UNIVERSIDADE FEDERAL DE SERGIPE
DEPARTAMENTO DE MATEMÁTICA DE ITABAIANA
CURSO DE MATEMÁTICA

JOSÉ ANTÔNIO SANTOS PIMENTEL

UMA INTRODUÇÃO À BASE DE GRÖBNER

ITABAIANA/SE
2025

JOSÉ ANTÔNIO SANTOS PIMENTEL

UMA INTRODUÇÃO À BASE DE GRÖBNER

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Sergipe, ao Departamento de Matemática de Itabaiana, como requisito avaliativo para obtenção do grau de Licenciado em Matemática.
Orientador: Prof. Me. Samuel Brito Silva.

ITABAIANA/SE
2025

José Antônio Santos Pimentel

UMA INTRODUÇÃO À BASE DE GRÖBNER

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática de Itabaiana, Universidade Federal de Sergipe, como requisito avaliativo para obtenção de grau de Licenciado(a) em Matemática.

Banca Examinadora:

Prof. Samuel Brito Silva, Me.
Universidade Federal de Sergipe

Prof. Andre Santana Dorsea, Dr.
Universidade Federal de Sergipe

Prof. Danilo de Rezende Santiago, Dr.
Instituto Federal de Sergipe

Resultado: Aprovado Data: 07 / 10 / 2025

AGRADECIMENTOS

Primeiramente, não poderia deixar de agradecer a Deus, aquele quem me dar força, me protege, me guia e me livra de todo o mal.

À minha querida mamãe, que não mediu esforços para me oferecer todo apoio, mesmo morando tão longe, agradeço por todas as conversas e, principalmente, por todos os puxões de orelha. Ao meu pai, que, mesmo com todas as limitações, lutou para me proporcionar conforto. À minha irmanzinha e à minha madrinha, que sempre cuidou de mim como um filho que ela não teve, meu profundo agradecimento.

Agradeço ao meu professor, amigo e orientador Samuel Brito, meu "pai acadêmico". Obrigado por todas as broncas e por nunca desistir de me apoiar. A jornada não foi nada TRIVIAL, mas nós conseguimos. Infelizmente, um parágrafo é pouco para expressar a dimensão da minha gratidão por tudo o que o senhor fez por mim. Serei eternamente agradecido por todas as vezes em que me estendeu a mão, especialmente por ter disponibilizado seu valioso tempo de estudo de doutorado quando fui indevidamente penalizado. Foi uma honra imensa ser seu orientando.

Agradeço à minha namorada e companheira de curso por todos os momentos de alegria, tristeza e raiva. O caminho não foi fácil, mas certamente teria sido muito mais difícil sem você ao meu lado. Obrigado por, incansavelmente, me explicar as coisas de uma forma brilhante; eu certamente não estaria aqui neste momento se não fosse por você.

À minha família e amigos, que durante quatro anos acreditaram no meu sonho de morar fora, me apoiando, aconselhando e, às vezes, até brigando comigo. Também agradeço aos meus professores e funcionários da minha escola em Tucano e da UFS.

Deixo aqui meu profundo agradecimento aos amigos da Universidade Federal de Sergipe; o caminho para a conclusão do meu curso tornou-se muito mais leve com vocês ao meu lado, rindo nos corredores do bloco D. Por último, expresso meu profundo respeito e admiração aos professores do DMAI. Sinto-me extremamente privilegiado por conviver, por quase quatro anos, com os senhores(as).

RESUMO

Neste trabalho, desenvolveremos um estudo na área da Álgebra Comutativa, com foco nos resultados relacionados a um tema especial conhecido como Base de Gröbner. Os principais tópicos abordados incluem os anéis de polinômios em várias variáveis, destacando-se a forma como podemos estabelecer uma ordem monomial e o algoritmo da divisão no anel $K[x_1, \ldots, x_n]$. O conhecimento adquirido ao longo do primeiro capítulo servirá como fundamento para o estudo dessa base. Em especial, analisaremos a importância e a aplicação do algoritmo de Buchberger, utilizado para determinar uma Base de Gröbner. Por fim, buscaremos aplicar a teoria desenvolvida na resolução de sistemas não lineares, abordando exemplos práticos como o problema da coloração de mapas e sistemas de malha rodoviária

Palavras-chave: Ordem Monomial; Base de Gröbner; Algoritmo de Buchberger; Problema de Coloração.

ABSTRACT

In this work, we will develop a study in the area of Commutative Algebra, focusing on results related to a special topic known as the Gröbner Basis. The main subjects addressed include polynomial rings in several variables, highlighting how we can establish a monomial order and the division algorithm in the ring $K[x_1, \ldots, x_n]$. The knowledge acquired throughout the first chapter will serve as the foundation for the study of this basis. In particular, we will analyze the importance and application of Buchberger's algorithm, used to determine a Gröbner Basis. Finally, we will seek to apply the developed theory to the resolution of nonlinear systems, addressing practical examples such as the map coloring problem and road network systems.

Keywords: Monomial Order; Gröbner Basis; Buchberger's Algorithm; Coloring Problem.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\mathrm{cl}(f)$	Coeficiente líder do polinômio f
$K[x_1, \ldots, x_n]$	Anel de polinômios em várias variáveis sobre o corpo K
$\mathbb{M}_n(f)$	Conjunto de todos os monômios de f
$\mathrm{gr}(f)$	Grau do polinômio f
$\mathrm{ml}(f)$	Monômio líder do polinômio f
$\mathrm{tl}(f)$	Termo líder do polinômio f
$\alpha(i)$	Vetor com n entradas inteiras
m_i	Monômio no anel de polinômios
$\preceq$	Relação de ordem
$\preceq_L$	Ordem lexicográfica
$\preceq_R$	Ordem reversa
$\preceq_{LG}$	Ordem lexicográfica graduada
$\langle g_1, \ldots, g_n \rangle$	Conjunto gerado pelos elementos g_i
$\overline{f}^F$	Resto da divisão de f pela s-upla ordenada $(f_i)_{i \in \mathbb{N}}$
$S(f, g)$	S-polinômio entre f e g
A_k^n	Espaço afim n-dimensional sobre um corpo K
$\mathcal{V}(S)$	Variedade algébrica afim

SUMÁRIO

1 INTRODUÇÃO

Uma das ferramentas mais poderosas da Matemática é a resolução de equações algébricas. Em particular, a resolução de equações lineares em n variáveis permite modelar diversos problemas matemáticos presentes no cotidiano.

Essas equações passaram a ser estudadas de forma sistemática em uma área específica da álgebra, denominada *Álgebra Linear*. Tal estudo evidenciou que sistemas lineares com n variáveis podem representar objetos geométricos em $\mathbb{R}^n$, conhecidos como hiperplanos. Os sistemas de equações lineares da forma

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = 0$$

foram amplamente desenvolvidos e compreendidos no âmbito da Álgebra Linear.

Entretanto, a compreensão do comportamento de sistemas de equações polinomiais de grau superior a 1, isto é, sistemas de equações não lineares do tipo

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ f_2(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases}$$

onde $f_i \in K[x_1, \ldots, x_n]$ para $i = 1, \ldots, m$, ainda representava um grande desafio. Tais sistemas envolvem conjuntos de pontos cujas relações algébricas são mais complexas e não podem ser tratadas pelos métodos lineares tradicionais.

Na segunda metade do século XX, sob a orientação de Wolfgang Gröbner (1899–1980), em 1965, seu aluno de doutorado Bruno Buchberger desenvolveu a teoria de Bases de Gröbner. Sua tese tinha como objetivo determinar um método para encontrar uma base para $K[x_1, \ldots, x_n]/I$ como um K-espaço vetorial. Tal estudo possibilitou determinar se um sistema de equações polinomiais possui solução e, em caso afirmativo, como descrevê-la. Neste trabalho, iremos usar a Base de Gröbner para determinar as soluções de sistemas não lineares.

O objetivo principal deste trabalho é entender as características e propriedades da Base de Gröbner de um ideal $I \subseteq K[x_1, \ldots, x_n]$. Além disso, vamos determinar, se existirem, as soluções de sistemas não lineares. Para tanto, no capítulo 2 deste trabalho, apresentaremos as características gerais dos anéis de polinômios sobre um anel A. Além disso, iremos apresentar o algoritmo da divisão para polinômios em uma e em várias variáveis. Isso será necessário para refletirmos sobre as diferenças entre as duas divisões. Dentre outras coisas, iremos notar que a principal característica advém de como definimos uma ordenação monomial no anel de polinômios.

No capítulo 3, abordaremos um tipo de ideal muito importante para o nosso estudo introdutório acerca da Base de Gröbner, os ideais monomiais. Com eles, iremos entender

o que vem a ser uma Base de Gröbner de um ideal I no anel de polinômios. Além disso, iremos aprender, através de um algoritmo denominado Algoritmo de Buchberger, como determinar uma base de Gröbner a partir de uma base geradora de um ideal I.

No capítulo 4, por fim, faremos algumas aplicações de tudo o que foi construído. Entre outras coisas, entenderemos como o uso da Base de Gröbner nos fornece respostas para a determinação das soluções de sistemas de equações polinomiais não lineares. Isso será necessário para tratar dos problemas modelados no final do capítulo sobre o deslocamento de um trem em uma malha rodoviária, solução para a coloração do mapa do Nordeste e, por fim, da coloração do mapa das cidades circunvizinhas a Itabaiana-SE.

2 ANEL DE POLINÔMIOS

Neste capítulo, vamos apresentar os conceitos e resultados essenciais para entender os anéis de polinômios. Entre outros tópicos, abordaremos suas propriedades e a ordem que pode ser estabelecida entre monômios. Por fim, discutiremos a forma generalizada do algoritmo de divisão para polinômios com várias variáveis.

Convenção: Para que possamos trabalhar todos os conceitos relacionados aos anéis de polinômios e toda a teoria derivada do Capítulo 2, sempre que estivermos falando de um anel A, este será um anel comutativo e com unidade.

2.1 DE POLINÔMIOS EM UMA VARIÁVEL

Neste capítulo, vamos revisitar os resultados estudados em um curso básico de Álgebra na graduação, buscaremos introduzir e estender a ideia de polinômios em uma "variável"(ou "indeterminada") do tipo

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots a_1 t + a_0$$

onde $a_n, \ldots, a_0$ são elementos de um anel A.

Definição 1. Uma *sequência* de elementos de um conjunto A é uma função $a : \mathbb{N} \longrightarrow A$, que associa cada número natural n a um elemento a_n em A.

Escrevemos $(a_0, \ldots, a_n)$ ou simplesmente $(a_n)_{n\in\mathbb{N}}$ para indicar a sequência cujo n-ésimo termo é a_n.

Definição 2. Seja $(A, +, \cdot)$ um anel. Uma sequência $a : \mathbb{N} \longrightarrow A$ tal que $a_i = 0$ para todo i maior que um certo $k \in \mathbb{N}$, é chamada de *polinômio em uma variável sobre* A. Assim, temos que um polinômio em uma variável sobre A é da forma $(a_0, a_1, \ldots, a_k, 0, 0, \ldots)$, onde $a_0, \ldots, a_k$ são chamados de *coeficientes do polinômio*.

Observação 1. Não se deve confundir a sequência $(a_n)_{n\in\mathbb{N}}$ com o conjunto $\{a_1, \ldots, a_n\}$. Por exemplo, a sequência $(7, 7, 7, \ldots, 7, \ldots)$ não é o mesmo que $\{7\}$.

Definição 3. Seja $p = (a_n)_{n\in\mathbb{N}}$ um polinômio numa variável sobre A. Caso $a_n = 0$ para qualquer n em $\mathbb{N}$, então dizemos que p é o polinômio *identicamente nulo*, e escrevemos simplesmente $p = 0$.

Definição 4. Dado um polinômio $p \neq 0$, chama-se *grau de* p ao maior m em $\mathbb{N}$ tal que $a_m \neq 0$, e denotaremos por $\mathrm{gr}(p) = m$ para indicar que o grau de p é igual a m. Chamaremos a_m de *coeficiente líder* do polinômio p.

Caso $m = 0$, dizemos que p é um *polinômio constante*. nesse caso, temos que $p = (a, 0, \dots, 0)$ e podemos escrever $p = a$. A partir disso, podemos identificar o anel A com um subconjunto do conjunto dos polinomios em uma variável sobre A, é porque os elementos de A são polinômios constantes pertencentes a tal conjunto. Se o coeficiente líder $a_m = 1$, dizemos que p é um *polinômio mônico*.

Seja A' o conjunto de todos os polinômios em uma variável sobre A. Dados dois elementos $f = (a_0, a_1, \dots)$ e $g = (b_0, b_1, \dots)$ podemos definir as operações de soma e produto, respectivamente, em A' da seguinte forma:

$$\begin{array}{rccc} + : & A' \times A' & \longrightarrow & A' \\ & (f, g) & \longmapsto & \displaystyle\sum_{i=0}(a_i + b_i) \end{array}$$

Definimos o produto

$$\begin{array}{rccc} \cdot : & A' \times A' & \longrightarrow & A' \\ & (f, g) & \longmapsto & \displaystyle\sum_{i=0} c_i \end{array}$$

onde $c_i = \displaystyle\sum_{j=0}^{i} a_j b_{i-j}$.

Observação 2. Podemos verificar que $(A', +, \cdot)$ é um anel com unidade. De fato, os axiomas de anel podem ser rapidamente verificados, sendo que os elementos neutros da soma $(+)$ e da multiplicação $(\cdot)$ são $(0, 0, 0, \dots)$ e $(1, 0, 0, \dots)$, respectivamente. Dado o elemento $(a_0, a_1, \dots, a_n, \dots)$, seu simétrico na soma é $(-a_0, -a_1, \dots, -a_n, \dots)$. Buscando facilitar a notação, definiremos o seguinte conjunto:

Definição 5. Chama-se A' de *anel de polinômios em uma variável* onde

$$A' = \left\{ \sum_{i=0}^{n} a_i x^i ; n \in \mathbb{N}, a_i \in A \right\}.$$

Iremos denotar o anel $(A', +, \cdot)$ por $A[x]$. O polinômio $f \in A'$ será denotado por $f(x) \in A[x]$. Além disso, o x^i é chamado de *monômio*, para todo $i = 1, \dots, n$, e o conjunto de todos os monômios de $f(x) \in A[x]$ é indicado por $\mathbb{M}(f)$.

Vamos indicar a unidade $(1, 0, 0, \dots)$ de A' por $1 = x^0$, e, indutivamente, pode-se tomar $x^n = (0, 0, \dots, \underbrace{1}_{n+1}, 0, \dots)$. A partir daí, dado $p = (a0, a_1, \dots, a_n, 0, 0, \dots) \in A'$, podemos escrever $p = a_0 + a_1 x^1 + \cdots + a_n x^n$. Com a **Observação 2**, o conjunto $A[x]$ é um anel com unidade, onde a soma e o produto são definidos como $(f+g)(x) = f(x)+g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$, respectivamente.

Exemplo 1. Dados $f(x), p(x)$ em $\mathbb{Z}[x]$ com $f(x) = 2 + 2x + 3x^2 + x^3$ e $g(x) = x + x^3$ temos que sua soma e produto são respectivamente:

$$(f + g)(x) = 2 + 3x + 3x^2 + 2x^3$$

e

$$(f \cdot g)(x) = 2x + 2x^2 + 5x^3 + 3x^4 + 3x^5 + x^6.$$

Como já havíamos mencionado, um ponto importante no anel $A[x]$ é que ele carrega algumas características do anel A. Os resultados a seguir garantem essa afirmação.

Teorema 1. Se A é um anel comutativo com unidade, então $A[x]$ também é.

Demonstração. Considere $f(x) = a_1 + \cdots + a_n x^n$ e $g(x) = b_1 + \cdots + b_m x^m$ dois elementos do anel $A[x]$. Nosso objetivo é mostar que $(f \cdot g)(x) = (g \cdot f)(x)$. Assim

$$(f \cdot g)(x) = c_{n+m}x^{n+m} + \cdots + c_1 x + c_0$$

onde

$$c_k = (a_k b_0) + (a_{k-1} b_1) + \cdots + (a_0 b_k) \tag{1}$$

para $k = 0, 1, \ldots, n + m$. Como A é um anel comutativo, então podemos comutar os elementos de (1) da seguinte forma

$$c_k = (b_0 a_k) + (b_1 a_{k-1}) + \cdots + (b_k a_0).$$

Assim, temos que

$$(f \cdot g)(x) = c_{m+n}x^{m+n} + \cdots + c_1 x + c_0 = (g \cdot f)(x)$$

o que prova o teorema. □

Corolário 1. Se A é um domínio de integridade, então $A[x]$ também é.

Demonstração. Considere $f(x), g(x)$ dois elementos do anel $A[x]$. Pelo **Teorema 1** sabemos que $A[x]$ é um anel comutativo com unidade. Suponha $f(x) \neq 0$ e $g(x) \neq 0$. Então existem $a_n, b_m \in A$ com $a_n, b_m \neq 0$, e n, m os maiores possíveis. Como o anel A é de integridade $a_n b_m \neq 0$. Logo,

$$(f \cdot g)(x) = c_{n+m}x^{n+m} + \cdots + c_0.$$

Como $c_{n+m} = a_n b_m \neq 0$, então

$$(f \cdot g)(x) \neq 0.$$

Portanto, $A[x]$ é anel de integridade. □

Definição 6. Dado $f(x)$ em $A[x]$ da forma

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

com $a_n \neq 0$. Chamaremos de *termo líder de* $f(x)$: $\mathrm{tl}(f) = a_n x^n$, o *coeficiente líder de* $f(x)$: $\mathrm{cl}(f) = a_n$, o *monômio líder de* $f(x)$: $\mathrm{ml}(f) = x^n$ onde $n = \mathrm{gr}(f(x))$, que denotaremos por $\mathrm{gr}(f) = n$ e teremos $\mathrm{gr}(f) = 0$ se, e somente se, $f(x) \in A - \{0\}$.

Exemplo 2. Sejam $f(x) = 5x^2 + 4x + 8$ e $g(x) = 8x^2 + 9$ com $f(x), g(x) \in \mathbb{R}[x]$, então

$$(f + g)(x) = 13x^2 + 4x + 17$$

e

$$(f \cdot g)(x) = 40x^4 + 32x^3 + 109x^2 + 36x + 72.$$

Logo

1. $\text{gr}(f) = 2, \text{gr}(g) = 2, \text{gr}(f + g) = 2, \text{gr}(f \cdot g) = 4$;
2. $\text{tl}(f) = 5x^2, \text{tl}(g) = 8x^2, \text{tl}(f + g) = 13x^2, \text{tl}(f \cdot g) = 40x^4$
3. $\text{cl}(f)= 5, \text{cl}(g) = 8, \text{cl}(f + g) = 13, \text{cl}(f \cdot g) = 40$;
4. $\text{ml}(f) = x^2, \text{ml}(g) = x^2, \text{ml}(f + g) = x^2, \text{ml}(f \cdot g) = x^4$
5. $\mathbb{M}(f) = \{x^2, x, 1\}, \mathbb{M}(g) = \{x^2, 1\}, \mathbb{M}(f+g) = \{x^2, x, 1\}, \mathbb{M}(f\cdot g) = \{x^4, x^3, x^2, x, 1\}$.

Proposição 1. Sejam $f(x)$ e $g(x)$ dois polinômios não nulos em $A[x]$ onde $\text{gr}(f) = m$ e $\text{gr}(g) = n$. Então, $\text{gr}(f + g) \leq \max\{\text{gr}(f), \text{gr}(g)\}$ e $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.

Demonstração. Considere $f(x) = \sum_{i=0}^{m} a_i x^i$ e $g(x) = \sum_{j=0}^{n} b_j x^j$. Sem perda de generalidade, suponha $m > n$, assim, temos que $f(x) + g(x) = \sum_{i=0}^{m} c_i x^i$, onde $c_i = a_i + bi$, ou seja, $c_m = a_m + b_m$ e como $\text{gr}(g) = n < m$ temos que $c_m = a_m + 0 = a_m$, e portanto $\text{gr}(f + g) = m = \max\{\text{gr}(f), \text{gr}(g)\}$. Por outro lado, se $m = n$ pode acontecer que $c_m = a_m + b_m = 0$, ou seja, $a_m = -b_m$ e portanto $\text{gr}(f + g) \leq \max\{\text{gr}(f), \text{gr}(g)\}$. Agora, $f(x) \cdot g(x) = \sum_{i=0}^{m+n} c_i x^i$ onde $c_{m+n} = a_m b_n \neq 0$, ou seja, $(f \cdot g)(x) = a_m b_n x^{m+n} + f_0(x)$ onde $\text{gr}(f_0) < m + n$ e além disso $c_k = 0$ para todo $k > m + n$, o que mostra a igualdade $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$. □

Vamos convencionar que $\text{gr}(0) = -\infty$ e que para cada $f(x) \in A[x]$ não nulo, temos que $\text{ml}(f) = \frac{\text{tl}(f)}{\text{cl}(f)}$.

Definição 7. Seja $A[x]$ um anel e $f(x) \in A[x] - \{0\}$. Dizemos que $\alpha \in A$ é raiz de $f(x)$ se $f(\alpha) = 0$.

Exemplo 3. Seja $f(x) \in \mathbb{Q}[x]$ tal que $f(x) = 7x^2 - 4x + \frac{1}{4}$. Então f tem como raízes os números racionais $\frac{1}{2}$ e $\frac{1}{14}$ são raízes de $f(x)$, já que $f\left(\frac{1}{2}\right) = f\left(\frac{1}{14}\right) = 0$.

Observação 3. Seja A um anel. Em alguns casos, podemos encontrar um polinômio em $A[x]$ que não possui raízes em A, mas sim em uma extensão de A. Por exemplo, o polinômio $p(x) = x^2 + 1 \in \mathbb{R}[x]$ não possui raízes reais, mas tem como raízes os números complexos i e $-i$, que pertencem a $\mathbb{C}$. Nessas condições, dizemos que i e $-i$ são algébricos sobre $\mathbb{R}$, pois são raízes de um polinômio com coeficientes reais.

2.2 ALGORITMO DA DIVISÃO EM $K[x]$

A partir deste ponto, consideraremos o anel A como sendo um corpo K, com as operações habituais de soma e multiplicação. Toda a teoria que será abordada estará centrada na seguinte questão: em que condição um polinômio não nulo de $K[x]$ divide outro polinômio?

Definição 8. Sejam $f(x)$ e $g(x)$ dois polinômios em $K[x]$, dizemos que o polinômio $f(x)$ *divide* o polinômio $g(x)$, se existir $q(x) \in K[x]$ tal que

$$g(x) = f(x) \cdot q(x)$$

Teorema 2 (Algoritmo da divisão em $K[x]$)**.** Sejam $f(x), g(x) \in K[x]$ e $g(x) \neq 0$. Então existem únicos $q(x), r(x) \in K[x]$ tais que

$$f(x) = q(x) \cdot g(x) + r(x) \tag{2}$$

onde $r(x) = 0$ ou $\text{gr}(r) < \text{gr}(g)$.

Demonstração. Primeiro, vamos mostrar que vale a equação (2). Para isso, sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$. Se $f(x) = 0$, basta tomar $q(x) = r(x) = 0$. Suponha então $f(x) \neq 0$, com $\text{gr}(f) = n$. Caso $n < m$, basta tomar $q(x) = 0$ e $r(x) = f(x)$. Assim, podemos assumir $n \geqslant m$.

Seja $f_1(x)$ o polinômio definido por:

$$f_1(x) = f(x) - a_nb_m^{-1}x^{n-m} \cdot g(x) \tag{3}$$

organizando os termos e fazendo a distributividade de $g(x)$ em (3) temos

$$f(x) = a_nb_m^{-1}b_0x^{n-m} + a_nb_m^{-1}b_1x^{n-m+1} + \cdots + a_nx^n + f_1(x)$$

como o $\text{gr}(f) = n$, que por sua vez tem como coeficiente líder a_n então temos que $\text{gr}(f_1) < \text{gr}(f)$. Vamos aplicar o segundo princípio de indução sobre o $\text{gr}(f) = n$ para demonstrar o teorema.

Se $n = 0$, como $n \geq m$ então $m = 0$, logo $f(x) = a_0 \neq 0, g(x) = b_0 \neq 0$ e temos que $f(x) = a_0b_0^{-1} \cdot g(x)$, basta tomar $q(x) = a_0b_0^{-1}$ e $r(x) = 0$, teremos $f(x) = a_0b_0^{-1} \cdot b_0 = a_0$. Temos então o primeiro passo de indução. Onde $\text{gr}(f_1) < \text{gr}(f) = n$, podemos então aplicar a hipótese de indução em $f_1(x)$. Ou seja, existem $q_1(x), r_1(x)$, tais que:

$$f_1(x) = q_1(x)g(x) + r_1(x) \tag{4}$$

em que $r_1(x) = 0$ ou $\text{gr}(r_1) < \text{gr}(g)$. Vamos escrever a equação (3) da seguinte forma

$$f_1(x) = a_nb_m^{-1}x^{n-m} \cdot g(x) + f_1(x). \tag{5}$$

Substituindo $f_1(x)$ da equação (4) na equação (5) obtemos a equação

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + [q_1(x)g(x) + r_1(x)] \tag{6}$$

colocando $g(x)$ em evidência e organizando os termos da equação (6), obtemos

$$f(x) = [q_1(x) + a_n b_m^{-1} x^{n-m}]g(x) + r_1(x)$$

quando tomamos $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r_1(x) = r(x)$, temos que

$$f(x) = q(x)g(x) + r(x)$$

onde $r(x) = 0$ ou $\text{gr}(r) < \text{gr}(g)$. Assim, está provada a equação (2). A seguir, vamos mostrar que $q(x)$ e $r(x)$ são unicamente determinados.

