UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

A Variedade das álgebras de Jordan de dimensão 2 e 3 a partir de Bases de Gröbner

FILIPE DO NASCIMENTO FORTES

Manaus - AM
2022

FILIPE DO NASCIMENTO FORTES

A Variedade das álgebras de Jordan de dimensão 2 e 3 a partir de Bases de Gröbner

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Amazonas, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Elkin Oveimar Quintero Vanegas.

Manaus - AM
2022

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Fortes, Filipe do Nascimento
F738v A variedade das álgebras de Jordan de dimensão 2 e 3 a partir de bases de Gröbner / Filipe do Nascimento Fortes . 2022
85 f.: il.; 31 cm.

Orientador: Elkin Oveimar Quintero Vanegas
Dissertação (Mestrado em Matemática) - Universidade Federal do Amazonas.

1. Bases de Gröbner. 2. Geometria algébrica. 3. Variedade afim. 4. Álgebras de Jordan. 5. Dimensão e componentes irredutíveis. I. Vanegas, Elkin Oveimar Quintero. II. Universidade Federal do Amazonas III. Título

Dedicatória

Dedico este trabalho à minha mãe que tem me apoiado e incentivado por toda minha vida, e cujos afáveis aconselhamento e zelo me permitiram concluir mais essa etapa em minha formação acadêmica.

Agradecimentos

Agradeço primeiramente a Deus, sem o qual nada do que foi feito se fez.

Agradeço ao meu orientador prof. Dr. Elkin Oveimar Quintero Vanegas, por ter me aceitado como orientando, cujo direcionamento e compreensão me permitiram avançar cada passo na caminhada de construção deste trabalho.

Agradeço também a todos os professores que participaram de minha formação nas disciplinas, em especial, ao prof. Dr. Sandro Dimy Barbosa Bitar cuja ferramenta de linguagem computacional por ele apresentada foi de imensa utilidade neste trabalho e aos professores doutores Gérman Alonso Benitez Monsalve e Stefan Josef Ehbauer que me receberam com generosa solicitude e incentivo nas linhas de pesquisa em Álgebra.

Aos membros da banca examinadora pelas correções e sugestões.

À CAPES pelo apoio financeiro.

FORTES, F. N. *A Variedade das álgebras de Jordan de dimensão 2 e 3 a partir de Bases de Gröbner.* 2022. 85 p. Dissertação de Mestrado, Universidade Federal do Amazonas, Manaus-AM.

Resumo

Neste trabalho serão apresentadas Bases de Gröbner e seu processo algorítmico de obtenção, bem como resultados de Geometria Algébrica sobre variedades afins. O cálculo de bases de Gröbner permitirá compreender o processo de análise da classificação da variedade afim das álgebras de Jordan de dimensões 2 e 3, as quais não são associativas. Com esse intuito, começamos com o estudo do algoritmo da divisão no anel de polinômios $\kappa[x_1, \ldots, x_n]$ sobre um corpo arbitrário κ e suas principais características, por meio de diferentes ordenações monomiais, detalhando sua implementação algorítmica. Em seguida, são estudados o processo de construção de uma base de Gröbner para um ideal polinomial $I \subset \kappa[x_1, \ldots, x_n]$ que permite responder, dentre outras perguntas, à questão de pertinência de um polinômio a dado ideal, e também alguns exemplos de computação de bases de Gröbner por meio da ferramenta computacional de grande utilidade SageMath. Logo após serão estudados os conceitos de espaço afim $\mathbb{A}^n(\kappa)$, variedade afim $V \subset \mathbb{A}^n(\kappa)$ e suas propriedades, particularmente dimensão e decomposição em componentes irredutíveis. Por fim, como aplicação das bases de Gröbner, apresentaremos a classificação das variedades de $Jor_2(\kappa)$ e $Jor_3(\kappa)$ sobre um corpo algebricamente fechado κ, estudando suas dimensões e componentes irredutíveis.

Palavras-chave: Bases de Gröbner; Geometria Algébrica; Variedade afim; Álgebras de Jordan; Dimensão e componentes irredutíveis.

FORTES, F. N. *The Variety of 2 and 3 dimensional Jordan Algebras and Gröbner bases.* 2022. 85 p. M. Sc. Dissertation, Federal University of Amazonas, Manaus-AM.

Abstract

In this work, we will present Gröbner basis and an algorithm to obtain them, as well as results from Algebraic Geometry on affine algebraic varieties. The calculation of Gröbner bases will allow us to understand the process of analyzing the classification of the affine variety of 2 and 3 dimensional Jordan algebras, which are not associative. For this purpose, we start with the study of the division algorithm in the polynomial ring $\kappa[x_1, \ldots, x_n]$ over an arbitrary field κ and its main characteristics, through different monomial orderings, detailing its algorithmic implementation. Then, the process of building a Gröbner base for a polynomial ideal $I \subset \kappa[x_1, \ldots, x_n]$ is studied, which allows us to answer, among other questions, the problem of ideal membership, and also some examples of computing Gröbner bases using the highly useful computational tool SageMath. Soon after, the concepts of affine space $\mathbb{A}^n(\kappa)$, affine variety $V \subset \mathbb{A}^n(\kappa)$ and their properties will be studied, in particular dimension and decomposition into irreducible components. Finally, as an application of Gröbner bases, we will present the classification of $Jor_2(\kappa)$ and $Jor_3(\kappa)$ over an algebraically closed field κ, studying its dimensions and irreducible components.

keywords: Gröbner bases; Algebraic Geometry; Affine Variety; Jordan algebras; Dimension and irreducible components.

LISTA DE SÍMBOLOS

$\emptyset$	conjunto vazio
$\mathbb{Z}$	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Z}_{\geq 0}^n$	conjunto das $n-$úplas de inteiros não-negativos
$\mathbb{Q}$	corpo dos números racionais
$\mathbb{R}$	corpo dos números reais
$\mathbb{C}$	corpo dos números complexos
A	anel algébrico
κ	corpo algébrico
$\overline{\kappa}$	fecho algébrico do corpo κ
$A[x]$	anel de polinômios com coeficientes no anel A
$\kappa[x_1, \ldots, x_n]$	anel de polinômios em n indeterminadas com coeficientes no corpo κ
$\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$	elementos de $\mathbb{Z}_{\geq 0}^n$
$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$	monômio em $\kappa[x_1, \ldots, x_n]$
$\lvert\alpha\rvert$	grau total de um monômio
$f = \sum_\alpha a_\alpha x^\alpha$	polinômio como combinação linear finita de monômios
f, g, h	polinômios em $\kappa[x_1, \ldots, x_n]$
I, J	ideais em $\kappa[x_1, \ldots, x_n]$
$\sqrt{I}$	radical do ideal I
$\langle f_1, \ldots, f_s \rangle$	ideal determinado pelos polinômios $f_1, \ldots, f_s$
$>_{lex}$	ordem monomial lexicográfica
$>_{grlex}$	ordem monomial lexicográfica graduada
$>_{grevlex}$	ordem monomial lexicográfica graduada reversa

$\mathrm{multideg}(f)$	multigrau do polinômio f
$LC(f)$	coeficiente líder do polinômio f
$LM(f)$	monômio líder do polinômio f
$LT(f)$	termo líder do polinômio f
$LT(I)$	conjunto dos termos líderes dos elementos não-nulos do ideal I
$\langle LT(I)\rangle$	ideal monomial gerado por $LT(I)$
$G = \{g_1, \ldots, g_t\}$	base de Gröbner para um ideal
$\overline{f}^F$	resto na divisão do polinômio f por uma $s-$úpla ordenada $F = (f_1, \ldots, f_s)$
$\mathrm{lcm}(\ )$	mínimo múltiplo comum
$S(f, g)$	$S-$polinômio dos polinômios f e g
$\mathbb{A}^n(\kappa)$	espaço afim $n-$dimensional sobre o corpo κ
$(a_1, \ldots, a_n)$	ponto no espaço afim $\mathbb{A}^n(\kappa)$
V, W, S	variedades afins
$\mathbf{V}(f_1, \ldots, f_s)$	variedade determinada pelos polinômios $f_1, \ldots, f_s$
$\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$	ideal associado à variedade $\mathbf{V}(f_1, \ldots, f_s)$
I_k	$k-$ésimo ideal de eliminação do ideal I
$\pi : \mathbb{A}^n(\kappa) \to \mathbb{A}^m(\kappa)$	aplicação projeção
I/J	ideal quociente
$\kappa[V]$	anel coordenado
$\kappa(V)$	corpo de frações de $\kappa[V]$
$[f]$	classe de equivalência do polinômio f módulo um ideal
$\binom{n}{p}$	coeficiente binomial
$\dim V$	dimensão da variedade V
${}^aHF$	função afim de Hilbert
${}^aHP$	polinômio afim de Hilbert
$Jor_n(\kappa)$	conjunto das álgebras de Jordan de dimensão n sobre um corpo κ

LISTA DE FIGURAS

CONTEÚDO

INTRODUÇÃO

O conceito de bases de Gröbner foi desenvolvido em 1965 por Bruno Buchberger [1] em sua tese de doutorado, o qual as nomeou em homenagem a seu orientador Wolfgang Gröbner. Inicialmente, Buchberger teve como interesse obter elementos bases do anel de classes residuais de um ideal polinomial zero-dimensional em $\kappa[x_1, \ldots, x_n]$, os quais embora já se soubesse que eram finitos ainda não havia um método para calcular e exibir tais geradores.

Com a apresentação e análise detalhada do processo algorítmico de construção de uma base de Gröbner em sua tese abriu-se espaço para diversas aplicações, e em particular a partir dos anos 80, com o advento de novas gerações de computadores baseados em microprocessadores e sistemas operacionais, possibilitou-se melhor e mais ampla implementação e uso em diferentes áreas como em problemas de engenharia, ciência da computação e matemática, relacionados a ideais polinomiais específicos.

Vale mencionar ainda que os conceitos de bases de Gröbner são estendidos inclusive a casos mais gerais, com os devidos ajustes, no estudo de cálculo de geradores para Módulos, do cálculo de homologia de uma resolução, de aplicação no estudo de criptanálise sobre anéis booleanos, e mesmo versões não-comutativas sobre álgebras de Quivers.

O objetivo central dessa dissertação é aplicar as bases de Gröbner para obter a classificação das variedades afins das álgebras não-associativas de Jordan de dimensão 2 e 3 sobre um corpo algebricamente fechado, cuja classificação pode ser encontrada de forma completa em [8]. Com este fim, será necessário estudar vários conceitos de Geometria Algébrica, fortemente apoiada em conhecimentos de Álgebra Comutativa.

A dissertação está estruturada da seguinte maneira: No Capítulo 1 veremos as noções preliminares de anel de polinômios em n indeterminadas sobre um corpo arbitrário κ, bem como definições e tipos distintos de ordens monomiais que serão extremamente importantes para compreender o processo de funcionamento do algoritmo de divisão em $\kappa[x_1, \ldots, x_n]$ e de construção do algoritmo de Buchberger para o cálculo de uma base de Gröbner para um ideal polinomial neste anel. Veremos de forma detalhada como funcionam esses algoritmos por meio de exem-

plos e implementações através do software computacional SageMath. Demonstraremos muitos resultados importantes utilizados nesse capítulo relacionados a ideais monomiais e bases de Gröbner. Ao fim desse capítulo teremos todas as ferramentas necessárias para obter um conjunto de geradores de um ideal polinomial, bem como para responder à questão de pertinência de um polinômio dado a certo ideal. As principais referências usadas na elaboração deste capítulo foram obtidas em [2] e [7].

No Capítulo 2 nos dedicaremos ao estudo de uma introdução à Geometria Algébrica. Ressaltamos que nos utilizaremos de diversos conceitos e resultados conhecidos de Álgebra Comutativa. Iniciaremos a primeira seção deste capítulo com as noções e propriedades de espaço afim e variedade afim, de ideal de uma variedade e sua relação com o ideal radical, bem como os teoremas importantes de Nullstellensatz. Na seguinte seção estudaremos o fecho de Zariski de uma variedade, sua decomposição em variedades irredutíveis e a decomposição primária do ideal polinomial relacionado. Prosseguiremos nas seguintes seções estudando noções importantes de Anel Coordenado, de Finitude e Normalização de Noether, concluindo o capítulo com o estudo da dimensão de uma variedade, suas propriedades e diferentes formas de definição e um processo para obter a dimensão de uma variedade a partir de uma base de Gröbner do ideal polinomial correspondente. Para a elaboração deste capítulo consultamos [2], [4], [5], [6] e [10].

No Capítulo 3 começaremos apresentando o conjunto das álgebras de Jordan de dimensão n sobre um corpo κ. Apresentaremos o processo de cálculo das identidades polinomiais de suas constantes de estrutura que determinam as variedades de $Jor_2(\kappa)$ e $Jor_3(\kappa)$ sobre um corpo algebricamente fechado, explicitaremos cada um desses polinômios calculados. Prosseguindo aplicaremos os conceitos estudados para o cálculo de uma base de Gröbner para o ideal dos polinômios que determinam $Jor_2(\kappa)$, calcularemos a dimensão dessa variedade e explicitaremos as componentes irredutíveis obtidas. Por fim, de modo análogo, comentaremos como é possível aplicar os mesmos passos para a classificação da variedade de $Jor_3(\kappa)$. Esta classificação embasada conforme [8].

CAPÍTULO 1

BASES DE GRÖBNER

Neste capítulo apresentamos as definições iniciais essenciais para a construção de nosso estudo das Bases de Gröbner em Geometria Algébrica. Iniciaremos definindo o anel de polinômios em n indeterminadas sobre um corpo κ, em seguida serão definidos os elementos monomiais desse anel, relações de ordem entre eles, ideais monomiais e alguns resultados sobre os mesmos, de modo a possibilitar a construção dos dois principais algoritmos a serem estudados nesse capítulo, a saber, o Algoritmo da Divisão e o Algoritmo de Buchberger para o cálculo de uma Base de Gröbner para um ideal polinomial.

1.1 Definições preliminares

Iniciemos esta seção definindo o anel com o qual trabalharemos, o anel $\kappa[x_1, \ldots, x_n]$.

Podemos definir o anel de polinômios em duas indeterminadas, denotadas por x e y do seguinte modo: seja $A_1 = \kappa[x]$ e definamos $A_2 = A_1[y]$. Temos que $A_1[y]$ é o anel de polinômios na indeterminada y com coeficientes em $A_1 = \kappa[x]$. Assim, um elemento de A_2 é da forma

$$f = f_0(x) + f_1(x)y + f_2(x)y^2 + \cdots + f_n(x)y^n, \text{ onde } f_i(x) \in A_1 \text{ e}$$

$$f_i(x)y^i = \left(\sum_{j=0}^{m_i} a_{ij}x^j\right) y^i = \sum_{j=0}^{m_i} a_{ij}x^j y^i, \text{ para } m_i \in \mathbb{Z}_{\geq 0} \text{ e } a_{ij} \in \kappa.$$

Desse modo, podemos simplesmente dizer que f é um polinômio nas indeterminadas x e y com coeficientes no corpo κ:

$$A_2 = A_1[y] = \kappa[x][y] = \kappa[x, y].$$

Então, procedendo recursivamente, podemos definir o Anel de Polinômios em n indeterminadas como:

$$A_n = A_{n-1}[x_n] = \kappa[x_1, \ldots, x_{n-1}][x_n] = \kappa[x_1, \ldots, x_n].$$

Observação: sempre que o anel em questão envolver apenas duas ou três indeterminadas, denotaremos, como usualmente, nas indeterminadas x, y e z.

Podemos então definir um monômio no anel $\kappa[x_1, \ldots, x_n]$.

Definição 1.1. Um monômio nas indeterminadas $x_1, x_2, \ldots, x_n$ é um produto da forma:

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

onde todos os expoentes $\alpha_1, \alpha_2, \ldots, \alpha_n$ são inteiros não-negativos. O grau total desse monômio é a soma $\alpha_1 + \alpha_2 + \cdots + \alpha_n$.

De modo a simplificar a notação podemos tomar $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, e escrever $x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. Dessa forma, para $\alpha = (0, 0, \ldots, 0)$ teremos $x^\alpha = 1$ e $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ denotará o grau total desse monômio.

Com a definição de mônomio podemos então definir um polinômio em $\kappa[x_1, \ldots, x_n]$.

Definição 1.2. Um polinômio f nas indeterminadas $x_1, x_2, \ldots, x_n$ com coeficientes em um corpo κ é uma combinação linear finita (com coeficientes em κ) de monômios. Escrevemos o polinômio f na forma:

$$f = \sum_\alpha a_\alpha x^\alpha, \text{com } a_\alpha \in \kappa,$$

com a soma sobre um número finito de $n-$úplas $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.

Como exemplo: $f = 2x^3y^2z + \dfrac{3}{2}y^3z^3 - 3xyz + y^2 \in \mathbb{Q}[x, y, z]$.

Uma vez definido um polinômio podemos, analogamente ao que é feito no anel de polinômios em uma indeterminada, definir a noção de grau de um polinômio em $\kappa[x_1, \ldots, x_n]$.

Definição 1.3. Seja $f = \sum_\alpha a_\alpha x^\alpha$ um polinômio em $\kappa[x_1, x_2, \ldots, x_n]$.

(i) Chamamos a_α de coeficiente do monômio x^α.

(ii) Se $a_\alpha \neq 0$, então chamamos $a_\alpha x^\alpha$ de termo do polinômio f.

(iii) O grau total de $f \neq 0$, denotado como $\deg(f)$, é o máximo $|\alpha|$ cujo coeficiente $a_\alpha \neq 0$.

Como exemplo: $f = 5x^3y^2z + 3y^3z^3 - 3xyz + z^2 \in \mathbb{R}[x, y, z]$, cujo grau total é $\deg(f) = 6$.

Note que, no anel de polinômios $\kappa[x_1, \ldots, x_n]$, podemos ter mais de um termo de um polinômio com o mesmo grau, o que não ocorre no anel $\kappa[x]$.

Concluindo esta seção, definiremos ideais no anel $\kappa[x_1, \ldots, x_n]$, subconjuntos para os quais veremos vários resultados e calcularemos, mais à frente, um conjunto de geradores para os mesmos.

Definição 1.4. Um subconjunto $I \subseteq \kappa[x_1, \ldots, x_n]$ é um ideal do anel $\kappa[x_1, \ldots, x_n]$ se satisfaz:

(i) $0 \in I$;

(ii) Se $f, g \in I$, então $f - g \in I$;

(iii) Se $f \in I$ e $h \in \kappa[x_1, \ldots, x_n]$, então $hf \in I$.

Podemos então estudar um conjunto determinado por um número finito de polinômios e verificar que ele, de fato, é um ideal em $\kappa[x_1, \ldots, x_n]$.

Definição 1.5. Sejam $f_1, \ldots, f_s$ polinômios não-nulos em $\kappa[x_1, \ldots, x_n]$. Definamos o conjunto denotado por $\langle f_1, \ldots, f_s \rangle$, da forma seguinte

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

O seguinte lema mostra que o conjunto definido acima é um ideal:

Lema 1.6. *Sejam $f_1, \ldots, f_s \in \kappa[x_1, \ldots, x_n]$, não-nulos, $\langle f_1, \ldots, f_s \rangle$ é um ideal de $\kappa[x_1, \ldots, x_n]$.*

Demonstração. Veja [2, pág 29].

Chamamos $\langle f_1, \ldots, f_s \rangle$ de ideal gerado por $f_1, \ldots, f_s$.

Questionamentos que podem surgir naturalmente nesse momento são os seguintes: será que todo ideal $I \subseteq \kappa[x_1, \ldots, x_n]$ possui um conjunto finito de geradores? Em outras palavras, podemos escrever $I = \langle f_1, \ldots, f_s \rangle$ para $f_i \in \kappa[x_1, \ldots, x_n]$? E outra pergunta poderia ser, dado $f \in \kappa[x_1, \ldots, x_n]$ e um ideal $I = \langle f_1, \ldots, f_s \rangle$, como determinar se $f \in I$?

Sabemos que no anel em uma indeterminada, dado um $I \subseteq \kappa[x]$, então $I = \langle g \rangle$ para algum $g \in \kappa[x]$. Assim dado $f \in \kappa[x]$, pelo algoritmo da divisão temos que $f = q \cdot g + r$ com $q, r \in \kappa[x]$ e $r = 0$ ou $\deg(r) < \deg(g)$. Também sabemos que $f \in I = \langle g \rangle$ se, e somente se $r = 0$. Mas será que isso também é válido em $\kappa[x_1, \ldots, x_n]$?

Para responder essas perguntas, precisamos definir mais alguns conceitos que serão importantes e centrais para as construções algorítmicas desse capítulo.

1.2 Ordens Monomiais

Nesta seção definiremos as ordens monomiais sobre o anel de polinômios $\kappa[x_1, \ldots, x_n]$. Essas ordens são essenciais para resolver, por exemplo, a ocorrência de mais de um termo com

mesmo grau em um polinômio, possibilitando definir, analogamente ao que é feito no anel $\kappa[x]$, monômios líderes e termos líderes, os quais serão amplamente utilizados.

Para definir uma ordem monomial, iniciemos definindo relação de ordem parcial sobre um conjunto.

Definição 1.7. Uma relação R sobre um conjunto E não-vazio é chamada relação de ordem parcial sobre E se R é reflexiva, anti-simétrica e transitiva, isto é, R satisfaz as seguintes propriedades:

(i) Se $x \in E$, então xRx;

(ii) Se $x, y \in E$, xRy e yRx, então $x = y$;

(iii) Se $x, y, z \in E$, xRy e yRz, então xRz.

Para expressar que aRb, usamos comumente a notação $a \leq b$. No caso em que aRb e $a \neq b$, usamos então a notação $a < b$. Note que, equivalentemente, temos $b \geq a$, bem como $b > a$ se $a \neq b$.

Definição 1.8. Classificamos um conjunto da seguinte forma:

(i) Um conjunto parcialmente ordenado é um conjunto sobre o qual está definida uma relação de ordem parcial;

(ii) Seja R uma relação de ordem parcial sobre um conjunto E, os elementos $a, b \in E$ se dizem comparáveis mediante R se $a \leq b$ ou $b \leq a$. No caso em que $a \neq b$, então $a < b$ ou $b < a$;

(iii) Se dois elementos quaisquer de um conjunto E forem comparáveis mediante R, então R é chamada relação de ordem total sobre E. Nesse caso, o conjunto E é dito totalmente ordenado por R.

Uma vez definida ordem parcial, temos o necessário para definir ordem monomial.

Definição 1.9. Uma ordem monomial $>$ sobre $\kappa[x_1, \ldots, x_n]$ é uma relação de ordem sobre $\mathbb{Z}^n_{\geq 0}$, ou equivalentemente, uma relação de ordem sobre o conjunto de monômios x^α, com $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfazendo:

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

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

(iii) $>$ é uma boa-ordenação sobre $\mathbb{Z}^n_{\geq 0}$, ou seja, todo subconjunto não-vazio de $\mathbb{Z}^n_{\geq 0}$ tem um menor elemento mediante $>$. Isto é, se $\emptyset \neq A \subseteq \mathbb{Z}^n_{\geq 0}$, então $\exists\ \alpha \in A$ tal que $\beta > \alpha\ \forall\ \beta \in A$, com $\beta \neq \alpha$.

Um primeiro resultado importante sobre ordenação será demonstrado no lema a seguir, a saber, quando uma relação de ordem é uma boa-ordenação.

Lema 1.10. *Uma relação de ordem $>$ sobre $\mathbb{Z}^n_{\geq 0}$, é uma boa-ordenação se, e somente se toda sequência estritamente descendente em $\mathbb{Z}^n_{\geq 0}$, $\alpha(1) > \alpha(2) > \alpha(3) > \cdots$ termina.*

Demonstração. Provemos pela contrapositiva: $>$ não é uma boa-ordenação se, e somente se existe uma sequência infinita estritamente descendente em $\mathbb{Z}^n_{\geq 0}$.

Se $>$ não é uma boa-ordenação, então algum subconjunto não-vazio $S \subseteq \mathbb{Z}^n_{\geq 0}$ não tem um menor elemento. Tomemos $\alpha(1) \in S$. Como $\alpha(1)$ não é o menor elemento, podemos encontrar $\alpha(1) > \alpha(2) \in S$. Como $\alpha(2)$ também não é o menor elemento, podemos encontrar $\alpha(1) > \alpha(2) > \alpha(3) \in S$. Prosseguindo dessa forma, conseguiremos uma sequência infinita estritamente descendente $\alpha(1) > \alpha(2) > \alpha(3) > \cdots$.

Reciprocamente, dada uma tal sequência infinita, então $\{\alpha(1), \alpha(2), \alpha(3), \dots\}$ é um subconjunto não-vazio de $\mathbb{Z}^n_{\geq 0}$ sem um menor elemento, e assim, $>$ não é uma boa-ordenação. ■

Bem definidas as noções de ordem parcial e ordem monomial, podemos então definir e exemplificar algumas das ordens monomiais sobre $\kappa[x_1, \dots, x_n]$.

Definição 1.11 (Ordem monomial lexicográfica)**.** Sejam $\alpha = (\alpha_1, \dots, \alpha_n)$ e $\beta = (\beta_1, \dots, \beta_n)$ em $\mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha >_{lex} \beta$ se a entrada não-nula mais à esquerda do vetor diferença $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ é positiva. Escrevemos $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.

Como exemplos:
Temos que $xy^2 >_{lex} y^3z^4$, uma vez que $\alpha = (1,2,0) >_{lex} \beta = (0,3,4)$, pois $\alpha - \beta = (1,2,0) - (0,3,4) = (1,-1,-4)$, ou seja, a entrada não-nula mais à esquerda, a primeira, é positiva.

Temos também que $x^3y^2z^4 >_{lex} x^3y^2z$, uma vez que $\alpha = (3,2,4) >_{lex} \beta = (3,2,1)$, pois $\alpha - \beta = (3,2,4) - (3,2,1) = (0,0,3)$, ou seja, novamente a entrada não-nula mais à esquerda, a última, é positiva.

A própria ordem usual das indeterminadas $x_1, x_2, \dots, x_n$ é lexicográfica:
$(1,0,\dots,0) >_{lex} (0,1,0,\dots,0) >_{lex} \cdots >_{lex} (0,\dots,0,1)$, assim $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$. Com efeito, note que sempre temos a entrada não-nula mais à esquerda positiva.

Note que podemos ordenar as indeterminadas $x_1, x_2, \dots, x_n$ com a ordem lexicográfica de $n!$ modos diferentes, isto é, permutando suas posições na ordenação. Assim, ordenando as indeterminadas em ordem decrescente $x_n >_{lex} x_{n-1} >_{lex} \cdots >_{lex} x_1$ ou permutando apenas x_1 e x_2, ou seja, $x_2 >_{lex} x_1 >_{lex} x_3 >_{lex} \cdots >_{lex} x_n$ são outros exemplos de ordenação a partir da ordem lexicográfica.

Mostremos então que a ordem lexicográfica é, de fato, uma ordem monomial.

Proposição 1.12. *A ordem lexicográfica sobre $\mathbb{Z}^n_{\geq 0}$ é uma ordem monomial.*

Demonstração. A ordem $>_{lex}$ é uma ordem total. Com efeito, vejamos que dois monômios quaisquer são sempre comparáveis, isto é, dados $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, um dos três ocorre, por definição:
$x^\alpha >_{lex} x^\beta$, ou seja, a entrada não-nula mais à esquerda em $\alpha - \beta$ é positiva, digamos $\alpha_i - \beta_i > 0$;
$x^\beta >_{lex} x^\alpha$, ou seja, a entrada não-nula mais à esquerda em $\beta - \alpha$ é positiva, digamos $\beta_i - \alpha_i > 0$;
$x^\alpha = x^\beta$, nesse caso ocorrendo que $\alpha_i - \beta_i = 0 \; \forall \; i = 1, \ldots, n$.

Note também que temos $x^\alpha \geq_{lex} x^\alpha$, já que, como $\mathbb{Z}_{\geq 0}$ é totalmente ordenado, segue que $\alpha_i \geq \alpha_i \; \forall \; i = 1, \ldots, n$. Assim satisfaz a propriedade reflexiva.

Se $x^\alpha \geq_{lex} x^\beta$ e $x^\beta \geq_{lex} x^\alpha$ então $x^\alpha = x^\beta$. De fato, se $x^\alpha \neq x^\beta$, então $\exists \; k \in \{1, \ldots, n\}$ tal que $\alpha_k \neq \beta_k$, e sendo j o menor índice tal que isso ocorra, então:
Se $\alpha_j < \beta_j$, não poderíamos ter $x^\alpha \geq_{lex} x^\beta$.
Se $\beta_j < \alpha_j$, não poderíamos ter $x^\alpha \leq_{lex} x^\beta$.
Portanto $x^\alpha = x^\beta$. Assim satisfaz a propriedade anti-simétrica.

Se $x^\alpha >_{lex} x^\beta$ e $x^\beta >_{lex} x^\gamma$. Então $\exists \; j$ tal que $\alpha_i = \beta_i$ se $i < j$, e $\alpha_j > \beta_j$. Similarmente, $\exists \; k$ tal que $\beta_i = \gamma_i$ se $i < k$, e $\beta_k > \gamma_k$. Como novamente, $\mathbb{Z}_{\geq 0}$ é totalmente ordenado, temos que ou $j = k$, ou $j < k$ ou $j > k$.
Se $j < k$, então $\alpha_i = \beta_i = \gamma_i$ se $i < j$, e $\alpha_j > \beta_j = \gamma_j$.
Se $k < j$, então $\alpha_i = \beta_i = \gamma_i$ se $i < k$, e $\alpha_k = \beta_k > \gamma_k$.
Se $j = k$, então $\alpha_i = \beta_i = \gamma_i$ se $i < j$, e $\alpha_j > \beta_j > \gamma_j$.
Em todos os casos, $\alpha >_{lex} \gamma$ e portanto $x^\alpha >_{lex} x^\gamma$. Assim satisfaz a propriedade transitiva.

Também temos que se $\alpha >_{lex} \beta$, então a entrada não-nula mais à esquerda em $\alpha - \beta$ é positiva, digamos $\alpha_i - \beta_i > 0$. Note que $x^\alpha \cdot x^\gamma = (x_1^{\alpha_1} \cdots x_n^{\alpha_n}) \cdot (x_1^{\gamma_1} \cdots x_n^{\gamma_n}) = x_1^{\alpha_1 + \gamma_1} \cdots x_n^{\alpha_n + \gamma_n} = x^{\alpha+\gamma}$ e, de modo análogo, $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$.
Como temos que $(\alpha + \gamma) - (\beta + \gamma) = (\alpha_1 + \gamma_1 - \beta_1 - \gamma_1, \ldots, \alpha_n + \gamma_n - \beta_n - \gamma_n) =$
$= (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n) = \alpha - \beta$, então a entrada não-nula mais à esquerda é novamente $\alpha_i - \beta_i > 0$.
Portanto $x^\alpha \cdot x^\gamma >_{lex} x^\beta \cdot x^\gamma$.

Por fim, suponhamos, por contradição, que $>_{lex}$ não seja uma boa-ordenação. Então, pelo Lema 1.10, deve existir uma sequência infinita estritamente descendente $\alpha(1) >_{lex} \alpha(2) >_{lex} \cdots$ de elementos de $\mathbb{Z}^n_{\geq 0}$.
Consideremos as primeiras entradas dos $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Por definição de ordem lexicográfica, essas primeiras entradas formam uma sequência não-crescente de inteiros não-negativos.
Como $\mathbb{Z}_{\geq 0}$ está bem-ordenado, as primeiras coordenadas dos $\alpha(i)$ devem eventualmente estabilizar. Em outras palavras, existe um l tal que todas as primeiras entradas dos $\alpha(i)$ com $i \geq l$ são iguais.

Começando em $\alpha(l)$, as segundas coordenadas e as subsequentes serão então as utilizadas para prosseguir determinando a ordenação.

As segundas coordenadas dos $\alpha(l), \alpha(l+1), \ldots$ formariam assim, novamente, uma sequência não-crescente de inteiros não-negativos. Eventualmente estabilizando de igual modo.

Prosseguindo dessa forma, concluímos que para algum m, as entradas dos $\alpha(m), \alpha(m+1),$

..., seriam todas iguais. O que contradiria a suposição de que $\alpha(m) >_{lex} \alpha(m+1)$.
Portanto a ordem lexicográfica é uma boa-ordenação.

■

Note que com a ordem monomial lexicográfica $x >_{lex} y >_{lex} z$ temos que um monômio em uma única variável é sempre maior pela ordem que outro monômio envolvendo as demais variáveis menores, por exemplo: $x >_{lex} y^5z^3$, já que $(1,0,0)-(0,5,3)=(1,-4,-3)$ e assim a entrada não-nula mais à esquerda, 1, é positiva.

Desse modo é possível que um monômio de grau total inferior seja maior, pela ordenação, que outro de grau total superior, como visto no exemplo anterior.

Para levar em conta também o grau do monômio para a ordenação, temos a ordem monomial lexicográfica graduada a seguir.

Definição 1.13 (Ordem monomial lexicográfica graduada)**.** Sejam $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha >_{grlex} \beta$ se $|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$, ou $|\alpha| = |\beta|$ e $\alpha >_{lex} \beta$.

Como exemplos:
Temos que $xy^2z^5 >_{grlex} x^3y^2$, uma vez que $|(1,2,5)| = 8 > 5 = |(3,2,0)|$.
Temos também que $xy^2z^4 >_{grlex} xyz^5$, uma vez que $|(1,2,4)| = 7 = |(1,1,5)|$ e $(1,2,4) >_{lex} (1,1,5)$.

Perceba que, quando temos dois monômios com mesmo grau total, então quem determina a ordenação é a ordem lexicográfica simples.

Análogo à ordem lexicográfica, a ordem lexicográfica graduada é uma ordem monomial.

Proposição 1.14. *A ordem lexicográfica graduada $>_{grlex}$ é uma ordem monomial.*

Demonstração. Veja [7, pág 9].

Também podemos definir uma ordem lexicográfica que beneficie o menor expoente da última indeterminada, de forma oposta à lexicográfica simples, que ordena pelo maior expoente da primeira indeterminada.

Definição 1.15 (Ordem monomial lexicográfica graduada reversa)**.** Sejam $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Dizemos que $\alpha >_{grevlex} \beta$ se $|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$, ou $|\alpha| = |\beta|$ e a entrada não-nula mais à direita de $\alpha - \beta \in \mathbb{Z}^n$ é negativa.

Como exemplos, temos que $xy^4z^7 >_{grevlex} x^4y^2z^3$, uma vez que $|(1,4,7)| = 12 > 9 = |(4,2,3)|$.
Também $xy^5z^2 >_{grevlex} x^4yz^3$, uma vez que $|(1,5,2)| = 8 = |(4,1,3)|$ e $(1,5,2)-(4,1,3) = (-3,4,-1)$.

