Universidade Federal da Amazonas
Instituto de Ciências Exatas
PROGRAMA
Mestrado em Matemática

Módulos irredutíveis de dimensão 3 sobre zero álgebras e bases de Gröbner

Eder Alejandro Rodríguez López

Manaus – AM
Fevereiro de 2024

Universidade Federal da Amazonas Instituto de Ciências Exatas
Programa
Mestrado em Matemática

Módulos irredutíveis de dimensão 3 sobre zero álgebras e bases de Gröbner

por

Eder Alejandro Rodríguez López

Sob a orientação de

Prof. Dr. Elkin Oveimar Quintero Vanegas
(Orientador)

Manaus – AM
Fevereiro de 2024

Ficha Catalográfica

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

Rodríguez López, Eder Alejandro
R696m Módulos irredutíveis de dimensão 3 sobre zero álgebras e bases de Gröbner / Eder Alejandro Rodríguez López . 2024
80 f.: il. color; 31 cm.

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

1. Bases de Gröbner. 2. Algoritmo da divisão general. 3. Critério de Buchberger. 4. Zero álgebra. 5. Módulos Irredutíveis. I. Vanegas, Elkin Oveimar Quintero. II. Universidade Federal do Amazonas III. Título

FOLHA DE APROVA

Eder Alejandro Rodríguez López

Módulos irredutíveis de dimensão 3 sobre zero álgebras e bases de Gröbner

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Amazonas, como requisito final para obtenção do título de Mestre em Matemática.

Aprovado por:

BANCA EXAMINADORA

Prof. Dr. Elkin Oveimar Quintero Vanegas (Presidente)
Universidade Federal do Amazonas - UFAM

Prof. Dr. Germán Alonso Benitez Monsalve (Membro)
Universidade Federal do Amazonas - UFAM

Prof. Dr. Thiago Castilho de Mello (Membro Externo)
Universidade Federal de São Paulo (Unifesp)

A serenidade proporcionada
pela sombra de uma árvore

Agradecimentos

Gostaria de expressar meu profundo agradecimento a todas as pessoas que contribuíram significativamente para a conclusão desta dissertação de mestrado. Seu apoio, orientação e incentivo foram fundamentais neste processo acadêmico.

Em primeiro lugar, gostaria de expressar a minha gratidão ao Professor Elkin Oveimar Quintero Vanegas, meu orientador, cuja sabedoria, paciência e dedicação foram essenciais para a conclusão deste projeto. Sua orientação especializada e comprometimento com meu crescimento acadêmico.

À Universidade Federal do Amazonas, meu sincero agradecimento por me dar a oportunidade de concluir o mestrado. Os recursos disponibilizados pela instituição CAPES foram fundamentais para o desenvolvimento deste trabalho.

Agradeço também aos professores que me acompanharam neste caminho desafiador principalmente, Dr. Elkin Quintero, Dr. Stefan Ehbauer, Dr. Germán Benitez, especialmente cujos conhecimentos e perspectivas enriqueceram minha perspectiva acadêmica.

Aos meus antigos professores, Dra. Verónica Cifuentes e Pedro Fernández, que lançaram as bases da minha formação, a sua influência foi decisiva no meu desenvolvimento académico.

Quero reconhecer a valiosa contribuição dos meus colegas de mestrado, Dzoara, Oscar, Edwin, Paola, Filipe, Gustavo e Erick. A sua colaboração, troca de ideias e apoio mútuo foram cruciais neste processo. Juntos formamos uma equipe que enriqueceu minha experiência acadêmica.

À minha família, meu maior pilar e apoio incondicional, em especial à minha mãe Eva e pai Hellman, aos meus irmãos Andrés, Danny e Jhon. Agradeço a Lilian, seu apoio, paciência e compreensão foram essenciais para superar os desafios e alcançar esta conquista acadêmica.

Em resumo, a todos que de alguma forma fizeram parte deste percurso académico, o meu sincero agradecimento. Essa conquista não teria sido possível sem cada um de vocês. Obrigado pelo seu constante apoio e contribuição para o meu desenvolvimento como estudante.

Resumo

Neste trabalho, descrevemos os Módulos Irredutíveis de dimensão 3 em zero álgebras, na classe de álgebras comutativas e de potências associativas de nilíndice quatro, utilizando a teoria das bases de Gröbner. A abordagem consiste em explorar o produto da álgebra sobre o módulo, representado por matrizes 3×3 ao fixar uma base do módulo. O objetivo é identificar as matrizes, excluindo aquelas relacionadas por conjugação. Mesmo a classificação dos módulos irredutíveis de dimensão 3 sobre a zero álgebra de dimensão dois seja conhecida, nós propomos um método computacional que utiliza as bases de Gröbner para obter essa classificação. Durante o processo de classificação, definimos a variedade afim das matrizes nilpotentes. No entanto, ao perceber que todos os polinômios que surgem na classificação proposta são homogêneos, é mais apropriado trabalhar com o espaço projetivo em vez do espaço afim. Apresentamos um procedimento computacional no sistema algébrico SageMath para calcular e simplificar esse processo. Embora a base de Gröbner obtida para matrizes 3×3 seja pequena, o programa SageMath não possui suporte executável em paralelo. Como resultado, a capacidade computacional do cluster, composto por 240 núcleos, foi equivalente à de um laptop comum. Portanto, com a versão em série, não foi possível concluir a classificação.

Palavras-chave: Bases de Gröbner; Orden Monomial; Algoritmo da divisão general; Critério de Buchberger; Variedade afim; Espaço projetivo; Polinômio homogêneo; Módulos Irredutíveis, Zero álgebra; Nilálgebra; Matriz nilpotente.

Abstract

In this work, we describe the Irreducible Modules of dimension 3 in zero algebras, in the class of commutative and power associative algebras of nilindex four, using the theory of Gröbner bases. The approach consists of exploring the product of the algebra over the module, represented by matrices 3×3 by fixing a base of the module. The objective is to identify the matrices, excluding those related by conjugation. Even though the classification of irreducible modules of dimension 3 over the zero algebra of dimension two is known, we propose a computational method that uses the Gröbner bases to obtain this classification. During the classification process, we define the affine manifold of nilpotent matrices. However, realizing that all polynomials that arise in the proposed classification are homogeneous, it is more appropriate to work with the projective space instead of the affine space. We present a computational procedure in the SageMath algebraic system to calculate and simplify this process. Although the Gröbner basis obtained for 3×3 matrices is small, the SageMath program does not have parallel executable support. As a result, the computational capacity of the cluster, made up of 240 cores, was equivalent to that of a common laptop. Therefore, with the serial version, it was not possible to complete the classification.

Keywords: Gröbner Bases; Monomial Order; General Division Algorithm; Buchberger's Criterion; Affine Variety; Projective Space; Homogeneous Polynomial; Irreducible Modules, Zero Algebra; Nil Algebra; Nilpotent Matrix.

Sumário

Introdução

Em geometria, todas as curvas obtidas cortando um cone com um plano são chamadas de seções cônicas. Os principais tipos de seções cônicas são círculos, elipses, parábolas e hipérboles. Essas curvas podem ser representadas algebricamente por equações polinomiais, por exemplo. Na geometria analítica, uma cônica pode ser definida como uma curva algébrica plana de grau 2; isto é, como o conjunto de pontos cujas coordenadas satisfazem uma equação quadrática em duas variáveis que podem ser escritas na forma $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$. Esta ideia pode ser estendida ao considerar polinômios de ordem superior ou equações mais complexas que envolvem múltiplos termos e parâmetros em um maior número de variáveis. Antes de continuar, devemos observar que ao trabalhar com polinômios em duas ou mais variáveis é necessário estender a ideia do algoritmo de divisão polinomial em uma única variável.

As bases de Gröbner foram introduzidas por Bruno Buchberger em 1965. A terminologia reconhece a influência de Wolfgang Gröbner no trabalho de Buchberger. A teoria das bases de Gröebner generaliza a divisão polinomial clássica para polinômios multivariados em álgebra. Parte da premissa de determinar se um polinômio está no ideal gerado por outros polinômios. Isto é conseguido através de uma generalização do processo de divisão, onde se obtém um quociente que é a soma dos multiplicadores dos monômios utilizados na divisão, resultando em uma forma eficaz de verificar a pertinência de um polinômio a um ideal se seu resto for zero. Esta generalização enfrenta desafios em casos onde não há um único gerador para o ideal, como no contexto de domínios de ideais principais (DIP). Além disso, exige uma ordenação específica dos termos para funcionar efetivamente. Também quando o "resto" da divisão de um polinômio multivariado por um determinado conjunto de polinômios é zero, ele pode ser expresso como uma combinação linear desses polinômios. Entretanto, não há garantia de que ao dividir um polinômio membro do ideal, pelos geradores do ideal se obterá um resto zero. O teorema chave Algoritmo de Buchberger afirma que é possível generalizar o algoritmo euclidiano para obter um conjunto que gera o mesmo ideal e produz "resto" zero para cada "divisão" com um membro do ideal como "dividendo". Esses conjuntos são chamados de bases de Gröebner.

O estudo de submódulos irredutíveis é fundamental em álgebra porque proporciona uma compreensão profunda da estrutura interna dos módulos. Portanto, nosso interesse reside na classificação da estrutura dos módulos e seus produtos em relação a uma álgebra bidimensional trivial, dentro do contexto da variedade de álgebras comutativas de potências associativas com nilíndice quatro. Propondo um método computacional que utiliza as bases de Gröbner para obter a classificação.

Na classificação, a variedade afim das matrizes nilpotentes é definida. No entanto, ao perceber que todos os polinômios que surgem na classificação proposta são homogêneos, é mais apropriado trabalhar com o espaço projetivo do que com o espaço afim. Este fato exclui o módulo trivial zero de nossas análises.

O Capítulo 1 inicia com definições preliminares essenciais para compreender os conceitos fundamentais da teoria de bases de Gröbner. São abordados temas como anéis polinomiais sobre um corpo k e ideais. Explora-se a importância das ordens monômiais na organização e comparação de polinômios (ordenação influencia a construção das bases de Gröbner). Então é possível definir o algoritmo da divisão generalizada que estende o tradicional algoritmo de divisão polinomial. O foco é a definição e propriedades das bases de Gröbner. São explorados os conceitos fundamentais de geração de ideais e como as bases de Gröbner facilitam a resolução de sistemas polinomiais. O teorema de Buchberger e outras propriedades importantes das bases de Gröbner são discutidos. A última parte do capítulo introduz o algoritmo F4, um avanço significativo na eficiência do cálculo de bases de Gröbner. Na elaboração deste capítulo, baseamo-nos principalmente em [4], [5] e [3].

O Capítulo 2 inicia explorando os conjuntos algébricos afins, que são soluções comuns de sistemas de equações polinomiais em várias variáveis. Conceitos fundamentais são estabelecidos para construir a base necessária para compreender a geometria algébrica a topologia de Zariski, uma abordagem topológica de aneis para entender conjuntos algébricos. Discutem-se os conceitos de fecho algébrico, conjuntos abertos e fechados de Zariski. Exploramos o Teorema dos Zeros de Hilbert, estabelecendo uma ponte entre a álgebra e a geometria. Introduz-se o espaço projetivo, o qual é o nosso foco principal, é uma extensão natural do espaço afim que lida com retas projetivas e coordenadas homogêneas. Discutimos as transformações entre o espaço afim e o projetivo. O capítulo conclui com uma discussão sobre a aplicação da topologia de Zariski no espaço projetivo. Na elaboração deste capítulo, baseamo-nos principalmente em [9] e [6].

O Capítulo 3 tem início com a definição da variedade afim das matrizes nilpotentes e das propriedades que serão posteriormente utilizadas. São apresentados os tipos de álgebras com os quais trabalharemos: zero álgebra, nilálgebra, álgebra nilpotente e álgebra de potências associativas. O propósito deste capítulo é investigar a estrutura de módulos e seus produtos em relação a uma álgebra bidimensional trivial, no contexto da variedade de álgebras comutativas de potências associativas com nilíndice quatro. Os módulos irredutíveis de dimensão 3 já foram classificados em uma abordagem diferente no trabalho de [10]. Finalmente, o procedimento computacional proposto no sistema algébrico computacional SageMath para calcular e simplificar o processo é apresentado. Na elaboração deste capítulo, baseamo-nos principalmente em [7] e [10].

Capítulo 1

Bases de Gröbner

Neste capítulo, direcionaremos nossa atenção para a seção 2 do livro [4] onde encontramos os conceitos que serão abordados com maior profundidade. Esses conceitos desempenham um papel fundamental no desenvolvimento dos objetivos deste trabalho, tornando-se peças-chave na compreensão e aplicação das ideias que exploraremos.

1.1 Definições preliminares

Antes de dar uma definição geral de polinômios, primeiro lembramos ao leitor um caso especial familiar: polinômios em uma variável ou indeterminada x com coeficientes reais. Tal polinômio é geralmente escrito na forma

$$f = \sum_{i=0}^{m} a_i x^i,$$

com $a_i \in \mathbb{R}$ para $0 \leq i \leq m$. Claramente, f é unicamente determinado por a_i. Agora vamos generalizar isso. Em primeiro lugar, os reais pode ser substituído por um anel arbitrário k, o que não causa nenhum problema de definição. Em segundo lugar, queremos permitir múltiplas variáveis, ou seja, precisamos de coeficientes não apenas para potências x^i de x, mas para produtos de potência de n variáveis $x_1, x_2, \ldots, x_n$

Definição 1.1.1. *Um **monômio** nas variáveis $x_1, \ldots, x_n$ 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** deste monômio é a soma $\alpha_1 + \cdots + \alpha_n$. De modo a simplificar a notação podemos tomar $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, e escrever*

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

Dessa forma, para $\alpha = (0, 0, \ldots, 0)$ teremos $x^\alpha = 1$ e $|\alpha| = \alpha_1 + \cdots + \alpha_n$ denotará o grau total desse monômio.

Definição 1.1.2. *Um **polinômio** f nas variáveis (ou indeterminadas) $x_1, x_2, \ldots, x_n$ com coeficientes em um corpo k é uma combinação linear finita de monômios nas variáveis $x_1, x_2, \ldots, x_n$. Escrevemos o polinômio f na forma:*

$$f = \sum a_\alpha x^\alpha \text{ com } a_\alpha \in k,$$

com a soma sobre um número finito de n-úplas $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. *O conjunto de todos os polinômios em* $x_1, \ldots, x_n$ *com coeficientes em* k *é denotado por* $k[x_1, \ldots, x_n]$.

Exemplo 1.1.3. *Os polinômios em um pequeno número de variáveis geralmente utilizam as variáveis* x, y *e* z. *Portanto, os polinômios em uma, duas e três variáveis são* $k[x]$, $k[x, y]$, *e* $k[x, y, z]$, *respectivamente. Assim,*

$$f(x, y, z) = xy^2z^3 + \frac{2}{5}y^3z^3 - 5z^2 + 9,$$

é um polinômio em $\mathbb{Q}[x, y, z]$.

Observação 1.1.4. *Denotamos por* $T(x_1, \ldots, x_n)$ *ou simplesmente por* T, *o conjunto de todos os Monômios.* T *forma um monóide abeliano com elemento neutro 1 sob multiplicação natural, onde dois monômios são multiplicados pela soma dos respectivos expoentes de cada variável:*

$$x^\alpha \cdot x^\beta = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \cdot x_1^{\beta_1} \cdots x_n^{\beta_n} = x_1^{\alpha_1+\beta_1} \cdots x_n^{\alpha_n+\beta_n} = x^{\alpha+\beta},$$

com $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ *e* $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ *em* $\mathbb{Z}^n_{\geq 0}$. *Um isomorfismo natural* $(T, 1, \cdot) \longrightarrow (\mathbb{Z}^n_{\geq 0}, (0), +)$ *é dado pela função expoente* η *que atribui a qualquer Monomial sua upla expoente, ou seja*

$$\eta(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}.$$

Uma vez que um polinômio é definido, podemos, de maneira análoga ao que é feito no anel de polinômios em uma única variável, definir as seguintes noções.

Definição 1.1.5. *Seja* $f = \sum a_\alpha x^\alpha$ *um polinômio em* $k[x_1, \ldots, x_n]$

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

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

(iii) O ***grau total*** *de* $f \neq 0$, *denotado* $\mathbf{deg(f)}$, *é o máximo* $|\alpha|$ *tal que o coeficiente* a_α *é diferente de zero.*

Exemplo 1.1.6. *Como exemplo, considere o polinômio* $f(x, y, z) = xy^2z^3 + \frac{2}{5}y^3z^3 - 5z^2 + 9$ *dado acima, que possui quatro termos e um grau total de seis. Observe que existem dois termos com o grau total máximo, algo que não acontece para polinômios de uma única variável.*

Agora vamos definir o conceito de ideal no anel de polinômios. Um ideal do anel de polinômios é um subconjunto de polinômios que possui propriedades fechadas sob adição e multiplicação. Os ideais desempenham um papel fundamental na descrição e estudo no trabalho a seguir.

Definição 1.1.7. *Um subconjunto* $I \subseteq k[x_1, \ldots, x_n]$ *é um* ***ideal*** *se satisfaz:*

(i) $0 \in I$.

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

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

Um exemplo comum de ideal é o ideal gerado por um conjunto finito de polinômios.

Definição 1.1.8. *Sejam $f_1, \ldots, f_s$ polinômios em $k[x_1, \ldots, x_n]$. Denotaremos por $\langle f_1, \ldots, f_s \rangle$ o* ***ideal gerado por*** *$f_1, \ldots, f_s$. Esse conjunto é definido como:*

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

É crucial destacar que o conjunto $\langle f_1, \ldots, f_s \rangle$ é, de fato, um ideal.

Lema 1.1.9. *Se $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, então $\langle f_1, \ldots, f_s \rangle$ é um ideal de $k[x_1, \ldots, x_n]$.*

Demonstração: Primeiro, $0 \in \langle f_1, \ldots, f_s \rangle$ onde $0 = \sum_{i=0}^{s} 0 \cdot f_i$. Em seguida, suponha que $f = \sum_{i=0}^{s} p_i f_i$ e $g = \sum_{i=0}^{s} g_i f_i$, e sejam $h \in k[x_1, \ldots, x_n]$. Então as equações

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

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

1.2 Ordens Monomiais

Uma vez que um polinômio é uma soma de monômios, surge a necessidade de organizar os termos de um polinômio de forma inequívoca em ordem decrescente ou crescente. Para isso, é preciso ser capaz de comparar cada par de monômios e estabelecer suas posições relativas adequadas. Portanto, é exigido que as ordenações sejam lineares ou totais. Isso significa que para cada par de monômios x^α e x^β, exatamente uma das três afirmações

$$x^\alpha > x^\beta, \quad x^\alpha = x^\beta, \quad x^\alpha < x^\beta$$

deve ser verdade.
Em seguida, devemos levar em consideração o efeito das operações de soma e produto em polinômios. Quando adicionamos polinômios, depois de combinar termos semelhantes, podemos simplesmente reorganizar os termos presentes na ordem apropriada, de modo que as somas não apresentem dificuldades. Os produtos são mais sutis, no entanto. Como a multiplicação em um anel polinomial se distribui pela adição, basta considerar o que acontece quando multiplicamos um monômio por um polinômio. Se isso mudasse a ordem relativa dos termos, problemas significativos poderiam resultar em qualquer processo semelhante ao algoritmo de divisão em $k[x]$, no qual devemos identificar os termos principais em polinômios. A razão é que o termo principal no

produto pode ser diferente do produto do monômio e o termo principal do polinômio original.
Portanto, exigiremos que todas as ordenações monomiais tenham a seguinte propriedade adicional. Se $x^\alpha > x^\beta$ e x^γ for qualquer monômio, então exigimos que $x^\alpha x^\gamma > x^\beta x^\gamma$. Em termos dos vetores expoentes, esta propriedade significa que se $\alpha > \beta$ em nossa ordenação em $\mathbb{Z}^n_{\geq 0}$, então, para todo $\gamma \in \mathbb{Z}^n_{\geq 0}$, $\alpha + \gamma > \beta + \gamma$. Com essas considerações em mente, fazemos a seguinte definição.

Definição 1.2.1. *Uma* ***ordem monomial*** $>$ *em* $k[x_1, \ldots, x_n]$ *é uma relação* $>$ *em* $\mathbb{Z}^n_{\geq 0}$*, ou equivalentemente, uma relação no conjunto de monômios* x^α*,* $\alpha \in \mathbb{Z}^n_{\geq 0}$*, satisfazendo:*

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

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

(iii) $>$ *é uma boa ordenação em* $\mathbb{Z}^n_{\geq 0}$*. Isso significa que todo subconjunto não vazio de* $\mathbb{Z}^n_{\geq 0}$ *tem um menor elemento sob* $>$*.*

O seguinte lema nos ajudará a entender o que significa a condição de boa ordenação da parte (*iii*) da definição.

Lema 1.2.2. *Uma relação de ordem* $>$ *em* $\mathbb{Z}^n_{\geq 0}$ *é uma boa ordenação se, e somente se, toda sequência estritamente decrescente em* $\mathbb{Z}^n_{\geq 0}$

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

eventualmente termina

Demonstração: Vamos provar isso na forma contrapositiva: $>$ não é uma boa ordenação se, e somente se, existe uma sequência infinita estritamente decrescente 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 o menor elemento. Agora escolha $\alpha(1) \in S$. Como $\alpha(1)$ não é o menor elemento, podemos encontrar $\alpha(1) > \alpha(2)$ em S. Então $\alpha(2)$ também não é o menor elemento, de modo que não é $\alpha(2) > \alpha(3)$ em S. Continuando assim, obtemos uma sequência infinita estritamente decrescente

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

Reciprocamente, dada tal sequência infinita, então $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ é um subconjunto não vazio de $\mathbb{Z}^n_{\geq 0}$ sem nenhum elemento mínimo e, portanto, $>$ não é uma boa ordenação. □

Uma vez que a noção de ordem monomial esteja clara, podemos prosseguir com a definição e exemplos de algumas ordens monomiais em $k[x_1, \ldots, x_n]$.

Definição 1.2.3. ***(Ordem lexicográfica)****. Seja* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *e* $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$*. Dizemos* $\alpha >_{lex} \beta$ *se, no vetor diferença* $\alpha - \beta \in \mathbb{Z}^n$*, a entrada não nula mais à esquerda é positiva. Escreveremos* $x^\alpha >_{lex} x^\beta$ *se* $\alpha >_{lex} \beta$*.*

Exemplo 1.2.4. *Alguns exemplos:*

a. *Temos* $xy^2z^4 >_{lex} xy^2z^2$, *pois* $\alpha = (1,2,4) >_{lex} (1,2,2) = \beta$, *já que* $\alpha - \beta = (1,0,-2)$.

b. *Temos* $xy^2z^4 >_{lex} xy^2z^2$, *pois* $\alpha = (1,2,4) >_{lex} (1,2,2) = \beta$, *já que* $\alpha - \beta = (0,0,2)$.

c. *As variáveis* $x_1, \ldots, x_n$ *são ordenadas da maneira usual pela ordem lex:*

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

então $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$.

É importante perceber que existem muitas ordens lex, correspondentes a como as variáveis são ordenadas. Até agora, usamos a ordem lex com $x_1 > x_2 > \cdots > x_n$. Mas dada qualquer ordenação das variáveis $x_1, \ldots, x_n$, existe uma ordem lex correspondente. Por exemplo, se as variáveis são x e y, obtemos uma ordem *lex* com $x > y$ e uma segunda com $y > x$. No caso geral de n variáveis, existem $n!$ ordens de *lex*. A seguir, a frase "ordem *lex*" se referirá àquela com $x_1 > \cdots > x_n$, salvo indicação em contrário. Na ordem *lex*, observe que uma variável domina qualquer monômio envolvendo apenas variáveis menores, independentemente de seu grau total. Assim, para a ordem lex com $x > y > z$, temos tem $x^2 >_{lex} xy^3z^2$.

Proposição 1.2.5. *A ordem lex sobre* $\mathbb{Z}^n_{\geq 0}$ *é uma ordem monomial.*

Demonstração: (i) Que $>_{lex}$ é uma ordem total segue diretamente da definição e do fato de que a ordem numérica usual em $\mathbb{Z}^n_{\geq 0}$ é uma ordem total.
(ii) Se $\alpha >_{lex} \beta$, então temos que a entrada não nula mais à esquerda em $\alpha - \beta$, digamos $\alpha_k - \beta_k$, é positiva. Mas $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ e $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Então, em $(\alpha+\gamma)-(\beta+\gamma) = \alpha-\beta$, a entrada não nula mais à esquerda é novamente $\alpha_k - \beta_k > 0$.
(iii) Suponha que $>_{lex}$ não seja uma boa ordenação. Então, pelo Lema 1.2.2, haveria uma sequência infinita estritamente decrescente.

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

de elementos de $\mathbb{Z}^n_{\geq 0}$. Mostraremos que isso leva a uma contradição. Considere as primeiras entradas dos vetores $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Pela definição da ordem lexicográfica, essas primeiras entradas formam uma sequência não crescente de inteiros não negativos. Como $\mathbb{Z}^n_{\geq 0}$ é bem-ordenado, as primeiras entradas das $\alpha(i)$ devem "estabilizar" eventualmente. Ou seja, existe um k tal que todos os primeiros componentes das $\alpha(i)$ com $i \geq k$ são iguais.
A partir de $\alpha(k)$, as segundas e subsequentes entradas entram em jogo para determinar a ordem lex. As segundas entradas de $\alpha(k), \alpha(k+1), \ldots$ formam uma sequência não crescente. Pelo mesmo raciocínio anterior, as segundas entradas "estabilizam" eventualmente também. Continuando da mesma forma, vemos que, para algum l, as $\alpha(l), \alpha(l+1), \ldots$ são todas iguais. Isso contradiz o fato de que $\alpha(l) >_{lex} \alpha(l+1)$. □

Definição 1.2.6. ***(Ordem lexicográfica reversa).*** *Seja* $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ *e* $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. *Dizemos* $\alpha >_{revlex} \beta$ *se, vetor diferença* $\alpha - \beta \in \mathbb{Z}^n$, *a entrada não nula mais à direita é negativa. Escreveremos* $x^\alpha >_{revlex} x^\beta$ *se* $\alpha >_{revlex} \beta$.

Exemplo 1.2.7. *Alguns exemplos:*

a. *Temos* $xy^3 >_{revlex} y^3z^2$, *pois* $\alpha = (1,3,0) >_{revlex} (0,3,2) = \beta$, *já que* $\alpha - \beta = (1,0,-2)$.

b. *Temos* $xy^2z^2 >_{revlex} xy^2z^4$, *pois* $\alpha = (1,2,2) >_{revlex} (1,2,4) = \beta$, *já que* $\alpha - \beta = (0,0,-2)$.

c. *As variáveis* $x_1, \ldots, x_n$ *são ordenadas da maneira usual pela ordem revlex:*

$$(1,0,\ldots,0) >_{revlex} (0,1,0,\ldots,0) >_{revlex} \cdots >_{revlex} (0,\ldots,0,1).$$

então $x_1 >_{revlex} x_2 >_{revlex} \cdots >_{revlex} x_n$.

Definição 1.2.8. ***(Ordem monomial lexicográfica graduada)*** *Sejam* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. *Dizemos que*

$$\alpha >_{grlex} \beta \text{ se } |\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ ou } (|\alpha| = |\beta| \text{ e } \alpha >_{lex} \beta).$$

Exemplo 1.2.9. *Alguns exemplos:*

a. *Temos* $y^3z^2 >_{grlex} xy^3$, *pois* $(0,3,2) >_{grlex} (1,3,0)$, *já que* $|(0,3,2)| = 5 > |(1,3,0)| = 4$.

b. *Temos* $xy^2z^4 >_{grlex} xy^2z^2$, *pois* $(1,2,4) >_{grlex} (1,2,2)$, *já que* $|(1,2,4)| = 7 > |(1,2,2)| = 5$.

c. *Temos* $x^4yz^3 >_{grlex} xy^5z^2$, *pois* $(4,1,3) >_{grlex} (1,5,2)$, *já que* $|(4,1,3)| = |(1,5,2)|$ *e* $(4,1,3) - (1,5,2) = (3,-4,1)$, *o que significa que* $(4,1,3) >_{lex} (1,5,2)$.

d. *As variáveis* $x_1, \ldots, x_n$ *são ordenadas da maneira usual pela ordem grlex:*

$$(1,0,\ldots,0) >_{grlex} (0,1,0,\ldots,0) >_{grlex} \cdots >_{grlex} (0,\ldots,0,1).$$

então $x_1 >_{grlex} x_2 >_{grlex} \cdots >_{grlex} x_n$.