Sejam $q_1(x), q_2(x), r_1(x)$ e $r_2(x)$ tais que:

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x) \tag{7}$$

onde $r_i(x) = 0$ ou $\text{gr}(r_i) < \text{gr}(g), i \in \{1, 2\}$. Note que na equação (7) podemos organizar os termos e chegar em

$$[q_1(x) - q_2(x)]g(x) = r_2(x) - r_1(x), \tag{8}$$

mas se $q_1(x) \neq q_2(x)$ observamos em (8) que o grau do polinômio $[q_1(x) - q_2(x)]g(x)$ é maior do que, ou igual ao grau de g. Ainda em (8), temos que $\text{gr}(r_1 - r_2) < \text{gr}(g)$ já que $\text{gr}(r_1), \text{gr}(r_2) < \text{gr}(g)$. O que gera um absurdo. Logo, $q_1(x) = q_2(x)$ portanto

$$r_1(x) = f(x) - q_1(x)g(x) = f(x) - q_2(x)g(x) = r_2(x) \tag{9}$$

concluímos por transitividade na equação (9) que $r_1(x) = r_2(x)$. Assim, está provado o teorema do algoritmo da divisão para polinômios em $K[x]$.

□

Exemplo 4. Considere o polinômio $f(x) = x^3 + 3x^2 + x$ e $g(x) = x^2 + 2$ em $A[x]$. Vamos fazer a divisão de $f(x)$ por $g(x)$ de acordo com o Teorema 2

$$\begin{array}{rr|l} x^3 & +3x^2+x & x^2+2 \\ \cline{3-3} -x^3 & -2x & q(x) = x+3 \\ \cline{1-2} 3x^2 & -x & \\ -3x^2 & -6 & \\ \cline{1-2} r(x) = -x & -6 & \end{array}$$

assim, podemos escrever $f(x)$ como no **Teorema 2**.

$$f(x) = x^3 + 3x^2 + x = \underbrace{(x^2+2)}_{g(x)} \cdot \underbrace{(x+3)}_{q(x)} + \underbrace{(-x-6)}_{r(x)}.$$

Definição 9. Seja A um anel, e $A[x]$ o anel dos polinômios com coeficientes em A. Um ideal $J \subseteq A[x]$ é dito *ideal principal* se existe um polinômio $p(x) \in A[x]$ tal que:

$$J = \langle p(x) \rangle = \{f(x) \cdot p(x); f(x) \in A[x]\}.$$

Exemplo 5. Seja $K = \mathbb{Q}$, o corpo dos números racionais. Considere o polinômio $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. O conjunto $I = \langle f(x) \rangle = \{g(x) \cdot (x^2 + 1) \mid g(x) \in \mathbb{Q}[x]\}$ é um ideal principal de $\mathbb{Q}[x]$, gerado por $f(x)$. Note que $x^5 + x^3 + x^2 + 1 \in I$, já que podemos escreve-lo como $(x^3 + 1)(x^2 + 1)$.

Definição 10. Um *domínio de ideais principais* é um domínio de integridade D tal que todo ideal de D é gerado por um único elemento. Geralmente dizemos que D é DIP.

Teorema 3 ($K[x]$ é Domínio de Ideal Principal)**.** Seja K um corpo. Então, todo ideal de $K[x]$ é principal.

Demonstração. Seja J um ideal de $K[x]$. Se $J = \{0\}$, então J é gerado por 0. Suponha então que $J \neq \{0\}$ e escolhemos $p(x)$ em J tal que $p(x) \neq 0$ e $\text{gr}(p) = n$. Pelo princípio da boa ordem, vamos considerar n o menor grau possível. Se $p(x) = a$ constante diferente de 0 então $1 = a \cdot a^{-1} \in J$ e assim segue imediatamente que $J = K[x]$ é gerado por 1.

Suponha agora que $\text{gr}(p) > 0$. Como $p(x) \in J$, temos que $K[x] \cdot p(x) \subseteq J$. Agora, vamos provar a inclusão contrária, ou seja, $J \subseteq K[x] \cdot p(x)$ e isso demonstrará o teorema, pois mostraremos que J será gerado por $p(x)$.

De fato, seja $f(x) \in J$ pelo **Teorema 2** temos que existem $q(x), r(x) \in K[x]$ tais que

$$f(x) = q(x)p(x) + r(x)$$

onde $r(x) = 0$ ou $\text{gr}(r) < \text{gr}(p)$. Agora, como $f(x), p(x) \in J$ segue que

$$r(x) = f(x) - q(x)p(x) \in J$$

e pela minimalidade de nossa escolha para $p(x) \in J$ segue que $r(x) = 0$ e portanto, temos

$$f(x) = q(x)p(x) \in K[x] \cdot p(x)$$

como queríamos. □

Definição 11. Seja $f(x) \in K[x]$ tal que $\text{gr}(f) \geq 1$. Dizemos que $f(x)$ é um polinômio *irredutível* sobre o corpo K se toda vez que $f(x) = g(x) \cdot h(x)$, onde $g(x), h(x) \in K[x]$ tivermos $g(x) = a$ constante em K ou $h(x) = b$ constante em K. Se f for não irredutível sobre K, diremos que $f(x)$ é *redutível* sobre K.

Exemplo 6. O polinômio $f(x) = x^2 + 1$ é irredutível sobre $\mathbb{R}$. De fato, se pudéssemos escrevê-lo como $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{R}[x]$, então um dos fatores deveria ser constante, pois $f(x)$ não possui raízes reais. Por outro lado, $f(x)$ é redutível sobre $\mathbb{C}$, já que nos complexos podemos escrever $f(x) = (x - i)(x + i)$.

Definição 12. Um domínio D é um domínio de fatoração única (DFU) se:

1. *Todo elemento de D não nulo e não unidade pode ser escrito como um produto de irredutíveis de D*
2. *A fatoração em irredutíveis é unica a menos de associados e da ordem em que aparecem.*

Teorema 4. Seja K um corpo. Então, todo polinômio $f(x) \in K[x] - \{0\}$ pode ser escrito na forma

$$f(x) = u \cdot p_1(x) \cdots p_m(x)$$

onde $u \in K - \{0\}$ e $p_1(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre K. (Não necessariamente distintos). Mais ainda, essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), \ldots, p_m(x)$.

Demonstração. Seja $f(x) \in K[x] - \{0\}$. Vamos provar por indução sobre o $\text{gr}(f) = n$.

Se $n = 0$, então $f(x) = u$ constante não nula. Assim, podemos assumir $\text{gr}(f) = n$ onde $n \geq 1$. Vamos supor pela hipótese do segundo princípio de indução que todo polinômio não nulo de grau menor que n pode ser escrito na expressão desejada, e vamos demonstrar que $f(x)$ também pode ser escrito de tal forma.

Suponha, por absurdo, que $f(x)$ não possa ser escrito como produto de irredutíveis. Então, $f(x)$ é um polinômio redutível sobre K. Logo, pelo **Teorema 2** existem $g(x), h(x) \in K[x]$ onde $1 \leq \text{gr}(g) < n, 1 \leq \text{gr}(h) < n$ tais que

$$f(x) = g(x)h(x). \tag{10}$$

Aplicando a hipótese de indução sobre $g(x)$ e $h(x)$

$$g(x) = ap_1(x) \cdots p_r(x) \tag{11}$$

onde $a \in K - \{0\}$ e $p_1(x), \ldots, p_r(x)$ são polinômios irredutíveis sobre K, e analogamente

$$h(x) = bp_{r+1}(x) \cdots p_m(x) \tag{12}$$

onde $b \in K - \{0\}$ e $p_{r+1}(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre K. Substituindo as equações (11) e (12) na equação (10). Ficamos com

$$f(x) = ap_1(x) \cdots p_r(x) \cdot bp_{r+1}(x) \cdots p_m(x) \tag{13}$$

em que $u = ab \in K - \{0\}$ e $p_1(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre K. Vamos agora demonstrar a unicidade da expressão. Suponha então que

$$f(x) = up_1(x) \cdots p_m(x) = u'p'_1(x) \cdots p'_s(x) \tag{14}$$

onde $u, u' \in K - \{0\}$ e $p_1(x), \ldots, p_m(x), p'_1(x), \ldots, p'_s(x)$ são polinômios irredutíveis sobre K. Observe que na equação (14) temos que $p_1(x)$ é fator do lado esquerdo, que por sua vez é igual ao lado direito, então

$$p_1(x) | p'_1(x) \cdots p'_s(x)$$

sabemos que todo elemento irredutível em um domínio é um elemento primo. Por isso, existe $u_i' \in K - \{0\}$ tal que $p_i'(x) = u_i' \cdot p_1(x)$, nesse caso, dizemos que $p_i'(x)$ e $p_1(x)$ são associados em $K[x]$. Agora o teorema segue por indução sobre m.

Se $m = 1$ e $p_1(x)$ é irredutível temos que necessariamente $s = 1$ onde $p_1(x)$ e $p_i'(x)$ são associados em $K[x]$. Suponha então que $m > 1$, $p_i'(x) = u_i' p_1(x)$ e sendo $K[x]$ um domínio de integridade temos que ao cancelar $p_1(x)$ na equação (14) ficamos com

$$up_2(x) \cdots p_m(x) = uu_i' p_1'(x) \cdots p_{i-1}(x) p_{i+1}(x) \cdots p_s(x). \tag{15}$$

Ao fazer o cancelamento em (15) segue que e o grau da equação fica menor que n, daí segue pela hipótese de indução que $m = s$ e cada $p_j'(x)$ está associado com algum $p_i(x)$ através de uma constante. O que demonstra o teorema. □

2.3 ANEL DE POLINÔMIOS EM VÁRIAS VARIÁVEIS

Começamos este capítulo definindo e estendendo a noção de anel de polinômios em uma variável. Agora, vamos estudar o anel de polinômios em várias variáveis. Uma observação simples e importante é que o anel de polinômios em várias variáveis também carrega as características do anel A. Observe que, se A é um domínio de integridade, temos que o anel $A[x_1]$ é um domínio de integridade; por sua vez, usando o **Corolário 1**, o anel $(A[x_1])[x_2]$ também é domínio de integridade. Com um argumento indutivo sobre o número de variáveis, concluímos que o anel de polinômios em várias variáveis é domínio de integridade. Assim, com o processo de acrescentar as variáveis mencionado acima, podemos definir o que é um elemento do anel $K[x_1, \ldots, x_n]$.

Definição 13. Seja K um corpo. um elemento $f(x_1, \ldots, x_n)$ não nulo de $K[x_1, \ldots, x_n]$ é da forma

$$f(x_1, \ldots, x_n) = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i}$$

com $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $a_\alpha \in K$ e $J \subseteq \mathbb{N}^n$.

Exemplo 7. Seja $J = \{(1,2), (3,1)\} \subseteq \mathbb{N}^2$, $a, \in K$, então de acordo com a definição acima podemos escrever $f \in K[x_1, x_2]$ da seguinte forma

$$f(x_1, x_2) = ax_1 x_2^2 + bx_1^3 x_2.$$

Convenção: Até então, estamos tratando os elementos de $K[x]$ como $p(x)$. Buscando simplificar a notação, sempre que não houver confusão iremos denotar o polinômio $f(x_1, \ldots, x_n)$ de $K[x_1, \ldots, x_n]$ por f.

Definição 14. Um termo $K[x_1, \ldots, x_n]$ é um elemento da forma $a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i}$ onde temos que $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. O elemento $a_\alpha \in K$ do termo é chamado de *coeficiente desse*

termo e $\prod_{i=1}^{n} x_i^{\alpha_i}$ é denominado *monômio*. Chamamos de *grau(total)* do monômio $\prod_{i=1}^{n} x_i^{\alpha_i}$ o número natural dado por $\sum_{i=1}^{n} \alpha_i$, o qual denotaremos por $\mathrm{gr}\left(\prod_{i=1}^{n} x_i^{\alpha_i}\right) := \sum_{i=1}^{n} \alpha_i$.

Sejam $(k_1, \ldots, k_n) \in K^n$ e $f \in K[x_1, \ldots, x_n]$ com

$$f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i}$$

denotaremos por

$$f(k_1, \ldots, k_n) := \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} k_i^{\alpha_i} \in K.$$

Definição 15. Sejam $f \in K[x_1, \ldots, x_n]$ e $\alpha = (\alpha_1, \ldots \alpha_n) \in K^n$, diremos que α é um *zero* de f se $f(\alpha_1, \ldots, \alpha_n) = 0$.

Se $f \in K[x_1, \ldots, x_n]$ é não nulo, vamos denotar por

$$\mathbb{M}_n(f) = \left\{ \prod_{i=1}^{n} x_i^{\alpha i} : a_\alpha \neq 0 \right\}$$

o conjunto de todos os monômios de f e chamaremos

$$\mathrm{gr}(f) = \max \left\{ \sum_{i=1}^{n} \alpha_i; \prod_{i=1}^{n} x_i^{\alpha_i} \in \mathbb{M}_n(f) \right\}$$

o grau total de f.

Definição 16. Sejam $f, g \in K[x_1, \ldots, x_n]$. Podemos definir as operações de soma $K[x_1, \ldots, x_n]$

$$\begin{array}{rccc} + : & K[x_1, \ldots, x_n] \times K[x_1, \ldots, x_n] & \longrightarrow & K[x_1, \ldots, x_n] \\ & (f, g) & \longmapsto & \sum_{\gamma \in J \cup L} (a_\gamma + b_\gamma) \prod_{i=1}^{n} x_i^{\gamma_i} \end{array}$$

e o produto

$$\begin{array}{rccc} \cdot : & K[x_1, \ldots, x_n] \times K[x_1, \ldots, x_n] & \longrightarrow & K[x_1, \ldots, x_n] \\ & (f, g) & \longmapsto & \sum_{\beta \in L} \sum_{\alpha \in J} a_\alpha b_\beta \prod_{i,j=1}^{n+m} x_i^{\alpha_i + \beta_j} \end{array}$$

com $\alpha + \beta = \gamma$ e $J, L \subseteq \mathbb{N}^n$ finitos e $a_\alpha, b_\beta \in K$.

Como no caso de polinômios em uma indeterminada, constatamos igualmente que

$$\mathrm{gr}(f + g) \leq \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$$

e também

$$\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$$

para $f, g \in K[x_1, \ldots, x_n]$.

Exemplo 8. Considere os polinômios $f = 2x^2y + 2y^2 + x$ e $g = 3x^3 + x^2y + 2$ em $\mathbb{R}[x, y]$. Vamos calcular $gr(f + g)$ e $gr(fg)$

$$f + g = 3x^3 + 3x^2y + 2y^2 + x + 2;$$
$$fg = 6x^5y + 3x^4 + 2x^4y^2 + 6x^3y^2 + x^3y + 2x^2y^3 + 4x^2y + 2x + 4y^2$$

onde podemos observar que,

$$\text{gr}(f + g) \leq \max\{\text{gr}(f), \text{gr}(g)\} = \{3, 3\} = 3$$

e

$$\text{gr}(fg) = \text{gr}(f) + \text{gr}(g) = 3 + 3 = 6.$$

2.4 ORDENS MONOMIAIS

Nosso principal objetivo, agora, é estender a divisão de polinômios vista no anel de polinômios $K[x]$ para o conjunto $K[x_1, \ldots, x_n]$. Para isso, devemos analisar cada passo do algoritmo, a fim de resolver todos os obstáculos que podem ser encontrados.

Para dar continuidade ao nosso trabalho, precisamos determinar o termo líder de um polinômio $f \in K[x_1, \ldots, x_n]$. Isso se faz necessário, pois precisamos determinar a ordem de um polinômio em relação a outro. Além disso, precisamos generalizar o conceito de coeficiente líder.

Definição 17. O conjunto de todos os monômios de $K[x_1, \ldots, x_n]$ será denotado por

$$\mathbb{M}_n = \left\{ \prod_{i=1}^{n} x_i^{\alpha i}; \alpha_1, \ldots, \alpha_n \in \mathbb{N} \right\},$$

onde $x_1^0 \cdots x_n^0$ será denotado por 1.

Em um primeiro contato com monômios de $K[x_1, \ldots, x_n]$ é natural tentarmos utilizar a mesma estratégia de ordenar monômios usada em $K[x]$. Vejamos o seguinte exemplo.

$$x^2yz^2, x^2y^2z, x^4y, x^3y^2, y^4z, x^4z \in K[x, y, z]. \tag{16}$$

sando o conceito de grau que definimos em $K[x]$ e, até mesmo, em $K[x_1, \ldots, x_n]$, percebemos que os monômios em (16) têm o mesmo grau, o que nos deixa em dúvida sobre como ordená-los. Por conta de problemas como esse, é necessário estudarmos ordens monomiais, tendo como objetivo determinar um maior elemento entre os monômios no anel $K[x_1, \ldots, x_n]$. Para iniciar nossos estudos acerca dessas ordenações, precisamos relembrar o conceito de relação de ordem em um conjunto.

Definição 18. *(Relação de Ordem)* Uma *relação de ordem*, ou uma *ordenação*, sobre um conjunto C não vazio é uma relação $\preceq$ satisfazendo:

1. *$c \preceq c$ para todo $c \in C$ (propriedade reflexiva);*
2. *Se $c_1, c_2 \in C$ são tais que $c_1 \preceq c_2$ e $c_2 \preceq c_1$, então $c_1 = c_2$ (propriedade anti-simétrica);*
3. *Sejam $c_1, c_2, c_3 \in C$. Se $c_1 \preceq c_2$ e $c_2 \preceq c_3$, então $c_1 \preceq c_3$ (propriedade transitiva).*

Observação 4. *Se $c_1 \preceq c_2$, mas $c_1 \neq c_2$, então indicaremos $c_1 \prec c_2$.*

Definição 19. Uma relação de ordem sobre o conjunto C é *total* quando para todo $a_1, a_2 \in C$ tivermos

$$a_1 \prec a_2, a_2 \prec a_1 \text{ ou } a_1 = a_2.$$

Queremos definir uma relação sobre $\mathbb{M}_n$ que seja total, pois com ela teremos bem definido o conceito de termo líder de um elemento f em $K[x_1, \ldots, x_n]$ onde

$$f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha i} \neq 0.$$

Com efeito, podemos definir o monômio líder $\mathrm{ml}(f)$ da seguinte forma

$$\mathrm{ml}(f) = \max \left\{ \prod_{i=1}^{n} x_{i=1}^{\alpha i} \right\} \in \mathbb{M}_n(f)$$

onde o máximo é tomado com respeito à ordem $\preceq$ fixada e considerando o *termo líder* de f, isto é, $\mathrm{tl}(f) = a_\alpha \cdot \mathrm{ml}(f)$.

Proposição 2. Existe uma bijeção entre $\mathbb{M}_n$ e $\mathbb{N}^n$.

Demonstração. De fato, basta considerar a seguinte aplicação

$$\begin{array}{rccc} \beta: & \mathbb{M}_n & \longrightarrow & \mathbb{N}^n \\ & m_i & \longmapsto & \alpha(i) \end{array}$$

onde $m_i = \prod_{i=1}^{n} x_i^{\alpha_i}$ e $\alpha(i) = (\alpha_{i1}, \ldots, \alpha_{in})$. □

Definição 20. Uma *ordem monomial* $\preceq$ sobre $\mathbb{M}_n$ é uma relação de ordem total que satisfaz:

1. Se $m_1, m_2 \in \mathbb{M}_n$ são tais que $m_1 \preceq m_2$, então $m_1 m_3 \preceq m_2 m_3$ para todo $m_3 \in \mathbb{M}_n$;
2. Todo subconjunto não vazio de $\mathbb{M}_n$ admite um menor elemento com respeito à $\preceq$.

Na maioria dos casos é difícil mostrar que existe uma relação monomial por conta da segundo condição da **Definição 20**. Por isso, vamos usar o lema a seguir para nos auxiliar nessa tarefa.

Lema 1. Uma relação de ordem $\preceq$ em $K[x_1, \ldots, x_n]$ é uma relação de ordem monomial se, e somente se, qualquer sequência decrescente de monômios (com respeito à $\preceq$)

$$m_1 \succeq m_2 \succeq m_3 \succeq \cdots$$

é finita.

Demonstração. Vamos provar a contrapositiva, ou seja: a condição dois não vaale se, e somente se, houver uma sequência de monômios estritamente decrescente infinita em $K[x_1, \ldots, x_n]$.

Se não vale a condição 2, então existe um subconjunto $S \subseteq K[x_1, \ldots, x_n]$ que não possui um menor elemento. Agora, tomemos $m_1 \in S$, e como m_1 não é o menor elemento, podemos encontrar $m_1 \succ m_2 \in S$. Deste modo, como $m_2 \in S$, então também não é o menor elemento, logo existe $m_2 \succ m_3 \in S$. Continuando dessa mesma forma, obtemos uma sequência estritamente decrescente infinita

$$m_1 \succ m_2 \succ m_3 \succ \cdots .$$

Por outro lado, seja $m_1 \succ m_2 \succ m_3 \succ \cdots$ uma sequência infinita e decrescente de elementos de $\mathbb{M}_n$. Se considerarmos $S = \{m_1, m_2, m_3, \ldots\} \neq \varnothing$, temos que o conjunto S não possui um menor elemento. O que prova o lema. □

Definição 21. *(Ordem lexicográfica $\preceq_L$)* Dados dois monômios $\prod_{i=1}^{n} x_i^{\alpha i}$ e $\prod_{i=1}^{n} x_i^{\beta i} \in \mathbb{M}_n$, dizemos que

$$\prod_{i=1}^{n} x_i^{\alpha i} \preceq_L \prod_{i=1}^{n} x_i^{\beta i}$$

se $\alpha_k = \beta_k$ para todo $k \in \{1, \ldots, n\}$, isto é, $\prod_{i=1}^{n} x_i^{\alpha i} = \prod_{i=1}^{n} x_i^{\beta i}$, ou existe $i \in \{1, \ldots, n\}$ tal que $\alpha_i < \beta_i$ e $\alpha_j = \beta_j$ para todo $j < i$. As variáveis $x_1, \ldots, x_n$ são ordenadas na forma lexicográfica, isso é $x_1 \succeq_L x_2 \succeq_L \cdots \succeq_L x_n$.

Observação 5. Com a **Definição 21** e o uso da bijeção na **Proposição 2** temos que

$$(1, 0, \ldots, 0) \succeq_L (0, 1, 0, \ldots, 0) \succeq_L \cdots \succeq_L (0, \ldots, 0, 1).$$

Usamos a mesma ordem do dicionário, ou seja, determinamos o termo líder pela posição da variável. Vejamos o exemplo a seguir

Exemplo 9. Considere os monômios $x^4, x^3y^{1000}z$, note que

$$x^3y^{1000}z \preceq_L x^4.$$

Note que por maior que seja o expoente da variável y, ela não tem importância desde que o valor do expoente da variável x do outro monômio seja maior.

Uma outra forma de observar a ordenação de $x^4, x^3y^{1000}z$ é usando a **Proposição 2** onde notamos que $\alpha = (3, 1000, 1) \preceq_L \beta = (4, 0, 0)$

Proposição 3. A ordem Lexicográfica em $K[x_1, \ldots, x_n]$ é uma ordem monomial.

Demonstração. Considere $m_1, m_2 \in \mathbb{M}_n$ tal que

$$m_1 = \prod_{i=1}^{n} x_i^{\alpha_i}, m_2 = \prod_{i=1}^{n} x_i^{\beta_i} \in \mathbb{M}_n.$$

Nosso objetivo é mostrar que $\preceq_L$ é uma ordem monomial. Para isso, vamos iniciar mostrando as condições de ordem da **Definição 18** e posteriormente fazer o uso do **Lema 1**.

Veja que $\preceq_L$ tem a propriedade reflexiva sobre $\mathbb{M}_n$, pois $m_1 = m_1$. Assim,

$$\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\alpha_i}.$$

Além disso, dados dois monômios tais que

$$\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\beta_i} \text{ e } \prod_{i=1}^{n} x_i^{\beta_i} \preceq_L \prod_{i=1}^{n} x_i^{\alpha_i}. \tag{17}$$

Então,

$$\prod_{i=1}^{n} x_i^{\alpha_i} = \prod_{i=1}^{n} x_i^{\beta_i}. \tag{18}$$

De fato, suponha que os monômios em (18) sejam diferentes, ou seja, existe pelo menos um índice onde os expoentes são distintos. Seja j o menor índice onde isso ocorre, caso $\alpha_j < \beta_j$, então temos

$$\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\beta_i},$$

mas não poderíamos ter ao mesmo tempo

$$\prod_{i=1}^{n} x_i^{\beta_i} \preceq_L \prod_{i=1}^{n} x_i^{\alpha_i},$$

o que contradiz a hipótese na equação (17). Analogamente, se $\beta_j < \alpha_j$, teríamos

$$\prod_{i=1}^{n} x_i^{\beta_i} \preceq_L \prod_{i=1}^{n} x_i^{\alpha_i},$$

mas não poderíamos ter ao mesmo tempo

$$\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\beta_i},$$

o que também contradiz a hipótese. Portanto, a única possibilidade é que os expoentes sejam iguais. Ou seja, garantimos a iguadade em (18) e $\preceq_L$ é anti-simétrica. Agora suponha que

$$\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\beta_i} \text{ e } \prod_{i=1}^{n} x_i^{\beta_i} \preceq_L \prod_{i=1}^{n} x_i^{\gamma_i}. \tag{19}$$

Se em algum dos casos ocorre a igualdade, obtemos o resultado de imediato

$$\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\gamma_i}.$$

Assumindo que nenhuma igualdade ocorra em (19), existem $i, k \in \{1, .., n\}$ tais que

$$\alpha_i < \beta_i \text{ e } \alpha_j = \beta_j \text{ para todo } j < i$$

e

$$\beta_k < \gamma_k \text{ e } \beta_l = \gamma_l \text{ para todo } l < k.$$

Se $i = k$, então $\alpha_i < \beta_i < \gamma_i$ e $\alpha_j = \beta_j$ para todo $j < i = k$ e $\beta_l = \gamma_l$ para todo $l < k$ como $j < k$ segue que $\beta_j = \gamma_j$. Logo, $\alpha_j = \gamma_j$ para todo $j < i$.