Note que ambas as ordens $>_{grlex}$ e $>_{grevlex}$ utilizam o grau total dos monômios da mesma forma. Contudo elas são distintas, vejamos por exemplo que $x^5yz >_{grlex} x^4yz^2$, já que esses

monômios tem o mesmo grau total e $(5,1,1)-(4,1,2)=(1,0,-1)$, ou seja, a entrada não-nula mais à esquerda é positiva; e também $x^5yz >_{grevlex} x^4yz^2$, mas nesse caso por outro motivo, já que a entrada não-nula mais à direita é negativa.

No entanto, $x^2yz^3 >_{grlex} xy^4z$, uma vez que esses monômios tem o mesmo grau total e $(2,1,3)-(1,4,1)=(1,-3,2)$, ou seja, a entrada não-nula mais à esquerda é positiva; e $xy^4z >_{grevlex} x^2yz^3$, já que a entrada não-nula mais à direita é negativa.

Comparando então esses três tipos de ordens monomiais temos que, dado $f=\sum_{\alpha} a_\alpha x^\alpha$ um polinômio não-nulo em $\kappa[x_1,\ldots,x_n]$ e escolhida uma ordem monomial $>$, podemos ordenar seus termos monomiais obtendo uma expressão para f relativa à essa ordem fixada.

Por exemplo, seja $f=4xy^2z+4z^2-5x^3+7x^2z^2\in\mathbb{R}[x_1,\ldots,x_n]$.
Com respeito à ordem $>_{lex}$ temos:
$f=-5x^3+7x^2z^2+4xy^2z+4z^2$;
Com respeito à ordem $>_{grlex}$ temos:
$f=7x^2z^2+4xy^2z-5x^3+4z^2$
Com respeito à ordem $>_{grevlex}$ temos:
$f=4xy^2z+7x^2z^2-5x^3+4z^2$.

1.3 Algoritmo da Divisão

Nesta seção apresentamos a construção do Algoritmo da divisão no anel de polinômios em n indeterminadas. Este algoritmo pode ser implementado em diversos softwares matemáticos, em nosso caso, utilizaremos o software livre SageMath [9] baseado na linguagem de programação Python.

Fixada uma ordem monomial podemos definir então os elementos essenciais para a implementação desse algoritmo, os monômios e termos líderes de um polinômio.

Definição 1.16. Seja $f=\sum_{\alpha} a_\alpha x^\alpha$ um polinômio não-nulo em $\kappa[x_1,\ldots,x_n]$ e seja $>$ uma ordem monomial. Definimos:

(i) O multigrau de f é $\text{multideg}(f)=max(\alpha\in\mathbb{Z}^n_{\geq 0} \mid a_\alpha\neq 0)$, onde o máximo é com respeito à ordem monomial $>$;

(ii) O coeficiente líder de f é $LC(f)=a_{\text{multideg}(f)}\in\kappa$;

(iii) O monômio líder de f é $LM(f)=x^{\text{multideg}(f)}$, (com coeficiente 1);

(iv) O termo líder de f é $LT(f)=LC(f)\cdot LM(f)=a_{\text{multideg}(f)}\,x^{\text{multideg}(f)}$.

Por exemplo, seja $f=4xy^2z+4z^2-5x^3+7x^2z^2$, e tomando a ordem $>_{lex}$, temos:
$\text{multideg}(f)=(3,0,0)$
$LC(f)=-5$

$LM(f) = x^3$
$LT(f) = -5x^3$

Enquanto que, tomando a ordem $>_{grlex}$, temos:
$\text{multideg}(f) = (2, 0, 2)$
$LC(f) = 7$
$LM(f) = x^2z^2$
$LT(f) = 7x^2z^2$

O resultado apresentado no lema a seguir, que será utilizado na demonstração do Algoritmo da Divisão mais à frente na seção, analisa o que ocorre com os multigraus de um produto e de uma soma de polinômios.

Lema 1.17. *Sejam $f, g \in \kappa[x_1, \ldots, x_n]$ polinômios não-nulos. Então:*

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

(ii) *Se $f + g \neq 0$, então* $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. *Se em adição,* $\text{multideg}(f) \neq \text{multideg}(g)$*, tem-se igualdade.*

Demonstração. Veja [2, pág 60].

Outra definição essencial para a construção do Algoritmo da Divisão é a de divisibilidade entre monômios.

Definição 1.18. Sejam $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Dizemos que um monômio x^α divide um monômio x^β se existe $\gamma \in \mathbb{Z}^n_{\geq 0}$ tal que $\beta = \gamma + \alpha$, isto é, $x^\beta = x^\gamma \cdot x^\alpha$.

Agora temos as ferramentas necessárias para a construção do Algoritmo da Divisão em $\kappa[x_1, \ldots, x_n]$ que nos permitirá dividir um polinômio $f \in \kappa[x_1, \ldots, x_n]$ por $f_1, \ldots, f_s \in \kappa[x_1, \ldots, x_n]$, de modo que possamos expressar f na forma $f = q_1f_1 + \cdots + q_sf_s + r$, com $q_1, \ldots, q_s$ e r em $\kappa[x_1, \ldots, x_n]$.

Passemos então à construção e prova da funcionalidade do algoritmo que fornece essa expressão para um polinômio arbitrário $f \in \kappa[x_1, \ldots, x_n]$.

Teorema 1.19 (Algoritmo da Divisão)**.** *Seja $>$ uma ordem monomial sobre $\mathbb{Z}^n_{\geq 0}$, e sejam $F = (f_1, \ldots, f_s)$ uma s-úpla ordenada de polinômios não-nulos em $\kappa[x_1, \ldots, x_n]$. Então todo $f \in \kappa[x_1, \ldots, x_n]$ pode ser escrito como $f = q_1f_1 + \cdots + q_sf_s + r$, onde $q_1, \ldots, q_s, r \in \kappa[x_1, \ldots, x_n]$, e $r = 0$ ou r é uma combinação linear, com coeficientes em κ, de monômios, nenhum dos quais é divisível por algum $LT(f_1), \ldots, LT(f_s)$. Chamamos r um resto de f na divisão por F. Além disso, se $q_if_i \neq 0$, então* $\text{multideg}(f) \geq \text{multideg}(q_if_i)$.

Demonstração. Provemos a existência de $q_1, \ldots, q_s$ e r por meio de um algoritmo para sua construção e mostrando que o algoritmo funciona para as entradas fornecidas:
Input: $f_1, \ldots, f_s, f$

Output: $q_1, \ldots, q_s, r$
$q_1 := 0; \ldots; q_s := 0; r := 0$
$p := f$
WHILE $(p \neq 0)$ DO
    $i := 1$
    $divisionocurred :=$ false
    WHILE $(i \leq s)$ AND $(divisionocurred :=$ false) DO
        IF $(LT(f_i))$ divides $(LT(p))$ THEN
            $q_i := q_i + LT(p)/LT(f_i)$
            $p := p - (LT(p)/LT(f_i))f_i$
            $divisionocurred :=$ true
        ELSE
            $i := i + 1$
    IF $(divisionocurred :=$ false) THEN
        $r := r + LT(p)$
        $p := p - LT(p)$
RETURN $q_1, \ldots, q_s, r$

Note que neste algoritmo a variável p representa o dividendo intermediário em cada estágio, $q_1, \ldots, q_s$ os quocientes e r o resto na divisão de f por F.
A variável booleana $divisionocurred$ indica quando algum $LT(f_i)$ divide o $LT(p)$ do dividendo intermediário, e assim em cada loop uma das duas coisas ocorre: Se algum $LT(f_i)$ divide $LT(p)$, o algoritmo, similarmente ao caso em uma indeterminada, opera para cancelar $LT(p)$ em p e segue preenchendo q_i; Se nenhum $LT(f_i)$ divide $LT(p)$, o algoritmo opera para cancelar $LT(p)$ em p e adiciona $LT(p)$ ao resto r.

Para verificar que o algoritmo funciona, mostremos que em cada estágio temos

$$f = q_1 f_1 + \cdots + q_s f_s + p + r \qquad (1)$$

Esta igualdade é claramente válida para os valores iniciais atribuídos. Com efeito:
$f = 0 \cdot f_1 + \cdots + 0 \cdot f_s + f + 0$.

Supondo que temos a igualdade (1) válida em um estágio do algoritmo, se o próximo estágio é um passo de divisão, ou seja, algum $LT(f_i)$ divide $LT(p)$, então da igualdade
$q_i f_i + p = q_i f_i + (LT(p)/LT(f_i))f_i - (LT(p)/LT(f_i))f_i + p = (q_i + LT(p)/LT(f_i))f_i +$
$+(p - (LT(p)/LT(f_i))f_i)$, podemos ver que o termo $q_i f_i + p$ permanece inalterado.

Como as demais variáveis também não se alteraram nesse passo, então a igualdade (1) continua válida.

Por outro lado, se o próximo estágio for um passo de resto, ou seja, cancelar $LT(p)$ em p e adicionar $LT(p)$ a r, então o termo $p + r$ permanece inalterado, já que, $(p - LT(p)) + (r +$

$LT(p)) = p + r$, e assim a igualdade (1) continua válida.

Note que o algoritmo pára quando $p = 0$, e nessa situação obtemos exatamente

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

Como os termos $LT(p)$ são adicionados a r somente quando não são divisíveis por nenhum dos $LT(f_i)$, então desse modo ou $r = 0$ ou r tem a propriedade desejada quando o algoritmo termina.

Agora, precisamos mostrar que o algoritmo eventualmente termina. Para isso, note que em cada estágio no qual atualizamos a variável p, só temos duas possibilidades: ou $\mathrm{multideg}(p)$ diminui (relativamente à ordem $>$), ou p se torna 0.

Com efeito, primeiro suponhamos que durante um passo de divisão tenhamos redefinido p como:

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

Como $LT(g)\cdot LT(h) = LC(g)LM(g)\cdot LC(h)LM(h) = LC(g)LC(h)x^{\mathrm{multideg}(g)}\cdot x^{\mathrm{multideg}(h)}$ $= LC(g)LC(h)x^{\mathrm{multideg}(g)+\mathrm{multideg}(h)} = LC(g)LC(h)x^{\mathrm{multideg}(gh)} = LT(gh)$.

Então:

$$LT((LT(p)/LT(f_i))f_i) = LT(LT(p)/LT(f_i))\cdot LT(f_i) = (LT(p)/LT(f_i))\cdot LT(f_i) = LT(p) \quad (2)$$

Desse modo, p e $(LT(p)/LT(f_i))f_i$ tem o mesmo termo líder. Consequentemente sua diferença, que resulta exatamente p', deve ter multigrau estritamente menor, sendo $p' \neq 0$. Resulta análogo se durante um passo de resto p tenha sido redefinido como

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

Claramente temos que $\mathrm{multideg}(p') < \mathrm{multideg}(p)$, sendo $p' \neq 0$ em ambos os casos.

Se o algoritmo nunca terminasse, ou seja, nunca chegássemos a $p = 0$, então teríamos uma sequência descendente estrita infinita de multigraus. Mas a boa-ordenação da ordem monomial $>$ garante que tal sequência não existe, portanto, eventualmente chegaremos a $p = 0$ e o algoritmo encerrará.

Por fim, note que o algoritmo inicia com $p = f$ e, como acabamos de mostrar, o multigrau de p diminui. Então temos $\mathrm{multideg}(p) \leq \mathrm{multideg}(f)$.

Note também que cada termo de um quociente q_i não-nulo é da forma $LT(p)/LT(f_i)$ para algum valor da variável p. Em outras palavras q_i é da forma
$0 + LT(p_1)/LT(f_i) + LT(p_2)/LT(f_i) + \cdots + LT(p_k)/LT(f_i)$, onde estamos denotando por p_j a variável p na $j-$ésima atualização de q_i.

Assim, pelo Lema 1.17 e por (2) temos:

$$\mathrm{multideg}(LT(p_1)/LT(f_i)) + \mathrm{multideg}(f_i) = \mathrm{multideg}((LT(p_1)/LT(f_i)\cdot f_i) = \mathrm{multideg}(p_1)$$

$\geq \text{multideg}(p_j) = \text{multideg}((LT(p_j)/LT(f_i) \cdot f_i) = \text{multideg}(LT(p_j)/LT(f_i)) + \text{multideg}(f_i)$.

Segue assim que $\text{multideg}(LT(p_1)/LT(f_i)) \geq \text{multideg}(LT(p_j)/LT(f_i))$ para todo $j = 1, \ldots, k$. Portanto $\text{multideg}(q_i) = \text{multideg}(LT(p_1)/LT(f_i))$. Logo $\text{multideg}(q_i f_i) =$
$= \text{multideg}((LT(p_1)/LT(f_i))f_i) = \text{multideg}(p_1) \leq \text{multideg}(f)$, quando $q_i f_i \neq 0$, o que conclui a demonstração. ■

Vejamos um exemplo de forma a aplicar os passos do algoritmo e esclarecer seu funcionamento:

Fixada a ordem monomial $x >_{grlex} y$. Sejam $f = -2xy^2 + x^2y^3 \in \kappa[x, y]$ e $f_1 = x^2y - 2x$, $f_2 = y^3 + 4$.

Então ordenando com a ordem $x >_{grlex} y$ temos $f = x^2y^3 - 2xy^2$, $f_1 = x^2y - 2x$, $f_2 = y^3 + 4$ e portanto $LT(f) = x^2y^3$, $LT(f_1) = x^2y$, $LT(f_2) = y^3$ e $p = f$.

Listemos p, os divisores, os quocientes e o resto:

$p : x^2y^3 - 2xy^2$

q_1: 0

q_2: 0

$f_1 : x^2y - 2x$

$f_2 : y^3 + 4$

$r : 0$

Note que ambos os $LT(f_i)$ dividem $LT(p)$, isto é, $(x^2y) \mid (x^2y^3)$ e $(y^3) \mid (x^2y^3)$.

Como f_1 está listado primeiro, então:

$$p = p - \frac{LT(p)}{LT(f_1)}(f_1) = x^2y^3 - 2xy^2 - \frac{x^2y^3}{x^2y}(x^2y - 2x) = x^2y^3 - 2xy^2 - y^2(x^2y - 2x) =$$

$$= x^2y^3 - 2xy^2 - x^2y^3 + 2xy^2 = 0 \text{ e}$$

$$q_1 = q_1 + \frac{LT(p)}{LT(f_1)} = 0 + y^2 = y^2.$$

Assim, atualizando as variáveis no algoritmo:

$p : 0$

$q_1 : y^2$

q_2: 0

$f_1 : x^2y - 2x$

$f_2 : y^3 + 4$

$r : 0$

Como $p = 0$, paramos e portanto obtemos:

$$f = q_1 f_1 + q_2 f_2 + r = y^2(x^2y - 2x) + 0 \cdot (y^3 + 4) + 0.$$

Se por outro lado listarmos os divisores em outra ordem:
$p : x^2y^3 - 2xy^2$
q_1: 0
q_2: 0
$f_1 : y^3 + 4$
$f_2 : x^2y - 2x$
$r : 0$

Novamente $(x^2y) \mid (x^2y^3)$ e $(y^3) \mid (x^2y^3)$. Mas como agora $y^3 + 4$ está listado primeiro:

$$p = p - \frac{LT(p)}{LT(f_1)}(f_1) = x^2y^3 - 2xy^2 - \frac{x^2y^3}{y^3}(y^3 + 4) = x^2y^3 - 2xy^2 - x^2(y^3 + 4) =$$

$$= x^2y^3 - 2xy^2 - x^2y^3 - 4x^2 = -2xy^2 - 4x^2 \text{ e}$$

$$q_1 = q_1 + \frac{LT(p)}{LT(f_1)} = 0 + x^2 = x^2.$$

Assim, atualizando as variáveis:
$p : -2xy^2 - 4x^2$
$q_1 : x^2$
q_2: 0
$f_1 : y^3 + 4$
$f_2 : x^2y - 2x$
$r : 0$

Como agora $(y^3) \nmid (-2xy^2)$ então passamos para f_2.

Como também temos que $(x^2y) \nmid (-2xy^2)$ então:

$$p = p - LT(p) = -2xy^2 - 4x^2 - (-2xy^2) = -4x^2 \text{ e}$$

$$r = r + LT(p) = 0 + (-2xy^2) = -2xy^2.$$

Assim, atualizando novamente as variáveis:
$p : -4x^2$
$q_1 : x^2$
q_2: 0
$f_1 : y^3 + 4$
$f_2 : x^2y - 2x$
$r : -2xy^2$

Por fim, como $(y^3) \nmid (-4x^2)$ e $(x^2y) \nmid (-4x^2)$ então:

$$p = p - LT(p) = -4x^2 - (-4x^2) = 0 \text{ e}$$

$$r = r + LT(p) = -2xy^2 - 4x^2 = -2xy^2 - 4x^2.$$

Portanto obtemos:

$$f = q_1 f_2 + q_2 f_1 + r = x^2(y^3 + 4) + 0 \cdot (x^2 y - 2x) + (-2xy^2 - 4x^2).$$

Note portanto que $r = 0$ é condição suficiente para termos $f \in I = \langle f_1, \ldots, f_s \rangle$, contudo não é condição necessária. No exemplo anterior, podemos perceber que obtivemos dois restos distintos quando alteramos a ordem dos polinômios divisores. Assim, diferente do que ocorre no anel $\kappa[x]$, o Algoritmo da Divisão em $\kappa[x_1, \ldots, x_n]$ pode apresentar expressões para f com restos distintos dependendo da ordem monomial fixada e da ordem em que os polinômios divisores estão listados.

Surge naturalmente outro questionamento: será que existe um conjunto de polinômios que gere o mesmo ideal para os quais o resto da divisão de um polinômio por eles seja único? Responderemos mais à frente, na seção Bases de Gröbner, à essa pergunta.

Para concluir essa seção, implementaremos o Algoritmo da divisão no software livre SageMath [9] em um exemplo.

Na primeira linha do código, precisamos definir o Anel de Polinômios com o qual iremos trabalhar, bem como a ordem monomial que será utilizada pelo algoritmo. Nesse exemplo, o anel será $\mathbb{Q}[x, y]$ e a ordem será a lexicográfica $x >_{lex} y$.

Note que precisaremos também definir uma função que nos retorne se o termo líder de uma lista ordenada de polinômios divisores $F = (f_1, \ldots, f_s)$ divide o termo líder do polinômio f. Definiremos essa função no algoritmo com o nome "does-divide", a qual retornará como resultado a variável $booleana$ "division-occurred", que retorna portanto os valores "verdadeiro", se a divisão ocorreu, ou "falso", se não ocorreu a divisão entre os termos líderes.

Definida essa função que estudará a divisibilidade, declaramos as variáveis necessárias, a saber, o polinômio dividendo f, uma lista ordenada com os polinômios divisores $F = (f_1, f_2)$ e inicializamos o resto $r = 0$, uma variável auxiliar $p = f$ e a lista de polinômios quocientes $A[i]$. Note que o tamanho da lista de quocientes depende do número "$len(F)$" de polinômios divisores, já que para cada f_i teremos um q_i correspondente.

Por fim implementamos o código visto no Teorema 1.19 em um exemplo, procedendo a divisão do polinômio $f = x^2y + xy^2 + y^2$ pelos polinômios $f_1 = xy - 1$ e $f_2 = y^2 - 1$.

```
SageMath version 9.3 Console

sage: P.<x, y> = PolynomialRing(QQ, 2, order = "lex")
sage: division_occurred = False
sage: def does_divide(m1, m2):
....:         for c in (vector(ZZ, m1.degrees()) - vector(ZZ, m2.degrees())):
....:                 if c < 0:
....:                         return False
....:         return True
....:
```

```
sage: F = [x*y - 1, y^2 - 1]
sage: f = x^2*y + x*y^2 + y^2
sage: A = [P(0) for i in range(0, len(F))]
sage: r = P(0)
sage: p = f
sage: while p != P(0):
....:         i = 0
....:         division_occurred = False
....:         while (i < len(F) and division_occurred == False):
....:                 print(A, r)
....:                 print(p)
....:                 if does_divide(p.lt(), F[i].lt()):
....:                         q = P(p.lt()/F[i].lt())
....:                         A[i] = A[i] + q
....:                         p = p -q*F[i]
....:                         division_occurred == False
....:                 else:
....:                         i = i+1
....:         if division_occurred == False:
....:                 r = r + p.lt()
....:                 p = p - p.lt()
....:
[0, 0] 0
x^2*y + x*y^2 + y^2
True
[x, 0] 0
x*y^2 + x + y^2
True
[x + y, 0] 0
x + y^2 + y
[x + y, 0] 0
x + y^2 + y
[x + y, 0] x
y^2 + y
[x + y, 0] x
y^2 + y
True
[x + y, 1] x
y + 1
[x + y, 1] x + y
1
[x + y, 1] x + y
1
sage: print(A)
[x + y, 1]
sage: print(r)
x + y + 1
```

```
sage: print(p)
0
sage:
```

Note que inserimos convenientemente dentro do segundo $while$ comandos para imprimir em cada passo os valores da lista de quocientes e o resto, $print(A, r)$, bem como a variável auxiliar $print(p)$. É exatamente esta variável p que determinará a parada do algoritmo já que ela foi inicializada como $p = f$, isto é, quando chegarmos a $p = 0$ o algoritmo encerra.

Por fim, após o algoritmo executar completamente, pedimos então para imprimir a lista de quocientes final, o resto, e a variável auxiliar p, a qual como esperado terminou com o valor $p = 0$.

Logo, obtivemos o resultado da divisão da forma:

$$f = q_1 f_1 + q_2 f_2 + r = (x + y)(xy - 1) + (1)(y^2 - 1) + (x + y + 1).$$

1.4 Ideais Monomiais

Nesta seção apresentaremos resultados importantes sobre ideais monomiais que serão amplamente utilizados na seção seguinte para a construção e implementação do Algoritmo da Base de Gröbner de um ideal polinomial.

Definimos ideal anteriormente na primeira seção e nesta seção definiremos um tipo particular de ideal chamado ideal monomial e veremos alguns resultados importantes sobre o ideal gerado pelos termos líderes de um conjunto de polinômios.

Definição 1.20. Um ideal $I \subseteq \kappa[x_1, \ldots, x_n]$ é um ideal monomial se existe um subconjunto $A \subseteq \mathbb{Z}^n_{\geq 0}$ (possivelmente infinito) tal que I consiste de todos os polinômios que são somas finitas da forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, onde $h_\alpha \in \kappa[x_1, \ldots, x_n]$. Nesse caso escrevemos $I = \langle x^\alpha \mid \alpha \in A \rangle$.

Como exemplo:
$I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle \subseteq \kappa[x, y]$.

Como primeiro resultado, veremos uma forma simples de verificar se um certo monômio está em dado ideal monomial.

Lema 1.21. *Seja $I = \langle x^\alpha \mid \alpha \in A \rangle$ um ideal monomial. Então um monômio x^β está em I se, e somente se x^β é divisível por x^α para algum $\alpha \in A \subseteq \mathbb{Z}^n_{\geq 0}$.*

Demonstração. Veja [2, pág 70].

Dessa forma, podemos verificar rapidamente se um monômio está em um ideal monomial, assim como também conhecer todos os monômios que estão nesse ideal. Vejamos um exemplo:

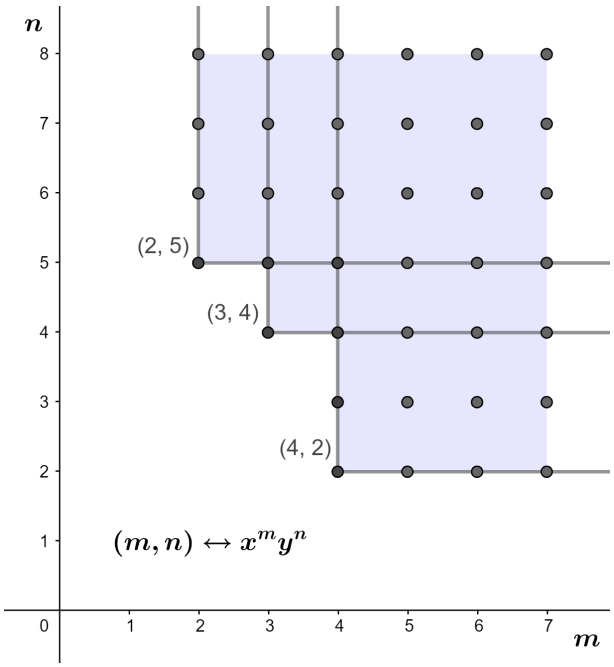

Figura 1.1: Expoentes dos monômios pertencentes a I.

Seja $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$. Então pelo lema anterior, os expoentes dos monômios em I formam o conjunto $((4,2)+\mathbb{Z}^2_{\geq 0}) \cup ((3,4)+\mathbb{Z}^2_{\geq 0}) \cup ((2,5)+\mathbb{Z}^2_{\geq 0})$. Os quais podem ser visualizados na Figura 1.1.

Note que todos os monômios à direita e acima de x^4y^2 pertencem ao ideal I. Contudo nenhum monômio à esquerda ou abaixo de x^3y^2 pertence ao ideal I, já que estes não seriam divisíveis por nenhum monômio que gera I.

Agora veremos um resultado que nos possibilita verificar quando certo polinômio pertence a dado ideal monomial.

Lema 1.22. *Seja $I = \langle x^\alpha \mid \alpha \in A \rangle$ um ideal monomial e seja $f \in \kappa[x_1, \ldots, x_n]$. Então $f \in I$ se, e somente se f é uma combinação $\kappa-$linear de monômios em I.*

Demonstração. Podemos ver que se cada monômio de f for divisível por algum $x^\alpha \in I$, então f pode ser escrito como $f = \sum_i h_i x^{\alpha(i)}$, e, por definição de ideal, $f \in I$.

Por outro lado, se $f \in I$, então novamente $f = \sum_i h_i x^{\alpha(i)}$. Expandindo cada h_i como combinação $\kappa-$linear de monômios em $\kappa[x_1, \ldots, x_n]$, segue que f será uma combinação $\kappa-$linear de monômios onde cada um deles é divisível por algum monômio em I. ■

Segue facilmente o próximo resultado, o qual será usado na demonstração do Lema de Dickson.

Lema 1.23. *Dois ideais monomiais são os mesmos se, e somente se possuem os mesmos monômios.*

Demonstração. Veja [2, pág 72].

O Lema de Dickson a seguir precede um resultado mais geral de Álgebra Comutativa, a saber, o Teorema da Base de Hilbert, o qual, como veremos adiante, garante que todo ideal polinomial possui uma base finita de polinômios. No caso particular do Lema de Dickson temos o mesmo resultado aplicado a ideais monomiais garantindo que os mesmos possuem uma base finita formada por monômios.

Lema 1.24 (Lema de Dickson)**.** *Seja* $I = \langle x^\alpha \mid \alpha \in A\rangle \subseteq \kappa[x_1, \ldots, x_n]$ *um ideal monomial. Então* I *pode ser escrito da forma* $I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\right\rangle$*, onde* $\alpha(1), \ldots, \alpha(s) \in A \subseteq \mathbb{Z}^n_{\geq 0}$.

Demonstração. Faremos por indução sobre o número de indeterminadas n.

Se $n = 1$, então I é gerado por monômios x_1^α, onde $\alpha \in A \subseteq \mathbb{Z}_{\geq 0}$. Seja β o menor elemento de A. Então $\beta \leq \alpha \ \forall \ \alpha \in A$, de modo que x_1^β divide todos os demais x_1^α. Segue então que $I = \left\langle x_1^\beta \right\rangle$.

Assumamos agora que $n > 1$ e que o lema é verdadeiro para $n - 1$. Escrevamos as indeterminadas como $x_1, \ldots, x_{n-1}, y$, de modo que os monômios em $\kappa[x_1, \ldots, x_{n-1}, y]$ podem ser escritos como $x^\alpha y^m$, com $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}^{n-1}_{\geq 0}$ e $m \in \mathbb{Z}_{\geq 0}$.

Seja $I \subseteq \kappa[x_1, \ldots, x_{n-1}, y]$ um ideal monomial. Para encontrar geradores para I, tomemos $J \subseteq \kappa[x_1, \ldots, x_{n-1}]$ ideal gerado pelos monômios x^α para os quais $x^\alpha y^m \in I$ para algum $m \geq 0$. Como J é um ideal monomial em $\kappa[x_1, \ldots, x_{n-1}]$, por hipótese de indução temos que $J = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\right\rangle$.

Para cada $1 \leq i \leq s$, temos da definição de J 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 $0 \leq l \leq m - 1$, consideremos os ideais $J_l \subseteq \kappa[x_1, \ldots, x_{n-1}]$ gerados pelos monômios $x^{\alpha(i)}$ tais que $x^{\alpha(i)} y^l \in I$.

Então, usando novamente a hipótese de indução, temos que $J_l = \left\langle x^{\alpha_l(1)}, \ldots, x^{\alpha_l(s_l)}\right\rangle$. Afirmamos que I é gerado pelos monômios listados a seguir:
De J : $x^{\alpha(1)} y^m, \ldots, x^{\alpha(s)} y^m$;
De J_0 : $x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)}$
De J_1 : $x^{\alpha_1(1)} y, \ldots, x^{\alpha_1(s_1)} y$
$\vdots$
De J_{m-1} : $x^{\alpha_{m-1}(1)} y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1}$.

Primeiramente, note que todo monômio em I é divisível por algum dessa lista. Com efeito, tome $x^\alpha y^p \in I$. Se $p \geq m$, então $x^\alpha \in J$, logo x^α é divisível por algum $x^{\alpha(i)}$, assim $x^\alpha y^p$ será divisível por algum $x^{\alpha(i)} y^m$.

Se $p \leq m - 1$, então, de forma análoga a $p \geq m$, $x^\alpha y^p$ será divisível por algum $x^{\alpha_p(j)} y^p$, pela forma como construímos os J_p.

Segue assim do Lema 1.21, que os monômios dessa lista geram um ideal que possui os mesmos monômios que I. E, do Lema 1.23, segue que o ideal gerado por esses monômios é o próprio I. Logo, a afirmação está provada. ■

Apliquemos o Lema de Dickson para analisar o exemplo de ideal monomial dado na Figura 1.2:
Seja $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$.

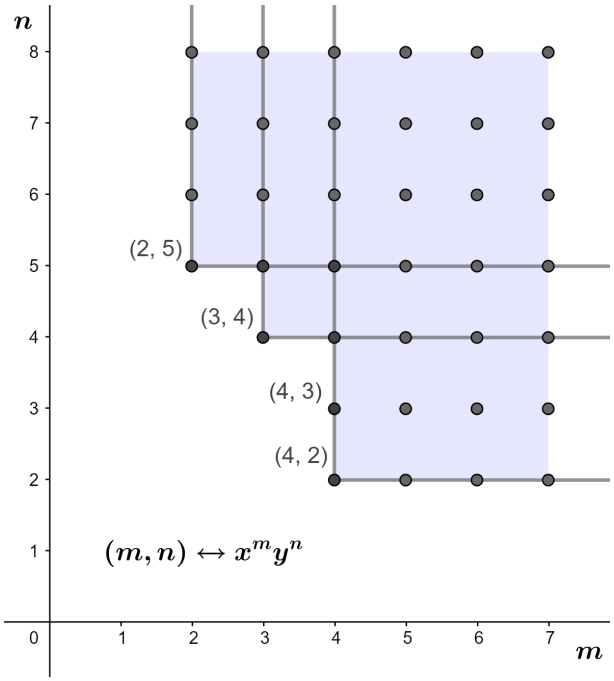

Figura 1.2: Expoentes dos monômios geradores de I.

Nesse caso, temos que $J = \langle x^2 \rangle \subseteq \kappa[x]$.
De $x^2y^5 \in I$, temos $m = 5$.

Então os J_l para $0 \leq l \leq m - 1 = 4$ são:
$J_0 = J_1 = \{0\}$;
$J_2 = J_3 = \langle x^4 \rangle$;
$J_4 = \langle x^3 \rangle$.

Portanto I é gerado pelos monômios: $I = \langle x^2y^5, x^4y^2, x^4y^3, x^3y^4 \rangle$.

1.5 Bases de Gröbner e Algoritmo de Buchberger

Nesta seção, já tendo discutido as definições e resultados necessários, poderemos definir Base de Göbner de um ideal polinomial, chegando no fim desta seção ao estudo do algoritmo que permite computar essa base, fixada uma ordem monomial.

Iniciemos com a definição de ideal gerado pelos termos líderes dos polinômios pertencentes a dado ideal.

Definição 1.25. Sejam $I \subseteq \kappa[x_1, \ldots, x_n]$ um ideal não-nulo, e $>$ uma ordem monomial sobre $\kappa[x_1, \ldots, x_n]$. Então:

(i) Denotamos por $LT(I)$ o conjunto dos termos líderes dos elementos não-nulos de I:
$LT(I) = \{cx^\alpha \mid \exists\ f \in I \setminus \{0\} \text{ com } LT(f) = cx^\alpha\}$.

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

Observação:

Caso $I = \langle f_1, \ldots, f_s\rangle$, temos que $\langle LT(f_1), \ldots, LT(f_s)\rangle$ e $\langle LT(I)\rangle$ podem ser ideais diferentes. É verdade que $LT(f_i) \in LT(I) \subseteq \langle LT(I)\rangle$, implicando que:
$\langle LT(f_1), \ldots, LT(f_s)\rangle \subseteq \langle LT(I)\rangle$. Contudo $\langle LT(I)\rangle$ pode ser estritamente maior.

Vejamos um exemplo para esclarecer este fato:
Seja $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$ e a ordem $>_{grlex}$ sobre $\kappa[x, y]$. Então:

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

Assim $x^2 = LT(x^2) \in \langle LT(I)\rangle$.

Contudo x^2 não é divisível por $LT(f_1) = x^3$ nem por $LT(f_2) = x^2y$, portanto, $x^2 \notin \langle LT(f_1), LT(f_2)\rangle$ pelo Lema 1.21.

Provemos então que o ideal gerado pelos termos líderes é um ideal monomial.

Proposição 1.26. *Seja $I \subseteq \kappa[x_1, \ldots, x_n]$ um ideal não-nulo.*

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

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

Demonstração. Sejam $LM(g)$ os monômios líder dos elementos $g \in I \setminus \{0\}$. Esses monômios geram o ideal monomial $\langle LM(g) \mid g \in I \setminus \{0\}\rangle$.

Como para qualquer $cx^\alpha \in \langle LT(g) \mid g \in I \setminus \{0\}\rangle$, com $0 \neq c \in \kappa$, temos que $c^{-1}cx^\alpha \in \langle LT(g) \mid g \in I \setminus \{0\}\rangle$, $c^{-1}cx^\alpha = x^\alpha \in \langle LM(g) \mid g \in I \setminus \{0\}\rangle$, então temos:

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

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

Logo, $\langle LT(I)\rangle = \langle LT(g) \mid g \in I \setminus \{0\}\rangle$ é também um ideal monomial.

Como $\langle LT(I)\rangle$ é um ideal monomial, então é gerado pelos monômios $LM(g)$ para $g \in I \setminus \{0\}$.

