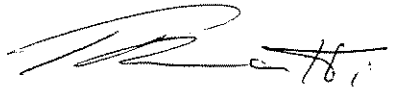
ALGUMAS APLICAÇÕES DE BASES DE GRÖBNER EM ÁLGEBRA COMUTATIVA

Este exemplar corresponde à redação final da dissertação devidamente corrigida por ADRIANA RAMOS e aprovada pela comissão julgadora.

Campinas, 25 de Abril de 2003.



.....

Prof. Dr. Paulo Roberto Brumatti
Orientador

Banca Examinadora

1 Prof. Dr. Arnaldo Leite Pinto Garcia
2 Prof. Dr. Paulo Roberto Brumatti
3 Prof. Dr. Plamen Emilov Koshlukov

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em MATEMÁTICA.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Ramos, Adriana

R147a Algumas aplicações de bases de Grobner em álgebra comutativa/Adriana Ramos -- Campinas, [S.P. :s.n.], 2003.

Orientador : Paulo Roberto Brumatti

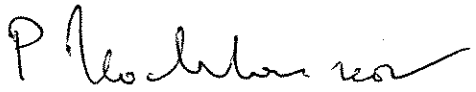
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1.Álgebra(Computadores). 2.Geometria algébrica. 3.Anéis polinominais . I. Brumatti, Paulo Roberto. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica.

Dissertação de Mestrado defendida em 27 de março de 2003 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof (a). Dr (a). PAULO ROBERTO BRUMATTI



Prof (a). Dr (a). PLAMEN EMILOV KOCHLOUKOV

Prof (a). Dr (a). ARNALDO LEITE PINTO GARCIA

Agradecimentos

À FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo), pelo apoio financeiro e institucional,

ao IMECC/Unicamp, em especial ao Prof. Dr. Marco Antonio Teixeira, por ter me concedido essa preciosa oportunidade de crescimento científico,

ao Prof. Dr. Paulo Roberto Brumatti, pela inestimável dedicação e generosidade com que me orientou em todos os momentos, acadêmicos e emocionais, desse projeto,

aos inesquecíveis professores de graduação da UFSCar, pela forma apaixonada com que me introduziram no estudo da Matemática,

aos amigos Renato e Lena, ao meu doce irmão Rodrigo e à minha querida companheira Fernanda, pelo amor e paciência, sem os quais eu jamais teria concluído essa empreitada,

e a todos aqueles que acreditaram em mim com seu incentivo, mesmo indiretamente, mesmo em silêncio, minha sincera gratidão.

Resumo

Nesta dissertação de mestrado, são discutidas algumas das principais idéias envolvidas em métodos computacionais algébricos. A importância desses métodos está na possibilidade de atacar temas clássicos em Álgebra Comutativa e Geometria Algébrica de uma maneira algorítmica, simplificando a abordagem e propiciando cálculos efetivos.
Nesse contexto, são estudados conceitos fundamentais em *bases de Gröbner* e suas propriedades.
Dentre as aplicações de *bases de Gröbner* em Álgebra Comutativa que são apresentadas aqui, destacam-se as provas computacionais para o *Lema da Normalização de Noether* e para o *Teorema de Quillen-Suslin.* Mais precisamente, são estudados o algoritmo que leva um dado ideal polinomial primo em sua posição normal de Noether e o algoritmo que calcula uma base livre para um dado módulo projetivo, sobre um anel de polinômios, apresentado como kernel, cokernel ou imagem de uma matriz polinomial.

Abstract

In this tese, some of the most important ideas envolved in algebraic computational methods are discussed. These methods importance resides in the possibilite of discussing classic themes in commutative algebra and algebraic geometry, in a algorithmic way, simplifying the studies and propitiating efective calculus.
In this context, fundamental topics in *Gröbner bases* and the respective proprieties are studied.
Between the *Gröbner bases* aplications that are shown in this work, the most important are the computational proofs of the *Noether Normalization Lemma* and of the *Quillen-Suslin Theorem.* Especiffically, the algorithm which puts a prime polynominal ideal into Noether normal position and the algorithm for computing a free basis of a projective module, over a polynomial ring, which is presented as the image, kernel, or cokernel of a polynomial matrix are the subjects studied.

Sumário

Introdução

Nesta dissertação de mestrado serão apresentadas algumas propriedades e aplicações, já conhecidas, das chamadas *bases de Gröbner* em temas clássicos de Geometria Algébrica e Álgebra Comutativa.

A importância do método das bases de Gröbner é, essencialmente, possibilitar que questões relativas a módulos, sobre anéis de polinômios, sejam tratadas de maneira algorítmica e computacional.

Mais precisamente, será mostrado como utilizar bases de Gröbner na abordagem dos problemas a seguir (S denota o anel de polinômios a n variáveis $K[X_1, \ldots, X_n]$ sobre um corpo K):

Questão 1: *Elementos de um Ideal*
Dados geradores de um ideal I em S e um elemento qualquer f de S. Em que condições $f \in I$? (Geometricamente, quando a variedade afim $\mathcal{V}(I)$ está contida na hipersuperfície definida por f?) Em que condições $f \in Rad(I)$?

Questão 2: *Resolução de um Sistema de Equações Polinomiais*
Encontrar todos os zeros comuns em K^n de um dado ideal I em S. Geometricamente, determinar os pontos de $\mathcal{V}(I)$.

Questão 3: *Implicitização*
Se um subconjunto W de K^n é dado parametricamente por funções racionais, como determinar sua "representação implícita", isto é, como determinar os polinômios de S que definem a menor variedade que contém W?

Questão 4: *Interseção e Quociente de Ideais*
Dados conjuntos geradores de dois ideais em S, calcular geradores para o seu ideal interseção e seu ideal quociente.

Questão 5: *Fecho Projetivo*
Para K corpo algebricamente fechado. Dada uma variedade algébrica no espaço afim n-dimensional, calcular o ideal que define o seu fecho de Zariski no espaço projetivo n-dimensional.

Questão 6: *Cálculo de Syzygies*
Considerando módulos finitamente gerados sobre S. Dado um homomorfismo ϕ entre módulos livres, determinar um conjunto de geradores para seus syzygies, ou seja, encontrar um sistema de geradores para $ker(\phi)$.
Teorema dos Syzygies de Hilbert: Calcular uma resolução livre finita para um dado módulo.

As próximas questões consistem em dar provas construtivas para dois teoremas de grande importância em Álgebra Comutativa:

Questão 7: *Lema da Normalização de Noether*
Assumindo K infinito, encontrar a matriz de mudança de variáveis que leva um dado ideal primo de S em sua posição normal de Noether.

Questão 8: *Teorema de Quillen-Suslin*
Determinar uma base livre para um S-módulo P projetivo e finitamente gerado, quando P é apresentado como imagem, kernel ou cokernel de uma matriz com entradas em S.

Os seis primeiros problemas enunciados são tratados em livros-textos de Álgebra Comutativa Computacional (destacamos as exposições de Cox e O'Shea [2] e Eisenbud [3]). Suas respostas serão dadas nos Capítulos 2 e 3, onde apresentaremos conceitos introdutórios em bases de Gröbner.

No Capítulo 4, estudaremos o artigo matemático *Uma Prova Computacional do Lema da Normalização de Noether*, de Alessandro Logar [7], obtendo um algoritmo para a sétima questão proposta.

Finalmente, no Capítulo 5, discutiremos a Questão 8 através de um estudo do artigo *Algoritmos para o Teorema de Quillen-Suslin*, de Alessandro Logar e Bernd Sturmfels [8].

Inúmeros trabalhos utilizando métodos de bases de Gröbner vêm sendo desenvolvidos nas últimas décadas, enfatizando o valor do seu caráter computacional. O objetivo desta dissertação é discutir algumas das principais idéias envolvidas no método, procurando demonstrar o seu extraordinário potencial de aplicações.

Capítulo 1

Conceitos Básicos

Neste primeiro capítulo, faremos um breve comentário sobre alguns conceitos e resultados básicos em Álgebra Comutativa e Geometria Algébrica. Para introdução e detalhes da teoria clássica, nossa principal referência é o livro-texto de E. Kunz [6].

Aqui, $\mathbf{A}^n(L)$ (ou L^n) denota o espaço afim n-dimensional sobre o corpo L; K é um subcorpo de L; e $K[X_1, \ldots, X_n]$ é o anel de polinômios nas variáveis $X_1, \ldots, X_n$ com coeficientes em K.

1.1 Variedades Algébricas

Serão enunciadas as definições de variedades algébricas afins e projetivas, assim como algumas de suas propriedades básicas e sua relação com a teoria de ideais.

1.1.1 Variedades Algébricas Afins

Definição 1.1. *Um subconjunto V de $\mathbf{A}^n(L)$ é uma* **K-variedade algébrica afim** *se existem polinômios $f_1, \ldots, f_s$ em $K[X_1, \ldots, X_n]$ tais que V é o conjunto solução, em $\mathbf{A}^n(L)$, do sistema de equações*

$$f_i(X_1, \ldots, X_n) = 0 \qquad (i = 1, \ldots, s).$$

Nessas condições, dizemos que $f_1, \ldots, f_s$ são os polinômios que definem V; K é o *corpo de definição* de V, e L é o seu *corpo de coordenadas.*

Observação. K-variedades definidas por um único polinômio (não constante) são chamadas *K-hipersuperfícies.* Chamamos as hipersuperfícies em $\mathbf{A}^2(L)$ de *curvas algébricas planas.* Os chamados *cones afins* são as variedades algébricas afins cujos polinômios de definição são todos homogêneos. As *variedades lineares*, objetos de estudo da Álgebra Linear, são os cones afins definidos por polinômios homogêneos de grau 1.

Há uma ligação bastante natural entre variedades algébricas afins e ideais polinomiais: Para cada subconjunto V de $\mathbf{A}^n(L)$, define-se o *ideal de V*, denotado por $\mathcal{I}(V)$, como sendo

o conjunto dos polinômios f em $K[X_1, \ldots, X_n]$ tais que $f(x) = 0$, para todo $x \in V$.
Para cada ideal I de $K[X_1, \ldots, X_n]$, define-se o *conjunto de zeros de* I, em $\mathbf{A}^n(L)$, denotado por $\mathcal{V}(I)$, como sendo o conjunto dos pontos x em $\mathbf{A}^n(L)$ tais que $f(x) = 0$, para todo $f \in I$.

Várias regras são obtidas relacionando as operações $\mathcal{I}$ e $\mathcal{V}$, por exemplo:
(a) para todo conjunto $V \subset \mathbf{A}^n(L)$, $\mathcal{I}(V)$ é um ideal radical, isto é, se o radical é denotado por *Rad*, temos $\mathcal{I}(V) = Rad(\mathcal{I}(V))$;
(b) se V é uma variedade algébrica, $\mathcal{V}(\mathcal{I}(V)) = V$;
(c) para quaisquer variedades V_1 e V_2, $V_1 \subset V_2$ se e somente se $\mathcal{I}(V_1) \supset \mathcal{I}(V_2)$;
(d) para quaisquer variedades V_1 e V_2, $\mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$ e $V_1 \cup V_2 = \mathcal{V}(\mathcal{I}(V_1) \cdot \mathcal{I}(V_2))$;
(e) para toda família $\{V_\lambda\}_{\lambda \in \Lambda}$ de variedades, $\bigcap_{\lambda \in \Lambda} V_\lambda = \mathcal{V}(\sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda))$.

No caso em que o corpo de definição L é algebricamente fechado, em particular infinito, a proposição seguinte torna-se bastante conveniente e decorre basicamente das definições.

Proposição 1.2. *Se L é um corpo infinito e $n \geq 1$, então fora de qualquer hipersuperfície em $\mathbf{A}^n(L)$ existem infinitos pontos de $\mathbf{A}^n(L)$. Se L é algebricamente fechado e $n \geq 2$, então qualquer hipersuperfície em $\mathbf{A}^n(L)$ é um conjunto infinito.*

Lembramos que um anel R é *Noetheriano* se, para toda cadeia

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$$

de ideais em R, existe j com $I_j = I_n$ para cada $n \geq j$; ou seja, se toda cadeia ascendente de ideais em R é *estacionária*. Equivalentemente, R é Noetheriano se todo ideal em R é gerado por um conjunto finito.

Proposição 1.3. **(Teorema da Base de Hilbert)**
Se R é um anel Noetheriano, então o anel de polinômios $R[X]$ também o é.

Uma prova construtiva para a proposição acima será apresentada no Teorema 2.8 do próximo capítulo.

Do Teorema da Base de Hilbert segue, por indução, que $K[X_1, \ldots, X_n]$ é anel Noetheriano. Com isso, tem-se que $\mathcal{V}(I)$ é uma K-variedade algébrica afim, para todo ideal I de $K[X_1, \ldots, X_n]$. Verifica-se, então, que uniões finitas e interseções quaisquer de K-variedades algébricas afins em $\mathbf{A}^n(L)$ são também K-variedades algébricas afins.
Assim, pode-se tomar as K-variedades como sendo os conjuntos fechados de uma topologia em $\mathbf{A}^n(L)$: a **topologia de Zariski** em $\mathbf{A}^n(L)$ com relação a K.

Considerando as variedades algébricas afins $V \subset \mathbf{A}^n(L)$ com a topologia de Zariski induzida de $\mathbf{A}^n(L)$, chega-se ao resultado que garante a decomposição de V em componentes irredutíveis.

Definição 1.4. *Seja X um espaço topológico. X é chamado* **irredutível** *se para qualquer decomposição da forma $X = A_1 \cup A_2$, com A_i $(i = 1, 2)$ subconjunto fechado de X, tem-se $X = A_1$ ou $X = A_2$. Uma* **componente irredutível** *de X é um subconjunto irredutível maximal de X.*

Um espaço topológico é dito ser *Noetheriano* se qualquer cadeia descendente de conjuntos fechados de X é estacionária. Do Teorema da Base de Hilbert segue, usando as operações $\mathcal{I}$ e $\mathcal{V}$, que toda variedade algébrica afim (munida da topologia de Zariski) é um espaço topológico Noetheriano.

Proposição 1.5. *Seja X um espaço topológico Noetheriano. Então, X possui no máximo uma quantidade finita de componentes irredutíveis, digamos, $X_1, \ldots, X_m$.*
Tem-se $X = X_1 \cup \ldots \cup X_m$, e nesta representação nenhuma componente X_i é "supérflua".

O Teorema dos Zeros de Hilbert deixa ainda mais estreita a ligação entre variedades algébricas e ideais polinomiais, dando uma condição necessária e suficiente para a resolvibilidade de um sistema de equações algébricas.

Teorema 1.6. **(Teorema dos Zeros de Hilbert)**
Se L é um corpo algebricamente fechado e I é um ideal de $K[X_1, \ldots, X_n]$, com $I \neq K[X_1, \ldots, X_n]$, então $\mathcal{V}(I) \neq \emptyset$.

O resultado acima será provado no Capítulo 2, Teorema 2.27.
Podemos, ainda, enunciá-lo da seguinte maneira: se L é algebricamente fechado, então a associação $V \longmapsto \mathcal{I}(V)$ define uma bijeção entre o conjunto de todas as K-variedades $V \subset \mathbf{A}^n(L)$ sobre o conjunto de todos os ideais I de $K[X_1, \ldots, X_n]$ tais que $\mathrm{Rad}(I) = I$.
Para todo ideal I de $K[X_1, \ldots, X_n]$, $\mathrm{Rad}(I) = \mathcal{I}(\mathcal{V}(I))$.
Nota-se que as variedades irredutíveis correspondem-se com os ideais primos.

Definição 1.7. *Para uma K-variedade $V \subset \mathbf{A}^n(L)$, o anel quociente $K[X_1, \ldots, X_n]/\mathcal{I}(V)$, denotado por $K[V]$, é chamado o* **anel de coordenadas de** V.

Uma *função polinomial em V* é por definição uma função polinomial de $\mathbf{A}^n(L)$ em L, com coeficientes em K, restrita a V. Assim, cada elemento de $K[V]$ é identificado por uma função polinomial em V. Para $I \subset K[V]$ e para $W \subset V$ pode-se definir, naturalmente, o *conjunto de zeros* $\mathcal{V}_V(I)$ de I em V e o *ideal* $\mathcal{I}_V(W)$ de W em $K[V]$.
Considerando $V \subset \mathbf{A}^n(L)$ uma K-variedade qualquer, verifica-se a versão mais geral do Teorema dos Zeros de Hilbert, em $K[V]$.

Spectrum de um Anel

Uma variedade algébrica V em $\mathbf{A}^n(K)$ é irredutível se, e somente se, $\mathcal{I}(V)$ é um ideal primo de S. Se K é algebricamente fechado então, usando as operações $\mathcal{I}$ e $\mathcal{V}$, vemos que: todo ideal radical I em S pode ser escrito de forma única como uma interseção finita de ideais primos $I = P_1 \cap \ldots \cap P_r$, com $P_i \not\subset P_j$ sempre que $i \neq j$; além disso, todo ideal maximal de S é gerado por n polinômios $X_1 - a_1, \ldots, X_n - a_n$, com $a_1, \ldots, a_n \in K$, ou seja, existe uma correspondência biunívoca entre os pontos de V e os ideais maximais do seu anel de coordenadas $K[V]$.

Tais resultados motivam uma generalização do conceito de variedades afins em um anel comutativo qualquer, estreitando ainda mais a ligação do estudo da teoria de anéis com o da geometria algébrica.

Definição 1.8. *Para um anel R, o* **spectrum de** R, *$Spec(R)$, é definido pelo conjunto de todos os ideais primos $\mathcal{P}$ de R, $\mathcal{P} \neq R$.*

Se I é um ideal de R, então o conjunto $\mathcal{V}(I)$ de todos os $\mathcal{P} \in Spec(R)$ com $\mathcal{P} \supset I$ é o *conjunto de zeros* de I em $Spec(R)$. Um subconjunto $A \subset Spec(R)$ é dito *fechado* se existe um ideal I de R com $A = \mathcal{V}(I)$.

Os conjuntos $\mathcal{V}(I)$, com I varrendo todo o conjunto dos ideais de R, formam os fechados de uma topologia em $Spec(R)$, a *topologia de Zariski* em $Spec(R)$.

Se A é um subconjunto qualquer de $Spec(R)$, o conjunto $\mathcal{I}(A)$ interseção de todos os primos $\mathcal{P} \in A$ é o *ideal de A* em R.

Com a notação acima, tem-se um resultado análogo ao Teorema dos Zeros de Hilbert, em um anel R qualquer: *Para qualquer ideal I em R, $\mathcal{I}(\mathcal{V}(I)) = Rad(I)$. Os subconjuntos fechados de $Spec(R)$ correspondem-se bijetivamente com os ideais radicais de R, e essa correspondência inverte o sentido das inclusões. Além disso, os subconjuntos fechados irredutíveis em $Spec(R)$ correspondem-se com os ideais primos de R.*

1.1.2 Variedades Algébricas Projetivas

O *espaço projetivo n-dimensional* sobre um corpo L, denotado por $\mathbf{P}^n(L)$, é o conjunto de todas as "retas" em L^{n+1} que passam pela origem.

Um ponto $x \in \mathbf{P}^n(L)$ pode ser representado por uma $(n+1)$-upla $(x_0, x_1, \ldots, x_n) \neq (0, \ldots, 0)$ em L^{n+1}, e $(x'_0, x'_1, \ldots, x'_n) \in L^{n+1}$ define o mesmo ponto se, e somente se, $(x'_0, x'_1, \ldots, x'_n) = \lambda(x_0, x_1, \ldots, x_n)$, para algum $\lambda \in L$, $\lambda \neq 0$. Uma $(n+1)$-upla $(x_0, x_1, \ldots, x_n)$ representando x é chamada um *sistema de coordenadas homogêneas* de x. Denota-se $x = (x_0 : x_1 : \ldots : x_n)$.

Definição 1.9. *Um subconjunto V de $\mathbf{P}^n(L)$ é uma K-***variedade algébrica projetiva** *se existem polinômios homogêneos $F_1, \ldots, F_m$ em $K[X_0, X_1, \ldots, X_n]$ tais que V é o conjunto solução, em $\mathbf{P}^n(L)$, do sistema de equações*

$$F_i(X_0, X_1, \ldots, X_n) = 0 \qquad (i = 1, \ldots, m).$$

Uma das vantagens em trabalhar no espaço projetivo é a existência de resultados a respeito da interseção de variedades, mais fortes do que no caso afim.

Proposição 1.10. *Se L é algebricamente fechado e $n \geq 2$, então:*
a) uma variedade linear de dimensão $d \geq 1$ e uma hipersuperfície projetiva sempre têm interseção não-nula;
b) duas hipersuperfícies projetivas sempre têm ponto em comum.

É conveniente recordar a definição de um anel graduado.

Definição 1.11. *Uma* **graduação** *de um anel G é uma família $\{G_k\}_{k \in \mathbf{Z}}$ (onde $\mathbf{Z}$ denota o anel dos números inteiros) de subgrupos G_k do grupo $(G, +)$ tal que*
(i) $G = \oplus_{k \in \mathbf{Z}} G_k$,
(ii) $G_i . G_j \subset G_{i+j}$, para quaisquer $i, j \in \mathbf{Z}$.

G é chamado um *anel graduado* se ele é munido de uma graduação $\{G_k\}_{k\in\mathbf{Z}}$. Se $G_k = 0$ para $k < 0$, G é chamado *positivamente graduado*. Os elementos de G_k são os *elementos homogêneos de grau* k de G. Se $g \in G$ é escrito como $g = \sum_{k\in\mathbf{Z}} g_k$ ($g_k \in G_k$), g_k é chamado a *componente homogênea* de grau k de g.

Dessa forma, vemos que qualquer anel polinomial $G = R[X_1, \ldots, X_n]$ sobre um anel R é positivamente graduado. Os elementos homogêneos de grau k são os polinômios homogêneos de grau k:

$$\sum_{\alpha_1+\ldots+\alpha_n=k} \rho_{\alpha_1\ldots\alpha_n} X_1^{\alpha_1} \ldots X_n^{\alpha_n}.$$

Um ideal de um anel graduado é chamado *ideal homogêneo* se ele possui um conjunto gerador formado apenas por elementos homogêneos. Assim, um ideal I em um anel graduado $G = \oplus_{k\in\mathbf{Z}} G_k$ é homogêneo se, e somente se, $I = \oplus_{k\in\mathbf{Z}} (I \cap G_k)$.

Exatamente como no caso afim, para uma K-variedade projetiva V em $\mathbf{P}^n(L)$, define-se o ideal de V, $\mathcal{I}(V) \subset K[X_0, X_1, \ldots, X_n]$, como sendo o conjunto de todos os polinômios que se anulam em todos os pontos de V. $\mathcal{I}(\emptyset)$ é, por definição, o ideal $(X_0, X_1, \ldots, X_n)$.
Se L é um corpo infinito, então $\mathcal{I}(V)$ é sempre um ideal homogêneo com $\mathcal{I}(V) = \mathrm{Rad}(\mathcal{I}(V))$.
O quociente $K[X_0, X_1, \ldots, X_n]/\mathcal{I}(V)$, denotado por $K[V]$, é chamado *anel de coordenadas homogêneas (ou projetivas) de* V. Esse anel é positivamente graduado e uma K-álgebra reduzida e Noetheriana.
Para qualquer ideal homogêneo $I \subset K[X_0, X_1, \ldots, X_n]$, o conjunto de zeros $\mathcal{V}(I)$ é definido como sendo o conjunto de todos os zeros comuns a todos os polinômios em I.

Uniões finitas e interseções quaisquer de K-variedades projetivas em $\mathbf{P}^n(L)$ são ainda K-variedades projetivas. Assim, as K-variedades projetivas são os fechados de uma topologia em $\mathbf{P}^n(L)$ (a *K-topologia de Zariski*).
Da mesma forma que no caso afim, toda K-variedade projetiva $V \subset \mathbf{P}^n(L)$ possui uma decomposição única em componentes irredutíveis. Se L é um corpo infinito, V é irredutível se e somente se $\mathcal{I}(V)$ é um ideal primo (homogêneo) de $K[X_0, X_1, \ldots, X_n]$.

É estabelecida uma bijeção entre o conjunto das variedades projetivas e o conjunto dos cones afins, do seguinte modo:
Para cada K-variedade projetiva $V \subset \mathbf{P}^n(L)$ associa-se o seu *cone afim* $\tilde{V}$, definido pelo conjunto de todos $(x_0, x_1, \ldots, x_n) \in \mathbf{A}^{n+1}(L)$, que aparecem como sistemas de coordenadas homogêneas de um ponto de V, acrescentado do ponto $(0, \ldots, 0)$ de $\mathbf{A}^{n+1}(L)$.

Com isso, observando que $\mathcal{I}(V) = \mathcal{I}(\tilde{V})$, chega-se ao Teorema dos Zeros de Hilbert para o caso projetivo:

Proposição 1.12. *Se L é algebricamente fechado, então: a aplicação $V \longmapsto \mathcal{I}(V)$ define uma bijeção entre o conjunto de todas as K-variedades $V \subset \mathbf{P}^n(L)$ sobre o conjunto de todos os ideais homogêneos $I \subset (X_0, \ldots, X_n)$ de $K[X_0, X_1, \ldots, X_n]$ tais que $Rad(I) = I$. A aplicação inversa é dada pela formação do conjunto de zeros.*
Para todo ideal homogêneo $I \neq K[X_0, X_1, \ldots, X_n]$ temos $Rad(I) = \mathcal{I}(\mathcal{V}(I))$.

Além da ligação, discutida acima, entre variedades projetivas e cones afins, o *fecho projetivo de uma variedade afim* estabalece maior conexão entre a geometria algébrica afim e a projetiva.

Considere o mergulho de $\mathbf{A}^n(L)$ em $\mathbf{P}^n(L)$ que a cada ponto $(x_1, \ldots, x_n)$ em $\mathbf{A}^n(L)$ associa $(1 : x_1 : \ldots : x_n) \in \mathbf{P}^n(L)$. Isso identifica $\mathbf{A}^n(L)$ com o complementar do hiperplano $X_0 = 0$, que é o chamado *hiperplano no infinito*, e seus pontos, os *pontos no infinito*.

Definição 1.13. *Para toda K-variedade $V \subset \mathbf{A}^n(L)$, o fecho $\bar{V} \subset \mathbf{P}^n(L)$ de V na K-topologia de $\mathbf{P}^n(L)$ é chamado o* **fecho projetivo** *de V. Os pontos de $\bar{V} \setminus V$ são os pontos no infinito de V.*

Se V é uma K-variedade afim dada pelo sistema de equações

$$F_i(X_1, \ldots, X_n) = 0 \qquad (i = 1, \ldots, m).$$

então, para cada i, considere o polinômio F_i^* "homogeneização" de F_i:

$$F_i^*(X_0, \ldots, X_n) \quad \stackrel{\text{def}}{=} \quad X_0^{degF_i} F_i\Big(\tfrac{X_1}{X_0}, \ldots, \tfrac{X_n}{X_0}\Big).$$

Se V^* é o conjunto solução em $\mathbf{P}^n(L)$ do sistema de equações homogêneas

$$F_i^*(X_0, \ldots, X_n) = 0 \qquad (i = 1, \ldots, m),$$

então $V^* \cap \mathbf{A}^n(L) = V$. Daí, $\bar{V} \cap \mathbf{A}^n(L) = V$.
Por outro lado, se uma K-variedade projetiva V é definida pelas equações homogêneas

$$F_i(X_0, \ldots, X_n) = 0 \qquad (i = 1, \ldots, m),$$

então $V_a \stackrel{\text{def}}{=} V \cap \mathbf{A}^n(L)$ é a K-variedade afim definida pelos polinômios

$$F_i(1, X_1, \ldots, X_n) = 0 \qquad (i = 1, \ldots, m),$$

(Dizemos que $F_i(1, X_1, \ldots, X_n)$ são obtidos dos polinômios homogêneos $F_i(X_0, X_1, \ldots, X_n)$ através da "desomogeneização" com relação a X_0).

Assim, *homogeneizando* polinômios em $K[X_1, \ldots, X_n]$ e *desomogeneizando* polinômios em $K[X_0, X_1, \ldots, X_n]$ com relação a X_0, vemos que a K-topologia de $\mathbf{A}^n(L)$ é a K-topologia relativa de $\mathbf{P}^n(L)$.

Notando que um subconjunto de um espaço topológico é irredutível se, e somente se, seu fecho o é, vemos que: Para qualquer variedade V em $\mathbf{A}^n(L)$, V é irredutível se, e somente se, seu fecho projetivo $\bar{V}$ é uma variedade irredutível em $\mathbf{P}^n(L)$. Se $V = V_1 \cup \ldots \cup V_m$ é a decomposição de V em componentes irredutíveis, então $\bar{V} = \bar{V}_1 \cup \ldots \cup \bar{V}_m$, onde $\bar{V}_i$ é o fecho projetivo de V_i, é a decomposição de $\bar{V}$ em componentes irredutíveis.
Para qualquer variedade projetiva irredutível $V^* \subset \mathbf{P}^n(L)$ que não está inteiramente contida no hiperplano no infinito $X_0 = 0$, $V^* = \bar{V}_a^*$.
Dessa forma, *a aplicação $V \longmapsto \bar{V}$, que a cada K-variedade $V \subset \mathbf{A}^n(L)$ associa seu fecho projetivo $\bar{V} \subset \mathbf{P}^n(L)$, é uma bijeção do conjunto de todas as K-variedades afins não vazias sobre o conjunto de todas as K-variedades projetivas que não possuem alguma de suas componentes irredutíveis inteiramente contida no hiperplano no infinito.*

Spectrum Homogêneo: Se $R = \bigoplus_{i\in\mathbf{Z}} R_i$ é um anel positivamente graduado, denotamos $\bigoplus_{i>0} R_i$ por R_+. O *spectrum homogêneo* de R, $Proj(R)$, é o conjunto de todos os ideais primos homogêneos $\mathcal{P}$ de R tais que $R_+ \not\subset \mathcal{P}$; dizemos que $Proj(R)$ é o conjunto dos *ideais primos relevantes* de R.

