Universidade Federal de Uberlândia
Faculdade de Matemática
Curso de Graduação em Matemática

# BASES DE GRÖBNER E OS TEOREMAS DE HILBERT

Victor Cruz Borges



Uberlândia-MG
2023

**Victor Cruz Borges**

# BASES DE GRÖBNER E OS TEOREMAS DE HILBERT

**Monografia** apresentada ao Curso de Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para a obtenção de título de **LICENCIATURA EM MATEMÁTICA**.

**Área de concentração:** Matemática
**Linha de pesquisa:** Geometria algébrica

**Orientador(a):** Victor Gonzalo Lopez Neumann



Uberlândia-MG
2023

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

B732 2023

Borges, Victor Cruz, 2001-
Bases de Gröbner e os Teoremas de Hilbert [recurso eletrônico] / Victor Cruz Borges. - 2023.

Orientador: Victor Gonzalo Lopez Neumann.
Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Uberlândia, Graduação em Matemática.
Modo de acesso: Internet.
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. I. Neumann, Victor Gonzalo Lopez,1974-, (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**
Faculdade de Matemática
Av. João Naves de Àvila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3239-4158/4156/4126 - www.famat.ufu.br - famat@ufu.br

# ATA DE DEFESA - GRADUAÇÃO

| | | | | | |
|---|---|---|---|---|---|
| Curso de Graduação em: | Matemática | | | | |
| Defesa de: | Trabalho de Conclusão de Curso 2 (FAMAT31804) | | | | |
| Data: | 23/11/2023 | Hora de início: | 09h00min | Hora de encerramento: | 10h30min |
| Matrícula do Discente: | 11911MAT001 | | | | |
| Nome do Discente: | Victor Cruz Borges | | | | |
| Título do Trabalho: | **Bases de Gröbner e os Teoremas de Hilbert** | | | | |
| A carga horária curricular foi cumprida integralmente? | ( x ) Sim ( ) Não | | | | |

Reuniu-se na Sala 1F129, Campus Santa Mônica, da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Curso de Graduação em Matemática, assim composta pelos Professores: Prof. Dr. Guilherme Chaud Tizziotti– FAMAT/UFU, Profa. Dra. Adriana Rodrigues da Silva - FAMAT/UFU e o Prof. Dr. Victor Gonzalo Lopez Neumann – FAMAT/UFU, orientador do candidato.

Iniciando os trabalhos, o presidente da mesa, Prof. Dr. Victor Gonzalo Lopez Neumann, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao discente a palavra, para a exposição do seu trabalho. A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do curso.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando a candidato:

(x) Aprovado ( ) Reprovado

Nota: 100

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 23/11/2023, às 10:47, 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 **Guilherme Chaud Tizziotti**, **Professor(a) do Magistério Superior**, em 23/11/2023, às 10:56, 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 **Adriana Rodrigues da Silva**, **Professor(a) do Magistério Superior**, em 23/11/2023, às 11:04, 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 **4967036** e o código CRC **ECEEC235**.

**Referência:** Processo nº 23117.080371/2023-50 SEI nº 4967036

# Agradecimentos

Agradeço aos meus pais pelo amor e suporte incondicional, e também à minha família pelo apoio e torcida. Vocês são minha inspiração! Amo vocês.

Expresso minha gratidão ao Programa de Educação Tutorial (PET) por todas as experiências, pelos colegas e amigos que conheci. Como bolsista do PET Matemática na Universidade Federal de Uberlândia, também agradeço ao Programa de Educação Tutorial da SESu/MEC pelo fomento.

Aos meus colegas de turma que me acompanharam desde 2019 até aqui, em especial a Fernanda Flor, Gabriel Mucci, Laura Goulart, Mateus Fernando, Victor Patrick, Júlia Bernardes e Selma Araújo. Sem vocês, minha graduação não teria sido a mesma!

Agradeço aos meus colegas de apartamento, Samuel e Salomão, que foram grandes parceiros desde minha chegada em Uberlândia. Vocês são muito importantes para mim, e desejo todo o sucesso do mundo para vocês!

Aos professores de matemática que tive no ensino básico, obrigado por abrirem meu coração para a matemática: Marilda, Adriano, Gisele, Mauro e Marcelo. Especial agradecimento à minha professora de português, Jéssica, que encantou-me com a metodologia de suas aulas e foi minha inspiração para seguir na carreira docente.

Agradeço aos professores que tive durante a graduação, especialmente a Marcus (Bronzi), Érika, Santos, Luís Renato, Luciana, Dylene, Fabiana, Olenir, Guilherme, Geraldo, Rodolfo, Elisa, Ana Cláudia e aos orientadores durante esse período: Germano, Cícero e Victor (querido Gonzalo). Vocês foram fundamentais para minha formação como professor, matemático e, quem sabe, futuro pesquisador!

À banca examinadora que aceitou o convite e dedicou-se a ler e avaliar este estudo, juntamente com meu orientador, os professores Guilherme Chaud Tizziotti e Adriana Rodrigues da Silva.

À Universidade Federal de Uberlândia (UFU), por proporcionar um estudo gratuito e de qualidade, através do trabalho de todos os seus colaboradores que a mantêm em funcionamento, desde o corpo docente até os terceirizados. Em especial, agradeço aos espaços esportivos promovidos pela minha atlética A.A.A. Exatas UFU e pela UFU como um todo, que foram pontos de entretenimento essenciais para mim durante a faculdade.

Agradeço a Deus por estar sempre comigo.

A você, leitor(a), que chegou ao final desta página, o meu sincero agradecimento.

# Resumo

Nesse trabalho apresentaremos as Bases de Gröbner, que são conjuntos de polinômios que simplificam a resolução de sistemas de equações polinomiais ao estabelecer uma ordenação entre polinômios de $\mathbb{K}[x_1,\ldots,x_n]$. Também falaremos sobre os Teorema dos Zeros de Hilbert que é uma ideia fundamental na geometria algébrica que relaciona ideais em $\mathbb{K}[x_1,\ldots,x_n]$ com variedades afins, mostrando que cada variedade tem um ideal associado e vice-versa. Esses conceitos têm um impacto significativo na matemática, permitindo traduzir problemas geométricos em problemas algébricos e estabelecendo uma profunda conexão entre a álgebra e a geometria.

**Palavras-chave:** Bases de Gröbner; polinômios; ideais; variedades.

# Abstract

In this work, we will present Gröbner Bases, which are sets of polynomials that simplify the resolution of systems of polynomial equations by establishing an ordering among polynomials in $\mathbb{K}[x_1,\ldots,x_n]$. We will also discuss the Hilbert's Nullstellensatz, which is a fundamental idea in algebraic geometry that relates ideals in $\mathbb{K}[x_1,\ldots,x_n]$ to affine varieties, showing that each variety has an associated ideal and vice versa. These concepts have a significant impact on mathematics, enabling the translation of geometric problems into algebraic ones and establishing a deep connection between algebra and geometry.

**Keywords:** Gröbner bases; polynomials; ideals; varieties.

# Sumário

**Introdução** **6**

**1 Geometria, Álgebra e Algumas Relações** **8**

1.1 Definições e Exemplos . . . . . 8

1.2 Variedades Afins . . . . . 10

1.3 Ideais . . . . . 12

**2 Bases de Gröbner** **17**

2.1 Ordenando os monômios em $\mathbb{K}[x_1,\ldots,x_n]$ . . . . . 17

2.2 Um algoritmo de divisão em $\mathbb{K}[x_1,\ldots,x_n]$ . . . . . 24

2.3 Ideais Monomiais e o Lema de Dickson . . . . . 28

2.4 O Teorema da Base de Hilbert e Bases de Gröbner. . . . . 32

2.5 Propriedades das Bases de Gröbner . . . . . 38

2.6 O Algoritmo de Buchberger . . . . . 43

**3 Uma Conexão entre Álgebra e Geometria** **49**

3.1 Os Teoremas da Extensão e Eliminação . . . . . 49

3.2 O Teorema dos Zeros de Hilbert . . . . . 51

3.3 Ideais Radicais e a Correspondência Ideal-Variedade . . . . . 57

**Referências Bibliográficas** **63**

# Introdução

A geometria algébrica é um ramo da matemática que estuda a interação entre a álgebra e a geometria. Utiliza conceitos e métodos algébricos para investigar as propriedades geométricas das soluções de sistemas de equações polinomiais. As variedades afins, que são conjuntos de soluções dessas equações, desempenham um papel central nessa área. Sua abordagem combina ferramentas analíticas e geométricas, proporcionando uma compreensão profunda das relações entre álgebra e geometria no contexto matemático.

Sob a orientação de Wolfgang Gröbner, a teoria de Bases de Gröbner foi desenvolvida por Bruno Buchberger, em sua tese de doutorado [1], durante a década de 1960. O problema principal da tese de Bruno era determinar um método para encontrar uma base para um ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$. Veremos adiante que um dos maiores problemas para se trabalhar com polinômios em $\mathbb{K}[x_1,\ldots,x_n]$ é que o algoritmo da divisão não se comporta como no caso da divisão com apenas uma variável. Quando lidamos com polinômios em uma única variável e coeficientes num corpo, a divisão euclidiana tem unicamente determinados o quociente e o resto. No caso de várias variáveis, a ordenação das variáveis, assim como a ordenação da divisão tem um impacto na divisão. Os dois principais algoritmos presentes na teoria são o Algoritmo da Divisão e o Algoritmo de Buchberger. Além disso, o presente trabalho visa apresentar uma introdução ao estudo de ideais e variedades afins e alguns resultados sobre suas relações.

No Capítulo 1, recordamos assuntos de álgebra abstrata, mais precisamente, revisamos conceitos como anéis, domínios, corpos e estudamos o que são ideais. Além disso, apresentaremos o conceito de variedades afins. As principais referências para esse capítulo são [4], [5], [6] e [7].

No Capítulo 2, apresentamos uma introdução ao estudo de Bases de Gröbner. Mais especificamente, abordamos formas de ordenar monômios em $\mathbb{K}[x_1,\ldots,x_n]$, como dividir polinômios em $\mathbb{K}[x_1,\ldots,x_n]$, definimos o que são Bases de Gröbner de um ideal, porquê elas são importantes, como as obter a partir de um conjunto gerador e quais ferramentas utilizar para inferir se um polinômio dado pertence a um ideal. As principais referências para esse capítulo são [2] e [4].

Por fim, no Capítulo 3, introduzimos os resultados que são base para a geometria algébrica. Esses resultados são as versões dos Teoremas dos Zeros de Hilbert (também conhecidos por Nullstellensatz) que nos permitirão associar uma variedade afim a um ideal radical (estrutura algébrica que será apresentada nesse capítulo) de forma biunívoca. Com esses resultados também será possível mostrar quando um polinômio pertence a um ideal radical dado. As principais referências para este capítulo são [3] e [4].

# CAPÍTULO 1

# Geometria, Álgebra e Algumas Relações

Um anel $A$ é um conjunto com operações de adição $+$ e multiplicação $\cdot$ . Com a adição, $A$ é um grupo abeliano e a multiplicação é associativa. Além disso, a adição é distributiva em relação à multiplicação (a esquerda e a direita). Se a multiplicação for comutativa, dizemos que o anel é comutativo. Se a multiplicação possui elemento neutro, dizemos que A é um anel com unidade. O elemento neutro da adição é denotado por 0 e o elemento neutro da multiplicação é denotado por 1.

Para todos os efeitos, trabalhamos sempre com anéis comutativos com unidade. Por isso que quando dizemos que $A$ é um anel, estaremos nos referindo a um anel comutativo com unidade (a menos que seja dito o contrário). Um domínio de integridade, ou simplesmente domínio, é um anel $D$, não nulo, em que seus elementos são todos não divisores de zero, exceto o próprio 0. Um domínio principal $P$ é um domínio de integridade onde cada ideal $I \subset P$ é gerado por um único elemento (nesse caso, dizemos que $I$ é um ideal principal). Um corpo $\mathbb{K}$, é um anel no qual todo elemento não nulo possui inverso para a multiplicação.

Este capítulo apresentará alguns dos temas básicos necessários para o trabalho. A geometria que nos interessa diz respeito a variedades afins, que são curvas e superfícies (e objetos de dimensões superiores) definidas por equações polinomiais. Para entender variedades afins será necessário um pouco de álgebra e, em particular, precisaremos estudar ideais no anel de polinômios $\mathbb{K}[x_1, \ldots, x_n]$.

## 1.1 Definições e Exemplos

Ao longo deste trabalho $\mathbb{K}$ denotará um corpo e $n$ um inteiro positivo.

**Definição 1.1** *Um **monômio** em $x_1, \cdots, x_n$ é um produto da forma*

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

*onde todos os expoentes $\alpha_1, \ldots, \alpha_n$ são inteiros não negativos. O **grau total** desse monômio é $\alpha_1 + \cdots + \alpha_n$.*

Podemos simplificar essa notação de monômios como segue. Seja $\alpha = (\alpha_1, \ldots, \alpha_n)$ uma n-upla de inteiros não negativos. Então denotaremos

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

Quando $\alpha = (0, \ldots, 0)$, note que $x^\alpha = 1$.

**Definição 1.2** *Um **polinômio** $f$ em $x_1, \ldots, x_n$ com coeficientes num corpo $\mathbb{K}$ é uma combinação linear finita com coeficientes em $\mathbb{K}$ (combinação $\mathbb{K}$-linear) de monômios. Vamos escrever um polinômio $f$ na forma*

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

*onde a soma é sobre um número finito de n-uplas $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. O conjunto de todos os polinômios em $x_1, \ldots, x_n$ com coeficientes em $\mathbb{K}$ é denotado por $\mathbb{K}[x_1, \ldots, x_n]$.*

Quando tratarmos de polinômios com uma, duas ou três variáveis diremos que, respectivamente, eles pertencem a $\mathbb{K}[x]$, $\mathbb{K}[x, y]$ e $\mathbb{K}[x, y, z]$.

**Definição 1.3** *Seja $f = \sum_\alpha a_\alpha x^\alpha$ um polinômio em $\mathbb{K}[x_1, \ldots, x_n]$.*

1. *Chamaremos de $a_\alpha$ o **coeficiente** do monômio $x^\alpha$.*
2. *Se $a_\alpha \neq 0$ então $a_\alpha x^\alpha$ é um **termo** de $f$.*
3. *O **grau total** de $f$, denotado por deg(f) é o maior $|\alpha|$ tal que o coeficiente $a_\alpha$ é não nulo, onde $|\alpha| = \alpha_1 + \ldots + \alpha_n$.*

Como um exemplo, o polinômio $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ tem quatro termos e grau total seis. Observe aqui que há dois termos com o maior grau total, o que não acontece com polinômios em uma variável. No capítulo seguinte veremos como ordenar os termos de um polinômio. O fato de que $\mathbb{K}[x_1, \ldots, x_n]$ é um anel é provado para $n = 1$ parcialmente em [6, Proposition 3.5.1] e a parte que

resta referente a associatividade da multiplicação pode ser encontrada em [7, Chapter 4.1]. Tendo em vista que $\mathbb{K}[x_1][x_2] = \mathbb{K}[x_1, x_2]$ (ver [5], Exercício resolvido I.2.2), de modo indutivo obtemos que $\mathbb{K}[x_1, \ldots, x_{n-1}][x_n] = \mathbb{K}[x_1, \ldots, x_n]$, portanto, $\mathbb{K}[x_1, \ldots, x_n]$ é um anel.

**Definição 1.4** *Define-se o* ***espaço afim*** *de dimensão n sobre* $\mathbb{K}$ *o conjunto*

$$\mathbb{K}^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in \mathbb{K}\}.$$

Para um exemplo de espaço afim, considere o caso $\mathbb{K} = \mathbb{R}$. Aqui obtemos o espaço $\mathbb{R}^n$ familiar do Cálculo Diferencial e Integral e Álgebra Linear. Em geral, $\mathbb{K}^1 = \mathbb{K}$ é a *reta afim* e $\mathbb{K}^2$ o *plano afim*.

## 1.2 Variedades Afins

Vamos agora definir o objeto geométrico básico desse trabalho.

**Definição 1.5** *Sejam* $f_1, \ldots, f_s$ *polinômios em* $\mathbb{K}[x_1, \ldots, x_n]$. *Define-se o conjunto*

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

*como a* ***variedade afim*** *definida por* $f_1, \ldots, f_s$.

Então, uma variedade afim $V \subset \mathbb{K}^n$ é o conjunto de todas as soluções do sistema de equações $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$. Nós utilizaremos as letras $V$, $W$, etc. para denotar variedades afins. Utilizando $\mathbb{K} = \mathbb{R}$, podemos desenhar imagens. Como exemplo, no plano $\mathbb{R}^2$ a variedade $V(x^2 + y^2 - 1)$ é a circunferência de raio 1 centrada na origem.

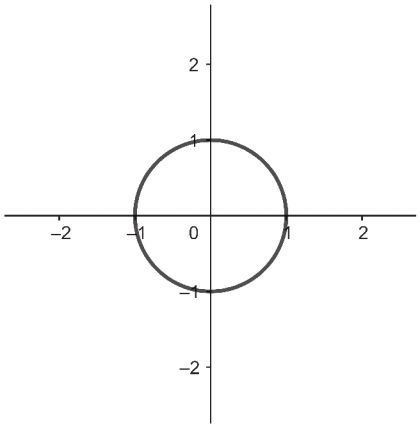



**FIGURA 1.1:** Circunferência com centro na origem e raio 1.

**Lema 1.6** *Se* $V, W \subset \mathbb{K}^n$ *são variedades afins, então* $V \cup W$ *e* $V \cap W$ *também são.*

**Demonstração:** Suponha que $V = \mathcal{V}(f_1,\ldots,f_s)$ e $W = \mathcal{V}(g_1,\ldots,g_t)$. Afirmamos que

$$V \cap W = \mathcal{V}(f_1,\ldots,f_s,g_1,\ldots,g_t) \qquad \text{e} \qquad V \cup W = \mathcal{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t).$$

Seja $(a_1,\ldots,a_n) \in V \cap W$, isso é equivalente a dizer que $(a_1,\ldots,a_n)$ anula ambos os polinômios $f_1,\ldots,f_s$ e $g_1,\ldots,g_t$, isto é, anula os polinômios $f_1,\ldots,f_s,g_1,\ldots,g_t$. Para a segunda igualdade: Se $(a_1,\ldots,a_n) \in V$, então todos os $f_i s$ se anulam nesse ponto, o que implica que $f_i g_j s$ também se anulam em $(a_1,\ldots,a_n)$. Então $V \subset \mathcal{V}(f_i g_j)$ e, de forma similar, $W \subset \mathcal{V}(f_i g_j)$. Isso prova que $V \cup W \subset \mathcal{V}(f_i g_j)$.

Por outro lado, seja $(a_1,\ldots,a_n) \in \mathcal{V}(f_i g_j)$. Se esse ponto está em $V$, a demonstração acaba aqui, caso contrário, então $f_{i_0}(a_1,\ldots,a_n) \neq 0$ para algum $i_0$, mas $f_{i_0} g_j$ se anula em $(a_1,\ldots,a_n)$ para todo $j$, então os $g_j s$ devem se anular nesse ponto, provando que $(a_1,\ldots,a_n) \in W$. Isso mostra que $\mathcal{V}(f_i g_j) \subset V \cup W$.

■

Esse Lema nos diz que interseções e uniões finitas de variedades afins são variedades afins. Considere, por exemplo, a união do plano $xy$ com o eixo $z$ no espaço afim de dimensão 3. Pela fórmula acima, temos

$$\mathcal{V}(z) \cup \mathcal{V}(x,y) = \mathcal{V}(zx,zy).$$

Além disso, observe que pela outra fórmula acima $\mathcal{V}(z) \cap \mathcal{V}(x,y) = \mathcal{V}(x,y,z)$, que é a origem $P = (0,0,0)$ de $\mathbb{R}^3$.

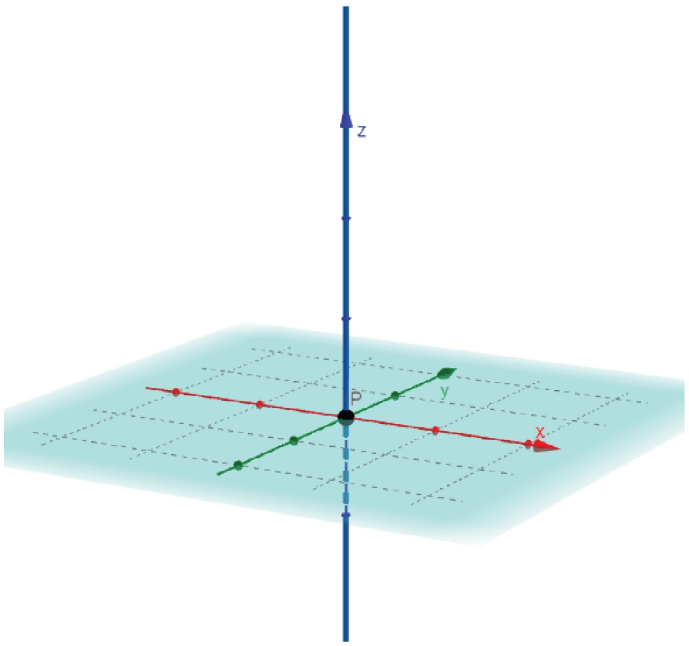



**FIGURA 1.2:** A união do plano $(x,y)$ com o eixo $z$.

Agora que temos uma caracterização de uniões e interseções de variedades afins, vale questio-

nar: Dados $f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$, será que é possível determinar se $\mathcal{V}(f_1,\ldots,f_s) \neq \emptyset$, isto é, se as equações $f_1 = \cdots = f_s = 0$ têm uma solução em comum?