Definição 1.2.10. ***(Ordem monomial lexicográfica graduada reversa)*** *Sejam* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. *Dizemos que*

$$\alpha >_{grevlex} \beta \text{ se } |\alpha| = \textstyle\sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ ou } (|\alpha| = |\beta| \text{ e } \alpha >_{revlex} \beta).$$

Exemplo 1.2.11. *alguns exemplos:*

a. *Temos* $y^3z^2 >_{grevlex} xy^3$, *pois* $(0,3,2) >_{grevlex} (1,3,0)$, *já que* $|(0,3,2)| = 5 > |(1,3,0)| = 4$.

b. *Temos* $xy^2z^4 >_{grevlex} xy^2z^2$, *pois* $(1,2,4) >_{grevlex} (1,2,2)$, *já que* $|(1,2,4)| = 7 > |(1,2,2)| = 5$.

c. *Temos* $xy^5z^2 >_{grevlex} x^4yz^3$, *pois* $(1,5,2) >_{grevlex} (4,1,3)$, *já que* $|(1,5,2)| = |(4,1,3)|$ *e* $(1,5,2) - (4,1,3) = (-3,4,-1)$, *o que significa que* $(1,5,2) >_{revlex} (4,1,3)$.

d. As variáveis $x_1, \ldots, x_n$ são ordenadas da maneira usual pela ordem grevlex:

$$(1, 0, \ldots, 0) >_{grevlex} (0, 1, 0, \ldots, 0) >_{grevlex} \cdots >_{grevlex} (0, \ldots, 0, 1).$$

então $x_1 >_{grevlex} x_2 >_{grevlex} \cdots >_{grevlex} x_n$.

A prova de que as últimas ordens definidas (revlex, grlex e grevlex) satisfazem a Definição 1.2.1 de uma ordem monomial é semelhante à Demonstração 1.2.5.
Agora podemos ordenar os polinômios. Se tivermos um polinômio $f = \sum a_\alpha x^\alpha$ com $a_\alpha \in k$, em $k[x_1, \ldots, x_n]$ e escolhermos uma ordem monomial $>$, então é possível ordenar os monômios de f de forma inequívoca em relação a $>$.

Exemplo 1.2.12. *Seja $f(x, y, z) = xy^2z^3 + 4x^2 + \frac{2}{5}y^3z^3 - 5z^2 + 9 \in k[x, y, z]$. Então reordenaríamos os termos de f em ordem decrescente como:*

a. Com relação à ordem $>_{lex}$,

$$f(x, y, z) = 4x^2 + xy^2z^3 + \frac{2}{5}y^3z^3 - 5z^2 + 9.$$

b. Com relação à ordem $>_{revlex}$,

$$f(x, y, z) = 4x^2 - 5z^2 + xy^2z^3 + \frac{2}{5}y^3z^3 + 9.$$

c. Com relação à ordem $>_{grlex}$,

$$f(x, y, z) = xy^2z^3 + \frac{2}{5}y^3z^3 + 4x^2 - 5z^2 + 9.$$

d. Com relação à ordem $>_{grevlex}$,

$$f(x, y, z) = xy^2z^3 + \frac{2}{5}y^3z^3 + 4x^2 - 5z^2 + 9.$$

Usaremos a seguinte terminologia, para a implementação do algoritmo de divisão generalizada e para o desenvolvimento da teoria em diante.

Definição 1.2.13. *Seja $f = \sum_\alpha a_\alpha x^\alpha$ um polinômio diferente de zero em $k[x_1, \ldots, x_n]$ e seja $>$ uma ordem monomial*

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

(ii) $LC(f) = a_{multideg(f)} \in k$ *(**coeficiente principal** de f).*

(iii) $LM(f) = x_{multideg(f)}$ *(**monômio principal** de f).*

(iv) $LT(f) = LC(f)LM(f)$ *(**termo principal** de f).*

Usaremos a notação $LT_>(f)$ para **(termo principal de f)**, ou simplesmente $LT(f)$ se não houver possibilidade de confusão sobre a ordem monomial que está sendo usado.

Exemplo 1.2.14. *seja $f(x, y, z) = xy^2z^3 + 4x^2 + \frac{2}{5}y^3z^3 - 5z^2 + 9 \in k[x, y, z]$. Então, com relação à ordem $>_{lex}$,*

$$f(x, y, z) = 4x^2 + xy^2z^3 + \frac{2}{5}y^3z^3 - 5z^2 + 9,$$

a. $multideg(f) = (2, 0, 0)$.

b. $LC(f) = 4$.

c. $LM(f) = x^2$.

d. $LT(f) = 4x^2$.

O seguinte Lema será usado na prova do algoritmo de divisão generalizada.

Lema 1.2.15. *Sejam $f, g \in k[x_1, \ldots, x_n]$ polinômios não-nulos. Então:*

(i) $multideg(fg) = multideg(f) + multideg(g)$;

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

Demonstração: Sejam $f = \sum_\alpha a_\alpha x^\alpha$ e $g = \sum_\alpha b_\alpha x^\alpha$.

(i)

$$\begin{aligned}
\text{multideg}(fg) &= \text{multideg}\left(\sum_\alpha \sum_\beta a_\alpha b_\beta x^{\alpha+\beta}\right) \\
&= \max_{a_\alpha b_\beta \neq 0} (\alpha + \beta) \\
&= \max_{a_\alpha \neq 0, b_\beta \neq 0} (\alpha + \beta) \\
&= \max_{a_\alpha \neq 0}(\alpha + \max_{b_\beta \neq 0} \beta) \\
&= \max_{a_\alpha \neq 0}(\alpha) + \max_{b_\beta \neq 0}(\beta) \\
&= \text{multideg}(f) + \text{multideg}(g).
\end{aligned}$$

(ii) Temos que

$$\begin{aligned}
\text{multideg}(f + g) &= \text{multideg}\left(\sum_\alpha (a_\alpha + b_\alpha) x^\alpha\right) \\
&= \max_{a_\alpha + b_\alpha \neq 0} (\alpha).
\end{aligned}$$

Observando que $\{\alpha \mid a_\alpha + b_\alpha \neq 0\} \subseteq \{\alpha \mid a_\alpha \neq 0 \text{ ou } b_\alpha \neq 0\}$, temos

$$\max_{a_\alpha + b_\alpha \neq 0} (\alpha) \leq \max_{a_\alpha \neq 0, b_\alpha \neq 0} (\alpha) = \max(\max_{a_\alpha \neq 0}(\alpha), \max_{b_\alpha \neq 0}(\alpha)) = \max(\text{multideg}(f), \text{multideg}(g)).$$

Se $\text{multideg}(f) \neq \text{multideg}(g)$: Suponha, sem perda de generalidade, que $\text{multideg}(f) > \text{multideg}(g)$. Então, temos $a_{\text{multideg}(f)} \neq 0$ e $b_{\text{multideg}(g)} = 0$. Observando que $\text{multideg}(f) \in \{\alpha \mid a_\alpha + b_\alpha \neq 0\}$, temos

$$\max_{a_\alpha + b_\alpha \neq 0} \alpha \geq \text{multideg}(f) = \max(\text{multideg}(f), \text{multideg}(g)).$$

O que é a desigualdade oposta ao (ii). Portanto,

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

Se $\text{multideg}(f) = \text{multideg}(g)$ e $LC(f) + LC(g) \neq 0$: Nesse caso, temos $a_{\text{multideg}(f)} + b_{\text{multideg}(g)} \neq 0$, e o mesmo argumento acima se aplica.

□

A partir deste ponto em diante, iremos supor que uma ordem monomial específica foi selecionada e que os termos principais, e elementos como os de a Definição 1.2.13, serão calculados exclusivamente com base nessa ordem.

1.3 Algoritmo da divisão generalizada

O algoritmo de divisão pode ser usado para resolver o problema de pertinência ideal para polinômios de uma variável. Para estudar este problema quando há mais variáveis, vamos formular um algoritmo de divisão para polinômios em $k[x_1, \dots, x_n]$, que envolve a divisão de um polinômio f em $k[x_1, \dots, x_n]$ por polinômios $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ para expressá-lo na forma $f = a_1 f_1 + \cdots + f_s + r$. O resto r deve ser cuidadosamente caracterizado usando ordens monomiais.

Exemplo 1.3.1. *Vamos primeiro dividir $f = x^2y + 1$ por $f_1 = xy + 1$ e $f_2 = y + 1$, usando ordem monomial $x >_{lex} y$ (que também estabelece a ordem na qual os polinômios divisores são listados e ordenados. $f_1 >_{lex} f_2$). Queremos empregar o mesmo esquema usado para a divisão de polinômios de uma variável, a diferença é que agora existem vários divisores e quocientes. Listando os divisores f_1, f_2 e os quocientes a_1, a_2 verticalmente, temos o*

$$\begin{array}{r|l}
a_1 : & \\
a_2 : & \qquad\qquad\qquad\qquad r \\
\hline
xy+1 & x^2y+1 \\
y+1 &
\end{array}$$

Os termos principais $LT(f_1) = xy$ e $LT(f_2) = y$ dividem o termo principal $LT(f) = x^2y$. Dado que f_1 aparece primeiro, optamos por utilizá-lo. Portanto, realizamos a divisão de x^2y por xy, o que resulta em x

$$\begin{array}{r|l}
a_1 : x & \\
a_2 : & \qquad\qquad\qquad\qquad r \\
\hline
xy+1 & x^2y+1 \\
y+1 & x^2y+x
\end{array}$$

e em seguida, subtraímos $x \cdot f_1$ de f:

$$\begin{array}{r|l}
a_1 : x & \\
a_2 : & \qquad\qquad\qquad\qquad r \\
\hline
xy+1 & x^2y+1 \\
y+1 & x^2y+x \\
\hline
 & \qquad -x+1
\end{array}$$

Agora, repetimos o mesmo processo para $-x + 1$. Neste caso, devemos testar f_2, pois $LT(f_1) = xy$ não divide $LT(-x + 1) = -x$. Mas $LT(f_2) = y$ também não divide $-x$.

Assim, se movermos $-x$ para o resto, podemos continuar dividindo, colocando $-x$ para a coluna do resto

a_1 : x				
a_2 :				r
$xy+1$	x^2y+1			
$y+1$	x^2y+x			
		$-x+1$	$\longrightarrow$	$-x$
		1		

de forma análoga ao passo anterior

a_1 : x				
a_2 :				r
$xy+1$	x^2y+1			
$y+1$	x^2y+x			
		$-x+1$	$\longrightarrow$	$-x$
		1	$\longrightarrow$	$-x+1$
		0		

Assim, o resto é $-x+1$, e obtemos

$$f = x^2y + 1 = x(xy+1) + 0(y+1) + (-x+1) = a_1f_1 + a_2f_2 + r.$$

Observação 1.3.2. *Observe que o resto é uma soma de monômios, nenhum dos quais é divisível pelos termos principais $LT(f_1)$ ou $LT(f_2)$.*

Observação 1.3.3. *Em todos os momentos, assumiremos k um corpo, e o anel polinomial $k[x_1, \ldots, x_n]$ sobre k também será denotado por $k[\bar{x}]$, se não houver possibilidade de confusão sobre as variaveis $x_1, \ldots, x_n$. Fixamos uma ordem monomial $>$ em T e denotamos a quase-ordem linear induzida em $k[\bar{x}]$ por $>$ também.*

Definição 1.3.4. *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, $x^\beta = x^\gamma \cdot x^\alpha$.*

Exemplo 1.3.5. *Sejam $x^2y, x^2y^3z, x^3 \in k[x, y, z]$.*

a. *Temos que x^2y divide x^2y^3z onde $(2, 3, 1) = (0, 2, 1) + (2, 1, 0)$, isto é, $x^2y^3z = y^2z \cdot x^2y$.*

b. *Temos que x^2y não divide x^3. Suponha que sim $(3, 0, 0) = (a, b, c) + (2, 1, 0)$, portanto $(a, b, c) = (1, -1, 0) \notin \mathbb{Z}^n_{\geq 0}$.*

Teorema 1.3.6. ***(Algoritmo da divisão generalizada)*** *Seja $k[\bar{x}] = k[x_1, \ldots, x_n]$. Fixe uma ordem monomial $>$ em $k[\bar{x}]$ e considere $F = (f_1, \ldots, f_s)$ uma s-upla ordenada de polinômios em $k[\bar{x}]$. Então, todo $f \in k[\bar{x}]$ pode ser expresso como*

$$f = a_1f_1 + \cdots + a_sf_s + r, \text{ com } a_i, r \in k[\bar{x}].$$

Onde $r = 0$ ou r é uma combinação linear de monômios, nenhum dos quais é divisível por $LT_>(f_1), \ldots, LT_>(f_s)$. Chamaremos r o resto de f na divisão por F. Além disso, se $a_if_i \neq 0$, então $multideg(f) \geq multideg(a_if_i)$.

Demonstração: Provemos a existência de $a_1, \ldots, a_s$ e r fornecendo um algoritmo para sua construção e mostrando que ele opera corretamente em qualquer dado de entrada.

Especifi: $(a_1, \ldots, a_s, r) \leftarrow DIVPOL(f, F)$
divisão de f por $F = (f_1, \ldots, f_s)$
Dado: $f_1, \ldots, f_s, f \in k[\bar{x}]$
Encon: $a_1, \ldots, a_s, r \in k[\bar{x}]$ polinômios com $f = \sum_{i=1}^{s} a_i f_i + r$ e
$max\{LT(a_i f_i), 1 \leq i \leq s\} \leq LT(f)$

começar
$a_i \leftarrow 0$ (para $1 \leq i \leq s$)
$r \leftarrow 0$
$p \leftarrow f$
enquanto $p \neq 0$ **fazer**
$i \leftarrow 1$
divisionoccurred $\leftarrow$ **falso**
enquanto $i \leq s$ **e** divisionoccurred $=$ **falso fazer**
se $LT(f_i)$ divide $LT(p)$ **então**
$a_i \leftarrow a_i + LT(p)/LT(f_i)$
$p \leftarrow p - (LT(p)/LT(f_i))f_i$
divisionoccurred $=$ **verdadeiro**
outro $i \leftarrow i + 1$
se divisionoccurred $=$ **falso então**
$r \leftarrow r + LT(p)$
$p \leftarrow p - LT(p)$
retornar $a_1, \ldots, a_s, r$

Podemos relacionar este algoritmo com o Exemplo 1.3.1 observando que a variável p representa o dividendo intermediário em cada estágio, a variável r representa a coluna do lado direito e as variáveis $a_1, \ldots, a_s$ como são os quocientes listados acima do radical. Finalmente, a variável booleana "divisionoccurred" nos diz quando algum $LT(f_i)$ divide o termo principal do dividendo intermediário. Você deve verificar isso toda vez que passarmos pelo loop principal **enquanto . . . fazer** , precisamente uma das duas coisas acontece:

(*i*) (Passo da divisão) Se algum $LT(f_i)$ divide $LT(p)$, então o algoritmo procede como no caso de uma variável.

(*ii*) (Passo resto) Se nenhum $LT(f_i)$ divide $LT(p)$, então o algoritmo adiciona $LT(p)$ ao resto.

Para provar que o algoritmo funciona, primeiro mostraremos que:

$$f = a_1 f_1 + \cdots + a_s f_s + p + r, \tag{1.1}$$

detém em todas as fases. Isso é claramente verdadeiro para os valores iniciais de $a_1, \ldots, a_s, p$ e r, com $f = 0 \cdot f_1 + \cdots + 0 \cdot f_s + f + 0$. Agora suponha que (1.1) seja válido em um passo do algoritmo. Se o próximo passo for um Passo de Divisão, então algum $LT(f_i)$ divide $LT(p)$, e a igualdade

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

mostra que $a_i f_i + p$ permanece inalterado. Como todas as outras variáveis não são afetadas, (1.1) permanece verdadeiro neste caso. Por outro lado, se a próximo passo for um passo de resto, então p e r serão alterados, mas a soma $p + r$ permanece inalterada, pois

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

Como antes, a igualdade (1.1) ainda é preservada.
Em seguida, observe que o algoritmo para quando $p = 0$. Nessa situação, (1.1) torna-se

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

Como os termos são adicionados a r apenas quando não são divisíveis por nenhum dos $LT(f_i)$, segue-se que $a_1, \ldots, a_s$ e r têm as propriedades desejadas quando o algoritmo termina. Finalmente, precisamos mostrar que o algoritmo eventualmente termina. A principal observação é que cada vez que redefinimos a variável p, ou seu multigrau cai (em relação à nossa ordenação de termos) ou se torna 0. Para ver isso, primeiro suponha que durante um passo de divisão, p é redefinido para ser

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

Pelo Lema 1.2.15, temos que

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

de forma que p e $(LT(p)/LT(f_i))f_i$ tem o mesmo termo principal. Portanto, sua diferença p' deve ter multigrau estritamente menor quando $p' \neq 0$. Em seguida, suponha que durante um passo Resto, p seja redefinido para ser

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

Aqui, é óbvio que $multideg(p') < multideg(p)$ quando $p' \neq 0$. Assim, em ambos os casos, o multigrau deve diminuir. Se o algoritmo nunca terminasse, obteríamos uma sequência infinita decrescente de multigraus. A propriedade de boa ordenação de $>$, como afirmado no Lema 1.2.2, mostra que isso não pode ocorrer. Assim, $p = 0$ deve acontecer eventualmente, de modo que o algoritmo termine após um número finito de passos. Resta estudar a relação entre $multideg(f)$ e $multideg(a_i f_i)$. Todo termo em a_i é da forma $LT(p)/LT(f_i)$ para algum valor da variável p. O algoritmo começa

com $p = f$, e acabamos de provar que o *multigrau* de p diminui. Isso mostra que $LT(p) < LT(f)$. Note também que cada termo de um quociente a_i não-nulo é da forma $LT(p)/LT(f_i)$ para algum passo da variável p. Em outras palavras a_i é da forma

$$a_i = 0 + LT(p_1)/LT(f_i) + LT(p_2)/LT(f_i) + \cdots + LT(p_k)/LT(f_i),$$

onde para $1 \leq j \leq k \leq s$ estamos denotado por p_j a variável p na j-ésima atualização de a_i.
Assim, pelo Lema 1.2.15 e por (1.1) temos:

$$\begin{aligned} multideg(LT(p_1)/LT(f_i)) + multideg(f_i) =& multideg((LT(p_1)/LT(f_i) \cdot f_i) \\ =& multideg(p_1) \\ \geq& multideg(p_j) \\ =& multideg((LT(p_j)/LT(f_i) \cdot f_i) \\ =& multideg(LT(p_j)/LT(f_i)) + multideg(f_i). \end{aligned}$$

Segue assim que $multideg(LT(p_1)/LT(f_i)) \geq multideg(LT(p_j)/LT(f_i))$ para todo $1 \leq j \leq k$. Portanto $multideg(a_i) = multideg(LT(p_1)/LT(f_i))$. Logo

$$multideg(a_i f_i) = multideg((LT(p_1)/LT(f_i))f_i) = multideg(p_1) \leq multideg(f),$$

quando $a_i f_i \neq 0$, o que conclui a demonstração. □

Exemplo 1.3.7. *Seja $f = x^2y + 1$ entre $F = (f_1, f_2)$ com $f_1 = xy + 1$ e $f_2 = y + 1$ além da ordem monomial $x >_{lex} y$, os polinômios já organizados de acordo com a ordem monomial $>_{lex}$ e $f_1 >_{lex} f_2$. Então, o algoritmo inicia com:*

$$a_1 = 0, \qquad r = 0,$$

$$a_2 = 0, \qquad p = x^2y + 1.$$

Como $LT(f_1) = xy$ divide $LT(p) = x^2y$, então, $LT(p)/LT(f_1) = x^2y/xy = x$ e atualizar

$$a_1 = a_1 + LT(p)/LT(f_1) = 0 + x = x,$$

$$a_2 = 0,$$

$$r = 0,$$

$$p = p - (LT(p)/LT(f_1))f_1 = x^2y + 1 - x(xy + 1) = -x + 1.$$

Como $LT(f_1) = xy$ e $LT(f_2) = y$ não dividem $LT(p) = -x$, de acordo com o algoritmo de divisão generalizada, atualizamos:

$$a_1 = x,$$

$$a_2 = 0,$$

$$r = r + LT(p) = 0 + (-x) = -x,$$

$$p = p - LT(p) = -x + 1 - (-x) = 1.$$

Novamente $LT(f_1) = xy$ e $LT(f_2) = y$ não dividem $LT(p) = 1$, de acordo com o algoritmo de divisão generalizada, atualizamos:

$$a_1 = x,$$

$$a_2 = 0,$$

$$r = r + LT(p) = -x + 1,$$

$$p = p - LT(p) = 1 - (1) = 0.$$

Já que temos $p = 0$, o algoritmo termina. Então

$$f = a_1 f_1 + a_2 f_2 + r = x(xy + 1) + 0(y + 1) + (-x + 1).$$

Exemplo 1.3.8. *Se listamos os polinômios da upla F no exemplo acima em outra ordem, ou seja, $f = x^2y + 1$ entre $F = (f_1, f_2)$ com $f_1 = y + 1$ e $f_2 = xy + 1$ e ordem monomial $x >_{lex} y$, os polinômios já organizados de acordo com a ordem monomial $>_{lex}$. Então, o algoritmo inicia com:*

$$a_1 = 0, \qquad r = 0,$$

$$a_2 = 0, \qquad p = x^2y + 1.$$

Como $LT(f_1) = y$ divide $LT(p) = x^2y$, então, $LT(p)/LT(f_1) = x^2y/y = x^2$ e atualizar

$$a_1 = a_1 + LT(p)/LT(f_1) = 0 + x^2 = x^2,$$

$$a_2 = 0,$$

$$r = 0,$$

$$p = p - (LT(p)/LT(f_1))f_1 = x^2y + 1 - x^2(y + 1) = -x^2 + 1.$$

Como $LT(f_1) = y, LT(f_2) = xy$ não dividem $LT(p) = -x^2$, de acordo com o algoritmo de divisão generalizada, atualizamos:

$$a_1 = x^2,$$

$$a_2 = 0,$$

$$r = r + LT(p) = 0 + (-x^2) = -x^2,$$

$$p = p - LT(p) = -x^2 + 1 - (-x^2) = 1.$$

Novamente $LT(f_1) = y, LT(f_2) = xy$ não dividem $LT(p) = 1$, de acordo com o algoritmo de divisão generalizada, atualizamos:

$$a_1 = x^2,$$

$$a_2 = 0,$$

$$r = r + LT(p) = -x^2 + 1,$$

$$p = p - LT(p) = 1 - (1) = 0.$$

Já que temos $p = 0$, o algoritmo termina. Então

$$f = a_1 f_1 + a_2 f_2 + r = x^2(y+1) + 0(xy+1) + (-x^2+1).$$

Ao comparar com o exemplo acima, é evidente que o resto é diferente. Isso demonstra que o resto r não é unicamente determinado pela condição de que nenhum de seus termos seja divisível por $LT(f_1), \ldots, LT(f_s)$. A situação não é completamente caótica: se seguirmos o algoritmo exatamente como declarado (o mais importante, testando $LT(p)$ para divisibilidade por $LT(f_1), LT(f_2), \ldots$ nessa ordem), então $a_1, \ldots, a_s$ e r são unicamente determinados. No entanto, os exemplos anteriores mostram que a ordenação da upla de polinômios $(f_1, \ldots, f_s)$ definitivamente importa, tanto em relação ao número de passos que o algoritmo levará para completar o cálculo quanto aos resultados obtidos. Os a_i e r podem mudar se simplesmente reorganizarmos os f_i. (Os a_i e r também podem mudar se mudarmos a ordem monomial). Uma boa característica do algoritmo de divisão em $k[x]$ é a maneira como ele resolve o problema de pertinência ao ideal. Podemos obter algo semelhante para várias variáveis? Um corolário fácil do Teorema 1.3.6 é que se, após a divisão de f por $F = (f_1, \ldots, f_s)$, obtemos um resto $r = 0$, então o polinômio f pertence ao ideal gerado por $f_1, \ldots, f_s$. No entanto, o contrário não é necessariamente verdadeiro: um polinômio pode pertencer ao ideal gerado por $f_1, \ldots, f_s$ sem ter resto zero após a divisão por F. A ordem dos polinômios e a ordem monomial desempenham papéis importantes nesse aspecto.

Consideraremos agora o problema de descrição e pertinência ao ideal para o caso especial de ideais monomiais.

Definição 1.3.9. *Um ideal $I \subset k[x_1, \ldots, x_n]$ é um **ideal monomial** se existe um subconjunto (possivelmente infinito) $A \subset \mathbb{Z}^n_{\geq 0}$ tal que I consiste em os polinômios que são somas finitas da forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, onde $h_\alpha \in K[x_1, \ldots, x_n]$. Neste caso, escrevemos $I = \langle x^\alpha : \alpha \in A \rangle$.*

Exemplo 1.3.10. $I = \langle x^5y^2, x^4y^3, x^2y^6 \rangle \subset k[x, y]$.

Lema 1.3.11. *Seja $I = \langle x^\alpha : \alpha \in A \rangle$ um ideal monomial. Então um monômio x^β está em I se, e somente se, x^β é divisível por x^α para algum $\alpha \in A$.*

Demonstração: Se x^β é um múltiplo de x^α para algum $\alpha \in A$, então $x^\beta \in I$ pela definição de ideal. Inversamente, se $x^\beta \in I$, então $x^\beta = \sum h_i x^{\alpha(i)}$, onde $h_i \in k[x_1, \ldots, x_n]$ e $\alpha(i) \in A$. Se expandirmos cada h_i como uma combinação linear de monômios, vemos que todo termo do lado direito da equação é divisível por algum $x^{\alpha(i)}$. Portanto, o lado esquerdo x^β deve ter a mesma propriedade. □

Observação 1.3.12. *x^β é divisível por x^α exatamente quando $x^\beta = x^\alpha \cdot x^\gamma$ para algum $\gamma \in \mathbb{Z}^n_{\geq 0}$. Isso é equivalente a $\beta = \alpha + \gamma$. Assim, o conjunto*

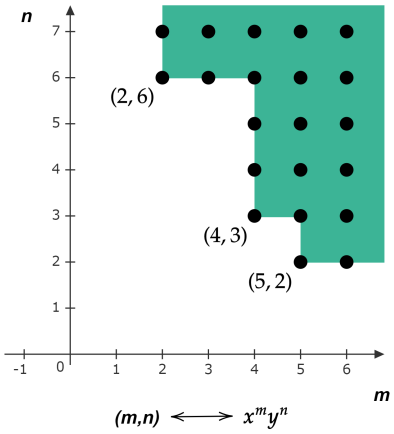
$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma : \gamma \in \mathbb{Z}^n_{\geq 0}\},$$

consiste nos expoentes de todos os monômios divisíveis por x^α. Esta observação e o Lema 1.2.2 nos permitem desenhar imagens dos monômios em um dado ideal monomial.

Exemplo 1.3.13. *Se* $I = \langle x^5y^2, x^4y^3, x^2y^6 \rangle$*, então os expoentes dos monômios em* I *formam o conjunto*

$$((5,2) + \mathbb{Z}^2_{\geq 0}) \cup ((4,3) + \mathbb{Z}^2_{\geq 0}) \cup ((2,6) + \mathbb{Z}^2_{\geq 0}).$$

Podemos visualizar este conjunto como a união dos pontos inteiros em três cópias transladadas do primeiro quadrante no plano:



No entanto, nenhum monômio com upla contida à esquerda e abaixo dos pontos $(2,6), (4,3), (5,2)$ *pertence ao ideal* I*, ja que eles não seriam divisíveis por nenhum dos monômios que geram* I*.*

Demonstraremos que é possível determinar se um determinado polinômio f pertence a um ideal monomial observando os monômios de f.

Lema 1.3.14. *Seja* $I = \langle x^\alpha : \alpha \in A \rangle$ *um ideal monomial, e seja* $f \in k[x_1, \ldots, x_n]$*. Então os seguintes são equivalentes:*

(i) $f \in I$*.*

(ii) Todo termo de f *está em* I*.*

(iii) f *é uma combinação* k*-linear dos monômios em* I*.*

Demonstração: As implicações $(iii) \implies (ii) \implies (i)$ são triviais. A prova de $(i) \implies (iii)$, se $f \in I$, então $f = \sum h_i x^{\alpha(i)}$, onde $h_i \in k[x_1, \ldots, x_n]$ e $\alpha(i) \in A$. Se expandirmos cada h_i como uma combinação linear de monômios, vemos que todo termo do lado direito da equação é divisível por algum $x^{\alpha(i)}$. Portanto, f sera uma combinação k-linear dos monômios em I. □

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

Corolário 1.3.15. *Dois ideais monomiais são iguais se, e somente se, eles contêm os mesmos monômios.*

Todos os ideais monomiais de $k[x_1, \ldots, x_n]$, são finitamente gerados. Essa propriedade de ter uma base finita de monômios é extremamente útil, pois simplifica o estudo e a manipulação de ideais monomiais. Podemos efetivamente trabalhar com um número limitado de monômios para representar o ideal monomial, o que facilita a análise e o cálculo relacionados a esse tipo de ideal.

