Universidade Federal de Uberlândia
Instituto de Matemática e Estatística

Licenciatura em Matemática

CONSTRUÇÃO DE BASES DE GRÖBNER PARA IDEAIS POLINOMIAIS SOBRE UM CORPO $\mathbb{K}$

Lucas Araújo Rodrigues

Uberlândia-MG

2026

Lucas Araújo Rodrigues

CONSTRUÇÃO DE BASES DE GRÖBNER PARA IDEAIS POLINOMIAIS SOBRE UM CORPO $\mathbb{K}$

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Uberlândia como requisito parcial para obtenção do título de licenciado em Matemática.

Orientadora: Francielle Rodrigues de Castro Coelho

Uberlândia-MG

2026

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

R696 Rodrigues, Lucas Araújo, 2001-
2026 CONSTRUÇÃO DE BASES DE GRÖBNER PARA IDEAIS POLINOMIAIS SOBRE UM CORPO K [recurso eletrônico] / Lucas Araújo Rodrigues. - 2026.

Orientadora: Francielle Rodrigues de Castro Coelho.
Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Uberlândia, Graduação em Matemática.
Modo de acesso: Internet.
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. I. Coelho, Francielle Rodrigues de Castro,1981-, (Orient.). II. Universidade Federal de Uberlândia. Graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Instituto de Matemática e Estatística
Av. João Naves de Àvila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3239-4158/4156/4126 - www.ime.ufu.br - ime@ufu.br

ATA DE DEFESA - GRADUAÇÃO

Curso de Graduação em:	Licenciatura em Matemática				
Defesa de:	Trabalho de Conclusão de Curso 2 (FAMAT 31804)				
Data:	04/08/2026	Hora de início:	14:00	Hora de encerramento:	15:20
Matrícula do Discente:	12311MAT009				
Nome do Discente:	Lucas Araújo Rodrigues				
Título do Trabalho:	CONSTRUÇÃO DE BASES DE GRÖBNER PARA IDEAIS POLINOMIAIS SOBRE UM CORPO K				

A carga horária curricular foi cumprida integralmente?	(X) Sim ( ) Não

Reuniu-se, na sala 1A240 do Campus Santa Mônica da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Curso de Graduação em Matemática, composta pelos docentes **Francielle Rodrigues de Castro Coelho** (IME-UFU), na qualidade de orientadora e presidente da banca, **Luciana Aparecida Alves** (IME-UFU) e **Victor Gonzalo Lopez Neumann** (IME-UFU).

Iniciando os trabalhos, a presidente da banca, professora Francielle Rodrigues de Castro Coelho, apresentou a Banca Examinadora e o candidato, agradeceu a presença do público e concedeu a palavra ao discente para a apresentação de seu trabalho. A duração da apresentação, bem como os tempos destinados à arguição e às respostas, ocorreu em conformidade com as normas do Curso de Graduação em Matemática.

Na sequência, a presidente concedeu a palavra, sucessivamente, aos examinadores, que procederam à arguição do candidato. Encerrada a arguição, desenvolvida em conformidade com as normas regimentais, a Banca Examinadora reuniu-se, em sessão reservada, para avaliar a apresentação oral e o trabalho escrito, atribuindo ao candidato o seguinte resultado:

Aprovado, com nota 100 (cem).

Nada mais havendo a tratar, a presidente encerrou os trabalhos. Para constar, foi lavrada a presente ata, que, após lida e aprovada, foi assinada pelos membros da Banca Examinadora.

Documento assinado eletronicamente por **Luciana Aparecida Alves**, **Professor(a) do Magistério Superior**, em 04/08/2026, às 15:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Francielle Rodrigues de Castro Coelho**, **Professor(a) do Magistério Superior**, em 04/08/2026, às 15:56, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 05/08/2026, às 10:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7513499** e o código CRC **D13029B7**.

Referência: Processo nº 23117.048718/2026-12 SEI nº 7513499

Agradecimentos

Aos meus pais, Cícera e Luciano, que, parafraseando Isaac Newton, foram os gigantes sobre cujos ombros pude me erguer. Se hoje estou finalizando mais esta etapa, é porque vocês me sustentaram a cada passo desta caminhada. Que este trabalho seja uma pequena retribuição por todo o amor e toda a confiança que depositaram em mim, até nos momentos em que eu mesmo não acreditei.

Aos meus avós maternos, Izabel e José, que já não podem mais sonhar, mas que seguem vivos em cada sonho meu que se realiza. Mesmo analfabetos, vocês sonharam com um futuro melhor para os seus. Celebrar esta conquista acadêmica é também celebrar tudo aquilo que vocês um dia desejaram e não puderam ver acontecer. Que esta vitória seja, de alguma forma, um pouco de vocês vivendo através de mim.

À professora Taciana, que me acompanhou e orientou com dedicação ao longo de todo este trabalho, meu sincero agradecimento pela paciência nos momentos de maior dificuldade, pela clareza com que sempre soube apontar o melhor caminho e por nunca deixar de acreditar no meu potencial.

À professora Francielle, que assumiu a orientação formal nesta etapa final, agradeço pela disponibilidade e pelo apoio.

Aos amigos que encontrei durante a graduação, agradeço pelo companheirismo e pela cumplicidade, por estarem ao meu lado nos momentos de ansiedade e por permanecerem lá para celebrar as minhas vitórias. A universidade impõe muitos desafios, mas vocês fizeram com que eles parecessem menores e tornaram esta caminhada muito mais leve.

Aos membros da banca examinadora, meu sincero agradecimento por terem aceitado gentilmente o convite e pelo tempo despendido na leitura deste trabalho. É uma honra encerrar esta etapa com professores que, de alguma forma, já contribuíram para minha formação.

À Universidade Federal de Uberlândia, por todos os anos de aprendizado, pelas oportunidades oferecidas e pela formação acadêmica e humana.

Resumo

Este trabalho apresenta uma introdução à teoria das bases de Gröbner para ideais polinomiais no anel $\mathbb{K}[x_1, \ldots, x_n]$ sobre um corpo $\mathbb{K}$ qualquer. O trabalho tem como objetivo desenvolver os principais fundamentos dessa teoria, estabelecendo os resultados necessários para a construção e caracterização de bases de Gröbner. Para isso, adota uma abordagem teórica, na qual desenvolve os conceitos, definições e demonstrações de maneira progressiva. Inicialmente, apresenta resultados fundamentais sobre a teoria de anéis, ordens monomiais e sobre o algoritmo da divisão em várias indeterminadas, estendendo ao caso multivariado ferramentas anteriormente disponíveis apenas para polinômios em uma indeterminada. Em seguida, caracteriza os ideais monomiais e demonstra o Lema de Dickson e o Teorema da Base de Hilbert, dos quais decorre a existência de bases de Gröbner para todo ideal polinomial. Na sequência, estabelece o Critério de Buchberger e o Algoritmo de Buchberger, culminando na caracterização das bases de Gröbner mínima e reduzida. Os resultados desenvolvidos evidenciam que as bases de Gröbner fornecem métodos efetivos para a resolução de problemas envolvendo ideais polinomiais e podem servir de base para o estudo futuro de aplicações da teoria.

Palavras-chave: bases de Gröbner; ideais polinomiais; ordenação monomial; algoritmo de Buchberger; álgebra.

Abstract

This work presents an introduction to the theory of Gröbner bases for polynomial ideals in the ring $\mathbb{K}[x_1, \ldots, x_n]$ over an arbitrary field $\mathbb{K}$. The aim of this work is to develop the main foundations of this theory, establishing the results necessary for the construction and characterization of Gröbner bases. To this end, it adopts a theoretical approach, in which the concepts, definitions, and proofs are developed progressively. Initially, it presents fundamental results on ring theory, monomial orderings, and the division algorithm in several indeterminates, extending to the multivariate case tools previously available only for polynomials in one indeterminate. Next, it characterizes monomial ideals and proves Dickson's Lemma and Hilbert's Basis Theorem, from which the existence of Gröbner bases for every polynomial ideal follows. Subsequently, it establishes Buchberger's Criterion and Buchberger's Algorithm, culminating in the characterization of minimal and reduced Gröbner bases. The results developed make it evident that Gröbner bases provide effective methods for solving problems involving polynomial ideals and can serve as a foundation for the future study of applications of the theory.

Keywords: Gröbner bases; polynomial ideals; monomial ordering; Buchberger's algorithm; algebra.

Sumário

Lista de Figuras

1. Introdução

O estudo dos polinômios consolidou-se, historicamente, como um dos pilares fundamentais da Álgebra moderna, estendendo-se das equações algébricas clássicas ao desenvolvimento da Geometria Algébrica e da Álgebra Comutativa. Nesse cenário, entre os problemas mais naturais associados aos ideais de um anel de polinômios destacam-se dois: o primeiro consiste em determinar se todo ideal admite um conjunto finito de geradores e como descrevê-lo de maneira conveniente; já o segundo consiste em decidir se um dado polinômio pertence a um ideal fixado. No anel de polinômios em uma variável, esses problemas admitem soluções relativamente simples. Como todo ideal polinomial em uma indeterminada sobre um corpo é principal, basta um único polinômio para gerar qualquer ideal, e o algoritmo da divisão permite decidir o pertinência de um polinômio a esse ideal por meio da análise do resto da divisão.

Entretanto, essa simplicidade desaparece quando se consideram anéis de polinômios em duas ou mais indeterminadas. Em geral, os ideais deixam de ser principais, e o algoritmo da divisão perde propriedades fundamentais observadas no caso de uma variável, tornando mais difícil tanto a descrição dos ideais quanto a verificação da pertinência de polinômios. Essas dificuldades motivaram o desenvolvimento de novos métodos capazes de estender, para o contexto multivariado, as vantagens oferecidas pelo algoritmo da divisão em uma variável.

Nesse contexto, surgem as bases de Gröbner, introduzidas por Bruno Buchberger em sua tese de doutorado, de 1965, como forma de homenagem ao seu orientador Wolfgang Gröbner. Associadas a uma ordem monomial previamente fixada, elas constituem conjuntos especiais de geradores de um ideal que tornam possível recuperar propriedades essenciais do algoritmo da divisão, fornecendo procedimentos efetivos para resolver os problemas da descrição de ideais e da pertinência de polinômios no caso multivariado.

A base teórica e metodológica desta exposição fundamenta-se, predominantemente, na obra Ideals, Varieties, and Algorithms, de Cox, Little e O'Shea [1]. Esse texto é reconhecido pela clareza com que desenvolve a teoria das bases de Gröbner, conciliando o rigor da Álgebra Comutativa com sua abordagem algorítmica, constituindo a principal referência para este trabalho. Como complemento em língua portuguesa, utilizou-se também a obra Um Primeiro Contato com Bases de Gröbner, de Marcelo Escudeiro Hernandes [2], que contribui para a consolidação dos conceitos aqui desenvolvidos.

Este trabalho está organizado da seguinte forma. No Capítulo 2, são apresentados os conceitos preliminares de teoria de anéis, ideais e anéis de polinômios necessários ao desenvolvimento do texto, tendo como principais referências as obras de Gonçalves [3] e Hefez [4], amplamente

utilizadas no estudo das estruturas algébricas. No Capítulo 3, introduzem-se as ordens monomiais e o algoritmo da divisão em várias variáveis, destacando as diferenças em relação ao caso de uma variável. No Capítulo 4, desenvolve-se a teoria das bases de Gröbner. Inicialmente, são estudados os ideais monomiais e resultados fundamentais, como o Lema de Dickson e o Teorema da Base de Hilbert, dos quais decorre a existência de bases de Gröbner para todo ideal polinomial. Em seguida, são estabelecidos o Critério de Buchberger e o Algoritmo de Buchberger, que nos permite encontrar uma base de Gröbner de um dado ideal, culminando na apresentação das noções de bases de Gröbner mínima e reduzida.

2. Conceitos Preliminares

Antes de iniciarmos o estudo dos anéis de polinômios em várias indeterminadas, reuniremos neste capítulo alguns conceitos e resultados clássicos da Teoria de Anéis que serão utilizados ao longo do texto, em particular nos argumentos que envolvem ideais maximais e anéis quocientes. Tais resultados são apresentados de forma independente do contexto de polinômios, valendo para um anel comutativo e com unidade qualquer.

2.1 Anéis e Ideais

Definição 2.1. Seja A um conjunto não vazio e sejam

$$\begin{array}{rccc} +: & A\times A & \longrightarrow & A \\ & (a,b) & \longmapsto & a+b, \end{array} \qquad \begin{array}{rccc} \cdot: & A\times A & \longrightarrow & A \\ & (a,b) & \longmapsto & a\cdot b, \end{array}$$

duas operações binárias em A, denominadas, respectivamente, soma e produto. Dizemos que a terna $(A,+,\cdot)$ é um anel se, para quaisquer $a,b,c\in A$, são satisfeitas as seguintes propriedades:

(i) $(a+b)+c=a+(b+c)$;

(ii) $a+b=b+a$;

(iii) Existe $0\in A$ tal que $a+0=a$;

(iv) Para todo $a\in A$, existe $-a\in A$ tal que $a+(-a)=0$;

(v) $(a\cdot b)\cdot c=a\cdot(b\cdot c)$;

(vi) $a\cdot(b+c)=a\cdot b+a\cdot c$ e $(a+b)\cdot c=a\cdot c+b\cdot c$.

Dizemos que A é um anel com unidade se existir $1\in A$, $1\neq 0$, tal que $a\cdot 1=1\cdot a=a$, para todo $a\in A$. Dizemos que A é comutativo se $a\cdot b=b\cdot a$, para quaisquer $a,b\in A$.

Neste trabalho, todos os anéis considerados serão comutativos e com unidade. Assim, sempre que mencionarmos um anel A, estaremos assumindo ambas as propriedades.

Definição 2.2. Um anel comutativo com unidade A é chamado domínio de integridade (ou simplesmente domínio) se não possuir divisores de zero, isto é, para quaisquer $a,b\in A$,

$$a\cdot b=0 \Longrightarrow a=0 \text{ ou } b=0.$$

Um anel comutativo com unidade A é chamado corpo se todo elemento não nulo $a \in A$ possuir um inverso multiplicativo, ou seja, se existir $b \in A$ tal que $a \cdot b = 1$.

Definição 2.3. Seja A um anel. Um subconjunto $I \subseteq A$ é um ideal de A se satisfizer:

(i) $0 \in I$.

(ii) Se $a, b \in I$, então $a + b \in I$.

(iii) Se $x \in I$ e $a \in A$, então $ax \in I$.

Os ideais $\{0\}$ e A são denominados ideais triviais de A. Um ideal I é dito próprio se $I \neq A$.

Definição 2.4. Um ideal próprio M de A é dito maximal se, para todo ideal I de A tal que $M \subseteq I \subseteq A$, tem-se $I = M$ ou $I = A$. Em outras palavras, M é maximal se não existir nenhum ideal de A estritamente compreendido entre M e A.

2.2 Anéis Quocientes

Definição 2.5. Sejam A um anel e I um ideal de A. Dados $a, b \in A$, dizemos que a é congruente a b módulo I, e escrevemos $a \equiv b \pmod{I}$, quando $a - b \in I$.

Lema 2.6. *A relação* $\equiv \pmod{I}$ *é uma relação de equivalência sobre* A.

Demonstração: (i) (Reflexividade) Como $0 \in I$, logo temos que $a - a = 0 \in I$. Portanto, $a \equiv a \pmod{I}$ qualquer que seja $a \in A$.

(ii) (Simetria) Se $a \equiv b \pmod{I}$, então $a - b \in I$. Como $1 \in A$, existe $-1 \in A$ tal que $1 + (-1) = 0$. Logo, como I é um ideal, $(-1)(a - b) = b - a \in I$.

Portanto, $b \equiv a \pmod{I}$.

(iii) (Transitividade) Se $a \equiv b \pmod{I}$ e $b \equiv c \pmod{I}$, então $a - b \in I$ e $b - c \in I$. Como I é fechado pela adição,

$$a - c = (a - b) + (b - c) \in I.$$

Consequentemente, $a \equiv c \pmod{I}$.

Portanto, $\equiv \pmod{I}$ é uma relação de equivalência. □

Observemos que $a \equiv b \pmod{I}$ se, e somente se, existir $x \in I$ tal que $a - b = x$, logo $a = b + x$. Portanto,

$$b + I = \{b + x \mid x \in I\}$$

consiste em todos os elementos de A congruentes a b módulo I.

O conjunto acima desempenha um papel fundamental na construção do anel quociente, como formalizaremos na definição a seguir.

Definição 2.7. Sejam A um anel e I um ideal de A. Para cada $a \in A$, definimos a classe de equivalência de a módulo I por

$$\overline{a} = a + I = \{a + x \mid x \in I\}.$$

O conjunto de todas as classes de equivalência módulo I, $A/I = \{\overline{a} \mid a \in A\}$, munido das operações

$$\overline{a} + \overline{b} = \overline{a + b} \quad \text{e} \quad \overline{a} \cdot \overline{b} = \overline{ab},$$

é denominado anel quociente de A por I, nomenclatura que se justificará por meio dos resultados a seguir.

Para que a Definição 2.7 faça sentido, é necessário garantir que as operações de soma e produto em A/I não dependam dos representantes escolhidos para cada classe. É o que mostra a proposição a seguir.

Proposição 2.8. *Sejam A um anel, I um ideal de A e $a, a', b, b' \in A$ tais que $a \equiv a' \pmod{I}$ e $b \equiv b' \pmod{I}$. Então*

$$a + b \equiv a' + b' \pmod{I} \quad e \quad a \cdot b \equiv a' \cdot b' \pmod{I}.$$

Demonstração: Por hipótese, $a - a' \in I$ e $b - b' \in I$. Para a soma, basta observar que

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I,$$

pois I é fechado em relação à soma. Logo $a + b \equiv a' + b' \pmod{I}$.

Para o produto, escrevemos

$$ab - a'b' = a(b - b') + (a - a')b'.$$

Como $b - b' \in I$ e I absorve multiplicação por elementos de A, temos $a(b - b') \in I$. Pelo mesmo motivo, $(a - a')b' \in I$. Logo $ab - a'b' \in I$. Segue que, $a \cdot b \equiv a' \cdot b' \pmod{I}$. □

Garantida a boa definição, resta verificar que as operações de A/I satisfazem as propriedades da Definição 2.1. É natural que A/I herde as propriedades de A, uma vez que suas operações são calculadas por meio de representantes de A.

Proposição 2.9. *Sejam A um anel comutativo com unidade e I um ideal de A tal que $I \neq A$. Então $(A/I, +, \cdot)$ é um anel comutativo com unidade.*

Demonstração: Pela Proposição 2.8, a soma e o produto em A/I estão bem definidos, de modo que podemos calcular com representantes arbitrários. Sejam $\overline{a}, \overline{b}, \overline{c} \in A/I$.

(i) $\left(\overline{a} + \overline{b}\right) + \overline{c} = \overline{a + b} + \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} + \overline{b + c} = \overline{a} + \left(\overline{b} + \overline{c}\right)$.

(ii) $\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}$.

(iii) Sendo $0 \in A$ seu elemento neutro aditivo, a classe $\overline{0} = 0 + I = I$ pertence a A/I. Para todo $\overline{a} \in A/I$,

$$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a},$$

de modo que $\overline{0}$ é o elemento neutro aditivo de A/I.

