \end{aligned}$$
Temos que o produto é dado por $fg = h_{\alpha_1}k_{\beta_1}x^{\alpha_1+\beta_1} + \sum_{\substack{\alpha \in A - \{\alpha_1\} \\ \beta \in B - \{\beta_1\}}} h_\alpha k_\beta x^{\alpha+\beta}$.
Disto segue que que $multigrau(fg) = \alpha_1 + \beta_1 = multigrau(f) + multigrau(g)$.

ii. Caso $TL(f)+TL(g) = 0$ então $f+g = \sum_{\alpha \in A - \{\alpha_1\}} h_\alpha x^\alpha + \sum_{\beta \in B - \{\beta_1\}} h_\beta x^\beta$. Assim, $multigrau(f+g) = \max((A-\{\alpha_1\}) \cup (B-\{\beta_1\})) < \begin{cases} \alpha_1 \\ \beta_1 \end{cases} \leq \max(\alpha_1, \beta_1) = \max(multigrau(f), multigrau(g))$.
Se $TL(f) + TL(g) \neq 0$, então $multigrau(f + g) = \max(multigrau(f), multigrau(g))$.

□

2.2 O Algoritmo da Divisão em $K[x_1, \ldots, x_n]$

A algoritmo da divisão em $K[x_1, \ldots, x_n]$ com uma determinada ordem monomial é similar ao algoritmo da divisão em $K[x]$. Ao dividirmos f por $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, tomaremos a divisão de f por f_1, e o resto da divisão será dividido por f_2. O processo se repete até que o restante da divisão no estágio $s-1$ é dividido por f_s e obtemos r como o resto que não é divisível por nenhum outro polinômio.

Exemplo 2.14. *Ao dividirmos $f = xy^2 + 1$ por $f_1 = xy + 1$ e $f_2 = y + 1$ em $\mathbb{R}[x, y]$ com a ordem lexicográfica $x > y$, obtemos*

$$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2.$$

É importante observar que em polinômios em várias variáveis, a divisão e o resto podem não ser únicos.

Exemplo 2.15. *Ao dividirmos $f = x^2y + xy^2 + y^2$ por $f_1 = xy - 1$ e $f_2 = y^2 - 1$ em $\mathbb{R}[x, y]$ com a ordem lexicográfica $x > y$, obtemos*

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1.$$

Agora, se dividirmos $f = x^2y + xy^2 + y^2$ por $f_1 = y^2 - 1$ e $f_2 = xy - 1$, obtemos

$$x^2y + xy^2 + y^2 = (x + 1) \cdot (y^2 - 1) + x \cdot (xy - 1) + 2x + 1.$$

O conceito é formalizado através do seguinte teorema:

Teorema 2.16 (Algoritmo da Divisão em $K[x_1, \ldots, x_n]$)**.** *Dada uma ordem monomial $>$ em $\mathbb{Z}^n_{\geq 0}$, seja $F = (f_1, \ldots, f_s)$ uma s-upla ordenada de polinômios em $K[x_1, \ldots, x_n]$. Então todo $f \in K[x_1, \ldots, x_n]$ pode ser escrito como*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

*onde $a_i, r \in K[x_1, \ldots, x_n]$, e $r = 0$ ou r é uma combinação linear de monômios com coeficientes em K, nenhum deles divisíveis por algum $TL(f_1), \ldots, TL(f_s)$. Chamaremos r de **resto da divisão** de f por F. Além disso, se $a_i f_i \neq 0$, então temos*

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

Demonstração. Consideremos, inicialmente, $a_1 = \cdots = a_n = r = 0$ e $p = f$. Procederemos da seguinte maneira: enquanto houver $i \in \{1, \cdots, s\}$ tal que $TL(f_i)$ divide $TL(p)$, fazemos

$$a_i = a_i + \frac{TL(p)}{TL(f_i)}; \quad p = p - \frac{TL(p)}{TL(f_i)} f_i.$$

No caso de haver mais de um $i \in \{1, \ldots, s\}$ tal que $TL(f_i)$ divide $TL(p)$, então tomamos aquele que for menor.

Agora, quando $TL(f_i)$ não dividir $TL(p)$, para todo $i \in \{1, \cdots, s\}$, então adicionamos $TL(p)$ a r, ou seja, tomamos $p = p - TL(p)$ e $r = r + TL(p)$. Notemos agora que, em qualquer estágio do processo, temos que $f = a_1 f_1 + \cdots + a_s f_s + p + r$. No caso de $TL(p)$ ser divisível por algum $TL(f_i)$, temos que

$$\begin{aligned} a_i f_i + p &= a_i f_i + \frac{TL(p)}{TL(f_i)} f_i - \frac{TL(p)}{TL(f_i)} f_i + p \\ &= \left(a_i + \frac{TL(p)}{TL(f_i)}\right) f_i + \left(p - \frac{TL(p)}{TL(f_i)} f_i\right). \end{aligned}$$

Neste caso, o termo $a_i f_i + p$ não é alterado, assim como as demais parcelas. Por outro lado, no caso de $TL(p)$ não ser divisível por nenhum $TL(f_i)$, temos que

$$p + r = p - TL(p) + TL(p) + r = (p - TL(p)) + (r + TL(p)),$$

ou seja, a soma $p + r$ não é alterada, assim como as demais parcelas. Logo, em qualquer uma das etapas podemos escrever $f = a_1 f_1 + \cdots + a_s f_s + p + r$.
Agora precisamos provar que em algum momento a parcela p se anulará. No caso de $TL(f_i)$ dividir $TL(p)$, temos que $p = p - \frac{TL(p)}{TL(f_i)} f_i$. Pelo Lema (2.13), temos que

$$\begin{aligned} TL(f)TL(g) &= CL(f)ML(f)CL(g)ML(g) \\ &= CL(f)CL(g)x^{multigrau(f)+multigrau(g)} \\ &= TL(fg). \end{aligned}$$

Logo, $TL\left(\frac{TL(p)}{TL(f_i)} f_i\right) = TL\left(\frac{TL(p)}{TL(f_i)}\right) TL(f_i) = \frac{TL(p)}{TL(f_i)} TL(f_i) = TL(p)$.
A segunda igualdade é válida porque $\frac{TL(p)}{TL(f_i)}$ é um monômio. Assim, o termo líder de p se anulará ao fazermos $p' = p - \frac{TL(p)}{TL(f_i)} f_i$. Portanto, $multigrau(p) > multigrau(p')$. Teríamos assim uma sequência decrescente: $multigrau(p_1) > multigrau(p_2) > \cdots$. Mas como $multigrau(p_i)$ é não negativo, em alguma iteração ele terá de ser zero, ou seja, $p_j = a \in k$ para algum j. Como vimos anteriormente, na próxima iteração tomaríamos

$$p_{j+1} = p_j - \frac{TL(p_j)}{TL(f_i)} f_i = 0 \text{ ou } p_{j+1} = p_j - TL(p_j) = 0.$$