Teorema 1.3.16. ***(Lema de Dickson).*** *Seja $I = \langle x^\alpha : \alpha \in A\rangle \subset k[x_1, \ldots, x_n]$ um ideal monomial. Então I pode ser escrito na forma $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$, onde $\alpha(1), \ldots, \alpha(s) \in A$. Em particular, I tem uma base finita.*

Demonstração: (Por indução em n, o número de variáveis). Se $n = 1$, então I é gerado pelos monômios x_1^α, onde $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Seja $\beta \leq \alpha$ o menor elemento de $A \subset \mathbb{Z}_{\geq 0}$. Então $\beta \leq \alpha$ para todo $\alpha \in A$, de modo que x_1^β, divida todos os outros geradores x_1^α. Daqui, $I = \langle x_1^\beta\rangle$ segue facilmente.
Agora assuma que $n > 1$ e que o teorema é verdadeiro para $n - 1$. Escreveremos as variáveis como $x_1, \ldots, x_{n-1}, y$, de modo que monômios em $k[x_1, \ldots, x_{n-1}, y]$ podem ser escritos como $x^\alpha y^m$, onde $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ e $m \in \mathbb{Z}_{\geq 0}$.
Suponha que $I \subset k[x_1, \ldots, x_{n-1}, y]$ seja um ideal monomial. Para encontrar geradores para I, seja J o ideal em $k[x_1, \ldots, x_{n-1}]$ gerado pelos monômios x^α para os quais $x^\alpha y^m \in I$ para algum $m \geq 0$. Visto que J é um ideal monomial em $k[x_1, \ldots, x_{n-1}]$, nossa hipótese indutiva implica que um número finito de x^α gera J, digamos $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$. O ideal J pode ser entendido como a "projeção" de I em $k[x_1, \ldots, x_{n-1}]$.
Para cada i entre 1 e s, a definição de J nos diz que $x^{\alpha(i)} y^{m_i} \in I$ para algum $m_i \geq 0$. Seja m o maior dos m_i. Então, para cada t entre 0 e $m - 1$, considere o ideal $J_t \subset k[x_1, \ldots, x_{n-1}]$ gerado pelos monômios x^β tais que $x^\beta y^t \in I$. Pode-se pensar em J_t como a "fatia" de I gerado por monômios contendo y exatamente à t-ésima potência. Usando nossa hipótese indutiva novamente, J_t tem um conjunto gerador finito de monômios, digamos $J_t = \langle x^{\alpha_t(1)}, \ldots, x^{\alpha_t(s_t)}\rangle$
Afirmamos que I é gerado pelos monômios na lista a seguir:

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

Primeiro observe que todo monômio em I é divisível por um dos monômios na lista acima. Para ver o porquê, seja $x^\alpha y^p \in I$. Se $p \geq m$, então $x^\alpha y^p$ é divisível por algum $x^{\alpha(i)} y^m$ pela construção de J. Por outro lado, se $p \leq m - 1$, então $x^\alpha y^p$ é divisível por algum $x^{\alpha_p(j)} y^p$ pela construção de J_p. Segue do Lema 1.3.11 que os monômios acima geram um ideal tendo os mesmos monômios que I. Pelo Corolário 1.3.15, isso força os ideais a serem os mesmos, e nossa afirmação é provada.
Para completar a prova do teorema, precisamos mostrar que o conjunto finito de geradores pode ser escolhido de um dado conjunto de geradores para o ideal. Se voltarmos a escrever as variáveis como $x_1, \ldots, x_n$, então nosso ideal monomial é $I = \langle x^\alpha : \alpha \in A\rangle \subset k[x_1, \ldots, x_n]$. Precisamos mostrar que I é gerado por um número finito de x^α, onde $\alpha \in A$. Pelo parágrafo anterior, sabemos que $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)}\rangle$ para alguns monômios $x^{\beta(i)}$ em I. Como $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A\rangle$, o Lema 1.3.11 nos diz que cada $x^{\beta(i)}$ é divisível por $x^{\alpha(i)}$ para algum $\alpha(i) \in A$. □

Exemplo 1.3.17. *Para entender melhor como a prova do Teorema 1.3.16 funciona, vamos aplicá-la ao ideal $I = \langle x^5y^2, x^4y^3, x^2y^6\rangle$ discutido anteriormente na seção. Pela*

imagem dos expoentes, você pode ver que a "projeção" é $J = \langle x^2 \rangle \subset k[x]$. *Como* $x^2y^6 \in I$, *temos* $m = 6$. *Então obtemos as "fatias"* J_t, $0 \leq t \leq 5 = m - 1$, *geradas por monômios contendo* y^t*:*

$$\begin{aligned} J_0 &= J_1 = \{0\}, \\ J_2 &= \left\langle x^5 \right\rangle, \\ J_3 &= J_4 = J_5 = \left\langle x^4 \right\rangle. \end{aligned}$$

Essas "fatias" são fáceis de ver usando a imagem dos expoentes. Então a prova do Teorema 1.3.16 dá $I = \langle x^2y^6, x^4y^3, x^4y^4, x^4y^5, x^5y^2 \rangle$.
O Teorema 1.3.16 resolve a descrição do ideal para ideais monomiais, demonstrando que tais ideais possuem uma base finita. Isso, por sua vez, nos permite solucionar o problema de pertinência ao ideal para ideais monomiais. Em outras palavras, se $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, *então podemos facilmente verificar se um dado polinômio* f *pertence a* I *ao verificar se o resto da divisão de* f *por* $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ *é igual a zero.*

1.4 Bases de Gröbner

Após a definição dos elementos essenciais, torna-se possível definir as bases de Gröbner de um ideal polinomial, que são conjuntos com propriedades favoráveis em relação ao algoritmo de divisão generalizada. No entanto, antes de prosseguir com essa discussão, é importante ressaltar que, dada uma ordem monomial, cada polinômio $f \in k[x_1, \ldots, x_n]$ possui um único termo principal $LT(f)$. Assim, é viável definir o ideal dos termos principais de qualquer ideal

Definição 1.4.1. *Seja* $I \subset k[x_1, \ldots, x_n]$ *um ideal distinto de* $\{0\}$.

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

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

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

Já vimos que os termos principais desempenham um papel importante no algoritmo de divisão. Isso traz um ponto sutil, mas importante, sobre $\langle LT(I) \rangle$. Ou seja, se for dado um conjunto gerador finito para I, digamos $I = \langle f_1, \ldots, f_s \rangle$, então $\langle LT(f_1), \ldots, LT(f_s) \rangle$ e $\langle LT(I) \rangle$ podem ser ideais diferentes. É verdade que $LT(f_i) \in LT(I) \subset \langle LT(I) \rangle$ por definição, implica que $\langle LT(f_1), \ldots, LT(f_s) \rangle \subset \langle LT(I) \rangle$. No entanto, $\langle LT(I) \rangle$ pode ser estritamente maior. Para ver isso, considere o seguinte exemplo.

Exemplo 1.4.2. *Seja* $I = \langle f_1, f_2 \rangle$, *onde* $f_1 = x^2y + x - y^3$ *e* $f_2 = -x^3 + xy^2$, *usando a ordem monomial lex em* $k[x, y]$. *Então*

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

Portanto, temos que $x^2 \in I$, *o que implica* $x^2 = LT(x^2) \in \langle LT(I) \rangle$. *No entanto, observe que* x^2 *não é divisível por* $LT(f_1) = x^2y$ *ou* $LT(f_2) = -x^3$, *e, consequentemente,* $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.

Mostraremos agora que $\langle LT(I)\rangle$ é um ideal monomial e tem uma base finita.

Teorema 1.4.3. *Seja $I \subset k[x_1, \ldots, x_n]$ um ideal.*

(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: (i) Os monômios líderes $LM(g)$ dos elementos $g \in I - \{0\}$ geram o ideal monomial $\langle LM(g) : g \in I - \{0\}\rangle$. Como $LM(g)$ e $LT(g)$ diferem por uma constante diferente de zero, esse ideal é igual a $\langle LT(g) : g \in I - \{0\}\rangle = \langle LT(I)\rangle$. Assim, $LT(I)$ é um ideal monomial.
(ii) Como $\langle LT(I)\rangle$ é gerado pelos monômios $LM(g)$ para $g \in I - \{0\}$, o Lema de Dickson 1.3.16 nos diz que $\langle LT(I)\rangle = \langle LM(g_1), \ldots, LM(g_t)\rangle$ para um número finito de $g_1, \ldots, g_t \in I$. Como $LM(g_i)$ difere de $LT(g_i)$ por uma constante diferente de zero, segue que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Isso completa a prova. □

Agora vamos estender o Lema 1.3.16 para um ideal arbitrário. O Teorema da Base de Hilbert, também conhecido como o Teorema da Base de Hilbert de Ideais, é um resultado importante na álgebra comutativa e na geometria algébrica. Prova a existência de um conjunto gerador finito de cada ideal polinomial em um anel de polinômios em várias variáveis.

Teorema 1.4.4. ***(Teorema da Base de Hilbert)*** *Todo ideal $I \subset k[x_1, \ldots, x_n]$ possui um conjunto gerador finito, ou seja, I pode ser escrito como $I = \langle g_1, \ldots, g_t\rangle$ para algum conjunto de polinômios $g_1, \ldots, g_t \in I$.*

Demonstração: Se $I = \{0\}$, consideramos nosso conjunto gerador como $\{0\}$, que certamente é finito. Se I contiver algum polinômio diferente de zero, então um conjunto gerador $g_1, \ldots, g_t$ para I pode ser construído como segue. Pela Proposição 1.4.3, 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 $I = \langle g_1, \ldots, g_t\rangle$. É claro que $\langle g_1, \ldots, g_t\rangle \subset I$ já que cada $g_i \in I$. Reciprocamente, seja $f \in I$ um polinômio qualquer. Se aplicarmos o algoritmo de divisão dado pelo Teorema 1.3.6 para dividir f por $(g_1, \ldots, g_t)$, obteremos uma expressão da forma

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

onde nenhum termo de r é divisível por qualquer um de $LT(g_1), \ldots, LT(g_t)$. Afirmamos que $r = 0$. Para ver isso, observe que

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

Se $r \neq 0$, então $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$ e pelo Lema 1.3.11, segue que $LT(r)$ deve ser divisível por algum $LT(g_i)$. Isso contradiz o que significa ser um resto e, consequentemente, r deve ser zero. Por isso,

$$f = a_1 g_1 + \cdots + a_t g_t + 0 \in \langle g_1, \ldots, g_t\rangle,$$

o que mostra que $I \subset \langle g_1, \ldots, g_t\rangle$. Isso completa a prova □

Considerando o Exemplo 1.4.2, é importante lembrar que nem todas as bases de um ideal apresentam o comportamento desejado. Portanto, bases que satisfazem a propriedade $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$ receberão um nome distinto.

Definição 1.4.5. ***(Base de Gröbner)*** *Defina uma ordem monomial. Um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal I é dito uma* ***base de Gröbner*** *se*

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

Observação 1.4.6. *Equivalentemente, mas mais informalmente. Uma base de Gröbner para I (em relação a $>$) é uma coleção finita de polinômios $G = \{g_1, \ldots, g_t\} \subset I$ com a propriedade que para todo $f \in I$ diferente de zero, $LT(f)$ é divisível por $LT(g_i)$ para algum i.*

O resultado a seguir é uma consequência direta do Teorema da Base de Hilbert 1.4.4, junto com a definição de Base de Gröbner.

Corolário 1.4.7. *Defina uma ordem monomial. Então todo ideal $I \subset K[x_1, \ldots, x_n]$ que não seja $\{0\}$ tem uma base de Gröbner. Além disso, qualquer base de Gröbner para um I ideal é uma base para I.*

1.5 Propriedades das bases de Gröbner

O Corolário 1.4.7 mostra que todo ideal não nulo $I \subset k[x_1, \ldots, x_n]$ possui uma base de Gröbner. Nesta seção, iremos estudar as propriedades das bases de Gröbner e aprender como identificar quando uma determinada base é uma base de Gröbner. Começaremos mostrando que o indesejável comportamento do algoritmo de divisão dado pelo Teorema 1.3.6 em $k[x_1, \ldots, x_n]$ não ocorre quando dividimos pelos elementos de uma base de Gröbner. Primeiro, vamos provar que o resto é determinado de forma única quando realizamos a divisão por uma base de Gröbner.

Proposição 1.5.1. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subset k[x_1, \ldots, x_n]$ e seja $f \in k[x_1, \ldots, x_n]$. Então existe um único $r \in k[x_1, \ldots, x_n]$ com as duas propriedades a seguir:*

(i) Nenhum termo de r é divisível por qualquer um de $LT(g_1), \ldots, LT(g_t)$.

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

Em particular, r é o resto da divisão de f por G, não importa como os elementos de G são listados ao usar o algoritmo de divisão.

Demonstração: O algoritmo de divisão dá $f = a_1g_1 + \cdots + a_tg_t + r$, onde r satisfaz (i) e (ii) fazendo $g = a_1g_1 + \cdots + a_tg_t \in I$. Isso prova a existência de r.
Para provar a unicidade, suponha que $f = g + r = g' + r'$ satisfaça (i) e (ii). Então $r - r' = g - g' \in I$, de modo que se $r \neq r'$, então $LT(r - r') \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Pelo Lema 1.3.11, segue que $LT(r - r')$ é divisível por algum $LT(g_i)$. Isso é impossível, pois nenhum termo de r, r' é divisível por um de $LT(g_1), \ldots, LT(g_t)$. Assim, $r - r'$ deve ser zero e a unicidade está provada. □

Observação 1.5.2. *O resto é às vezes chamado de forma normal de f com respeito a G. De fato, as bases de Gröbner podem ser caracterizadas pela unicidade do resto*

Corolário 1.5.3. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subset k[x_1, \ldots, x_n]$ e seja $f \in k[x_1, \ldots, x_n]$. Então $f \in I$ se, e somente se, o resto da divisão de f por G é zero.*

Definição 1.5.4. *Denotamos $\bar{f}^F$ para o* ***resto da divisão*** *de f pela s-upla ordenada $F = (f_1, \ldots, f_s)$. Se F é uma base de Gröbner para $(f_1, \ldots, f_s)$, então podemos considerar F como um conjunto (sem ordem particular) pela Proposição 1.5.1.*

Exemplo 1.5.5. *Se $F = \langle x^2y - y^2, xy^2 - y\rangle \subset k[x, y]$, usando a ordem lex, temos*

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

logo,

$$\overline{x^3y^2}^F = y^2.$$

Agora é discutido como determinar se um conjunto gerador de polinômios é uma base de Gröbner para um ideal.

Definição 1.5.6. *Seja $f, g \in k[x_1, \ldots, x_n]$ diferentes de zero. Fixe uma ordem monomial.*

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

(ii) O ***S-polinômio*** *de f e g, denotado $S(f, g)$, é o polinômio*

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

Observação 1.5.7. *Observe que por definição $S(f, g) \in \langle f, g\rangle$.*

Exemplo 1.5.8. *Com $f = x^3y + 5x^2y + x$ e $g = 2x^4 - 3xy$ em $\mathbb{Q}[x, y]$, e usando $>_{lex}$, temos $\gamma = (4, 1)$ logo $x^\gamma = x^4y$, e*

$$\begin{aligned} S(f, g) &= \frac{x^4y}{x^3y}f - \frac{x^4y}{2x^4}g \\ &= xf - \left(\frac{y}{2}\right)g \\ &= 5x^3y + x^2 + \frac{3}{2}xy^2. \end{aligned}$$

Observe que $LT(S(f, g))$ é divisível por $LT(f)$, ao dividir por $F = (f, g)$ com $\overline{S(f, g)}^F = -25x^2y + x^2 + 3/2xy^2 - 5x$ e $LT(\overline{S(f, g)}^F) = -25x^2y$ não é divisível nem por $LT(f)$ nem por $LT(g)$.

Note que um S-polinômio $S(f, g)$ é projetado para realizar o cancelamento de termos principais.

Lema 1.5.9. *Suponha que temos uma soma $\sum_{i=1}^s c_i f_i$, onde $c_i \in k$ e $multideg(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ para todo i. Se $multideg(\sum_{i=1}^s c_i f_i) < \delta$, então $\sum_{i=1}^s c_i f_i$ é uma combinação linear, com coeficientes em k, dos S-polinômios $S(f_j, f_k)$ para $1 \leq j, k \leq s$. Além disso, cada $S(f_i, f_k)$ tem multigrau $< \delta$.*

Demonstração: Seja $d_i = LC(f_i)$, de modo que $c_i d_i$ seja o coeficiente líder de $c_i f_i$. Como todos os $c_i f_i$ têm *multigrau* δ e sua soma tem *multigrau* estritamente menor, segue-se facilmente que $\sum_{i=1}^{s} c_i d_i = 0$.
Defina $p_i = f_i/d_i$ e observe que p_i tem coeficiente principal 1. Considere a soma telescópica

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

Por hipótese, $LT(f_i) = d_i x^\delta$, o que implica que o mínimo múltiplo comum de $LT(f_j)$ e $LM(f_k)$ é x^δ. Por isso

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

Usando esta equação e $\sum_{i=1}^{s} c_i d_i = 0$, a soma telescópica acima torna-se

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

que é uma soma da forma desejada. Como p_j e p_k têm *multigrau* δ e coeficiente líder 1, a diferença $p_j - p_k$ tem *multigrau* $< \delta$. Pela Equação (1), o mesmo vale para $S(f_j, f_k)$, e o lema é provado. □

Quando $f_1, \ldots, f_s$ satisfazem a hipótese do Lema 1.5.9, obtemos uma equação da forma

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_{jk} S(f_j, f_k).$$

Vamos considerar onde ocorre o cancelamento. Na soma da esquerda, todo somando $c_i f_i$ tem multigrau δ, então o cancelamento ocorre somente após somá-los. Porém, na soma da direita, cada soma $c_{jk} S(f_j, f_k)$ possui *multigrau* $< \delta$, de forma que o cancelamento já ocorreu. Intuitivamente, isso significa que todo cancelamento pode ser contabilizado por S-polinômios. Usando S-polinômios e o Lema 1.5.9, podemos agora provar o seguinte critério de Buchberger para quando uma base de um ideal é uma base de Gröbner.

Teorema 1.5.10. ***(Critério de Buchberger)*** *Seja I um ideal polinomial. Então uma base $G = \{g_1, \ldots, g_t\}$ para I é uma base de Gröbner para I se, e somente se, para todos os pares $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por G (listado em algum ordem) é zero.*

Demonstração: $\Rightarrow$: Se G é uma base de Gröbner, então como $S(g_i, g_j) \in I$, o resto da divisão por G é zero pelo Corolário 1.5.3.
$\Leftarrow$: Seja $f \in I$ um polinômio diferente de zero. Devemos mostrar que se todos os S-polinômios têm resto zero na divisão por G, então $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Antes de dar os detalhes, vamos esboçar a estratégia da prova.
Dado $f \in I = \langle g_1, \ldots, g_t \rangle$, existem polinômios $h_i \in k[x_1, \ldots, x_n]$ tais que

$$f = \sum_{i=1}^{t} h_i g_i, \tag{1.2}$$

Do Lema 1.2.15 segue-se que

$$multideg(f) \leq max(multideg(h_i g_i)). \tag{1.3}$$

Se a igualdade não ocorrer, então algum cancelamento deve ocorrer entre os termos principais de (1.2). O Lema 1.5.9 nos permitirá reescrever isso em termos de S-polinômios. Então, nossa suposição de que S-polinômios têm restos zero nos permitirá substituir os S-polinômios por expressões que envolvam menos cancelamento. Assim, obteremos uma expressão para f que tem menos cancelamento de termos principais. Continuando desta forma, eventualmente encontraremos uma expressão (1.2) para f onde a igualdade em (1.3) ocorre. Então $multideg(f) = multideg(h_i g_i)$ para algum i, e segue que $LT(f)$ é divisível por $LT(g_i)$. Isso mostrará que $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$, que é o que queremos provar.
Agora damos os detalhes da prova. Dada uma expressão (1.2) para f, seja $m(i) = multideg(h_i g_i)$, e defina $\delta = max(m(1), \ldots, m(t))$. Então a desigualdade (1.3) se torna

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

Agora considere todas as maneiras possíveis pelas quais f pode ser escrita na forma (1.2). Para cada uma dessas expressões, obtemos um δ possivelmente diferente. Como uma ordem monomial é uma boa ordenação, podemos selecionar uma expressão (1.2) para f tal que δ seja mínimo.
Mostraremos que uma vez escolhido este mínimo δ, temos $multideg(f) = \delta$. Então a igualdade ocorre em (1.3), e como observamos, segue que $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$. Isso provará o teorema.
Resta mostrar $multideg(f) = \delta$. Vamos argumentar isso por contradição. A igualdade pode falhar apenas quando $multideg(f) < \delta$. Para isolar os termos de *multigrau* δ, vamos escrever f na seguinte forma:

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} LT(h_i)\, g_i + \sum_{m(i)=\delta} (h_i - LT(h_i))\, g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{1.4}$$

Os monômios que aparecem na segunda e terceira somas em (1.4) têm todos *multigraus* $< \delta$. Assim, a suposição $multigrau(f) < \delta$ significa que a primeira soma também possui $multigrau < \delta$.
Seja $LT(h_i) = c_i x^{\alpha(i)}$. Então a primeira soma $\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ tem exatamente a forma descrita no Lema 1.5.9 com $f_i = x^{\alpha(i)} g_i$. Assim, o Lema 1.5.9 implica que esta soma é uma combinação linear dos S-polinômios $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$.
No entanto

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

onde $x^{\gamma_{jk}} = LCM(LM(g_j), LM(g_k))$. Assim, existem constantes $c_{jk} \in k$ tais que

$$\sum_{m(i)=\delta} LT(h_i)\, g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k). \tag{1.5}$$

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

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{1.6}$$

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

$$multideg(a_{ijk} g_i) \leq multideg(S(g_j, g_k)), \tag{1.7}$$

para todo i, j, k (ver Teorema 1.3.6). Intuitivamente, isso diz que quando o resto é zero, podemos encontrar uma expressão para $S(g_j, g_k)$ em termos de G onde os termos principais não se cancelam.
Para explorar isso, multiplique a expressão $S(g_j, g_k)$ por $x^{\delta-\gamma_{jk}}$ para obter

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

onde $b_{ijk} = x^{\delta-\gamma_{jk}} a_{ijk}$. Então (1.7) e o Lema 1.5.9 implicam que

$$multideg(b_{ijk} g_i) \leq multideg(x^{\delta-\gamma_{jk}} S(g_j, g_k)) < \delta. \tag{1.8}$$

Se substituirmos a expressão acima por $x^{\delta-\gamma_{jk}} S(g_j, g_k)$ em (1.5), obteremos

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

que por (1.8) tem a propriedade que para todo i,

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

Para a etapa final da prova, substituímos $\sum_{m(i)=\delta} LT(h_i)\, g_i = \sum_i \tilde{h}_i g_i$ na Equação (1.4) para obter uma expressão de f como uma combinação polinomial dos g_i,

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

onde todos os termos têm $multigrau < \delta$. Isso contradiz a minimalidade de δ. Logo $multideg(f) = \delta$, e segue que $multideg(f) = \delta = \delta_i(h) = multideg(h_i g_i)$ 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. □

O Critério de Buchberger, dado no Teorema 1.5.10, é um resultado significativo em

relação às bases de Gröbner. As bases de Gröbner possuem várias propriedades favoráveis, mas determinar se uma determinada base é uma base de Gröbner tem sido um desafio até agora. No entanto, com a introdução dos critérios do S-par, tornou-se mais fácil verificar se uma determinada base é uma base de Gröbner. Além disso, será demonstrado que o critério S-par leva naturalmente a um algoritmo para computar bases de Gröbner.

Exemplo 1.5.11. *Para ilustrar a utilização do Teorema 1.5.10, vamos considerar o ideal $I = \langle x^2y - y^2, y^4 - y^2\rangle$. Afirmamos que o conjunto $G = \{x^2y - y^2, y^4 - y^2\}$ forma uma base de Gröbner ao usar a ordem lexicográfica com $x > y > z$. Para provar essa afirmação, precisamos examinar os S-polinômios.*

$$S(x^2y - y^2, y^4 - y^2) = \frac{x^2y^4}{x^2y}(x^2y - y^2) - \frac{x^2y^4}{y^4}(y^4 - y^2) = x^2y^2 - y^5.$$

Usando o algoritmo de divisão, encontra-se

$$x^2y^2 - y^5 = y(x^2y - y^2) + (-y)(y^4 - y^2) + 0,$$

de modo que $\overline{S(x^2y - y^2, y^4 - y^2)} = 0$. Assim, pelo Teorema 1.5.10, G é uma base de Gröbner para I.

Exemplo 1.5.12. *Considere o anel $k[x, y]$ com ordem lex, e seja $I = \langle f_1, f_2\rangle = \langle -x^3 + xy^2, x^2y + x - y^3\rangle$. Lembre-se que $\{f_1, f_2\}$ não é uma base de Gröbner para I (Exemplo 1.4.2), já que $x^\gamma = -x^3y$ e*

$$S(f_1, f_2) = (-y)f_1 - xf_2 = -x^2.$$

$LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2)\rangle$.
Como $S(f_1, f_2) = -x^2 \in I$ e $\overline{S(f_1, f_2)}^F = -x^2 \neq 0$ com $F = (f_1, f_2)$, devemos incluir esse restante em nosso conjunto gerador, como um novo gerador $f_3 = -x^2$. Se definirmos $F = (f_1, f_2, f_3)$, podemos usar o Teste de Buchberger para testar se esse novo conjunto é uma base de Gröbner para I. Calculamos

$$\begin{aligned}
S(f_1, f_2) &= f_3,\\
\overline{S(f_1, f_2)}^F &= 0, \text{ com } F = (f_1, f_2, f_3),\\
S(f_1, f_3) &= (-1)(-x^3 + xy^2) - (-x)(-x^2) = -xy^2,\\
\overline{S(f_1, f_3)}^F &= -xy^2 \neq 0, \text{ com } F = (f_1, f_2, f_3).
\end{aligned}$$

Portanto, devemos adicionar $f_4 = -xy^2$ ao nosso conjunto gerador. Se fizermos $F = (f_1, f_2, f_3, f_4)$, então

$$\begin{aligned}
\overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = 0,\\
S(f_1, f_4) &= (-y^2)(-x^3 + xy^2) - (-x^2)(-xy^2) = -xy^4\\
&= y^2 f_4,\\
\overline{S(f_1, f_4)}^F &= 0,\\
S(f_2, f_3) &= (1)(x^2y + x - y^3) - (-y)(-x^2) = x - y^3,\\
\overline{S(f_2, f_3)}^F &= x - y^3 \neq 0.
\end{aligned}$$

Portanto, devemos adicionar $f_5 = x - y^3$ *ao nosso conjunto gerador. Se fizermos* $F = (f_1, f_2, f_3, f_4, f_5)$*, então*

$$\begin{aligned}
\overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = \overline{S(f_1, f_4)}^F = \overline{S(f_2, f_3)}^F = 0,\\
S(f_1, f_5) &= (-1)(-x^3 + xy^2) - (x^2)(x - y^3) = x^2y^3 - xy^2,\\
\overline{S(f_1, f_5)}^F &= y^5 \neq 0.
\end{aligned}$$

Portanto, também devemos adicionar $f_6 = y^5$ *ao nosso conjunto gerador. Definindo* $F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$*, pode-se calcular que*

$$\begin{aligned}
\overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = \overline{S(f_1, f_4)}^F = \overline{S(f_1, f_5)}^F = \overline{S(f_2, f_3)}^F = 0,\\
S(f_1, f_6) &= (-y^5)(-x^3 + xy^2) - (x^3)(y^5) = -xy^7,\\
\overline{S(f_1, f_6)}^F &= 0,\\
S(f_2, f_4) &= (y)(x^2y + x - y^3) - (-x)(-xy^2) = xy - y^4,\\
\overline{S(f_2, f_4)}^F &= 0,\\
S(f_2, f_5) &= (1)(x^2y + x - y^3) - (xy)(x - y^3) = xy^4 + x - y^3,\\
\overline{S(f_2, f_5)}^F &= 0,\\
S(f_2, f_6) &= (y^4)(x^2y + x - y^3) - (x^2)(y^5) = xy^4 - y^7,\\
\overline{S(f_2, f_6)}^F &= 0,\\
S(f_3, f_4) &= (-y^2)(-x^2) - (-x)(-xy^2) = 0,\\
\overline{S(f_3, f_4)}^F &= 0,\\
S(f_3, f_5) &= (-1)(-x^2) - (x)(x - y^3) = xy^3,\\
\overline{S(f_3, f_5)}^F &= 0,\\
S(f_3, f_6) &= (-y^5)(-x^2) - (x^2)(y^5) = 0,\\
\overline{S(f_3, f_6)}^F &= 0,\\
S(f_4, f_5) &= (-1)(-xy^2) - (y^2)(x - y^3) = y^5,\\
\overline{S(f_4, f_5)}^F &= 0,\\
S(f_4, f_6) &= (-y^3)(-xy^2) - (x)(y^5) = 0,\\
\overline{S(f_4, f_6)}^F &= 0,\\
S(f_5, f_6) &= (y^5)(x - y^3) - (x)(y^5) = -y^8,\\
\overline{S(f_5, f_6)}^F &= 0.
\end{aligned}$$

Pelo Teorema 1.5.10, segue que uma base de Gröbner para I *é dada por*

$$\{f_1, f_2, f_3, f_4, f_5, f_6\} = \{-x^3 + xy^2, x^2y + x - y^3, -x^2, -xy^2, x - y^3, y^5\}.$$

O exemplo acima sugere que, em geral, deve-se tentar estender uma base F a uma base de Gröbner adicionando sucessivamente restos diferentes de zero $\overline{S(f_i, f_j)}^F$ a F. Essa ideia é uma consequência natural do critério do S-par e leva ao seguinte algoritmo devido a Buchberger para calcular uma base de Gröbner.