Assim, pelo Lema de Dickson, $\langle LT(I)\rangle = \langle LM(g_1), \ldots, LM(g_t)\rangle$ para alguns $g_1, \ldots, g_t \in I$. Como $LM(g_i)$ e $LT(g_i)$ diferem apenas por um coeficiente não-nulo $LC(g_i) \in \kappa$, segue que:

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

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

Com os resultados já demonstrados poderemos apresentar uma prova construtiva do seguinte resultado importantíssimo de Álgebra Comutativa, que já havíamos mencionado, e que possibilitará responder também a um questionamento anterior, a saber, se todo ideal polinomial possui uma base geradora finita.

Teorema 1.27 (Teorema da Base de Hilbert)**.** *Todo ideal $I \subseteq \kappa[x_1, \ldots, x_n]$ possui um conjunto gerador finito. Em outras palavras, $I = \langle g_1, \ldots, g_t \rangle$ para alguns $g_1, \ldots, g_t \in I$.*

Demonstração. Se $I = \{0\}$, então não há nada a provar.

Se I possui algum polinômio não-nulo, então podemos construir um conjunto gerador finito para I da seguinte forma:
Primeiramente fixamos uma ordem monomial $>$. Associado à ordem, calculamos o ideal de termos líderes $\langle LT(I) \rangle$. Pela Proposição 1.26, existem $g_1, \ldots, g_t \in I$ tais que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Afirmamos que $I = \langle g_1, \ldots, g_t \rangle$. Está claro que $\langle g_1, \ldots, g_t \rangle \subseteq I$ já que cada $g_i \in I$.

Reciprocamente, seja um polinômio qualquer $f \in I$. Então dividindo f por $(g_1, \ldots, g_t)$, podemos expressar f, pelo Algoritmo da Divisão na forma $f = q_1 g_1 + \cdots + q_t g_t + r$, onde nenhum termo de r é divisível por algum dos $LT(g_1), \ldots, LT(g_t)$.

Note que $r = f - q_1 g_1 - \cdots - q_t g_t \in I$. Se $r \neq 0$, então teríamos $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Mas então, pelo Lema 1.21 seguiria que $LT(r)$ deve ser divisível por algum $LT(g_i)$. Dessa contradição segue que $r = 0$.

Portanto $f = q_1 g_1 + \cdots + q_t g_t \in \langle g_1, \ldots, g_t \rangle$, mostrando que $I \subseteq \langle g_1, \ldots, g_t \rangle$. Logo a afirmação está provada. ■

Podemos enfim, definir Base de Gröbner de um ideal polinomial.

Definição 1.28. Fixada uma ordem monomial sobre $\kappa[x_1, \ldots, x_n]$. Um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal $I \subseteq \kappa[x_1, \ldots, x_n]$ não-nulo é dito ser uma base de Gröbner se

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

O resultado seguinte é consequência imediata do Teorema da Base de Hilbert e da definição de Base de Gröbner.

Corolário 1.29. *Fixada uma ordem monomial sobre $\kappa[x_1, \ldots, x_n]$. Todo ideal $I \subseteq \kappa[x_1, \ldots, x_n]$ possui 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 da Base de Hilbert é uma base de Gröbner para I por definição.

Note agora que se $\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle$ então, como argumentado na prova do Teorema da Base de Hilbert, temos que $I = \langle g_1, \ldots, g_t \rangle$. Portanto o conjunto G é uma base para I. ■

Podemos então estudar algumas propriedades importantes sobre a Base de Gröbner de um ideal, permitindo, inclusive, responder um questionamento anterior sobre a existência de um conjunto de polinômios para os quais tenhamos a unicidade do resto, independente da ordem dos polinômios divisores.

Proposição 1.30. *Seja $I \subseteq \kappa[x_1, \ldots, x_n]$ um ideal e $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para I. Então dado $f \in \kappa[x_1, \ldots, x_n]$, existe um único $r \in \kappa[x_1, \ldots, x_n]$ com as seguintes propriedades:*

(i) *Nenhum termo de r é divisível por algum dos $LT(g_1), \ldots, LT(g_t)$.*

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

Em particular, r é o resto na divisão de f por $G = (g_1, \ldots, g_t)$ não importando como os elementos de G estão listados.

Demonstração. Da divisão de f por G obtemos $f = q_1 g_1 + \cdots + q_t g_t + r$, onde r satisfaz (i).

Para satisfazer (ii) basta tomar $g = q_1 g_1 + \cdots + q_t g_t$. Assim a existência de r está provada.

Para provar a unicidade, suponhamos que $f = g + r = g' + r'$ satisfazendo (i) e (ii).

Então $r - r' = g' - g \in I$, de modo que se $r - r' \neq 0$ então teríamos $LT(r - r') \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Mas pelo Lema 1.21, seguiria que $LT(r - r')$ seria divisível por algum $LT(g_i)$. Absurdo, já que nenhum dos termos de r, r' é divisível por algum $LT(g_i)$. Logo $r - r' = 0$, e a unicidade está provada. ■

Como havíamos comentado anteriormente, o fato de termos $r = 0$ no Algoritmo da Divisão é condição suficiente mas não necessária para dizer que um polinômio dado pertence ao ideal gerado pelos polinômios divisores. Lembre que essa afirmação decorre do fato de podermos ter restos distintos de acordo com a ordem em que os polinômios divisores são listados.

Contudo, o resultado seguinte nos permite saber exatamente se um polinômio f pertence a dado ideal, bastando para isso proceder à divisão do mesmo pelos polinômios da Base de Gröbner do ideal dado.

Corolário 1.31. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subseteq \kappa[x_1, \ldots, x_n]$ e seja $f \in \kappa[x_1, \ldots, x_n]$. Então $f \in I$ se, e somente se o resto na divisão de f por G é nulo.*

Demonstração. Se $r = 0$, então, como visto anteriormente, já seria suficiente para termos $f \in I$.

Reciprocamente, dado $f \in I$ então escrevendo $f = f + 0$ satisfazemos as duas condições da Proposição 1.30. Assim, como o resto é único na divisão de f por G, segue que $r = 0$. ■

As definições seguintes são importantes para a construção do Critério de Buchberger que veremos adiante, o qual será uma ferramenta de grande utilidade para a construção do algoritmo que possibilite encontrar uma Base de Gröbner para um ideal dado.

Definição 1.32. Denotaremos por $\overline{f}^F$ o resto na divisão de f pela s-úpla ordenada $F = (f_1, \ldots, f_s)$. Note que se F é uma base de Gröbner para $\langle f_1, \ldots, f_s \rangle$, pela Proposição 1.30 podemos considerar F independente da ordem dos f_i.

Vejamos um exemplo para esclarecer essa definição, seja $F = (x^2y - y^2, x^4y^2 - y^2) \subseteq \kappa[x, y]$ e $f = x^5y$. Então realizando a divisão de f por F, fixando $>_{lex}$, obtemos:

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

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

Definição 1.33. Sejam $f, g \in \kappa[x_1, \ldots, x_n]$ polinômios não-nulos.

(i) Se $\text{multideg}(f) = \alpha$ e $\text{multideg}(g) = \beta$, então tome $\gamma = (\gamma_1, \ldots, \gamma_n)$, onde $\gamma_i = max(\alpha_i, \beta_i)$ para cada $1 \leq i \leq n$. Chamamos x^γ de mínimo múltiplo comum de $LM(f)$ e $LM(g)$, e escrevemos $x^\gamma = \text{lcm}(LM(f), LM(g))$.

(ii) O $S-$polinômio de f e g é: $S(f, g) = \dfrac{x^\gamma}{LT(f)} \cdot f - \dfrac{x^\gamma}{LT(g)} \cdot g$.

Vale comentar que o nome "$S-$polinômio" vêm do termo $Syzygy$ polinomial. Veja [2, Definição 2, pág 110].

Vejamos um exemplo para calcular o $S-$polinômio de um par de polinômios dados:

Sejam $f = x^3y^2 - x^2y^3 + x$ e $g = 3x^4y + y^2$ em $\mathbb{R}[x, y]$ com a ordem $> lex$. Então $\gamma = (4, 2)$ e

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

$$S(f, g) = x(x^3y^2 - x^2y^3 + x) - (1/3)y(3x^4y + y^2)$$

$$S(f, g) = -x^3y^3 + x^2 - (1/3)y^3.$$

O Lema seguinte será importante na demonstração do Critério de Buchberger adiante.

Lema 1.34. *Suponha que temos uma soma* $\sum_{i=1}^{s} c_i f_i$, *com* $c_i \in \kappa$, *onde* $\text{multideg}(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ $\forall$ i. *Se* $\text{multideg}\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$, *então* $\sum_{i=1}^{s} c_i f_i$ *é uma combinação linear, com coeficientes em* κ, *dos* $S-$*polinômios* $S(f_j, f_k)$ *para* $1 \leq j, k \leq s$. *Além disso cada* $S(f_j, f_k)$ *tem* $\text{multideg} < \delta$.

Demonstração. Seja $d_i = LC(f_i)$, de modo que $c_i d_i x^\delta$ é o termo líder de $c_i f_i$ para cada i. Como $\text{multideg}(c_i f_i) = \delta$ e o multigrau de $\sum_{i=1}^{s} c_i f_i$ é estritamente menor que δ, segue que

$\sum_{i=1}^{s} c_i d_i = 0$, pois do contrário teríamos $LT\left(\sum_{i=1}^{s} c_i f_i\right) = \left(\sum_{i=1}^{s} c_i d_i\right) x^\delta$ e assim o multigrau seria igual a δ. Seja p_i o polinômio mônico $\frac{f_i}{d_i}$. Então

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

Como $LT(f_i) = d_i x^\delta$ para cada i, temos $\operatorname{lcm}(LM(f_j), LM(f_k)) = x^\delta$ para $1 \leq j, k \leq s$. Assim:

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

Como $\sum_{i=1}^{s} c_i d_i = 0$, então resulta que:

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

Como $LT(p_i) = x^\delta \ \forall\, i$, segue que $\operatorname{multideg}(S(f_j, f_k)) = \operatorname{multideg}(p_j - p_k) < \delta$. ■

Com os resultados já demonstrados, estamos aptos para compreender a demonstração do Critério de Buchberger, que nos permite saber se um conjunto de polinômios formam uma Base de Gröbner de um ideal.

Teorema 1.35 (Critério de Buchberger)**.** *Seja $I \subseteq \kappa[x_1, \ldots, x_n]$ um ideal. Então um conjunto de geradores $G = \{g_1, \ldots, g_t\}$ para I é uma base de Gröbner para I se, e somente se para todos os pares $i \neq j$, o resto na divisão de $S(g_i, g_j)$ por G (listado em alguma ordem) é zero.*

Demonstração. ($\Rightarrow$) Se G é uma base de Gröbner, então $S(g_i, g_j) \in I$, já que é combinação de pares de polinômios de G, e segue pelo Corolário 1.31 que $\overline{S(g_i, g_j)}^{G} = 0$.

($\Leftarrow$) Seja $f \in I$ não-nulo. Devemos mostrar que $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Dado que G é uma conjunto de geradores, existem $h_i \in \kappa[x_1, \ldots, x_n]$ tais que

$$f = \sum_{i=1}^{t} h_i g_i \tag{1.1}$$

Do Lema 1.17 sabemos que $\operatorname{multideg}(f) \leq max(\operatorname{multideg}(h_i g_i) \mid h_i g_i \neq 0)$.

Definamos $H = \{(h_1, \ldots, h_t) \in \kappa^t[x_1, \ldots, x_n] \mid f = \sum h_i g_i\}$. Para todo $h \in H$ considere $\delta_i(h) = \operatorname{multideg}(h_i g_i)$, $\delta(h) = max\{\delta_i(h)\}$ e $\delta = \min_{h \in H} \delta(h)$. Assim $\operatorname{multideg}(f) \leq \delta$.

Escolhido esse δ, mostremos que $\operatorname{multideg}(f) = \delta$. Suponhamos, por contradição, que

$\text{multideg}(f) < \delta$. Então poderíamos escrever f da seguinte forma

$$\begin{aligned} f = \sum_{\delta_i=\delta} h_i g_i + \sum_{\delta_i<\delta} h_i g_i &= \sum_{\delta_i=\delta} (h_i g_i + LT(h_i)g_i - LT(h_i)g_i) + \sum_{\delta_i<\delta} h_i g_i \\ &= \sum_{\delta_i=\delta} (LT(h_i)g_i + (h_i - LT(h_i))g_i) + \sum_{\delta_i<\delta} h_i g_i \\ &= \sum_{\delta_i=\delta} LT(h_i)g_i + \sum_{\delta_i=\delta} (h_i - LT(h_i))g_i + \sum_{\delta_i<\delta} h_i g_i. \end{aligned} \tag{1.2}$$

Observe que a segunda soma em (1.2) tem multigrau menor que δ, já que pelo Lema 1.17:

$$\begin{aligned} \text{multideg}((h_i - LT(h_i))g_i) &= \text{multideg}(h_i - LT(h_i)) + \text{multideg}(g_i) \\ &< \text{multideg}(h_i) + \text{multideg}(g_i) = multideg(h_i g_i) = \delta_i = \delta. \end{aligned}$$

Como o mesmo vale para a terceira soma, então a primeira soma em (1.2) também deve ter multigrau menor que δ. Seja $LT(h_i) = a_i x^{\alpha_i}$. Então, pelo Lema 1.34, $\sum_{\delta_i=\delta} LT(h_i)g_i$, pode ser escrita como combinação linear dos $S-$polinômios $S(x^{\alpha_j} g_j, x^{\alpha_k} g_k)$. Como $S(x^{\alpha_j} g_j, x^{\alpha_k} g_k) = \dfrac{x^\delta}{x^{\alpha_j} LT(g_j)} \cdot (x^{\alpha_j} g_j) - \dfrac{x^\delta}{x^{\alpha_k} LT(g_k)} \cdot (x^{\alpha_k} g_k) = \dfrac{x^\delta}{LT(g_j)} \cdot g_j - \dfrac{x^\delta}{LT(g_k)} \cdot g_k$ $= \dfrac{x^\delta}{x^{\gamma_{jk}}} \cdot \dfrac{x^{\gamma_{jk}}}{LT(g_j)} \cdot g_j - \dfrac{x^\delta}{x^{\gamma_{jk}}} \cdot \dfrac{x^{\gamma_{jk}}}{LT(g_k)} \cdot g_k = x^{\delta - \gamma_{jk}} S(g_j, g_k)$, onde $\gamma_{jk} = \text{lcm}(LM(g_j), LM(g_k))$, então, existem $c_{jk} \in \kappa$ tais que

$$\sum_{\delta_i=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) \tag{1.3}$$

Agora para cada $S-$polinômio, por hipótese do Teorema, temos que $\overline{S(g_j, g_k)}^G = 0$. Assim podemos escrever cada $S(g_j, g_k)$ como

$$S(g_j, g_k) = \sum_{i=1}^{t} q_{ijk} g_i, \tag{1.4}$$

para alguns $q_{ijk} \in \kappa[x_1, \ldots, x_n]$. Temos ainda, pelo Algoritmo da Divisão, que:

$$\text{multideg}(q_{ijk} g_i) \leq \text{multideg}(S(g_j, g_k)) \tag{1.5}$$

Assim,

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

e fazendo $b_{ijk} = x^{\delta-\gamma_{jk}} q_{ijk}$, obtemos:

$$x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i \tag{1.6}$$

Observe que:

$$\begin{aligned}\text{multideg}(b_{ijk}g_i) &= \text{multideg}(x^{\delta-\gamma_{jk}} q_{ijk} g_i) = \text{multideg}(x^{\delta-\gamma_{jk}}) + \text{multideg}(q_{ijk}g_i) \\ &\overset{(1.5)}{\leq} \text{multideg}(x^{\delta-\gamma_{jk}}) + \text{multideg}(S(g_j, g_k)) = \\ &= \text{multideg}(x^{\delta-\gamma_{jk}} S(g_j, g_k)) = \text{multideg}(S(x^{\alpha_j} g_j, x^{\alpha_k} g_k)) < \delta.\end{aligned}$$

Assim, substituindo (1.6) em (1.3) resulta:

$$\sum_{\delta_i=\delta} LT(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk} \left(\sum_{i=1}^{t} b_{ijk} g_i \right) = \sum_{\gamma} \tilde{h_\gamma} g_\gamma$$

onde $\text{multideg}(\tilde{h_\gamma} g_\gamma) < \delta$ para todo γ.

Finalmente, substituindo esse resultado em (1.2) obtemos:

$$f = \sum_{\gamma} \tilde{h_\gamma} g_\gamma + \sum_{\delta_i=\delta} (h_i - LT(h_i)) g_i + \sum_{\delta_i<\delta} h_i g_i.$$

Assim, obtemos uma expressão para f como combinação dos polinômios g_i onde cada termo tem multigrau menor que δ, o que contradiz a minimalidade de δ.

Logo $\text{multideg}(f) = \delta$, e segue que $\text{multideg}(f) = \delta = \delta_i(h) = \text{multideg}(h_i g_i)$ para algum $i \in \{1, \ldots, t\}$.

Assim $LM(f) = LM(h_i g_i)$, isto é, $LM(f)$ é múltiplo de $LM(g_i)$ e portanto $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$, como queríamos mostrar. ■

Vejamos a seguir um exemplo para aplicação do Critério de Buchberger com o intuito de obtermos uma Base de Gröbner para o ideal dado:

Sejam $g_1 = x^3 - 2xy$ e $g_2 = x^2y - 2y^2 + x$ em $\kappa[x, y]$. Considerando $I = \langle g_1, g_2 \rangle$ e $G = \{g_1, g_2\}$ com a ordem $>_{grlex}$.

Calculemos os $S-$polinômios para cada par de polinômios e verifiquemos se o resto da divisão pelos polinômios do conjunto G é nulo, já que esta é a condição necessária pelo Critério de Buchberger.

Note que não precisamos calcular $S(g_1, g_2)$ e $S(g_2, g_1)$ já este último resultaria apenas no polinômio oposto do primeiro, ou seja, com os sinais dos coeficientes opostos.

$S(g_1, g_2) = \dfrac{x^3 y}{x^3}(x^3 - 2xy) - \dfrac{x^3 y}{x^2 y}(x^2 y - 2y^2 + x) = -x^2$, e $\overline{-x^2}^G = -x^2 \neq 0$.

Portanto $G = \{g_1, g_2\}$ não é base de Gröbner para I.

Façamos então $g_3 = -x^2$ e $G = \{g_1, g_2, g_3\}$. Assim:

$S(g_1, g_2) = -x^2$ e agora $\overline{-x^2}^G = 0$

Agora calculemos para o segundo par:

$S(g_1, g_3) = \frac{x^3y}{x^3}(x^3 - 2xy) - \frac{x^3y}{-x^2}(-x^2) = -2xy$ e $\overline{-2xy}^G = -2xy \neq 0$.

Portanto $G = \{g_1, g_2, g_3\}$ não é base de Gröbner para I.

Façamos $g_4 = -2xy$ e $G = \{g_1, g_2, g_3, g_4\}$. Assim:

$S(g_1, g_2) = -x^2$ e $\overline{(-x^2)}^G = 0$

$S(g_1, g_3) = -2xy$ e agora $\overline{(-2xy)}^G = 0$

$S(g_1, g_4) = \frac{x^3y}{x^3}(x^3 - 2xy) - \frac{x^3y}{-2xy}(-2xy) = -2xy^2$ e $\overline{(-2xy^2)}^G = 0$

$S(g_2, g_3) = \frac{x^2y}{x^2y}(x^2y - 2y^2 + x) - \frac{x^2y}{-x^2}(-x^2) = -2y^2 + x$ e $\overline{(-2y^2 + x)}^G = -2y^2 + x \neq 0$

Portanto $G = \{g_1, g_2, g_3, g_4\}$ não é base de Gröbner para I.

Façamos $g_5 = -2y^2 + x$ e $G = \{g_1, g_2, g_3, g_4, g_5\}$. Assim:

$S(g_1, g_2) = -x^2$ e $\overline{(-x^2)}^G = 0$

$S(g_1, g_3) = -2xy$ e $\overline{(-2xy)}^G = 0$

$S(g_1, g_4) = -2xy^2$ e $\overline{(-2xy^2)}^G = 0$

$S(g_1, g_5) = \frac{x^3y^2}{x^3}(x^3 - 2xy) - \frac{x^3y^2}{-2y^2}(-2y^2 + x) = -2xy^3 + \frac{1}{2}x^4$ e $\overline{(-2xy^3 + \frac{1}{2}x^4)}^G = 0$

$S(g_2, g_3) = -2y^2 + x$ e agora $\overline{(-2y^2 + x)}^G = 0$

$S(g_2, g_4) = \frac{x^2y}{x^2y}(x^2y - 2y^2 + x) - \frac{x^2y}{-2xy}(-2xy) = -2y^2 + x$ e $\overline{(-2y^2 + x)}^G = 0$

$S(g_2, g_5) = \frac{x^2y^2}{x^2y}(x^2y - 2y^2 + x) - \frac{x^2y^2}{-2y^2}(-2y^2 + x) == -2y^3 + xy + \frac{1}{2}x^3$ e $\overline{(-2y^3 + xy + \frac{1}{2}x^3)}^G = 0$

$S(g_3, g_4) = \frac{x^2y}{-x^2}(-x^2) - \frac{x^2y}{-2xy}(-2xy) = 0$ e $\overline{(0)}^G = 0$

$S(g_3, g_5) = \frac{x^2y^2}{-x^2}(-x^2) - \frac{x^2y^2}{-2y^2}(-2y^2 + x) = \frac{1}{2}x^3$ e $\overline{(\frac{1}{2}x^3)}^G = 0$

$S(g_4, g_5) = \frac{xy^2}{-2xy}(-2xy) - \frac{xy^2}{-2y^2}(-2y^2 + x) = \frac{1}{2}x^2$ e $\overline{(\frac{1}{2}x^2)}^G = 0$

Nesse caso obtivemos $\overline{S(g_i, g_j)}^G = 0$ para todo $i \neq j$ com $1 \leq i, j \leq 5$.

Portanto $G = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$ é uma base de Gröbner para $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$.

Uma vez demonstrado e exemplificado o Critério de Buchberger podemos provar o Algoritmo de Buchberger, que permite obter uma Base de Gröbner para um ideal polinomial dado.

Nesse algoritmo, declaramos os polinômios candidatos à base de Gröbner e inicializamos a possível base G com esses polinômios. Em seguida inicializamos um conjunto auxiliar G', o qual será utilizado para calcular os $S-$polinômios. Note que o critério de parada do algoritmo

é justamente quando todos os restos da divisão de cada $S-$polinômio pelos polinômios que estão no conjunto auxiliar G' for nulo. Para isso, cada vez que este resto não é nulo para algum $S-$polinômio, atualizamos G adicionando esse resto não-nulo, ou seja $G = G \cup \{r\}$. E repetimos o processo atualizando também o conjunto auxiliar $G' = G$.

Se em algum passo todos os restos forem nulos, então a igualdade $G = G'$ será verdadeira, já que nenhum resto terá sido adicionado a G e o algoritmo encerra.

Provaremos o funcionamento desse algoritmo, isto é, que, de fato, em algum passo esse resto será nulo para cada $S-$polinômio e teremos assim uma Base de Gröbner.

Teorema 1.36 (Algoritmo de Buchberger)**.** *Seja $I = \langle f_1, \ldots, f_s \rangle$ um ideal polinomial não-nulo. Então uma base de Gröbner para I pode ser construída em um número finito de passos pelo seguinte algoritmo:*

Input: $F = (f_1, \ldots, f_s)$
Output: uma base de Gröbner $G = (g_1, \ldots, g_t)$ *para* I*, com* $F \subseteq G$
$G := F$
REPEAT
$G' := G$
FOR cada par p, q*,* $p \neq q$ *em* G' *DO*
$r := \overline{S(p,q)}^{G'}$
IF $r \neq 0$ *THEN* $G := G \cup \{r\}$
UNTIL $G = G'$
RETURN G

Demonstração. Seja $G = \{g_1, \ldots, g_t\}$ então:

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

Mostremos que $G \subseteq I$ em cada estágio do algoritmo.

Isso é claramente verdade inicialmente, já que $G = F \subseteq I$. Suponhamos que em dada etapa temos $G \subseteq I$. Então, para $p, q \in G'$, com $p \neq q$, temos que $r = \overline{S(p,q)}^{G'} \in I$ já que $S(p,q) = q_1 g_1 + \cdots + q_t g_t + \overline{S(p,q)}^{G'}$.

Assim:

$$\overline{S(p,q)}^{G'} = S(p,q) - (q_1 g_1 + \cdots + q_t g_t) \in I.$$

Então no passo seguinte, adicionando r a G, obtemos $G := G \cup \{r\} \subseteq I$. Note ainda que, como G contém o conjunto F, então G possui os polinômios que determinam I. O algoritmo termina quando $G = G'$, ou seja, quando $\overline{S(p,q)}^{G'} = 0$ para todo par $\{p, q\}$.

Pelo Critério de Buchberger segue então que G é uma base de Gröbner para $I = \langle G \rangle$.

Resta mostrar que o algoritmo, de fato, termina.

Considerando o que ocorre em cada passo temos que o conjunto G consiste de G' (o antigo G) juntamente com os restos não-nulos de $S-$polinômios na divisão por G'. De modo

$\langle LT(G')\rangle \subseteq \langle LT(G)\rangle$, já que $G' \subseteq G$. Além disso, se $G' \neq G$, então $\langle LT(G')\rangle \subsetneq \langle LT(G)\rangle$, uma vez que se um resto não-nulo r foi adicionado a G então $LT(r)$ não é divisível por nenhum dos termos líderes dos elementos de G', e desse modo $LT(r) \notin \langle LT(G')\rangle$. Mas $LT(r) \in \langle LT(G)\rangle$.

Assim, de $\langle LT(G')\rangle \subseteq \langle LT(G)\rangle$, vemos que os ideais $\langle LT(G')\rangle$ formam uma cadeia ascendente de ideais em $\kappa[x_1, \ldots, x_n]$:

$$\langle LT(G'_1)\rangle \subseteq \langle LT(G'_2)\rangle \subseteq \cdots$$

Como $\kappa[x_1, \ldots, x_n]$ é anel noetheriano [10, Teorema 6.2.1], então a condição de cadeia ascendente de ideais garante que após um número finito $N \geq 1$ de iterações essa cadeia estabilizará, de modo que eventualmente teremos $\langle LT(G'_N)\rangle = \langle LT(G'_{N+1})\rangle = \cdots$.

Portanto teremos $\langle LT(G'_N)\rangle = \langle LT(G)\rangle$, e assim $G' = G$, em um número finito de passos. ■

O lema seguinte será importante para a definição de uma Base de Gröbner reduzida para um ideal polinomial, que veremos logo adiante.

Lema 1.37. *Seja G uma base de Gröbner para um ideal $I \subseteq \kappa[x_1, \ldots, x_n]$. Seja $p \in G$ um polinômio tal que $LT(p) \in \langle LT(G \setminus \{p\})\rangle$. Então $G \setminus \{p\}$ é também uma base de Gröbner para I.*

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

Definição 1.38. Uma base de Gröbner reduzida para um ideal polinomial I é uma base de Gröbner G para I tal que:

(i) $LC(p) = 1$ para todo $p \in G$;

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

Vale observar, neste momento, que cada um dos diversos softwares de aplicação matemática como o Macaulay, Singular, Magma, *Mathematica*, bem como o SageMath, que estamos utilizando em nosso trabalho, tem rotinas e comandos próprios para calcular a Base de Gröbner de um ideal polinomial declarado.

Para aplicar ao exemplo já visto onde calculamos uma Base de Gröbner para o ideal $I = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$, vejamos então o comando e o retorno apresentado, em SageMath:

```
SageMath version 9.3 Console

sage: P.<x, y> = PolynomialRing(QQ, 2, order = "deglex")
sage: f_1 = x^3 - 2*x*y
```

```
sage: f_2 = x^2*y - 2*y^2 + x
sage: I = ideal([f_1, f_2])
sage: G = I.groebner_basis('toy:buchberger')
sage: print(G)
[x^3 - 2*x*y, x^2*y - 2*y^2 + x, x^2, x*y, y^2 - 1/2*x]
sage:
```

Note que na primeira linha declaramos o anel de polinômios com o qual vamos trabalhar, neste exemplo $\mathbb{Q}[x, y]$, bem como a ordem monomial fixada que será a ordem lexicográfica graduada $>_{grlex}$ que em SageMath se denota por $deglex$. Em seguida declaramos os polinômios f_1 e f_2 geradores do ideal I, e em seguida geramos este ideal com o comando $I = ideal([f_1, f_2])$. Prosseguindo, o comando que calcula uma Base de Gröbner para o ideal dado é $I.groebner\_basis('toy : buchberger')$. Observe ainda que o comando $'toy : buchberger'$ indica que estamos computando uma base pelo Critério de Buchberger, como visto no exemplo anterior, que não é uma base reduzida, pois se omitirmos esse comando a base obtida será uma base reduzida.

Finalmente, visualizamos a Base de Gröbner para o ideal I:
$G = \{x^3 - 2xy, x^2y - 2xy^2 + x, x^2, xy, y^2 - (1/2)x\}$

Observe que o software SageMath retorna, por padrão, uma Base de Gröbner com os polinômios todos mônicos. Daí as diferenças entre os coeficientes de alguns dos polinômios que calculamos no exemplo e os retornados pelo SageMath.

CAPÍTULO 2

INTRODUÇÃO À GEOMETRIA ALGÉBRICA

Neste capítulo veremos as definições de espaço afim e de variedades afim, bem como conceitos importantes de Geometria Algébrica com o objetivo de termos as ferramentas necessárias para o cálculo da dimensão de uma variedade afim determinada por um ideal polinomial. É importante observar que esses conceitos se apoiam em resultados notadamente conhecidos de Álgebra Comutativa.

2.1 Espaço Afim e Variedades

Iniciaremos esta seção com as definições de espaço afim $n-$dimensional e variedade afim nesse espaço.

Definição 2.1. Dado um corpo κ e um inteiro positivo n, definimos o espaço afim $n-$dimensional sobre κ como sendo o conjunto

$$\mathbb{A}^n(\kappa) = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \kappa\}$$

Como exemplo de espaço afim, podemos considerar o caso em que $\kappa = \mathbb{R}$. Nesse caso obtemos o espaço $\mathbb{R}^n$ com o qual se trabalha em Álgebra Linear.
Note ainda que podemos relacionar polinômios ao espaço afim, observando que um polinômio $f = \sum_\alpha a_\alpha x^\alpha$ do anel de polinômios $\kappa[x_1, \ldots, x_n]$ nos fornece uma função polinomial $f : \mathbb{A}^n(\kappa) \to \kappa$ definida por $f(a_1, \ldots, a_n) \in \kappa$.

Definição 2.2. Seja κ um corpo e sejam $f_1, \ldots, f_s$ polinômios em $\kappa[x_1, \ldots, x_n]$. Então o conjunto $\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n(\kappa) \mid f_i(a_1, \ldots, a_n) = 0 \ \forall \ 1 \leq i \leq s\}$ é chamado de variedade afim definida por $f_1, \ldots, f_s$.

O Lema seguinte caracteriza a união e interseção de variedades afins e a proposição adiante o ideal de uma variedade.

Lema 2.3. *Se $V, W \subseteq \mathbb{A}^n(\kappa)$ são variedades afins, então são também $V \cup W$ e $V \cap W$.*

Demonstração. Veja [2, pág 11].

Proposição 2.4. *Seja $V \subseteq \mathbb{A}^n(\kappa)$ uma variedade afim. Então o conjunto*

$$\boldsymbol{I}(V) = \{f \in \kappa[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \forall \ (a_1, \ldots, a_n) \in V\}$$

é um ideal, chamado o ideal de V.

Demonstração. Veja [4, pág 20].

Note que tomando polinômios $f_1, \ldots, f_s \in \kappa[x_1, \ldots, x_n]$, obtemos a variedade $\mathbf{V}(f_1, \ldots, f_s)$ determinada por eles, e em seguida podemos obter o ideal dessa variedade $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$. Então surge um questionamento natural: será que sempre $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$?

Podemos estudar uma variedade $V \subseteq \mathbb{A}^n(\kappa)$ passando para o ideal de todos os polinômios que se anulam nela:

$$\mathbf{I}(V) = \{f \in \kappa[x_1, \ldots, x_n] \mid f(a) = 0 \ \forall \ a \in V\}.$$

Desse modo, conseguimos uma relação $V \to \mathbf{I}(V)$. Por outro lado, dado um ideal $I \subseteq \kappa[x_1, \ldots, x_n]$ podemos definir o conjunto:

$$\mathbf{V}(I) = \{a \in \mathbb{A}^n(\kappa) \mid f(a) = 0 \ \forall f \in I\}.$$

Esse conjunto é, de fato, uma variedade, já que pelo Teorema 1.27 existem $f_1, \ldots, f_s \in I$ tais que $I = \langle f_1, \ldots, f_s \rangle$. Assim $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$. De modo que também temos uma relação $I \to \mathbf{V}(I)$.

Lema 2.5. *Sejam $f_1, \ldots, f_s \in \kappa[x_1, \ldots, x_n]$. Então $\langle f_1, \ldots, f_s \rangle \subseteq \boldsymbol{I}(\boldsymbol{V}(f_1, \ldots, f_s))$.*

Demonstração. Veja [2, pág 34].

Note que podemos ter $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ estritamente maior que $\langle f_1, \ldots, f_s \rangle$. Seja $\langle x^2, y^2 \rangle$, verifiquemos que a inclusão $\langle x^2, y^2 \rangle \subseteq \mathbf{I}(\mathbf{V}(x^2, y^2))$ não é uma igualdade. Com efeito, calculemos $\mathbf{I}(\mathbf{V}(x^2, y^2))$. Temos das equações $x^2 = y^2 = 0$ que $\mathbf{V} = \{(0, 0)\}$.
Contudo, podemos verificar que $\mathbf{I}(\{(0, 0)\}) = \langle x, y \rangle$, ou seja, $\mathbf{I}(\mathbf{V}(x^2, y^2)) = \langle x, y \rangle$. Com efeito, a primeira direção da igualdade é trivial, já que qualquer polinômio da forma $A(x, y)x +$

$B(x,y)y$ se anula na origem. Reciprocamente, suponha que $f = \sum_{i,j} a_{ij}x^i y^j$ se anula na origem. Então o termo constante deve ser nulo $a_{00} = f(0,0) = 0$ e consequentemente:

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

Mas, note que o ideal $\langle x,y\rangle$ é estritamente maior que $\langle x^2,y^2\rangle$, já que, por exemplo $x \notin \langle x^2,y^2\rangle$.

A proposição seguinte mostra um fato importante sobre o comportamento de reversão de inclusão quando aplicamos **I** a duas variedades.

Proposição 2.6. *Sejam V e W variedades afins em $\mathbb{A}^n(\kappa)$. Então:*

$$V \subseteq W \Leftrightarrow \boldsymbol{I}(V) \supseteq \boldsymbol{I}(W).$$

Demonstração. Veja [4, pág 20].