Se $i < k$ temos que $\alpha_j = \beta_j = \gamma_j$ para $j < i$, pois $\beta_l = \gamma_l$ para todo $l < k$, em particular $l = i$. No índice i, temos que $\alpha_i < \beta_i = \gamma_i$, isso ocorre porque $i < k$, os expoentes de β e γ coincidem até o índice k, ou seja, $\beta_i = \gamma_i$.

Se $k < i$, para $l < k$ por definição temos que $\beta_l = \gamma_l$ e como $\alpha_j = \beta_j$ para todo $j < i$, onde $k < i$, temos $\alpha_l = \beta_l = \gamma_l$ para todo $l < k$. Observando a definição, no índice k sabemos que $\beta_k < \gamma_k$ e como $k < i, \alpha_k = \beta_k$. Logo, $\alpha_k = \beta_k < \gamma_k$. Concluímos garantindo que qualquer uma dessas possibilidades nos permite encontrar

$$\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\gamma_i}$$

e portanto, $\preceq_L$ é transitiva.

Se $m_1 \preceq_L m_2$, então $\alpha_{k \preceq_L \beta_k}$, ou seja, $\alpha_{k-\beta_k>0}$, onde k é a posição da primeira coordenada não nula de $m_1 - m_2$. Note que dado $\gamma \in \mathbb{N}^n, (\alpha + \gamma) - (\beta + \gamma) = \alpha - \gamma$. Assim, a primeira coordenada não nula é novamente $\alpha_{k-\beta_k>0}$.

Por último, vamos fazer o uso do **Lema 1** para mostrar que a ordem lexográfica é uma ordem monomial. Suponha então que $\preceq_L$ não seja ordem monomial. Pelo **Lema 1** haverá uma sequência estritamente decrescente infinita

$$m_1 \succ_L m_2 \succ_L m_3 \succ_L \cdots$$

de elementos em $\mathbb{M}_n$. Vamos mostrar que isso nos leva a uma contradição.

Considere $m_i = \prod_{i=0}^{n} x_i^{\alpha_i}$ usando a **Proposição** 2 sabemos que $\alpha(i) = (\alpha_{i1}, \ldots, \alpha_{in})$ é um vetor em $\mathbb{Z}^n_{\geq}$. Pela de **Definição 21**, estas coordenadas formam uma sequência não crescente de números inteiros não negativos, portanto devem se estabilizar. Assim, existe um k tal que a primeira coordenada de todos os $\alpha(i)$ com $i \geq k$ é igual.

A partir de $\alpha(k)$, as segundas coordenadas determinam a ordem lexicográfica e, pelo mesmo motivo apresentado acima, formam uma sequência não crescente de números inteiros não negativos e, portanto, devem também estabilizar. Continuando esse processo, que para algum $l, \alpha(l), \alpha(l+1), \ldots$, são todos iguais, que é um absurdo pois $\alpha(l) \succ_L \alpha(l+1)$. Isto é, $m_l \succ_L m_{l+1}$. □

Definição 22. *(Ordem Reversa $\preceq_R$)* Dados dois monômios $\prod_{i=1}^{n} x_i^{\alpha i}$ e $\prod_{i=1}^{n} x_i^{\beta i} \in \mathbb{M}_n$, dizemos que

$$\prod_{i=1}^{n} x_i^{\beta i} \preceq_R \prod_{i=1}^{n} x_i^{\alpha i}$$

se $\alpha_k = \beta_k$ para todo $k \in \{1, \ldots, n\}$, isto é $\prod_{i=1}^{n} x_i^{\alpha i} = \prod_{i=1}^{n} x_i^{\beta i}$, ou existe $i \in \{1, \ldots, n\}$ tal que $\beta_i < \alpha_i$ e $\beta_j = \alpha_j$ para todo $j > i$. As variáveis $x_1, \ldots, x_n$ são ordenadas na forma reversa, ou seja, $x_n \succeq_R x_{n-1} \succeq_R \cdots \succeq_R x_1$.

No caso da ordem reversa, usaremos a ordem reversa do dicionário, ou seja, determinaremos o termo líder pela posição da variável de "z"até "a". Vejamos o seguinte exemplo.

Exemplo 10. Considere os monômios $x^{17}y^{11}, x^{1978}y^2$, note que

$$y^2x^{1978} \preceq_R y^{11}x^{17}.$$

Por maior que seja o expoente da variável x, ela não tem importância, desde que o valor da variável y do outro monômio seja maior. Outro ponto é que, com a definição de ordem reversa, comparamos os monômios de forma "contrária"à ordem lexicográfica.

Corolário 2. A ordem Reversa é uma ordem monomial.

A prova para mostrar que a ordem reversa é uma ordem monomial é análoga à da ordem lexicográficas. As propriedades fundamentais usadas na prova permanecem válidas, apenas mudando a regra de comparação entre monômios.

Definição 23. *(Ordem lexicográfica graduada $\preceq_{LG}$)* Dados dois $\prod_{i=1}^{n} x_i^{\alpha i}$ e $\prod_{i=1}^{n} x_i^{\beta i} \in \mathbb{M}_n$, dizemos que

$$\prod_{i=1}^{n} x_i^{\alpha i} \preceq_{LG} \prod_{i=1}^{n} x_i^{\beta i}$$

se

1. $\operatorname{gr}\left(\prod_{i=1}^{n} x_i^{\alpha i}\right) < \operatorname{gr}\left(\prod_{i=1}^{n} x_i^{\beta i}\right)$ ou;
2. $\operatorname{gr}\left(\prod_{i=1}^{n} x_i^{\alpha i}\right) = \operatorname{gr}\left(\prod_{i=1}^{n} x_i^{\beta i}\right)$ e existe $k \in \{1, \ldots, n\}$ tal que $\alpha_k < \beta_k$ e $\alpha_j = \beta_j$ para todo $j < k$.

Exemplo 11. Considere os monômios $x^4, x^3y^{1000}z$, note que

$$x^4 \preceq_{LG} x^3y^{1000}z$$

veja agora que o valor da variável x não é relevante, tendo em vista que o grau total do monômio $x^3y^{1000}z$ é 1004, enquanto o grau do polinômio x^4 tem seu grau igual a 4. Desta forma, uma vez que $1004 > 4$. Logo, $x^4 \preceq_{LG} x^3y^{1000}z$.

Exemplo 12. Observe que, de acordo com a **Definição 23**, quando o grau entre os monômios é o mesmo, iremos recorrer à ordem lexicográfica como critério de ordenação. Vejamos o seguinte caso:

$$x^4y^3z \succeq_{LG} x^3y^4z$$

Ambos os monômios têm grau igual a 8, mas, de acordo com a ordem lexicográfica, $x^4 \succeq_L x^3$, o que justifica a ordenação acima.

Como podemos perceber, as ordens dos monômios é distinta de acordo com a ordenação que definimos para fazer a comparação. Observe o seguinte exemplo, onde são feitas as ordenações considerando a ordem lexicográfica, reversa e lexicográfica graduada.

Exemplo 13. Considere os monômios

$$x^3yz, x^4y^4, y^4z^2, x^8, x^5y^2z^4, x^2y^3z^2 \in K[x, y, z]$$

Vamos fazer a ordenação dos monômios considerando as definições acima.

$$y^4z^2 \preceq_L x^2y^3z^2 \preceq_L x^3yz \preceq_L x^4y^4 \preceq_L x^5y^2z^4 \preceq_L x^8;$$
$$x^8 \preceq_R y^4x^4 \preceq_R zyx^3 \preceq_R z^2y^3x^2 \preceq_R z^2y^4 \preceq_R z^4y^2x^5;$$
$$x^3yz \preceq_{LG} y^4z^2 \preceq_{LG} x^2y^3z^2 \preceq_{LG} x^4y^4 \preceq_{LG} x^8 \preceq_{LG} x^5y^2z^4.$$

Até então, observamos que o grau total de um monômio é uma característica importante para que possamos estabelecer uma ordem graduada. Também constatamos o quanto uma ordem monomial é relevante para a continuidade do nosso estudo acerca dos polinômios em várias variáveis. A seguir, vamos definir o conceito de *multigrau*, que, posteriormente, será muito útil nas aplicações de uma base de Gröbner.

Definição 24. Seja $\preceq$ uma ordem monomial qualquer e seja $f \in K[x_1, \ldots, x_n]$ um polinômio. Suponha que o termo líder de f, com respeito à ordem $\preceq$, seja dado por

$$\mathrm{ml}(f) = a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} = a_\alpha x^\alpha,$$

com $a_\alpha \neq 0$ e $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Chamamos o vetor α de *multigrau* de f, denotado por $\mathrm{multigrau}(f) = \alpha$.

Exemplo 14. Considere o polinômio $f = 4xy^2z+4z^2-5x^3+7x^2z^2 \in \mathbb{R}[x,y,z]$, de acordo com a ordem lexicográfica, temos que multigrau$(f) = (3,0,0)$, em relação a ordem reversa multigrau$(f) = (2,0,2)$ e usando a ordem lexicográfica graduada multigrau$(f) = (2,2,0)$.

Observação 6. Geralmente, quando queremos nos referir ao multigrau de um polinômio $f \in K[x_1,\ldots,x_n]$ iremos usar a notação $\text{ml}(f) = x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ como $\text{ml}(f) = X^{\alpha}$ onde $\alpha = (\alpha_1,\alpha_2,\ldots,\alpha_n)$, ou seja, multigrau$(f) = (\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Proposição 4. Sejam $f, g \in K[x_1,\ldots,x_n]$ polinômios não-nulos. Então,

1. multigrau$(f\cdot g)$ = multigrau(f) + multigrau(g);
2. Se $f+g \neq 0$, então multigrau$(f+g) \leq \max\{\text{multigrau}(f), \text{multigrau}(g)\}$.

Além disso, se multigrau$(f) \neq$ multigrau(g) então

$$\text{multigrau}(f+g) = \max\{\text{multigrau}(f), \text{multigrau}(g)\}.$$

Demonstração. Suponha, sem perda de generalidade que multigrau$(f) = (\alpha_1,\ldots,\alpha_n)$ e multigrau$(g) = (\beta_1,\ldots,\beta_m)$. Note que

$$\begin{aligned} f\cdot g &= \left(\sum_{\alpha\in\mathbb{N}^n} a_i \prod_{i=1}^{n} x_i^{\alpha_i}\right)\cdot\left(\sum_{\beta\in\mathbb{N}^n} b_i \prod_{i=1}^{m} x_i^{\beta_i}\right) \\ &= \sum_{\alpha\in\mathbb{N}^n}^{n}\sum_{\beta\in\mathbb{N}^n}^{m} a_ib_j \prod^{m+n} x_i^{\alpha_i+\beta_j} \\ &= a_1b_1 \prod_{i=j=1}^{m+n} x^{\alpha_1+\beta_1} + \sum_{i=2}^{n} a_ib_1 \prod_{i=2}^{n} x^{\alpha_i+\beta_j} + \sum_{i=1}^{n}\sum_{j=2}^{m} a_ib_j \prod_{i=1}^{m+n} x^{\alpha_i+\beta_j}. \end{aligned}$$

Como $\alpha_1+\beta_1 > \alpha_i+\beta_j$ para todo $1 \leq i \leq n, 1 \leq j \leq m$ e $a_1b_1 \neq 0$, já que K é corpo então

$$\text{multigrau}(f\cdot g) = \text{multigrau}(f) + \text{multigrau}(g).$$

Se f e g são polinômios tais que $f+g \neq 0$, então multigrau$(f+g)$ está definido. Suponha que multigrau$(f) \neq$ multigrau(g). Nesse caso

$$f+g = \sum_{\alpha\in\mathbb{N}^n}^{n} a_\alpha \prod_{i=1}^{n} x_{i=1}^{\alpha_i} + \sum_{\alpha\in\mathbb{N}^n}^{m} a_\alpha \prod_{j=1}^{m} x_{j=1}^{\beta_j}. \tag{20}$$

Como trata-se de uma soma, e multigrau$(f) \neq$ multigrau(g), então não há possibilidade de cancelamento entre os termos líderes. Nesse caso

$$\text{multigrau}(f+g) = \max\{\text{multigrau}(f), \text{multigrau}(g)\}$$

Entretanto, se multigrau$(f) =$ multigrau(g) temos que observar duas possibilidades. Primeiro,

(i) $\text{tl}(f) = -\,\text{tl}(g)$.

Nesse caso, os termos líderes se anulam e por isso

$$\text{multigrau}(f+g) < \text{multigrau}(f) = \text{multigrau}(g)$$

ou seja

$$\text{multigrau}(f+g) < \max\{\text{multigrau}(f), \text{multigrau}(g)\}$$

O outro possível caso é quando

(ii) $\text{tl}(f) \neq -\text{tl}(g)$.

Nesse caso, os termos líderes não se anulam e pela equação (20) segue que

$$\text{multigrau}(f+g) = \max\{\text{multigrau}(f), \text{multigrau}(g)\}.$$

□

Verificamos no **Exemplo 13** acima que a ordenação dos monômios está diretamente ligada à ordem que escolhemos. É pensando nisso que surge a seguinte questão: a divisão entre polinômios de mais de uma variável mudará de acordo com a ordem escolhida? Essa e outras questões podem ser respondidas com o próximo teorema. Com ele, vamos generalizar o **Teorema 2**. No caso geral, o objetivo é dividir $f \in K[x_1, \ldots, x_n]$ por $f_1, \ldots, f_s$, com $f_i \in K[x_1, \ldots, x_n]$. Veremos que isso significa expressar f na forma $f = q_1 f_1 + \cdots + q_s f_s + r$, onde os "quocientes"$q_1, \ldots, q_s$ e o resto r pertencem a $K[x_1, \ldots, x_n]$. Essa possibilidade é a maior diferença entre o algoritmo apresentado no **Teorema 2** e o próximo resultado. Entretanto, será necessário cuidado ao decidir como caracterizar o resto. É aqui que usaremos as ordens monomiais.

2.5 ALGORITMO DA DIVISÃO EM $K[x_1, ..., x_n]$

Teorema 5. *(Algoritmo da divisão em $K[x_1, \ldots, x_n]$)* Fixando uma ordem monomial $\preceq$ e dados $f, g_1, \ldots, g_s \in K[x_1, \ldots, x_n]$ com $g_i \neq 0$ para todo $i = 1, \ldots, s$, existem polinômios $q_1, \ldots, q_s, r \in K[x_1, \ldots, x_n]$ tais que

$$f = \sum_{i=1}^{s} q_i g_i + r$$

com $\text{ml}(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$, para todo $i = 1, \ldots, s$.

Demonstração. Para fazer a demonstração desse teorema, vamos estabelecer um um algoritmo, e justifica-lo posteriormente. Então, considere o algoritmo abaixo:

Entrada: $f, g_1, \ldots, g_s \in K[x_1, \ldots, x_n]$ com $g_i \neq 0$ para todo $i = 1, \ldots, s$. Defina

$$q_1 := \cdots := q_s := r = 0 \text{ e } h = f$$

enquanto $h \neq 0$ faça, se existir $i \in \{1, \ldots, s\}$ tal que $\mathrm{ml}(g_i) \mid \mathrm{ml}(h)$, então escolha o menor índice i e faça

$$q_i := q_i + \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)}; \tag{21}$$

$$h := h - \frac{\mathrm{tl}(h)}{tl(g_i)} g_1. \tag{22}$$

Caso contrário

$$r := r + \mathrm{tl}(h) \tag{23}$$

$$h := h - \mathrm{tl}(h) \tag{24}$$

Saída: $q_1, \ldots, q_s \in K[x_1, \ldots, x_n]$ tais que $f = \sum_{j=1}^{s} q_j g_j + r, \mathrm{ml}(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $i = 1, \ldots, s$.

A primeira observação que podemos fazer sobre o algoritmo acima, é que ele sempre nos fornece uma resposta independente do valor dado a h, já que estabelecemos condições que no pior caso temos $h = f$. Assim, independente do valor de entrada em um número finito de passos teremos uma saída. Podemos ter essa garantia, pois sempre vamos redefinir h de modo que seu monômio líder m_i vai satisfazer $m_i \preceq m_{i-1}$, como pode ser observado na equação (22) sendo m_{i-1} o monômio líder de h no passo anteiro.

De fato, se existir $i \in \{1, \ldots, s\}$ tal que $\mathrm{ml}(g_i) \mid \mathrm{ml}(h)$, então temos obrigatoriamente que

$$\mathrm{ml}(h) \succ \mathrm{ml}\left(h - \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} g_i\right),$$

pois por (22) temos que $m_{i-1} \succeq m_i$ onde m_{i-1} é o monômio líder do passo anterior. Caso contrário, temos que $\mathrm{ml}(h) \succ \mathrm{ml}(h - \mathrm{tl}(h))$, como podemos ver em (24). Observando o **Lema 1**, sabemos que toda sequência decrescente de monômios é finita, portanto em algum momento $h = 0$, como consequência o algoritmo finaliza.

Para entender como o algoritmo acima nos dá uma resposta adequada, devemos perceber que em cada passo do algorimo temos a igualdade

$$f = \sum_{j=1}^{s} q_j g_j + r + h. \tag{25}$$

Para confirmar, iniciaremos com $h = f, r = q_i = 0$ para todo $i = 1, \ldots, s$ e note que assim a afirmação é verdadeira.

Caso exista $i \in \{1, \ldots, s\}$ tal que $\mathrm{ml}(g_i) \mid \mathrm{ml}(h)$, então redefinimos

$$q_i \text{ por } q_i + \frac{tl(h)}{\mathrm{tl}(g_i)} \text{ e } h \text{ por } h - \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} g_i$$

como vimos nas equações (21) e (22). Assim ficamos em (25) da seguinte forma

$$\sum_{j=1, j\neq i}^{s} q_j g_j + \left(q_i + \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)}\right) g_i + r + \left(h - \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} g_i\right) \tag{26}$$

organizando e colocando em evidência os termos na equação (26), temos

$$\sum_{j=1,j\neq 1}^{s} q_j g_j + g_i \left(q_i + \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} - \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} \right) + r$$

cancelando os termos e fazendo as distributividades

$$\sum_{j=1}^{s} q_j g_j + r + h = f.$$

Caso contrário, iremos redefinir r por $r + \mathrm{tl}(h), h$ por $h - tl(h)$ e assim temos

$$\sum_{j=1}^{s} q_j g_j + (r + \mathrm{tl}(h)) + (h - tl(h))$$

ficando com

$$\sum_{j=1}^{s} q_j g_j + r + h = f.$$

Assim, a equação (25) verifica-se em todos os passos do procedimento feito. Como o algorimto finaliza com $h = 0$, após um número finito de etapas obtemos

$$f = \sum_{j=1}^{s} q_j g_j + r.$$

Perceba que pela construção do procedimento visto acima, temos $\mathrm{ml}(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $j = 1, \ldots, s$, já que se $\mathrm{ml}(g_i)|m$ para algum $i \in \{1, \ldots, s\}$ e para todo $m \in \mathbb{M}(r)$ bastava definir $r = h$ assim, continuaríamos até $h = 0$. E isso prova o teorema. □

Observação 7. Uma observação importante, é que considerando uma ordem monomial em $Z^n_{\geq}$, e dados f e $g_1, \ldots, g_s \in K[x_1, \ldots, x_n]$ usando o **Teorema 5**, ao dividir f por g_i temos que multigrau$(f) \geq$ multigrau$(q_i g_i)$ para todo $i = 1, \ldots, n$

A seguir, vamos mostrar que a ordem monomial usada é fundamental para entender como funciona a divisão de um polinômio por outro. Vejamos três exemplos onde cada um deles refere-se a uma ordem monomial e um quarto exemplo, onde mostraremos que a depender da ordem a divisão tem resultados distintos.

Exemplo 15. Considere os polinômios

$$f = xy^4 + x^4 + x^3y + y^3 \ \ e \ g = y^3 + x^2 \in \mathbb{R}[x, y].$$

Ordenando os polinômios na ordem lexicográfica em seguida fazemos a divisão de $f = x^4 + x^3y + xy^4 + y^3$ por $g = x^2 + y^3$. Usando o **Teorema 5** temos que f pode ser escrito como $f = q \cdot g + r$, assim

$$\begin{array}{rl|l} x^4 & +x^3y+xy^4+y^3 & x^2+y^3 \\ \cline{3-3} -x^4 & -x^2y^3 & x^2+xy-y^3 \\ \cline{1-2} x^3y & -x^2y^3+xy^4+y^3 & \\ -x^3y & -xy^4 & \\ \cline{1-2} -x^2y^3 & +y^3 & \\ x^2y^3 & +y^6 & \\ \cline{1-2} y^6 & +y^3 & \end{array}$$

Logo, de acordo com o **Teorema 5**

$$f = (x^2 + xy - y^3) \cdot (x^2 + y^3) + (y^6 + y^3).$$

Exemplo 16. Considere os polinômios

$$f = y^5 + x^4 + 2xy + x^3 \text{ e } g = x^2 + y \in \mathbb{R}[x, y].$$

Vamos ordená-los com a ordem Lexicográfica Graduada e calcular a divisão de $f = y^5 + x^4 + x^3 + 2xy$ por $g = x^2 + y$. Então usando o **Teorema 5**, o polinômio f pode ser escrito como $f = q \cdot g + r$, pois

$$\begin{array}{rrl|l} y^5 & +x^4 & +x^3+2xy & x^2+y \\ \cline{4-4} -x^4 & -x^2y & & x^2+x-y \\ \cline{1-3} y^5 & -x^3 & -x^2y+2xy & \\ -x^3y & -xy & & \\ \cline{1-3} y^5 & -x^2y & +xy & \\ x^2y & +y^2 & & \\ \cline{1-3} y^5 & +xy & +y^2 & \end{array}$$

Concluímos que:

$$f = (x^2 + x - y) \cdot (x^2 + y) + (y^5 + xy + y^2).$$

Exemplo 17. Considere os polinômios

$$f = y^3 + x^3 + xy^2 \text{ e } g = x + y^2 \in \mathbb{R}[x, y].$$

Vamos ordená-los com a ordem Reversa e calcular a divisão de $f = y^3 + y^2x + x^3$ por $g = y^2 + x$.

$$\begin{array}{rrl|l} y^3 & +y^2x & +x^3 & y^2+x \\ \cline{4-4} -y^3 & -xy & & y+x \\ \cline{1-3} y^2x & -yx & +x^3 & \\ -y^2x & +x^2 & & \\ \cline{1-3} -yx & +x^3y & +x^2 & \end{array}$$

então usando o **Teorema 5** f pode ser escrito como $f = q \cdot g + r$, concluímos que

$$f = (y + x) \cdot (y^2 + x) + (-yx + x^3 - x^2). \tag{27}$$

Exemplo 18. Agora, consideremos os polinômios f e g do **Exemplo 17**. Já sabemos pelo **Teorema 5** a resultante da divisão seguindo a ordem Reversa. Vejamos agora usando a ordem Lexicográfica

$$f = (x^2 - xy^2 + y^4 + y^2) \cdot (x + y^2) + (-y^6 + y^5 - y^4). \tag{28}$$

Por último, usando os mesmos polinômios do **Exemplo 17**, mas dessa vez usando a ordem Lexicográfica Graduada, teremos que

$$f = (y^3 - xy + x) \cdot (y^2 + x) + (yx^2 + x^3 - x^2) \tag{29}$$

Uma observação importante é que dividindo o polinômio $f = y^5 + x^3 + xy^2$ por $g = x + y^2 \in \mathbb{R}[x, y]$, fica claro pelas igualdades (27), (28) e (29) que a divisão dependerá exclusivamente da ordem monomial escolhida. Podemos observar isso em mais exemplos

Precismos destacar um ponto importante no **Teorema 5** envolvendo a equação (23). Note que em alguns casos precisamos mover o $\mathrm{ml}(h_i)$ para o resto da divisão para executar a divisão até o fim. Isso irá ficar claro no próximo exemplo.