Teorema 1.5.13. ***(Algoritmo de Buchberger).*** *Seja $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ um ideal polinomial. Então uma base de Gröbner para I pode ser construída em um número finito de passos pelo seguinte algoritmo:*

Especifi: *critério de Buchberger*
Dado: $F = (f_1, \ldots, f_s) \subset k[\bar{x}]$
Encon: *Uma base de Gröbner $G = \{g_1, \ldots, g_t\}$ para $I = \langle F \rangle$, com $F \subset G$*
começar
$G := F$
repetir
$G' := G$
para *cada par* $\{p, q\}, p \neq q$ *em* G' ***fazer***
$S := \overline{S(p,q)}^{G'}$
se $S \neq 0$ ***então*** $G := G \cup \{S\}$
ate $G = G'$

Demonstração: Começamos com algumas notações usadas com frequência. Se $G = \{g_1, \ldots, g_t\}$, então $\langle G \rangle$ e $\langle LT(G) \rangle$ denotam os seguintes ideais:

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

Primeiro mostramos que $G \subset I$ vale em cada estágio do algoritmo. Isso é verdade inicialmente, e cada vez que aumentamos G, fazemos isso adicionando o restante $S = \overline{S(p,q)}^{G'}$ para $p, q \in G$. Portanto, se $G \subset I$, então p, q e $S(p,q)$ estão em I, e como estamos dividindo por $G' \subset I$, obtemos $G \cup \{S\} \subset I$. Também notamos que G contém a base dada F de I, então G é na verdade uma base de I.

$$\overline{S(p,q)}^{G'} = pm + qn + S(p,q) \in I, \text{ com } m = \frac{x^\gamma}{LT(p)}, n = \frac{x^\gamma}{LT(q)}.$$

O algoritmo termina quando $G = G'$, o que significa que $S = \overline{S(p,q)}^{G'} = 0$ para todo $p, q \in G$. Portanto, G é uma base de Gröbner de $\langle G \rangle = I$ pelo Teorema de Buchberger. Resta mostrar que o algoritmo termina. Precisamos considerar o que acontece após cada etapa do loop principal. O conjunto G consiste em G' (o antigo G) junto com os restos diferentes de zero de S-polinômios de elementos de G'. Então

$$\langle LT(G') \rangle \subset \langle LT(G) \rangle. \tag{1.9}$$

Além disso, se $G' \neq G$, afirmamos que $LT(G')$ é estritamente menor que $LT(G)$. Para ver isso, suponha que um resíduo diferente de zero r de um polinômio S tenha sido associado a G. Como r é um resto da divisão por G', $LT(r)$ não é divisível pelos termos principais dos elementos de G' e portanto $LT(r) \notin LT(G')$. No entanto, $LT(r) \in LT(G)$, o que prova nossa afirmação.
Por (1.9), os ideais $\langle LT(G') \rangle$ de iterações sucessivas do loop formam uma cadeia ascendente de ideais em $K[x_1, \ldots, x_n]$. Portanto, a condição da Cadeia Ascendente implica que, após um número finito de iterações, a cadeia se estabilizará, de modo que

$\langle LT(G')\rangle = \langle LT(G)\rangle$ eventualmente ocorra. Pelo parágrafo anterior, isso implica que $G' = G$, então o algoritmo deve terminar após um número finito de passos. □

Essas contribuições de Buchberger são centrais para o desenvolvimento do assunto, fornecem uma base algorítmica para a teoria das bases de Gröbner, mas não é uma forma muito prática de fazer o cálculo. As bases de Gröbner calculadas usando o algoritmo do Teorema 1.5.13 geralmente são maiores do que o necessário. Podemos eliminar alguns geradores desnecessários usando o seguinte fato.

Lema 1.5.14. *Seja G uma base de Gröbner para o ideal polinomial I. Seja $p \in G$ um polinômio tal que $LT(p) \in \langle LT(G - \{p\})\rangle$. Então $G - \{p\}$ também é uma base de Gröbner para I.*

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

Ajustando as constantes para tornar todos os coeficientes principais 1 e removendo qualquer p com $LT(p) \in LT(G - p)$ de G, chegamos ao que chamaremos de base de Gröbner mínima.

Definição 1.5.15. ***(base mínima de Gröbner)*** *Uma* ***base de Gröbner mínima*** *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 $p \in G$, $LT(p) \notin \langle LT(G - \{p\})\rangle$.

Definição 1.5.16. ***(base de Gröbner reduzida)*** *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* $p \in \langle LT(G - \{p\})\rangle$.

1.6 Um novo algoritmo eficiente para computação Bases de Gröbner (F4)

Nesta seção do Capítulo 1, apresentamos o algoritmo padrão que utiliza o sistema computacional SageMath para calcular bases de Gröbner. O resultado é uma base de Gröbner na forma reduzida. Para isso focaremos no artigo [8] onde encontraremos este algoritmo com mais detalhes.

Sejam $f, g, p \in k[\overline{x}]$ com $p \neq 0$, T o conjunto definido na Observação 1.1.4 e seja F um subconjunto finito de $k[\overline{x}]$. Então, dizemos que:

(i) f reduz a g módulo p (notação $f \underset{p}{\longrightarrow} g$) se existem $t \in T(f)$ e $s \in T$ tais que $s \cdot LM(p) = t$ e $g = f - \frac{a}{LC(p)} \cdot s \cdot p$, onde a é o coeficiente de t em p.

(ii) f reduz a g módulo P (notação $f \underset{P}{\longrightarrow} g$) se $f \underset{p}{\longrightarrow} g$ para algum $p \in P$.

(iii) f é redutível módulo p se existe $g \in k[\overline{x}]$ tal que $f \underset{p}{\longrightarrow} g$.

(iv) f é redutível módulo P se existe $g \in k[\overline{x}]$ tal que $f \underset{P}{\longrightarrow} g$.

(v) f é top redutível módulo P se existe $g \in k[\overline{x}]$ tal que $f \underset{P}{\longrightarrow} g$ e $\mathrm{LM}(g) < \mathrm{LM}(f)$.

(vi) $f \underset{P}{\overset{*}{\longrightarrow}} g$ é o fecho reflexivo-transitivo de $\underset{P}{\longrightarrow}$.

Definição 1.6.1. *Por convenção se M é uma matriz $s \times m$, $M_{i,j}$ é o j-ésimo elemento da i-ésima linha de M. Se $T_M = [t_1, \ldots, t_m]$ um conjunto ordenado de termos, seja $(\varepsilon_i)_{i=1,\ldots,m}$ a base canônica de k^m, consideramos a aplicação linear $\varphi_{T_M} : V_{T_M} \longrightarrow k^m$ (onde V_{T_M} é o submódulo de $k[\bar{x}]$ gerado por T_M) tal que $\varphi_{T_M}(t_i) = \varepsilon_i$. A função inversa será denotada por ψ_{T_M}. A aplicação ψ_{T_M} permite interpretar vetores de k^n como polinômios. Notamos por (M, T_M) uma matriz com tal interpretação.*

Definição 1.6.2. *Se (M, T_M) for uma matriz $s \times m$ com tal interpretação, então podemos construir o conjunto de polinômios:*

$$Rows(M, T_M) := \{\psi_{T_M}(row(M, i)) \mid i = 1, \ldots, s\} \setminus \{0\},$$

onde $row(M, i)$ é a i-ésima linha de M (um elemento de k^m). Por outro lado, se l é uma lista de polinômios e T_l um conjunto ordenado de termos, podemos construir uma matriz $s \times m$ A (onde $s = size(l)$, $m = size(T_l)$):

$$A_{i,j} := coeff(l[i], T_l[j]), i = 1, \ldots, s, j = 1, \ldots, m.$$

Notamos $A^{(l,T_l)}$ a matriz $(A_{i,j})$.

$$M = \begin{array}{c} \\ f_{i_1} \\ f_{i_2} \\ \vdots \\ f_{i_{2k}} \\ f_{i_{2k+1}} \\ f_{i_s} \end{array} \begin{array}{c} \begin{array}{cccc} t_1 & t_2 & t_3 & \cdots \end{array} \\ \left(\begin{array}{cccc} \times & \times & \times & \cdots \\ \times & \times & \times & \cdots \\ \vdots & \vdots & \vdots & \ldots \\ \times & \times & \times & \cdots \\ \times & \times & \times & \cdots \\ \times & \times & \times & \cdots \end{array} \right) \end{array} \tag{1.10}$$

Definição 1.6.3. *Seja M uma matriz $s \times m$, e $Y = [Y_1, \ldots, Y_m]$ novas variáveis. Então $F = Rows(M, Y)$ é um conjunto de equações, portanto, podemos calcular $\tilde{F}$ uma base de Gröbner reduzida de F para uma ordenação lexicográfica tal que $Y_1 > \cdots > Y_m$. A partir desta base podemos reconstruir uma matriz $\tilde{M} = A^{(\tilde{F}, \overline{Y})}$. Chamamos $\tilde{M}$ a (única) forma escalonada de M. Dizemos também que $\tilde{F}$ é uma base escalonada de linhas de F.*

$$M = \begin{array}{c} \\ f_{j_1} \\ f_{j_2} \\ \vdots \\ f_{j_l} \\ f_{j_{l+1}} \\ \vdots \\ f_{j_m} \end{array} \begin{array}{c} \begin{array}{ccccccc} t_1 & t_2 & \cdots & t_k & t_{k+1} & \cdots & t_m \end{array} \\ \begin{pmatrix} 1 & 0 & \dots & 0 & \times & \dots & \times \\ 0 & 1 & \dots & 0 & \times & \dots & \times \\ & & \ddots & & \times & \dots & \times \\ 0 & 0 & \dots & 1 & \times & \dots & \times \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ & & \vdots & & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} \end{array}$$

onde $\times$ denota um elemento possivelmente diferente de zero. No caso de polinômios temos uma denição similar:

Definição 1.6.4. *Seja F um subconjunto finito de $k[\overline{x}]$ e $>$ uma ordenação admissível. Definimos $T_>(F)$ como $\boldsymbol{Sort}(\{T(f) \mid f \in F\}, >)$, $A := A^{(F;T_>(F))}$ e $\tilde{A}$ a forma escalonada de linhas de A. Vamos dizer que $\tilde{F} = Rows(\tilde{A}; T_>(F))$ é a forma escalonada de linhas de F em relação a $>$.*

As propriedades elementares de matrizes escalonadas de linhas são resumidas pelo seguinte teorema:

Teorema 1.6.5. *Seja M uma matriz $s \times m$; e $Y = [Y_1, \dots, Y_m]$ novas variáveis; $F = Rows(M, Y)$; $\tilde{M}$ a forma escalonada por linhas de M; $\tilde{F} = Rows(\tilde{M}, \overline{Y})$. Definimos*

$$\tilde{F}^+ = \{g \in \tilde{F} \mid LM(g) \notin LM(F)\};$$
$$\tilde{F}^- = \tilde{F}^+ \setminus \tilde{F}.$$

Para qualquer subconjunto F' de F tal que $size(F') = size(LM(F))$ e $LM(F') = LM(F)$; então $G = \tilde{F}^+ \cup F'$ é uma base triangular do k-módulo V_M gerado por F. Ou seja; para todo $f \in V_M$ existem $(\lambda_k)_k$ elementos de k e $(g_k)_k$ elementos de G tais que $f = \sum_k \lambda_k g_k$, $LM(g_1) = LM(f)$ e $LM(g_k) > LM(g_{k+1})$.

Demonstração: Como os termos principais de G são distintos dois a dois, G é linearmente independente. Afirmamos que também é um sistema gerador de V_M. Suponha por contradição que existe $f \in V_M$ tal que $f \xrightarrow[G]{*} f' \neq 0$. Pela definição de uma base Gröbner, $f' \xrightarrow[F]{*} 0$, conseqüentemente f' é top-redutível módulo G $LM(\tilde{F}) = LM(\tilde{F}^+) \cup LM(\tilde{F}^-) = LM(\tilde{F}^+) \cup LM(F') = LM(G)$, de modo que f' top-redutível módulo G. Isso é uma contradição. □

Podemos transpor imediatamente o teorema para polinômios:

Corolário 1.6.6. *Seja F um subconjunto finito de E e $<$ uma ordenação admissível; e $\tilde{F}$ a forma escalonada de linhas de F em relação a $>$ Nós definimos*

$$\tilde{F}^+ = \{g \in \tilde{F} \mid LM(g) \notin LM(F)\}.$$

Para todo subconjunto F' de F tal que $size(F') = size(LM(F))$ e $LM(F') = LM(F)$, então $G = \tilde{F}^+ \cup F'$ é uma base triangular de V_M o k-módulo gerado por F. Para todo $f \in V_M$ existem $(\lambda_k)_k$ elementos de k e $(g_k)_k$ elementos de G tal que $f = \sum_k \lambda_k g_k$, $LM(g_1) = LM(f)$ e $LM(g_k) > LM(g_{k+1})$.

Definição 1.6.7. *Um* ***par crítico*** *de dois polinômios* (f_i, f_j) *é um elemento de* $T^2 \times k[\bar{x}] \times T \times k[\bar{x}]$*;* $Pair(f_i, f_j) := (lcm_{ij}, t_i, f_i, t_j, f_j)$ *tal que*

$$lcm(Pair(f_i, f_j)) = lcm_{ij} = LM(t_i f_i) = LM(t_j f_j) = lcm(LM(f_i), LM(f_j)) :$$

Definição 1.6.8. *Dizemos que o grau do par crítico* $p_{i,j} = Par(f_i, f_j)$*,* $deg(p_{i,j})$*, é* $deg(lcm_{i,j})$*. Definimos as duas projeções* $\boldsymbol{Esquerda}(p_{i,j}) := (t_i, f_i)$ *e* $\boldsymbol{Direita}(p_{i,j}) := (t_j, f_j)$*. Se* $(t, p) \in T \times k[\bar{x}]$ *então notamos* $\boldsymbol{mult}((t, p))$ *o produto avaliado* $t \cdot p$*.*

Agora temos as ferramentas necessárias para apresentar a versão básica do nosso algoritmo. Todas as matrizes que ocorrem nos algoritmos a seguir são a representação de uma lista de polinômios através do conjunto de todos os seus termos, conforme explicado na Definição 1.6.2.

Especifi: Algoritmo F4

Dado: F um subconjunto finito de $k[\bar{x}]$
$\mathcal{S}el$ uma função $\mathcal{S}el : List(Pairs) \longrightarrow List(Pairs)$
tal que $\mathcal{S}el(l) \neq \emptyset$ se $l \neq \emptyset$

Encon: um subconjunto finito de $k[\bar{x}]$
$G := F, \tilde{F}_0^+ := F$ e $d := 0$
$P := \{Pair(f, g) \mid f, g \in G \text{ com } f \neq g\}$
enquanto $P \neq 0$ **fazer**
$d := d + 1$
$P_d := \mathcal{S}el(P)$
$P := P \setminus P_d$
$L_d := \text{Esquerda}(P_d) \cup \text{Direita}(P_d)$
$\tilde{F}_d^+ := \text{Redução}(L_d, G)$
para $h \in \tilde{F}_d^+$ **fazer**
$P := P \cup \{Pair(h, g) \mid g \in G\}$
$G := G \cup \{h\}$

retornar G

Precisamos estender a redução de um módulo polinomial de um subconjunto de $k[\bar{x}]$ para a redução de um subconjunto de $k[\bar{x}]$-módulo outro subconjunto de $k[\bar{x}]$:

Especifi: Redução
Dado: F um subconjunto finito de $T \times k[\bar{x}]$
G um subconjunto finito de $k[\bar{x}]$
Encon: um subconjunto finito de $k[\bar{x}]$
$F :=$ Pré-processamento Simbólico(L, G)
$\tilde{F} :=$ Redução à Forma Escalonada por Linhas de F em relação a $>$
$\tilde{F}^+ := \{f \in \tilde{F} \mid LM(f) \notin LM(F)\}$
retornar $\tilde{F}^+$

Observação 1.6.9. *Pelo Lema 1.6.12, veremos que uma definição equivalente (porém mais lenta) de $\tilde{F}^+$ poderia ser $\tilde{F}^+ := \{f \in \tilde{F} \mid f$ top-redutível módulo $G\}$.*

Temos agora que descrever a função principal do nosso algoritmo, ou seja, a construção da "matriz" F. Este subalgoritmo pode ser visto como uma redução usual de todos os polinômios considerados se substituirmos a aritmética padrão por: seja $0 \neq x$, $0 \neq y \in k$, então $x + y = 1$, $x \cdot y = 1$, $x \cdot 0 = 0$ e $x + 0 = 1$. Portanto, este é realmente um pré-processamento simbólico.

Especifi: Pré-processamento Simbólico
Dado: L um subconjunto finito de $T \times k[\bar{x}]$
G um subconjunto finito de $k[\bar{x}]$
Encon: um subconjunto finito de $k[\bar{x}]$
$F := \{t \cdot f \mid (t, f) \in L\}$
$Feito := LM(F)$
enquanto $T(F) \neq Feito$ **fazer**
m um elemento de $T(F) \setminus Feito$
$Feito := Feito \cup \{m\}$
se m top-redutível módulo G **então**
$m = m' \cdot LM(f)$ para alguns $f \in G$ e alguns $m' \in T$
$F := F \cup \{m' \cdot f\}$
retornar F

Observação 1.6.10. *Parece que os valores iniciais de $Feito$ deveriam ser $\emptyset$ mas em todas as aplicações desta função o resultado é de fato o mesmo com menos iterações.*

Observação 1.6.11. *O pré-processamento simbólico é muito eficiente visto que sua complexidade é linear no tamanho de sua saída se $size(G)$ for menor que o tamanho final de tf $T(F)$ que normalmente é o caso.*

Lema 1.6.12. *Seja G um subconjunto finito de $k[\bar{x}]$, L seja a imagem por mult de um subconjunto finito de $T \times G$ e $\tilde{F}^+ =$ Redução(L, G). Então para todo $h \in \tilde{F}^+$, $LM(h) \notin \langle LM(G) \rangle$.*

Demonstração: Seja F o conjunto calculado pelo algoritmo Pré-processamento Simbólico (L, G). Assuma para uma contradição que existe $h \in \tilde{F}^+$ tal que $t = LM(h) \in \langle LM(G)\rangle$. Portanto, $LM(g)$ divide t por algum $g \in G$. Então t está em $T(\tilde{F}^+) \subset T(\tilde{F}) \subset T(F)$ e é top-redutível módulo g, portanto $\frac{t}{LM(g)} \cdot g$ é inserido em F por Pré-processamento Simbólico (ou outro produto com o mesmo termo principal). Isso contradiz o fato de que $LM(h) \notin LM(F)$. □

O lema a seguir é útil para provar a correção do algoritmo.

Lema 1.6.13. *Seja G um subconjunto finito de $k[\bar{x}]$, L seja a imagem por mult de um subconjunto finito de $T \times G$ e $\tilde{F}^+ = Redução(L, G)$. Então $\tilde{F}^+$ é um subconjunto de $\langle G\rangle$. Além disso, para todo f no k-módulo gerado por L, $f \xrightarrow[G\cup\tilde{F}^+]{*} 0$.*

Demonstração: Aplique o Corolário 1.6.6 a F o conjunto gerado pelo Pré-processamento Simbólico(L, G). Claramente F é um subconjunto de $F \cup \langle G\rangle$, mas é óbvio que L é um subconjunto de $\langle G\rangle$, de modo que F é um subconjunto de $\langle G\rangle$. Portanto, qualquer F' satisfazendo a hipótese do Teorema 1.6.5 é um subconjunto de $\langle G\rangle$. Isso conclui a prova do lema já que o k-módulo gerado por L é um submódulo do k-módulo gerado por F. □

Observação 1.6.14. *Seja G um subconjunto finito de $k[\bar{x}]$. É possível que $f \xrightarrow[G]{*} 0$ mas aquela $NormalForm(f, G) \neq 0$ onde $NormalForm$ é a redução que é usada no algoritmo de Buchberger. A razão para isso é que o resultado de $NormalForm$ depende de muitas escolhas (estratégias).*

Teorema 1.6.15. *O algoritmo F4 calcula uma base de Gröbner G em $k[\bar{x}]$ tal que $F \subset G$ e $\langle G\rangle = \langle F\rangle$.*

Demonstração: Término: Assuma, por contradição, que o loop **enquanto** não termina. Vemos que existe uma sequência ascendente (d_i) de números naturais tal que $\tilde{F}^+_{d_i} \neq \emptyset$ para todo i. Digamos que $q_i \in \tilde{F}^+_{d_i}$ (daí q_i pode ser qualquer elemento em $\tilde{F}^+_{d_i}$). Seja U_i e $U_{i-1} + \langle LM(q_i)\rangle$ para $i > 1$ e $U_0 = (0)$. Pelo Lema 1.6.12 temos $U_{i-1} \subsetneq U_i$. Isso contradiz o fato de que $k[\bar{x}]$ é noetheriano.
Correção: Temos $G = \cup_{d\leq 0}\tilde{F}^+_{d_i}$. Afirmamos que os seguintes são loop invariantes do loop **enquanto** : G é um subconjunto finito de $k[\bar{x}]$ tal que $F \subset G \subset \langle F\rangle$ e $S(g_1, g_2) \xrightarrow[G]{*} 0$ para todo $g_1, g_2 \in G$ tal que $\{g_1, g_2\} \notin P$. A primeira afirmação é uma consequência imediata da primeira parte do Lema 1.6.13. Para o segundo, se $\{g_1, g_2\} \notin P$, isso significa que $Pair(g_1, g_2) = (lcm_{1,2}, t_1, g_1, t_2, g_2)$ foi selecionado em uma etapa anterior (digamos d) pela função $\mathcal{S}el$. Portanto, $t_1 \cdot g_1$ e $t_2 \cdot g_2$ estão em L_d, então $S(g_1, g_2)$ é um elemento do k-módulo gerado por L_d, portanto, pelo Lema 1.6.13, $S(g_1, g_2) \xrightarrow[G]{*} 0$. □

Observação 1.6.16. *Se $size(\mathcal{S}el(l)) = 1$ para todo $l \neq \emptyset$ então o algoritmo F4 é o algoritmo Buchberger. Nesse caso, a função $\mathcal{S}el$ corresponde à estratégia de seleção no algoritmo de Buchberger.*

Exemplo 1.6.17. *Alguém pode se perguntar por que na prova do término do algoritmo consideramos apenas um elemento de $\tilde{F}^+_d$ e não todo o $\tilde{F}^+_d$. Se $x > y > z$ para uma ordenação lexicográfica, $F = \{f_1 = xy^2 + 1, f_2 = xz^2 + 1, f_3 = y^3 + y^2\}$ e*

$\mathcal{S}el$ = identidade, encontramos $P_1 = \{Pair(f_1, f_2), Par(f_2, f_3), Pair(f_1, f_3)\}$ *e* $\tilde{F}_1^+ = \{y^2 - z^2, y + 1\}$ *de forma que* $\langle LM(\tilde{F}_1^+)\rangle = \{y\}$*. Portanto, ao contrário do Algoritmo de Buchberger, não é verdade que após cada operação* $G' := G \cup \{h\}$*, temos* $\langle LM(G)\rangle \subsetneqq \langle LM(G')\rangle$*.*

Capítulo 2

Geometria Algébrica

Neste capítulo, direcionaremos nossa atenção para algumas seções do Capítulo 1 das Notas de aula [6] e capítulos 4 e 5 das Notas de aula [9] onde encontramos os conceitos que serão abordados com maior profundidade. Esses conceitos desempenham um papel fundamental no desenvolvimento dos objetivos deste trabalho, tornando-se peças-chave na compreensão e aplicação das ideias que exploraremos.

2.1 Conjuntos algébricos afins

Definição 2.1.1. *O **espaço afim** sobre k de dimensão n, denotado como $\mathbb{A}_k^n$, é o conjunto definido por*

$$\mathbb{A}_k^n = \{(a_1, \ldots, a_n) \mid a_i \in k, \ \forall i \in \{1, \ldots, n\}\}.$$

Observação 2.1.2. *Observe que, como conjuntos, $\mathbb{A}_k^n$ e k^n são idênticos. No entanto, O conjunto k^n será dotado de uma estrutura a ser construída. Usaremos a notação $\mathbb{A}_k^n$ para nos referir a k^n. Se $n = 1, 2, 3$, o espaço afim $\mathbb{A}_k^n$ é chamado de **linha afim, plano afim, espaço afim** respectivamente.*

Definição 2.1.3. *Um **conjunto algébrico afim (ou variedade afim)** em k é um subconjunto de $\mathbb{A}_k^n$ na forma*

$$V(S) := \{(a_1, \ldots, a_n) \in \mathbb{A}_k^n \mid f(a_1, \ldots, a_n) = 0, \forall f \in S\}.$$

onde S é um subconjunto de $k[x_1, \ldots, x_n]$.

Observação 2.1.4. *Para simplificar, usaremos a notação $p = (a_1, \ldots, a_n) \in \mathbb{A}_k^n$. Dizemos que $X \subset \mathbb{A}_k^n$ é um conjunto algébrico (ou variedade algébrica) se $X = V(S)$ para algum $S \subset k[x_1, \ldots, x_n]$. Se $S = \{f_1, \ldots, f_r\}$ for um conjunto finito, escrevemos $V(S) = V(f_1, \ldots, f_r)$.*

A seguir, demonstraremos que todo conjunto algébrico afim pode ser definido através de um ideal de polinômios.

Proposição 2.1.5. *Se S é um subconjunto de $k[x_1, \ldots, x_n]$ e $\langle S \rangle$ é o ideal de $k[x_1, \ldots, x_n]$ gerado por S então $V(\langle S \rangle) = V(S)$.*

Demonstração: Vamos mostrar que $V(\langle S\rangle) \subseteq V(S)$. Com efeito, seja $p \in V(\langle S\rangle)$ qualquer. Então $f(p) = 0$, $\forall f \in \langle S\rangle$. Em particular, $f(p) = 0$, $\forall p \in S$ e assim $p \in V(S)$.
Reciprocamente, seja $p \in V(S)$, De acordo com o Teorema 1.4.4, qualquer ideal em $k[x_1, \ldots, x_n]$ é finitamente gerado. Em outras palavras, existem $f_1, f_2, \ldots, f_r \in S$ tais que $\langle S\rangle = \langle f_1, \ldots, f_r\rangle$. Portanto, dado qualquer $f \in \langle S\rangle$, podemos escrever $f = g_1 f_1 + \cdots + g_r f_r$ com $g_1, \ldots, g_r \in k[x_1, \ldots, x_n]$ e $f_1, \ldots, f_r \in S$. Como $p \in V(S)$ então $f_i(p) = 0$, $\forall i \in \{1, \ldots, r\}$ e assim

$$f(p) = g_1(p)f_1(p) + \cdots + g_r(p)f_r(p) = g_1(p)0 + \cdots + g_r(p)0 = 0.$$

Logo, $p \in V(\langle S\rangle)$. □

No próximo resultado, apresentaremos as propriedades fundamentais dos conjuntos algébricos afins e como essas propriedades se relacionam com a inclusão, interseção e união.