(iv) Dado $a \in A$, tome $-a \in A$. Então, $\overline{a}, \overline{-a} \in A/I$ e

$$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}.$$

Dessa forma, escrevemos $\overline{-a} = -\overline{a}$.

(v) $\left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right)$.

(vi) $\overline{a} \cdot \left(\overline{b} + \overline{c}\right) = \overline{a} \cdot \overline{b + c} = \overline{a(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$ e, de modo análogo, $\left(\overline{a} + \overline{b}\right) \cdot \overline{c} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$.

Verificadas as seis propriedades, concluímos que $(A/I, +, \cdot)$ é um anel.

Por fim, devemos mostrar que A/I é comutativo e possui unidade. Como A é comutativo,

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a},$$

e portanto A/I é comutativo. Seja 1 a unidade de A. Para todo $\overline{a} \in A/I$,

$$\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a},$$

de modo que $\overline{1}$ é a unidade de A/I. Falta verificar que $\overline{1} \neq \overline{0}$. Se tivéssemos $\overline{1} = \overline{0}$, então $1 \in I$, e como I é ideal, teríamos $I = A$, contrariando a hipótese. Logo $\overline{1} \neq \overline{0}$, e A/I é um anel comutativo com unidade. □

Lema 2.10. *Seja A um anel comutativo com unidade. Então A é um corpo se, e somente se, os únicos ideais de A são os ideais triviais $\{0\}$ e A.*

Demonstração: Sejam A um corpo e I um ideal não nulo de A. Tomemos $a \in I$, $a \neq 0$. Como A é um corpo, existe $a^{-1} \in A$ e, pelo item (iii) da Definição 2.3, temos $a^{-1}a = 1 \in I$. Assim, para todo $x \in A$, temos $x = x \cdot 1 \in I$, o que implica $I = A$.

Reciprocamente, sejam $\{0\}$ e A os únicos ideais de A. Dado $a \in A$, $a \neq 0$. Considere o ideal $\langle a \rangle = \{ax \mid x \in A\}$, como $a \neq 0$, temos $\langle a \rangle \neq \{0\}$, logo, por hipótese, $\langle a \rangle = A$. Em particular, $1 \in \langle a \rangle$, dessa forma, $ax = 1$ para algum $x \in A$. Logo todo elemento não nulo de A é invertível, ou seja, A é um corpo. □

Teorema 2.11. *Sejam A um anel comutativo com unidade e M um ideal de A. Então M é maximal se, e somente se, A/M é um corpo.*

Demonstração: Se $\{0\}$ é um ideal maximal, então $\{0\}$ e A são os únicos ideais de A. Assim, pelo Lema 2.10, a propriedade está provada.

Por outro lado, seja $M \neq \{0\}$ um ideal maximal. Como M é próprio, existe $a \in A$ tal que $a \notin M$.

Definindo o conjunto

$$I = \{m + ax \mid m \in M,\ x \in A\},$$

é fácil ver que I é um ideal de A. De fato, tomando $m = 0$ e $x = 0$, temos $0 \in I$. Além disso, se $m + ax,\ m' + ax' \in I$, então

$$(m + ax) + (m' + ax') = (m + m') + a(x + x') \in I,$$

pois $m + m' \in M$ e $x + x' \in A$.

Agora, dado $m + ax \in I$ e $r \in A$, temos

$$(m + ax)r = mr + a(xr) \in I,$$

pois $mr \in M$, dado que M é um ideal, e $xr \in A$.

Além disso, $M \subseteq I$, pois, para todo $m \in M$, temos $m = m + a \cdot 0 \in I$. Por outro lado, $a = 0 + a \cdot 1 \in I$ e, por construção, $a \notin M$. Logo, $M \neq I$. Como M é maximal, segue que $I = A$. Em particular, $1 \in I$, isto é, existem $m \in M$ e $x \in A$ tais que $1 = m + ax$. Assim, $1 - ax = m \in M$, ou seja, $1 \equiv ax \pmod{M}$. Portanto, $\overline{1} = \overline{ax} = \overline{a} \cdot \overline{x}$. Dessa maneira, mostramos que todo elemento não nulo $\overline{a} \in A/M$ é invertível, mostrando que A/M é um corpo.

Reciprocamente, seja A/M um corpo e seja I um ideal de A tais que $M \subsetneq I \subseteq A$. Tomemos $x \in I \setminus M$. Como $x \notin M$, temos $\overline{x} \neq \overline{0}$ em A/M, logo existe $a \in A$ tal que $\overline{1} = \overline{a} \cdot \overline{x} = \overline{ax}$, isto é, $1 - ax \in M \subsetneq I$. Como $x \in I$ e I é ideal, segue que $1 = ax - (ax - 1) \in I$. Logo, para todo $y \in A$, $y = y \cdot 1 \in I$. Portanto, $I = A$ e M é maximal. □

2.3 Homomorfismos de Anéis

Definição 2.12. Sejam A e A' anéis. Uma função $f : A \to A'$ é um homomorfismo de anéis se, para quaisquer $x, y \in A$, valem

$$f(x + y) = f(x) + f(y) \quad \text{e} \quad f(x \cdot y) = f(x) \cdot f(y).$$

Quando f é bijetiva, dizemos que f é um isomorfismo e que A e A' são anéis isomorfos, o que denotamos por $A \cong A'$.

Vejamos que, se $f : A \to A'$ é um homomorfismo de anéis, então $f(0) = 0'$, em que 0 e $0'$ denotam, respectivamente, os elementos neutros aditivos de A e A'. De fato, $f(0) = f(0+0) = f(0) + f(0)$ e, ao adicionarmos $-f(0)$ a ambos os membros da igualdade, obtemos $f(0) = 0'$.

Definição 2.13. Seja $f : A \to A'$ um homomorfismo de anéis. O núcleo de f é o conjunto

$$\mathrm{N}(f) = \{a \in A \mid f(a) = 0'\}$$

e a imagem de f é o conjunto

$$\mathrm{Im}(f) = \{f(a) \mid a \in A\}.$$

Abaixo, veremos dois resultados que nos auxiliarão na demonstração de um importante teorema acerca de isomorfismos.

Lema 2.14. *Seja $f : A \to A'$ um homomorfismo de anéis. Então, $N(f)$ é um ideal de A.*

Demonstração: Verifiquemos os três itens da Definição 2.3.

(i) Como, $f(0) = 0'$, logo $0 \in \mathrm{N}(f)$.

(ii) Sejam $a, b \in \mathrm{N}(f)$. Então $f(a+b) = f(a) + f(b) = 0' + 0' = 0'$, logo $a + b \in \mathrm{N}(f)$.

(iii) Sejam $a \in \mathrm{N}(f)$ e $x \in A$. Então $f(ax) = f(a) \cdot f(x) = 0' \cdot f(x) = 0'$, logo $ax \in \mathrm{N}(f)$.

Portanto, $\mathrm{N}(f)$ é um ideal de A. □

Lema 2.15. *Um homomorfismo de anéis $f : A \to A'$ é injetivo se, e somente se, $N(f) = \{0\}$.*

Demonstração: Seja f um homomorfismo injetivo. Se $a \in \mathrm{N}(f)$, então $f(a) = 0' = f(0)$ e, pela injetividade, segue que $a = 0$.

Reciprocamente, suponha que $\mathrm{N}(f) = \{0\}$ e sejam $x, y \in A$ tais que $f(x) = f(y)$. Então $f(x - y) = f(x) - f(y) = 0'$, ou seja, $x - y \in \mathrm{N}(f) = \{0\}$, implicando $x = y$, o que conclui a demonstração. □

Teorema 2.16 (**Primeiro Teorema do Isomorfismo**). *Seja $f : A \to A'$ um homomorfismo de anéis. Então*

$$A/\mathrm{N}(f) \;\cong\; \mathrm{Im}(f).$$

Demonstração: Denotemos $N = \mathrm{N}(f)$ e definamos $\varphi : A/N \to \mathrm{Im}(f)$ por $\varphi(\overline{x}) = f(x)$.

Mostremos, inicialmente, que φ está bem definida, isto é, que seu valor não depende do representante escolhido na classe $\overline{x}$. Se $\overline{x} = \overline{y}$, então $x \equiv y \pmod{N}$, ou seja, $x - y \in N = \mathrm{N}(f)$. Logo

$$f(x) - f(y) = f(x - y) = 0'.$$

Assim, $f(x) = f(y)$, ou ainda, $\varphi(\overline{x}) = \varphi(\overline{y})$.

A função φ é sobrejetiva por construção, dado que todo elemento de $\mathrm{Im}(f)$ é da forma $f(x) = \varphi(\overline{x})$ para algum $x \in A$.

Para a injetividade, sejam $\overline{x}, \overline{y} \in A/N$ tais que $\varphi(\overline{x}) = \varphi(\overline{y})$, isto é, $f(x) = f(y)$. Então $f(x - y) = 0'$, logo $x - y \in \mathrm{N}(f) = N$, o que implica $x \equiv y \pmod{N}$. Portanto, $\overline{x} = \overline{y}$.

Por fim, φ é homomorfismo de anéis, pois

$$\varphi(\overline{x} + \overline{y}) = \varphi(\overline{x + y}) = f(x + y) = f(x) + f(y) = \varphi(\overline{x}) + \varphi(\overline{y})$$

e, analogamente, $\varphi(\overline{x} \cdot \overline{y}) = \varphi(\overline{x}) \cdot \varphi(\overline{y})$.

Dessa maneira, conclui-se que $A/\mathrm{N}(f) \cong \mathrm{Im}(f)$. □

Com os conceitos apresentados acima, passamos agora ao estudo dos anéis de polinômios em várias indeterminadas sobre um corpo $\mathbb{K}$ qualquer.

3. Anéis de Polinômios em Várias Indeterminadas sobre um Corpo $\mathbb{K}$

O estudo dos anéis de polinômios em várias indeterminadas constitui a base fundamental da Geometria Algébrica e da Álgebra Comutativa. Enquanto o comportamento de polinômios em uma única variável é bem compreendido através de algoritmos clássicos, como a divisão euclidiana, a transição para o cenário multivariado introduz dificuldades estruturais que exigem ferramentas mais sofisticadas.

Neste capítulo, estabeleceremos as propriedades essenciais do anel $\mathbb{K}[x_1, \ldots, x_n]$, formalizando conceitos como ordens monomiais e o algoritmo de divisão multivariada. Estas definições são os pilares necessários para a construção das bases de Gröbner, foco central deste trabalho, as quais consistem em um conjunto especial de geradores de um ideal que permite resolver problemas computacionais desafiadores, como o problema da pertinência de um polinômio a um ideal de $\mathbb{K}[x_1, \ldots, x_n]$ e a solução de sistemas de equações polinomiais não lineares.

3.1 Polinômios em Várias Indeterminadas sobre um Corpo

Definição 3.1. Um monômio nas variáveis $x_1, \ldots, x_n$ é um produto da forma

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

em que todos os expoentes $\alpha_1, \ldots, \alpha_n$ são números inteiros não negativos. O grau total desse monômio é a soma $\alpha_1 + \cdots + \alpha_n$.

A notação utilizada para monômios pode ser simplificada da seguinte maneira: seja $\alpha = (\alpha_1, \ldots, \alpha_n)$ uma n-upla de inteiros não negativos. Assim, definimos

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Veja que para $\alpha = (0, \ldots, 0)$ tem-se $x^\alpha = 1$. O grau total do monômio x^α pode ser denotado por $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

Definição 3.2. Um polinômio f nas variáveis $x_1, \ldots, x_n$ com coeficientes em um corpo $\mathbb{K}$ é uma combinação linear finita, com coeficientes em $\mathbb{K}$, de monômios. Escreveremos um polinômio f

na forma

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad a_\alpha \in \mathbb{K}$$

em que a soma é feita sobre uma quantidade finita de n-uplas $\alpha = (\alpha_1, \ldots, \alpha_n)$. O conjunto de todos os polinômios em $x_1, \ldots, x_n$ com coeficientes em $\mathbb{K}$ é denotado por $\mathbb{K}[x_1, \ldots, x_n]$.

Observação 3.3. Verifica-se que, com as operações usuais de soma e multiplicação:

$$\sum_{\alpha} a_\alpha x^\alpha + \sum_{\alpha} b_\alpha x^\alpha = \sum_{\alpha} (a_\alpha + b_\alpha) x^\alpha$$

$$\left(\sum_{\alpha} a_\alpha x^\alpha \right) \cdot \left(\sum_{\beta} b_\beta x^\beta \right) = \sum_{\gamma} \left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta \right) x^\gamma$$

o conjunto $\mathbb{K}[x_1, \ldots, x_n]$ é um anel comutativo com unidade $1 = x_1^0 \ldots x_n^0$, que identificamos com a unidade $1 \in \mathbb{K}$. Tal conjunto é denominado **anel de polinômios nas indeterminadas** $x_1, \ldots, x_n$ **com coeficientes no corpo** $\mathbb{K}$. Elementos de $\mathbb{K} \subset \mathbb{K}[x_1, \ldots, x_n]$ são chamados de polinômios constantes.

Definição 3.4. Sejam $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Assim, definimos o conjunto

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \;\middle|\; h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n] \right\}.$$

Veremos que esse conjunto é um ideal.

Lema 3.5. *Se $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, então $\langle f_1, \ldots, f_s \rangle$ é um ideal de $\mathbb{K}[x_1, \ldots, x_n]$. O conjunto $\langle f_1, \ldots, f_s \rangle$ será chamado de ideal gerado por $f_1, \ldots, f_s$. Quando $s = 1$, o ideal $\langle f_1 \rangle = \{hf_1 \mid h \in \mathbb{K}[x_1, \ldots, x_n]\}$ é denominado ideal principal gerado por f_1.*

Demonstração: Primeiramente, note que $0 \in \langle f_1, \ldots, f_s \rangle$, pois $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Agora, suponhamos $f = \sum_{i=1}^{s} p_i f_i$ e $g = \sum_{i=1}^{s} q_i f_i$ e seja $h \in \mathbb{K}[x_1, \ldots, x_n]$. Logo

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i \in \langle f_1, \ldots, f_s \rangle,$$

e

$$hf = \sum_{i=1}^{s} (hp_i) f_i \in \langle f_1, \ldots, f_s \rangle.$$

Mostrando, dessa forma, que $\langle f_1, \ldots, f_s \rangle$ é um ideal.

□

3.2 Ordens sobre Monômios em $\mathbb{K}[x_1, \ldots, x_n]$

Se analisarmos o algoritmo da divisão em $\mathbb{K}[x]$ com atenção, seremos capazes de ver que a noção de ordenar os termos dos polinômios é parte fundamental do processo, mesmo que não

frequentemente ressaltada. Ao dividirmos f por g, onde $f, g \in \mathbb{K}[x]$, procederíamos de acordo com a sequência abaixo

- Escrever os termos dos polinômios em ordem decrescente de grau em x.
- No primeiro passo, identificamos o termo líder de f, isto é, o termo de maior grau de f, e o expressamos como q vezes o termo de maior grau de g, onde q é o quociente entre esses termos. Em seguida, subtraímos de f o produto $q \cdot g$, cancelando assim o termo líder de f.
- Repetimos o mesmo processo para o polinômio resultante, até obtermos um polinômio de grau inferior ao grau de g.

No processo de divisão de polinômios de uma variável, a ordenação dos monômios é feita de acordo com seus graus:

$$\cdots \succ x^{m+1} \succ x^m \succ \cdots \succ x^2 \succ x \succ 1.$$

O sucesso do algoritmo depende de operar sistematicamente com os termos líderes de f e g, e não de cancelar termos de f de forma arbitrária utilizando termos quaisquer de g.

O exposto acima sugere que um componente essencial para qualquer extensão do algoritmo da divisão para várias variáveis seja a ordenação dos termos dos polinômios em $\mathbb{K}[x_1, \ldots, x_n]$.

Da Definição 3.1, podemos reconstruir o monômio $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ a partir da n-upla de expoentes $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$, onde $\mathbb{Z}_{\geq 0}^n$ denota o conjunto de todas as n-uplas de inteiros não negativos. Dessa forma, é estabelecida uma bijeção entre os monômios em $\mathbb{K}[x_1, \ldots, x_n]$ e $\mathbb{Z}_{\geq 0}^n$. Adicionalmente, qualquer ordem $\succ$ que for estabelecida em $\mathbb{Z}_{\geq 0}^n$ nos fornecerá uma ordem sobre os monômios, ou seja, se $\alpha \succ \beta$ em relação a essa ordem, também diremos que $x^\alpha \succ x^\beta$.

Para começar, como um polinômio é uma soma de monômios, gostaríamos de ser capazes de ordenar os termos de um polinômio de forma não ambígua. Para isso, devemos ser capazes de comparar todo par de monômios a fim de estabelecer suas posições relativas. Portanto, exigiremos que uma ordem sobre os monômios seja uma relação de ordem total, o que significa que para qualquer par x^α e x^β, exatamente uma das três afirmações

$$x^\alpha \succ x^\beta, \quad x^\alpha = x^\beta, \quad x^\beta \succ x^\alpha$$

deve ser verdadeira.

Em seguida, devemos levar em conta o efeito das operações de soma e produto sobre os polinômios. Ao somarmos polinômios, podemos simplesmente reorganizar os termos presentes na ordem apropriada. Já na multiplicação, por possuir a propriedade distributiva em relação à adição, é suficiente considerar o que acontece ao multiplicarmos um monômio por um polinômio. Para garantir que essa operação preserve a ordem entre os termos, exigiremos que uma ordem monomial satisfaça a seguinte propriedade: se $x^\alpha \succ x^\beta$ e x^γ é um monômio qualquer, então $x^\alpha x^\gamma \succ x^\beta x^\gamma$. Em termos dos vetores de expoentes, isso significa que se $\alpha \succ \beta$, então, para todo $\gamma \in \mathbb{Z}_{\geq 0}^n$, temos $\alpha + \gamma \succ \beta + \gamma$.

Definição 3.6. Uma ordem monomial $\succ$ sobre $\mathbb{K}[x_1, \ldots, x_n]$ é uma relação $\succ$ sobre $\mathbb{Z}^n_{\geq 0}$, isto é, uma relação sobre o conjunto dos monômios $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$, satisfazendo:

(i) $\succ$ é uma relação de ordem total sobre $\mathbb{Z}^n_{\geq 0}$.

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

(iii) $\succ$ é uma boa ordem em $\mathbb{Z}^n_{\geq 0}$. Isso significa que qualquer subconjunto não vazio de $\mathbb{Z}^n_{\geq 0}$ tem um menor elemento em relação a $\succ$. Ou ainda, se $A \subseteq \mathbb{Z}^n_{\geq 0}$ é não vazio, então existe $\alpha \in A$ tal que, para todo $\beta \in A \setminus \{\alpha\}$, temos $\beta \succ \alpha$.

Dada uma ordem monomial $\succ$, definimos $\alpha \succeq \beta$ quando $\alpha \succ \beta$ ou $\alpha = \beta$.

Lema 3.7. *Uma relação de ordem total $\succ$ sobre $\mathbb{Z}^n_{\geq 0}$ é uma boa ordem se, e somente se, toda sequência estritamente decrescente em $\mathbb{Z}^n_{\geq 0}$*

$$\alpha(1) \succ \alpha(2) \succ \alpha(3) \succ \cdots$$

eventualmente termina.