## 1.3 Ideais

Vamos agora definir o objeto algébrico básico desse trabalho.

**Definição 1.7** *Um subconjunto $I \subset \mathbb{K}[x_1,\ldots,x_n]$ é um **ideal** se satisfaz as seguintes condições:*

1. $0 \in I$.
2. *Se $f, g \in I$, então $f+g \in I$.*
3. *Se $f \in I$ e $h \in \mathbb{K}[x_1,\ldots,x_n]$, então $hf \in I$.*

O seguinte exemplo de ideal é um dos que mais será usado nesse texto.

**Definição 1.8** *Sejam $f_1,\ldots,f_s$ polinômios de $\mathbb{K}[x_1,\ldots,x_n]$. Definimos o conjunto*

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

O resultado a seguir nos diz que $\langle f_1,\ldots,f_s\rangle$ é um ideal.

**Lema 1.9** *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 $\mathbb{K}[x_1,\ldots,x_n]$. Chamaremos $\langle f_1,\ldots,f_s\rangle$ de **ideal gerado por** $f_1,\ldots,f_s$.*

**Demonstração:** Primeiramente, $0 \in \langle f_1,\ldots,f_s\rangle$ $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Agora, sejam $f = \sum_{i=1}^{s} p_i f_i$ e $g = \sum_{i=1}^{s} q_i f_i$ e seja $h \in \mathbb{K}[x_1,\ldots,x_n]$. Então as seguintes equações

$$f+g = \sum_{i=1}^{s} (p_i + q_i) f_i,$$

$$hf = \sum_{i=1}^{s} (hp_i) f_i$$

completam a prova de que $\langle f_1,\ldots,f_s\rangle$ é um ideal. ■

O ideal $\langle f_1,\ldots,f_s\rangle$ tem uma boa interpretação em termos de equações polinomiais. Dados $f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$, considere o sistema de equações

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_s &= 0. \end{aligned}$$

Dessas equações é possível derivar outras algebricamente. Por exemplo, se multiplicamos a primeira equação por $h_1 \in \mathbb{K}[x_1,\ldots,x_n]$, a segunda por $h_2 \in \mathbb{K}[x_1,\ldots,x_n]$, etc., e somarmos as equações resultantes, obteremos

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0,$$

a qual é uma consequência do nosso sistema original. Note que o lado esquerdo da equação é exatamente um elemento do ideal $\langle f_1,\ldots,f_s\rangle$. Assim, podemos pensar em $\langle f_1,\ldots,f_s\rangle$ como o conjunto consistindo de "lados esquerdos" de todas as "consequências" das equações $f_1 = f_2 = \cdots = f_s = 0$.

Dizemos que um ideal $I$ é *finitamente gerado* se existem $f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$ tais que $I = \langle f_1,\ldots,f_s\rangle$, e dizemos que $f_1,\ldots,f_s$ são uma *base* de $I$. Mais adiante provaremos o fato de que *todo* ideal de $\mathbb{K}[x_1,\ldots,x_n]$ é finitamente gerado (conhecido como o Teorema da Base de Hilbert).

**Proposição 1.10** *Se $f_1,\ldots,f_s$ e $g_1,\ldots,g_t$ são bases do mesmo ideal em $\mathbb{K}[x_1,\ldots,x_n]$, ou seja, $\langle f_1,\ldots,f_s\rangle = \langle g_1,\ldots,g_t\rangle$, então nós temos que $\mathcal{V}(f_1,\ldots,f_s) = \mathcal{V}(g_1,\ldots,g_t)$.*

**Demonstração:** Seja $(a_1,\ldots,a_n) \in \mathcal{V}(f_1,\ldots,f_s)$, pela hipótese, sabemos que, para cada $1 \leq i \leq t$, existem $h_{i1},\ldots h_{is}$ tais que $g_i = h_{i1}f_1 + \cdots + h_{is}f_s$ e, como $(a_1,\ldots,a_n) \in \mathcal{V}(f_1,\ldots,f_s)$, então $g_i(a_1,\ldots,a_n) = h_{i1}0 + \cdots + h_{is}0 = 0$, o que nos dá que $(a_1,\ldots,a_n) \in \mathcal{V}(g_1,\ldots,g_t)$ e assim $\mathcal{V}(f_1,\ldots,f_s) \subset \mathcal{V}(g_1,\ldots,g_t)$. De forma análoga obtém-se $\mathcal{V}(g_1,\ldots,f_t) \subset \mathcal{V}(f_1,\ldots,f_s)$ e a prova termina aqui. ■

**Exemplo 1.11** *Considere a variedade $\mathcal{V}(2x^2+3y^2-11, x^2-y^2-3)$. Vamos mostrar que $\langle 2x^2+3y^2-11, x^2-y^2-3\rangle = \langle x^2-4, y^2-1\rangle$, de fato:*

$$\begin{aligned} f \in \langle 2x^2+3y^2-11, x^2-y^2-3\rangle &\Rightarrow f = h_1(2x^2+3y^2-11) + h_2(x^2-y^2-3),\ h_1,h_2 \in \mathbb{K}[x_1,\ldots,x_n] \\ &\Rightarrow f = h_1(2(x^2-4)+3(y^2-1)) + h_2(1(x^2-4)-1(y^2-1)),\ h_1,h_2 \in \mathbb{K}[x_1,\ldots,x_n] \\ &\Rightarrow f = (2h_1+h_2)(x^2-4) + (3h_1-h_2)(y^2-1),\ h_1,h_2 \in \mathbb{K}[x_1,\ldots,x_n] \\ &\Rightarrow f \in \langle x^2-4, y^2-1\rangle. \end{aligned}$$

*Então,* $\langle 2x^2+3y^2-11, x^2-y^2-3\rangle \subset \langle x^2-4, y^2-1\rangle$. *De forma similar, tendo em vista que* $x^2-4 = \frac{1}{5}(2x^2+3y^2-11)+\frac{3}{5}(x^2-y^2-3)$ *e* $y^2-1=\frac{1}{5}(2x^2+3y^2-11)-\frac{2}{5}(x^2-y^2-3)$, *obtém-se que* $\langle 2x^2+3y^2-11, x^2-y^2-3\rangle \supset \langle x^2-4, y^2-1\rangle$ *e assim* $\langle 2x^2+3y^2-11, x^2-y^2-3\rangle = \langle x^2-4, y^2-1\rangle$. *Portanto, pela proposição acima*

$$\mathcal{V}(2x^2+3y^2-11, x^2-y^2-3) = \mathcal{V}(x^2-4, y^2-1) = \{(\pm 2, \pm 1)\}.$$

*Assim, ao mudar a base do ideal, pode-se facilitar a determinação dos pontos da variedade dos polinômios que geram esse ideal.*

**Definição 1.12** *Seja* $V \subset \mathbb{K}^n$ *uma variedade afim. Define-se*

$$\mathcal{I}(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0,\ \forall\ (a_1, \ldots, a_n) \in V\}.$$

A seguir, veremos que $\mathcal{I}(V)$ é um ideal de $\mathbb{K}[x_1, \ldots, x_n]$.

**Lema 1.13** *Se* $V \subset \mathbb{K}^n$ *é uma variedade afim, então* $\mathcal{I}(V) \subset \mathbb{K}[x_1, \ldots, x_n]$ *é um ideal. Chamaremos* $\mathcal{I}(V)$ *por* ***ideal de*** $V$.

**Demonstração:** $0 \in \mathcal{I}(V)$ já que o polinômio nulo se anula em todos os pontos de $\mathbb{K}^n$, em particular, nos pontos de $V$. Em seguida, suponha que $f, g \in \mathcal{I}(V)$ e que $h \in \mathbb{K}[x_1, \ldots, x_n]$. Seja $(a_1, \ldots, a_n)$ um ponto arbitrário de $V$. Logo,

$$\begin{aligned} f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) &= 0 + 0 = 0, \\ h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) &= h(a_1, \ldots, a_n) \cdot 0 = 0 \end{aligned}$$

e segue que $\mathcal{I}(V)$ é um ideal. ■

**Exemplo 1.14** *Considere a variedade* $\{(0,0)\}$ *formada pela origem em* $\mathbb{K}^2$. *Então, seu ideal* $\mathcal{I}(\{(0,0)\})$ *consiste de todos os polinômios que se anulam na origem, e afirmamos que*

$$\mathcal{I}(\{(0,0)\}) = \langle x, y\rangle.$$

*Observe que todo polinômio da forma* $A(x,y)x + B(x,y)y$ *se anula na origem. Por outro lado, suponha*

*que* $f = a_{00} + \sum_{(i,j)\neq(0,0)} a_{ij}x^i y^j$, *então* $a_{00} = f(0,0) = 0$ *e, consequentemente,*

$$f = a_{00} + \sum_{(i,j)\neq(0,0)} a_{ij}x^i y^j = 0 + \left(\sum_{\substack{i>0\\ j\geq 0}} a_{ij}x^{i-1}y^j\right)x + \left(\sum_{j>0} a_{0j}y^{j-1}\right)y \in \langle x,y\rangle.$$

*A afirmação está provada.*

**Lema 1.15** *Se* $f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$, *então* $\langle f_1,\ldots,f_s\rangle \subset \mathcal{I}(\mathcal{V}(f_1,\ldots,f_s))$, *embora a igualdade não necessariamente ocorra.*

**Demonstração:** Seja $f \in \langle f_1,\ldots,f_s\rangle$, ou seja, existem $h_1,\ldots,h_s \in \mathbb{K}[x_1,\ldots,x_n]$ tais que $f = \sum_{i=1}^{s} h_i f_i$. Como $f_1,\ldots,f_s$ se anulam em $\mathcal{V}(f_1,\ldots,f_s)$, então obrigatoriamente $f = \sum_{i=1}^{s} h_i f_i$ se anulará nesse conjunto, o que prova que $f \in \mathcal{I}(\mathcal{V}(f_1,\ldots,f_s))$.

Para a segunda parte do Lema, considere o seguinte exemplo onde $\mathcal{I}(\mathcal{V}(f_1,\ldots,f_s))$ é estritamente maior que $\langle f_1,\ldots,f_s\rangle$: Mostraremos que

$$\langle x^2,y^2\rangle \subset \mathcal{I}(\mathcal{V}(x^2,y^2))$$

não pode ser igualdade. Primeiro vamos calcular os elementos de $\mathcal{I}(\mathcal{V}(x^2,y^2))$. As equações $x^2 = y^2 = 0$ implicam que $\mathcal{V}(x^2,y^2) = \{(0,0)\}$. Mas o exemplo anterior nos mostrou que o ideal de $\{(0,0)\}$ é $\langle x,y\rangle$, então $\mathcal{I}(\mathcal{V}(x^2,y^2)) = \langle x,y\rangle$. Note que $x \notin \langle x^2,y^2\rangle$ polinômios da forma $h_1(x,y)x^2 + h_2(x,y)y^2$ têm monômios cujos graus totais são maiores ou iguais a dois, logo $\mathcal{I}(\mathcal{V}(x^2,y^2))$ contém estritamente $\langle x^2,y^2\rangle$. ■

Em corpos arbitrários, a relação entre $\langle f_1,\ldots,f_s\rangle$ e $\mathcal{I}(\mathcal{V}(f_1,\ldots,f_s))$ pode ser um pouco sutil, contudo, sobre um corpo algebricamente fechado como $\mathbb{C}$, existe uma relação direta entre esses ideais, que será explorada no Capítulo 3. Embora para um corpo qualquer $\mathcal{I}(\mathcal{V}(f_1,\ldots,f_s))$ possa não ser igual a $\langle f_1,\ldots,f_s\rangle$, o ideal de uma variedade sempre contém informações suficientes para determinar os elementos dessa variedade.

**Proposição 1.16** *Sejam V e W variedades afins em* $\mathbb{K}^n$. *Então*

1. $V \subset W$ *se e só se* $\mathcal{I}(V) \supset \mathcal{I}(W)$.
2. $V = W$ *se e só se* $\mathcal{I}(V) = \mathcal{I}(W)$.

**Demonstração:** Para provar o primeiro item, suponha que $V \subset W$. Então qualquer polinômio que se anula em $W$ deve se anular em $V$, o que prova que $\mathscr{I}(W) \subset \mathscr{I}(V)$. Em seguida, assuma que $\mathscr{I}(W) \subset \mathscr{I}(V)$. Sabemos que $W$ é uma variedade definida por alguns polinômios $g_1,\ldots,g_t \in \mathbb{K}[x_1,\ldots,x_n]$. Então, $g_1,\ldots,g_t \in \mathscr{I}(W) \subset \mathscr{I}(V)$ e então os $g_i s$ se anulam em $V$. Como $W$ contém todos as raízes comuns dos $g_i s$, segue que $V \subset W$.

Para provar o segundo item, observe que, pelo primeiro item, temos

$$V = W \Longleftrightarrow V \subset W \text{ e } W \subset V \Longleftrightarrow \mathscr{I}(V) \supset \mathscr{I}(W) \text{ e } \mathscr{I}(W) \supset \mathscr{I}(V) \Longleftrightarrow \mathscr{I}(V) = \mathscr{I}(W). \qquad \blacksquare$$

Existe uma rica relação entre ideais e variedades afins que será explorada mais adiante, no Capítulo 3, onde veremos que alguns teoremas provados sobre ideais têm fortes implicações geométricas. Para encerrar esse capítulo, trazemos três problemas acerca dos ideais de $\mathbb{K}[x_1,\ldots,x_n]$.

- **(Descrição de um ideal)** É possível qualquer ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$ ser escrito na forma $\langle f_1,\ldots,f_s\rangle$ para alguns $f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$?
- **(Membro de um ideal)** Se $f, f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$, como saber se $f \in \langle f_1,\ldots,f_s\rangle$?
- **(Os Zeros de Hilbert)** Dados $f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$, qual a relação entre $\langle f_1,\ldots,f_s\rangle$ e $\mathscr{I}(\mathscr{V}(f_1,\ldots,f_s))$?

# CAPÍTULO 2

# Bases de Gröbner

Neste capítulo apresentamos um algoritmo para realizar divisões de um polinômio por uma quantidade finita de polinômios, todos em $n$ variáveis. Além disso falaremos de Base de Gröbner, como inferir se um conjunto gerador de um ideal é uma Base de Gröbner e, dado um conjunto gerador, como obter uma Base de Gröbner a partir dele.

## 2.1 Ordenando os monômios em $\mathbb{K}[x_1,\ldots,x_n]$

Ao examinarmos em detalhes o algoritmo da divisão realizado para dividir polinômios $f,g \in \mathbb{K}[x]$, percebe-se que há uma *ordenação* dos termos dos polinômios que são essenciais para o processo, mesmo que ela não seja enfatizada. Por exemplo, na divisão de $f(x) = 2x^4 - 3x^3 + x - 1$ por $g(x) = x^2 - 2x + 3$ pelo método padrão, teríamos que:

- Escrever os termos dos polinômios em ordem decrescente de suas potências de $x$.
- No primeiro passo, o termo líder (termo de maior grau), em $f$ é $2x^4 = 2x^2 \cdot x^2 = 2x^2 \cdot$(termo líder de $g$). Então, subtrairíamos $2x^2 \cdot g(x)$ de $f$ para cancelar o termo líder, obtendo $x^3 - 6x^2 + x - 1$.
- Em seguida, repetiríamos o mesmo processo em $f(x) - 2x^4 \cdot g(x)$, etc., até obtermos um polinômio de grau menor que 2.

Para realizar algoritmo da divisão em polinômios em uma variável, estamos lidando com a ordenação de graus nos monômios de uma variável:

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

O sucesso desse algoritmo depende do trabalho sucessivo nos termos líderes dos polinômios $f$ e $g$ que fazem parte da divisão, e não removendo termos "aleatoriamente" de $f$ usando termos quaisquer de $g$.

Primeiramente, podemos reescrever o monômio $x^\alpha = x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdot\ldots\cdot x_n^{\alpha_n}$ pela n-upla $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}_{\geq 0}^n$, quando necessário. Isso estabelece uma correspondência biunívoca dos monômios de $\mathbb{K}[x_1,\ldots,x_n]$ e $\mathbb{Z}_{\geq 0}^n$. Além disso, qualquer ordenação $>$ que for estabelecida em $\mathbb{Z}_{\geq 0}^n$ nos dará uma ordenação dos monômios: Se $\alpha > \beta$ por essa ordenação, então diremos que $x^\alpha > x^\beta$. Para começar, como um polinômio é uma soma de monômios, gostaríamos de poder organizar os termos de um polinômio em ordem decrescente (ou crescente). Para fazer isso, devemos ser capazes de comparar cada par de monômios para estabelecer suas posições relativas adequadas. Assim, exigiremos que nossas ordenações sejam de *ordem total*. Isso quer dizer que, dados dois monômios $x^\alpha$ e $x^\beta$ apenas uma das seguintes sentenças

$$x^\alpha > x^\beta, \qquad x^\alpha = x^\beta, \qquad x^\beta > x^\alpha$$

será verdadeira.

Vamos pedir também que todas as ordenações monomiais satisfaçam a seguinte propriedade: Se $x^\alpha > x^\beta$ e $x^\gamma$ é um monômio qualquer, então vamos exigir que $x^\alpha x^\gamma > x^\beta x^\gamma$. Em termos de $n$-uplas essa propriedade quer dizer que $\alpha > \beta$ em uma ordenação que estivermos usando em $\mathbb{Z}_{\geq 0}^n$, então, para todos $\gamma \in \mathbb{Z}_{\geq 0}^n$, $\alpha + \gamma > \beta + \gamma$.

Então vamos definir o que é uma *ordem monomial*.

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

1. *$>$ é de ordem total em $\mathbb{Z}_{\geq 0}^n$.*
2. *Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}_{\geq 0}^n$, então $\alpha + \gamma > \beta + \gamma$.*
3. *$>$ é de boa ordem em $\mathbb{Z}_{\geq 0}^n$. Isso significa que qualquer conjunto não vazio de $\mathbb{Z}_{\geq 0}^n$ possui menor elemento para a ordem $>$.*

O lema seguinte irá nos ajudar a entender o que significa uma relação ser de boa ordem de acordo com a parte 3 da Definição acima:

**Lema 2.2** *Uma relação de ordem $>$ em $\mathbb{Z}_{\geq 0}^n$ é de boa ordem se e somente se qualquer sequência estritamente decrescente em $\mathbb{Z}_{\geq 0}^n$*

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

*termina em algum momento.*

**Demonstração:** Vamos provar pela forma contrapositiva da sentença: $>$ não é de boa ordem $\Leftrightarrow$ Existe uma sequência decrescente infinita em $\mathbb{Z}^n_{\geq 0}$.

Por um lado, se $>$ não é de boa ordem, então algum $S \subset \mathbb{Z}^n_{\geq 0}$ não vazio "não tem um menor elemento". Seja $\alpha(1) \in S$. Desde que $\alpha(1)$ não é o menor elemento, podemos encontrar $\alpha(1) > \alpha(2)$ em $S$. Como $\alpha(2)$ não é o menor elemento, então existe $\alpha(2) > \alpha(3)$ em $S$. Continuando esse caminho, obteremos a seguinte sequência estritamente decrescente

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

Por outro lado, dada uma sequência infinita, então $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ é um subconjunto não vazio de $\mathbb{Z}^n_{\geq 0}$ sem um menor elemento, e assim, $>$ não é de boa ordem. ■

**Definição 2.3 (Ordem lexicográfica)** *Sejam $\alpha = (\alpha_1,\ldots,\alpha_n)$ e $\beta = (\beta_1,\ldots,\beta_n) \in \mathbb{Z}^n_{\geq 0}$. Dizemos $\alpha >_{lex} \beta$ se, na n-upla diferença $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$, a primeira entrada não-nula da esquerda para a direita é positiva. Escrevemos $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.*

Alguns exemplos:

- $(1,2,0) >_{lex} (0,3,4)$ pois $\alpha - \beta = (1,-1,-4)$
- $(3,2,4) >_{lex} (3,2,1)$ pois $\alpha - \beta = (0,0,3)$
- As variáveis $x_1,\ldots,x_n$ são ordenadas de forma usual pela ordem lexicográfica:

$$(1,0,\ldots,0) >_{lex} (0,1,0,\ldots,0) >_{lex} \ldots >_{lex} (0,\ldots,0,1)$$

  então $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$. Na prática, vamos também assumir que a ordem alfabética $x > y > z$ nas variáveis será usada para definir a ordem lexicográfica, a menos que digamos o contrário.