Exemplo 19. Sejam $f = x^2y + xy^2 + y^2, g_1 = xy - 1$ e $g_2 = y^2 - 1$, vamos fazer a divisão de f por g_1 e g_2, respectivamente, usando a ordem lexicográfica.

$$\begin{array}{rrr|l}
x^2y & +xy^2 + y^2 & & xy - 1 \\
 & & & y^2 - 1 \\
\hline
-x^2y & +x & & q_1 = x + y \\
\hline
h_1 = xy^2 & +x & +y^2 & q_2 = 1 \\
-xy^2 & +y & & \\
\hline
h_2 = x & +y^2 & +y & \\
\hline
h_2' := y^2 & +y & & \\
-y^2 + & 1 & & \\
\hline
r = \mathrm{ml}(h_2) & +y & +1 &
\end{array}$$

note que $\mathrm{ml}(h_2) = x \nmid \mathrm{ml}(g_1) = xy$ e $\mathrm{ml}(h_2) = x \nmid \mathrm{ml}(g_2) = y^2$. Para que possamos continuar a divisão, usaremos a equação (23) do **Teorema 5** e devemos mover $\mathrm{ml}(h_2) = x$ para o resto. Assim, conseguiremos fazer a divisão e escrever

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

Exemplo 20. Considere os polinômios

$$f = xy^3 + y^2 + x^2 + y^3, g_1 = xy - x, g_2 = x + y \in \mathbb{R}[x, y].$$

Considerando a ordem lexicográfica, vamos dividir f por g_1 e g_2 de acordo com o **Teorema 5**.

$$
\begin{array}{rl|l}
x^2 & +xy^3+y^3+y^2 & \begin{array}{|l} xy-x \\ \hline x+y \end{array} \\
\hline
-x^2 & -xy & q_1 = y^2+y \\
\hline
h_1 = xy^3 & -xy+y^3+y^2 & q_2 = x \\
-xy^3 & +xy^2 & \\
\hline
h_2 = xy^2 & -xy+y^3+y^2 & \\
-xy^2 & +xy & \\
\hline
h_3 = y^3 & +y^2 &
\end{array}
$$

Observe que $\mathrm{ml}(g_1) \nmid \mathrm{ml}(h_3)$ e $\mathrm{ml}(g_2) \nmid \mathrm{ml}(h_3)$, logo $f = q_1g_1 + q_2g_2 + r$, onde $h_3 = r$, ou seja,

$$f = (y^2+y)(xy-x) + x(x+y) + (y^3+y^2).$$

Agora vamos fazer a divisão de f por g_1 e g_2 respectivamente de acordo com a ordem reversa. Observe

$$
\begin{array}{rl|l}
y^3x & +y^3+y^2+x^2 & \begin{array}{|l} yx-x \\ \hline y+x \end{array} \\
\hline
-y^3x & +y^2x & q_1 = y^2-1 \\
\hline
h_1 = y^3 & +y^2x+y^2+x^2 & q_2 = y^2+y \\
-y^3 & -y^2x & \\
\hline
h_2 = y^2 & +x^2 & \\
-y^2 & -yx & \\
\hline
h_3 = -yx & +x^2 & \\
yx & -x & \\
\hline
h_4 = x^2 & -x &
\end{array}
$$

Logo, pelo **Teorema 5**

$$f = (y^2-1)(yx-x) + (y^2+y)(y+x) + (x^2-x).$$

É importante observar que, pelo **Exemplo 20**, vimos que f pode ser escrito de diferentes maneiras usando o **Teorema 5**. Também podemos notar que a maior diferença entre os **Teoremas 2** e o **Teorema 5** é que, além de viabilizar a divisão por n divisores, o teorema não estabelece um resto unicamente determinado.

Além disso, uma característica interessante do algoritmo da divisão em $K[x]$ é a forma como ele resolve o problema de pertinência ideal. Isto é, se quisermos saber se $f \in \langle g \rangle$, basta dividir f por g. Caso $r = 0$, então $f(x) = q(x)g(x)$ e, portanto, $f \in \langle g \rangle$. Isso ocorre pela unicidade do resto no algoritmo da divisão para polinômios em $K[x]$.

Naturalmente, surge o questionamento: obtemos algo semelhante para polinômios em várias variáveis? Uma implicação é um corolário fácil do **Teorema 5**: se, após a divisão de f por $g_1, \ldots, g_n$, obtivermos um resto $r = 0$, então

$$f = q_1g_1 + \cdots + q_ng_n$$

de modo que $f \in \langle g_1, \ldots, g_n \rangle$. Assim, $r = 0$ é uma condição suficiente para pertinência ideal.

No entanto, como o exemplo a seguir mostra, ao trocarmos a ordem dos divisores, teremos uma diferença na escrita de f, o que implicará em restos que não são unicamente determinados. Isso significa que, mesmo que $f \in \langle g_1, \ldots, g_n \rangle$, ao fazer a divisão de f por $g_1, \ldots, g_n$, em um primeiro contato, podemos ter $r \neq 0$, e só ao mudar a ordem dos divisores possamos encontrar $r = 0$.

Exemplo 21. Seja $g_1 = xy + 1, g_2 = y^2 - 1 \in K[x, y]$ com respeito a ordem lexicográfica. Dividindo $f = xy^2 - x$ por g_1 e g_2 respectivamente:

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

Agora dividindo por g_2 e g_1 respectivamente:

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

O exemplo anterior mostra que $f \in \langle g_1, g_2 \rangle$, apesar de o resto da divisão de f por g_1 e g_2 ser diferente de zero.

Observamos que a escolha da ordem monomial, bem como a ordem dos divisores, influencia diretamente o resultado do resto obtido. Por essa razão, a teoria desenvolvida busca contornar tais dificuldades, isto é, saber se conseguimos um resto unicamente determinado. No próximo capítulo, veremos que as *Bases de Gröbner* possuem exatamente essas "boas" propriedades, garantindo a obtenção de um resto único. Essa característica é fundamental para o problema de pertinência a um ideal, pois, dado um conjunto de polinômios $g_1, \ldots, g_n \in K[x_1, \ldots, x_n]$ tal que $I = \langle g_1, \ldots, g_n \rangle$, será possível verificar, de forma algorítmica, se um polinômio $f \in K[x_1, \ldots, x_n]$ pertence ou não a I.

3 BASE DE GRÖBNER E SISTEMAS DE EQUAÇÕES POLINOMIAIS

Neste capítulo, daremos continuidade ao estudo iniciado nos capítulos anteriores, concentrando-nos em um tipo especial de ideal no anel de polinômios: os ideais monomiais. A partir deles, construiremos o conceito central deste trabalho: a Base de Gröbner. Essa base, introduzida por Bruno Buchberger em 1965, constitui uma ferramenta essencial na Álgebra Comutativa e na Geometria Algébrica, permitindo tratar problemas relacionados à resolução de sistemas de equações polinomiais de maneira sistemática e algorítmica.

Um dos aspectos mais importantes dessa teoria é a obtenção de um resto unicamente determinado no processo de divisão de polinômios, independentemente da ordem em que os divisores são considerados. Tal propriedade garante consistência e eficiência nos cálculos algébricos, sendo um dos pilares que fundamentam a definição e a utilidade das Bases de Gröbner.

Nosso objetivo é compreender como, a partir de um conjunto gerador de um ideal, podemos determinar uma Base de Gröbner utilizando o Algoritmo de Buchberger, além de analisar as propriedades que garantem sua unicidade e aplicabilidade.

Convenção: No nosso estudo acerca da Base de Gröbner, sempre que não houver dúvida, vamos nos referir ao monômio $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ por x^α onde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq}^n$

Definição 25. Um ideal $I \subseteq K[x_1, \ldots, x_n]$ é um *ideal monomial* quando pode ser gerado por monômios.

Exemplo 22. O ideal $I = \langle x^3 + xy^4, y^2 \rangle$ é ideal monomial. Para tanto, basta observar que $I = \langle x^3, y^2 \rangle$. Observe que tomando $f \in I$, então $f = (x^3 + xy^4)g_1 + y^2 g_2$, organizando os termos e colocando em envidência, temos que $f = x^3 g_1' + y^2 g_2'$ onde $g_1' = g_1$ e $g_2' = xy^2 g_1 + g_2$ e portanto, $I \subseteq \langle x^3, y^2 \rangle$. Reciprocamente, tome $f \in \langle x^3, y^2 \rangle$ então $f = x^3 h_1 + h_2 y^2$, escrevendo $x^3 = (x^3 + xy^4) - xy^2(y^2)$ podemos escrever $f = [(x^3 + xy^4) - xy^2(y^2)]h_1 + y^2 h_2$ assim, tomando $h_1' = h_1$ e $h_2' = -xy^2 h_1 + h_2$ temos que $f = (x^3 + xy^4)h_1' + y^2 h_2' \in I$, e portanto, segue a igualdade.

Observação 8. Se $I = \langle f_1, \ldots, f_n \rangle$, e $J = \langle g_1, \ldots, g_n \rangle$ onde $\{f_1, \ldots, f_n\} \subseteq J$ e $\{g_1, \ldots, g_n\} \subseteq I$. Então $I = J$.

Exemplo 23. Considere dois ideais monomiais $I = \langle x^2, xy \rangle$ e $J = \langle x^2, xy, x^3y^2 \rangle$ no anel $k[x, y]$. Vamos verificar que $I = J$.

Primeiramente, é claro que $I \subseteq J$, pois os geradores de I também estão em J. Agora, para mostrar que $J \subseteq I$, basta observar que o monômio extra em J, isto é, x^3y^2, pode ser escrito como:

$$x^3y^2 = x \cdot x^2 \cdot y^2 = x^2 \cdot (xy^2).$$

Como $x^2 \in I$, então $x^2 \cdot (xy^2) \in I$. Logo, $x^3y^2 \in I$, o que implica que $J \subseteq I$. Portanto, $I = J$.

Lema 2. 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. Considere que x^β é divisível por x^α, então $x^\beta = x^\alpha \cdot x^\gamma$ mas como $x^\alpha \in I$ temos que $x^\alpha \cdot x^\gamma = x^\beta \in I$. Reciprocamente, seja $x^\beta \in I = \langle x^\alpha : \alpha \in A \rangle$ então

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha_i} \tag{30}$$

onde $h_i \in K[x_1, \ldots, x_n]$ e $\alpha_i \in A$. Escrevendo cada h_i como soma de monômios, temos $h_i = \sum_{j=1}^{t_i} a_{ij} x^{\gamma_{ij}}$. Assim a equação (30) pode ser escrita como

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

Fazendo a distributibuição, os produtos e agrupando os termos semelhantes da equação acima

$$x^\beta = \sum_{k=1}^{s} a_{\gamma_k} x^{\gamma_k} \tag{31}$$

onde $a_{\gamma_k} \in K$.

Note que cada parcela do lado direito de (31) é divisível por algum x^{α_i} com $\alpha_i \in A$. Além disso, se o lado esquerdo da igualdade (31) é um monômio, então o lado direito também é. Assim, $x^\beta = \sum_{k=1}^{s} a_{\gamma_k} x^{\gamma_k}$ se, e somente se, $t = 1$ e a_{γ_1}, ou seja,

$$x^\beta = x^{\gamma_1}.$$

Como x^{α_i} divide x^{γ_1} então divide x^β, o que conclui a demonstração. □

Exemplo 24. O ideal $J = \langle x + y \rangle$ não é um ideal monomial, pois seu gerador $x + y$ não é um monômio. *Suponha, por absurdo, que $J = \langle x + y \rangle$ seja um ideal monomial. Então existe um conjunto de monômios $M = \{m_1, m_2, \ldots\}$ tal que $J = \langle m_1, m_2, \ldots \rangle$. Como $x + y \in J$, temos $x + y = \sum_i h_i m_i$, com $h_i \in K[x, y]$. Expandindo e agrupando termos, o lado direito é uma soma de monômios. Pelo* ***Lema 2****, cada monômio do lado direito é divisível por algum m_i. Como x e y são os únicos monômios em $x + y$, deve existir m_i que divide x e m_j que divide y. Assim, $x, y \in J$. Contudo, $x \notin \langle x + y \rangle$, pois não existe $f \in K[x, y]$ tal que $x = (x + y)f$. De fato, se f fosse constante, teríamos $x = c(x + y)$, o que é impossível, já que o termo em y não desaparece. Logo, obtemos uma contradição, e portanto $J = \langle x + y \rangle$ não é um ideal monomial.*

Lema 3. Seja I um ideal monomial, e seja $f \in K[x_1, \ldots, x_n]$. Então, as seguintes condições são equivalentes:

1. $f \in I$;
2. todo termo de f está em I;

3. f é uma combinação linear com coeficientes em K de monômios em I.

Demonstração. Primeiro, vamos mostrar que $3 \Rightarrow 2$. Seja $f = a_1x^{\alpha_1} + \cdots + a_nx^{\alpha_n}$ onde $a_i \in K$ e $\alpha_i \in A \subseteq \mathbb{Z}^n_{\geq 0}$ com $i = 1, \ldots, n$. Como $x^{\alpha_i} \in I$, então $a_ix^{\alpha_i} \in I$. Logo, todo termo de f está em I. Agora, mostraremos que $2 \Rightarrow 1$. Claramente, se todo termo de f está em I, que por sua vez é um ideal, então f deverá está em I.

Por último, mostraremos que $1 \Rightarrow 3$. Seja $f \in I$, então $f = \sum_{i=1}^{s} h_ix^{\alpha_i}$, com $h_i \in K[x_1, \ldots, x_n]$. Escrevendo h_i como soma de monômios e expandindo, temos:

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

assim,

$$f = a_{11}x^{\gamma_{11}}x^{\alpha_1} + \cdots + a_{1t_1}x^{\gamma_{1t_1}}x^{\alpha_1} + \cdots + a_{st_s}x^{\gamma_{st_s}}x^{\alpha_s}$$

como $x^{\gamma_{ij}}x^{\alpha_i} \in I$ para cada $i = 1, \ldots, s$ e $j = 1, \ldots, t_s$ temos que f é uma combinação linear com coeficientes em K de monômios de I. □

Corolário 3. Dois ideais monomiais são iguais se, e somente se, eles contém os mesmos monômios.

Demonstração. Se os ideais são iguais, então eles claramente contêm os mesmos monômios. Reciprocamente, se I e J são dois ideais monomiais que contêm os mesmos monômios, tomemos $f \in I$. Então, pelo **Lema 3**, f é uma combinação linear com coeficientes em K de monômios em I. Mas, como I e J contêm os mesmos monômios, f é também uma combinação linear com coeficientes em K de monômios em J. Ou seja, novamente pelo **Lema 3**, concluímos que $f \in J$. Analogamente, observamos que $J \subset I$.

□

Lema 4. *(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 um conjunto finito de geradores.

Demonstração. Provaremos por indução em n. Para o caso inicial, tome $n = 1$, então I é gerado por monômios de x_1^α, com $\alpha \in \mathbb{Z}_{\geq 0}$. Tomando β como o menor elemento de A teremos que $\beta \leq \alpha$, $\alpha \in A$ e consequentemente, pelo **Lema 2**, x_1^β divide todos os elemtentos de I, pois $x_1^\alpha = x_1^\beta x_1^k$. Logo $I = \langle x_1^\beta\rangle$. Suponha agora que $n > 1$ e que o resultado é válido 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 escritos na forma $x^\alpha y^\beta$ com $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}^{n-1}_{\geq 0}$ e $\beta \in \mathbb{Z}_{\geq 0}$.

Como $I \subset K[x_1, \ldots, x_{n-1}, y]$ é ideal monomial. Defina

$$J = \langle x^\alpha : x^\alpha y^m \in I \text{ para algum } m \in \mathbb{Z}_{\geq 0}\rangle$$

em $K[x_1, \ldots, x_{n-1}]$. Cmo J é um ideal monomial de $K[x_1, \ldots, x_{n-1}]$, aplicando a hipótese de indução J pode ser escrito como $J = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$. Por construção, para cada $1 \leq i \leq s$ existe $m_i \in \mathbb{Z}_{\geq}$ tal que $x^{\alpha_i} y^{m_i} \in I$, já que cada $x^{\alpha_i} \in J$. Defina m o maior dos m_i. Defina também mais m ideais, ou seja para cada $0 \leq k \leq m-1$, considere

$$J_k = \langle x^{\alpha} : x^{\alpha} y^k \in I \rangle$$

em $K[x_1, \ldots, x_{n-1}]$, note que pela hipótese de indução, temos que J_k possui um número finito de geradores.

Considere a seguinte afirmação: I é gerado pelos monômios da seguinte lista:

$$\begin{aligned} J: &\quad x^{\alpha_1} y^m, \ \ldots, \ x^{\alpha_{s_1}} y^m \\ J_0: &\quad x^{\alpha_1}, \ \ldots, \ x^{\alpha_{s_0}} \\ &\vdots \\ J_{m-1}: &\quad x^{\alpha_1} y^{m-1}, \ \ldots, \ x^{\alpha_{s_{m-1}}} y^{m-1} \end{aligned}$$

perceba que todo monômio em I é divisível por algum monômio da lista. Para justificar esse fato, basta considerar um monômio $x^{\alpha} y^p \in I$

1. Se $p \geq m$, então $x^{\alpha} y^p = (x^{\alpha} y^m) y^{p-m}$, pela construção de I, $x^{\alpha} \in J$. Como $J = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, então existe $y \in \mathbb{N}^n$ tal que $x^{\alpha} = x^{\alpha_i} x^{\gamma}$. Logo, $x^{\alpha} y^p = x^{\alpha_i} x^{\gamma} y^m y^{p-m} = (x^{\alpha_i} y^m) x^{\gamma} y^{p-m}$. Assim, $x^{\alpha} y^p$ é divisível por um elemento da lista.

2. Se $x^{\alpha} y^p \in I$ com $p \leq m-1$, por construção, $x^{\alpha} \in J_p$, como $J_p = \langle x^{\alpha_{p_1}}, \ldots, x^{\alpha_{p_s}} \rangle$. Então, existe $\gamma \in \mathbb{Z}^n_{\leq}$ tal que $x^{\alpha} = x^{\alpha_p} x^{\gamma}$. Assim, $x^{\alpha} y^p = x^{\alpha_{pj}} x^{\gamma} y^p = (x^{\alpha_{pj}} y^p) x^{\gamma}$. O que implica que $x^{\alpha} y^p$ é multiplo de $x^{\alpha_{p_j}} y^p$ pertence a lista. Portanto, $x^{\alpha} y^p$ é divisível por algum elemento da lista.

Assim, pelo **Lema 2** os monômios geram I, e pelo **Corolário 3** implica que os ideais são iguais. O que prova nossa afirmação.

Para completar a demonstração, vamos mostrar que um conjunto finito de geradores pode ser escolhido a partir de um dado conjunto de geradores do ideal. Seja $I = \langle x^{\alpha} : \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$ um ideal monomial. Queremos mostrar que I é gerado por algum conjunto finito de monômios $x^{\beta_i} \in I$ onde cada β_i pertencendo a A. Lembremos que pelo argumento anterior, I tem um número finito de geradores, ou seja

$$I = \langle x^{\beta_1}, \ldots, x^{\beta_s} \rangle,$$

para certos monômios $x^{\beta_i} \in I$. Como $x^{\beta_i} \in I = \langle x^{\alpha} : \alpha \in A \rangle$, temos que pelo **Lema 2**, cada x^{β_i} é divisível por x^{α_i} para algum $\alpha_i \in A$ e portanto,

$$x^{\beta_i} = h_i x^{\alpha_i}$$

onde $h_i \in K[x_1, \ldots, x_n]$ para $i = 1, \ldots, s$. Assim, tomando f em I.

Podemos escrever f da seguinte forma:

$$f = \sum_{i=1}^{s} a_i x^{\beta_i} = \sum_{i=1}^{s} (a_i h_i) x^{\alpha_i}$$

onde $a_i h_i \in K[x_1, \ldots, x_n]$ e portanto, $f \in \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$. Logo $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, o que conclui a demonstração. □

Corolário 4. Seja $\geq$ uma relação em $\mathbb{Z}^n_{\geq 0}$ satisfazendo as seguintes condições:

1. $\geq$ é uma ordem total em $\mathbb{Z}^n_{\geq 0}$;
2. Se $\alpha \geq \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$, então $\alpha + \gamma \geq \beta + \gamma$.

Então, $\geq$ é uma boa ordem se, e somente se, $\alpha \geq 0$ para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$. Onde $0 = (0, \ldots, 0) \in \mathbb{Z}^n$

Demonstração. Suponha que $\geq$ é uma boa ordem e tome α_0 como o menor elemento de $\mathbb{Z}^n_{\geq 0}$. Suponha por absurdo que $0 > \alpha_0$, pelo item 2 da hipótese, teríamos que $0 + \alpha_0 > \alpha_0 + \alpha_0$, ou seja $\alpha_0 > 2\alpha_0$, 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 $I = \langle x^\alpha : \alpha \in A \rangle$, um ideal monomial, pelo **Lema 4**, segue que $\{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$ com $\alpha_i \in A$, onde $1 \leq i \leq s$ é um conjunto gerador de I. Sem perda de generalidade, suponha $\alpha_1, \ldots, \alpha_s \in A$ tal que $\alpha_1 < \alpha_2 < \cdots < \alpha_s$. Mostremos agora que α_1 é o menor elemento de A. Note que $x^\alpha \in I$ e pelo **Lema 2** segue que algum x^{α_i} divide x^α, ou seja $x^\alpha = x^{\alpha_i} x^\gamma$, para algum $x^\gamma \in K[x_1, \ldots, x_n]$ e $\gamma \in \mathbb{Z}^n_{\geq}$.

Podemos então escrever $\alpha = \alpha_i + \gamma$ para algum $\gamma \in \mathbb{Z}^n_{\geq 0}$. Como $\gamma \geq 0$, pelo item 2 da hipótese, temos

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

Isso vale porque organizamos α_i de forma crescente. Portanto, α_1 é o menor elemento de A.

□

3.1 TEOREMA DA BASE DE HILBERT

O termo Noetheriano é uma homenagem à matemática alemã Emmy Noether cujas contribuições matemáticas revolucionaram a Álgebra Abstrata. No presente capítulo, iremos definir e caracterizar os *Anéis Noetherianos*. Ademais, iremos conhecer o Lema de Zorn e o Teorema da Base de Hilbert bastante usados em diversas áreas da matemática, principalmente na teoria dos anéis e ideais.

Definição 26. Uma sequência de ideais $I_1, I_2, I_3, \ldots, I_n, \ldots$ de um anel A é chamada de *cadeia de ascendente de ideais* se, para todo i, tivermos $I_i \subseteq I_{i+1}$.

Lema 5. *(Lema de Zorn)* Se $R = \varnothing$ é um conjunto parcialmente ordenado tal que toda cadeia em R tem cota superior em R, então R possui elemento maximal.

Tendo em vista que nosso objetivo referente ao Lema de Zorn é a sua aplicação, não iremos fazer sua prova. Caso o leitor tenha interesse, a demonstração pode ser encontrada em (HALMOS, 2001)

Teorema 6. Todo anel $A \neq \varnothing$ possui algum ideal maximal.

Demonstração. Considere S como o conjunto de todos os ideais próprios de um anel A. Ou seja, são ideais que não contêm o elemento 1_A. Note que $S \neq \varnothing$, pois o ideal trivial $\{0\} \in S$. Sendo S ordenado pela inclusão usual, considere uma cadeia $C = \{I_\lambda\}_{\lambda \in L} \subseteq S$. Como C é uma cadeia, para quaisquer $\alpha, \beta \in L$, temos $I_\alpha \subseteq I_\beta$ ou $I_\beta \subseteq I_\alpha$. Defina

$$I = \bigcup_{\lambda \in L} I_\lambda.$$

Note que I é um ideal próprio do anel A, pois é a união de ideais próprios de A onde os ideais I_λ formam uma cadeia de ideais. Além disso, I é uma cota superior para a cadeia C no conjunto S. Portanto, pelo Lema de Zorn, S possui um elemento maximal. Nesse contexto, A possui um ideal maximal. □

Definição 27. *(Anel Noetheriano)* Um anel A é um *anel Noetheriano* se toda cadeia ascendente de ideais de A

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

é estacionária, isto é, existe $m \geq 0$ tal que $I_m = I_j$, para todo $j \geq m$.

Exemplo 25. O anel $\mathbb{Z}$ dos números inteiros é um anel Noetheriano.

De fato, considere a seguinte cadeia ascendente de ideais de $\mathbb{Z}$, ou seja,

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots \subseteq \langle a_n \rangle \subseteq \cdots$$

Com $\langle a_1 \rangle \subseteq \langle a_2 \rangle$, temos que $a_1 = a_2 \cdot r_1$, ou seja, $a_2 \mid a_1$. Analogamente, $\langle a_2 \rangle \subseteq \langle a_3 \rangle$ e, portanto, $a_2 = a_3 \cdot r_2$ e $a_3 \mid a_2$. Mas, como $a_2 \mid a_1$ e $a_3 \mid a_2$, então $a_3 \mid a_1$. Assim, até um certo $j \in \mathbb{N}$, $a_j \mid a_1$. Como o conjunto de divisores de um número inteiro é finito, temos que, para algum $m \geq 0$, ocorre $\langle a_m \rangle = \langle a_j \rangle$, para todo $j \geq m$.

Exemplo 26. Considerando K um corpo. O anel de polinômios em infinitas variáveis $K[x_1, \ldots, x_n, \ldots]$ não é Noetheriano. De fato, basta tomar a seguinte cadeia ascendete de ideais

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \cdots \subseteq \langle x_1, \ldots, x_{n-1} \rangle \subseteq \langle x_1, \ldots, x_n \rangle \subseteq \cdots$$

que claramente não satisfaz a condição de cadeia estacionária.

Teorema 7. Um anel A é Noetheriano se, e somente se, todo ideal de A é finitamente gerado.

Demonstração. Seja I um ideal de A, como A é um anel Noetheriano, toda cadeia ascendente de ideais de A é estacionária. A seguir, vamos mostrar que um ideal I de A é finitamente gerado. Para isso, defina como Ω o conjunto de todos os ideais finitamente gerados de A. Note que Ω é não vazio, pois $\{0\} \in \Omega$, Logo Ω possui um elemento maximal I_0. Se $I \neq I_0$ então existe $n \in I$ tal que $n \notin I_0$. Considere $J = I_0 + \langle n \rangle$, assim temos que J é finitamente gerado, pois todos os seus elementos são formados de ideais finitamente gerados, e além disso, $I_0 \subseteq J$, o que é um absurdo, pois I_0 é maximal e não deveria ter outro conjunto contendo I_0.