Assim, $p_{j+1} = 0$ em ambos os casos.
Finalmente, nos resta provar que $multigrau(f) \geq multigrau(a_i f_i)$, para todo $i = 1, \ldots, s$ e com $a_i f_i \neq 0$. Notemos que

$$a_{i1} = 0; \quad a_{i2} = 0 + \frac{TL(p_1)}{TL(f_i)}; \quad a_{i3} = 0 + \frac{TL(p_1)}{TL(f_i)} + \frac{TL(p_2)}{TL(f_i)}; \quad \cdots$$

onde p_j é o polinômio p, do algoritmo, na j-ésima iteração. Como

$$\begin{aligned} multigrau\left(\tfrac{TL(p_1)}{TL(f_i)}\right) + multigrau(f_i) &= multigrau\left(\tfrac{TL(p_1)}{TL(f_i)} f_i\right) \\ &= multigrau\left(\tfrac{TL(p_1)}{TL(f_i)} TL(f_i)\right) = \\ multigrau(TL(p_1)) = multigrau(p_1) > multigrau(p_j) &= multigrau(TL(p_j)) \\ &= multigrau\left(\tfrac{TL(p_j)}{TL(f_i)}\right) + multigrau(f_i) \end{aligned}$$

Concluímos assim que $multigrau(\frac{TL(p_1)}{TL(f_i)} > multigrau(\frac{TL(p_j)}{TL(f_i)}$, para todo $j = 2, \ldots, k$. Agora como

$$a_i = \frac{TL(p_1)}{TL(f_i)} + \cdots + \frac{TL(p_k)}{TL(f_i)},$$

segue pelo Lema (2.2), que $multigrau(a_i) = multigrau(\frac{TL(p_1)}{TL(f_i)}$. Portanto,

$$multigrau(a_i f_i) = multigrau\left(\frac{TL(p_1)}{TL(f_i)} f_i\right) = multigrau(p_1) \leq multigrau(f).$$

□

Exemplo 2.17. *Seja $f_1 = xy - 1, f_2 = y^2 - 1 \in K[x, y]$ com a ordem lexicográfica $x > y$. Dividindo $f = xy^2 - x$ por $F = (f_1, f_2)$ o resultado é*

$$xy^2 - x = y \cdot (xy - 1) + 0 \cdot (y^2 - 1) + (-x + y)$$

A divisão de f por $F = (f_2, f_1)$ é

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy - 1) + 0$$

Este segundo cálculo mostra que $f \in \langle f_1, f2\rangle$. Assim, o primeiro cálculo mostra que mesmo se $f \in \langle f_1, f_2\rangle$, é possível obter um resto não nulo na divisão por $F = (f_1, f_2)$.

2.3 Ideais Monomiais e o Lema de Dickson

Definição 2.18. *Um ideal $I \subset K[x_1, \ldots, x_n]$ é um **ideal monomial** se existe um subconjunto $A \in \mathbb{Z}^n_{\geq 0}$ tal que I consiste em todos os polinômios que são somas finitas da forma*

$$\sum_{\alpha \in A} h_\alpha x^\alpha, \text{ onde } h_\alpha \in K[x_1, \ldots, x_n].$$

Neste caso, escrevemos $I = \langle x^\alpha : \alpha \in A \rangle$.

Lema 2.19. *Seja $I = \langle x^\alpha : \alpha \in A \rangle$ um ideal monomial. Então um monômio x^β pertence a I se, e somente se, x^β é divisível por x^α para algum $\alpha \in A$.*

Demonstração. Se x^β pertence a I, então podemos escrever $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha_i}$, onde $h_i \in K[x_1, \ldots, x_n]$. Escrevendo cada h_i como soma de monômios, temos $h_i = \sum_{j=1}^{t_i} a_{ij} x^{\gamma_{ij}}$.
Assim,

$$x^\beta = \left(\sum_{j=1}^{t_1} a_{1j} x^{\gamma_{1j}} \right) x^{\alpha_1} + \cdots + \left(\sum_{j=1}^{t_s} a_{sj} x^{\gamma_{sj}} \right) x^{\alpha_s}.$$

Como cada parcela do lado direito da soma é divisível por algum x^{α_i}, segue que x^β também deve ser.
Reciprocamente, se x^β é um múltiplo de x^α, para algum $\alpha \in A$, então $x^\beta \in I$ pela definição de ideal. □

Exemplo 2.20. *Se $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$, então os expoentes dos monômios em I formam o conjunto*

$$((4,2) + \mathbb{Z}^2_{\geq 0}) \cup ((3,4) + \mathbb{Z}^2_{\geq 0}) \cup ((2,5) + \mathbb{Z}^2_{\geq 0}),$$

que é representado pela figura a seguir, fazendo-se a identificação $(m,n) \longleftrightarrow x^m y^n$.

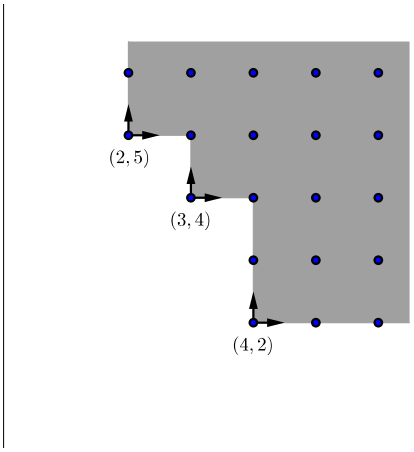


Figura 1: Um ideal monomial em $\mathbb{Z}^2_{\geq 0}$.

Lema 2.21. *Seja I um ideal monomial, e seja $f \in K[x_1, \ldots, x_n]$. Então as seguintes condições são equivalentes:*

i. $f \in I$.

ii. Todo termo de f está em I.

iii. f é uma combinação linear com coeficientes em K dos monômios em I.

Demonstração. As implicações $iii. \Rightarrow ii.$ e $ii. \Rightarrow i.$ são óbvias.

Agora, para mostrar que $i. \Rightarrow iii.$, seja $f \in I$, então $f = \sum_{i=1}^{s} h_i x^{\alpha_i}$, com $h_i \in K[x_1, \ldots, x_n]$. Escrevendo h_i como soma de monômios e expandindo, temos

$$f = \left(\sum_{j=1}^{t_1} a_{1j} \underbrace{x^{\gamma_{1j}} \cdot x^{\alpha_1}}_{\in I} \right) + \cdots + \left(\sum_{j=1}^{t_s} a_{sj} \underbrace{x^{\gamma_{sj}} \cdot x^{\alpha_s}}_{\in I} \right).$$

□

Corolário 2.22. *Dois ideais monomiais são iguais se, e somente se, eles contém os mesmos monômios.*

Demonstração. Se os ideais são iguais, então eles claramente contém os mesmos monômios. Reciprocamente, se I e J são dois ideais monomiais que contém os mesmos monômios,

$$\begin{array}{rcl} f \in I & \Leftrightarrow & f \text{ é uma } K-\text{combinação linear dos monômios em I} \\ & \Leftrightarrow & f \text{ é uma } K-\text{combinação linear dos monômios em J} \\ & \Leftrightarrow & f \in J. \end{array}$$