Vamos verificar, de fato, que a ordem lexicográfica satisfaz as três condições da Definição 2.1.

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

**Demonstração:** Vamos provar os três itens que definem uma ordem monomial:

1. $>_{lex}$ é assimétrica: De fato, se $\alpha$ e $\beta \in \mathbb{Z}^n_{\geq 0}$ de modo que $\alpha >_{lex} \beta$, então a primeira entrada não nula de $\alpha - \beta$ é positiva, o que implica que a primeira entrada não nula de $\beta - \alpha$ é negativa e assim $\beta \not>_{lex} \alpha$.

   $>_{lex}$ é transitiva: Se $\alpha$, $\beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$ tais que $\alpha >_{lex} \beta$ e $\beta >_{lex} \gamma$, por definição $\alpha - \beta$ tem a primeira entrada à esquerda não nula e $\beta - \gamma$ também. Então $(\alpha - \beta) + (\beta - \gamma) = \alpha - \gamma$ tem a primeira entrada não nula positiva e assim $\alpha >_{lex} \gamma$.

   $>_{lex}$ é de ordem total: Se $\alpha \neq \beta$ em $\mathbb{Z}^n_{\geq 0}$, então $\alpha - \beta \neq 0 \in \mathbb{Z}^n_{\geq 0}$, então $\alpha - \beta$ tem pelo menos uma entrada não-nula. Se a primeira entrada não nula à esquerda de $\alpha - \beta$ for positiva, então $\alpha >_{lex} \beta$. Caso contrário, $\beta >_{lex} \alpha$.

   $\therefore >_{lex}$ é de ordem total.

2. Sejam $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$ tais que $\alpha >_{lex} \beta$, então temos que a primeira entrada não nula de $\alpha - \beta$, chamemos de $\alpha_k - \beta_k$, é positiva. Mas $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ e $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Mas como $(\alpha+\gamma)-(\beta+\gamma) = \alpha - \beta$, temos que a primeira entrada não nula de $(\alpha+\gamma)-(\beta+\gamma)$ à esquerda é $\alpha_k - \beta_k > 0$. Portanto, $\alpha + \gamma >_{lex} \beta + \gamma$.

3. Suponha que $>_{lex}$ não é de boa ordem. Então, pelo Lema 2.2, existe uma sequência infinita e estritamente decrescente

   $$\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \ldots$$

   de elementos de $\mathbb{Z}^n_{\geq 0}$. Vamos mostrar que isso chega a uma contradição.

   Considere as primeiras entradas das n-uplas $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Pela definição de ordem lexicográfica, essas primeiras entradas formam uma sequência não crescente de inteiros não negativos. Como $\mathbb{Z}_{\geq 0}$ (ou $\mathbb{Z}^+$ é bem ordenado, as primeiras entradas dos $\alpha(i)$s devem "estabilizar" em algum momento. Isto é, existe um $k$ tal que todas as primeiras componentes dos $\alpha(i)$s com $i \geq k$ são iguais.

   Começando por $\alpha(k)$, a segunda entrada e suas subsequentes entram numa dinâmica pela ordem lexicográfica: As segundas entradas de $\alpha(k)$, $\alpha(k+1),\ldots$ formam uma sequência não crescente. Pela mesma razão de antes, essas entradas vão "estabilizar" em algum momento Continuando esse caminho, vamos ter que, para algum $l$, $\alpha(l)$, $\alpha(l+1),\ldots$ são todos iguais. O que contradiz o fato de $\alpha(l) >_{lex} \alpha(l+1)$. Assim, $>_{lex}$ é de boa ordem.

■

É importante perceber que existem muitas ordens lexicográficas correspondentes à forma como as variáveis são ordenadas. Até agora, usamos a ordem lexicográfica com $x_1 > x_2 > \ldots > x_n$. Mas dada qualquer ordenação das variáveis $x_1,\ldots,x_n$, existe uma ordem lexicográfica correspondente. Por exemplo, se as variáveis são $x$ e $y$, então obtemos uma ordem lexicográfica com $x > y$ e uma segunda ordem com $y > x$. No caso geral de $n$ variáveis, existem $n!$ ordens lexicográficas. No que se segue, a frase "ordem lexicográfica" se referirá àquela com $x_1 > \ldots > x_n$, a menos que se indique o contrário. Na ordem lexicográfica, observe que uma variável domina *qualquer* monômio que envolva apenas variáveis menores, desconsiderando o seu grau total. Tal como temos que $x >_{lex} y^5z^3$, é possível também levar em conta os graus totais dos monômios e ordenar primeiro os monômios de grau maior. Uma maneira de fazer isso é utilizando a ordem lexicográfica graduada.

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

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

Alguns exemplos:

- $(1,2,3) >_{grlex} (3,2,0)$ pois $|(1,2,3)| = 6 > |(3,2,0)| = 5$,
- $(1,2,4) >_{grlex} (1,1,5)$ pois $|(1,2,4)| = |(1,1,5)|$ e $(1,2,4) >_{lex} (1,1,5)$,
- As variáveis são ordenadas de acordo com a ordem lexicográfica, isto é,

$$x_1 >_{grlex} \cdots >_{grlex} x_n.$$

**Proposição 2.6** *A ordem lexicográfica graduada é uma ordem monomial.*

**Demonstração:** Vamos provar mais uma vez os três itens que definem uma ordem monomial:

1. $>_{grlex}$ é assimétrica: De fato, se $\alpha$ e $\beta \in \mathbb{Z}^n_{\geq 0}$ de modo que $\alpha >_{grlex} \beta$, então $|\alpha| > |\beta|$, ou $|\alpha| = |\beta|$ e $\alpha >_{lex} \beta$. Em ambos os casos é impossível ter $\beta >_{grlex} \alpha$.

   $>_{grlex}$ é transitiva: Se $\alpha$, $\beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$ tais que $\alpha >_{grlex} \beta$ e $\beta >_{grlex} \gamma$, então $|\alpha| > |\beta|$ ou $|\alpha| = |\beta|$ e $\alpha >_{lex} \beta$. Além disso, $|\beta| > |\gamma|$ ou $|\beta| = |\gamma|$ e $\beta >_{lex} \gamma$. Todas as combinações possíveis implicam que $|\alpha| > |\gamma|$ ou $|\alpha| = |\gamma|$ e $\alpha >_{lex} \gamma$, isto é, $\alpha >_{grlex} \gamma$.

   $>_{grlex}$ é de ordem total: Se $\alpha \neq \beta$ em $\mathbb{Z}^n_{\geq 0}$, então $|\alpha| < |\beta|$ ou $|\alpha| = |\beta|$, ou $|\alpha| > |\beta|$. Note que $|\alpha| < |\beta|$ ou $|\alpha| > |\beta|$ nos dá que $\beta >_{grlex} \alpha$ ou $\alpha >_{grlex} \beta$. Já, quando $|\alpha| = |\beta|$, comparamos $\alpha$ e $\beta$ pela relação "$>_{lex}$", que já provamos ser de ordem total.

   $\therefore >_{grlex}$ é de ordem total.

2. Se $\alpha,\beta,\gamma \in \mathbb{Z}^n_{\geq 0}$ tais que $\alpha >_{grlex} \beta$, então temos que, se $|\alpha| > |\beta|$, então $\sum_{k=1}^{n} \alpha_k > \sum_{k=1}^{n} \beta_k$, logo $|\alpha+\gamma| = \sum_{k=1}^{n} \alpha_k+\gamma_k = \sum_{k=1}^{n} \alpha_k + \sum_{k=1}^{n} \gamma_k > \sum_{k=1}^{n} \beta_k + \sum_{k=1}^{n} \gamma_k = \sum_{k=1}^{n} \beta_k+\gamma_k = |\beta+\gamma|$. Por outro lado, se $|\alpha| = |\beta|$ e $\alpha >_{lex} \beta$, analogamente prova-se que $|\alpha+\gamma| = |\beta+\gamma|$ e observe que então $\alpha+\gamma >_{lex} \beta+\gamma$. Em ambos os casos, só é possível que $|\alpha+\gamma| > |\beta+\gamma|$ ou $|\alpha+\gamma| = |\beta+\gamma|$ e $\alpha+\gamma >_{lex} \beta+\gamma$. Assim, $\alpha+\gamma >_{grlex} \beta+\gamma$.

3. Suponha que $>_{grlex}$ não é de boa ordem. Então, pelo Lema 2.2, existe uma sequência infinita e estritamente decrescente

$$\alpha(1) >_{grlex} \alpha(2) >_{grlex} \alpha(3) >_{grlex} \cdots$$

de elementos de $\mathbb{Z}^n_{\geq 0}$. Vamos mostrar que isso chega a uma contradição. Observe inicialmente que existe um inteiro positivo $l$ tal que $|\alpha(l)| = |\alpha(l+1)| = \cdots$, pois $|\alpha(k)| \in \mathbb{Z}_{\geq 0}$ para todo inteiro positivo $k$. Assim, a partir desse índice $l$, teríamos que

$$\alpha(l) >_{lex} \alpha(l+1) >_{lex} \alpha(l+2) >_{lex} \cdots$$

seria uma sequência infinita e estritamente decrescente, o que é um absurdo pois sabemos que $>_{lex}$ é de boa ordem. ■

Da mesma forma que na ordem lexicográfica, existem $n!$ ordens graduadas lexicográficas em $n$ variáveis, dependendo de como elas estarão ordenadas.

Existe um outro tipo (menos intuitivo) de ordenação monomial, a ordem graduada lexicográfica reversa.

**Definição 2.7 (Ordem lexicográfica reversa graduada)** *Sejam $\alpha$ e $\beta \in \mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha >_{grevlex} \beta$ se*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \text{ ou } |\alpha| = |\beta| \text{ e a primeira entrada à direita não nula de } \alpha-\beta \in \mathbb{Z}^n_{\geq 0} \text{ é negativa.}$$

Alguns exemplos:

- $(4,7,1) >_{grevlex} (4,2,3)$ pois $|(4,7,1)| = 12 > |(4,2,3)| = 9$
- $(1,5,2) >_{grevlex} (4,1,3)$ pois $|(1,5,2)| = |(4,1,3)|$ e $(1,5,2)-(4,1,3) = (-3,4,-1)$
- Note que a ordem das variáveis $x_1,\ldots,x_n$ é a mesma com $lex$ e $grevlex$. Isto é,

$$x_1 >_{lex} \cdots >_{lex} x_n \quad \text{e} \quad x_1 >_{grevlex} \cdots >_{grevlex} x_n.$$

A demonstração de que $>_{grevlex}$ é uma ordem monomial segue passos similares aos que foram feitos nas Proposições 2.4 e 2.6.

**Exemplo 2.8** *Seja* $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in \mathbb{K}[x,y,z]$.

1. *Com respeito a ordem lexicográfica, podemos reescrever os termos de* $f$ *em ordem decrescente da seguinte forma*
$$f = -5x^3 + 7x^2z^2 + 4xyz^2 + 4z^2.$$

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

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

**Definição 2.9** *Seja* $f = \Sigma_\alpha a_\alpha x^\alpha \neq 0$ *em* $\mathbb{K}[x_1,\ldots,x_n]$ *e seja* $>$ *uma ordem monomial:*

- *O* ***multigrau*** *de* $f$ *é* $multigrau(f) = max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0)$. *(o máximo é pego com respeito a* $>$*).*
- *O* ***coeficiente líder*** *de* $f$ *é* $LC(f) = a_{multigrau(f)} \in \mathbb{K}$.
- *O* ***líder monomial*** *de* $f$ *é* $LM(f) = x^{multigrau(f)}$ *(com coeficiente 1).*
- *O* ***termo líder*** *de* $f$ *é* $LT(f) = LC(f) \cdot LM(f)$.

Para ilustrar, seja $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ e $>$ a ordem lexicográfica. Então
$$multigrau(f) = (3,0,0),\ LC(f) = -5,\ LM(f) = x^3 \text{ e } LT(f) = -5x^3.$$

**Lema 2.10** *Sejam* $f,g \in \mathbb{K}[x_1,\ldots,x_n]$ *polinômios não nulos. Então:*

1. $multigrau(f \cdot g) = mulitigrau(f) + multigrau(g)$.
2. *Se* $f+g \neq 0$, *então* $multigrau(f+g) \leq max(multigrau(f), multigrau(g))$. *Se ainda* $multigrau(f) \neq multigrau(g)$, *então a igualdade ocorre.*

**Demonstração:** A prova desse resultado segue as ideias de [2, Lema 2.11].

1. Por definição, o multigrau de $f \cdot g$ é o expoente do termo líder de $f \cdot g$. É claro que o termo líder de $f \cdot g$ é igual ao termo líder de $f$ vezes o termo líder de $g$. Seja $LT(f) = a_\alpha x^\alpha$, onde $\alpha = multigrau(f)$ e $LT(g) = b_\beta x^\beta$, onde $\beta = multigrau(g)$. Assim $LT(f) \cdot LT(g) = a_\alpha x^\alpha \cdot b_\beta x^\beta = a_\alpha b_\beta x^{\alpha+\beta}$, onde $multigrau(f \cdot g) = \alpha + \beta = multigrau(f) + multigrau(g)$.

2. Se $f+g \neq 0$, afirmamos que o multigrau de $f+g$ é menor ou igual que o máximo dos multigraus de $f$ e $g$ pois, como estamos somando dois polinômios, o multigrau da soma obviamente não pode ser aumentado, isto poderia acontecer se fizéssemos a multiplicação de $f$ e $g$, porém com a soma isto é impossível. O que pode acontecer é que nessa soma alguns termos de $f$ e $g$ se cancelem, inclusive os termos líderes, fazendo com que o multigrau da soma seja menor que o máximo dos multigraus. Porém como não podemos garantir que isso ocorra sempre, segue que $multigrau(f+g) \leq max(multigrau(f), multigrau(g))$.
   Se $multigrau(f) \neq multigrau(g)$ então suponha sem perda de generalidade que $multigrau(f) > multigrau(g)$, assim não existe a possibilidade do termo líder de $f$ ser cancelado por nenhum termo de $g$, logo $multigrau(f+g) = multigrau(f) = max(multigrau(f), multigrau(g))$.

■

De agora em diante, assumiremos que uma ordem monomial específica foi selecionada, e que os termos líderes, multigraus, etc. serão calculados apenas em relação a essa ordem.

## 2.2 Um algoritmo de divisão em $\mathbb{K}[x_1,\ldots,x_n]$

Pelo algoritmo da divisão em uma variável, podemos determinar se um polinômio pertence ou não a um ideal de $\mathbb{K}[x]$. Como todo ideal $I$ de $\mathbb{K}[x]$ é da forma $I = \langle f \rangle$, para algum $f \in \mathbb{K}[x]$, é possível determinar se um polinômio $g$ pertence ao ideal $I$ realizando a divisão de $g$ por $f$. Se o resto é zero, então $g \in I$, e se o resto não for zero, $g \notin I$. Para resolver esse problema para mais variáveis, apresentaremos aqui um algoritmo para dividir polinômios em mais de uma variável que estende o algoritmo em $\mathbb{K}[x]$.

**Teorema 2.11 (Algoritmo da divisão)** *Sejam $>$ uma ordem monomial em $\mathbb{Z}^n_{\geq 0}$ e $F = (f_1,\ldots,f_s)$ uma s-upla ordenada de polinômios em $\mathbb{K}[x_1,\ldots,x_n]$. Então todo $f \in \mathbb{K}[x_1,\ldots,x_n]$ pode ser escrito por*

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

*onde* $a_i, r \in \mathbb{K}[x_1,\ldots,x_n]$ *e* $r = 0$ *ou* $r$ *é uma combinação linear com coeficientes em* $\mathbb{K}$*, de monômios, nenhum deles divisível por nenhum dos* $LT(f_1),\ldots,LT(f_s)$*. Vamos chamar de* $r$ *o* ***resto*** *da divisão de* $f$ *por* $F$*. Além disso, se* $a_i f_i \neq 0$*, então nós temos*

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

**Demonstração:** A prova é feita a partir do seguinte algoritmo.

**Entrada:** $f_1,\ldots,f_s,f$.

**Saída:** $a_1,\ldots,a_s,r$.

1. $a_1 := 0;\ldots;a_s := 0; r := 0$
2. $p := f$
3. ENQUANTO $p \neq 0$ FAZER
4. $\quad i := 1$
5. $\quad$ divisaoocorrida := falso
6. $\quad$ ENQUANTO $i \leq s$ e divisaoocorrida=falso FAZER
7. $\quad\quad$ SE $LT(f_i)$ divide $LT(p)$ ENTÃO
8. $\quad\quad\quad a_i := a_i + LT(p)/LT(f_i)$
9. $\quad\quad\quad p := p - (LT(p)/LT(f_i))f_i$
10. $\quad\quad\quad$ divisaocorrida:=verdadeiro
11. $\quad\quad$ SENÃO
12. $\quad\quad\quad i = i + 1$
13. $\quad$ SE divisaoocorrida=falso ENTÃO
14. $\quad\quad r := r + LT(p)$
15. $\quad\quad p := p - LT(p)$

Onde a variável "divisaoocorrida" nos diz se algum $LT(f_i)$ divide o termo líder de algum dividendo intermediário. Observe que cada vez que passamos pelo loop "ENQUANTO...FAZER", precisamente uma das seguintes afirmações acontecerá:

- (Etapa da divisão) Se algum $LT(f_i)$ divide $LT(p)$, então o algoritmo segue da forma que no caso de uma variável.
- (Etapa do resto) Se nenhum $LT(f_i)$ divide $LT(p)$, então o algoritmo adiciona $LT(p)$ ao resto.

No exemplo seguinte mostraremos como organizar essa divisão. Para provar que o algoritmo funciona, vamos começar mostrando que

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \tag{2.1}$$

vale em todas as fases. Para os valores iniciais de $a_1,\ldots,a_s,p$ e $r$, (2.1) é verdadeira. Agora suponha que (2.1) seja válida em alguma etapa do algoritmo. Se a próxima etapa é a da divisão, então algum $LT(f_i)$ divide $LT(p)$, e a igualdade

$$a_i f_i + p = (a_i + LT(p)/LT(f_i))f_i + (p - (LT(p)/LT(f_i))f_i)$$

mostra que $a_i f_i + p$ permanece inalterado. Como todas as outras variáveis não são afetadas, (2.1) continua sendo verdade nesse caso. Por outro lado, se a próxima etapa é a do resto, então $p$ e $r$ serão alterados, mas a soma $p+r$ não se altera porquê

$$p + r = (p - LT(p)) + (r + LT(p)).$$

E como antes, a equação (2.1) ainda é preservada.

Em seguida, note que o algoritmo para quando $p = 0$. Nessa situação, (2.1) se torna

$$a_1 f_1 + \cdots + a_s f_s + r.$$

Como os termos são adicionados a $r$ somente quando não são divisíveis por nenhum dos $LT(f_i)$, segue-se que $a_1,\ldots,a_s$ e $r$ têm as propriedades desejadas quando o algoritmo termina. Finalmente, precisamos mostrar que o algoritmo em algum momento terminará. O ponto chave é que cada vez que redefinimos a variável $p$, ou seu multigrau diminui (em relação à nossa ordenação de termos) ou se torna 0. Para ver isso, primeiro suponha que durante uma Etapa de Divisão, $p$ seja redefinido para ser

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

Pelo Lema 2.10, temos que

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

então $p$ e $(LT(p)/LT(f_i))f_i$ têm o mesmo termo líder. Logo, a diferença entre eles $p'$ deve ter um multigrau estritamente menor enquanto $p' \neq 0$. Em seguida, suponha que em alguma etapa do

resto, $p$ é redefinido a ser

$$p' = p - LT(p).$$

Aqui fica claro que $multigrau(p') < multigrau(p)$ quando $p' \neq 0$. Portanto, em cada caso, o multigrau vai diminuir. Se o algoritmo nunca termina, então obteremos uma sequência decrescente infinita de multigraus. A boa ordenação de $>$, como enunciada no Lema 2.2, nos mostra que isso não pode acontecer. Então $p = 0$ irá acontecer em algum momento, e o algoritmo terminará em um número finito de passos.