Reciprocamente, queremos mostrar que a cadeia de ideais do anel A é estacionária. Dada uma cadeia ascendente de ideais $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$, então $M = \bigcup_{n=1}^{\infty} I_n$ é um ideal de A. É importante observar que nem sempre a união de ideais de um anel A é um ideal, mas, nesse caso, dados $a, b \in M$, existem índices i, j tais que $a \in I_i$ e $b \in I_j$. Como a cadeia é crescente, temos $I_i \subseteq I_j$ ou $I_j \subseteq I_i$; assim, ambos os elementos pertencem a um mesmo ideal da cadeia, digamos I_k, e como I_k é ideal, as operações entre a e b permanecem em $I_k \subseteq M$. Como I_{n_i} é finitamente gerado, existem $x_1, x_2, \ldots, x_r$ tais que são geradores de M, onde $x_i \in I_{n_i}$, e seja $n = \max\{n_1, n_2, \ldots, n_r\}$. Daí segue que cada x_i pertence a I_n, pois $I_{n_0} \subseteq I_{n_1} \subseteq \cdots \subseteq I_n$, logo a cadeia ascendente é estacionária e, portanto, A é um anel Noetheriano. □

Definição 28. Seja $I \subset K[x_1, \ldots, x_n]$ um ideal diferente de $\{0\}$.

1. Denotamos por $\mathrm{tl}(I)$ o conjunto dos termos líderes dos elementos de I. Assim,

$$\mathrm{tl}(I) = \{cx^{\alpha} : \exists\ f\ \in I \text{ com } \mathrm{tl}(f) = cx^{\alpha}\};$$

2. Denotamos por $\langle \mathrm{tl}(I) \rangle$ o ideal gerado pelos elementos de $\mathrm{tl}(I)$.

Proposição 5. Seja $I \subset K[x_1, \ldots, x_n]$ um ideal.

1. $\langle \mathrm{tl}(I) \rangle$ é um ideal monomial;
2. Existem $g_1, \ldots, g_t \in I$ tais que $\langle \mathrm{tl}(I) \rangle = \langle \mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_t) \rangle$.

Demonstração. Primeiro, vamos mostrar o item 1. Os monômios líderes $\mathrm{ml}(g)$ dos elementos de $g \in I - \{0\}$ geram o ideal monomial $\langle \mathrm{ml}(g) : g \in I - \{0\} \rangle$. Como $\mathrm{tl}(g) = \mathrm{cl}(g) \cdot \mathrm{ml}(g)$, temos que $\mathrm{ml}(g)$ e $\mathrm{tl}(g)$ são multiplos por uma constante não nula, ou seja o ideal $\langle \mathrm{ml}(g) : g \in I - \{0\} \rangle = \langle \mathrm{tl}(I) \rangle$. Diante da igualdade, concluímos que $\langle \mathrm{tl}(I) \rangle$ é ideal monomial.

Agora, provaremos o item 2. Como $\langle \mathrm{tl}(I) \rangle$ é um ideal monomial gerado pelos monômios $\mathrm{ml}(g)$ para $g \in I - \{0\}$, pelo **Lema 4** temos que $\langle \mathrm{tl}(I) \rangle = \langle \mathrm{ml}(g_1), \ldots, \mathrm{ml}(g_t) \rangle$ para um número finito de polinômios $g_1, \ldots, g_t \in I$. Como $\mathrm{ml}(g_i)$ é múltiplo de $\mathrm{tl}(g_i)$ por

uma constante não nula para cada $i = 1, \ldots, t$, segue pelo **Lema 2** que cada $tl(g_i)$ está em $\langle \mathrm{tl}(I) \rangle$, ou seja concluímos que $\langle \mathrm{tl}(I) \rangle = \langle \mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_t) \rangle$. □

Observação 9. Seja $I = \langle f_1, \ldots, f_t \rangle$, então $\langle \mathrm{tl}(f_1), \ldots, \mathrm{tl}(f_t) \rangle$ e $\langle \mathrm{tl}(I) \rangle$ podem ser ideais diferentes. Para exemplificar, seja $I = \langle f_1, f_2 \rangle$, tal que $f_1 = x^3 - 2xy$ e $f_2 = x^2y - 2y^2 + x$. Usando a ordem lexicográfica graduada em $\mathbb{R}[x, y]$ temos

$$-y \cdot (x^3 - 2xy) + x \cdot (x^2y - 2y^2 + x) = x^2$$

onde $x^2 \in I$. Assim, $x^2 = \mathrm{tl}(x^2) \in \langle \mathrm{tl}(I) \rangle$. Porém, x^2 não é divisível por $\mathrm{tl}(f_1) = x^3$ e nem por $\mathrm{tl}(f_2) = x^2y$. Logo pelo **Lema 2** temos que $x^2 \notin \langle \mathrm{tl}(f_1), \mathrm{tl}(f_2) \rangle$.

Teorema 8. *(Base 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 $g_1, \ldots, g_t \in I$. Em outras palavras, $K[x_1, \ldots, x_n]$ é um anel Noetheriano.

Demonstração. Se $I = \{0\}$, basta tomar o cojunto gerador com $\langle 0 \rangle$. Se $I \neq \langle 0 \rangle$ pela **Proposição 5** existem $g_1, \ldots, g_t \in I$ tais que $\langle \mathrm{tl}(I) \rangle = \langle \mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_t) \rangle$. Vamos mostrar que $I = \langle g_1, \ldots, g_t \rangle$. De fato, para cada $i, g_i \in I$. Logo, $\langle g_1, \ldots, g_t \rangle \subset I$. Reciprocamente, seja f um polinômio em I e divida f por $g_1, \ldots, g_t$. Pelo **Teorema 5**, obtemos uma expressão da forma

$$f = q_1 g_1 + \cdots + q_t g_t + r, \tag{32}$$

onde nenhum termo de r é divisível por algum $\mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_t)$. Vamos mostrar que $r = 0$, ou seja $f \in I$. Escrevendo de uma outra forma a equação (32) temos

$$r = f - q_1 g_1 - \cdots - q_t g_t$$

que nos mostra que $r \in I$, já que $f \in I$ e $q_1 g_1 - \cdots - q_t g_t \in I$. Se $r \neq 0$, então $\mathrm{tl}(r) \in \langle \mathrm{tl}(I) \rangle = \langle \mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_t) \rangle$, e pelo **Lema 2**, segue que $\mathrm{tl}(r)$ deve ser divisível por algum $\mathrm{tl}(g_i)$ com $i = 1, \ldots, t$, o que contradiz o fato de r ser o resto da divisão. Assim,

$$f = q_1 g_1 + \cdots + q_t g_t$$

ou seja, $f \in \langle g_1, \ldots, g_t \rangle$ e portanto $I = \langle g_1, \ldots, g_t \rangle$. □

3.2 BASE DE GRÖBNER

Definição 29. *(Base de Gröbner)* Seja I um ideal de $K[x_1, \ldots, x_n]$. Dada uma ordem monomial, um subconjunto $G = \{g_1, \ldots, g_n\} \subseteq I$ é uma *Base de Gröbner* se

$$\langle \mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_n) \rangle = \langle \mathrm{tl}(I) \rangle.$$

Observação 10. Pela **Proposição 5**, existe um número finito de polinômios $g_1, \ldots, g_t \in I$ tais que $\langle \mathrm{tl}(I) \rangle = \langle \mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_t) \rangle$. Além disso, pelo **Teorema da Base de Hilbert**, todo ideal de $K[x_1, \ldots, x_n]$ é finitamente gerado. Ademais, mostramos que o conjunto gerador de I é $G = \{g_1, \ldots, g_t\}$, que por sua vez, constitui uma base de Gröbner para I.

Proposição 6. Seja $G = \{g_1, \ldots, g_n\}$ uma base de Gröbner para um 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:

1. Nenhum termo de r é divisível pelos $\mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_n)$;
2. Existe $g \in I$ tal que $f = g + r$.

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

Demonstração. Pelo **Teorema 5**, podemos escrever $f = q_1 g_1 + \cdots q_n g_n + r$, com r satisfazendo a condição do item 1. Se definirmos $g = q_1 g_1 + \cdots q_n g_n \in I$, então temos que $f = g + r$, o que mostra o item 2 onde garantimos existência de r. Para provar que r é único, suponha que $f = g + r = g' + r'$ satisfazendo simultaneamente 1 e 2. Então $r - r' = g - g' \in I$, já que $g, g' \in I$. Suponha por absurdo que $r \neq r'$, então $\mathrm{tl}(r - r') \in I$, que por sua vez possue uma base de Gröbner, logo $\mathrm{tl}(r - r') \in \langle \mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_n) \rangle$. Observe que $\mathrm{tl}(r - r') = \pm \mathrm{tl}(r')$ ou, $\mathrm{tl}(r - r') = \pm \mathrm{tl}(r)$, ou $\mathrm{tl}(r - r') \prec \mathrm{tl}(r')$. E assim, pelo **Lema 2**, segue que $\mathrm{tl}(r - r')$ é divisível por algum $\mathrm{tl}(g_i)$, o que pelo item 1 é um absurdo. Logo, $r = r'$ o que nos garante a unicidade de r. □

Corolário 5. Seja $G = \{g_1, \ldots, g_n\}$ 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 todos os elementos de G é zero.

Demonstração. Considere a divisão de f por $g_1, \ldots, g_n$ onde $r = 0$, então pelo **Teorema 5**, podemos expressar f da seguinte forma: $f = q_1 g_1 + \cdots + q_n g_n \in I$, já que $g_1, \ldots g_n \in I$. Reciprocamente, considere $f = f + 0 \in I$ satisfaz as duas condições da **Proposição 6**, ou seja, zero é o resto da divisão de f por $g_1, \ldots, g_n$. □

Definição 30. Escrevemos $\overline{f}^F$ 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 ordem em particular).

Nosso próximo objetivo é demonstrar o Algoritmo de Buchberger, que, por sua vez, nos fornece ferramentas, através de um número finito de passos, para estabelecer uma base de Gröbner para um conjunto I finitamente gerado. Além de outras coisas, vamos definir a seguinte generalização de mínimo múltiplo comum.

Definição 31. Sejam $f, g \in K[x_1, \ldots, x_n]$ polinômios não nulos e uma ordem monomial fixada.

1. Se multigrau$(f) = (\alpha_1, \ldots, \alpha_n)$ e multigrau$(g) = (\beta_1, \ldots, \beta_n)$, tome $\gamma = (\gamma_1, \ldots, \gamma_n)$, onde $\gamma_i = \max(\alpha_i, \beta_i)$ para todo i. Chamaremos de $x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_n^{\gamma_n}$ de *mínimo múltiplo comum* de ml(f) e ml(g), denotado por $X^\gamma = \text{mmc}(\text{ml}(f), \text{ml}(g))$;
2. O *S-polinômio* de f e g é a combinação

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

Observação 11. Devemos tomar cuidado para não confundir o mmc com o monômio líder que mencionamos na **Observação 6**.

Exemplo 27. Seja $f = x^{13}y^8 - x^{15}y^2 + x$ e $g = 3x^{18}y^6 + y^2 \in \mathbb{R}[x,y]$ com respeito a ordem lexicográfica graduada, $\text{tl}(f) = x^{13}y^8, \text{tl}(g) = 3x^{18}y^6$ temos que $\gamma = (18, 8)$, logo

$$\begin{aligned} S(f,g) &= \frac{x^{18}y^8}{x^{13}y^8} \cdot f - \frac{x^{18}y^8}{3x^{18}y^6} \cdot g \\ &= x^5 \cdot f - \left(\frac{1}{3}\right) y^2 \cdot g \\ &= -x^{20}y^2 + x^6 - \frac{1}{3}y^4. \end{aligned}$$

Observe que o *S-polinômio* $S(f,g)$ é construído de uma forma que o ocorra o cancelamento entre os termos líderes. O lema abaixo detalha esse tipo de cancelamento de termos líderes.

Lema 6. Considere a soma $\sum_{i=1}^s c_i f_i$, onde $c_i \in K$ e multigrau$(f_i) = \delta \in \mathbb{Z}_{\geq}^n$ para todo $i = 1, \ldots, s$. Se multigrau$\left(\sum_{i=1}^s c_i f_i\right) < \delta$, 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, multigrau$(S(f_j, f_k)) < \delta$

Demonstração. Para todo $i \in \{1, \ldots\ s\}$ considere $d_i = \text{cl}(f_i)$, de modo que $c_i d_i$ é o coeficiente líder de $c_i f_i$, onde multigrau$(c_i f_i) = \delta$. Note que

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 f_1 + \cdots + c_s d_s f_s \tag{33}$$

onde ml$(f_i) = x_1^{\delta_1} \cdots x_s^{\delta_s}$, ou seja, $c_i f_i = d_i c_i x_1^{\delta_1} \cdots x_s^{\delta_s} + f_{i_0}$, onde multigrau$(f_{i_0}) < \delta$. Denotaremos $x_1^{\delta_1} \cdots x_s^{\delta_s}$ por X^δ em que $\delta = (\delta_1, \ldots, \delta_s) \in \mathbb{Z}_{\geq}^n$. Assim, temos na equação (33) da seguinte forma

$$c_1 d_1 X^\delta + f_{1_0} + \cdots + c_s d_s X^\delta + f_{s_0}$$

colocando X^δ em evidência

$$X^\delta \left(\sum_{i=1}^{s} c_i d_i\right) + \sum_{i=1}^{s} f_{i_0}.$$

Como por hipótese o multigrau da soma é menor que δ, segue que $\sum_{i=0}^s c_i d_i = 0$.

Considere $p_i = \frac{f_i}{d_i}$ onde $d_i = \mathrm{cl}(f_i)$, ou seja, $\mathrm{cl}(p_i) = 1$. Considere a soma

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i \tag{34}$$

reescrevendo o lado direito de (34) temos

$$c_1d_1p_1 - c_1d_1p_2 + c_1d_1p_2 + c_2d_2p_2 - c_2d_2p_3 + c_2d_2p_3 + \cdots + c_{s-1}d_{s-1}p_s + c_sd_sp_s$$

colocando os termos em evidência, podemos escrever (34) da seguinte forma

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i =& c_1d_1(p_1 - p_2) + (c_1d_1 + c_2d_2)(p_2 - p_3) + \cdots + \\ & (c_1d_1 + \cdots + c_{s-1}d_{s-1})(p_{s-1} - p_s) + (c_1d_1 + \cdots + c_sd_s)p_s.\end{aligned}$$

Por construção, $\mathrm{tl}(f_i) = d_iX^{\delta}$. Logo, $\mathrm{mmc}(\mathrm{ml}(f_i), \mathrm{ml}(f_k)) = X^{\delta}$ e portanto

$$\begin{aligned}S(f_j, f_k) &= \frac{X^{\delta}}{\mathrm{tl}(f_j)} \cdot f_j - \frac{X^{\delta}}{\mathrm{tl}(f_k)} \cdot f_k \\ &= \frac{X^{\delta}}{d_jX^{\delta}} \cdot f_j - \frac{X^{\delta}}{d_kX^{\delta}} \cdot f_k \\ &= \frac{f_j}{d_j} - \frac{f_k}{d_k} = p_j - p_k.\end{aligned}$$

Usando o fato de que $\sum_{i=1}^{s} c_i d_i = 0$ temos (34) escrito da seguinte forma

$$\sum_{i=1}^{s} c_i f_i = c_1d_1S(f_1, f_2) + (c_1d_1 + c_2d_2)S(f_2, f_3) + \cdots + (c_1d_1 + \cdots c_{s-1}d_{s-1})S(f_{s-1}, f_s)$$

que é uma combinação linear de coeficientes em K e *S-polinômios*. Além disso, como p_j e p_k têm multigrau igual a δ e coeficiente líder 1, então $\mathrm{multigrau}(p_j - p_k) < \delta$, pois os termos líderes vão se cancelar. Por esse mesmo motivo, $\mathrm{multigrau}(S(f_j, f_k)) < \delta$. □

De acordo com a **Proposição 6**, dado $G = g_1, \ldots, g_s$, uma base de Gröbner, ao fazer a divisão de f por todos os elementos de G, temos que o resto da divisão é unicamente determinado. Além disso, dado $I = \langle g_1, \ldots, g_s \rangle$, e fazendo uso do **Corolário 5**, conseguimos determinar, de uma forma fácil, se f pertence ou não a um ideal I.

Perceba que a facilidade nos cálculos advém de saber que G é base de Gröbner. Contudo, além da **Definição 29**, não sabemos ao certo identificar se um conjunto gerador é ou não uma base de Gröbner. Muitas vezes, isso torna-se difícil. Por isso, apresentaremos o próximo Teorema com o intuito de facilitar a identificação de uma base de Gröbner.

Teorema 9. Seja I um ideal polinomial. Então a base $G = \{g_1, \ldots, g_s\}$ de I é uma base de Gröbner de I se, e somente se, para todo $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por todos os elementos de G (em qualquer ordem) é zero.

Demonstração. Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner, notemos que $S(g_i, g_j)$ é uma combinação de elementos de G para todo $i \neq j$, ou seja, aplicando o **Teorema 5** e fazendo a divisão de $S(g_i, g_j)$ por $g_1, \ldots, g_s$, em qualquer ordem, obtemos o resto é igual a zero.

Reciprocamente, seja $f \in I$ um polinômio não nulo. Queremos mostrar que se todos os *S-polinômios* têm resto zero quando dividido por todos os elementos de G, então $\mathrm{tl}(f) \in \langle \mathrm{tl}(g_1), \ldots \mathrm{tl}(g_t) \rangle$, ou seja $G = \{g_1, \ldots, g_t\}$ é uma base de Gröbner para I.

Dado $f \in I = \langle g_1, \ldots, g_s \rangle$, existem polinômios $h_i \in K[x_1, \ldots, x_n]$ com $i = 1, \ldots, t$ tais que

$$f = \sum_{i=1}^{t} h_i g_i. \tag{35}$$

Pela **Proposição 4** temos

$$\mathrm{multigrau}(f) = \mathrm{multigrau}(h_1 g_1 + \cdots + h_t g_t) \leq \max_{1<i<t} \{\mathrm{multigrau}(h_i g_i)\} \tag{36}$$

Se a igualdade não ocorrer em (36) então deve ocorrer cancelamento dos termos líderes. Usando o **Lema 6**, todo cancelamento dos termos líderes se dá por *S-polinômios*, então podemos reescrever $f \in I$ em termos destes. Nosso objetivo agora é mostrar que

$$\mathrm{multigrau}(f) = \max\{\mathrm{multigrau}(h_i g_i)\}.$$

Ou seja, vamos mostrar que $\mathrm{tl}(f)$ é divisível por $\mathrm{tl}(g_i)$ para algum i. Daí, pelo **Lema 2** teremos que $\mathrm{tl}(f) \in \langle \mathrm{tl}(g_1), \ldots \mathrm{tl}(g_t) \rangle$ e isso provará o teorema.

Considere f como em (35) e $m(i) = \mathrm{multigrau}(h_i g_i)$. Vamos considerar $\delta = \max\{m(1), \ldots, m(t)\}$, ou seja, $\mathrm{multigrau}(f) \leq \delta$. Considere agora todas as possíveis formas de escrever f na equação (35). Para cada possibilidade, temos δ distinto. Porém, como visto na **Definição 20**, toda ordem monomial é uma boa ordenação, e portanto, podemos escolher uma expressão tal que δ seja o mínimo possível, e verificar a igualdade $\mathrm{multigrau}(f) = \delta$, e assim mostraremos que $\mathrm{tl}(f) \in \langle \mathrm{tl}(g_1), \ldots, \mathrm{tl}(g_t) \rangle$.

Assim, suponha por absurdo que $\mathrm{multigrau}(f) < \delta$ e escrevemos f convenientemente de modo a isolar os termos de multigrau δ, ou seja, vamos separar f em duas somas da seguinte forma

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} (\mathrm{tl}(h_i) + h_i - \mathrm{tl}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathrm{tl}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{tl}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{37}$$

Podemos observar que os termos que aparecem na segunda e terceira soma de (37) têm multigrau $< \delta$, já que ao fazer $h_i - \mathrm{tl}(h_i)$ cancelará o $\mathrm{tl}(h_i)$. E assim, como supomos

multigrau$(f) < \delta$ implica que a primeira soma de (37) tem multigrau menor que δ, ou seja

$$\text{multigrau}\left(\sum_{m(i)=\delta} \text{tl}(h_i)g_i\right) < \delta. \tag{38}$$

Seja $\text{tl}(h_i) = c_i x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ onde denotaremos tal termo por $c_i X^{\alpha_i}$. Então,

$$\sum_{m(i)=\delta} \text{tl}(h_i)g_i = \sum_{m(i)=\delta} c_i X^{\alpha_i} g_i \tag{39}$$

note que (38) satisfaz a hipótese do **Lema 6**, onde chamaremos, de acordo com tal Lema $f_i = X^{\alpha_i} g_i$, e portanto, f_i pode ser reescrito como uma combinação de *S-polinômio* $S(X^{\alpha_j} g_j, X^{\alpha_k} g_k)$. Assim,

$$\begin{aligned} S(X^{\alpha_j} g_j, X^{\alpha_k} g_k) &= \frac{X^{\delta}}{X^{\alpha_j}\,\text{tl}(g_j)} \cdot X^{\alpha_j} g_j - \frac{X^{\delta}}{X^{\alpha_k}\,\text{tl}(g_k)} \cdot X^{\alpha_k} g_k \\ &= \frac{X^{\delta-\gamma_{jk}+\gamma_{jk}}}{\text{tl}(g_j)} \cdot g_j - \frac{X^{\delta-\gamma_{jk}+\gamma_{jk}}}{\text{tl}(g_k)} \cdot g_k \\ &= X^{\delta-\gamma_{jk}} \left[\frac{X^{\gamma_{jk}}}{\text{tl}(g_j)} \cdot g_j - \frac{X^{\gamma_{jk}}}{\text{tl}(g_k)} \cdot g_k\right] \\ &= X^{\delta-\gamma_{jk}} S(g_j, g_k) \end{aligned} \tag{40}$$

onde $X^{\gamma_{jk}} = \text{mmc}(\text{ml}(g_j), \text{ml}(g_k))$. Logo, pelo **Lema 6** existem coeficientes $c_{jk} \in K$ tais que substituindo $f_i = X^{\alpha_i} g_i$ em (39) e usando (40) ficamos com

$$\sum_{m(i)=\delta} \text{tl}(h_i)g_i = \sum_{m(i)=\delta} c_{jk} X^{\delta-\gamma_{jk}} S(g_j, g_k). \tag{41}$$

O próximo passo é usar nossa hipótese de que o resto da divisão de $S(g_j, g_k)$ por $g_1, \ldots g_t$ é zero. De acordo com o **Teorema 5** temos que

$$S(g_j, g_k) = \sum_{i=1}^{t} q_{ijk} g_i, \tag{42}$$

onde $q_{ijk} \in K[x_1, \ldots, x_n]$. Além disso, pela **Observação 7** sabemos que

$$\text{multigrau}(q_{ijk} g_i) \leq \text{multigrau}(S(g_i, g_k)) \tag{43}$$

para todo i, k, j.

Indutivamente, isso mostra que, quando o resto da divisão é zero, podemos encontrar uma expressão para $S(g_j, g_k)$ em termos dos elementos de G, onde nem todo termo líder se cancela, já que, se houvesse o cancelamento, a desigualdade (43) seria estritamente menor, gerando uma contradição.

Pensando no argumento destacado, multiplicaremos ambos os lados da equação (42) por $X^{\delta-\gamma_{jk}}$ para obter

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

onde $b_{ijk}=X^{\delta-\gamma_{jk}}q_{ijk}$. Assim, aplicando o **Lema 6** podemos observar que

$$\text{multigrau}(b_{ijk}g_i)\leq\text{multigrau}(X^{\delta-\gamma_{jk}}S(g_j,g_k)).$$

Onde por (40)

$$X^{\delta-\gamma_{jk}}S(g_j,g_k)=S(X^{\alpha_j}g_j,X^{\alpha_k}g_k)$$

e pelo **Lema 6**

$$\text{multigrau}(X^{\delta-\gamma_{jk}}S(g_j,g_k))=\text{multigrau}(S(X^{\alpha_j}g_j,X^{\alpha_k}g_k))<\delta. \tag{44}$$

Substituindo a informação encontrada na expressão (44) acima e usando (41) e (42) obtemos

$$\begin{aligned}\sum_{m(i)=\delta}\text{tl}(h_i)g_i&=\sum_{j,k}c_{jk}X^{\delta-\gamma_{jk}}S(g_j,g_k)\\&=\sum_{j,k}c_{jk}\left(\sum_i b_{ijk}g_i\right)\\&=\sum_i w_ig_i\end{aligned}$$

onde concluímos que $\text{multigrau}(w_ig_i)<\delta$ para todo i.

Assim, substituindo $\sum_{m(i)=\delta}\text{tl}(h_i)g_i=\sum_i w_ig_i$ em (37), obtemos

$$f=\sum_i w_ig_i+\sum(h_i-\text{tl}(h_i))g_i+\sum h_ig_i$$

como combinação dos polinômios $g_1,\ldots,g_t$, onde todos os termos têm multigrau menor que δ, o que é um absurdo, já que contradiz a minimalidade de δ. Ou seja, $\text{multigrau}(f)=\delta=\max\{\text{multigrau}(h_ig_i)\}$, ou seja, $\text{tl}(f)$ é divisível por $\text{tl}(g_i)$. Daí, $\text{tl}(f)\in\langle\text{tl}(g_1),\ldots,\text{tl}(g_t)\rangle$. O que completa a demonstração. □

Exemplo 28. Seja o ideal $I=\langle -x+z^2,-y+z^3\rangle$. Vamos mostrar, usando o Teorema acima que $G=\{-x+z^2,-y+z^3\}$ é uma base de Gröbner considerando a ordem lexicográfica. Seja $f=-x+z^2$ e $g=-y+z^3$, onde $\text{multigrau}(f)=(1,0,0)$ e $\text{multigrau}(g)=(0,1,0)$ ou seja, $\text{mmc}(\text{ml}(f),\text{ml}(g))=\text{mmc}(x,y)=xy$. Logo, o *S-polinômio* $S(f,g)$ é dado por

$$\begin{aligned}S(f,g)&=\frac{xy}{\text{tl}(f)}\cdot f-\frac{xy}{\text{tl}(g)}\cdot g\\&=\frac{xy}{-x}\cdot(-x+z^2)-\frac{xy}{-y}\cdot(-y+z^3)\\&=xz^3-yz^2.\end{aligned}$$

Como $S(f,g) = xz^3 - yz^2$, que por sua vez pode ser escrito como

$$S(f,g) = -z^3(-x + z^2) + z^2(-y + z^3) + 0.$$

Temos que ao aplicarmos o **Teorema 5** $S(f,g)$ deixa resto igual a zero na divisão por todos os elementos de G. Logo, pelo **Teorema 9** G é uma base de Gröbner.