□

Teorema 2.23 (Lema de Dickson)**.** *Um ideal monomial $I = \langle x^\alpha : \alpha \in A \rangle \subset K[x_1, \ldots, x_n]$ pode ser escrito da forma $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, onde $\alpha_1, \ldots, \alpha_s \in A$. Em particular, I tem uma base finita.*

Demonstração. Procederemos por indução em n. Se $n = 1$, então I é gerado por monômios x_1^α, com $\alpha \subset \mathbb{Z}_{\geq 0}$. Tome β como o menor elemento de A. Assim, $\beta \leq \alpha$ para todo $\alpha \in A$, e consequentemente x_1^β divide todos os geradores de I. Portanto $I = \langle x_1^\beta \rangle$.
Suponha agora que $n > 1$ e que o resultado é valido para $n - 1$. Escreveremos as variáveis como $x_1, \ldots, x_{n-1}, y$, de modo que os monômios em $K[x_1, \ldots, x_{n-1}, y]$ possam ser escrito na forma $x^\alpha y^m$, com $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ e $m \in \mathbb{Z}_{\geq 0}$.
Suponha que $I \subset K[x_1, \ldots, x_{n-1}, y]$ é um ideal monomial. Para encontrar um conjunto finito de geradores de I, definimos um ideal J de $K[x_1, \ldots, x_{n-1}]$ gerado pelos monômios x^α para os quais $x^\alpha y^m \in I$ para algum $m \geq 0$. Como J é um ideal monomial em $K[x_1, \ldots, x_{n-1}]$, pela hipótese de indução temos que um número finito de x^α geram J, digamos que $J = \langle x^{\alpha_1}, \ldots, x^{\alpha_n} \rangle$.
Para $1 \leq i \leq s$, pela definição de J temos que $x^{\alpha_i} y^{m_i} \in I$ para algum $m_i \geq 0$. Tome m como o maior de todos os m_i. Então, para cada $0 \leq k \leq m - 1$, considere o ideal $J_k \subset K[x_1, \ldots, x_{n-1}]$ gerado pelos monômios x^β tais que $x^\beta y^k \in I$. Novamente, pela hipótese de indução, temos que J_k possui um número finito de geradores , digamos que $J_k = \langle x^{\alpha_k,1}, \ldots, x^{\alpha_k,s_k} \rangle$.
Se tomarmos a seguinte lista de monômios, veremos que I é gerado por monômios nela contidos:

$$\begin{array}{rcl} J_0 & \leftrightarrows & x^{\alpha_0,1}, \ldots, x^{\alpha_0,s_0}, \\ J_1 & \leftrightarrows & x^{\alpha_1,1} y, \ldots, x^{\alpha_1,s_1} y, \\ & \vdots & \\ J_{m-1} & \leftrightarrows & x^{\alpha_{m-1},1} y^{m-1}, \ldots, x^{\alpha_{m-1},s_{m-1}} y^{m-1}, \\ J & \leftrightarrows & x^{\alpha,1} y^m, \ldots, x^{\alpha,s} y^m. \end{array}$$

Observe agora que cada monômio de I é divisível por algum monômio acima listado. De fato, tome $x^\alpha y^p \in I$. Se $p \geq m$, algum $x^{\alpha_i} y^m$ dividirá $x^\alpha y^p$ pela construção de J. Por outro lado, se $p \leq m - 1$, então algum $x^{\alpha_{p,j}} y^p$ divide $x^\alpha y^p$ pela construção de J_p. Do lema (2.19) segue que os monômios acima listados geram o ideal que contem os mesmos monômios que I. Pelo corolário (2.22), os ideais são os mesmos. □

Exemplo 2.24. *Ao aplicarmos a demonstração do Lema de Dickson no ideal $I = \langle x^4 y^2, x^3 y^4, x^2 y^5 \rangle$, obtemos um conjunto finito de geradores para I, a saber,*

$$I = \langle x^2 y^5, x^4 y^2, x^4 y^3, x^3 y^4 \rangle.$$

Corolário 2.25. *Seja $>$ uma relação em $\mathbb{Z}^n_{\geq 0}$ satisfazendo as seguintes condições:*

i. *$>$ é uma ordem total em $\mathbb{Z}^n_{\geq 0}$*

ii. *Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$, então $\alpha + \gamma > \beta + \gamma$.*

Então $>$ é uma boa ordem se, e somente se, $\alpha \geq 0$ para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Demonstração. Suponha que $>$ é uma boa ordem e tome α_0 como o menor elemento de $\mathbb{Z}^n_{\geq 0}$. Se $0 > \alpha_0$, pelo item $ii.$ da hipótese, teríamos $\alpha_0 > 2\alpha_0$, o que é um absurdo, pois α_0 é o menor elemento de $\mathbb{Z}^n_{\geq 0}$. Portanto, $\alpha_0 \geq 0$.
Reciprocamente, suponha que $\alpha_0 \geq 0$ para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$ e seja $A \subset \mathbb{Z}^n_{\geq 0}$ não vazio. Tome $I = \langle x^\alpha : \alpha \in A \rangle$, que é um ideal monomial e pelo Lema de Dickson segue que $\alpha_1, \ldots, \alpha_s \in A$ é um conjunto gerador para I. Sem perda de generalidade, podemos supor $\alpha_1 < \alpha_2 < \cdots < \alpha_s$. Mostremos agora que α_1 é o menor elemento de A. De fato, tome $a \in A$ e note que $x^\alpha \in I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$ e pelo (2.19), segue que algum x^{α_i} divide x^α. Podemos então escrever $\alpha = \alpha_i + \gamma$ para algum $\gamma \in \mathbb{Z}^n_{\geq 0}$. Como $\gamma \geq 0$, pelo item $ii.$ da hipótese temos

$$\alpha = \alpha_i + \gamma \geq \alpha_i + 0 = \alpha_i \geq \alpha_1.$$

Portanto α_1 é o menor elemento de A. □

2.4 O Teorema das Bases de Hilbert e Bases de Gröbner

Veremos agora que todo ideal em $K[x_1, \ldots, x_n]$ é finitamente gerado, e que qualquer cadeia ascendente de ideais em $K[x_1, \ldots, x_n]$ eventualmente torna-se estacionária.

