Edney Augusto Jesus de Oliveira

Ideais Iniciais Genéricos

Universidade Federal de Minas Gerais

2011

Edney Augusto Jesus de Oliveira

Ideais Iniciais Genéricos

Dissertação de mestrado apresentada como requisito da obtenção do título de Mestre pelo Departamento de Matemática do Instituto de Ciências Exatas, Universidade Federal de Minas Gerais.

Orientador: Israel Vainsencher

Universidade Federal de Minas Gerais 2011

Agradecimentos

Agradeço a minha mãe que sempre esteve ao meu lado.

Ao meu orientador Israel Vainsencher, pelos ensinamentos.

A minha tia Léa, pela hospitalidade.

A minha noiva por todo apoio.

Aos meus amigos.

Muito obrigado!

Resumo

No presente trabalho, concentraremos nossa atenção no estudo do cálculo da dimensão de variedades algébricas afins, apresentando uma forma computacional para o seu cálculo utilizando as teorias de Bases de Gröebner e do polinômio afim de Hilbert. O propósito deste trabalho é definir ideal inicial genérico e destacar sua importância no cálculo da dimensão de variedades algébricas afins. Mostraremos a existência do ideal inicial genérico por meio de técnicas de álgebra exterior e propriedades de polinômios com coeficientes em um corpo infinito. Definiremos ainda ideais Borel-fixos e sua relação com ideais iniciais genéricos.

Abstract

In this work, we focus our attention on the study of the calculus of the dimension of affine algebraic varieties, presenting a computational way with the theoretical background of Gröebner basis and the affine Hilbert polynomial. Our goal is to define generic initial ideal and to point out its importance in the calculus of the dimension of affine algebraic varieties. We will prove the existence of the generic initial ideal by the means of exterior algebra tecniques and the properties of polynomials with coeficients over an infinity field. We will also define Borel-fixed ideals and their relation with generic initial ideals.

Sumário

Introdução

Este trabalho tem como objetivo tratar de um tópico central na Geometria Algébrica: o cálculo efetivo da dimensão e do grau de variedades algébricas. A principal ferramenta utilizada é a teoria de Bases de Gröbner.

Uma variedade algébrica afim sobre um corpo k é qualquer subconjunto $V \subseteq k^n$ definido como conjunto solução de um sistema de equações polinomiais. Dizemos também que V é uma subvariedade (algébrica afim) de k^n.

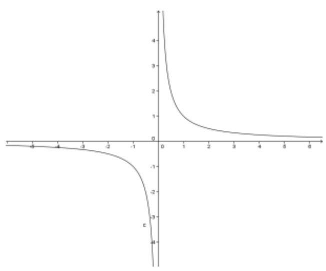
Calcular dimensão de subespaços vetoriais, caso de um sistema de equações lineares homogêneas, é simples. A ideia central é reduzir o cálculo da dimensão de variedades algébricas ao caso linear.

O conjunto das equações de uma subvariedade $V \subseteq k^n$ gera um ideal $I \subseteq k[x_1, \ldots, x_n]$.

Iremos inicialmente tratar do caso mais simples que é quando I é um ideal monomial. Como veremos, o cálculo da dimensão é direto.

No caso de um ideal qualquer, esse cálculo não é direto e em geral pode ser muito complicado. Para contornar esse problema, vamos associar a esse ideal outro ideal (que será monomial), de modo que saibamos ter a mesma dimensão. Para obtermos tal ideal, recorreremos às *"bases de Gröbner "*.

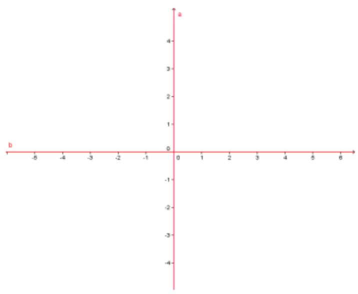
Esse novo ideal, é chamado de **"ideal inicial"** e ele será o principal personagem desse trabalho. Para exemplificar esse fato, considere a variedade $V = V(< xy - 1 >)$ sobre $k[x, y]$. Neste caso, a figura associada a essa variedade é:



a qual tem dimensão 1. Mas suponha que não saibamos que a variedade dada não represente uma curva (ou heuristicamente falando, não saibamos como é tal figura). Então, através de técnicas estudadas no trabalho, poderemos verificar que o ideal monomial associado a $< xy-1 >$ é $< xy >$. Deste modo, teremos a seguinte associação:

$$\dim_k V(< xy-1 >) = \dim_k V(< xy >) = 1.$$

A vantagem de se utilizar essa igualdade é que o cálculo da dimensão pode ser feito utilizando propriedades simples, como por exemplo $V(x \cdot y) = V(x) \cup V(y)$, e podemos associar a variedade $V(x)$ a um espaço vetorial coordenado onde apenas a variável x é nula. No exemplo acima, $V(x)$ é uma reta (mais precisamente, o eixo-y), pois estamos trabalhando com apenas duas coordenadas, e ao fixarmos $x = 0$, resta apenas a coordenada correspondente a variável y. Analogamente vemos que $V(y)$ é também uma reta. A figura associada a essa nova variedade é:



Com isso, observamos que o ideal inicial é muito importante para o cálculo de dimensão. Iremos estudar com mais cuidado algumas de suas propriedades. Veremos que dentre os ideais iniciais, há alguns que são mais “fortes” no sentido de que eles não dependem da escolha do sistema de coordenadas, os quais são chamados de **“ideais iniciais genéricos”** . Veremos ainda uma condição necessária para que um ideal seja inicial genérico, através do conceito de ideal fixo de Borel.

A menos que se explicite o contrário, para nós k é sempre um corpo infinito.

1 Dimensão de Variedades Algébricas Afins

Estudaremos o conceito de dimensão de uma variedade algébrica afim. O objetivo central é apresentar uma forma computacional para o seu cálculo.

1.1 Generalidades

Denotaremos por $S := k[x_1, \cdots, x_n]$, o anel de polinômios com coeficientes no corpo k. Um ideal $I \subset S$ é dito **monomial** se I é gerado por monômios de S. Um **termo** é um produto entre um monômio de S e um escalar de k. Um monômio típico de S tem a seguinte forma:

$$X^\alpha = x_1^{a_1} \cdots x_n^{a_n},$$

onde $\alpha = (a_1, \ldots, a_n)$ e cada a_i é um número inteiro não negativo, convencionando-se $x_i^0 = 1$.

Em um anel de polinômios a uma variável, $k[x]$, definimos o grau de um monômio como sendo o valor de seu expoente. Em mais variáveis, definimos o grau de um monômio como a soma dos expoentes das variáveis,ou seja,

$$|X^\alpha| = |x_1^{a_1} \cdots x_n^{a_n}| = \sum_{i=1}^{n} a_i.$$

Para realizarmos um estudo sobre a ordenação monomial, iremos fazer a seguinte associação:

$$x_1^{a_1} \cdots x_n^{a_n} \leftrightarrow (a_1, \ldots, a_n) = \alpha,$$

onde $\alpha \in \mathbb{Z}_+^n$.

Definição 1.1. *Sejam X^α,X^β e X^γ monômios de S. Uma ordem monomial é uma relação $<$ entre monômios de S satisfazendo:*

1. *$<$ é uma ordem total no conjunto de monômios, ou equivalentemente em $\mathbb{Z}_+^n$;*

2. *se $X^\alpha < X^\beta$, então $X^\alpha \cdot X^\gamma < X^\beta \cdot X^\gamma$.*

Abaixo definiremos algumas ordens monomiais que serão utilizadas ao longo do texto.

Definição 1.2. *Sejam $\alpha = (a_1, \dots, a_n)$ e $\beta = (b_1, \dots, b_n)$, e sejam X^α e X^β os seus respectivos monômios associados.*

1. *Ordem* ***lexicográfica*** *- (**lex**), que denotaremos por $<_{lex}$.*
   Dizemos que:
   $X^\alpha <_{lex} X^\beta$ se $a_i < b_i$ para o menor i tal que $a_i \neq b_i$.

2. *Ordem* ***lexicográfica graduada*** *- (**grlex**), que denotaremos por $<_{grlex}$.*
   Dizemos que:
   $X^\alpha <_{grlex} X^\beta$ se $|X^\alpha| < |X^\beta|$, ou se $X^\alpha <_{lex} X^\beta$ em caso de $|X^\alpha| = |X^\beta|$.

3. *Ordem* ***lexicográfica reversa graduada*** *- (**grevlex**), que denotaremos por $<_{grevlex}$.*
   Dizemos que:
   $X^\alpha <_{grevlex} X^\beta$ se $|X^\alpha| < |X^\beta|$, ou se $a_i > b_i$ para o menor i tal que $a_i \neq b_i$ em caso de $|X^\alpha| = |X^\beta|$.

Exemplo 1.1. Sejam os monômios x^4yz, xy^5 e $z^{12} \in k[x,y,z]$. Se $z < y < x$, então

(i)- $z^{12} \ <_{lex} \ xy^5z^6 \ <_{lex} \ x^4yz$;

(ii)- $x^4yz \ <_{grlex} \ z^{12} \ <_{grlex} \ xy^5z^6$;

(iii)- $x^4yz \ <_{grevlex} \ xy^5z^6 \ <_{grevlex} \ z^{12}$.[1]

Um polinômio $p = c_nX^{\alpha_n} + \cdots + c_1X^{\alpha_1}$ está escrito na forma normal (segundo uma ordem monomial $<$) se $X^{\alpha_n} > \cdots > X^{\alpha_1}$. Nesse caso, dizemos que $c_nX^{\alpha_n}$ é o *termo líder* e o denotaremos por $\text{in}_<(p)$ (iremos também escrever $\text{in}(p)$ quando não houver risco de confusão sobre qual ordem monomial está sendo utilizada). Ainda no exemplo anterior, se $p = x^4yz + xy^5 + z^{12}$, então p escrito na forma normal é dado por

(i)- $(\text{lex}): p = x^4yz + xy^5z^6 + z^{12}$ e $\text{in}_{<_{lex}}(p) = x^4yz$;

(ii)- $(\text{grlex}): p = xy^5z^6 + z^{12} + x^4yz$ e $\text{in}_{<_{grlex}}(p) = xy^5z^6$;

(iii)- $(\text{grevlex}): p = z^{12} + xy^5z^6 + x^4yz$ e $\text{in}_{<_{grevlex}}(p) = z^{12}$.

Definição 1.3. *Sejam $f, g \in S$ e $<$ uma ordem monomial. Sejam ainda $in(f) = X^\alpha$, e $in(g) = X^\beta$, onde $\alpha = (a_1, \dots, a_n)$ e $\beta = (b_1, \dots, b_n)$.*

1. *Seja $\delta = (d_1, \dots, d_n)$, onde $d_i = max\{a_i, b_i\}$.*
   Dizemos então que X^δ é um mínimo múltiplo comum de $in(f)$ e $in(g)$, denotado por $MMC(in(f), in(g))$.