Como $Proj(R) \subset Spec(R)$, considera-se $Proj(R)$ com a topologia relativa de $Spec(R)$. No caso em que $R = K[V]$ para V uma K-variedade projetiva, da Proposição 1.12 segue que os ideais primos relevantes de R correspondem-se bijetivamente com as subvariedades irredutíveis não vazias de V.

1.2 Dimensão

A partir de um conceito mais geral de dimensão, será apresentada uma medida natural para o "tamanho" de uma variedade algébrica.

Nesta seção, ao se falar de uma K-variedade, o seu corpo de coordenadas L será assumido algebricamente fechado.

Definição 1.14. *A* **dimensão de Krull** *de um espaço topológico $X \neq \emptyset$, dim X, é o supremo dos comprimentos n de todas as cadeias*

$$X_0 \subset X_1 \subset \ldots \subset X_n \qquad (X_{i+1} \neq X_i)$$

dos subconjuntos não vazios $X_i \subset X$ fechados irredutíveis. Se $Y \subset X$ é fechado e irredutível, $Y \neq \emptyset$, a codimensão de Y, $codim_X Y$, é o supremo de todas as cadeias da forma acima com $X_0 = Y$.
A dimensão de Krull de um anel R, dim R, é definida como sendo a dimensão de $Spec(R)$. Ou seja, para $R \neq \{0\}$, dim R é o supremo dos comprimentos n de todas as cadeias de ideais primos

$$\mathcal{P}_0 \subset \mathcal{P}_1 \subset \ldots \subset \mathcal{P}_n \qquad (\mathcal{P}_{i+1} \neq \mathcal{P}_i)$$

em $Spec(R)$. A altura $h(\mathcal{P})$ de $\mathcal{P} \in Spec(R)$ é o supremo dos comprimentos de todas as cadeias da forma acima com $\mathcal{P} = \mathcal{P}_n$. Para um ideal qualquer $I \neq R$, a altura $h(I)$ é definida como sendo o ínfimo das alturas dos divisores primos de I. Além disso, a dimensão do ideal I, dim I, é a dimensão do anel R/I.

Observa-se que *dim V = dim $K[V]$*, para $V \subset \mathbf{A}^n(L)$ uma K-variedade afim; e *dim$V$ = dim $Proj(K[V])$*, para uma K-variedade projetiva $V \subset \mathbf{P}^n(L)$. Logo, o estudo da dimensão de variedades reduz-se ao estudo da dimensão de álgebras finitamente geradas sobre corpos (também chamadas *álgebras afins*).

Teorema 1.15. (Lema da Normalização de Noether)
Sejam A uma álgebra afim sobre um corpo K, $I \subset A$ um ideal, $I \neq A$. Existem números naturais $\delta \leq d$ e elementos $Y_1, \ldots, Y_d \in A$ tais que:
a) $Y_1, \ldots, Y_d \in A$ são algebricamente independentes sobre K.
b) A é finitamente gerada como um $K[Y_1, \ldots, Y_d]$-módulo.
c) $I \cap K[Y_1, \ldots, Y_d] = (Y_{\delta+1}, \ldots, Y_d)$.
Se K é infinito e $A = K[x_1, \ldots, x_n]$, então temos também
d) Para $i = 1, \ldots, \delta$, Y_i é da forma $Y_i = \sum_{j=1}^{n} a_{ij}x_j$, com $a_{ij} \in K$.

Veremos uma prova computacional para o teorema anterior no Capítulo 4.

Definição 1.16. *Para uma K-álgebra afim $A \neq \{0\}$, $K[Y_1, \ldots, Y_d] \subset A$ é uma* **Normalização de Noether** *se $Y_1, \ldots, Y_d$ são algebricamente independentes sobre K e A é finitamente gerada como um $K[Y_1, \ldots, Y_d]$-módulo.*

Do Teorema 1.15 e dos teoremas de Cohen-Seidenberg (*Going-up* e *Going-down*) seguem importantes resultados sobre a dimensão de álgebras afins e suas cadeias de ideais primos. O mais forte deles: *se $K[Y_1, \ldots, Y_d]$ em A é uma Normalização de Noether, então dim $A = d$.* Tais resultados são imediatamente aplicados no estudo da dimensão de variedades algébricas afins e suas cadeias de subvariedades irredutíveis.

Proposição 1.17. *Para toda K-variedade $V \subset \mathbf{A}^n(L)$, tem-se:*

a) dim V é independente da escolha do corpo de definição K.
b) dim $V \leq n$. E, dim $V = n$ se e somente se $V = \mathbf{A}^n(L)$.
c) Se todas as componentes irredutíveis de V têm a mesma dimensão e se $W \subset V$ é uma subvariedade irredutível, $W \neq \emptyset$, então

$$dim\ V = dim\ W + codim_V W.$$

d) $dim V = 0$ se, e somente se, V é um conjunto finito.
e) Suponha $K[V]$ fatorial, $W \subset V$, $\emptyset \neq W \neq V$. Todas as componentes irredutíveis de W têm codimensão 1 em V se, e somente se, o ideal $\mathcal{I}_V(W)$ de W em $K[V]$ é um ideal principal.

Considerando o mergulho $\mathbf{A}^n(L) \longrightarrow \mathbf{P}^n(L)$ dado na seção anterior e verificando que, para cada K-variedade afim $V \subset \mathbf{A}^n(L)$, $dim V = dim \bar{V}$, onde $\bar{V} \subset \mathbf{P}^n(L)$ é o fecho projetivo de V, os resultados sobre a dimensão de variedades afins são carregados para variedades projetivas.

Proposição 1.18. *Seja V uma K-variedade projetiva em $\mathbf{P}^n(L)$.*

a) dim $V \leq n$; além disso, dim $V = n$ se e somente se $V = \mathbf{P}^n(L)$.
b) Se $\tilde{V} \subset \mathbf{A}^{n+1}(L)$ é o cone afim de V, então

$$dim\ \tilde{V} = dim\ V + 1.$$

c) dim V é independente da escolha do corpo de definição K.
d) Se todas as componentes irredutíveis de V têm a mesma dimensão e se $W \subset V$ é uma subvariedade irredutível, então

$$dim\ V = dim\ W + codim_V W.$$

e) dim $V = 0$ se, e somente se, V possui somente um número finito de pontos.
f) V é uma hipersuperfície em $\mathbf{P}^n(L)$ se, e somente se, todas as suas componentes irredutíveis têm codimensão 1 em $\mathbf{P}^n(L)$.

Capítulo 2

Bases de Gröbner para Ideais Polinomiais

Neste capítulo serão estudados a ordenação entre os monômios de um anel polinomial, o algoritmo da divisão generalizada e o conceito de *base de Gröbner* para um ideal, procurando evidenciar seu caráter computacional através de suas propriedades básicas.
A teoria de bases de Gröbner foi construída pelo matemático austríaco Bruno Buchberger, em sua tese de doutorado de 1965 (o termo propriamente dito foi dado mais tarde, por Buchberger, como uma homenagem ao seu orientador Wolfgang Gröbner).

Como exemplos de aplicações serão tratadas, essencialmente, as cinco primeiras questões enunciadas na introdução desta dissertação: o problema de decidir se um polinômio pertence ou não a um dado ideal; a resolução de sistemas de equacões algébricas; a implicitização de um conjunto no espaço afim, dado parametricamente; o cálculo de interseções de ideais e de ideais quociente; o fecho projetivo de uma variedade afim.

Aqui, S sempre denota o anel de polinômios $K[X_1, \ldots, X_n]$ a n variáveis com coeficentes no corpo K. Como S é um K-espaço vetorial, chamaremos os elementos de K de escalares.

2.1 Monômios e Ordenação monomial

Como será visto adiante, a idéia-chave das bases de Gröbner é simplificar a abordagem de qualquer questão em S reduzindo-a a questões relativas a **monômios**. Escrevemos os monômios de S indentificando-os com as n-uplas de números inteiros não negativos. Se $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}^n_{\geq 0}$, então denotaremos por X^α o monômio $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$.

Um ideal gerado por tais monômios é chamado **ideal monomial**. Dados $m \in S$ e um ideal monomial $M \subset S$ qualquer, é trivial que: $m \in M$ se, e somente se, m é divisível por algum dos monômios geradores de M.

As operações entre monômios são bem mais simples do que entre polinômios quaisquer; por exemplo, o cálculo imediato do *máximo divisor comum* e do *mínimo múltiplo comum*: se $\beta = (\beta_1, \ldots, \beta_n)$, então,

$$MDC(X^\alpha, X^\beta) = X_1^{min\{\alpha_1,\beta_1\}} X_2^{min\{\alpha_2,\beta_2\}} \ldots X_n^{min\{\alpha_n,\beta_n\}},$$
$$MMC(X^\alpha, X^\beta) = X_1^{max\{\alpha_1,\beta_1\}} X_2^{max\{\alpha_2,\beta_2\}} \ldots X_n^{max\{\alpha_n,\beta_n\}}.$$

Tais operações são naturalmente estendidas para **termos** em S, isto é, para monômios multiplicados por escalares.

Teorema 2.1. (Lema de Dickson)
Um ideal monomial $I = (X^\alpha \mid \alpha \in A \subset \mathbf{Z}^n_{\geq 0})$ *em* S *pode ser escrito na forma* $I = (X^{\alpha(1)}, \ldots, X^{\alpha(s)})$, *onde* $\alpha(1), \ldots, \alpha(s) \in A$.
Em particular, I *é finitamente gerado.*

Prova. (Por indução sobre o número n de variáveis.)
Se $n = 1$, então $I = (X^\alpha \mid \alpha \in A \subset \mathbf{Z}_{\geq 0})$. Se β é o menor elemento de A, então $I = (X^\beta)$ e, portanto, o teorema é válido.
Suponha $n > 1$ e o teorema válido para $n - 1$. Tome $X_1, \ldots, X_{n-1}, Y$ como sendo as variáveis; assim, os monômios em $K[X_1, \ldots, X_{n-1}, Y]$ podem ser escritos na forma $X^\alpha Y^m$, com $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbf{Z}^{n-1}_{\geq 0}$ e $m \in \mathbf{Z}_{\geq 0}$.
Seja $I \subset K[X_1, \ldots, X_{n-1}, Y]$ um ideal monomial. Considere então J como sendo o ideal de $K[X_1, \ldots, X_{n-1}]$ gerado pelos X^α tais que $X^\alpha Y^m \in I$, para algum $m \geq 0$. (J é a projeção de I sobre $K[X_1, \ldots, X_{n-1}]$). Da hipótese de indução segue que $J = (X^{\alpha(1)}, \ldots, X^{\alpha(s)})$, para certos $X^{\alpha(1)}, \ldots, X^{\alpha(s)}$ em J.
Pela construção de J, para cada $X^{\alpha(i)}$ existe $m_i \geq 0$ tal que $X^{\alpha(i)} Y^{m_i} \in$ I.
Seja $M = max\{m_i : 1 \leq i \leq s\}$; e tome $X^\beta Y^p \in I$ qualquer.
Se $M \leq p$ então é claro que $X^\beta Y^p \in (X^{\alpha(1)} Y^M, \ldots, X^{\alpha(s)} Y^M)$.
Se $0 \leq p \leq M - 1$, considere J_p o ideal de $K[X_1, \ldots, X_{n-1}]$ gerado pelos X^α com $X^\alpha Y^p$ em I. Da hipótese de indução, $J_p = (X^{\alpha_p(1)}, \ldots, X^{\alpha_p(s_p)})$. Logo, $X^\beta \in J_p$, o que implica $X^\beta Y^p \in (X^{\alpha_p(1)} Y^p, \ldots, X^{\alpha_p(s_p)} Y^p)$. Portanto, I é gerado por

$$X^{\alpha(i)} Y^M \qquad (i = 1, \ldots, s)$$

$$X^{\alpha_p(j)} Y^p \qquad (p = 1, \ldots, M-1) \quad (j = 1, \ldots, s_p)$$

E dessa forma o teorema está provado. □

Se $J \subset S$ é um ideal monomial, então o conjunto A de todos os monômios que não estão em J formam uma base para o K-espaço vetorial S/J. Como todo ideal monomial é descrito por um conjunto finito de monômios geradores, é algorítmico verificar se um monômio está em J: teste a divisibilidade por cada um dos monômios geradores de J.
Se I é um ideal qualquer de S, veremos no Teorema 2.5 uma maneira similar para obter uma base monomial de S/I.

Observamos que no algoritmo da divisão entre polinômios de uma variável e no método da eliminação de Gauss, para resolver sistemas de equações lineares, o ingrediente crucial é a ordenação entre os termos; isso é suficiente para despertar a necessidade de ordenar também os termos de S.

Definição 2.2. *Uma* **ordenação monomial** *em* S *é qualquer relação* $>$ *no conjunto dos monômios de* S, *ou equivalentemente em* $\mathbf{Z}^n_{\geq 0}$, *satisfazendo as seguintes condições:*
(i) $>$ *é uma ordenação total;*
(ii) se $X^\alpha > X^\beta$ *e* $X^\gamma \neq 1$, *então* $X^\alpha X^\gamma > X^\beta X^\gamma > X^\beta$.

Vale notar que qualquer ordem monomial em S é **Artiniana** (todo subconjunto não vazio possui um menor elemento). De fato, se X é um conjunto qualquer de monômios de S, o Lema de Dickson garante que o ideal gerado por X possui um conjunto finito Y $\subset$ X de geradores. Daí, o menor elemento de Y será o menor elemento de X, pois qualquer elemento de X é divisível por algum elemento de Y.

Vejamos alguns exemplos importantes de ordens monomiais. Escrevendo os multiíndices $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$, consideramos os monômios $u = X^\alpha$ e $v = X^\beta$.

Ordem Lexicográfica: $u >_{lex} v$ se $\alpha_i > \beta_i$ para o *primeiro* índice i com $\alpha_i \neq \beta_i$.

Ordem Lexicográfica Homogênea: $u >_{hlex} v$ se

$$\sum_{i=1}^n \alpha_i = |\alpha| > |\beta| = \sum_{i=1}^n \beta_i$$

ou

$$|\alpha| = |\beta| \text{ e } \alpha >_{lex} \beta.$$

Ordem Lexicográfica Homogênea Reversa: $u >_{hrlex} v$ se

$$|\alpha| > |\beta|$$

ou

$$|\alpha| = |\beta| \text{ e } \alpha_i < \beta_i \text{ para o } \textit{último} \text{ índice } i \text{ com } \alpha_i \neq \beta_i.$$

Notamos que nos três exemplos $X_1 > X_2 > \ldots > X_n$. A diferença entre as ordens lexicográficas homogênea e homogênea reversa está em monômios de mesmo grau total: a primeira dá maior "peso" ao *maior* expoente da *maior* variável, enquanto a reversa dá maior "peso" ao *menor* expoente da *menor* variável. Por exemplo,

$$X_1X_3 >_{hlex} X_2^2, \text{ enquanto que, } X_2^2 >_{hrlex} X_1X_3.$$

Definição 2.3. *Fixada uma ordem monomial em S, para cada um de seus polinômios não nulos $f = \sum a_\alpha X^\alpha$, definimos:*
- o **multigrau** *de f, $multideg(f)$, é o maior α dentre aqueles em que $a_\alpha \neq 0$;*
- o **monômio principal** *de f é $MP(f) = X^{multideg(f)}$;*
- o **coeficiente principal** *de f é $CP(f) = a_{multideg(f)}$;*
- o **termo principal** *de f é $TP(f) = CP(f) \cdot MP(f)$.*

Observe que $multideg(f \cdot g) = multideg(f) + multideg(g)$, para quaisquer polinômios f, g não nulos.

Usando a notação acima enunciamos propriedades características de lex, hlex e hrlex.

Proposição 2.4.
a) Se $TP_{lex}(f) \in K[X_m, \ldots, X_n]$ para algum m, então $f \in K[X_m, \ldots, X_n]$.
b) Se f é homogêneo e $TP_{hlex}(f) \in K[X_m, \ldots, X_n]$ para algum m, então $f \in K[X_m, \ldots, X_n]$.
c) Se f é homogêneo e $TP_{hrlex}(f) \in (X_m, \ldots, X_n)$ para algum m, então $f \in (X_m, \ldots, X_n)$.

Prova. Direta das definições. □

Para cada ideal I de S denotamos $TP(I) = (TP(f) \mid f \in I)$.

Teorema 2.5. *(Macaulay) Seja I um ideal qualquer de S. Para toda ordem monomial $>$ em S, o conjunto A de todos os monômios que não aparecem em $TP(I)$ formam uma K-base para S/I.*

Prova. Para mostrar que A é K-linearmente independente, basta notar que se existisse uma relação

$$f = \sum k_i u_i \in I, \text{ com } u_i \in A, \text{ dois a dois distintos, } 0 \neq k_i \in K,$$

então $TP(f) \in TP(I)$. Como $TP(f)$ é um dos $k_i u_i$, e u_i não aparece em $TP(I)$, chegaríamos a uma contradição.
Para provar que a imagem de A em S/I gera o K-espaço vetorial S/I, suporemos o contrário. Considere então o conjunto B, não vazio, de todos os polinômios tais que: não estão em I e suas imagens em S/I não são K-combinações lineares das imagens dos monômios de A. Tome $g \in B$ com termo principal mínimo. Se $TP(g) \in A$, então $g - TP(g) \in B$ com termo principal menor que g. Logo, $TP(g) \in TP(I)$, mas disso segue que existe $h \in I$ com $TP(h) = TP(g)$, chegando a $g - h \in B$ que também contraria a minimalidade de f. □

2.2 Algoritmo da Divisão em S

Uma das operações básicas e mais importantes com polinômios de uma variável é a "divisão com resto": dados polinômios f e $g \neq 0$, um algoritmo fornece uma expressão da forma $f = qg + r$, com $deg(f) = deg(qg)$ e $deg(r) < deg(g)$ (ou $r = 0$), onde o *resto da divisão* r é único. Estenderemos essa operação para polinômios de várias variáveis.

Teorema 2.6. **(Algoritmo da Divisão Generalizada)**
Fixada uma ordem monomial $>$ em S, para toda $F = [f_1, \ldots, f_s]$ s-upla ordenada de polinômios em S, cada $f \in S$ pode ser escrito como

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

com $q_i \in S$, e $r \in S$ tal que: $r = 0$ ou nenhum dos seus monômios está no ideal $(TP(f_1), \ldots, TP(f_s))$.
Dizemos que r é o **resto** *da divisão de f por F.*
Além disso, se $q_i f_i \neq 0$, então $multideg(f) \geq multideg(q_i f_i)$.

Prova. Existe um algoritmo para a obtenção de tais $q_1, \ldots, q_s, r$:
ENTRADA: $f_1, \ldots, f_s, f$
SAIDA: $q_1, \ldots, q_s,\ r$

$q_i := 0$ para cada $i = 1, \ldots, s;\ r := 0$
$p := f$

ENQUANTO $p \neq 0$ faça
    $i := 1$
    ocorredivisão := *falso*

ENQUANTO $i \leq s$ e *ocorredivisão* = *falso* faça

SE $TP(f_i)$ divide $TP(p)$ ENTÃO

$q_i := q_i + \frac{TP(p)}{TP(f_i)}$

$p := p - \frac{TP(p)}{TP(f_i)} \cdot f_i$

ocorredivisão := *verdadeiro*

CASO CONTRÁRIO $i := i + 1$

SE *ocorredivisão* = *falso* ENTÃO

$r := r + TP(p)$

$p := p - TP(p)$

Como o $multideg(p)$ decresce estritamente em cada um dos passos, o fato de $>$ ser Artiniana garante que necessariamente deve aparecer $p = 0$ e, assim, o algoritmo termina.
Observando a construção das variáveis $q_1, \ldots, q_s, r$ no algoritmo, fica claro que elas satisfazem a equação

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

Além disso, como todos os termos de q_i são da forma $\frac{TP(p)}{TP(f_i)}$, para algum valor da variável p, e $TP(p) \leq TP(f)$ em todos os estágios, vê-se que $multideg(q_i f_i) \leq multideg(f)$ sempre que $q_i f_i \neq 0$. □

Em $K[X_1]$, a unicidade do resto no algoritmo da divisão permite resolver o problema da pertinência de um dado polinômio a um certo ideal. Apenas com o algoritmo anterior, tal problema ainda não está resolvido em S, pois r não é necessariamente único (fixada uma ordem monomial, ele depende da ordenação da s-upla de divisores). Obviamente, $r = 0$ é condição *suficiente* para $f \in (f_1, \ldots, f_s)$, mas não é *necessária*, como mostra o exemplo a seguir.

Exemplo 2.7. *Considere* $f_1 = XY - 1$, $f_2 = X^2 + 1$ *e* $f = X^2Y + Y$ *em* $K[X, Y]$ *com a ordem lex* $X > Y$. *Pergunta:* $f \in (f_1, f_2)$*?*
Dividindo f pelo par ordenado $F = [f_1, f_2]$, o resultado é a expressão

$$f = X \cdot f_1 + 0 \cdot f_2 + (X + Y).$$

Apesar do resto $r = X + Y$ obtido nessa divisão ser diferente de zero, quando reordenamos os polinômios divisores fazendo $F = [f_2, f_1]$, obtemos

$$f = 0 \cdot f_1 + Y \cdot f_2 + 0,$$

donde segue que $f \in (f_1, f_2)$.

Como veremos na próxima seção , esse "defeito" do algoritmo da divisão em S é reparado quando a divisão é feita por bases de Gröbner.

2.3 Bases de Gröbner

Teorema 2.8. (**Teorema da Base de Hilbert**) *Todo ideal I de S é finitamente gerado.*

Prova. Se $I = \{0\}$, $I = (0)$. Fixe uma ordem monomial. Se I contém um polinômio não nulo, então considere o ideal $TP(I)$. Do Lema de Dickson segue a existência de $g_1, \ldots, g_t \in I$ tais que $TP(I) = (TP(g_1), \ldots, TP(g_t))$. Seja f um elemento qualquer de I. Dividindo f pela t-upla $[g_1, \ldots, g_t]$, obtemos $f = q_1 g_1 + \ldots + q_t g_t + r$ e, então, $r = f - (q_1 g_1 + \ldots + q_t g_t) \in I$. Se $r \neq 0$, $TP(r) \in TP(I) = (TP(g_1), \ldots, TP(g_t))$, o que implica $TP(r)$ divisível por algum $TP(g_i)$, contrariando as propriedades do resto da divisão. Logo, $r = 0$. Donde segue que $I = (g_1, \ldots, g_t)$. □

O conjunto de geradores dado na demonstração anterior é justamente o que chamamos de *base de Gröbner.*

Definição 2.9. *Fixada uma ordem monomial em S, um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal I de S é chamado uma* **base de Gröbner** *para I se*

$$TP(I) = (TP(g_1), \ldots, TP(g_t)).$$

Corolário 2.10. *Fixada uma ordem monomial, todo ideal I de S, $I \neq (0)$, possui uma base de Gröbner. Além disso, qualquer base de Gröbner é um conjunto gerador de I.*

Prova. Imediata da demonstração do Teorema 2.8. □

Vejamos uma boa propriedade das bases de Gröbner com relação ao algoritmo da divisão.

Proposição 2.11. *Sejam $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal I de S (fixada uma ordem monomial) e $f \in S$. Então, existe um único r em S tal que:*
(i) Nenhum termo de r é divisível por algum dos $TP(g_1), \ldots, TP(g_t)$.
(ii) Existe $g \in I$ com $f = g + r$.

Prova. A existência segue do algoritmo da divisão. Para provar a unicidade, considere r_1, r_2 satisfazendo as condições da proposição; por *(ii)*, temos que $r_1 - r_2 \in I$. Se $r_1 - r_2 \neq 0$ então $TP(r_1 - r_2) \in TP(I)$ e, como G é uma base de Gröbner, isso implica $TP(r_1 - r_2)$ divisível por pelo menos um dos $TP(g_i)$, contrariando a condição *(i)*. Portanto, $r_1 - r_2 = 0$. □

Dessa forma, vemos que o resto da divisão de f por G não depende da ordenação da t-upla G (nem da ordem monomial adotada).

Corolário 2.12. *Sejam $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal I de S (fixada uma ordem monomial qualquer) e $f \in S$. Então, para qualquer ordenação da lista de elementos de G, temos: $f \in I$ se, e somente se, o resto da divisão de f por G é zero.*

2.4 Algoritmo de Buchberger

Seguimos agora para o estudo de um algoritmo que calcula bases de Gröbner. Para isso, discutiremos as condições para que um dado conjunto gerador $\{g_1, \ldots, g_t\}$ de um ideal I em S seja uma tal base.
Pela definição, o que pode impedi-lo é a ocorrência de combinações lineares dos g_i, com coeficientes polinomiais, cujos termos principais não são divisíveis por pelo menos um dos $TP(g_i)$. Uma maneira disso acontecer é se os termos principais em uma combinação do tipo

$$aX^{\alpha}g_i - bX^{\beta}g_j \in I$$

cancelam-se, deixando apenas termos menores.

Definição 2.13. *Para $\{g_1, \ldots, g_t\} \subset S$ escreveremos, para cada par i, j:*

$$u_{ij} = \frac{MMC(MP(g_i), MP(g_j))}{TP(g_j)}$$

$$\sigma_{ij} = u_{ji}g_i - u_{ij}g_j$$

Tais σ_{ij}, chamados *s-polinômios*, são construídos para produzir cancelamentos de termos principais. Na verdade, o resultado a seguir mostra que todo cancelamento dos termos principais entre polinômios de mesmo multigrau vêm de cancelamentos desse tipo.

Lema 2.14. *Considere uma soma da forma $\sum_{i=1}^{t} c_i X^{\alpha(i)} g_i$, com c_i escalares e $\alpha(i) + multideg(g_i) = \delta$ sempre que $c_i \neq 0$. Se essa soma tem multigrau $< \delta$, então existem escalares c_{jk} tais que*

$$\sum_{i=1}^{t} c_i X^{\alpha(i)} g_i = \sum_{j<k} c_{jk} X^{\delta - \gamma_{jk}} \sigma_{jk},$$

onde $X^{\gamma_{jk}} = MMC(MP(g_j), MP(g_k))$. Além disso, cada $X^{\delta-\gamma_{jk}}\sigma_{jk}$ tem multigrau $< \delta$.

Prova. Seja $d_i = CP(g_i)$; então $c_i d_i = CP(c_i X^{\alpha(i)} g_i)$. Como, por hipótese, o multigrau de cada $c_i X^{\alpha(i)} g_i$ é igual a δ, e o multigrau da soma $\sum_{i=1}^{t} c_i X^{\alpha(i)} g_i$ é estritamente menor do que δ, temos $\sum_i c_i d_i = 0$.
Defina $p_i := \frac{X^{\alpha(i)} g_i}{d_i}$ $(CP(p_i) = 1)$. Considere então:

$\sum_{i=1}^{t} c_i X^{\alpha(i)} g_i = \sum_{i=1}^{t} c_i d_i p_i =$

$$= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \ldots +$$

$$+ (c_1 d_1 + \ldots c_{t-1} d_{t-1})(p_{t-1} - p_t) + (c_1 d_1 + \ldots + c_t d_t) p_t. \quad (1)$$

Seja $d_i X^{\beta(i)} = TP(g_i)$. Por hipótese, $\alpha(i) + \beta(i) = \delta$. Logo, $MP(g_i)$ divide X^{δ}, para todo i, o que implica $MMC(MP(g_j), MP(g_k)) := X^{\gamma_{jk}}$ divide X^{δ}, para todo j, k. Assim, chegamos a:

$$X^{\delta-\gamma_{ik}}\sigma_{jk} = \frac{X^{\alpha(j)}}{d_j} g_j - \frac{X^{\alpha(k)}}{d_k} g_k = p_j - p_k \quad (2)$$

Substituindo (2) em (1), e lembrando que $\sum_i c_i d_i = 0$, obtemos a soma desejada. Como p_j, p_k têm multigrau δ e coeficientes principais iguais a 1, $p_j - p_k = X^{\delta-\gamma_{ik}}\sigma_{jk}$ tem multigrau estritamente menor que δ. □

Com a notação anterior, temos:

Teorema 2.15. (Critério de Buchberger)
O conjunto gerador $G = \{g_1, \ldots, g_t\}$ do ideal I é uma base de Gröbner se, e somente se, para todos os pares $i < j$, o resto da divisão de σ_{ij} por G (listados em alguma ordem) é igual a zero.