O lema seguinte será importante para as definições e resultados relacionados a ideais radicais adiante.

Lema 2.7. *Seja V uma variedade. Se $f^m \in \boldsymbol{I}(V)$, então $f \in \boldsymbol{I}(V)$.*

Demonstração. Seja $a \in V$. Se $f^m \in \mathbf{I}(V)$, então $(f(a))^m = 0$. Mas isso ocorre somente se $f(a) = 0$. Como $a \in V$ é arbitrário, devemos ter $f \in \mathbf{I}(V)$. ■

Definição 2.8. Seja $I \subseteq \kappa[x_1,\ldots,x_n]$ um ideal. O radical de I, denotado por $\sqrt{I}$, é o conjunto $\{f \mid f^m \in I \text{ para algum inteiro } m \geq 1\}$.

Note que desse modo sempre temos $I \subset \sqrt{I}$ já que $f \in I$ implica que $f^1 \in I$ e, consequentemente, $f \in \sqrt{I}$ por definição.

Definição 2.9. Um ideal I é radical se $I = \sqrt{I}$, ou seja, se $f^m \in I$ para algum inteiro $m \geq 1$ implica que $f \in I$.

Segue imediatamente do Lema 2.7 que $\mathbf{I}(V)$ é um ideal radical.

Lema 2.10. *Se I é um ideal em $\kappa[x_1,\ldots,x_n]$, então $\sqrt{I}$ é um ideal em $\kappa[x_1,\ldots,x_n]$ contendo I.*

Demonstração. Veja [2, pág 182].

Proposição 2.11. *Se I é um ideal de $\kappa[x_1,\ldots,x_n]$, então $\sqrt{I}$ é um ideal radical em $\kappa[x_1,\ldots,x_n]$.*

Demonstração. O lema anterior mostra que $\sqrt{I}$ é um ideal em $\kappa[x_1,\ldots,x_n]$, assim segue que $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$.
Reciprocamente, seja $f \in \sqrt{\sqrt{I}}$, então existe um inteiro m tal que $f^m \in \sqrt{I}$. E assim existem um inteiro l tal que $(f^m)^l \in I \Rightarrow f^{ml} \in I \Rightarrow f \in \sqrt{I}$. Portanto $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$ implicando na igualdade $\sqrt{\sqrt{I}} = \sqrt{I}$. Logo $\sqrt{I}$ é um ideal radical em $\kappa[x_1,\ldots,x_n]$. ■

Nos aproximamos nesse ponto, da relação entre o ideal de uma variedade e seu ideal radical. Para demonstrarmos então a versão forte do Teorema Nullstellensatz, precisamos da versão fraca que nos garante que uma variedade nunca é vazia.

Teorema 2.12 (Nullstellensatz (fraco))**.** *Seja $I \subset \kappa[x_1, \ldots, x_n]$ um ideal e $\overline{\kappa}$ o fecho algébrico de κ. Consideremos I como um subconjunto do anel de polinômios $\overline{\kappa}[x_1, \ldots, x_n]$. Então são equivalentes:*

- $\mathbf{V(I)} = \emptyset$*;*
- $1 \in I$*, isto é,* $I = \kappa[x_1, \ldots, x_n]$.

Demonstração. Veja [4, pág 43].

Teorema 2.13 (Nullstellensatz (forte))**.** *Seja $\kappa = \overline{\kappa}$ e $I \subset \kappa[x_1, \ldots, x_n]$ um ideal. Então:*

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

Demonstração. Afirmamos que sendo $\kappa = \overline{\kappa}$, dados $f, f_1, \ldots, f_s \in \kappa[x_1, \ldots, x_n]$, então $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ se, e somente se $f^m \in \langle f_1, \ldots, f_s \rangle$ para algum $m \geq 1$.
Com efeito, dado um polinômio f que se anula em todo zero comum dos polinômios $f_1, \ldots, f_s$, queremos mostrar que existe um inteiro $m \geq 1$ e polinômios $F_1, \ldots, F_s$ tais que:

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

Considere o ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq \kappa[x_1, \ldots, x_n, y]$. Afirmamos que $\mathbf{V}(\tilde{I}) = \emptyset$. Suponha por absurdo que $\mathbf{V}(\tilde{I}) \neq \emptyset$ e seja $(a_1, \ldots, a_n, a_{n+1}) \in \mathbf{V}(\tilde{I})$. Então $f_i(a_1, \ldots, a_n) = f_i(a_1, \ldots, a_n, a_{n+1}) = 0$, e por hipótese temos que $f(a_1, \ldots, a_n) = 0$. No entanto, temos que $1 - a_{n+1} f(a_1, \ldots, a_n) = 1$. Assim $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$, o que é uma contradição. Portanto $\mathbf{V}(\tilde{I}) = \emptyset$. Aplicando agora o Teorema 2.12 concluímos que $1 \in \tilde{I}$, consequentemente:

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

para alguns polinômios $p_i, q \in \kappa[x_1, \ldots, x_n, y]$. Fazendo $y = 1/f(x_1, \ldots, x_n)$ segue que:

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i$$

Note que existe m suficientemente grande tal que, ao multiplicar por f^m, elimine todos os denominadores e
$f^m = \sum_{i=1}^{s} F_i f_i$ para alguns polinômios $F_i \in \kappa[x_1, \ldots, x_n]$ como se queria.

Para a outra inclusão, note que se $f \in \sqrt{I}$ então $f^m \in I$ para algum $m \geq 1$. Consequentemente, f^m se anula em $\mathbf{V}(I)$, o que implica que f se anula em $\mathbf{V}(I)$. Assim $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$, e concluímos a demonstração. ■

O Teorema 2.13 permite completar a correspondência entre ideais e variedades da forma:

(i) variedades afins $\underset{V}{\overset{I}{\rightleftarrows}}$ ideais, de modo que se $I_1 \subseteq I_2$ então $\mathbf{V}(I_1) \supseteq \mathbf{V}(I_2)$ e se $V_1 \subseteq V_2$ então $\mathbf{I}(V_1) \supseteq \mathbf{I}(V_2)$.

(ii) Para qualquer variedade V, $\mathbf{V}(\mathbf{I}(V)) = V$, e para qualquer ideal I, $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$.

(iii) Quando κ é algebricamente fechado, então as relações I e V, restritas aos ideais radicais, são bijeções que revertem inclusão e inversas uma da outra.

2.2 Fecho de Zariski e Variedades irredutíveis

Nesta seção estudaremos o fecho de Zariski de uma variedade e resultados importantes sobre sua decomposição em componentes irredutíveis e sua correspondência com a decomposição primária do ideal relacionado.

Note que a partir do Teorema 2.12 juntamente com o fato de que se $I \subseteq J$ então $\mathbf{V}(I) \supseteq \mathbf{V}(J)$ e com a seguinte proposição teremos satisfeitos os axiomas para conjuntos fechados de uma topologia sobre $\mathbb{A}^n(\kappa)$.

Proposição 2.14. *Seja $R = \kappa[x_1, \ldots, x_n]$, então:*

- *Se $I, J \in R$ então $\mathbf{V}(I) \cup \mathbf{V}(J) = \mathbf{V}(I \cap J)$.*
  Em particular, toda união finita de variedades afins é uma variedade afim.
- *Se $\{I_\lambda\}$ é uma família de ideais de R então*

$$\bigcap_\lambda \mathbf{V}(I_\lambda) = \mathbf{V}\left(\sum_\lambda I_\lambda\right)$$

  Em particular, a interseção de qualquer família de variedades afins é uma variedade afim.

Demonstração. Veja [5, pág 16].

Desse modo, nessa topologia chamada topologia de Zariski, os conjuntos fechados são as variedades $V \subset \mathbb{A}^n(\kappa)$ e os conjuntos abertos são os complementos $\mathbb{A}^n(\kappa) \setminus V$.

Proposição 2.15. *Se $S \subseteq \mathbb{A}^n(\kappa)$, a variedade afim $\mathbf{V}(I(S))$, onde $I(S) = \{f \in \kappa[x_1, \ldots, x_n] \mid : f(a) = 0 \ \forall \ a \in S\}$, é a menor variedade contendo S, isto é, se $W \subseteq \mathbb{A}^n(\kappa)$ é outra variedade qualquer contendo S então $\mathbf{V}(I(S)) \subseteq W$.*

Demonstração. Seja W uma variedade afim contendo S, assim $W \supseteq S$ e $I(W) \subseteq I(S)$. Daí, segue que $\mathbf{V}(I(W)) \supseteq \mathbf{V}(I(S))$. Como W é uma variedade afim, então $\mathbf{V}(I(W)) = W$ e o resultado segue imediatamente. ■

Definição 2.16. O fecho de Zariski de um subconjunto do espaço afim é a menor variedade algébrica contendo o subconjunto. Se $S \subseteq \mathbb{A}^n(\kappa)$, o fecho de Zariski de S, denotado por $\bar{S}$, é igual a $V(I(S))$.

Para o próximo teorema precisaremos de uma definição de um tipo de ideal, chamado ideal de eliminação.

Definição 2.17. *Dado um ideal $I \subset \kappa[x_1, \ldots, x_n]$ e um inteiro $0 \leq k < n$, o k-ésimo ideal de eliminação de I é o ideal $I_k = I \cap \kappa[x_{k+1}, \ldots, x_n]$. Note que $I_0 = I$ e I_n é um ideal de κ.*

Teorema 2.18 (Teorema do Fecho)**.** *Seja κ algebricamente fechado, $V = V(f_1, \ldots, f_s) \subseteq \mathbb{A}^n(\kappa)$, e seja $\pi_l : \mathbb{A}^n(\kappa) \to \mathbb{A}^{n-l}(\kappa)$ a aplicação polinomial projeção sobre as últimas $n - l$ coordenadas. Se I_l é o $l-$ésimo ideal de eliminação $I_l = \langle f_1, f_2, \ldots, f_s \rangle \cap \kappa[x_{l+1}, \ldots, x_n]$ então $V(I_l)$ é o fecho de Zariski de $\pi_l(V)$.*

Demonstração. Veja [4, pág 36].

Em geral, se V é uma variedade, então dizemos que um subconjunto $S \subseteq V$ é Zariski denso em V se $V = \overline{S}$, isto é, se V é o fecho de Zariski de S. Assim o Teorema 2.18 nos diz que $\pi_l(V)$ é Zariski denso em $V(I_l)$ quando κ é algebricamente fechado.

Para chegarmos à decomposição de uma variedade serão necessárias as definições seguintes.

Definição 2.19. *Uma variedade afim $V \subseteq \mathbb{A}^n(\kappa)$ é dita irredutível se quando V é escrita na forma $V = V_1 \cup V_2$, com V_1 e V_2 variedades afins, então ou $V_1 = V$ ou $V_2 = V$.*

Desse modo, uma variedade V é irredutível se não pode ser expressa como união $V = V_1 \cup V_2$ de variedades afins V_1, V_2 propriamente contidas em V. Caso contrário, V é dita redutível.

Definição 2.20. *Um ideal $I = \kappa[x_1, \ldots, x_n]$ é dito primo se quando $f, g \in \kappa[x_1, \ldots, x_n]$ e $fg \in I$, então $f \in I$ ou $g \in I$.*

Agora, podemos relacionar uma variedade irredutível ao seu ideal.

Proposição 2.21. *Seja $V \subseteq \mathbb{A}^n(\kappa)$ uma variedade afim. Então V é irredutível se, e somente se $\boldsymbol{I}(V)$ é um ideal primo.*

Demonstração. Veja [5, pág 23].

Relembremos a definição de ideal maximal e um resultado importante em seguida.

Definição 2.22. Um ideal $I \in \kappa[x_1, \ldots, x_n]$ é dito maximal se $I \neq \kappa[x_1, \ldots, x_n]$ e para qualquer ideal J que contenha I tenha-se que $J = I$ ou $J = \kappa[x_1, \ldots, x_n]$.

Proposição 2.23. *Se κ é um corpo qualquer, um ideal $I \subseteq \kappa[x_1, \ldots, x_n]$ da forma*

$$I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

é maximal, onde $a_1, \ldots, a_n \in \kappa$.

Demonstração. Suponhamos que J é um ideal contendo estritamente I. Então deve existir $f \in J$ tal que $f \notin I$. Sabemos pelo Algoritmo da Divisão que podemos escrever $f = q_1(x - a_1) + \cdots + q_n(x - a_n) + r$ com $q_1, \ldots, q_n \in \kappa[x_1, \ldots, x_n]$ e $r \in \kappa$. Como $q_1(x - a_1) + \cdots + q_n(x - a_n) \in I$ e $f \notin I$ então $r \neq 0$. Agora, como $f \in J$ e $q_1(x - a_1) + \cdots + q_n(x - a_n) \in I \subset J$, também temos

$$r = f - (q_1(x - a_1) + \cdots + q_n(x - a_n)) \in J.$$

Sendo $r \neq 0$ então $1 = (1/r) \cdot r \in J$ e logo $J = \kappa[x_1, \ldots, x_n]$ ■

Note que como $\mathbf{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$ então todo ponto $(a_1, \ldots, a_n) \in \kappa[x_1, \ldots, x_n]$ corresponde a um ideal maximal $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

Proposição 2.24. *Se κ é um corpo qualquer, um ideal maximal em $\kappa[x_1, \ldots, x_n]$ é primo.*

Demonstração. Veja [2, pág 210].

Agora, poderemos ver que todos os ideais maximais em $\kappa[x_1, \ldots, x_n]$ são exatamente os vistos na Proposição 2.23.

Teorema 2.25. *Se κ é um corpo algebricamente fechado, então todo ideal maximal de $\kappa[x_1, \ldots, x_n]$ é da forma $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ para alguns $a_1, \ldots, a_n \in \kappa$.*

Demonstração. Seja $I \subseteq \kappa[x_1, \ldots, x_n]$ maximal. Então $I \neq \kappa[x_1, \ldots, x_n]$ e segue pelo Teorema 2.12 que $\mathbf{V}(I) \neq \emptyset$. Assim existe algum ponto $(a_1, \ldots, a_n) \in \mathbf{V}(I)$, ou seja, todo $f \in I$ se anula nesse ponto de modo que $f \in \mathbf{I}(\{(a_1, \ldots, a_n)\})$. Então $I \subseteq \mathbf{I}(\{(a_1, \ldots, a_n)\})$. Mas como também temos que $\mathbf{I}(\{(a_1, \ldots, a_n)\} = \langle x - a_1, \ldots, x_n - a_n \rangle$ e da inclusão acima obtemos

$$I \subseteq \langle x - a_1, \ldots, x_n - a_n \rangle \subsetneq \kappa[x_1, \ldots, x_n]$$

Portanto, como I é maximal segue que $I = \langle x - a_1, \ldots, x_n - a_n \rangle$. ■

Vejamos agora como podemos caracterizar a decomposição de uma variedade afim.

Proposição 2.26. *Seja $V \in \mathbb{A}^n(\kappa)$ uma variedade afim. Então V pode ser escrita como uma união finita $V = V_1 \cup \cdots \cup V_m$, onde cada V_i é uma variedade irredutível.*

Demonstração. Seja V uma variedade redutível. Então podemos escrever V como $V = V_1 \cup V_1'$, onde por definição $V \neq V_1$ e $V \neq V_1'$. Se V_1 e V_1' são uniões finitas de irredutíveis, então V também seria. Digamos, sem perda de generalidade, que V_1' não seja uma união finita de

irredutíveis. Então repetindo a argumentação, digamos que $V_1' = V_2 \cup V_2'$, com $V_1' \neq V_2$ e $V_1' \neq V_2'$. Digamos agora que V_2' não seja uma união finita de irredutíveis. Prosseguindo dessa forma, obteremos uma sequência de variedades afins:

$$V \supseteq V_1' \supseteq V_2' \supseteq \cdots, \text{com } V \neq V_1' \neq V_2' \neq \ldots$$

Aplicando **I**, obtemos então uma sequência de ideais, revertendo a inclusão:

$$\mathbf{I}(V) \subseteq \mathbf{I}(V_1') \subseteq \mathbf{I}(V_2') \subseteq \cdots$$

Como $\kappa[x_1, \ldots, x_n]$ é Noethereriano, pela condição de cadeia ascendente de ideais temos para algum índice N que $\mathbf{I}(V_N') = \mathbf{I}(V_{N+i}')\ \forall\ i \geq 1$, seguindo que $V_N' = V_{N+i}'\ \forall\ i \geq 1$. Portanto obtemos que V_N é irredutível e logo a variedade V pode ser escrita como uma união finita de irredutíveis. ■

Definição 2.27. Seja $V \in \mathbb{A}^n(\kappa)$ uma variedade afim. Uma decomposição $V = V_1 \cup \cdots \cup V_m$, onde cada V_i é uma variedade irredutível, é chamada decomposição minimal se $V_i \nsubseteq V_j$ para $i \neq j$.

Teorema 2.28. *Seja $V \in \mathbb{A}^n(\kappa)$ uma variedade afim. Então V possui uma decomposição minimal $V = V_1 \cup \cdots \cup V_m$, com $V_i \nsubseteq V_j$ para $i \neq j$. Além disso essa decomposição minimal é única a não ser pela ordem na qual $V_1, \ldots, V_m$ estão escritas.*

Demonstração. Veja [5, pág 26].

Quando obtemos uma decomposição minimal para uma variedade V, essas variedades irredutíveis V_i são chamadas componentes irredutíveis de V.

Definição 2.29. Um ideal próprio $\mathfrak{q} \in A = \kappa[x_1, \ldots, x_n]$ é dito primário se $f, g \in A$ e $fg \in \mathfrak{q}$ implica que $f \in \mathfrak{q}$ ou $g \in \sqrt{\mathfrak{q}}$.

Assim, claramente, todo ideal primo é primário.

Definição 2.30. Seja $I \subset \kappa[x_1, \ldots, x_n]$ um ideal. Uma decomposição primária de I é uma expressão para I como uma interseção finita de ideais primários

$$I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \mathfrak{q}_t.$$

Essa decomposição é chamada minimal se os $\sqrt{\mathfrak{q}_i}$ são todos distintos e se $\mathfrak{q}_i \not\supset \bigcap_{j \neq i} \mathfrak{q}_j$ para todo i.

Teorema 2.31 (Lasker-Noether)**.** *Todo ideal $I \in \kappa[x_1, \ldots, x_n]$ possui uma decomposição primária minimal.*

Demonstração. Veja [5, pág 28].

Assim para obter a decomposição de uma variedade afim em suas componentes irredutíveis, basta procurar a decomposição primária minimal do ideal correspondente.

2.3 Anel Coordenado

Nesta seção comentaremos sobre o Anel Coordenado de uma variedade afim e sua relação com a definição de variedades isomorfas. Começamos com as definições e resultados de aplicações polinomiais.

Definição 2.32. Sejam $V \in \mathbb{A}^m(\kappa)$ e $W \in \mathbb{A}^n(\kappa)$ variedades. Uma função $\phi : V \to W$ é dita ser uma aplicação polinomial se existem polinômios $f_1, \ldots, f_n \in \kappa[x_1, \ldots, x_m]$ tais que $\phi(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$ para todo $(a_1, \ldots, a_m) \in V$.
Dizemos que a $n-$upla de polinômios $(f_1, \ldots, f_n) \in (\kappa[x_1, \ldots, x_m])^n$ representa ϕ e os f_i são as componentes dessa representação.

Proposição 2.33. *Seja $V \in \mathbb{A}^m(\kappa)$ uma variedade afim. Então:*

(i) *f e $g \in \kappa[x_1, \ldots, x_m]$ representam a mesma função polinomial sobre V se, e somente se $f - g \in I(V)$.*

(ii) *$(f_1, \ldots, f_n)$ e $(g_1, \ldots, g_n)$ representam a mesma aplicação polinomial de V em $\mathbb{A}^n(\kappa)$ se, e somente se $f_i - g_i \in I(V)$ para cada $1 \leq i \leq n$.*

Demonstração. Se $f - g = h \in I(V)$, então para qualquer ponto $p = (a_1, \ldots, a_m) \in V$ temos $f(p) - g(p) = h(p) = 0$. Consequentemente, f e g representam a mesma função sobre V.
Reciprocamente, se f e g representam a mesma função polinomial, então, em todo $p \in V$ temos $f(p) - g(p) = 0$. Assim $f - g \in I(V)$ por definição.
O item (ii) segue diretamente de (i). ■

Podemos definir agora o Anel Coordenado.

Definição 2.34. Denotamos por $\kappa[V]$ a coleção de funções polinomiais $\phi : V \to \kappa$, e chamamos esse conjunto de Anel Coordenado da Variedade Afim $V \subseteq \mathbb{A}^n(\kappa)$.

Note que, de fato, esse conjunto é um anel com as seguintes operações:
Sejam duas funções polinomiais $f, g \in \kappa[V]$, então temos para todo $p \in V$ que:

(i) $(f + g)(p) = f(p) + g(p)$;

(ii) $(f \cdot g)(p) = f(p) \cdot g(p)$.

Podemos construir um isomorfismo natural $\kappa[x_1, \ldots, x_n]/\mathbf{I}(V) \cong \kappa[V]$. De modo que os elementos de $\kappa[V]$ podem ser vistos tanto como funções polinomiais quanto como classes residuais de polinômios módulo $\mathbf{I}(V)$, como veremos adiante.

Vejamos, primeiramente, alguns resultados importantes sobre a congruência módulo um ideal.

Definição 2.35. Seja $I \subseteq \kappa[x_1, \ldots, x_n]$ um ideal e sejam $f, g \in \kappa[x_1, \ldots, x_n]$. Dizemos que f e g são congruentes módulo I, e escrevemos $f \equiv g \ mod \ I$, se $f - g \in I$.

Proposição 2.36. *Seja $I \subseteq \kappa[x_1, \ldots, x_n]$ um ideal. Então congruência módulo I é uma relação de equivalência sobre $\kappa[x_1, \ldots, x_n]$.*

Demonstração. Veja [2, pág 240].

Definição 2.37. O quociente de $\kappa[x_1, \ldots, x_n]$ módulo I, é o conjunto das classes de equivalência com a congruência módulo I:

$$\kappa[x_1, \ldots, x_n]/I = \{[f] \mid f \in \kappa[x_1, \ldots, x_n]\}.$$

Proposição 2.38. *Seja I um ideal em $\kappa[x_1, \ldots, x_n]$. O quociente $\kappa[x_1, \ldots, x_n]/I$ é um anel comutativo com a soma e o produto definidos da forma:*

(i) $[f] + [g] = [f + g]$*, com a soma em* $\kappa[x_1, \ldots, x_n]$*;*

(ii) $[f] \cdot [g] = [f \cdot g]$*, com o produto em* $\kappa[x_1, \ldots, x_n]$.

Demonstração. Veja [2, pág 242].

Note que a correspondência entre os elementos de $\kappa[V]$ e os elementos de $\kappa[x_1, \ldots, x_n]/\mathbf{I}(V)$ preserva somas e produtos.

Proposição 2.39. *Seja $\Phi : \kappa[x_1, \ldots, x_n]/\mathbf{I}(V) \to \kappa[V]$ e sejam $[f], [g] \in \kappa[x_1, \ldots, x_n]/\mathbf{I}(V)$ então:*

(i) $\Phi([f + g]) = \Phi([f]) + \Phi([g])$;

(ii) $\Phi([f \cdot g]) = \Phi([f]) \cdot \Phi([g])$.

Demonstração. Veja [2, pág 243]

A seguinte proposição relaciona os ideais de um anel quociente com os ideais no anel original.

Proposição 2.40. *Seja I um ideal em $\kappa[x_1, \ldots, x_n]$. Os ideais no anel quociente $\kappa[x_1, \ldots, x_n]/I$ estão em correspondência bijetiva com os ideais de $\kappa[x_1, \ldots, x_n]$ contendo I, isto é, os ideais J satisfazendo $I \subseteq J \subseteq \kappa[x_1, \ldots, x_n]$.*

Demonstração. Veja [2, pág 244].

Vejamos uma relação importante entre um ideal radical no anel coordenado e seu correspondente em $\kappa[x_1, \ldots, x_n]$.

Proposição 2.41. *Um ideal $J \subseteq \kappa[V]$ é radical se, e somente se o ideal correspondente $\tilde{J} = \{f \in \kappa[x_1, \ldots, x_n] \mid [f] \in J\} \subseteq \kappa[x_1, \ldots, x_n]$ é radical.*

Demonstração. Assumindo J como ideal radical, e sendo $f \in \kappa[x_1, \ldots, x_n]$ satisfazendo $f^m \in \tilde{J}$ para algum $m \geq 1$. Então $[f^m] = \underbrace{[f] \cdots [f]}_{m\ vezes} = [f]^m \in J$. Como J é, por hipótese, radical, isso implica que $[f] \in J$, e consequentemente $f \in \tilde{J}$. Portanto $\tilde{J}$ também é um ideal radical. Reciprocamente, se $\tilde{J}$ é radical e $[f]^m \in J$, então $[f^m] \in J$, e assim $f^m \in \tilde{J}$. Como $\tilde{J}$ é radical, por hipótese, segue que $f \in \tilde{J}$, e consequentemente $[f] \in J$. Assim J também é um ideal radical. ■

Prossigamos agora caracterizando variedades isomorfas em espaços afins arbitrários.

Definição 2.42. Sejam $V \subseteq \mathbb{A}^m(\kappa)$ e $W \subseteq \mathbb{A}^n(\kappa)$ variedades afins. Dizemos que V e W são isomorfas se existem funções polinomiais $\alpha : V \to W$ e $\beta : W \to V$ tais que $\alpha \circ \beta = id_W$ e $\beta \circ \alpha = id_V$

Proposição 2.43. *Sejam V e W variedades (possivelmente em diferentes espaços afins).*

(i) *Seja $\alpha : V \to W$ uma função polinomial. Então para toda função polinomial $\phi : W \to \kappa$, a composição $\phi \circ \alpha : V \to \kappa$ também é uma função polinomial. Além disso, a função $\alpha^* : \kappa[W] \to \kappa[V]$ definida por $\alpha^*(\phi) = \phi \circ \alpha$ é um homomorfismo de anéis, que é a identidade para funções constantes $\kappa \subseteq \kappa[W]$.*
Note que α^* vai em direção oposta à α, já que ela leva funções de W em funções de V. Por essa razão chamamos α^* de função pull-back.

(ii) *Reciprocamente, seja $\Phi : \kappa[W] \to \kappa[V]$ um homomorfismo de anéis que é a identidade para funções constantes. Então existe uma única função polinomial $\alpha : V \to W$ tal que $\Phi = \alpha^*$.*

Demonstração. (i) Supondo que $V \subseteq \mathbb{A}^m(\kappa)$ tem coordenadas $x_1, \ldots, x_m$ e $W \subseteq \mathbb{A}^n(\kappa)$ tem coordenadas $y_1, \ldots, y_n$. Então $\phi : W \to \kappa$ pode ser representada por um polinômio $f(y_1, \ldots, y_n)$ e $\alpha : V \to W$ pode ser representada por uma $n-$upla de polinômios:
$\alpha(x_1, \ldots, x_m) = (h_1(x_1, \ldots, x_m), \ldots, h_n(x_1, \ldots, x_m))$
Calculando a composição $\phi \circ \alpha$ substituindo $\alpha(x_1, \ldots, x_m)$ em ϕ, obtemos:
$(\phi \circ \alpha)(x_1, \ldots, x_m) = f(\alpha(x_1, \ldots, x_m)) = f(h_1(x_1, \ldots, x_m), \ldots, h_n(x_1, \ldots, x_m))$, que é um polinômio em $x_1, \ldots, x_m$. Consequentemente $\phi \circ \alpha$ é uma função polinomial.
Assim sendo, podemos definir $\alpha^* : \kappa[W] \to \kappa[V]$.
Para mostrar que α^* é um homomorfismo de anéis, seja ψ outro elemento de $\kappa[W]$, representado por um polinômio $g(y_1, \ldots, y_n)$. Então:

$$\begin{aligned}(\alpha^*(\phi + \psi))(x_1, \ldots, x_m) &= ((\phi + \psi) \circ \alpha)(x_1, \ldots, x_m) \\ &= (\phi \circ \alpha)(x_1, \ldots, x_m) + (\psi \circ \alpha)(x_1, \ldots, x_m) \\ &= (\alpha^*(\phi) + \alpha^*(\psi))(x_1, \ldots, x_m).\end{aligned}$$

Portanto $\alpha^*(\phi + \psi) = \alpha^*(\phi) + \alpha^*(\psi)$.
De modo análogo:

$$\begin{aligned}(\alpha^*(\phi \cdot \psi))(x_1, \ldots, x_m) &= ((\phi \cdot \psi) \circ \alpha)(x_1, \ldots, x_m) \\ &= (\phi \circ \alpha)(x_1, \ldots, x_m) \cdot (\psi \circ \alpha)(x_1, \ldots, x_m) \\ &= (\alpha^*(\phi) \cdot \alpha^*(\psi))(x_1, \ldots, x_m).\end{aligned}$$

Portanto $\alpha^*(\phi \cdot \psi) = \alpha^*(\phi) \cdot \alpha^*(\psi)$. Logo α^* é um homomorfismo de anéis.
Por fim, considere $[a] \in \kappa[W]$ para algum $a \in \kappa$. Então $[a]$ é uma função constante em W de valor a, e segue que $\alpha^*([a]) = [a] \circ \alpha$ é constante em V novamente com valor a. Assim $\alpha^* = [a]$, de forma que α^* é a função identidade para funções constantes.

(ii) Agora, seja $\Phi : \kappa[W] \to \kappa[V]$ um homomorfismo de anéis que é a identidade para funções constantes. Precisamos mostrar que Φ vem de alguma função polinomial $\alpha : V \to W$. Já que $W \subseteq \mathbb{A}^n(\kappa)$ tem coordenadas $y_1, \ldots, y_n$, podemos conseguir funções coordenadas $[y_i] \in \kappa[W]$. Assim $\Phi([y_i]) \in \kappa[V]$ e uma vez que $V \subseteq \mathbb{A}^m(\kappa)$ tem coordenadas $x_1, \ldots, x_m$, podemos escrever $\Phi([y_i]) = [h_i(x_1, \ldots, x_m)] \in \kappa[V]$ para algum polinômio $h_i \in \kappa[x_1, \ldots, x_m]$.
Consideremos então a função polinomial:

$$\alpha = (h_1(x_1, \ldots, x_m), \ldots, h_n(x_1, \ldots, x_m))$$

Vamos mostrar que α leva V em W e que $\Phi = \alpha^*$. Dado um polinômio $F \in \kappa[y_1, \ldots, y_n]$ qualquer, afirmamos que $[F \circ \alpha] = \Phi([F])$ em $\kappa[V]$.
Para verificar isso, note que:
$[F \circ \alpha] = [F(h_1, \ldots, h_n)] = F([h_1], \ldots, [h_n]) = F(\Phi([y_1]), \ldots, \Phi([y_n]))$
Onde a segunda igualdade segue das definições de soma e produto em $\kappa[V]$, e a terceira igualdade segue de $[h_i] = \Phi([y_i])$.
Mas $[F] = [F(y_1, \ldots, y_n)]$ é uma combinação $\kappa-$linear de produtos de $[y_i]$, de modo que:
$F(\Phi([y_1]), \ldots, \Phi([y_n])) = \Phi([F(y_1, \ldots, y_n)]) = \Phi([F])$ já que Φ é homomorfismo de anéis que é a identidade sobre κ. Logo $[F \circ \alpha] = \Phi([F])$ em $\kappa[V]$.
Para mostrarmos agora que α leva V em W, dado um ponto $(c_1, \ldots, c_m) \in V$, devemos mostrar que $\alpha(c_1, \ldots, c_m) \in W$. Se $F \in I(W)$, então $[F] = 0$ em $\kappa[W]$, e sendo Φ um homomorfismo de anéis, temos que $\Phi([F]) = 0$ em $\kappa[V]$. Implicando que $[F \circ \alpha]$ é a função nula em V.
Assim, em particular temos:

$$[F \circ \alpha](c_1, \ldots, c_m) = F(\alpha(c_1, \ldots, c_m)) = 0.$$

Como F foi tomado arbitrariamente em $I(W)$, segue que $\alpha(c_1, \ldots, c_m) \in W$ como desejado.
Uma vez sabendo que α leva V em W temos então que $[F] \circ \alpha = \Phi([F])$ para qualquer $[F]$ em $\kappa[W]$. E como $\alpha^*([F]) = [F] \circ \alpha$, segue que $\Phi = \alpha^*$.

Resta somente mostrar que α é unicamente determinado. Supondo que tenhamos $\beta : V \to W$ com $\Phi = \beta^*$.
Se β está representado por $\beta(x_1, \ldots, x_m) = (\tilde{h_1}(x_1, \ldots, x_m), \ldots, \tilde{h_n}(x_1, \ldots, x_m))$, então notamos que $\beta^*([y_i]) = [y_i] \circ \beta = [\tilde{h_i}(x_1, \ldots, x_m)]$. E como $\alpha^* = \Phi = \beta^*$ temos que $[h_i] = [\tilde{h_i}]$ para todo i. Dessa forma h_i e $\tilde{h_i}$ dão o mesmo polinômio em V, e consequentemente $\alpha(h_1, \ldots, h_n)$ e $\beta(\tilde{h_1}, \ldots, \tilde{h_n})$ definem a mesma função em V. Daí $\alpha = \beta$ e a unicidade está provada. ■

Teorema 2.44. *Duas variedades afins $V \subseteq \mathbb{A}^m(\kappa)$ e $W \subseteq \mathbb{A}^n(\kappa)$ são isomorfas se, e somente se existe um isomorfismo $\kappa[V] \cong \kappa[W]$ de anéis coordenados que é a identidade para funções constantes.*

Demonstração. Suponha-se que $\alpha : V \to W$ e $\beta : W \to V$ sejam funções polinomiais inversas uma da outra. Então $\alpha \circ \beta = id_W$, onde $id_W : W \to W$ é função identidade. Isso implica que $(\alpha \circ \beta)^*(\phi) = id_W^*(\phi) = \phi \circ id_W = \phi, \ \forall \ \phi \in \kappa[W]$.
Contudo, também temos que $(\alpha \circ \beta)^*(\phi) = \phi \circ (\alpha \circ \beta) = (\phi \circ \alpha) \circ \beta = \alpha^*(\phi) \circ \beta = \beta^*(\alpha^*(\phi)) = (\beta^* \circ \alpha^*)(\phi)$. Consequentemente $(\alpha \circ \beta)^* = \beta^* \circ \alpha^* = id_{\kappa[W]}$ como função identidade de $\kappa[W]$ nele mesmo.
De modo análogo, podemos mostrar que $(\beta \circ \alpha)^* = \alpha^* \circ \beta^* = id_{\kappa[V]}$.
Daí, se V e W são variedades isomorfas, então $\kappa[V] \cong \kappa[W]$, e pela Proposição 2.43 esse isomorfismo é a identidade para funções constantes.
Para a recíproca, devemos mostrar que se temos um isomorfismo de anéis $\Phi : \kappa[W] \to \kappa[V]$ que é a identidade para funções constantes, então Φ e Φ^{-1} vem de funções polinomiais inversas entre V e W.
Pela Proposição 2.43, já sabemos que $\Phi = \alpha^*$ para alguma $\alpha : V \to W$ e $\Phi^{-1} = \beta^*$ para alguma $\beta : W \to V$. Precisamos mostrar então que α e β são funções inversas.
Consideremos a composição $\alpha \circ \beta : W \to W$, a qual é claramente uma função polinomial, e para qualquer $\phi \in \kappa[W]$:

$$(\alpha \circ \beta)^*(\phi) = \beta^*(\alpha^*(\phi)) = \Phi^{-1}(\Phi(\phi)) = \phi.$$

Como a função identidade $id_W : W \to W$ é uma função polinomial sobre W, e $id_W^*(\phi) = \phi, \ \forall \ \phi \in \kappa[W]$, podemos concluir que $(\alpha \circ \beta)^* = id_W^*$ e então $\alpha \circ \beta = id_W$, cuja unicidade também segue da Proposição 2.43.
De modo análogo, pode-se obter que $\beta \circ \alpha = id_V$, e consequentemente α e β são funções inversas, e concluímos a demonstração. ■

2.4 Finitude Relativa e Normalização de Noether

Nesta seção estudaremos conceitos de finitude que ajudarão a compreender a noção algébrica de dimensão de uma variedade que veremos adiante.