Demonstração: Provaremos tal afirmação através da sua contrapositiva: $\succ$ não é uma boa ordem se, e somente se, existir uma sequência infinita estritamente decrescente em $\mathbb{Z}^n_{\geq 0}$.

Se $\succ$ não é uma boa ordem, então algum $S \subseteq \mathbb{Z}^n_{\geq 0}$, não vazio, não possui menor elemento. Tome $\alpha(1) \in S$. Como $\alpha(1)$ não é o menor elemento, conseguimos encontrar $\alpha(1) \succ \alpha(2)$ em S. Da mesma forma, $\alpha(2)$ não é o menor elemento, logo há $\alpha(2) \succ \alpha(3)$ em S. Repetindo tal procedimento, obtemos uma sequência infinita estritamente decrescente.

$$\alpha(1) \succ \alpha(2) \succ \alpha(3) \succ \cdots .$$

Reciprocamente, dada tal sequência infinita, o conjunto $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ é um subconjunto não vazio de $\mathbb{Z}^n_{\geq 0}$ sem menor elemento, logo, $\succ$ não é uma boa ordem.

□

Definição 3.8 (Ordem Lexicográfica). Dados $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $\beta = (\beta_1, \ldots, \beta_n)$ em $\mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha \succ_{lex} \beta$ se a primeira entrada não nula mais à esquerda do vetor diferença $\alpha - \beta \in \mathbb{Z}^n$ é positiva. Teremos que $x^\alpha \succ_{lex} x^\beta$ se $\alpha \succ_{lex} \beta$.

Observe que as variáveis $x_1, x_2, \ldots, x_n$ ficam ordenadas da forma usual pela ordem lexicográfica:

$$(1, 0, \ldots, 0) \succ_{lex} (0, 1, \ldots, 0) \succ_{lex} \cdots \succ_{lex} (0, 0, \ldots, 1)$$

ou

$$x_1 \succ_{lex} x_2 \succ_{lex} \cdots \succ_{lex} x_n.$$

Perceba que a ordem lexicográfica não é unicamente determinada, pois ela depende da ordenação escolhida para as variáveis. Até o momento, utilizamos a ordem lexicográfica com

$x_1 \succ x_2 \succ \cdots \succ x_n$, mas para cada ordenação das variáveis $x_1, \ldots, x_n$ existe uma ordem lexicográfica correspondente. Assim, com n variáveis, há exatamente $n!$ ordens lexicográficas possíveis.

Em geral, ao trabalharmos com polinômios em duas ou três variáveis, chamaremos as variáveis de x, y, z ao invés de x_1, x_2, x_3. Além disso, assumiremos que a ordem alfabética $x \succ y \succ z$ nas variáveis é usada para definir a ordem lexicográfica a menos que indiquemos o contrário de maneira explícita.

Proposição 3.9. *A ordem lexicográfica sobre $\mathbb{Z}^n_{\geq 0}$ é uma ordem monomial.*

Demonstração: (i) O fato de que $\succ_{lex}$ é uma relação de ordem total segue da definição e do fato de que a ordem numérica usual sobre $\mathbb{Z}_{\geq 0}$ é uma relação de ordem total.

(ii) Se $\alpha \succ_{lex} \beta$, então a primeira entrada não nula mais à esquerda de $\alpha - \beta$, digamos $\alpha_i - \beta_i$, é positiva. Seja $\gamma \in \mathbb{Z}^n_{\geq 0}$, logo em $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, teremos a primeira entrada não nula mais à esquerda igual a $\alpha_i - \beta_i > 0$. Assim, $\alpha + \gamma \succ_{lex} \beta + \gamma$.

(iii) Suponhamos que $\succ_{lex}$ não é uma boa ordem. Então, pelo Lema 3.7, existe uma sequência infinita estritamente decrescente de elementos de $\mathbb{Z}^n_{\geq 0}$:

$$\alpha(1) \succ_{lex} \alpha(2) \succ_{lex} \alpha(3) \succ_{lex} \cdots .$$

Mostremos que isso leva a uma contradição. Seja $\alpha_1(i)$ a primeira entrada do vetor $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Como $\alpha(i) \succ_{lex} \alpha(i+1)$, temos que $\alpha_1(i) - \alpha_1(i+1) \geq 0$ implicando em $\alpha_1(i) \geq \alpha_1(i+1)$, isto é, as primeiras entradas formam uma sequência não crescente de inteiros não negativos. Como $\mathbb{Z}_{\geq 0}$ é bem ordenado, tal sequência deve "estabilizar" eventualmente, ou seja, existe um $m \in \mathbb{N}$ tal que

$$\alpha_1(m) = \alpha_1(m+1) = \alpha_1(m+2) = \cdots .$$

Agora, partindo de $\alpha(m)$ analisemos as segundas entradas. De forma análoga, as segundas entradas de $\alpha(m), \alpha(m+1), \ldots$ formam uma sequência não crescente que eventualmente "estabiliza". Dessa forma, para algum l, as n-uplas $\alpha(l), \alpha(l+1), \ldots$ possuem todas as entradas iguais. Contradizendo, assim, que $\alpha(l) \succ_{lex} \alpha(l+1)$.

□

Em uma ordem lexicográfica, uma variável domina qualquer monômio que envolva apenas variáveis menores que ela. Dependendo do objetivo, pode ser interessante considerar ordens monomiais que levem em consideração, primeiramente, o grau total do monômio.

Definição 3.10 (Ordem Lexicográfica Graduada). Sejam $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha \succ_{grlex} \beta$ se

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

Assim como na ordem lexicográfica, na ordem lexicográfica graduada as variáveis ficam ordenadas de maneira usual. Isto é,

$$(1,0,\ldots,0) \succ_{grlex} (0,1,\ldots,0) \succ_{grlex} \cdots \succ_{grlex} (0,0,\ldots,1)$$

ou

$$x_1 \succ_{grlex} x_2 \succ_{grlex} \cdots \succ_{grlex} x_n.$$

Proposição 3.11. *A ordem lexicográfica graduada sobre $\mathbb{Z}^n_{\geq 0}$ é uma ordem monomial.*

Demonstração: (i) O fato de que $\succ_{grlex}$ é uma relação de ordem total segue da definição e do fato de que a ordem numérica usual sobre $\mathbb{Z}_{\geq 0}$ é uma relação de ordem total. De fato, dados $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, temos $|\alpha| > |\beta|$, $|\beta| > |\alpha|$ ou $|\alpha| = |\beta|$. No caso de igualdade, a comparação é feita pela ordem lexicográfica, a qual é uma relação de ordem total.

(ii) Primeiramente, observe que para quaisquer $\alpha, \gamma \in \mathbb{Z}^n_{\geq 0}$, vale

$$|\alpha + \gamma| = \sum_{i=1}^{n}(\alpha_i + \gamma_i) = \sum_{i=1}^{n}\alpha_i + \sum_{i=1}^{n}\gamma_i = |\alpha| + |\gamma|.$$

Agora, se $\alpha \succ_{grlex} \beta$, então $|\alpha| > |\beta|$ ou $|\alpha| = |\beta|$ e $\alpha \succ_{lex} \beta$. No primeiro caso, como $|\alpha| > |\beta|$, então $|\alpha + \gamma| = |\alpha| + |\gamma| > |\beta| + |\gamma| = |\beta + \gamma|$, logo $\alpha + \gamma \succ_{grlex} \beta + \gamma$. Já no segundo caso, $|\alpha + \gamma| = |\beta + \gamma|$ e, como $\succ_{lex}$ é ordem monomial, temos $\alpha + \gamma \succ_{lex} \beta + \gamma$, logo $\alpha + \gamma \succ_{grlex} \beta + \gamma$.

(iii) Por absurdo, suponha que $\succ_{grlex}$ não é uma boa ordem. Então, pelo Lema 3.7, existem $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$ tais que

$$\alpha(1) \succ_{grlex} \alpha(2) \succ_{grlex} \alpha(3) \succ_{grlex} \cdots .$$

Por definição, $|\alpha(i)| \geq |\alpha(i+1)|$, isto é, os graus totais dos monômios formam uma sequência de inteiros não negativos não crescente. Como $\mathbb{Z}_{\geq 0}$ é bem ordenado, existe $m \in \mathbb{N}$ tal que

$$|\alpha(m)| = |\alpha(m+1)| = |\alpha(m+2)| = \cdots .$$

Dessa forma, para todo $k \geq m$, temos $\alpha(k) \succ_{lex} \alpha(k+1)$. Isso contradiz o fato de que a ordem lexicográfica é uma boa ordem em $\mathbb{Z}^n_{\geq 0}$.

□

Definição 3.12 (Ordem Lexicográfica Graduada Reversa). Sejam $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha \succ_{grevlex} \beta$ se

$$|\alpha| = \sum_{i=1}^{n}\alpha_i > |\beta| = \sum_{i=1}^{n}\beta_i \quad \text{ou} \quad |\alpha| = |\beta| \text{ e a primeira entrada não nula mais à direita de } \alpha - \beta \in \mathbb{Z}^n \text{ é negativa.}$$

Observe que, da mesma forma que nas duas ordens monomiais acima, a ordem lexicográfica graduada reversa ordena as variáveis de maneira usual.

$$x_1 \succ_{grevlex} x_2 \succ_{grevlex} \cdots \succ_{grevlex} x_n.$$

Proposição 3.13. *A ordem lexicográfica graduada reversa sobre $\mathbb{Z}_{\geq 0}^n$ é uma ordem monomial.*

Demonstração: (i) O fato de que $\succ_{grevlex}$ é uma relação de ordem total segue da definição e do fato de que a ordem numérica usual sobre $\mathbb{Z}_{\geq 0}$ é uma relação de ordem total. De fato, dados $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$, temos $|\alpha| > |\beta|$, $|\beta| > |\alpha|$ ou $|\alpha| = |\beta|$. No caso de igualdade, a comparação é feita analisando a primeira entrada não nula mais à direita de $\alpha - \beta$, o que sempre determina uma ordem total.

(ii) Se $\alpha \succ_{grevlex} \beta$, então $|\alpha| > |\beta|$ ou $|\alpha| = |\beta|$ e a primeira entrada não nula mais à direita de $\alpha - \beta$ é negativa. Se $|\alpha| > |\beta|$, então $|\alpha + \gamma| = |\alpha| + |\gamma| > |\beta| + |\gamma| = |\beta + \gamma|$, logo $\alpha + \gamma \succ_{grevlex} \beta + \gamma$. No segundo caso, $|\alpha + \gamma| = |\beta + \gamma|$ e, observe que

$$(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta,$$

logo $(\alpha+\gamma)-(\beta+\gamma)$ e $\alpha-\beta$ possuem a mesma primeira entrada não nula mais à direita, que é negativa. Portanto, $\alpha + \gamma \succ_{grevlex} \beta + \gamma$.

(iii) Por absurdo, suponha que $\succ_{grevlex}$ não é uma boa ordem. Então, pelo Lema 3.7, existem $\alpha(i) \in \mathbb{Z}_{\geq 0}^n$ tais que

$$\alpha(1) \succ_{grevlex} \alpha(2) \succ_{grevlex} \alpha(3) \succ_{grevlex} \cdots .$$

Por definição, $|\alpha(i)| \geq |\alpha(i+1)|$, isto é, os graus totais dos monômios formam uma sequência de inteiros não negativos não crescente. Como $\mathbb{Z}_{\geq 0}$ é bem ordenado, existe $m \in \mathbb{N}$ tal que

$$|\alpha(m)| = |\alpha(m+1)| = |\alpha(m+2)| = \cdots .$$

Dessa forma, para todo $k \geq m$, a primeira entrada não nula mais à direita de $\alpha(k)-\alpha(k+1)$ deve ser negativa, isto é, $\alpha_n(k) - \alpha_n(k+1) \leq 0$, implicando em $\alpha_n(k) \leq \alpha_n(k+1)$, ou seja, as últimas entradas formam uma sequência não decrescente de inteiros não negativos começando em $\alpha_n(m)$. Além disso, tal sequência é limitada superiormente, pois qualquer que seja $k \geq m$ vale

$$0 \leq \alpha_n(k) \leq |\alpha(k)| = |\alpha(m)|.$$

Portanto, essa sequência eventualmente "estabiliza". Procedendo de forma análoga para as demais entradas sempre obtemos uma sequência não decrescente que possui $|\alpha(m)|$ como um limite superior. Dessa forma, existe $l \geq m$ tal que $\alpha(l) = \alpha(l+1)$, o que contradiz o fato de que $\alpha(l) \succ_{grevlex} \alpha(l+1)$.

□

No exemplo a seguir, ordenaremos os monômios de um polinômio segundo essas três ordens monomiais.

Exemplo 3.14. Seja $h = 3x^4 - 2xy^2z^2 + x^2y^3 + y^4z \in \mathbb{Q}[x, y, z]$. Os termos de h com coeficiente não nulo correspondem aos vetores de expoentes

$$S = \{\alpha \in \mathbb{Z}^3_{\geq 0} \mid a_\alpha \neq 0\} = \{(4, 0, 0),\ (1, 2, 2),\ (2, 3, 0),\ (0, 4, 1)\}.$$

Ordenamos S em relação às três ordens.
(Ordem lexicográfica) Comparando os vetores dois a dois,

$$(4, 0, 0) - (2, 3, 0) = (2, -3, 0),$$

cuja entrada não nula mais à esquerda é a primeira, igual a $2 > 0$. Logo, $(4, 0, 0) \succ_{lex} (2, 3, 0)$. Em seguida,

$$(2, 3, 0) - (1, 2, 2) = (1, 1, -2),$$

cuja entrada não nula mais à esquerda é a primeira, igual a $1 > 0$. Assim, $(2, 3, 0) \succ_{lex} (1, 2, 2)$. Por fim,

$$(1, 2, 2) - (0, 4, 1) = (1, -2, 1),$$

cuja entrada não nula mais à esquerda é a primeira, igual a $1 > 0$, de modo que, $(1, 2, 2) \succ_{lex} (0, 4, 1)$. Das comparações acima temos

$$(4, 0, 0) \succ_{lex} (2, 3, 0) \succ_{lex} (1, 2, 2) \succ_{lex} (0, 4, 1),$$

o que equivale a

$$3x^4 \ \succ_{lex} \ x^2y^3 \ \succ_{lex} \ -2xy^2z^2 \ \succ_{lex} \ y^4z.$$

(Ordem lexicográfica graduada) Os graus totais dos quatro vetores são

$$|(4, 0, 0)| = 4 + 0 + 0 = 4, \qquad |(1, 2, 2)| = 1 + 2 + 2 = 5,$$

$$|(2, 3, 0)| = 2 + 3 + 0 = 5, \qquad |(0, 4, 1)| = 0 + 4 + 1 = 5.$$

Como $4 < 5$, o vetor $(4, 0, 0)$ ocupará a última posição. Os outros três vetores apresentam o mesmo grau total, de modo que o desempate entre eles é feito pela ordem lexicográfica, já calculado no item anterior, a saber $(2, 3, 0) \succ_{lex} (1, 2, 2) \succ_{lex} (0, 4, 1)$. Concluímos que

$$(2, 3, 0) \succ_{grlex} (1, 2, 2) \succ_{grlex} (0, 4, 1) \succ_{grlex} (4, 0, 0).$$

Ou, equivalentemente,

$$x^2y^3 \ \succ_{grlex} \ -2xy^2z^2 \ \succ_{grlex} \ y^4z \ \succ_{grlex} \ 3x^4.$$

(Ordem lexicográfica graduada reversa) Como no item anterior, o vetor $(4, 0, 0)$ permanece na

última posição, pois possui o menor grau total. Entre os três vetores de grau total 5, porém, o desempate passa a olhar a entrada não nula mais à direita da diferença. Comparando $(2,3,0)$ com $(1,2,2)$,

$$(2,3,0)-(1,2,2)=(1,1,-2),$$

cuja entrada não nula mais à direita é a terceira, igual a $-2<0$. Logo, $(2,3,0)\succ_{grevlex}(1,2,2)$. Comparando $(2,3,0)$ com $(0,4,1)$,

$$(2,3,0)-(0,4,1)=(2,-1,-1),$$

cuja entrada não nula mais à direita é a terceira, igual a $-1<0$. Portanto, $(2,3,0)\succ_{grevlex}(0,4,1)$. Comparando, por fim, $(1,2,2)$ com $(0,4,1)$,

$$(1,2,2)-(0,4,1)=(1,-2,1),$$

cuja entrada não nula mais à direita é a terceira, igual a $1>0$, de modo que $(1,2,2)\prec_{grevlex}(0,4,1)$. Combinando as três comparações,

$$(2,3,0)\succ_{grevlex}(0,4,1)\succ_{grevlex}(1,2,2)\succ_{grevlex}(4,0,0),$$

o que equivale a

$$x^2y^3\ \succ_{grevlex}\ y^4z\ \succ_{grevlex}\ -2xy^2z^2\ \succ_{grevlex}\ 3x^4.$$

Essa ordenação difere da obtida com $\succ_{grlex}$ exatamente na posição dos termos $-2xy^2z^2$ e y^4z, que trocam de lugar, pois seus correspondentes vetores de expoentes empatam em grau total e os critérios de desempate analisam extremos opostos desses vetores.

Definição 3.15. Seja $f=\sum_{\alpha} a_\alpha x^\alpha$ um polinômio não identicamente nulo em $\mathbb{K}[x_1,\ldots,x_n]$ e fixe uma ordem monomial $\succ$.

(i) O multigrau de f é

$$\text{multideg}(f)=\max\{\alpha\in\mathbb{Z}^n_{\geq 0}\mid a_\alpha\neq 0\}$$

em que o máximo é tomado em relação à ordem monomial $\succ$.

(ii) O coeficiente líder de f é

$$\text{LC}(f)=a_{\text{multideg}(f)}\in\mathbb{K}.$$

(iii) O monômio líder de f é

$$\text{LM}(f)=x^{\text{multideg}(f)}$$

cujo coeficiente é 1.

(iv) O termo líder de f é

$$\text{LT}(f)=\text{LC}(f)\cdot\text{LM}(f).$$

Exemplo 3.16. Seja $f = x + y^3 \in \mathbb{Q}[x, y]$. Os termos de f com coeficiente não nulo correspondem aos vetores de expoentes

$$S = \{(1, 0),\ (0, 3)\}.$$

Adotada a ordem lexicográfica graduada, comparamos os graus totais dos monômios que aparecem em f,

$$|(1, 0)| = 1 \qquad \text{e} \qquad |(0, 3)| = 3.$$

Como $1 < 3$, temos $(0, 3) \succ_{grlex} (1, 0)$, o que equivale a $y^3 \succ_{grlex} x$. Assim, segue que

(i) O multigrau de f é

$$\text{multideg}(f) = (0, 3).$$

(ii) O coeficiente líder de f é

$$\text{LC}(f) = a_{(0,3)} = 1 \in \mathbb{Q}.$$

(iii) O monômio líder de f é

$$\text{LM}(f) = x^{(0,3)} = y^3.$$

(iv) O termo líder de f é

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f) = 1 \cdot y^3 = y^3.$$

Lema 3.17. *Sejam $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ polinômios não identicamente nulos. Então*

(i) $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.