Prova. ($\Rightarrow$) Se G é uma base de Gröbner então, como $\sigma_{ij} \in I$, o resto na divisão por G é zero, pelo Corolário 2.12.
($\Leftarrow$) Seja $f \in I = (g_1, \ldots, g_t)$ um polinômio não nulo. Precisamos mostrar que $TP(f)$ está em $(TP(g_1), \ldots, TP(g_t))$.
Considere todas as formas possíveis para escrever $f = \sum_{i=1}^{t} h_i g_i$, com $h_i \in S$. Para cada uma dessas expressões, seja $\delta = max\{m(i) \mid i = 1, \ldots, t\}$, onde $m(i) := multideg(h_i g_i)$. Assim, $multideg(f) \leq \delta$. Escolha a expressão para f tal que δ seja mínimo.
Se mostrarmos que $multideg(f) = \delta$ o teorema está provado, pois δ é igual a $multideg(h_i g_i)$, para algum i.
Suponha então que $multideg(f) < \delta$. Vamos escrever f da seguinte maneira:

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i =$$
$$= \sum_{m(i)=\delta} TP(h_i) g_i + \sum_{m(i)=\delta} (h_i - TP(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \qquad (3)$$

Todos os monômios que aparecem nas segunda e terceira somas da segunda linha têm multigrau $< \delta$. Logo, a suposição de $multideg(f) < \delta$ significa que a primeira soma também tem multigrau $< \delta$. Dessa forma, estamos nas condições do Lema 2.14, donde segue que

$$\sum_{m(i)=\delta} TP(h_i) g_i = \sum_{j,k} c_{jk} X^{\delta-\gamma_{jk}} \sigma_{jk}, \qquad (4)$$

onde $c_{jk} \in K$ e $X^{\gamma_{jk}} = MMC(MP(g_j), MP(g_k))$.
Como o resto da divisão de σ_{jk} por $g_1, \ldots, g_t$ é zero, cada σ_{jk} pode ser escrito na forma

$$\sigma_{jk} = \sum_{i=1}^{t} q_i^{(jk)} g_i,$$

onde $q_i^{(jk)} \in S$ e $multideg(q_i^{(jk)} g_i) \leq multideg(\sigma_{jk})$.
Multiplicamos essa expressão por $X^{\delta-\gamma_{jk}}$ para obter

$$X^{\delta-\gamma_{jk}} \sigma_{jk} = \sum_{i=1}^{t} p_i^{(jk)} g_i,$$

com $p_i^{(jk)} := X^{\delta-\gamma_{jk}} q_i^{(jk)}$. Então, $multideg(p_i^{(jk)} g_i) \leq multideg(X^{\delta-\gamma_{ik}} \sigma_{jk}) < \delta$ (essa última desigualdade é dada pelo Lema 2.14).
Usando a igualdade anterior na equação (4), chegamos a uma expressão da forma

$$\sum_{m(i)=\delta} TP(h_i) g_i = \sum_i h'_i g_i,$$

com $multideg(h'_i g_i) < \delta$.
Daí, substituindo em (3), obtemos

$$f = \sum_i h'_i g_i + \sum_{m(i)=\delta} (h_i - TP(h_i))g_i + \sum_{m(i)<\delta} h_i g_i.$$

Assim, encontramos uma expressão para f como combinação dos g_i em que todos os termos têm multigrau $< \delta$, o que contraria a minimalidade de δ. □

Com o dispositivo dado pelo Teorema 2.15 chegamos ao **Algoritmo de Buchberger**, que é considerado o alicerce da geometria algébrica computacional:

Teorema 2.16. *Seja $I = (f_1, \ldots, f_s) \neq (0)$ um ideal em S. Então, uma base de Gröbner para I pode ser construída, em um número finito de passos, pelo algoritmo a seguir:*

ENTRADA: $F = \{f_1, \ldots, f_s\}$
SAÍDA: uma base de Gröbner $G = \{g_1, \ldots, g_t\}$ *para* I *com* $F \subset G$

$G := F$
REPITA
    $G' := G$
    PARA *cada par* $i \neq j$ *em* G' FAÇA
        $h :=$ *o resto da divisão de* σ_{ij} *por* G'
        SE $h \neq 0$ ENTÃO $G := G \cup \{h\}$
ATÉ QUE $G = G'$

Prova. O Teorema 2.15 garante que o conjunto fornecido ao final desse procedimento é de fato uma base de Gröbner para I. Como o ideal gerado pelos termos principais de $g_1, \ldots, g_t$ está estritamente contido no ideal gerado pelos termos principais de $g_1, \ldots, g_t, h$, esse processo necessariamente termina após finitos passos. □

A versão do Algoritmo de Buchberger que apresentamos é bastante rudimentar, mas é suficiente para entender o seu funcionamento.

Observe que a base de Gröbner calculada é maior do que o necessário, contendo polinômios "supérfluos". Para G uma base de Gröbner de um ideal I, se $p \in G$ é tal que $TP(p) \in (TP(G \setminus \{p\}))$, então é claro que $G \setminus \{p\}$ será também uma base de Gröbner para I, e portanto podemos descartar p.

Definição 2.17. *Uma* **base de Gröbner minimal** *para um ideal polinomial I é uma base de Gröbner G para I com as seguintes propriedades:*
(i) $CP(p) = 1$ *para todo* $p \in G$;
(ii) $\forall p \in G$, $TP(p) \notin (TP(G \setminus \{p\}))$.

Infelizmente, um ideal pode ter várias bases de Gröbner minimais. Contudo, a unicidade é garantida se acrescentarmos condições mais fortes.

Definição 2.18. *Uma* **base de Gröbner reduzida** *para um ideal polinomial I é uma base de Gröbner G para I com as seguintes propriedades:*
(i) $CP(p) = 1$ *para todo* $p \in G$;
(ii) $\forall p \in G$, *nenhum monômio de* p *está em* $(TP(G \setminus \{p\}))$.

Proposição 2.19. *Seja* $I \neq 0$ *um ideal em* S. *Então, fixada uma ordem monomial,* I *tem uma única base de Gröbner reduzida.*

Prova. Seja G uma base de Gröbner minimal para I. Dizemos que $g \in G$ *é reduzido para* G se nenhum de seus monômios está em $(TP(G \setminus \{g\}))$. Assim, uma base de Gröbner é reduzida se todos os seus elementos são reduzidos.
Vale observar que se um elemento é reduzido para uma base de Gröbner minimal de I, o será também para qualquer outra que tenha os mesmos termos principais.
Tome $g \in G$, defina $\tilde{g}$ como sendo o resto da divisão de g por $G\setminus\{g\}$ e faça $\tilde{G} = (G\setminus\{g\})\cup\{\tilde{g}\}$. Note que, devido à propriedade (ii) de base de Gröbner minimal, na divisão de g por $G \setminus \{g\}$, $TP(g)$ necessariamente vai para o resto; logo, $TP(\tilde{g}) = TP(g)$, implicando que $TP(G) = TP(\tilde{G})$. Claramente $\tilde{G} \subset I$, então vemos que $\tilde{G}$ é uma base de Gröbner para I, e a minimalidade continua. Pela construção, $\tilde{g}$ é reduzido em $\tilde{G}$.
Se repitirmos o processo acima para um elemento de $\tilde{G}$, e assim sucessivamente, obteremos uma base de Gröbner em que todos os elementos são reduzidos. A base de Gröbner pode mudar na vez em que cada um dos elementos entra no processo, mas a observação feita anteriormente mostra que uma vez que o elemento foi reduzido, contunuará sendo, já que os termos principais não mudam. Dessa forma, obtemos uma base de Gröbner reduzida para I.
Para mostrar a unicidade, suponha que G e H sejam bases de Gröbner reduzidas para I. Em particular, G e H são bases de Gröbner minimais. Se $g \in G$ então existe $h \in H$ tal que $TP(g)$ é múltiplo de $TP(h)$; e, por sua vez, existe $g' \in G$ tal que $TP(h)$ é múltiplo de $TP(g')$; logo, $TP(g)$ é múltiplo de $TP(g')$. Como G é minimal, temos necessariamente $g = g'$. Assim, $TP(g)$ é múltiplo de $TP(h)$ e vice-versa (ambos com coeficiente 1), logo $TP(g) = TP(h)$. Repetindo o mesmo argumento tomando elementos de H, concluímos que G e H possuem exatamente os mesmos termos principais, ou seja, $TP(G) = TP(H)$.
Agora, se $g \in G$ e $h \in H$ são tais que $TP(g) = TP(h)$, mostraremos que $g = h$ e, portanto, a proposição estará provada.
Dividindo $g - h$ por G encontramos resto $r = 0$, já que $g - h \in I$. Notamos que ocorre um cancelamento dos termos principais em $g - h$ e os termos restantes não são divisíveis por qualquer um dos $TP(G) = TP(H)$, pois G e H são reduzidas. Isso mostra que $r = g - h$, daí, $g - h = 0$. □

Uma conseqüência da unicidade dada pela proposição acima é um **algoritmo para a igualdade de dois ideais**, ou seja, um algoritmo que permite identificar se dados conjuntos de polinômios geram ou não o mesmo ideal: fixada uma ordem monomial, os ideais gerados são iguais se, e somente se, eles têm a mesma base de Gröbner reduzida.

2.5 Teoria da Eliminação

Bases de Gröbner podem ser utilizadas como método computacional na resolução de sistemas de equações polinomiais quaisquer. Esse método é similar ao de *Gauss* para sistemas lineares.

Definição 2.20. *Dado $I = (f_1, \ldots, f_s) \subset S$, o* **k-ésimo ideal de eliminação** *de I é o ideal de $K[X_{k+1}, \ldots, X_n]$ definido por*

$$I_k = I \cap K[X_{k+1}, \ldots, X_n].$$

De forma imediata e excelente, as bases de Gröbner determinam os elementos de I_k.

Teorema 2.21. **(Teorema da Eliminação)**
Seja $I \subset S$ um ideal e seja G uma base de Gröbner para I, com relação à ordem lex $X_1 > \ldots > X_n$. Então, para cada $0 \leq k \leq n$, o conjunto

$$G_k = G \cap K[X_{k+1}, \ldots, X_n]$$

é uma base de Gröbner de I_k.

Prova. (Observe que $G_k = \emptyset$ se, e somente se , $I_k = 0$.) Fixe k entre 0 e n e suponha $G = \{g_1, \ldots, g_t\}$. Reenumerando quando necessário, podemos assumir que $G_k = \{g_1, \ldots, g_s\}$. É claro que $G_k \subset I_k$. Mostraremos que G_k gera o ideal I_k e, em seguida, usaremos o critério de Buchberger.
Inicialmente, observamos que para qualquer polinômio em I, o resto de sua divisão por G é zero, já que G é base de Gröbner. E mais: como $g_{s+1}, \ldots, g_t$ possuem termos envolvendo (efetivamente) uma das variáveis $X_1, \ldots, X_k$, e adotamos a ordem lex com $X_1 > \ldots > X_n$, seus termos principais devem envolver uma das variáveis $X_1, \ldots, X_k$ e, portanto, são maiores que qualquer monômio de $K[X_{k+1}, \ldots, X_n]$.
Seja $f \in I_k \subset I$ qualquer. Das observações que fizemos segue, efetuando a divisão de f por G, que:

$$f = h_1 g_1 + \ldots + h_s g_s + 0 \cdot g_{s+1} + \ldots + 0 \cdot g_t + 0.$$

Dessa forma, notamos que dividir qualquer polinômio em I_k por G é o mesmo que dividi-lo por G_k.
Para cada $1 \leq i < j \leq s$, $\sigma_{ij} \in I_k$ e, então, o resto da divisão de σ_{ij} por G_k é igual ao resto da divisão de σ_{ij} por G, que por sua vez, é igual a zero. Usando o Teorema 2.15, encerramos a prova. □

O teorema da Eliminação mostra que uma base de Gröbner com relação à ordem lex elimina a primeira variável, as duas primeiras variáveis, as três primeiras, e assim por diante. Esse fato terá diversas aplicações como exemplificaremos no final deste capítulo.

Estudando um método que permita resolver sistemas de equações polinomiais quaisquer de forma similar ao da eliminação de Gauss para sistemas lineares, temos preocupação com duas etapas:
1) *Eliminação:* eliminar sucessivamente as variáveis, chegando assim a equações mais simples;
2) *Extensão:* resolvida a equação com menos variáveis, ou seja, obtida uma *solução parcial*, estendê-la a uma *solução completa* do sistema original.

O teorema a seguir dá condições para essa segunda etapa do método. É suficiente nos concentrarmos na primeira variável.

A partir deste ponto, usaremos a notação introduzida no Capítulo 1 e, por simplicidade de exposição, assumimos $L = K$.

Teorema 2.22. (**Teorema da Extensão**)
Assumindo K um corpo algebricamente fechado, sejam $I = (f_1, \ldots, f_s)$ ideal de S e I_1 o seu primeiro ideal de eliminação. Para cada $1 \leq i \leq s$, escreva f_i na forma

$$f_i = g_i(X_2, \ldots, X_n){X_1}^{N_i} + \text{ termos com grau } < N_i \text{ em } X_1,$$

onde $N_i \geq 0$ e $g_i \in K[X_2, \ldots, X_n]$ é não nulo.
Suponha a existência de uma solução parcial $(a_2, \ldots, a_n) \in \mathcal{V}(I_1)$.
Se $(a_2, \ldots, a_n) \notin \mathcal{V}(g_1, \ldots, g_s)$, então existe $a_1 \in L$ tal que $(a_1, a_2, \ldots, a_n) \in \mathcal{V}(I)$.

Prova. A demonstração baseia-se na teoria clássica de *resultantes*, presente em livros-textos de introdução à Álgebra. Tendo em vista o nosso contexto, optamos por não apresentá-la aqui, indicando a exposição de Cox e O'Shea [2] para os detalhes. □

Corolário 2.23. *Seja $I = (f_1, \ldots, f_s) \subset S$, com K algebricamente fechado, e suponha que para algum i, f_i é da forma*

$$f_i = c{X_1}^N + \text{ termos com grau } < N \text{ em } X_1,$$

onde $c \in K$ é diferente de zero e $N > 0$. Se I_1 é o primeiro ideal de eliminação de I e $(a_2, \ldots, a_n) \in \mathcal{V}(I_1)$, então existe $a_1 \in K$ tal que $(a_1, a_2, \ldots, a_n) \in \mathcal{V}(I)$.

Veremos agora uma interpretação geométrica para os dois teoremas anteriores. A idéia-chave consiste no fato de um ideal de eliminação corresponder a uma projeção de uma variedade, sobre um subespaço de dimensão menor.

Seja $V = \mathcal{V}(f_1, \ldots, f_s) \subset K^n$ uma variedade algébrica afim qualquer. Vale lembrar que determinar os pontos de V é resolver o sistema de equações polinomiais $f_1 = \ldots = f_s = 0$. A eliminação das k primeiras variáveis em $I = (f_1, \ldots, f_s)$ relaciona-se com a eliminação das k primeiras coordenadas das n-uplas de V, como mostra o lema a seguir.

Lema 2.24. *Com a notação anterior, seja I_k o k-ésimo ideal de eliminação de I. Considere a projeção sobre as $n - k$ últimas coordenadas,*

$$\pi_k : K^n \longrightarrow K^{n-k}, \qquad (a_1, \ldots, a_n) \mapsto (a_{k+1}, \ldots, a_n).$$

Então, em K^{n-k}, temos $\pi_k(V) \subset \mathcal{V}(I_k)$.

Prova. Se $(a_{k+1}, \ldots, a_n) \in \pi_k(V)$ então $(a_1, \ldots, a_k, a_{k+1}, \ldots, a_n) \in V$, para certos $a_1, \ldots, a_k$ em K. Para cada $f \in I_k \subset I$, $f(a_1, \ldots, a_n) = 0$. Além disso, como f envolve apenas as variáveis $X_{k+1}, \ldots, X_n$, podemos escrever $f(a_{k+1}, \ldots, a_n) = f(a_1, \ldots, a_n) = 0$. Logo, $(a_{k+1}, \ldots, a_n) \in \mathcal{V}(I_k)$. □

Ora, os pontos de $\mathcal{V}(I_k)$ são exatamente aqueles que chamamos de soluções parciais. Usando o lema anterior, podemos então dizer que:

$$\pi_k(V) = \{\ (a_{k+1}, \ldots, a_n) \in \mathcal{V}(I_k) \mid \exists\ a_1, \ldots, a_k \in K \text{ com } (a_1, \ldots, a_n) \in V\ \}.$$

Ou ainda, $\pi_k(V)$ é o conjunto de soluções parciais que podem ser estendidas a soluções completas.

Teorema 2.25. *(K algebricamente fechado.) Dado $V = \mathcal{V}(f_1, \ldots, f_s) \subset K^n$, seja g_i como no Teorema 2.22. Se I_1 é o primeiro ideal de eliminação de $I = (f_1, \ldots, f_s) \subset S$ então temos a seguinte igualdade, em K^{n-1}:*

$$\mathcal{V}(I_1) = \pi_1(V) \cup (\mathcal{V}(g_1, \ldots, g_s) \cap \mathcal{V}(I_1)),$$

onde $\pi_1 : K^n \longrightarrow K^{n-1}$ é a projeção sobre as últimas $n-1$ coordenadas.

Prova. Uma inclusão é óbvia, pelo Lema 2.24. Para mostrar a outra, se $(a_2, \ldots, a_n) \in \mathcal{V}(I_1)$, com $(a_2, \ldots, a_n) \notin \mathcal{V}(g_1, \ldots, g_s)$, então segue do Teorema 2.22 que $(a_2, \ldots, a_n) \in \pi_1(V)$. □

Temos uma versão geométrica para o Corolário 2.23:

Corolário 2.26. *(K algebricamente fechado) Seja $V = \mathcal{V}(f_1, \ldots, f_s) \subset K^n$ e suponha que, para algum i, f_i é da forma*

$$f_i = cX_1^N + \text{ termos com grau } < N \text{ em } X_1,$$

onde $c \in K$ é não nulo e $N > 0$. Se I_1 é o primeiro ideal de eliminação para $I = (f_1, \ldots, f_s)$ em S então, em K^{n-1},

$$\pi_1(V) = \mathcal{V}(I_1),$$

onde π_1 é a projeção nas últimas $n-1$ coordenadas.

O *Teorema do Fecho* dá uma relação precisa entre $\pi_k(V)$ e $\mathcal{V}(I_k)$: *$\mathcal{V}(I_k)$ é o fecho de Zariski de $\pi_k(V)$, em K^{n-k}.* A prova desse teorema, assim como a de inúmeros outros resultados em Geometria Algébrica (ver Capítulo 1), segue do *Teorema dos Zeros de Hilbert.*

Teorema dos Zeros de Hilbert

Teorema 2.27. *Se K é um corpo algebricamente fechado e I é um ideal de $K[X_1, \ldots, X_n]$ com $\mathcal{V}(I) = \emptyset$, então $I = K[X_1, \ldots, X_n]$.*

Prova. Por indução sobre o número n de variáveis.
Para $n = 1$ é imediato, já que $K[X_1]$ é domínio de ideais principais e K é algebricamente fechado.
Suponha (hipótese de indução) que o teorema é válido para anéis polinomiais em $n-1$ variáveis. Seja $I = (f_1, \ldots, f_s)$ um ideal qualquer de $K[X_1, \ldots, X_n]$ com $\mathcal{V}(I) = \emptyset$. Podemos assumir que o grau total de f_1 é $N \geq 1$, pois do contrário não haveria nada a provar.
Considere agora a seguinte mudança linear de variáveis:

$$\begin{aligned} X_1 &= Y_1 \\ X_2 &= Y_2 + a_2 Y_1 \\ &\vdots \\ X_n &= Y_n + a_n Y_n, \end{aligned}$$

onde os escalares $a_2, \ldots, a_n$ ainda serão determinados.
Com isso, obtemos:
$f_1(X_1, \ldots, X_n) = f_1(Y_1, Y_2 + a_2 Y_1, \ldots, Y_n + a_n Y_n) =$

$$= c(a_2, \ldots, a_n) {Y_1}^N + \text{termos em que } Y_1 \text{ tem grau} < N,$$

Como K é por hipótese algebricamente fechado, em particular ele é infinito; então podemos escolher $a_2, \ldots, a_n$ tais que $c(a_2, \ldots, a_n) \neq 0$.
Com esse argumento, podemos assumir que f_1 tem a forma

$$f_1 = c {X_1}^N + \text{termos com grau} < N \text{ em } X_1,$$

onde c é um escalar não nulo. Desse modo estamos nas condições do Corolário 2.26, donde segue que: se $I_1 = I \cap K[X_2, \ldots, X_n]$ então $\pi_1(\mathcal{V}(I)) = \mathcal{V}(I_1)$, em K^{n-1}.
Como $\mathcal{V}(I) = \emptyset$, chegamos a $\mathcal{V}(I_1) = \pi_1(\emptyset) = \emptyset$; o que implica, pela hipótese de indução, que $I_1 = K[X_2, \ldots, X_n]$. Portanto, $1 \in I_1 \subset I$ e o teorema está provado. □

Observamos que $\{1\}$ é a (única) base de Gröbner reduzida para $K[X_1, \ldots, X_n]$, adotando qualquer ordem monomial. Com o teorema anterior, obtemos um **algoritmo para a consistência**, ou seja, para a questão da resolvibilidade de um dado sistema de equações polinomiais, quando K é algebricamente fechado: Dados $f_1 = \ldots = f_s = 0$, onde os $f_i's$ são polinômios em $K[X_1, \ldots, X_n]$, calcule uma base de Gröbner reduzida G para o ideal $(f_1, \ldots, f_s)$. Se $G = \{1\}$ o sistema não tem solução em K^n. Se $G \neq \{1\}$, $f_1, \ldots, f_s$ devem ter zeros comuns.

Teorema 2.28. (Teorema dos Zeros de Hilbert)
Se o corpo K é algebricamente fechado então, para todo ideal I em $S = K[X_1, \ldots, X_n]$, $\mathcal{I}(\mathcal{V}(I)) = Rad(I)$.

Prova. A inclusão $\mathcal{I}(\mathcal{V}(I)) \supset Rad(I)$ segue direta das operações $\mathcal{I}$, $\mathcal{V}$ e Rad.
Para provar a inclusão contrária, seja f um elemento qualquer de $\mathcal{I}(\mathcal{V}(I))$. Tome um conjunto gerador $\{f_1, \ldots, f_s\} \subset S$ de I e considere o ideal

$$J = (f_1, \ldots, f_s, 1 - Yf) \subset S[Y]$$

Afirmamos que $\mathcal{V}(J) = \emptyset$. Para justificar essa afirmação, seja $(a_1, \ldots, a_{n+1})$ um elemento qualquer de K^{n+1}.
Se $(a_1, \ldots, a_n) \in \mathcal{V}(I)$ então $f(a_1, \ldots, a_n) = 0$, já que $f \in \mathcal{I}(\mathcal{V}(I))$. Como f não depende da última variável, teremos $f(a_1, \ldots, a_n, a_{n+1}) = 0$ e portanto $(1 - Yf)(a_1, \ldots, a_n, a_{n+1}) \neq 0$.
Se $(a_1, \ldots, a_n) \notin \mathcal{V}(I)$ então $f_i(a_1, \ldots, a_n) \neq 0$, para algum i. Daí, como os f_i não dependem da última variável, $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$.
Assim, em qualquer dos casos possíveis, $(a_1, \ldots, a_n, a_{n+1})$ não é um zero comum para J e,

portanto, $\mathcal{V}(J) = \emptyset$.
Do Teorema 2.27 segue que $1 \in J$. Isto é,

$$1 = \sum_{i=1}^{s} p_i(X_1, \ldots, X_n, Y)\ f_i + q(X_1, \ldots, X_n, Y)(1 - Yf),$$

para certos $p_i,\ q \in S[Y]$.

Agora faça $Y = \frac{1}{f(X_1,\ldots,X_n)}$. Então a relação acima implica que

$$1 = \sum_{i=1}^{s} p_i(X_1, \ldots, X_n, 1/f) \cdot f_i$$

Multiplicando os dois lados dessa igualdade por f^N, com N suficientemente grande para cancelar todos os denominadores, chegamos a uma expressão

$$f^N = \sum_{i=1}^{s} A_i \cdot f_i\ ,$$

para certos polinômios $A_i \in S$. Donde segue que $f \in Rad(I)$. □

Voltemos agora ao Teorema do Fecho.

Lema 2.29. *Se $Z \subset K^n$, então $\mathcal{V}(\mathcal{I}(Z))$ é a menor variedade algébrica afim (com relação à inclusão) contendo Z.*

Prova. Seja $W \subset K^n$ uma variedade afim contendo Z; então $\mathcal{I}(W) \subset \mathcal{I}(Z)$ e, portanto, $W = \mathcal{V}(\mathcal{I}(W)) \supset \mathcal{V}(\mathcal{I}(Z))$. □

Teorema 2.30. *Assumindo K algebricamente fechado, sejam V a variedade $\mathcal{V}(f_1, \ldots, f_s)$ em K^n e $\pi_k : K^n \longrightarrow K^{n-k}$ a projeção sobre as últimas $n-k$ coordenadas.*
Se $I_k = (f_1, \ldots, f_s) \cap K[X_{k+1}, \ldots, X_n]$, então $\mathcal{V}(I_k)$ é o fecho de $\pi_k(V)$ em K^{n-k}, com relação à topologia de Zariski.

Prova. Usando o Lema 2.24, temos $\pi_k(V) \subset \mathcal{V}(I_k)$; e então o Lema 2.29 garante que $\mathcal{V}(I_k) \supset \mathcal{V}(\mathcal{I}(\pi_k(V)))$, restando provar a inclusão contrária.
Se $f \in \mathcal{I}(\pi_k(V)) \subset K[X_{k+1}, \ldots, X_n]$ então $f(a_{k+1}, \ldots, a_n) = 0$, para todo $(a_{k+1}, \ldots, a_n)$ em $\pi_k(V)$. Considerado como um elemento de S, certamente $f(a_1, \ldots, a_n) = 0$, para todo $(a_1, \ldots, a_n) \in V$.
Pelo Teorema 2.28, existe algum natural N tal que $f^N \in (f_1, \ldots, f_s)$. Como f não depende de $X_1, \ldots, X_k$, f^N também não depende e então temos $f^N \in I_k$. Logo, $f \in Rad(I_k)$.
Dessa forma, mostramos que $\mathcal{I}(\pi_k(V)) \subset Rad(I_k)$, donde segue que $\mathcal{V}(\mathcal{I}(\pi_k(V)))$ contém $\mathcal{V}(Rad(I_k)) = \mathcal{V}(I_k)$. □

2.6 Primeiras Aplicações

Encerramos este capítulo, dando respostas algorítmicas para algumas questões sobre ideais polinomiais e variedades algébricas. Com isso, começamos a demonstrar o caráter computacional das bases de Gröbner e o seu potencial de aplicações.

Pertinência a um Ideal

Dados $I = (f_1, \ldots, f_s)$ ideal e f polinômio em S. Determinar uma base para o K-espaço vetorial S/I. Calcular a imagem de f em S/I em termos dessa base. Se $f \in I$, calcular uma expressão para f como combinação linear dos geradores $f_1, \ldots, f_s$, com coeficientes em S. Como decidir se $f \in Rad(I)$?

A primeira parte do problema é resolvida pelo Teorema 2.5 e o algoritmo da divisão: escolha uma ordem monomial em S; entrando com os geradores $f_1, \ldots, f_s$ calcule uma base de Gröbner $G = \{g_1, \ldots, g_t\}$ para o ideal I. O conjunto dos monômios que não estão em $TP(I)$, ou seja, que não são divisíveis por algum dos $TP(g_i)$, formam uma base para S/I.

Para calcular a imagem de f em S/I: efetue a divisão de f por G. Como todos os termos do resto r não são divisíveis por algum dos $TP(g_i)$ e $f - r \in I$, r é justamente a única expressão da imagem de f em termos daquela base.

Se $f \in I$, o processo de divisão de f pela base de Gröbner G exibirá f como combinação dos g_i, pois o resto é zero. Por outro lado, o algoritmo de Buchberger produziu os g_i como combinação dos f_j. Então, substituindo uma combinação na outra, obtemos f como combinação linear dos geradores originais f_j.

Finalmente, daremos um algoritmo para decidir se o dado polinômio f está ou não no radical de I, $Rad(I)$.

Proposição 2.31. *Seja $I = (f_1, \ldots, f_s) \subset S$ um ideal. Então: $f \in Rad(I)$ se e somente se $1 \in J$, onde $J := (f_1, \ldots, f_s, 1 - Yf)$ é ideal em $S[Y]$.*

Prova. Das equações na prova do Teorema 2.28, vemos que $1 \in J$ implica $f \in Rad(I)$. Por outro lado, suponha que $f \in Rad(I)$, então $f^N \in I \subset J$ para algum N. Como $1 - Yf$ também está em J, temos que

$$1 = Y^N f^N + (1 - Y^N f^N) = Y^N f^N + (1 - Yf) \cdot (1 + Yf + \ldots + Y^{N-1} f^{N-1}) \in J.$$

E assim a prova está completa. □

Com o algoritmo da consistência (Teorema 2.27) e a proposição acima, chegamos imediatamente ao **algoritmo da pertinência ao radical**: adotando uma ordem monomial qualquer em S[Y], calcule a base de Gröbner reduzida para o ideal $(f_1, \ldots, f_s, 1 - Yf)$. Se o resultado for $\{1\}$, então $f \in Rad(I)$. Caso contrário, $f \notin Rad(I)$.

Apesar de não apresentá-lo nesta dissertação, é válido citar a existência de um algo-

ritmo para calcular os geradores do radical de um dado ideal, trabalho de Eisenbud, Huneke e Vasconcelos [4]. Tal algoritmo já encontra-se implementado no sistema computacional algébrico *Macaulay*.