Resta apenas analisar a relação entre $multigrau(f)$ e $multigrau(a_i f_i)$. Cada termo em $a_i$ é da forma $LT(p)/LT(f_i)$ para algum valor da variável $p$. O algoritmo começa com $p = f$, e acabamos de provar que o multigrau de $p$ diminui. Isso mostra que $LT(p) \leq LT(f)$, e então segue, (usando a condição 2 da Definição 2.1) que $multigrau(a_i f_i) \leq multigrau(f)$ quando $a_i f_i \neq 0$. Isso completa a prova do Teorema. ■

**Exemplo 2.12** *Vamos dividir* $f = x^2y + xy^2 + y^2$ *por* $f_1 = y^2 - 1$ *e* $f_2 = xy - 1$ *com a ordem lexicográfica, considerando* $x > y$.

| | $x+1$ , $x$ | $r$ |
|---|---|---|
| $x^2y + xy^2 + y^2$ | $y^2 - 1$ , $xy - 1$ | |
| $-x^2y + x$ | | |
| $xy^2 + x + y^2$ | | |
| $-xy^2 + x$ | | |
| $2x + y^2$ | | |
| $-2x$ | | $2x$ |
| $y^2$ | | |
| $-y^2 + 1$ | | |
| $1$ | | |
| $-1$ | | $2x + 1$ |
| $0$ | | |

*Isso mostra que*

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

Realizando a divisão mudando a ordem dos divisores $f_1 = xy - 1$ e $f_2 = y^2 - 1$, obtém-se (ver [4, Example 2.3.2])

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

O exemplo acima é uma ilustração de como funciona o algoritmo de divisão. Também nos mostra

uma propriedade que queremos que o resto tenha: Nenhum dos seus termos deve ser divisível pelos termos principais dos polinômios pelos quais estamos dividindo.

Um fato interessante do algoritmo da divisão em $\mathbb{K}[x]$ é que, após realizá-lo, o problema do membro de um ideal é resolvido. Mas e para mais de uma variável?

Se dividirmos um polinômio $f$ por $F = (f_1, \ldots, f_s)$ e obtemos resto 0, então, pelo Teorema 2.11,

$$f = a_1 f_1 + \cdots + a_s f_s.$$

Ou seja, $f \in \langle f_1, \ldots, f_s \rangle$. Logo, $r = 0$ é uma condição *suficiente* para falar que um polinômio é membro de um ideal. Contudo, como o seguinte exemplo mostra, $r = 0$ não é uma condição *necessária* para ele estar no ideal.

**Exemplo 2.13** *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 $F = (f_1, f_2)$, o resultado é*

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

*Mas considerando $F = (f_2, f_1)$, obtemos*

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

*O segundo cálculo mostra que $f \in \langle f_1, f_2 \rangle$ enquanto o primeiro mostra que, mesmo que $f \in \langle f_1, f_2 \rangle$, ainda é possível o resto de sua divisão por $F = (f_1, f_2)$ não ser 0.*

Portanto, podemos concluir que o algoritmo da divisão dado no Teorema 2.11 é uma generalização imperfeita do algoritmo realizado em uma variável. Dado um ideal $I$ ainda podemos perguntar se pode haver um conjunto gerador "bom" para $I$. Para tal conjunto, gostaríamos que o resto r na divisão pelos "bons" geradores deve ser determinado exclusivamente e a condição r = 0 deve ser equivalente à "pertença ao ideal". Mais adiante, na seção 2.4, veremos o conceito de Base de Gröbner, que tem exatamente essas "boas" propriedades.

## 2.3 Ideais Monomiais e o Lema de Dickson

Para dar início a essa seção, vamos definir o que são ideais monomiais em $\mathbb{K}[x_1, \ldots, x_n]$.

**Definição 2.14** *Um ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$ é um* ***ideal monomial*** *se existe $A \subset \mathbb{Z}^n_{\geq 0}$ tal que $I$ está gerado por $\{x^\alpha : \alpha \in A\}$. Isto é, $I$ consiste de todos os polinômios que são somas finitas da forma $\sum_{\alpha\in A} h_\alpha x^\alpha$ onde $h_\alpha \in \mathbb{K}[x_1,\ldots,x_n]$. Nesse caso, escrevemos $I = \langle x^\alpha \ : \ \alpha \in A\rangle$.*

Um exemplo de ideal monomial é dado por $I = \langle x^4y^2, x^3y^4, x^2y^5\rangle \subset \mathbb{K}[x,y]$.

Agora, precisamos caracterizar todos os monômios que se encontram em um dado ideal monomial.

**Lema 2.15** *Seja $I = \langle x^\alpha \ ; \ \alpha \in A\rangle$, um ideal monomial. Então, um monômio $x^\beta$ está em $I$ se, e somente se, $x^\beta$ é divisível por $x^\alpha$ para algum $\alpha \in A$.*

**Demonstração:** Se $x^\beta$ é múltiplo de $x^\alpha$, para algum $\alpha \in A$, então $x^\beta \in I$ pela definição de ideal. Por outro lado, se $x^\beta \in I$, então $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, onde, por construção, $h_i \in \mathbb{K}[x_1,\ldots,x_n]$ e $\alpha(i) \in A$. Observe que para cada $i \in \{1,\ldots,s\}$ existe um conjunto $B_i \subset \mathbb{Z}^n_{\geq 0}$ tal que $h_i = \sum_{\gamma\in B_i} a_\gamma x^\gamma$, onde $a_\gamma \in \mathbb{K}$, para todo $\gamma \in B_i$. Assim, $x^\beta = \sum_{i=1}^{s}\sum_{\gamma\in B_i} a_\gamma x^{\gamma+\alpha(i)}$. Por se tratar de uma igualdade, $x^\beta$ também deve aparecer do lado direito. Logo, devem existir $i \in \{1,\ldots,s\}$ e $\gamma \in B_i$ tais que $x^\beta = x^{\gamma+\alpha(i)}$ ou, em outras palavras, $x^\beta$ é divisível por $x^{\alpha(i)}$. ■

Note que $x^\beta$ é divisível por $x^\alpha$ exatamente quando existe um $\gamma \in \mathbb{Z}^n_{\geq 0}$ tal que $x^\beta = x^\alpha \cdot x^\gamma$, isso é equivalente a $\beta = \alpha + \gamma$. Então, o conjunto $\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma : \gamma \in \mathbb{Z}^n_{\geq 0}\}$ consiste de todos os expoentes dos monômios que são divisíveis por $x^\alpha$. Essa observação juntamente com o Lema 2.15 nos permite desenhar os monômios em um determinado ideal monomial. Por exemplo, se $I = \langle x^3y^1, x^2y^2, x^1y^2\rangle$, então os expoentes dos monômios de $I$ formam o conjunto

$$((3,1) + \mathbb{Z}^2_{\geq 0}) \cup ((2,2) + \mathbb{Z}^2_{\geq 0}) \cup ((1,2) + \mathbb{Z}^2_{\geq 0}).$$

Podemos visualizar este conjunto como a união dos pontos com coordenadas inteiras no primeiro quadrante do plano $(x,y)$ como segue:

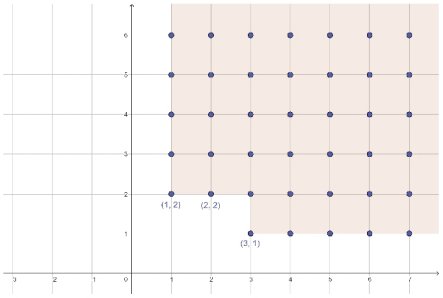



**FIGURA 2.1:** $(m,n) \leftrightarrow x^m y^n$.

Vamos mostrar a seguir que um dado polinômio $f$ está ou não em um ideal monomial ao olharmos para cada um de seus monômios.

**Lema 2.16** *Seja $I$ um ideal monomial e seja $f \in \mathbb{K}[x_1,\ldots,x_n]$. Então são equivalentes:*

1. *$f \in I$;*
2. *Cada termo de $f$ está em $I$;*
3. *$f$ é uma combinação $\mathbb{K}$-linear dos monômios em $I$.*

**Demonstração:** Note que $3 \Rightarrow 2 \Rightarrow 1$ acontecem diretamente por definição. Provemos agora $1 \Rightarrow 3$. Suponha que $I$ seja da forma $I = \langle x^\alpha : \alpha \in A\rangle$, em que $\emptyset \neq A \subset \mathbb{Z}^n_{\geq 0}$. Por definição, $f = \sum_{i=1}^{s} h_i x^{\alpha(i)}$ com $h_i \in \mathbb{K}[x_1,\ldots,x_n]$ e $\alpha(i) \in A$, então $f = h_1 x^{\alpha(1)} + h_2 x^{\alpha(2)} + \ldots + h_s x^{\alpha(s)}$. Analisando o lado direito da igualdade, temos que, para cada termo de $f$, existe $i \in \{1,\ldots,s\}$ tal que $x^{\alpha(i)}$ divide esse termo. Logo $f$ é uma combinação $\mathbb{K}$-linear dos monômios de $I$. ■

Uma consequência imediata da parte 3 do Lema acima é que um ideal monomial é determinado unicamente por seus monômios. Assim, temos o seguinte Corolário.

**Corolário 2.17** *Dois ideais monomiais são iguais se, e somente se, eles contêm os mesmos monômios.*

O principal resultado dessa seção é que todos os ideais monomiais de $\mathbb{K}[x_1,\ldots,x_n]$ são finitamente gerados.

**Teorema 2.18 (Lema de Dickson)** *Seja $I = \langle x^\alpha : \alpha \in A\rangle \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal monomial. Então $I$ pode ser escrito na forma $I = \langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle$, onde $\alpha(1),\ldots,\alpha(s) \in A$. Em particular, $I$ tem uma base finita.*

**Demonstração:** Procedamos por indução em $n$, o número de variáveis.

Seja $n = 1$ e $\beta$ o menor elemento de $A \subset \mathbb{Z}_{\geq 0} = \mathbb{Z}^+$. Então $\beta \leq \alpha$ para todo $\alpha \in A$, o que significa $x_1^\beta$ divide todos os outros geradores $x_1^\alpha$. Daí, segue que $I = \langle x_1^\beta\rangle$.

Agora assuma que o Teorema vale para $n-1 \geq 1$. Escreveremos as variáveis como $x_1,\ldots,x_{n-1},y$, de modo que os monômios em $\mathbb{K}[x_1,\ldots,x_{n-1},y]$ possam ser escritos como $x^\alpha y^m$, onde $\alpha = (\alpha_1,\ldots,\alpha_{n-1}) \in \mathbb{Z}^{n-1}_{\geq 0}$ e $m \in \mathbb{Z}_{\geq 0} = \mathbb{Z}^+$.

Suponha que $I \subset \mathbb{K}[x_1,\ldots,x_{n-1},y]$ seja um ideal monomial. Para achar os geradores de $I$, considere $J$ o ideal em $\mathbb{K}[x_1,\ldots,x_{n-1}]$ gerado pelos monômios $x^\alpha$ 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 existe uma quantidade finita de $x^\alpha$s que geram $J$, então seja $J = \langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle$. O ideal $J$ pode ser entendido como a "projeção" de $I$ em $\mathbb{K}[x_1,\ldots,x_{n-1}]$.

Para cada $i$ entre 1 e $s$, a definição de $J$ nos diz que $x^{\alpha(i)}y^{m_i} \in I$ para algum $m_i \geq 0$. Seja $m$ o maior dos $m_i$. Então, para cada $k$ de 1 até $m-1$, considere o ideal $J_k \subset \mathbb{K}[x_1,\ldots,x_{n-1}]$ gerado pelos monômios $x^\beta$ tal que $x^\beta y^k \in I$. Pode-se pensar em $J_k$ como a "fatia" de $I$ gerada por monômios contendo $y$ exatamente elevado à $k$-ésima potência. Usando nossa hipótese de indução mais uma vez, temos que $J_k$ tem um conjunto gerador finito de monômios, isto é, $J_k = \langle x^{\alpha_k(1)},\ldots,x^{\alpha_k(s_k)}\rangle$.

Afirmamos que $I$ é gerado pelos monômios na lista:

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

Primeiramente, note que todo monômio em $I$ é divisível por algum monômio da lista. Para ver o porquê, seja $x^\alpha y^p \in I$. Suponha primeiro $p \geq m$. Como $x^\alpha y^p \in I$, então $x^\alpha \in J$, isso implica que $x^\alpha$ é divisível por algum $x^{\alpha(i)}$. Portanto, $x^{\alpha(i)}y^p$ é divisível por $x^\alpha y^m$. Por outro lado, se $p \leq m-1$, então $x^\alpha \in J_p$, logo existe $x^{\alpha_p(i)}$ que divide $x^\alpha$. Portanto, $x^{\alpha_p(i)}y^p$ divide $x^\alpha y^p$. Pelo Corolário 2.17, isso força os ideais a serem os mesmos, e nossa afirmação está provada.

Para completar a prova do Teorema, precisamos mostrar que o conjunto finito de geradores pode ser escolhido a partir do conjunto inicial de geradores do ideal. Se voltamos a escrever as variáveis como $x_1,\ldots,x_n$, então nosso ideal monomial é $I = \langle x^\alpha : \alpha \in A\rangle \subset \mathbb{K}[x_1,\ldots,x_n]$. Precisamos mostrar que $I$ é gerado por um número finito de $x^\alpha$s, onde $\alpha \in A$. Pelo parágrafo anterior, sabemos que $I = \langle x^{\beta(1)},\ldots,x^{\beta(s)}\rangle$ para alguns monômios $x^{\beta(i)}$ em $I$. Como $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A\rangle$, novamente pelo Lema 2.15 temos que cada $x^{\beta(i)}$ é divisível por $x^{\alpha(i)}$ para algum $\alpha(i) \in A$. Dessa forma, $I = \langle x^{\beta(1)},\ldots,x^{\beta(s)}\rangle \subseteq \langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle$. Como $\alpha(i) \in A$, então $\langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle \subseteq \langle x^\alpha : \alpha \in A\rangle = I$. Isso mostra que $I = \langle x^{\alpha(1)}\ldots x^{\alpha(s)}\rangle$. ■

O Lema de Dickson resolve o problema da descrição de ideais monomiais e nos diz que tais ideais têm uma base finita. Isso nos permite resolver também o problema de membro de um ideal

para ideais monomiais. Isto é, se $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, vamos mostrar que $f \in I$ se e só se o resto de $f$ na divisão de $f$ por $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ for zero:

A volta é trivial. Por outro lado, seja $f \in I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, pelo Lema 2.16 cada termo de $f$ está em $I$, pelo Lema 2.15, cada termo de $f$ deverá ser divisível por algum $x^{\alpha(i)}$, o que torna o resto da divisão de $f$ por $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ igual a 0.

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

**Corolário 2.19** *Seja $>$ uma relação em $\mathbb{Z}^n_{\geq 0}$ satisfazendo:*

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

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

**Demonstração:** $\Rightarrow$: Assumindo que $>$ é de boa ordem, existe o menor elemento de $\mathbb{Z}^n_{\geq 0}$ que chamaremos de $\alpha_0$. É suficiente mostrar que $\alpha_0 \geq 0$: Se $0 > \alpha_0$, então pela segunda hipótese, podemos adicionar $\alpha_0$ dos dois lados e obter $\alpha_0 > 2\alpha_0$, o que é impossível já que $\alpha_0$ é o menor elemento de $\mathbb{Z}^n_{\geq 0}$.

$\Leftarrow$: Assumindo que $\alpha \geq 0$ para todos $\alpha \in \mathbb{Z}^n_{\geq 0}$, seja $A \subset \mathbb{Z}^n_{\geq 0}$ não vazio. Precisamos mostrar que $A$ tem um menor elemento. Como $I = \langle x^\alpha : \alpha \in A \rangle$ é um ideal monomial, o Lema de Dickson nos dá que existem elementos $\alpha(1), \ldots, \alpha(s) \in A$ tais que $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Suponha, sem perda de generalidade, que $\alpha(1) < \alpha(2) < \cdots < \alpha(s)$. Afirmamos que $\alpha(1)$ é o menor elemento de $A$. Para provar isso, seja $\alpha \in A$. Então $x^\alpha \in I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, então pelo Lema 2.15, $x^\alpha$ é divisível por algum $x^{\alpha(i)}$. Isso nos dá que $\alpha = \alpha(i) + \gamma$ para algum $\gamma \in \mathbb{Z}^n_{\geq 0}$. Então $\gamma \geq 0$ e, pela hipótese (ii),

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

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

## 2.4 O Teorema da Base de Hilbert e Bases de Gröbner.

**Definição 2.20** *Seja $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal não-nulo.*

1. *Denotamos por $LT(I)$ o conjunto dos termos líderes dos elementos de $I$. Então,*

$$LT(I) = \{cx^{\alpha} : \exists f \in I \text{ que satisfaz } LT(f) = cx^{\alpha}\}; \tag{2.2}$$

2. *Denotamos por $\langle LT(I)\rangle$ o ideal gerado pelos elementos do $LT(I)$.*

Por definição $LT(f_i) \in LT(I) \subset \langle LT(I)\rangle$, o que implica que $\langle LT(f_1),\ldots,LT(f_s)\rangle$ está contido em $\langle LT(I)\rangle$. Contudo, $\langle LT(I)\rangle$ pode ser estritamente maior. Para ver isso, considere o seguinte exemplo.

**Exemplo 2.21** *Seja $I = \langle f_1, f_2\rangle$, onde $f_1 = x^3 - 2xy$ e $f_2 = x^2y - 2y^2 + x$, e use a ordem graduada lexicográfica dos monômios em $\mathbb{K}[x,y]$. Como*

$$x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^2, \tag{2.3}$$

*então $x^2 \in I$. Logo $x^2 = LT(x^2) \in \langle LT(I)\rangle$. Todavia, $x^2$ não é divisível por $LT(f_1) = x^3$ ou $LT(f_2) = x^2y$, portanto $x^2 \notin \langle LT(f_1), LT(f_2)\rangle$ pelo Lema 2.17.*

Mostremos agora que $\langle LT(I)\rangle$ é um ideal monomial.

**Proposição 2.22** *Seja $I \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal.*

1. *$\langle LT(I)\rangle$ é um ideal monomial;*

2. *Existem $g_1,\ldots,g_t \in I$ que satisfazem $\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$.*

**Demonstração:** 1. Os líderes monomiais $LM(g)$ dos elementos $g \in I - \{0\}$ geram o ideal monomial $\langle LM(g) : g \in I - \{0\}\rangle$. Como $LM(g)$ e $LT(g)$ são múltiplos um do outro, esse ideal é igual ao ideal $\langle LT(g) : g \in I - \{0\}\rangle = \langle LT(I)\rangle$. Então, $\langle LT(I)\rangle$ é um ideal monomial.
2. Desde que $\langle LT(I)\rangle$ é gerado pelos monômios $LM(g)$ para $g \in I - \{0\}$, o Lema de Dickson nos diz que $\langle LT(I)\rangle = \langle LM(g_1),\ldots,LM(g_t)\rangle$ para $g_1,\ldots,g_t \in I$. Como $LM(g_i)$ é múltiplo de $LT(g_i)$, segue que $\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$. Isso completa a prova. ■

Assim, a Proposição 2.22 e o algoritmo da divisão provam juntos a existência de um conjunto gerador para qualquer ideal polinomial, nos dando uma resposta afirmativa para o nosso **problema da descrição de um ideal**. Seja $I \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal qualquer e considere o ideal associado $\langle LT(I)\rangle$ como na Definição 2.20. Como de costume, selecionamos uma ordenação monomial particular para usar no algoritmo da divisão e para calcular alguns termos líderes.

**Teorema 2.23 (Teorema da Base de Hilbert)** *Todo ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$ tem um conjunto gerador finito. Isto é, existem $g_1,\ldots,g_t \in I$ tais que $I = \langle g_1,\ldots,g_t\rangle$.*

**Demonstração:** Se $I = \{0\}$, nosso conjunto gerador procurado é $\{0\}$, que é finito. Se $I$ contém algum polinômio não-nulo, então, pela última Proposição, existem $g_1,\ldots,g_t \in I$ tais que $\langle LT(I)\rangle$ é igual ao ideal $\langle LT(g_1),\ldots,LT(g_t)\rangle$. Provemos que $I = \langle g_1,\ldots,g_t\rangle$.

É claro que $\langle g_1,\ldots,g_t\rangle \subset I$ pois cada $g_i \in I$. Agora, seja $f \in I$ um polinômio qualquer. Se aplicarmos o algoritmo da divisão (Teorema 2.11) para dividir $f$ por $g_1,\ldots,g_t$, obtemos a expressão

$$f = a_1g_1 + \ldots + a_tg_t + r, \tag{2.4}$$

onde nenhum termo de $r$ é divisível por qualquer um dos $LT(g_1),\ldots,LT(g_t)$.