3.3 ALGORITMO DE BUCHBERGER.

Já sabemos que, pela **Proposição 5** e pelo Teorema da Base de Hilbert, todo ideal não nulo $I \subseteq k[x_1, \ldots, x_n]$ tem uma base de Gröbner. Até agora, com o **Teorema 9**, conseguimos verificar se um conjunto gerador $g_1, \ldots, g_s$ é ou não uma base de Gröbner, apenas usando o resto da divisão de $S(g_i, g_j)$.

Nesta seção, apresentaremos o *Algoritmo de Buchberger*, que nos fornecerá uma base de Gröbner de um ideal $I \subseteq K[x_1, \ldots, x_n]$. Para isso, vamos expandir o conjunto original de geradores de I, adicionando os restos não nulos de $S(g_i, g_j)$ até formar uma base de Gröbner, onde $G = g_1, \ldots, g_s$. Vejamos o exemplo a seguir.

Exemplo 29. Seja $I = \langle g_1, g_2 \rangle = \langle x^2y - 1, xy^2 - x \rangle \in \mathbb{C}[x,y]$ onde consideraremos a ordem lexicográfica. Temos que $\mathrm{ml}(g_1) = x^2y$ e $\mathrm{ml}(g_2) = xy^2$, observe também que $\text{multigrau}(g_1) = (2,1)$ e $\text{multigrau}(g_2) = (1,2)$, ou seja $\mathrm{mmc}(\mathrm{ml}(g_1, \mathrm{ml}(g_2)) = x^2y^2$. Assim

$$S(g_1, g_2) = \frac{x^2y^2}{x^2y}(x^2y - 1) - \frac{x^2y^2}{xy^2}(xy^2 - x) = x^2 - y$$

Ao fazer a divisão de $S(g_1, g_2)$ por $G = \{g_1, g_2\}$, o resto é diferente de zero, ou seja $\overline{S(g_1, g_2)}^{G} = x^2 - y \neq 0$, e consequentemente, G não é uma base de Gröbner. Porém, se adicionarmos $g_3 = x^2 - y$ a G, ou seja $G_3 = \{g_1, g_2, x^2 - y\}$ temos que $\overline{S(g_1, g_2)}^{G_3} = 0$. Entretando,

$$S(g_1, g_3) = \frac{x^2y}{x^2y}(x^2y - 1) - \frac{x^2y}{x^2}(x^2 - y) = y^2 - 1$$

Fazendo as mesmas ponderações, temos que $\overline{S(g_1, g_3)}^{G_3} = y^2 - 1 \neq 0$. Então acrescentando $g_4 = y^2 - 1$ e denotando $G_4 = \{g_1, g_2, g_3, y^2 - 1\}$. Note que $\overline{S(g_1, g_3)}^{G_4} = 0$ e

$$S(g_1, g_4) = \frac{x^2y^2}{x^2y}(xy^2 - 1) - \frac{x^2y^2}{y^2}(y^2 - 1) = x^2 - y = g_3$$

como $S(g_1, g_4) = g_3$ temos que $\overline{S(g_1, g_4)}^{G_4} = 0$, já que $g_3 \in G_4$. Porém

$$S(g_2, g_3) = \frac{x^2y^2}{xy^2}(xy^2 - x) - \frac{x^2y^2}{x^2}(x^2 - y) = -x^2 + y^3$$

onde $\overline{S(g_2,g_3)}^{G_4} = -x^2+y^3 \neq 0$. Assim, devemos adicionar $g_5 = -x^2+y^3$ e teremos automaticamente que $\overline{S(g_2,g_3)}^{G_5} = 0$. Note ainda que

$$S(g_2,g_4) = 0 \Rightarrow \overline{S(g_2,g_4)}^{G_5} = 0;$$
$$S(g_3,g_4) = x^2 - y^5 \Rightarrow \overline{S(g_3,g_4)}^{G_5} = 0;$$
$$S(g_2,g_5) = S(g_4,g_5) = -x^2+y^5 \Rightarrow \overline{S(g_2,g_5)}^{G_5} = 0;$$
$$S(g_3,g_5) = -y^4 - y^2 = y(y^2-1) = y^2 g_4 \Rightarrow \overline{S(g_3,g_5)}^{G_5} = 0;$$
$$S(g_1,g_5) = y^4 - 1 = (y^2-1)(y^2+1) = (y^4+1)g_4 \Rightarrow \overline{S(g_1,g_5)}^{G_5} = 0.$$

Assim, pelo **Teorema 9** $G = \{g_1,g_2,g_3,g_4,g_5\}$ é uma base de Gröbner.

Teorema 10. *(Algoritmo de Buchberger)* 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 passos através do seguinte algoritmo:

Entrada: $\{g_1,\ldots,g_s\} \subseteq K[x_1,\ldots,x_n]$;

Defina $G_0 := \varnothing, G_1 = \{g_1,\ldots,g_s\}$ e $\ := 1$;

Enquanto $G_{i-1} \neq G_i$ faça

Se existir $f,h \in G_i$tais que o resto r da divisão de $S(f,h)$ por G_i é diferente de de zero,

Então $G_{i+1} := G_i \cup \{r\}$;

Senão $G_{i+1} := G_i$;

$i := i+1$

Saída: $G := G_i$ Base de Gröbner para I.

Demonstração. Caso, em algum momento, a condicional "Se", dada nos procedimentos do algoritmo, for negativa, então a proposição anterior nos garante que G_i é uma Base de Gröbner para o ideal gerado por G_i e, consequentemente, para I, uma vez que todos os *S-polinômios* dos elementos de G_i deixam resto zero na divisão por todos os elementos de G_i.

Basta mostrar que o algoritmo termina com um número finito de passos. Para isso, suponha que o procedimento seja infinito. Nesse caso, teríamos uma sequência infinita de conjuntos

$$G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_i \subsetneq \cdots$$

em que $G_i := G_{i+1}$ é obtido a partir de G_i pela adjunção de um elemento $r \neq 0$ tal que $\mathrm{ml}(g_i) \nmid \mathrm{ml}(r)$ para todo $g \in G_i$.

Desse modo, teríamos uma sequência infinita de ideais monomiais

$$\langle \mathrm{ml}(G_1)\rangle \subsetneq \langle \mathrm{ml}(G_3)\rangle \subsetneq \cdots \subsetneq \langle \mathrm{ml}(G_i)\rangle \subsetneq \cdots . \tag{45}$$

No entanto, como $\langle \mathrm{ml}(G_k)\rangle$ para todo k é um ideal de $K[x_1,\ldots,x_n]$, que por sua vez é um anel Noetheriano, não podemos ter a cadeia ascendente infinita descrita em (45).

Assim, existe $i \in \mathbb{N}$ tal que $G_i = G_{i+1}$, e portanto o algoritmo finaliza em um número finito de passos. □

Em geral, bases de Gröbner determinadas pelo Algoritmo de Buchberger são maiores que o necessário. O lema a seguir mostra que podemos eliminar geradores desnecessários.

Lema 7. Seja $G = \{g_1, \ldots, g_s\}$ uma Base de Gröbner do ideal I com respeito a uma ordem monomial fixada. Se temos $\mathrm{ml}(g_i) \mid \mathrm{ml}(g_j)$ em que $i, j \in \{1, \ldots, s\}$ com $i \neq j$, então $H = G - \{g_j\}$ é ainda uma Base de Gröbner para I.

Demonstração. Seja $f \in I$. Como G é uma Base de Gröbner para I, existe $g_k \in G$ tal que $\mathrm{ml}(g_k) \mid \mathrm{ml}(f)$. Se $g_k \neq g_j$, então $g_k \in H$. Por outro lado, se $g_k = g_j$, então como $\mathrm{ml}(g_i) \mid \mathrm{ml}(g_j) = \mathrm{ml}(g_k)$ e $\mathrm{ml}(g_k) \mid \mathrm{ml}(f)$ temos que $\mathrm{ml}(g_i) \mid \mathrm{ml}(f)$ e $g_i \in H$. Portanto, de qualquer modo, dado $f \in I$, existe $g \in H$ tal que $\mathrm{ml}(g) \mid \mathrm{ml}(f)$, indicando assim, que H é uma Base de Gröbner para I. □

Definição 32. Fixada uma ordem monomial, dizemos que G é uma *Base de* Gröbner *Minimal* para um ideal I, se $\mathrm{ml}(g_i) \nmid \mathrm{ml}(g_j)$, para todo $g_i, g_j \in G$ com $g_i \neq g_j$.

Observe que, usando o Algoritmo de Buchberger e o **Lema 7**, podemos constituir uma base de Gröbner minimal para um determinado ideal não nulo. Vamos considerar a base de Gröbner obtida no **Exemplo 29** e encontrar uma a Base Minimal.

Exemplo 30. Seja $G = \{f_1, f_2, f_3, f_4, f_5\}$ uma base de Gröbner obtida no **Exemplo 29**, ou seja

$$G = \{x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1, -x^2 + y^3\}.$$

Notemos que $\mathrm{tl}(f_1) = x^2y = y\,\mathrm{tl}(f_3)$. Então pelo **Lema 7** podemos retirar f_1. Do mesmo modo, podemos retirar f_2 e f_5 pois $\mathrm{tl}(f_2) = xy^2 = x\,\mathrm{tl}(f_4)$ e $\mathrm{tl}(f_5) = -x^2 = (-1)\,\mathrm{tl}(f_3)$. Consequentemente,

$$\bar{f_3} = x^2 - y, \text{ e } \bar{f_4} = y^2 - 1$$

forma uma base de Gröbner minimal de I.

Definição 33. Uma Base de Gröbner Minimal para um ideal I é chamada de *Base de* Gröbner *Reduzida* com respeito a uma ordem monomial, se os elementos de G são mônicos e todo $g \in G$, coincide com seu resto na divisão por todos os elementos de $G - \{g\}$.

Exemplo 31. Vamos determinar Base de Gröbner Reduzida para o conjunto $G = \{f_1 = x^2y - 1, f_2 = xy^2 - x, f_3 = x^2 - y, f_4 = y^2 - 1, f_5 = -x^2 + y^3\}$ do **Exemplo 30**. Sabemos que a Base de Gröbner Minimal é $H = \{\bar{f_3} = x^2 - y, \bar{f_4} = y^2 - 1\}$. Como os polinômios da base minimal são mônicos e todo $\bar{f_i}$ coincide com seu resto na divisão por todos os elementos de H, temos que H é uma Base de Gröbner Reduzida.

4 APLICAÇÕES

Após o desenvolvimento teórico sobre anéis de polinômios, ordens monomiais e Bases de Gröbner, este capítulo tem como objetivo apresentar algumas de suas aplicações práticas. As Bases de Gröbner constituem um instrumento fundamental no estudo estrutural de ideais polinomiais e na resolução de sistemas não lineares.

Sua principal vantagem está na capacidade de transformar sistemas de equações polinomiais em formas mais simples, semelhantes ao escalonamento de sistemas lineares, o que possibilita resolver problemas algébricos, geométricos e combinatórios de forma sistemática e eficiente.

Neste capítulo, serão analisadas aplicações representativas dessa teoria, com ênfase na resolução de sistemas de equações polinomiais e na modelagem de situações reais, como o controle de tráfego ferroviário e o problema da coloração de mapas.

4.1 SISTEMAS DE EQUAÇÕES POLINOMIAIS

Neste seção iremos conhecer o que é o espaço afim, uma variedade algébrica e suas propriedades. Para isso, vamos trabalhar com conjuntos de pontos em um espaço e ideais de um anel de polinômios $K[x_1, \ldots, x_n]$.

Definição 34. *(Espaço afim)* Seja K um corpo O *espaço afim n-dimensional* sobre K é definido por

$$A_k^n = \{(a_1, \ldots, a_n); a_i \in K, i \in \{1, \ldots, n\}\}.$$

Definição 35. *(Variedade algébrica)* Seja K um corpo. Um subconjunto $X \subseteq A_K^n$ é dito uma *variedade algébrica afim*, ou simplesmente *variedade algébrica* se for o conjunto-solução de um sistema de equações:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

onde $f_1, f_2, \ldots, f_m$ são polinômios no anel $K[x_1, \ldots, x_n]$.

Seja $S = \{f_1, \ldots, f_m\}$, podemos escrever o conjunto X da definição acima como

$$X = \mathcal{V}(S) = \{(a_1, \ldots, a_n) \in A_K^n; f(a_1, \ldots, a_n) = 0 \ \forall \ f \in S\}.$$

É notável que uma variedade algébrica[1]

[1] Dado o espaço afim A_K^n, a *Topologia de Zariski* é definida ao se considerar como fechados os conjuntos de zeros de ideais de polinômios com coeficientes em k. Esses conjuntos, denotados por $\mathcal{V}(I)$, são precisamente os subconjuntos de A_K^n onde todos os polinômios de um ideal I se anulam. $\mathcal{V}(I)$ é simplesmente a interseção dos conjuntos de zeros definidos por cada polinômio do sistema dado.

Exemplo 32. Vamos determinar a variedade algébrica de $S = \{y^2 - x^3, y - x^2\} \subseteq \mathbb{R}[x, y]$. Ou seja, queremos é determinar os pontos no espaço afim que zeram todos os polinômios de S.

$$\begin{cases} y^2 - x^3 = 0 \\ y - x^2 = 0 \end{cases}$$

resolvendo o sistema, observamos que $y = x^2$, Assim, na primeira equação obtemos $x^4 = x^3$. Logo, resolvendo tal equação em $\mathbb{R}$ teremos que $x = 0$ então $y = 0$ e, $x = 1$ então $y = 1$. Portanto, $\mathcal{V}(S) = \{(0, 0), (1, 1)\}$. Neste caso, temos um conjunto finito de pontos.

Nesse caso, podemos ter um recorte geométrico da variedade acima.

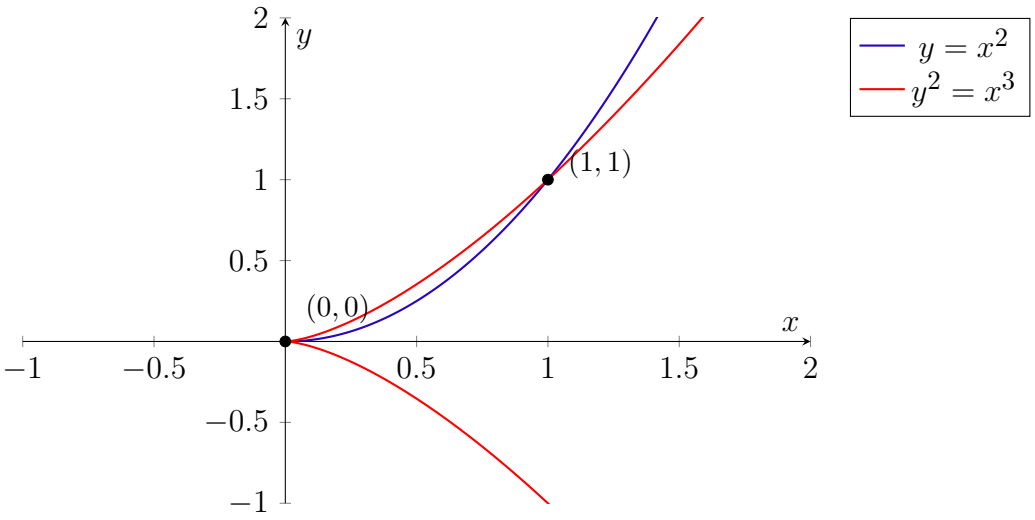


Figura 1 – $\mathcal{V}(y^2 - x^3, y - x^2)$

Proposição 7. Seja S um subconjunto de $K[x_1, \ldots, x_n]$ tal que $I = \langle S \rangle$. Então, $\mathcal{V}(\langle S \rangle) = \mathcal{V}(S)$.

Demonstração. Seja $P \in \mathcal{V}(\langle S \rangle)$, isto é, $g(P) = 0$ para todo $g \in \langle S \rangle$ queremos mostrar que $P \in \mathcal{V}(S)$. De fato, tome $f \in S$, temos que $f \in \langle S \rangle$ já que $f = 1 \cdot f$, por esse motivo $f(P) = 0$, ou seja $P \in S$ e assim $\mathcal{V}(\langle S \rangle) \subseteq \mathcal{V}(S)$.

Reciprocamente, vamos mostrar que $\mathcal{V}(S) \subseteq \mathcal{V}(\langle S \rangle)$. Para isso, tome $P \in \mathcal{V}(S)$, além disso, considere $f \in \langle S \rangle$, temos então que $f = h_1 g_1 + \cdots + h_n g_n$, onde $h_i \in K[x_1, \ldots, x_n]$ e $g_1, \ldots, g_n \in S$ com $i \in \{1, \ldots, n\}$ Como $P \in \mathcal{V}(S)$, então P anula todo $g_i, i \in \{1, \ldots, n\}$. Logo, aplicando

$$\begin{aligned} f(P) &= (h_1 g_1 + \cdots + h_n g_n)(P) \\ &= h_1(P) g_1(P) + \cdots + h_n(P) g_n(P) \\ &= h_1(P) \cdot 0 + \cdots + h_n(P) \cdot 0 = 0 \end{aligned}$$

logo, $P \in \mathcal{V}(\langle S \rangle)$, já que encontramos um polinômio em $f \in \langle S \rangle$ que anula P. □

Exemplo 33. Se tomarmos o espaço afim $A^2_{\mathbb{R}}$, dado o ideal $I = \langle x^2 - y \rangle \subset \mathbb{R}[x, y]$, temos que $V(I) \subset A^2_{\mathbb{R}}$ representa uma parábola no plano bidimensional sobre $\mathbb{R}$. Se, por outro lado, considerarmos o ideal $I = \langle xy - 1 \rangle$, então $V(I)$ representa uma hipérbole em $A^2_{\mathbb{R}}$.

Proposição 8. Seja A^n_k um espaço afim qualquer, então são satisfeitas as seguintes propriedades:

1. Os conjuntos $\varnothing$ e A^n_K são variedades algébricas;
2. Seja $I \subseteq J \subset K[x_1, \ldots, x_n]$, então $\mathcal{V}(J) \subseteq \mathcal{V}(I)$;
3. Sejam $I, J \subseteq K[x_1, \ldots, x_n]$ então $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$.

Demonstração. Queremos mostrar que os 3 itens acima são verdadeiros. Para verificar que $\varnothing$ é uma variedade, precisamos encontrar um ideal em $k[x_1, \ldots, x_n]$ tal que $\mathcal{V}(I) = \varnothing$. Considere então $I = \langle 1 \rangle$, note que nenhum ponto no espaço afim pode zerar qualquer polinômio constante. Logo, $\mathcal{V}(I) = \varnothing$. Analogamente, para mostrar que A^n_k é um variedade, considere $J = \langle 0 \rangle$, note que qualquer ponto no espaço afim zera o polinômio identicamente. Portanto, $\mathcal{V}(J) = A^n_K$.

Por definição, temos que $\mathcal{V}(J) = \{(a_1, \ldots, a_n) \in A^n_K \mid f(a_1, \ldots, a_n) = 0 \ \forall \ f \in J\}$. Assim, tomando $P \in \mathcal{V}(J)$, temos que $f(P) = 0$ para todo $f \in J$. Como $I \subseteq J$, em particular $f(P) = 0$ para todo $f \in I$. Portanto, todo ponto de $\mathcal{V}(J)$ é também zero de todos os polinômios de I, ou seja, $\mathcal{V}(J) \subseteq \mathcal{V}(I)$.

Observe agora que $I \cap J \subseteq I$, tal como $I \cap J \subseteq J$. Isso significa que $\mathcal{V}(I) \subseteq \mathcal{V}(I \cap J)$ e, analogamente, que $\mathcal{V}(J) \subseteq \mathcal{V}(I \cap J)$. Assim, $\mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(I \cap J)$. Reciprocamente, tome $P \in \mathcal{V}(I \cap J)$. Se $P \notin \mathcal{V}(I)$, então existe um polinômio $f \in I$ tal que $f(P) \neq 0$. Para todo $g \in J$, temos que $h = f \cdot g \in I \cap J$, e portanto $h(P) = f(P)g(P) = 0$. Como $f(P) \neq 0$, segue que $g(P) = 0$ para todo $g \in J$, o que implica que $P \in \mathcal{V}(J)$. Logo, $\mathcal{V}(I \cap J) \subseteq \mathcal{V}(I) \cup \mathcal{V}(J)$.

□

Diante desses resultados, vamos centrar nosso estudo em como determinar o conjunto solução de um sistema como o da **Definição 4.2**. Observe que, para o caso em que f_i da **Definição 4.2** é de grau total igual a 1, conseguimos, por métodos clássicos, a parametrização do sistema.

4.1.1 Solução de um sistema de equações

No seção anterior, estabelecemos algumas condições para determinar um conjunto gerador de Gröbner de um ideal $I \subseteq K[x_1, \ldots, x_n]$. Nessa seção, vamos mostrar como podemos usar essas bases para resolver um sistema de equações polinomiais em várias variáveis. De forma grosseira, nosso objetivo é transformar um sistema dado de equações em várias variáveis em outro sistema equivalente, composto por equações com menos variáveis.

Para isso, precisamos entender que resolver um sistema com m equações

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0 \tag{46}$$

com $f_i \in K[x_1, \ldots, x_n]$ para $i = 1, \ldots, m$.

Uma solução para o sistema (46) é uma n-úpla $(a_1, \ldots, a_n) \in K^n$ tal que $f_i(a_1, \ldots, a_n) = 0$ para todo $i = 1, \ldots, m$.

Ao sistema (46) associamos o ideal $I = \langle f_1, \ldots, f_m \rangle$. Estamos interessados em responder as questão: O sistema adimite soluções, ou seja, $\mathcal{V}(I) \neq \varnothing$? Note que estudar uma solução de um sistema de equações é, na verdade, entender a variedade algébrica $\mathcal{V}(I)$.

Teorema 11. *(Teorema dos Zeros de Hilbert-Versão Fraca)* Seja K um corpo algebricamente fechado, temos $\mathcal{V}(I) \neq \varnothing$ para qualquer $I \subsetneq K[x_1, \ldots, x_n]$.

Como nosso objetivo, em relação ao Teorema dos Zeros de Hilbert acima, é apenas discutir quando um sistema tem solução, não iremos prová-lo. Para um aprofundamento em um dos teoremas mais clássicos da Geometria Algébrica, indicamos ao leitor sua demonstração em (HERNANDES, 2023).

Assim, um sistema terá solução quando $I \neq K[x_1, \ldots, x_n]$, ou seja $1 \notin I$.

Exemplo 34. Vamos resolver, em $\mathbb{C}^2$ o sistema de equações

$$\begin{cases} x^2 + 2y^2 = 3 \\ x^2 + xy + y^2 = 3 \end{cases} \tag{47}$$

Inicialmente, vamos considerar o ideal

$$I = \langle x^2 + 2y^2 - 3, x^2 + xy + y^2 - 3 \rangle.$$

Notemos que a solucão do sistema acima é simplesmente o conjunto de $\mathcal{V}(I)$. Pela **proposição 7**, sabemos que podemos determinar $\mathcal{V}(I)$ usando qualquer conjunto gerador de I, em particular, uma base de Gröbner. Considere $F = \{f_1 = x^2 + 2y^2 - 3, f_2 = x^2 + xy + y^2 - 3\}$ e usando o Algoritmo de Buchberger, vamos determinar uma base de Gröbner para I.