Resolver Sistemas de Equações Polinomiais

Dado um sistema de equações polinomiais em S:

$$f_1(X_1, \ldots, X_n) = \ldots = f_s(X_1, \ldots, X_n) = 0$$

Encontrar seu conjunto solução (de zeros comuns) em K^n. Ou, equivalentemente, determinar os pontos de $\mathcal{V}(f_1, \ldots, f_s)$.

Adote a ordem lex com $X_1 > \ldots > X_n$, e calcule uma base de Gröbner $G = \{g_1, \ldots, g_t\}$ para o ideal $I = (f_1, \ldots, f_s)$.

Pelo teorema da Eliminação 2.21, $G \cap K[X_{k+1}, \ldots, X_n]$ é uma base de Gröbner para o k-ésimo ideal de eliminação $I_k = I \cap K[X_{k+1}, \ldots, X_n]$; o que garante uma eliminação de variáveis entre os polinômios de G.

Logo, o sistema dado é equivalente a $g_1 = \ldots = g_t = 0$, o qual envolve equações relativamente mais fáceis; em especial, se a última equação é de apenas uma variável!

Então, substituímos as soluções (parciais) obtidas nas outras equações do sistema e resolvemos para uma variável maior, e assim por diante. Vale notar que esse procedimento "voltar substituindo" é análogo ao método usado para resolver um sistema linear triangular.

O teorema da Extensão 2.22 nos dá condições suficientes (no caso do corpo K ser algebricamente fechado) para que uma solução parcial obtida possa ser estendida a uma completa. Apesar dele tratar somente o caso do primeiro ideal de eliminação, podemos usá-lo em todos os casos. Basta observar que I_2 é o primeiro ideal de eliminação de I_1, I_3 é o primeiro ideal de eliminação de I_2, e assim por diante.

Vejamos um exemplo clássico do funcionamento desse método, análogo ao "escalonamento". Sempre usamos o *software Macaulay* para os cálculos.

Exemplo 2.32. *Resolver em $\mathbf{C}^4$ o sistema de equações algébricas a seguir, onde $\mathbf{C}$ denota o corpo dos números complexos.*

$$(1) \qquad \begin{cases} xz - yw - z + 1 = 0 \\ yz + xw - w - 2 = 0 \\ y^2 + x^2 - 1 = 0 \\ z^2 + w^2 - 1 = 0 \end{cases}$$

(Veja aplicações em robótica, Cox e O'Shea [2].)

Calculando uma base de Gröbner para o ideal

$$I = (xz - yw - z + 1,\ yz + xw - w - 2,\ y^2 + x^2 - 1,\ z^2 + w^2 - 1),$$

adotando a ordem lex $x > y > z > w$, obtemos:

$$g_1 = x + z - 2w - 1,$$
$$g_2 = y - 2z - w,$$
$$g_3 = z - 2w - 5/2,$$
$$g_4 = w^2 + 2w + 21/20.$$

Assim, determinamos w por g_4, substituímos os valores encontrados em g_3 para obter os respectivos valores de z, em seguida substituímos em g_2, encontrando os de y e, finalmente, em g_1 para determinar x (obviamente, neste exemplo, todas as soluções parciais obtidas são estendidas a soluções completas).
Como os elementos da base de Gröbner têm os mesmos zeros comuns do sistema original, o conjunto solução do sistema (1) em $\mathbf{C}^4$ é então dado por:

$$w_1 = \tfrac{-10+i\sqrt{5}}{10}, \quad z_1 = \tfrac{5+2i\sqrt{5}}{10}, \quad y_1 = \tfrac{i\sqrt{5}}{2}, \quad x_1 = \tfrac{-25+4i\sqrt{5}}{10}$$
$$w_2 = \tfrac{-10-i\sqrt{5}}{10}, \quad z_2 = \tfrac{5-2i\sqrt{5}}{10}, \quad y_2 = \tfrac{-i\sqrt{5}}{2}, \quad x_2 = \tfrac{-25-4i\sqrt{5}}{10},$$

onde i é a unidade imaginária.

Encontrar as Equações Satisfeitas por dados Elementos de uma Álgebra Afim

Sejam o anel de polinômios $R := K[T_1, \ldots, T_m]$ e a álgebra afim R/I, onde $I = (h_1, \ldots, h_s)$ é certo ideal de R. Dados $f_1, \ldots, f_n \in R/I$ defina o homomorfismo

$$\varphi : S = K[X_1, \ldots, X_n] \longrightarrow R/I, \qquad X_i \mapsto f_i$$

Encontrar $ker(\varphi)$.

Considere o anel $Q := K[T_1, \ldots, T_m, X_1, \ldots, X_n]$. Para cada i, seja $F_i \in R$ cuja imagem em R/I é f_i e considere o ideal $H \subset Q$ descrito por

$$H = (h_1, \ldots, h_s)Q + (X_1 - F_1, \ldots, X_n - F_n).$$

Proposição 2.33. *$ker(\varphi) = H \cap S$.*

Prova. Considere a aplicação $\bar{\varphi} : Q \longrightarrow R$ associando $X_i \mapsto F_i$, $T_j \mapsto T_j$, e o ideal $J := (X_1 - F_1, \ldots, X_n - F_n)$ de Q. Obviamente, $J \subset ker(\bar{\varphi})$. Além disso, como cada X_i é igual, mod J, a um polinômio nas variáveis T_i, temos $ker(\bar{\varphi}) \subset J$.
Disso segue que o kernel da composição $Q \longrightarrow R \longrightarrow R/I$ é igual a H, e portanto o kernel da composição φ, $S \hookrightarrow Q \longrightarrow R \longrightarrow R/I$, é $H \cap S$. □

Pelo Teorema 2.21 e a proposição anterior obtemos um **algoritmo para determinar** $ker(\varphi)$: calcule uma base de Gröbner G para

$$H = (h_1, \ldots, h_s, X_1 - F_1, \ldots, X_n - F_n) \subset Q,$$

adotando a ordem lex com todos os T_i maiores que todos os X_i. Os elementos de G que não envolvem os T_i geram $ker(\varphi)$.

Implicitização (a versão geométrica do problema anterior)

Considere um conjunto no espaço afim K^n, com K corpo infinito, dado parametricamente pelas equações:

$$x_1 = \frac{f_1(t_1,\ldots,t_m)}{g_1(t_1,\ldots,t_m)} \ , \ \ldots \ , \ x_n = \frac{f_n(t_1,\ldots,t_m)}{g_n(t_1,\ldots,t_m)} \ , \tag{1}$$

onde os f_i e os $g_i \neq 0$ são polinômios em $K[t_1,\ldots,t_m]$.
Encontrar as equações em $S = K[x_1,\ldots,x_n]$ que definem o fecho de Zariski dessa parametrização.

Vale lembrar que a hipótese de K infinito permite identificar os polinômios com as funções polinomiais.

Geometricamente, pensamos na parametrização (1) como sendo a função

$$F : K^m \setminus W \longrightarrow K^n, \qquad F(t_1,\ldots,t_m) = \left(\frac{f_1(t_1,\ldots,t_m)}{g_1(t_1,\ldots,t_m)}, \ldots, \frac{f_n(t_1,\ldots,t_m)}{g_n(t_1,\ldots,t_m)} \right)$$

onde $W = \mathcal{V}(g_1 \cdots g_n)$.

Considere o anel de polinômios $R := K[y, t_1,\ldots,t_m, x_1,\ldots,x_n]$ e seja $g := g_1 \cdots g_n$ tal que $W = \mathcal{V}(g)$. Considere então o ideal

$$J := (g_1x_1 - f_1, \ldots, g_nx_n - f_n, 1 - gy) \subset R$$

e as aplicações

$$j : K^m \setminus W \longrightarrow K^{n+m+1},$$

$$(t_1,\ldots,t_m) \mapsto \left(\frac{1}{g(t_1,\ldots,t_m)}, t_1, \ldots, t_m, \frac{f_1(t_1,\ldots,t_m)}{g_1(t_1,\ldots,t_m)}, \ldots, \frac{f_n(t_1,\ldots,t_m)}{g_n(t_1,\ldots,t_m)} \right);$$

$$\pi_{m+1} : K^{n+m+1} \longrightarrow K^n,$$

$$(y, t_1,\ldots,t_m, x_1,\ldots,x_n) \mapsto (x_1,\ldots,x_n).$$

Assim, a composição $\pi_{m+1} \circ j$

$$K^m \setminus W \longrightarrow K^{n+m+1} \longrightarrow K^n$$

é igual a F, com $j(K^m \setminus W) = \mathcal{V}(J)$. Logo,

$$F(K^m \setminus W) = \pi_{m+1}(j(K^m \setminus W)) = \pi_{m+1}(\mathcal{V}(J))$$

Teorema 2.34. (Implicitização Racional)
Se K é um corpo infinito, seja $F : K^m \setminus W \longrightarrow K^n$ a função correspondente à parametrização racional (1). Considere o ideal

$$J = (g_1x_1 - f_1, \ldots, g_nx_n - f_n, 1 - gy) \text{ em } K[y, t_1,\ldots,t_m, x_1,\ldots,x_n],$$

em que $g = g_1 \cdots g_n$, e seja $J_{m+1} := J \cap K[x_1,\ldots,x_n]$ o $(m+1)$-ésimo ideal de eliminação de J.
Então, $\mathcal{V}(J_{m+1})$ é o fecho de Zariski de $F(K^m \setminus W)$ em K^n.

Prova. Considere um corpo L, algebricamente fechado, extensão de K. Se $K = L$, então a prova segue diretamente do Teorema 2.30.
No caso em que K está estritamente contido em L, denotaremos $\mathcal{V}_K$ e $\mathcal{V}_L$ o conjunto dos zeros em K^n e em L^n, respectivamente.
Pelo Lema 2.24, $F(K^m \setminus W) = \pi_{m+1}(\mathcal{V}_K(J)) \subset \mathcal{V}_K(J_{m+1})$.
Se $Z_K = \mathcal{V}_K(h_1, \ldots, h_s) \subset K^n$ é qualquer variedade algébrica afim de K^n contendo $F(K^m \setminus W)$, precisamos mostrar que Z_K contém $\mathcal{V}_K(J_{m+1})$.
Inicialmente, observamos que $h_i = 0$ em Z_K implica $h_i = 0$ no subconjunto $F(K^m \setminus W)$, e então $h_i \circ F = 0$ em $K^m \setminus W$, com $h_i \circ F \in K[t_1, \ldots, t_m]$.
Ou seja, cada $h_i \circ F$ é um polinômio que se anula em $K^m \setminus \mathcal{V}(g)$. Logo, $(h_i \circ F) \cdot g$ zera em todo K^m. Portanto, como K é infinito e $g \neq 0$, cada $h_i \circ F$ é o polinômio nulo.
Dessa forma, certamente os h_i zeram em $F(L^m)$. Isso significa que $Z_L = \mathcal{V}_L(h_1, \ldots, h_s)$ é uma variedade afim de L^m contendo $F(L^m)$. Como o teorema é válido em L, $\mathcal{V}_L(J_{m+1}) \subset Z_L$ em L^n.
Olhando para as soluções que estão em K^n, temos $\mathcal{V}_K(J_{m+1}) \subset Z_K$. □

Vale notar que $\mathcal{I}(\mathcal{V}(J_{m+1}))$ é um ideal primo e, portanto, $\mathcal{V}(J_{m+1})$ é uma variedade irredutível.

Com o teorema acima chegamos a um **algoritmo da implicitização para parametrizações racionais**: Dada uma parametrização da forma (1), considere o ideal

$$J = (g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy)$$

em $K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$. Calcule uma base de Gröbner G com relação à ordem lex, onde y e todos os t_i são maiores que todos os x_i.
Os elementos de G que não envolvem as variáveis $y, t_1, \ldots, t_m$ definem o fecho de Zariski em K^n do conjunto parametrizado na forma (1).

Observamos que para o caso particular de **parametrizações polinomiais**, basta considerar $(x_1 - f_1, \ldots, x_n - f_n)$ no lugar de J, sendo desnecessário o uso da variável y.

Exemplo 2.35. *Encontrar a representação implícita nos casos a seguir.*

a) *Em* $\mathbf{C}[x, y, z, w]$, *da parametrização*

$$\begin{cases} x = uv^2 \\ y = u^2 v \\ z = uv \\ w = v + 1 \end{cases} \tag{2}$$

Adotando a ordem lex $u > v > x > y > z$, calculamos uma base de Gröbner para o ideal

$$J = (x - uv^2,\ y - u^2 v,\ z - uv,\ w - v - 1) \subset \mathbf{C}[u, v, x, y, z, w],$$

obtendo:

$$g_1 = yw - y - z^2, \qquad g_2 = x - zw + z, \qquad g_3 = v - w + 1,$$
$$g_4 = uw - u - z, \qquad g_5 = uz - y.$$

Logo o ideal (primo) I em $\mathbf{C}[x,y,z,w]$ que define o fecho de Zariski da parametrização (2) é dado por

$$I = (yw - y - z^2,\ x - zw + z)$$

No Capítulo 4, calcularemos a matriz de mudança de variáveis que leva I em sua posição normal de Noether.

b) *Em* $\mathbf{C}[x,y,z]$, *da parametrização*

$$\text{(3)} \qquad \begin{cases} x = t^3 \\ y = t^4 \\ z = t^5 \end{cases}$$

Calculando uma base de Gröbner para o ideal

$$J = (x - t^3,\ y - t^4,\ z - t^5) \subset \mathbf{C}[t,x,y,z],$$

em relação à ordem lex $t > x > y > z$, obtemos:

$$\begin{array}{lll} g_1 = y^5 - z^4, & g_2 = xz - y^2, & g_3 = xy^3 - z^3, \\ g_4 = x^2y - z^2, & g_5 = x^3 - yz, & g_6 = tz - x^2, \\ g_7 = ty - z, & g_8 = tx - y, & g_9 = t^3 - x. \end{array}$$

Logo a representação implícita de (3) é a variedade em $\mathbf{C}^3$ definida pelo ideal (primo)

$$I = (y^5 - z^4, xz - y^2, xy^3 - z^3, x^2y - z^2, x^3 - yz) \subset \mathbf{C}[x,y,z].$$

Observação: Pode-se descartar polinômios da base acima chegando a um conjunto *minimal* de geradores para o ideal I (ou seja, um conjunto gerador que tem o menor número de elementos possível). Isso pode ser feito pelo *software Macaulay*, onde obtemos o sistema de geradores minimal formado por:

$$f_1 = x^3 - yz\ \ f_2 = y^2 - xz,\ \ f_3 = z^2 - x^2y.$$

Vendo I como o kernel do K-homomorfismo $\varphi : K[x,y,z] \longrightarrow K[t]$; $\varphi(x) = t^3$, $\varphi(y) = t^4$, $\varphi(z) = t^5$; notamos que a altura de I, $h(I)$, é igual a 2.
No anel $R := \mathbf{C}[x,y,z]/(f_3)$, $z^2 \equiv x^2y$. Com isso, temos

$${f_1}^2 \equiv x^2(x^4 - 2xyz + y^3) \bmod (f_3), \qquad {f_2}^2 \equiv y(x^4 - 2xyz + y^3) \bmod (f_3)$$

com $p := x^4 - 2xyz + y^3 \in I$, já que $x, y \notin I$ e I é primo.
Disso segue que $I = Rad(I) = Rad(p, f_3)$ e, portanto, I é um *conjunto-teórico interseção completa.* (Lembrando que esse nome é dado a todo ideal F, em um anel Noetheriano, que satisfaz a seguinte propriedade: *exitem* m *elementos* $a_1, \ldots, a_m$ *em* F, *onde* m *é sua altura* $h(F)$, *tais que* $Rad(F) = Rad(a_1, \ldots, a_m)$.) Observe ainda que I não é um *ideal-teórico interseção completa*, isto é, sua altura $h(I) = 2$ não é igual ao número de elementos $\mu(I) = 3$ de seu sistema minimal de geradores.

Veja, em [6], uma generalização do que foi discutido neste exemplo, para curvas parametrizadas na forma (3): $x = t^q, y = t^r, z = t^s$, com $MDC(q,r,s) = 1$. Todas essas curvas são conjuntos-teóricos interseção completa; e ainda, pode-se explicitar quais delas são ideais-teóricos interseção completa (tais curvas foram investigadas por Herzog [5]).

Interseção de Ideais

Dados os geradores dos ideais I e J em $S = K[X_1, \ldots X_n]$, calcular os geradores de $I \cap J$.

Para expressar que um polinômio g envolve as variáveis $X_1, \ldots, X_n$, escreveremos $g = g(X)$.

Lema 2.36.
(i) Se I é gerado, como um ideal de S, pelos polinômios $p_1(X), \ldots, p_r(X)$, então $f(t)I$ é gerado pelos polinômios $f(t) \cdot p_1(X), \ldots, f(t) \cdot p_r(X)$ em $S[t]$.
(ii) Se $g(X,t) \in f(t)I$ e c é um escalar, então $g(X,c) \in I$.

Prova. Segue diretamente da definição de conjunto gerador. □

Teorema 2.37. *Sejam I, J ideais de S e considere o ideal $tI + (1-t)J$ de $S[t]$. Então*

$$I \cap J = (tI + (1-t)J) \cap S.$$

Prova. Se $f \in I \cap J$ então $t \cdot f \in tI$ e $(1-t) \cdot f \in (1-t)J$.
Daí, $f = t \cdot f + (1-t) \cdot f \in tI + (1-t)J$. Como $I, J \subset S$, $f \in (tI + (1-t)J) \cap S$.
Para estabelecer a inclusão contrária, seja $f \in (tI + (1-t)J) \cap S$ qualquer. Então, $f(X) = g(X,t) + h(X,t)$ para certos $g(X,t) \in tI$ e $h(X,t) \in (1-t)J$.
Primeiro, faça $t = 0$ na expressão acima. Como todo elemento de tI é um múltiplo de t, temos que $g(X,0) = 0$. Com isso, chegamos a $f(X) = h(X,0)$ e da condição (ii) do lema segue que $f(X) \in J$.
Fazendo $t = 1$ em $f(X) = g(X,t) + h(X,t)$ e usando os mesmos argumentos, concluímos que $f(X) = g(X,1) \in I$.
Logo $f \in I \cap J$, o que completa a prova. □

Com o teorema acima e o Teorema 2.21 obtemos um **algoritmo para calcular interseções de ideais**: Se $I = (f_1, \ldots, f_r)$ e $J = (g_1, \ldots, g_s)$ são ideais de S, considere o ideal

$$(tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s) \subset S[t]$$

e calcule uma base de Gröbner G, adotando a ordem lex em que t é maior que todos os X_i. Os elementos de G que não envolvem a variável t formam uma base (de Gröbner) para o ideal interseção $I \cap J$.

Ideais Quociente e Saturação

Dados os sistemas de geradores de dois ideais em $S = K[X_1, \ldots, X_n]$, calcular os geradores do ideal quociente. Geometricamente: dadas as variedades algébricas afins V e W, calcular as equações que definem o fecho de Zariski da diferença, $\overline{W \setminus V}$.

Inicialmente, convém apresentar alguns detalhes dessa questão.

Proposição 2.38. *Se V e W são variedades algébricas com $V \subset W$, então*

$$W = V \cup (\overline{W \setminus V}).$$

Prova. Como $W \setminus V \subset W$, e $V \subset W$, devemos ter $V \cup (\overline{W \setminus V}) \subset W$. Por outro lado, se $x \in W$ então $x \in V$ ou $x \in W \setminus V \subset (\overline{W \setminus V})$. E portanto $x \in V \cup (\overline{W \setminus V})$. □

Teorema 2.39. *Sejam I, J ideais de S. Denotaremos o ideal quociente de I por J por $I : J = \{f \in S \mid fJ \subset I\}$. Então*

$$\mathcal{V}(I : J) \supset \overline{\mathcal{V}(I) \setminus \mathcal{V}(J)}.$$

Se K é algebricamente fechado e I é um ideal radical, $I = Rad(I)$, então

$$\mathcal{V}(I : J) = \overline{\mathcal{V}(I) \setminus \mathcal{V}(J)}.$$

Prova. Provaremos que $I : J \subset \mathcal{I}(\mathcal{V}(I) \setminus \mathcal{V}(J))$.
De fato, $f \in I : J$ implica $fg \in I$, para todo $g \in J$. Então, para $x \in \mathcal{V}(I) \setminus \mathcal{V}(J)$, $f(x)g(x) = 0$, para todo $g \in J$, e existe $g \in J$ com $g(x) \neq 0$. Logo $f(x) = 0$, ou seja, $f \in \mathcal{I}(\mathcal{V}(I) \setminus \mathcal{V}(J))$.
Para provar a segunda parte do teorema, supomos K algebricamente fechado e $I = Rad(I)$. Seja $x \in \mathcal{V}(I : J)$. Então,

$$hg \in I, \ \forall g \in J \ \Rightarrow \ h(x) = 0.$$

Considere $h \in \mathcal{I}(\mathcal{V}(I) \setminus \mathcal{V}(J))$ qualquer. Se $g \in J$, então hg anula-se em $\mathcal{V}(I)$. Pelo teorema dos Zeros de Hilbert, hg está em $Rad(I) = I$. Logo $hg \in I, \forall g \in J$, implicando $h(x) = 0$. E portanto $x \in \mathcal{V}(\mathcal{I}(\mathcal{V}(I) \setminus \mathcal{V}(J))$.
Assim, mostramos que $\mathcal{V}(I : J) \subset \overline{\mathcal{V}(I) \setminus \mathcal{V}(J)}$. □

Corolário 2.40. *Sejam V e W variedades em K^n. Então*

$$\mathcal{I}(V) : \mathcal{I}(W) = \mathcal{I}(V \setminus W)$$

Prova. Uma das inclusões segue direto do Teorema 2.39, fazendo $I = \mathcal{I}(V)$ e $J = \mathcal{I}(W)$. A outra, vem da definição de ideal quociente. □

Destacamos agora algumas das propriedades mais óbvias de ideais quociente.

Proposição 2.41. *Sejam I, J e H ideais de S. Então:*
(i) $I \subset I : J$
(ii) $I : S = I$
(iii) $IJ \subset H$ se, e somente se, $I \subset H : J$
(iv) $J \subset I$ se, e somente se, $I : J = S$

A proposição seguinte é útil para relacionar o quociente com as demais operações entre ideais.

Proposição 2.42. *Sejam I, I_i, J, J_i e H ideais de S, para $1 \leq i \leq r$. Então:*

(1) $\quad (\bigcap_{i=1}^{r} I_i) : J = \bigcap_{i=1}^{r} (I_i : J)$

(2) $\quad I : (\sum_{i=1}^{r} J_i) = \bigcap_{i=1}^{r} (I : J_i)$

(3) $\quad (I : J) : H = I : JH$

Denotamos $I : (f)$ por, simplesmente, $I : f$. E observamos um caso especial de (2):

(4) $\quad I : (f_1, \ldots, f_r) = \bigcap_{i=1}^{r} (I : f_i)$.

Teorema 2.43. *Seja I um ideal e g um elemento de S. Se $\{h_1, \ldots, h_p\}$ é um sistema gerador do ideal $I \cap (g)$, então $\{h_1/g, \ldots, h_p/g\}$ gera $I : g$.*

Prova. Se $a \in (g)$ então $a = bg$, para algum polinômio b.
Se $f \in (h_1/g, \ldots, h_p/g)$ então $af = bgf \in (h_1, \ldots, h_p) \subset I \cap (g) \subset I$. Logo, $f \in I : g$.
Reciprocamente, se $f \in I : g$ então $gf \in I \cap (g) = (h_1, \ldots, h_p)$. Daí, $gf = \sum_{i=1}^{p} q_i h_i$ para certos polinômios q_i.
Como cada $h_i \in (g)$, $f = \sum_{i=1}^{p} q_i \frac{h_i}{g} \in (h_1/g, \ldots, h_p/g)$. □

Com esse teorema, o algoritmo para calcular interseção de ideais e a equação (4), chegamos a um **algoritmo para calcular os geradores do ideal quociente**:
Dados ideais $I = (f_1, \ldots, f_r)$ e $J = (g_1, \ldots, g_s)$ de S. Para cada i, calcularemos um conjunto de geradores para $I : g_i$. Tendo em vista o Teorema 2.43, primeiro calcule uma base de Gröbner para $(f_1, \ldots, f_r) \cap (g_i)$: encontre uma base de Gröbner para $(tf_1, \ldots, tf_r, (1-t)g_i)$, adotando a ordem lex com t maior que todos os X_i, e tome os seus elementos que não dependem da variável t. Usando o algoritmo da divisão, divida cada um desses elementos por g_i encontrando um conjunto gerador para $I : g_i$.
Finalmente, calcule um conjunto gerador para $I : J$ aplicando o algoritmo da interseção $s-1$ vezes: calcule uma base de Gröbner para o ideal quociente $I : (g_1, g_2) = (I : g_1) \cap (I : g_2)$, em seguida, um base para $I : (g_1, g_2, g_3) = (I : (g_1, g_2)) \cap (I : g_3)$, e assim por diante.

Calculando ideais quociente, podemos encontrar a *saturação de I em relação a J*, ou seja, determinar a união

$$I : J^{\infty} = \bigcup_{d=1}^{\infty} \subset S$$

Para ver isso, lembramos que para todo d, $I : J^d \subset (I : J^d) : J$ e $(I : J^d) : J = I : J^{d+1}$. Então obtemos uma cadeia ascendente de ideais em S:

$$I : J \subset I : J^2 \subset I : J^3 \subset \cdots \subset I : J^d \subset I : J^{d+1} \subset \cdots$$

Como S é Noetheriano, essa cadeia necessariamente estaciona. Isso significa que existe um natural D tal que $I : J^d = I : J^D$, para todo $d \geq D$. Ou seja, $I : J^{\infty} = I : J^D$.

Observamos ainda que, para cada d,

$$I : J^d = I : J^{d+1} \Rightarrow I : J^{d+1} = I : J^{d+2} \Rightarrow I : J^{d+2} = I : J^{d+3} \Rightarrow \cdots$$

Algoritmo para calcular o ideal saturação: Fixada uma ordem monomial, calcule sistemas geradores para $I : J$ e $I : J^2 = (I : J) : J$ e, em seguida, suas bases de Gröbner reduzidas; se elas forem iguais, faça $D := 1$. Caso contrário, repita o processo para $I : J^2$ e $I : J^3 = (I : J^2) : J$; se eles tiverem a mesma base de Gröbner reduzida, faça D:=2. Caso contrário, repita o processo para $I : J^3$ e $I : J^4 = (I : J^3) : J$, e assim sucessivamente.
Pelas observações que fizemos anteriormente, obteremos $I : J^{\infty} = I : J^D$ após um número finito de passos.

O Fecho Projetivo de uma Variedade Afim

Dada uma variedade algébrica no espaço afim n-dimensional, calcular as equações (homogêneas) que definem o seu fecho de Zariski no espaço projetivo n-dimensional.

Usamos a notação do Capítulo 1, com $L = K$.

Primeiro, lembramos que o mergulho de $\mathbf{A}^n(K)$ em $\mathbf{P}^n(K)$, que a cada ponto $(x_1, \ldots, x_n)$ em $\mathbf{A}^n(K)$ associa $(1 : x_1 : \ldots : x_n)$ em $\mathbf{P}^n(K)$, identifica o espaço afim $\mathbf{A}^n(K)$ com o conjunto $U_0 \subset \mathbf{P}^n(K)$,

$$U_0 := \{ \ (x_0 : x_1 : \ldots : x_n) \in \ \mathbf{P}^n(K) \ \mid x_0 \neq 0 \ \},$$

complementar do hiperplano no infinito.

Definição 2.44. *Seja I um ideal em $K[X_1, \ldots, X_n]$. Definimos a* **homogeneização de** *I sendo o ideal homogêneo*

$$I^* = (f^* \mid f \in I) \subset K[X_0, \ldots, X_n],$$

onde f^* é a "homogeneização" de f como no Capítulo 1.

O teorema a seguir mostra mais uma boa propriedade das bases de Gröbner.

Teorema 2.45. *Sejam I um ideal de $K[X_1, \ldots, X_n]$ e $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para I, com relação a uma ordem monomial homogênea (isto é, uma ordem $>$ que ordena primeiro pelo grau total: $X^\alpha > X^\beta$ sempre que $|\alpha| > |\beta|$).*
Então $G^* = \{g_1^*, \ldots, g_t^*\}$ é uma base (de Gröbner) para $I^* \subset K[X_0, \ldots, X_n]$.

Na demonstração, usaremos o lema a seguir.