Definição 2.26. *Seja $I \subset K[x_1, \ldots, x_n]$ um ideal diferente de $\{0\}$.*

i. *Denotamos por $TL(I)$ o conjunto dos termos líderes dos elementos de I. Assim,*

$$TL(I) = \{cx^\alpha : \text{ existe } f \in I \text{ com } TL(f) = cx^\alpha\}$$

ii. *Denotamos por $\langle TL(I) \rangle$ o ideal gerado pelos elementos de $TL(I)$.*

Proposição 2.27. *Seja $I \subset K[x_1, \ldots, x_n]$ um ideal.*

i. *$\langle TL(I) \rangle$ é um ideal monomial.*

ii. *Existem $g_1, \ldots, g_t \in I$ tais que $\langle TL(I) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$.*

Demonstração.

i. Os monômios líderes $ML(g)$ dos elementos $g \in I - \{0\}$ geram o ideal monomial $\langle ML(g) : g \in I - \{0\} \rangle$. Como $ML(g)$ e $TL(g)$ são múltiplos por uma constante não nula, temos que o ideal $\langle TL(g) : g \in I - \{0\} \rangle = \langle TL(I) \rangle$. Portanto, $\langle TL(I) \rangle$ é um ideal monomial.

ii. Como $\langle TL(I) \rangle$ é gerado pelos monômios $ML(g)$ para $g \in I - \{0\}$, pelo Lema de Dickson temos que $\langle TL(I) \rangle = \langle ML(g_1), \ldots, ML(g_t) \rangle$ para um número finito de polinômios $g_1, \ldots, g_t \in I$. Como $ML(g_i)$ é múltiplo de $TL(g_i)$ por uma constante não nula, segue que $\langle TL(I) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$.

□

Teorema 2.28 (Teorema das Bases de Hilbert)**.** *Todo ideal $I \subset K[x_1, \ldots, x_n]$ possui um conjunto gerador finito, isto é, $I = \langle g_1, \ldots, g_t \rangle$ para $g_1, \ldots, g_t \in I$.*

Demonstração. Se $I = \{0\}$, basta tomar o conjunto gerador como $\{0\}$.
Se I contem polinômios não nulos então o conjunto gerador $g_1, \ldots, g_t$ para I pode ser construido da seguinte maneira: Pela proposição (2.27), existem $g_1, \ldots, g_t \in I$ tais que $\langle TL(I)\rangle = \langle TL(g_1), \ldots, TL(g_t)\rangle$. Vamos mostrar que $\langle I\rangle = \langle g_1, \ldots, g_t\rangle$.
Como cada $g_i \in I$, é claro que $\langle g_1, \ldots, g_t\rangle \subset I$.
Reciprocamente, seja f um polinômio em I e divida f por $(g_1, \ldots, g_t)$. Pelo algoritmo da divisão obtemos uma expressão da forma

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

onde nenhum termo de r é divisível por algum $TL(g_1), \ldots, TL(g_t)$. Vamos mostrar que $r = 0$.
Rearranjando termos, podemos escrever

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

Se $r \neq 0$, então $TL(r) \in \langle TL(I)\rangle = \langle TL(g_1), \ldots, TL(g_t)\rangle$, e pelo lema (2.19), segue que $TL(r)$ deve ser divisível por algum $TL(g_i)$, o que contradiz o fato de r ser o resto da divisão. Assim,

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

e portanto $I \subset \langle g_1, \ldots, g_t\rangle$. □

Definição 2.29. *Dada uma ordem monomial, um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal é uma* ***base de Gröbner*** *(ou* ***base padrão****) se*

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

Originalmente Bruno Buchberger havia dado o nome de Base padrão ao que hoje conhecemos como Bases de Gröbner. Alguns anos após a defesa de sua tese, Bruno escreveu um artigo em que propunha a mudança de terminologia como uma forma de homenagem ao seu orientador de doutorado. A mudança foi aceita e é amplamente mais usada que o termo original, embora ambos sejam corretos e equivalentes.

O seguinte resultado mostra que todo ideal admite base de Gröbner:

Corolário 2.30. *Dada uma ordem monomial, então todo ideal $I \subset K[x_1, \ldots, x_n]$ diferente de $\{0\}$ possui uma base de Gröbner. Além disso, toda base de Gröbner para um ideal I é também uma base para I.*

Demonstração. Dado um ideal não nulo, o conjunto $G = \{g_1, \ldots, g_t\}$ construído na demonstração do Teorema das Bases de Hilbert é uma base de Gröbner por definição. Agora, para mostrar que qualquer base de Gröbner do dado ideal é também uma base para o mesmo, observe que se $\langle TL(I)\rangle = \langle TL(g_1), \ldots, TL(g_t)\rangle$, então pelo mesmo argumento do teorema anterior temos que $I = \langle g_1, \ldots, g_t\rangle$, portanto G é uma base para I. □

Exemplo 2.31. *Consideremos o ideal $J = \langle g_1, g_2\rangle = \langle x + z, y - z\rangle$. Mostraremos que g_1 e g_2 formam uma base de Gröbner com respeito a ordem lexicográfica em $\mathbb{R}[x, y, z]$. Para isto, precisamos mostrar que qualquer elemento não nulo de J se encontra no ideal $\langle TL(g_1), TL(g_2)\rangle = \langle x, y\rangle$. Pelo Lema* (2.19)*, isto é equivalente a mostrar que o termo líder de qualquer elemento não nulo de J é divisível por x ou y.*

Tome $f = Ag_1 + Bg_2 \in J$. Suponha que f é um polinômio não nulo e que $TL(f)$ não é divisível por x e y. Como estamos considerando a ordem lexicográfica segue que f deve ser um polinômio apenas na variável z. Entretanto f se anula na variedade $L = \mathcal{V}(x + z, y - z) \subset \mathbb{R}^3$, pois $f \in J$. Como o único polinômio que se anula em todos os pontos de L é o polinômio nulo temos $J = 0$, o que é uma contradição.
Segue então que $\langle g_1, g_2\rangle$ é uma base de Gröbner para J.

Teorema 2.32 (Condição de Cadeia Ascendente)**.** *Seja*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

uma cadeia ascendente de ideais em $K[x_1, \ldots, x_n]$. Então existe $N \geq 1$ tal que

$$I_N = I_{N+1} = I_{N+2} = \cdots.$$

Demonstração. Dada a cadeia ascendente de ideais $I_1 \subset I_2 \subset I_3 \subset \cdots$, considere o conjunto $I = \bigcup_{i=1}^{\infty} I_i$. Vamos mostrar que I é um ideal. De fato, Como $0 \in I_i$ para todo i, segue que $0 \in \bigcup_{i=1}^{\infty} I_i$.
Agora, sejam $f, g \in I$, então existem índices p, q tais que $f \in I_p$ e $g \in I_q$. Sem perda de generalidade podemos supor que $p \geq q$. Como temos a cadeia ascendente, segue que $f, g \in I_p$ e consequentemente $f + g \in I_p$, pois I_p é um ideal. Logo, $f + g \in \bigcup_{i=1}^{\infty} I_i$.
Suponha agora que $f \in I$ e $r \in K[x_1, \ldots, x_n]$, então $f \in I_k$ para algum k e $fr \in I_k$, pois I_k é um ideal. Logo, $fr \in \bigcup_{i=1}^{\infty} I_i$.