Para isso, fixemos a ordem lexicográfica. Observe que multigrau(f_1) = multigrau(f_2) = $(2, 0)$. Então,

$$S(f_1, f_2) = \frac{x^2}{x^2}(x^2 + 2y^2 - 3) - \frac{x^2}{x^2}(x^2 + xy + y^2 - 3) = -xy + y^2$$

e consequentemente, $\overline{S(f_1, f_2)}^F = -xy + y^2 \neq 0$. Adicionando então o polinômio $f_3 = -xy + y^2$ a F. Continuando a usar o Algoritmo de Buchberger, temos que

$$S(f_1, f_3) = \frac{x^2 y}{x^2}(x^2 + 2y^2 - 3) - \frac{x^2 y}{-xy}(-xy + y^2) = xy^2 + 2y^3 - 3y$$

onde $\overline{S(f_1, f_3)}^F = 3y^3 - 3y \neq 0$, ou seja, devemos adicionar $f_4 = 3y^3 - 3y$ a F. Efetuando os cálculos

$$S(f_1, f_4) = \frac{x^2y^3}{x^2}(x^2 + 2y^2 - 3) - \frac{x^2y^3}{3y^3}(3y^3 - 3y) = x^2y + 2y^5 - 3y^3$$

donde ao dividir $S(f_1, f_4)$ por F, temos que $\overline{S(f_1, f_4)}^F = 0$. Além disso,

$$S(f_2, f_3) = \frac{x^2y}{x^2}(x^2 + xy + y^2 - 3) - \frac{x^2y}{-xy}(-xy + y^2) = 2xy^2 + y^3 - 3y$$

onde $\overline{S(f_2, f_3)}^F = 0$, analogamente

$$S(f_2, f_4) = \frac{x^2y^3}{x^2}(x^2 + xy + y^2 - 3) - \frac{x^2y^3}{3y^3}(3y^3 - 3y) = x^2y + xy^4 + y^5 - 3y^3$$

novamente, $\overline{S(f_2, f_4)}^F = 0$. Por último,

$$S(f_3, f_4) = \frac{xy^3}{-xy}(-xy + y^2) - \frac{xy^3}{3y^3}(3y^3 - 3y) = xy - y^4.$$

Com o último cálculo, chegamos que $\overline{S(f_1, f_4)}^F = \overline{S(f_2, f_3)}^F = \overline{S(f_2, f_4)}^F = \overline{S(f_3, f_4)}^F = 0$. O que mostra que $F = \{f_1, f_2, f_3, f_4\}$ é uma base de Gröbner para I. Dessse modo, segue que o sistema (47) e o sistema

$$\begin{cases} f_1 = x^2 + 2y^2 - 3 = 0 \\ f_2 = x^2 + xy + y^2 - 3 \\ f_3 = -xy + y^2 = 0 \\ f_4 = 3y^3 - 3y \end{cases}$$

são equivalentes, ou seja, têm o mesmo conjunto solução. De $f_4 = 0$ temos

$$3y^3 - 3y = 0 \implies y(y^2 - 1) = 0$$

donde concluímos que os possíveis valores de y são -1, 0 ou 1. Substituindo esses valores nas outras equações do novo sistema, obtemos os pares (x, y) que são soluções, isto é

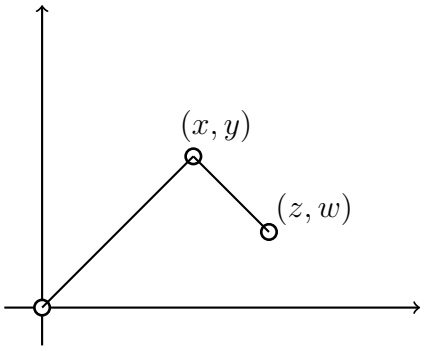
$$(-\sqrt{3}, 0), (\sqrt{3}, 0), (1, 1), (-1, -1).$$

Observe que a ideia básica para resolução do sistema consiste em duas etapas: **Etapa um:** Buscar um gerador f_i onde figure apenas uma variável (no exemplo anterior $f_4 = 3y^3 - 3y$). **Etapa dois:** Uma vez encontradas as raízes da equação mais simples $f_i = 0$, extendemos estas soluções para a solução do sistema original.

4.2 BRAÇO MECÂNICO

Estudar conjuntos de soluções de sistemas de equações polinomiais é algo interessante, tanto do ponto de vista aplicado quanto do ponto de vista teórico. Dentre outras possibilidades, podemos considerar uma aplicação do Teorema dos Zeros de Hilbert, que busca relacionar conjuntos de pontos em K^n com polinômios em $k[x_1, \ldots, x_n]$. Em outras palavras, o teorema estabelece uma conexão entre duas áreas da álgebra abstrata: os conjuntos algébricos e os geométricos. Entretanto, nosso objetivo aqui é apresentar aplicações da base teórica que foi exposta até o momento.

Apresentamos um modelo simples de braço mecânico composto por duas hastes de comprimento 1 e 2



A configuração do braço é completamente determinada pelas coordenadas (x, y) e (z, w), como mostra a figura. Assim, se quisermos determinar todas as configurações possíveis para esse braço mecânico, devemos determinar o conjunto solução do seguinte sistema.

$$\begin{cases} x^2 + y^2 = 4 \\ (x - z)^2 + (y - w)^2 = 1 \end{cases}$$

A resolução de sistemas como o apresentado acima evidencia a relevância da correspondência entre ideais e variedades algébricas. Por meio da interpretação geométrica dos conjuntos de zeros de polinômios, é possível descrever todas as posições assumidas pelo braço mecânico, o que ilustra de forma concreta a aplicação da teoria algébrica desenvolvida. Assim, o estudo das soluções polinomiais, mediado pelo Teorema dos Zeros de Hilbert, permite transitar entre o campo algébrico e o geométrico, mostrando como resultados teóricos abstratos podem ser utilizados para modelar e compreender fenômenos reais.

4.3 CONTROLE DE TRÁFEGO FERROVIÁRIO

Uma malha ferroviária é um sistema de transporte composto por trilhos, trens e estações, que interliga diferentes regiões por meio de linhas férreas. Essa infraestrutura é

fundamental para o transporte de cargas e passageiros, contribuindo para a mobilidade e o desenvolvimento econômico de um país. No Brasil, existem cerca de trinta mil quilômetros de malha ferroviária. Nosso objetivo aqui é controlar uma malha ferroviária dada; isto é, usando as bases de Gröbner, iremos determinar se um trem pode partir de um ponto e chegar em outro. Por "controlar", queremos dizer que podemos verificar se um trem pode se locomover de forma segura, ou seja, sem colidir e chegando a um ponto sem passar por sinais vermelhos.

Cada trecho da ferrovia será denominado setor, onde cada setor estará entre semáforos ou desvios. Observe a situação 1.

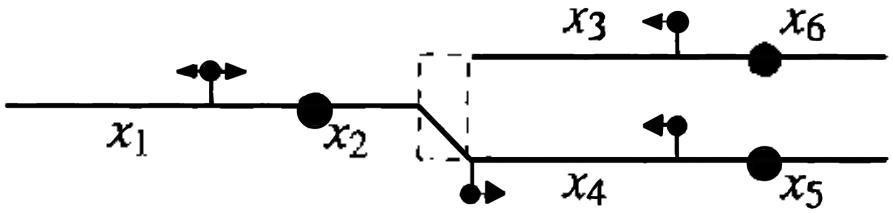
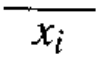


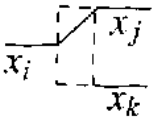
Figura 2 – Situação 1

em que devemos destacar os seguintes pontos

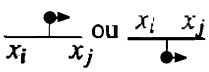


Indica que o setor x_i da ferrovia não está ocupado por um trem.

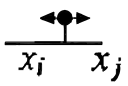
Indica que o setor x_i da ferrovia que está ocupado por um trem.



Indica um desvio ativo do setor x_i para o setor x_j e de x_j para x_i, mas inativo para o setor x_k.



Indica um semáforo controlando o deslocamento do setor x_i para o setor x_j com passagem proibida.



Indica um semáforo controlando o deslocamento do setor x_i para o setor x_j e o deslocamento do setor x_j para o setor x_i com passagem proibida em ambas as direções.

Uma observação muito importante, é que de um setor para o outro vale a transitividade, isso significa, que se é permitido o movimento, sem colisão, desvio inativo ou semáforos do setor x_i para o setor x_j, tal como do setor x_j para o setor x_k então podemos ir do setor x_i para o setor x_k sem problemas. Apesar de ser uma informação bastante trivial, percebemos que um trem pode ir do setro x_i para o setor x_j a menos que alguma das condições acorra:

I. Há um desvio inativo do setor x_i para o setor x_j;

II. Há um semáforo entre os setores x_i e x_j que proíbe tal passagem

Observe que a condição II acima, se o semáforo controla apenas o setor x_j para x_i então o movimento de x_i para x_j está permitido. Podemos observar que na Situação 1, os trens que ocupam os setores x_2, x_5 e x_6 estão em posições seguras, isto é, sem risco de colisão ou sem ultrapssar sinais vermelhos. No entanto, vamos apresentar a Situação 2 a seguir onde isso não ocorre

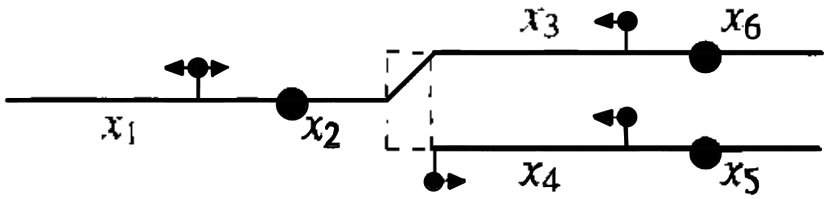


Figura 3 – Situação 2

Observe que existe uma situação perigosa com possível colisão no setor x_6, já que o trem que está no setor x_2 pode se movimentar até o setor x_6 (onde temos um trem) sem impedimentos. Com essas informações, vamos utilizar ferramentas algébricas para modelar o problema de locomoção de uma locomotiva em uma malha ferroviária M.

Vamos identificar cada trem por um número natural $\alpha \neq 0$; vamos usar o polinômio $x_i - \alpha$ para indicar que o trem α está localizado no setor x_i. Pode acontecer de um trem ter um número elevado de vagões e eventualmente ocupar dois setores distintos; ou seja, podemos considerar $x_i - \alpha$ e $x_j - \alpha$. Um ponto importante é que considerar $x_i - \alpha$ e $x_i - \beta$ com $\alpha \neq \beta$ representa uma situação preocupante, pois indica que dois trens distintos ocupam um mesmo setor, que, por sua vez, pode ocasionar uma colisão.

O fato de que é possível deslocar-se do setor x_i para um setor consecutivo x_j será indicado pelo polinômio $x_i(x_i - x_j)$. Analogamente, se tivermos a possibilidade de locomoção em ambas as direções, vamos considerar $x_j(x_j - x_i)$ para indicar que podemos ir de x_j para x_i.

Para nossa malha a seguir, vamos considerar que os trens ocupam apenas um setor e que os semáforos são usados apenas para controlar passagens de um setor para o outro em pontos da ferrovia onde há um desvio.

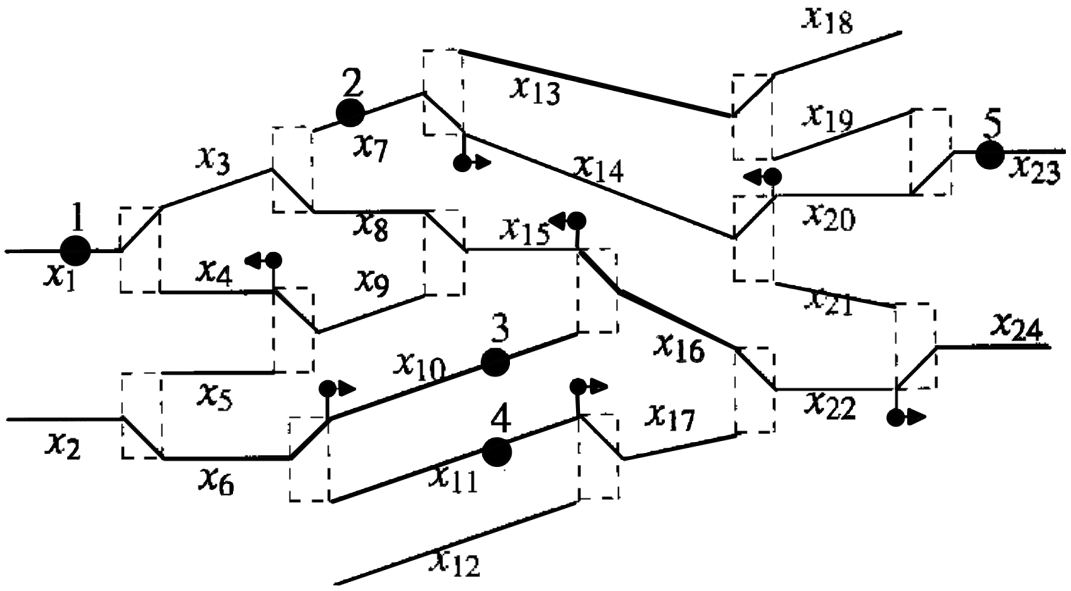


Figura 4 – Malha Ferroviária M

Vamos agrupar os polinômios nos seguintes conjuntos

$T = \{\ x_i - \alpha : \quad \text{o trem indicado por } \alpha \in \mathbb{N} \text{ está no setor } x_i\}\,;$

$L = \left\{\ x_i(x_i - x_j),\ x_j(x_j - x_i) : \text{ há um desvio ativo entre } x_i \text{ e } x_j\right\};$

$S = \left\{\ x_i(x_i - x_j) : \text{ há um semáforo que proíbe o deslocamento do setor } x_i \text{ para } x_j\right\}.$

Vamos definir o conjunto de todos os polinômios que representam a acessibilidade de um setor a outro como $H = L - S$. Portanto, considerando a Malha M definida acima, temos que o conjunto **T** é o conjunto dos polinômios

$$T = \{x_1 - 1, x_7 - 2, x_{10} - 3, x_{11} - 4, x_{23} - 5\}\,.$$

O conjunto **L** é o conjunto com os polinômios:

- $x_1(x_1 - x_3)$
- $x_2(x_2 - x_6)$
- $x_3(x_3 - x_8)$
- $x_4(x_4 - x_9)$
- $x_6(x_6 - x_{10})$
- $x_7(x_7 - x_{14})$
- $x_8(x_8 - x_{15})$
- $x_{11}(x_{11} - x_{17})$
- $x_{13}(x_{13} - x_{18})$
- $x_{14}(x_{14} - x_{20})$
- $x_{15}(x_{15} - x_{16})$
- $x_{16}(x_{16} - x_{22})$
- $x_{20}(x_{20} - x_{23})$
- $x_{22}(x_{22} - x_{24})$
- $x_3(x_3 - x_1)$
- $x_6(x_6 - x_2)$
- $x_8(x_8 - x_3)$
- $x_9(x_9 - x_4)$
- $x_{10}(x_{10} - x_6)$
- $x_{14}(x_{14} - x_7)$
- $x_{15}(x_{15} - x_8)$
- $x_{17}(x_{17} - x_{11})$
- $x_{18}(x_{18} - x_{13})$
- $x_{20}(x_{20} - x_{14})$
- $x_{16}(x_{16} - x_{15})$
- $x_{22}(x_{22} - x_{16})$
- $x_{23}(x_{23} - x_{20})$
- $x_{24}(x_{24} - x_{22})$

O conjunto **S** é o conjunto que tem os seguintes polinômios

- $x_6(x_6 - x_{10})$
- $x_7(x_7 - x_{14})$
- $x_9(x_9 - x_4)$
- $x_{11}(x_{11} - x_{17})$
- $x_{16}(x_{16} - x_{15})$
- $x_{20}(x_{20} - x_{14})$
- $x_{22}(x_{22} - x_{24})$

E finalmente, o conjunto **H** com os polinômios:

- $x_1(x_1 - x_3)$
- $x_3(x_3 - x_1)$
- $x_{10}(x_{10} - x_6)$
- $x_2(x_2 - x_6)$
- $x_6(x_6 - x_2)$
- $x_{14}(x_{14} - x_7)$
- $x_3(x_3 - x_8)$
- $x_8(x_8 - x_3)$
- $x_4(x_4 - x_9)$
- $x_8(x_8 - x_{15})$
- $x_{15}(x_{15} - x_8)$
- $x_{17}(x_{17} - x_{11})$
- $x_{13}(x_{13} - x_{18})$
- $x_{18}(x_{18} - x_{13})$
- $x_{15}(x_{15} - x_{16})$
- $x_{16}(x_{16} - x_{22})$
- $x_{22}(x_{22} - x_{16})$
- $x_{14}(x_{14} - x_{20})$
- $x_{20}(x_{20} - x_{23})$
- $x_{23}(x_{23} - x_{20})$
- $x_{24}(x_{24} - x_{22})$

Proposição 9. O trem α localizado no setor x_i pode se deslocar para o setor x_j se, e somente se

$$x_j - \alpha \in I := \langle H \rangle + \langle x_i - \alpha \rangle.$$

em que $\langle H \rangle$ denota o ideal gerado por H em $\mathbb{Q}[x_1, \ldots, x_n]$

Demonstração. De fato, suponha que o trem α localizado no setor x_i pode se deslocar para o setor x_j. Assim, usando a transitividade da movimentação na malha, podemos nos ater ao caso em que x_i e x_j são setores consecutivos. Note que o trem pode se deslocar de x_i para x_j se, e somente se $x_i(x_i - x_j) \in H$. Temos assim que se, o deslocamento de x_i para x_j é possível então $x_i(x_i - x_j), x_i - \alpha \in I$ e consequentemente temos:

$$\frac{1}{\alpha}(x_i - x_j + \alpha)(x_i - \alpha) - \frac{1}{\alpha}[x_i(x_i - x_j)] \in I.$$

Desenvolvendo a equação acima, temos

$$\frac{x_i^2}{\alpha} - \frac{x_j x_i}{\alpha} + \frac{x_i \alpha}{\alpha} - \frac{x_i \alpha}{\alpha} + \frac{x_j \alpha}{\alpha} - \frac{\alpha^2}{\alpha} - \frac{x_i^2}{\alpha} + \frac{x_j x_i}{\alpha} = x_j - \alpha.$$

Ou seja, $x_j - \alpha \in I$

Por outro lado, se $x_j - \alpha \in I$, então

$$x_i(x_i - x_j) = (x_i - x_j + \alpha)(x_i - \alpha) - \alpha(x_j - \alpha) \in \langle H \rangle + \langle x_i - \alpha \rangle.$$

Como x_i e x_j são setores consecutivos, devemos ter obrigatoriamente que $x_i(x_i - x_j) \in H$, e desse modo, podemos concluir que o trem α pode se deslocar de x_i para x_j. □

Como foco da nossa aplicação é mostrar que um trem pode ir de um setor x_i ao setor x_k sem problemas, vamos mostrar que o trem 1, localizado no setor x_1 pode acessar o setor x_{16}. Para isso, de acordo com (HERNANDES, 2023) determinamos a seguinte base de Gröbner G para o ideal $\langle H\rangle + \langle x_1 - 1\rangle$. Utilizando a ordem lexicográfica graduada, obtemos

$$G = \begin{Bmatrix} x_1 - 1, & x_2^2 - x_2x_6, & x_2x_6 - x_6^2, & x_2x_{10}^2 - x_6^2x_{10}, & x_2 - x_8^2, \\ x_4^2 - x_4x_9, & x_6x_{10} - x_{10}^2, & x_7x_{14} - x_{14}^2, & x_8 - x_{15}^2, & x_{11}x_{17} - x_{17}^2, \\ x_{13}^2 - x_{13}x_{18}, & x_{13}x_{18} - x_{18}^2, & x_{14}^2 - x_{14}x_{20}, & x_{15} - x_{22}, & \\ x_{16} - x_{22}, & x_{20}^2 - x_{20}x_{23}, & x_{20}x_{23} - x_{23}, & x_{22} - 1, & x_{24}^2 - x_{24} \end{Bmatrix}.$$

Usando o **Teorema 5** podemos dividir $x_{16} - 1$ por G, nesse caso, temos

$$x_{16} - 1 = 1(x_{16} - x_{22}) + 1(x_{22} - 1)$$

Assim, $x_{16} - 1 \in G \subseteq \langle H\rangle + \langle x_1 - 1\rangle$, temos que o trem 1 que ocupa o setor x_1 pode se deslocar até o setor x_{16} com as configurações de desvios e semáforos.

Por outro lado, o trem 1 que ocupa a posição x_1 não pode acessar o setor x_{24}. Claramente podemos ver tal fato ao observarmos a Malha Ferroviária, podemos constatar que $x_{24} - 1 \notin G \subseteq \langle H\rangle + \langle x_1 - 1\rangle$, já que o resto da divisão de $x_{24} - 1$ por todos os elementos de G não é nulo.

4.4 O PROBLEMA DAS 4 CORES DE GUTHRIE

Em 1852, logo após ter concluído seus estudos no University College, em Londres, o jovem matemático *Francis Guthrie*, enquanto coloria um mapa, tomava cuidado para não colorir com a mesma cor países vizinhos que tivessem alguma linha de fronteira comum. Notou então que apenas quatro cores bastariam para colorir.

Recém-formado, Guthrie tentou provar, usando argumentos matemáticos, que apenas quatro cores seriam suficientes para colorir qualquer mapa. Pensando nisso, o jovem apresentou o problema para seu professor De Morgan, que, por sua vez, argumentou que, em qualquer mapa, não existiam cinco países tais que cada um tivesse fronteira com os outros quatro; ou seja, em cada agrupamento de cinco países, ao menos dois deles não são vizinhos.

De Morgan passou o problema para seus alunos e colegas da universidade. Depois de 26 anos, o problema formulado por Guthrie foi divulgado pela London Mathematical Society. O problema ganhou relevância e foi supostamente resolvido por Arthur Cayley.

Apesar de diversas tentativas feitas por renomados matemáticos, o problema proposto por Guthrie ficou em aberto por 120 anos, até que, em 1976, com ajuda computacional, Kenneth Appel e Wolfgang Haken apresentaram uma prova para o teorema das quatro cores; entretanto, foram necessárias mais de mil horas de uso de computadores potentes para resolver o problema.

Desse modo, muitos matemáticos continuaram a buscar uma prova mais simples. Apenas em 1994, depois de 142 anos, Paul D. Seymour apresentou uma prova que reduzia a quantidade de cálculos a níveis bastante aceitáveis para o problema de Guthrie, mas sem dispensar o uso computacional.

Como observado por Guthrie, podemos colorir um mapa com quatro cores. Entretanto, sob quais condições podemos colorir um mapa com apenas três cores? Nessa seção, apresentaremos como essa questão pode ser formulada por meio de equações polinomiais, que, por sua vez, podem ser respondidas usando ferramentas da base de Gröbner.

4.5 PROBLEMA DE COLORAÇÃO DE MAPAS

O problema de coloração de mapas é um dos temas mais clássicos e fascinantes da Matemática Discreta e da Teoria dos Grafos. Em termos gerais, consiste em determinar o menor número de cores necessárias para colorir as regiões de um mapa de modo que regiões adjacentes (ou seja, que compartilham uma fronteira comum) recebam cores distintas. Esse tipo de problema, inicialmente proposto de forma intuitiva no século XIX, tornou-se um importante campo de estudo por sua relevância tanto teórica quanto prática.

4.5.1 O Problema de Coloração do Nordeste

Queremos usar três cores para colorir o mapa. Com o intuito de "algebrizar"o problema, vamos representar cada cor por uma raiz cúbica da unidade; ou seja, cada cor será uma raiz do polinômio $f = x^3 - 1$, e cada região será representada por uma incógnita x_i, que, por sua vez, pode assumir apenas um desses três valores (cores) possíveis. Então, temos que $x_i^3 - 1 = 0$ para todo $i = 1, \ldots, n$, onde n representa o número de regiões do mapa.

É importante observar que duas regiões vizinhas não podem ter a mesma cor. Como duas regiões vizinhas x_i e x_j são raízes da unidade, temos

$$x_i^3 - 1 = 0 \quad \text{e} \quad x_j^3 - 1 = 0$$

ou seja, $x_i^3 = x_j^3$. Logo,

$$x_i^3 - x_j^3 = (x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0.$$

Como $x_i \neq x_j$ (pois são regiões vizinhas), temos

$$x_i^2 + x_i x_j + x_j^2 = 0$$

Assim, o problema de coloração de mapas usando três cores se resume a obter as soluções do seguinte sistema de equações polinômiais

$$\begin{cases} x_i^3 - 1 = 0, & \text{para } 1 \leq i \leq n; \\ x_i^2 + x_i x_j + x_j^2 = 0, & \text{sempre que } x_i \text{ e } x_j \text{ forem regiões vizinhas.} \end{cases}$$

O Teorema Fundamental da Álgebra assegura que todo polinômio não constante $f \in \mathbb{C}[x]$ adimite $\mathrm{gr}(f)$ raízes, onde em alguns casos acontece a repetição de raízes. Assim, o polinômio $f = x^n - 1$ adimite n raízes que denotaremos por $\omega_0, \ldots, \omega_{n-1} \in \mathbb{C}$ e chamamos cada ω_i com $i = 0, \ldots n-1$ de *raíz n-ésimas da unidade.*

As raízes n-ésimas da unidade são distintas e são precisamenteos elementos do conjunto

$$\mathcal{V}(\langle x^n - 1\rangle) = \left\{\omega_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right); k = 0, \ldots, n-1\right\}.$$

Essa informação será importante para resolver a equação $x_i^3 - 1 = 0$. Observemos agora o mapa da região do nordeste do Brasil. Considerando duas possibilidades

Figura 5 – Mapa do Nordeste brasileiro

A cada um dos nove estados que compõem esta região, vamos atribuir uma variável de $\mathbb{C}[x_1, \ldots, x_9]$. Defina, sem perda de generalidade que

x_1 :=Maranhão	x_2 := Piauí	x_3 :=Ceará
x_4 :=Rio G. do Norte	x_5 := Paraíba	x_6 := Pernambuco
x_7 :=Alagoas	x_8 := Sergipe	x_9 :=Bahia

Tabela 1 – Estados da Região Nordeste do Brasil

Mapa do Nordeste com $x_i, i = 1, \ldots, 9$

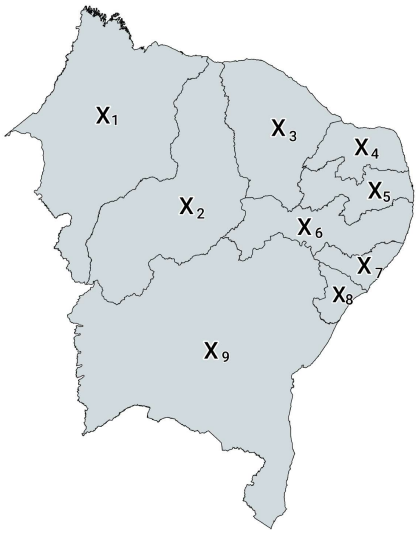


Figura 6 – Estados do nordeste representados por variáveis x_i com $i = 1, \ldots, 9$

Determinar se é possível colorir o mapa acima com apenas três cores é o mesmo que determinar as soluções, se existirem, do seguinte sistema de equações polinomiais.