[1] tentar interpretar a observação do Bahiano

2. *Seja* $\varepsilon = (e_1, \ldots, e_n)$*, onde* $e_i = min\{a_i, b_i\}$*.*
   Dizemos então que X^{ε} *é um máximo divisor comum de* $in(f)$ *e* $in(g)$*, denotado por* $MDC(in(f), in(g))$*.*

Seja I um ideal de S. O conjunto

$$\sqrt{I} = \{f \in S | f^n \in I \text{ para algum } n \in \mathbb{Z}^+\},$$

é chamado **radical** de I. Dizemos que um ideal I é radical (ou perfeito) se $I = \sqrt{I}$.

O próximo resultado nos dará uma caracterização para o radical de ideais monomiais.

Proposição 1.1. *Se I é um ideal monomial, então seu radical $\sqrt{I}$ também é monomial.*[2]

Demonstração. O Teorema da base de Hilbert nos dá que o ideal I é finitamente gerado (mas não diz que os geradores são necessariamente monômios!). Seja $\{g_1, \ldots, g_m\}$ um conjunto de geradores do ideal I. Observe que cada g_i pode ser escrito como:

$$g_i = \sum_{j=1}^{k} a_{ik} X^{\alpha_{ij}}.$$

Com isso, temos para todo i e j que $X^{\alpha_{ij}}$ pertence a I.(veja [2], p. 71, Lema 3). Isso mostra que o conjunto dos monômios $X^{\alpha_{ij}}$ (para todo i e j) geram I.

Após reindexamento, seja $I =< X^{\alpha_1}, \ldots, X^{\alpha_t} >$, onde X^{α_i} são monômios de S.

Se $X^{\alpha_i} = \prod_{j=1}^{n} x_i^{a_{i,j}}$, defina o suporte de X^{α_i} como suporte$(X^{\alpha_i}) = \prod_{j=1}^{n} x_i^{b_{i,j}} = X^{\beta_i}$, onde

$$b_{i,j} = \begin{cases} 1 & \text{se} \quad a_{i,j} \neq 0, \\ 0 & \text{se} \quad a_{i,j} = 0. \end{cases}$$

Mostraremos que $\sqrt{I} = J :=< X^{\beta_1}, \ldots, X^{\beta_t} >$.

É imediato ver que $J \subset \sqrt{I}$. Para verificar a outra inclusão, suponha $f \in \sqrt{I}$. Então existe r inteiro positivo tal que $f^r \in I$. Se $m_1 = \text{in}(f)$ então $m_1^r = \text{in}(f^r) \in I$, de onde segue que $m_1 \in \sqrt{I}$.

Repetindo o processo para $f - m_1 \in \sqrt{I}$, veremos que $m_2 = \text{in}(f - m) \in \sqrt{I}$, e assim sucessivamente veremos que todos os monômios de f também pertencem a $\sqrt{I}$.

Temos ainda que para cada j, X^{α_i} divide m_j^r para algum $1 \leqslant i \leqslant t$ (veja [2], p. 70, Lema 2). Como X^{β_i} divide X^{α_i} segue que X^{β_i} divide m_j^r. Decorre disso que para algum i, X^{β_i} divide m_j, pois as variáveis que estão presentes em m_j^r são as mesmas que aparecem em m_j, e em X^{β_i} as variáveis presentes figuram em número mínimo. Isso mostra que $m_j \in J$.

Portanto $f \in J$. □

[2]ver observação bahiano

Uma consequência da proposição acima é que somos capazes de listar todos os ideais radicais que são monomiais. Neste caso, os seus geradores são monômios onde o grau de cada variável presente é 1.

Exemplo 1.2. Todos os ideais monomiais que são radicais de $k[x,y]$ são $< x >$, $< y >$, $< x,y >$ e $< xy >$.

1.2 Variedades Algébricas Afins

Veremos nesta seção a definição de variedade algébrica afim e estudaremos algumas de suas propriedades. Trabalharemos ainda o conceito de dimensão de variedades algébricas.

Definição 1.4. *Sejam $p_1, \cdots, p_r \in S$. O subconjunto de k^n formado pelos pontos que anulam simultaneamente todos os polinômios $p_1, \cdots, p_r \in S$ é uma variedade algébrica.*

$$V(p_1, \cdots, p_r) = \{(a_1, \cdots, a_n) \in k^n | p_i(a_1, \cdots, a_n) = 0, \ \forall i = 1, \cdots, r\}.$$

Ainda na definição acima, iremos usualmente escrever $V(I)$, onde $I \subset S$ é um ideal, significando que

$$V(I) = \{(a_1, \cdots, a_n) | p(a_1, \cdots, a_n) = 0, \ \forall p \in I\}.$$

Note que se $p_1, \cdots, p_r$ é um conjunto de geradores de I, então vale o seguinte:

$$V(I) = V(p_1, \cdots, p_r).$$

Esse fato é bastante útil, pois sabemos do Teorema da Base de Hilbert (ver [2], p. 76, Teorema 4) que todo ideal de S é finitamente gerado, e isso reduz o cálculo da variedade de um ideal I ao cálculo dos zeros simultâneos dos polinômios do conjunto finito de geradores de I.

Observe que a definição de variedade algébrica afim nos diz que para cada ideal I, temos uma varidedade algébrica $V(I) \subseteq k^n$. É fácil verificar que a escolha dessa variedade é única. Por outro lado, se temos uma variedade algébrica, então definimos o ideal $\mathscr{I}(V)$ é o ideal gerado pelos elementos de S que se anulam em V. O capítulo 4 de [2] faz a construção da relação entre ideais de S e as subvariedades de k^n mostrando que toda variedade algébrica afim pode ser escrita como $V(I)$, onde I é um ideal de S.

Vejamos agora algumas propriedades de variedades algébricas que serão úteis:

Proposição 1.2. *Sejam $V(A)$ e $V(B)$ variedades algébricas definidas pelos zeros dos elementos dos subconjuntos A e B de S, respectivamente. São válidos:*

(i) $V(0) = k^n$ *e* $V(1) = \varnothing$*;*

(ii) $V(A \cdot B) = V(A) \cup V(B)$ *(onde* $A \cdot B := \{ab | \forall a \in A \text{ e } \forall b \in B\}$*);*

(iii) Se A_i é uma coleção arbitrária de subconjuntos de S, temos $\cap_i V(A_i) = V(\cup_i A_i)$;

(iv) Se $A \subset B \Rightarrow V(B) \subset V(A)$.

Demonstração. A primeira e segunda afirmações seguem imediatamente da definição de variedade algébrica afim.

A terceira afirmação segue do seguinte fato:

$$\begin{aligned} V(\cup_i A_i) &= \{\alpha \in k^n | f(\alpha) = 0 \; \forall f \in \cup_i A_i\} \\ &= \cap_i \{\alpha \in k^n | f(\alpha) = 0 \; \forall f \in A_i\} \\ &= \cap_i V(A_i). \end{aligned}$$

Para a quarta afirmação, considere o conjunto $C = B - A$. Logo, $B = A \cup C$, e daí,

$$V(B) = V(A \cup C) = V(A) \cap V(C) \subset V(A).$$

□

Exemplo 1.3. Vejamos que $V(I) = V(\sqrt{I})$. Segue da definição de radical de um ideal que $I \subset \sqrt{I}$, e pela propriedade (iv) da proposição anterior, segue que $V(\sqrt{I}) \subset V(I)$. Seja $a = (a_1, \ldots, a_n) \in V(I)$. Se $f \in \sqrt{I}$, então $f^n \in I$, e consequentemente, f^n se anula em a. Como k é um corpo, concluiremos que f se anula em α. Portanto $\alpha \in V(\sqrt{I})$.

Dada uma variedade $V(I) \subset k^n$, denotaremos por $D(I)$ como o conjunto complementar de $V(I)$ em k^n. Definimos

$$\mathscr{Z} := \{D(I) | I \subset S\}.$$

Utilizando as propriedades enunciadas na Proposição 1.2, somos capazes de mostrar que os elementos de $\mathscr{Z}$ satisfazem os axiomas para abertos de uma topologia: interseção arbitrária de abertos é um aberto, a união finita de abertos é um aberto e $\varnothing$, $k^n \in \mathscr{Z}$. Esse fato nos motiva a seguinte definição:

Definição 1.5. *A topologia que $\mathscr{Z}$ gera em k^n é chamada* ***topologia de Zariski****.*

Na topologia de Zariski, *fechado* é sinônimo de subvariedade algébrica. Uma informação útil sobre abertos de Zariski é fornecida pelo próximo resultado.

Proposição 1.3. *Sejam V uma variedade algébrica irredutível e U, $W \subset V$ abertos não vazios de Zariski. Então $U \cap W \neq \varnothing$.*

Demonstração. Observe que se U é um aberto (de Zariski), então pode definição é o conjunto complementar de uma subvariedade algébrica $V_1 = V(I_1)$, onde I_1 é um ideal de S, e portanto $U = D(I_1)$. Analogamente, $W = D(I_2)$, com I_2 um ideal de S. Segue daí que:

$$\begin{aligned} \varnothing &= U \cap W = D(I_1) \cap D(I_2) = V(I_1)^c \cap V(I_2)^c \\ &= (V(I_1) \cup V(I_2))^c = (V(I_1 \cdot I_2))^c. \end{aligned}$$

Isso nos diz que $V(I_1 \cdot I_2) = k^n$, o que implica em $\sqrt{< I_1 \cdot I_2 >} = \{0\}$.

Com isso mostremos que ou $I_1 = \{0\}$ ou $I_2 = \{0\}$. De fato, para todo produto $f_1 f_2$, com $f_1 \in I_1$ e $f_2 \in I_2$, existe um inteiro k tal que $f_1^k f_2^k = (f_1 f_2)^k = 0$. Como S é um domínio de integridade, concluiremos que ou $f = 0$ ou $g = 0$. Agora suponha que $I_2 \neq \{0\}$, e portanto, existe $g \in I_2$, tal que $g \neq 0$, e consequentemente, toda potência de g também é não nula.

Observe o conjunto $gI_1 = \{gf_1 | f_1 \in I_1\}$. Para cada f_1, existe um inteiro k tal que $g^k f_1^k = (gf_1)^k \in < I_1 \cdot I_2 >$. Como $g \neq 0$, então $f_1 = 0$. Isso mostra que $I_1 = \{0\}$. Segue que $U = D(I_1) = \varnothing$, o que prova o enunciado. $\square$

[3]

Dizemos que um espaço topológico X é irredutível se sempre que tivermos $X = X_1 \cup X_2$ com X_i fechado em X implicar em $X = X_1$ ou $X = X_2$. Em particular, uma variedade algébrica $V(I)$ é irredutível se, sempre que $V(I) = V_1 \cup V_2$ implicar em $V(I) = V_1$ ou $V(I) = V_2$.

O próximo resultado nos fornecerá uma técnica para verificar a irredutibilidade de $V(I)$.

Proposição 1.4. *Seja $I \subset S$ um ideal. $V(I)$ é irredutível se, e somente se, $\sqrt{I}$ for primo.*

Demonstração. Primeiro suponha $V(I)$ irredutível. Seja $fg \in \sqrt{I}$. Defina $V_1 = V(I) \cap V(f)$ e $V_2 = V(I) \cap V(g)$. Daí,

$$\begin{aligned} V_1 \cup V_2 &= [V(I) \cap V(f)] \cup [V(I) \cap V(g)] = V(I) \cap [V(f) \cup V(g)] \\ &= V(I) \cap V(fg) = V(I, fg) = V(\sqrt{I}) \end{aligned}$$

É de simples verificar que $V(\sqrt{I}) = V(I)$. Daí, temos que $V(I) = V_1 \cup V_2$. Por hipótese $V(I)$ é irredutível, donde $V(I) = V_1$ ou $V(I) = V_2$. Digamos que $V(I) = V_2$. Assim $V(I) = V(I) \cap V(g)$, o que implica em $V(I) \subset V(g)$, e consequentemente $g \in \mathscr{I}(V(I)) = \sqrt{I}$ pelo Teorema de Zeros de Hilbert Forte, cf. [9, p. 31], [2, p. 173]. Portanto $\sqrt{I}$ é primo.