Proposição 2.1.6. *Sejam k um corpo e I, J ideais de $k[x_1, \ldots, x_n]$*

(i) $V(0) = \mathbb{A}_k^n$ *e* $V(1) = \emptyset$,

(ii) *Se* $I \subseteq J$ *então* $V(J) \subseteq V(I)$;

(iii) *Seja* $\{I_\alpha\}_{\alpha \in L}$ *uma coleção arbitrária de ideais de* $k[x_1, \ldots, x_n]$. *Então*

$$\bigcap_{\alpha \in L} V(I_\alpha) = V\left(\bigcup_{\alpha \in L} I_\alpha\right) = V\left(\sum_{\alpha \in L} I_\alpha\right).$$

Em particular, a interseção de uma família arbitrária de conjuntos algébricos afins também é um conjunto algébrico afim.

(iv) $V(I \cdot J) = V(I) \cup V(J)$. *Em particular, a união finita de conjuntos algébricos afins também é um conjunto algébrico afim.*

(v) *Sejam* $a_1, \ldots, a_n \in k$ *e considere o ideal* $\langle x_1 - a_1, \ldots, x_n - a_n\rangle \subset k[x_1, \ldots, x_n]$. *Então* $V(\langle x_1 - a_1, \ldots, x_n - a_n\rangle) = \{(a_1, \ldots, a_n)\}$. *Em particular, qualquer subconjunto finito de* $\mathbb{A}_k^n$ *é um conjunto algébrico afim.*

Demonstração:

(*i*) Claramente, o polinômio nulo anula todos os elementos de $\mathbb{A}_k^n$, enquanto o polinômio constante 1 não anula nenhum deles em $\mathbb{A}_k^n$.

(*ii*) Seja $p \in V(J)$. Isso implica que $f(p) = 0$ para todo $f \in J$. Dado que $I \subseteq J$, temos que $f(p) = 0$ para todo $f \in I$. Portanto, concluímos que $p \in V(I)$.

(*iii*) Vamos mostrar inicialmente que $\bigcap_{\alpha \in L} V(I_\alpha) \subseteq V\left(\bigcup_{\alpha \in L} I_\alpha\right)$.
Seja $p \in \bigcap_{\alpha \in L} V(I_\alpha)$. Para qualquer $f \in \bigcup_{\alpha \in L} I_\alpha$, existirá um $\beta \in L$ tal que $f \in I_\beta$. Como $p \in V(I_\beta)$, temos que $f(p) = 0$. Portanto, concluímos que $p \in V\left(\bigcup_{\alpha \in L} I_\alpha\right)$.

Reciprocamente, como $I_\alpha \subseteq \bigcup_{\lambda\in L} I_\lambda$, de acordo com o item (ii), temos que $V\left(\bigcup_{\lambda\in L} I_\lambda\right) \subseteq V(I_\alpha)$ para todo $\alpha \in L$. Portanto, temos $V\left(\bigcup_{\alpha\in L} I_\alpha\right) \subseteq \bigcap_{\alpha\in L} V(I_\alpha)$.

$$\bigcap_{\alpha\in L} V\left(I_\alpha\right) = V\left(\bigcup_{\alpha\in L} I_\alpha\right).$$

Além disso, pelo fato de o ideal gerado por $\bigcup_{\alpha\in L} I_\alpha$ ser $\sum_{\alpha\in L} I_\alpha$, de acordo com a Proposição 2.1.5, concluímos que:

$$V\left(\bigcup_{\alpha\in L} I_\alpha\right) = V\left(\sum_{\alpha\in L} I_\alpha\right).$$

(iv) Devido ao fato de $I \cdot J \subseteq I$ e $I \cdot J \subseteq J$, pelo item (ii), podemos concluir que $V(I) \subseteq V(I \cdot J)$ e $V(J) \subseteq V(I \cdot J)$. Portanto, temos que $V(I) \cup V(J) \subseteq V(I \cdot J)$. Reciprocamente, vamos mostrar que $V(I \cdot J) \subseteq V(I) \cup V(J)$. Seja $p \in V(I \cdot J)$ qualquer ponto. Se $p \in V(I)$, então não há nada a provar. Suponha agora que $p \notin V(I)$. Isso significa que existe $f \in I$ tal que $f(p) \neq 0$. Para qualquer $g \in J$ arbitrário, temos que $f \cdot g \in I \cdot J$ e, como $p \in V(I \cdot J)$, temos $(f \cdot g)(p) = 0$. Portanto, $f(p) \cdot g(p) = 0$ e, como $f(p) \neq 0$, concluímos que $g(p) = 0$. Assim, temos que $p \in V(J)$ e, portanto, $p \in V(I) \cup V(J)$.

(v) É evidente que $\{(a_1, \ldots, a_n)\} \subseteq V(\langle x_1 - a_1, \ldots, x_n - a_n\rangle)$. Por outro lado, seja $p \in V(\langle x_1 - a_1, \ldots, x_n - a_n\rangle))$ arbitrário. Escrevendo $p = (p_1, \ldots, p_n)$, segue imediatamente que $p_i - a_i = 0$ para todo $i \in \{1, \ldots, n\}$. Em outras palavras, temos que $p = (a_1, \ldots, a_n)$. □

Exemplo 2.1.7. *Os únicos conjuntos algébricos afins em $\mathbb{A}^1_k$ consistem nos subconjuntos finitos de $\mathbb{A}^1_k$ e o próprio $\mathbb{A}^1_k$. Suponha que X seja um conjunto afim em $\mathbb{A}^1_k$, ou seja, $X = V(I)$ para algum ideal $I \subset k[x]$. Como $k[x]$ é um domínio de ideais principais (PID), existe um polinômio $f \in I$ tal que $I = \langle f\rangle$. Distinguimos dois casos:*

a. Se $f = 0$, então $I = \{0\}$ e $X = V(0) = \mathbb{A}^1_k$.

b. Se $f \neq 0$, então f possui um número finito de raízes (possivelmente nenhuma se o corpo k não for algebricamente fechado). Assim, $X = V(f) = \{p \in \mathbb{A}^1_k \mid f(p) = 0\}$ é um conjunto finito em $\mathbb{A}^1_k$.

Portanto, os únicos conjuntos algébricos afins em $\mathbb{A}^1_k$ são os subconjuntos finitos de $\mathbb{A}^1_k$ e o próprio $\mathbb{A}^1_k$.

Por definição, um conjunto algébrico afim $X \subseteq \mathbb{A}^n_k$ é o conjunto de zeros de uma coleção S de polinômios em n indeterminadas. A princípio, não há garantia de que o conjunto $S \subseteq k[x_1, \ldots, x_n]$ que determina X deva ser finito. No entanto, mostraremos que é sempre possível descrever X a partir de um número finito de equações polinomiais.

Proposição 2.1.8. *Se $X \subseteq \mathbb{A}^n_k$ é um conjunto algébrico afim, então existem $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ tais que $X = V(f_1, \ldots, f_r)$. Portanto, X é o conjunto solução do sistema de equações polinomiais representado por $f_1, \ldots, f_r$.*

$$\begin{cases} f_1\left(x_1, \ldots, x_n\right) = & 0 \\ \qquad\vdots & \vdots \\ f_r\left(x_1, \ldots, x_n\right) = & 0. \end{cases}$$

Demonstração: Como X é um conjunto algébrico, de acordo com a Proposição 2.1.5, existe um ideal I em $k[x_1, \ldots, x_n]$ tal que $X = V(I)$. De acordo com o Teorema 1.4.4, qualquer ideal em $k[x_1, \ldots, x_n]$ é finitamente gerado. Portanto, existem $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ que geram o ideal I. □

Definição 2.1.9. *Uma* ***hipersuperfície afim*** *em $\mathbb{A}_k^n$ é um conjunto algébrico afim definida por um único polinômio $f \in k[x_1, \ldots, x_n]$.*

A Proposição 2.1.8 estabelece que todo conjunto algébrico afim pode ser expresso como a interseção finita de hipersuperfícies. Em outras palavras, qualquer conjunto algébrico afim em $\mathbb{A}_k^n$ pode ser descrito como a interseção de um número finito de hipersuperfícies. Vamos lembrar um conceito importante em Álgebra Comutativa.

Definição 2.1.10. *Seja A um anel e I um ideal em A. O* ***radical*** *de I é definido como*

$$\sqrt{I} := \{a \in A \mid \text{existe } n \in \mathbb{N}^* \text{ tal que } a^n \in I\}.$$

O radical de I é um ideal de A que contém I. Um ideal I é dito radical se $I = \sqrt{I}$, incluindo a possibilidade de $I = A$. Para todo ideal I, o ideal $\sqrt{I}$ é um ideal radical.

Anteriormente, introduzimos o conceito de conjunto algébrico afim em $\mathbb{A}_k^n$ com base em um subconjunto de polinômios em n indeterminadas. Na próxima definição, seguiremos um caminho inverso.

Definição 2.1.11. *Seja $X \subseteq \mathbb{A}_k^n$. Definimos*

$$I(X) := \{f \in k[x_1, \ldots, x_n] \mid f(p) = 0, \forall p \in X\}.$$

Da mesma forma que a construção $V(\ )$, a construção $I(\ )$ possui algumas propriedades clássicas, que serão apresentadas no próximo resultado.

Proposição 2.1.12. *Seja k um corpo. $X, Y \subseteq \mathbb{A}_k^n$ e $S \subseteq k[x_1, \ldots, x_n]$*

(i) $I(X)$ *é um ideal radical de* $k[x_1, \ldots, x_n]$.

(ii) Se $X \subseteq Y$, *então* $I(Y) \subseteq I(X)$.

(iii) $I(\emptyset) = k[x_1, \ldots, x_n]$, *e se* k *é um corpo infinito, então* $I(\mathbb{A}_k^n) = \{0\}$.

(iv) $S \subseteq I(V(S))$ *e* $V(I(V(S))) = V(S)$.

(v) $X \subseteq V(I(X))$ *e* $I(V(I(X))) = I(X)$.

(vi) Se J *é um ideal de* $k[x_1, \ldots, x_n]$, *então* $V(J) = V(\sqrt{J})$ *e* $\sqrt{J} \subseteq I(V(J))$.

Demonstração:

(*i*) Claramente, $0 \in I(X)$. Agora, sejam $f, g \in I(X)$ e $h \in k[x_1, \ldots, x_n]$. Para todo $p \in X$, temos que

$$(hf + g)(p) = h(p)f(p) + g(p) = h(p) \cdot 0 + 0 = 0.$$

Logo, $hf + g \in I(X)$ e, portanto, $I(X)$ é um ideal de $k[x_1, \ldots, x_n]$.
Vamos mostrar que $I(X)$ é um ideal radical de $k[x_1, \ldots, x_n]$. Para isso, seja $f \in \sqrt{I(X)}$. Isso significa que existe um número natural r tal que $f^r \in I(X)$. Para todo $p \in X$, segue que $f^r(p) = 0 \Rightarrow (f(p))^r = 0 \Rightarrow f(p) = 0$. Logo, $f \in I(X)$ e, portanto, $I(X)$ é um ideal radical de $k[x_1, \ldots, x_n]$.

(*ii*) Seja $f \in I(Y)$. Isso implica que $f(p) = 0$ para todo $p \in Y$. Como $X \subseteq Y$, temos que $f(p) = 0$ para todo $p \in X$. Portanto, concluímos que $f \in I(X)$.

(*iii*) Por vacuidade, temos que $I(\emptyset) = k[x_1, \ldots, x_n]$. Vamos mostrar por indução em n que $I(\mathbb{A}_k^n) = \{0\}$.

Para o caso de $n = 1$, sabemos que o polinômio nulo é o único polinômio em uma única variável que possui um número infinito de raízes. Suponha, por indução, que para $n > 1$, temos $I(\mathbb{A}_k^{n-1}) = \{0\}$. É claro que $\{0\} \subseteq I(\mathbb{A}_k^n)$. Por outro lado, seja $f \in I(\mathbb{A}_k^n)$. Portanto, $f(p) = 0$ para todo $p \in \mathbb{A}_k^n$. Como $f \in k[x_1, \ldots, x_n]$, existem $f_0, \ldots, f_r \in k[x_1, \ldots, x_{n-1}]$ tais que

$$f = f_0 + f_1 x_n + \cdots + f_r x_n^r.$$

Para cada $q \in \mathbb{A}_k^{n-1}$, consideremos o polinômio $f_q \in k[x_n]$ definido por

$$f_q := f_0(q) + f_1(q)x_n + \cdots + f_r(q)x_n^r.$$

Para todo $q \in \mathbb{A}_k^{n-1}$ e $t \in k$, temos que $f_q(t) = f(q, t) = 0$. Portanto, $f_q \in k[x_n]$ possui infinitas raízes para todo $q \in \mathbb{A}_k^{n-1}$. Assim, temos que $f_q = 0$, então $f_j(q) = 0$ para todo $q \in \mathbb{A}_k^{n-1}$ e todo $j \in \{0, \ldots, r\}$. Isso implica que $f_j \in I(\mathbb{A}_k^{n-1})$ para todo $j \in \{0, \ldots, r\}$. Mas, por hipótese de indução, $I(\mathbb{A}_k^{n-1}) = \{0\}$. Portanto, temos que $f_j = 0$ para todo $j \in \{0, \ldots, r\}$. Assim, concluímos que $f = 0$.

(*iv*) Observe que se $f \in S$, então $f(p) = 0$ para todo $p \in V(S)$. Portanto, $f \in I(V(S))$. Logo, $S \subseteq I(V(S))$. Pela Proposição 2.1.6 (*ii*), segue que $V(I(V(S))) \subseteq V(S)$. Por outro lado, para qualquer ponto $p \in V(S)$, claramente $f(p) = 0$ para todo $f \in I(V(S))$. Logo, $p \in V(I(V(S)))$ e, portanto, $V(I(V(S))) = V(S)$.

(*v*) Observe que se $p \in X$, então $f(p) = 0$ para todo $f \in I(X)$. Portanto, $p \in V(I(X))$. Logo, $X \subseteq V(I(X))$. Pelo item (*ii*), segue que $I(V(I(X))) \subseteq I(X)$. Por outro lado, para todo $f \in I(X)$, temos que $f(p) = 0$ para todo $p \in V(I(X))$, o que implica que $f \in I(V(I(X)))$. Portanto, $I(V(I(X))) = I(X)$.

(*vi*) Como $J \subseteq \sqrt{J}$, temos que $V(\sqrt{J}) \subseteq V(J)$. Reciprocamente, seja $p \in V(J)$. Para todo $f \in \sqrt{J}$, existe um número natural r tal que $f^r \in J$. Assim, $f^r(p) = 0 \Rightarrow (f(p))^r = 0 \Rightarrow f(p) = 0$. Logo, $p \in V(\sqrt{J})$. Portanto, $V(\sqrt{J}) = V(J)$.
Finalmente, seja $f \in \sqrt{J}$ qualquer. Então, existe um número natural r tal que $f^r \in J$. Para todo $p \in V(J)$, temos que $f^r(p) = 0 \Rightarrow f(p) = 0$. Logo, $f \in I(V(J))$, e portanto $J \subseteq I(V(J))$. □

Exemplo 2.1.13. *Seja $S = \langle x^2 + 1 \rangle \subset \mathbb{R}[x]$. Trata-se de um ideal maximal e, portanto, um ideal radical. Neste caso, $I(V(S)) = I(\emptyset) = \mathbb{R}[x]$. Portanto, $\sqrt{S} = S \subsetneq \mathbb{R}[x] = I(V(S))$. Isso mostra que no item (vi) a igualdade não é verdadeira em geral. Analogamente, $I(V(S)) = \mathbb{R}[x] \neq S$. Portanto, o item (iv) não implica que se S for um ideal radical, então $I(V(S)) = S$.*

Assim, as noções de conjunto algébrico V e ideal I podem ser vistas como pontes, ou seja, funções que conectam dois mundos distintos: o mundo algébrico dos polinômios

e o mundo geométrico das soluções desses polinômios.

$$\begin{array}{ccc} V : \{ \text{ ideais de } k[x_1, \ldots, x_n]\} & \longrightarrow & \{ \text{ conjuntos algébricos em } \mathbb{A}_k^n\} \\ J & \longmapsto & V(J) \\ I : \{ \text{ conjuntos algébricos em } \mathbb{A}_k^n\} & \longrightarrow & \{ \text{ ideais de } k[x_1, \ldots, x_n]\} \\ X & \longmapsto & I(X) \end{array}$$

A partir deste ponto, buscamos compreender as relações existentes entre essas funções.

2.2 Topologia de Zariski

Com as hipóteses e noções que acabamos de introduzir na seção anterior, utilizando os conjuntos $V(I)$ como fechados, onde I é um ideal em $k[x_1, \ldots, x_n]$, agora demonstraremos que isso é suficiente para definir uma topologia. Assim, por razões de simplicidade, dotamos $\mathbb{A}_k^n$ com a topologia definida dessa maneira.

Definição 2.2.1. *A **Topologia de Zariski** em $\mathbb{A}_k^n$ é definida de tal maneira que seus fechados são todos os conjuntos da forma $V(I)$, onde I é um ideal em $k[x_1, \ldots, x_n]$. Naturalmente, os abertos de $\mathbb{A}_k^n$ são da forma $\mathbb{A}_k^n - V(I)$.*

Proposição 2.2.2. *A Topologia de Zariski é uma topologia em $\mathbb{A}_k^n$.*

Demonstração: A Proposição 2.1.6 (i) estabelece que o conjunto vazio $\emptyset$ e o conjunto $\mathbb{A}_k^n$ são fechados em $\mathbb{A}_k^n$. Além disso, a Proposição 2.1.6 (iii) assegura que a interseção arbitrária de conjuntos fechados em $\mathbb{A}_k^n$ ainda é um conjunto fechado. Por fim, de acordo com a Proposição 2.1.6 (iv), a união finita de conjuntos fechados em $\mathbb{A}_k^n$ também é um conjunto fechado de $\mathbb{A}_k^n$. Portanto V define uma topologia em $\mathbb{A}_k^n$. □

Observação 2.2.3. *A seguir, vamos considerar uma classe especial de conjuntos abertos em $\mathbb{A}_k^n$. Para cada $f \in k[x_1, \ldots, x_n]$, vamos definir o **conjunto aberto de Zariski** como sendo:*

$$D_f := \mathbb{A}_k^n - V(f).$$

Esse conjunto aberto é o complementar de uma hipersuperfície em $\mathbb{A}_k^n$ e é chamado de aberto básico de $\mathbb{A}_k^n$. O próximo resultado mostra que qualquer conjunto aberto em $\mathbb{A}_k^n$ pode ser obtido a partir dos abertos básicos.

Proposição 2.2.4. *A coleção $B := \{D_f \mid f \in k[x_1, \ldots, x_n]\}$ é uma base de abertos da Topologia de Zariski em $\mathbb{A}_k^n$.*

Demonstração: Seja U um aberto em $\mathbb{A}_k^n$. Então, existe um ideal I em $k[x_1, \ldots, x_n]$ tal que

$$U = \mathbb{A}_k^n - V(I) = \mathbb{A}_k^n - \bigcup_{f \in I} V(f) = \bigcap_{f \in I} (\mathbb{A}_k^n - V(f)) = \bigcap_{f \in I} D_f. \quad \square$$

O resultado a seguir estabelece uma relação entre o fecho de um subconjunto de $\mathbb{A}_k^n$ e o conjunto algébrico definido pelo ideal induzido por esse subconjunto.

Proposição 2.2.5. *Se $X \subseteq \mathbb{A}_k^n$, então $V(I(X)) = \overline{X}$. Em particular, se X é um conjunto algébrico afim em $\mathbb{A}_k^n$, então $V(I(X)) = X$.*

Demonstração: Pela Proposição 2.1.12, temos $X \subseteq V(I(X))$, o que implica

$$\overline{X} \subseteq \overline{V(I(X))} \subseteq V(I(X)).$$

Suponha, por absurdo, que $V(I(X)) \nsubseteq \overline{X}$. Isso significa que existe um ponto $p \in V(I(X))$ tal que $p \notin \overline{X}$. Portanto, existe um aberto básico D_f em $\mathbb{A}_k^n$ contendo p tal que $X \cap D_f = \emptyset$ para algum $f \in k[x_1, \ldots, x_n]$. Logo, $f(p) \neq 0$.
Por outro lado, como $X \cap D_f = \emptyset$, temos que $f(x) = 0$ para todo $x \in X$, ou seja, $f \in I(X)$. No entanto, $p \in V(I(X))$ implica que $f(p) = 0$, o que é uma contradição. Portanto, concluímos que $V(I(X)) = X$. $\square$

2.3 Espaços topológicos irredutíveis

No contexto dos conjuntos algébricos afins, temos uma noção especial do que seria a versão adequada de conexidade no estudo de topologia: a irredutibilidade. Veremos que essa propriedade está intimamente ligada ao conceito de ideais primos. Um espaço topológico é considerado irredutível se ele não pode ser expresso como uma união própria de dois conjuntos fechados, ou seja, ele não pode ser decomposto em duas partes não vazias e disjuntas que sejam fechadas em relação à topologia.

Definição 2.3.1. ***(Espaço topológico irredutível)*** *Um espaço topológico não vazio X é **redutível** se existem conjuntos fechados próprios X_1 e X_2 de X, tais que, $X = X_1 \cup X_2$. Caso contrário, dizemos que X é **irredutível**.*

Exemplo 2.3.2. *Se k é um corpo infinito, então $\mathbb{A}_k^1$ é irredutível. De fato, se $\mathbb{A}_k^1(k)$ fosse redutível, então existiriam conjuntos fechados próprios X_1 e X_2 de $\mathbb{A}_k^1$ tais que $\mathbb{A}_k^1 = X_1 \cup X_2$. No entanto, pelo Exemplo 2.1.7, podemos concluir que X_1 e X_2 seriam finitos. Isso implicaria que o corpo k é finito, o que é uma contradição. Portanto, chegamos à conclusão de que $\mathbb{A}_k^1$ é irredutível quando k é infinito.*

Teorema 2.3.3. *Seja X um espaço topológico. As seguintes afirmações são equivalentes:*

(i) *X é irredutível,*

(ii) *Para quaisquer abertos não-vazios U_1 e U_2 de X, tem-se que $U_1 \cap U_2 \neq \emptyset$,*

(iii) *Todo aberto não-vazio de X é denso em X.*

Demonstração:

$(i) \Rightarrow (ii)$ Suponha, por absurdo, que existem abertos não vazios U_1, U_2, tais que $U_1 \cap U_2 = \emptyset$. Nesse caso, podemos escrever X como a união de dois conjuntos fechados próprios: $X = (X - U_1) \cup (X - U_2)$. Como $X - U_1$ e $X - U_2$ são fechados em X, e X é irredutível, temos que $X = X - U_1$ ou $X = X - U_2$, o que implica que $U_1 = \emptyset$ ou $U_2 = \emptyset$, isto contradição, pois ambos U_1 e U_2 são não vazios. Portanto, $U_1 \cap U_2$ não é vazio.

$(ii) \Rightarrow (iii)$ Essa implicação é imediata.

$(iii) \Rightarrow (i)$ Suponha que X pode ser expresso como a união de dois conjuntos fechados F e G, ou seja, $X = F \cup G$. Suponha, por absurdo, que $F \subsetneq X$ e $G \subsetneq X$. Isso significa que $X - F$ e $X - G$ são abertos não vazios em X, e consequentemente, são densos em X. Em particular, $(X - F) \cap (X - G) \neq \emptyset$. Portanto, existe $x \in (X - F) \cap (X - G)$, o que implica que $x \in X$, $x \notin F$ e $x \notin G$. Mas isso leva à conclusão de que $X \nsubseteq F \cup G$, o que é um absurdo. Logo, $X = F$ ou $X = G$. Portanto, X é irredutível. □

Corolário 2.3.4. *Seja X um espaço topológico irredutível. Se U é um aberto não vazio em X, então U é irredutível em X*

Demonstração: Suponha por absurdo que U seja redutível. Então existem U_1 e U_2 fechados em U tais que $U = U_1 \cup U_2$, com $U_i \subsetneq U$, $\forall i \in \{1, 2\}$. Existem X_1 e X_2 fechados em X tais que $U_i = X_i \cap U$, $\forall i \in \{1, 2\}$.
Se $X_i = X$, para algum $i \in \{1, 2\}$ então $U_i = X_i \cap U = X \cap U = U$, contradição. Logo $X_i \subsetneq X$, $\forall i \in \{1, 2\}$. Daí $X - X_1$, $X - X_2$ e U são abertos não-vazios de X e pelo item anterior $(X - X_1) \cap (X - X_2) \cap U \neq \emptyset$. Tome $p \in (X - X_1) \cap (X - X_2) \cap U$. Daí $p \in U$ e $p \notin X_1 \cup X_2$. Por outro lado, como $U = U_1 \cup U_2 = (X_1 \cap U) \cup (X_2 \cap U) = U \cap (X_1 \cup X_2)$ então $U \subseteq X_1 \cup X_2$. Visto que $p \in U$ então $p \in X_1 \cup X_2$, contradição. Portanto, U é irredutível. □
Se $X \subseteq \mathbb{A}_k^n$, consideramos X com a topologia induzida pela Topologia de Zariski de $\mathbb{A}_k^n$, a chamamos de **Topologia de Zariski em** X. No próximo resultado, relacionamos o conceito de irredutibilidade é de primalidade de um ideal.

Proposição 2.3.5. *Seja $X \subseteq \mathbb{A}_k^n$ um conjunto algébrico afim. Então: X é irredutível se, e somente se, $I(X)$ é um ideal primo de $k[x_1, \ldots, x_n]$.*

Demonstração: ($\Rightarrow$) Suponha por absurdo que $I(X)$ não é um ideal primo. Então existem $f, g \in k[x_1, \ldots, x_n]$ tais que $fg \in I(X)$ com $f \notin I(X)$ e $g \notin I(X)$. Sejam $A := X \cap V(f)$ e $B := X \cap V(g)$ que são fechados em X.
Se $A = X$ então $X \subseteq V(f)$. Daí $I(V(f)) \subseteq I(X)$ e como $\langle f \rangle \subseteq I(V(f))$ então $f \in I(X)$, contradição. Logo, $A \subsetneq X$. Analogamente, $B \subsetneq X$.
Já sabemos que $A \cup B \subseteq X$. Reciprocamente, dado $p \in X$ arbitrario, como $fg \in I(X)$ então $(fg)(p) = 0$, ou seja, $f(p)g(p) = 0$. Como k é um corpo então $f(p) = 0$ ou $g(p) = 0$. Logo, $p \in A$ ou $p \in B$. Portanto, $X = A \cup B$. Como A e B são fechados próprios de X então X é redutível, absurdo. Logo, $I(X)$ é um ideal primo de $k[x_1, \ldots, x_n]$.
($\Leftarrow$) Suponha por absurdo que X seja redutível. Então existem A, B fechados em X tais que $X = A \cup B$ com $A \subsetneq X$ e $B \subsetneq X$. Assim $I(X) \subsetneq I(A)$ e $I(X) \subsetneq I(B)$. Daí podemos tomar $f \in I(A)$, $g \in I(B)$ tais que $f, g \notin I(X)$.
Afirmamos que $fg \in I(X)$. De fato, dado $p \in X$ qualquer, segue que $p \in A$ ou $p \in B$. Se $p \in A$, como $f \in I(A)$ então $f(p) = 0$, logo $(fg)(p) = 0$. Analogamente, se $p \in B$ conclui-se que $fg(p) = 0$. Assim, $fg \in I(X)$ com $f, g \notin I(X)$, o que contraria o fato de $I(X)$ ser um ideal primo de $k[x_1, \ldots, x_n]$. □

Corolário 2.3.6. *Seja k um corpo. Então, k é infinito se, e somente se, $\mathbb{A}_k^n$ é irredutível.*

Demonstração: ($\Rightarrow$) Como k é um corpo infinito, temos $I(\mathbb{A}_k^n) = \{0\}$, que é um ideal primo de $k[x_1, \ldots, x_n]$, visto que este anel de polinômios é um domínio. Pela Proposição 2.3.5, concluímos que $\mathbb{A}_k^n$ é irredutível.
($\Leftarrow$) Suponha que k seja finito. Claramente, $\mathbb{A}_k^n$ também é finito e pode ser representado como a união finita de seus pontos. Como todo ponto é um conjunto fechado em $\mathbb{A}_k^n$, concluímos que $\mathbb{A}_k^n$ é redutível, o que é uma contradição. Portanto, k é infinito. □

2.4 Teorema dos Zeros de Hilbert

Até este ponto, não impusemos nenhuma restrição ao corpo k. A partir desta seção, concentraremos nossa atenção principalmente em corpos que sejam algebricamente fechados. Nesse contexto, há uma conexão significativa entre a Topologia de Zariski em $\mathbb{A}_k^n$ e a estrutura do anel $k[x_1, \ldots, x_n]$, uma relação que se deve ao Teorema dos Zeros de Hilbert em sua versão forte.