Começamos com um resultado importante sobre o complemento do ideal dos termos líderes $\langle LT(I)\rangle$.

Proposição 2.45. *Fixe uma ordem monomial sobre $\kappa[x_1,\ldots,x_n]$ e seja $I \subseteq \kappa[x_1,\ldots,x_n]$ um ideal. Todo $f \in \kappa[x_1,\ldots,x_n]$ é congruente módulo I a um único polinômio r que é uma combinação $\kappa-$linear dos monômios no complemento de $\langle LT(I)\rangle$.*

Demonstração. Seja G uma base de Gröbner para I e seja $f \in \kappa[x_1,\ldots,x_n]$. Pelo algoritmo da divisão, o resto $r = \bar{f}^G$ satisfaz $f = q + r$, com $q \in I$. Consequentemente $f - r = q \in I$, e então $f \equiv r \ mod \ I$. Também temos que r é uma combinação $\kappa-$linear dos monômios $x^\alpha \notin \langle LT(I)\rangle$. ■

Como comentamos anteriormente, no desenvolvimento histórico de aplicação das bases de Gröbner, Buchberger tinha o interesse de encontrar representantes padrão para as classes residuais em anéis quocientes. Note também que dado $I = I(V)$ para uma variedade V, então a Proposição 2.45 fornece representantes padrão para as funções polinomiais $\phi \in \kappa[V]$. Desse modo, podemos aplicar esta proposição para descrever a estrutura algébrica do anel quociente $\kappa[x_1,\ldots,x_n]/I$.

Proposição 2.46. *Seja $I \subseteq \kappa[x_1,\ldots,x_n]$ um ideal. Então $\kappa[x_1,\ldots,x_n]/I$ é isomorfo como um espaço $\kappa-$vetorial a $S = Span(x^\alpha |\ x^\alpha \notin \langle LT(I)\rangle)$.*

Demonstração. Veja [2, pág 250].

Note desse modo que dado um ideal $I \subset \kappa[x_1,\ldots,x_n]$ e $\mathcal{G}$ uma base de Gröbner para I, então para todo $[f] \in \kappa[x_1,\ldots,x_n]/I$ podemos encontrar um representante padrão $\overline{f} = \overline{f}^{\mathcal{G}}$ em $S = Span(x^\alpha |\ x^\alpha \notin \langle LT(I)\rangle)$, onde:

- $[f] + [g]$ será representado por $\overline{f} + \overline{g}$ e
- $[f] \cdot [g]$ será representado por $\overline{f \cdot g} \in S$

O Teorema seguinte permite determinar quando uma variedade contém apenas um número finto de pontos, isto é, de forma equivalente quando um sistema de equações polinomiais possui apenas um número finito de soluções no espaço afim.

Teorema 2.47 (Teorema da Finitude)**.** *Seja $I \subseteq \kappa[x_1,\ldots,x_n]$ um ideal, $>$ uma ordem monomial sobre $\kappa[x_1,\ldots,x_n]$ e considerando as seguintes afirmações:*

i *Para cada i, $1 \leq i \leq n$, existe algum $m_i \geq 0$ tal que $x_i^{m_i} \in \langle LT(I)\rangle$.*

ii *Seja G uma base de Gröbner para I. Então para cada i, $1 \leq i \leq n$, existe algum $m_i \geq 0$ tal que $x_i^{m_i} = LM(g)$ para algum $g \in G$.*

iii *O conjunto $\{x^\alpha \mid x^\alpha \notin \langle LT(I)\rangle\}$ é finito.*

iv *O espaço $\kappa-$vetorial $\kappa[x_1, \ldots, x_n]/I$ é finito-dimensional.*

v $V(I) \subseteq \mathbb{A}^n(\kappa)$ *é um conjunto finito.*

Então (i)-(iv) são equivalentes e todos implicam em (v). Além disso, se κ é algebricamente fechado, então (i)-(v) são todos equivalentes.

Demonstração. Veja [2, pág 252].

Definição 2.48. Uma $\kappa-$álgebra é um anel que contém o corpo κ como um subanel. E também:

(i) Uma $\kappa-$álgebra é finitamente gerada se contém um número finito de elementos tais que todo elemento pode ser expresso como um polinômio (com coeficientes em κ) nesses finitos elementos.

(ii) Um homomorfismo de $\kappa-$álgebras é um homomorfismo de anéis que é a identidade nos elementos de κ.

Além disso, uma $\kappa-$álgebra é um espaço vetorial sobre κ, onde a adição é definida pela adição no anel, e a multiplicação por escalar é a multiplicação pelos elementos do subanel κ. Um exemplo é o Anel Coordenado de uma variedade não-vazia.

Definição 2.49. Dado um anel comutativo S e um subanel $R \subseteq S$, dizemos que S é finito sobre R se existem finitos elementos $s_1, \ldots, s_l \in S$ tais que todo $s \in S$ pode ser escrito da forma

$$s = a_1 s_1 + \cdots + a_l s_l, \text{ com } a_1, \ldots, a_l \in R$$

A partir dessa definição temos a seguinte proposição sobre a finitude de um subconjunto.

Proposição 2.50. *Assumindo que S é finito sobre R. Então todo $s \in S$ satisfaz uma equação da forma*

$$s^l + a_1 s^{l-1} + \cdots + a_l = 0, \text{ com } a_1, \ldots, a_l \in R$$

Demonstração. Veja [2, pág 279].

Note que em geral, um elemento $s \in S$ é inteiro sobre um subanél R se satisfaz uma equação como na proposição anterior. Desse modo a Proposição 2.50 nos diz que se S é finito sobre R, então todo elemento de S é inteiro sobre R.

Veremos a seguir uma versão relativa do Teorema 2.47, para a qual precisamos da seguinte definição de ordem monomial.

Definição 2.51. Fixe um inteiro $1 \leq l \leq n$. Dizemos que uma ordem monomial $>$ sobre $\kappa[x_1, \ldots, x_n]$ é do tipo de $l-$eliminação se qualquer monômio envolvendo uma das variáveis $x_1, \ldots, x_l$ é maior que todos os monômios em $\kappa[x_{l+1}, \ldots, x_n]$.

Teorema 2.52 (Finitude Relativa)**.** *Seja $I \subseteq \kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]$ um ideal tal que $I \cap \kappa[y_1, \ldots, y_m] = \{0\}$ e fixe uma ordem do tipo de $l-$eliminação. Então as seguintes afirmações são equivalentes:*

(i) *Para cada i, $1 \leq i \leq l$, existe algum $m_i \geq 0$ tal que $x_i^{m_i} \in \langle LT(I)\rangle$.*

(ii) *Seja G uma base de Gröbner para I. Então para cada i, $1 \leq i \leq l$, existe algum $m_i \geq 0$ tal que $x_i^{m_i} = LM(g)$ para algum $g \in G$.*

(iii) *O conjunto $\{x^\alpha \mid \exists\ \beta \in \mathbb{Z}^m_{\geq 0}$ tal que $x^\alpha y^\beta \notin \langle LT(I)\rangle\}$ é finito.*

(iv) *O anel $\kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]/I$ é finito sobre o subanel $\kappa[y_1, \ldots, y_m]$.*

Demonstração. (i)⇔(ii) Análoga ao Teorema 2.47.
(ii)⇒(iii) Se alguma potência $x_i^{m_i} \in \langle LT(I)\rangle$ para $1 \leq i \leq n$, então qualquer monômio $x^\alpha y^\beta = x_1^{\alpha_1} \cdots x_n^{\alpha_n} y^\beta$ para o qual algum $\alpha_i \geq m_i$ está em $\langle LT(I)\rangle$. Consequentemente um monômio no complemento de $\langle LT(I)\rangle$ deve ter $\alpha_i \leq m_i - 1$ para todo $1 \leq i \leq n$. Como resultado, existem no máximo $m_1 \cdot m_2 \cdots m_n$ monômios x^α tais que $x^\alpha y^\beta \notin \langle LT(I)\rangle$.
(iii)⇒(iv) Tome $f \in \kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]$ arbitrário e divida f por G pelo algoritmo da divisão. Obteremos assim $f = g + r$, onde $g \in I$ e r é uma combinação linear de monômios $x^\alpha y^\beta \notin \langle LT(I)\rangle$. Por suposição, apenas um número finito de x^α's aparecem nesses monômios, digamos $x^{\alpha_1}, \ldots, x^{\alpha_l}$. Agrupando os termos de r que compartilham o mesmo x^{α_j}, podemos escrever f da forma

$$f = g + b_1 x^{\alpha_1} + \cdots + b_l x^{\alpha_l}, \text{com } b_j \in \kappa[y_1, \ldots, y_m]$$

Tomando $[f]$ para denotar a classe de equivalência de f no anel quociente $\kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]/I$, como $g \in I$, segue da equação anterior que
$[f] = [g + b_1 x^{\alpha_1} + \cdots + b_l x^{\alpha_l}] = [g] + [b_1 x^{\alpha_1}] + \cdots + [b_l x^{\alpha_l}] = [b_1 x^{\alpha_1}] + \cdots + [b_l x^{\alpha_l}] = b_1[x^{\alpha_1}] + \cdots + b_l[x^{\alpha_l}]$, em $\kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]/I$.
Assim $[x^{\alpha_1}], \ldots, [x^{\alpha_l}]$ satisfazem a definição, mostrando que o anel $\kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]/I$ é finito sobre o subanél $\kappa[y_1, \ldots, y_m]$.
(iv)⇒(i) Fixe $1 \leq i \leq n$. Por (iv) e pela Proposição 2.50, existe uma equação
$[x_i]^d + a_1[x_i]^{d-1} + \cdots + a_d = 0$, com $a_j \in \kappa[y_1, \ldots, y_m]$ em $\kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]/I$.
Voltando para o anel $\kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]$, isso significa que

$$x_i^d + a_1 x_i^{d-1} + \cdots + a_d \in I.$$

Como a ordem utilizada é do tipo de $n-$eliminação, então x_i é maior que qualquer monômio em $y_1, \ldots, y_m$. Como os $a_j \in \kappa[y_1, \ldots, y_m]$, isso implica que $x_i^d > LT(a_j x_i^{d-j})$ para $1 \leq j \leq d$. Segue então que $x_i^d = LT(x_i^d + a_1 x_i^{d-1} + \cdots + a_d) \in \langle LT(I)\rangle$ como desejado. ■

Do Teorema da Finitude temos que $\mathbf{V}(I)$ finito é equivalente aos demais itens quando κ é algebricamente fechado. Surge então uma pergunta, de modo natural, sobre um significado geométrico similar para o Teorema da Finitude Relativa no caso em que κ é algebricamente fechado.

Primeiramente vejamos o significado geométrico de um ideal $I \subseteq \kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]$. A inclusão de $\kappa-$álgebras $\kappa[y_1, \ldots, y_m] \subseteq \kappa[x_1, \ldots, x_n, y_1, \ldots, y_m]$ corresponde à projeção $\kappa^{n+m} \to \kappa^m$ que leva um ponto $(a, b) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$ em suas últimas m coordenadas b. O ideal I fornece uma variedade $V(I) \subseteq \mathbb{A}^{n+m}(\kappa)$. Compondo essa inclusão com a projeção obtemos: $\pi : V(I) \to \mathbb{A}^m(\kappa)$.

Assim um ponto $b = (b_1, \ldots, b_m)$ fornece dois objetos: um algébrico, o ideal $I_b \in \kappa[x_1, \ldots, x_n]$, que é obtido fazendo $y_i = b_i$ em todos os elementos desse ideal; e um geométrico, a fibra $\pi^{-1}(b) = V(I) \cap (\mathbb{A}^m(\kappa) \times \{b\})$, que consiste de todos os pontos de $V(I)$ cujas últimas m coordenadas são dadas por b.

Definição 2.53. Elementos $u_1, \ldots, u_m$ em uma $\kappa-$álgebra A são ditos algebricamente independentes sobre κ quando o único polinômio $f \in A$ com coeficientes em κ satisfazendo $f(u_1, \ldots, u_m) = 0$ é o polinômio nulo.
Quando isso ocorre, o subanel $\kappa[u_1, \ldots, u_m] \subseteq A$ é isomorfo a um anel de polinômios em m indeterminadas.

Para finalizar essa seção, vejamos um resultado importante sobre essa independência algébrica.

Teorema 2.54 (Normalização de Noether)**.** *Seja κ um corpo infinito e seja A uma $\kappa-$álgebra finitamente gerada. Então:*

(i) *Existem elementos algebricamente independentes $u_1, \ldots, u_m \in A$ tais que A é finito sobre $\kappa[u_1, \ldots, u_m]$.*

(ii) *Se A é gerado por $s_1, \ldots, s_l$ como uma $\kappa-$álgebra então $m \leq l$ e $u_1, \ldots, u_m$ podem ser escolhidos para serem combinações $\kappa-$lineares de $s_1, \ldots, s_l$.*

Demonstração. Veja [5, pág 123].

Note que para encontrar uma normalização de Noether para $\kappa[x_1, \ldots, x_n]/I$, podemos computar uma base de Gröbner $\mathcal{G}$ para I com ordem lexicográfica. Escolhendo as coordenadas de modo que cada ideal de eliminação não-nulo $I_{k-1} = I \cap \kappa[x_k, \ldots, x_n]$ contém um polinômio mônico em x_k, então se c é o menor inteiro tal que $I_c = \langle 0 \rangle$ obtemos uma sequência de extensões inteiras de anéis

$$\kappa[x_{c+1}, \ldots, x_n] \subset \kappa[x_c, \ldots, x_n]/I_{c-1} \subset \cdots \subset S$$

cuja composição é uma normalização de Noether para S com $m = n - c$. Assim para cada $1 \leq k \leq c-1$, checamos se $\mathcal{G}$ possui um polinômio nas variáveis $x_k, \ldots, x_n$ que seja mônico em x_k. Se possuir então a composição

$$\kappa[x_{c+1}, \ldots, x_n] \subset \kappa[x_1, \ldots, x_n] \to S = \kappa[x_1, \ldots, x_n]/I$$

é uma normalização de Noether.

2.5 Dimensão de uma Variedade e Função de Hilbert

Nessa seção veremos a definição de dimensão de uma variedade afim, bem como resultados importantes a partir da função de Hilbert e ao final um processo para o cálculo da dimensão a partir do ideal dos termos líderes da base de Gröbner computada para o ideal correspondente à variedade.

Definição 2.55. Seja $S \subset \{x_1, \ldots, x_n\}$, um conjunto não-vazio qualquer de variáveis. A variedade $V(S)$ obtida igualando cada variável $x_i \in S$ a zero, é chamado um subespaço coordenado em $\kappa[x_1, \ldots, x_n]$.

Assim, por exemplo, para o ideal monomial $I = \langle x^2y, x^3 \rangle \subset \kappa[x, y]$, denotando $H_x = V(x)$ para $x = 0$ e $H_y = V(y)$ para $y = 0$, temos que:

$$\begin{aligned} V(I) &= V(x^2y) \cap V(x^3) \\ &= (H_x \cup H_y) \cap H_x \\ &= (H_x \cap H_x) \cup (H_y \cap H_x) \\ &= H_x \end{aligned}$$

Proposição 2.56. *A variedade de um ideal monomial em $\kappa[x_1, \ldots, x_n]$ é uma união finita de subespaços coordenados de $\mathbb{A}^n(\kappa)$.*

Demonstração. Note que se $x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_r}^{\alpha_r}$ é um monômio em $\kappa[x_1, \ldots, x_n]$ com $\alpha_j \geq 1$ para $1 \leq j \leq r$, então

$$V(x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_r}^{\alpha_r}) = H_{x_{i_1}} \cup H_{x_{i_2}} \cup \cdots \cup H_{x_{i_r}}, \text{ onde } H_l = V(x_l).$$

Assim a variedade definida por um monômio é uma união de hiperplanos coordenados. Note ainda que existem apenas n tais hiperplanos. Como um ideal monomial é gerado por uma coleção finita de monômios, a variedade correspondendo a um ideal monomial é uma interseção finita de uniões de hiperplanos coordenados. Assim, pela propriedade distributiva de interseções sobre uniões, qualquer interseção finita de uniões de hiperplanos coordenados pode ser reescrita como uma união finita de interseções de hiperplanos coordenados. Como a interseção

de qualquer coleção de hiperplanos coordenados é um subespaço coordenado, então segue o resultado desejado. ■

Note que quando escrevemos a variedade de um ideal monomial I como uma união de finitos subespaços coordenados podemos omitir um subespaço que esteja contido em outro na união. Assim escrevemos $V(I)$ como uma união de subespaços coordenados: $V(I) = V_1 \cup V_2 \cup \cdots \cup V_p$, onde $V_i \subsetneq V_j$ para $i \neq j$.

Definição 2.57. Seja V uma variedade, a qual é a união de finitos subespaços lineares de $\mathbb{A}^n(\kappa)$. Então a dimensão de V, denotada $\dim V$, é a maior das dimensões dos subespaços.

Assim, por exemplo, a dimensão da união de dois planos e uma reta é 2, e a dimensão da união de três retas é 1.

Computar a dimensão de uma variedade correspondendo a um ideal monomial é encontrar o máximo das dimensões dos subespaços coordenados contidos em $V(I)$.
Seja $I = \langle m_1, \ldots, m_t \rangle$ um ideal próprio gerado pelos monômios m_j, para computar $\dim V(I)$ precisamos obter a componente de maior dimensão em

$$V(I) = \bigcap_{j=1}^{t} V(m_j).$$

Se podemos encontrar uma coleção de variáveis $x_{i_1}, \ldots, x_{i_r}$ tais que ao menos uma delas apareça em cada m_j, então o subespaço coordenado definido pelas equações $x_{i_1} = \cdots = x_{i_r} = 0$ está contido em $V(I)$. Isso significa que devemos buscar as variáveis que ocorrem em tantos diferentes m_j quanto possível.

Assim para $1 \leq j \leq t$ temos $M_j = \{l \in \{1, \ldots, n\} \mid x_l \text{ divide o monômio } m_j\}$ sendo o conjunto de índices das variáveis ocorrendo com expoente ≥ 1 em m_j. Seja $\mathcal{M} = \{J \subseteq \{1, \ldots, n\} \mid J \cap M_j \neq \emptyset \; \forall \; 1 \leq j \leq t\}$ consiste de todos os subconjuntos de $\{1, \ldots, n\}$ que não possuem interseção vazia com todo conjunto M_j. Denotemos por $|J|$ o número de elementos em um conjunto J.
Com a notação acima, temos a seguinte proposição.

Proposição 2.58. *A dimensão da variedade determinada por um ideal monomial é*

$$\dim V(I) = n - min(|J| \mid J \in \mathcal{M})$$

Demonstração. Seja $J = \{i_1, \ldots, i_r\}$ um elemento de $\mathcal{M}$ tal que $|J| = r$ é minímo em $\mathcal{M}$. Como cada monômio m_j contém alguma potência de algum x_{i_l} para $1 \leq l \leq r$, o subespaço coordendo $W = V(x_{i_1}, \ldots, x_{i_r})$ está contido em $V(I)$. A dimensão de W é $n - r = n - |J|$ e, consequentemente, pela Definição 2.57, a dimensão de $V(I)$ é ao menos $n - |J|$.
Se $V(I)$ tivesse dimensão maior que $n - r$, então para algum $s < r$ existiria um subespaço coordenado $W' = V(x_{l_1}, \ldots, x_{l_s})$ contido em $V(I)$. Cada monômio m_j se anularia em W' e,

em particular, se anularia no ponto de W' cuja l_i-ésima coordenada é 0 para $1 \leq i \leq s$ e cujas demais coordenadas são 1. Consequentemente, ao menos um dos x_{l_i} deve dividir m_j, e seguiria que $J' = \{l_1, \ldots, l_s\} \in \mathcal{M}$. Como $|J'| = s < r$, isso contradiria a minimalidade de r.
Portanto a dimensão de $V(I)$ é $n - |J|$. ■

Exemplo 2.59. *Seja* $I = \langle x_2^2x_3^3, x_1^5x_3^4, x_1^2x_2x_3^2\rangle = \langle m_1, m_2, m_3\rangle$, *onde* $m_1 = x_2^2x_3^3, m_2 = x_1^5x_3^4, m_3 = x_1^2x_2x_3^2$.
Assim $M_1 = \{2, 3\}, M_2 = \{1, 3\}$ *e* $M_3 = \{1, 2, 3\}$ *e então* $\mathcal{M} = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{3\}\}$.
Portanto $min(|J| \mid J \in \mathcal{M}) = 1$, *implicando que* $\dim V(I) = 3 - 1 = 2$.

Exemplo 2.60. *Consideremos um ideal próprio monomial* $I \subset \kappa[x, y]$. *Sendo* $I \neq \kappa[x, y]$, *então* $V(I)$ *é uma das possibilidades:*

(a) *A origem* $O = \{(0, 0)\}$, $V(x, y)$;

(b) *O eixo das abscissas* Ox, $V(y)$;

(c) *O eixo das ordenadas* Oy, $V(x)$;

(d) *A união dos eixos* Ox *e* Oy, $V(xy)$.

Note que podemos analisar cada caso a partir do fato que $I \subseteq \sqrt{I}$. No caso (a), devemos ter $x^a \in I$ e $y^b \in I$ para alguns inteiros $a, b > 0$. Desse modo o número de monômios que não estão em I é finito. Observe na Figura 2.1.

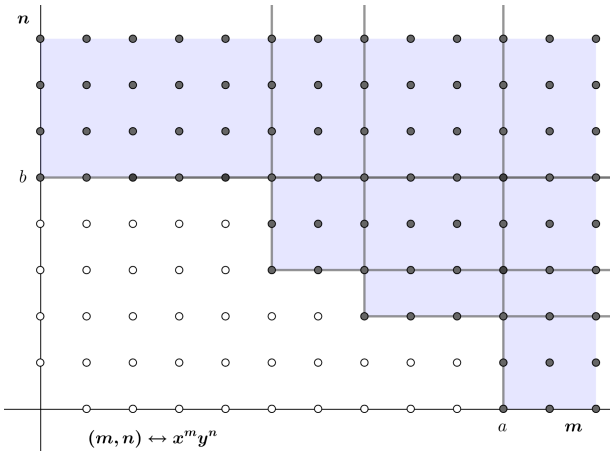

Figura 2.1: Monômios que não estão no ideal I-caso a.

No caso (b), como $V(I)$ é o eixo Ox, nenhuma potência x^a de x pode pertencer a I, devemos ter $y^b \in I$ para algum inteiro $b > 0$. Observe na Figura 2.2.

Seja l o mínimo expoente de y que ocorre entre todos os monômios em I. Note que $l \leq b$ e $l > 0$ já que nenhuma potência de x está em I. Portanto os monômios no complemento de I são os monômios $\{x^iy^j \mid i \in \mathbb{Z}_{\geq 0}, 0 \leq j \leq l - 1\}$, que correspondem precisamente aos expoentes em l cópias do eixo horizontal em $\mathbb{Z}^2_{\geq 0}$, juntamente com um número finito de outros monômios,

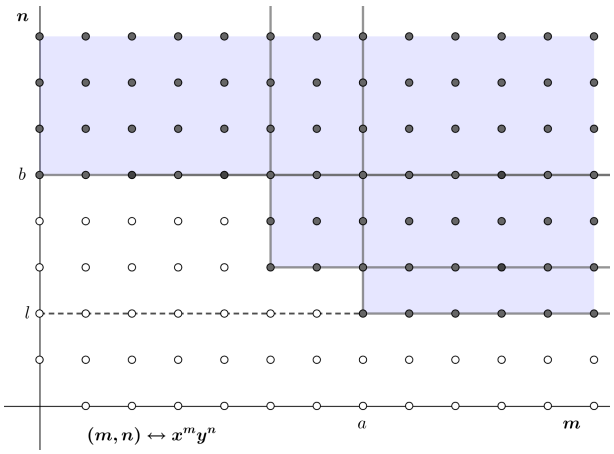

Figura 2.2: Monômios que não estão no ideal I-caso b.

os quais podem ser caracterizados como $m \notin I$ tais que $x^r m \in I$ para algum $r > 0$. Assim, os monômios no complemento de I consistem de l 'retas' de monômios juntamente com um conjunto finito de monômios.

No caso (c) a situação é análoga ao caso (b), com a diferença que as 'retas' serão paralelas ao eixo vertical em $\mathbb{Z}^2_{\geq 0}$.

No caso (d), seja l_1 o expoente mínimo de x que ocorre entre todos os monômios de I, e similarmente l_2 o expoente mínimo de y. Assim, os monômios no complemento de I consistem de l_1 'retas' de monômios $\{x^i y^j \mid 0 \leq j \leq l_1 - 1, j \in \mathbb{Z}_{\geq 0}\}$ paralelas ao eixo vertical, de l_2 'retas' de monômios $\{x^i y^j \mid 0 \leq j \leq l_2 - 1, i \in \mathbb{Z}_{\geq 0}\}$ paralelas ao eixo horizontal juntamente com um número finito de outros monômios.

Portanto os monômios no complemento de um ideal monomial $I \subset \kappa[x, y]$ consistem de um número de infinitas famílias de monômios paralelas aos subespaços coordenados em $\mathbb{Z}^2_{\geq 0}$, juntamente com uma coleção finita de outros monômios.

Generalizando, para cada ideal monomial I seja $C(I) = \{\alpha \in \mathbb{Z}^n_{\geq 0} \mid x^\alpha \notin I\}$ o conjunto de expoentes dos monômios que não estão em I. Sejam também
$e_1 = (1, 0, \ldots, 0)$;
$e_2 = (0, 1, \ldots, 0)$;
$\vdots$
$e_n = (0, 0, \ldots, 1)$.

Definição 2.61. Definimos o subespaço coordenado determinado por $e_{i_1}, \ldots, e_{i_r}$ como sendo o conjunto $[e_{i_1}, \ldots, e_{i_r}] = \{a_1 e_{i_1} + \cdots + a_r e_{i_r} \mid a_j \in \mathbb{Z}_{\geq 0}, 1 \leq j \leq r\}$. Dizemos que $[e_{i_1}, \ldots, e_{i_r}]$ é um subespaço coordenado r-dimensional.

Definição 2.62. Um subconjunto de $\mathbb{Z}^n_{\geq 0}$ é uma translação de um subespaço coordenado $[e_{i_1}, \ldots, e_{i_r}]$ se é da forma $\alpha + [e_{i_1}, \ldots, e_{i_r}] = \{\alpha + \beta \mid \beta \in [e_{i_1}, \ldots, e_{i_r}]\}$, onde $\alpha = \sum_{i \notin \{i_1, \ldots, i_r\}} a_i e_i$, com $a_i \geq 0$ inteiros.

Essa restrição sobre α significa que estamos transladando por um vetor perpendicular a $[e_{i_1}, \ldots, e_{i_r}]$. Por exemplo, $\{(1, l) \mid l \in \mathbb{Z}_{\geq 0}\} = e_1 + [e_2]$ é uma translação do subespaço $[e_2]$ no plano de expoentes $\mathbb{Z}^2_{\geq 0}$.

A partir dessas definições, a discussão sobre os monômios no complemento de ideais monomiais em $\kappa[x, y]$ pode ser resumida como:

(a) Se $V(I)$ é a origem, então $C(I)$ consiste de um número finito de pontos;

(b) Se $V(I)$ é o eixo Ox, então $C(I)$ consiste de um número finito de translações de $[e_1]$ e, possivelmente um número finito de pontos que não estão nessas translações;

(c) Se $V(I)$ é o eixo Oy, então $C(I)$ consiste de um número finito de translações de $[e_2]$ e, possivelmente um número finito de pontos que não estão nessas translações;

(d) Se $V(I)$ é a união dos eixos Ox e Oy, então $C(I)$ consiste de um número finito de translações de $[e_1]$, um número finito de translações de $[e_2]$ e, possivelmente um número finito de pontos que não estão nessas translações.

Assim, podemos fornecer um primeiro resultado para a definição de dimensão de uma variedade correspondente a um ideal monomial.

Proposição 2.63. *Seja $I \subset \kappa[x_1, \ldots, x_n]$ um ideal monomial próprio.*

(i) *O subespaço coordenado $V(x_i \mid i \notin \{i_1, \ldots, i_r\})$ está contido em $V(I)$ se, e somente se $[e_{i_1}, \ldots, e_{i_r}] \subseteq C(I)$, isto é, $V(x_i \mid i \notin \{i_1, \ldots, i_r\}) \subseteq V(I) \Leftrightarrow I \subseteq \langle x_i \mid i \notin \{i_1, \ldots, i_r\}\rangle$.*

(ii) *A dimensão de $V(I)$ é a dimensão do maior subespaço coordenado em $C(I)$.*

Demonstração. (i) $\Rightarrow$ Observe que $W = V(x_i \mid i \notin \{i_1, \ldots, i_r\})$ contém o ponto p cuja i_j-ésima coordenada é 1 para $1 \leq j \leq r$ e cujas demais coordenadas são 0. Para qualquer $\alpha \in [e_{i_1}, \ldots, e_{i_r}]$, o monômio x^α pode ser escrito na forma $x^\alpha = x_{i_1}^{\alpha_{i_1}} \cdots x_{i_r}^{\alpha_{i_r}}$. Então $x^\alpha = 1$ em p, de modo que $x^\alpha \notin I$ já que $p \in W \subseteq V(I)$ por hipótese. Portanto $\alpha \in C(I)$.
$\Leftarrow$ Suponhamos que $[e_{i_1}, \ldots, e_{i_r}] \subseteq C(I)$. Dado um monômio $m \in I$ existe $i \notin \{i_1, \ldots, i_r\}$ tal que $m = x_i m'$ para algum monômio m'. Assim $m \in \langle x_i \mid i \notin \{i_1, \ldots, i_r\}\rangle$. Portanto $I \subseteq \langle x_i \mid i \notin \{i_1, \ldots, i_r\}\rangle$, concluindo que $V(x_i \mid i \notin \{i_1, \ldots, i_r\}) \subseteq V(I)$.

(ii) O subespaço coordenado $V(x_i \mid i \notin \{i_1, \ldots, i_r\})$ tem dimensão r. Segue de (i) que as dimensões dos subespaços coordenados de $\mathbb{A}^n(\kappa)$ contidos em $V(I)$ e os subespaços coordenados de $\mathbb{Z}^n_{\geq 0}$ contidos em $C(I)$ são os mesmos. Por definição, $\dim V(I)$ é o máximo das dimensões dos subespaços coordenados contidos em $V(I)$. ■

Exemplo 2.64. *Considere o ideal $I = \langle x^4y^3, x^2y^5\rangle$.*

Podemos verificar que nesse caso $C(I)$ é a união finita
$C(I) = [e_1] \cup (e_2 + [e_1]) \cup (2e_2 + [e_1]) \cup [e_2] \cup (e_1 + [e_2]) \cup \{(3, 4)\} \cup \{(3, 3)\} \cup \{(2, 4)\} \cup \{(2, 3)\}$.

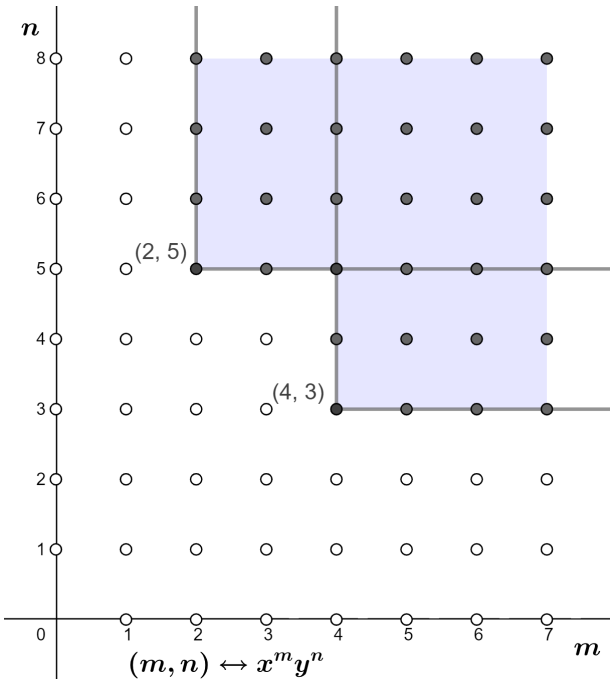

Figura 2.3: Monômios no complemento $C(I)$.

Note que os últimos quatro conjuntos são translações do subespaço coordenado 0*-dimensional que é a origem em* $\mathbb{Z}^n_{\geq 0}$*. Veja que como a dimensão do maior subespaço coordenado em* $C(I)$ *é* 1 *então temos* $\dim V(I) = 1$*. Retomaremos esse exemplo mais adiante.*

Teorema 2.65. *Se* $I \subset \kappa[x_1, \ldots, x_n]$ *é um ideal monomial próprio, então* $C(I)$ *pode ser escrito como uma união finita (mas não necessariamente disjunta) de translações de subespaços coordenados de* $\mathbb{Z}^n_{\geq 0}$*.*

Demonstração. Veja [2, pág 477].

Relembrando algumas noções de combinatória, vejamos no lema seguinte uma forma de contar os monômios de certo grau, que será útil para a construção do polinômio de Hilbert.

Lema 2.66. *O número de monômios de grau total* $\leq s$ *em* $\kappa[x_1, \ldots, x_m]$ *é o coeficiente binomial* $\binom{m+s}{s}$.

Demonstração. Veja [2, pág 478].

Assim segue do Lema 2.66 que o número de pontos de grau total $\leq s$ em um subespaço coordenado $m-$dimensional de $\mathbb{Z}^n_{\geq 0}$ é $\binom{m+s}{s}$.