Provemos que $r = 0$. De fato, note que

$$r = f - a_1g_1 - \ldots - a_tg_t, \tag{2.5}$$

ou seja, $r \in I$. Se $r \neq 0$, então $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$ e pelo Lema 2.17, temos que $LT(r)$ deve ser divisível por algum $LT(g_i)$ com $i \in \{1,\ldots,t\}$, o que contradiz o fato de $r$ ser um resto da divisão e, consequentemente, $r$ deve ser zero. Então

$$f = a_1g_1 + \ldots + a_tg_t \in \langle g_1,\ldots,g_t\rangle, \tag{2.6}$$

o que mostra que $I \subset \langle g_1,\ldots,g_t\rangle$ e assim temos que $I = \langle g_1,\ldots,g_t\rangle$. ■

Note que a base $g_1,\ldots,g_t$ usada na prova do Teorema da Base de Hilbert tem uma propriedade especial: $\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$. Como vimos no último exemplo, nem todas as bases de um ideal se comportam assim. As bases que possuem esse comportamento, têm um nome especial.

**Definição 2.24 (Base de Gröbner)** *Dada uma ordem monomial num anel de $\mathbb{K}[x_1,\ldots,x_n]$, um subconjunto $G = \{g_1,\ldots,g_t\} \subset \mathbb{K}[x_1,\ldots,x_n]$ de um ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$ não nulo é dito* ***Base de Gröbner*** *(ou* ***Base Padrão****) se*

$$\langle LT(g_1),\ldots,LT(g_t)\rangle = \langle LT(I)\rangle. \tag{2.7}$$

*Convencionando que $\langle\varnothing\rangle = \{0\}$, definimos que o conjunto vazio $\varnothing$ é a Base de Gröbner do ideal nulo $\{0\}$.*

**Corolário 2.25** *Fixe uma ordem monomial. Então qualquer ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$ não nulo tem uma Base de Gröbner. Além disso, qualquer Base de Gröbner para um ideal $I$ é uma base de $I$.*

**Demonstração:** Dado um ideal não nulo, o conjunto $G = \{g_1,\ldots,g_t\}$ construído na prova do Teorema de Hilbert é uma Base de Gröbner por definição. Sobre a segunda afirmação, note que se $\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$ então pelo mesmo Teorema sabemos que $I = \langle g_1,\ldots,g_t\rangle$, de forma que $G$ é uma base para $I$. ■

**Exemplo 2.26** *Considere o ideal $I$ do exemplo 2.21 que tem a base $B = \{f_1,f_2\} = \{x^3-2xy, x^2y-2y^2+x\}$. Logo, como $x^2 \in \langle LT(I)\rangle$, mas $x^2 \notin \langle LT(f_1),LT(f_2)\rangle$, $B$ não é uma Base de Gröbner para $I$ com respeito a ordem graduada lexicográfica. Mais adiante veremos como achar uma Base de Gröbner para $I$.*

**Exemplo 2.27** *Em seguida, 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 $J$ usando a ordem lexicográfica em $\mathbb{R}[x,y,z]$. Assim, temos que mostrar que o termo líder de qualquer elemento não nulo de $J$ pertence ao ideal $\langle LT(g_1),LT(g_2)\rangle = \langle x,y\rangle$. Pelo Lema 2.15, isso é equivalente a mostrar que o termo líder de qualquer elemento não nulo de $J$ é divisível por $x$ ou $y$.*

*Para provar isso, considere qualquer $f = h_1g_1 + h_2g_2 \in J$. Suponha, por absurdo que $f$ não é o polinômio nulo e que $LT(f)$ não é divisível nem por $x$, nem por $y$. Pela definição de ordem lexicográfica, $f$ deve ser um polinômio que dependa apenas de $z$. Contudo, $f$ se anula no conjunto $L = \mathcal{V}(x+z,y-z) \subset \mathbb{R}^3$, pois $f \in J$. Observe que todo ponto da forma $(-t,t,t) \in L$ para qualquer número real $t$. O único polinômio que depende apenas de $z$ que se anula em todos os pontos de $L$ então é o polinômio nulo, que é uma contradição. Portanto, segue que $\langle g_1,g_2\rangle$ é uma Base de Gröbner para $J$.*

Concluiremos essa seção com duas aplicações do Teorema da Base de Hilbert. A primeira é algébrica pois tange aos ideais de $\mathbb{K}[x_1,\ldots,x_n]$. Uma **cadeia ascendente** de ideais é uma sequência ordenada estritamente crescente:

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

Por exemplo, a sequência

$$\langle x_1\rangle \subset \langle x_1,x_2\rangle \subset \cdots \subset \langle x_1,\ldots,x_n\rangle \tag{2.8}$$

forma uma (finita) cadeia ascendente de ideais. Se tentarmos estender essa cadeia incluindo qualquer outro gerador $f \in \mathbb{K}[x_1,\ldots,x_n]$, duas possibilidades podem acontecer. Se $f \in \langle x_1,\ldots,x_n\rangle$,

temos que $\langle x_1,\ldots,x_n,f\rangle = \langle x_1,\ldots,x_n\rangle$ e nada mudou. Por outro lado, se $f \notin \langle x_1,\ldots,x_n\rangle$, afirmamos que $\langle x_1,\ldots,x_n,f\rangle = \mathbb{K}[x_1,\ldots,x_n]$. De fato, se $f \notin \langle x_1,\ldots,x_n\rangle$, então pelo algoritmo da divisão, $f = a_1x_1+\cdots+a_nx_n+r$, com $r \in \mathbb{K}$ não nulo. Dessa forma, $1 = r^{-1}(f - a_1x_1 - \cdots - a_nx_n) \in \langle x_1,\ldots,x_n,f\rangle$. Logo, $\langle x_1,\ldots,x_n,f\rangle = \mathbb{K}[x_1,\ldots,x_n]$ e nossa afirmação está provada. Em ambos os casos, a cadeia ascendente (2.8) estabilizou após um número finito de etapas, no sentido em que todos os ideais a partir de um certo ponto serão iguais. Nosso próximo resultado mostra que o mesmo fenômeno ocorre em *qualquer* cadeia de ideais de $\mathbb{K}[x_1,\ldots,x_n]$.

**Teorema 2.28 (A Condição da Cadeia Ascendente)** *Seja*

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

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

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

**Demonstração:** Dada a cadeia ascendente $I_1 \subset I_2 \subset I_3 \subset \cdots$, considere o conjunto $I = \bigcup_{i=1}^{\infty} I_i$. Mostremos que $I$ é um ideal em $\mathbb{K}[x_1,\ldots,x_n]$. Primeiramente, $0 \in I$ já que $0 \in I_i$ para todo $i$. Em seguida, se $f,g \in I$, então, por definição, $f \in I_i$ e $g \in I_j$ para alguns $i$ e $j$ (não necessariamente iguais). Como os ideais estão em cadeia ascendente, sem perda de generalidade suponha que $i \leq j$, então ambos $f,g$ estão em $I_j$. Como $I_j$ é um ideal, a soma $f+g \in I_j$, assim $f+g \in I$. Além disso, se $f \in I$ e $r \in \mathbb{K}[x_1,\ldots,x_n]$, então $f \in I_i$ para algum $i$, e $r \cdot f \in I_i \subset I$. Portanto, $I$ é um ideal.

Pelo Teorema da Base de Hilbert, o ideal $I$ deve ter um conjunto gerador finito: $I = \langle f_1,\ldots,f_s\rangle$. Mas cada um desses geradores está contido em algum $I_j$, digamos que $f_i \in I_{j_i}$, para algum $j_i, i = 1,\ldots,s$. Tome $N$ como o maior entre os $j_i s$. Então, por definição da cadeia ascendente, $f_i \in I_N$ para todo $i$. Assim, temos

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

Como resultado, a cadeia ascendente se estabiliza em $I_N$. Todos os ideais seguintes na cadeia são iguais. ■

Nossa próxima aplicação do Teorema da Base de Hilbert será geométrica. Até esse ponto, consideramos variedades afins como o conjunto de soluções de um sistema de equações polinomiais:

$$\mathcal{V}(f_1,\ldots,f_s) = \{(a_1,\ldots,a_n) \in \mathbb{K}^n : f_i(a_,\ldots,a_n) = 0 \text{ para todo } i\}.$$

O Teorema da Base de Hilbert mostra, na verdade, que faz sentido falar de variedades afins definida por um ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$.

**Definição 2.29** *Seja $I \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal. Denotaremos $\mathcal{V}(I)$ como o conjunto*

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

Como um ideal $I$ não nulo contém infinitos polinômios, o conjunto $\mathcal{V}(I)$ ainda pode ser definido por um conjunto finito de equações polinomiais.

**Proposição 2.30** *$\mathcal{V}(I)$ é uma variedade afim. Em particular, se $I = \langle f_1,\ldots,f_s\rangle$ então $\mathcal{V}(I) = \mathcal{V}(f_1,\ldots,f_s)$.*

**Demonstração:** Pelo Teorema da Base de Hilbert, existem $f_1,\ldots,f_s \in I$ tais que $I = \langle f_1,\ldots,f_s\rangle$. Afirmamos que $\mathcal{V}(I) = \mathcal{V}(f_1,\ldots,f_s)$. Primeiramente, como $f_i \in I$, se $f(a_1,\ldots,a_n) = 0$ para todos $f \in I$, então $f_i(a_1,\ldots,a_n) = 0$, então $f_i(a_1,\ldots,a_n) = 0$, então $\mathcal{V}(I) \subset \mathcal{V}(f_1,\ldots,f_s)$. Por outro lado, seja $(a_1,\ldots,a_n) \in \mathcal{V}(f_1,\ldots,f_s)$ e seja $f \in I$. Já que $I = \langle f_1,\ldots,f_s\rangle$, podemos escrever

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

para algum $h_i \in \mathbb{K}[x_1,\ldots,x_n]$. Mas daí

$$f(a_1,\ldots,a_n) = \sum_{i=1}^{s} h_i(a_1,\ldots,a_n) f_i(a_1,\ldots,a_n)$$

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

■

Então, $\mathcal{V}(f_1,\ldots,f_s) \subset \mathcal{V}(I)$ e, assim, esses conjuntos são iguais.

O ponto chave dessa Proposição é que *variedades são determinadas por ideais*. Por exemplo, na Proposição 1.10 verificamos que $\mathcal{V}(f_1,\ldots,f_s) = \mathcal{V}(g_1,\ldots,g_t)$ quando $\langle f_1,\ldots,f_s\rangle = \langle g_1,\ldots,g_t\rangle$. Essa Proposição é um Corolário imediato da Proposição 2.30.

## 2.5 Propriedades das Bases de Gröbner

Como foi mostrado no capítulo anterior, todo ideal não nulo $I \subset \mathbb{K}[x_1,\ldots,x_n]$ tem uma Base de Gröbner. Aqui, estudaremos as propriedades desse tipo de base e aprenderemos a como detectar quando uma base é uma Base de Gröbner.

Primeiramente, provemos que o resto de uma divisão é unicamente determinado quando os divisores formam uma Base de Gröbner.

**Proposição 2.31** *Seja $G = \{g_1,\ldots,g_t\}$ uma Base de Gröbner para um ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$ e seja $f \in \mathbb{K}[x_1,\ldots,x_n]$. Então existe um único resto $r \in \mathbb{K}[x_1,\ldots,x_n]$ com as seguintes propriedades:*

1. *Nenhum termo de $r$ é divisível por qualquer um dos $LT(g_1),\ldots,LT(g_t)$.*
2. *Existe $g \in I$ tal que $f = g + r$.*

*Em particular, $r$ é o resto da divisão de $f$ por $G$ não importa a ordem em que os elementos de $G$ são listados usando o algoritmo da divisão.*

**Demonstração:** O algoritmo da divisão nos dá que $f = a_1g_1 + \ldots + a_tg_t + r$, onde $r$ satisfaz *1*. Tomando $g = a_1g_1 + \ldots + a_tg_t \in I$, temos que *2* também é satisfeito. Isso prova a existência de $r$.

Para provar a unicidade, suponha que $f = g+r = g'+r'$ satisfazendo *1* e *2*. Então $r-r' = g'-g \in I$. Se $r \neq r'$ então, pela Definição 2.24, $LT(r-r') \in \langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$. Pelo Lema 2.15, segue que $LT(r-r')$ é divisível por algum $LT(g_i)$. Isso é impossível pois nenhum termo de $r$ ou $r'$ é divisível por qualquer um dos $LT(g_1),\ldots,LT(g_t)$. Portanto $r-r'$ deve ser zero e a unicidade está provada.

A parte final da Proposição também é verdade por conta da unicidade de $r$, provada nessa demonstração. ■

Para uma Base de Gröbner, apesar do resto $r$ ser único, os "quocientes" $a_i$ produzidos pelo algoritmo da divisão $f = a_1g_1 + \ldots + a_tg_t + r$ podem mudar se listarmos os divisores numa ordem diferente.

**Exemplo 2.32** *Vamos provar na conclusão desta seção que $G = \{y-x^2, z-x^3\}$ é uma Base de Gröbner para a ordem lexicográfica com $y > z > x$. Dividindo $xyz$ por $y-x^2, z-x^3$, nessa ordem, obtemos pelo Algoritmo da divisão (Teorema 2.11) que*

$$xyz = xz(y-x^2) + x^3(z-x^3) + x^6$$

*e, na ordem contrária, dividindo $xyz$ por $z-x^3, y-x^2$, obtemos que*

$$xyz = xy(z-x^3)+x^4(y-x^2)+x^6.$$

*Mesmo obtendo o mesmo resto em ambas as divisões, os "quocientes" são diferentes nelas. Isso nos mostra que o máximo que podemos esperar é a unicidade do resto na divisão de um polinômio por uma Base de Gröbner.*

**Corolário 2.33** *Seja $G = \{g_1,\ldots,g_t\}$ uma Base de Gröbner para um ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$ e seja $f \in \mathbb{K}[x_1,\ldots,x_n]$. Então, $f \in I$ se e só se o resto da divisão de $f$ por $G$ é zero.*

**Demonstração:** Se o resto da divisão é zero, já vimos que $f \in I$. Por outro lado, dado $f \in I$, temos que $f = f+0$ e isso satisfaz as duas condições da Proposição anterior. Segue que 0 é o resto da divisão de $f$ por $G$. ■

O Corolário 2.33 nos dá um algoritmo para resolver o problema do *membro de um ideal* desde que conheçamos uma Base de Gröbner $G$ para o ideal em questão - só precisa calcular um resto em relação a $G$ para determinar se $f \in I$. Assim sendo, precisamos apenas de um algoritmo para construir uma Base de Gröbner, que será feito na próxima seção.

**Definição 2.34** *Denotamos o resto da divisão de $f$ pela s-upla ordenada $F = (f_1,\ldots,f_s)$ por $\overline{f}^F$. Se $F$ é uma Base de Gröbner para $\langle f_1,\ldots,f_s\rangle$ então, pela Proposição anterior, podemos considerar $F$ como um conjunto (sem qualquer ordem particular).*

Por exemplo, para $F = (x^2y-y^2, x^4y^2-y^2) \subset \mathbb{K}[x,y]$, usando a ordem lexicográfica, temos $\overline{x^5y}^F = xy^3$, pois o algoritmo da divisão nos dá

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

No que vem a seguir discutiremos sobre como inferir que um dado conjunto gerador de um ideal $I$ é uma Base de Gröbner.

**Definição 2.35** *Sejam $f,g \in \mathbb{K}[x_1,\ldots,x_n]$ polinômios não nulos.*

1. *Se multigrau$(f) = \alpha$ e multigrau$(g) = \beta$ então defina $\gamma = (\gamma_1,\ldots,\gamma_n)$, onde $\gamma_i = max(\alpha_i,\beta_i)$ para cada $i$. Chamamos $x^\gamma$ de **mínimo múltiplo comum** de $LM(f)$ e $LM(g)$, escrito $x^\gamma = MMC(LM(f),LM(g))$.*

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

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

Como exemplo, sejam $f = x^3y^2 - x^2y^3 + x$ e $g = 3x^4y + y^2$ em $\mathbb{R}[x,y]$ com a ordem lexicográfica graduada. Então $\gamma = (4,2)$ e

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

Um S-polinômio $S(f,g)$ é "designado" para produzir cancelamento de termos líderes. De fato, o seguinte Lema mostra que todo cancelamento de termos líderes entre polinômios de mesmo multigrau resulta desse tipo de cancelamento.

**Lema 2.36** *Suponha que temos uma soma $\sum_{i=1}^{s} c_i f_i$, onde $c_i \in \mathbb{K}$ e o multigrau$(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ para todo $i$. Se multigrau$\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$ então $\sum_{i=1}^{s} c_i f_i$ é uma combinação $\mathbb{K}$-linear, de S-polinômios $S(f_j,f_k)$ com $1 \leq j,k \leq s$. Além disso, $S(f_j,f_k)$ tem multigrau $< \delta$.*

**Demonstração:** Seja $d_i = LC(f_i)$, então $c_id_i$ é o coeficiente líder de $c_if_i$. Como todos os $c_if_i$ têm multigrau $\delta$ e sua soma tem multigrau estritamente menor, obrigatoriamente $\sum_{i=1}^{s} c_id_i = 0$, caso contrário o multigrau de $\sum_{i=1}^{s} c_if_i$ seria $\delta$, o que é impossível.

Defina $p_i = f_i/d_i$ e observe que $LC(p_i) = 1$. Considere a soma telescópica

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

Pela hipótese, $LT(f_i) = d_ix^\delta$ e o mínimo múltiplo comum de $LT(f_j)$ e $LT(f_k)$ é $x^\delta$. Então

$$S(f_j,f_k) = \frac{x^\delta}{LT(f_j)}f_j - \frac{x^\delta}{LT(f_k)}f_k = \frac{x^\delta}{d_jx^\delta}f_j - \frac{x^\delta}{d_kx^\delta}f_k = p_j - p_k, \tag{2.9}$$

Usando essa equação e que $\sum_{i=1}^{s} c_id_i = 0$, a soma telescópica acima se torna

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

que é uma soma na forma desejada. Como $p_j$ e $p_k$ têm multigrau $\delta$ e coeficiente líder 1, a diferença

$p_j - p_k$ tem multigrau menor que $\delta$. Pela equação (2.9), isso também vale para $S(f_j, f_k)$ e o Lema está provado. ■

Usando S-polinômios e o lema anterior, podemos agora provar o Critério de Buchberger para deduzir quando uma base de um ideal é uma Base de Gröbner.

**Teorema 2.37 (Critério de Buchberger)** *Seja $I$ um ideal polinomial. Então uma base $G = \{g_1, \ldots, g_t\}$ para $I$ é uma Base de Gröbner para $I$ se, e somente se, para todos os pares $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por $G$ (listado em qualquer ordem) é zero.*

**Demonstração:** ($\Rightarrow$) Se $G$ é uma Base de Gröbner então, como $S(g_i, g_j) \in I$, o resto da divisão de $S(g_i, g_j)$ por $G$ é zero pelo Corolário 2.33.

($\Leftarrow$) Seja $f \in I$ um polinômio não nulo. Devemos mostrar que se todos os S-polinômios têm resto zero na divisão por $G$ então $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$. Dado $f \in I = \langle g_1, \ldots, g_t\rangle$, existem polinômios $h_i \in \mathbb{K}[x_1, \ldots, x_n]$ tais que

$$f = \sum_{i=1}^{t} h_i g_i. \tag{2.10}$$

Das propriedades do multigrau, segue que

$$multigrau(f) \leq max(multigrau(h_i g_i)). \tag{2.11}$$

Se a igualdade não ocorre então algum cancelamento de termos líderes de (2.10) deve ocorrer. Dada uma expressão (2.10) para $f$, seja $m(i) = multigrau(h_i g_i)$ e defina $\delta = max(m(1), \ldots, m(t))$. Assim, a inequação (2.11) se torna

$$multigrau(f) \leq \delta.$$

Agora, considere todas as formas possíveis nas quais $f$ pode ser escrito na forma (2.10). Para cada expressão, obtemos um multigrau $\delta$. Como uma ordem monomial é uma boa ordem, podemos selecionar uma expressão na forma (2.10) tal que $\delta$ é mínimo. Mostremos que, uma vez que esse $\delta$ é escolhido, temos $multigrau(f) = \delta$. Então a igualdade ocorre em (2.11), assim $multigrau(f) = multigrau(h_i g_i)$ para algum $i$ e seguirá que o termo líder de $f$ é divisível pelo termo líder de $g_i$. Isso mostrará que $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$, que é o que queremos provar. Resta mostrar que $multigrau(f) = \delta$. Suponha por absurdo que $multigrau(f) < \delta$. Para isolar os termos que têm multigrau $\delta$, vamos escrever $f$ da seguinte forma:

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \tag{2.12}$$

Todos os monômios que aparecem no segundo e terceiro somatórios têm multigrau menor que $\delta$. Então, como assumimos que $multigrau(f) < \delta$, temos que o primeiro somatório também deve ter multigrau menor que $\delta$.