Suponha agora $\sqrt{I}$ primo. Seja $V(I) = V_1 \cup V_2$, onde $V_1 = V(J_1)$ e $V_2 = V(J_2)$. Temos:

$$\sqrt{I} = \mathscr{I}(V(I)) = \mathscr{I}(V_1 \cup V_2) = \mathscr{I}(V(J_1) \cup V(J_2)) = \mathscr{I}(V(J_1 \cdot J_2)) = \sqrt{J_1 \cdot J_2} \supseteq J_1 \cdot J_2.$$

Como $\sqrt{I} \supseteq J_1 \cdot J_2$, então pela primalidade de $\sqrt{I}$ temos que $J_1 \subset \sqrt{I}$ ou $J_2 \subset \sqrt{I}$. Digamos $J_1 \subset \sqrt{I}$. Decorre disso que

$$V(J_1) \supseteq V(I) = V(J_1) \cup V(J_2),$$

e portanto $V(I) = V(J_1)$, o que mostra que $V(I)$ é irredutível. $\square$

[3] sugestão bahiano

Exemplo 1.4. A variedade $V(x_{i_1},\ldots,x_{i_r}) \subset k^n$, onde $x_{i_1},\ldots,x_{i_r}$ são variáveis, é uma variedade irredutível. De fato, como facilmente se verifica, $\sqrt{< x_{i_1},\ldots,x_{i_r} >} = < x_{i_1},\ldots,x_{i_r} >$ é um ideal primo, donde o afirmado segue da Proposição 1.4.

Na topologia habitual de $\mathbb{R}^n$, a definição de irredutibilidade não é útil, pois nesse caso, concluiremos que os únicos espaços irredutíveis são os contendo somente um ponto. No entanto, na topologia de Zariski em k^n, essa noção é bastante rica. O conceito de irredutibilidade nos permite apresentar a noção de dimensão de variedades algébricas, como veremos na próxima definição.

Definição 1.6. *Seja $V \subset k^n$ uma variedade algébrica. Sejam V_j fechados irredutíveis distintos de k^n. Dizemos que*

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = k^n$$

é uma cadeia de fechados irredutíveis de k^n de comprimento n.

*Definimos a dimensão de **Krull** de V como o máximo dos comprimentos de cadeias de fechados irredutíveis de V:*

$$V_0 \subset V_1 \subset \cdots \subset V_n \subseteq V.$$

Denotaremos com a dimensão de Krull de V por $Kdim_k V$.

Outra forma de definir dimensão de variedades algébricas é através da noção de elementos algebricamente independentes, como veremos a seguir.

O **anel de coordenadas** de V, denotado por $k[V]$ é o conjunto das funções polinomiais de V em k, $\phi : V \to k$ (ver [2], p. 239).

Dados elementos $a_1,\ldots,a_t \in k[V]$, dizemos que $a_1,\ldots,a_t$ são algebricamente independentes sobre k se para todo polinômio p em t variáveis não nulo com coeficientes em k tivermos que $p(a_1,\ldots,a_t) \neq 0$ módulo $\mathscr{I}(V)$.

Desde que $k[V]$ é uma k-álgebra finitamente gerada, segue do *Lema de Normalização de Noether* (ver [9], p. 29) que $k[V]$ contém um anel de polinômios $R = k[x_1,\ldots,x_d]$, tal que $k[V]$ é uma extensão inteira de R.

$$\begin{tikzcd}
k[V] \arrow[dd, dash] \arrow[dr, dash, "\text{inteira}"] & \\
& R = k[x_1,\ldots,x_d] \arrow[dl, dash] \\
k &
\end{tikzcd}$$

Consequentemente, o número máximo de elementos algebricamente independentes de

$k[V]$ é igual ao número máximo de elementos algebricamente independentes de R sobre k, que é igual a d.

Nesse contexto, é possível mostrar que $\mathrm{Kdim}_k V = d$. Embora essa igualdade não seja óbvia, o seu estudo não é o foco deste trabalho. O estudo detalhado deste resultado encontra-se em [9] na seção (2.5.3).

A definição de dimensão de Krull é puramente abstrata, e o calcular a dimensão de uma variedade ultilizando essa definição (a menos de casos particulares) é muito complicado, pois teriamos de ser capazes de conhecer todas as subvariedades irredutíveis contidas na variedade em questão, e isso torna essa definição inviável do ponto de vista computacional.

Por outro lado, calcular o número máximo de elementos algébricamente independentes de $k[V]$ é muito complicado, pois teríamos que testar a independência algébrica de todos os subconjuntos de elementos de $k[V]$, e a menos de casos particulares, esse cálculo é computacionalmente inviável.

Quando não houver risco de confusão, denotaremos a dimensão de V simplesmente por $\mathrm{Kdim}V$ ao invés de $\mathrm{Kdim}_k V$.

Nosso objetivo agora é apresentar uma técnica computacional para o calculo da dimensão de variedades algébicas afins. Para tal, os próximos resultados serão úteis, pois nos fornecem informações que podem simplificar o cálculo da dimensão da variedade.

Teorema 1. *Uma variedade algébrica V ou é irredutível ou pode ser decomposta em uma união finita de subvariedades V_i irredutíveis.*

A prova desse teorema pode ser vista em [7] na página 90, e uma consequência dessa propriedade no contexto de dimensão é a seguinte proposição:

Proposição 1.5. *Seja V uma variedade tal que $V = \cup_{i=1}^{t} V_i$, onde cada V_i é uma subvariedade algébrica fechada e irredutível. A dimensão (de Krull) de V é igual a*

$$max_{i=1,\dots,t}\{Kdim\ V_i\}.$$

A prova dessa proposição pode ser encontrada em [9] na página 68. A partir desse resultado é possível simplificar o cálculo da dimensão, nos permitindo calcular a dimensão de uma variedade irredutível $V_i \subset V$ (que possivelmente será mais simples) ao invés de calcularmos a dimensão de V diretamente.

1.3 Dimensão de Variedades - Caso Monomial

Vamos abordar o caso particular de variedades algébicas afins $V(I)$ quando I for um ideal monomial.

Seja $V(x_i^a) \subset k^n$ uma variedade algébrica afim. Essa variedade é composta por todos os pontos de k^n cuja a i-ésima coordenada é nula. Decorre disso que $V(x_i^a)$ é um subespaço vetorial de k^n.

O conjunto do todos os pontos de k^n, onde fixamos algumas coordenadas iguais a zero e as demais são livres é um subespaço vetorial de k^n e nesse caso são chamados de subespaços coordenados. Exemplo de tais subespaços são os eixos coordenados, planos contendo dois eixos coordenados e etc..

É fácil ver que se a variedade algébrica V_i é um subespaço coordenado, então V_i é do tipo $V(x_{i_1}^{a_{i_1}}, \ldots, x_{i_l}^{a_{i_l}})$, onde os índices $i_j \in \{i_1, \ldots, i_l\}$ correspondem as coordenadas dos elementos de V_i que são nulas.

Nem toda variedade algébrica afim é um subespaço de k^n, mas em alguns casos V pode ser escrito como uma união de subespaços coordenados, como por exemplo, $V(xy) \subset k^3$. De fato, pois $V(xy) = V(x) \cup V(y)$. O próximo resultado nos mostra uma condição suficiente para que a variedade possa ser decomposta em uma união finita de subespaços coordenados.

Proposição 1.6. *A variedade de um ideal monomial em S é a união finita de subespaços coordenados de k^n.*

A ideia da prova da proposição acima é aplicar indução sobre o número de geradores do ideal I (que é finito) e utilizar as propriedades vistas na Proposição 1.2.

Seja $I \subset S$ um ideal monomial. Segue da Proposição 1.6 que $V(I)$ é igual a uma união finita de subespaços coordenados V_i. Vimos no Exemplo 1.4 que os V_i são variedades irredutíveis, e pela Proposição 1.5 a dimensão de $V(I)$ é igual a maior dimensão dentre $\text{Kdim} V_i$.

Com isso, nosso trabalho se reduz a calcular a dimensão (de Krull) do maior subespaço contido em $V(I)$. Veremos agora que a dimensão de um subespaço coordenado V_i (como espaço vetorial sobre k) é igual a dimensão de Krull da variedade V_i.

Primeiro analisemos o caso de $V(x_i^a) \subset k^n$. Inicialmente, vamos exibir uma cadeia de subvariedades irredutíveis contida em $V(x_i)$:

$$V(x_i^a, x_1, \ldots, x_n) \subset V(x_i^a, x_1, \ldots, x_{n-1}) \subset \cdots \subset V(x_i^a, x_1) \subsetneq V(x_i^a).$$

O comprimento dessa cadeia é $n-1$. Isso mostra que a dimensão de Krull de $V(x_i^a)$ é maior ou igual a $n-1$. Como $V(x_i^a)$ é um subconjunto próprio de k^n, a dimensão de Krull de $V(x_i^a)$ é menor do que n. Portanto a dimensão de Krull de $V(x_i^a)$ é $n-1$.

Por outro lado, $V(x_1^a)$ é um subespaço de k^n, onde a primeira coordenada é nula, e com isso, tem como base o conjunto $\{(0,1,0,\ldots,0), (0,0,1,0,\ldots,0), \ldots (0,\ldots,0,1)\}$, ou seja, possui dimensão (vetorial) igual a $n-1$, coincidindo com a dimensão de Krull.

Suponha agora que $V = V(x_{i_1}^{a_{i_1}}, x_{i_2}^{a_{i_2}})$ é uma subvariedade de $V_1 = V(x_{i_1}^{a_{i_1}})$. Seguindo o raciocínio feito acima para o caso de $V(x_1^a)$, veremos que a dimensão de Krull é maior ou igual a $n-2$ e menor do n. Como $V \neq V_1$, segue que a dimensão de Krull de V_2 não pode ser $n-1$. Portanto a dimensão de Krull de V é $n-2$.

Repetindo o processo do parágrafo anterior obteremos que a dimensão de Krull de $V(x_{i_1}^{a_{i_1}}, \ldots, x_{i_l}^{a_{i_l}})$ é $n-l$, mostrando que se V é uma variedade algébrica que é um subespaço coordenado de k^n, a sua dimensão de Krull coincide com a sua dimensão como espaço vetorial.

Por outro lado, temos

$$V = V(x_{i_1}^{a_{i_1}}, \ldots, x_{i_l}^{a_{i_l}}) = V(x_{i_1}, \ldots, x_{i_l}).$$

Ou seja, V é constituído dos vetores de k^n cujas j-ésimas coordenadas são nulas, onde $j \in \{i_1, \ldots, i_l\}$. Deduzimos disso que a dimensão do subespaço vetorial V sobre k é $n-l$.