Note que quando m está fixado, a expressão binomial $\binom{m+s}{s} = \binom{m+s}{m} = \frac{(s+m)!}{(s!)(m!)} =$

$= \dfrac{(s+m)(s+m-1)\cdots(s+1)s!}{s!m!} = \dfrac{1}{m!}(s+m)(s+m-1)\cdots(s+1)$ é um polinômio de grau m na variável s cujo coeficiente de s^m é $\dfrac{1}{m!}$.

Lema 2.67. *Seja $\alpha + [e_{i_1}, \ldots, e_{i_m}]$ uma translação do subespaço coordenado $[e_{i_1}, \ldots, e_{i_m}] \subseteq \mathbb{Z}^n_{\geq 0}$, onde $\alpha = \sum_{i \notin \{i_1,\ldots,i_m\}} a_i e_i$.*

i *Dado $s > |\alpha|$, então o número de pontos em $\alpha + [e_{i_1}, \ldots, e_{i_m}]$ de grau total $\leq s$ é igual a* $\binom{m+s-|\alpha|}{s-|\alpha|}$.

ii *Esse número de pontos é uma função polinomial de grau m na variável s, cujo coeficiente de s^m é $\frac{1}{m!}$.*

Demonstração. Veja [2, pág 479].

Teorema 2.68. *Se $I \subset \kappa[x_1, \ldots, x_n]$ é um ideal monomial com $\dim V(I) = d$, então para todo s suficientemente grande, o número de monômios que não estão em I de grau total $\leq s$ é um polinômio de grau d na variável s.*

Demonstração. Precisamos determinar o número de pontos em $C(I)$ de grau total $\leq s$. Pelo Teorema 2.65, sabemos que $C(I)$ pode ser escrito como uma união finita

$$C(I) = T_1 \cup T_2 \cup \cdots \cup T_t,$$

onde cada T_i é uma translação de um subespaço coordenado em $\mathbb{Z}^n_{\geq 0}$. Podemos assumir que $T_i \neq T_j$ para $i \neq j$. A dimensão de cada T_i é a dimensão do subespaço associado. Como I é um ideal, segue que um subespaço coordenado $[e_{i_1}, e_{i_2}, \ldots, e_{i_r}]$ está em $C(I)$ se, e somente se alguma translação está. Por hipótese $\mathbf{V}(I)$ tem dimensão d, então pela Proposição 2.63 cada T_i tem dimensão $\leq d$, com a igualdade ocorrendo para ao menos um dos T_i.
Para contar o número total de pontos de grau total $\leq s$ em $C(I)$, lembre que $C(I)$ é uma união de subespaços coordenados de $\mathbb{Z}^n_{\geq 0}$ não necessariamente disjunta. Então usando o sobrescrito s para denotar o subespaço consistindo de elementos de grau total $\leq s$ temos:

$$C(I)^s = T_1^s \cup T_2^s \cdots \cup T_t^s.$$

Denotemos o número de elementos de em $C(I)^s$ como $|C(I)^s|$.

Para proceder a contagem, note que, como os subespaços podem conter elementos comuns, então não podemos simplesmente somar o número total de elementos de cada subespaço, já que alguns seriam contados mais de uma vez. Ou seja, aqueles que aparecem também nas intersecções devem ser excluídos.

Aplicando o princípio da inclusão-exclusão obtemos:

$$|C(I)^s| = \sum_i |T_i^s| - \sum_{i<j} |T_i^s \cap T_j^s| + \sum_{i<j<k} |T_i^s \cap T_j^s \cap T_k^s| - \cdots$$

Pelo Lema 2.67 sabemos que para s suficientemente grande, o número de pontos em cada T_i^s é um polinômio de grau $m_i = \dim(T_i) \leq d$ na variável s, cujo coeficiente de s^{m_i} é $1/(m_i!)$. Note que o primeiro somatório é um polinômio de grau exatamente d na variável s, já que algum T_i tem dimensão d e os coeficientes, por serem todos positivos, não se cancelam.
Se os polinômios correspondentes aos demais somatórios tiverem grau menor, então $|C(I)^s|$ é um polinômio de grau d na variável s.
Note que a interseção de duas translações distintas de subespaços coordenados de dimensões m e r em $\mathbb{Z}_{\geq 0}^n$ ou é vazia ou é uma translação de um subespaço de dimensão $< max(m, r)$. Assim, no segundo somatório, como $T_i \neq T_j$ então cada $T_i \cap T_j$ é uma translação de subespaços coordenados de $\mathbb{Z}_{\geq 0}^n$ de dimensão $< d$. Portanto, pelo Lema 2.67, o número de pontos em cada $T_i^s \cap T_j^s$ é um polinômio de grau $< d$. Somando estas interseções para $i < j$, obtemos então um polinômio de grau $< d$ na variável s.
Analogamente procede-se aos demais somatórios, seguindo portanto que $|C(I)^s|$ é polinômio de grau d na variável s como desejado. ■

Retomando o Exemplo 2.64, temos $I = \langle x^4y^3, x^2y^5 \rangle$, com $C(I) = C_0 \cup C_1$, onde
$C_1 = [e_1] \cup (e_2 + [e_1]) \cup (2e_2 + [e_1]) \cup [e_2] \cup (e_1 + [e_2])$ e
$C_0 = \{(3, 4), (3, 3), (2, 4), (2, 3)\}$.
Para contar o número de pontos em C_1 de grau $\leq s$ devemos contar em cada translação e subtrair aqueles que foram contados mais de uma vez. O número de pontos em $[e_2]$ é $\binom{1+s}{s} = \binom{1+s}{1} = s + 1$. O número de pontos em $e_1 + [e_2]$ é $\binom{1+(s-1)}{s-1} = s$. Similarmente, o número de pontos em $[e_1]$, $e_2 + [e_1]$ e $2e_2 + [e_1]$ é, respectivamente, $s + 1$, s e $s - 1$.
De todas as possíveis interseções, as únicas não-vazias consistem de um único ponto, a saber: $(1, 2), (1, 1), (1, 0), (0, 2), (0, 1), (0, 0)$. Portanto, para s suficientemente grande, o número de pontos em C_1 de grau $\leq s$ é dado por:

$$|C_1^s| = (s + 1) + s + (s + 1) + s + (s - 1) - 6 = 5s - 5$$

Como em C_0 temos quatro pontos, então:

$$|C(I)^s| = (5s - 5) + 4 = 5s - 1.$$

Seja $R = \kappa[x_1, \ldots, x_n]$. Denote por $R_{\leq s} = \kappa[x_1, \ldots, x_n]_{\leq s}$ o conjunto de polinômios com

grau total $\leq s$ em R. Então $R_{\leq s}$ pode ser visto como um espaço vetorial de dimensão $\binom{n+s}{s}$. Dado um ideal $I \subseteq R$, denotemos por $I_{\leq s} = I \cap R_{\leq s}$, o conjunto de polinômios em I de grau total $\leq s$, de modo que $I_{\leq s}$ é um subespaço vetorial de $R_{\leq s}$.

Definição 2.69. *A função afim de Hilbert de um ideal $I \subseteq R = \kappa[x_1, \ldots, x_n]$ é a função ${}^aHF_{R/I}$ sobre os inteiros não-negativos definida por:*

$$ {}^aHF_{R/I}(s) = \dim(R_{\leq s}/I_{\leq s}) = \dim R_{\leq s} - \dim I_{\leq s}, $$

com $s \in \mathbb{Z}_{\geq 0}$.

Assim com essa terminologia podemos reescrever os resultados para ideais monomiais a seguir:
Seja I um ideal monomial em $R = \kappa[x_1, \ldots, x_n]$. Então:

(i) Para $s \geq 0$ inteiro, ${}^aHF_{R/I}(s)$ é o número de monômios que não estão em I de grau total $\leq s$;

(ii) Para s suficientemente grande, a função afim de Hilbert de I é dada pela função polinomial ${}^aHF_{R/I}(s) = \sum_{i=0}^{d} b_i \binom{s}{d-i}$, com $b_i \in \mathbb{Z}$ e $b_0 > 0$;

(iii) O grau do polinômio correspondente à função é o máximo das dimensões dos subespaços coordenados contidos em $V(I)$.

A proposição seguinte será importante para o processo de obtenção da dimensão de uma variedade a partir do ideal monomial dos termos líderes.

Note que precisamos fixar uma ordem monomial cujo primeiro critério de ordenação seja o grau total dos monômios, como é o caso na ordem lexicográfica graduada.

Proposição 2.70. *Seja $I \subseteq R = \kappa[x_1, \ldots, x_n]$ um ideal e $>$ uma ordem monomial graduada sobre R. Então o ideal monomial $\langle LT(I) \rangle$ tem a mesma função afim de Hilbert que I.*

Demonstração. Assumamos que $I \neq \{0\}$. Fixe s e considere o conjunto dos monômios líderes $LM(f)$ de todos os elementos $f \in I_{\leq s}$:

$$ \{LM(f) \mid f \in I_{\leq s}\} = \{LM(f_1), \ldots, LM(f_m)\}. \tag{2.1} $$

para alguns polinômios $f_i \in I_{\leq s}$.
Ordenando e suprimindo os duplicados, podemos assumir que $LM(f_1) > LM(f_2) > \cdots > LM(f_m)$. Afirmamos que $f_1, \ldots, f_m$ formam uma base para $I_{\leq s}$ como um espaço vetorial sobre κ.
Para verificar isso, considere uma combinação linear não-trivial $a_1 f_1 + \cdots + a_m f_m$ e escolha

o menor i tal que $a_i \neq 0$. Então da forma que ordenamos os monômios líderes não há termo que cancele $a_i LM(f_i)$, de modo que essa combinação linear é não-nula. Consequentemente $f_1, \ldots, f_m$ são linearmente independentes.
Seja $W = [f_1, \ldots, f_m] \subseteq I_{\leq s}$ o subespaço gerado por $f_1, \ldots, f_m$. Se $W \neq I_{\leq s}$, tome $f \in I_{\leq s} \setminus W$ com $LM(f)$ mínimo. Então $LM(f) = LM(f_i)$ para algum i e, consequentemente $LT(f) = \lambda LT(f_i)$ para algum $\lambda \in \kappa$. Assim $f - \lambda f_i \in I_{\leq s}$ e seu monômio líder tem grau menor que f, de modo que $f - \lambda f_i \in W$ pela minimalidade de $LM(f)$. Isso implicaria que $f \in W$, uma contradição. Portanto, segue que $W = [f_1, \ldots, f_m] = I_{\leq s}$, e $f_1, \ldots, f_m$ formam uma base para $I_{\leq s}$.
O ideal monomial $\langle LT(I) \rangle$ é gerado pelos termos líderes, e portanto pelos monômios líderes dos elementos de I. Assim $LM(f_i) \in \langle LT(I) \rangle_{\leq s}$ já que $f_i \in I_{\leq s}$. Afirmamos agora que $LM(f_1), \ldots, LM(f_m)$ formam uma base para $\langle LT(I) \rangle_{\leq s}$ como espaço vetorial. De modo análogo ao feito acima, podemos ver que $LM(f_1), \ldots, LM(f_m)$ são linearmente independentes. E assim, resta mostrar que $[LM(f_1), \ldots, LM(f_m)] = \langle LT(I) \rangle_{\leq s}$.
Isso equivale a verificar que

$$\{LM(f_1), \ldots, LM(f_m)\} = \{LM(f) \mid f \in I, \deg(LM(f)) \leq s\}. \tag{2.2}$$

Mas note que como $>$ é uma ordem monomial graduada, então para todo $0 \neq f \in \kappa[x_1, \ldots, x_n]$ temos $\deg(LM(f)) = \deg(f)$. Assim, em particular, se $\deg(LM(f)) \leq s$ então $\deg(f) \leq s$. Portanto (2.2) segue imediatamente de (2.1). Como $I_{\leq s}$ e $\langle LT(I) \rangle_{\leq s}$ possuem a mesma dimensão, implica que suas funções afins de Hilbert são

$$^aHF_{R/I}(s) = \dim(R_{\leq s}/I_{\leq s}) = \dim(R_{\leq s}/\langle LT(I) \rangle_{\leq s}) = {}^aHF_{R/\langle LT(I) \rangle}(s).$$

■

Com as definições e proposições seguintes podemos caracterizar a dimensão de uma variedade a partir do polinômio de Hilbert.

Definição 2.71. O polinômio correspondente à função afim de Hilbert $^aHF_{R/I}(s)$ para s suficientemente grande é chamado polinômio afim de Hilbert de I e é denotado por $^aHP_{R/I}(s)$.

Proposição 2.72. *Seja $I \subseteq R = \kappa[x_1, \ldots, x_n]$ um ideal, então os polinômios afins de Hilbert de I e $\sqrt{I}$ possuem o mesmo grau.*

Demonstração. Veja [2, pág 489].

Definição 2.73. *A dimensão de uma variedade afim $V \subseteq \mathbb{A}^n(\kappa)$ não-vazia, denotada por $\dim V$, é o grau do polinômio afim de Hilbert do ideal correspondente $I = \mathbf{I}(V) \subseteq \kappa[x_1, \ldots, x_n]$.*

O teorema seguinte mostra que quando κ é algebricamente fechado então para obter a dimensão de uma variedade afim $\mathbf{V}(I)$ podemos usar o processo de obtenção da dimensão da variedade do ideal monomial $\mathbf{V}(\langle LT(I) \rangle)$.

Teorema 2.74 (Teorema da Dimensão)**.** *Seja $V = \mathbf{V}(I)$ uma variedade afim não-vazia, onde $I \subseteq R = \kappa[x_1, \ldots, x_n]$ é um ideal. Se κ é algebricamente fechado, então* $\dim V = \deg({}^aHP_{R/I})$. *Se, além disso, $>$ é uma ordem monomial graduada então* $\dim V = \deg {}^aHP_{R/\langle LT(I)\rangle}$.

Demonstração. Sendo κ algebricamente fechado, segue pelo Teorema 2.13 que

$$\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$$

Assim, pela Definição 2.73 temos que: $\dim V = \deg({}^aHP_{R/\mathbf{I}(V)}) = \deg({}^aHP_{R/\sqrt{I}}) = \deg({}^aHP_{R/I})$, com a última igualdade seguindo da Proposição 2.72. Se $>$ é uma ordem graduada então pela Proposição 2.70 segue que: $\dim V = \deg({}^aHP_{R/I}) = \deg {}^aHP_{R/\langle LT(I)\rangle}$. ■

Assim, o Teorema 2.74 nos permite calcular a dimensão de uma variedade afim $V = \mathbf{V}(I)$ da seguinte forma:

- Calculamos uma base de Gröbner $\mathcal{G}$ para o ideal I, usando uma ordem graduada;
- Calculamos a dimensão d do maior subespaço coordenado contido em $\mathbf{V}(\langle LT(I)\rangle)$, o que pode ser feito seguindo os passos da Proposição 2.58.
- Por fim, segue do Teorema anterior que $\dim V = d$.

CAPÍTULO 3

A VARIEDADE DAS ÁLGEBRAS DE JORDAN DE DIMENSÃO 2 E 3

Definição 3.1. Uma $\kappa-$álgebra de Jordan A, é uma álgebra onde a multiplicação $*$ satisfaz as seguintes identidades para quaisquer x, y na álgebra:

- $x * y = y * x$;
- $((x^2) * y) * x = (x^2) * (y * x)$

Podemos notar que é uma álgebra comutativa mas com uma associatividade fraca. Em nosso estudo consideraremos o caso em que κ é um corpo algebricamente fechado de $char(\kappa) = 0$, e omitiremos $*$. Denotaremos por $Jor_n(\kappa)$ o conjunto das álgebras de Jordan de dimensão n.

Seja $(a, b, c) = (ab)c - a(bc)$ o associador de a, b, c e tomando $J(x, y) = (x^2, y, x)$. Seja ainda $\{e_1, e_2\}$ base de $A \in Jor_2(\kappa)$, isto é, de uma álgebra de Jordan de dimensão 2 com as constantes de estrutura a seguir:

$$\begin{cases} e_1^2 = x_1e_1 + x_2e_2 \\ e_1e_2 = x_3e_1 + x_4e_2 = e_2e_1 \\ e_2^2 = x_5e_1 + x_6e_2 \end{cases}$$

Obtenhamos as identidades polinomiais que relacionam essas constantes de estrutura. Para tal, note primeiramente que $J(x, y)$ é linear na segunda entrada $J(x, \_)$ mas não é linear na primeira entrada $J(\_, y)$. De fato:

$$\begin{aligned} J(x, y + z) = (x^2, y + z, x) &= ((x^2)(y + z))x - (x^2)((y + z)x) \\ &= (x^2y + x^2z)x - x^2(yx + zx) \end{aligned}$$

$$
\begin{aligned}
&= (x^2y)x + (x^2z)x - x^2(yx) - x^2(zx)\\
&= J(x,y) + J(x,z)
\end{aligned}
$$

Mas

$$
\begin{aligned}
J(x+z,y) &= ((x+z)^2, y, x+z) = ((x+z)^2y)(x+z) - (x+z)^2(y(x+z))\\
&= ((x^2+2(xz)+z^2)y)(x+z) - (x^2+2(xz)+z^2)(yx+yz)\\
&= (x^2y+2(xz)y+z^2y)(x+z) - (x^2)(yx) - (x^2)(yz) - 2(xz)(yx) -\\
&- 2(xz)(yz) - (z^2)(yx) - (z^2)(yz)\\
&= (x^2y)x + (x^2y)z + 2((xz)y)x + 2((xz)y)z + (z^2y)x + (z^2y)z -\\
&- (x^2)(yx) - (x^2)(yz) - 2(xz)(yx) - 2(xz)(yz) - (z^2)(yx) - (z^2)(yz)\\
&= J(x,y) + J(z,y) + (x^2,y,z) + (z^2,y,x) +\\
&+ 2[((xz)y)x - (xz)(yx)] + 2[((xz)y)z - (xz)(yz)]\\
&= J(x,y) + J(z,y) + 2[((xz)y)x - (xz)(yx)] + 2[((xz)y)z - (xz)(yz)] +\\
&+ (x^2,y,z) + (z^2,y,x)
\end{aligned}
$$

Desse modo, precisamos calcular $J(e_1,e_1), J(e_1,e_2), J(e_2,e_1), J(e_2,e_2), J(e_1+te_2,e_1)$ e $J(e_1+te_2,e_2)$, onde o parâmetro $t \in \kappa$.

Calculemos $J(e_1,e_1)$:

$$
\begin{aligned}
J(e_1,e_1) &= (e_1^2e_1)e_1 - e_1^2(e_1e_1)\\
&= ((x_1e_1+x_2e_2)e_1)e_1 - (x_1e_1+x_2e_2)(x_1e_1+x_2e_2)\\
&= (x_1e_1^2 + x_2e_2e_1)e_1 - x_1^2e_1^2 - 2x_1x_2e_1e_2 - x_2^2e_2^2\\
&= (x_1(x_1e_1+x_2e_2) + x_2(x_3e_1+x_4e_2))e_1 -\\
&- x_1^2(x_1e_1+x_2e_2) - 2x_1x_2(x_3e_1+x_4e_2) - x_2^2(x_5e_1+x_6e_2)\\
&= x_1^2e_1^2 + x_1x_2e_1e_2 + x_2x_3e_1^2 + x_2x_4e_2e_1 -\\
&- x_1^3e_1 - x_1^2x_2e_2 - 2x_1x_2x_3e_1 - 2x_1x_2x_4e_2 - x_2^2x_5e_1 - x_2^2x_6e_2\\
&= x_1^2(x_1e_1+x_2e_2) + x_1x_2(x_3e_1+x_4e_2) + x_2x_3(x_1e_1+x_2e_2) +\\
&+ x_2x_4(x_3e_1+x_4e_2) - x_1^3e_1 - x_1^2x_2e_2 - 2x_1x_2x_3e_1 -\\
&- 2x_1x_2x_4e_2 - x_2^2x_5e_1 - x_2^2x_6e_2\\
&= (x_1^3 + x_1x_2x_3 + x_1x_2x_3 + x_2x_3x_4 - x_1^3 - 2x_1x_2x_3 - x_2^2x_5)e_1 +\\
&+ (x_1^2x_2 + x_1x_2x_4 + x_2^2x_3 + x_2x_4^2 - x_1^2x_2 - 2x_1x_2x_4 - x_2^2x_6)e_2\\
&= (-x_2^2x_5 + x_2x_3x_4)e_1 + (-x_1x_2x_4 + x_2^2x_3 - x_2^2x_6 + x_2x_4^2)e_2
\end{aligned}
$$

Assim, como $J(e_1,e_1) = 0$, obtemos as duas primeiras identidades polinomiais:
$f_{11}^1 = -x_2^2x_5 + x_2x_3x_4 = 0$ e

$f_{11}^2 = -x_1x_2x_4 + x_2^2x_3 - x_2^2x_6 + x_2x_4^2 = 0,$
onde f_{ij}^k denota o polinômio obtido em $J(e_i, e_j)$ com respeito à componente e_k.

De modo análogo, calculando $J(e_1, e_2), J(e_2, e_1), J(e_2, e_2)$ obtemos as seguintes identidades polinomiais:
$f_{12}^1 = x_1x_2x_5 - x_2x_3^2 + x_2x_3x_6 - x_2x_4x_5 = 0;$
$f_{12}^2 = x_2^2x_5 - x_2x_3x_4 = 0;$
$f_{21}^1 = x_2x_5^2 - x_3x_4x_5 = 0;$
$f_{21}^2 = x_1x_4x_5 - x_2x_3x_5 + x_2x_5x_6 - x_4^2x_5 = 0;$
$f_{22}^1 = -x_1x_5^2 + x_3^2x_5 - x_3x_5x_6 + x_4x_5^2 = 0;$
$f_{22}^2 = -x_2x_5^2 + x_3x_4x_5 = 0.$

Calculemos agora o caso $J(e_1 + te_2, e_2)$:

$$\begin{aligned}
J(e_1+te_2,e_2) &= ((e_1+te_2)^2e_2)(e_1+te_2) - (e_1+te_2)^2(e_2(e_1+te_2)) \\
&= ((e_1^2+2te_1e_2+t^2e_2^2)e_2)(e_1+te_2) - (e_1^2+2te_1e_2+t^2e_2^2)(e_2e_1+te_2^2) \\
&= ((e_1^2)e_2+2t(e_1e_2)e_2+(t^2e_2^2)e_2)(e_1+te_2) - (e_1^2(e_2e_1)+e_1^2(te_2^2)+(2te_1e_2)(e_2e_1)+ \\
&+ (2te_1e_2)(te_2^2)+(t^2e_2^2)(e_2e_1)+(t^2e_2^2)(te_2^2)) \\
&= (e_1^2e_2)e_1 - e_1^2(e_2e_1) + ((te_2)^2e_2)(te_2) - (te_2)^2(e_2(te_2)) + ((x_1e_1+x_2e_2)e_2)(te_2)+ \\
&+ (t^2(x_5e_1+x_6e_2)e_2)e_1 + (2t(x_3e_1+x_4e_2)e_2)e_1 + (2t(x_3e_1+x_4e_2)e_2)(te_2)- \\
&- (x_1e_1+x_2e_2)(t(x_5e_1+x_6e_2)) - (2t(x_3e_1+x_4e_2)(x_3e_1+x_4e_2))- \\
&- (2t(x_3e_1+x_4e_2))(t(x_5e_1+x_6e_2)) - (t^2(x_5e_1+x_6e_2))(x_3e_1+x_4e_2) \\
&= J(e_1,e_2)+J(te_2,e_2)+(x_1e_1e_2+x_2e_2^2)(te_2)+(t^2x_5e_1e_2+t^2x_6e_2^2)e_1+ \\
&+ (2tx_3e_1e_2+2tx_4e_2^2)e_1 + (2tx_3e_1e_2+2tx_4e_2^2)(te_2)- \\
&- (tx_1x_5e_1^2+tx_1x_6e_1e_2+tx_2x_5e_2e_1+tx_2x_6e_2^2)- \\
&- (2tx_3^2e_1^2+2tx_3x_4e_1e_2+2tx_3x_4e_2e_1+2tx_4^2e_2^2)- \\
&- (2t^2x_3x_5e_1^2+2t^2x_3x_6e_1e_2+2t^2x_4x_5e_2e_1+2t^2x_4x_6e_2^2)- \\
&- (t^2x_3x_5e_1^2+t^2x_4x_5e_1e_2+t^2x_3x_6e_2e_1+t^2x_4x_6e_2^2) \\
&= tx_1x_3e_1e_2+tx_1x_4e_2^2+tx_2x_5e_1e_2+tx_2x_6e_2^2+ \\
&+ t^2x_3x_5e_1^2+t^2x_4x_5e_2e_1+t^2x_5x_6e_1^2+t^2x_6^2e_2e_1+ \\
&+ 2tx_3^2e_1^2+2tx_3x_4e_2e_1+2tx_4x_5e_1^2+2tx_4x_6e_2e_1+ \\
&+ 2t^2x_3^2e_1e_2+2t^2x_3x_4e_2^2+2t^2x_4x_5e_1e_2+2t^2x_4x_6e_2^2- \\
&- tx_1^2x_5e_1-tx_1x_2x_5e_2-tx_1x_3x_6e_1-tx_1x_4x_6e_2- \\
&- tx_2x_3x_5e_1-tx_2x_4x_5e_2-tx_2x_5x_6e_1-tx_2x_6^2e_2- \\
&- 2tx_1x_3^2e_1-2tx_2x_3^2e_2-2tx_3^2x_4e_1-2tx_3x_4^2e_2- \\
&- 2tx_3^2x_4e_1-2tx_3x_4^2e_2-2tx_4^2x_5e_1-2tx_4^2x_6e_2-
\end{aligned}$$

$$
\begin{aligned}
&- 2t^2x_1x_3x_5e_1 - 2t^2x_2x_3x_5e_2 - 2t^2x_3^2x_6e_1 - 2t^2x_3x_4x_6e_2 - \\
&- 2t^2x_3x_4x_5e_1 - 2t^2x_4^2x_5e_2 - 2t^2x_4x_5x_6e_1 - 2t^2x_4x_6^2e_2 - \\
&- t^2x_1x_3x_5e_1 - t^2x_2x_3x_5e_2 - t^2x_3x_4x_5e_1 - t^2x_4^2x_5e_2 - \\
&- t^2x_3^2x_6e_1 - t^2x_3x_4x_6e_2 - t^2x_4x_5x_6e_1 - t^2x_4x_6^2e_2 \\
&= (t(x_1x_3^2 + x_1x_4x_5 + x_2x_3x_5 + x_2x_5x_6 + \\
&+ 2x_1x_3^2 + 2x_3^2x_4 + 2x_1x_4x_5 + 2x_3x_4x_6 - \\
&- x_1^2x_5 - x_1x_3x_6 - x_2x_3x_5 - x_2x_5x_6 - \\
&- 2x_1x_3^2 - 2x_3^2x_4 - 2x_3^2x_4 - 2x_4^2x_5) + \\
&+ t^2(x_1x_3x_5 + x_3x_4x_5 + x_1x_5x_6 + x_3x_6^2 + \\
&+ 2x_3^3 + 2x_3x_4x_5 + 2x_3x_4x_5 + 2x_4x_5x_6 - \\
&- 2x_1x_3x_5 - 2x_3^2x_6 - 2x_3x_4x_5 - 2x_4x_5x_6 - \\
&- x_1x_3x_5 - x_3x_4x_5 - x_3^2x_6 - x_4x_5x_6))e_1 + \\
&+ (t(x_1x_3x_4 + x_1x_4x_6 + x_2x_4x_5 + x_2x_6^2 + \\
&+ 2x_2x_3^2 + 2x_3x_4^2 + 2x_2x_4x_5 + 2x_4^2x_6 - \\
&- x_1x_2x_5 - x_1x_4x_6 - x_2x_4x_5 - x_2x_6^2 - \\
&- 2x_2x_3^2 - 2x_3x_4^2 - 2x_3x_4^2 - 2x_4^2x_6) + \\
&+ t^2(x_2x_3x_5 + x_4^2x_5 + x_2x_5x_6 + x_4x_6^2 + \\
&+ 2x_3^2x_4 + 2x_3x_4x_6 + 2x_4^2x_5 + 2x_4x_6^2 - \\
&- 2x_2x_3x_5 - 2x_3x_4x_6 - 2x_4^2x_5 - 2x_4x_6^2 - \\
&- x_2x_3x_5 - x_4^2x_5 - x_3x_4x_6 - x_4x_6^2))e_2
\end{aligned}
$$

Assim, com as devidas simplificações, obtemos as quatro identidades polinomiais seguintes:
$f^1_{t,2} = -x_1^2y_5 + x_1x_3^2 - x_1x_3x_6 + 3x_1x_4x_5 - 2x_3^2x_4 + 2x_3x_4x_6 - 2x_4^2x_5 = 0$;
$f^1_{t^2,2} = -2x_1x_3x_5 + x_1x_5x_6 + 2x_3^3 - 3x_3^2x_6 + 2x_3x_4x_5 + x_3x_6^2 - x_4x_5x_6 = 0$;
$f^2_{t,2} = -x_1x_2y_5 + x_1x_3x_4 + 2x_2x_4x_5 - 2x_3x_4^2 = 0$;
$f^2_{t^2,2} = -2x_2x_3x_5 + x_2x_5x_6 + 2x_3^2x_4 - x_3x_4x_6 = 0$,
onde $f^i_{t,k}$ e $f^i_{t^2,k}$ denotam o polinômio obtido em $J(e_1 + te_2, e_i)$ com respeito à componente e_k e ao parâmetro t ou t^2, respectivamente.

De modo análogo, calculando $J((e_1 + te_2, e_1))$ obtemos as demais quatro identidades polinomiais seguintes:
$f^1_{t,1} = x_1x_2x_5 - x_1x_3x_4 + 2x_3x_4^2 - 2x_2x_4x_5 = 0$;
$f^1_{t^2,1} = -2x_3^2x_4 + 2x_2x_3x_5 + x_3x_4x_6 - x_2x_5x_6 = 0$;
$f^2_{t,1} = x_1^2x_4 - x_1x_2x_3 + x_1x_2x_6 - 3x_1x_4^2 + 2x_2x_3x_4 - 2x_2x_4x_6 + 2x_4^3 = 0$;
$f^2_{t^2,1} = 2x_1x_3x_4 - 2x_3x_4^2 - x_1x_4x_6 - 2x_2x_3^2 + 3x_2x_3x_6 - x_2x_6^2 + x_4^2x_6 = 0$

Assim a variedade afim das álgebras de Jordan de dimensão 2, $Jor_2(\kappa)$, no espaço afim $\mathbb{A}^6(\kappa)$, é determinada por 16 polinômios que denotaremos por:

$$g_1 = f^1_{11}, g_2 = f^2_{11}, g_3 = f^1_{12}, g_4 = f^2_{12}, g_5 = f^1_{21}, g_6 = f^i_{21} g_7 = f^1_{22}, g_8 = f^2_{22},$$

$$g_9 = f^1_{t,2}, g_{10} = f^1_{t^2,2}, g_{11} = f^2_{t,2}, g_{12} = f^2_{t^2,2}, g_{13} = f^1_{t,1}, g_{14} = f^1_{t^2,1}, g_{15} = f^2_{t,1}, g_{16} = f^2_{t^2,1}$$

Portanto para obter sua dimensão e componentes irredutíveis, precisamos calcular uma base de Gröbner para o ideal $I = \langle g_1, \ldots, g_{16} \rangle \subset \kappa[x_1, x_2, x_3, x_4, x_5, x_6]$. Para tal, adotaremos a ordem monomial lexicográfica graduada $x_1 >_{grlex} \cdots >_{grlex} x_6$.

Dessa forma, seja a $16-$úpla ordenada $G = (g_1, \ldots, g_{16})$, iniciemos o cálculo com os $S-$polinômios dos primeiros pares de polinômios:

$$\begin{aligned} S(g_1, g_2) &= \frac{x_1 x_2^2 x_4 x_5}{-x_2^2 x_5}(-x_2^2 x_5 + x_2 x_3 x_4) - \frac{x_1 x_2^2 x_4 x_5}{-x_1 x_2 x_4}(-x_1 x_2 x_4 + x_2^2 x_3 - x_2^2 x_6 + x_2 x_4^2) \\ &= -x_1 x_2 x_3 x_4^2 + x_2^3 x_3 x_5 - x_2^3 x_5 x_6 + x_2^2 x_4^2 x_5 \end{aligned}$$

Onde o resto por G é $\overline{S(g_1, g_2)}^G = 0$, uma vez que $S(g_1, g_2) = (-x_2 x_3 + x_2 x_6 - x_4^2) g_1 + (x_3 x_4) g_2$.

$$\begin{aligned} S(g_1, g_3) &= \frac{x_1 x_2^2 x_5}{-x_2^2 x_5}(-x_2^2 x_5 + x_2 x_3 x_4) - \frac{x_1 x_2^2 x_5}{x_1 x_2 x_5}(x_1 x_2 x_5 - x_2 x_3^2 + x_2 x_3 x_6 - x_2 x_4 x_5) \\ &= -x_1 x_2 x_3 x_4 + x_2^2 x_3^2 - x_2^2 x_3 x_6 + x_2^2 x_4 x_5 \end{aligned}$$

Onde o resto por G é $\overline{S(g_1, g_3)}^G = 0$, uma vez que $S(g_1, g_3) = (-x_4) g_1 + (x_3) g_2$.

$$S(g_1, g_4) = \frac{x_2^2 x_5}{-x_2^2 x_5}(-x_2^2 x_5 + x_2 x_3 x_4) - \frac{x_2^2 x_5}{x_2^2 x_5}(x_2^2 x_5 - x_2 x_3 x_4) = 0$$

Onde, claramente, o resto por G é $\overline{S(g_1, g_4)}^G = 0$.

Prosseguindo, de modo análogo, obtemos que o resto dos $S-$polinômios $\overline{S(g_1, g_i)}^G = 0$ para $5 \leq i \leq 16$. Bem como, verifica-se que o resto dos $S-$polinômios $\overline{S(g_2, g_j)}^G = 0$ para $3 \leq j \leq 8$.

Contudo, ao calcular $S(g_2, g_9)$, obtemos:

$$\begin{aligned} S(g_2, g_9) &= \frac{x_1 x_2 x_4 x_5}{-x_1 x_2 x_4}(-x_1 x_2 x_4 + x_2^2 x_3 - x_2^2 x_6 + x_2 x_4^2) - \\ &\quad - \frac{x_1 x_2 x_4 x_5}{x_1 x_2 x_5}(x_1 x_2 x_5 - x_1 x_3 x_4 + 2 x_3 x_4^2 - 2 x_2 x_4 x_5) \\ &= x_1 x_3 x_4^2 - x_2^2 x_3 x_5 + x_2^2 x_5 x_6 + x_2 x_4^2 x_5 - 2 x_3 x_4^3 \end{aligned}$$

Onde o resto por G é:

$$\overline{S(g_2, g_9)}^G = \frac{1}{2} x_1 x_4^2 x_6 - \frac{1}{2} x_2 x_3 x_4 x_6 + x_2 x_4^2 x_5 + \frac{1}{2} x_2 x_4 x_6^2 - x_3 x_4^3 - \frac{1}{2} x_4^3 x_6$$

$$= \frac{1}{2}x_4(x_1x_4x_6 - x_2x_3x_6 + 2x_2x_4x_5 + x_2x_6^2 - 2x_3x_4^2 - x_4^2x_6) \neq 0$$

Portanto, como obtivemos um $S-$polinômio cujo resto por G é não-nulo, então $\mathcal{G}= \{g_1, \ldots, g_{16}\}$ não é uma base de Gröbner para o ideal $I = \langle g_1, \ldots, g_{16}\rangle$.