Pelo Teorema das Bases de Hilbert, segue que I possui um conjunto gerador finito, digamos $I = \langle f_1, \ldots, f_s \rangle$. Observe que cada gerador está contido em algum I_j, digamos $f_i \in I_{j_i}$ para algum j_i, $i = 1, \ldots, s$. Se tomarmos N como o máximo de todos os j_i, então pela definição de cadeia ascendente segue que $f_i \in I_N$ para todo i. Temos então

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

Disto resulta que a cadeia ascendente se estabiliza em I_N, desta forma todos os ideais subsequentes na cadeia são iguais. □

2.5 Propriedades e aplicações das Bases de Gröbner

Proposição 2.33. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para o ideal $I \subset K[x_1, \ldots, x_n]$ e seja $f \in K[x_1, \ldots, x_n]$. Então existe um único $r \in K[x_1, \ldots, x_n]$ satisfazendo as seguintes propriedades:*

i. Nenhum termo de r é divisível pelos $TL(g_1), \ldots, TL(g_t)$.

ii. Existe $g \in I$ tal que $f = g + r$.

Em particular, r é o resto da divisão de f por G independentemente da ordem na qual os elementos de G estão.

Demonstração. Pelo algoritmo da divisão, podemos escrever $f = a_1 g_1 + \cdots + a_t g_t + r$, com r satisfazendo a condição $i.$. Se definirmos $g = a_1 g_1 + \cdots a_t g_t \in I$, então temos que a condição $ii.$ é satisfeita e garantimos a existência de r.
Para provar que r é único, suponha que $f = g + r = \bar{g} + \bar{r}$ satisfazendo simultaneamente $i.$ e $ii.$. Então $r - \bar{r} = \bar{g} - g \in I$ e se $r \neq \bar{r}$ segue que $TL(r - \bar{r}) \in \langle TL(I) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$. Pelo lema (2.19), segue que $TL(r - \bar{r})$ é divisível por algum $TL(g_i)$, logo $r - \bar{r}$ deve ser zero e portanto r é único. □

O resultado a seguir resolve o problema da pertinência de um polinômio em um ideal em $K[x_1, \ldots, x_n]$.

Corolário 2.34. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para o ideal $I \subset K[x_1, \ldots, x_n]$ e seja $f \in K[x_1, \ldots, x_n]$. Então $f \in I$ se, e somente se, o resto da divisão de f por G é zero.*

Definição 2.35. *Escreveremos $\bar{f}^F$ para o resto da divisão de f pela s-upla ordenada $F = (f_1, \ldots, f_s)$. Se F é uma base de Gröbner para $\langle f_1, \ldots, f_s \rangle$, então podemos tomar F como um conjunto (sem uma ordem em particular).*

A definição a seguir generaliza o conceito de mínimo múltiplo comum:

Definição 2.36. *Sejam $f, g \in K[x_1, \ldots, x_n]$ polinômios não nulos.*

*i. Se $multigrau(f) = \alpha$ e $multigrau(g) = \beta$, tome $\gamma = (\gamma_1, \ldots, \gamma_n)$, onde $\gamma_i = \max(\alpha_i, \beta_i)$ para todo i. Chamaremos x^γ de **mínimo múltiplo comum** de $ML(f)$ e $ML(g)$, denotado por $x^\gamma = mmc(ML(f), ML(g))$.*

ii. O ***S-polinômio*** *de f e g é a combinação*

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

Exemplo 2.37. *Seja $f = x^3y^2 - x^2y^3 + x$ e $g = 3x^4y + y^2$ em $\mathbb{R}[x,y]$ com respeito a ordem lexicográfica graduada. Temos que $\gamma = (4,2)$, logo*

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - \left(\frac{1}{3}\right) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - \left(\frac{1}{3}\right) y^3. \end{aligned}$$

Lema 2.38. *Suponha que temos a soma $\sum_{i=1}^s c_i f_i$, onde $c_i \in K$ e $multigrau(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ 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 dos S-polinômios $S(f_j, f_k)$, para $1 \leq j,k \leq s$. Além disso, todo $S(f_i, f_k)$ tem $multigrau < \delta$.*

Demonstração. Seja $d_i = CL(f_i)$ de modo que $c_i d_i$ seja o coeficiente líder de $c_i f_i$. Como $multigrau(c_i f_i) = \delta$ e sua soma é estritamente menor que δ, segue então que $\sum_{i=1}^s c_i d_i = 0$.
Tome $p_i = \frac{f_i}{d_i}$ e note que p_i é mônico. Considere agora

$$\begin{aligned} \sum_{i=1}^s c_i f_i &= \sum_{i=1}^s c_i d_i p_i \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) \\ &\quad + (c_1 d_1 + \cdots + c_s d_s) p_s. \end{aligned}$$

Por hipótese $TL(f_i) = d_i x^\delta$, o que implica que o $mmc(CL(f_i), CL(f_k)) = x^\delta$. Assim,

$$S(f_j, f_k) = \frac{x^\delta}{TL(f_i)} f_j - \frac{x^\delta}{TL(f_k)} f_k = f_j \frac{x^\delta}{d_j x^\delta} - f_k \frac{x^\delta}{d_k x^\delta} = p_j - p_k.$$

Como $\sum_{i=1}^s c_i d_i = 0$ e pela equação 2.5 a soma acima pode ser reescrita como

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

que é uma soma na forma desejada. Como $multigrau(p_j) = multigrau(p_k) = \delta$ e p_j e p_k são mônicos, segue que $multigrau(p_j - p_k) < \delta$. Pela equação 2.5 o mesmo vale para $S(f_j, f_k)$. □

O próximo teorema é uma caracterização para bases de Gröbner:

Teorema 2.39. *Seja I um ideal em $K[x_1, \ldots, x_n]$. Então a 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 (em alguma ordem) é zero.*

Demonstração. Suponha que G é uma base de Gröbner, então como $S(g_i, g_j) \in I$ pelo Corolário (2.34) o resto da divisão por G é zero.

Reciprocamente seja $f \in I$ um polinômio não nulo. Devemos mostrar que se o $S-$polinômios têm restos iguais a zero na divisão por G, então $TL(f) \in \langle TL(g_1), \ldots, TL(g_t) \rangle$. Por definição, existem polinômios $h_i \in K[x_1, \ldots, x_n]$ tais que

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

Tome $m(i) = multigrau(h_i, g_i)$ e defina $\delta = \max(m(1), \ldots, m(t))$. Pelo Lema (2.13) temos que

$$multigrau(f) \leq \max(multigrau(h_i, g_i)) \leq \delta.$$

Considere agora todos os possiveis modos em que f pode ser escrito como na equação 1. Para cada expressão, obtemos um δ que pode ser diferente. Como a ordem monomial é bem ordenada, podemos tomar uma expressão 1 para f de modo que δ é mínimo.
Mostremos agora que $multigrau(f) = \delta$. Suponha que vale $multigrau(f) < \delta$. Podemos reescrever f isolando os termos cujo multigrau é δ da seguinte maneira:

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} TL(h_i) g_i + \sum_{m(i)=\delta} (h_i - TL(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{2}$$