Seja $LT(h_i) = c_i x^{\alpha(i)}$. Então, o primeiro somatório $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ tem exatamente a forma descrita no Lema anterior com $f_i = x^{\alpha(i)} g_i$. Assim, ainda por esse mesmo Lema, esse somatório é uma combinação $\mathbb{K}$-linear de S-polinômios $S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)$. Contudo,

$$S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k) = \frac{x^\delta}{x^{\alpha(j)}LT(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(k)}LT(g_k)} x^{\alpha(k)} g_k = x^{\delta - \gamma_{jk}} S(g_j, g_k), \tag{2.13}$$

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

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

O próximo passo é usar nossa hipótese de que o resto de $S(g_j, g_k)$ na divisão por $g_1, \ldots, g_t$ é zero. Usando o algoritmo da divisão (Teorema 2.11), temos que cada S-polinômio pode ser escrito na forma

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{2.14}$$

onde $a_{ijk} \in \mathbb{K}[x_1, \ldots, x_n]$. O algoritmo da divisão também nos diz que

$$multigrau(a_{ijk}g_i) \leq multigrau(S(g_j, g_k)) \tag{2.15}$$

para todos $i, j, k$. Intuitivamente, isso nos diz que quando o resto é zero, nós podemos encontrar uma expressão para $S(g_j, g_k)$ em termos de $G$, onde nem todos os termos líderes se cancelam.

Para explorar isso, multiplicando a expressão de $S(g_j, g_k)$ por $x^{\delta - \gamma_{jk}}$ obtemos

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

onde $b_{ijk} x^{\delta - \gamma_{jk}} a_{ijk}$. Assim, a equação (2.15) junta com o último Lema nos diz que

$$multigrau(b_{ijk}g_i) \leq multigrau(x^{\delta - \gamma_{jk}} S(g_j, g_k)) < \delta. \tag{2.16}$$

Se analisamos a expressão acima para $x^{\delta - \gamma_{jk}} S(g_j, g_k)$ e substituímos ela em (2.13), obtemos a equação

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

a qual, por (2.16), tem a propriedade de que para todo $i$

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

Por fim, substituindo $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_i \tilde{h}_i g_i$ na equação (2.12), obtemos uma expressão para $f$, a qual é uma combinação polinomial dos $g_i s$ tal que todos os termos têm multigrau menor que $\delta$, o que contradiz a minimalidade de $\delta$ e completa a prova do Teorema. ■

O Critério de Buchberger dado nesse último teorema é um dos resultados chave sobre Bases de Gröbner. Vimos que Bases de Gröbner têm muitas propriedades interessantes, mas, até agora, tem sido difícil determinar se uma base de um ideal é uma Base de Gröbner. Usando o Critério do Buchberger, no entanto, agora é fácil mostrar se uma determinada base é uma Base de Gröbner. Como exemplo, considere o ideal $I = \langle y - x^2, z - x^3 \rangle$ (cúbica torcida em $\mathbb{R}^3$). Provemos que $G = \{y - x^2, z - x^3\}$ é uma Base de Gröbner para a ordem lexicográfica com $y > z > x$. Para isso, considere o S-polinômio

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Usando o algoritmo da divisão, obtemos

$$-zx^2 + yx^3 = x^3(y - x^2) + (-x^2)(z - x^3) + 0.$$

Assim, $\overline{S(y - x^2, z - x^3)}^G = 0$. E, pelo último Teorema, $G$ é uma Base de Gröbner para $I$.

## 2.6 O Algoritmo de Buchberger

No Corolário 2.25 vimos que qualquer ideal em $\mathbb{K}[x_1, \ldots, x_n]$ não nulo tem uma Base de Gröbner. Contudo, a demonstração desse resultado não nos dá uma forma de produzir tal Base. Assim sendo, dado um ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, como podemos construir uma Base de Gröbner para $I$?

**Teorema 2.38 (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 seguindo o seguinte algoritmo em um número finito de passos:*

***Entrada:*** *$F = (f_1, \ldots, f_s)$.*

***Saída:*** *Uma Base de Gröbner $G = (g_1, \ldots, g_t)$ para $I$, com $F \subset G$.*

*1. $G := F$*

*2. REPITA*

*3.* $G' := G$

*4.* *PARA cada par* $\{p,q\}$, $p \neq q$ *em* $G'$ *FAÇA*

*5.* $S := \overline{S(p,q)}^{G'}$

*6.* *SE* $S \neq 0$ *ENTÃO* $G := G \cup \{S\}$

*7. ATÉ QUE* $G = G'$

**Demonstração:** Começaremos com uma notação diferente. Se $G = \{g_1, \ldots, g_t\}$, então $\langle LT(G)\rangle$ representará o ideal $\langle LT(g_1), \ldots, LT(g_t)\rangle$.

Inicialmente, mostraremos que $G \subset I$ em todas as etapas do algoritmo. Previamente, isso já acontece, e sempre que ampliamos $G$ adicionando o resto $S = \overline{S(p,q)}^{G'}$ para $p,q \in G$. Logo, se $G \subset I$, então $S(p,q)$ está em $I$ pois $p,q \in G$, e como estamos dividindo por $G' \subset I$, temos que $G \cup \{S\} \subset I$. Note também que $G$ contém a base $F$ de $I$ dada, de modo que $G$ é na verdade uma base de $I$.

O algoritmo termina com $G = G'$, o que significa que $S = \overline{S(p,q)}^{G'} = 0$ para todos $p,q \in G$. Nesse caso, $G$ é uma Base de Gröbner pelo Critério de Buchberger.

Resta mostrar que o algoritmo termina. Precisamos então considerar o que acontece após cada passo do loop principal. O conjunto $G$ consiste de $G'$ (o antigo $G$) junto com os restos não nulos dos S-polinômios dos elementos de $G'$. Então

$$\langle LT(G')\rangle \subset \langle LT(G)\rangle \tag{2.17}$$

já que $G' \subset G$. Além disso, se $G' \neq G$, afirmamos que $\langle LT(G')\rangle$ está estritamente contido em $\langle LT(G)\rangle$. Para ver o porquê, suponha que um resto não nulo $r$ de um S-polinômio foi adicionado a $G$. Como $r$ é o resto da divisão por $G'$, $LT(r)$ não é divisível pelos termos líderes dos elementos de $G'$, e assim $LT(r) \notin \langle LT(G')\rangle$. Mas $LT(r) \in \langle LT(G)\rangle$, o que prova nossa afirmação.

Por (2.17), os ideais $\langle LT(G')\rangle$ das iterações sucessivas do loop formam um cadeia ascendente de ideais em $\mathbb{K}[x_1, \ldots, x_n]$. Então, a Condição da Cadeia Ascendente nos dá que após um a quantidade finita de iterações a cadeia vai estabilizar. Isto é, $\langle LT(G')\rangle = \langle LT(G)\rangle$ irá acontecer em algum momento. Pelo parágrafo anterior, isso implica que $G' = G$, em outras palavras, o algoritmo deve terminar após um número finito de passos. ■

Juntos, o Critério de Buchberger e o Algoritmo de Buchberger trouxeram um algoritmo básico para a teoria de Bases de Gröbner.

**Exemplo 2.39** *Considere o anel* $\mathbb{C}[x,y]$ *com a ordem graduada lexicográfica e seja* $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. *Relembre que pelo exemplo 2.21* $\{f_1, f_2\}$ *não é uma Base de Gröbner para* $I$ *já que* $LT(S(f_1,f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2)\rangle$.

*Quais novos geradores devemos adicionar para obter uma Base de Gröbner? Considerando* $F = (f_1, f_2)$, *pelo algoritmo de Buchberger temos que* $S(f_1,f_2) = -x^2 \in I$, *e* $\overline{S(f_1,f_2)}^F = -x^2$, *que não é zero. Assim, adicionamos o gerador* $f_3 = -x^2$ *a* $F$ *para ter uma nova possível Base de Gröbner, a qual é verificada se é Base de Gröbner ou não pelo Critério de Buchberger, nos levando a calcular* $\overline{S(f_1,f_2)}^F$, $\overline{S(f_1,f_3)}^F$ *e* $\overline{S(f_2,f_3)}^F$. *Se todos derem 0, temos uma Base de Gröbner, caso contrário, paramos no primeiro* $\overline{S(f_i,f_j)}^F \neq 0$, $1 \leq i,j \leq 3, i \neq j$ *e o adicionamos a* $F$. *Esse processo segue até que as hipóteses do Critério de Buchberger sejam satisfeitas e obtenhamos uma Base de Gröbner. Assim, temos que*

$$\begin{aligned} S(f_1,f_2) &= f_3, \quad \textit{então} \\ \overline{S(f_1,f_2)}^F &= 0, \\ S(f_1,f_3) &= x^3 - 2xy - (-x)(-x^2) = -2xy, \quad \textit{mas} \\ \overline{S(f_1,f_3)}^F &= -2xy \neq 0 \end{aligned}$$

*Logo, temos que adicionar* $f_4 = -2xy$ *ao nosso conjunto gerador. Sendo* $F = (f_1, f_2, f_3, f_4)$, *temos que*

$$\begin{aligned} \overline{S(f_1,f_2)}^F &= \overline{S(f_1,f_3)}^F = 0, \\ S(f_1,f_4) &= y(x^3 - 2xy) - \left(\frac{1}{2}\right)x^2(-2xy) = -2xy^2 = yf_4, \quad \textit{então} \\ \overline{S(f_1,f_4)}^F &= 0, \\ S(f_2,f_3) &= (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \quad \textit{mas} \\ \overline{S(f_2,f_3)}^F &= -2y^2 + x \neq 0. \end{aligned}$$

*Assim, devemos adicionar também* $f_5 = -2y^2 + x$ *ao nosso conjunto gerador. Considerando* $F = (f_1, f_2, f_3, f_4, f_5)$, *obtemos pelo Algoritmo da divisão (Teorema 2.11) que*

$$\overline{S(f_i,f_j)}^F = 0, \quad \textit{para todo } 1 \leq i \leq j \leq 5.$$

*Pelo Critério de Buchberger, segue que uma Base de Gröbner para* $I$, *pela ordem graduada lexicográfica, é dada por*

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

Como vemos no algoritmo acima, conseguimos obter uma Base de Gröbner para um ideal dado. Mas nesse exemplo também vimos que uma Base de Gröbner pode ser muito grande. Os seguintes resultados nos permitem reduzí-las.

**Lema 2.40** *Seja $G$ uma de Gröbner para o ideal polinomial $I$. Seja $p \in G$ um polinômio tal que $LT(p) \in \langle LT(G - \{p\})\rangle$. Então $G - \{p\}$ também é uma Base de Gröbner para $I$.*

**Demonstração:** Sabemos que $\langle LT(G)\rangle = \langle LT(I)\rangle$. Se $LT(p) \in \langle LT(G - \{p\})\rangle$, então temos $\langle LT(G - \{p\})\rangle = \langle LT(G)\rangle$. Por definição, segue que $G - \{p\}$ também é uma Base de Gröbner para $I$. ■

Ajustando os coeficientes para fazer todos os coeficientes líderes iguais a 1 e removendo qualquer polinômio $p$ com $LT(p) \in \langle LT(G - \{p\})\rangle$ de $G$, obtemos o que chamaremos de Base de Gröbner *minimal*.

**Definição 2.41** *Uma **Base de Gröbner minimal** para um ideal polinomial $I$ é uma Base de Gröbner $G$ para $I$ tal que*

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

Podemos construir uma Base de Gröbner minimal para um dado ideal diferente de zero aplicando o algoritmo de Buchberger e depois usando o Lema 2.40 para eliminar quaisquer geradores desnecessários que possam ter sido incluídos.

**Exemplo 2.42** *Ainda no ideal $I$ do exemplo 2.39, usando a ordem graduada lexicográfica, obtemos a Base de Gröbner $G = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\} = \{f_1, \ldots, f_5\}$. Como alguns dos coeficientes principais são diferentes de 1, o primeiro passo é multiplicar os geradores por constantes adequadas para tornar isso verdade. Então observe que $LT(f_1) = x^3 = -x \cdot LT(f_3)$. Pelo Lema 2.40, podemos dispensar $f_1$ da Base de Gröbner minimal. Analogamente, como $LT(f_2) = x^2y = -\frac{1}{2}x \cdot LT(f_4)$, podemos também eliminar $f_2$. Assim sendo, como não há casos em que o termo líder de um gerador divide o termo líder de outro gerador, temos que $\tilde{G} = \{x^2, xy, y^2 - \frac{1}{2}x\} = \{\tilde{f_3}, \tilde{f_4}, \tilde{f_5}\}$ é uma Base de Gröbner minimal para $I$.*

Infelizmente, um determinado ideal pode ter muitas bases minimais de Gröbner. Por exemplo, no ideal $I$ considerado acima, é fácil verificar que $\tilde{G}_a = \{x^2 + axy, xy, y^2 - \frac{1}{2}x\}$ é também uma Base de

Gröbner minimal, onde $a \in \mathbb{K}$ é uma constante. Então, podemos produzir infinitas Bases de Gröbner minimais (supondo que $\mathbb{K}$ é infinito). Mas ainda existe uma base minimal que é melhor que as outras. Sua definição é a seguinte.

**Definição 2.43** *Uma **Base de Gröbner reduzida** para um ideal polinomial $I$ é uma Base de Gröbner para $I$ tal que*

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

Observe que, no parágrafo que antecede à Definição 2.43, apenas a Base de Gröbner na qual $a = 0$ é a única Base de Gröbner reduzida para $I$. Em geral, Bases de Gröbner reduzidas têm a seguinte propriedade interessante.

**Proposição 2.44** *Seja $I \neq \{0\}$ um ideal polinomial. Então, para uma ordem monomial dada, $I$ tem uma única Base de Gröbner reduzida.*

**Demonstração:** Seja $G$ uma Base de Gröbner minimal para $I$. Dizemos que $g \in G$ é reduzido para $G$ desde que nenhum monômio de $g$ esteja em $\langle LT(G - \{g\})\rangle$. Nosso objetivo é modificar $G$ até que todos os seus elementos estejam reduzidos.

Uma primeira observação é que se $g$ é reduzido para $G$, então $g$ também é reduzido para qualquer outra Base de Gröbner minimal de $I$ que contenha $g$ e tenha o mesmo conjunto de termos líderes. Isto ocorre porque a definição de reduzido envolve apenas os termos líderes.

Em seguida, dado $g \in G$, seja $g' = \overline{g}^{G-\{g\}}$ e defina $G' = (G - \{g\}) \cup \{g'\}$. Afirmamos que $G'$ é uma Base de Gröbner minimal para $I$. De fato, primeiramente note que $LT(g') = LT(g)$, pois quando dividimos $g$ por $G - \{g\}$, $LT(g)$ vai para o resto, pois não é divisível por nenhum elemento de $LT(G - \{g\})$. Isso mostra que $\langle LT(G')\rangle = \langle LT(G)\rangle$. Como $G'$ está claramente contida em $I$, temos que $G'$ é uma Base de Gröbner, e a minimalidade segue. Finalmente, note que $g'$ é reduzido por $G'$ por construção.

Agora, pegue os elementos de $G$ e aplique o processo acima até que cada um esteja reduzido. A Base de Gröbner pode mudar cada vez que realizamos o processo, mas a nossa observação anterior mostra que, uma vez reduzido um elemento, ele permanece reduzido, porque nunca alteramos os termos líderes. Assim, acabamos com uma Base de Gröbner reduzida.

Finalmente, para provar a unicidade, suponha que $G = \{g_1, \ldots, g_s\}$ e $\tilde{G} = \{\tilde{g}_1, \ldots, \tilde{g}_t\}$ são Bases de Gröbner reduzidas para $I$. Em particular, $G$ e $\tilde{G}$ são Bases de Gröbner minimais. Afirmamos que $G$ e $\tilde{G}$ têm os mesmos termos líderes. De fato, por construção, temos que cada $LT(g_i), 1 \leq i \leq s$ divide algum $LT(\tilde{g}_j), 1 \leq j \leq t$. Como $G$ e $\tilde{G}$ são minimais, segue que $j$ é único e para $i_1 \neq i_2$, tem-se que $LT(\tilde{g}_{j_1}) \neq LT(\tilde{g}_{j_2})$, logo $s \leq t$. De forma análoga, temos que $t \leq s$ e assim $s = t$ e, por construção, temos que $LT(g_i) = LT(\tilde{g}_j)$ e assim os termos líderes de $G$ e $\tilde{G}$ são os mesmos, e nossa afirmação está provada. Se mostrarmos que $g_i = \tilde{g}_j$, seguirá que $G = \tilde{G}$ e a unicidade estará provada também.

Considere o polinômio $g_i - \tilde{g}_j \in I$. Como $G$ é uma Base de Gröbner, segue que $\overline{g_i - \tilde{g}_j}^{G} = 0$. Mas sabemos que $LT(g_i) = LT(\tilde{g}_j)$. Então esses termos líderem se cancelam em $g_i - \tilde{g}_j$, e nenhum dos termos restantes são divisíveis por nenhum dos termos líderes de $G$ e $\tilde{G}$ já que $G$ e $\tilde{G}$ são reduzidas. Logo só é possível que $\overline{g_i - \tilde{g}_j}^{G} = g_i - \tilde{g}_j$, e então $g_i = \tilde{g}_j$. ■

Uma vantagem da unicidade da Proposição 2.44 é que temos um *algoritmo para igualdade de ideais* para ver quando dois conjuntos de polinômios $\{f_1, \ldots, f_s\}$ e $\{g_1, \ldots, g_t\}$ geram o mesmo ideal: Fixe uma ordem monomial e calcule a Base de Gröbner reduzida de $\langle f_1, \ldots, f_s \rangle$ e $\langle g_1, \ldots g_t \rangle$. Então os ideais são iguais se, e somente se, essas Bases calculadas forem as mesmas.

# CAPÍTULO 3

# Uma Conexão entre Álgebra e Geometria

A correspondência entre ideais e variedades é um dos princípios fundamentais a ser mostrado nesse capítulo. Ela estabelece uma conexão profunda entre os conjuntos algébricos (ideais) e geométricos (variedades).

Além desse resultado fascinante, serão apresentados aqui os ideais radicais e um algoritmo específico para determinar se um polinômio pertence a um ideal radical dado.

## 3.1 Os Teoremas da Extensão e Eliminação

Antes de prosseguir para a próxima seção, precisaremos de alguns resultados que trabalham com a eliminação de variáveis de um sistema de equações polinomiais.

**Definição 3.1** *Dado* $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$*, o* $l$*-ésimo* ***ideal de eliminação*** $I_l$ *é o ideal de* $\mathbb{K}[x_{l+1}, \ldots, x_n]$ *definido por*

$$I_l = I \cap \mathbb{K}[x_{l+1}, \ldots, x_n].$$

Observe que $I_l$ é um ideal de $\mathbb{K}[x_{l+1}, \ldots, x_n]$ já que $0 \in I$ e $0 \in \mathbb{K}[x_{l+1}, \ldots, x_n]$, dados $f, g \in I_l$, por definição temos que $f + g \in I$ e $f + g \in \mathbb{K}[x_{l+1}, \ldots, x_n]$; dados $f \in I_l$ e $h \in \mathbb{K}[x_{l+1}, \ldots, x_n]$, temos que $f \in I \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$ e consequentemente $fh \in \mathbb{K}[x_{l+1}, \ldots, x_n]$.

**Teorema 3.2 (Teorema da Eliminação)** *Seja* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *um ideal e seja* $G$ *uma Base de Gröbner de* $I$ *com respeito a ordem lexicográfica* $x_1 > x_2 > \cdots > x_n$*. Então, para cada* $0 \leq l \leq n$*, o conjunto*

$$G_l = G \cap \mathbb{K}[x_{l+1}, \ldots, x_n]$$

*é uma Base de Gröbner para o $l$-ésimo ideal de eliminação $I_l$.*

**Demonstração:** Fixe $l$ entre 0 e $n$. Como $G_l \subset I_l$ por construção, é suficiente mostrar que

$$\langle LT(I_l)\rangle = \langle LT(G_l)\rangle$$

pela definição de Base de Gröbner. Uma inclusão é clara, e para provar a inclusão $\langle LT(I_l)\rangle \subset \langle LT(G_l)\rangle$ é necessário que, dado um $f \in I_l$, o seu termo líder $LT(f)$ é divisível por $LT(g)$ para algum $g \in G_l$. Para provar isso, note que, já que $f \in I$ também, então como $G$ é uma Base de Gröbner para $I$, temos que existe $g \in G$ tal que $LT(g)$ divide $LT(f)$. Como $f \in I_l$, isso nos dá que $LT(g)$ envolve apenas as variáveis $x_{l+1},\ldots,x_n$. E o ponto chave agora é que, como estamos usando a ordem lexicográfica $x_1 > \cdots > x_n$, qualquer monômio envolvendo as variáveis $x_1,\ldots,x_l$ é maior do que qualquer monômio em $\mathbb{K}[x_{l+1},\ldots,x_n]$. Isso mostra que $g \in G_l$ e o Teorema está provado. ■

**Exemplo 3.3** *Seja $I = \langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1\rangle$, utilizando o Algoritmo de Buchberger (Teorema 2.38) uma Base de Gröbner com respeito a ordem lexicográfica é dada por $G = \{x+y+z^2-1, y^2-y-z^2+z, 2yz^2+z^4-z^2, z^6-4z^4+4z^3-z^2\}$. Pelo Teorema da Eliminação, temos que*

$$I_1 = I \cap \mathbb{C}[y,z] = \langle y^2-y-z^2+z, 2yz^2+z^4-z^2, z^6-4z^4+4z^3-z^2\rangle,$$

$$I_2 = I \cap \mathbb{C}[z] = \langle z^6-4z^4+4z^3-z^2\rangle$$

O Teorema da Eliminação mostra que uma Base de Gröbner para ordem lexicográfica elimina não apenas a primeira variável, mas também as duas primeiras variáveis, as três primeiras variáveis, e assim por diante.