(ii) Se $f + g \neq 0$, então $\text{multideg}(f + g) \preceq \max\{\text{multideg}(f), \text{multideg}(g)\}$ *e a igualdade ocorre quando* $\text{multideg}(f) \neq \text{multideg}(g)$.

Demonstração: Sejam $f = \sum_{\alpha} a_\alpha x^\alpha$ e $g = \sum_{\beta} b_\beta x^\beta$. Definamos $\alpha_0 = \text{multideg}(f)$ e $\beta_0 = \text{multideg}(g)$. Assim, escrevemos $f = a_{\alpha_0} x^{\alpha_0} + \sum_{\alpha \prec \alpha_0} a_\alpha x^\alpha$ e $g = b_{\beta_0} x^{\beta_0} + \sum_{\beta \prec \beta_0} b_\beta x^\beta$.

(i) Veja que $a_{\alpha_0} b_{\beta_0} \neq 0$, pois $a_{\alpha_0} \neq 0$ e $b_{\beta_0} \neq 0$. Agora

$$\begin{aligned} fg &= a_{\alpha_0} b_{\beta_0} x^{\alpha_0+\beta_0} + a_{\alpha_0} x^{\alpha_0} \sum_{\beta \prec \beta_0} b_\beta x^\beta + b_{\beta_0} x^{\beta_0} \sum_{\alpha \prec \alpha_0} a_\alpha x^\alpha + \left(\sum_{\alpha \prec \alpha_0} a_\alpha x^\alpha \right) \left(\sum_{\beta \prec \beta_0} b_\beta x^\beta \right) \\ &= a_{\alpha_0} b_{\beta_0} x^{\alpha_0+\beta_0} + \sum_{\beta \prec \beta_0} a_{\alpha_0} b_\beta x^{\alpha_0+\beta} + \sum_{\alpha \prec \alpha_0} a_\alpha b_{\beta_0} x^{\alpha+\beta_0} + \sum_{\substack{\alpha \prec \alpha_0 \\ \beta \prec \beta_0}} a_\alpha b_\beta x^{\alpha+\beta}. \end{aligned}$$

Pela definição de multigrau temos que $\alpha_0 \succ \alpha$ e $\beta_0 \succ \beta$ para todo $\alpha \neq \alpha_0$ e para todo $\beta \neq \beta_0$ que aparecem nos polinômios. Como $\succ$ é uma ordem monomial, a ordem é preservada pela adição de n-uplas de inteiros não negativos, isto é,

$$\alpha_0 + \beta_0 \succ \alpha + \beta_0 \succ \alpha + \beta$$

e

$$\alpha_0 + \beta_0 \succ \alpha_0 + \beta \succ \alpha + \beta.$$

Concluímos que $\text{multideg}(fg) = \alpha_0 + \beta_0 = \text{multideg}(f) + \text{multideg}(g)$.

(ii) Suponhamos, sem perda de generalidade, que $\alpha_0 \succeq \beta_0$, então

$$f + g = \sum_{\gamma} (a_\gamma + b_\gamma) x^\gamma,$$

onde γ "varre" as n-uplas admitidas por α e β e definimos $a_\gamma = 0$ se x^γ não aparece em f e, analogamente, $b_\gamma = 0$ se x^γ não aparece em g. Dessa forma, como $f + g \neq 0$, existe uma maior n-upla γ_0, com respeito a $\succ$, para a qual o coeficiente de x^{γ_0} é não nulo. Ou seja,

$$\text{multideg}(f + g) = \gamma_0 \preceq \alpha_0 = \max\{\text{multideg}(f), \text{multideg}(g)\}.$$

Se $\alpha_0 \succ \beta_0$, então $b_{\alpha_0} = 0$. Como $a_{\alpha_0} \neq 0$, segue que $a_{\alpha_0} + b_{\alpha_0} = a_{\alpha_0} \neq 0$. Assim, o monômio x^{α_0} possui coeficiente não nulo em $f + g$. Como nenhum expoente pode ser maior que α_0, concluímos que $\gamma_0 = \alpha_0$ e, portanto,

$$\text{multideg}(f + g) = \alpha_0 = \max\{\text{multideg}(f), \text{multideg}(g)\}.$$

□

3.3 Dividindo Polinômios em Mais de uma Variável

Sabemos, do estudo de polinômios em $\mathbb{K}[x]$, que o algoritmo da divisão pode ser utilizado para verificar se um polinômio g pertence ao ideal gerado por outro polinômio f. Nesse contexto, ao dividir g por f, obtemos $g = qf + r$ com $q, r \in \mathbb{K}[x]$ e $\deg(r) < \deg(f)$ ou $r = 0$. Temos então que $g \in \langle f \rangle$ se, e somente se, $r = 0$. A fim de estudar esse problema para o caso multivariável, definiremos um algoritmo da divisão para polinômios em $\mathbb{K}[x_1, \ldots, x_n]$ que estenda o algoritmo utilizado no caso univariado. De forma geral, o objetivo é dividir $f \in \mathbb{K}[x_1, \ldots, x_n]$ por $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, isto é, 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 $\mathbb{K}[x_1, \ldots, x_n]$.

Teorema 3.18 (**Algoritmo da divisão multivariável**). *Sejam $\succ$ uma ordem monomial sobre $\mathbb{Z}^n_{\geq 0}$ e $F = (f_1, \ldots, f_s)$ uma s-upla ordenada de polinômios em $\mathbb{K}[x_1, \ldots, x_n]$. Então, qualquer $f \in \mathbb{K}[x_1, \ldots, x_n]$ pode ser escrito como*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

em que $q_i, r \in \mathbb{K}[x_1, \ldots, x_n]$ e $r = 0$ ou r é uma combinação linear, com coeficientes em $\mathbb{K}$, de monômios, nenhum deles divisível por nenhum dos $LT(f_1), \ldots, LT(f_s)$. Diremos que r é o resto da divisão de f por F. Adicionalmente, se $q_i f_i \neq 0$, então

$$\text{multideg}(f) \succeq \text{multideg}(q_i f_i).$$

Demonstração: Provaremos a existência de $q_1, \ldots, q_s$ e r apresentando um algoritmo que os constrói e mostrando que ele opera de maneira correta qualquer que seja a entrada.

Algoritmo 1: Algoritmo da Divisão Multivariável

Entrada: $f_1, \ldots, f_s, f$
Saída: $q_1, \ldots, q_s, r$

$q_1 := 0; \ldots; q_s := 0;$
$r := 0;$
$p := f;$
ENQUANTO $p \neq 0$ **FAÇA**
  $i := 1;$
  divisaocorreu := falso;
  ENQUANTO $i \leq s$ **E** *divisaocorreu* = falso **FAÇA**
    SE $\text{LT}(f_i)$ *divide* $\text{LT}(p)$ **ENTÃO**
      $q_i := q_i + \dfrac{\text{LT}(p)}{\text{LT}(f_i)};$
      $p := p - \left(\dfrac{\text{LT}(p)}{\text{LT}(f_i)}\right) f_i;$
      divisaocorreu := verdadeiro;
    SENÃO
      $i := i + 1;$
  SE *divisaocorreu* = *falso* **ENTÃO**
    $r := r + \text{LT}(p);$
    $p := p - \text{LT}(p);$
RETORNA $q_1, \ldots, q_s, r$

Observe que a variável booleana "divisaocorreu" sinaliza se existe algum $\text{LT}(f_i)$ que divide o termo líder do dividendo intermediário. Note que, a cada iteração do laço ENQUANTO principal, ocorre exatamente uma das seguintes situações:

- (Passo de Divisão) Se algum $\text{LT}(f_i)$ divide $\text{LT}(p)$, então o algoritmo procede como no caso univariado.

- (Passo do Resto) Se nenhum $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$, então o algoritmo adiciona $\mathrm{LT}(p)$ ao resto r.

Para mostrar que o algoritmo funciona, mostraremos que a igualdade

$$f = q_1 f_1 + \cdots + q_s f_s + p + r \tag{3.1}$$

se verifica a cada novo passo. Para os valores iniciais de $q_1, \ldots, q_s, p$ e r temos que $f = 0 + \cdots + 0 + f + 0$ que é claramente verdadeira. Suponhamos que (3.1) seja satisfeita para algum passo do algoritmo. Se o próximo passo for um Passo de Divisão, então algum $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$. Assim

$$q_i' = q_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$$

e

$$p' = p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i.$$

Logo,

$$q_i' f_i + p' = \left(q_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i + p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i = q_i f_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i + p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i = q_i f_i + p,$$

mostrando que $q_i f_i + p$ não é alterado. Dado que as demais variáveis não são afetadas, (3.1) permanece válida nesse caso. Por outro lado, se o próximo passo for um Passo do Resto, então p e r sofrerão alterações, mas a soma $p + r$ permanecerá a mesma, isto é

$$p' = p - \mathrm{LT}(p)$$

e

$$r' = r + \mathrm{LT}(p).$$

Logo,

$$p' + r' = p - \mathrm{LT}(p) + r + \mathrm{LT}(p) = p + r.$$

Como anteriormente, a igualdade (3.1) é preservada.

Agora, perceba que o algoritmo chega ao fim quando $p = 0$. Nesse caso, (3.1) se torna

$$f = q_1 f_1 + \cdots + q_s f_s + r.$$

Dado que termos são adicionados a r apenas se não forem divisíveis por nenhum dos $\mathrm{LT}(f_i)$, então $q_1, \ldots, q_s$ e r irão possuir as propriedades desejadas quando o algoritmo encerrar.

A seguir, devemos mostrar que, de fato, o algoritmo eventualmente termina. A observação fundamental é que a cada vez que a variável p é redefinida, ou seu multigrau diminui (em relação à nossa ordem monomial fixada) ou p se torna 0. Para que vejamos isso, suponha que

durante um Passo de Divisão, p seja redefinido para

$$p' = p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i.$$

Pelo item (i) do Lema 3.17, temos

$$\mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\right) = \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot \mathrm{LT}(f_i) = \mathrm{LT}(p),$$

logo p e $(\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$ possuem o mesmo termo líder. Desse modo, p' deve possuir um multigrau estritamente menor caso $p' \neq 0$. Em seguida, suponhamos que durante um Passo do Resto, p seja redefinido para

$$p' = p - \mathrm{LT}(p).$$

É evidente que $\mathrm{multideg}(p') \prec \mathrm{multideg}(p)$ quando $p' \neq 0$. Portanto, em ambos os casos o multigrau deve diminuir. Se o algoritmo nunca chegar ao fim, então teremos uma sequência infinita estritamente decrescente de multigraus. Devido ao fato de que $\succ$ é uma boa ordem, como visto no Lema 3.7, isso não pode ocorrer. Logo $p = 0$ ocorrerá eventualmente e então o algoritmo se encerra após uma quantidade finita de passos.

Resta estudar a relação entre $\mathrm{multideg}(f)$ e $\mathrm{multideg}(q_i f_i)$. Qualquer um dos termos que compõem q_i é da forma $\mathrm{LT}(p)/\mathrm{LT}(f_i)$ para algum valor assumido pela variável p, ou seja, cada monômio $a_\alpha x^\alpha$ adicionado a q_i terá multigrau $\alpha = \mathrm{multideg}(p) - \mathrm{multideg}(f_i)$. Sabemos que o algoritmo inicia com $p = f$, e acabamos de mostrar que o multigrau de p decresce a cada passo, portanto $\mathrm{multideg}(p) \preceq \mathrm{multideg}(f)$. Dessa maneira, escrevendo

$$q_i = \sum_\alpha a_\alpha x^\alpha,$$

temos

$$q_i f_i = \sum_\alpha a_\alpha x^\alpha f_i$$

e para cada termo

$$\mathrm{multideg}(a_\alpha x^\alpha f_i) = \alpha + \mathrm{multideg}(f_i) = \mathrm{multideg}(p) \preceq \mathrm{multideg}(f).$$

Concluímos que todos os monômios de $q_i f_i$ têm multigrau menor ou igual a $\mathrm{multideg}(f)$. Em particular, se $q_i f_i \neq 0$,

$$\mathrm{multideg}(q_i f_i) \preceq \mathrm{multideg}(f).$$

□

Nesse momento, emerge o questionamento se o algoritmo de divisão em $\mathbb{K}[x_1, \ldots, x_n]$ mantém as "boas" propriedades do algoritmo em $\mathbb{K}[x]$, como a unicidade do resto. Os exemplos a seguir mostrarão que não.

Exemplo 3.19. Dividiremos $f = x^2y + xy^2 + y^2$ por $f_1 = y^2 - 1$ e $f_2 = xy - 1$. Adotando a

ordem lexicográfica com $x \succ y$, segue que

$$\begin{array}{rrrrrrrrrrrrrrrrrrrrr}
 & x^2y & + & xy^2 & + & y^2 & & & & & & & & & y^2 & - & 1, & xy & - & 1 \\
(-) & x^2y & - & x & & & & & & & & & & & x & + & 1, & x & & \\
\cline{2-6}
 & & & xy^2 & + & x & + & y^2 & & & & & & & & & & & & \\
 & & (-) & xy^2 & - & x & & & & & & & & & & & & & & \\
\cline{3-7}
 & & & & & 2x & + & y^2 & \longrightarrow & r & = & 2x & & & & & & & & \\
\cline{5-7}
 & & & & & & & y^2 & & & & & & & & & & & & \\
 & & & & & & (-) & y^2 & - & 1 & & & & & & & & & & \\
\cline{6-8}
 & & & & & & & 1 & \longrightarrow & r & = & 2x & + & 1 & & & & & & \\
\cline{7-7}
 & & & & & & & 0 & & & & & & & & & & & &
\end{array}$$

Isso mostra que

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

Exemplo 3.20. Dividiremos $f = x^2y + xy^2 + y^2$ por $f_1 = xy - 1$ e $f_2 = y^2 - 1$. Utilizaremos a ordem lexicográfica com $x \succ y$. Perceba que estamos realizando a mesma divisão do Exemplo 3.19 apenas invertendo a ordem dos divisores. Temos

$$\begin{array}{rrrrrrrrrrrrrrrrrrrrr}
 & x^2y & + & xy^2 & + & y^2 & & & & & & & & & xy & - & 1, & y^2 & - & 1 \\
(-) & x^2y & - & x & & & & & & & & & & & x & + & y, & 1 & & \\
\cline{2-6}
 & & & xy^2 & + & x & + & y^2 & & & & & & & & & & & & \\
 & & (-) & xy^2 & - & y & & & & & & & & & & & & & & \\
\cline{3-7}
 & & & & & x & + & y^2 & + & y & \longrightarrow & r & = & x & & & & & & \\
\cline{5-9}
 & & & & & & & y^2 & + & y & & & & & & & & & & \\
 & & & & & & (-) & y^2 & - & 1 & & & & & & & & & & \\
\cline{6-8}
 & & & & & & & & & y & + & 1 & \longrightarrow & r & = & x & + & y & \\
 & & & & & & & & & & & 1 & \longrightarrow & r & = & x & + & y & + & 1 \\
\cline{9-9}
 & & & & & & & & & & & 0 & & & & & & & &
\end{array}$$

Portanto,

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

Comparando os resultados obtidos nos exemplos anteriores, é possível perceber que o resto não é caracterizado apenas pelo fato de não ser divisível por nenhum dos $\mathrm{LT}(f_i)$, o resto é dependente, também, da ordem em que os polinômios aparecem na s-upla $F = (f_1, \ldots, f_s)$ e da ordem monomial fixada.

Em relação ao problema de pertinência ao ideal, em $\mathbb{K}[x]$ temos que $f \in \langle f_1 \rangle$ se, e somente se, o resto da divisão de f por f_1 é zero. Agora, para o caso em várias variáveis, observemos que uma das implicações é um corolário do Teorema 3.18: se ao dividir f por $F = (f_1, \ldots, f_s)$ obtivermos um resto $r = 0$, então

$$f = q_1 f_1 + \cdots + q_s f_s,$$

isto é, $f \in \langle f_1, \ldots, f_s \rangle$.

Vejamos, agora, que a recíproca não é verdadeira, isto é, $r = 0$ é condição suficiente, mas não necessária, para a pertinência ao ideal gerado por $f_1, \ldots, f_s$.

Exemplo 3.21. Sejam $f_1 = xy - 1$, $f_2 = y^2 - 1 \in \mathbb{K}[x, y]$ com a ordem lexicográfica. Dividindo $f = xy^2 - x$ por $F = (f_1, f_2)$, obtemos

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

Porém, com $F = (f_2, f_1)$ temos

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

A segunda igualdade mostra que $f \in \langle f_1, f_2 \rangle$. Já a primeira evidencia que ainda é possível obter resto não nulo na divisão por $F = (f_1, f_2)$ mesmo que $f \in \langle f_1, f_2 \rangle$.

Desse modo, concluímos que o algoritmo da divisão apresentado no Teorema 3.18 é uma generalização imperfeita da sua versão para uma variável. Para contornar esse problema, ao invés de lidarmos com a coleção de polinômios $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, atacaremos o ideal I gerado por eles, pois isso nos permite passar de $f_1, \ldots, f_s$ para um outro conjunto de geradores de I. A questão que surge, então, é se existe um conjunto de geradores de I tal que o resto r da divisão de um polinômio f seja unicamente determinado e que $r = 0$ seja equivalente à pertinência de f ao ideal. Veremos que as bases de Gröbner possuem exatamente essas "boas" propriedades.

4. Bases de Gröbner

4.1 Ideais Monomiais e o Lema de Dickson

Consideremos o problema de descrição de ideais, apresentado anteriormente. Analisaremos agora esse problema no caso particular dos ideais monomiais. Para isso, faz-se necessário estudar algumas propriedades dessa classe de ideais. Comecemos, então, definindo os ideais monomiais em $\mathbb{K}[x_1, \ldots, x_n]$.

Definição 4.1. Um ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ é dito um ideal monomial se houver um subconjunto $A \subseteq \mathbb{Z}^n_{\geq 0}$, potencialmente infinito, tal que I é formado por todos os polinômios que são somas finitas da forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, com $h_\alpha \in \mathbb{K}[x_1, \ldots, x_n]$. Nesse caso, denotamos $I = \langle x^\alpha \mid \alpha \in A \rangle$.

O seguinte lema nos dará uma caracterização para todos os monômios que pertencem a um dado ideal monomial.