Os monômios que aparecem na segunda e terceira soma da segunda linha têm multigrau menor que δ. Assim, pela hipótese que $multigrau(f) < \delta$ segue que a primeira soma também tem multigrau menor que δ.
Seja $TL(h_i) = c_i x^{\alpha(i)}$. Então a primeira soma $\sum_{m(i)=\delta} TL(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ se encaixa nas hipóteses do Lema (2.38) com $f_i = x^{\alpha(i)} g_i$. Pelo Lema (2.38) temos que esta soma é uma combinação linear de $S-$polinômios $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$. Entretanto,

$$\begin{aligned} S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) &= \frac{x^\delta}{x^{\alpha(j)} TL(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(k)} TL(g_k)} x^{\alpha(k)} g_k \\ &= x^{\delta - \gamma_{jk}} S(g_j, g_k), \end{aligned}$$

onde $x^{\gamma_{jk}} = mmc(ML(g_j), ML(g_k))$. Logo existem constantes $c_{jk} \in K$ tais que

$$\sum_{m(i)=\delta} TL(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k). \tag{3}$$

Por hipótese o resto de $S(g_j, g_k)$ na divisão por $g_1, \ldots, g_t$ é zero. Pelo algoritmo da divisão, isto significa que cada $S-$polinômio pode ser escrito da forma

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{4}$$

onde $a_{ijk} \in K[x_1, \ldots, x_n]$. Ainda, do algoritmo da divisão temos que

$$multigrau(a_{ijk} g_i) \leq multigrau(S(g_j, g_k)) \tag{5}$$

para todo i, j, k. Multiplicando a expressão $S(g_j, g_k)$ por $x^{\delta - \gamma_{jk}}$ obtemos

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

onde $b_{ijk} = x^{\delta - \gamma_{jk}} a_{ijk}$. Por 5 e pelo Lema (2.38) temos que

$$multigrau(b_{ijk} g_i) \leq multigrau(x^{\delta - \gamma_{jk}} S(g_j, g_k)) < \delta. \tag{6}$$

Substituindo a expressão acima em 3 obtemos a equação

$$\sum_{m(i)=\delta} TL(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk} \left(\sum_i b_{ijk} g_i \right) = \sum_i \tilde{h}_i g_i,$$

e por 6 segue que $multigrau(\tilde{h}_i g_i) < \delta$.
Agora, substituindo $\sum_{m(i)=\delta} TL(h_i) g_i = \sum_i \tilde{h}_i g_i$ na equação 2 podemos obter uma expressão para f como uma combinação polinomial de g_is onde todos os termos têm multigrau menor que δ, e isto contradiz a minimalidade de δ. □

2.6 O Algoritmo de Buchberger

Teorema 2.40. *Seja $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ um ideal de polinômios. Então a base de Gröbner para I pode ser construída em um número finito de etapas através do seguinte algoritmo:*

```
Entrada: F = (f_1, ..., f_s)
Saída: uma base de Gröbner G = (g_1, ..., g_t) para I,
com F subconjunto de G

G := F
Repetir
    G' := G
    Para cada par {p, q} com p != q em G', faça
        S : = resto da divisão de S(p, q) por G
        Se S != 0, então G := G unido de {S}
Até G = G'
```

Demonstração. Para facilitar, denotaremos $\langle G \rangle = \langle g_1, \ldots, g_t \rangle$ se $G = \{g_1, \ldots, g_t\}$ e $\langle TL(G) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$.
Primeiramente, vamos verificar que $G \subseteq I$ está garantido em cada estágio do algoritmo. Inicialmente $G = F \subset I$. Suponha agora que $G \subseteq I$ e vamos verificar que $G \cup \{S\} \subseteq I$. Notemos que, dados $p, q \in G$, com $p \neq q$, temos

$$S(p,q) = a_1 g_1 + \cdots + a_t g_t + \overline{S(p,q)^{G'}}$$

onde $g_i \in G$ e $a_i \in K[x_1, \ldots, x_n]$ para todo $i = 1, \ldots, t$.
Logo,

$$S = \overline{S(p,q)^{G'}} = S(p,q) - (a_1 g_1 + \cdots + a_t g_t) \in G.$$

Assim, $G \cup \{S\} = G \subseteq I$, o que significa que a cada iteração, ampliamos G por meio de adição de elementos do próprio G. Notemos também que $F = \{f_1, \cdots, f_s\}$, que é uma base de I, está contida em G, isto implica que G é uma base de I.
O algoritmo termina quando $G = G'$, o que significa que $S = \overline{S(p,q)^{G'}} = 0$, para todo $p, q \in G$. Pelo Critério de Buchberger, segue entao que G é uma base de Gröbner.

Agora resta verificar apenas que o algoritmo termina. Para isto, vamos analisar o que acontece com G após cada iteração. O conjunto G consiste de G' (antigo G) junto com os restos não nulos de S-polinômios de elementos e G'. Então, como $G' \subset G$, segue que

$$\langle TL(G') \rangle \subset \langle TL(G) \rangle \tag{7}$$

Além disso, se $G' \neq G$, vamos mostrar que $\langle TL(G') \rangle$ é estritamente menor que $\langle TL(G) \rangle$. Para ver isto, suponha que um resto não nulo r de S-polinômios foi adicionado a G. Desde que r é o resto da divisão por G', segue que $TL(r)$ não é divisível por nenhum dos termos líderes dos elementos de G'. Logo, $TL(r) \notin \langle TL(G') \rangle$, ainda que $TL(r) \in \langle TL(G) \rangle$. Concluímos assim que $\langle TL(G') \rangle$ está contido estritamente em $\langle TL(G) \rangle$.

Por (7), os ideais $\langle TL(G') \rangle$ obtidos pelas sucessivas iterações formam uma cadeia ascendente de ideais em $K[x_1, \ldots, x_n]$. Assim, pelo Teorema (2.32), após um número finito de iterações, esta cadeia se estabilizará. Eventualmente $\langle TL(G) \rangle = \langle TL(G') \rangle$. Pelo parágrafo anterior, temos $G = G'$ e, portanto, o algoritmo irá terminar em um número finito de passos. □

Exemplo 2.41. *Considere em $\mathbb{Q}[x,y]$ com a ordem grlex $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. Note que $F = \{f_1, f_2\}$ não é uma base de Gröbner para I, pois $TL(S(f_1, f_2)) = -x^2 \notin \langle TL(f_1), TL(f_2)\rangle$. Seguindo o algoritmo, tome inicialmente $G = F$ e considere $G' = G$. Em seguida, calculamos $\overline{S(f_1, f_2)^{G'}}$. Note que*

$$S(f_1, f_2) = -x^2 \Rightarrow \overline{S(f_1, f_2)^{G'}} = -x^2 \neq 0$$

Logo, fazemos $G = G \cup \{\overline{S(f_1, f_2)^{G'}}\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2\} = \{f_1, f_2, f_3\}$. Como $G' \neq G$, o processo continua. Agora, consideramos $G' = G = \{f_1, f_2, f_3\}$. Temos

$$S(f_1, f_3) = -2xy \Rightarrow \overline{S(f_1, f_3)^{G'}} = -2xy \neq 0.$$

E, portanto,

$$G = G \cup \{\overline{S(f_1, f_3)^{G'}}\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy\} = \{f_1, f_2, f_3, f_4\}$$