Tomemos então $g_{17} = x_1x_4x_6 - x_2x_3x_6 + 2x_2x_4x_5 + x_2x_6^2 - 2x_3x_4^2 - x_4^2x_6$ e consideremos $\mathcal{G}= \{g_1, \ldots, g_{17}\}$.

Agora, temos que $\overline{S(g_2, g_9)}^G = 0$ uma vez que $S(g_2, g_9) = (x_3-x_6)g_1+\frac{1}{2}x_4(g_{12})+\frac{1}{2}x_4(g_{17})$.

Calculando, de modo análogo, obtemos que $\overline{S(g_i, g_j)}^G = 0$ para todos os pares $1 \leq i < j \leq 17$ e logo $\mathcal{G}= \{g_1, \ldots, g_{17}\}$ é uma base de Gröbner para o ideal I.

Implementando o cálculo da base por meio do algoritmo no software SageMath, obtemos o seguinte resultado:

```
SageMath version 9.3 Console

sage: P.<x_1, x_2, x_3, x_4, x_5, x_6> = PolynomialRing(CC, 6, order = "deglex")
sage: g_1 = - x_2^2*x_5 + x_2*x_3*x_4
sage: g_2 = - x_1*x_2*x_4 + x_2^2*x_3 - x_2^2*x_6 + x_2*x_4^2
sage: g_3 = x_1*x_2*x_5 - x_2*x_3^2 + x_2*x_3*x_6 - x_2*x_4*x_5
sage: g_4 = x_2^2*x_5 - x_2*x_3*x_4
sage: g_5 = x_2*x_5^2 - x_3*x_4*x_5
sage: g_6 = x_1*x_4*x_5 - x_2*x_3*x_5 + x_2*x_5*x_6 - x_4^2*x_5
sage: g_7 = - x_1*x_5^2 + x_3^2*x_5 - x_3*x_5*x_6 + x_4*x_5^2
sage: g_8 = - x_2*x_5^2 + x_3*x_4*x_5
sage: g_9 = x_1*x_2*x_5 - x_1*x_3*x_4 + 2*x_3*x_4^2 - 2*x_2*x_4*x_5
sage: g_10 = - 2*x_3^2*x_4 + 2*x_2*x_3*x_5 + x_3*x_4*x_6 - x_2*x_5*x_6
sage: g_11 = x_1^2*x_4 - x_1*x_2*x_3 + x_1*x_2*x_6 - 3*x_1*x_4^2 + 2*x_2*x_3*x_4
....: - 2*x_2*x_4*x_6 + 2*x_4^3
sage: g_12 = 2*x_1*x_3*x_4 - 2*x_3*x_4^2 - x_1*x_4*x_6 - 2*x_2*x_3^2 + 3*x_2*x_3
....: *x_6 - x_2*x_6^2 + x_4^2*x_6
sage: g_13 = - x_1^2*x_5 + x_1*x_3^2 - x_1*x_3*x_6 + 3*x_1*x_4*x_5 - 2*x_3^2*x_4
....: + 2*x_3*x_4*x_6 - 2*x_4^2*x_5
sage: g_14 = - 2*x_1*x_3*x_5 + x_1*x_5*x_6 + 2*x_3^3 - 3*x_3^2*x_6 + 2*x_3*x_4*x
....: _5 + x_3*x_6^2 - x_4*x_5*x_6
sage: g_15 = -x_1*x_2*x_5 + x_1*x_3*x_4 + 2*x_2*x_4*x_5 - 2*x_3*x_4^2
sage: g_16 = -2*x_2*x_3*x_5 + x_2*x_5*x_6 + 2*x_3^2*x_4 - x_3*x_4*x_6
sage: I = ideal([g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_10, g_11, g_12,
....: g_13, g_14, g_15, g_16])
sage: G = I.groebner_basis('toy:buchberger')
sage: print(G)
[x_1^2*x_4 - x_1*x_2*x_3 + x_1*x_2*x_6 + (-3.00000000000000)*x_1*x_4^2 + 2.00000000
....: 000000*x_2*x_3*x_4 + (-2.00000000000000)*x_2*x_4*x_6 + 2.00000000000000*x_4^3,
....: x_1^2*x_5 - x_1*x_3^2 + x_1*x_3*x_6 + (-3.00000000000000)*x_1*x_4*x_5 + 2.000
....: 00000000000*x_3^2*x_4 + (-2.00000000000000)*x_3*x_4*x_6 + 2.00000000000000*x_4
....: ^2*x_5, x_1*x_2*x_4 - x_2^2*x_3 + x_2^2*x_6 - x_2*x_4^2, x_1*x_2*x_5 - x_1*x_3
....: *x_4 + (-2.00000000000000)*x_2*x_4*x_5 + 2.00000000000000*x_3*x_4^2, x_1*x_2*x
```

```
....: _5 - x_2*x_3^2 + x_2*x_3*x_6 - x_2*x_4*x_5, x_1*x_2*x_5 - x_1*x_3*x_4 + (-2.00
....: 000000000000)*x_2*x_4*x_5 + 2.00000000000000*x_3*x_4^2, x_1*x_3*x_4 + (-0.5000
....: 00000000000)*x_1*x_4*x_6 - x_2*x_3^2 + 1.50000000000000*x_2*x_3*x_6 + (-0.5000
....: 00000000000)*x_2*x_6^2 - x_3*x_4^2 + 0.500000000000000*x_4^2*x_6, x_1*x_3*x_5
....: + (-0.500000000000000)*x_1*x_5*x_6 - x_3^3 + 1.50000000000000*x_3^2*x_6 - x_3*
....: x_4*x_5 + (-0.500000000000000)*x_3*x_6^2 + 0.500000000000000*x_4*x_5*x_6, x_1*
....: x_4*x_5 - x_2*x_3*x_5 + x_2*x_5*x_6 - x_4^2*x_5, x_1*x_4*x_6 - x_2*x_3*x_6 + 2
....: .00000000000000*x_2*x_4*x_5 + x_2*x_6^2 + (-2.00000000000000)*x_3*x_4^2 - x_4^
....: 2*x_6, x_1*x_5^2 - x_3^2*x_5 + x_3*x_5*x_6 - x_4*x_5^2, x_2^2*x_5 - x_2*x_3*x_
....: 4, x_2^2*x_5 - x_2*x_3*x_4, x_2*x_3*x_5 + (-0.500000000000000)*x_2*x_5*x_6 - x
....: _3^2*x_4 + 0.500000000000000*x_3*x_4*x_6, x_2*x_3*x_5 + (-0.500000000000000)*x
....: _2*x_5*x_6 - x_3^2*x_4 + 0.500000000000000*x_3*x_4*x_6, x_2*x_5^2 - x_3*x_4*x_
....: 5, x_2*x_5^2 - x_3*x_4*x_5]
sage: len(G)
17
sage: H =I.groebner_basis()
sage: print(H)
[x_1^2*x_4 - x_1*x_2*x_3 + x_1*x_2*x_6 + (-3.00000000000000)*x_1*x_4^2 + 2.000000000
....: 00000*x_2*x_3*x_4 + (-2.00000000000000)*x_2*x_4*x_6 + 2.00000000000000*x_4^3,
....: x_1^2*x_5 - x_1*x_3^2 + x_1*x_3*x_6 + 1.50000000000000*x_2*x_5*x_6 - x_3^2*x_4
....: + (-0.500000000000000)*x_3*x_4*x_6 - x_4^2*x_5, x_1*x_2*x_4 - x_2^2*x_3 + x_2^
....: 2*x_6 - x_2*x_4^2, x_1*x_2*x_5 - x_2*x_3^2 + x_2*x_3*x_6 - x_2*x_4*x_5, x_1*x_
....: 3*x_4 - x_2*x_3^2 + x_2*x_3*x_6 + x_2*x_4*x_5 + (-2.00000000000000)*x_3*x_4^2,
....: x_1*x_3*x_5 + (-0.500000000000000)*x_1*x_5*x_6 - x_3^3 + 1.50000000000000*x_3^
....: 2*x_6 - x_3*x_4*x_5 + (-0.500000000000000)*x_3*x_6^2 + 0.500000000000000*x_4*x
....: _5*x_6, x_1*x_4*x_5 + 0.500000000000000*x_2*x_5*x_6 - x_3^2*x_4 + 0.5000000000
....: 00000*x_3*x_4*x_6 - x_4^2*x_5, x_1*x_4*x_6 - x_2*x_3*x_6 + 2.00000000000000*x_
....: 2*x_4*x_5 + x_2*x_6^2 + (-2.00000000000000)*x_3*x_4^2 - x_4^2*x_6, x_1*x_5^2 -
....: x_3^2*x_5 + x_3*x_5*x_6 - x_4*x_5^2, x_2^2*x_5 - x_2*x_3*x_4, x_2*x_3*x_5 + (-
....: 0.500000000000000)*x_2*x_5*x_6 - x_3^2*x_4 + 0.500000000000000*x_3*x_4*x_6, x_
....: 2*x_5^2 -x_3*x_4*x_5]
sage: len(H)
12
```

Note que o comando utilizado foi $I.groebner\_basis('toy : buchberger')$ para o cálculo de uma base de Gröbner pelo Critério de Buchberger.

A seguir também utilizamos o comando $len(G)$ para retornar o número de polinômios dessa base computada, o qual retornou 17.

Portanto obtivemos uma base de Gröbner para o ideal, constando dos seguintes 17 polinômios:

$\mathcal{G} = \{x_1^2x_4 - x_1x_2x_3 + x_1x_2x_6 - 3x_1x_4^2 + 2x_2x_3x_4 - 2x_2x_4x_6 + 2x_4^3, x_1^2x_5 - x_1x_3^2 + x_1x_3x_6 - 3x_1x_4x_5 + 2x_3^2x_4 - 2x_3x_4x_6 + 2x_4^2x_5, x_1x_2x_4 - x_2^2x_3 + x_2^2x_6 - x_2x_4^2, x_1x_2x_5 - x_1x_3x_4 - 2x_2x_4x_5 + 2x_3x_4^2, x_1x_2x_5 - x_2x_3^2 + x_2x_3x_6 - x_2x_4x_5, x_1x_2x_5 - x_1x_3x_4 - 2x_2x_4x_5 + 2x_3x_4^2, x_1x_3x_4 - 0.5x_1x_4x_6 - x_2x_3^2 + 1.5x_2x_3x_6 - 0.5x_2x_6^2 - x_3x_4^2 + 0.5x_4^2x_6, x_1x_3x_5 - 0.5x_1x_5x_6 - x_3^3 + 1.5x_3^2x_6 - x_3x_4x_5 - 0.5x_3x_6^2 + 0.5x_4x_5x_6, x_1x_4x_5 - x_2x_3x_5 + x_2x_5x_6 - x_4^2x_5, x_1x_4x_6 - x_2x_3x_6 + 2x_2x_4x_5 +$

$x_2x_6^2 - 2x_3x_4^2 - x_4^2x_6, x_1x_5^2 - x_3^2x_5 + x_3x_5x_6 - x_4x_5^2, x_2^2x_5 - x_2x_3 * x_4, x_2^2x_5 - x_2x_3x_4, x_2x_3x_5 - 0.5x_2x_5x_6 - x_3^2x_4 + 0.5x_3x_4x_6, x_2x_3x_5 - 0.5x_2x_5x_6 - x_3^2x_4 + 0.5x_3x_4x_6, x_2x_5^2 - x_3x_4x_5, x_2x_5^2 - x_3x_4x_5\}$

Note que são exatamente os 17 polinômios calculados anteriormente, com diferenças apenas nos coeficientes de alguns, visto que em SageMath os polinômios retornados são todos mônicos.

Podemos observar também que alguns dos polinômios nessa base são simétricos uns dos outros, de fato, note que $g_1 = -g_4$, $g_5 = -g_8$, $g_9 = -g_{15}$ e $g_{10} = -g_{16}$.

Observe que para a base reduzida, utilizando o comando $I.groebner\_basis()$, obtivemos os seguintes 12 polinômios:
$\mathcal{H} = \{x_1^2x_4 - x_1x_2x_3 + x_1x_2x_6 - 3x_1x_4^2 + 2x_2x_3x_4 - 2x_2x_4x_6 + 2x_4^3, x_1^2x_5 - x_1x_3^2 + x_1x_3x_6 + 1.5x_2x_5x_6 - x_3^2x_4 - 0.5x_3x_4x_6 - x_4^2x_5, x_1x_2x_4 - x_2^2x_3 + x_2^2x_6 - x_2x_4^2, x_1x_2x_5 - x_2x_3^2 + x_2x_3x_6 - x_2x_4x_5, x_1x_3x_4 - x_2x_3^2 + x_2x_3x_6 + x_2x_4x_5 - 2x_3x_4^2, x_1x_3x_5 - 0.5x_1x_5x_6 - x_3^3 + 1.5x_3^2x_6 - x_3x_4x_5 - 0.5x_3x_6^2 + 0.5x_4x_5x_6, x_1x_4x_5 + 0.5x_2x_5x_6 - x_3^2x_4 + 0.5x_3x_4x_6 - x_4^2x_5, x_1x_4x_6 - x_2x_3x_6 + 2x_2x_4x_5 + x_2x_6^2 - 2x_3x_4^2 - x_4^2x_6, x_1x_5^2 - x_3^2x_5 + x_3x_5x_6 - x_4x_5^2, x_2^2x_5 - x_2x_3x_4, x_2x_3x_5 - 0.5x_2x_5x_6 - x_3^2x_4 + 0.5x_3x_4x_6, x_2x_5^2 - x_3x_4x_5\}$

Para obter a dimensão da variedade, seguimos os passos vistos na Proposição 2.58 e Teorema 2.74. Utilizando a base de Gröbner reduzida temos que:

$$\begin{aligned}\langle LT(I)\rangle &= \langle LT(g_1), LT(g_2), \ldots, LT(g_{12})\rangle \\ &= \left\langle x_1^2x_4, x_1^2x_5, x_1x_2x_4, x_1x_2x_5, x_1x_3x_4, x_1x_3x_5, x_1x_4x_5, x_1x_4x_6, x_1x_5^2, x_2^2x_5, x_2x_3x_5, x_2x_5^2\right\rangle\end{aligned}$$

Sejam os monômios $m_1 = x_1^2x_4$, $m_2 = x_1^2x_5$, $m_3 = x_1x_2x_4$, $m_4 = x_1x_2x_5$, $m_5 = x_1x_3x_4$, $m_6 = x_1x_3x_5$, $m_7 = x_1x_4x_5$, $m_8 = x_1x_4x_6$, $m_9 = x_1x_5^2$, $m_{10} = x_2^2x_5$, $m_{11} = x_2x_3x_5$ e $m_{12} = x_2x_5^2$.

Temos os seguintes conjuntos de índices das indeterminadas nesses monômios:
$M_1 = \{1,4\}$, $M_2 = \{1,5\}$, $M_3 = \{1,2,4\}$, $M_4 = \{1,2,5\}$, $M_5 = \{1,3,4\}$, $M_6 = \{1,3,5\}$, $M_7 = \{1,4,5\}$, $M_8 = \{1,4,6\}$, $M_9 = \{1,5\}$, $M_{10} = \{2,5\}$, $M_{11} = \{2,3,5\}$ e $M_{12} = \{2,5\}$.

Portanto, sendo $\mathcal{M} = \{J \subseteq \{1,2,3,4,5,6\} \mid J \cap M_i \neq \emptyset\ \forall i\}$, temos que
$\dim V(I) = \dim V(\langle LT(I)\rangle) = n - min\{|J| \mid J \in \mathcal{M}\}$.

Verificando, podemos ver que $\{1\} \cap M_{10} = \emptyset$, $\{2\} \cap M_1 = \emptyset$, $\{3\} \cap M_2 = \emptyset$, $\{4\} \cap M_4 = \emptyset$, $\{5\} \cap M_5 = \emptyset$, $\{6\} \cap M_6 = \emptyset$. Mas $\{1,2\} \cap M_i \neq \emptyset\ \forall i$.

Logo $min\{|J| \mid J \in \mathcal{M}\} = 2$ e, concluímos que $\dim V(I) = 6 - 2 = 4$.

Prosseguindo com a análise da variedade das álgebras de Jordan de dimensão 2, $Jor_2(\kappa)$, também podemos obter no SageMath a decomposição primária do ideal I:

```
SageMath version 9.3 Console

sage: P.<x_1, x_2, x_3, x_4, x_5, x_6> = PolynomialRing(CC, 6, order = "deglex")
sage: g_1 = - x_2^2*x_5 + x_2*x_3*x_4
sage: g_2 = - x_1*x_2*x_4 + x_2^2*x_3 - x_2^2*x_6 + x_2*x_4^2
sage: g_3 = x_1*x_2*x_5 - x_2*x_3^2 + x_2*x_3*x_6 - x_2*x_4*x_5
sage: g_4 = x_2^2*x_5 - x_2*x_3*x_4
sage: g_5 = x_2*x_5^2 - x_3*x_4*x_5
sage: g_6 = x_1*x_4*x_5 - x_2*x_3*x_5 + x_2*x_5*x_6 - x_4^2*x_5
sage: g_7 = - x_1*x_5^2 + x_3^2*x_5 - x_3*x_5*x_6 + x_4*x_5^2
sage: g_8 = - x_2*x_5^2 + x_3*x_4*x_5
sage: g_9 = x_1*x_2*x_5 - x_1*x_3*x_4 + 2*x_3*x_4^2 - 2*x_2*x_4*x_5
sage: g_10 = - 2*x_3^2*x_4 + 2*x_2*x_3*x_5 + x_3*x_4*x_6 - x_2*x_5*x_6
sage: g_11 = x_1^2*x_4 - x_1*x_2*x_3 + x_1*x_2*x_6 - 3*x_1*x_4^2 + 2*x_2*x_3*x_4
....: - 2*x_2*x_4*x_6 + 2*x_4^3
sage: g_12 = 2*x_1*x_3*x_4 - 2*x_3*x_4^2 - x_1*x_4*x_6 - 2*x_2*x_3^2 + 3*x_2*x_3
....: *x_6 - x_2*x_6^2 + x_4^2*x_6
sage: g_13 = - x_1^2*x_5 + x_1*x_3^2 - x_1*x_3*x_6 + 3*x_1*x_4*x_5 - 2*x_3^2*x_4
...:  + 2*x_3*x_4*x_6 - 2*x_4^2*x_5
sage: g_14 = - 2*x_1*x_3*x_5 + x_1*x_5*x_6 + 2*x_3^3 - 3*x_3^2*x_6 + 2*x_3*x_4*x
....: _5 + x_3*x_6^2 - x_4*x_5*x_6
sage: g_15 = -x_1*x_2*x_5 + x_1*x_3*x_4 + 2*x_2*x_4*x_5 - 2*x_3*x_4^2
sage: g_16 = -2*x_2*x_3*x_5 + x_2*x_5*x_6 + 2*x_3^2*x_4 - x_3*x_4*x_6
sage: I = ideal([g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_10, g_11, g_12,
....: g_13, g_14, g_15, g_16])
sage: I.primary_decomposition()
[Ideal (x_5, 2*x_3 - x_6, x_2, x_1 - 2*x_4) of Multivariate Polynomial Ring in
....: x_1, x_2, x_3, x_4, x_5, x_6 over Complex Field,
Ideal (x_2*x_5 - x_3*x_4, x_1*x_5 - x_3^2 + x_3*x_6 - x_4*x_5, x_1*x_4 - x_2*x_3
....: + x_2*x_6 - x_4^2) of Multivariate Polynomial Ring in x_1, x_2, x_3, x_4,
....: x_5, x_6 over Complex Field]
```

Assim, a partir da decomposição primária, obtemos a decomposição correspondente da variedade em duas componentes irredutíveis:
$\mathbf{V}(g_1, \ldots, g_{16}) = \mathbf{V}(x_5, 2x_3 - x_6, x_2, x_1 - 2x_4) \cup \mathbf{V}(x_2x_5 - x_3x_4, x_1x_5 - x_3^2 + x_3x_6 - x_4x_5, x_1x_4 - x_2x_3 + x_2x_6 - x_4^2)$

Note que a primeira componente tem dimensão 2 e a segunda componente tem dimensão 4.

Desse modo, concluímos que a variedade das álgebras de Jordan de dimensão 2, $Jor_2(\kappa)$, é uma variedade afim de dimensão 4, com duas componentes irredutíveis, conforme [8, pág 88].

Para o estudo da variedade das álgebras de Jordan de dimensão 3, $Jor_3(\kappa)$, seja $\{e_1, e_2, e_3\}$ base de $A \in Jor_3(\kappa)$, isto é, de uma álgebra de Jordan de dimensão 3 com as constantes de estrutura a seguir:

$$\begin{cases} e_1^2 = x_1e_1 + x_2e_2 + x_3e_3 \\ e_1e_2 = x_4e_1 + x_5e_2 + x_6e_3 = e_2e_1 \\ e_1e_3 = x_7e_1 + x_8e_2 + x_9e_3 = e_3e_1 \\ e_2^2 = x_{10}e_1 + x_{11}e_2 + x_{12}e_3 \\ e_2e_3 = x_{13}e_1 + x_{14}e_2 + x_{15}e_3 = e_3e_2 \\ e_3^2 = x_{16}e_1 + x_{17}e_2 + x_{18}e_3 \end{cases}$$

Calculamos as identidades:

$J(e_1, e_1), J(e_1, e_2), J(e_2, e_1), J(e_1, e_3), J(e_3, e_1), J(e_2, e_2), J(e_2, e_3), J(e_3, e_2), J(e_3, e_3)$, $J(e_1 + te_2, e_1), J(e_1 + te_2, e_2), J(e_1 + te_2, e_3), J(e_2 + te_3, e_1), J(e_2 + te_3, e_2), J(e_2 + te_3, e_3)$, $J(e_1 + te_3, e_1), J(e_1 + te_3, e_2)$ e $J(e_1 + te_3, e_3)$, com o parâmetro $t \in \kappa$.

Assim, com cálculos análogos aos de $Jor_2(\kappa)$, obtivemos que a variedade afim das álgebras de Jordan de dimensão 3, $Jor_3(\kappa)$, no espaço afim $\mathbb{A}^{18}(\kappa)$, é determinada pelos seguintes 81 polinômios:

$g_1 = x_2^2x_{10} + 2x_2x_3x_{13} - x_2x_4x_5 - x_2x_6x_7 + x_3^2x_{16} - x_3x_4x_8 - x_3x_7x_9$

$g_2 = x_1x_2x_5 + x_1x_3x_8 - x_2^2x_4 + x_2^2x_{11} - x_2x_3x_7 + 2x_2x_3x_{14} - x_2x_5^2 - x_2x_6x_8 + x_3^2x_{17} - x_3x_5x_8 - x_3x_8x_9$

$g_3 = x_1x_2x_6 + x_1x_3x_9 + x_2^2x_{12} - x_2x_3x_4 + 2x_2x_3x_{15} - x_2x_5x_6 - x_2x_6x_9 - x_3^2x_7 + x_3^2x_{18} - x_3x_6x_8 - x_3x_9^2$

$g_4 = -x_1x_2x_{10} - x_1x_3x_{13} + x_2x_4^2 - x_2x_4x_{11} + x_2x_5x_{10} + x_2x_6x_{13} - x_2x_7x_{12} + x_3x_4x_7 - x_3x_4x_{14} + x_3x_5x_{13} + x_3x_6x_{16} - x_3x_7x_{15}$

$g_5 = -x_2^2x_{10} - x_2x_3x_{13} + x_2x_4x_5 + x_2x_6x_{14} - x_2x_8x_{12} + x_3x_4x_8 + x_3x_6x_{17} - x_3x_8x_{15}$

$g_6 = -x_2x_3x_{10} + x_2x_4x_6 + x_2x_5x_{12} - x_2x_6x_{11} + x_2x_6x_{15} - x_2x_9x_{12} - x_3^2x_{13} + x_3x_4x_9 + x_3x_5x_{15} - x_3x_6x_{14} + x_3x_6x_{18} - x_3x_9x_{15}$

$g_7 = -x_1x_3x_{16} - x_1x_2x_{13} + x_2x_4x_7 - x_2x_4x_{14} - x_2x_7x_{15} + x_2x_8x_{10} + x_2x_9x_{13} - x_3x_4x_{17} + x_3x_7^2 - x_3x_7x_{18} + x_3x_8x_{13} + x_3x_9x_{16}$

$g_8 = -x_2^2x_{13} - x_2x_3x_{16} + x_2x_5x_7 - x_2x_5x_{14} + x_2x_8x_{11} - x_2x_8x_{15} + x_2x_9x_{14} - x_3x_5x_{17} + x_3x_7x_8 + x_3x_8x_{14} - x_3x_8x_{18} + x_3x_9x_{17}$

$g_9 = -x_2x_3x_{13} + x_2x_6x_7 - x_2x_6x_{14} + x_2x_8x_{12} - x_3^2x_{16} - x_3x_6x_{17} + x_3x_7x_9 + x_3x_8x_{15}$

$g_{10} = -x_2x_{10}^2 - x_3x_{10}x_{13} + x_4x_5x_{10} + x_5x_{12}x_{13} + x_6x_7x_{10} + x_6x_{12}x_{16} - x_8x_{10}x_{12} - x_9x_{12}x_{13}$

$g_{11} = -x_1x_5x_{10} + x_2x_4x_{10} - x_2x_{10}x_{11} - x_3x_{10}x_{14} + x_4x_8x_{12} + x_5^2x_{10} - x_5x_7x_{12} + x_5x_{12}x_{14} + x_6x_8x_{10} + x_6x_{12}x_{17} - x_8x_{11}x_{12} - x_9x_{12}x_{14}$

$g_{12} = -x_1x_6x_{10} - x_2x_{10}x_{12} + x_3x_4x_{10} - x_3x_{10}x_{15} + x_4x_9x_{12} + x_5x_6x_{10} + x_5x_{12}x_{15} - x_6x_7x_{12} + x_6x_9x_{10} + x_6x_{12}x_{18} - x_8x_{12}^2 - x_9x_{12}x_{15}$

$g_{13} = x_1x_{10}^2 - x_4^2x_{10} + x_4x_{10}x_{11} - x_4x_{12}x_{13} - x_5x_{10}^2 - x_6x_{10}x_{13} + 2x_7x_{10}x_{12} - x_{10}x_{12}x_{14} +$

$x_{11}x_{12}x_{13} + x_{12}^2x_{16} - x_{12}x_{13}x_{15}$

$g_{14} = x_2x_{10}^2 - x_4x_5x_{10} - x_5x_{12}x_{13} - x_6x_{10}x_{14} + 2x_8x_{10}x_{12} + x_{12}^2x_{17} - x_{12}x_{14}x_{15}$

$g_{15} = x_3x_{10}^2 - x_4x_6x_{10} - x_5x_{10}x_{12} + x_6x_{10}x_{11} - x_6x_{10}x_{15} - x_6x_{12}x_{13} + 2x_9x_{10}x_{12} + x_{11}x_{12}x_{15} - x_{12}^2x_{14} + x_{12}^2x_{18} - x_{12}x_{15}^2$

$g_{16} = x_1x_{10}x_{13} - x_4x_7x_{10} + x_4x_{10}x_{14} - x_4x_{12}x_{16} + x_7x_{10}x_{15} + x_7x_{12}x_{13} - x_8x_{10}^2 - x_9x_{10}x_{13} - x_{10}x_{12}x_{17} + x_{12}x_{13}x_{14} - x_{12}x_{13}x_{18} + x_{12}x_{15}x_{16}$

$g_{17} = x_2x_{10}x_{13} - x_5x_7x_{10} + x_5x_{10}x_{14} - x_5x_{12}x_{16} - x_8x_{10}x_{11} + x_8x_{10}x_{15} + x_8x_{12}x_{13} - x_9x_{10}x_{14} - x_{11}x_{12}x_{17} + x_{12}x_{14}^2 - x_{12}x_{14}x_{18} + x_{12}x_{15}x_{17}$

$g_{18} = x_3x_{10}x_{13} - x_6x_7x_{10} + x_6x_{10}x_{14} - x_6x_{12}x_{16} - x_8x_{10}x_{12} + x_9x_{12}x_{13} - x_{12}^2x_{17} + x_{12}x_{14}x_{15}$

$g_{19} = -x_2x_{13}x_{16} - x_3x_{16}^2 + x_4x_8x_{16} - x_5x_{13}x_{17} - x_6x_{16}x_{17} + x_7x_9x_{16} + x_8x_{10}x_{17} + x_9x_{13}x_{17}$

$g_{20} = -x_1x_8x_{16} + x_2x_7x_{16} - x_2x_{14}x_{16} - x_3x_{16}x_{17} - x_4x_8x_{17} + x_5x_7x_{17} + x_5x_8x_{16} - x_5x_{14}x_{17} - x_6x_{17}^2 + x_8x_9x_{16} + x_8x_{11}x_{17} + x_9x_{14}x_{17}$

$g_{21} = -x_1x_9x_{16} - x_2x_{15}x_{16} + x_3x_7x_{16} - x_3x_{16}x_{18} - x_4x_9x_{17} - x_5x_{15}x_{17} + x_6x_7x_{17} + x_6x_8x_{16} - x_6x_{17}x_{18} + x_8x_{12}x_{17} + x_9^2x_{16} + x_9x_{15}x_{17}$

$g_{22} = x_1x_{13}x_{16} - x_4x_7x_{16} + x_4x_{14}x_{16} + x_4x_{13}x_{17} - x_5x_{13}x_{16} - x_6x_{16}^2 - x_7x_{10}x_{17} + x_7x_{15}x_{16} + x_{10}x_{14}x_{17} - x_{11}x_{13}x_{17} - x_{12}x_{16}x_{17} + x_{13}x_{15}x_{17}$

$g_{23} = x_2x_{13}x_{16} - x_4x_8x_{16} + x_5x_{13}x_{17} - x_6x_{16}x_{17} - x_8x_{10}x_{17} + x_8x_{15}x_{16} - x_{12}x_{17}^2 + x_{14}x_{15}x_{17}$

$g_{24} = x_3x_{13}x_{16} - x_4x_9x_{16} - x_5x_{15}x_{16} + x_6x_{13}x_{17} + x_6x_{14}x_{16} - x_6x_{16}x_{18} - x_9x_{10}x_{17} + x_9x_{15}x_{16} - x_{11}x_{15}x_{17} + x_{12}x_{14}x_{17} + x_{15}^2x_{17} - x_{12}x_{17}x_{18}$

$g_{25} = x_1x_{16}^2 + 2x_4x_{16}x_{17} - x_7^2x_{16} - x_7x_{13}x_{17} + x_7x_{16}x_{18} - x_8x_{13}x_{16} - x_9x_{16}^2 + x_{10}x_{17}^2 - x_{13}x_{14}x_{17} + x_{13}x_{17}x_{18} - x_{15}x_{16}x_{17}$

$g_{26} = x_2x_{16}^2 + 2x_5x_{16}x_{17} - x_7x_8x_{16} - x_8x_{14}x_{16} - x_8x_{13}x_{17} + x_8x_{16}x_{18} - x_9x_{16}x_{17} + x_{11}x_{17}^2 - x_{14}^2x_{17} + x_{14}x_{17}x_{18} - x_{15}x_{17}^2$

$g_{27} = x_3x_{16}^2 + 2x_6x_{16}x_{17} - x_7x_9x_{16} - x_8x_{15}x_{16} - x_9x_{13}x_{17} + x_{12}x_{17}^2 - x_{14}x_{15}x_{17}$

$g_{28} = -x_1x_2x_{10} - x_1x_3x_{13} + x_1x_4x_5 + x_1x_6x_7 + 2x_2x_5x_{10} + 2x_2x_6x_{13} + 3x_3x_5x_{13} + 3x_3x_6x_{16} - x_3x_8x_{10} - x_3x_9x_{13} - 2x_4x_5^2 - 2x_4x_6x_8 - 2x_5x_6x_7 - 2x_6x_7x_9$

$g_{29} = -2x_2x_4x_{10} + x_2x_{10}x_{11} + x_2x_{12}x_{13} - 2x_3x_4x_{13} + x_3x_{11}x_{13} + x_3x_{12}x_{16} + 2x_4^2x_5 - x_4x_5x_{11} + 2x_4x_6x_7 - x_4x_8x_{12} + 2x_5x_6x_{13} + 2x_6^2x_{16} - x_6x_7x_{11} - 2x_6x_8x_{10} - 2x_6x_9x_{13} - x_7x_9x_{12}$

$g_{30} = x_1^2x_5 - x_1x_2x_4 + x_1x_2x_{11} + x_1x_3x_{14} - 3x_1x_5^2 - 3x_1x_6x_8 + 2x_2x_4x_5 - 2x_2x_5x_{11} + 2x_2x_6x_7 - 2x_2x_6x_{14} - x_3x_4x_8 + x_3x_5x_7 - 3x_3x_5x_{14} - 3x_3x_6x_{17} + x_3x_8x_{11} + x_3x_9x_{14} + 2x_5^3 + 4x_5x_6x_8 + 2x_6x_8x_9$

$g_{31} = 2x_1x_4x_5 - x_1x_5x_{11} - x_1x_8x_{12} - 2x_2x_4^2 + 3x_2x_4x_{11} + x_2x_7x_{12} - x_2x_{11}^2 - x_2x_{12}x_{14} + 2x_3x_4x_{14} - x_3x_{11}x_{14} - x_3x_{12}x_{17} - 2x_4x_5^2 - 4x_4x_6x_8 + x_5^2x_{11} + 2x_5x_6x_7 - 2x_5x_6x_{14} + x_5x_8x_{12} - 2x_6^2x_{17} + 3x_6x_8x_{11} + 2x_6x_9x_{14} + x_8x_9x_{12}$

$g_{32} = x_1^2x_6 + x_1x_2x_{12} - x_1x_3x_4 + x_1x_3x_{15} - 3x_1x_5x_6 - 3x_1x_6x_9 - 2x_2x_5x_{12} - 2x_2x_6x_{15} + 2x_3x_4x_5 - x_3x_4x_9 - 3x_3x_5x_{15} + 3x_3x_6x_7 - 3x_3x_6x_{18} + x_3x_8x_{12} + x_3x_9x_{15} + 2x_5^2x_6 + 2x_5x_6x_9 + 2x_6^2x_8 + 2x_6x_9^2$