Teorema 2.4.1. *Se k é um corpo qualquer, o ideal $I \subset k[x_1, \ldots, x_n]$ dado por*

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

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

Demonstração: Suponhamos que J seja um ideal estritamente contendo I. Nesse caso, deve existir um polinômio $f \in J$ tal que $f \notin I$. Pelo Algoritmo da Divisão, sabemos que podemos escrever $f = q_1(x-a_1)+\ldots+q_n(x-a_n)+r$, onde $q_1, \ldots, q_n \in k[x_1, \ldots, x_n]$ e $r \in k$. Dado que $q_1(x - a_1) + \ldots + q_n(x - a_n) \in I$ e $f \notin I$, concluímos que $r \neq 0$. Agora, uma vez que $f \in J$ e $q_1(x - a_1) + \ldots + q_n(x - a_n) \in I \subset J$, temos também que

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

Como $r \neq 0$, podemos considerar $\frac{1}{r} \cdot r = 1$ e, assim, temos $1 \in J$. Consequentemente, $J = k[x_1, \ldots, x_n]$. Isso conclui a demonstração. □

O teorema a seguir é conhecido como a versão fraca do Teorema dos Zeros de Hilbert, e estabelece que o conjunto algébrico afim determinado por um ideal próprio do anel de polinômios não é vazio.

Teorema 2.4.2. *Seja k um corpo algebricamente fechado e I um ideal próprio de $k[x_1, \ldots, x_n]$. Então, $V(I) \neq \emptyset$.*

O próximo resultado conclui a descrição de todos os ideais maximais de $k[x_1, \ldots, x_n]$, quando k é um corpo algebricamente fechado.

Corolário 2.4.3. *Para um corpo k algebricamente fechado e um ideal maximal J em $k[x_1, \ldots, x_n]$, existe uma n-upla $(a_1, \ldots, a_n) \in V(J)$ tal que*

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

Demonstração: De acordo com o Teorema 2.4.2, temos que $V(J) \neq \emptyset$. Escolhamos $(a_1, \ldots, a_n) \in V(J)$. Portanto, temos a inclusão

$$J \subseteq I(V(J)) \subseteq I(\{(a_1, \ldots, a_n)\}) \subseteq \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$

Como tanto J quanto $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ são ideais maximais de $k[x_1, \ldots, x_n]$, concluímos que $J = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

Exemplo 2.4.4. *Observa-se que o ideal* $\langle x^2+1\rangle$ *é um ideal maximal de* $\mathbb{R}[x]$*, uma vez que* $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$*, é um corpo. Portanto, o anel* $\mathbb{R}[x]$ *possui ideais maximais distintos dos da forma* $\langle x-a\rangle$*, onde* $a \in \mathbb{R}$*.*

Já vimos que se X é um conjunto algébrico afim, então $V(I(X)) = X$. Isso estabelece uma relação entre as funções I e V, definidas na seção 2.1. Naturalmente surge a pergunta: o que acontece se compusermos as funções I e V de outra forma? Mais precisamente, o que é $I(V(J))$, se J é um ideal de $k[x_1,\ldots,x_n]$? O próximo teorema responde a esta pergunta.

Teorema 2.4.5. ***(Teorema dos Zeros de Hilbert):*** *Seja* k *um corpo algebricamente fechado e* J *um ideal de* $k[x_1,\ldots,x_n]$*. Então,*

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

A demonstração deste teorema pode ser encontrada no livro [2]. Dado que as implicações deste teorema desempenham um papel fundamental no estudo da Geometria Algébrica,

Corolário 2.4.6. *Considere* k *um corpo algebricamente fechado. Então, as funções abaixo estabelecem bijeções, onde uma é inversa da outra:*

$$\begin{aligned} V : \{\textit{ideais radicais de } k[x_1,\ldots,x_n]\} &\longrightarrow \{\textit{conjuntos algébricos em } \mathbb{A}^n_k\} \\ J &\longmapsto V(J) \\ I : \{\textit{conjuntos algébricos em } \mathbb{A}^n_k\} &\longrightarrow \{\textit{ideais radicais de } k[x_1,\ldots,x_n]\} \\ X &\longmapsto I(X) \end{aligned}$$

Corolário 2.4.7. *Considere* k *um corpo algebricamente fechado. Então, as funções abaixo estabelecem bijeções, onde uma é inversa da outra:*

$$\begin{aligned} V : \{\textit{ideais primos de } k[x_1,\ldots,x_n]\} &\longrightarrow \{\textit{conj. algébricos irredutíveis em } \mathbb{A}^n_k\} \\ J &\longmapsto V(J) \\ I : \{\textit{conj. algébricos em irredutíveis } \mathbb{A}^n_k\} &\longrightarrow \{\textit{ideais primos de } k[x_1,\ldots,x_n]\} \\ X &\longmapsto I(X) \end{aligned}$$

Corolário 2.4.8. *Considere* k *um corpo algebricamente fechado. Então, as funções abaixo estabelecem bijeções, onde uma é inversa da outra:*

$$\begin{aligned} V : \{\textit{ideais maximais de } k[x_1,\ldots,x_n]\} &\longrightarrow \{\textit{pontos de } \mathbb{A}^n_k\} \\ J &\longmapsto V(J) \\ I : \{\textit{pontos de } \mathbb{A}^n_k\} &\longrightarrow \{\textit{ideais maximais de } k[x_1,\ldots,x_n]\} \\ (a_1,\ldots,a_n) &\longmapsto I(\{(a_1,\ldots,a_n)\}) \end{aligned}$$

Resumo das Conexões do Teorema dos Zeros de Hilbert: As implicações proporcionadas pelo Teorema dos Zeros de Hilbert em relação a um corpo algebricamente fechado k podem ser sintetizadas da seguinte maneira:

$$\begin{array}{ccc} \{\text{ideais radicais de } k[x_1,\ldots,x_n]\} & \longleftrightarrow & \{\text{conjuntos algébricos em } \mathbb{A}^n_k\} \\ \bigcup & & \\ \{\text{ideais primos de } k[x_1,\ldots,x_n]\} & \longleftrightarrow & \{\text{conjuntos algébricos irredutíveis em } \mathbb{A}^n_k\} \\ \bigcup & & \\ \{\text{ideais maximais de } k[x_1,\ldots,x_n]\} & \longleftrightarrow & \{\text{pontos em } \mathbb{A}^n_k\} \end{array}$$

2.5 O espaço projetivo

De forma simplificada, o espaço projetivo se baseia na observação do espaço afim e na identificação de pontos que estão na mesma reta que passa pela origem. Para formalizar esta noção, Definimos o n-espaço projetivo sobre o corpo k, denotado como $\mathbb{P}^n_k$ ou simplesmente $\mathbb{P}^n$, como o conjunto de classes de equivalência de $(n+1)$-uplas $(a_0, a_1, \ldots, a_n)$ de elementos pertencentes para k, não todos nulos, com base na relação de equivalência que será definida no conjunto $\mathbb{A}^{n+1}_k - \{0\}$. Definimos a seguinte relação de equivalência. Para $u, v \in \mathbb{A}^{n+1}_k - \{0\}$,

$$u \sim v \text{ se, e somente se, existe } \lambda \in k - \{0\} \text{ tal que } u = \lambda v.$$

Definição 2.5.1. ***(Espaço Projetivo)*** *O espaço projetivo n-dimensional é definido como o conjunto quociente*

$$\mathbb{P}^n_k := \frac{\mathbb{A}^{n+1}_k - \{0\}}{\sim}$$

Para qualquer $(a_0, \ldots, a_n) \in \mathbb{A}^{n+1}_k - \{0\}$, sua classe de equivalência será representada por $[a_0, \ldots, a_n]$.

Exemplo 2.5.2 (Reta Projetiva)**.** *A reta projetiva $\mathbb{P}^1_k$ pode ser decomposta como a união de dois conjuntos abertos, U_0 e U_1, onde*

$$U_0 = \{[1, a] \mid a \in k\} \quad e \quad U_1 = \{[a, 1] \mid a \in k\}.$$

Além disso, definimos o ponto $\infty := [0, 1] \in \mathbb{P}^1_k$, que é referido como o "ponto no infinito". Observamos que $\mathbb{P}^1_k - U_0 = \{\infty\}$, e assim podemos escrever

$$\mathbb{P}^1_k = U_0 \cup \{\infty\} \quad \text{'}=\text{'} \quad \mathbb{A}^1_k \cup \{\infty\},$$

onde a igualdade em aspas representa uma equivalência a ser formalmente estabelecida.

Estabelecendo a Noção de Conjuntos Algébricos no Espaço Projetivo: Desejamos desenvolver uma compreensão de conjuntos algébricos no espaço projetivo. No entanto, ao contrário do caso afim, a situação no caso projetivo é mais sutil no que se refere aos tipos de ideais nos anéis de polinômios que devem ser considerados. Por esse motivo, vamos revisar o conceito de homogeneidade em $k[x_1, \ldots, x_n]$. Devido à relação de equivalência introduzida na Definição 2.5.1, devemos levar em conta polinômios que exibem um "bom comportamento" em relação à multiplicação por um escalar $\lambda \in k - \{0\}$.

Definição 2.5.3. *Para um polinômio não nulo $f \in k[x_1, \ldots, x_n]$, definimos $f_{(d)}$ como a soma dos monômios de grau d de f. A essa soma, damos o nome de "parte homogênea de grau d de f". Um polinômio não nulo é dito* ***homogêneo*** *se existe $d \in \mathbb{N}$ tal que $f = f_{(d)}$, ou seja, todos os monômios têm o mesmo grau.*

Observação 2.5.4. *É evidente que, se d for maior que o grau de f, então $f_{(d)} = 0$.*

Exemplo 2.5.5. *Veja os seguintes polinômios:*

a. *Consideremos o polinômio* $f(x,y,z) = x^3 - xz^2 + xy + y^2 - z - 2$. *Temos,* $f_{(3)} = x^3 - xz^2$, $f_{(2)} = xy + y^2$, $f_{(1)} = -z$ *e* $f_{(0)} = -2$. *Podemos observar que o polinômio* f *não é homogêneo.*

b. *Considere o polinômio* $f(x,y,z) = x^2 - 3xy - y^2$. *Notamos que* $f = f_{(2)}$, *indicando que* f *é um polinômio homogêneo de grau* 2.

Teorema 2.5.6. *Um polinômio não nulo* $f \in k[x_1, \ldots, x_n]$ *é homogêneo de grau* d *se, e somente se,* $f(\lambda a) = \lambda^d f(a)$ *para todos* $a \in \mathbb{A}_k^n$ *e* $\lambda \in k$.

Demonstração: ($\Rightarrow$) É óbvio, pois todos os monômios de f têm grau d.
($\Leftarrow$) Seja $f = f_{(0)} + f_{(1)} + \cdots + f_{(d)}$. Podemos observar que $\lambda^d f(a) = f(\lambda a) = f_{(0)} + \lambda f_{(1)}(a) + \cdots + \lambda^d f_{(d)}(a)$. Fixando $a \in \mathbb{A}_k^n$, definimos $q(\lambda) := f_{(0)} + \lambda f_{(1)}(a) + \cdots + \lambda^d f_{(d)}(a) - \lambda^d f(a)$. Este é um polinômio em λ que é identicamente nulo. Portanto, todos os seus coeficientes são nulos, ou seja, $f_{(0)} = 0$, $f_{(1)}(a) = 0$, $\ldots$, $f_{(d-1)}(a) = 0$, $f_{(d)}(a) - f(a) = 0$. Como isso é verdade para qualquer a, concluímos que $f_{(0)} = \cdots = f_{(d-1)} = 0$ e $f = f_{(d)}$. □

Após a definição dos polinômios homogêneos, procederemos à análise dos ideais gerados por polinômios desse tipo.

Definição 2.5.7. *Um ideal* $I \subset k[x_1, \ldots, x_n]$ *é chamado de homogêneo se satisfizer a seguinte condição: para todo* $f \in I$ *não nulo e* $d \in \mathbb{N}$, *temos que* $f_{(d)} \in I$.

Exemplo 2.5.8. *Considere*

a. *O ideal* $\langle x, x^2 + yz \rangle$ *é um exemplo de ideal homogêneo em* $k[x,y,z]$.

b. *O ideal* $\langle x + 1 \rangle$ *não é um exemplo de ideal homogêneo em* $k[x]$.

c. *O ideal* $\langle x + y^2, y^2 \rangle$ *é um exemplo de ideal homogêneo em* $k[x,y]$.

Teorema 2.5.9. *Seja* $I \subset k[x_1, \ldots, x_n]$. *As seguintes condições são equivalentes:*

(i) I *é um ideal homogêneo;*

(ii) Existe uma família finita de geradores de I *composta por polinômios homogêneos;*

(iii) Existe uma família de geradores de I *composta por polinômios homogêneos.*

Demonstração:

$(i) \Rightarrow (ii)$ Considere $I = \langle f_1, \ldots, f_k \rangle$. Por hipótese, temos $(f_i)_{(d)} \in I$ para todos $i \in \{1, \ldots, k\}$ e $d \in \mathbb{N}$. Logo, I é gerado pela família finita $\{(f_i)_{(d)}\}$.

$(ii) \Rightarrow (iii)$ Esta implicação é óbvia.

$(iii) \Rightarrow (i)$ Seja $I = \langle \{f_i\}_{i \in J} \rangle$, onde f_i é homogêneo de grau d_i. Para $f \in I$, podemos escrever $f = q_1 f_{i_1} + \ldots + q_k f_{i_k}$, com $i_1, \ldots, i_k \in J$ e $q_1, \ldots, q_k \in k[x_1, \ldots, x_n]$. Para todo $d \in \mathbb{N}$, temos $f_{(d)} = (q_1)_{(d-d_1)} f_{i_1} + \ldots + (q_k)_{(d-d_k)} f_{i_k} \in I$. □

Corolário 2.5.10. *Um ideal principal* $I = \langle f \rangle$ *em* $k[x_1, \ldots, x_n]$ *é homogêneo se, e somente se, o polinômio* f *é homogêneo ou nulo.*

Demonstração: $\Rightarrow$ Segue imediatamente da Proposição 2.5.9 (ii).
$\Leftarrow$ Suponhamos, por absurdo, que $f_{(d_1)}$ e $f_{(d_2)}$ sejam duas componentes homogêneas distintas de f, onde $d_1 > d_2$. Se $q \in \langle f \rangle$ e $q \neq 0$, então f divide q, implicando que $\deg(q) \geq \deg(f) \geq d_1$. Isso mostra que $f_{(d_2)} \notin \langle f \rangle$, o que implica que $\langle f \rangle$ não é homogêneo, uma contradição. □

Teorema 2.5.11. *Temos as seguintes observações:*

(i) *Se $I \subset k[x_1, \ldots, x_n]$ for um ideal homogêneo, então $\sqrt{I}$ também é homogêneo.*

(ii) *Um ideal homogêneo $I \subset k[x_1, \ldots, x_n]$ é radical se, e somente se, a seguinte condição é válida: para todo $f \in k[x_1, \ldots, x_n]$ homogêneo, se existir $m \in \mathbb{N}^*$ tal que $f^m \in I$, então $f \in I$.*

Demonstração:

(i) Seja $f = f_{(0)} + \ldots + f_{(d)} \in \sqrt{I}$ não nulo. Escolhemos $m \in \mathbb{N}^*$ tal que $f^m \in I$. Portanto, $(f_{(0)} + \ldots + f_{(d)})^m \in I$. A parte homogênea de grau md de f^m é $f_{(d)}^m$. Como I é homogêneo, temos $f_{(d)}^m \in I$, o que implica que $f_{(d)} \in \sqrt{I}$. Isso, por sua vez, significa que $f - f_{(d)} = f_{(0)} + \ldots + f_{(d-1)} \in I$. Repetindo esse argumento até $f_{(0)}$, concluímos que $f_{(h)} \in \sqrt{I}$ para todo $h \in \mathbb{N}$.

(ii) $(\Rightarrow)$ Isso é óbvio, pois é um caso particular da definição de ideal radical.

$(\Leftarrow)$ Suponhamos que $f = f_{(0)} + \ldots + f_{(d)} \in k[x_1, \ldots, x_n]$ e $m \in \mathbb{N}^*$ tal que $f^m \in I$, ou seja, $(f_{(0)} + \ldots + f_{(d)})^m \in I$. A componente de grau md de f^m é $f_{(d)}^m$, que, sendo I homogêneo, implica que $f_{(d)}^m \in I$. Usando a hipótese, temos $f_{(d)} \in I$. Isso, por sua vez, implica que $f - f_{(d)} = f_{(0)} + \ldots + f_{(d-1)} \in I$. Continuando dessa maneira, mostramos que $f_{(0)}, \ldots, f_{(d)} \in I$, o que finalmente implica que $f \in I$. □

Exemplo 2.5.12. *Em geral, a Proposição 2.5.11 (i) não é válida a volta. Por exemplo, considere $I = \langle x^2 + y, y^2 \rangle \subset k[x, y]$. O ideal I não é um ideal homogêneo, pois não contém y, que é a parte homogênea de grau 1 em $x^2 + y$. No entanto, $\sqrt{I} = \langle x, y \rangle$, que é um ideal homogêneo.*

Teorema 2.5.13. *Seja $f \in k[x_0, \ldots, x_n]$ um polinômio homogêneo. Se $(a_0, \ldots, a_n)$, $(b_0, \ldots, b_n) \in \mathbb{A}_k^{n+1} - \{0\}$ são pontos tais que $[a_0, \ldots, a_n] = [b_0, \ldots, b_n]$ e $f(a_0, \ldots, a_n) = 0$, então $f(b_0, \ldots, b_n) = 0$.*

Demonstração: Seja d o grau de f. Como $[a_0, \ldots, a_n] = [b_0, \ldots, b_n]$, então existe $\lambda \in k - \{0\}$ tal que $(b_0, \ldots, b_n) = \lambda(a_0, \ldots, a_n)$. Visto que f é homogêneo de grau d, pelo Teorema 2.5.6, segue que:

$$f(b_0, \ldots, b_n) = f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n) = \lambda^d \cdot 0 = 0.$$

□

2.6 Conjuntos algébricos projetivos

Antes de podermos definir conjuntos algébricos projetivos, é fundamental compreender o conceito de um ponto no espaço projetivo ser uma solução para uma equação polinomial.

Definição 2.6.1. *Considere $f \in k[x_0, \ldots, x_n]$ e $p \in \mathbb{P}^n_k$. Dizemos $f(p) = 0$ quando, para cada $(a_0, \ldots, a_n) \in \mathbb{A}^{n+1}_k - \{0\}$ tal que $p = [a_0, \ldots, a_n]$, temos $f(a_0, \ldots, a_n) = 0$.*

O Teorema 2.5.13 demonstra que, no caso em que f é homogêneo, é suficiente que exista um representante de classe $(a_0, \ldots, a_n)$ de p tal que $f(a_0, \ldots, a_n) = 0$ para concluir que $f(p) = 0$.

Definição 2.6.2. *Considere $S \subseteq k[x_0, \ldots, x_n]$ um conjunto de polinômios homogêneos. Introduzimos a notação $V^*(S)$ definida por*

$$V^*(S) := \{p \in \mathbb{P}^n_k \mid f(p) = 0, \text{ para todo } f \in S\}.$$

O próximo lema será uma ferramenta crucial na definição dos conjuntos algébricos projetivos.

Lema 2.6.3. *Considere $S, S_0 \subseteq k[x_0, \ldots, x_n]$ subconjuntos formados por polinômios homogêneos. Se $\langle S \rangle = \langle S_0 \rangle$, então temos $V^*(S) = V^*(S_0)$.*

Demonstração: Para qualquer $p \in V^*(S)$, afirmamos que $p \in V^*(S_0)$. Consideremos um $f \in S_0$ arbitrário. Como $f \in (S_0) = (S)$, podemos expressá-lo como

$$f = h_1 g_1 + \ldots + h_t g_t,$$

onde $h_1, \ldots, h_t \in k[x_0, \ldots, x_n]$ e $g_1, \ldots, g_t \in S$. Dado que $p \in V^*(S)$, temos $g_i(p) = 0$ para $i \in \{1, \ldots, t\}$. Seja $(a_0, \ldots, a_n) \in \mathbb{A}^{n+1}_k - \{0\}$ tal que $p = [a_0, \ldots, a_n]$. Assim, $g_i(a_0, \ldots, a_n) = 0$ para $i \in \{1, \ldots, t\}$. Portanto,

$$\begin{aligned} f(a_0, \ldots, a_n) &= h_1(a_0, \ldots, a_n) g_1(a_0, \ldots, a_n) + \ldots + h_t(a_0, \ldots, a_n) g_t(a_0, \ldots, a_n) \\ &= h_1(a_0, \ldots, a_n) \cdot 0 + \ldots + h_t(a_0, \ldots, a_n) \cdot 0 = 0. \end{aligned}$$

Isso implica que $f(p) = 0$ para todo $f \in S_0$, ou seja, $p \in V^*(S_0)$. Portanto, $V^*(S) \subseteq V^*(S_0)$. Analogamente, $V^*(S_0) \subseteq V^*(S)$. □

Observação 2.6.4. *Como no Teorema 2.5.9, Para um ideal homogêneo I em $k[x_0, \ldots, x_n]$, existe um conjunto S formado por polinômios homogêneos em $k[x_0, \ldots, x_n]$ tal que $I = \langle S \rangle$. Nós definimos $V^*(I)$ como $V^*(S)$.*

O Lema 2.6.3 assegura que a definição acima é independente da escolha do conjunto gerador do ideal homogêneo I.

Definição 2.6.5. *Um subconjunto $X \subseteq \mathbb{P}^n_k$ é denominado **conjunto algébrico projetivo** se existir um ideal homogêneo I em $k[x_0, \ldots, x_n]$ tal que $X = V^*(I)$.*

Assim como no caso afim, os subconjuntos do espaço projetivo também dão origem a ideais de polinômios, com as devidas adaptações.

Definição 2.6.6. *Considere o subconjunto $X \subseteq \mathbb{P}^n_k$. Definimos $\overline{I}(X)$ como sendo o ideal em $k[x_0, \ldots, x_n]$ gerado pelo conjunto*

$$\{f \in k[x_0, \ldots, x_n] \mid f \text{ é homogêneo e } f(p) = 0, \forall p \in X\}.$$

Dessa forma, $\overline{I}(X)$ é um ideal homogêneo.

O próximo resultado é uma propriedade antecipada que deve ser comprovada, uma vez que estamos abordando o caso projetivo de forma – até certo ponto – análoga ao que foi realizado no caso afim.

Teorema 2.6.7. *Considere I um ideal homogêneo em $k[x_0, \ldots, x_n]$ e $p \in \mathbb{P}_k^n$. Assim, temos que*

$$p \in V^*(I) \text{ se, e somente se, } f(p) = 0 \text{ para todo } f \in I.$$

Demonstração: Dado que I é um ideal homogêneo em $k[x_0, \ldots, x_n]$, existe um conjunto S composto por polinômios homogêneos em $k[x_0, \ldots, x_n]$ tal que $I = \langle S \rangle$. Assim, temos $V^*(I) = V^*(S)$.
($\Rightarrow$) Suponha $p \in V^*(I)$, implicando $p \in V^*(S)$.
Seja $f \in I$. Podemos escrever $f = h_1 g_1 + \ldots + h_t g_t$, onde $h_1, \ldots, h_t \in k[x_0, \ldots, x_n]$ e $g_1, \ldots, g_t \in S$. Se $(a_0, \ldots, a_n) \in \mathbb{A}_k^{n+1} - \{0\}$ tal que $p = [a_0, \ldots, a_n]$, uma vez que $g_1, \ldots, g_t \in S$, temos $g_1(p) = \ldots = g_t(p) = 0$, o que implica

$$g_1(a_0, \ldots, a_n) = \ldots = g_t(a_0, \ldots, a_n) = 0.$$

Portanto, $f(a_0, \ldots, a_n) = 0$, concluindo que $f(p) = 0$ para todo $f \in I$.
($\Leftarrow$) Em particular, como $S \subseteq I$, temos $f(p) = 0$ para todo $f \in S$. Portanto, $p \in V^*(S) = V^*(I)$. $\square$

As relações de inclusão observadas para $V^*(\ )$ e $I^*(\ )$ seguem uma estrutura similar àquelas que envolvem $V(\ )$ e $I(\ )$ no caso afim, e essas semelhanças podem ser exploradas com mais detalhe.
Com o objetivo estender o Teorema dos Zeros de Hilbert para o contexto projetivo, a próxima proposição desempenhará um papel crucial. Além disso, essa proposição estabelece uma conexão entre os conjuntos algébricos, tanto afim quanto projetivo, que emergem de um mesmo ideal.

Teorema 2.6.8. *Considere J como um ideal homogêneo em $k[x_0, \ldots, x_n]$, e $u \in \mathbb{A}_k^{n+1} - \{0\}$. Então:*
u pertence a $V(J)$ se, e somente se, $[u]$ pertence a $V^*(J)$.

Demonstração: Dado que J é um ideal homogêneo, podemos encontrar um conjunto S composto por polinômios homogêneos em $k[x_0, \ldots, x_n]$ tal que $J = \langle S \rangle$. Consequentemente, temos $V(J) = V(S)$ e $V^*(J) = V^*(S)$.
($\Rightarrow$) Suponha que $u \in V(J)$, o que implica que $u \in V(S)$. Afirmamos que $[u] \in V^*(S)$. De fato, para qualquer $f \in S$, visto que $u \in V(S)$, temos $f(u) = 0$. Dado que f é homogêneo, isso implica que $f([u]) = 0$, ou seja, $[u] \in V^*(S) = V^*(J)$.
($\Leftarrow$) Suponha que $[u] \in V^*(J)$, ou seja, $[u] \in V^*(S)$. Afirmamos que $u \in V(S)$. Para qualquer $f \in S$, temos $f([u]) = 0$ por definição, o que implica que $f(u) = 0$. Portanto, $u \in V(S) = V(J)$. $\square$

Agora possuímos as ferramentas necessárias para formular e demonstrar o Teorema dos Zeros de Hilbert projetivo.

Teorema 2.6.9. ***(Teorema dos Zeros de Hilbert projetivo)*** *Sejam k um corpo algebricamente fechado e J um ideal homogêneo em $k[x_0, \ldots, x_n]$.*

(*i*) $V^*(J) = \emptyset$ *se, e somente se,* $\langle x_0, \ldots, x_n \rangle \subseteq \sqrt{J}$.

(*ii*) *Se* $V^*(J) \neq \emptyset$, *então* $I^*(V^*(J)) = \sqrt{J}$.

Demonstração:

(*i*) ($\Rightarrow$) Inicialmente, afirmamos que $V(J) \subseteq \{0\}$. Suponha $u \in V(J)$ para algum $u \in \mathbb{A}_k^{n+1} - \{0\}$. Se $u \neq 0$, então pela Teorema 2.6.8, temos $[u] \in V^*(J) = \emptyset$, o que é um absurdo. Portanto, $u = 0$. Isso implica que $V(J) \subseteq \{0\}$, e, $I(\{0\}) \subseteq I(V(J)) \Rightarrow \langle x_0, \ldots, x_n \rangle \subseteq \sqrt{J}$.

($\Leftarrow$) Agora, suponha que $\langle x_0, \ldots, x_n \rangle \subseteq \sqrt{J}$. Isso implica que $V(J) = V(\sqrt{J}) \subseteq V(x_0, \ldots, x_n) = \{0\}$, e novamente pela Teorema 2.6.8, temos $V^*(J) = \emptyset$.