Continuamos tendo $G \neq G'$, então consideramos $G' = \{f_1, f_2, f_3, f_4\}$ e repetimos o processo.

$$\begin{aligned} S(f_1, f_4) = -2xy^2 = yf_4 &\Rightarrow \overline{S(f_1, f_4)^{G'}} = 0 \\ S(f_2, f_3) = -2y^2 + x &\Rightarrow \overline{S(f_2, f_3)^{G'}} = -2y^2 + x \neq 0. \end{aligned}$$

Então,

$$G = G \cup \{\overline{S(f_2, f_3)^{G'}}\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\} = \{f_1, f_2, f_3, f_4, f_5\}.$$

Finalmente, é fácil verificar que para este G, temos que

$$S = \overline{S(f_i, f_j)^G} = 0, \text{ com } 1 \leq i < j \leq 5.$$

Portanto, a partir deste passo, teremos $G = G'$ e então finalizamos o algoritmo aqui. Agora, pelo critério de Buchberger, segue que uma base de Gröbner para I é dada por

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

O próximo resultado nos permite eliminar geradores "desnecessários"e assim, reduzir nossa base de Gröbner.

Lema 2.42. *Seja G uma base de Gröbner para o ideal de polinômios I. Seja $p \in G$ um polinômio tal que $TL(p) \in \langle TL(G - \{p\})\rangle$. Então $G - \{p\}$ é também uma base de Gröbner para I.*

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

Ao ajustarmos as constantes de modo que todos os coeficientes líderes sejam 1 e removendo termos redundantes de G, chegamos a uma base que chamamos de minimal no seguinte sentido:

Definição 2.43. *Uma **base de Gröbner minimal** para um ideal de polinômios I é uma base de Gröbner G que satisfaz as seguintes condições:*

i. $CL(p) = 1$, para todo $p \in G$.

ii. Para todo $p \in G$, $TL(p) \notin \langle TL(G - \{p\})\rangle$.

Exemplo 2.44. *Temos que $G = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$ é uma base de Gröbner para o ideal $I = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$.*
Ainda,

$$\begin{aligned} x^3 &= (-x)(-x^2) \\ x^2y &= \left(-\frac{1}{2}x\right)(-2xy) \end{aligned}$$

Pelo lema anterior temos que $G = \{-x^2, -2xy, -2y^2 + x\}$ é uma base de Grobner para I. Agora considere:

$$\begin{aligned} x^2 &= (-1)(-x^2) \\ xy &= \left(-\frac{1}{2}\right)(-2xy) \\ y^2 - \frac{1}{2}x &= \left(-\frac{1}{2}\right)(-2y^2 + x). \end{aligned}$$

Assim, a base de Gröbner mininal é $G = \{x^2, xy, y^2 - \frac{1}{2}x\}$.

Quando G é uma base de Gröbner minimal, os termos líderes $TL(p), p \in G$ formam uma única base minimal de $\langle TL(I)\rangle$. Infelizmente, o ideal original I pode admitir várias bases de Gröbner minimais. O ideal I acima, por exemplo, admite

$$\tilde{f}_3 = x^2 + axy, \tilde{f}_4 = xy, \tilde{f}_5 = y^2 - \frac{1}{2}x \tag{8}$$

como base de Gröbner minimal, com $a \in \mathbb{Q}$ qualquer. Podemos então produzir infinitas bases de Gröbner minimais. Há uma maneira de escolher uma base que é "melhor", no seguinte sentido:

Definição 2.45. *Uma **base de Gröbner reduzida** para um ideal de polinômios I é uma base de Gröbner G que satisfaz as seguintes condições:*

i. $CL(p) = 1$, para todo $p \in G$.

ii. Para todo $p \in G$, nenhum monômio de p está em $\langle TL(G - \{p\})\rangle$.

Tomando $a = 0$ em (8), segue que esta base é reduzida. As bases reduzidas possuem a seguinte propriedade:

Proposição 2.46. *Seja $I \neq \{0\}$ um ideal de polinômios. Então dada uma ordem monomial, I possui uma única base de Gröbner reduzida.*

Demonstração. Seja G uma base de Gröbner minimal para I. Dizemos que $g \in G$ é reduzido em G se nenhum monômio de g pertence a $\langle TL(G - \{g\})\rangle$. Nosso objetivo é modificar G de forma que todos os seus elementos fiquem reduzidos.

Uma primeira observação é que se g é um elemento reduzido em G então g também será reduzido em qualquer outra base F de Gröbner mininal de I que contem g e eles contêm o mesmos termos líderes. De fato, seja F uma base de Gröbner minimal para I, tal que $g \in F$ e $TL(G) = TL(F)$ então $TL(G - \{g\}) = TL(F - \{g\})$, assim temos que $\langle TL(F - \{g\})\rangle = \langle TL(G - \{g\})\rangle$, como nenhum monômio de g não pertencem a $\langle TL(G - \{g\})\rangle$ então nenhum monômio de g pertence a $\langle TL(F - \{g\})\rangle$.

Dado, $g \in G$, seja $g' = \overline{g}^{G-\{g\}}$, temos que o conjunto $G' = (G - \{g\}) \bigcup \{g'\}$ é uma base de Gröbner minimal para I.

Temos que $TL(g) = TL(g')$. De fato temos que G é uma base de Gröbner minimal, assim, $TL(g)$ não é divisível por nenhum dos termos líderes de $G - \{g\}$, logo $TL(g) = TL(g')$.

Agora iremos mostrar que G' é uma bases de Gröbner para I. De fato, $g \in I$ e $(G - \{g\}) \subset I$, segue que o resto $g' \in I$. Logo $G' \subset I$. Sabemos que $TL(g) = TL(g')$, então $TL(G) = TL(G')$, assim $\langle TL(G)\rangle = \langle TL(G')\rangle = \langle TL(I)\rangle$. Portanto G' é uma base de Gröbner.

Iremos mostrar que G' é minimal para I. De fato, temos que G é uma base de Gröbner minimal e que $(G - \{g\}) \bigcup \{g'\}$. Notemos que $(G' - \{g'\}) = (G - \{g\})$ e $TL(g) = TL(g')$ segue que

$$TL(g) \notin \langle TL(G - \{g\})\rangle \Rightarrow TL(g') \notin \langle TL(G' - \{g'\})\rangle.$$

O fato de G ser o minimal implica que $TL(g') = 1$, para todo $g \in G'$.

Temos que g é um elemento reduzido. De fato, g' é o resto da divisão de g por $G - \{g\}$, assim cada monômio de g' não é divisível por nenhum elemento de $TL(G - \{g\})$ e consequentemente g' é reduzido.