Lema 2.46. *Se $f \in K[X_1, \ldots, X_n]$ e $>$ é uma ordem homogênea em $S = K[X_1, \ldots, X_n]$, então*

$$MP_{>^*}(f^*) = MP_>(f),$$

onde $>^*$ é a ordem monomial em $K[X_0, \ldots, X_n]$ definida por:
(X^α, X^β monômios em $K[X_1, \ldots, X_n]$)

$$X^\alpha X_0^r >^* X^\beta X_0^s \quad se \quad X^\alpha > X^\beta \quad ou, \quad X^\alpha = X^\beta \ e \ r > s.$$

Prova. Como $>$ é uma ordem homogênea, para todo $f \in K[X_1, \ldots, X_n]$, $MP_>(f)$ é um dos monômios X^α que aparecem na componente homogênea de f com grau total máximo. Na homogeneização, esse termo não se altera. Se $X^\beta X_0^s$ é qualquer um dos outros monômios que aparecem em f^*, então $\alpha > \beta$. Pela definição de $>^*$, segue que $X^\alpha >^* X^\beta X_0^s$. □

Prova do Teorema 2.45. É claro que cada $g_i^* \in I^*$. Então é suficiente mostrar que o ideal dos termos principais $TP_{>^*}(I^*)$ é gerado por $TP_{>^*}(G^*)$.
Para isso, considere $F \in I^*$. Como I^* é um ideal homogêneo, cada componente homogênea de F está em I^* e, por isso, podemos assumir que F é homogêneo. Por definição,

$$F \in I^* \Rightarrow F = \sum_j A_j f_j^*,$$

para certos $A_j \in K[X_0, \ldots, X_n]$ e $f_j \in I$.
Considere a "desomogeneização" $f = F(1, X_1, \ldots, X_n)$ de F e faça $X_0 = 1$ na equação anterior, obtendo:

$$f = F(1, X_1, \ldots, X_n) = \sum_j A_j(1, X_1, \ldots, X_n) f_j^*(1, X_1, \ldots, X_n))$$
$$\Rightarrow f = \sum_j A_j(1, X_1, \ldots, X_n) f_j.$$

O que mostra que $f \in I \subset K[X_1, \ldots, X_n]$.
A homogeneização de f é da forma $F = X_0^s \cdot f^*$, para algum $s \geq 0$. Daí, usando o Lema 2.46, concluímos que

$$MP_{>^*}(F) = X_0^s \cdot MP_{>^*}(f^*) = X_0^s \; MP_>(f).$$

Como G é base de Gröbner para I, $MP_>(f)$ é divisível por algum $MP_>(g_i) = MP_{>^*}(g_i^*)$ (usamos o lema novamente). Portanto, $MP_{>^*}(F)$ é divisível por $MP_{>^*}(g_i^*)$. □

Teorema 2.47. *Se K é um corpo algebricamente fechado, seja $I \subset S$ um ideal. Então, $\mathcal{V}(I^*) \subset \mathbf{P}^n(K)$ é o fecho projetivo de $\mathcal{V}(I) \subset \mathbf{A}^n(K)$.*

Prova. Denotaremos $W = \mathcal{V}(I) \subset \mathbf{A}^n(K)$ e $Z = \mathcal{V}(I^*) \subset \mathbf{P}^n(K)$.
É claro que Z é uma variedade projetiva com $W \subset Z$. Logo, resta provar que Z é a menor dentre essas.
Considere então $V = \mathcal{V}(F_1, \ldots, F_s)$ uma variedade de $\mathbf{P}^n(K)$ contendo W.
As desomogeneizações $f_i = F_i(1, X_1, \ldots, X_n)$ estão em $\mathcal{I}(W) \subset S$ e K é algebricamente fechado, logo

$$f_i \in \mathcal{I}(W) = Rad(I).$$

O que significa que $f_i^N \in I$, para algum natural N. Disso, segue que

$$(f_i^*)^N = (f_i^N)^* \in I^*,$$

e portanto f_i^* anula-se em Z.
Como $F_i = X_0^{s_i} f_i^*$, F_i também se anula em todos os pontos de Z; ou seja, $Z \subset V$. □

Dos dois teoremas anteriores, tiramos um **algoritmo para calcular o fecho projetivo de uma variedade afim**, sobre um corpo K algebricamente fechado: Dada uma variedade afim $W \subset \mathbf{A}^n(K)$ definida pelas equações $f_1 = \ldots = f_r = 0$, calcule uma base de Gröbner $G = \{g_1, \ldots, g_t\}$ para o ideal $(f_1, \ldots, f_r)$, adotando uma ordem monomial homogênea (por exemplo, hlex). Então, o fecho projetivo de W em $\mathbf{P}^n(K)$ é definido por $g_1^* = \ldots = g_t^* = 0$.

Capítulo 3

Syzygies

Os conceitos e resultados de bases de Gröbner para ideais polinomiais são imediatamente estendidos para o caso geral de submódulos de um módulo livre, sobre anéis polinomiais.

O maior tópico deste capítulo é um estudo para *syzygies*, procurando explorar mais a fundo as questões que foram introduzidas pelos s-polinômios no capítulo anterior.

Do algoritmo de Buchberger seguirá um método para calcular syzygies, e ainda uma demonstração construtiva para o *Teorema dos Syzygies de Hilbert*. Com essa demonstração, chegaremos a um método algorítmico para calcular resoluções livres (finitas) para módulos *construídos*, sobre anéis polinomiais.

Trabalharemos com o anel de polinômios $S = K[X_1, \ldots, X_n]$ sobre um corpo K. Os elementos de K serão chamados de escalares. Todos os S-módulos mencionados serão assumidos finitamente gerados. Portanto, como S é Noetheriano, os módulos serão também Noetherianos.

3.1 Bases de Gröbner para Módulos

Nesta primeira seção, serão apresentadas versões mais gerais de temas introduzidos no Capítulo 2.

3.1.1 Monômios e Ordenação Monomial

Seja F um S-módulo livre com base $\{e_i\}$.

Um **monômio em F** é um elemento da forma $u = X^\alpha e_i$, para algum i, com X^α monômio em S. Diremos que tal u **envolve o elemento base** e_i.

Um **submódulo monomial de F** é um submódulo M gerado por monômios em F; assim, M pode ser escrito como

$$M = \bigoplus I_j e_j \subset \bigoplus S e_j = F$$

com I_j ideal monomial de S gerado por aqueles monômios u tais que $ue_j \in M$.

Um **termo de** F é um monômio multiplicado por um escalar. Todo elemento de F é escrito de forma única como uma soma de termos não nulos envolvendo monômios distintos.

Todas essas definições dependem da base $\{e_i\}$ escolhida para F. Sempre que possível, supriremos a base atual $\{e_i\}$ da nossa notação e falaremos de F, simplesmente, como um módulo livre com base.

Dizemos que $u = aX^\alpha e_i$ é **divisível** por $v = bX^\beta e_j$ se, e somente se, $i = j$ e X^α é divisível por X^β; nesse caso, o quociente é denotado por $u/v := X^\alpha/X^\beta$ em S.
Um dado mônomio u pertence a um submódulo monomial M de F se, e somente se, u é divisível por algum dos monômios de M.
Se u e v são monômios de F envolvendo o mesmo elemento base e_i , definimos o *Máximo Divisor Comum* e o *Mínimo Múltiplo Comum* entre u e v:

$$MDC(u,v) := MDC(X^\alpha, X^\beta)e_i$$
$$MMC(u,v) := MMC(X^\alpha, X^\beta)e_i$$

Definição 3.1. *Uma* **ordem monomial** *em F é uma ordem total $>$ no conjunto dos monômios de F tais que, se u_1, u_2 são monômios em F e $v \neq 1$ é um monômio em S, então:*

$$u_1 > u_2 \text{ implica } \quad v \cdot u_1 > v \cdot u_2 > u_2.$$

Usaremos a mesma notação para termos: se au e bv são termos de F, com $0 \neq a, b \in K$ e u, v monômios, então: $u > v \Rightarrow au > bv$.
Fixada uma ordem monomial em F, para cada $f \in F$ não nulo, o *termo principal de f*, denotado por $TP(f)$, é o maior termo de f. Como K é um corpo, a distinção entre termos e monômios não será regra na exposição de nossos argumentos. Se M é um submódulo de F, $TP(M)$ denota o submódulo monomial gerado pelos $TP(f)$, para todo $f \in M$.

Encerramos esta subseção, vendo um exemplo de como fabricar ordens monomiais no S-módulo livre F com base $\{e_i\}$, a partir das ordens monomiais de S.

Exemplo 3.2. *Escolha uma ordem $>_1$ entre os elementos da base $\{e_i\}$ de F e considere uma ordem monomial $>_2$ em S. Defina então a ordem monomial $>$ no conjunto dos monômios de F da seguinte forma:* $X^\alpha e_i > X^\beta e_j \quad \Leftrightarrow \quad e_i >_1 e_j \quad$ ou, $\quad e_i = e_j \;$ e $X^\alpha >_2 X^\beta$.

Observação: O que fizemos no exemplo acima é chamado *produto lexicográfico* das ordens parciais $>_1$ e $>_2$.

3.1.2 Algoritmo da Divisão

Proposição 3.3. *Seja F um S-módulo livre com base e ordem monomial $>$.*
Se $f, g_1, \ldots, g_t \in F$, então existe uma expressão

$$f = \sum q_i g_i + r,$$

com $q_i \in S$; e $r \in F$ tem a seguinte propriedade: nenhum de seus monômios está em $(TP(g_1), \ldots, TP(g_t))$; além disso, $TP(f) \geq TP(q_i g_i)$ para todo i. Nessas condições, r é chamado um **resto** *de f com relação a $g_1, \ldots, g_t$, e uma expressão da forma acima é chamada uma* **expressão canônica** *para f em termos dos g_i.*

Prova. A prova consiste do Algoritmo 2.6. Nele, os q_i e r encontrados dependem apenas da ordem monomial adotada e da ordenação previamente imposta à lista dos $g_1, \ldots, g_t$. Por isso, tal algoritmo é muitas vezes chamado *algoritmo da divisão determinada.* □

O que apresentaremos a seguir é uma versão "aleatória" para a divisão.

Algoritmo 3.4. *Seja F um S-módulo livre com base e fixe uma ordem monomial em F. Se $f, g_1, \ldots, g_t \in F$, então podemos produzir uma expressão canônica*

$$f = \sum_{j=1}^{t} u_j g_{i_j} + r$$

para f, com relação a $g_1, \ldots, g_t$, definindo os índices i_j e os termos u_j indutivamente. Escolhidos $i_1, \ldots i_p$ e $u_1, \ldots, u_p$, se

$$\bar{r}_p = f - \sum_{j=1}^{p} u_j g_{i_j} \neq 0$$

e $u := TP(\bar{r}_p)$ é divisível por algum $TP(g_l)$, então faça

$$i_{p+1} := l$$
$$u_{p+1} := \frac{u}{TP(g_l)}$$

Este processo termina quando $\bar{r}_p = 0$ ou nenhum dos monômios de $\bar{r}_p$ é divisível por algum $TP(g_l)$; o resto r é então o último $\bar{r}_p$ produzido.
Esse algoritmo necessariamente termina após finitos passos porque o termo principal de $\bar{r}_p$ decresce em cada estágio, e toda ordem monomial é Artiniana.

O algoritmo da divisão torna-se mais interessante no caso em que os g_i formam uma base de Gröbner.

Definição 3.5. *Seja M um submódulo de F com base e considere uma ordem monomial qualquer em F. Se $g_1, \ldots, g_t \in M$ são tais que*

$$TP(M) = (TP(g_1), \ldots, TP(g_t)),$$

então dizemos que $\{g_1, \ldots, g_t\}$ é uma base de Gröbner para M.

Adotada uma ordem monomial em F, todo submódulo M de F possui uma base de Gröbner, e toda base de Gröbner para M é um conjunto gerador de M.
No Capítulo 2 foram apresentadas provas construtivas para essa afirmação. Com os lemas a seguir justificamos esse fato usando argumentos mais abstratos.

Lema 3.6. *Se $N \subset M$ são submódulos de F e $TP(N) = TP(M)$ (considerando uma ordem monomial qualquer) então $N = M$.*

Prova. Se $N \neq M$, então considere $M \setminus N \neq \emptyset$. Dentre os elementos de $M \setminus N$, tome f com termo principal mínimo.
Como $TP(f) \in TP(M) = TP(N)$, podemos escrever $TP(f) = TP(g)$, para certo $g \in N$.

Daí, $f-g \in M \setminus N$ e seu termo principal é menor do que o de f, contrariando a minimalidade de f. □

Lema 3.7. *Todo submódulo M de F, adotando uma ordem monomial qualquer, possui uma base de Gröbner.*

Prova. Se $g_1, \ldots, g_t$ geram M e não são uma base de Gröbner, então existe $g_{t+1} \in M$ com $(TP(g_1), \ldots, TP(g_t)) \subset (TP(g_1), \ldots, TP(g_{t+1}))$.
Repetindo o processo para $g_1, \ldots, g_t, g_{t+1}$ e, assim por diante, construímos uma cadeia ascendente em $TP(M)$, que é finitamente gerado (pois, F é Noetheriano).
Logo, existirão $g_{t+1}, \ldots, g_{t'} \in M$ com $(TP(g_1), \ldots, TP(g_{t'})) = TP(M)$. □

Daqui em diante, concentraremos nosso estudo nos elementos das bases de Gröbner produzidos pelo *Algoritmo de Buchberger.*

3.2 O Algoritmo de Buchberger

Os s-polinômios, introduzidos no Capítulo 2, foram construídos para cancelar termos principais. Naquele momento, observamos que s-polinômios são responsáveis por todos os possíveis cancelamentos de termos principais. Exploraremos melhor essa questão através da noção de *syzygy.* (De fato: s-polinômio é justamente uma abreviação de "polinômio syzygy").

De modo geral, definimos **syzygies** (ou **relações**) como sendo os elementos do kernel de um homomorfismo entre módulos livres.

3.2.1 Syzygies de Submódulos Monomiais

No que segue, F é um S-módulo livre com base $\{e_i\}$ e M um submódulo de F gerado pelos monômios $u_1, \ldots, u_t$. Considere o homomorfismo

$$\phi : \bigoplus_{j=1}^{t} S\varepsilon_j \longrightarrow F; \qquad \varepsilon_j \mapsto u_j$$

de S-módulos livres, cuja imagem é M. ($\{\varepsilon_j\}$ é a base canônica de S^t).

Um **syzygy nos monômios** $u_1, \ldots, u_t$ é um elemento $\sum h_j\varepsilon_j \in ker(\phi)$; ou seja, é tal que

$$\sum h_j u_j = 0.$$

Para cada par de índices i, j tais que u_i e u_j envolvem o mesmo elemento base de F, definimos

$$u_{ij} = \frac{MMC(u_i, u_j)}{u_j} \in S$$

e σ_{ij} sendo o elemento de $ker(\phi)$ dado por

$$\sigma_{ij} = u_{ji}\varepsilon_i - u_{ij}\varepsilon_j.$$

O resultado a seguir não somente fornece geradores para os syzygies de um submódulo monomial, como também exibe informações precisas sobre os coeficientes necessários para expressar syzygies quaisquer em termos desses geradores.
Vale observar que se todos os u_i envolvem elementos base de F distintos (dois a dois), então claramente teremos $ker(\phi) = (0)$.

Lema 3.8. *Com a notação anterior, $ker(\phi)$ é gerado pelos σ_{ij}.*

Prova. Inicialmente mostraremos que, como um espaço vetorial sobre K, $ker(\phi)$ é a soma direta, sobre todos monômios v de F, dos espaços vetoriais

$$(ker\phi)_v = \{\sum a_l v_l \varepsilon_l \in ker\phi \mid u_l \text{ divide } v,\ v_l = v/u_l, \text{ e } a_l \in K\}.$$

De fato, seja $\sigma = \sum p_i \varepsilon_i \in S^t$, onde $p_i \in S$, um syzygy nos monômios u_i: $\sum p_i u_i = 0$.
Para cada v monômio de F que aparece em um dos $p_j u_j$, e para cada i, seja $p_{i,v}$ o termo (qualquer) de p_i tal que $p_{i,v}u_i$ é um escalar vezes v.
Assim, fixado v, $\sum_i p_{i,v}u_i$ é igual ao termo de $\sum p_i u_i$ correspondente ao v. Devemos ter $\sum_i p_{i,v}u_i = 0$, o que implica $\sum_i p_{i,v}\varepsilon_i \in ker\phi$, com $p_{i,v}$ igual a um escalar vezes $v/u_i \in S$.
Ou seja, $\sum_i p_{i,v}\varepsilon_i \in (ker\phi)_v$.
Então, temos

$$\sigma = \sum_v \sum_i p_{i,v}\varepsilon_i$$

e tal representação é única.
Dessa forma podemos assumir que $\sigma = \sum a_l v_l \varepsilon_l \in (ker\phi)_v$, e mostraremos que σ está no módulo gerado pelos σ_{ij}, por indução sobre o número de termos não nulos de σ.
Se $\sigma \neq 0$, então pelo fato de σ ser um syzygy, ao menos dois dos $a_l v_l$ devem ser não nulos: digamos que sejam o i-ésimo e o j-ésimo, com $i < j$.
Isso significa que v é divisível por u_i e u_j; logo, v_i é divisível por

$$\frac{MMC(u_i, u_j)}{u_i} = u_{ji}.$$

Assim, o i-ésimo termo de

$$\sigma - a_i \cdot \frac{v_i}{u_{ji}} \cdot \sigma_{ij}$$

deve ser zero, e o único outro termo afetado é o j-ésimo. Assim, de σ foi produzido um syzygy em $(ker\phi)_v$ com menos termos. Repetindo esse processo, podemos então escrever σ com uma combinação dos σ_{ij}. □

A demonstração acima oferece um resultado mais forte, que será usado no *Critério de Buchberger* para reconhecer bases de Gröbner.

Lema 3.8′. *Com a notação do Lema 3.8, todo elemento do $ker\phi$ é escrito, de forma única, como uma soma dos elementos $\tau = \sum a_l v_l \varepsilon_l \in ker\phi$ tais que todos os $v_l u_l$ são iguais ao mesmo monômio v de F. Além disso, tais elementos podem ser escritos na forma*

$$\tau = \sum v_{ij}\sigma_{ij},$$

onde a soma é sobre todos $i < j$ tais que $MMC(u_i, u_j)$ divide v, e v_{ij} é um escalar vezes o monômio $v/MMC(u_i, u_j) = v_i/u_{ji}$ em S.

3.2.2 Critério de Buchberger

Seja F um S-módulo livre com base e uma ordem monomial. Seja $M \neq (0)$ o submódulo gerado por $g_1, \ldots, g_t \in F$, e considere o homomorfismo

$$\phi : \bigoplus_{j=1}^{t} S\varepsilon_j \longrightarrow F; \qquad \varepsilon_i \mapsto g_i,$$

cuja imagem é M.

Para cada par de índices i, j tais que $TP(g_i), TP(g_j)$ envolvem o mesmo elemento base de F, definimos

$$u_{ij} = \frac{MMC(TP(g_i), TP(g_j))}{TP(g_j)} \in S,$$

e fazemos

$$\sigma_{ij} = u_{ji}\varepsilon_i - u_{ij}\varepsilon_j,$$

tais que os σ_{ij} geram os syzygies nos elementos $TP(g_i)$, pelo Lema 3.8.

E ainda: para cada par i, j, escolhemos uma expressão canônica

$$u_{ji}g_i - u_{ij}g_j = \sum f_l^{ij} g_l + h_{ij}$$

para $u_{ji}g_i - u_{ij}g_j$ com relação aos $g_1, \ldots, g_t$.
Note que:

$$TP(f_l^{ij} g_l) \leq TP(u_{ji}g_i - u_{ij}g_j) < TP(u_{ji}g_i)$$

Por conveniênica, fazemos $h_{ij} = 0$ se $TP(g_i), TP(g_j)$ envolvem elementos base distintos.

Com a notação acima, temos:

Teorema 3.9. (Critério de Buchberger) *Os elementos $g_1, \ldots, g_t$ formam uma base de Gröbner para M se, e somente se, $h_{ij} = 0$, para todo $i < j$.*

Prova. A prova seguirá o mesmo enredo da demonstração do Teorema 2.15 (caso particular em que $F = S$).
($\Rightarrow$) Como os h_{ij} estão em M, $TP(h_{ij}) \in TP(M)$. Se $g_1, \ldots, g_t$ formam uma base de Gröbner para M, então $TP(M) = (TP(g_1), \ldots, TP(g_t))$. Assim, se algum h_{ij} fosse diferente de zero, seu termo principal seria divisível por algum $TP(g_i)$, o que contrariaria as propriedades do resto. Logo, $h_{ij} = 0$, $\forall\, i, j$.
($\Leftarrow$) Suponha todos os h_{ij} iguais a zero, tais que $\phi(\sigma_{ij}) = \sum f_l^{ij} g_l$, com $TP(f_l^{ij} g_l) < TP(u_{ji}g_i)$.
Vale observar que se todos os $TP(g_i)$ envolvem elementos base de F distintos (dois a dois), então é imediato que $\{g_1, \ldots, g_t\}$ é uma base de Gröbner.
Se $g_1, \ldots, g_t$ não formam uma base de Gröbner, então escolha uma expressão

$$f = \sum f_l g_l \text{ com } TP(f) \notin (TP(g_1), \ldots, TP(g_t)).$$

Seja u o máximo entre os termos $TP(f_l g_l)$. Podemos assumir ainda que a expressão para f foi escolhida tendo u o menor possível.
Agora, considere $\sum' f_l g_l$ a soma de todos aqueles $f_l g_l$ para os quais $TP(f_l g_l)$ é u vezes um escalar.
Podemos escrever $TP(f_l g_l) = v_l TP(g_l)$, onde v_l é determinado termo de f_l.
Se a soma correspondente dos termos principais

$$\sum{}' TP(f_l g_l) = \sum{}' v_l TP(g_l) \neq 0$$

então, como u é máximo, esse será o termo principal de f. Daí, como $TP(f)$ é um múltiplo de u, e u é múltiplo dos $TP(g_l)$, $TP(f)$ é divisível pelos $TP(g_l)$, contrariando a forma como f foi tomado.
Logo, devemos ter

$$\sum{}' v_l TP(g_l) = 0,$$

e então $\sum' v_l \varepsilon_l$ é um syzygy nos termos principais dos g_l.
Pelo Lema 3.8', podemos escrever $\sum' v_l \varepsilon_l = \sum_{i<j} b_{ij}\sigma_{ij}$, onde b_{ij} é um escalar vezes o monômio $\frac{u}{MMC(TP(g_i),TP(g_j))}$ de S. Assim, aplicando ϕ nessa igualdade, substituindo $\phi(\sigma_{ij})$ por $\sum f_l^{ij} g_l$, e lembrando que $TP(f_l^{ij} g_l) < TP(u_{ji} g_i)$, chegamos a uma equação da forma

$$\sum{}' v_l g_l = \sum h_s g_s$$

com todos os $TP(h_s g_s)$ menores que u.
Subtraindo a expressão $\sum' v_l g_l = \sum h_s g_s$ da expressão original de f e cancelando os termos de $\sum' v_l g_l$, obtemos uma nova expressão para f, mas nela o máximo dos $TP(f_l g_l)$ é menor do que u, contariando nossa construção.
Assim, concluímos que $TP(f) \in (TP(g_1), \ldots, TP(g_t))$, para todo $f \in M$. Ou seja, $\{g_1, \ldots, g_t\}$ é uma base de Gröbner para M. □

Do Teorema 3.9 segue um método algorítmico para, entrando com um conjunto gerador de um submódulo qualquer M de F, calcular uma base de Gröbner para M.

Algoritmo de Buchberger 3.10. *Na situação do Teorema 3.9, seja $M = (g_1, \ldots, g_t)$ um submódulo de F. Calcule os restos h_{ij}. Se todos os h_{ij} são nulos, então os g_i formam uma base de Gröbner para M. Se algum h_{ij} é diferente de zero, então substitua $\{g_1, \ldots, g_t\}$ por $\{g_1, \ldots, g_t, h_{ij}\}$ e repita o processo.*
Como o submódulo gerado pelos termos principais dos $g_1, \ldots, g_t, h_{ij}$ contém estritamente aquele gerado pelos termos principais dos $g_1, \ldots, g_t$, este processo necessariamente termina após finitos passos.

O algoritmo de Buchberger chama a atenção não somente por produzir uma base de Gröbner, mas também pelos elementos envolvidos no seu processo. De fato, o Teorema 3.11 mostra que as equações $h_{ij} = 0$, obtidas se os g_i formam uma base de Gröbner para M, geram todos os syzygies em M. Esse é o *algoritmo de Schreyer* para calcular syzygies.

3.3 Cálculo de Syzygies

Usaremos a notação introduzida na seção anterior.

Existe um bônus do algoritmo de Buchberger: um método efetivo para calcular syzygies. O processo do Algoritmo 3.10 fornece combinações lineares dos g_l, os h_{ij}. Daí, se $h_{ij} = 0$, obtemos um syzygy. Na verdade, esses syzygies geram todo o módulo de syzygies nos g_i.

A notação que usaremos é a mesma desenvolvida para o Teorema 3.9. Além disso, para $i < j$, tais que $TP(g_i), TP(g_j)$ envolvem o mesmo elemento base de F, definimos

$$\tau_{ij} := u_{ji}\varepsilon_i - u_{ij}\varepsilon_j - \sum_l f_l^{ij}\varepsilon_l.$$

Teorema 3.11.(*Schreyer*)
Com a notação acima, suponha que $g_1, \ldots, g_t$ formam uma base de Gröbner. Seja $>_F$ uma ordem monomial qualquer em F, e considere $>$ a ordem monomial em $\bigoplus_{j=1}^t S\varepsilon_j$ definida por : $u\varepsilon_l > v\varepsilon_m$ se, e somente se,

$$TP(ug_l) >_F TP(vg_m)$$

ou

$$TP(ug_l) = TP(vg_m) \quad \textit{(salvo multiplicação por escalar) e} \quad l < m.$$

Então, os τ_{ij} geram os syzygies nos g_i.
Mais precisamente, os τ_{ij} formam uma base de Gröbner para os syzygies, com relação à ordem $>$; e $TP(\tau_{ij}) = u_{ji}\varepsilon_i$.

Prova. Primeiro mostraremos que $TP(\tau_{ij}) = u_{ji}\varepsilon_i$. Para isso, observamos que $TP(u_{ji}g_i) = MMC(TP(g_i), TP(g_j)) = TP(u_{ij}g_j)$ e esses termos são maiores que qualquer outro que apareça nos $f_l^{ij}g_l$. Logo, o termo principal de τ_{ij} é $u_{ji}\varepsilon_i$ ou $u_{ij}\varepsilon_j$, pela primeira parte da definição de $>$. Então, como $i < j$, temos $u_{ji}\varepsilon_i > u_{ij}\varepsilon_j$.
Os τ_{ij} estão no $ker\phi$ ($\phi : \oplus S^t \to F$, $\varepsilon_i \mapsto g_i$), pois estamos assumindo que os g_i formam uma base de Gröbner. Resta mostrar que eles formam uma base de Gröbner para $ker\phi$.
Seja $\tau = \sum f_l\varepsilon_l \in ker\phi$. Para cada índice l, escrevemos $TP(f_l\varepsilon_l) = v_l\varepsilon_l$, para certo termo v_l de f_l. Como tais termos não podem ser cancelados (pois, envolvem ε_l diferentes), $TP(\sum f_l\varepsilon_l) = v_i\varepsilon_i$, para certo i.
Seja $\sigma = \sum' v_l\varepsilon_l$ a soma sobre todos os índices l tais que $v_lTP(g_l) = v_iTP(g_i)$; com todos os l dessa soma $\geq i$, já que assumimos $v_i\varepsilon_i$ sendo o termo principal de τ.
Assim, $\sum' v_lTP(g_l) = 0$; o que significa que σ é um syzygy nos $TP(g_l)$, com $l \geq i$. Pelo Lema 3.8, tais syzygies são gerados pelos σ_{ml} com $m, l \geq i$, e aqueles em que ε_i aparece são os σ_{ij}, para $j > i$. Além disso, o Lema 3.8′ nos conta que v_i está no ideal gerado pelos u_{ji}, com $j > i$. Portanto, $TP(\tau)$ é divisível por $u_{ji}\varepsilon_i = TP(\tau_{ij})$.
Dessa forma, está provado que os τ_{ij} formam uma base de Gröbner para os syzygies nos g_i.
□

Esse teorema oferece um **algoritmo para calcular syzygies**: dados $g_1, \ldots, g_t$ em F. Use o algoritmo de Buchberger para obter uma base de Gröbner para o submódulo $(g_1, \ldots, g_t)$, e os syzygies nos elementos dessa base. Para determinar os syzygies nos g_i,

basta substituir, naqueles syzygies encontrados, os elementos da base de Gröbner por suas expressões em termos dos g_i.

Vejamos um exemplo simples, a fim de esclarecer melhor esse roteiro.