Com o que vimos nos paragráfos anteriores, quando a variedade algébrica V for um subespaço de k^n, podemos calcular a sua dimensão vetorial ao invés de tentarmos obter uma cadeia de subvariedades irredutíveis de comprimento máximo ou determinar o número máximo de elementos algebricamente independentes de $k[V]$. Doravante, usaremos a notação $\dim V = d$ para representar que $\mathrm{Kdim}\, V = d$, ou a dimensão vetorial de V, no caso de V ser um subespaço de k^n.

Vejamos alguns exemplos.

Exemplo 1.5. Dado $I = < x^2y^3z, xy^5, xyz^4 > \subset k[x,y,z]$. Temos

$$V(I) = V(x^2y^3z, xy^5, xyz^4) = V(x^2y^3z) \cap V(xy^5) \cap V(xyz^4) = V(xy) = V(x) \cup V(y).$$

Como vimos no Exemplo 1.4, $V(x)$ e $V(y)$ são irredutíveis, então segue que a dimensão de V é igual a maior entre $\dim V(x)$ e $\dim V(y)$. A variedade $V(x)$ é exatamente o subespaço de k^3 onde $x = 0$, ou seja, onde a primeira coordenada é nula. Geometricamente isso representa o plano yz, e portanto sua dimensão é igual a 2. O mesmo raciocínio mostra que $\dim V(y) = 2$. Portanto, pela Proposição 1.5, a dimensão de V é 2.

Exemplo 1.6. Consideremos a seguinte variedade algébrica afim $V = V(yz - zx^2, z^2 - zx^3) \subset k^3$. Segue que

$$V = V(yz - zx^2, z^2 - zx^3) = V(z(y - x^2), z(z - x^3)) = V(z) \cup V(y - x^2, z - x^3).$$

Note que $V(z)$ é o plano xy, cuja dimensão é 2 e $V(y - x^2, z - x^3)$ é a variedade irredutível chamada *cúbica reversa afim*, e sua dimensão é 1, como veremos em (1.15). Logo $\dim V = 2$.

Exemplo 1.7. Seja $I = < xy^3z, xy^4, yz^4 > \subset k[x,y,z]$. A variedade definida pelos zeros de I é

$$V(I) = V(xy^3z, xy^4, yz^4) = V(y) \cup V(x,z) = V(y) \cup (V(x) \cap V(z)).$$

Neste contexto, $V(y)$ é um subespaço de k^3 isomorfo a k^2, ou seja, um plano (a saber, o plano xz), e $V(x) \cap V(z)$ é a interseção de dois planos coordenados resultando no eixo y. Portanto, a dimensão de V é 2.

Com os resultados vistos até o momento, temos então uma forma de se calcular a dimensão de uma variedade algébrica $V(I)$, quando I for um ideal monomial, descrita nos seguintes passos

1. Decompomos $V(I)$ em uma união finita de subespaços coordenados $V_i,\ 1 \leq i \leq j$ (Proposição 1.6);

2. Calculamos a dimensão de cada um dos subespaços coordenados $V_i,\ 1 \leq i \leq j$ obtidos acima;

3. Concluímos que a dimensão de $V(I)$ será igual a maior das dimensões dos subespaços coordenados $V_i,\ 1 \leq i \leq j$ (Proposição 1.5).

No caso em que I não é um ideal monomial, o cálculo da dimensão não é tão simples, e para tal precisamos de mais ferramentas, que serão apresentadas na próxima seção.

1.4 Base de Gröbner

Vimos na seção anterior uma forma computacional de calcular a dimensão de uma variedade algébrica determinada por um ideal monomial. Para o caso geral, iremos associar cada ideal de S a um ideal monomial, cuja a dimensão seja a mesma. Essa associação será feita via teoria das Bases de Gröbner.

Definição 1.7. *Dado $I \subset S$ e $<$ uma ordem monomial, definimos o **ideal inicial** como*

$$in_<(I) := < in_<(f) \mid f \in I > .$$

Quando estiver claro no contexto qual a ordem monomial $<$ estamos utilizando, denotaremos $\text{in}_<(I)$ por $\text{in}(I)$.

Segue por definição que $\text{in}(I)$ é um ideal monomial, e pelo que vimos na seção anterior, somos capazes de calcular a dimensão de $V(\text{in}(I))$. A importância desse ideal é que

$$\dim V(\text{in}(I)) = \dim V(I),$$

como veremos na Seção 1.6.

Sabemos do Teorema da Base de Hilbert que $\text{in}(I)$ é finitamente gerado. Se

$$I = < f_1, \ldots, f_m >,$$

queremos explicitar uma base para o ideal $\mathrm{in}(I)$. Em um primeiro momento, guiados pela definição de ideal inicial, somos tentados a querer dizer que $\{\mathrm{in}(f_1),\ldots,\mathrm{in}(f_m)\}$ é uma base para $\mathrm{in}(I)$. Infelizmente não é sempre verdade, como vemos no seguinte exemplo:

Exemplo 1.8. Considere o ideal $I = < x^2-y, x^2-z > \subset k[x,y,z]$, $<$ a ordem monomial lexicográfica reversa graduada. Os termos líderes deste ideal são iguais a x^2. Mas

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

e portanto $y \in \mathrm{in}(I)$, mas $y \notin < x^2 >$. Isso mostra que $\{\mathrm{in}(x^2-y), \mathrm{in}(x^2-z)\}$ não é uma base para $\mathrm{in}(I)$.

Mas há casos especiais em que $\{\mathrm{in}(f_1),\ldots,\mathrm{in}(f_m)\}$ é uma base para $\mathrm{in}(I)$. Isso nos leva a seguinte definição:

Definição 1.8. *Seja $I \subset S$ um ideal. Seja $\mathscr{M} = \{f_1,\ldots,f_m\}$ uma base de I. Então, $\mathscr{M}$ é dita uma **base de Gröbner**[4] de I se $in_< I = < in_<(f_1),\ldots,in_<(f_m) >$.*

Afim de que essa definição seja útil para os nossos interesses, temos que ser capazes de resolver os seguintes problemas: o primeiro é saber verificar se uma dada base de I é ou não uma base de Gröbner. O segundo é saber se todo ideal admite uma base de Gröbner.

Para resolver o primeiro problema, precisamos antes da seguinte definição:

Definição 1.9. *Sejam $f,g \in S$ e $<$ uma ordem monomial. O σ–polinômio de f e g é:*

$$\sigma(f,g) = \frac{MMC(in(f),in(g))}{in(f)} \cdot f - \frac{MMC(in(f),in(g))}{in(g)} \cdot g.$$

Perceba que o σ–polinômio de f e g é definido de modo a tentar obter um outro polinômio contido no ideal gerado por $< f,g >$ que possua seu monômio líder menor (segundo a ordem monomial adotada) do que os monômios líderes de f e g. Quando isso é possível, $\{f,g\}$ não é uma base de Gröbner para $< f,g >$. Esse fato será generalizado a seguir no Teorema 2.

Um fato importante a ser considerado é a divisão entre polinômios com várias variáveis. No caso de uma variável, temos o conhecido algoritmo de Divisão Euclidiana, que nos diz que dados $f(x),\ g(x) \in k[x]$ existem $q(x)$ e $r(x)$ unicamente determinados em $k[x]$ tais que

$$f(x) = g(x)q(x) + r(x),$$

onde o grau de $r(x)$ ou é menor do que o grau de $g(x)$ ou é zero. Esse fato ainda é válido para o caso de mais variáveis (fixada uma ordem monomial). Podemos ainda considerar uma pseudodivisão de um polinômio $f(x_1,\ldots,x_n)$ por um conjunto finito de polinômios

[4]A teoria das bases de Gröbner para anéis de polinômios foi desenvolvida por *Bruno Buchberger* em 1966 em sua tese, e foi assim denominada em homenagem ao seu orientador *Wolfgang Gröbner*(1899-1980).

$g_1(x_1,\ldots,x_n),\ldots,g_t(x_1,\ldots,x_n)$. Para uma tal divisão, devemos escolher uma ordem de divisão para os divisores $g_1,\ldots,g_t$. Assim obtemos a seguinte expressão:

$$f = g_1q_1 + \ldots + g_tq_t + r,$$

onde $q_1,\ldots,q_t \in S$ são os quocientes e r o resto da divisão. Diferente do caso de uma variável, os polinômios $q_1,\ldots,q_t,r$ dependem da ordem dos divisores no processo de divisão. (Veja [2], seção (2.3)).

Teorema 2 (Teste de Buchberger)**.** *Seja I um ideal. Seja $\mathscr{M} = \{f_1,\ldots,f_m\}$ uma base para I. Então $\mathscr{M}$ é uma base de Gröbner para I se, e somente se, para todo par $i \neq j$, o resto da divisão de $\sigma(f_i,f_j)$ por $\mathscr{M}$ (em qualquer ordem) seja zero.*

A prova da existência de bases de Gröbner é dada por:

Teorema 3 (Algoritmo de Buchberger)**.** *Seja $I \subset S$ um ideal. Seja $G = \{f_1,\ldots,f_m\}$ um conjunto de geradores para I. A base de Gröbner pode ser construída repetindo o algoritmo descrito abaixo um número finito de vezes:*

1. *Teste se G é uma base de Gröbner para I, utilizando o teste do Teorema 2.*

   i *Se sim, o algoritmo termina;*

   ii *Se não, defina*
   $G' = G \cup \{\text{todos os restos não nulos obtidos durante o Teste de Buchberger}\}$.

2. *Escreva $G = G'$ e volte em* 1.

O cálculo de uma base de Gröbner via algoritmo de Buchberger pode ser inviável de se fazer a mão. Por isso, somos levados a utilizar de programas computacionais. Diversos softwares matemáticos são capazes de realizar tal trabalho, e nesta dissertação opto por utilizar o Singular (veja [3]).

Exemplo 1.9. Vamos calcular a base de Gröbner de $I =< y-x^2, z-x^3 >\subset k[x,y,z]$.

Afim de elucidar o uso desse programa, apresentarei um pequeno tutorial para a obtenção da base de Gröbner de um dado ideal I:

```
> ring S = 0, (x,y,z),dp;
> poly f1 = y-x^2;
> poly f2 = z-x^3;
> ideal I = f1, f2;
> std(I);
```

A primeira linha serve para definir um anel de característica zero, cujas variáveis são x, y, z e dp informa que a ordem monomial adotada é a lexicográfica graduada reversa. A segunda e terceira linhas servem para definir os polinômios $f1 = y - x^2$ e $f2 = z - x^3$ respectivamente. A quarta linha serve para definir o ideal $I =< f1, f2 >$. Por fim, a quinta linha serve para obter uma base de Gröbner para o ideal I (neste caso, o Singular já elimina polinômios redundantes).

Voltando ao exemplo, temos que a base de Gröbner de I:

1. com a ordem lexicográfica graduada reversa é $\{y^2 - xz, xy - z, x^2 - y\}$;
2. com a ordem lexicográfica é $\{y^3 - z^2, xz - y^2, xy - z, x^2 - y\}$;
3. com a ordem lexicográfica graduada é $\{xz - y^2, xy - z, x^2 - y, y^3 - z^2\}$.

Este exemplo deixa claro que a base de Gröbner obtida pelo algoritmo de Buchberger depende da escolha da ordem monomial.