(*ii*) Consideremos $I^*(V^*(J)) = \langle L \rangle$, onde

$$L := \{g \in k[x_0, \ldots, x_n] \mid g \text{ é homogêneo e } g(p) = 0 \text{ para todo } p \in V^*(J)\}.$$

Como $V^*(J) \neq \emptyset$, temos $I^*(V^*(J)) \neq I^*(\emptyset) = k[x_0, \ldots, x_n]$, o que implica que $I^*(V^*(J))$ é um ideal próprio de $k[x_0, \ldots, x_n]$. Portanto, grau$(g) \geq 1$ para todo $g \in L$.

a. Vamos mostrar que $I^*(V^*(J)) \subseteq I(V(J))$.
Seja $f \in I^*(V^*(J))$. Podemos escrever

$$f = h_1 g_1 + \ldots + h_t g_t,$$

onde $h_1, \ldots, h_t \in k[x_0, \ldots, x_n]$ e $g_1, \ldots, g_t \in L$. Como $g_1, \ldots, g_t$ são polinômios homogêneos de grau ≥ 1, temos

$$g_1(0) = \ldots = g_t(0) = 0.$$

Portanto, para todo $u \in V(J)$, se $u = 0$, então

$$f(u) = h_1(0)g_1(0) + \ldots + h_t(0)g_t(0) = 0.$$

Se $u \neq 0$, então pelo Teorema 2.6.8, temos $[u] \in V^*(J)$ e como $g_1, \ldots, g_t \in L$, obtemos $g_1(u) = \ldots = g_t(u) = 0$, o que implica $f(u) = 0$. Portanto, $f \in I(V(J))$.

b. Agora mostraremos que $\sqrt{J} \subseteq I^*(V^*(J))$.
Seja $f \in \sqrt{J}$ arbitrário. Como J é um ideal homogêneo, pelo Teorema 2.5.11 (*i*), $\sqrt{J}$ também é um ideal homogêneo em $k[x_0, \ldots, x_n]$. Portanto, existe um conjunto de polinômios homogêneos S tal que $\sqrt{J} = \langle S \rangle$. Logo,

$$V(S) = V(\sqrt{J}) = V(J).$$

Como $f \in \sqrt{J} = \langle S \rangle$, podemos escrever

$$f = h_1 g_1 + \ldots + h_t g_t,$$

onde $h_1, \ldots, h_t \in k[x_0, \ldots, x_n]$ e $g_1, \ldots, g_t \in S$. Afirmamos que $g_i \in L$ para todo $i \in \{1, \ldots, t\}$. Para cada i, qualquer, $g_i \in S$ e assim g_i é homogêneo. Dado $p \in V^*(J)$, podemos escrever $p = [u]$ para algum $u \in \mathbb{A}_k^{n+1} - \{0\}$. Como $[u] \in V^*(J)$, pelo Teorema 2.6.8, temos $u \in V(J) = V(S)$. Visto que $g_i \in S$, temos $g_i(u) = 0$, o que implica $g_i(p) = 0$. Portanto, $g_i \in L$. Assim,

$$f = h_1 g_1 + \ldots + h_t g_t \in \langle L \rangle = I^*(V^*(J)).$$

Portanto, concluímos que $I^*(V^*(J)) = \sqrt{J}$.

□

2.7 Topologia de Zariski em $\mathbb{P}^n_k$

A topologia de Zariski em $\mathbb{P}^n_k$ é definida de maneira análoga ao caso afim.

Definição 2.7.1. *Dizemos que um subconjunto X de $\mathbb{P}^n_k$ é um **fechado** (na topologia de Zariski) se X é um conjunto algébrico projetivo. Portanto, um subconjunto U de $\mathbb{P}^n_k$ é considerado **aberto** se U é o complemento de um fechado em $\mathbb{P}^n_k$.*

No caso projetivo, a topologia de Zariski possui uma base de abertos semelhante àquela do caso afim.

Definição 2.7.2. *Para cada polinômio homogêneo $f \in k[x_0, \ldots, x_n]$, definimos*

$$D^*(f) := \{p \in \mathbb{P}^n_k \mid f(p) \neq 0\} = \mathbb{P}^n_k - V^*(f),$$

onde $V^*(f)$ é o conjunto de zeros de f no espaço projetivo $\mathbb{P}^n_k$. Portanto, $D^*(f)$ é um conjunto aberto em $\mathbb{P}^n_k$.

Teorema 2.7.3. *Seja S o conjunto de todos os polinômios homogêneos em $k[x_0, \ldots, x_n]$. Então, a coleção $\{D^*(f)\}_{f \in S}$ forma uma base para a topologia de Zariski em $\mathbb{P}^n_k$.*

Demonstração: Seja U um aberto em $\mathbb{P}^n_k$. Portanto, existe um conjunto $T \subseteq S$ tal que $U = \mathbb{P}^n_k - V^*(T)$. Assim, temos:

$$U = \mathbb{P}^n_k - V^*(T) = \mathbb{P}^n_k - \bigcup_{f \in T} V^*(f) = \bigcap_{f \in T} (\mathbb{P}^n_k - V^*(f)) = \bigcap_{f \in T} D^*(f).$$

□

A seguir, vamos demonstrar que o espaço projetivo é coberto por abertos homeomorfos a conjuntos afins. Para cada $i \in \{0, \ldots, n\}$, definimos

$$U_i := \{[a_0, \ldots, a_n] \mid a_i \neq 0\}.$$

Claramente, esses subconjuntos formam uma cobertura de $\mathbb{P}^n_k$, ou seja,

$$\mathbb{P}^n_k = \bigcup_{i=0}^{n} U_i.$$

Definição 2.7.4. *Considere $f = f_{(0)} + \ldots + f_{(d-1)} + f_{(d)} \in k[x_1, \ldots, x_n]$. O polinômio homogeneizado, ou **homogeneização de** f, é o polinômio*

$$\overline{f} := f_{(0)}x_0^d + \ldots + f_{(d-1)}x_0 + f_{(d)} \in k[x_0, \ldots, x_n].$$

que é um polinômio homogêneo de grau d.

Observação 2.7.5. *Na definição anterior, sem perda de generalidade, podemos escolher $f \in k[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. Portanto, a homogeneização de f em x_i é o polinômio $\overline{f} := f_{(0)}x_i^d + f_{(1)}x_i^{d-1} + \ldots + f_{(d-1)}x_i + f_{(d)} \in k[x_0, \ldots, x_n]$.*

É evidente que $p = \overline{p}$ se, e somente se, p é um polinômio homogêneo. Agora podemos estender essa definição de homogeneização aos ideais.

Definição 2.7.6. *Seja $I \subset k[x_1, \ldots, x_n]$. O **ideal homogeneizado**, ou, a homogeneização de I, é o ideal $I \subset k[x_1, \ldots, x_{n+1}]$ gerado pelas homogeneizações dos elementos de I.*

Teorema 2.7.7. *Se $p \in k[x_1, \ldots, x_n]$ e $I = \langle p \rangle$, então $\overline{I} = \langle \overline{p} \rangle$.*

Demonstração: Como $p \in I$, segue imediatamente da definição de $\overline{I}$ que $(\overline{p}) \subseteq \overline{I}$. Reciprocamente, seja $q \in \overline{I}$. Isso significa que existem $r_1, \ldots, r_k, s_1, \ldots, s_k \in K[n]$ tais que $q = s_1\overline{r_1 p} + \ldots + s_k\overline{r_k p} = (s_1\overline{r_1} + \ldots + s_k\overline{r_k})\overline{p}$. Portanto, $\overline{I} \subseteq (\overline{p})$. □

O Teorema 2.7.7 não pode ser generalizada para qualquer ideal. De fato, dada uma família de geradores de um ideal não principal, em geral, as homogeneizações dos geradores não geram o ideal homogeneizado completo.

Exemplo 2.7.8. *Considere o ideal $I := \langle x, y \rangle \subset k[x, y]$. Este é um ideal homogêneo, uma vez que as partes homogêneas de um polinômio com termo constante nulo também têm termo constante nulo. Portanto, $\overline{I} = I$. No entanto, o mesmo ideal pode ser descrito na forma $I = \langle x - y^2, y \rangle$, pois $x = (x - y^2) + y \cdot y$ pertence a $\langle x - y^2, y \rangle$. No entanto, $\langle xu - y^2, y \rangle \subsetneq \overline{I}$, pois $x \notin \langle xu - y^2, y \rangle$. Isso ilustra que, homogeneizando os geradores $x - y^2$ e y de I, não obtemos o ideal $\overline{I}$.*

No próximo resultado, demonstraremos que cada conjunto U_i é homeomorfo a um espaço afim n-dimensional.

Teorema 2.7.9. *Para $i \in \{0, \ldots, n\}$ considere:*

$$U_i = \{[a_0, \ldots, a_n] \in \mathbb{P}_k^n \,|\, a_i \neq 0\}$$

e defina as funções:

$$\begin{aligned} \phi_i : \mathbb{A}_k^n &\to U_i \\ (b_1, \ldots, b_n) &\mapsto [b_1, \ldots, b_i, 1, b_{i+1}, \ldots, b_n] \end{aligned}$$

$$\begin{aligned} \psi_i : U_i &\to \mathbb{A}_k^n \\ [a_0, \ldots, a_n] &\mapsto \left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i} \right). \end{aligned}$$

(*i*) *$U_i = \mathbb{P}_k^n - V^*(X_i)$. Em particular, $\{U_0, \ldots, U_n\}$ forma uma cobertura aberta de $\mathbb{P}_k^n$;*

(*ii*) *ϕ_i e ψ_i são homeomorfismos.*

Demonstração: Vamos estabelecer a boa-definição de ψ_i.
Consideremos $[a_0, \ldots, a_n]$ e $[b_0, \ldots, b_n]$ pertencentes a U_i com a suposição de que

$$[a_0, \ldots, a_n] = [b_0, \ldots, b_n].$$

Isso implica que $a_i \neq 0$, $b_i \neq 0$ e existe $\lambda \in k - \{0\}$ tal que $a_j = \lambda b_j$ para todo $j \in \{0, \ldots, n\}$. Portanto,

$$\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) = \left(\frac{\lambda b_0}{\lambda b_i}, \ldots, \frac{\lambda b_{i-1}}{\lambda b_i}, \frac{\lambda b_{i+1}}{\lambda b_i}, \ldots, \frac{\lambda b_n}{\lambda b_i}\right)$$
$$= \left(\frac{b_0}{b_i}, \ldots, \frac{b_{i-1}}{b_i}, \frac{b_{i+1}}{b_i}, \ldots, \frac{b_n}{b_i}\right).$$

Isso demonstra que ψ_i é bem definida.
Demonstraremos que $\psi_i \circ \phi_i = \mathrm{id}_{\mathbb{A}^n_k}$ e $\phi_i \circ \psi_i = \mathrm{id}_{U_i}$. Para qualquer $(b_1, \ldots, b_n)$, temos:

$$\begin{aligned}\psi_i \circ \phi_i(b_1, \ldots, b_n) &= \psi_i([b_1, \ldots, b_i, 1, b_{i+1}, \ldots, b_n]) \\ &= \left(\frac{b_1}{1}, \ldots, \frac{b_i}{1}, \frac{b_{i+1}}{1}, \ldots, \frac{b_n}{1}\right) \\ &= (b_1, \ldots, b_n).\end{aligned}$$

Para qualquer $[a_0, \ldots, a_n] \in U_i$, temos:

$$\phi_i \circ \psi_i\left([a_0, \ldots, a_n]\right) = \phi_i\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right)$$
$$= \left[\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right] = \left[a_0, \cdots, a_n\right].$$

Portanto, $\psi_i \circ \phi_i = \mathrm{id}_{\mathbb{A}^n_k}$ e $\phi_i \circ \psi_i = \mathrm{id}_{U_i}$.
Afirmamos que ϕ_i é uma função contínua.
Para demonstrar isso, consideremos F como um conjunto fechado em U_i. Isso implica que existe um ideal homogêneo J em $k[x_0, \ldots, x_n]$ tal que $F = U_i \cap V^*(J)$. Definimos o conjunto

$$J_0 = \{g(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \mid g \in J\} \subseteq k[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n].$$

Vamos demonstrar que $\phi_i^{-1}(F) \subseteq V(J_0)$.
Seja $u = (b_1, \ldots, b_n) \in \phi_i^{-1}(F)$. Isso implica que $[b_1, \ldots, b_i, 1, b_{i+1}, \ldots, b_n] = \phi_i(u) \in U_i \cap V^*(J)$. Para qualquer $h \in J_0$, existe $g \in J$ tal que

$$h = g(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n).$$

Consequentemente,

$$h(u) = h(b_1, \ldots, b_n) = g(b_1, \ldots, b_i, 1, b_{i+1}, \ldots, b_n) = 0.$$

Portanto, $u \in V(J_0)$.
Vamos demonstrar que $V(J_0) \subseteq \phi_i^{-1}(F)$.
Seja $u = (b_1, \ldots, b_n) \in V(J_0)$. Isso implica que $\phi_i(u) \in U_i$. Afirmamos que $\phi_i(u) \in V^*(J)$. Para isso, seja $g \in J$ qualquer. Então, $t = g(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \in J_0$, e como $u \in V(J_0)$, temos

$$0 = t(b_1, \ldots, b_n) = g(b_1, \ldots, b_i, 1, b_{i+1}, \ldots, b_n) \Rightarrow g(\phi_i(u)) = 0.$$

Portanto, $\phi_i(u) \in U_i \cap V^*(J) = F$, o que implica $u \in \phi_i^{-1}(F)$.
Concluímos que $\phi_i^{-1}(F) = V(J_0)$, que é um conjunto fechado em $\mathbb{A}^n_k$.

Vamos agora demonstrar a continuidade de ψ_i.
Comecemos considerando V, um conjunto fechado em $\mathbb{A}^n_k$. Isso implica a existência de um ideal I em $k[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ tal que $V = V(I)$. De acordo com a notação da Definição 2.7.4, definimos

$$\overline{I} := \{\overline{g} \mid g \in I\} \subseteq k[x_0, \ldots, x_n],$$

onde $\overline{g}$ é obtido ao homogeneizar todos os polinômios de I em x_i.
Agora, vamos demonstrar que $\psi_i^{-1}(V) \subseteq V^*(\overline{I})$.
Suponhamos $w = [a_0, \ldots, a_n] \in \psi_i^{-1}(V)$. Isso implica $\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) = \psi_i(w) \in V = V(I)$. Para qualquer $g \in I$,

$$g\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) = 0.$$

Podemos decompor g em termos homogêneos como

$$g = g_0 + \ldots + g_d,$$

onde g_j é homogêneo de grau j para $j \in \{0, \ldots, d\}$. Dessa forma, obtemos

$$\overline{g} = x^d g_0 + x^{d-1} g_1 + \ldots + x_i g_{d-1} + g_d.$$

Note que $w = \left[\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right]$ e

$$\overline{g}(w) = \sum_{j=0}^{d} 1^{d-j} g_j \left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right).$$

Isso simplifica para

$$\overline{g}(w) = \sum_{j=0}^{d} g_j \left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) = g\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) = 0.$$

Uma vez que $\overline{g}$ é homogêneo, $\overline{g}(w) = 0$. Assim, $w \in V^*(\overline{I})$.
Afirmamos que $V^*(\overline{I}) \cap U_i \subseteq \psi_i^{-1}(V)$. Para mostrar isso, consideremos $w = [a_0, \ldots, a_n] \in V^*(\overline{I}) \cap U_i$. Dado $g \in I$, temos $\overline{g} \in \overline{I}$, e uma vez que $w \in V^*(\overline{I})$, temos $\overline{g}(w) = 0$. Como $w \in U_i$, temos $w = \left[\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right]$. Portanto,

$$\overline{g}\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) = 0.$$

Analogamente ao argumento anterior, isso nos leva a concluir que

$$\begin{aligned} g\left(\psi_i(w)\right) &= g\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) \\ &= \overline{g}\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, 1, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) = 0. \end{aligned}$$

Assim, $g(\psi_i(w)) = 0$ para todo $g \in I$, o que implica que $\psi_i(w) \in V(I) = V$, levando a $w \in \psi_i^{-1}(V)$.
Uma vez que $\psi_i^{-1}(V) \subseteq U_i$, combinando as conclusões de $V(J_0) \subseteq \phi_i^{-1}(F)$ e $V^*(\overline{I}) \cap U_i \subseteq \psi_i^{-1}(V)$, obtemos que $\psi_i^{-1}(V) = V^*(\overline{I}) \cap U_i$, é um fechado em U_i.
Dessa forma, concluímos que ϕ_i e ψ_i são funções contínuas e, pelo argumento $\psi_i \circ \phi_i = \mathrm{id}_{\mathbb{A}_k^n}$ e $\phi_i \circ \psi_i = \mathrm{id}_{U_i}$, chegamos à conclusão de que ϕ_i e ψ_i são homeomorfismos, e também $\phi_i = \psi_i^{-1}$. $\square$

Capítulo 3

Resultados

Neste capítulo, descrevemos os Módulos Irredutíveis de dimensão 3 em zero álgebras, na classe de álgebras comutativas e de potências associativas de nilíndice quatro, utilizando a teoria das bases de Gröbner. A abordagem consiste em explorar o produto da álgebra sobre o módulo, que fixando uma base do módulo, este produto é representado por matrizes 3×3. O propósito é identificar as matrizes, à exceção das relacionadas por conjugação. Os módulos irredutíveis de dimensão 3 já foram classificados em uma abordagem diferente no trabalho de [10]. Para isso focaremos no artigo [10] onde encontramos mais detalhes.

Iniciamos apresentando uma das definições fundamentais, porém cruciais, deste capítulo.

Definição 3.0.1. *Uma matriz $N \in \mathbb{M}(n;\mathbb{C})$ é dita* ***nilpotente*** *se existir um número natural $r \in \mathbb{N}$ tal que $N^r = 0$.*

Observação 3.0.2. *Denotamos como $\mathcal{N}_n$ o conjunto de todas as matrizes nilpotentes $n \times n$.*

No seguinte resultado, introduzimos uma condição necessária e suficiente para que uma matriz $N \in \mathbb{M}(n;\mathbb{C})$ seja uma matriz nilpotente. Esta condição será fundamental para estabelecer critérios em nosso problema de classificação dos módulos irredutíveis de dimensão 3.

Teorema 3.0.3. *Uma matriz $N \in \mathbb{M}(n;\mathbb{C})$ é nilpotente se, e somente se, para todo número natural r, temos*

$$tr(N^r) = 0.$$

Observação 3.0.4. *Portanto, podemos considerar $\mathcal{N}_n$ como uma variedade afim, ou seja, o conjunto dos zeros de $\{tr((-)^r) \mid 1 \leq r \leq n\}$.*

Nas definições a seguir, introduziremos os tipos de álgebras com as quais trabalharemos. Seja A uma álgebra de dimensão finita sobre k. Com k um corpo de característica diferente de 2, 3 e 5.

Definição 3.0.5. *Uma álgebra A é chamada de* ***zero álgebra*** *(ou álgebra com zero multiplicação) se, para qualquer $a, b \in A$, $a \cdot b = 0$.*

Exemplo 3.0.6. *Considere o conjunto de todas as matrizes estritamente triangulares superiores com a soma e produto usuais de matrizes*

$$\left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \ : \ a \in \mathbb{C} \right\}. \tag{3.1}$$

Definição 3.0.7. *Seja A uma álgebra não associativa. Para qualquer $x \in A$, definimos as potências principais (à direita) de x de forma indutiva da seguinte maneira:*

$$\begin{aligned} x^1 &= x, \\ x^{r+1} &= x^r x \quad \text{se } r \geq 1. \end{aligned}$$

Algumas potências da álgebra são dadas por:

$$\begin{aligned} A^1 &= A, \\ A^{r+1} &= \sum_{i+j=r+1} A^i A^j \quad \text{se } r \geq 1. \end{aligned}$$

Nesta definição, a potência A^{r+1} é obtida como a soma de todos os produtos possíveis da forma $A^i A^j$, onde i e j não são negativos e somam $r+1$. A não associatividade da álgebra implica que a ordem de multiplicação é importante e não se assume que $A^i A^j = A^j A^i$.

Definição 3.0.8. *Uma álgebra A é chamada **nil** ou **nilálgebra** se, para todo x em A, existe um número natural $r > 0$, tal que $x^r = 0$. Se existe um número natural $r > 0$ (o menor valor r) tal que $x^r = 0$ para todo x em A, então esse valor r é chamado de **nilíndice** de A.*

Definição 3.0.9. *Uma álgebra A é chamada **nilpotente** se existe um número natural r tal que $A^r = 0$.*

Observação 3.0.10. *É importante notar a diferença em uma álgebra que não é associativa. Os conceitos de nilálgebra e nilpotência são distintos. Uma nilálgebra atende à Definição 3.0.8, mas a Definição 3.0.9 implica que existe um número natural n tal que o produto de qualquer n-elementos é sempre nulo. Por exemplo, se tivermos elementos $x_1, x_2, \ldots, x_n \in A$, então a multiplicação*

$$x_1 x_2 \cdots x_n = (\ldots((x_1 x_2) x_3) \cdots) x_{n-1}) x_n = \ldots = x_1(x_2(\cdots(x_{n-2}(x_{n-1} x_n))\ldots) = 0.$$

Também é importante notar que uma álgebra nilpotente é uma nilálgebra, mas o oposto não é necessariamente verdadeiro em todos os casos.

Exemplo 3.0.11. *Tomamos a álgebra associativa e comutativa (sem unidade) dos polinômios nas variáveis $x_1, x_2, \ldots$, e consideramos o quociente pelo ideal gerado por $x_1^2, x_2^2, \ldots$. Essa álgebra é nil: o quadrado de todo monômio é igual a zero e, se um polinômio f tem m termos, então a expressão f^{m+1} é composta por termos nos quais pelo menos um dos monômios se repete; portanto, $f^{m+1} = 0$. No entanto, ela não é nilpotente, uma vez que os produtos $x_1 x_2 \cdots x_n$ são não nulos para todo n.*

Definição 3.0.12. *Seja A uma álgebra comutativa. Para cada elemento $x \in A$, definimos de forma indutiva as potências de x por $x^1 = x$ e $x^{r+1} = x \cdot x^r$ para $r \geq 1$. A álgebra A é denominada **álgebra de potências associativas** se $x^i x^j = x^{i+j}$ para todos os inteiros positivos i e j.*

Exemplo 3.0.13. *Seja k um corpo de característica $\neq 2$. Um k-espaço vetorial $\mathcal{B}$, juntamente com uma aplicação $\mathcal{B} \times \mathcal{B} \to \mathcal{B}, (u, v) \mapsto u \circ v$, é chamado de* ***álgebra de Jordan*** *se, para todo $u, v, w \in \mathcal{B}$ e $\alpha \in k$, satisfizerem*

a. $u \circ v = v \circ u$,
$u \circ (v + w) = u \circ v + u \circ w$, $(\alpha u) \circ v = \alpha(u \circ v)$,

b. $u \circ (u^2 \circ v) = u^2 \circ (u \circ v)$, *onde* $u^2 = u \circ u$.

Observamos que se trata de uma álgebra comutativa, embora apresente uma associatividade fraca. Se $\mathcal{B}$ é uma álgebra de Jordan, então $u^r \circ u^s = u^{r+s}$ é válido para todo $u \in \mathcal{B}$, $r \geq 1$ e $s \geq 1$. mostra que a lei associativa é válida para as potências de cada elemento em $\mathcal{B}$. Portanto, $\mathcal{B}$ é uma álgebra de potências associativas.

O problema a seguir é conhecido como o Problema de Albert [1], que é um problema notável envolvendo as álgebras que definimos anteriormente.

O problema de Albert: Toda nilálgebra comutativa de potências associativas sobre um corpo de característica $\neq 2$ de dimensão finita é solúvel?

Uma abordagem para a questão de Albert pode ser obtida usando módulos no seguinte resultado

Lema 3.0.14. *Seja A uma álgebra com zero multiplicação e V um A-bimódulo irredutível na variedade de álgebras comutativa de potências associativas, ambos de dimensão finita. Suponha que seja possível definir um produto em V com valores em A: $(u, v) \mapsto u \cdot v \in A$, de modo que $V \cdot V = A$. Se o espaço vetorial $Q = A \oplus V$ com a multiplicação*

$$(a + u)(b + v) = av + ub + u \cdot v,$$

é uma álgebra comutativa de potências associativas, então Q é nil e simples. fornecendo um contraexemplo para o Problema de Albert.

O lema anterior mostra a importância dos módulos irredutíveis como ferramenta para estudar o problema de Albert. O propósito deste capítulo é investigar a estrutura de módulos e seus produtos em relação a uma álgebra bidimensional trivial dentro do contexto das álgebras comutativas de potências associativas com um nilíndice de quatro.

Ao longo deste texto, assumiremos que as álgebras estão definidas em um corpo algebricamente fechado k, com característica diferente a $2, 3$ ou 5. Vamos denotar o conjunto $k - \{0\}$ como k^*. Seja $\mathcal{A}$ uma classe de álgebras e considere uma álgebra A nessa classe. Um A-bimódulo na classe $\mathcal{A}$, ou simplesmente um bimódulo para A, é um espaço vetorial M sobre k com dois transformações bilineares: $A \times M \to M$ e $M \times A \to M$, que levam (a, m) em am e (m, a) em ma, de modo que a álgebra $E = A \oplus M$, com a multiplicação definida por $(a + m)(b + n) = ab + (an + mb)$ para todos $a, b \in A$ e $m, n \in M$, também pertence a classe $\mathcal{A}$.
Para uma álgebra arbitrária A e um bimódulo M para A, denotamos as transformações lineares L_a e R_a em M, definidas por $x \to ax$ e $x \to xa$, respectivamente. Como as

álgebras consideradas neste capítulo são comutativas, utilizaremos apenas as multiplicações à esquerda L_a. Observa-se também que, no caso de A ser comutativo, as noções de A-módulo e A-bimódulo são idênticas.
Em [10] é importante notar que a variedade de álgebras comutativas de potências associativas, sobre um corpo k de característica diferente de 2, 3 e 5, é definida pelas identidades $xy = yx$ e

$$x(xx^2) = x^2x^2. \tag{3.2}$$

A identidade (3.2) foi introduzida em [1]. A partir da primeira linearização da identidade (3.2), obtemos o seguinte resultado.

$$2x(x(xy)) + x(x^2y) + x^3y = 4x^2(xy). \tag{3.3}$$

Observação 3.0.15. *O processo de linearização de um polinômio implica em converter um polinômio de grau superior em um linear, onde cada passo deste processo reduz um grau do polinômio original, mas aumenta o número de variáveis envolvidas. Isso é feito tipicamente para simplificar a análise ou resolver problemas que são mais manejáveis em um formato linear. A teoria pode ser consultada na página 9 do livro [12]. A primeira linearização da identidade (3.2) em relação à variável x coincide com a primeira derivada de (3.2) em relação a x, considerando y como sua derivada interna.*

3.1 Módulos para uma Álgebra Bidimensional Trivial

A partir deste ponto, consideremos $A = k\langle a, b\rangle$ uma álgebra bidimensional trivial sobre k, e M um A-módulo finitamente dimensional. Dado que $A^2 = 0$, a identidade (3.3) se simplifica para $L_x^3 = 0$, ou $x(x(xy)) = 0$ para todos $x \in A$ e $y \in M$. A linearização desta identidade resulta em

$$x_1(x_1(x_2y)) + x_1(x_2(x_1y)) + x_2(x_1(x_1y)) = 0, \tag{3.4}$$

e, portanto

$$L_{x_1}^2L_{x_2} + L_{x_1}L_{x_2}L_{x_1} + L_{x_2}L_{x_1}^2 = 0.$$

Em particular, denotaremos $L_a = \mathfrak{a}$ e $L_b = \mathfrak{b}$. Então

$$\mathfrak{a}^3 = \mathfrak{b}^3 = 0; \quad \mathfrak{a}^2\mathfrak{b} + \mathfrak{a}\mathfrak{b}\mathfrak{a} + \mathfrak{b}\mathfrak{a}^2 = 0; \quad \mathfrak{b}^2\mathfrak{a} + \mathfrak{b}\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{b}^2 = 0. \tag{3.5}$$

Defina $V = \ker \mathfrak{a}$. Como $\mathfrak{a}^3 = 0$, temos $V \neq 0$. Seja $\varphi : V \to V$ definido por $\varphi(v) = \mathfrak{a}\mathfrak{b}(v)$ para todo $v \in V$. Observe que φ é uma aplicação bem definida, uma vez que $\varphi(V) \subseteq V$, pois temos $\mathfrak{a}\varphi(v) = \mathfrak{a}^2\mathfrak{b}v = -\mathfrak{a}\mathfrak{b}\mathfrak{a}v - \mathfrak{b}\mathfrak{a}^2v = 0$ para tudo $v \in V$. Como k é um espaço vetorial algebricamente fechado, a aplicação φ tem pelo menos um autovalor.

Observação 3.1.1. *O fato de que $L_a^3 = \mathfrak{a}^3 = 0$ é um dos pontos cruciais deste capítulo, pois essa condição assegura que, em termos de matrizes de dimensão 3×3, elas serão nilpotentes com nilíndice 3. Da mesma forma para L_b*

O lema a seguir encontrado no artigo [10] descreve a estrutura dos A-módulos irredutíveis M sob a ação dos operadores $\mathfrak{a}$ e $\mathfrak{b}$. Considerando as identidades em (3.5).