Exemplo 3.12. *Considere $S = F = K[x, y]$ com a ordem lex $x > y$, e sejam $g_1 = x^2$ e $g_2 = xy + y^2$. Seguindo os passos do Algoritmo 3.10, encontraremos uma base de Gröbner para o ideal (g_1, g_2) e, também, os syzygies nos elementos dessa base.*

Observando que $TP(g_1) = x^2, TP(g_2) = xy$ e que o MMC entre eles é x^2y, consideramos o s-polinômio (com a notação da seção anterior)

$$u_{21}g_1 - u_{12}g_2 = \frac{x^2y}{TP(g_1)} \cdot g_1 - \frac{x^2y}{TP(g_2)} \cdot g_2 = yg_1 - xg_2 = -xy^2$$

Efetuando a divisão de $-xy^2$ pelo par ordenado $[g_1, g_2]$ (estamos usando o algoritmo da divisão determinada), obtemos a expressão

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

Assim, encontramos o resto $h_{12} = y^3 \neq 0$. Fazemos $g_3 := h_{12} = y^3$, e daí temos

$$g_3 = yg_1 - xg_2 + yg_2$$

e o syzygy

$$\tau_{12} = y\varepsilon_1 - x\varepsilon_2 + y\varepsilon_2 - \varepsilon_3$$

Repetimos o processo para g_1, g_3 e obtemos

$$u_{31}g_1 - u_{13}g_3 = y^3g_1 - x^2g_3 = 0$$

(pois, g_1, g_3 são monômios!). Portanto, $h_{13} = 0$ e temos o syzygy

$$\tau_{13} = y^3\varepsilon_1 - x^2\varepsilon_3$$

Agora, para g_2, g_3:

$$u_{32}g_2 - u_{23}g_3 = y^2g_2 - xg_3 = y^4$$

Do algoritmo da divisão por g_1, g_2, g_3, segue então que:

$$h_{23} = 0; \quad y^2g_2 - xg_3 = yg_3;$$
$$\tau_{23} = y^2\varepsilon_2 - (x + y)\varepsilon_3$$

Pelo critério de Buchberger, o algoritmo termina fornecendo uma base de Gröbner para o ideal (g_1, g_2): $\{x^2, xy + y^2, y^3\}$
O Teorema 3.11 afirma que $\tau_{12}, \tau_{13}, \tau_{23}$ geram todos os syzygies nos elementos da base encontrada.
Para obter os syzygies nos geradores originais, basta usar a expressão dada em τ_{12}, substituindo g_3 por $yg_1 + (y - x)g_2$ nos outros syzygies.
Dessa forma encontramos:
$\tau_{12} = 0$;

$\tau_{13} = y^3\varepsilon_1 - x^2[y\varepsilon_1 + (y-x)\varepsilon_2]$
$\Rightarrow \tau_{13} = (y^3 - x^2y)\varepsilon_1 + (x^3 - x^2y)\varepsilon_2;$
$\tau_{23} = y^2\varepsilon_2 - (x+y)[y\varepsilon_1 + (y-x)\varepsilon_2]$
$\Rightarrow \tau_{23} = x^2\varepsilon_2 - (xy + y^2)\varepsilon_1.$

Observe que, neste exemplo, $\tau_{13} = (x-y)\tau_{23}$ e, portanto, todos os syzygies nos g_1, g_2 são gerados por τ_{23}.

Do Teorema 3.11 segue uma prova construtiva para o *Teorema dos Syzygies de Hilbert*, o qual garante que todo S-módulo finitamente gerado possui uma resolução livre de comprimento $\leq n$.

Corolário 3.13. *Com a mesma notação do Teorema 3.11, suponha que os g_i são arranjados de tal forma que: se $TP(g_i), TP(g_j)$ envolvem o mesmo elemento base de F, digamos $TP(g_i) = v_ie, TP(g_j) = v_je$, com $v_i, v_j \in S$, então $v_i > v_j$ sempre que $i < j$, na ordem lex. Se as variáveis $X_1, \ldots, X_k$ não aparecem nos termos principais dos g_i, então as variáveis $X_1, \ldots, X_{k+1}$ não aparecem nos $TP(\tau_{ij})$.*
Além disso, $F/(g_1, \ldots, g_t)$ possui uma resolução livre de comprimento $\leq n-k$. Em particular, todo S-módulo finitamente gerado tem uma resolução livre de comprimento $\leq n$.

Prova. Pelo Teorema 3.11, $TP(\tau_{ij}) = u_{ji}\varepsilon_i$, onde

$$u_{ji} = \frac{MMC(TP(g_i), TP(g_j))}{TP(g_i)} = \frac{TP(g_j)}{MDC(TP(g_i), TP(g_j))}$$

Como $i < j$, $TP(g_i) > TP(g_j)$, pela maneira com que arranjamos os g_i. Daí, se X_{k+1} aparece em $TP(g_j)$ também deverá aparecer, com potência maior ou igual, em $TP(g_i)$, pois estamos considerando a ordem lex $(X_1 > \ldots > X_n)$. Logo, a potência de X_{k+1} em $MDC(TP(g_i), TP(g_j))$ é exatamente a mesma que a de X_{k+1} em $TP(g_j)$. Disso segue que X_{k+1} não aparece em u_{ji}. E portanto $X_1, \ldots, X_{k+1}$ não aparecem nos $TP(\tau_{ij})$.

Agora, mostraremos que $F/(g_1, \ldots, g_t)$ tem uma resolução livre de comprimento $\leq n-k$, por indução sobre $n-k$.
Para $n-k = 0$, nenhuma das variáveis $X_1, \ldots, X_n$ aparece em $TP(g_i)$, para todo i. Afirmamos que $F/(g_1, \ldots, g_t)$ é livre. De fato, com essas hipóteses, todos os termos principais dos g_i devem ser escalares vezes elementos base de F. Então, $TP(g_1, \ldots, g_t) = (TP(g_1), \ldots, TP(g_t))$ é o submódulo de F gerado pelos e_i que são envolvidos nos $TP(g_i)$. Seja F' o submódulo livre gerado pelos outros e_j e considere a composição

$$F' \hookrightarrow F \twoheadrightarrow F/(g_1, \ldots, g_t)$$

Pelo Teorema 2.5 (imediatamente estendido para o caso geral de S-módulos), $F/(g_1, \ldots, g_t)$ possui uma base consistindo exatamente dos monômios de F'. Então, a composição acima é um isomorfismo e, portanto, $F' \simeq F/(g_1, \ldots, g_t)$ é livre.

Finalmente, suponha $n-k > 0$. Como $X_1, \ldots, X_{k+1}$ não aparecem nos termos principais dos τ_{ij}. Podemos ordenar os τ_{ij} de tal forma que estejam nas mesmas condições dos g_i (lembre-se que os τ_{ij} também formam uma base de Gröbner). Então, segue da hipótese de indução que $\bigoplus S\varepsilon_i/(\{\tau_{ij}\})$ tem uma resolução livre de comprimento $\leq n-k-1$. Digamos

$$\cdots \to F_1 \to F_0 \to \frac{\bigoplus S\varepsilon_i}{(\{\tau_{ij}\})} \to 0$$

Mas, $\bigoplus S\varepsilon_i/(\{\tau_{ij}\})$ é isomorfo ao submódulo $im\ \phi = (g_1, \ldots, g_t)$ de F, pois $ker\phi = (\{\tau_{ij}\})$; então temos essa mesma resolução livre para $(g_1, \ldots, g_t)$,

$$\cdots \to F_1 \to F_0 \to (g_1, \ldots, g_t) \to 0,$$

chegando a uma resolução livre para $F/(g_1, \ldots, g_t)$:

$$\cdots \to F_1 \to F_0 \to F \to F/(g_1, \ldots, g_t) \to 0,$$

de comprimento $\leq n - k$.

Se N é um S-módulo qualquer finitamente gerado, então ele é isomorfo a F/M, para certos F S-módulo livre e M submódulo de F. Daí, encontrando uma base de Gröbner para M, entramos nas condições do que provamos acima, concluindo que N necessariamente terá uma resolução livre de comprimento $\leq n$. □

Dizemos que um S-módulo N finitamente gerado foi **construído**, quando podemos escrevê-lo na forma F/M, onde F é um S-módulo livre e M é um submódulo de F com um sistema de geradores explícito; ou equivalentemente, quando N é apresentado como o cokernel de um homomorfismo de S-módulos livres com imagem M.

Para encerrar este capítulo, analisaremos o processo indutivo na demonstração do Corolário 3.13, vendo um **algoritmo para calcular resoluções livres para S-módulos construídos**: Dados S-módulo $N = F/M$, $M = (f_1, \ldots, f_s)$ submódulo do módulo livre F. Calcule uma base de Gröbner $\{g_1, \ldots, g_t\}$ para M, nas condições do Corolário 3.13. Nessas mesmas condições, calcule sucessivamente:

os t_1 geradores $\tau_{ij}^{(1)}$ dos syzygies nos g_i;

os t_2 geradores $\tau_{ij}^{(2)}$ dos syzygies nos $\tau_{ij}^{(1)}$;

os t_3 geradores $\tau_{ij}^{(3)}$ dos syzygies nos $\tau_{ij}^{(2)}$;

...

os t_{n-1} geradores $\tau_{ij}^{(n-1)}$ dos syzygies nos $\tau_{ij}^{(n-2)}$;

os t_n geradores $\tau_{ij}^{(n)}$ dos syzygies nos $\tau_{ij}^{(n-1)}$.

Nos termos principais dos primeiros syzygies $\tau_{ij}^{(1)}$ aparecem no máximo as $n-1$ últimas variáveis. Pela mesma razão, a cada passo, os termos principais dos syzygies $\tau_{ij}^{(k)}$ perdem pelo menos uma variável em comparação aos termos principais dos syzygies anteriores $\tau_{ij}^{(k-1)}$. Logo, certamente, os termos principais dos $\tau_{ij}^{(n)}$ são escalares vezes elementos base; donde segue que $P := \left(\tau_{ij}^{(n-1)} \mid i, j\right)$, isomorfo a $S^{t_{n-1}}/(\tau_{ij}^{(n)} \mid i, j)$, é livre.

Com os argumentos acima encontramos uma resolução livre para $N = F/M$:

$$0 \longrightarrow P \longrightarrow S^{t_{n-2}} \longrightarrow \ldots \longrightarrow S^{t_1} \longrightarrow S^t \longrightarrow F \longrightarrow N$$

de comprimento $\leq n$.

Capítulo 4

Algoritmos para a Normalização de Noether

Este capítulo é um bom exemplo de aplicação de bases de Gröbner em Álgebra Comutativa, destacando o seu caráter algorítmico.

Trata-se de um estudo do texto *Uma Prova Computacional do Lema da Normalização de Noether*, de Alessandro Logar [7], onde é dado um algoritmo probabilístico que fornece a mudança de coordenadas responsável por levar um dado ideal polinomial primo em sua *posição normal de Noether*.

Dessa forma, o Lema da Normalização de Noether, cujas demonstrações clássicas já são bastante construtivas (ver Kunz [6]), é computacionalmente provado para o caso de ideais primos.

Teorema 4.1. (Lema da Normalização de Noether)
Seja I um ideal de $S = K[X_1, \ldots, X_n]$, com K sendo um corpo infinito. Então existe uma conveniente mudança de variáveis

$$A : S \longrightarrow S, \quad X_i \mapsto Y_i = \sum_{j=1}^{n} a_{ij} X_i, \quad a_{ij} \in K,$$

que leva I em um ideal tal que:

- $Y_1, \ldots, Y_d$ são algebricamente independentes mod I
(isto é, as imagens de $Y_1, \ldots, Y_d$ em S/I são algebricamente independentes sobre K);

- $Y_{d+1}, \ldots, Y_n$ são integrais sobre $K[Y_1, \ldots, Y_d]$ mod I
(ou ainda, S/I é finitamente gerado como um $K[Y_1, \ldots, Y_d]$-módulo).

Nessas condições, dizemos que A leva o ideal I em sua **posição normal de Noether**.

Observe que um conjunto $\mathcal{X}$ de variáveis é algebricamente independente mod I se, e somente se, $I \cap K[\mathcal{X}] = (0)$.

4.1 Resultados Preliminares

Daqui até o final deste capítulo, $\mathcal{P} \subset K[X_1, \ldots, X_n]$ é um ideal primo não nulo e G é uma base de Gröbner para $\mathcal{P}$ com relação à ordem *lexicográfica* $X_1 < X_2 < \ldots < X_n$. (Essa é a mesma ordem monomial *lex* definida no Capítulo 2, no entanto, agora estamos identificando os monômios X^α com as n-uplas de números inteiros não negativos $\alpha = (\alpha_1, \ldots \alpha_n)$ da seguinte forma: $X^\alpha = X_n^{\alpha_1} X_{n-1}^{\alpha_2} \ldots X_1^{\alpha_n}$.)

Algoritmo 4.2.
INICIE com $T_0 := \emptyset$

PARA $0 < j \leq n$, *faça:*
$\quad$ *SE* $G \cap (K[X_1, \ldots, X_j] \setminus K[X_1, \ldots, X_{j-1}]) \neq \emptyset$, *ENTÃO* $T_j := T_{j-1}$;
$\quad$ *CASO CONTRÁRIO,* $T_j := T_{j-1} \cup \{X_j\}$.

DEFINA $T_\mathcal{P} := T_n$.

Observando o algoritmo acima para construção de $T_\mathcal{P}$ vemos que, para todo $0 < j \leq n$, X_j pertence a $T_\mathcal{P}$ se, e somente se, para cada polinômio g da base G, g depende "efetivamente" de alguma variável maior que X_j ou g depende apenas das variáveis menores que X_j.

Proposição 4.3. *Com $T_\mathcal{P}$ dado pelo Algoritmo 4.2, temos:*
(i) $T_\mathcal{P}$ é algebricamente independente mod $\mathcal{P}$;
(ii) dim $\mathcal{P}$ = card($T_\mathcal{P}$).

Na prova dessa proposição, é utilizado o lema a seguir.

Lema 4.4. *Seja g um polinômio irredutível em $K[X]$ e seja $f \in K[Y_1, Y_2, \ldots, Y_d, X]$ tal que $f \notin (g)$. Então, $(f, g) \cap K[Y_1, Y_2, \ldots, Y_d] \neq (0)$.*

Prova. Das hipóteses segue que f e g são relativamente primos no anel $K[Y_1, \ldots, Y_d][X]$. Logo, por Gauss, f e g também são relativamente primos em $K(Y_1, \ldots, Y_d)[X]$. Ou seja, existem polinômios $h \in K[Y_1, \ldots, Y_d]$ (com $h \neq 0$) , a_1, $a_2 \in K[Y_1, \ldots, Y_d, X]$, tais que

$$h = a_1 f + a_2 g.$$

Assim, temos um polinômio não nulo em $(f, g) \cap K[Y_1, Y_2, \ldots, Y_d]$. □

Prova da Proposição 4.3. Por indução sobre o número n de variáveis.

Se $n = 1$, $G \cap (K[X_1] \setminus K) = G \neq \emptyset$, pois $\mathcal{P} \neq K[X_1]$, o que implica $T_\mathcal{P} = T_1 := T_0 = \emptyset$. Assim, $\mathcal{P} \cap K[\emptyset] = \mathcal{P} \cap K = (0)$, donde segue que $T_\mathcal{P}$ é algebricamente independente mod $\mathcal{P}$ com $card(T_\mathcal{P}) = 0$; e ainda, $dim\ \mathcal{P} = dim(K[X_1]/\mathcal{P}) = 0$, pois $\mathcal{P}$ é um ideal maximal em $K[X_1]$.

Suponha $n > 1$ e a proposição válida para $n - 1$.

CASO I: X_1 é algebricamente independente mod $\mathcal{P}$.
Sejam $L := K(X_1)$ e $\mathcal{Q} := \mathcal{P}L[X_2, \ldots, X_n]$.
Como $\mathcal{P} \cap K[X_1]$ é nulo, $X_1 \in T_\mathcal{P}$. Usando a definição de bases de Gröbner e lembrando que

adotamos a ordem *lex* em $K[X_1,\ldots,X_n]$ com X_1 sendo a menor das variáveis, verifica-se facilmente que G é uma base de Gröbner para $\mathcal{Q}$, em relação à ordem *lex* $X_2 < \ldots < X_n$ em $L[X_2,\ldots,X_n]$. Além disso, o conjunto de variáveis $\{X_1, X_{i_1}, X_{i_2},\ldots,X_{i_\delta}\}$ $(i_j \neq 1)$ é algebricamente independente mod $\mathcal{P}$ em $K[X_1,\ldots,X_n]$ se, e somente se, $\{X_{i_1}, X_{i_2},\ldots,X_{i_\delta}\}$ é algebricamente independente mod $\mathcal{Q}$ em $L[X_2,\ldots,X_n]$.
Assim, como $T_\mathcal{Q}$ é, por hipótese de indução, algebricamente independente mod $\mathcal{Q}$, temos que $T_\mathcal{Q} \cup \{X_1\} = T_\mathcal{P}$ é algebricamente independente mod $\mathcal{P}$.
Considerando os conjuntos

$$C := \{\ q \in Spec(L[X_2,\ldots X_n]) \mid q \subset \mathcal{Q}\ \}, \quad D := \{\ p \in Spec(K[X_1,\ldots X_n]) \mid p \subset \mathcal{P}\ \}$$

e a aplicação sobrejetiva $\psi : C \longrightarrow D,\ q \mapsto q \cap K[X_1,\ldots X_n]$, vemos que $h(\mathcal{P}) = h(\mathcal{Q})$. Daí, como

$$n = K[X_1,\ldots X_n] = h(\mathcal{P}) + dim\ \mathcal{P},$$
$$n-1 = L[X_2,\ldots X_n] = h(\mathcal{Q}) + dim\ \mathcal{Q},$$

temos $dim\ \mathcal{P} = dim\ \mathcal{Q} + 1$.
Portanto, como $card(T_\mathcal{Q}) = dim\ \mathcal{Q}$ (por hipótese de indução) e $card(T_\mathcal{P}) = card(T_\mathcal{Q}) + 1$, a proposição está provada para este caso.

CASO II: X_1 é algébrico mod $\mathcal{P}$. (Ou seja, $\mathcal{P} \cap K[X_1] \neq 0$).
Então, existe um polinômio irredutível $g \neq 0$ com $\mathcal{P} \cap K[X_1] = (g)K[X_1]$, pois $\mathcal{P} \cap K[X_1]$ é um ideal primo não nulo ($\Leftrightarrow$ maximal) do domínio de ideais principais $K[X_1]$. Pelo Teorema 2.21, $G \cap K[X_1]$ é uma base de Gröbner para $\mathcal{P} \cap K[X_1]$, logo podemos tomar g em G. Obviamente, $X_1 \notin T_\mathcal{P}$.
Considere o corpo $L := K[X_1]/(g)$ e a aplicação quociente

$$\phi : K[X_1,\ldots,X_n] \longrightarrow L[X_2,\ldots,X_n],$$

com $\mathcal{Q} := \phi(\mathcal{P})$.
Como ϕ é um homomorfismo sobrejetivo com $ker(\phi) \subset \mathcal{P}$, temos que o ideal $\mathcal{Q}$ é primo. Então, segue da hipótese de indução que $T_\mathcal{Q}$ é algebricamente independente mod $\mathcal{Q}$; e ainda, $card(T_\mathcal{Q}) = dim\ \mathcal{Q}$.
Afirmamos que $\mathcal{X} = \{\ X_{i_1}, X_{i_2},\ldots,X_{i_\delta}\ \}$ $(i_j \neq 1)$ é algebricamente independente mod $\mathcal{P}$ em $K[X_1,\ldots,X_n]$ se, e somente se, $\mathcal{X} = \{\ X_{i_1}, X_{i_2},\ldots,X_{i_\delta}\ \}$ $(i_j \neq 1)$ é algebricamente independente mod $\mathcal{Q}$ em $L[X_2,\ldots,X_n]$. De fato, se $\mathcal{Q} \cap L[\mathcal{X}] \neq 0$ então seja $0 \neq F$ em $\mathcal{Q} \cap L[X_{i_1}, X_{i_2},\ldots,X_{i_\delta}]$ e considere f em $\mathcal{P} \cap K[X_1, X_{i_1}, X_{i_2},\ldots,X_{i_\delta}]$ tal que $\phi(f) = F$ e $f \notin (g)K[X_1,\ldots,X_n]$. Com isso, usando o Lema 4.4, temos que $(f,g) \cap K[X_{i_1}, X_{i_2},\ldots,X_{i_\delta}] \neq 0$ e, portanto, $\mathcal{P} \cap K[\mathcal{X}] \neq 0$. A outra implicação é imediata.
Temos também $dim\ \mathcal{P} = dim\ \mathcal{Q}$, pois a aplicação ϕ induz um isomorfismo entre os anéis $K[X_1,\ldots,X_n]/\mathcal{P}$ e $L[X_2,\ldots,X_n]/\mathcal{Q}$.
Usando a definição de bases de Gröbner, o fato de X_1 ser a menor das variáveis implica que G é uma base de Gröbner para $\mathcal{Q}$ com relação à ordem *lex* $X_2 < \ldots < X_n$ em $L[X_2,\ldots,X_n]$. Logo, $T_\mathcal{P} = T_\mathcal{Q}$. E, assim, concluímos a prova da proposição. □

Observação. Para um ideal I que não é primo, a igualdade $dim\ I = card(T_I)$ pode não ser válida.
Para ilustrar essa observação, considere o ideal monomial $I = (X^2, XY)$ em $K[X,Y]$. Obviamente, $G = \{X^2, XY\}$ é uma base de Gröbner para I, com relação à qualquer ordem monomial.
Temos $T_I = \emptyset$, daí $card(T_I) = 0$. No entanto, $dim\ I = dim\ K[X,Y]/(X^2,XY) = 1$.

4.2 Bases de Gröbner e o Lema de Noether

A partir daqui, assumimos que K é um corpo infinito.

Uma variável X_s é chamada *integral* sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}$ se existe um polinômio $0 \neq F$ em $\mathcal{P} \cap K[X_1, \ldots, X_s]$ mônico em X_s.

O resultado a seguir fornece um método para determinar quais variáveis X_s são integrais sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}$, através dos polinômios de G.

Proposição 4.5. *X_s é integral sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}$ se, e somente se, existe um polinômio em G cujo monômio principal é uma potência de X_s.*

Prova. Uma das implicações é trivial.
Para provar a outra, suponha X_s integral sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}$. Então, existe um polinômio

$$F = g_0(X_1, \ldots, X_{s-1}) + g_1(X_1, \ldots, X_{s-1})X_s + \ldots + g_{m-1}(X_1, \ldots, X_{s-1})X_s^{m-1} + X_s^m,$$

em $\mathcal{P}$, com $g_i \in K[X_1, \ldots, X_{s-1}]$.
Como adotamos a ordem *lex* com $X_s > \ldots > X_1$, $MP(F) = X_s^m$. Então, X_s^m deve ser divisível pelo monômio principal de algum $g \in G$, donde segue que, necessariamente, $MP(g)$ deve ser uma potência de X_s. □

Proposição 4.6. *Se X_s é integral sobre o anel $K[X_1, X_2, \ldots, X_{s-1}, X_{i_j}, \ldots, X_{i_\delta}]$ mod $\mathcal{P}$ (onde $X_{i_j}, \ldots, X_{i_\delta}$ são as variáveis em $T_\mathcal{P}$ maiores que X_s), então X_s é integral sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}$.*

Prova. Seja $F := X_s^m + H(X_1, \ldots, X_{s-1}, X_s, X_{i_j}, \ldots, X_{i_\delta}) \in \mathcal{P}$, com grau de H em X_s menor do que m. Se $MP(F)$ está em $K[X_1, \ldots, X_s]$, então $F \in K[X_1, \ldots, X_s]$, pois adotamos a ordem *lex* com $X_s < X_{i_j} < \ldots < X_{i_\delta}$, (neste caso, $MP(F) = X_s^m$). Logo, X_s é integral sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}$.
Suponha que $MP(F) = \mu\nu$, com μ sendo um monômio em $K[X_1, \ldots, X_s]$ e $\nu \neq 1$ um monômio em $K[X_{i_j}, \ldots, X_{i_\delta}]$. Notamos que X_s deve aparecer em μ com grau $< m$.
Considere $g \in K[X_1, \ldots, X_{s-1}, X_s, X_{i_j}, \ldots, X_{i_\delta}] \cap G$. O fato de X_{i_δ} pertencer a $T_\mathcal{P}$ implica $g \in K[X_1, \ldots, X_s, X_{i_j}, \ldots, X_{i_{\delta-1}}]$; podemos aplicar o mesmo argumento, sucessivamente, para $X_{i_{\delta-1}}, \ldots, X_{i_j}$. Assim, vemos que $g \in K[X_1, \ldots, X_s]$.
Em particular, $F \notin G$. Seja p o polinômio de G cujo monômio principal é divisor de $MP(F)$. Pelo que observamos anteriormente, $p \in K[X_1, \ldots, X_s]$.
Temos: $MP(F) = \nu\xi MP(p)$, para certo ξ monômio em $K[X_1, \ldots, X_s]$. Note que todos os monômios de $\xi\ p$ têm grau $< m$ em X_s.
Faça $F_1 := F - \alpha\xi\nu p$, com $\alpha \in K$ tal que $\alpha\xi\nu TP(p) = TP(F)$.
Então, $F_1 = X_s^m + H_1(X_1, \ldots, X_{s-1}, X_s, X_{i_j}, \ldots, X_{i_\delta}) \in \mathcal{P}$, com grau de H_1 em X_s menor do que m. Se $MP(F_1)$ está em $K[X_1, \ldots, X_s]$, a proposição está provada. Caso contrário, $MP(F_1) = \mu_1\nu_1$, com μ_1 sendo um monômio em $K[X_1, \ldots, X_s]$ e $\nu_1 (\neq 1)$, um monômio em $K[X_{i_j}, \ldots, X_{i_\delta}]$. Destacamos que $MP(F) > MP(F_1)$. Assim, podemos repetir o argumento acima, e após um número finito de passos chegamos a

$$F' := X_s^m + H'(X_1, \ldots, X_{s-1}, X_s, X_{i_j}, \ldots, X_{i_\delta}) \in \mathcal{P},$$

com $MP(F') = X_s^m$. Conseqüentemente, $F' \in K[X_1, \ldots, X_s]$ fornece a relação desejada: X_s é integral sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}$. □

A partir deste ponto, estamos assumindo que $dim\ \mathcal{P} = d$; logo, pela Proposição 4.3(i), $card(T_{\mathcal{P}}) = d$. Suponha então que $T_{\mathcal{P}} = \{X_{i_1}, \ldots, X_{i_d}\}$ e sejam $X_{i_{d+1}}, \ldots, X_{i_n}$ as variáveis que não estão em $T_{\mathcal{P}}$. Podemos arranjar esses índices de tal forma que:

$$X_{i_1} < \ldots < X_{i_d} \text{ e } X_{i_{d+1}} < \ldots < X_{i_n}.$$

Fazendo $Y_\delta := X_{i_\delta}$, definimos uma permutação das variáveis tal que as d primeiras $Y_1, \ldots, Y_d$ são exatamente as algebricamente independentes mod $\mathcal{P}$.
Após tal permutação, é bem possível que G não seja mais uma base de Gröbner para $\mathcal{P}$ com relação à ordem *lex* $Y_1 < Y_2 < \ldots < Y_n$. Mesmo assim, ainda podemos usar G para reconhecer as variáveis Y_s que são integrais sobre $K[Y_1, \ldots, Y_{s-1}]$. Para isso, observamos que:

Corolário 4.7. *Com a permutação de variáveis dada acima, $Y_s = X_j$ é integral sobre $K[Y_1, \ldots, Y_{s-1}]$ mod $\mathcal{P}$ se, e somente se, X_j é integral sobre $K[X_1, \ldots, X_{j-1}]$ mod $\mathcal{P}$.*

Prova. ($\Rightarrow$) Suponha que $X_j = X_{i_s}$ é integral sobre $K[X_{i_1}, \ldots, X_{i_{s-1}}]$ mod $\mathcal{P}$. Pela forma com que arranjamos os índices dos X_{i_δ}, se $X_{i_r} > X_{i_s}$ e $r < s$ então certamente $X_{i_r} \in T_{\mathcal{P}}$. Com isso, segue da Proposição 4.6 que X_j é integral sobre $K[X_1, \ldots, X_{j-1}]$ mod $\mathcal{P}$.
($\Leftarrow$) Suponha que $Y_s = X_{i_s} = X_j$ é integral sobre $K[X_1, \ldots, X_{j-1}]$ mod $\mathcal{P}$. Então, da Proposição 4.5 segue que $X_j \notin T_{\mathcal{P}}$ e, portanto, $X_{i_s} < \ldots < X_{i_n}$. Assim, se $Y_r = X_{i_r} = X_l$, para $1 \leq l \leq j-1$, devemos ter $r < s$. □

Com esse corolário e a Proposição 4.5, podemos então calcular o conjunto

$$J := \{s \mid Y_s \text{ é integral sobre } K[Y_1, \ldots, Y_{s-1}] \text{ mod } \mathcal{P}\}.$$

Claramente, todo $s \in J$ é maior do que d.

Considerando o que discutimos acima, podemos assumir então que $\{X_1, \ldots, X_d\}$ é o conjunto das variáveis algebricamente independentes mod $\mathcal{P}$, e J é o conjunto dos índices s ($s > d$) tais que X_s é integral sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}$. Sendo assim, para encerrar a prova do Teorema 4.1, precisamos encontrar uma transformação de coordenadas que mantenha a propriedade já conseguida para as primeiras d variáveis e faça com que todas as demais $X_{d+1}, \ldots, X_n$ sejam integrais sobre $K[X_1, \ldots, X_d]$ mod $\mathcal{P}$.

Tendo esse objetivo, primeiro vamos considerar as matrizes $A(n \times n)$ da forma,

$$A := \left(\begin{array}{c|ccccc} & 0 & \ldots & \lambda_1 & \ldots & 0 \\ Id_d & \vdots & \vdots & \vdots & \vdots & \vdots \\ & 0 & \ldots & \lambda_d & \ldots & 0 \\ \hline 0 & \multicolumn{5}{c}{Id_{n-d}} \end{array}\right),$$

onde os $\lambda_i's$ estão na r-ésima coluna $(r > d)$.