Para todos os exemplos em que fizermos o uso do Singular ao longo desse trabalho, apresentaremos apenas os comandos, omitindo os resultados. Em todos os casos, o Singular retornou uma lista de geradores para a Base de Gröbner dos ideais previamente definidos nos comandos. Dada essa lista de geradores, coletamos apenas os termos iniciais de cada gerador e os apresentamos nos respectivos exemplos.

1.5 A Função e o Polinômio de Hilbert

Nosso objetivo agora é mostrar que $\dim V(\text{in}(I)) = \dim V(I)$. Para isso, precisaremos utilizar o polinômio de Hilbert e suas propriedades.

Definição 1.10. *Seja I um ideal monomial de S. O conjunto $C(I)$ é a coleção dos expoentes dos monômios de S que não pertencem a I. Temos $C(I) \subset \mathbb{Z}^n_{\geq 0}$.*

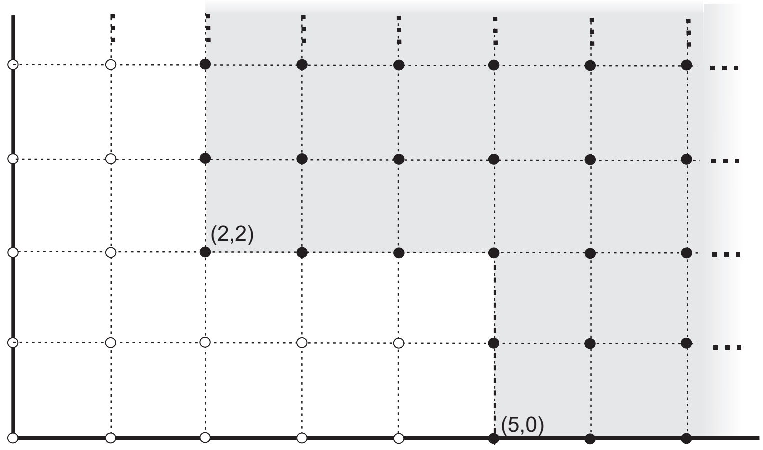
Note que $C(I)$ não é um conjunto de monômios, mas como cada monômio está associado a um único elemento de $\mathbb{Z}^n_{\geq 0}$, eventualmente cometeremos um abuso ao dizer que o monômio $X^\alpha = x_1^{a_1} \cdots x_n^{a_n} \in C(I)$, significando na realidade que o elemento $\alpha = (a_1, \ldots, a_n) \in C(I)$.

Exemplo 1.10. O conjunto $C(I)$ pode ser ilustrado da seguinte forma. Seja

$$I =< x^2y^2, x^5 >\subset k[x,y]$$

um ideal do anel de polinômios a duas variáveis. Os monômios nesse caso são do tipo x^my^n, aos quais associamos os elementos (m,n).

Observe que $x \notin I$, enquanto que $x^5 \in I$. Podemos associar $C(I)$ ao seguinte diagrama:



onde convencionamos que os monômios associados a pares ordenados representados por bolas cheias pertencem a I, e caso o monômio esteja associado a um par ordenado cuja representação é feita por uma bola vazia, significa que o monômio pertence a $C(I)$.

No exemplo acima, ainda podemos observar que $C(I)$ é formado pelo eixo coordenado formado pelos pontos do tipo $(0,n)$ (que estou convencionando como $[y]$) e a translação de $[y]$ formada pelos pontos $(1,n)$ (que na notação adotada é representado por $x+[y]$) mais os pontos $(2,0),(3,0),(4,0),(2,1),(3,1),(4,1)$. Ou seja, conseguimos dividir $C(I)$ em dois conjuntos de natureza distinta em relação a sua dimensão. Esse fato nos leva a seguinte definição:

Definição 1.11. *Seja I um ideal e seja o conjunto $C(I)$*[5].

1. $C_0(I) :=$ *o conjunto de pontos de $C(I)$ que não pertencem a nenhum dos eixos coordenados.*

2. $C_1(I) :=$ *o conjunto dos eixos de $C(I)$ que não pertencem a nenhum plano contido em $C(I)$.*

3. $C_2(I) :=$ *o conjunto dos planos de $C(I)$ que não pertencem a nenhum hiperplano contido em $C(I)$ de dimensão 3.*

4. ...

5. $C_m(I) :=$ *o conjunto dos hiperplanos de $C(I)$ de dimensão m que não pertencem a nenhum hiperplano contido em $C(I)$ de dimensão $m+1$.*

5 Cometemos um abuso de linguagem ao usarmos o termo hiperplano (plano e reta), pois o que existe na verdade é a interseção de um hiperplano coordenado com o reticulado $\mathbb{Z}^n_{\geqslant 0}$.

No Exemplo 1.10, temos que $C_0(I) = \{(2,0),(3,0),(4,0),(2,1),(3,1),(4,1)\}$ e $C_1(I) = \{[y],[y]+x\}$.

Afim de padronizar e simplificar a notação, segue a definição:

Definição 1.12. *A cada variável x_i, associemos a um elemento da base de k^n, que denotaremos por e_i. Denotaremos a translação de $[x_j]$ na direção do monômio $X^\alpha = x_1^{a_1}\cdots x_n^{a_n}$ como $X^\alpha + [e_j]$. Mais geralmente, denotaremos a translação do hiperplano formado pelas variáveis $x_{j_1},\ldots,x_{j_d}$ na direção do monômio X^α como $X^\alpha + [e_{j_1},\ldots,e_{j_d}]$.*
Ainda, quando não for necessário explicitar quais variáveis estão presentes no subespaço coordenado, denotaremos simplesmente por T^j, onde j é um índice de contagem.

Cada um dos $C_i(I)$, $i \geqslant 1$, são formados por uniões de subespaços coordenados de k^n de dimensão i e de suas translações (como $x+[y]$ no exemplo anterior).

É possível provar que $C(I)$ pode ser escrito como uma união finita de translações de subespaços coordenados T^j distintos dois a dois, mas não necessariamente disjuntos (ver [2], p. 447) mais uma quantidade finita de pontos.

Ainda no exemplo 1.10, podemos escrever

$$C(I) = \{x^2,x^3,x^4,x^2y,x^3y,x^4y,[e_2],[e_2]+x\}.$$

Exemplo 1.11. Seja $I = < x^4y^2, xy^5 >$. Então
$C(I) = \{[e_1];xy,xy^2,xy^3,xy^4,x^2y,x^2y^2,x^2y^3,x^2y^4,x^3y,x^3y^2,x^3y^3,x^3y^4,x^4y,[e_2]\}$.

Os monômios de $C(I)$ são aqueles que "sobrevivem" quando são aplicados aos vetores de $V(I)$. É essa propriedade que irá relacionar $C(I)$ com o foco central deste trabalho, que é a dimensão de V.

Proposição 1.7. *Seja I um ideal monomial. Temos então*

$$dim\, V(I) = \; max\, \{dim\, T^j \mid T^j \text{ é um subespaço de } C(I)\}.$$

Demonstração. Primeiro iremos mostrar que $[e_{i_1},\ldots,e_{i_r}] \subset C(I)$ se, e somente se, $V(x_j : j \in \Lambda) \subset V(I)$, onde Λ é o complementar do conjunto $\{i_1,\ldots,i_r\}^C$ em $\{1,\ldots,n\}$.

Se $[e_{i_1},\ldots,e_{i_r}] \subset C(I)$, então todo monômio $m \in I$ deve conter ao menos uma variável x_j, $j \in \Lambda$ (caso contrário, se algum monômio $m \in I$ contivesse apenas variáveis x_i, $i \notin \Lambda$, teríamos que $m = \prod_{i\notin\Lambda} x_i^{a_i}$. Como cada x_i, com $i \notin \Lambda$, não se anula em $V(I)$, o seu produto também não irá se anular. Daí, m não se anularia em nenhum ponto de $V(I)$, contrariando o fato de $m \in I$). Segue disso que $I \subset < x_j : j \in \Lambda >$, o que resulta em $V(x_j : j \in \Lambda) \subset V(I)$.

Por outro lado, se $V(x_j : j \in \Lambda) \subset V(I)$, seja $\omega \in V(x_j : j \in \Lambda)$ tal que o valor da i-ésima coordenada é 1 para todo $i \in \{i_1,\ldots,i_r\}$ e zero para $i \in \Lambda$. Para todo $\alpha \in [e_{i_1},\ldots,e_{i_r}]$, o seu monômio associado X^α é tal que $X^\alpha(\omega) = 1 \neq 0$. Como $\omega \in V(I)$, segue $X^\alpha \notin I$. Portanto $\alpha \in C(I)$.

Note que
$$V(x_j : j \in \Lambda) = \cap_{j\in\Lambda} V(x_j).$$

Observamos que dado $\beta = (b_1, \ldots, b_n) \in V(x_j)$ arbitrário, a j-ésima coordenada de β é a sua única coordenada que deve ser identicamente nula, ou seja, $b_j = 0$. Se $\beta \in V(x_j : \ j \in \Lambda)$, então todas as j-ésimas coordenadas de β são necessariamente nulas. Como $|\Lambda| = n - r$, o número de coordenadas que podem variar livremente em $\beta \in V(x_j : \ j \in \Lambda)$ é r, e portanto, $\dim V(x_j : \ j \in \Lambda) = r = \dim\,[e_{i_1}, \ldots, e_{i_r}]$.

Se I é monomial, então $V(I)$ pode ser escrita como uma união finita de subespaços coordenados (Proposição 1.6):
$$V(I) = \cup_{i=1}^{k} V_i.$$

Acima, vimos que a cada V_i, associa-se um subespaço coordenado T^i de $C(I)$ com a mesma dimensão. No Exemplo 1.4, concluímos que cada V_i é irredutível. Assim, a dimensão de $V(I)$ é igual a $\max_{i=1,\ldots,t}\{\dim V_i\}$ (Proposição 1.5). Digamos que $\dim V(I) = \dim V_1 = d$. Temos que existe um subespaço de $C(I)$, digamos T^1, tal que $\dim T^1 = \dim V_1 = d$. Mais,
$$\dim E_1 = \max\{\dim T^i | T^i \text{ é subespaço coordenado de } C(I)\}.$$

□

Os seguintes resultados nos fornecem uma forma de contar o número de elementos de $C(I)$.

Lema 1. *O número de monômios de grau total menor ou igual a r em S é*
$$\binom{n+r}{r}.$$

Demonstração. A prova será por indução sobre o grau r e o número de variáveis n.

Claramente a fórmula vale para $n = r = 2$, pois $\frac{(2+2)(2+1)}{2} = 6$, e os monômios de grau menor ou igual a 2 com duas variáveis são $1, x, y, xy, x^2, y^2$.

Agora suponha válida a expressão para $n-1$ variáveis e grau $r-1$. Queremos mostrar que
$$|S_{\leqslant r}| = \binom{n+r}{r}.$$

Para simplificar a notação, sejam:

- $A = \{m \in k[x_1, \ldots, x_{n-1}] \mid m \text{ é um monômio}\}$;

- $A_{<r} = \{m \in A \mid m \text{ é um monômio de grau menor do que } r\}$;

- $A_r = \{m \in A \mid m$ é um monômio de grau igual a $r\}$;

- $B = \{x_n^a m \mid m \in A\}$;

- $B_{<r} = \{m \in B \mid m$ é um monômio de grau menor do que $r\}$;

- $B_r = \{m \in B \mid m$ é um monômio de grau igual a $r\}$.