$g_{33} = 2x_1x_4x_6 - x_1x_6x_{11} - x_1x_9x_{12} + 2x_2x_4x_{12} - x_2x_{11}x_{12} - x_2x_{12}x_{15} - 2x_3x_4^2 + x_3x_4x_{11} + 2x_3x_4x_{15} - x_3x_{11}x_{15} + x_3x_7x_{12} - x_3x_{12}x_{18} - 2x_4x_5x_6 - 4x_4x_6x_9 + x_5x_6x_{11} - 2x_5x_6x_{15} +$

$2x_6^2x_7 - 2x_6^2x_{18} + 3x_6x_8x_{12} + x_6x_9x_{11} + 2x_6x_9x_{15} + x_9^2x_{12}$

$g_{34} = x_1^2x_{10} - x_1x_4^2 + x_1x_4x_{11} - 3x_1x_5x_{10} - 3x_1x_6x_{13} + x_1x_7x_{12} - x_3x_4x_{13} + x_3x_7x_{10} - x_3x_{10}x_{14} + x_3x_{11}x_{13} + x_3x_{12}x_{16} - x_3x_{13}x_{15} + 2x_4^2x_5 - 2x_4x_5x_{11} + 2x_4x_6x_7 - 2x_4x_6x_{14} + 2x_5^2x_{10} - 2x_5x_7x_{12} + 4x_5x_6x_{13} + 2x_6^2x_{16} - 2x_6x_7x_{15}$

$g_{35} = 2x_1x_4x_{10} - x_1x_{10}x_{11} - x_1x_{12}x_{13} - 2x_4^3 + 3x_4^2x_{11} - 2x_4x_5x_{10} - x_4x_{11}^2 - 4x_4x_6x_{13} + 3x_4x_7x_{12} - x_4x_{12}x_{14} + x_5x_{10}x_{11} + x_5x_{12}x_{13} + 3x_6x_{11}x_{13} + 2x_6x_7x_{10} - 2x_6x_{10}x_{14} + 3x_6x_{12}x_{16} - 2x_6x_{13}x_{15} - x_7x_{11}x_{12} - x_7x_{12}x_{15}$

$g_{36} = -x_1x_2x_{10} + x_1x_4x_5 + x_1x_6x_{14} - x_1x_8x_{12} + 2x_2x_5x_{10} + 2x_2x_6x_{13} + x_3x_5x_{13} - x_3x_{12}x_{17} - x_3x_8x_{10} + x_3x_{14}x_{15} - 2x_4x_5^2 - 2x_4x_6x_8 - 2x_5x_6x_{14} + 2x_5x_8x_{12} - 2x_6^2x_{17} + 2x_6x_8x_{15}$

$g_{37} = -2x_2x_4x_{10} + x_2x_{10}x_{11} + x_2x_{12}x_{13} + 2x_4^2x_5 - x_4x_5x_{11} + 2x_4x_6x_{14} - 3x_4x_8x_{12} + 2x_5x_6x_{13} - 2x_6x_8x_{10} - x_6x_{11}x_{14} - 3x_6x_{12}x_{17} + 2x_6x_{14}x_{15} + x_8x_{11}x_{12} + x_8x_{12}x_{15}$

$g_{38} = -x_1x_3x_{10} + x_1x_4x_6 + x_1x_5x_{12} - x_1x_6x_{11} + x_1x_6x_{15} - x_1x_9x_{12} + 2x_3x_5x_{10} + 3x_3x_6x_{13} - x_3x_9x_{10} - x_3x_{11}x_{15} + x_3x_{12}x_{14} - x_3x_{12}x_{18} + x_3x_{15}^2 - 2x_4x_5x_6 - 2x_4x_6x_9 - 2x_5^2x_{12} + 2x_5x_6x_{11} - 4x_5x_6x_{15} + 2x_5x_9x_{12} + 2x_6^2x_{14} - 2x_6^2x_{18} + 2x_6x_9x_{15}$

$g_{39} = -2x_3x_4x_{10} + x_3x_{10}x_{11} + x_3x_{12}x_{13} + 2x_4^2x_6 + 2x_4x_5x_{12} - 3x_4x_6x_{11} + 2x_4x_6x_{15} - 3x_4x_9x_{12} - x_5x_{11}x_{12} - x_5x_{12}x_{15} + 2x_6^2x_{13} - 2x_6x_9x_{10} + x_6x_{11}^2 - 3x_6x_{11}x_{15} + 3x_6x_{12}x_{14} - 3x_6x_{12}x_{18} + 2x_6x_{15}^2 + x_9x_{11}x_{12} + x_9x_{12}x_{15}$

$g_{40} = x_1^2x_{13} - x_1x_4x_7 + x_1x_4x_{14} - 2x_1x_5x_{13} - 2x_1x_6x_{16} + x_1x_7x_{15} - x_1x_8x_{10} - x_1x_9x_{13} - x_3x_4x_{16} - x_3x_{10}x_{17} + x_3x_7x_{13} + x_3x_{13}x_{14} - x_3x_{13}x_{18} + x_3x_{15}x_{16} + 2x_4x_5x_7 - 2x_4x_5x_{14} - 2x_4x_6x_{17} - 2x_5x_7x_{15} + 2x_5x_8x_{10} + 2x_5x_9x_{13} + 2x_6x_7^2 - 2x_6x_7x_{18} + 2x_6x_8x_{13} + 2x_6x_9x_{16}$

$g_{41} = 2x_1x_4x_{13} - x_1x_{11}x_{13} - x_1x_{12}x_{16} - 2x_4^2x_7 + 2x_4^2x_{14} - 2x_4x_6x_{16} + x_4x_7x_{11} + 2x_4x_7x_{15} + 2x_4x_8x_{10} - 2x_4x_9x_{13} - x_4x_{11}x_{14} - x_4x_{12}x_{17} + 2x_6x_7x_{13} - 2x_6x_{10}x_{17} + 2x_6x_{13}x_{14} - 2x_6x_{13}x_{18} + 2x_6x_{15}x_{16} - x_7x_{11}x_{15} - x_7x_{12}x_{18} + x_7^2x_{12} + x_8x_{10}x_{11} + x_8x_{12}x_{13} + x_9x_{11}x_{13} + x_9x_{12}x_{16}$

$g_{42} = x_1x_2x_{13} - x_1x_5x_7 + x_1x_5x_{14} - x_1x_8x_{11} + x_1x_8x_{15} - x_1x_9x_{14} - 2x_2x_5x_{13} - 2x_2x_6x_{16} - x_3x_5x_{16} + x_3x_8x_{13} - x_3x_{11}x_{17} + x_3x_{14}^2 - x_3x_{14}x_{18} + x_3x_{15}x_{17} + 2x_5^2x_7 - 2x_5^2x_{14} - 2x_5x_6x_{17} + 2x_5x_8x_{11} - 2x_5x_8x_{15} + 2x_5x_9x_{14} + 2x_6x_7x_8 + 2x_6x_8x_{14} - 2x_6x_8x_{18} + 2x_6x_9x_{17}$

$g_{43} = x_2x_4x_{13} - x_2x_{11}x_{13} - x_2x_{12}x_{16} - 2x_4x_5x_7 + 2x_4x_5x_{14} - 2x_4x_8x_{11} + 2x_4x_8x_{15} - x_4x_9x_{14} - 2x_5x_6x_{16} + x_5x_7x_{11} - x_5x_{11}x_{14} - x_5x_{12}x_{17} + 2x_6x_8x_{13} - 2x_6x_{11}x_{17} + 2x_6x_{14}^2 - 2x_6x_{14}x_{18} + 2x_6x_{15}x_{17} + x_7x_8x_{12} + x_8x_{11}^2 - x_8x_{11}x_{15} - x_8x_{12}x_{18} + x_8x_{12}x_{14} + x_9x_{11}x_{14} + x_9x_{12}x_{17}$

$g_{44} = x_1x_3x_{13} - x_1x_6x_7 + x_1x_6x_{14} - x_1x_8x_{12} - 2x_3x_5x_{13} - 3x_3x_6x_{16} + x_3x_9x_{13} - x_3x_{12}x_{17} + x_3x_{14}x_{15} + 2x_5x_6x_7 - 2x_5x_6x_{14} + 2x_5x_8x_{12} - 2x_6^2x_{17} + 2x_6x_7x_9 + 2x_6x_8x_{15}$

$g_{45} = 2x_3x_4x_{13} - x_3x_{11}x_{13} - x_3x_{12}x_{16} - 2x_4x_6x_7 + 2x_4x_6x_{14} - 2x_4x_8x_{12} - 2x_6^2x_{16} + x_6x_7x_{11} + 2x_6x_9x_{13} - x_6x_{11}x_{14} - 3x_6x_{12}x_{17} + 2x_6x_{14}x_{15} + x_7x_9x_{12} + x_8x_{11}x_{12} + x_8x_{12}x_{15}$

$g_{46} = -x_1x_2x_{13} - x_1x_3x_{16} + x_1x_4x_8 + x_1x_7x_9 - x_2x_5x_{13} - x_2x_6x_{16} + 3x_2x_8x_{10} + 3x_2x_9x_{13} + 2x_3x_8x_{13} + 2x_3x_9x_{16} + 2x_4x_5x_8 + 2x_4x_8x_9 - 2x_6x_7x_8 - 2x_7x_9^2$

$g_{47} = -2x_2x_7x_{13} + x_2x_{10}x_{17} + x_2x_{13}x_{18} - 2x_3x_7x_{16} + x_3x_{13}x_{17} + x_3x_{16}x_{18} - x_4x_5x_{17} + 2x_4x_7x_8 - x_4x_8x_{18} - 2x_5x_8x_{13} - x_6x_7x_{17} - 2x_6x_8x_{16} + 2x_7^2x_9 - x_7x_9x_{18} + 2x_8^2x_{10} + 2x_8x_9x_{13}$

$g_{48} = x_1^2x_8 - x_1x_2x_7 + x_1x_2x_{14} + x_1x_3x_{17} - 3x_1x_5x_8 - 3x_1x_8x_9 + 3x_2x_4x_8 - x_2x_5x_7 + x_2x_5x_{14} + x_2x_6x_{17} + 2x_2x_7x_9 - 3x_2x_8x_{11} - 3x_2x_9x_{14} - 2x_3x_8x_{14} - 2x_3x_9x_{17} + 2x_5^2x_8 + 2x_5x_8x_9 +$

$2x_6x_8^2 + 2x_8x_9^2$

$g_{49} = -x_1x_5x_{17} + 2x_1x_7x_8 - x_1x_8x_{18} + x_2x_4x_{17} - 2x_2x_7^2 + 2x_2x_7x_{14} + x_2x_7x_{18} - x_2x_{11}x_{17} - x_2x_{14}x_{18} + 2x_3x_7x_{17} - x_3x_{14}x_{17} - x_3x_{17}x_{18} + 2x_4x_8^2 + x_5^2x_{17} - 4x_5x_7x_8 + 2x_5x_8x_{14} + x_5x_8x_{18} + 3x_6x_8x_{17} - 2x_7x_8x_9 - 2x_8^2x_{11} - 2x_8x_9x_{14} + x_8x_9x_{18}$

$g_{50} = x_1^2x_9 + x_1x_2x_{15} - x_1x_3x_7 + x_1x_3x_{18} - 3x_1x_6x_8 - 3x_1x_9^2 + x_2x_4x_9 + x_2x_5x_{15} - x_2x_6x_7 + x_2x_6x_{18} - 3x_2x_8x_{12} - 3x_2x_9x_{15} + 2x_3x_4x_8 + 2x_3x_7x_9 - 2x_3x_8x_{15} - 2x_3x_9x_{18} + 2x_5x_6x_8 + 4x_6x_8x_9 + 2x_9^3$

$g_{51} = -x_1x_6x_{17} + 2x_1x_7x_9 - x_1x_9x_{18} + 2x_2x_7x_{15} - x_2x_{12}x_{17} - x_2x_{15}x_{18} + x_3x_4x_{17} - 2x_3x_7^2 + 3x_3x_7x_{18} - x_3x_{15}x_{17} - x_3x_{18}^2 + 2x_4x_8x_9 + x_5x_6x_{17} + 2x_5x_8x_{15} - 4x_6x_7x_8 + 3x_6x_8x_{18} + x_6x_9x_{17} - 2x_7x_9^2 - 2x_8^2x_{12} - 2x_8x_9x_{15} + x_9^2x_{18}$

$g_{52} = x_1^2x_{13} - x_1x_4x_7 + x_1x_4x_{14} - x_1x_5x_{13} - x_1x_6x_{16} + x_1x_7x_{15} - 2x_1x_8x_{10} - 2x_1x_9x_{13} + x_2x_4x_{13} - x_2x_7x_{10} + x_2x_{10}x_{14} - x_2x_{11}x_{13} - x_2x_{12}x_{16} + x_2x_{13}x_{15} + 2x_4^2x_8 + 2x_4x_7x_9 - 2x_4x_8x_{11} - 2x_4x_9x_{14} + 2x_5x_8x_{10} + 2x_5x_9x_{13} + 2x_6x_8x_{13} + 2x_6x_9x_{16} - 2x_7x_8x_{12} - 2x_7x_9x_{15}$

$g_{53} = 2x_1x_7x_{13} - x_1x_{10}x_{17} - x_1x_{13}x_{18} + x_4^2x_{17} - 2x_4x_7^2 + 2x_4x_7x_{14} + x_4x_7x_{18} + 2x_4x_8x_{13} - x_4x_{11}x_{17} - x_4x_{14}x_{18} - 2x_5x_7x_{13} + x_5x_{10}x_{17} + x_5x_{13}x_{18} - 2x_6x_7x_{16} + 2x_7^2x_{15} - 2x_7x_8x_{10} - x_7x_{12}x_{17} - x_7x_{15}x_{18} + 2x_8x_{10}x_{14} - 2x_8x_{11}x_{13} - 2x_8x_{12}x_{16} + 2x_8x_{13}x_{15} + x_6x_{13}x_{17} + x_6x_{16}x_{18}$

$g_{54} = x_1x_2x_{13} - x_1x_4x_8 - x_1x_6x_{17} + x_1x_8x_{15} + x_2x_5x_{13} - 3x_2x_8x_{10} - 2x_2x_9x_{13} - x_2x_{12}x_{17} + x_2x_{14}x_{15} + 2x_4x_5x_8 + 2x_4x_8x_9 + 2x_6x_8x_{14} + 2x_6x_9x_{17} - 2x_8^2x_{12} - 2x_8x_9x_{15}$

$g_{55} = 2x_2x_7x_{13} - x_2x_{10}x_{17} - x_2x_{13}x_{18} + x_4x_5x_{17} - 2x_4x_7x_8 + x_4x_8x_{18} + 2x_5x_8x_{13} - 2x_6x_7x_{17} + x_6x_{14}x_{17} + x_6x_{17}x_{18} + 2x_7x_8x_{15} - 2x_8^2x_{10} - 3x_8x_{12}x_{17} + 2x_8x_{14}x_{15} - x_8x_{15}x_{18}$

$g_{56} = x_1x_3x_{13} - x_1x_4x_9 - x_1x_5x_{15} + x_1x_6x_{14} - x_1x_6x_{18} + x_1x_9x_{15} + x_2x_6x_{13} - x_2x_9x_{10} - x_2x_{11}x_{15} + x_2x_{12}x_{14} - x_2x_{12}x_{18} + x_2x_{15}^2 - 2x_3x_8x_{10} - 2x_3x_9x_{13} + 2x_4x_6x_8 + 2x_4x_9^2 + 2x_5x_8x_{12} + 2x_5x_9x_{15} - 2x_6x_8x_{11} + 2x_6x_8x_{15} - 2x_6x_9x_{14} + 2x_6x_9x_{18} - 2x_8x_9x_{12} - 2x_9^2x_{15}$

$g_{57} = 2x_3x_7x_{13} - x_3x_{10}x_{17} - x_3x_{13}x_{18} + x_4x_6x_{17} - 2x_4x_7x_9 + x_4x_9x_{18} - 2x_5x_7x_{15} + x_5x_{12}x_{17} + x_5x_{15}x_{18} + 2x_6x_7x_{14} - 2x_6x_7x_{18} + 2x_6x_8x_{13} - x_6x_{11}x_{17} - x_6x_{14}x_{18} + x_6x_{15}x_{17} + x_6x_{18}^2 + 2x_7x_9x_{15} - 2x_8x_9x_{10} - 2x_8x_{11}x_{15} + 2x_8x_{12}x_{14} + 2x_8x_{15}^2 - x_9x_{12}x_{17} - 2x_8x_{12}x_{18} - x_9x_{15}x_{18}$

$g_{58} = x_1^2x_{16} + x_1x_4x_{17} - x_1x_7^2 + x_1x_7x_{18} - 3x_1x_8x_{13} - 3x_1x_9x_{16} + x_2x_4x_{16} - x_2x_7x_{13} + x_2x_{10}x_{17} - x_2x_{13}x_{14} + x_2x_{13}x_{18} - x_2x_{15}x_{16} + 2x_4x_7x_8 - 2x_4x_8x_{14} - 2x_4x_9x_{17} + 2x_7^2x_9 - 2x_7x_8x_{15} - 2x_7x_9x_{18} + 2x_8^2x_{10} + 4x_8x_9x_{13} + 2x_9^2x_{16}$

$g_{59} = 2x_1x_7x_{16} - x_1x_{13}x_{17} - x_1x_{16}x_{18} + 3x_4x_7x_{17} + 2x_4x_8x_{16} - x_4x_{14}x_{17} - x_4x_{17}x_{18} - 2x_7^3 + 3x_7^2x_{18} - 4x_7x_8x_{13} - 2x_7x_9x_{16} - x_7x_{15}x_{17} - x_7x_{18}^2 - 2x_8x_{13}x_{14} + 3x_8x_{10}x_{17} + 3x_8x_{13}x_{18} - 2x_8x_{15}x_{16} + x_9x_{13}x_{17} + x_9x_{16}x_{18}$

$g_{60} = -x_1x_2x_{16} - x_1x_5x_{17} + x_1x_7x_8 + x_1x_8x_{14} - x_1x_8x_{18} + x_1x_9x_{17} - x_2x_5x_{16} + 3x_2x_8x_{13} + 2x_2x_9x_{16} - x_2x_{11}x_{17} + x_2x_{14}^2 - x_2x_{14}x_{18} + x_2x_{15}x_{17} - 2x_5x_7x_8 + 2x_5x_8x_{14} + 2x_5x_9x_{17} - 2x_7x_8x_9 - 2x_8^2x_{11} + 2x_8^2x_{15} - 4x_8x_9x_{14} + 2x_8x_9x_{18} - 2x_9^2x_{17}$

$g_{61} = -2x_2x_7x_{16} + x_2x_{13}x_{17} + x_2x_{16}x_{18} - 3x_5x_7x_{17} - 2x_5x_8x_{16} + x_5x_{14}x_{17} + x_5x_{17}x_{18} + 2x_7^2x_8 + 2x_7x_8x_{14} - 3x_7x_8x_{18} + 2x_7x_9x_{17} + 2x_8^2x_{13} - 3x_8x_{11}x_{17} + 2x_8x_{14}^2 - 3x_8x_{14}x_{18} + 3x_8x_{15}x_{17} + x_8x_{18}^2 - x_9x_{14}x_{17} - x_9x_{17}x_{18}$

$g_{62} = x_1x_3x_{16} + x_1x_6x_{17} - x_1x_7x_9 - x_1x_8x_{15} + x_2x_6x_{16} + x_2x_{12}x_{17} - x_2x_{14}x_{15} - x_2x_9x_{13} -$

$2x_3x_8x_{13} - 2x_3x_9x_{16} + 2x_6x_7x_8 - 2x_6x_8x_{14} - 2x_6x_9x_{17} + 2x_7x_9^2 + 2x_8^2x_{12} + 2x_8x_9x_{15}$

$g_{63} = 2x_3x_7x_{16} - x_3x_{13}x_{17} - x_3x_{16}x_{18} + 3x_6x_7x_{17} + 2x_6x_8x_{16} - x_6x_{14}x_{17} - x_6x_{17}x_{18} - 2x_7^2x_9 - 2x_7x_8x_{15} + x_7x_9x_{18} - 2x_8x_9x_{13} + 3x_8x_{12}x_{17} - 2x_8x_{14}x_{15} + x_8x_{15}x_{18}$

$g_{64} = -3x_2x_{10}x_{13} - x_3x_{10}x_{16} - 2x_3x_{13}^2 + 2x_4x_5x_{13} + x_4x_8x_{10} - x_5x_{11}x_{13} + 2x_5x_{13}x_{15} + 2x_6x_7x_{13} - x_6x_{11}x_{16} + 2x_6x_{15}x_{16} + x_7x_9x_{10} + x_8x_{10}x_{11} - 2x_8x_{10}x_{15} + x_9x_{11}x_{13} - 2x_9x_{13}x_{15}$

$g_{65} = -x_2x_{10}x_{16} - 2x_2x_{13}^2 - 3x_3x_{13}x_{16} + x_4x_5x_{16} + 2x_4x_8x_{13} - 2x_5x_{13}x_{14} + x_5x_{13}x_{18} + x_6x_7x_{16} - 2x_6x_{14}x_{16} + x_6x_{16}x_{18} + 2x_7x_9x_{13} + 2x_8x_{10}x_{14} - x_8x_{10}x_{18} + 2x_9x_{13}x_{14} - x_9x_{13}x_{18}$

$g_{66} = -2x_1x_5x_{13} - x_1x_8x_{10} + 2x_2x_4x_{13} + x_2x_7x_{10} - x_2x_{10}x_{14} - 2x_2x_{11}x_{13} - x_3x_{10}x_{17} - 2x_3x_{13}x_{14} - x_4x_8x_{11} + 2x_4x_8x_{15} + 2x_5^2x_{13} + x_5x_7x_{11} - 2x_5x_7x_{15} + x_5x_8x_{10} - x_5x_{11}x_{14} + 2x_5x_{14}x_{15} + 2x_6x_8x_{13} - x_6x_{11}x_{17} + 2x_6x_{15}x_{17} + x_8x_9x_{10} + x_8x_{11}^2 - 2x_8x_{11}x_{15} + x_9x_{11}x_{14} - 2x_9x_{14}x_{15}$

$g_{67} = -x_1x_5x_{16} - 2x_1x_8x_{13} + x_2x_4x_{16} + 2x_2x_7x_{13} - x_2x_{11}x_{16} - 2x_2x_{13}x_{14} - 2x_3x_{13}x_{17} - x_3x_{14}x_{16} - 2x_4x_8x_{14} + x_4x_8x_{18} + x_5^2x_{16} + 2x_5x_7x_{14} - x_5x_7x_{18} + 2x_5x_8x_{13} - 2x_5x_{14}^2 + x_5x_{14}x_{18} + x_6x_8x_{16} - 2x_6x_{14}x_{17} + x_6x_{17}x_{18} + 2x_8x_9x_{13} + 2x_8x_{11}x_{14} - x_8x_{11}x_{18} + 2x_9x_{14}^2 - x_9x_{14}x_{18}$

$g_{68} = -2x_1x_6x_{13} - x_1x_9x_{10} - x_2x_{10}x_{15} - 2x_2x_{12}x_{13} + 2x_3x_4x_{13} + x_3x_7x_{10} - x_3x_{10}x_{18} - 2x_3x_{13}x_{15} + 2x_4x_9x_{15} - x_4x_9x_{11} + 2x_5x_6x_{13} - x_5x_{11}x_{15} + 2x_5x_{15}^2 + x_6x_7x_{11} - 2x_6x_7x_{15} + x_6x_8x_{10} + 2x_6x_9x_{13} - x_6x_{11}x_{18} + 2x_6x_{15}x_{18} + x_8x_{11}x_{12} - 2x_8x_{12}x_{15} + x_9^2x_{10} + x_9x_{11}x_{15} - 2x_9x_{15}^2$

$g_{69} = -x_1x_6x_{16} - 2x_1x_9x_{13} - x_2x_{12}x_{16} - 2x_2x_{13}x_{15} + x_3x_4x_{16} + 2x_3x_7x_{13} - 2x_3x_{13}x_{18} - x_3x_{15}x_{16} - 2x_4x_9x_{14} + x_4x_9x_{18} + x_5x_6x_{16} - 2x_5x_{14}x_{15} + x_5x_{15}x_{18} + 2x_6x_7x_{14} - x_6x_7x_{18} + 2x_6x_8x_{13} + x_6x_9x_{16} - 2x_6x_{14}x_{18} + x_6x_{18}^2 + 2x_8x_{12}x_{14} - x_8x_{12}x_{18} + 2x_9^2x_{13} + 2x_9x_{14}x_{15} - x_9x_{15}x_{18}$

$g_{70} = -3x_1x_{10}x_{13} + 2x_4^2x_{13} + x_4x_7x_{10} - x_4x_{10}x_{14} - 3x_4x_{11}x_{13} + 2x_4x_{13}x_{15} + 3x_5x_{10}x_{13} + x_6x_{10}x_{16} + 2x_6x_{13}^2 + x_7x_{10}x_{11} - 3x_7x_{10}x_{15} - 2x_7x_{12}x_{13} - x_{10}x_{11}x_{14} + 2x_{10}x_{14}x_{15} + x_{11}^2x_{13} + x_{11}x_{12}x_{16} - 3x_{11}x_{13}x_{15} - 2x_{12}x_{15}x_{16} + 2x_{13}x_{15}^2$

$g_{71} = -x_1x_{10}x_{16} - 2x_1x_{13}^2 + x_4^2x_{16} + 2x_4x_7x_{13} - x_4x_{11}x_{16} - 4x_4x_{13}x_{14} + x_4x_{13}x_{18} + x_5x_{10}x_{16} + 2x_5x_{13}^2 + x_{10}x_{14}x_{18} - x_{11}x_{13}x_{18} + 3x_6x_{13}x_{16} - 2x_{10}x_{14}^2 + 2x_{11}x_{13}x_{14} + 2x_{12}x_{14}x_{16} - x_{12}x_{16}x_{18} - 2x_{13}x_{14}x_{15} + x_{13}x_{15}x_{18} + 2x_7x_{10}x_{14} - x_7x_{10}x_{18} - x_7x_{12}x_{16} - 2x_7x_{13}x_{15}$

$g_{72} = -3x_2x_{10}x_{13} + 2x_4x_5x_{13} + x_4x_8x_{10} - x_5x_{11}x_{13} + 2x_5x_{13}x_{15} + x_6x_{10}x_{17} + 2x_6x_{13}x_{14} + x_8x_{10}x_{11} - 3x_8x_{10}x_{15} - 2x_8x_{12}x_{13} + x_{11}x_{12}x_{17} - x_{11}x_{14}x_{15} + 2x_{14}x_{15}^2$

$g_{73} = -x_2x_{10}x_{16} - 2x_2x_{13}^2 + x_4x_5x_{16} + 2x_4x_8x_{13} - 2x_5x_{13}x_{14} + x_5x_{13}x_{18} + 2x_6x_{13}x_{17} + x_6x_{14}x_{16} + 2x_8x_{10}x_{14} - x_8x_{10}x_{18} - x_8x_{12}x_{16} - 2x_8x_{13}x_{15} + 2x_{12}x_{14}x_{17} - 2x_{12}x_{15}x_{17} - x_{12}x_{17}x_{18} - 2x_{14}^2x_{15} + x_{14}x_{15}x_{18}$

$g_{74} = -3x_3x_{10}x_{13} + 2x_4x_6x_{13} + x_4x_9x_{10} + x_5x_{10}x_{15} + 2x_5x_{12}x_{13} - x_6x_{10}x_{14} + x_6x_{10}x_{18} - 3x_6x_{11}x_{13} + 4x_6x_{13}x_{15} + x_9x_{10}x_{11} - 3x_9x_{10}x_{15} - 2x_9x_{12}x_{13} + x_{11}^2x_{15} - x_{11}x_{12}x_{14} + x_{11}x_{12}x_{18} - 3x_{11}x_{15}^2 + 2x_{12}x_{14}x_{15} - 2x_{12}x_{15}x_{18} + 2x_{15}^3$

$g_{75} = -x_3x_{10}x_{16} - 2x_3x_{13}^2 + x_4x_6x_{16} + 2x_4x_9x_{13} + x_5x_{12}x_{16} + 2x_5x_{13}x_{15} - x_6x_{11}x_{16} - 4x_6x_{13}x_{14} + 3x_6x_{13}x_{18} + x_6x_{15}x_{16} + 2x_9x_{10}x_{14} - x_9x_{10}x_{18} - x_9x_{12}x_{16} - 2x_9x_{13}x_{15} + 2x_{11}x_{14}x_{15} - x_{11}x_{15}x_{18} - 2x_{12}x_{14}^2 + 3x_{12}x_{14}x_{18} - x_{12}x_{18}^2 - 2x_{14}x_{15}^2 + x_{15}^2x_{18}$

$g_{76} = -x_1x_{10}x_{16} - 2x_1x_{13}^2 + 2x_4x_7x_{13} - x_4x_{10}x_{17} - x_4x_{11}x_{16} - 2x_4x_{13}x_{14} + 2x_4x_{15}x_{16} + x_7^2x_{10} - x_7x_{10}x_{18} + x_7x_{11}x_{13} - 4x_7x_{13}x_{15} + 3x_8x_{10}x_{13} + x_9x_{10}x_{16} + 2x_9x_{13}^2 - x_{10}x_{11}x_{17} +$

$2x_{10}x_{15}x_{17} + x_{11}x_{13}x_{14} - x_{11}x_{13}x_{18} + x_{11}x_{15}x_{16} - 2x_{13}x_{14}x_{15} + 2x_{13}x_{15}x_{18} - 2x_{15}^2x_{16}$

$g_{77} = -3x_1x_{13}x_{16} + x_4x_7x_{16} - 2x_4x_{13}x_{17} - 3x_4x_{14}x_{16} + x_4x_{16}x_{18} + 2x_7^2x_{13} + 2x_7x_{13}x_{14} - 3x_7x_{13}x_{18} - x_7x_{15}x_{16} + x_8x_{10}x_{16} + 2x_8x_{13}^2 + 3x_9x_{13}x_{16} - 2x_{10}x_{14}x_{17} + x_{10}x_{17}x_{18} + 2x_{13}x_{14}^2 - 3x_{13}x_{14}x_{18} + x_{13}x_{18}^2 + 2x_{14}x_{15}x_{16} - x_{15}x_{16}x_{18}$

$g_{78} = -x_2x_{10}x_{16} - 2x_2x_{13}^2 + 2x_5x_7x_{13} - x_5x_{10}x_{17} - x_5x_{11}x_{16} - 2x_5x_{13}x_{14} + 2x_5x_{15}x_{16} + x_7x_8x_{10} + x_8x_{10}x_{14} - x_8x_{10}x_{18} + 3x_8x_{11}x_{13} - 4x_8x_{13}x_{15} + x_9x_{10}x_{17} + 2x_9x_{13}x_{14} - x_{11}^2x_{17} + x_{11}x_{14}^2 - x_{11}x_{14}x_{18} + 3x_{11}x_{15}x_{17} - 2x_{14}^2x_{15} + 2x_{14}x_{15}x_{18} - 2x_{15}^2x_{17}$

$g_{79} = -3x_2x_{13}x_{16} + x_5x_7x_{16} - 2x_5x_{13}x_{17} - 3x_5x_{14}x_{16} + x_5x_{16}x_{18} + 2x_7x_8x_{13} + x_8x_{11}x_{16} + 4x_8x_{13}x_{14} - 3x_8x_{13}x_{18} - x_8x_{15}x_{16} + 2x_9x_{13}x_{17} + x_9x_{14}x_{16} - 2x_{11}x_{14}x_{17} + x_{11}x_{17}x_{18} + 2x_{14}^3 - 3x_{14}^2x_{18} + 2x_{14}x_{15}x_{17} + x_{14}x_{18}^2 - x_{15}x_{17}x_{18}$

$g_{80} = -x_3x_{10}x_{16} - 2x_3x_{13}^2 + 2x_6x_7x_{13} - x_6x_{10}x_{17} - x_6x_{11}x_{16} - 2x_6x_{13}x_{14} + 2x_6x_{15}x_{16} + x_7x_9x_{10} + x_8x_{10}x_{15} + 2x_8x_{12}x_{13} + x_9x_{11}x_{13} - 2x_9x_{13}x_{15} - x_{11}x_{12}x_{17} + x_{11}x_{14}x_{15} + 2x_{12}x_{15}x_{17} - 2x_{14}x_{15}^2$

$g_{81} = -3x_3x_{13}x_{16} + x_6x_7x_{16} - 2x_6x_{13}x_{17} - 3x_6x_{14}x_{16} + x_6x_{16}x_{18} + 2x_7x_9x_{13} + x_8x_{12}x_{16} + 2x_8x_{13}x_{15} + 2x_9x_{13}x_{14} - x_9x_{13}x_{18} - 2x_{12}x_{14}x_{17} + x_{12}x_{17}x_{18} + 2x_{14}^2x_{15} - x_{14}x_{15}x_{18}$

Infelizmente por limitação da capacidade computacional em nosso estudo, ou seja, tempo de execução do algoritmo em SageMath demasiado elevado juntamente com a insuficiência de memória disponível, não foi possível obtermos o retorno da computação de uma base de Gröbner para o ideal $I = \langle g_1, \ldots, g_{81} \rangle$.

Contudo sabemos que, se computada uma base de Gröbner, poderia-se obter de modo análogo à variedade $Jor_2(\kappa)$ a classificação de $Jor_3(\kappa)$ conforme [8, pág 90], isto é, obteria-se uma variedade afim de dimensão 9 com 5 componentes irredutíveis.

BIBLIOGRAFIA

[1] BUCHBERGER, B., *Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*. Journal of symbolic computation, v. 41, n.3-4, p. 475-511. Elsevier, 2006.

[2] COX, D.A. and LITTLE, J. and O'SHEA, D., *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate texts in Mathematics, 4ª ed. Springer International Publishing, New York, 2015.

[3] COX, D.A. and LITTLE, J. and O'SHEA, D., *Using Algebraic Geometry*, Graduate texts in Mathematics, 4ª ed. Springer, New York, 2013.

[4] DECKER, W. and PFISTER, G., *A First Course in Computational Algebraic Geometry*, AIMS Library Series. Cambridge University Press, 2013.

[5] DECKER, W. and SCHREYER, F. O., *Varieties, Groebner Bases, and Algebraic Curves*. Springer, 2007.

[6] EISENBUD, D., *Commutative Algebra: with a View toward Algebraic Geometry*, vol 150 of Graduate Texts in Mathmatics. Springer-Verlag, New York, 1995.

[7] HANCOCK, M., *Gröbner Bases and Invariant Theory*, 2005.

[8] MARTIN, M. E., *Deformações e isotopias de álgebras de Jordan*. Tese. Universidade de São Paulo, 2013.

[9] *SageMath, the Sage Mathematics Software System (Version 9.3)*, The Sage Developers, 2019, https://www.sagemath.org.

[10] TENGAN, E. e BORGES, H., *Algebra Comutativa em 4 Movimentos*. IMPA, Rio de Janeiro, 2014.