Lema 4.2. *Seja $I = \langle x^\alpha \mid \alpha \in A \rangle$ um ideal monomial. Temos que x^β pertence a I se, e somente se, x^β é divisível por algum x^α, com $\alpha \in A$.*

Demonstração: Se x^β é um múltiplo de x^α, então $x^\beta \in I$ pela definição do ideal. Reciprocamente, se $x^\beta \in I$, então $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, em que $h_i \in \mathbb{K}[x_1, \ldots, x_n]$ e $\alpha(i) \in A$. Se expandirmos cada h_i como soma de seus termos, obtemos

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} = \sum_{i=1}^{s} \left(\sum_j c_{i,j} x^{\beta(i,j)} \right) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}.$$

ou ainda,

$$x^\beta = \sum_{\substack{i,j \\ \beta(i,j)+\alpha(i)=\beta}} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)} + \sum_{\substack{i,j \\ \beta(i,j)+\alpha(i)\neq\beta}} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}.$$

Comparando termo a termo, como o lado esquerdo não possui nenhum termo x^γ para $\gamma \neq \beta$, o segundo somatório deve ser nulo. Além disso, o coeficiente de x^β deve ser igual a 1, isto é,

$$\sum_{\substack{i,j \\ \beta(i,j)+\alpha(i)=\beta}} c_{i,j} = 1.$$

Dessa forma, existe pelo menos um par (i, j) tal que $\beta(i, j) + \alpha(i) = \beta$, o que implica $x^\beta = x^{\beta(i,j)} \cdot x^{\alpha(i)}$. Portanto, x^β é divisível por $x^{\alpha(i)}$, com $\alpha(i) \in A$. □

Observe que x^β é divisível por x^α justamente quando $x^\beta = x^\alpha \cdot x^\gamma$ para algum $\gamma \in \mathbb{Z}^n_{\geq 0}$. Sabemos que isso equivale a $\beta = \alpha + \gamma$. Daí, o conjunto

$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma \mid \gamma \in \mathbb{Z}^n_{\geq 0}\}$$

é formado pelos expoentes de todos os monômios divisíveis por x^α. Através dessa observação e do Lema 4.2, podemos apresentar um esquema que representa os monômios em um dado ideal monomial. Por exemplo, se $I = \langle x^4y^2, x^3y^4, x^2y^5\rangle$, então os expoentes dos monômios em I formam o conjunto

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

Podemos visualizar esse conjunto como a união dos pontos de coordenadas inteiras em três cópias transladadas do primeiro quadrante do plano:

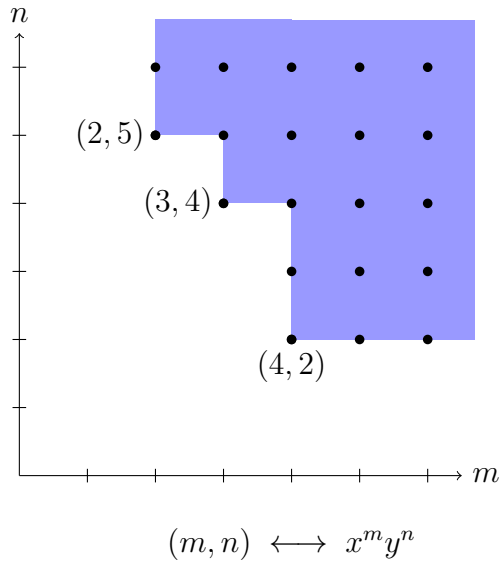

Figura 4.1: Representação visual de expoentes dos monômios em I.

Lema 4.3. *Sejam I um ideal monomial e $f \in \mathbb{K}[x_1, \ldots, x_n]$. As seguintes afirmações são equivalentes:*

(i) $f \in I$.

(ii) *Todo termo de f pertence a I.*

(iii) *f é uma combinação $\mathbb{K}$-linear de monômios em I.*

Demonstração: (iii) $\Rightarrow$ (ii): Se f é uma combinação $\mathbb{K}$-linear de monômios em I, então f pode ser escrito como $f = \sum_{i=1}^{s} a_i x^{\alpha(i)}$, com $x^{\alpha(i)} \in I$ e $a_i \in \mathbb{K} \subseteq \mathbb{K}[x_1, \ldots, x_n]$, como I é um ideal, logo $a_i x^{\alpha(i)} \in I$.

(ii) $\Rightarrow$ (i): Dado que um polinômio é a soma de seus termos, se cada termo de f pertence a I e I é fechado em relação à soma, então $f \in I$.

(i) $\Rightarrow$ (iii): Como $f \in I$, podemos escrever $f = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, com $h_i \in \mathbb{K}[x_1, \ldots, x_n]$ e $x^{\alpha(i)} \in I$. Expandindo cada h_i como soma de seus termos, obtemos

$$f = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}, \quad c_{i,j} \in \mathbb{K}$$

em que cada $x^{\beta(i,j)} x^{\alpha(i)}$ é um monômio divisível por $x^{\alpha(i)} \in I$, portanto pertence a I pelo Lema 4.2. Logo, f é uma combinação $\mathbb{K}$-linear de monômios em I.

□

Uma consequência imediata da parte (iii) do lema é que um ideal monomial é unicamente determinado por seus monômios. Assim, segue o corolário abaixo.

Corolário 4.4. *Dois ideais monomiais são iguais se, e somente se, contêm os mesmos monômios.*

Demonstração: Se dois ideais monomiais são iguais, é evidente que terão os mesmos monômios. Reciprocamente, sejam I e J ideais monomiais que contêm os mesmos monômios. Se $f \in I$, pelo item (iii) do Lema 4.3, f pode ser escrito como $f = \sum_{i=1}^{s} a_i x^{\alpha(i)}$, com $a_i \in \mathbb{K}$ e $x^{\alpha(i)} \in I$. Por hipótese, $x^{\alpha(i)} \in J$ para todo i, logo f é uma combinação $\mathbb{K}$-linear de monômios em J, e pelo mesmo lema segue que $f \in J$, ou seja, $I \subseteq J$. Analogamente, $J \subseteq I$, portanto $I = J$.

□

Teorema 4.5 (Lema de Dickson). *Seja $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ um ideal monomial. Então I pode ser escrito na forma $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, em que $\alpha(1), \ldots, \alpha(s) \in A$. Em particular, I é finitamente gerado.*

Demonstração: A demonstração será feita por indução sobre o número de variáveis n. Para o caso base $n = 1$, o ideal I é gerado por monômios da forma x_1^α, com $\alpha \in A \subseteq \mathbb{Z}_{\geq 0}$. Seja β o menor elemento de A. Como $\beta \leq \alpha$ para todo $\alpha \in A$, segue que x_1^β divide todos os demais geradores x_1^α. Portanto, $I = \langle x_1^\beta \rangle$.

Suponha $n > 1$ e que o teorema seja válido para $n-1$ variáveis. Seja $I \subseteq \mathbb{K}[x_1, \ldots, x_{n-1}, x_n]$ um ideal monomial. A fim de facilitar a notação, escreveremos $x_n = y$. Para encontrar geradores de I, tome J o ideal em $\mathbb{K}[x_1, \ldots, x_{n-1}]$ gerado pelos monômios x^α para os quais $x^\alpha y^m \in I$ para algum $m \geq 0$. Como J é um ideal monomial em $\mathbb{K}[x_1, \ldots, x_{n-1}]$, pela hipótese de indução, temos que existe um número finito de monômios da forma x^α que geram J, digamos $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Podemos pensar o ideal J como sendo a "projeção" de I sobre $\mathbb{K}[x_1, \ldots, x_{n-1}]$.

Para cada i variando de 1 até s, sabemos, pela definição de J, que $x^{\alpha(i)} y^{m_i} \in I$ para algum $m_i \geq 0$. Seja m o máximo dos m_i. Então, para todo l variando de 0 até $m-1$, considere o ideal $J_l \subseteq \mathbb{K}[x_1, \ldots, x_{n-1}]$ gerado pelos monômios x^β tais que $x^\beta y^l \in I$. Podemos pensar que os J_l capturam os monômios em x que acompanham a l-ésima potência de y em

I. Novamente pela hipótese de indução, J_l tem um conjunto finito de monômios geradores, digamos $J_l = \langle x^{\alpha_l(1)}, \ldots, x^{\alpha_l(s_l)} \rangle$.

Afirmamos que I é gerado pelos monômios das listas a seguir:

$$\begin{aligned} \text{obtidos a partir de } J &: x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m, \\ \text{obtidos a partir de } J_0 &: x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)}, \\ \text{obtidos a partir de } J_1 &: x^{\alpha_1(1)}y, \ldots, x^{\alpha_1(s_1)}y, \\ &\vdots \\ \text{obtidos a partir de } J_{m-1} &: x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}. \end{aligned}$$

Observe que qualquer monômio em I é divisível por algum dos monômios das listas. Com efeito, seja $x^\alpha y^p \in I$. Se $p \geq m$, então $x^\alpha y^p$ é divisível por algum monômio da forma $x^{\alpha(i)}y^m$ pela maneira com que J foi construído. Por outro lado, se $p \leq m-1$, então $x^\alpha y^p$ é divisível por algum $x^{\alpha_p(j)}y^p$ pela construção de J_p. Seja B o conjunto de todos os monômios presentes nas listas. Segue do Lema 4.2 que todo monômio de I pertence a $\langle B \rangle$ e, como cada monômio de B pertence a I por construção, e I é ideal, todo monômio de $\langle B \rangle$ pertence a I. Logo, I e $\langle B \rangle$ possuem os mesmos monômios e, pelo Corolário 4.4, $I = \langle B \rangle$, o que prova a afirmação.

Para completar a demonstração, é necessário mostrar que, dado um conjunto de geradores de I, é possível extrair um subconjunto finito que ainda gera I. Retomando a notação $x_1, \ldots, x_n$ para as variáveis, então nosso ideal monomial será $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Do parágrafo anterior, segue que $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$ para alguns monômios $x^{\beta(i)} \in I$. Como $I = \langle x^\alpha \mid \alpha \in A \rangle$, o Lema 4.2 nos garante que cada $x^{\beta(i)}$ é divisível por $x^{\alpha(i)}$ para algum $\alpha(i) \in A$, logo todo monômio de I está também em $\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Agora, dado um monômio $x^\alpha \in \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, novamente pelo Lema 4.2, x^α é divisível por algum $x^{\alpha(i)} \in I$, logo $x^\alpha \in I$. Pelo Corolário 4.4, conclui-se que $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, encerrando a demonstração. □

O Teorema 4.5 resolve o problema da descrição para ideais monomiais, mostrando que tais ideais possuem um conjunto finito de geradores. Isso nos permite resolver o problema de pertinência para ideais monomiais, conforme o corolário a seguir.

Corolário 4.6. *Seja $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ um ideal monomial e $f \in \mathbb{K}[x_1, \ldots, x_n]$. Então $f \in I$ se, e somente se, o resto da divisão de f por $(x^{\alpha(1)}, \ldots, x^{\alpha(s)})$ é zero.*

Demonstração: Se $f \in I$, então $f = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, com $h_i \in \mathbb{K}[x_1, \ldots, x_n]$, o que exibe f como combinação dos geradores com resto zero. Reciprocamente, se o resto da divisão de f por $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ é zero, então todo termo de f é divisível por algum $x^{\alpha(i)}$, logo, pertence a I pelo Lema 4.2. Pelo Lema 4.3, conclui-se que $f \in I$. □

Podemos utilizar o Lema de Dickson para provar o seguinte fato importante acerca de ordens monomiais sobre $\mathbb{K}[x_1, \ldots, x_n]$.

Corolário 4.7. *Seja $\succ$ uma relação sobre $\mathbb{Z}^n_{\geq 0}$ satisfazendo:*

(i) *$\succ$ é uma relação de ordem total sobre $\mathbb{Z}^n_{\geq 0}$.*

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

Logo, $\succ$ *é uma boa ordem se, e somente se,* $\alpha \succeq 0$ *para todo* $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Demonstração: Sejam $\succ$ uma boa ordem e α_0 o menor elemento de $\mathbb{Z}^n_{\geq 0}$ com respeito a $\succ$. Desse modo, basta mostrar que $\alpha_0 \succeq 0$. Suponha, por absurdo, que $0 \succ \alpha_0$, por (ii), podemos adicionar α_0 em ambos os lados e obteremos $\alpha_0 \succ 2\alpha_0$, com $2\alpha_0 \in \mathbb{Z}^n_{\geq 0}$. O que contradiz a afirmação de que α_0 é o menor elemento de $\mathbb{Z}^n_{\geq 0}$, portanto $\alpha_0 \succeq 0$.

Por outro lado, suponha $\alpha \succeq 0$ para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$ e seja $A \subseteq \mathbb{Z}^n_{\geq 0}$ não vazio. É necessário mostrar que A possui um menor elemento. Dado que $I = \langle x^\alpha \mid \alpha \in A \rangle$ é um ideal monomial, o Lema de Dickson garante a existência de $\alpha(1), \ldots, \alpha(s) \in A$ tais que $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Suponha, sem perda de generalidade, que $\alpha(1) \prec \alpha(2) \prec \cdots \prec \alpha(s)$. Afirmamos que $\alpha(1)$ é o menor dos elementos de A. Para provar a afirmação, tome $\alpha \in A$, então $x^\alpha \in I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ que implica, pelo Lema 4.2, que x^α é divisível por algum $x^{\alpha(i)}$. Assim, $\alpha = \alpha(i) + \gamma$ para algum $\gamma \in \mathbb{Z}^n_{\geq 0}$. Logo, por hipótese, $\gamma \succeq 0$ e (ii) implica que

$$\alpha = \alpha(i) + \gamma \succeq \alpha(i) + 0 = \alpha(i) \succeq \alpha(1).$$

Portanto, $\alpha(1)$ é o menor elemento de A. □

Como consequência do corolário acima, a definição de uma ordem monomial apresentada na Definição 3.6 pode ser simplificada. As condições (i) e (ii) da definição permaneceriam inalteradas, mas a condição (iii) poderia ser substituída pela condição $\alpha \succeq 0$ qualquer que seja $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Proposição 4.8. *Um ideal monomial* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *possui um conjunto de geradores* $\{x^{\alpha(1)}, \ldots, x^{\alpha(s)}\}$ *com a propriedade segundo a qual* $x^{\alpha(i)}$ *não divide* $x^{\alpha(j)}$ *com* $i \neq j$. *Além disso, esse conjunto de geradores é único e denominado* ***base mínima*** *de* I.

Demonstração: Existência: Do Teorema 4.5, I tem um conjunto finito de geradores formado por monômios. Se algum dos monômios nesse conjunto dividir outro, então podemos descartar esse outro e ainda teremos uma base. Repetindo esse processo até que não haja monômios distintos que se dividam nesse conjunto, provamos a existência da base mínima $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$.

Unicidade: Suponha que exista $x^{\beta(1)}, \ldots, x^{\beta(t)}$ uma segunda base mínima de I. Como $x^{\alpha(1)} \in I$, do Lema 4.2 segue que $x^{\beta(i)} \mid x^{\alpha(1)}$ para algum i. Da mesma maneira para a outra base, $x^{\beta(i)} \in I$ e novamente do Lema 4.2 segue que $x^{\alpha(j)} \mid x^{\beta(i)}$ para algum j. Por transitividade, temos que $x^{\alpha(j)} \mid x^{\alpha(1)}$, logo a minimalidade implica $j = 1$. Daí, temos

$$x^{\beta(i)} \mid x^{\alpha(1)} \quad \text{e} \quad x^{\alpha(1)} \mid x^{\beta(i)}.$$

Logo, existem $\gamma, \delta \in \mathbb{Z}^n_{\geq 0}$ tais que

$$x^{\beta(i)} = x^{\alpha(1)} \cdot x^\gamma \quad \text{e} \quad x^{\alpha(1)} = x^{\beta(i)} \cdot x^\delta.$$

Isso implica

$$x^{\alpha(1)} = x^{\alpha(1)} \cdot x^{\gamma} \cdot x^{\delta} = x^{\alpha(1)} \cdot x^{\gamma+\delta},$$

$$x^{\gamma+\delta} = 1,$$

$$\gamma + \delta = (0, \ldots, 0).$$

Como $\gamma, \delta \in \mathbb{Z}^n_{\geq 0}$, possuem todas as entradas não negativas, então $\gamma = \delta = (0, \ldots, 0)$. Portanto $x^{\gamma} = x^{\delta} = 1$, e conclui-se que $x^{\beta(i)} = x^{\alpha(1)}$. □

4.2 O Teorema da Base de Hilbert e as Bases de Gröbner

O estudo desenvolvido a seguir nos conduzirá a bases de ideais com "boas" propriedades em relação ao algoritmo da divisão apresentado anteriormente. A ideia fundamental é que a escolha de uma ordem monomial confere a cada polinômio não nulo $f \in \mathbb{K}[x_1, \ldots, x_n]$ um termo líder único $\mathrm{LT}(f)$. Desse modo, dado um ideal I, podemos definir o ideal de seus termos líderes como segue.

Definição 4.9. Seja $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ um ideal diferente de $\{0\}$ e fixada uma ordem monomial sobre $\mathbb{K}[x_1, \ldots, x_n]$. Então:

(i) Denotaremos por $\mathrm{LT}(I)$ o conjunto dos termos líderes de elementos não nulos de I. Isto é,

$$\mathrm{LT}(I) = \{cx^{\alpha} \mid \exists f \in I \setminus \{0\} \text{ tal que } \mathrm{LT}(f) = cx^{\alpha}\}.$$

(ii) Denotaremos por $\langle \mathrm{LT}(I) \rangle$ o ideal gerado pelos elementos de $\mathrm{LT}(I)$.

Vimos anteriormente que os termos líderes dos polinômios desempenham um papel importante no algoritmo da divisão. Assim, é importante que foquemos em um detalhe sutil envolvendo o ideal $\langle \mathrm{LT}(I) \rangle$. Mais especificamente, dado um conjunto finito de geradores de I, digamos $I = \langle f_1, \ldots, f_s \rangle$, os ideais $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ e $\langle \mathrm{LT}(I) \rangle$ podem ser distintos. É evidente que $\mathrm{LT}(f_i) \in \mathrm{LT}(I) \subseteq \langle \mathrm{LT}(I) \rangle$ por definição, o que implica $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \subseteq \langle \mathrm{LT}(I) \rangle$. No entanto, $\langle \mathrm{LT}(I) \rangle$ pode ser estritamente maior. A fim de ilustrar tal possibilidade, considere o exemplo a seguir.

Exemplo 4.10. Sejam $f_1 = x^3 - 2xy$ e $f_2 = x^2y - 2y^2 + x$, e considere $I = \langle f_1, f_2 \rangle$, adotando-se a ordem lexicográfica graduada sobre os monômios de $\mathbb{K}[x, y]$. Então

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

de modo que $x^2 \in I$. Portanto, $x^2 = \mathrm{LT}(x^2) \in \langle \mathrm{LT}(I) \rangle$. No entanto, x^2 não é divisível nem por $\mathrm{LT}(f_1) = x^3$ nem por $\mathrm{LT}(f_2) = x^2y$, implicando que $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$ pelo Lema 4.2.

Agora, mostraremos que $\langle \mathrm{LT}(I) \rangle$ é um ideal monomial. Isso nos permitirá aplicar os resultados obtidos acerca de tais ideais. Em particular, seremos capazes de concluir que $\langle \mathrm{LT}(I) \rangle$ é gerado por uma quantidade finita de termos líderes.