Com os conjuntos acima definidos, podemos escrever:

$$\begin{aligned} S_{\leqslant r} &= S_{<r} \cup S_r \text{ (observe que se trata de uma união disjunta.)} \\ &= S_{<r} \cup (A_r \cup B_r) \text{ (a união apresentada entre os parênteses é também disjunta.)} \\ &= S_{<r} \cup A_r \cup B_r. \end{aligned}$$

Como todas as uniões acima são disjuntas, segue que

$$|S_{\leqslant r}| = |S_{<r}| + |A_r| + |B_r|.$$

Por hipótese de indução,

$$|S_{<r}| = \begin{pmatrix} (r-1)+n \\ (r-1) \end{pmatrix} = \begin{pmatrix} r+n-1 \\ r-1 \end{pmatrix}.$$

O número de elementos de A_r é a combinação completa[6] de $n-1$ variáveis tomadas r a r,

$$\mathrm{CR}_{n-1,r} = \mathrm{C}_{r+(n-1)-1,r} = \mathrm{C}_{r+n-2,r} = \begin{pmatrix} r+n-2 \\ r \end{pmatrix}.$$

Para calcular o número de elementos de B_r, note que todos os seus monômios são do tipo $x_n m$, onde $m \in S_{r-1}$. Disso resulta que $|B_r| = |S_{r-1}|$. Daí,

$$|B_r| = |S_{r-1}| = \mathrm{CR}_{n,r-1} = \mathrm{C}_{(r-1)+n-1,r-1} = \mathrm{C}_{r+n-2,r-1} = \begin{pmatrix} r+n-2 \\ r-1 \end{pmatrix}.$$

Portanto,

$$\begin{aligned} |S_{\leqslant r}| &= |S_{<r}| + |A_r| + |B_r| \\ &= \begin{pmatrix} r+n-1 \\ r-1 \end{pmatrix} + \begin{pmatrix} r+n-2 \\ r \end{pmatrix} + \begin{pmatrix} r+n-2 \\ r-1 \end{pmatrix} \\ &= \begin{pmatrix} r+n-1 \\ r-1 \end{pmatrix} + \begin{pmatrix} r+n-1 \\ r \end{pmatrix} \\ &= \begin{pmatrix} r+n \\ r \end{pmatrix}, \end{aligned}$$

como queríamos demonstrar. $\square$

[6] A expressão para o cálculo de uma combinação completa de n tomados r a r $\mathrm{CR}_{n,r}$ pode ser encontrada em [11].

Teorema 4. *Seja $I \subset S$ um ideal monomial com $\dim V(I) = d$. Então para r suficientemente grande, o número de monômios que não pertencem a I de grau total menor ou igual a r é dado por um polinômio de grau d na variável r.*

Demonstração. A ideia desta demonstração é realizar a contagem dos monômios de grau menor ou igual a r associados aos elementos de $C(I)$, o qual denotaremos por $|C(I)_{\leqslant r}|$, e verificar que para r_0 suficientemente grande, $|C(I)_{\leqslant r}|$ é dado por um polinômio na variável r para todo $r > r_0$. Mas antes iremos fazer algumas observações sobre o conjunto $C(I)$.

O primeiro fato a se observar é que se uma translação T^j de um subespaço coordenado $[e_{i_1}, \dots, e_{i_t}]$ pertence a $C(I)$, então o próprio espaço coordenado pertence a $C(I)$. De fato, seja $f \in T^j = X^\alpha + [e_{i_1}, \dots, e_{i_t}]$, assim $f = c x_{i_1}^{a_{i_1}} \cdots x_{i_t}^{a_{i_t}}$. Isso nos diz que f não se anula em nenhum ponto de $V(I)$. Como S é um domínio de integridade, $x_{i_1}^{a_{i_1}} \cdots x_{i_t}^{a_{i_t}}$ também não se anula em nenhum ponto de $V(I)$, ou seja $x_{i_1}^{a_{i_1}} \cdots x_{i_t}^{a_{i_t}} \in C(I)$.

Como por hipótese $\dim V = d$, então todos os subespaços coordenados contidos em $C(I)$ possuem dimensão menor ou igual a d, e além disso, pelo menos um deles tem dimensão d (Proposição 1.7).

Iremos agora realizar a contagem do número de elementos de cada tipo de componente de $C(I)$ separadamente. Primeiro caso: número de elementos de um espaço coordenado de dimensão t. Neste caso, o número de elementos de grau total menor ou igual a r é dado por

$$\binom{t+r}{r} = \binom{t+r}{t} = \frac{(r+t)!}{t!r!} = \frac{1}{t!}(r+t)\cdots(r+1). \tag{1.1}$$

Note que a expressão obtida em (1.1) é um polinômio na variável r de grau t, cujo coeficiente líder é $\frac{1}{t!}$ (positivo!).

O segundo tipo de componente são as translações T^j dos subespaços coordenados. Digamos que $T^j = X^\alpha + [e_{i_1}, \dots, e_{i_t}]$ (observe então que $\dim T^j = t$). Neste caso, o número de elementos de T^j de grau menor ou igual a r, denotado por $|T^j|_{\leqslant r}$ é dado por:

$$|T^j|_{\leqslant r} = \begin{cases} 0 & \text{se} \quad r < |X^\alpha|, \\ \dbinom{t+r-|\alpha|}{r-|\alpha|} & \text{se} \quad r \geqslant |X^\alpha|. \end{cases}$$

Para simplificar a notação, quando não for necessário explicitar a composição de um subespaço coordenado $[e_{i_1}, \dots, e_{i_t}]$, será denotado também por $T^j = X^\alpha + [e_{i_1}, \dots, e_{i_t}]$, onde j é um índice de contagem e nesse caso $\alpha = 1$.

Assim, a contagem final dos elementos de grau menor ou igual a r de $C(I)$, denotado por $|C(I)_{\leqslant r}|$ é dada por

$$
\begin{aligned}
|C(I)_{\leqslant r}| &= |T^1_{\leqslant r} \cup \cdots \cup T^s_{\leqslant r}| \\
&= \sum_{k=1}^{s} (-1)^{k-1} \Big(\sum_{1 \leqslant i_1 < \ldots < i_k \leqslant s} |T^{i_1}_{\leqslant r} \cap \cdots \cap T^{i_k}_{\leqslant r}| \Big) \\
&= \sum_{k=1}^{s} |T^k| - \sum_{1 \leqslant i_1 < i_2 \leqslant s} |T^{i_1}_{\leqslant r} \cap T^{i_2}_{\leqslant r}| + \sum_{1 \leqslant i_1 < i_2 < i_3 \leqslant s} |T^{i_1}_{\leqslant r} \cap T^{i_2}_{\leqslant r} \cap T^{i_3}_{\leqslant r}| - \ldots
\end{aligned} \tag{1.2}
$$

Essa penúltima igualdade é um resultado de contagem conhecido por *Princípio de Inclusão e Exclusão* e pode ser encontrado em [11]. O uso desse princípio se fez necessário, pois em geral os subespaços coordenados e suas translações não são disjuntos, e sendo assim, devemos considerar suas interseções.

Pelo que vimos anteriormente a parcela $\sum_{k=1}^{s} |T^k_{\leqslant r}|$, quando r é suficientemente grande, é a soma de polinômios de graus menores ou iguais a d com pelo menos um deles possuindo grau d, cujos coeficientes líderes são positivos, e portanto sua soma é um polinômio de grau d na variável r, digamos $p_1(r)$.

O próximo passo é mostrar que a soma das demais parcelas de $|C(I)_{\leqslant r}|$ formam (quando r é suficientemente grande) um polinômio na variável r de grau estritamente menor que d, digamos $p_2(r)$. Com isso teremos que

$$|C(I)_{\leqslant r}| = p(r) = p_1(r) + p_2(r),$$

onde $p(r)$ é a soma de um polinômio na variável r de grau d com outro na variável r de grau estritamente menor do que d. Isso prova o teorema.

Para mostrar que $p_2(r)$ é um polinômio na variável r de grau menor do que d é suficiente mostrar que se $T^i_{\leqslant r} \neq T^j_{\leqslant r}$ $(i \neq j)$, $T^i_{\leqslant r} \cap T^j_{\leqslant r}$ é uma translação de um subespaço coordenado e que $\dim\{T^i_{\leqslant r} \cap T^j_{\leqslant r}\} < \max_{k=j,i} \{\dim(T^k)\}$. Se $T^i_{\leqslant r} \cap T^j_{\leqslant r} = \varnothing$, não há nada o que fazer.

Suponha $T^i_{\leqslant r} \cap T^j_{\leqslant r} \neq \varnothing$. Suponhamos também que $T^i = X^\alpha + [e_{i_1}, \ldots, e_{i_m}]$, onde $\alpha = \sum_{i \notin \{i_1, \ldots, i_m\}} a_i e_i$, e $T^j = X^\beta + [e_{j_1}, \ldots, e_{j_q}]$, onde $\beta = \sum_{j \notin \{j_1, \ldots, j_r\}} b_j e_j$.

Por construção, as variáveis que aparecem efetivamente em X^α (ou seja, que possuem seu expoente diferente de zero) não pertencem a $\{x_{i_1}, \ldots, x_{i_m}\}$, daí podemos escrever (após reindexamento) $X^\alpha = x_{i_{m+1}}^{a_1} \cdots x_{i_{m+\lambda}}^{a_\lambda}$ com $a_i > 0\ \forall i$. Analogamente $X^\beta = x_{j_{q+1}}^{b_1} \cdots x_{j_{q+\delta}}^{b_\delta}$ com $b_j > 0\ \forall j$.

O próximo passo é mostrar que $[e_{i_1}, \ldots, e_{i_m}] \neq [e_{j_1}, \ldots, e_{j_q}]$. Para tal, suponha por absurdo que $[e_{i_1}, \ldots, e_{i_m}] = [e_{j_1}, \ldots, e_{j_q}]$. Neste caso temos que $m = r$ e com isso podemos supor que $e_{i_k} = e_{j_k}\ \forall 1 \leqslant k \leqslant m$.

Ainda, temos que existem $f \in T^i_{\leqslant r} \cap T^j_{\leqslant r}$ e $c_1, \ldots, c_m, d_1, \ldots, d_m$ tais que:

$$f = x_{i_1}^{c_1} \cdots x_{i_m}^{c_m} \cdot x_{i_{m+1}}^{a_1} \cdots x_{i_{m+\lambda}}^{a_\lambda} \tag{1.3}$$

e

$$f = x_{i_1}^{d_1} \cdots x_{i_m}^{d_m} \cdot x_{j_{q+1}}^{b_1} \cdots x_{j_{q+\delta}}^{b_\delta}. \tag{1.4}$$

Por definição de f, cada par de índices diferentes remetem a variáveis diferentes. Logo, $c_{i_l} = d_{i_l}$ $\forall 0 \leqslant l \leqslant m$. Deste fato segue que podemos reescrever a equação (1.4) como:

$$f = x_{i_1}^{c_1} \cdots x_{i_m}^{c_m} \cdot x_{j_{q+1}}^{b_1} \cdots x_{j_{q+\delta}}^{b_\delta}. \tag{1.5}$$

Comparando as equações (1.3) e (1.5), concluímos que:

$$\begin{aligned} X^\alpha &= x_{i_{m+1}}^{a_{i_1}} \cdots x_{i_{m+\lambda}}^{a_{i_\lambda}} \\ &= x_{j_{q+1}}^{b_1} \cdots x_{j_{q+\delta}}^{b_\delta} \\ &= X^\beta. \end{aligned}$$

Com isso concluímos que $T^i_{\leqslant r} = T^j_{\leqslant r}$, contradição. Portanto devemos ter $[e_{i_1}, \ldots, e_{i_m}] \neq [e_{j_1}, \ldots, e_{j_q}]$.