Aplicando este processo para todo $g \in G$, obteremos uma base de Gröbner reduzida para I. Suponha G e $\hat{G}$ são duas bases de Gröbner reduzidas para I. Em particular G e G' são bases de Gröbner minimais. Pelo lema anterior,

$$TL(G) = TL(G')$$

Assim, temos que para todo $g \in G$, existe um $\hat{g} \in \hat{G}$ tal que $TL(g) = TL(\hat{g})$. Então, basta mostrar que $g = \hat{g}$ ou $g - \hat{g} = 0$.

Notemos que $g - \hat{g} \in I$, e como G é uma base de Gröbner, segue que $\overline{g - \hat{g}}^G = 0$. Agora, do fato de $TL(g) = TL(g')$, estes termos irão se aular em $g - g'$. E do fato de G ser reduzido, segue que nenhum monômio de g pertence a $\langle TL(G - \{g\})\rangle$, e portanto apenas $TL(g)$ pertence a $\langle TL(G)\rangle = \langle TL(G')\rangle$. Sendo assim, $0 = \overline{g - \hat{g}}^G = g - \hat{g}$ e portanto $g = \hat{g}$. □

Agora, afim de apresentarmos a solução que Buchberger deu ao problema enunciado no inicio deste trabalho, introduziremos o seguinte conceito:

Definição 2.47. *Seja $I \subset K[x_1, \ldots, x_n]$ um ideal. A **pegada** de I (com respeito à uma ordem monomial fixada) é o conjunto*

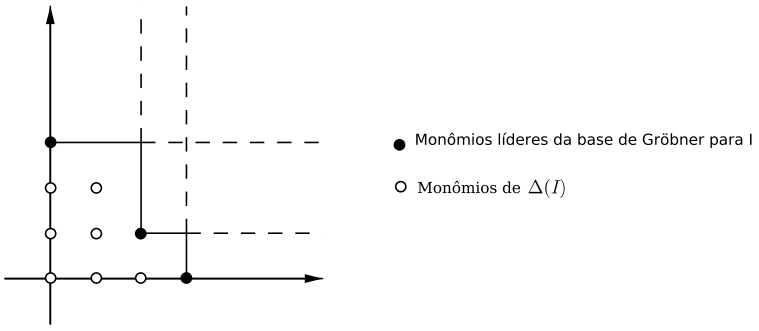
$$\Delta(I) = \{M \text{ monômio} : M \text{ não é o monômio líder de nenhum polinômio em } I\}.$$

O resultado seguinte mostra a relação entre a pegada de um ideal e uma base de Gröbner para I.

Proposição 2.48. *Seja $I \subset K[x_1, \ldots, x_n]$ um ideal e seja $\{g_1, \ldots, g_s\}$ uma base de Gröbner para I. Então um monômio M pertence a $\Delta(I)$ se, e somente se, M não é um múltiplo de $ML(g_i)$ para todo $i \in \{1, \ldots, s\}$.*

Demonstração. Se M é um monômio em $\Delta(I)$, pela definição de pegada segue que M não é o monômio líder de nenhum polinômio em I, em particular, M não é múltiplo de $ML(g_i)$ para todo $i \in \{1, \ldots, s\}$.
Reciprocamente, da definição de base de Gröbner sabemos que se M não é um múltiplo de $ML(g_i)$ para todo $i \in \{1, \ldots, s\}$, então M não é o monômio líder de nenhum polinômio em I. □

Exemplo 2.49. *Seja $I = \langle x^3 - x, y^3 - y, x^2y - y\rangle \subset \mathbb{R}[x, y]$ e adotemos a ordem lexicográfica (escolhendo $y < x$). Uma verificação mostra $\{x^3 - x, y^3 - y, x^2y - y\}$ é uma base de Gröbner para I. Temos $ML(x^3 - x) = x^3, ML(y^3 - y) = y^3, ML(x^2y - y) = x^2y$ e aplicando a proposição acima, a seguinte representação nos mostra a pegada. Novamente usaremos a identificação $x^\alpha y^\beta \longleftrightarrow (\alpha, \beta)$.*



Os pontos $(3,0),(0,3)$ *e* $(2,1)$ *correspondem aos monômios líderes da base de Gröbner e a partir destes é possível determinar quais monômios não são múltiplos de pelo menos um deles. Segue que* $\Delta(I) = \{1, x, x^2, y, xy, y^2, xy^2\}$.

O teorema a seguir é o principal resultado da tese de doutorado de Bruno Buchberger [5], e foi o que motivou a introdução por ele do conceito de bases de Gröbner.

Teorema 2.50. *Seja* $I \subset K[x_1, \ldots, x_n]$ *um ideal. Então*

$$\mathcal{B} = \{M + I : M \in \Delta(I)\}$$

é uma base para $K[x_1, \ldots, x_n]/I$ *como um* $K-$*espaço vetorial.*

Demonstração. Seja $\mathcal{G}$ uma base de Gröbner para I com respeito à mesma ordem monomial usada para determinar $\Delta(I)$, e seja $f \in K[x_1, \ldots, x_n]$. Dividindo f por $\mathcal{G}$ obtemos um resto na forma $r = \sum_{i=1}^{t} a_i M_i$ onde $a_i \in K[x_1, \ldots, x_n]$ e $M_i \in \Delta(I)$ para todo $i = 1, \ldots, t$.
Como $f + I = r + I$ segue que $\mathcal{B}$ gera $K[x_1, \ldots, x_n]/I$ como um $K-$espaço vetorial. Vejamos agora que os vetores em $\mathcal{B}$ são linearmente independentes.
Suponha que $\sum_{i=1}^{l} b_i(M_i + I) = 0 + I$, onde $b_i \in K$ e $M_i \in \Delta(I)$ para todo $i = 1, \ldots, l$. Então $\sum_{i=1}^{l} b_i M_i \in I$ e assim devemos ter que cada $b_i = 0$ para todo $i = 1, \ldots, l$, pois caso contrário $\sum_{i=1}^{l} b_i M_i$ seria um elemento não nulo de I cujo monômio líder não é o monômio líder de um polinômio em I.

□

Exemplo 2.51. *Tomando o exemplo* (2.49)*, temos que o conjunto*

$$\{1 + I, x + I, x^2 + I, y + I, xy + I, y^2 + I, xy^2 + I\}$$

é uma base para $\mathbb{R}[x, y]/I$ *como um* $\mathbb{R}$*-espaço vetorial.*

Referências

[1] David A. Cox, John B. Little, Donal O'Shea. *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 4th edition, 2010.

[2] David A. Cox, John B. Little, Donal O'Shea. *Using Algebraic Geometry*, Springer, 1997.

[3] Thomas Becker, Volker Weispfenning, Heinz Kredel. *Gröbner Bases: A Computational Approach to Commutative Algebra*, Springer-Verlag, 1st edition, 1993.

[4] William W. Adams, Philippe Loustaunau. *An Introduction to Gröbner Bases*, AMS, Volume 3, 1994.

[5] Bruno Buchberger. *Ein algorithmus zum affinden der basiselemente des restklassen-rings nach einem nulldimensionalen polynomideal*, Tese de Doutorado, Mathematical Institutde, University of Innsbruck, 1965.