A estabelece uma mudança de coordenadas:

$$X'_i := X_i + \lambda_i X_r, \text{ se } i \leq d.$$

Proposição 4.8. *Para quase toda d-upla $\Lambda = (\lambda_1, \ldots, \lambda_d)$ (isto é, para todas as d-uplas Λ que não são zeros de um certo polinômio em d variáveis), temos:*

(1) $X'_1, \ldots, X'_d$ *são algebricamente independentes mod $\mathcal{P}$;*

(2) X'_r $(= X_r)$ *é integral sobre $K[X'_1, \ldots, X'_d]$ mod $\mathcal{P}$;*

(3) X'_s $(= X_s)$ $(s > d, s \neq r)$ *integral sobre $K[X_1, \ldots, X_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}$ implica X'_s integral sobre $K[X'_1, \ldots, X'_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}$;*

(4) *No caso em que $r < s$, se X_s é algébrico mod $\mathcal{P}$, mas não é integral sobre o anel $K[X_1, \ldots, X_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}$, então $X'_s (= X_s)$ é algébrico e não integral sobre $K[X'_1, \ldots, X'_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}$.*

Prova. É claro que $K[X'_1, \ldots, X'_d, X_r] = K[X_1, \ldots, X_d, X_r]$.
Seja $\mathcal{Q} = \mathcal{P} \cap K[X_1, \ldots, X_d, X_r] \neq (0)$, já que $X_r \notin T_{\mathcal{P}}$. Então, $dim\ \mathcal{Q} = d \Rightarrow h(\mathcal{Q}) = 1$ e, daí, $\mathcal{Q} = (F)$, para algum $F \neq 0$ (lembrando que, em domínios fatoriais, um ideal tem altura 1 se e somente se ele é principal). Podemos escrever $F = F_0 + F_1 + \ldots + F_m$, onde F_j é a componente homogênea de grau j. Em particular,

$$F_m(X_1, \ldots, X_d, X_r) = \sum_{i_1 + \ldots + i_d + i_r = m} a_{i_1, \ldots, i_d, i_r} X_1^{i_1} \ldots X_d^{i_d} X_r^{i_r},$$

com $a_{i_1, \ldots, i_d, i_r} \in K$.
Vamos expressar F com relação a $X'_1, \ldots, X'_d, X_r$. Se usarmos as relações $X'_i := X_i + \lambda_i X_r$ $(i = 1, \ldots, d)$ e tratarmos F como um polinômio em X_r com coeficientes em $K[X'_1, \ldots, X'_d]$, obtemos

$$F = F_m(-\lambda_1, -\lambda_2, \ldots, -\lambda_d, 1) X_r^m + F'$$

com o grau de F' em X_r menor do que m. Como K é infinito, temos infinitos valores para λ_i $(i = 1, \ldots, d)$ tais que $F_m(-\lambda_1, -\lambda_2, \ldots, -\lambda_d, 1) \neq 0$. Logo, X_r é integral sobre $K[X'_1, \ldots, X'_d]$ mod $\mathcal{Q}$ e, portanto, mod $\mathcal{P}$, provando (2); além disso, neste caso, $X'_1, \ldots, X'_d$ são algebricamente independentes mod $\mathcal{Q}$, e daí também o são mod $\mathcal{P}$, o que prova (1).
(3) Seja X_s integral sobre $K[X_1, \ldots, X_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}$.
Se $r < s$, temos $K[X'_1, \ldots, X'_d, X_{d+1}, \ldots, X_{s-1}] = K[X_1, \ldots, X_d, X_{d+1}, \ldots, X_{s-1}]$ e não há nada a provar. Se $r > s$, então existe

$$g_0 + g_1 X_s + \ldots + g_{p-1} X_s^{p-1} + X_s^p \in \mathcal{P},$$

com $g_0, g_1, \ldots, g_{p-1} \in K[X_1, \ldots, X_d, X_{d+1}, \ldots, X_{s-1}]$.
Daí,

$$g_0(X'_1 - \lambda_1 X_r, \ldots, X'_d - \lambda_d X_r, X_{d+1}, \ldots, X_{s-1}) + \ldots +$$
$$+ g_{p-1}(X'_1 - \lambda_1 X_r, \ldots, X'_d - \lambda_d X_r, X_{d+1}, \ldots, X_{s-1}) X_s^{p-1} + X_s \in \mathcal{P}.$$

Isso mostra que X_s é integral sobre $K[X'_1, \ldots, X'_d, X_{d+1}, \ldots, X_{s-1}, X_r]$ mod $\mathcal{P}$; e, como X_r é integral sobre $K[X'_1, \ldots, X'_d]$ mod $\mathcal{P}$, segue da transitividade da dependência integral que X_s é integral sobre $K[X'_1, ..., X'_d, X_{d+1}, ..., X_{s-1}]$ mod $\mathcal{P}$.
A prova de (4) é imediata pois, se $r < s$ $(s > d)$, então

$$K[X'_1, \ldots, X'_d, X_{d+1}, \ldots, X_{s-1}] = K[X_1, \ldots, X_d, X_{d+1}, \ldots, X_{s-1}]. \qquad \square$$

Agora, vamos considerar as matrizes da forma

$$A := \left(\begin{array}{c|ccc} & a_{1,d+1} & \cdots & a_{1n} \\ Id_d & \vdots & & \vdots \\ & a_{d,d+1} & \cdots & a_{dn} \\ \hline 0 & \multicolumn{3}{c}{Id_{n-d}} \end{array}\right),$$

com $a_{1s} = a_{2s} = \ldots = a_{ds} = 0$, se $s \in J$.

Então A fornece a seguinte mudança de coordenadas:

$$X'_i := X_i + \textstyle\sum_{s \notin J, s>d} a_{is} X_s, \quad (i = 1, \ldots, d).$$

Usando a Proposição 4.8, indutivamente, vamos finalmente provar o resultado que encerra a demonstração do Teorema 4.1:

Proposição 4.9. *Para quase toda escolha das entradas a_{ij} de A $(i = 1, \ldots, d,\ j \notin J,\ j > d)$, tem-se:*

(1) $X'_1, \ldots, X'_d$ *algebricamente independentes mod* $\mathcal{P}$;

(2) $X_{d+1}, \ldots, X_n$ *são integrais sobre* $K[X'_1, \ldots, X'_d]$ *mod* $\mathcal{P}$.

Prova. Seja $r = \text{mín}\{s > d \mid s \notin J\}$.
Considere a transformação dada por $U_i := X_i + a_{ir} X_r$, $i = 1, \ldots, d$. Depois de tal transformação obtemos o seguinte, para $s > d$:
- se $s \notin J$ e $s \neq r$ então, pela Proposição 4.8 (4), X_s é algébrico, mas não é integral sobre $K[U_1, \ldots, U_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}$;
- se $s \in J$, então X_s é integral sobre $K[U_1, \ldots, U_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}$, pela Proposição 4.8 (3);
- se $s = r$, então X_r é integral sobre $K[U_1, \ldots, U_d]$ mod $\mathcal{P}$, por 4.8 (2).
Assim, $\{s > d \mid X_s$ é integral sobre $K[U_1, \ldots, U_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}\} = J \cup \{r\} = J'$; e ainda, $U_1, \ldots, U_d$ são algebricamente independentes mod $\mathcal{P}$, por 4.8 (1).
Podemos repetir o argumento acima para r'=mín$\{s > d \mid s \notin J'\}$, e assim por diante. Após um número finito de repetições, chegamos à matriz A desejada, tendo X_s integral sobre $K[U_1, \ldots, U_d, X_{d+1}, \ldots, X_{s-1}]$ mod $\mathcal{P}$, para cada $s = d+1, \ldots, n$.
Disso, pela transitividade da dependência integral, segue que X_s é integral sobre o anel

$K[U_1, \ldots, U_d]$ mod $\mathcal{P}$, para cada $s = d+1, \ldots, n$. E ainda $X'_1, \ldots, X'_d$ são algebricamente independentes mod $\mathcal{P}$. □

Como conseqüência direta da proposição acima e das considerações anteriores, chegamos ao algoritmo que tem como "dados de saída" a matriz de mudança de coordenadas responsável por levar um dado ideal primo $\mathcal{P}$ à sua posição normal de Noether.

Algoritmo 4.10.
Entrada: *um ideal primo $\mathcal{P}$ de $K[X_1, \ldots, X_n]$*
Saída: *uma matriz A $(n \times n)$ que leva $\mathcal{P}$ em sua posição normal de Noether, com relação às variáveis $X := AX$*

Passo 1: *calcule uma base de Gröbner G para $\mathcal{P}$, com relação à ordem lex $X_1 < \ldots < X_n$; com o Algoritmo 4.2 determine $T_{\mathcal{P}}$; $A := Id_{\,n\times n}$*

Passo 2: *permute as variáveis de modo que $X_1, \ldots, X_d$ sejam os elementos de $T_{\mathcal{P}}$ e $X_{d+1}, \ldots, X_n$, os demais.*
Após a permutação, adote em $K[X_1, \ldots, X_n]$ a ordem lex com $X_1 < \ldots < X_n$.
Defina A_1 como sendo a matriz que fornece essa transformação.
$A := A_1\, A$.

Passo 3: *Calcule $J := \{s \mid X_s$ é integral sobre $K[X_1, \ldots, X_{s-1}]$ mod $\mathcal{P}\}$.*
(usando o Corolário 4.7 e a Proposição 4.5)

Passo 4: *PARA $r := 1$ a d faça*
$a_{rr} := 1$; $a_{ir} := 0$ *para* $i \neq r$;
PARA $r := d+1$ a n faça

SE $r \in J$ ENTÃO
$a_{rr} := 1$; $a_{ir} := 0$ *para* $i \neq r$;
CASO CONTRÁRIO, se $r \notin J$
escolha aleatoriamente $a_{1r}, a_{2r}, \ldots, a_{dr} \in K$;
$X_i := X_i + a_{ir}X_r$, *para* $i = 1, \ldots, d$;
$a_{rr} := 1$; $a_{ir} := 0$, *para* $i \neq r, i > d$;
$A_2 := (a_{ij})$;
$A := A_2 A$;

Passo 5: *calcular uma base de Gröbner G de $\mathcal{P}$ em relação a $X := AX$ com respeito à ordem lex $X_1 < \ldots < X_n$.*

Passo 6: *SE "$G \cap K[X_1, \ldots, X_d] \neq \emptyset$" ou "existe s, com $d+1 \leq s \leq n$ tal que nenhuma potência de X_s aparece como monômio principal de um polinômio de G" (Proposição 4.5) ENTÃO volte ao Passo 2.*

Esse algoritmo termina com $\mathcal{P}$ na posição normal de Noether, com relação às novas variáveis $X := AX$. □

Exemplo 4.11. *Considere o ideal primo, obtido no Exemplo 2.35,*

$$\mathcal{P} = (YW - Y - Z^2,\ X - ZW + Z) \subset \mathbf{C}[X, Y, Z, W].$$

Encontraremos a mudança de variáveis que leva $\mathcal{P}$ em sua posição normal de Noether.

Passo 1: Adotando a ordem *lex* $W > Z > Y > X$, calculamos a base de Gröbner reduzida para $\mathcal{P}$, obtendo

$$G = \{Z^3 - YX, WY - Z^2 - Y, WZ - Z - X\}.$$

Então, determinamos $T_{\mathcal{P}} = \{X, Y\}$.
Passo 2: $A := A_1 := Id_{4\times 4}$.
Passo 3: $J := \{Z\}$.
Passo 4: $A := A_2 := \begin{pmatrix} 1 & 0 & 0 & a_{14} \\ 0 & 1 & 0 & a_{24} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Escolhendo por exemplo $a_{14} = a_{24} = 1$, consideramos a mudança de coordenadas:

$$X := X + W,\ Y := Y + W,\ Z := Z,\ W := W.$$

Passo 5: Feita a mudança de coordenadas, calculamos a base de Gröbner reduzida para $\mathcal{P} := (W^2+WY-W-Z^2-Y, -WZ+W+Z+X)$, com relação à ordem *lex* $W > Z > Y > X$, obtendo

$$\begin{aligned} G := \{&Z^4 - 2Z^3 + Z^2 - ZYX - ZY - ZX - Z + YX + Y - X^2 - X, \\ &WX + W - Z^3 + Z^2 + YX + Y,\ WZ - W - Z - X, \\ &W^2 + WY - W - Z^2 - Y\}. \end{aligned}$$

Passo 6: Vemos que $G \cap K[X, Y] = \emptyset$ e potências de Z e de W aparecem como monômios principais de elementos de G.
Logo o Algoritmo 4.9 termina: o ideal $(W^2 + WY - W - Z^2 - Y, -WZ + W + Z + X)$ é a posição normal de Noether do ideal inicial $\mathcal{P}$.

Observe que se tivéssemos feito $a_{14} = a_{24} = 0$, o algoritmo não terminaria logo no primeiro *loop*, ou seja, $\mathcal{P}$ não foi dado já em sua posição normal de Noether.

Capítulo 5

Algoritmos para o Teorema de Quillen-Suslin

Apresentaremos neste capítulo um estudo do artigo [8] de A. Logar e B. Sturmfels, que fornece um algoritmo para calcular uma base livre para um dado $\mathbf{C}[x_1, \ldots, x_n]$-módulo projetivo, apresentado como imagem, kernel ou cokernel de uma matriz polinomial. ($\mathbf{C}$ denota o corpo dos números complexos).
Conseqüentemente, obtém-se uma nova prova para a **Conjectura de Serre** (1955) – *todo módulo projetivo sobre um anel de polinômios é livre* – provada em 1976 por D. Quillen e A. Suslin, simultânea e independentemente, para módulos finitamente gerados.

5.1 Notas Preliminares

Vamos recordar, brevemente, alguns conceitos básicos em Álgebra Comutativa dos quais faremos uso durante o estudo proposto aqui. Para introdução e detalhes da teoria, nossas principais referências são os livros-textos [3] e [6].

Módulos Projetivos

Seja R um anel qualquer. Um R-módulo M é dito ser *projetivo* se existe um R-módulo M' tal que a soma direta $M \oplus M'$ é livre.
Equivalentemente: um R-módulo M é projetivo se, e somente se, qualquer seqüência exata de R-módulos da forma

$$0 \longrightarrow C \xrightarrow{\alpha} D \xrightarrow{\beta} M \longrightarrow 0$$

cinde (isto é, existe um R-homomorfismo $\gamma : M \to D$ com $\beta(\gamma(m)) = m, \ \forall m \in M$).

Proposição 5.1. *Se a seqüência exata* $0 \longrightarrow C \xrightarrow{\alpha} D \xrightarrow{\beta} M \longrightarrow 0$ *cinde, então:*
(a) D *é* R*-isomorfo a* $C \oplus M$*;*
(b) existe $\delta : D \to C$ *homomorfismo tal que* $\delta(\alpha(c)) = c, \forall c \in C$.

Prova. Seja $\gamma : M \to D$ o homomorfismo tal que $\beta(\gamma(m)) = m, \forall m \in M$. A prova de (a) é dada pelo R-isomorfismo $\psi : C \oplus M \to D$, $(c, m) \mapsto \alpha(c) + \gamma(m)$. (b) segue da composição

$\pi \circ \psi^{-1}$, onde π é a projeção de $C \oplus M$ em C e ψ^{-1} é a inversa de ψ. □

Seja R um anel qualquer. Um R-módulo M é dito ser *estavelmente livre* se existe um R-módulo livre F tal que $M \oplus F$ é um R-módulo livre.

Proposição 5.2. *(Serre) Seja P um módulo projetivo sobre um anel R. Se P tem um resolução livre finita, então P é estavelmente livre.*

Prova. Seja

$$0 \longrightarrow F_n \xrightarrow{\alpha_{n-1}} F_{n-1} \xrightarrow{\alpha_{n-2}} \cdots \xrightarrow{\alpha_1} F_1 \xrightarrow{\alpha_0} F_0 \xrightarrow{\epsilon} P \longrightarrow 0$$

uma resolução livre de P. Como P é projetivo, a seqüência exata

$$0 \longrightarrow im\ \alpha_0 \longrightarrow F_0 \longrightarrow P \longrightarrow 0$$

cinde, implicando $F_0 \simeq P \oplus im\ \alpha_0$. Daí, $im\ \alpha_0$ é também projetivo. Conseqüentemente a seqüência exata

$$0 \longrightarrow im\ \alpha_1 \longrightarrow F_1 \longrightarrow im\ \alpha_0 \longrightarrow 0$$

cinde, implicando $F_1 \simeq im\ \alpha_0 \oplus im\ \alpha_1$.
Repetindo esse procedimento, indutivamente, vemos que $F_i \simeq im\ \alpha_{i-1} \oplus im\ \alpha_i$, para cada $1 \leq i \leq n-1$. Donde segue que:

$$\begin{aligned} P \oplus im\ \alpha_0 \simeq F_0 \Rightarrow P \oplus im\ \alpha_0 \oplus im\ \alpha_1 \oplus im\ \alpha_2 \oplus \ldots \oplus im\ \alpha_{n-1} \simeq \\ \simeq F_0 \oplus im\ \alpha_1 \oplus im\ \alpha_2 \oplus \ldots \oplus im\ \alpha_{n-1} \\ \Rightarrow P \oplus F_1 \oplus F_3 \oplus \ldots \simeq F_0 \oplus F_2 \oplus F_4 \oplus \ldots \end{aligned}$$

Portanto, $P\oplus$ módulo livre $\simeq$ módulo livre. □

Da proposição acima e do teorema dos Syzygies de Hilbert (Corolário 3.12) segue que: *todo módulo projetivo finitamente gerado sobre o anel de polinômios $K[x_1, \ldots, x_n]$, onde K é um corpo, é estavelmente livre.*

Ideais Fitting

Alguns dos nossos argumentos futuros usarão *ideais Fitting*. Enunciaremos apenas os resultados que, pelo contexto, nos interessam diretamente. Para introdução e detalhes da teoria, veja [3].

Sejam F, G módulos livres finitamente gerados, sobre um anel R qualquer, de postos r e s, respectivamente, e seja $\varphi : F \longrightarrow G$ um R-homomorfismo.
Escolhidas bases para F e G, φ é representado por uma matriz $s \times r$ com entradas em R.
O ideal gerado pelos *menores* da matriz de φ (isto é, determinantes das submatrizes) de tamanho j independe das bases escolhidas para F e G, e é então denotado por $I_j\varphi$. Convenciona-se que $I_j\varphi = R$, para $j \leq 0$.

O teorema a seguir diz que esses ideais de menores são invariantes em um módulo.

Teorema 5.3. **(Lema de Fitting)** *Sejam M um R-módulo finitamente gerado e*

$$\varphi : F \to G \to M \to 0,\ \varphi' : F' \to G' \to M \to 0$$

duas apresentações, com G e G' R-módulos livres de postos finitos r e r'.
Para cada número $0 \leq i < \infty$ temos $I_{r-i}\varphi = I_{r'-i}\varphi'$, e define-se o i-ésimo Fitting invariante de M sendo o ideal

$$Fitt_i(M) = I_{r-i}\varphi \subset R.$$

Os ideais Fitting funcionam como um "termômetro" para indicar o número de geradores para um módulo, no seguinte sentido: para um anel local R, um R-módulo M pode ser gerado por j elementos se, e somente se, $Fitt_j(M) = R$.
No caso geral, R um anel qualquer e M um R-módulo, o 0-ésimo Fitting está contido no anulador de M. Além disso, os ideais Fitting testam a "projetividade": M é projetivo de posto constante r se, e somente se, $Fitt_r(M) = R$ e $Fitt_{r-1}(M) = 0$.
(As provas desses resultados baseiam-se, essencialmente, em localização e na unicidade de resoluções livres minimais, vide [3].)

O Teorema de Quillen-Suslin

Por simplicidade de exposição, o estudo que se segue é restrito ao corpo $\mathbf{C}$ dos números complexos.

Seja P um módulo projetivo finitamente gerado sobre $R := \mathbf{C}[x_1, \ldots, x_n]$. Como P é estavelmente livre, $P \oplus R^l \simeq R^m$ $(l \leq m)$. Então, P é isomorfo ao kernel de um R-epimorfismo $A : R^m \to R^l$. Considere a matriz A' $(l+m) \times m$ sobre R definida por

$$A' = \begin{pmatrix} A \\ 0 \end{pmatrix},\ \text{e a apresentação } A' : R^m \longrightarrow R^l \times R^m \xrightarrow{\pi} R^m \longrightarrow 0,$$

onde π é a projeção sobre as m últimas coordenadas. Assim, temos

$$R = Fitt_m(R^m) = I_{(l+m)-m}A' = I_l A' = I_l A.$$

Ou seja, a unidade em R está no ideal gerado pelos menores maximais da matriz A. Uma matriz que satisfaz essa propriedade é chamada *unimodular*.

Dessa forma, mostrar que P é livre é o mesmo que provar o seguinte resultado:

Teorema 5.4. **(Quillen-Suslin)** *Seja A uma $(l \times m)$-matriz unimodular $(l \leq m)$ sobre $R := \mathbf{C}[x_1, \ldots, x_n]$. Então, existe uma $(m \times m)$-matriz unimodular U sobre R tal que*

$$A \cdot U = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & \ldots & 0 \end{pmatrix}$$

Na Seção 5.3, consideraremos um R-módulo projetivo P qualquer, que é apresentado como imagem, kernel ou cokernel de uma matriz polinomial (não necessariamente unimodular). Então, será mostrado como calcular uma base livre para P, usando o algoritmo da Seção 5.2 como subrotina.

Corolário 5.5. *Na situação do Teorema 5.4, as últimas $m-l$ colunas de U formam uma base do R-módulo livre $ker(A) \subset R^m$.*

Prova. Denotamos por $u'_{l+1}, \ldots, u'_m \subset R^m$ as $m-l$ últimas colunas de U. Identificamos R^l com o subconjunto de R^m formado pelos elementos que possuem as $m-l$ últimas coordenadas todas nulas, e R^{m-l} com os elementos de R^m que possuem as l primeiras coordenadas todas nulas.
Inicialmente, observamos que restrita ao $kerA$, $\varphi : kerA \xrightarrow{U^{-1}} R^{m-l}$ é um R-isomorfismo. De fato, φ é um R-homomorfismo injetivo, pois U^{-1} o é; resta mostrar que φ está bem definido e é sobrejetivo.
Para qualquer $x \in kerA$, $(A \cdot U \cdot U^{-1})(x) = 0$. Se $U^{-1}(x) := y = (y_1, \ldots, y_m)$ está em R^m, então $(A \cdot U)(y_1, \ldots, y_m) = (y_1, \ldots, y_l, 0, \ldots, 0) = 0$; o que implica $y_1 = \ldots = y_m = 0$. Logo, $y \in R^{m-l} \subset R^m$.
Agora, seja $y \in R^{m-l}$ qualquer. Como U^{-1} é sobrejetiva, existe $x \in R^m$ tal que $U^{-1}(x) = y = (0, \ldots, 0, y_{l+1}, \ldots, y_m)$. Daí, $A(x) = (A \cdot U \cdot U^{-1})(x) = (A \cdot U)(0, \ldots, 0, y_{l+1}, \ldots, y_m) = 0$. Assim, mostramos que de fato U^{-1} induz um R-isomorfismo entre $kerA$ e R^{m-l}, o que significa que $kerA$ é livre de posto $m-l$.
Como U é invertível, suas colunas formam um conjunto linearmente independente. Logo, $u'_{l+1}, \ldots, u'_m \subset kerA$ são linearmente independentes e, portanto, formam uma base para $kerA$. □

Vale notar ainda que, na situação do Teorema 5.4, A é igual às l primeiras linhas de U^{-1}. Assim, encontrar U é equivalente a completar A para uma matriz quadrada invertível.

5.2 Cálculo de uma Base Livre para Módulos Estavelmente Livres

O algoritmo para o Teorema 5.4 será dado por indução sobre o número l de linhas da matriz A. Assim, o problema é reduzido às *linhas unimodulares.*

Teorema 5.6. (*Propriedade da Linha Unimodular*)
Seja $\mathtt{f} = (f_1, \ldots, f_m) \in \mathbf{C}[x_1, \ldots, x_n]^m$ *uma linha unimodular (os elementos $f_1, \ldots, f_m$ geram a unidade em $\mathbf{C}[x_1, \ldots, x_n]$). Então, existe uma $(m \times m)$-matriz unimodular sobre $\mathbf{C}[x_1, \ldots, x_n]$ tal que $\mathtt{f} \cdot U = (1, 0, \ldots, 0)$.*

Prova. Caso I: Se $m = 1$, óbvio!

Caso II: Se $m = 2$ ou $n = 1$. Se $m = 2$, a unidade está no ideal gerado por f_1, f_2 em $\mathbf{C}[x_1, \ldots, x_n]$, então usando o algoritmo de Buchberger, calculamos $h_1, h_2 \in \mathbf{C}[x_1, \ldots, x_n]$ tais que $h_1 f_1 + h_2 f_2 = 1$. Logo,

$$U := \begin{pmatrix} h_1 & -f_2 \\ h_2 & f_1 \end{pmatrix}$$

é tal que $\mathtt{f} \cdot U = (1, 0)$.

Se $n = 1$, U é o produto de certas matrizes elementares, obtidas de forma algorítmica da seguinte maneira:
Permutando as colunas de $\mathtt{f}$ chegamos a $\mathtt{f}' = (f'_1, \ldots, f'_m)$, linha equivalente a $\mathtt{f}$, tendo f'_1 sua entrada de menor grau.
Para cada $j \geq 2$ com $f'_j \neq 0$, faça a divisão de Euclides de f'_j por f'_1:

$$f'_j = q_j f'_1 + r_j,$$

com $r_j = 0$ ou $\text{grau}(r_j) < \text{grau}(f'_1)$.
Substitua a j-ésima coluna de $\mathtt{f}'$ por

(j-ésima coluna) - $q_j \cdot$ (primeira coluna),

obtendo $\mathtt{f}^{(1)} = (f_1{}^{(1)}, \ldots, f_m{}^{(1)})$, linha equivalente $\mathtt{f}$.
Repita o procedimento anterior para $\mathtt{f}^{(1)}$ no lugar de $\mathtt{f}$; e assim sucessivamente.
Dessa forma, após um número finito de passos, chegamos à linha

$$(MDC(f_1, \ldots, f_m), 0, \ldots, 0),$$

equivalente a $\mathtt{f}$.
Para concluir esse caso, basta lembrar que se $\mathtt{f} = (f_1, \ldots, f_m) \in \mathbf{C}[x_1]^m$ é uma linha unimodular então $MDC(f_1, \ldots, f_m) = 1$.

Caso III: Se $n \geq 2$ e $m \geq 3$. O procedimento será por indução sobre o número n de variáveis.
Como $\mathbf{C}$ é infinito, podemos fazer uma mudança K-linear de variáveis e rearranjar os $f_i's$ obtendo $f_1(x_1, \ldots, x_{n-1}, t)$ mônico em $t = x_n$ (veja a prova da Proposição 4.8(2)).
Fazemos $R := \mathbf{C}[x]$ em que $x = (x_1, \ldots, x_{n-1})$, e $k := 0$.

LOOP LOCAL

$k := k + 1$.
Usando bases de Gröbner, encontre $a_k = (a_k^{(1)}, \ldots, a_k^{(n-1)}) \in \mathbf{C}^{n-1}$ um zero comum de $r_1, \ldots, r_{k-1}$ (a_1 é aleatório).
Considere $\mathcal{M}_k = \{g \in R \mid g(a_k) = 0\}$; note que $\mathcal{M}_k$ é o ideal maximal de R gerado por $x_1 - a_k^{(1)}, \ldots, x_{n-1} - a_k^{(n-1)}$.
Defina $\tilde{f}_i(t) := f_i(a_k, t)$, para todo $1 \leq i \leq m$.
Calcule o polinômio $p := MDC(\tilde{f}_2, \ldots, \tilde{f}_m)$ usando o algoritmo de Euclides em $\mathbf{C}[t]$, e ainda, a matriz unimodular $E(t)$, $(m-1) \times (m-1)$, produto de matrizes elementares, tal que

$$(\tilde{f}_2(t), \ldots, \tilde{f}_m(t)) \cdot E(t) = (p(t), 0, \ldots, 0) \tag{1}$$

Como $\mathtt{f}(a_k, t) = (\tilde{f}_1, \tilde{f}_2, \ldots, \tilde{f}_m)$ é uma linha unimodular sobre $\mathbf{C}[t]$ e p é o gerador do ideal $\langle \tilde{f}_2, \ldots, \tilde{f}_m \rangle$ em $\mathbf{C}[t]$,

$$\langle \tilde{f}_1 \rangle + \langle p \rangle = \mathbf{C}[t] \tag{2}$$

Da definição de $\tilde{f}_i$ segue que $f_i(x,t) - \tilde{f}_i(t) = h_i(x,t) \in \mathcal{M}_k[t]$.
Então, usando (1), obtemos:

$$\mathtt{f}(x,t) \cdot \begin{pmatrix} 1 & 0 \\ 0 & E(t) \end{pmatrix} = (f_1, \ldots, f_m) \cdot \begin{pmatrix} 1 & 0 \\ 0 & E(t) \end{pmatrix}$$

$$= (f_1, \tilde{f}_2 + h_2, \ldots, \tilde{f}_m + h_m) \cdot \begin{pmatrix} 1 & 0 \\ 0 & E(t) \end{pmatrix}$$

$$= (f_1, (\tilde{f}_2, \ldots, \tilde{f}_m) \cdot E(t) + (h_2, \ldots, h_m) \cdot E(t))$$

$$= (f_1, (p, 0, \ldots, 0) + (q_2, \ldots, q_m)).$$

Portanto,

$$f(x,t) \cdot \begin{pmatrix} 1 & 0 \\ 0 & E(t) \end{pmatrix} = (f_1(x,t), p(t) + q_2(x,t), q_3(x,t), \ldots, q_m(x,t)), \tag{3}$$

com $q_i \in \mathcal{M}_k[t]$, para todo i.
Se $p + q_2 \in R$, defina $r_k := p + q_2$, $v(x,t) := 0$, $w(x,t) := 1$. Caso contrário, calcule o resultante $r_k(x) \in \langle f_1, p + q_2 \rangle \cap R$ dos dois polinômios f_1 e $p + q_2$, com relação à variável t, e usando bases de Gröbner encontre $v, w \in R[t]$ tais que

$$v(x,t) \cdot f_1(x,t) + w(x,t) \cdot [p(t) + q_2(x,t)] = r_k(x) \tag{4}$$

Como f_1 é mônico em t, a teoria de resultantes (ver Cox e O'Shea [2]) nos diz que: *para* $x_0 \in \mathbf{C}^{n-1}, r_k(x_0) = 0$ *se, e somente se,* $f_1(x_0,t)$ *e* $p(t) + q_2(x_0,t)$ *têm uma raiz comum em* $\mathbf{C}$. Assim, como $q_2 \in \mathcal{M}_k[t]$ implica $q_2(a_k,t) = 0$, e de (2) segue que $f_1(a_k,t)$ e $p(t)$ não têm zeros comuns, devemos ter $r_k(a_k) \neq 0$.
Então, $r_k \notin \mathcal{M}_k$; o que significa que r_k é invertível no anel local correspondente $R_{\mathcal{M}_k}$, e a $(m \times m)$-matriz $U_k(x,t)$ definida pelo produto

$$U_k(x,t) := \begin{pmatrix} 1 & 0 \\ 0 & E(t) \end{pmatrix} \begin{pmatrix} v{r_k}^{-1} & -p - q_2 & & & \\ w{r_k}^{-1} & f_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -q_3 & \cdots & -q_m \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \tag{5}$$

é unimodular sobre $R_{\mathcal{M}_k}[t]$. Afirmamos que

$$\mathtt{f}(x,t) \cdot U_k(x,t) = (1, 0, \ldots, 0) \tag{6}$$

De fato, por (3), temos:

$$\mathtt{f}(x,t)\begin{pmatrix} 1 & 0 \\ 0 & E(t) \end{pmatrix} = (f_1, p+q_2, q_3, \ldots, q_m);$$

agora, usando (4), vemos que:

$$(f_1, p+q_2, q_3, \ldots, q_m)\begin{pmatrix} {vr_k}^{-1} & -p-q_2 & & & \\ {wr_k}^{-1} & f_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} =$$

$$= (f_1 {vr_k}^{-1} + (p+q_2){wr_k}^{-1}, 0, q_3, \ldots, q_m) = (1, 0, q_3, \ldots, q_m);$$

e, finalmente:

$$(1, 0, q_3, \ldots, q_m)\begin{pmatrix} 1 & 0 & -q_3 & \ldots & -q_m \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} = (1, 0, \ldots, 0);$$

o que prova nossa afirmação.