- $x_1^3 - 1 = 0$
- $x_2^3 - 1 = 0$
- $x_3^3 - 1 = 0$
- $x_4^3 - 1 = 0$
- $x_5^3 - 1 = 0$
- $x_6^3 - 1 = 0$
- $x_7^3 - 1 = 0$
- $x_8^3 - 1 = 0$
- $x_9^3 - 1 = 0$
- $x_1^2 + x_1x_2 + x_2^2 = 0$
- $x_2^2 + x_2x_6 + x_6^2 = 0$
- $x_3^2 + x_3x_4 + x_4^2 = 0$
- $x_3^2 + x_3x_6 + x_6^2 = 0$
- $x_5^2 + x_5x_6 + x_6^2 = 0$
- $x_6^2 + x_6x_9 + x_9^2 = 0$
- $x_7^2 + x_7x_8 + x_8^2 = 0$
- $x_7^2 + x_7x_9 + x_9^2 = 0$
- $x_8^2 + x_8x_9 + x_9^2 = 0$
- $x_2^2 + x_2x_3 + x_3^2 = 0$
- $x_2^2 + x_2x_9 + x_9^2 = 0$
- $x_3^2 + x_3x_5 + x_5^2 = 0$
- $x_4^2 + x_4x_5 + x_5^2 = 0$
- $x_6^2 + x_6x_7 + x_7^2 = 0$

Para isso, vamos determinar inicialmente uma base de Gröbner G para o ideal I cujos geradores são os polinômios que compõem o sistema de equações acima. Para isso, vamos usar o Algoritmo de Buchberger, visto no cápitulo anterior. Devido ao número elevado de operações, utilizaremos o software *Macaulay 2* com o seguinte *script*: *script*:

```
Macaulay2, version 1.25.06-1650-ga4e0c130e7-dirty (vanilla)
Type help to see useful commands

i1 : R = QQ[x1,x2,x3,x4,x5,x6,x7,x8,x9, MonomialOrder => GRevLex];

i2 :
```

```
I = ideal(
x1^3 - 1,
x1^2 + x1*x2 + x2^2,
x5^2 + x5*x6 + x6^2,
x2^3 - 1,
x2^2 + x2*x6 + x6^2,
x6^2 + x6*x7 + x7^2,
x3^3 - 1,
x3^2 + x3*x6 + x6^2,
x7^2 + x7*x8 + x8^2,
x4^3 - 1,
x3^2 + x3*x4 + x4^2,
x7^2 + x7*x9 + x9^2,
x5^3 - 1,
x6^2 + x6*x9 + x9^2,
x2^2 + x2*x3 + x3^2,
x6^3 - 1,
x2^2 + x2*x9 + x9^2,
x3^2 + x3*x5 + x5^2,
x7^3 - 1,
x4^2 + x4*x5 + x5^2,
x8^2 + x8*x9 + x9^2,
);
```

```
o2 : Ideal of R
```

```
i3 : G = gb I;
```

Assim, com ordenação lexicográfica, uma base de Gröbner para o ideal I é o conjunto G tal que

$$G = \begin{Bmatrix} x_9^3 - 1,\ x_8^2 + x_8x_9 + x_9^2,\ x_7 + x_8 + x_9,\ x_6 - x_8,\ x_5 + x_8 + x_9, \\ x_4 - x_8,\ x_3 - x_9,\ x_2 + x_8 + x_9,\ x_1^2 - x_1x_8 - x_1x_9 + x_8x_9 \end{Bmatrix}$$

Desse modo, o sistema inicial é equivalente ao seguinte sistema

$$\begin{cases} x_9^3 - 1 = 0 \\ x_8^2 + x_8x_9 + x_9^2 = 0 \\ x_7 + x_8 + x_9 = 0 \\ x_6 - x_8 = 0 \\ x_5 + x_8 + x_9 = 0 \\ x_4 - x_8 = 0 \\ x_3 - x_9 = 0 \\ x_2 + x_8 + x_9 = 0 \\ x_1^2 - x_1x_8 - x_1x_9 + x_8x_9 = 0 \end{cases} \tag{48}$$

Denotando por $1, \omega, \omega^2$ como as raízes cúbicas da unidade, note que $1 + \omega + \omega^2 = 0$ onde as três raízes são distintas. De fato pois $z^3 - 1 = 0$, temos

$$1, \quad \omega = \left[\cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)\right] \quad \text{e} \quad \omega^2 = \left[\cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right)\right]$$

ou seja, as raízes cúbicas da unidade são $1, \omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ e $\omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, onde segue que

$$1 + \omega + \omega^2 = 0. \tag{49}$$

Note que cada variável do sistema de equações polinomiais (48) é uma raiz cúbica da unidade, e cada uma destas raízes está associada a uma cor que irá colorir o mapa.

Vamos agora determinar a solução do sistema (48). Para começar, observe que a equação $x_9^3 - 1 = 0$ indica que podemos escolher qualquer raiz para x_9; digamos $x_9 = 1$. Como vimos, $x_8^2 + x_8x_9 + x_9^2$ indica que x_8 faz fronteira com x_9, ou seja, não podemos atribuir a cor 1 para x_8; por isso, vamos tomar $x_8 = \omega$.

Conforme visto em (49), a equação $x_7 + x_8 + x_9 = 0$ deve admitir soluções entre as raízes cúbicas complexas da unidade; ou seja, x_7, x_8 e x_9 devem assumir valores distintos, e portanto devemos atribuir a cor ω^2 para x_7. O mesmo pode ser observado nas equações $x_5 + x_8 + x_9 = 0$ e $x_2 + x_8 + x_9 = 0$. Assim, reservamos a cor ω^2 para x_2 e x_5.

As equações $x_6 - x_8 = 0$ e $x_4 - x_8 = 0$ nos informam que x_6 e x_4 têm a mesma cor que x_8, ou seja, ambas têm a cor ω. O mesmo fato ocorre em $x_3 - x_9 = 0$, donde 1 assume o valor de x_3.

Analisaremos agora a equação

$$0 = x_1^2 - x_1x_8 - x_1x_9 + x_8x_9 = (x_1 - x_8)(x_1 - x_9).$$

Note que temos as possibilidades $x_1 - x_8 = 0$ ou $x_1 - x_9 = 0$. Isso significa que, podemos colorir o estado x_1 com a cor de x_8 ou com a cor de x_9, ou seja, ω ou 1 respectivamente.

Baseado nas informações que destacamos no texto acima, vamos atribuir as seguintes cores para $1, \omega$ e ω^2:

$$1 := \text{Vermelho}, \ \omega := \text{Roxo} \ , \ \omega^2 := \text{Amarelo}$$

temos as seguintes colorações para o mapa da região do nordeste vamos ter dois casos possíveis

$$\begin{cases} x_1 = x_4 = x_6 = x_8 = \omega & \text{(Roxo)} \\ x_2 = x_5 = x_7 = \omega^2 & \text{(Amarelo)} \\ x_3 = x_9 = 1 & \text{(Vermelho)} \end{cases} \quad \text{ou} \quad \begin{cases} x_4 = x_6 = x_8 = \omega & \text{(Roxo)} \\ x_2 = x_5 = x_7 = \omega^2 & \text{(Amarelo)} \\ x_1 = x_3 = x_9 = 1 & \text{(Vermelho)} \end{cases}$$

Por fim, podemos apresentar os mapas coloridos conforme o sistema (48).

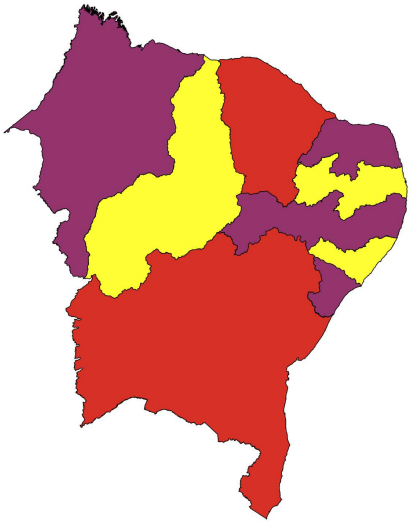


Figura 7 – Caso em que $x_8 = x_1$

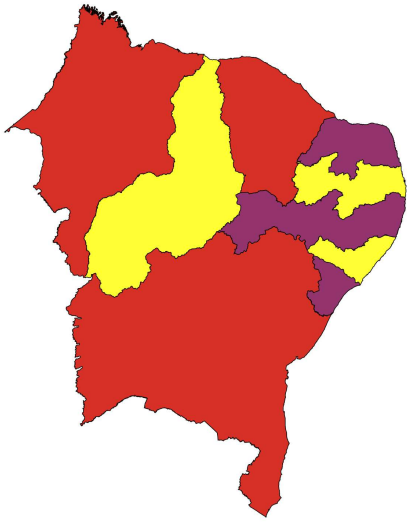


Figura 8 – Caso em que $x_9 = x_1$

4.5.2 Problema de Coloração de algumas ciadades do estado de Sergipe

Agora, vamos usar a mesma ideia para fazer a coloração de algumas cidades do estado de Sergipe. Vamos considerar nove cidades em uma região próxima, como podemos ver no mapa abaixo e tentar colorir o mapa com três cores. Isto é

$$\begin{cases} x_i^3 - 1 = 0, & \text{para } 1 \leq i \leq n; \\ x_i^2 + x_i x_j + x_j^2 = 0, & \text{sempre que } x_i \text{ e } x_j \text{ forem regiões vizinhas.} \end{cases}$$

Agora, vamos tentar usar as ferramentas no problema anterior para colorir as cidades a seguir

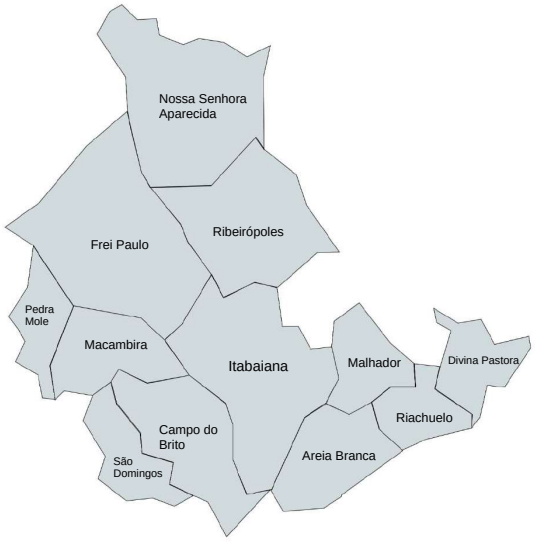


Figura 9 – Mapa das cidades situadas nas proximidades de Itabaiana

A cada uma das doze cidades que compõem esta região, vamos atribuir uma variável de $\mathbb{C}[x_1, \ldots, x_{12}]$. Defina, sem perda de generalidade que

x_1 :=Itabaiana	x_2 := Campo do Brito	x_3 :=São Domingos
x_4 :=Macambira	x_5 := Pedra Mole	x_6 :=Frei Paulo
x_7 :=Ribeirópoles	x_8 := Nossa Senhora Aparecida	x_9 :=Malhador
x_{10} :=Areira Branca	x_{11} := Riachuelo	x_{12} :=Divina Pastora

Tabela 2 – Cidades da área circunvizinha a Itabaiana

Assim, podemos representar nosso mapa da seguinte forma:

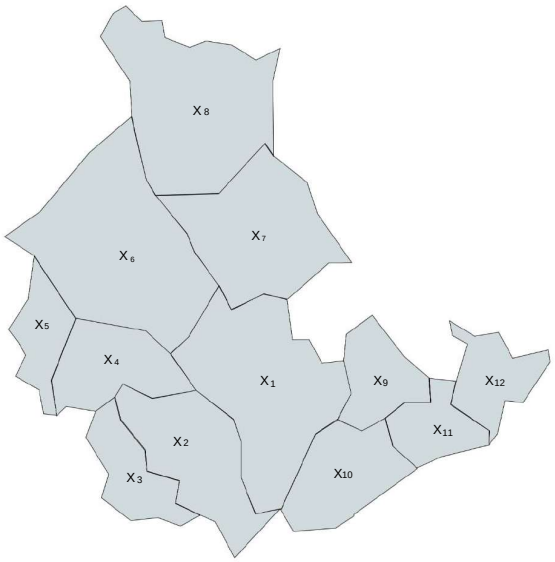


Figura 10 – Reigião circuvizinha a Itabaiana representadas com x_i com $i = 1, \ldots, 12$

Determinar se é possível colorir o mapa acima com apenas três cores é o mesmo que determinar as soluções, se existire, do seguinte sistema de equações polinomiais.

- $x_1^3 - 1 = 0$
- $x_2^3 - 1 = 0$
- $x_3^3 - 1 = 0$
- $x_4^3 - 1 = 0$
- $x_5^3 - 1 = 0$
- $x_6^3 - 1 = 0$
- $x_7^3 - 1 = 0$
- $x_8^3 - 1 = 0$
- $x_9^3 - 1 = 0$
- $x_{10}^3 - 1 = 0$
- $x_{11}^3 - 1 = 0$
- $x_{12}^3 - 1 = 0$
- $x_1^2 + x_1x_2 + x_2^2 = 0$
- $x_1^2 + x_1x_4 + x_4^2 = 0$
- $x_1^2 + x_1x_6 + x_6^2 = 0$
- $x_1^2 + x_1x_7 + x_7^2 = 0$
- $x_1^2 + x_1x_9 + x_9^2 = 0$
- $x_1^2 + x_1x_{10} + x_{10}^2 = 0$
- $x_2^2 + x_2x_3 + x_3^2 = 0$
- $x_2^2 + x_2x_4 + x_4^2 = 0$
- $x_2^2 + x_2x_{10} + x_{10}^2 = 0$
- $x_3^2 + x_3x_4 + x_4^2 = 0$
- $x_4^2 + x_4x_5 + x_5^2 = 0$
- $x_4^2 + x_4x_6 + x_6^2 = 0$
- $x_5^2 + x_5x_6 + x_6^2 = 0$
- $x_6^2 + x_6x_7 + x_7^2 = 0$
- $x_6^2 + x_6x_8 + x_8^2 = 0$
- $x_7^2 + x_7x_8 + x_8^2 = 0$
- $x_9^2 + x_9x_{10} + x_{10}^2 = 0$
- $x_9^2 + x_9x_{11} + x_{11}^2 = 0$
- $x_{10}^2 + x_{10}x_{11} + x_{11}^2 = 0$
- $x_{11}^2 + x_{11}x_{12} + x_{12}^2 = 0$

A seguir, usando o software *Macaulay 2* para determinar uma base de Gröbner F para o ideal J cujos geradores são os polinômios que compõem o sistema de equações acima. Para isso, vamos usar o seguinte *script*:

```
        Macaulay2, version 1.25.06-1650-ga4e0c130e7-dirty (vanilla)
Type help to see useful commands

        i1 : R = QQ[x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,x11,x12, MonomialOrder => GRevLex];
```

```
       i2 :
I = ideal(
x1^3 - 1,
x1^2 + x1*x2 + x2^2,
x5^2 + x5*x6 + x6^2,
x2^3 - 1,
x1^2 + x1*x4 + x4^2,
x6^2 + x6*x7 + x7^2,
x3^3 - 1,
x1^2 + x1*x6 + x6^2,
x6^2 + x6*x8 + x8^2,
x4^3 - 1,
x1^2 + x1*x7 + x7^2,
x7^2 + x7*x8 + x8^2,
x5^3 - 1,
x1^2 + x1*x9 + x9^2,
x9^2 + x9*x10 + x10^2,
x6^3 - 1,
x1^2 + x1*x10 + x10^2,
x9^2 + x9*x11 + x11^2,
x7^3 - 1,
x2^2 + x2*x3 + x3^2,
x10^2 + x10*x11 + x11^2,
x8^3 - 1,
x2^2 + x2*x4 + x4^2,
x11^2 + x11*x12 + x12^2,
x9^3 - 1,
x2^2 + x2*x10 + x10^2,
x10^3 - 1,
x3^2 + x3*x4 + x4^2,
x11^3 - 1,
x4^2 + x4*x5 + x5^2,
x12^3 - 1,
x4^2 + x4*x6 + x6^2
); o2 : Ideal of R i3 : G = gb I;
```

Assim, considerando a ordem lexicográfica, o conjunto F abaixo é uma base de Gröbner para o ideal J

$$F = \left\{ \begin{matrix} x_{12}^3 - 1,\ x_4 - x_{10}\ x_7 - x_{10},\ x_1 - x_{11},\ x_3 - x_{11},\ x_5 - x_{11},\ x_8 - x_{11},\ x_9 + x_{10} + x_{11}, \\ x_2 + x_{10} + x_{11},\ x_6 + x_{10} + x_{11},\ x_{11}^2 + x_{11}x_{12} + x_{12}^2,\ x_{10}^2 + x_{10}x_{11} - x_{11}x_{12} - x_{12}^2 \end{matrix} \right\}$$

Desse modo, o sistema citado anteriormente tem o conjunto solução os pontods de $\mathcal{V}(F)$. Em outras palavras, queremos determinar a solução do sistema a seguir

$$\begin{cases} x_{12}^3 - 1 = 0 \\ x_4 - x_{10} = 0 \\ x_7 - x_{10} = 0 \\ x_1 - x_{11} = 0 \\ x_3 - x_{11} = 0 \\ x_5 - x_{11} = 0 \\ x_8 - x_{11} = 0 \\ x_9 + x_{10} + x_{11} = 0 \\ x_2 + x_{10} + x_{11} = 0 \\ x_6 + x_{10} + x_{11} = 0 \\ x_{11}^2 + x_{11}x_{12} + x_{12}^2 = 0 \\ x_{10}^2 + x_{10}x_{11} - x_{11}x_{12} - x_{12}^2 = 0 \end{cases} \tag{50}$$

Novamente, vamos denotar ω, ω^2 e 1 como raízes cúbicas da unidade, onde por (49) sabemos que $\omega + \omega^2 + 1 = 0$. Assim, podemos fazer a seguinte anállise do sistema (50)

Como cada x_i com $i = 1, \ldots, 12$ são raízes cúbicas da unidade, notamos que $x_2 + x_{10} + x_{11} = 0$ por (49) temos que x_2, x_{10} e x_{11} assumem cores distintas, digamos $x_{11} = 1, x_2 = \omega^2$ e $x_{10} = \omega$. Por $x_9 + x_{10} + x_{11} = 0$ e $x_6 + x_{10} + x_{11} = 0$ temos que $x_2 = x_6 = x_9 = \omega^2$. Além disso, $x_1 = x_3 = x_5 = x_8 = x_{11} = 1$ e também $x_4 = x_7 = x_{10} = \omega$. Observe que na equação $x_{11}^2 + x_{11}x_{12} + x_{12}^2 = 0$ obtemos $x_{11} \neq x_{12}$, ou seja, $x_{12} \neq 1$, digamos então $x_{12} = \omega$. Logo, definindo

$$1 := \text{Vermelho},\ \omega := \text{Roxo}\ ,\ \omega^2 := \text{Amarelo}$$

temos as seguintes colorações para o mapa da região próxima a Itabaiana.

$$\begin{cases} x_{10} = x_{12} = x_4 = x_7 = \omega & \text{(Roxo)} \\ x_2 = x_6 = x_9 = \omega^2 & \text{(Amarelo)} \\ x_1 = x_{11} = x_8 = x_3 = x_5 = 1 & \text{(Vermelho)} \end{cases}$$

Que pode ser vista no mapa da seguinte forma:

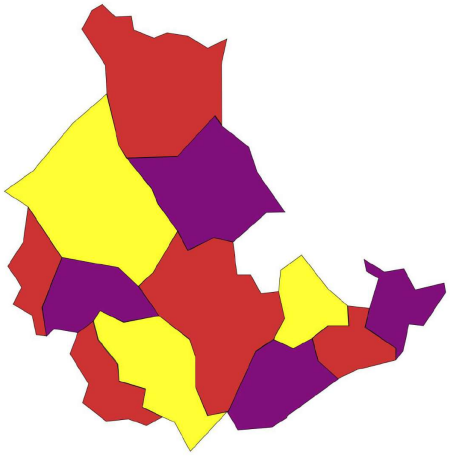


Figura 11 – Coloração da região próxima a Itabaiana

Para finalizar nosso trabalho, precisamos destacar algo que até agora não foi dito. O que acontece quando não conseguimos pintar o mapa com três cores? Como isso aparece em termos de equações polinomiais? No nosso mapa da região próxima a Itabaiana, vamos acrescentar o município de Moita Bonita, onde difiniremos $x_{13} :=$ Moita Bonita.

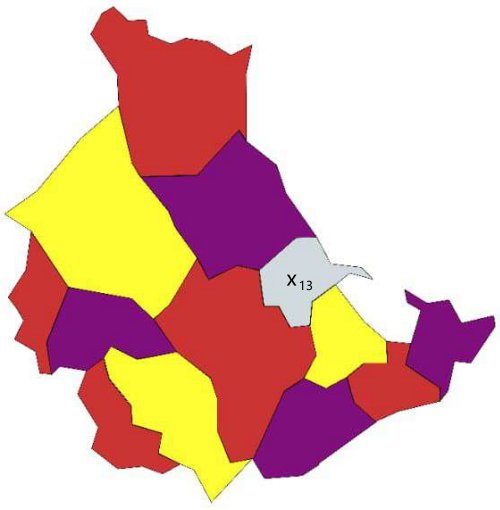


Figura 12 – Cidades circunvizinhas a Itabaiana acrescida com o município $x_{13} :=$ Moita Bonita

Com ajuda da tabela, podemos perceber que Moita Bonita faz fronteira com três cidades do mapa, são elas: Itabaiana, Ribeirópolis e Malhador. Em outras palavras, x_{13} faz fronteira com x_1, x_7 e x_9, respectivamente. Isso significa que, para encontrarmos nossa base de Gröbner, deveríamos acrescentar as quatro equações a seguir aos geradores do ideal J, junto com os geradores já mencionados anteriormente.

$$\begin{cases} x_{13}^3 - 1 = 0 \\ x_{13}^2 + x_{13}x_1 + x_1^2 = 0 \\ x_{13}^2 + x_{13}x_7 + x_7^2 = 0 \\ x_{13}^2 + x_{13}x_9 + x_9^2 = 0 \end{cases} \tag{51}$$

Com o auxílio do *Macauly 2*, ao efetuar os cálculos encontramos a seguinte resposta:

```
gens G
04:(1)
04:Matrix R^1 ← R^1
i5:
```

Isso significa que, quando definimos J como o ideal gerado por todos os polinômios citados anteriormente, unidos com os polinômios de (51), e buscamos uma base de Gröbner através do *software Macaulay2*, o polinômio 1 está na base de Gröbner do ideal J. Logo, pelo **Teorema 11**, o sistema não tem solução.

Portanto, quando adicionamos as equações referentes ao município de Moita Bonita, ou seja, as equações de (51), temos $\mathcal{V}(J) = \varnothing$. Logo, para colorir o mapa seriam necessárias mais de três cores.

Assim, chegamos ao fim de nossas observações sobre as aplicações da base de Gröbner na coloração de mapas. Vale destacar que algumas outras aplicações podem ser vistas em (HERNANDES, 2023). Dentre elas, destaca-se um método de resolução do puzzle *Sudoku*, através de ferramentas parecidas com as que apresentamos aqui.

REFERÊNCIAS

ARAUJO, Lauro César. **A classe abntex2**: Modelo canônico de trabalhos acadêmicos brasileiros compatível com as normas ABNT NBR 14724:2011, ABNT NBR 6024:2012 e outras. [*S.l.*], 2015. Disponível em: http://www.abntex.net.br/. Acesso em: 16 ago. 2019.

COELHO, Sabrina. **O Algoritmo da Divisão para Polinômios em Várias Variáveis**. 2018. Trabalho de Conclusão de Curso – Universidade Federal de Santa Catarina, Santa Catarina.

COX, D.;LITTLE, J.;O'SHEA, D.; **Ideals, Varieties, and Algorithims**. 3. ed. New York: Springer, 2007. P. 539.

GIANNEKAS, Minas. **MapChart – Create your own custom map**. Grécia: [*s.n.*], 2014. Acesso em: 15 de jul. 2025. Disponível em: https://www.mapchart.net/.

GONÇALVES, A. **Introdução à Algebra**. 5. ed. Rio de Janeiro: IMPA, 2007. P. 194.

HALMOS, Paul R. **Teoria Ingênua dos Conjuntos**. 1. ed. São Paulo: Edusp, 2001. P. 130.

HERNADES, ESCUDEIRO M. **Um Primeiro Contato com Base de Gröbner e suas Aplicações**. 1. ed. Rio de Janeiro: SBM, 2023. P. 247.

SAMPAIO, J. C. V. **Quatro Cores e Matemática**: Minicurso apresentado na II Bienal da SBM, UFBA. Salvador, Brasil: [*s.n.*], 2004. Acesso em: 23 de jun. 2025. Disponível em: http://www.bienasbm.ufba.br/M35.pdf.

VILANOVA, Fábio Fontes. **Sistemas de equações polinomiais e base de Gröbner**. 2015. Dissertação (Mestrado Profissional Matemática) – Universidade Federal de Sergipe, Sergipe.

ZINN-JUSTIN, Paul. **Macaulay2Web: interface web para Macaulay2**. Austrália: [*s.n.*], 2018. Acesso em: 01 ago. 2025. Disponível em: https://www.unimelb-macaulay2.cloud.edu.au/#home.