Suponha que temos um sistema de equações polinomiais em $n$ variáveis e obtemos uma solução $(a_2,\ldots,a_n)$ eliminando a primeira variável. O Teorema da Extensão enuncia que essa solução pode ser, de fato, extendida para resolver o sistema original, desde que uma das equações tenha, considerado como um polinômio na primeira variável, um coeficiente líder que não desaparece em $(a_2,\ldots,a_n)$.

**Teorema 3.4 (Teorema da Extensão)** *Seja $I = \langle f_1,\ldots,f_s\rangle \subset \mathbb{K}[x_1,\ldots,x_n]$ e seja $I_1$ o primeiro ideal de eliminação de $I$. Para cada $1 \le i \le s$, escreva $f_i$ na forma*

$$f_i = g_i(x_2,\ldots,x_n)x_1^{N_i} + \textit{ termos em que } x_1 \textit{ tem grau } < N_i,$$

*onde* $N_i \geq 0$ *e* $g_i \in \mathbb{K}[x_2,\ldots,x_n]$ *é não nulo. Suponha que exista uma solução parcial* $(a_2,\ldots,a_n) \in \mathcal{V}(I_1)$. *Se* $(a_2,\ldots,a_n) \notin \mathcal{V}(g_1,\ldots,g_s)$, *então existe* $a_1 \in \mathbb{K}$ *tal que* $(a_1,a_2,\ldots,a_n) \in \mathcal{V}(I)$.

**Demonstração:** Ver [4, Theorem 3.5.3]. ■

## 3.2 O Teorema dos Zeros de Hilbert

Anteriormente, no Capítulo 1 vimos que uma variedade $V \subset \mathbb{K}^n$ pode ser estudada ao analisar para o ideal $\mathcal{I}(V) = \{f \in \mathbb{K}[x_1,\ldots,x_n] : f(a_1,\ldots,a_n) = 0,\ \forall\ (a_1,\ldots,a_n) \in V\}$ de todos os polinômios que se anulam em $V$.

Por outro lado, dado um ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$, podemos definir o conjunto $\mathcal{V}(I) = \{x \in \mathbb{K}^n : f(x) = 0, \text{ para todo } f \in I\}$. O Teorema da Base de Hilbert (Teorema 2.23) nos assegura que $\mathcal{V}(I)$ é uma variedade afim, pois de acordo com esse Teorema, existe um conjunto finito de polinômios $f_1,\ldots,f_s \in I$ tais que $I = \langle f_1,\ldots,f_s\rangle$, e a Proposição 2.30 mostra que $\mathcal{V}(I)$ é o conjunto das raízes comuns desses polinômios.

O primeiro ponto a ressaltar é que ideais diferentes podem ter a mesma variedade. Por exemplo, $\langle x\rangle$ e $\langle x^2\rangle$ são ideais diferentes em $\mathbb{R}[x]$ que têm a mesma variedade $\mathcal{V}(x) = \mathcal{V}(x^2) = \{0\}$.

Outro problema sério pode ocorrer quando $\mathbb{K}$ não é algebricamente fechado: Considere os três polinômios $1, 1+x^2, 1+x^2+x^4$ em $\mathbb{R}[x]$. Cada um desses gera um ideal diferente

$$I_1 = \langle 1\rangle = \mathbb{R}[x], \qquad I_2 = \langle 1+x^2\rangle, \qquad I_3 = \langle 1+x^2+x^4\rangle,$$

mas cada polinômio não tem raiz real. Então, as variedades correspondentes são todas vazias:

$$\mathcal{V}(I_1) = \mathcal{V}(I_2) = \mathcal{V}(I_3) = \emptyset.$$

Será que esse problema de ter ideais diferentes representando a variedade vazia desaparece se o corpo $\mathbb{K}$ é algebricamente fechado? Para provar o Teorema Fraco dos Zeros de Hilbert, precisamos do seguinte resultado:

**Corolário 3.5** *Dado* $\mathbb{K}$ *um corpo algebricamente fechado, seja* $I = \langle f_1,\ldots,f_s\rangle \subset \mathbb{K}[x_1,\ldots,x_n]$ *e assuma que para algum* $i$, $f_i$ *é da forma*

$$f_i = cx_1^{N_i} + \textit{ termos em } x_1 \textit{ que tenham grau total menor que } N_i,$$

*onde $c \neq 0$ é um elemento de $\mathbb{K}$ e $N_i > 0$. Se $I_1 = I \cap \mathbb{K}[x_2,\ldots,x_n]$ é o primeiro ideal de eliminação de $I$, e $(a_2,\ldots,a_n) \in \mathcal{V}(I_1)$, então existe $a_1 \in \mathbb{K}$ tal que $(a_1,\ldots,a_n) \in \mathcal{V}(I)$.*

**Demonstração:** A demonstração segue diretamente do Teorema 3.4: Como $c_i \in \mathbb{K}$ é não nulo, isso implica em $\mathcal{V}(c_1,\ldots,c_s) = \emptyset$, e temos que $(a_2,\ldots,a_n) \notin \mathcal{V}(c_1,\ldots,c_s)$ para todas as soluções parciais $(a_2,\ldots,a_n)$. ■

Antes de prosseguir para o próximo resultado, precisaremos trabalhar com o conceito de polinômios homôgeneos. A seguinte definição foi retirada de [3].

**Definição 3.6** *Um polinômio $f \in \mathbb{K}[x_1,\ldots,x_n]$ é dito* ***homogêneo de grau*** *$s$ se*

$$f(\lambda x_1,\ldots,\lambda x_n) = \lambda^s f(x_1,\ldots,x_n)$$

*para todo $\lambda \in \mathbb{K}$. Os polinômios homogêneos de grau $s$ são então da forma*

$$f = \sum_{s_1+\ldots+s_n=s} c_{s_1,\ldots,s_n} x_1^{s_1} \cdots x_n^{s_n}.$$

*Assim, todo polinômio $f \in \mathbb{K}[x_1,\ldots,x_n]$ se escreve como uma soma $f = f_0 + \cdots + f_d$ onde $f_i \in \mathbb{K}[x_1,\ldots,x_n]$ é um polinômio homgêneo de grau $i$. Dizemos que $f_0,\ldots,f_d$ são as componentes homogêneas de $f$.*

**Teorema 3.7 (Teorema Fraco dos Zeros de Hilbert)** *Seja $\mathbb{K}$ um corpo algebricamente fechado e seja $I \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal satisfazendo $\mathcal{V}(I) = \emptyset$. Então, $I = \mathbb{K}[x_1,\ldots,x_n]$.*

**Demonstração:** Para provar que um ideal é igual a $\mathbb{K}[x_1,\ldots,x_n]$, a estratégia principal consiste em mostrar que o polinômio constante 1 está em $I$, pois se $1 \in I$, então $I$ é todo o anel de polinômios.

No caso de uma variável, isto é, quando o anel de polinômios é $\mathbb{K}[x]$, por [5, Teorema 1.3.8] e [5, Teorema 2.2.2] $\mathbb{K}[x]$ é um domínio principal. Então, podemos escrever $I = \langle f \rangle$, para algum polinômio $f \in \mathbb{K}[x]$. Logo, $\mathcal{V}(I)$ é o conjunto das raízes de $f$ em $\mathbb{K}$. Já que $\mathbb{K}$ é algebricamente fechado, cada polinômio não constante em $\mathbb{K}[x]$ tem uma raiz. Isso significa que se $\mathcal{V}(I) = \emptyset$, então $f$ é uma constante não nula. Nesse caso, $\frac{1}{f} \in \mathbb{K}$ e, portanto, $g = (\frac{1}{f})g \cdot f \in I$, para todo $g \in \mathbb{K}[x]$. Isso mostra que $I = \mathbb{K}[x]$.

Agora assuma que o resultado foi provado para os anéis de polinômios em $n-1$ variáveis, que escreveremos por $\mathbb{K}[x_2,\ldots,x_n]$. Considere qualquer ideal $I = \langle f_1,\ldots,f_s \rangle \subset \mathbb{K}[x_1,\ldots,x_n]$ para o qual $\mathcal{V}(I) = \emptyset$. Podemos assumir que $f_1$ não é constante, pois, caso fosse, não teríamos nada a provar.

Então, suponha que $f_1$ tenha grau total $N \geq 1$. Em seguida, mudaremos as coordenadas para que $f_1$ tenha uma forma especialmente agradável. Ou seja, considere a mudança linear de variáveis

$$\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2\tilde{x}_1 \\ &\vdots \\ x_n &= \tilde{x}_n + a_n\tilde{x}_1, \end{aligned} \tag{3.1}$$

onde os $a_i$ são constantes em $\mathbb{K}$, ainda a serem determinadas. Realizando a substituição (3.1) em $f_1$, obtemos

$$\begin{aligned} f_1(x_1,\ldots,x_n) &= f_1(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\ldots,\tilde{x}_n+a_n\tilde{x}_1) \\ &= c(a_2,\ldots,a_n)\tilde{x}_1^N + \text{ termos em } \tilde{x}_1 \text{ que tenham grau total menor que } N. \end{aligned}$$

Vamos mostrar que $c(a_2,\ldots,a_n)$ é uma expressão não nula em $(a_2,\ldots,a_n)$.

Atenção: Por conveniência, trataremos $f_1 = f$ por enquanto para facilitar alguns cálculos e notações.

Como $f$ tem grau total $N$, escrevamos $f$ como soma de polinômios homogêneos

$$f = f_N + f_{N-1} + \cdots + f_1 + f_0.$$

Defina $g(\tilde{x}_1,\ldots,\tilde{x}_n) = f(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\ldots,\tilde{x}_1+a_n\tilde{x}_1) = \sum_{i=0}^{N} f_i(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\ldots,\tilde{x}_1+a_n\tilde{x}_1)$. Veja que cada $g_i(\tilde{x}_1,\ldots,\tilde{x}_n) = f_i(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\ldots,\tilde{x}_1+a_n\tilde{x}_1)$ é homogêneo de grau $i$ nas variáveis $\tilde{x}_1,\ldots,\tilde{x}_n$, pois, para $\lambda \in \mathbb{K}$:

$$g_i(\lambda\tilde{x}_1,\ldots,\lambda\tilde{x}_n) = f_i(\lambda\tilde{x}_1,\lambda\tilde{x}_2+\lambda a_2\tilde{x}_1,\ldots,\lambda\tilde{x}_1+\lambda a_n\tilde{x}_1) = f_i(\lambda\tilde{x}_1,\lambda(\tilde{x}_2+a_2\tilde{x}_1),\ldots,\lambda(\tilde{x}_1+a_n\tilde{x}_1))$$

$$= \lambda^i f_i(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\ldots,\tilde{x}_1+a_n\tilde{x}_1) = \lambda^i g(\tilde{x}_1,\ldots,\tilde{x}_n).$$

Escrevendo $g_i$ como polinômio em $\tilde{x}_1$

$$g_i(\tilde{x}_1,\ldots,\tilde{x}_n) = h_i^{(i)}\tilde{x}_1^i + h_{i-1}^{(i)}\tilde{x}_1^{i-1} + \cdots + h_0^{(i)},$$

temos então que

$$g_N(\tilde{x}_1,\ldots,\tilde{x}_n) = h_N^{(N)}\tilde{x}_1^N + h_{N-1}^{(N)}\tilde{x}_1^{N-1} + \cdots + h_0^{(N)},$$

$$g_{N-1}(\tilde{x}_1,\ldots,\tilde{x}_n) = h_{N-1}^{(N-1)}\tilde{x}_1^i + h_{N-2}^{(N-1)}\tilde{x}_1^{N-2} + \cdots + h_0^{(N-1)},$$

e assim sucessivamente até

$$g_0(\tilde{x}_1,\ldots,\tilde{x}_n) = h_0^{(0)} = f_0 \in \mathbb{K}.$$

Assim, podemos reescrever $g$ da seguinte forma

$$h_N^{(N)}\tilde{x}_1^N + (h_{N-1}^{(N)} + h_{N-1}^{(N-1)})\tilde{x}_1^{N-1} + \cdots + (h_0^{(N)} + h_0^{(N-1)} + h_0^{(0)}).$$

Em particular, $g_i$, além de ser homogêneo em $\tilde{x}_1,\ldots,\tilde{x}_n$, possui grau total $i$. Como $g_i = h_i^{(i)}\tilde{x}_1^i + h_{i-1}^{(i)}\tilde{x}_1^{i-1} + \cdots + h_j^{(i)}\tilde{x}_1^j + \cdots + h_0^{(i)}$, temos que cada $h_j^{(i)}$ é homogêneo em $\tilde{x}_2,\ldots,\tilde{x}_n$ de grau total $i-j$. Em particular $h_N^{(N)} = h_N^{(N)}(a_2,a_3,\ldots,a_n)$.

Relembre que $g_N(\tilde{x}_1,\ldots,\tilde{x}_n) = h_N^{(N)}\tilde{x}_1^N + h_{N-1}^{(N)}\tilde{x}_1^{N-1} + \cdots + h_0^{(N)}$ e considere $\tilde{x}_1 = 1, \tilde{x}_2 = 0,\ldots,\tilde{x}_n$.

Como $h_{N-i}^{(N)}$ é homogêneo de grau $i$, então

$$h_{N-i}^{(N)}(\tilde{x}_2 = 0,\ldots,\tilde{x}_n = 0) = 0 \text{ para } i \geq 1.$$

Logo

$$g_N(1,0,\ldots,0) = h_N^{(N)} = f_N(1,a_2,\ldots,a_n) = 0.$$

Sabemos que $f_N$ é homogêneo de grau $N$, $f_N \neq 0$, então podemos escrever $f_N$ da seguinte forma

$$f_N = t_N(x_2,\ldots,x_n)\cdot x_1^N + \ldots + t_0(x_2,\ldots,x_n),$$

onde pelo menos um $t_i \neq 0$ $f_N \neq 0$.

Seja $j = max\{i,\ t_i \neq 0\}$, daí $f_N = t_j(x_2,\ldots,x_n) + t_{j-1}(x_2,\ldots,x_n) + \cdots t_0(x_2,\cdots x_n) \neq 0$ por construção. Então, podemos escolher $a_2,\ldots,a_n$ tais que

$$0 \neq f_N(1,a_2,\ldots,a_n) \in \mathbb{K}[a_2,\ldots,a_n] \Rightarrow f_N(1,\ldots,a_n) = c(a_2,\ldots,a_n) \neq 0.$$

De [4, Proposition 1.1.5], podemos escolher $a_2,\ldots,a_n \in \mathbb{K}$ tais que $c(a_2,\ldots,a_n) \neq 0$. Com essa escolha de $a_2,\ldots,a_n$, sob a mudança de variáveis (3.1), todo polinômio $f \in \mathbb{K}[x_1,\ldots,x_n]$ pode ser reescrito como um polinômio $\tilde{f} \in \mathbb{K}[\tilde{x}_1,\ldots,\tilde{x}_n]$. É possível mostrar que

$\tilde{I} = \{\tilde{f} : f \in I\}$ é um ideal em $\mathbb{K}[\tilde{x}_1, \ldots, \tilde{x}_n]$.

Note ainda que $\mathcal{V}(\tilde{I}) = \emptyset$ pois, se as equações transformadas tivessem solução(ões), as originais também teriam. Além disso, se pudermos mostrar que $1 \in \tilde{I}$, então $1 \in I$ seguirá, já que as constantes não são alteradas pela operação $\tilde{}$.

Logo, é suficiente provar que $1 \in \tilde{I}$. Pelo parágrafo anterior, $f_1 \in I$ se torna $\tilde{f}_1 \in \tilde{I}$ com a propriedade

$$\tilde{f}_1(\tilde{x}_1, \ldots, \tilde{x}_n) = c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{ termos em } \tilde{x}_1 \text{ com grau total menor que } N,$$

onde $c(a_2, \ldots, a_n) \neq 0$. Seja agora

$$\pi_1 : \mathbb{K}^n \to \mathbb{K}^{n-1}$$

o mapeamento de projeção nas últimas $n-1$ coordenadas. Se definimos $\tilde{I}_1 = \tilde{I} \cap \mathbb{K}[\tilde{x}_2, \ldots, \tilde{x}_n]$, então, pelo Lema 3.5, temos que soluções parciais em $\mathbb{K}^{n-1}$ sempre se estendem, isto é, $\mathcal{V}(\tilde{I}_1) = \pi_1(\mathcal{V}(\tilde{I}))$. Isso implica que $\mathcal{V}(\tilde{I}_1) = \pi_1(\mathcal{V}(\tilde{I})) = \pi_1(\emptyset) = \emptyset$. Pela hipótese de indução, segue que $\tilde{I}_1 = \mathbb{K}[\tilde{x}_2, \ldots, \tilde{x}_n]$. Mas isso implica que $1 \in \tilde{I}_1 \subset \tilde{I}$, e a prova está completa. ■

Relembremos da última pergunta feita na seção 1.2: Agora, será que é possível determinar se $\mathcal{V}(f_1, \ldots, f_s) = \emptyset$, isto é, se as equações $f_1 = \cdots = f_s = 0$ têm uma solução em comum?

Observe que o Teorema Fraco dos Zeros de Hilbert nos ajuda a resolver o problema: Os polinômios falham em ter uma solução em comum se, e só se $\mathcal{V}(f_1, \ldots, f_s) = \emptyset$. Pelo Teorema Fraco dos Zeros de Hilbert, essa última sentença vale se e só se $1 \in \langle f_1, \ldots, f_s \rangle$. Assim, para resolver esse problema, precisamos estar aptos a determinar se 1 pertence a um ideal. Isso é facilitado pela observação de que, para qualquer ordenação monomial, $\{1\}$ é a única Base de Gröbner reduzida para o ideal $\langle 1 \rangle$.

Para ver isso, seja $\{g_1, \ldots, g_t\}$ uma Base de Gröbner do ideal $I = \langle 1 \rangle$. Então, $1 \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Pelo Lema 2.15 temos que, sem perda de generalidade, $LT(g_1)$ é constante. Assim, como qualquer outro $LT(g_i)$ é múltiplo dessa constante, então $g_2, \ldots, g_t$ podem ser removidos da Base de Gröbner pelo Lema 2.40. Como $LT(g_1)$ é constante, $g_1$ também será já que qualquer monômio não constante tem multigrau maior que o polinômio constante 1 pelo Lema 2.19. Portanto, podemos multiplicar $g_1$ por $\frac{1}{g_1}$ (relembre que $g_1 \neq 0$ já que $LT(g_1)$ divide 1) e obter que $\{1\}$ é a Base de Gröbner reduzida para $I$.

Resumindo, temos o seguinte **algoritmo de consistência**: Se tivermos polinômios $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, nós computamos uma Base de Gröbner reduzida do ideal que eles geram com respeito a qualquer ordenação. Se essa Base for $\{1\}$, os polinômios não têm raiz comum em $\mathbb{K}^n$; se a base não é $\{1\}$, eles devem ter um zero em comum. Note que esse algoritmo funciona apenas em corpos

algebricamente fechados.

Se $\mathbb{K}$ não é um corpo algebricamente fechado, então o algoritmo de consistência funciona em um sentido: Se $\{1\}$ é uma Base de Gröbner reduzida de $\langle f_1,\ldots,f_s\rangle$, então as equações $f_1 = \cdots = f_s = 0$ não têm solução comum. Contudo, a volta não é válida pelos exemplos anteriores ao Teorema Fraco dos Zeros de Hilbert.