Proposição 4.11. *Seja $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ um ideal diferente de $\{0\}$ e fixada uma ordem monomial sobre $\mathbb{K}[x_1, \ldots, x_n]$. Então:*

(i) $\langle \mathrm{LT}(I) \rangle$ *é um ideal monomial.*

(ii) *Existem $g_1, \ldots, g_t \in I$ tais que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.*

Demonstração: (i) Os monômios líderes $\mathrm{LM}(g)$ de elementos $g \in I \setminus \{0\}$ geram o ideal monomial $\langle \mathrm{LM}(g) \mid g \in I \setminus \{0\} \rangle$. Como $\mathrm{LT}(g) = \mathrm{LC}(g) \cdot \mathrm{LM}(g)$ com $\mathrm{LC}(g) \in \mathbb{K}$ e $\mathrm{LC}(g) \neq 0$, temos que $\mathrm{LT}(g)$ é uma combinação $\mathbb{K}$-linear de monômios em $\langle \mathrm{LM}(g) \mid g \in I \setminus \{0\} \rangle$. Pelo item (iii) do Lema 4.3, conclui-se que $\mathrm{LT}(g)$ pertence ao ideal $\langle \mathrm{LM}(g) \mid g \in I \setminus \{0\} \rangle$, isto é,

$$\langle \mathrm{LT}(g) \mid g \in I \setminus \{0\} \rangle \subseteq \langle \mathrm{LM}(g) \mid g \in I \setminus \{0\} \rangle.$$

De maneira análoga, basta ver que $\mathrm{LM}(g) = \mathrm{LC}(g)^{-1} \cdot \mathrm{LT}(g)$, assim

$$\langle \mathrm{LM}(g) \mid g \in I \setminus \{0\} \rangle \subseteq \langle \mathrm{LT}(g) \mid g \in I \setminus \{0\} \rangle.$$

Portanto, $\langle \mathrm{LM}(g) \mid g \in I \setminus \{0\} \rangle = \langle \mathrm{LT}(g) \mid g \in I \setminus \{0\} \rangle = \langle \mathrm{LT}(I) \rangle$.

(ii) Dado que $\langle \mathrm{LT}(I) \rangle$ é gerado pelos monômios de $\langle \mathrm{LM}(g) \mid g \in I \setminus \{0\} \rangle$, o Lema de Dickson (Teorema 4.5) nos diz que existem $g_1, \ldots, g_t \in I$ tais que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t) \rangle$. Como cada $\mathrm{LT}(g_i)$ difere de $\mathrm{LM}(g_i)$ por uma constante não nula, segue que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

□

Usaremos a seguir a Proposição 4.11 e o algoritmo da divisão para provar a existência de um conjunto finito de geradores para qualquer ideal de polinômios em $\mathbb{K}[x_1, \ldots, x_n]$.

Teorema 4.12 (**Teorema da Base de Hilbert**). *Qualquer ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ é finitamente gerado. Em outras palavras, $I = \langle g_1, \ldots, g_t \rangle$ com $g_1, \ldots, g_t \in I$.*

Demonstração: Se $I = \{0\}$, então tomamos $\{0\}$ como conjunto gerador que é, de fato, finito. Se I possui um polinômio não identicamente nulo, então um conjunto finito de geradores pode ser construído como será visto a seguir.

Primeiramente, fixamos uma ordem monomial a fim de aplicar o algoritmo da divisão e de obter os termos líderes. Dessa forma, I possui um ideal de termos líderes $\langle \mathrm{LT}(I) \rangle$. Da Proposição 4.11, sabemos que existem $g_1, \ldots, g_t \in I$ tais que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Afirmamos que $I = \langle g_1, \ldots, g_t \rangle$.

É imediato que $\langle g_1, \ldots, g_t \rangle \subseteq I$, pois cada $g_i \in I$. Reciprocamente, seja $f \in I$ um polinômio qualquer. Aplicando o algoritmo da divisão para dividir f por $(g_1, \ldots, g_t)$, obtemos uma expressão da forma

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

em que nenhum termo de r é divisível por nenhum dos $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Afirmamos que $r = 0$. Para provar essa afirmação, observe que

$$r = f - q_1 g_1 - \cdots - q_t g_t \in I.$$

Se $r \neq 0$, então $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ e, pelo Lema 4.2, segue que $\mathrm{LT}(r)$ deve ser divisível por algum $\mathrm{LT}(g_i)$, o que contraria o fato de r ser o resto da divisão. Portanto, $r = 0$. Dessa maneira,

$$f = q_1 g_1 + \cdots + q_t g_t \in \langle g_1, \ldots, g_t \rangle$$

o que confirma que $I \subseteq \langle g_1, \ldots, g_t \rangle$. Daí, concluímos que $I = \langle g_1, \ldots, g_t \rangle$. □

Como vimos no Exemplo 4.10, nem toda base de um ideal satisfaz $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. No entanto, a base $\{g_1, \ldots, g_t\}$ construída na demonstração do Teorema 4.12 possui exatamente essa propriedade. Logo abaixo daremos a tais bases uma nomenclatura especial.

Definição 4.13. Fixada uma ordem monomial sobre o anel de polinômios $\mathbb{K}[x_1, \ldots, x_n]$, um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ diferente de $\{0\}$ é dito ser uma **base de Gröbner** se

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

Usando a convenção de que $\langle \emptyset \rangle = \{0\}$, definimos o conjunto vazio $\emptyset$ como sendo a base de Gröbner do ideal nulo $\{0\}$.

De maneira equivalente, um conjunto $\{g_1, \ldots, g_t\} \subseteq I$ é uma base de Gröbner de I se, e somente se, o termo líder de qualquer elemento não nulo de I é divisível por algum dos $\mathrm{LT}(g_i)$. Tal fato segue diretamente do Teorema 4.12 e do Lema 4.2.

Corolário 4.14. *Fixada uma ordem monomial, todo ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ possui uma base de Gröbner. Além disso, toda base de Gröbner de um ideal I é uma base de I.*

Demonstração: Dado um ideal não nulo, o conjunto $G = \{g_1, \ldots, g_t\}$ como construído na demonstração do Teorema 4.12 é uma base de Gröbner por definição. Já para a segunda afirmação, observe que se $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, então a argumentação apresentada no Teorema 4.12 prova que $I = \langle g_1, \ldots, g_t \rangle$, isto é, G é um conjunto de geradores de I. □

As bases de Gröbner são aqueles conjuntos de geradores de um ideal I, com as "boas" propriedades, ou ainda, as propriedades desejáveis em relação ao algoritmo da divisão multivariada. Estudaremos, em um momento posterior, as propriedades de tais bases.

Vejamos alguns exemplos relacionados às bases de Gröbner.

Exemplo 4.15. Consideremos o ideal I do Exemplo 4.10, que possui $\{f_1, f_2\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$ como conjunto de geradores. No entanto, $\{f_1, f_2\}$ não é uma base de Gröbner para

I com respeito à ordem lexicográfica graduada, pois, como vimos, $x^2 \in \langle \mathrm{LT}(I) \rangle$, mas $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$.

Exemplo 4.16. Considere o ideal $J = \langle g_1, g_2 \rangle = \langle x + z, y - z \rangle$. Afirmamos que g_1 e g_2 formam uma base de Gröbner para J, adotando a ordem lexicográfica sobre $\mathbb{R}[x, y, z]$. Assim, devemos provar que $\langle \mathrm{LT}(J) \rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2) \rangle = \langle x, y \rangle$. Como a inclusão $\langle x, y \rangle \subseteq \langle \mathrm{LT}(J) \rangle$ é trivial, pois $g_1, g_2 \in J$, basta provar que o termo líder de cada elemento não identicamente nulo de J pertence a $\langle x, y \rangle$. Equivalentemente, pelo Lema 4.2 é suficiente mostrar que o termo líder de qualquer elemento não identicamente nulo de J é divisível por x ou y.

A fim de provar isso, tome

$$f = A \cdot (x + z) + B \cdot (y - z) \in J, \quad \text{com} \quad A, B \in \mathbb{R}[x, y, z].$$

Suponha, por contradição, que f é não nulo e que $\mathrm{LT}(f)$ não é divisível por x nem por y. Então, pela definição de ordem lexicográfica, f deve ser um polinômio apenas na indeterminada z. Assim, tem-se

$$f(z) = A(x, y, z) \cdot (x + z) + B(x, y, z) \cdot (y - z).$$

Qualquer que seja $t \in \mathbb{R}$, considere o ponto $(x, y, z) = (-t, t, t)$, logo

$$f(t) = A(-t, t, t) \cdot (-t + t) + B(-t, t, t) \cdot (t - t)$$

$$f(t) = A(-t, t, t) \cdot 0 + B(-t, t, t) \cdot 0$$

$$f(t) = 0, \quad \forall t \in \mathbb{R}.$$

Portanto, f é identicamente nulo, contradizendo a hipótese de que $f \neq 0$. Assim, fica provada a afirmação inicial.

Vejamos, agora, uma aplicação do Teorema da Base de Hilbert. Essa aplicação consiste em um enunciado algébrico acerca dos ideais em $\mathbb{K}[x_1, \ldots, x_n]$. Uma cadeia ascendente de ideais é uma sequência aninhada crescente:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots .$$

A título de exemplo, a sequência

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \cdots \subseteq \langle x_1, x_2, \ldots, x_n \rangle$$

forma uma cadeia ascendente finita de ideais. Para tal sequência, ao tentarmos estender essa cadeia através da inclusão de um outro ideal com uma quantidade maior de geradores, uma das seguintes situações ocorre para o ideal $\langle x_1, \ldots, x_n, f \rangle$, com $f \in \mathbb{K}[x_1, \ldots, x_n]$:

(i) Se $f \in \langle x_1, \ldots, x_n \rangle$, então $\langle x_1, \ldots, x_n, f \rangle = \langle x_1, \ldots, x_n \rangle$, ou seja, permanecemos com o mesmo ideal.

(ii) Se $f \notin \langle x_1, \ldots, x_n \rangle$, então afirmamos que $\langle x_1, \ldots, x_n, f \rangle = \mathbb{K}[x_1, \ldots, x_n]$.

Para verificar esse fato, basta provar que $\langle x_1, \ldots, x_n \rangle$ é um ideal maximal, ou de forma equivalente, pelo Teorema 2.11, que o anel quociente $\mathbb{K}[x_1, \ldots, x_n]/\langle x_1, \ldots, x_n \rangle$ é um corpo. Para tal, mostraremos que

$$\mathbb{K}[x_1, \ldots, x_n]/\langle x_1, \ldots, x_n \rangle \cong \mathbb{K}.$$

Considere a função a seguir:

$$\varphi : \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}, \qquad f \mapsto f(0, \ldots, 0).$$

A função φ é homomorfismo de anéis, isto é, dados $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ temos

$$\varphi(f+g) = (f+g)(0, \ldots, 0) = f(0, \ldots, 0) + g(0, \ldots, 0) = \varphi(f) + \varphi(g)$$

e

$$\varphi(fg) = (fg)(0, \ldots, 0) = f(0, \ldots, 0) \cdot g(0, \ldots, 0) = \varphi(f)\varphi(g).$$

Além disso, φ é sobrejetor, já que todo $c \in \mathbb{K}$ é imagem do polinômio constante $f = c$. Por fim, $\mathrm{N}(\varphi) = \langle x_1, \ldots, x_n \rangle$, pois $f \in \mathrm{N}(\varphi)$ se, e somente se, $f(0, \ldots, 0) = 0$, isto é, f não possui termo constante, o que equivale a $f \in \langle x_1, \ldots, x_n \rangle$. Pelo primeiro Teorema do Isomorfismo, concluímos que $\mathbb{K}[x_1, \ldots, x_n]/\langle x_1, \ldots, x_n \rangle \cong \mathbb{K}$ e, como $\mathbb{K}$ é um corpo, segue que $\langle x_1, \ldots, x_n \rangle$ é maximal.

Como consequência, a cadeia $\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \cdots \subseteq \langle x_1, x_2, \ldots, x_n \rangle$ poderá continuar apenas de duas formas, seja pela repetição do último ideal de maneira indiscriminada, seja tornando-se igual a $\mathbb{K}[x_1, \ldots, x_n]$ e sua posterior repetição infinita. De qualquer maneira, a cadeia crescente terá "estabilizado" após um número finito de passos, ou seja, todos os ideais a partir de certo ponto da cadeia serão iguais. O resultado a seguir mostra que o mesmo fenômeno ocorre em qualquer cadeia ascendente de ideais em $\mathbb{K}[x_1, \ldots, x_n]$.

Teorema 4.17 (**Condição de Cadeia Ascendente**). *Seja*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

uma cadeia ascendente de ideais sobre $\mathbb{K}[x_1, \ldots, x_n]$. *Então, existe um* $N \in \mathbb{N}$ *de tal modo que*

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

Demonstração: Dada a cadeia ascendente $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$, consideremos o seguinte conjunto $I = \bigcup_{i=1}^{\infty} I_i$. Primeiramente, mostremos que I é um ideal sobre $\mathbb{K}[x_1, \ldots, x_n]$. O elemento $0 \in I$ dado que $0 \in I_i$ para qualquer i. Tomando $f, g \in I$, temos, pela definição de I, que $f \in I_i$ e $g \in I_j$ para algum par (i, j). No entanto, como os ideais I_i formam uma cadeia ascendente, podemos supor, sem perda de generalidade, que $i \leq j$, o que implica que tanto f quanto g pertencem a I_j. Como I_j é um ideal, a soma $f + g \in I_j$, logo $f + g \in I$. Da mesma

forma, tomando $f \in I$ e $r \in \mathbb{K}[x_1, \ldots, x_n]$, temos $f \in I_i$ para algum i e $rf \in I_i \subseteq I$. Portanto, I é um ideal.

Do Teorema da Base de Hilbert, sabemos que o ideal I deve possuir um conjunto finito de geradores, isto é, $I = \langle f_1, \ldots, f_s \rangle$. Dado que cada um dos geradores vem de algum dos I_j, digamos $f_i \in I_{j_i}$ para algum j_i, com $i = 1, \ldots, s$. Tomamos N como o máximo dos j_i. Então, pela definição de cadeia ascendente, $f_i \in I_N$ para todo i. Logo, temos

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

Dessa maneira, podemos dizer que a cadeia ascendente de ideais estabiliza em I_N, ou seja, qualquer ideal I_i, com $i \geq N$, é igual a I_N. □

A afirmação de que toda cadeia ascendente de ideais sobre $\mathbb{K}[x_1, \ldots, x_n]$ eventualmente estabiliza é chamada, em geral, de **Condição de Cadeia Ascendente**, ou CCA, de forma abreviada. Vejamos agora que a Condição de Cadeia Ascendente é equivalente à conclusão do Teorema da Base de Hilbert. Isto é, tomando a CCA como hipótese, segue que todo ideal é finitamente gerado.

Teorema 4.18. *Se toda cadeia ascendente de ideais*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

em $\mathbb{K}[x_1, \ldots, x_n]$ *é estacionária, isto é, existe* $N \in \mathbb{N}$ *tal que*

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

então todo ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *é finitamente gerado.*

Demonstração: Suponha, por contradição, que exista um ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ que não é finitamente gerado. Em particular, $I \neq \{0\}$, pois $\{0\} = \langle 0 \rangle$. Dessa maneira, podemos escolher $g_1 \in I$, com g_1 não identicamente nulo, e definir $I_1 = \langle g_1 \rangle$. Como I não é finitamente gerado, temos $I_1 \neq I$, de modo que existe $g_2 \in I \setminus I_1$. Definindo $I_2 = \langle g_1, g_2 \rangle$ e repetindo o argumento, obtemos $g_3 \in I \setminus I_2$. Continuando esse processo, constrói-se uma sequência $g_1, g_2, g_3, \ldots$ de elementos de I tal que

$$g_{m+1} \notin \langle g_1, \ldots, g_m \rangle$$

para todo m. Definindo $I_m = \langle g_1, \ldots, g_m \rangle$, obtemos uma cadeia ascendente de ideais

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots.$$

Essa cadeia é estritamente crescente, pois $g_{m+1} \in I_{m+1}$, mas $g_{m+1} \notin I_m$. Sendo assim, a cadeia nunca estabiliza, contradizendo a Condição de Cadeia Ascendente. Portanto, todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ é finitamente gerado. □

4.3 Propriedades das Bases de Gröbner

Tendo sido estabelecida a existência de bases de Gröbner para quaisquer ideais não nulos de $\mathbb{K}[x_1, \ldots, x_n]$, passa-se agora ao estudo de suas propriedades. Nosso objetivo será também compreender como verificar se uma determinada base constitui, de fato, uma base de Gröbner.

Mostremos, em primeiro lugar, que o resto da divisão é unicamente determinado quando realizamos a divisão pelos elementos de uma base de Gröbner.

Proposição 4.19. *Seja $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ um ideal, e seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para I. Então, para cada $f \in \mathbb{K}[x_1, \ldots, x_n]$, existe um único $r \in \mathbb{K}[x_1, \ldots, x_n]$ satisfazendo as duas propriedades seguintes:*

(i) *Nenhum dos termos de r é divisível por nenhum dos $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.*

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

Dessa maneira, r é o resto da divisão de f por G qualquer que seja a ordenação escolhida para os elementos de G no algoritmo da divisão.

Demonstração: Pelo algoritmo da divisão, segue que $f = q_1 g_1 + \cdots + q_t g_t + r$, em que r satisfaz (i). A propriedade (ii) pode ser satisfeita tomando $g = q_1 g_1 + \cdots + q_t g_t \in I$. Assim, está provada a existência de r.

A fim de provar a unicidade, suponha que $f = g + r = g' + r'$, com ambas decomposições satisfazendo (i) e (ii). Então, $r - r' = g' - g \in I$. Se tivermos $r \neq r'$, logo $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Do Lema 4.2, temos que $\mathrm{LT}(r - r')$ é divisível por algum dos $\mathrm{LT}(g_i)$, o que é impossível, dado que nenhum dos termos de r ou de r' é divisível por nenhum dos $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Portanto, $r - r'$ deve ser nulo, isto é, $r - r' = 0$, ou ainda, $r = r'$. Dessa maneira, temos

$$g' - g = r - r' = 0,$$

$$g' = g.$$

E a unicidade está provada. □

O resto r é por vezes denominado *forma normal* de f. Mesmo quando se trabalha com uma base de Gröbner, a unicidade do resto r não garante a unicidade dos "quocientes" q_i. De fato, na expressão obtida pelo algoritmo da divisão, $f = q_1 g_1 + \cdots + q_t g_t + r$, os polinômios q_i podem variar caso os geradores sejam apresentados em outra ordem.

Como corolário da Proposição 4.19, obtemos o critério a seguir para quando um dado polinômio pertence a um ideal.

Corolário 4.20. *Sejam $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ e $f \in \mathbb{K}[x_1, \ldots, x_n]$. Temos que $f \in I$ se, e somente se, o resto de f na divisão por G é zero.*

Demonstração: Sabemos que G é uma base de Gröbner de I, isto é, $I = \langle G \rangle$. Se o resto da divisão de f por G é zero, então f é, por definição, elemento de I. Reciprocamente, dado $f \in I$, logo $f = f + 0$ satisfaz ambas as condições apresentadas na Proposição 4.19. Dessa forma, conclui-se que 0 é o resto da divisão de f por G. □

Por vezes, a propriedade apresentada no Corolário 4.20 pode ser adotada como definição de uma base de Gröbner, pois é possível mostrar que tal propriedade é verdadeira se, e somente se, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

É através do Corolário 4.20 que obtemos um algoritmo que resolve o problema de pertinência ao ideal, desde que conheçamos uma base de Gröbner G para o ideal em questão: basta calcular o resto de f na divisão por G para determinar se $f \in I$ ou não. Posteriormente, neste texto, estabeleceremos um algoritmo para a obtenção de uma base de Gröbner e, dessa forma, solucionaremos de maneira completa o problema de pertinência ao ideal.