Para mostrar que $T^i_{\leqslant r} \cap T^j_{\leqslant r}$ é uma translação contida em $C(I)$, observe que temos

$$[e_{i_1}, \ldots, e_{i_m}] \cap [e_{j_1}, \ldots, e_{j_q}] = [e_{k_1}, \ldots, e_{k_t}]$$

onde $t \leqslant \min\{m, q\}$ e $e_{k_l} \in \{e_{i_1}, \ldots, e_{i_m}, e_{j_1}, \ldots, e_{j_q}\}$.

Isso mostra que $[e_{k_1}, \ldots, e_{k_t}] \subset C(I)$. Desde que $\alpha, \beta \in C(I)$, segue que $\alpha \cap \beta \in C(I)$. Decorre disso que $T^i_{\leqslant r} \cap T^j_{\leqslant r} \subset C(I)$.

Observe que a dimensão da translação $T^i_{\leqslant r} \cap T^j_{\leqslant r}$ é igual a dimensão do subespaço coordenado $[e_{k_1}, \ldots, e_{k_t}]$, que é igual a $t \leqslant m_1 = \min\{m, q\}$.

Se $t < m_1$, segue que $t < m_2 = \max\{m, q\}$. Caso $m = m_1 = t$ (análogo se $m_1 = q$), segue que $[e_{i_1}, \ldots, e_{i_m}] \subset [e_{j_1}, \ldots, e_{j_q}]$. Nestas condições, se $t = m_2 = \max\{m, q\}$, teríamos $T^i_{\leqslant r} = T^j_{\leqslant r}$. Logo devemos ter $t < m_2$.

Isso mostra que $\dim\{T^i_{\leqslant r} \cap T^j_{\leqslant r}\} < \max\{m, q\} = \max_{k=i,j}\{\dim T^k_{\leqslant r}\}$.

Com isso concluímos que para r suficientemente grande, $|C(I)_{\leqslant r}|$ é um polinômio de grau d na variável r. □

Definição 1.13. *Definimos $S_{\leqslant r} = \{f \in S |$ grau total de f seja menor ou igual a $r\}$ e $S_r = \{f \in S |$ grau total de f seja igual a $r\}$.*

O conjunto $S_{\leqslant r}$ é um espaço vetorial de dimensão finita sobre k e sua base é $\{X^\alpha | \alpha \in \mathbb{Z}_{\geqslant 0}$ e $|\alpha| \leqslant r\}$. Além disso, o número de elementos do conjunto $S_{\leqslant r}$ é igual a $\begin{pmatrix} n+r \\ r \end{pmatrix}$.

Definição 1.14. *Se $I \subset S$ é um ideal arbitrário, definimos $I_{\leqslant r} = I \cap S_{\leq r}$ e $I_r = I \cap S_r$.*

Observe que $I_{\leqslant r}$ é um subespaço vetorial de $S_{\leqslant r}$, no entanto não é um ideal.

Definição 1.15. *Dado I um ideal de S, a função afim de Hilbert de I é*

$$^{a}HF_I(r) = dim\ S_{\leqslant r}/I_{\leqslant r} = dim\ S_{\leqslant r} - dim\ I_{\leqslant r}, \forall r \geqslant 0.$$

Caso I seja um ideal monomial, a função afim correspondente a Hilbert (de forma equivalente a apresentada acima) é a função que mapeia r à quantidade de monômios que não pertencem a I cujo grau total é menor ou igual a r. De fato, temos por definição que a função conta todos os monômios de grau menor ou igual a r em S e subtrai a quantidade presente a I.

Pelo Teorema 4, temos que para r suficientemente grande, a função afim de Hilbert de um ideal monomial é um polinômio.

Exemplo 1.12. Vamos obter a função afim de Hilbert de $V(y^2, z^2) \subset k^4$. Como foi observado acima, no caso de I ser um ideal monomial, uma propriedade da $^{a}HF(r)$ é fazer a contagem dos monômios que não pertencem ao ideal que define a variedade. Neste caso o ideal é $I = < y^2, z^2 > \subset k[x,y,z,w]$.

Sejam os conjuntos:

1. $A_1 = \{\, x^a w^b \mid a,b \in \mathbb{Z}_+\}$ e $A_1^k = \{\, x^a w^b \mid a,b \in \mathbb{Z}_+,\ a+b \leqslant k\}$;
2. $A_2 = \{\, yx^a w^b \mid a,b \in \mathbb{Z}_+\}$ e $A_2^k = \{\, yx^a w^b \mid a,b \in \mathbb{Z}_+,\ a+b+1 \leqslant k\}$;
3. $A_3 = \{\, zx^a w^b \mid a,b \in \mathbb{Z}_+\}$ e $A_3^k = \{\, zx^a w^b \mid a,b \in \mathbb{Z}_+,\ a+b+1 \leqslant k\}$;
4. $A_4 = \{\, yzx^a w^b \mid a,b \in \mathbb{Z}_+\}$ e $A_4^k = \{\, yzx^a w^b \mid a,b \in \mathbb{Z}_+,\ a+b+2 \leqslant k\}$.

Observe que

$$C(I) = \cup_{i=1}^{4} A_i$$

e mais, $A_i^k \cap A_j^k = \varnothing\ \forall i \neq j$ e $\forall k > 0$. Com isso, temos que o número de elementos de grau total menor ou igual a k de $C(I)$ pode ser obtido como a soma da quantidade de elementos de cada A_i^k (o qual denoto por $|A_i^k|$).

Utilizando de técnicas de contagem, obtemos que $|A_1^k|$ é $\frac{(k+2)(k+1)}{2}$. Em geral temos:

Grau Total k	$\lvert A_1^k\rvert$	$\lvert A_2^k\rvert$	$\lvert A_3^k\rvert$	$\lvert A_4^k\rvert$	${}^aHF(k)$
0	1	0	0	0	1
1	3	1	1	0	5
2	6	3	3	1	13
3	10	6	6	3	25
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r	$\frac{(r+2)(r+1)}{2}$	$\frac{(r+1)r}{2}$	$\frac{(r+1)r}{2}$	$\frac{r(r-1)}{2}$	$2r^2+2r+1$

A tabela acima fornece a função afim de Hilbert. Observe que quando escrevemos $k = r$, obtemos um polinômio na variável r que satisfaz a função de Hilbert para todo $r \geqslant 0$. Com isso concluímos que

$$^aHF_I(r) = 2r^2 + 2r + 1 \ \forall r > 0.$$

Exemplo 1.13. Para encontrar a função afim de Hilbert de $V(x^2y^2, x^5) \subset k^2$, analogamente ao exemplo anterior, vamos fazer a contagem dos elementos de $C(I)$, onde

$$I =< x^2y^2, x^5 >\subset k[x,y].$$

Note que $C(I)$ é ilustrado no Exemplo 1.10.

Sejam os conjuntos:

1. $B_1 = \{\ y^a \mid a \in \mathbb{Z}_+\}$ e $B_1^k = \{\ y^a \mid a \in \mathbb{Z}_+,\ a \leqslant k\}$;
2. $B_2 = \{\ xy^a \mid a \in \mathbb{Z}_+\}$ e $B_2^k = \{\ xy^a \mid a \in \mathbb{Z}_+,\ a+1 \leqslant k\}$;
3. $B_3 = \{x^2, x^3, x^4, x^2y, x^3y, x^4y\}$ e $B_3^k = \{m \mid m \in B_3, \partial m \leqslant k\}$.

Observe que

$$C(I) = \cup_{i=1}^3 B_i.$$

Ainda, $B_i^k \cap B_j^k = \varnothing\ \forall i \neq j$ e $\forall k > 0$. Logo ${}^aHF(k) = \sum_{i=1}^3 |B_i^k|$. Daí,

Grau Total k	$\|B_1^k\|$	$\|B_2^k\|$	$\|B_3^k\|$	${}^aHF(k)$
0	1	0	0	1
1	2	1	0	3
2	3	2	1	6
3	4	3	3	10
4	5	4	4	13
5	6	5	6	17
6	7	6	6	19
7	8	7	6	21
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r	$r+1$	r	6	$2r+7$

A tabela acima fornece a função afim de Hilbert. Note que a expressão polinomial obtida quando fazemos $k = r$ não é válida para $k = 0,1,2,3,4$. Isso ocorre pois não conseguimos padronizar a contagem do número de elementos de B_3^k em função do grau total k. Entretanto esse problema ocorre somente enquanto estivermos considerando $k < 5$ (o maior dos graus dos monômios de B_3^k). Após esse valor, $|B_3^k| = 6\ \forall k \geqslant 5$. Nesse caso temos

$$
{}^aHF_I(r) = \begin{cases} 1, & \text{se} \quad r = 0; \\ 3, & \text{se} \quad r = 1; \\ 6, & \text{se} \quad r = 2; \\ 10, & \text{se} \quad r = 3; \\ 13, & \text{se} \quad r = 4; \\ 2r+7, & \text{se} \quad r \geqslant 5. \end{cases}
$$

O próximo resultado exibe a relação entre a função afim de Hilbert do ideal I e do seu ideal inicial $\mathrm{in}(I)$.

Proposição 1.8. *Seja $I \subset S$ um ideal e $<$ uma ordem monomial graduada. Então o ideal monomial $in(I)$ tem a mesma função afim de Hilbert de I.*

Demonstração. Fixemos r e considere todos os monômios líderes de todos os elementos $f \in I_{\leq r}$. Como o conjunto de monômios de grau menor ou igual a r é finito, então o conjunto de todos os monômios líderes de todos os elementos de $I_{\leq r}$ (a menos de repetições) é um conjunto finito, isto é,

$$\{\min(f)\,|\, f \in I_{\leq r}\} = \{\min(f_1), \ldots, \min(f_m)\}. \tag{1.6}$$

Podemos assumir que $\min(f_1) > \ldots > \min(f_m)$. Mostremos que $\{f_i\}$ forma uma base para $I_{\leq r}$ como espaço vetorial sobre k.

Para provar esse fato, vamos mostrar inicialmente que $\{f_i\}$ é um conjunto linearmente independente. Considere uma combinação linear não trivial sendo igual a zero:

$$a_1 f_1 + \ldots + a_m f_m = 0. \tag{1.7}$$

Escolha o menor i , digamos i_0, tal que $a_i \neq 0$. Temos então que:

$$0 f_1 + \ldots + 0 f_{i_0 - 1} + a_{i_0} f_{i_0} + a_{i_0+1} f_{i_0+1} + \ldots + a_m f_m = 0, \tag{1.8}$$

donde obtemos que

$$f_{i_0} = -a_{i_0}^{-1} \left(a_{i_0+1} f_{i_0+1} + \ldots + a_m f_m \right), \tag{1.9}$$

o que é um absurdo, pois cada $f_i \in I_{\leq r}$, com $i > i_0$ é menor que f_{i_0}.