Enunciemos o Teorema dos Zeros de Hilbert:

**Teorema 3.8 (Teorema dos Zeros de Hilbert)** *Seja $\mathbb{K}$ um corpo algebricamente fechado. Se $f, f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots x_n]$ são tais que $f \in \mathcal{I}(\mathcal{V}(f_1,\ldots,f_s))$, então existe um inteiro $m \geq 1$ tal que $f^m \in \langle f_1,\ldots,f_s\rangle$ e vice-versa.*

**Demonstração:** Dado um polinômio $f$ não nulo que se anula em todo zero comum dos polinômios $f_1,\ldots,f_s$, temos que mostrar que existe um inteiro $m \geq 1$ e polinômios $A_1,\ldots,A_s$ tais que

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

Considere o ideal $\tilde{I} = \langle f_1,\ldots,f_s, 1-yf\rangle \subset \mathbb{K}[x_1,\ldots,x_n,y]$, onde $f, f_1,\ldots,f_s$ são como acima. Afirmamos que $\mathcal{V}(\tilde{I}) = \emptyset$. Para ver isso, observe que para $(a_1,\ldots,a_n,a_{n+1}) \in \mathbb{K}^{n+1}$ tem-se

- $(a_1,\ldots,a_n)$ é uma raiz comum de $f_1,\ldots,f_s$, ou
- $(a_1,\ldots,a_n)$ não é uma raiz comum de $f_1,\ldots,f_s$.

No primeiro caso $f(a_1,\ldots,a_n) = 0$, pois $f$ desaparece em qualquer zero comum de $f_1,\ldots,f_s$. Então, o polinômio $1-yf$ assume o valor $1-a_{n+1}f(a_1,\ldots,a_n) = 1 \neq 0$ no ponto $(a_1,\ldots,a_n,a_{n+1})$. Em particular, $(a_1,\ldots,a_{n+1}) \notin \mathcal{V}(\tilde{I})$. No segundo caso, para algum $i$, $1 \leq i \leq s$, nós temos que ter $f_i(a_1,\ldots,a_n) \neq 0$. Analisando $f_i$ como uma função de $n+1$ variáveis que não depende da última variável, temos que $f_i(a_1,\ldots,a_n,a_{n+1}) \neq 0$. Em particular, concluímos novamente que $(a_1,\ldots,a_n,a_{n+1}) \notin \mathcal{V}(\tilde{I})$. Como $(a_1,\ldots,a_n,a_{n+1}) \in \mathbb{K}^{n+1}$ foi arbitrário, concluímos que $\mathcal{V}(\tilde{I}) = \emptyset$, como afirmado. Agora aplique o Teorema Fraco dos Zeros de Hilbert para concluir que $1 \in \tilde{I}$. Ou seja,

$$1 = \sum_{i=1}^{s} p_i(x_1,\ldots,x_n,y) f_i + q(x_1,\ldots,x_n,y)(1-yf) \tag{3.2}$$

para polinômios $p_i, q \in \mathbb{K}[x_1,\ldots,x_n,y]$. Agora, defina $y = \frac{1}{f(x_1,\ldots,x_n)}$. Então, a relação acima implica que

$$1 = \sum_{i=1}^{s} p_i\left(x_1,\ldots,x_n,\frac{1}{f}\right) f_i. \tag{3.3}$$

Multiplicando os dois lados da igualdade por uma potência $f^m$, onde $m$ é escolhido suficientemente grande para limpar todos os denominadores, obtemos

$$f^m = \sum_{i=1}^{s} A_i f_i \tag{3.4}$$

para polinômios $A_i$ em $\mathbb{K}[x_1,\ldots,x_n]$, como queríamos demonstrar. ■

O Teorema dos Zeros de Hilbert nos afirma que, sobre um corpo $\mathbb{K}$ algebricamente fechado, a única forma de dois ideais diferentes definirem a mesma variedade é que para todo polinômio do conjunto de geradores de um dos ideais, alguma potência desse polinômio pertença ao outro ideal, e vice-versa.

## 3.3 Ideais Radicais e a Correspondência Ideal-Variedade

Para explorar ainda mais a relação entre ideais e variedades, iremos reformular o Teorema dos Zeros de Hilbert em termos de ideais. Podemos caracterizar os tipos de ideais que aparecem como ideais de uma variedade? Isto é, podemos identificar aqueles ideais que consistem em todos os polinômios que se anulam em alguma variedade $V$? A observação principal está contida no seguinte Lema.

**Lema 3.9** *Seja $V$ uma variedade. Se $f^m \in \mathcal{I}(V)$, então $f \in \mathcal{I}(V)$.*

**Demonstração:** Seja $x \in V$. Se $f^m \in \mathcal{I}(V)$, então $(f(x))^m = 0$. Mas isso acontece se e só se $f(x) = 0$. Desde que $x \in V$ foi arbitrário, devemos ter que $f \in \mathcal{I}(V)$. ■

Assim, um ideal consistindo de todos os polinômios que se anulam em uma variedade $V$ tem a propriedade de que se alguma potência de um polinômio pertence ao ideal, então o próprio polinômio deve pertencer ao ideal. Isso nos leva à seguinte definição:

**Definição 3.10** *Um ideal $I$ é dito **radical** se $f^m \in I$ para algum inteiro $m \geq 1$ implica que $f \in I$.*

Podemos reescrever o Lema 3.9 em termos de ideais radicais, obtendo o seguinte Corolário:

**Lema 3.11** *$\mathcal{I}(V)$ é um ideal radical.*

Por outro lado, a contrapositiva do Teorema dos Zeros de Hilbert nos diz que a única maneira pela qual um ideal arbitrário $I$ pode deixar de ser o ideal de todos os polinômios que se anulam em $\mathcal{V}(I)$ é se $I$ conter potências $m-ésimas$ de polinômios $f$ que não estão em $I$ - em outras palavras, se $I$ não é um ideal radical.

**Definição 3.12** *Seja $I \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal. O **radical** de I, denotado por $\sqrt{I}$, é o conjunto*

$$\{f : f^m \in I \text{ para algum inteiro } m \geq 1\}.$$

Note que sempre temos $I \subset \sqrt{I}$ já que $f \in I$ implica que $f^1 \in I$ e, assim, $f \in \sqrt{I}$. Afirmamos que $I$ é um ideal radical se, e somente se, $I = \sqrt{I}$. De fato, se $I$ é um ideal radical, tome $f \in \sqrt{I}$, sabemos que existe um $m \geq 1$ inteiro tal que $f^m \in I$, mas como $I$ é radical, segue que $f \in I$ e assim $\sqrt{I} \subset I$, juntando com a afirmação do início desse parágrafo, obtemos que $I = \sqrt{I}$. Por outro lado, se $I = \sqrt{I}$, seja $f^m \in I$ com $m \geq 1$ inteiro, logo $f \in \sqrt{I} = I$, assim, $I$ é um ideal radical. Nossa afirmação está provada.

Outra afirmação surpreendente é que o radical de um ideal é sempre um ideal.

**Lema 3.13** *Seja $I$ um ideal $\mathbb{K}[x_1,\ldots,x_n]$, então $\sqrt{I}$ é um ideal em $\mathbb{K}[x_1,\ldots,x_n]$ que contém $I$. Mais ainda, $\sqrt{I}$ é um ideal radical.*

**Demonstração:** Já mostramos que $I \subset \sqrt{I}$. Para mostrar que $\sqrt{I}$ é um ideal, sejam $f,g \in \sqrt{I}$, sejam $f,g \in \sqrt{I}$. Então existem $m,l \in \mathbb{Z}$ tais que $f^m, g^l \in I$. Na expansão binomial $(f+g)^{m+l-1}$ cada termo tem um fator $f^i g^j$ com $i+j = m+l-1$. Como $i \geq m$ ou $j \geq l$, então $f^i$ ou $g^j$ está em $I$, donde temos que $f^i g^j \in I$ e cada termo da expansão binomial está em $I$. Assim, $(f+g)^{m+l-1} \in I$ e, portanto, $f+g \in \sqrt{I}$. Finalmente, suponha que $f \in \sqrt{I}$ e $h \in \mathbb{K}[x_1,\ldots,x_n]$. Logo $f^m \in I$ para algum inteiro $m \geq 1$. Desde que $I$ é um ideal, temos que $(h \cdot f)^m = h^m \cdot f^m \in I$. Logo, $h \cdot f \in \sqrt{I}$. Isso mostra que $\sqrt{I}$ é um ideal.

Para provar que $\sqrt{I}$ é um ideal radical, usaremos como apoio a caracterização de ideais radicais presente após a definição de ideal radical. De fato, seja $f \in \sqrt{\sqrt{I}}$, isso implica que existe um inteiro $m \geq 1$ tal que $f^m \in \sqrt{I}$, o que nos dá pela definição de ideal radical que existe um inteiro $n \geq 1$ tal que $(f^m)^n = f^{m \cdot n} \in I$, como $m \cdot n$ segue sendo um número inteiro maior ou igual a 1, segue que $f \in \sqrt{I}$, e assim $\sqrt{\sqrt{I}} = \sqrt{I}$ e, pela caracterização de ideais radicais, está provado que $\sqrt{I}$ é um ideal radical. ■

**Exemplo 3.14** *Seja $J = \langle x^2, y^3 \rangle \subset \mathbb{K}[x,y]$. Nem $x$ e tampouco $y$ estão em $J$ e é claro que $x \in \sqrt{J}$ e*

$y \in \sqrt{J}$. *Note que* $(x \cdot y)^2 = x^2 \cdot y^2 \in J$ *desde que* $x^2 \in J$*; então,* $x \cdot y \in \sqrt{J}$. *Veja também que* $x + y \in \sqrt{J}$*:*

$$(x+y)^4 = x^4 + 4x^3 + 6x^2y^2 + 4xy^3 + y^4 \in J,$$

*pois* $x^4, 4x^3y, 6x^2y^2 \in J$ *(todos são múltiplos de* $x^2$*) e* $4xy^3, y^4 \in J$ *(pois são múltiplos de* $y^3$*). Logo* $x + y \in \sqrt{J}$. *Em contraste* $xy$ *e* $x + y$ *não pertencem a* $J$.

Estamos prontos agora para enunciar a forma ideal do Teorema dos Zeros de Hilbert.

**Teorema 3.15 (Teorema Forte dos Zeros de Hilbert)** *Seja* $\mathbb{K}$ *um corpo algebricamente fechado e seja* $I$ *um ideal de* $\mathbb{K}[x_1, \ldots, x_n]$*, então*

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}.$$

**Demonstração:** Certamente temos que $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$ porque $f \in \sqrt{I}$ implica que $f^m \in I$, para algum $m$. Logo, $f^m$ se anula em $\mathcal{V}(I)$, o que implica que $f$ se anula em $\mathcal{V}(I)$. Logo, $f \in \mathcal{I}(\mathcal{V}(I))$.

Por outro lado, suponha que $f \in \mathcal{I}(\mathcal{V}(I))$. Assim, por definição, $f$ se anula em $\mathcal{V}(I)$. Pelo Teorema dos Zeros de Hilbert, existe um inteiro $m \geq 1$ tal que $f^m \in I$. Mas isso significa que $f \in \sqrt{I}$. Desde que $f$ é arbitrário, $\mathcal{I}(\mathcal{V}(I)) \subset \sqrt{I}$. A prova acaba aqui. ■

A consequência mais importante do Teorema Forte dos Zeros de Hilbert é que ele nos permite estabelecer um "dicionário" entre geometria e álgebra. A base desse dicionário está no seguinte Teorema:

**Teorema 3.16 (A Correspondência Ideal-Variedade)**

- *As funções*

$$\textit{variedades afins} \xrightarrow{\mathcal{I}} \textit{ideais} \qquad e \qquad \textit{ideais} \xrightarrow{\mathcal{V}} \textit{variedades afins}$$

  *são de inclusão-reversa, isto é, se* $I_1 \subset I_2$ *são ideais, então* $\mathcal{V}(I_1) \supset \mathcal{V}(I_2)$ *e, similarmente, se* $V_1 \subset V_2$ *são variedades afins, então* $\mathcal{I}(V_1) \supset \mathcal{I}(V_2)$. *Além disso, para qualquer variedade* $V$*, temos* $\mathcal{V}(\mathcal{I}(V)) = V$.

- *Seja* $\mathbb{K}$ *um corpo algebricamente fechado, então*

$$\textit{variedades afins} \xrightarrow{\mathcal{I}} \textit{ideais radicais} \qquad e \qquad \textit{ideais radicais} \xrightarrow{\mathcal{V}} \textit{variedades afins}$$

  *são bijetoras de inclusão reversa e inversa uma da outra.*

**Demonstração:**

- Vamos mostrar inicialmente que $I$ e $V$ são de inclusão reversa:

  Sejam $I_1$, $I_2$ ideais em $\mathbb{K}[x_1,\ldots,x_n]$ tal que $I_1 \subset I_2$ e considere $x \in \mathcal{V}(I_2)$, temos que $f(x) = 0$ para todos $f \in I_2$, em particular para todos $f \in I_1 \subset I_2$, daí $x \in \mathcal{V}(I_1)$ e assim $\mathcal{V}(I_2) \subset \mathcal{V}(I_1)$.

  Sejam $V_1, V_2$ variedades afins e tome $g \in \mathcal{I}(V_2)$, temos que $g(y) = 0$, para todos $y \in V_2$, em particular para $y \in V_1 \subset V_2$, daí $g \in \mathcal{I}(V_1)$ e assim $\mathcal{I}(V_2) \subset \mathcal{I}(V_1)$.

  Resta provar que $\mathcal{V}(\mathcal{I}(V)) = V$ quando $V = \mathcal{V}(f_1,\ldots,f_s)$ é uma subvariedade de $\mathbb{K}^n$. Como cada $f \in \mathcal{I}(V)$ se anula em $V$, a inclusão $V \subset \mathcal{V}(\mathcal{I}(V))$ segue diretamente da definição de $V$. Indo para o outro lado, note que $f_1,\ldots,f_s \in \mathcal{I}(V)$ pela definição de $I$ e, assim, $\langle f_1,\ldots,f_s\rangle \subset \mathcal{I}(V)$. Desde que $V$ é de inclusão reversa, segue que $\mathcal{V}(\mathcal{I}(V)) \subset \mathcal{V}(\langle f_1,\ldots,f_s\rangle) = V$. Isso prova a igualdade desejada $\mathcal{V}(\mathcal{I}(V)) = V$ e, consequentemente, $\mathcal{I}$ é injetora, pois tem inversa à esquerda.

- Como $\mathcal{I}(V)$ é radical pelo Lema 3.11, podemos pensar em $\mathcal{I}$ como uma função que leva variedades a ideais radicais. Mais ainda, nós sabemos que $\mathcal{V}(\mathcal{I}(V)) = V$ para qualquer variedade $V$. Resta provar que $\mathcal{I}(\mathcal{V}(I)) = I$ onde $I$ é um ideal radical: O Teorema do Zero nos diz que $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, e $I$ sendo radical implica que $I = \sqrt{I}$. Isso dá a igualdade desejada. Assim, $V$ e $I$ são inversas uma da outra e, assim, definem bijeções entre o conjunto de ideais radicais e variedades afins. O Teorema está provado. ■

Agora podemos questionar:

- (*Membro de um ideal radical*) Dado $f \in I$ e $I = \langle f_1,\ldots,f_s\rangle \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal, existe um algoritmo que determina se $f \in \sqrt{I}$?

Para testar se $f \in \sqrt{I}$, podemos usar o algoritmo de pertinência de um ideal para checar quando $f^m \in I$, para algum inteiro $m \geq 1$. Isso não é satisfatório porque poderíamos aplicar o algoritmo com potências muito grandes de $m$ e isso não necessariamente nos dará se $f \notin I$. Felizmente, podemos adaptar a prova do Teorema dos Zeros de Hilbert para fornecer um algoritmo para determinar se $f \in \sqrt{\langle f_1,\ldots,f_s\rangle}$.

**Proposição 3.17** *Seja $\mathbb{K}$ um corpo arbitrário e seja $I = \langle f_1,\ldots,f_s\rangle \subset \mathbb{K}[x_1,\ldots,x_n]$ um ideal. Então $f \in \sqrt{I}$ se e somente se o polinômio constante 1 pertence ao ideal $\overline{I} = \langle f_1,\ldots,f_s, 1-yf\rangle \subset \mathbb{K}[x_1,\ldots,x_n,y]$ (nesse caso, $\overline{I} = \mathbb{K}[x_1,\ldots,x_n,y]$).*

**Demonstração:** Das equações (3.2), (3.3) e (3.4) da demonstração do Teorema dos Zeros de Hilbert, temos que $1 \in \overline{I}$ implica que $f^m \in I$ para algum inteiro positivo $m$, o que implica que $f \in \sqrt{I}$.

Indo para o outro lado, suponha que $f \in \sqrt{I}$. Então $f^m \in I \subset \overline{I}$ para algum $m$. Mas temos também que $1 - yf \in \overline{I}$ e, consequentemente,

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + \cdots + y^{m-1} f^{m-1}) \in \overline{I},$$

como desejado. ■

A Proposição 3.17 juntamente com o que foi construído até aqui para determinar de 1 pertence a um ideal dado nos leva automaticamente ao algoritmo para determinar se um polinomio está no radical desse ideal, conhecido como **algoritmo do membro do ideal radical** [4]. Isto é, para determinar se $f \in \sqrt{\langle f_1, \ldots, f_s \rangle} \subset \mathbb{K}[x_1, \ldots, x_n]$, calculamos a Base de Gröbner reduzida para o ideal $\langle f_1, \ldots, f_s, 1 - yf \rangle \subset \mathbb{K}[x_1, \ldots, x_n, y]$ com respeito a sua ordenação. Se o resultado é $\{1\}$, então $f \in \sqrt{I}$. Caso contrário, $f \notin \sqrt{I}$.

**Exemplo 3.18** *Considere o ideal* $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$ *de* $\mathbb{K}[x, y]$. *Vamos testar se* $-x^2 + y + 1$ *pertence a* $\sqrt{I}$. *Usando a ordem lexicográfica em* $\mathbb{K}[x, y, z]$, *pelo Algoritmo de Buchberger (Teorema 2.38) e a Proposição 2.44 é possível checar que o ideal*

$$\tilde{I} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(-x^2 + y + 1) \rangle \subset \mathbb{K}[x, y, z]$$

*tem Base de Gröbner reduzida* $\{1\}$. *Segue que* $-x^2 + y + 1 \in \sqrt{I}$ *pela Proposição 3.17.*

*Na verdade, usando o algoritmo de divisão (Teorema 2.11), podemos verificar qual potência de* $-x^2 + y + 1$ *está em* $I$*:*

$$\begin{aligned} \overline{-x^2 + y + 1}^G &= -x^2 + y + 1, \\ \overline{(-x^2 + y + 1)^2}^G &= -2x^2 y + 2y, \\ \overline{(-x^2 + y + 1)^3}^G &= 0, \end{aligned}$$

*onde* $G = \{x^4 - 2x^2 + 1, y^2\}$ *é uma Base de Gröbner com respeito à ordem lexicográfica e* $\overline{p}^G$ *é o resto de* $p$ *na divisão* $G$. *Como uma consequência, vimos que* $(-x^2 + y + 1)^3 \in I$, *mas nenhuma potência menor de* $-x^2 + y + 1$ *pertence a* $I$ *(em particular,* $-x^2 + y + 1 \notin I$*).*

# Conclusão

Neste trabalho introduzimos a Teoria de Bases de Gröbner e as relações entre álgebra e geometria por meio dos Teoremas de Hilbert.

As Bases de Gröbner são uma ferramenta poderosa e versátil na teoria dos polinômios e álgebra comutativa, pois elas desempenham um papel fundamental em diversas áreas, desde geometria algébrica até resolução de problemas práticos em ciência da computação como os que modelam fenômenos descritos por polinômios em mais de uma variável. Sua importância reside não apenas na teoria matemática, mas também na aplicabilidade prática, tornando-as uma boa ferramenta para pesquisadores e profissionais.

Por sua vez, os Teoremas dos Zeros de Hilbert emergem como um pilar fundamental na geometria algébrica, proporcionando uma correspondência profunda entre ideais em $\mathbb{K}[x_1, \ldots, x_n]$ e variedades afins. Ao estabelecer que cada ideal está associado a uma variedade e vice-versa, é estabelecido um "dicionário" entre conceitos algébricos e geométricos.

# Referências Bibliográficas


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

[2] CAMPOS, Arthur. ***Bases de Gröbner***. Monografia de Graduação. 2018.

[3] COELHO, JULIANA. ***Introdução à Geometria Algébrica***. 2009.

[4] DAVID COX, John Little e O'SHEA, Donal. ***Ideals, Variethes and Algorthms: An Introduction to Computational Algebraic Geometry and Commutative Algebra***. 4ª ed. Springer, 2013.

[5] GARCIA, Arnaldo e LEQUAIN, Yves. ***Elementos de álgebra***. 1ª ed. Projeto Euclides, 2014.

[6] GRILLET, Pierre Antoine. ***Abstract algebra***. Vol. 242. Springer Science & Business Media, 2007.

[7] LANG, Serge. ***Undergraduate algebra***. Springer Science & Business Media, 2005.