Lema 3.1.2. *Se $v \in V_\lambda = ker(\varphi - \lambda I_V)$, onde $v \neq 0$ e $\lambda \neq 0$, com λ autovalor de φ, então $M_v = \langle v, \mathfrak{b}v, \mathfrak{b}^2 v\rangle$ é um A-submódulo irredutível de M com dimensão 3. As matrizes de $\mathfrak{a}_{|M_v}$ e $\mathfrak{b}_{|M_v}$ em relação à base $\{v, \mathfrak{b}v, \mathfrak{b}^2 v\}$ são dadas por*

$$h(\lambda) = \begin{pmatrix} 0 & \lambda & 0 \\ 0 & 0 & -\lambda \\ 0 & 0 & 0 \end{pmatrix} \quad e \quad T = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{3.6}$$

Teorema 3.1.3. *Todo A-módulo irredutível de potências associativas M possui dimensão 1 ou 3. Se M tem dimensão 1, então $AM = \{0\}$; se M tem dimensão 3, então, para uma escolha adequada de base e um escalar não nulo λ, a ação de a, b em M é dada por (3.6), respectivamente.*

O seguinte Teorema representa a classificação dos subespaços lineares nilpotentes maximais em $\mathbb{M}(3;\mathbb{C})$, conforme ao artigo [7].

Teorema 3.1.4. *Todo subespaço linear nilpotente máximal de $\mathbb{M}(3;\mathbb{C})$ é conjugado a exatamente um dos seguintes subespaços:*

$$\boldsymbol{V} = \left\{ \begin{pmatrix} 0 & x & y \\ 0 & 0 & z \\ 0 & 0 & 0 \end{pmatrix} : x, y, z \in \mathbb{C} \right\}, \tag{3.7}$$

$$\boldsymbol{W} = \left\{ \begin{pmatrix} 0 & x & 0 \\ y & 0 & x \\ 0 & -y & 0 \end{pmatrix} : x, y \in \mathbb{C} \right\}. \tag{3.8}$$

Observação 3.1.5. *Seguindo a abordagem apresentada no artigo [10], obtivemos as matrizes $h(\lambda)$ e T em (3.6). Observando a classificação encontrada no artigo [7], a menos de conjugação, vemos que o subespaço W em (3.8) é o subespaço gerado pelas matrizes $h(\lambda)$ e T. Portanto, descrever os módulos irredutíveis para uma Álgebra Bidimensional Trivial equivale a estudar os subespaços lineares nilpotentes maximais de $\mathbb{M}(3;\mathbb{C})$.*

Nossa próxima etapa é encontrar essa classificação utilizando a teoria das bases de Gröbner.

3.2 Procedimento computacional proposto SageMath

Para visualizar o procedimento a seguir na busca pela classificação dos Módulos Irredutíveis de dimensão 3 em zero álgebras, pertencentes à classe de álgebras comutativas de potências associativas de nilíndice quatro, vamos examinar um exemplo específico para determinar os subespaços lineares nilpotentes maximais de $\mathbb{M}(2;\mathbb{C})$.

Exemplo 3.2.1. *Vamos determinar os subespaços lineares nilpotentes maximais de $\mathbb{M}(2;\mathbb{C})$. Primeiro definimos uma matriz quadrada B de tamanho 2×2 com variáveis (ou indeterminadas) como entradas da matriz, da seguinte maneira*

$$B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}. \tag{3.9}$$

Portanto, para identificar as matrizes nilpotentes, neste caso, o nilíndice coincide com dois. Então

$$B^2 = \begin{pmatrix} x^2+yz & wy+xy \\ wz+xz & w^2+yz \end{pmatrix} = 0. \tag{3.10}$$

Utilizando a caracterização das matrizes nilpotentes em relação ao traço na Definição 3.0.3 e, adicionalmente, o fato de que o determinante de uma matriz nilpotente é zero, podemos estabelecer o seguinte sistema de equações.

$$\begin{cases} w+x &= 0 \\ w^2+x^2+2yz &= 0 \\ wx-yz &= 0. \end{cases} \tag{3.11}$$

Observe que as entradas em B e B^2 podem ser interpretadas como polinômios no anel de polinômios $k[x,y,z,w]$. Nesse caso, podemos tomar as equações de (3.11) como os geradores do ideal $I = \langle w+x, w^2+x^2+2yz, wx-yz\rangle$. Portanto, calculamos a base de Gröbner de I com ordem monomial Lex.

$$G = \{x+w, yz+w^2\}. \tag{3.12}$$

Onde a forma normal de todos os polinômios de (3.11), quando divididos pelos elementos da base de Gröbner G, é igual a zero. Além disso, a base de Gröbner G compartilha as mesmas soluções do Sistema (3.11). Então, se considerarmos as equações de G como um sistema

$$\begin{cases} x+w &= 0 \\ yz+w^2 &= 0 \end{cases}, \tag{3.13}$$

resolvendo o Sistema (3.13) obtemos as soluções

$$x = -\sqrt{(-rt)}, y = t, z = r, w = \sqrt{(-rt)}, \tag{3.14}$$

$$x = \sqrt{(-rt)}, y = t, z = r, w = -\sqrt{(-rt)}, \tag{3.15}$$

portanto, temos que

$$B = \begin{pmatrix} -\sqrt{(-rt)} & t \\ r & \sqrt{(-rt)} \end{pmatrix}. \tag{3.16}$$

Se $t = 0$, então B é uma matriz triangular inferior. Para $t \neq 0$, $x = -\sqrt{(-rt)}$ temos

$$B = \begin{pmatrix} x & t \\ -\frac{x^2}{t} & -x \end{pmatrix}. \tag{3.17}$$

Assim o subespaço linear nilpotente maximal é

$$\left\{ \begin{pmatrix} x & t \\ -\frac{x^2}{t} & -x \end{pmatrix} \; : \; x, t \in \mathbb{C}, t \neq 0 \right\}. \tag{3.18}$$

Considere a matriz

$$B = \begin{pmatrix} x & t \\ -\frac{x^2}{t} & -x \end{pmatrix}.$$

Definimos os vetores $\mathbf{e}_1 = (1,0)$ *e* $\mathbf{e}_2 = (0,1)$. *Em seguida, introduzimos os vetores*

$$\begin{aligned}\mathbf{w}_1 &= t\mathbf{e}_1 - x\mathbf{e}_2,\\ \mathbf{w}_2 &= \mathbf{e}_2.\end{aligned}$$

Dessa forma, construímos a base $\{\mathbf{w}_1, \mathbf{w}_2\}$. *Agora, podemos calcular a mudança de base:*

$$\begin{aligned}B(\mathbf{w}_1) &= tB(\mathbf{e}_1) - xB(\mathbf{e}_2)\\ &= t(x\mathbf{e}_1 - \frac{x^2}{t}\mathbf{e}_2) - x(t\mathbf{e}_1 - x\mathbf{e}_2)\\ &= tx\mathbf{e}_1 - x^2\mathbf{e}_2 - tx\mathbf{e}_1 + x^2\mathbf{e}_2 = (0,0),\end{aligned}$$

e

$$B(\mathbf{w}_2) = B(\mathbf{e}_2) = t\mathbf{e}_1 - x\mathbf{e}_2 = \mathbf{w}_1.$$

Portanto, a matriz de B *na base* $\{\mathbf{w}_1, \mathbf{w}_2\}$ *é*

$$[B]_{\{\mathbf{w}_1,\mathbf{w}_2\}} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

As matrizes de transição de base são dadas por

$$D = \begin{pmatrix} t & 0 \\ -x & 1 \end{pmatrix} \text{ e } D^{-1} = \begin{pmatrix} \frac{1}{t} & 0 \\ \frac{x}{t} & 1 \end{pmatrix}.$$

onde

$$D^{-1}LD = \begin{pmatrix} \frac{1}{t} & 0 \\ \frac{x}{t} & 1 \end{pmatrix}\begin{pmatrix} x & t \\ -\frac{x^2}{t} & -x \end{pmatrix}\begin{pmatrix} t & 0 \\ -x & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

portanto, as matrizes $\begin{pmatrix} x & t \\ -\frac{x^2}{t} & -x \end{pmatrix}$ *e* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *são conjugadas.*

Observação 3.2.2. *Note que, no Exemplo 3.2.1, todos os polinômios em* B, B^2, *no Sistema (3.11), o ideal* I *e a base de Gröbner* G *são polinômios homogêneos. Uma das motivações para trabalhar no espaço projetivo* $\mathbb{P}^n_k$ *é buscar que a matriz* A *seja nilpotente, o que significa que pelo menos uma de suas entradas seja diferente de zero. Além de considerar o conjunto algébrico projetivo* $V^*()$ *para os zeros dos Sistemas (3.11) y (3.13).*

Exemplo 3.2.3. *Para os cálculos anteriores no Exemplo 3.2.1, utilizamos o sistema algébrico computacional SageMath para simplificar o processo. Agora, vamos apresentar o código e os resultados obtidos com o SageMath. Primeiro definimos as variáveis que representarão as entradas da matriz e calculamos a potência quadrada da matriz dada em (3.9).*

```
var('x y z w')
B=matrix([[x,y],[z,w]])
H=B^2
print(H)
[x^2 + y*z w*y + x*y]
[w*z + x*z w^2 + y*z]
```

Definimos as expressões para o traço e o determinante de B em (3.11).

```
E1=B.trace()
E2=H.trace()
E3=B.determinant()
print(E1)
print(E2)
print(E3)
w + x
w^2 + x^2 + 2*y*z
w*x - y*z
```

Definimos o anel de polinômios que será usado, com variáveis x, y, z e w, juntamente com a ordem monomial (Lex) que adotaremos sobre o corpo dos números racionais. Em seguida, definimos o ideal gerado pelos elementos de (3.11) e calculamos sua base de Gröbner reduzida e sua base de Gröbner usando o algoritmo de Buchberger.

```
P.<x,y,z,w> = PolynomialRing(QQ, 4, order = 'lex')
I1=P.ideal([E1,E2,E3])
G1=I1.groebner_basis()
G2=I1.groebner_basis('toy:buchberger')
print('Base de Gröbner: ',G1)
print('número de elementos na Base de Gröbner: ',len(G1))
print('Base de Gröbner No reduzida: ',G2)
print('número de elementos na Base de Gröbner: ',len(G2))
Base de Gröbner:  [x + w, y*z + w^2]
número de elementos na Base de Gröbner:  2
Base de Gröbner No reduzida:  [x^2 + 2*y*z + w^2, x*w - y*z,
x + w, y*z + w^2]
número de elementos na Base de Gröbner:  4
```

Definimos o sistema de equações com base nos elementos da base de Gröbner em (3.12) e procedemos à sua resolução.

```
s=solve([x + w, y*z + w^2],x,y,z,w)
print(s)
show(s)
[
[x == -sqrt(-r20*r21), y == r20, z == r21, w == sqrt(-r20*r21)],
[x == sqrt(-r22*r23), y == r22, z == r23, w == -sqrt(-r22*r23)]
]
```

Exemplo 3.2.4. *Vamos determinar os subespaços lineares nilpotentes maximais de $\mathbb{M}(3;\mathbb{C})$. Primeiro definimos uma matriz quadrada B de tamanho 3×3 com variáveis (ou indeterminadas) como entradas da matriz, da seguinte maneira*

$$B=\begin{pmatrix} a & b & c \\ d & f & g \\ x & y & z \end{pmatrix}. \tag{3.19}$$

Portanto, para identificar as matrizes nilpotentes, com nilíndice 3, levando em consideração a Observação (3.1.1).

$$B^2 = \begin{pmatrix} a^2+bd+cx & ab+bf+cy & ac+bg+cz \\ ad+df+gx & bd+f^2+gy & cd+fg+gz \\ ax+dy+xz & bx+fy+yz & cx+gy+z^2 \end{pmatrix}.$$

$$V_1 = \begin{pmatrix} (a^2+bd+cx)\,a+(ab+bf+cy)d+(ac+bg+cz)x \\ (ad+df+gx)a+(bd+f^2+gy)\,d+(cd+fg+gz)x \\ (ax+dy+xz)a+(bx+fy+yz)d+(cx+gy+z^2)\,x \end{pmatrix},$$

$$V_2 = \begin{pmatrix} (a^2+bd+cx)\,b+(ab+bf+cy)f+(ac+bg+cz)y \\ (ad+df+gx)b+(bd+f^2+gy)\,f+(cd+fg+gz)y \\ (ax+dy+xz)b+(bx+fy+yz)f+(cx+gy+z^2)\,y \end{pmatrix},$$

$$V_3 = \begin{pmatrix} (a^2+bd+cx)\,c+(ab+bf+cy)g+(ac+bg+cz)z \\ (ad+df+gx)c+(bd+f^2+gy)\,g+(cd+fg+gz)z \\ (ax+dy+xz)c+(bx+fy+yz)g+(cx+gy+z^2)\,z \end{pmatrix},$$

$$B^3 = (V_1 \quad V_2 \quad V_3) = 0.$$

Utilizando a caracterização das matrizes nilpotentes em relação ao traço na Definição 3.0.3 e, adicionalmente, o fato de que o determinante de uma matriz nilpotente é zero, podemos estabelecer o seguinte sistema de equações.

$$\begin{cases} a+f+z &= 0 \\ a^2+2bd+f^2+2cx+2gy+z^2 &= 0 \\ (a^2+bd+cx)a+(ad+df+gx)b+(ax+dy+xz)c & \\ +(ab+bf+cy)d+(bd+f^2+gy)f+(bx+fy+yz)g & \\ +(ac+bg+cz)x+(cd+fg+gz)y+(cx+gy+z^2)z &= 0 \\ -(gy-fz)a+(cy-bz)d-(cf-bg)x &= 0. \end{cases} \tag{3.20}$$

Observe que as entradas em B, B^2 e B^3 podem ser interpretadas como polinômios no anel de polinômios $k[a,b,c,d,f,g,x,y,z]$. Nesse caso, podemos tomar as equações de (3.20) como os geradores do ideal $I = \langle a+f+z, \ldots, -(gy-fz)a+(cy-bz)d-(cf-bg)x\rangle$. Portanto, calculamos a base de Gröbner de I .

$$\begin{aligned} G = \{&a+f+z, bd+cx+f^2+fz+gy+z^2, \\ &bgx+cdy-cfx+cxz+fgy+2gyz+z^3, \\ &cd^2y-cdfx+cdxz-cgx^2+dfgy+2dgyz+dz^3-f^2gx-fgxz-g^2xy-gxz^2\}. \end{aligned}$$

Onde a forma normal de todos os polinômios de (3.20), quando divididos pelos elementos da base de Gröbner G, é igual a zero. Além disso, a base de Gröbner G compartilha as mesmas soluções do Sistema (3.20). Então, se considerarmos as equações de G como um sistema

$$\begin{cases} a+f+z &= 0 \\ bd+cx+f^2+fz+gy+z^2 &= 0 \\ bgx+cdy-cfx+cxz+fgy+2gyz+z^3 &= 0 \\ cd^2y-cdfx+cdxz-cgx^2+dfgy & \\ +2dgyz+dz^3-f^2gx-fgxz-g^2xy-gxz^2 &= 0. \end{cases} \tag{3.21}$$

tentando resolver o Sistema (3.21) computacionalmente, não estamos obtendo soluções. Vamos, portanto, tentar algumas estratégias para ver se alcançamos nosso objetivo.

Exemplo 3.2.5. *Para os cálculos anteriores no Exemplo 3.2.4, utilizamos o sistema algébrico computacional SageMath para simplificar o processo. Agora, vamos apresentar o código e os resultados obtidos com o SageMath. Primeiro definimos as variáveis que representarão as entradas da matriz e calculamos a potência quadrada da matriz dada em (3.19).*

```
a,b,c,d,f,g,x,y,z=var('a,b,c,d,f,g,x,y,z')
B=matrix([[a,b,c],[d,f,g],[x,y,z]])
H=B^2
K=B^3
print(B)
print(H)
print(K)
[a b c]
[d f g]
[x y z]
[a^2 + b*d + c*x a*b + b*f + c*y a*c + b*g + c*z]
[a*d + d*f + g*x b*d + f^2 + g*y c*d + f*g + g*z]
[a*x + d*y + x*z b*x + f*y + y*z c*x + g*y + z^2]
[(a^2 + b*d + c*x)*a + (a*b + b*f + c*y)*d + (a*c + b*g + c*z)*x
(a^2 + b*d + c*x)*b + (a*b + b*f + c*y)*f + (a*c + b*g + c*z)*y
(a^2 + b*d + c*x)*c + (a*b + b*f + c*y)*g + (a*c + b*g + c*z)*z]
[(a*d + d*f + g*x)*a + (b*d + f^2 + g*y)*d + (c*d + f*g + g*z)*x
(a*d + d*f + g*x)*b + (b*d + f^2 + g*y)*f + (c*d + f*g + g*z)*y
(a*d + d*f + g*x)*c + (b*d + f^2 + g*y)*g + (c*d + f*g + g*z)*z]
[(a*x + d*y + x*z)*a + (b*x + f*y + y*z)*d + (c*x + g*y + z^2)*x
(a*x + d*y + x*z)*b + (b*x + f*y + y*z)*f + (c*x + g*y + z^2)*y
(a*x + d*y + x*z)*c + (b*x + f*y + y*z)*g + (c*x + g*y + z^2)*z]
```

Definimos as expressões para o traço e o determinante de B em (3.20).

```
T1=B.trace()
T2=H.trace()
T3=K.trace()
T4=B.determinant()
print('T1: ',T1)
print('T2: ',T2)
print('T3: ',T3)
print('T4: ',T4)
T1:  a + f + z
T2:  a^2 + 2*b*d + f^2 + 2*c*x + 2*g*y + z^2
T3:  (a^2 + b*d + c*x)*a + (a*d + d*f + g*x)*b + (a*x + d*y + x*z)*c
+ (a*b + b*f + c*y)*d + (b*d + f^2 + g*y)*f + (b*x + f*y + y*z)*g
+ (a*c + b*g + c*z)*x + (c*d + f*g + g*z)*y + (c*x + g*y + z^2)*z
T4:  -(g*y - f*z)*a + (c*y - b*z)*d - (c*f - b*g)*x
```

Definimos o anel de polinômios que será usado, com variáveis a, b, c, d, f, g, x, y e z, juntamente com a ordem monomial (Lex) que adotaremos sobre o corpo dos números racionais. Em seguida, definimos o ideal gerado pelos elementos de (3.20) e calculamos sua base de Gröbner reduzida e sua base de Gröbner usando o algoritmo de Buchberger.

```
R4.<a,b,c,d,f,g,x,y,z>=PolynomialRing(QQ,'a,b,c,d,f,g,x,y,z',order='lex')
I4=R4.ideal([T1,T2,T3,T4])
G4=I4.groebner_basis()
G10=I4.groebner_basis('toy:buchberger')
print('Base de Gröbner: ',G4)
print('número de elementos na Base de Gröbner: ',len(G4))
print('Base de Gröbner não reduzida: ',G10)
print('número de elementos na Base de Gröbner: ',len(G10))
```

```
Base de Gröbner:  [a + f + z, b*d + c*x + f^2 + f*z + g*y + z^2,
b*g*x + c*d*y - c*f*x + c*x*z + f*g*y + 2*g*y*z + z^3,
c*d^2*y - c*d*f*x + c*d*x*z - c*g*x^2 + d*f*g*y + 2*d*g*y*z
+ d*z^3 - f^2*g*x - f*g*x*z - g^2*x*y - g*x*z^2]
número de elementos na Base de Gröbner:  4
Base de Gröbner não reduzida:  [a^3 + 3*a*b*d + 3*a*c*x + 3*b*d*f
+ 3*b*g*x + 3*c*d*y + 3*c*x*z + f^3 + 3*f*g*y + 3*g*y*z + z^3,
a^2 + 2*b*d + 2*c*x + f^2 + 2*g*y + z^2,
a*f*z - a*g*y - b*d*z + b*g*x + c*d*y - c*f*x,
a + f + z, b*d + c*x + f^2 + f*z + g*y + z^2,
b*g*x + c*d*y - c*f*x + c*x*z + f*g*y + 2*g*y*z + z^3,
c*d^2*y - c*d*f*x + c*d*x*z - c*g*x^2 + d*f*g*y + 2*d*g*y*z
+ d*z^3 - f^2*g*x - f*g*x*z - g^2*x*y - g*x*z^2]
número de elementos na Base de Gröbner:  7
```

Definimos o sistema de equações com base nos elementos da base de Gröbner em no Exemplo (3.2.4) e procedemos à sua resolução.

```
s10=solve([a^3 + 3*a*b*d + 3*a*c*x + 3*b*d*f + 3*b*g*x
+ 3*c*d*y + 3*c*x*z + f^3 + 3*f*g*y + 3*g*y*z + z^3==0,
a^2 + 2*b*d + 2*c*x + f^2 + 2*g*y + z^2==0,
a*f*z - a*g*y - b*d*z + b*g*x + c*d*y - c*f*x==0,
a + f + z==0, b*d + c*x + f^2 + f*z + g*y + z^2==0,
b*g*x + c*d*y - c*f*x + c*x*z + f*g*y + 2*g*y*z + z^3==0,
c*d^2*y - c*d*f*x + c*d*x*z - c*g*x^2 + d*f*g*y +
2*d*g*y*z + d*z^3 - f^2*g*x - f*g*x*z - g^2*x*y -
g*x*z^2==0],a,b,c,d,f,g,x,y,z)
print(s10)
print('número de elementos do sistema: ',len(s10))
```

```
[
a + f + z == 0,
-c*f*x + b*g*x + c*d*y - a*g*y - b*d*z + a*f*z == 0,
a^2 + 2*b*d + f^2 + 2*c*x + 2*g*y + z^2 == 0,
b*d + f^2 + c*x + g*y + f*z + z^2 == 0,
-c*f*x + b*g*x + c*d*y + f*g*y + c*x*z + 2*g*y*z + z^3 == 0,
```

```
a^3 + 3*a*b*d + 3*b*d*f + f^3 + 3*a*c*x + 3*b*g*x
+3*c*d*y + 3*f*g*y + 3*c*x*z + 3*g*y*z + z^3 == 0,
-c*d*f*x - f^2*g*x - c*g*x^2 + c*d^2*y + d*f*g*y
-g^2*x*y + c*d*x*z - f*g*x*z + 2*d*g*y*z - g*x*z^2
+d*z^3 == 0
]
número de elementos do sistema: 7
```

Computacionalmente, não estamos obtendo soluções do sistema. Vamos, portanto, tentar outra estratégia. Vamos definir o ideal I gerado pelas entradas da matriz B^3 e calcular a sua base de Gröbner.

```
R3.<a,b,c,d,f,g,x,y,z>=PolynomialRing(QQ,'a,b,c,d,f,g,x,y,z',order='lex')
#R3.<a,b,c,d,f,g,x,y,z>=
PolynomialRing(QQ,'a,b,c,d,f,g,x,y,z',order='degrevlex')
I3=R3.ideal([K[0,0],K[0,1],K[0,2],K[1,0],K[1,1],K[1,2],K[2,0],K[2,1],K[2,2]])
G3=I3.groebner_basis()
print('Base de Gröbner: ',G3)
print('número de elementos na Base de Gröbner: ',len(G3))
Base de Gröbner:  Polynomial Sequence with 39 Polynomials in 9 Variables
número de elementos na Base de Gröbner:  39
Polynomial Sequence with 39 Polynomials in 9 Variables
```

Adicionando a condição de traço de B aos geradores de I e fatorando os polinômios.

```
I3=R3.ideal([K[0,0],K[0,1],K[0,2],K[1,0],K[1,1],
K[1,2],K[2,0],K[2,1],K[2,2],a + f + z])
G3=I3.groebner_basis()
for s in range(0,len(G3)):
    print(G3[s].factor())
print('número de elementos na Base de Gröbner: ',len(G3))
a + f + z
b * (b*d + c*x + f^2 + f*z + g*y + z^2)
c * (b*d + c*x + f^2 + f*z + g*y + z^2)
d * (b*d + c*x + f^2 + f*z + g*y + z^2)
f * (b*d + c*x + f^2 + f*z + g*y + z^2)
g * (b*d + c*x + f^2 + f*z + g*y + z^2)
x * (b*d + c*x + f^2 + f*z + g*y + z^2)
y * (b*d + c*x + f^2 + f*z + g*y + z^2)
z * (b*d + c*x + f^2 + f*z + g*y + z^2)
b*g*x + c*d*y - c*f*x + c*x*z + f*g*y + 2*g*y*z + z^3
(-1) * (-c*d^2*y + c*d*f*x - c*d*x*z + c*g*x^2 - d*f*g*y
- 2*d*g*y*z - d*z^3 + f^2*g*x + f*g*x*z + g^2*x*y + g*x*z^2)
número de elementos na Base de Gröbner:  11
```

Observe que se $bd + cx + f^2 + fz + gy + z^2 \neq 0$, então $B = 0$. Nosso objetivo é encontrar soluções não nulas. Portanto, conseguimos um sistema mais amigável para tentar resolver.

```
s9=solve([a + f + z==0, b*d + c*x + f^2 + f*z + g*y + z^2==0,
b*g*x + c*d*y - c*f*x + c*x*z + f*g*y + 2*g*y*z + z^3==0,
(-1) * (-c*d^2*y + c*d*f*x - c*d*x*z + c*g*x^2 - d*f*g*y
- 2*d*g*y*z - d*z^3 + f^2*g*x + f*g*x*z + g^2*x*y + g*x*z^2)==0]
,a,b,c,d,f,g,x,y,z)
print(s9)
[
a + f + z == 0,
b*d + f^2 + c*x + g*y + f*z + z^2 == 0,
-c*f*x + b*g*x + c*d*y + f*g*y + c*x*z + 2*g*y*z + z^3 == 0,
-c*d*f*x - f^2*g*x - c*g*x^2 + c*d^2*y + d*f*g*y
- g^2*x*y + c*d*x*z - f*g*x*z + 2*d*g*y*z - g*x*z^2 + d*z^3 == 0
]
```

Entretanto, mesmo após essas tentativas, ainda não conseguimos uma solução para o sistema de equações. Vamos prosseguir tentando fornecer ao sistema computacional os cálculos necessários para a resolução. Lamentavelmente, devido às limitações computacionais em nosso estudo e à falta de memória disponível durante a execução do algoritmo no SageMath, o programa não possui suporte executável em paralelo. Como resultado, a capacidade computacional do cluster, composto por 240 núcleos, foi equivalente à de um laptop comum. Portanto, com a versão em série, não foi possível obter os resultados da computação dos sistemas de equações propostos. No entanto, é importante observar que, caso fossem computados os sistemas de equações propostos, poderíamos obter resultados de maneira análoga ao caso de dimensão dois.

Referências Bibliográficas

[1] A. A. Albert, *Power-associative rings*, Trans. Amer. Math. Soc. 64, 1948.

[2] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Series in Mathematics, 1969.

[3] T. Becker and V. Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics, 141, Springer, New York, 1993.

[4] D. A. Cox, J. B. Little and D. B. O'Shea, *Ideals, varieties, and algorithms*, Undergraduate Texts in Mathematics, Springer, New York, 1992.

[5] D. A. Cox, J. B. Little and D. B. O'Shea, *Using algebraic geometry*, Graduate Texts in Mathematics, 185, Springer, New York, 1998.

[6] T. F. da Silva, *GEOMETRIA ALGÉBRICA*, Notas de aula, junho de 2020. *https : //drive.google.com/file/d/14sp0sl8j8quB0ki − 20wdKUaSvBLlN3hd/view?usp = drive*$_{l}$*ink*

[7] M. A. Fasoli, *Classification of Nilpotent Linear Spaces in* $\mathbb{M}(4; C)$, Comm. Algebra, 25, 1997.

[8] J. C. Faugére, *A new effcient algorithm for computing Gröbner bases (F4)* , Journal of Pure and Applied Algebra 139, 1999.

[9] F. Ferrari Ruffino, *Introdução à Geometria Algébrica*. Notas de aula, Depart.ufscar, 2023. *https : //drive.google.com/file/d/16mw*$_{W}$*QL9Sk3QPyOAzx1zUef*$_{B}$*8hfAjMa/view*

[10] J. C. Gutierrez Fernandez, A. Grishkov, Mary L. R. Montoya & Lucia S. I. Murakami, *Commutative Power-Associative Algebras of Nilindex Four*, Communications in Algebra, 2011.

[11] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer, New York, 1977.

[12] Zhevlakov, Konstantin Aleksandrovich *Rings that are nearly associative*, Academic press, 1982.