Adotaremos, agora, a seguinte notação para o resto.

Definição 4.21. Denotaremos por $\overline{f}^F$ 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 considerar F como um conjunto, sem qualquer ordem particular, pela Proposição 4.19.

Para ilustrar, tomemos $F = (x^2y - y^2,\ x^4y^2 - y^2) \subseteq \mathbb{K}[x, y]$, com a ordem lexicográfica. Nesse caso, o resto da divisão de x^5y por F é dado por

$$\overline{x^5y}^F = xy^3.$$

De fato, pelo algoritmo da divisão, obtemos

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3.$$

Discutiremos agora como reconhecer se um determinado conjunto de geradores de um ideal é uma base de Gröbner. Como visto anteriormente, o principal entrave para que um conjunto $\{f_1, \ldots, f_s\}$ seja uma base de Gröbner está na possível existência de polinômios resultantes da combinação dos f_i cujos termos líderes não pertençam ao ideal gerado por $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$.

Esse fenômeno pode ocorrer quando, em uma combinação adequada,

$$ax^\alpha f_i - bx^\beta f_j$$

há cancelamento dos termos líderes, restando apenas termos de ordem menor. Por outro lado,

$$ax^\alpha f_i - bx^\beta f_j \in I,$$

logo, seu termo líder pertence a $\langle \mathrm{LT}(I) \rangle$.

A fim de estudar esse fenômeno de cancelamento, introduzimos as combinações especiais a seguir.

Definição 4.22. Sejam $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ polinômios não nulos.

(i) Se $\text{multideg}(f) = \alpha$ e $\text{multideg}(g) = \beta$, então definimos $\gamma = (\gamma_1, \ldots, \gamma_n)$, em que

$$\gamma_i = \max\{\alpha_i, \beta_i\}$$

para cada i. Chamamos x^γ de **mínimo múltiplo comum** de $\text{LM}(f)$ e $\text{LM}(g)$, denotado por

$$x^\gamma = \text{mmc}(\text{LM}(f), \text{LM}(g)).$$

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

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

(Observe que, aqui, também estamos invertendo os coeficientes líderes.)

Consideremos, por exemplo, os polinômios $f = x^3y^2 - x^2y^3 + x$ e $g = 3x^4y + y^2$ em $\mathbb{R}[x,y]$, adotando a ordem lexicográfica graduada.

Nessa ordem, temos

$$\text{multideg}(f) = (3,2), \qquad \text{multideg}(g) = (4,1).$$

Assim, tomando o máximo coordenada a coordenada, obtemos

$$\gamma = (\max\{3,4\}, \max\{2,1\}) = (4,2).$$

Portanto,

$$S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = xf - \frac{1}{3}yg.$$

Substituindo f e g, segue que

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

Observe que os termos líderes x^4y^2 se cancelam, como esperado pela construção do S-polinômio.

O lema a seguir mostra que todo cancelamento de termos líderes entre polinômios de mesmo multigrau decorre do cancelamento presente nos S-polinômios.

Lema 4.23. *Suponha que tenhamos uma soma* $\sum_{i=1}^{s} p_i$, *em que* $\text{multideg}(p_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ *qualquer que seja* i. *Se* $\text{multideg}\left(\sum_{i=1}^{s} p_i\right) \prec \delta$, *então* $\sum_{i=1}^{s} p_i$ *é uma combinação linear, com coeficientes em* $\mathbb{K}$, *dos S-polinômios* $S(p_j, p_l)$, *para* $1 \leq j, l \leq s$. *Além disso, cada* $S(p_j, p_l)$ *possui multigrau menor que* δ.

Demonstração: Seja $d_i = \mathrm{LC}(p_i)$, de modo que $d_i x^\delta$ é o termo líder de p_i. Dado que a soma $\sum_{i=1}^{s} p_i$ possui multigrau estritamente menor que δ, o coeficiente do monômio x^δ nessa soma deve ser nulo, isto é, $\sum_{i=1}^{s} d_i = 0$.

Agora, vejamos que, como p_i e p_j possuem o mesmo monômio líder, ao calcular $S(p_i, p_j)$ obtemos

$$\begin{aligned} S(p_i, p_j) &= \frac{x^\delta}{\mathrm{LT}(p_i)} p_i - \frac{x^\delta}{\mathrm{LT}(p_j)} p_j \\ &= \frac{x^\delta}{d_i x^\delta} p_i - \frac{x^\delta}{d_j x^\delta} p_j \\ &= \frac{1}{d_i} p_i - \frac{1}{d_j} p_j. \end{aligned}$$

Essa igualdade torna evidente que $\mathrm{multideg}(S(p_i, p_j)) \prec \delta$. Além disso, segue que

$$\begin{aligned} \sum_{i=1}^{s-1} d_i S(p_i, p_s) &= d_1 \left(\frac{1}{d_1} p_1 - \frac{1}{d_s} p_s \right) + d_2 \left(\frac{1}{d_2} p_2 - \frac{1}{d_s} p_s \right) + \cdots + d_{s-1} \left(\frac{1}{d_{s-1}} p_{s-1} - \frac{1}{d_s} p_s \right) \\ &= p_1 + p_2 + \cdots + p_{s-1} - \frac{1}{d_s} (d_1 + d_2 + \cdots + d_{s-1}) p_s \\ &= p_1 + p_2 + \cdots + p_{s-1} - \frac{1}{d_s} \left(\sum_{i=1}^{s} d_i - d_s \right) p_s \\ &= p_1 + p_2 + \cdots + p_{s-1} - \frac{1}{d_s} (-d_s) p_s \\ &= p_1 + p_2 + \cdots + p_{s-1} + p_s. \end{aligned}$$

Portanto, $\sum_{i=1}^{s} p_i$ é uma combinação $\mathbb{K}$-linear de S-polinômios, conforme queríamos demonstrar. □

Sob as hipóteses do Lema 4.23, para os polinômios $p_1, \ldots, p_s$, obtemos uma igualdade da seguinte forma:

$$\sum_{i=1}^{s} p_i = \sum_{j,l} c_{jl} S(p_j, p_l).$$

Analisemos agora onde ocorrem os cancelamentos. No somatório à esquerda, cada parcela p_i possui multigrau δ, logo o cancelamento ocorre após a soma de todas elas. Já no somatório à direita, cada parcela $c_{jl} S(p_j, p_l)$ possui multigrau menor que δ, isto é, o cancelamento já ocorreu.

Antes de apresentarmos o Critério de Buchberger, que caracteriza bases de Gröbner para um dado ideal, registramos dois lemas auxiliares que serão utilizados em sua demonstração. O primeiro formaliza o fato de que o S-polinômio é construído precisamente para cancelar os termos líderes dos polinômios envolvidos, garantindo uma queda no multigrau. O segundo relaciona os S-polinômios obtidos a partir de certos múltiplos monomiais dos geradores com os S-polinômios dos próprios geradores. Essas observações permitirão simplificar a demonstração

do critério.

Lema 4.24. *Sejam $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ não nulos e $x^\gamma = \text{mmc}(\text{LM}(f), \text{LM}(g))$. Se $S(f,g) \neq 0$, então* $\text{multideg}(S(f,g)) \prec \gamma$.

Demonstração: Sejam $f = \sum_\alpha a_\alpha x^\alpha$ e $g = \sum_\beta b_\beta x^\beta$. Definamos $\alpha_0 = \text{multideg}(f)$ e $\beta_0 = \text{multideg}(g)$. Assim, escrevemos $f = a_{\alpha_0}x^{\alpha_0} + \sum_{\alpha \prec \alpha_0} a_\alpha x^\alpha$ e $g = b_{\beta_0}x^{\beta_0} + \sum_{\beta \prec \beta_0} b_\beta x^\beta$. Seja $x^\gamma = \text{mmc}(x^{\alpha_0}, x^{\beta_0})$.

Calculando $\dfrac{x^\gamma}{\text{LT}(f)} f$ obtemos

$$\frac{x^\gamma}{\text{LT}(f)} f = \frac{1}{a_{\alpha_0}} x^{\gamma-\alpha_0}\left(a_{\alpha_0}x^{\alpha_0} + \sum_{\alpha \prec \alpha_0} a_\alpha x^\alpha\right) = x^\gamma \; + \sum_{\alpha \prec \alpha_0} \frac{a_\alpha}{a_{\alpha_0}}\, x^{\gamma-\alpha_0+\alpha}.$$

Analogamente,

$$\frac{x^\gamma}{\text{LT}(g)} g = x^\gamma \; + \sum_{\beta \prec \beta_0} \frac{b_\beta}{b_{\beta_0}}\, x^{\gamma-\beta_0+\beta}.$$

Subtraindo, o termo x^γ cancela, resultando

$$S(f,g) = \sum_{\alpha \prec \alpha_0} \frac{a_\alpha}{a_{\alpha_0}}\, x^{\gamma-\alpha_0+\alpha} \; - \sum_{\beta \prec \beta_0} \frac{b_\beta}{b_{\beta_0}}\, x^{\gamma-\beta_0+\beta}.$$

Resta mostrar que todo expoente que aparece nessa expressão é estritamente menor que γ. Dado que toda ordem monomial é compatível com a adição, isto é, $\alpha \prec \alpha_0$ implica $\alpha + \delta \prec \alpha_0 + \delta$ para qualquer $\delta \in \mathbb{Z}^n_{\geq 0}$. Tomando $\delta = \gamma - \alpha_0$

$$\alpha + (\gamma - \alpha_0) \prec \alpha_0 + (\gamma - \alpha_0) = \gamma \quad \text{para todo } \alpha \prec \alpha_0,$$

e, da mesma forma, $\beta + (\gamma - \beta_0) \prec \gamma$ para todo $\beta \prec \beta_0$.

Logo todo monômio de $S(f,g) = \sum_{\alpha \prec \alpha_0} \frac{a_\alpha}{a_{\alpha_0}} x^{\gamma-\alpha_0+\alpha} - \sum_{\beta \prec \beta_0} \frac{b_\beta}{b_{\beta_0}} x^{\gamma-\beta_0+\beta}$ tem expoente menor que γ. Portanto, se $S(f,g) \neq 0$ então $\text{multideg}(S(f,g)) \prec \gamma$. □

Lema 4.25. *Sejam $g_i, g_j \in \mathbb{K}[x_1, \ldots, x_n]$ não nulos, com $i \neq j$, e $x^{\gamma_{ij}} = \text{mmc}(\text{LM}(g_i), \text{LM}(g_j))$. Sejam $h_i, h_j \in \mathbb{K}[x_1, \ldots, x_n]$ tais que, pondo $p_i = \text{LT}(h_i)g_i$ e $p_j = \text{LT}(h_j)g_j$, vale*

$$\text{multideg}(p_i) = \text{multideg}(p_j) = \delta.$$

Então:

(i) $x^{\gamma_{ij}}$ *divide* x^δ, *isto é,* $\delta \in \gamma_{ij} + \mathbb{Z}^n_{\geq 0}$.

(ii) $S(p_i, p_j) = x^{\delta-\gamma_{ij}} S(g_i, g_j)$.

Demonstração: (i) Como $\mathrm{LT}(p_i) = \mathrm{LT}(h_i)\,\mathrm{LT}(g_i)$, a hipótese $\mathrm{multideg}(p_i) = \delta$ diz que $\mathrm{LM}(h_i)\cdot \mathrm{LM}(g_i) = x^\delta$, ou seja, $x^{\mathrm{multideg}(g_i)}$ divide x^δ, o que equivale a

$$\delta \in \mathrm{multideg}(g_i) + \mathbb{Z}^n_{\geq 0}.$$

Aplicando o mesmo argumento a p_j, obtemos $\delta \in \mathrm{multideg}(g_j) + \mathbb{Z}^n_{\geq 0}$. Logo

$$\delta \ \in \ \Big(\mathrm{multideg}(g_i) + \mathbb{Z}^n_{\geq 0}\Big) \cap \Big(\mathrm{multideg}(g_j) + \mathbb{Z}^n_{\geq 0}\Big).$$

Escrevendo $\alpha = \mathrm{multideg}(g_i)$ e $\beta = \mathrm{multideg}(g_j)$, afirmamos que essa interseção é exatamente $\gamma_{ij} + \mathbb{Z}^n_{\geq 0}$, onde $x^{\gamma_{ij}} = \mathrm{mmc}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$. De fato, δ pertence a $(\alpha + \mathbb{Z}^n_{\geq 0}) \cap (\beta + \mathbb{Z}^n_{\geq 0})$ se, e somente se, $\delta - \alpha \in \mathbb{Z}^n_{\geq 0}$ e $\delta - \beta \in \mathbb{Z}^n_{\geq 0}$, isto é, se, e somente se, cada entrada de δ é maior ou igual à entrada correspondente de α e à entrada correspondente de β. Como cada entrada de γ_{ij} é, por definição, o maior valor entre as entradas correspondentes de α e β, essa condição equivale a dizer que cada entrada de δ é maior ou igual à entrada correspondente de γ_{ij}, ou seja, $\delta - \gamma_{ij} \in \mathbb{Z}^n_{\geq 0}$. Concluímos, portanto, que

$$\delta \in \gamma_{ij} + \mathbb{Z}^n_{\geq 0}$$

ou de forma equivalente, $x^{\gamma_{ij}} | x^\delta$.
(ii) Como $\mathrm{multideg}(p_i) = \mathrm{multideg}(p_j) = \delta$, temos $\mathrm{mmc}(\mathrm{LM}(p_i), \mathrm{LM}(p_j)) = x^\delta$ e, pela definição de S-polinômio,

$$\begin{aligned} S(p_i, p_j) &= \frac{x^\delta}{\mathrm{LT}(p_i)} p_i - \frac{x^\delta}{\mathrm{LT}(p_j)} p_j \\ &= \frac{x^\delta}{\mathrm{LT}(h_i)\,\mathrm{LT}(g_i)}\,\mathrm{LT}(h_i) g_i - \frac{x^\delta}{\mathrm{LT}(h_j)\,\mathrm{LT}(g_j)}\,\mathrm{LT}(h_j) g_j \\ &= \frac{x^\delta}{\mathrm{LT}(g_i)} g_i - \frac{x^\delta}{\mathrm{LT}(g_j)} g_j. \end{aligned}$$

Por (i), $x^\delta = x^{\delta - \gamma_{ij}} x^{\gamma_{ij}}$, logo

$$S(p_i, p_j) = x^{\delta - \gamma_{ij}} \left(\frac{x^{\gamma_{ij}}}{\mathrm{LT}(g_i)} g_i - \frac{x^{\gamma_{ij}}}{\mathrm{LT}(g_j)} g_j \right) = x^{\delta - \gamma_{ij}} S(g_i, g_j).$$

□

A partir dos S-polinômios e dos lemas anteriores, podemos agora demonstrar o seguinte Critério de Buchberger, que caracteriza quando um conjunto de geradores de um ideal é uma base de Gröbner.

Teorema 4.26 (**Critério de Buchberger**). *Fixada uma ordem monomial sobre $\mathbb{K}[x_1, \ldots, x_n]$, seja I um ideal. Um conjunto de geradores $G = \{g_1, \ldots, g_t\}$ de I é uma base de Gröbner para I, com respeito a essa ordem, se, e somente se, para todo par (i, j) com $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por G é zero, qualquer que seja a ordem em que os elementos de G estejam listados.*

Demonstração: Se G é uma base de Gröbner, então como $S(g_i, g_j) \in I$, pelo Corolário 4.20, o resto da sua divisão por G deve ser zero.

Reciprocamente, seja $f \in I$ não nulo. Mostraremos que $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Representemos f por

$$f = \sum_{i=1}^{t} h_i g_i, \quad h_i \in \mathbb{K}[x_1, \ldots, x_n].$$

Do Lema 3.17, segue que

$$\mathrm{multideg}(f) \preceq \max\{\mathrm{multideg}(h_i g_i) \mid h_i g_i \neq 0\}. \tag{4.1}$$

Nessa demonstração, a estratégia será escolher a representação mais eficiente para f, isto é, dentre todas as representações $f = \sum_{i=1}^{t} h_i g_i$, tomaremos aquela em que

$$\delta = \max\{\mathrm{multideg}(h_i g_i) \mid h_i g_i \neq 0\}$$

é mínimo. A existência de um δ mínimo é garantida pela propriedade de boa ordenação da ordem monomial escolhida. Pela desigualdade (4.1), tem-se que $\mathrm{multideg}(f) \preceq \delta$.

Se a igualdade ocorre, então $\mathrm{multideg}(f) = \mathrm{multideg}(h_i g_i)$ para algum i. Lembrando que $\mathrm{multideg}(h_i g_i) = \mathrm{multideg}(h_i) + \mathrm{multideg}(g_i)$, isso implica que

$$\mathrm{multideg}(f) \in \mathrm{multideg}(g_i) + \mathbb{Z}^n_{\geq 0}$$

o que é precisamente a condição de $\mathrm{LT}(g_i)$ dividir $\mathrm{LT}(f)$. Portanto, $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

Resta-nos agora considerar o caso em que o δ mínimo satisfaz $\mathrm{multideg}(f) \prec \delta$. Usaremos para isso o fato de que $\overline{S(g_i, g_j)}^{G} = 0$ quando $i \neq j$ para obter uma nova expressão para f em que $\max\{\mathrm{multideg}(h_i g_i) \mid h_i g_i \neq 0\} \prec \delta$, contradizendo, dessa forma, a minimalidade de δ.

Dada uma expressão $f = \sum_{i=1}^{t} h_i g_i$ com δ mínimo, comecemos por separar as parcelas do somatório que possuem multigrau igual a δ.

$$\begin{aligned} f &= \sum_{\mathrm{multideg}(h_i g_i) = \delta} h_i g_i + \sum_{\mathrm{multideg}(h_i g_i) \prec \delta} h_i g_i \\ &= \sum_{\mathrm{multideg}(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i + \sum_{\mathrm{multideg}(h_i g_i) = \delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{\mathrm{multideg}(h_i g_i) \prec \delta} h_i g_i. \end{aligned} \tag{4.2}$$

Os monômios que aparecem na segunda e terceira somas da segunda linha têm multigrau menor que δ. Como $\mathrm{multideg}(f) \prec \delta$, a primeira soma dessa mesma linha terá, também, multigrau menor que δ.

A estratégia para obter uma nova expressão para f com $\max\{\mathrm{multideg}(h_i g_i) \mid h_i g_i \neq 0\} \prec \delta$ consiste em reescrever a primeira soma em duas etapas. Primeiro, aplicamos o Lema 4.25 para expressá-la em termos de S-polinômios dos próprios g_i, g_j. Em seguida, usamos o fato de que $\overline{S(g_i, g_j)}^{G} = 0$ para reescrever esses S-polinômios sem cancelamentos.

Para escrever a primeira soma da segunda linha de (4.2) em termos de S-polinômios, observe que

$$\sum_{\text{multideg}(h_i g_i)=\delta} \text{LT}(h_i)g_i \tag{4.3}$$

satisfaz as hipóteses do Lema 4.23. De fato, tomando $p_i = \text{LT}(h_i)g_i$, cada p_i tem multigrau δ, enquanto a soma tem multigrau menor que δ. Portanto, essa soma pode ser escrita como uma combinação $\mathbb{K}$-linear de S-polinômios $S(p_i, p_j)$.