Obviamente, se $r_k \in \mathbf{C}$, em algum estágio k, esse *loop* já é suficiente para fornecer a matriz invertível U desejada: $U = U_k$.

De modo geral, usamos o seguinte critério para encerrar o *loop* local: calcule uma base de Gröbner reduzida G para o ideal $\langle r_1, \ldots, r_k \rangle$; se $G = \{1\}$, então saia do *loop*; caso contrário, volte ao início.
Ou seja, o *loop* termina quando $\langle r_1, \ldots, r_k \rangle = R$.
Note que $r_k \notin \langle r_1, \ldots, r_{k-1} \rangle$, em cada passo k, pois $r_k \in \langle r_1, \ldots, r_{k-1} \rangle$ implicaria $r_k(a_k) = 0$, já que a_k é tomado em $\mathcal{V}(r_1, \ldots, r_{k-1})$.
Dessa forma, construímos uma cadeia estritamente ascendente de ideais em R; do teorema da Base de Hilbert segue que, necessariamente, a condição para o término do *loop* será atingida após um número finito de passos.

Ao sair do *loop* teremos então $\langle r_1, \ldots, r_k \rangle = R$. Logo, $\langle {r_1}^m, \ldots, {r_k}^m \rangle = R$ (a escolha desse expoente m ficará clara mais adiante). Usando o método de bases de Gröbner, encontramos $g_1, \ldots, g_k \in R$ tais que

$$g_1 {r_1}^m + \ldots + g_k {r_k}^m = 1 \text{ em } R \tag{7}$$

No que segue abreviamos $U_i(t) := U_i(x,t)$.

Introduza duas novas variáveis s e z e defina as matrizes

$$\Delta_i(s,z) = U_i(s) \cdot U_i^{-1}(s+z), \text{ para } i = 1, \ldots, k \tag{8}$$

unimodulares sobre $R_{\mathcal{M}_i}[s,z]$, já que U_i e U_i^{-1} o são.
Lembramos que $r_i \in R$ é um denominador comum em $U_i(s)$ e $U_i(s+z)$. A inversa de $U_i(s+z)$ é igual à sua adjunta (salvo multiplicação pelo escalar $det(U_i)$).
Na definição de U_i em (5), temos:

$$\begin{pmatrix} vr_i^{-1} & -p-q_2 & & & \\ wr_i^{-1} & f_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -q_3 & \dots & -q_m \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} vr_i^{-1} & -p-q_2 & -vr_i^{-1}q_3 & \dots & -vr_i^{-1}q_m \\ wr_i^{-1} & f_1 & -wr_i^{-1}q_3 & \dots & -wr_i^{-1}q_m \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

implicando que r_i^{m-1} é um denominador comum para as entradas de U_i^{-1}. Isso mostra que r_i^m é um denominador comum para $\Delta_i(s,z)$.

Escrevendo cada polinômio entrada de $\Delta_i(s,z)$ como polinômios na variável z com coeficientes em $R_{\mathcal{M}_i}[s]$, podemos escrever $\Delta_i(s,z)$ como um polinômio em z, cujos coeficientes são matrizes sobre $R_{\mathcal{M}_i}[t,s]$:

$$\Delta_i(s,z) = \Delta_{i0}(s) + \Delta_{i1}(s)z + \Delta_{i2}(s)z^2 + \ldots + \Delta_{id_i}(s)z^{d_i} \tag{9}$$

De (8) segue, imediatemente, que $\Delta_{i0}(s) = \Delta_i(s,0)$ é igual à matriz identidade Id_m.
Substituindo z por zr_i^m chegamos a

$$\Delta_i(s, zr_i^m) = Id_m + r_i^m\Delta_{i1}(s)z + r_i^{2m}\Delta_{i2}(s)z^2 + \ldots + r_i^{d_i m}\Delta_{id_i}(s)z^{d_i} \tag{10}$$

Como r_i^m é um denominador comum em $\Delta_i(s,z)$, também o será em todas as parcelas de Δ_i na expansão (9). Assim, em (10) elimina-se todos os denominadores, fazendo de $\Delta_i(s, zr_i^m)$ uma matriz unimodular sobre o anel de *polinômios* $R[s,z]$.
Além disso, usando (8) e (6) vemos que:

$$\begin{aligned} \mathtt{f}(s) \cdot \Delta_i(s, zr_i^m) &= \mathtt{f}(x,s) \cdot U_i(x,s) \cdot U_i^{-1}(x, s+zr_i^m) = \\ &= (1,0,\ldots,0) \cdot U_i^{-1}(x, s+zr_i^m) = \mathtt{f}(s+zr_i^m). \end{aligned}$$

Logo,

$$\mathtt{f}(s) \cdot \Delta_i(s, zr_i^m) = \mathtt{f}(s+zr_i^m) \text{ em } R[s,z] \tag{11}$$

Finalmente, defina

$$
\begin{aligned}
U(t) := \Delta_1(t, -tg_1{r_1}^m) \cdot \Delta_2(t - tg_1{r_1}^m, -tg_2{r_2}^m) \cdot \\
\Delta_3(t - tg_1{r_1}^m - tg_2{r_2}^m, -tg_3{r_3}^m) \cdot \\
\cdots \\
\Delta_{k-1}\left(t - \textstyle\sum_{i=1}^{k-2} tg_i{r_i}^m, -tg_{k-1}{r_{k-1}}^m\right) \cdot \\
\Delta_k\left(t - \textstyle\sum_{i=1}^{k-1} tg_i{r_i}^m, -tg_k{r_k}^m\right)
\end{aligned} \tag{12}
$$

As k matrizes fatores em (12) são obtidas de $\Delta_i(s, z{r_i}^m)$ por especializações polinomiais $R[s,z] \longrightarrow R[t]$, logo $U(t)$ é uma $(m \times m)$-matriz unimodular sobre $R[t]$.

Aplicando (11) k vezes em $\mathtt{f}(t) \cdot U(t)$ chegamos a

$$
\begin{aligned}
\mathtt{f}(t) \cdot U(t) = \mathtt{f}(t) \cdot \Delta_1(t, -tg_1{r_1}^m) \cdot \Delta_2 \cdots \Delta_k = \\
= \mathtt{f}(t - tg_1{r_1}^m) \cdot \Delta_2(t - tg_1{r_1}^m, -tg_2{r_2}^m) \cdot \Delta_3 \cdots \Delta_k = \\
= \mathtt{f}(t - tg_1{r_1}^m - tg_2{r_2}^m) \cdot \Delta_3 \cdots \Delta_k = \ldots = \\
= \mathtt{f}\left(t - \textstyle\sum_{i=1}^{k} tg_i{r_i}^m\right) = \mathtt{f}\left(t - t\textstyle\sum_{i=1}^{k} g_i{r_i}^m\right)
\end{aligned}
$$

Então, usando (7) obtemos:

$$\mathtt{f}(t) \cdot U(t) = \mathtt{f}(0) \tag{13}$$

A linha $\mathtt{f}(0) = (f_1(x,0), \ldots, f_m(x,0))$ é unimodular em $n-1$ variáveis. Então, por indução sobre o número de variáveis, temos $(m \times m)$-matriz U' unimodular sobre R com $\mathtt{f}(0) \cdot U' = (1, 0, \ldots, 0)$.
Daí, $U(t) \cdot U'$ é a matriz unimodular sobre $\mathbf{C}[x_1, \ldots, x_n]$ tal que

$$\mathtt{f}(t) \cdot U(t) \cdot U' = \mathtt{f}(0) \cdot U' = (1, 0, \ldots, 0);$$

o que completa o algoritmo e encerra a prova do Teorema 5.6. □

Exemplo 5.7. *Considere a linha unimodular* $\mathtt{f} = (yt + 1, xyz - 1, xzt)$ *com entradas no anel de polinômios* $\mathbf{C}[x, y, z, t]$. *Seguindo o roteiro da prova do Teorema 5.6, vamos calcular a matriz invertível* $U_{3\times 3}$ *tal que* $\mathtt{f} \cdot U = (1, 0, 0)$.

(Usamos o *software Macaulay* para auxiliar nos cálculos). Fazendo a mudança de variáveis $y := y + t$ nas entradas de $\mathtt{f}$, obtemos:

$$\mathtt{f}' := (f_1, f_2, f_3) = (t^2 + yt + 1, xyz + xzt - 1, xzt),$$

com f_1 mônico em t.
Definimos

$$a_1 := (0,0,0);\ \ \tilde{f}_1 := f_1(a_1, t) = t^2 + 1,\ \ \tilde{f}_2 := f_2(a_1, t) = -1,\ \ \tilde{f}_3 := f_3(a_1, t) = 0.$$

Assim, temos:

$$(\tilde{f}_2, \tilde{f}_3) \cdot \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = (1, 0).$$

E ainda,

$$(f_1, f_2, f_3) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (f_1, -f_2, f_3).$$

Calculamos o resultante r_1 entre f_1 e $-f_2$ com relação à variável t,

$$r_1 = det \begin{pmatrix} 1 & -xz & 0 \\ y & -xyz+1 & -xz \\ 1 & 0 & -xyz+1 \end{pmatrix} = 1 - xyz + x^2z^2,$$

e usando o método de bases de Gröbner, encontramos

$$v(x,y,z,t) = x^2z^2 - xyz - xzt + 1 \quad \text{e} \quad w(x,y,z,t) = xzt - yt - t^2,$$

tais que $v \cdot f_1 + w \cdot (-f_2) = r_1$.
Calculamos a matriz U_1,

$$U_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} {vr_1}^{-1} & f_2 & 0 \\ {wr_1}^{-1} & f_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -f_3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} {vr_1}^{-1} & f_2 & -{vr_1}^{-1}f_3 \\ -{wr_1}^{-1} & -f_1 & {wr_1}^{-1}f_3 \\ 0 & 0 & 1 \end{pmatrix},$$

e sua inversa ${U_1}^{-1}$,

$${U_1}^{-1} = \begin{pmatrix} f_1 & f_2 & f_3 \\ -{wr_1}^{-1} & -{vr_1}^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Agora, como $\langle r_1 \rangle \neq \mathbf{C}[x,y,z]$, voltamos ao início: tomamos $a_2 := (1,0,i)$ (onde i é a unidade imaginária) um zero de r_1 e calculamos $\tilde{f}_1 := f_1(a_2,t) = t^2 + 1$, $\tilde{f}_2 := f_2(a_2,t) = it - 1$, $\tilde{f}_3 := f_3(a_2,t) = it$. Daí, temos:

$$(\tilde{f}_2, \tilde{f}_3) \cdot \begin{pmatrix} -1 & -it \\ 1 & it-1 \end{pmatrix} = (1,0).$$

E ainda,

$$(f_1, f_2, f_3) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -it \\ 0 & 1 & it-1 \end{pmatrix} = (f_1, -xyz+1, -ixyzt - xzt + it).$$

Como $-xyz + 1 \in \mathbf{C}[x,y,z]$, fazemos $r_2 = -xyz + 1$.
Então, calculamos a matriz U_2,

$$U_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -it \\ 0 & 1 & it-1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -r_2 & 0 \\ {r_2}^{-1} & -f_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & ixyzt + xzt - it \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & -r_2 & 0 \\ -{r_2}^{-1} & -f_1 & -{r_2}^{-1}(ixyzt + xzt - it) - it \\ {r_2}^{-1} & f_1 & {r_2}^{-1}(ixyzt + xzt - it) + it - 1 \end{pmatrix},$$

e sua inversa ${U_2}^{-1}$:

$$ {U_2}^{-1} = \begin{pmatrix} f_1 & f_2 & f_3 \\ -{r_2}^{-1} & 0 & 0 \\ 0 & -1 & -1 \end{pmatrix}. $$

Agora, temos $\langle r_1, r_2 \rangle = \mathbf{C}[x,y,z]$ e, portanto, saímos do *loop*.
Usando bases de Gröbner, calculamos

$$ g_1 = y^2, \quad g_2 = 1 + xyz - y^2, $$

tais que $g_1 \cdot r_1 + g_2 \cdot r_2 = 1$.
Com a notação introduzida em (8), calculamos então as matrizes $\Delta_1 = U_1(t) \cdot {U_1}^{-1}(t - t g_1 r_1)$ e $\Delta_2 = U_2(t - t g_1 r_1) \cdot {U_2}^{-1}(0)$:

$$ \Delta_1 = \left(\begin{array}{c|c|c} \begin{array}{c} x^4y^4z^4t^2 - xy^2zt - x^2y^2z^2t^2 + \\ x^2y^4z^2t^2 - x^3y^5z^3t^2 + 1 \end{array} & -x^3y^2z^3t & \begin{array}{c} -x^3y^2z^3t + x^2y^3z^2t + \\ x^2y^2z^2t^2 - xy^2zt \end{array} \\ \hline \begin{array}{c} xy^2zt^3 - xy^4zt^3 + x^2y^5z^2t^3 - x^3y^4z^3t^3 + \\ 2y^2t^2 - y^4t^2 + xy^5zt^2 - x^2y^4z^2t^2 + \\ y^3t - xy^2zt \end{array} & \begin{array}{c} x^2y^2z^2t^2 + \\ xy^2zt + 1 \end{array} & \begin{array}{c} -xy^2zt^3 - xy^3zt^2 + \\ x^2y^2z^2t^2 \end{array} \\ \hline 0 & 0 & 1 \end{array} \right), $$

$$ \Delta_2 = \left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline \begin{array}{c} 2x^2y^4z^2t^2 - y^3t + yt + xy^2zt - 2y^2t^2 + \\ y^4t^2 - xy^5zt^2 + t^2 + xyzt^2 \\ -x^2y^2z^2t^2 - x^3y^3z^3t^2 \end{array} & \begin{array}{c} -xy^2zt + xzt + \\ x^2yz^2t + 1 \end{array} & \begin{array}{c} -xy^2zt + xzt + \\ x^2yz^2t \end{array} \\ \hline \begin{array}{c} -2x^2y^4z^2t^2 + y^3t - yt - xy^2zt + 2y^2t^2 \\ -y^4t^2 + xy^5zt^2 - t^2 - xyzt^2 + \\ x^2y^2z^2t^2 + x^3y^3z^3t^2 \end{array} & \begin{array}{c} xy^2zt - xzt \\ -x^2yz^2t \end{array} & \begin{array}{c} xy^2zt - xzt \\ -x^2yz^2t + 1 \end{array} \end{array} \right). $$

Dessa forma, temos que:

$$ \mathtt{f}' \cdot \Delta_1 \cdot \Delta_2 = (1, xyz - 1, 0). $$

Agora, se

$$ E := \begin{pmatrix} 1 & 1 - xyz & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, $$

então $(1, xyz - 1, 0) \cdot E = (1, 0, 0)$. Disso segue que

$$ U' := \Delta_1 \cdot \Delta_2 \cdot E $$

é a matriz invertível tal que $\mathtt{f}' \cdot U' = (1, 0, 0)$.

Finalmente, fazendo a mudança de variáveis $y := y - t$ nos polinômios entradas de U', obtemos a matriz invertível U desejada: $\mathtt{f} \cdot U = (1, 0, 0)$.
Neste exemplo, os polinômios que aparecem na tal matriz U possuem dezenas de termos, por isso preferimos não exibi-la aqui.

Prova do Teorema 5.4. Seja $A = (a_{ij})$ uma $(l \times m)$-matriz unimodular sobre $R := \mathbf{C}[x_1, \ldots, x_n]$, com $l \leq m$. O procedimento para encontrar a matriz U, nas condições do teorema, é indutivo sobre as linhas.

$A = (a_{ij})$ unimodular implica que todas as linhas de A são unimodulares. De fato: da apresentação

$$R^m \xrightarrow{A} R^l \longrightarrow R^l/imA \longrightarrow 0$$

segue que $Fitt_0(R^l/imA) = I_l A = R$, e então $R^l/imA = (0)$, pois o 0-ésimo ideal Fitting de um módulo está contido no seu anulador. Em particular, existe $(g_1, \ldots, g_m) \in R^m$ tal que $a_{11}g_1 + \ldots + a_{1m}g_m = 1$. Com o algoritmo do Teorema 5.6, calculamos uma $(m \times m)$-matriz U' unimodular com $(a_{11}, \ldots, a_{1m}) \cdot U' = (1, 0, \ldots, 0)$.

A matriz $A' := A \cdot U'$ é unimodular, pois U' é invertível. Logo, temos

$$A' = \left(\begin{array}{c|ccc} 1 & 0 & \ldots & 0 \\ \hline b_{21} & & & \\ \vdots & & B & \\ b_{21} & & & \end{array}\right)$$

com B matriz $(l-1) \times (m-1)$ claramente unimodular.

Assim, por indução segue $V_{(m-1)\times(m-1)}$ unimodular tal que

$$B \cdot V = \left(\begin{array}{c|c} Id_{l-1} & 0 \end{array} \right)_{q \times p}$$

Considerando

$$V' = \left(\begin{array}{c|ccc} 1 & 0 & \ldots & 0 \\ \hline 0 & & & \\ \vdots & & V & \\ 0 & & & \end{array}\right),$$

invertível, chegamos a

$$A' \cdot V' = \left(\begin{array}{c|ccc} 1 & & & \\ \hline b'_{21} & & & \\ \vdots & & Id_{l-1} & \\ b'_{l1} & & & \end{array}\right),$$

Logo, com certa matriz elementar $E_{m\times m}$, determinamos a matriz unimodular $m \times m$ desejada, $U := U' \cdot V' \cdot E$. □

5.3 Algoritmo que Reduz ao Caso Estavelmente Livre

Nesta seção, consideramos um módulo projetivo qualquer, apresentado como a imagem, kernel ou cokernel de uma matriz polinomial. Será dado um algoritmo que calcula uma base livre para P, usando o procedimento da Seção 5.2 como uma subrotina.

Deste ponto em diante, R denotará o anel de polinômios $\mathbf{C}[x_1, \ldots, x_n]$.

Lema 5.8. *Uma $(r \times s)$-matriz A sobre R $(r \geq s)$ é unimodular se, e somente se, A possui uma matriz inversa à esquerda.*

Prova. ($\Leftarrow$) Suponha que A tem inversa à esquerda, então existe B matriz $s \times r$ sobre R tal que $B \cdot A = Id_s$. Para quaisquer $x_1, x_2 \in R^s$, $A(x_1) = A(x_2)$ implica $BA(x_1) = BA(x_2)$ e, portanto, $x_1 = x_2$. Isso significa que $kerA = (0)$, donde segue que $R^s \simeq imA$.
Identificamos $imA \simeq R^s$ com os elementos de R^r que possuem as $r - s$ últimas coordenadas nulas. Agora, considere a apresentação

$$R^s \xrightarrow{A} R^r \xrightarrow{\pi} R^{r-s} \longrightarrow 0,$$

onde π é a projeção nas R^{r-s} últimas coordenadas.
Então, $R = Fitt_{r-s}(R^{r-s}) = I_{r-(r-s)}A = I_sA$. E, portanto, A é unimodular.
($\Rightarrow$) Suponha que A é unimodular; conseqüentemente, sua transposta A^t também é uma matriz unimodular. Considere, então, a apresentação

$$R^r \xrightarrow{A^t} R^s \longrightarrow R^s/imA^t \longrightarrow 0.$$

Então , $Fitt_0(R^s/im\ A^t) = I_sA^t = R$; implicando $R^s/imA^t = (0)$. Disso segue que as linhas de A geram o R-módulo R^s.
Claramente, os elementos da base canônica $\{e_1, \ldots, e_s\}$ formam a única base de Gröbner reduzida para R^s. No processo de cálculo dessa base de Gröbner, encontramos a matriz B de transformação, que é então a inversa à esquerda de A. □

No que segue, P é um R-módulo qualquer finitamente gerado, apresentado por um R-epimorfismo $\varphi : R^l \longrightarrow P$ de tal forma que temos (ou podemos calcular) $ker\varphi$. Por exemplo, P pode ser dado como:

(1) um cokernel, isto é, temos uma seqüência exata explícita

$$R^m \xrightarrow{A} R^l \longrightarrow P \longrightarrow 0;$$

(2) como um espaço coluna, isto é, temos uma seqüência exata explícita

$$R^m \longrightarrow P = imA \longrightarrow 0;$$

(3) como o kernel de uma matriz polinomial A, isto é, temos uma seqüência exata

$$0 \longrightarrow P \longrightarrow R^m \xrightarrow{A} R^l.$$

Observe que no caso (3) podemos calcular um subconjunto finito de R^m que gera P (algoritmo para calcular syzygies, Capítulo 3), assim esse caso é reduzido ao caso (2).

Em qualquer desses três casos, podemos calcular uma resolução livre finita de P

$$0 \longrightarrow R^{r_t} \xrightarrow{A_t} R^{r_{t-1}} \xrightarrow{A_{t-1}} R^{r_{t-2}} \xrightarrow{A_{t-2}} \cdots \xrightarrow{A_1} R^{r_0} \xrightarrow{\varphi} P \longrightarrow 0, \tag{14}$$

onde cada A_j é uma matriz $r_{j-1} \times r_j$ $(r_{j-1} \geq r_j)$ com entradas em R. (No Capítulo 3, damos uma algoritmo para calcular resoluções livres finitas usando bases de Gröbner).

Se P é projetivo, então a seqüência exata curta

$$0 \longrightarrow ker\varphi \longrightarrow R^{r_0} \longrightarrow P \longrightarrow 0$$

cinde, implicando $R^{r_0} \simeq P \oplus ker\varphi$. Logo, $ker\varphi = imA_1$ é projetivo. Por indução (como na prova da Proposição 5.2) vemos que imA_j é projetivo, para todo j. Em particular, para $j = t-1$; implicando que a seqüência exata

$$0 \longrightarrow R^{r_t} \xrightarrow{A_t} R^{r_{t-1}} \xrightarrow{A_{t-1}} imA_{t-1} \longrightarrow 0$$

cinde. Por isso, existe uma matriz B_t inversa à esquerda de A_t; então A_t é unimodular e B_t pode ser calculada como no Lema 5.8. Observe que, como B_t é um epimorfismo, B_t também é unimodular.

Usando o algoritmo dado na Seção 2 para B_t, encontramos U_{t-1} matriz $r_{t-1} \times r_{t-1}$ unimodular tal que

$$B_t \cdot U_{t-1} = \left(\; Id_{r_t} \;\middle|\; 0 \; \right).$$

Como $B_t \cdot A_t = Id_{R^{r_t}}$, vemos que as primeiras r_t colunas de U_{t-1} são iguais a A_t. E ainda, pelo Corolário 5.5, as $r_{t-1} - r_t$ colunas restantes de U_{t-1} formam uma base para o R-módulo livre $kerB_t$; denotaremos essa submatriz $r_{t-1} \times (r_{t-1} - r_t)$ por V_{t-1}. Finalmente, calcule a $r_{t-2} \times (r_{t-1} - r_t)$-matriz $C_{t-1} := A_{t-1}V_{t-1}$.

Proposição 5.9. *Nas condições anteriores, a seqüência*

$$0 \longrightarrow R^{r_{t-1}-r_t} \xrightarrow{C_{t-1}} R^{r_{t-2}} \xrightarrow{A_{t-2}} R^{r_{t-3}} \xrightarrow{A_{t-3}} \cdots \xrightarrow{A_1} R^{r_0} \xrightarrow{\varphi} P \longrightarrow 0, \tag{15}$$

é uma resolução livre finita de P.

Prova. Basta mostrar que C_{t-1} é um isomorfismo entre $R^{r_{t-1}-r_t}$ e $kerA_{t-2}$. Para isso, considere o seguinte diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^{r_t} & \underset{\xleftarrow{B_t}}{\xrightarrow{A_t}} & R^{r_{t-1}} & \xrightarrow{A_{t-1}} & imA_{t-1} & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle V_{t-1}} & & & & \\ & & & & R^{r_{t-1}-r_t} & & & & \\ & & & & \uparrow & & & & \\ & & & & 0 & & & & \end{array}$$

Pela construção de V_{t-1}, temos $imV_{t-1} = kerB_t$. E $imA_{t-1} = kerA_{t-2}$, pois (14) é exata. Como $B_tA_t = Id_{R^{r_t}}$, vemos que $kerB_t \longrightarrow R^{r_{t-1}}/imA_t$, $x \mapsto x+imA_t$, é um homomorfismo injetivo entre R-módulos livres de mesmo posto, e portanto é um R-isomorfismo. Disso e de $imA_t = kerA_{t-1}$ segue que A_{t-1} induz um isomorfismo entre $kerB_t$ e imA_{t-1}.
Então, $C_{t-1} = A_{t-1}V_{t-1}$ é um isomorfismo entre $R^{r_{t-1}-r_t}$ e imA_{t-1}; provando que (15) é uma seqüência exata. □

Como conseqüência da Proposição 5.8, vemos que de qualquer resolução livre finita de P com comprimento t, podemos calcular uma resolução livre com comprimento $t-1$.
Assim, se repetirmos esse processo t vezes, chegaremos a um isomorfismo

$$0 \longrightarrow R^s \xrightarrow{C_0} P \longrightarrow 0,$$

onde $C_0 := \varphi \cdot V_0$; encontrando portanto uma base livre para o módulo projetivo P (dada por C_0).
Note que $s = \sum_{j=0}^{t} (-1)^j r_j$ é o posto do R-módulo livre P.
Dessa forma, completamos o algoritmo que dá uma prova construtiva para o Teorema de Quillen-Suslin.

Referências Bibliográficas

[1] Atiyah, M. F. and I. G. Macdonald, *Introduction to Commutative Algebra.* Addison-Wesley, Reading, Massachusetts, 1969.

[2] Cox, D. J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms.* Springer-Verlag, New York, 1992.

[3] Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry.* Springer-Verlag, New York, 1995.

[4] Eisenbud, D., C. Huneke and W. Vasconcelos, Direct Methods for Primary Decomposition, *Invent. Math.* **110**, 1992, 207-235.

[5] Herzog, J., Generators and Relations of Abelian Semigroups and Semigroup-Rings, *Manuscripta Math.* **3**, 1970, 153-193.

[6] Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhauser, Boston, MA, 1985.

[7] Logar, A., A Computacional Proof of the Noether Normalization Lemma, *in Proceedings 6th AAECC, Rome*, Lecture Notes in Computer Science **357**. Springer-Verlag, Berlin/Heidberg/New York, 1988, 259-273.

[8] Logar, A. and B. Sturmfels, Algorithms for the Quillen-Suslin Theorem, *J. Algebra* **145**, 1992, 231-239.

[9] Vasconcelos, W., *Arithmetic of Blowup Algebras.* Cambridge University Press, Cambridge, U.K., 1994.

[10] Vasconcelos, W., Computing the Integral Closure of an Affine Domain, *Proc. Amer. Math. Soc.* **85**, 1991, 281-289.