Pelo Lema 4.25, aplicado a cada par (i, j) que aparece em (4.3), segue que esse somatório é combinação $\mathbb{K}$-linear de termos da forma $x^{\delta-\gamma_{ij}}S(g_i, g_j)$.

Dado que $\overline{S(g_i, g_j)}^{G} = 0$, qualquer que seja o par (i, j) com $i \neq j$, o algoritmo da divisão multivariada nos permite escrever

$$S(g_i, g_j) = \sum_{l=1}^{t} A_l g_l, \tag{4.4}$$

em que $A_l \in \mathbb{K}[x_1, \ldots, x_n]$. Além disso, para todo índice l tal que $A_l g_l \neq 0$, temos

$$\text{multideg}(A_l g_l) \preceq \text{multideg}(S(g_i, g_j)). \tag{4.5}$$

Multiplicando ambos os lados de (4.4) por $x^{\delta-\gamma_{ij}}$, obtemos

$$x^{\delta-\gamma_{ij}}S(g_i, g_j) = \sum_{l=1}^{t} B_l g_l, \tag{4.6}$$

onde $B_l = x^{\delta-\gamma_{ij}}A_l$. A desigualdade (4.5) implica que, sempre que $B_l g_l \neq 0$,

$$\text{multideg}(B_l g_l) \preceq \text{multideg}\Big(x^{\delta-\gamma_{ij}}S(g_i, g_j)\Big) = (\delta - \gamma_{ij}) + \text{multideg}(S(g_i, g_j)). \tag{4.7}$$

Pelo Lema 4.24 aplicado ao par (g_i, g_j), temos $\text{multideg}(S(g_i, g_j)) \prec \gamma_{ij}$. Logo

$$\text{multideg}(B_l g_l) \prec (\delta - \gamma_{ij}) + \gamma_{ij} = \delta, \tag{4.8}$$

para todo l tal que $B_l g_l \neq 0$.

Do exposto acima podemos concluir que

$$\sum_{\text{multideg}(h_i g_i)=\delta} \text{LT}(h_i)g_i = \sum_{l=1}^{t} \tilde{B}_l g_l \tag{4.9}$$

tal que $\text{multideg}(\tilde{B}_l g_l) \prec \delta$ quando $\tilde{B}_l g_l \neq 0$.

Substituindo (4.9) de volta na segunda linha de (4.2), obtemos uma nova representação para f como combinação dos elementos de G em que todas as parcelas têm multigrau estritamente menor que δ, o que contradiz a minimalidade de δ.

Essa contradição mostra que o caso $\text{multideg}(f) \prec \delta$ não pode ocorrer, isto é, deve valer $\text{multideg}(f) = \delta$, situação já tratada acima, na qual concluímos que $\text{LT}(f) \in$

$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Como $f \in I$ foi tomado de forma arbitrária, isso prova que $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$, ou seja, G é uma base de Gröbner para I. □

O Critério de Buchberger, apresentado anteriormente, figura como uma ferramenta fundamental no estudo das bases de Gröbner, pois permite verificar se um dado conjunto de geradores de um ideal I é, de fato, uma base de Gröbner desse ideal. A seguir, veremos como esse critério aponta para um procedimento algorítmico capaz de produzir bases de Gröbner.

4.4 Algoritmo de Buchberger

A existência de bases de Gröbner para todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ já foi garantida no Corolário 4.14. Contudo, esse resultado não nos forneceu uma maneira de construir tais conjuntos de geradores. Sendo assim, o estudo a seguir tem como objetivo conduzir à construção de um procedimento para a obtenção de bases de Gröbner a partir de um conjunto de geradores de um dado ideal I.

Exemplo 4.27. Fixada a ordem lexicográfica graduada sobre $\mathbb{Q}[x, y]$, seja $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy,\ x^2y - 2y^2 + x \rangle$. Como $\mathrm{mmc}(\mathrm{LM}(f_1), \mathrm{LM}(f_2)) = \mathrm{mmc}(x^3, x^2y) = x^3y$, temos

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

Como $S(f_1, f_2) \in I$, temos $\mathrm{LT}(S(f_1, f_2)) = -x^2 \in \mathrm{LT}(I)$. No entanto, nem $x^3 = \mathrm{LT}(f_1)$ nem $x^2y = \mathrm{LT}(f_2)$ dividem $-x^2$, segue do Lema 4.2 que $-x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$. Logo,

$$\langle \mathrm{LT}(I) \rangle \neq \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle,$$

e, portanto, $\{f_1, f_2\}$ não é uma base de Gröbner para I.

Ampliaremos o conjunto inicial de geradores do ideal, como estratégia para construir uma base de Gröbner para ele. Assim, incorporamos $f_3 = -x^2$ ao conjunto de geradores.

Consideremos agora $F = (f_1, f_2, f_3)$. Pelo Critério de Buchberger, devemos verificar os restos das reduções dos S-polinômios. Como $S(f_1, f_2) = f_3$, temos imediatamente

$$\overline{S(f_1, f_2)}^{F} = 0.$$

Além disso, $S(f_1, f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy$, e seu resto na divisão por F é o próprio polinômio $\overline{S(f_1, f_3)}^{F} = -2xy \neq 0$. Assim, acrescentamos mais um gerador, $f_4 = -2xy$.

Tomemos agora $F = (f_1, f_2, f_3, f_4)$. Já sabemos que

$$\overline{S(f_1, f_2)}^{F} = \overline{S(f_1, f_3)}^{F} = 0.$$

Além disso, $S(f_1, f_4) = y(x^3 - 2xy) - \left(-\frac{1}{2}x^2\right)(-2xy) = -2xy^2 = yf_4$, de modo que

$$\overline{S(f_1, f_4)}^{F} = 0.$$

Por outro lado,

$$S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x,$$

cujo resto da divisão por F continua sendo não nulo:

$$\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0.$$

Portanto, adicionamos o gerador

$$f_5 = -2y^2 + x.$$

Finalmente, considerando

$$F = (f_1, f_2, f_3, f_4, f_5),$$

verifica-se que $\overline{S(f_i, f_j)}^F = 0$, $1 \leq i < j \leq 5$. Assim, pelo Critério de Buchberger,

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

é uma base de Gröbner de I com respeito à ordem lexicográfica graduada.

Vejamos, então, um teorema que formaliza o processo realizado acima.

Teorema 4.28 (**Algoritmo de Buchberger**). *Seja $I = \langle f_1, \ldots, f_s\rangle \neq \{0\}$ um ideal polinomial. Então, uma base de Gröbner para I pode ser construída através de uma quantidade finita de passos de acordo com o seguinte algoritmo:*

Algoritmo 2: Algoritmo de Buchberger

Entrada: $F = (f_1, \ldots, f_s)$
Saída: *Uma base de Gröbner $G = (g_1, \ldots, g_t)$ para I, com $F \subseteq G$*

```
G := F;
REPITA
    G' := G;
    PARA CADA par {p, q}, p ≠ q em G' FAÇA
        r := S(p, q)^{G'};
        SE r ≠ 0 ENTÃO
            G := G ∪ {r};
ATÉ QUE G = G';
RETORNA G
```

Demonstração: Se $G = \{g_1, \ldots, g_t\}$, então $\langle G\rangle$ e $\langle \mathrm{LT}(G)\rangle$ denotam os ideais a seguir:

$$\langle G\rangle = \langle g_1, \ldots, g_t\rangle$$

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

Comecemos por mostrar que $G \subseteq I$ vale em qualquer etapa do algoritmo. A afirmação é verdadeira inicialmente, e sempre que aumentamos G, o fazemos pela adição do resto $r = \overline{S(p,q)}^{G'}$ para $p, q \in G' \subseteq G$. Assim, se $G \subseteq I$, então p, q e, portanto, $S(p,q)$ pertencem a I. Como o algoritmo da divisão multivariável garante que $r = S(p,q) - (q_1 g_1 + \cdots + q_k g_k)$, com $g_i \in G' \subseteq I$ e $q_i \in \mathbb{K}[x_1, \ldots, x_n]$, concluímos que $r \in I$, e portanto $G \cup \{r\} \subseteq I$. Observamos ainda que F é sempre um subconjunto de G, logo G é uma base para I.

O algoritmo chega ao fim quando $G = G'$, isto é, quando $r = \overline{S(p,q)}^{G'} = 0$ para todo $p, q \in G'$. Dessa forma, pelo Teorema 4.26, conclui-se que o algoritmo se encerra quando G é uma base de Gröbner para $\langle G \rangle = I$.

Agora, resta provar que o algoritmo eventualmente se encerra. Vejamos o que ocorre após cada etapa do laço principal. Como o conjunto G é obtido pela adição dos restos não nulos dos S-polinômios a G' (o G anterior), então

$$\langle \mathrm{LT}(G') \rangle \subseteq \langle \mathrm{LT}(G) \rangle \tag{4.10}$$

dado que $G' \subseteq G$. No entanto, se $G' \neq G$, afirmamos que $\langle \mathrm{LT}(G') \rangle$ será estritamente menor que $\langle \mathrm{LT}(G) \rangle$. De forma a provar a afirmação, suponha que um resto r não nulo de algum S-polinômio foi acrescido a G. Tendo em vista que r é um resto na divisão por G', $\mathrm{LT}(r)$ não é divisível por nenhum dos termos líderes dos elementos de G'. Assim, pelo Lema 4.2, $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$. Por outro lado, como r foi acrescido a G, temos $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$. Isso demonstra a afirmação.

De (4.10), os ideais $\langle \mathrm{LT}(G') \rangle$ resultantes de sucessivas iterações do laço principal do pseudocódigo formam uma cadeia ascendente de ideais sobre $\mathbb{K}[x_1, \ldots, x_n]$. Portanto, a CCA (Teorema 4.17) garante que tal cadeia estabiliza após uma quantidade finita de iterações. Logo, $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$ deve ocorrer eventualmente, o que implica $G' = G$. Concluímos, assim, que o algoritmo termina após um número finito de passos. □

Podemos observar que o algoritmo apresentado no Teorema 4.28 pode ser otimizado. Note que, se em uma dada etapa obtivermos $\overline{S(p,q)}^{G'} = 0$, então esse resto permanecerá nulo independentemente da adjunção de novos geradores nas etapas subsequentes do laço principal. Isso porque, ao adicionarmos novos geradores f_j um a um, será necessário analisar apenas os S-polinômios $\overline{S(f_i, f_j)}^{G'}$ para $1 \leq i \leq j-1$, uma vez que os pares considerados em etapas anteriores não precisam ser recalculados.

Além disso, é possível que uma base de Gröbner produzida pelo algoritmo de Buchberger contenha elementos redundantes. Vejamos, a seguir, um resultado que permite eliminar esses geradores desnecessários sem que o conjunto deixe de ser uma base de Gröbner.

Lema 4.29. *Seja G uma base de Gröbner para um ideal I com respeito a uma ordem monomial. Seja $p \in G$ um polinômio tal que $\mathrm{LT}(g) \mid \mathrm{LT}(p)$ para algum $g \in G$ com $g \neq p$. Então $G \setminus \{p\}$ é também uma base de Gröbner para I.*

Demonstração: Seja $f \in I$ um polinômio arbitrário. Queremos mostrar que $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G \setminus \{p\})\rangle$, isto é, pelo Lema 4.2, que existe um polinômio de $G \setminus \{p\}$ cujo termo líder divide $\mathrm{LT}(f)$.

Se $\mathrm{LT}(p) \nmid \mathrm{LT}(f)$, então, como G é uma base de Gröbner para I, existe algum $g \in G$ tal que $\mathrm{LT}(g) \mid \mathrm{LT}(f)$, em que $g \neq p$, pois, caso contrário, $\mathrm{LT}(p) \mid \mathrm{LT}(f)$. Logo, $g \in G \setminus \{p\}$.

Por outro lado, se $\mathrm{LT}(p) \mid \mathrm{LT}(f)$, por hipótese existe $g \in G \setminus \{p\}$ tal que $\mathrm{LT}(g) \mid \mathrm{LT}(p)$ e, por transitividade, $\mathrm{LT}(g) \mid \mathrm{LT}(f)$. Portanto, em ambos os casos, $G \setminus \{p\}$ é uma base de Gröbner para I.

□

Utilizando o lema anterior para eliminar os geradores desnecessários e normalizando os coeficientes líderes para que sejam iguais a 1, obtemos uma forma mais simples de uma base de Gröbner, denominada **base de Gröbner mínima**. Nessa situação, para quaisquer $p, g \in G$ distintos, tem-se

$$\mathrm{LT}(g) \nmid \mathrm{LT}(p),$$

isto é, nenhum termo líder é divisível pelo termo líder de outro elemento da base.

Exemplo 4.30. Dada a base de Gröbner

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

do ideal $I = \langle x^3 - 2xy,\ x^2y - 2y^2 + x\rangle$, obtida no Exemplo 4.27, calculemos agora uma base de Gröbner mínima de I. Sob a ordem lexicográfica graduada, os termos líderes de $f_1, \ldots, f_5$ são

$$\mathrm{LT}(f_1) = x^3, \quad \mathrm{LT}(f_2) = x^2y, \quad \mathrm{LT}(f_3) = -x^2, \quad \mathrm{LT}(f_4) = -2xy, \quad \mathrm{LT}(f_5) = -2y^2.$$

Como x^2 divide x^3, o gerador f_1 é redundante. Além disso, x^2 também divide x^2y, de modo que o gerador f_2 é igualmente redundante. Removendo f_1 e f_2, resta o conjunto $\{f_3, f_4, f_5\}$, em que $\mathrm{LT}(f_i) \nmid \mathrm{LT}(f_j)$ para quaisquer $i \neq j$.

Sendo assim, resta apenas normalizar os coeficientes líderes para 1. Multiplicando f_3 por -1, f_4 por $-\frac{1}{2}$ e f_5 por $-\frac{1}{2}$, obtemos a base mínima

$$G_{\min} = \left\{ x^2,\ xy,\ y^2 - \tfrac{1}{2}x \right\}.$$

Segue diretamente da Proposição 4.8 que, dada uma base de Gröbner mínima G de I, o conjunto de geradores de $\langle \mathrm{LT}(G)\rangle$ é único, ou seja, quaisquer duas bases de Gröbner mínimas de I possuem o mesmo conjunto de termos líderes $\mathrm{LT}(G)$. Entretanto, uma base de Gröbner mínima não é, em geral, única.

Definição 4.31. Uma base de Gröbner G para um ideal polinomial I é chamada de **base de Gröbner reduzida**, em relação a uma ordem monomial fixada, se:

(i) $\mathrm{LC}(p) = 1$ para todo $p \in G$.

(ii) Para todo $p \in G$, nenhum monômio de p é divisível por $\mathrm{LT}(g)$ para qualquer $g \in G$ com $p \neq g$.

Teorema 4.32. *Seja I um ideal não nulo de $\mathbb{K}[x_1, \ldots, x_n]$. Então, fixada uma ordem monomial, existe uma única base de Gröbner reduzida para I.*

Demonstração: (Existência): Seja G uma base de Gröbner mínima para I. Dizemos que um elemento $g \in G$ está *completamente reduzido* em relação a G quando nenhum dos monômios de g é divisível pelo termo líder de qualquer elemento de $G \setminus \{g\}$. Essa propriedade independe da base de Gröbner mínima escolhida, pois, como visto anteriormente, quaisquer duas bases de Gröbner mínimas de I possuem o mesmo conjunto de termos líderes.

Agora, para cada $g \in G$, substituímos g pelo resto $\overline{g}^{G\setminus\{g\}}$. Como G é uma base de Gröbner mínima, o termo líder de g não é divisível pelo termo líder de nenhum elemento de $G \setminus \{g\}$, logo passa diretamente para o resto. Assim,

$$\mathrm{LT}\left(\overline{g}^{G\setminus\{g\}}\right) = \mathrm{LT}(g).$$

Logo, substituir g por $\overline{g}^{G\setminus\{g\}}$ não altera o conjunto dos termos líderes da base e, consequentemente, o conjunto obtido continua sendo uma base de Gröbner mínima para I.

Além disso, pela propriedade do algoritmo da divisão, nenhum monômio do resto $\overline{g}^{G\setminus\{g\}}$ é divisível pelo termo líder de qualquer elemento de $G\setminus\{g\}$. Portanto, $\overline{g}^{G\setminus\{g\}}$ está completamente reduzido em relação à nova base. Repetindo esse procedimento para todos os elementos de G, obtemos uma base de Gröbner reduzida para I.

(Unicidade): Sejam G e H duas bases de Gröbner reduzidas para o ideal I. Sendo assim, G e H possuem o mesmo conjunto de termos líderes, isto é, $\mathrm{LT}(G) = \mathrm{LT}(H)$. Logo, para qualquer $g \in G$, existirá $h \in H$ de tal forma que $\mathrm{LT}(g) = \mathrm{LT}(h)$.

Consideremos, então, o polinômio $g - h$. Como $g, h \in I$, segue que $g - h \in I$. Além disso, como G é base de Gröbner para I, tem-se que $\overline{g-h}^{G} = 0$. Por outro lado, os termos líderes se cancelam em $g - h$ e, pelo fato de que G e H são bases reduzidas, nenhum dos termos restantes é divisível por nenhum dos $\mathrm{LT}(G) = \mathrm{LT}(H)$. Portanto, $\overline{g-h}^{G} = g - h$ e daí $g - h = 0$, o que implica $g = h$. □

Diante do exposto, conclui-se que a teoria das bases de Gröbner ocupa um lugar de destaque na Álgebra Comutativa e na Geometria Algébrica contemporâneas, pois fornece um método efetivo para lidar com ideais polinomiais em várias indeterminadas. Antes de sua introdução por Buchberger, problemas fundamentais, como a decisão sobre a pertinência de um polinômio a um ideal e a determinação de um conjunto finito de geradores, permaneciam sem uma solução algorítmica satisfatória no caso multivariado. Ao estender de maneira consistente as propriedades do algoritmo da divisão univariada para várias variáveis, as bases de Gröbner passaram a desempenhar papel central em áreas tão diversas quanto a Geometria Algébrica computacional, a Criptografia e a Teoria de Códigos. Assim, compreender essa teoria oferece uma porta de entrada para um vasto conjunto de aplicações modernas, o que reforça a rele-

vância de seu estudo tanto para a formação matemática quanto para o desenvolvimento de ferramentas computacionais aplicadas.

Referências Bibliográficas

[1] COX, D. A.; LITTLE, J.; O'SHEA, D. *Ideals, Varieties, and Algorithms*: An introduction to computational algebraic geometry and commutative algebra. 4. ed. Cham: Springer, 2015. (Undergraduate Texts in Mathematics).

[2] HERNANDES, M. E. *Um Primeiro Contato com Bases de Gröbner*. Rio de Janeiro: IMPA, 2011. (28º Colóquio Brasileiro de Matemática).

[3] GONÇALVES, A. *Introdução à Álgebra*. 6. ed. Rio de Janeiro: IMPA, 2017.

[4] HEFEZ, A. *Curso de Álgebra*. Rio de Janeiro: IMPA, 2014. (Coleção Matemática Universitária).