Mostremos que $\{f_i\}$ forma um conjunto de geradores. Seja $W = \langle f_1, \cdots, f_m \rangle \subset I_{\leq r}$. Suponha que $W \neq I_{\leq r}$. Então existe $g \in I_{\leq r} - W$. Dentre tais possíveis, tome aquele cujo $\min(g)$ seja mínimo.

Decorre de (1.6) que deve existir algum i_b tal que $\min(g) = \min(f_{i_b})$, o que implica $\mathrm{in}(g) = c\,\mathrm{in}(f_{i_b})$, onde $c \in k$. Segue então que $h = g - c f_{i_b} \in I_{\leq r}$ tem o seu monômio líder de grau menor do que g. Como por hipótese tomamos g aquele cujo monômio líder é o de menor grau, h deve pertencer a W. Mas se $h \in W$ então $h + c f_{i_b} \in W$, logo $g \in W$, o que é absurdo. Portanto $\{f_1, \ldots, f_m\}$ é uma base para $I_{\leq r}$.

De modo análogo, $\{\min(f_1), \ldots, \min(f_m)\}$ forma uma base para $\mathrm{in}(I)_{\leq r}$. Com isso temos que as bases para $I_{\leq r}$ e $\mathrm{in}(I)_{\leq r}$ possuem o mesmo número de elementos, ou seja, a mesma dimensão vetorial sobre k. E segue da definição de função afim de Hilbert que:

$$\begin{aligned} {}^a HF_I(r) &= \dim S_{\leq r} - \dim I_{\leq r} \\ &= \dim S_{\leq r} - \dim \mathrm{in}(I)_{\leq r} \\ &= {}^a HF_{\mathrm{in}(I)}(r). \end{aligned} \qquad \square$$

O resultado acima nos diz que dado um ideal $I \subset S$ qualquer, a função afim de Hilbert ${}^a HF_I(r)$ é um polinômio para r suficientemente grande (Teorema 4). Dizemos que esse polinômio é o **polinômio afim de Hilbert de** I, e o denotamos por ${}^a HP_I(r)$.

Exemplo 1.14. Sejam $I = < y^2, z^2 >$ e $J = < x^2 y^2, x^5 >$. Pelos Exemplos 1.12 e 1.13, temos que:

$${}^a HP_I(r) = 2r^2 + 2r + 1 \ \text{ e } \ {}^a HP_J(r) = 2r + 7.$$

1.6 Dimensão de Variedades Algébricas

Nesta seção iremos abordar o caso em que $V = V(I)$, onde I é um ideal qualquer de S. O primeiro passo será relacionar o polinômio afim de Hilbert de I com o polinômio afim de

Hilbert de $\sqrt{I}$.

Lema 2. *Se $I_1 \subset I_2$ então $deg^a HP_{I_2} \leq deg^a HP_{I_1}$.*

Demonstração. Observe que

$$\begin{aligned} I_1 \subset I_2 \quad &\Rightarrow \quad \text{in}(I_1) \subset \text{in}(I_2) \\ &\Rightarrow \quad \text{C}(\text{in}(I_1)) \supseteq \text{C}(\text{in}(I_2)). \end{aligned} \tag{1.10}$$

Agora, fixando $r \geq 0$, nós sabemos que ${}^aHF_{\text{in}(I_i)}(r)$ é o número de monômios de grau menor ou igual a r que não pertencem a $\text{in}(I_i)$, ou seja, o número de elementos de $\text{C}(\text{in}(I_i))$. Com isso, segue de (1.10) e da Proposição 1.8, o seguinte:

$${}^aHF_{I_1}(r) \;=\; {}^aHF_{\text{in}(I_1)}(r) \;\text{ e }\; {}^aHF_{\text{in}(I_2)}(r) \;=\; {}^aHF_{I_2}(r). \tag{1.11}$$

Como a desigualdade acima deve valer para todo $r \geq 0$, então devemos ter que

$$\deg{}^aHF_{\text{in}(I_1)}(r) \geq \deg{}^aHF_{\text{in}(I_2)}(r),$$

pois caso contrário teríamos (para r suficientemente grande, ${}^aHF$ é um polinômio):

$$\lim_{r\to\infty} \frac{{}^aHF_{\text{in}(I_1)}(r)}{{}^aHF_{\text{in}(I_2)}(r)} = 0.$$

Esse limite nos diz que o denominador se tornará muito maior do que o numerador a partir de algum momento, o que é um absurdo, pois por (1.10) o numerador é sempre maior ou igual ao denominador, e nunca menor.

Segue de (1.11) que $\deg{}^aHF_{I_1}(r) \geq \deg{}^aHF_{I_2}(r)$. $\square$

Proposição 1.9. *Se $I \subset S$ é um ideal, então o polinômio afim de Hilbert de I e $\sqrt{I}$ possuem o mesmo grau.*

Demonstração. Vamos mostrar primeiro o caso em que I é um ideal monomial. Vimos na Proposição 1.1 que se I é um ideal monomial, então $\sqrt{I}$ é monomial. Pelo Exemplo 1.3, $V(I) = V(\sqrt{I})$, e portanto $\dim V(I) = \dim V(\sqrt{I})$. Assim, pelo Teorema 4 temos $\deg{}^aHP_{\sqrt{I}} = \deg{}^aHP_I$. Isso mostra que o resultado vale no caso de ideais monomiais.

Se $I \subset S$ um ideal, então valem as inclusões:

$$\text{in}(I) \subset \text{in}(\sqrt{I}) \subset \sqrt{\text{in}(I)}. \tag{1.12}$$

A primeira inclusão segue diretamente do fato de $I \subset \sqrt{I}$. Para mostrar a segunda, tome $X^k \in \text{in}(\sqrt{I})$. Então existe $f \in \sqrt{I}$ tal que $\text{in}(f) = X^k$. Temos também que se $f \in \sqrt{I}$, então existe $n \geq 0$ tal que $f^n \in I$. Segue então que:

$$\text{in}(f^n) = (\text{in}(f))^n = (X^k)^n = X^{kn} \in \text{in}(I). \tag{1.13}$$

Segue daí que $X^k \in \sqrt{\text{in}(I)}$. Aplicando o Lema 2 a (1.12) temos que

$$\deg^a HP_{\sqrt{\mathrm{in}(I)}} \leq \deg^a HP_{\mathrm{in}(\sqrt{I})} \leq \deg^a HP_{\mathrm{in}(I)}. \tag{1.14}$$

Pela Proposição 1.8, são válidas

$$\deg^a HP_I = \deg^a HP_{\mathrm{in}(I)} \text{ e } \deg^a HP_{\sqrt{I}} = \deg^a HP_{\mathrm{in}(\sqrt{I})}.$$

Ainda, como vimos no início desta demonstração, temos

$$\deg^a HP_{\mathrm{in}(\sqrt{I})} = \deg^a HP_{\sqrt{\mathrm{in}(I)}}. \tag{1.15}$$

Então as desigualdades apresentadas em (1.14) na realidade são igualdades. Utilizando a Proposição 1.8, obtemos o seguinte:

$$\begin{array}{ccccc} \deg^a HP_{\sqrt{\mathrm{in}(I)}} & = & \deg^a HP_{\mathrm{in}(\sqrt{I})} & = & \deg^a HP_{\mathrm{in}(I)} \\ & & \shortparallel & & \shortparallel \\ & & \deg^a HP_{\sqrt{I}} & & \deg^a HP_I \end{array}$$

o que prova o resultado afirmado. □

Na seção anterior vimos na Proposição 1.8 que ${}^aHP_I = {}^a HP_{\mathrm{in}(I)}$. A Proposição 1.9 mostra que o grau do polinômio de Hilbert de I e $\sqrt{I}$ são iguais. Esses resultados mostram que um grande número de ideais associados a mesma variedade V possuem seus polinômios afim de Hilbert com o mesmo grau.

No Teorema 4, temos para o caso de ideais monomiais uma associação entre o grau do polinômio de Hilbert e a dimensão (de Krull). Esse fato pode ser generalizado para ideais quaisquer e a prova desse fato é dada na seção 5.6 de [8]. A partir desse fato, podemos enunciar a seguinte definição.

Definição 1.16. *Seja $V \subset k^n$ uma variedade algébrica afim. Definimos*

$$dim V = deg^a HP_{\mathscr{I}(V)}.$$

Uma consequência direta da definição acima e do teorema de zeros de Hilbert é que $\dim V(I)$ é igual a $\deg^a HP_{\sqrt{I}}$, onde I é um ideal qualquer de S.

O próximo teorema trás um resumo de todos os resultados apresentados neste capítulo.

Teorema 5. *Seja $V = V(I)$ uma variedade afim, onde $I \subset S$ é um ideal. Se k é algebricamente fechado então*

$$dim\, V = deg^a HP_I.$$

Além disso, se $<$ é uma ordem graduada sobre S, então

$$\begin{aligned} dim\, V &= deg^a HP_{in(I)} \\ &= \text{máximo das dimensões dos subespaços de } V(in(I)). \end{aligned}$$

Finalmente, as duas últimas igualdades são válidas sobre qualquer corpo quando $I = \mathscr{I}(V)$.

Demonstração. Pela Definição 1.16, a dimensão de uma variedade afim $V(I) \subset k^n$ é o grau do polinômio afim de Hilbert do ideal $\mathscr{I}(V) \subset S$. Deste fato, segue que

$$\dim V = \deg^a HP_{\mathscr{I}(V)} = \deg^a HP_{\sqrt{I}},$$

pois no caso de k ser algebricamente fechado, temos que $\mathscr{I}(V) = \sqrt{I}$ (Teorema de Zeros de Hilbert). Com isso, nosso objetivo é mostrar que

$$\deg^a HP_{\sqrt{I}} = \deg^a HP_I = \deg^a HP_{\text{in}(I)}. \tag{1.16}$$

Temos que a primeira igualdade dada em (1.16) é verificada pela Proposição 1.9, e a segunda é dada pela Proposição 1.8. Isso mostra que

$$\dim V = \deg^a HP_{\text{in}(I)}.$$

Como $\text{in}(I)$ é um ideal monomial, pela Proposição 1.6, $V(\text{in}(I))$ pode ser escrito como uma união finita de subespaços coordenados de k^n. Portanto $\deg^a HP_{\text{in}(I)}$ é igual ao máximo das dimensões dos subespaços de $\text{V}(\text{in}(I))$.

Agora, num corpo qualquer, se vale que

$$I = \mathscr{I}(V)$$

então, segue diretamente da definição de dimensão que:

$$\dim V = \deg^a HP_{\mathscr{I}(V)} = \deg^a HP_I.$$

□

Com os resultados deste capítulo, somos capazes de calcular a dimensão de uma variedade $V = V(I)$, onde I é um ideal qualquer de S, realizando os seguintes passos:

1º - Obter uma base de Gröbner do ideal, usando alguma ordem graduada, obtendo assim $\text{in}(I)$.

2º - Decompor $V(\text{in}(I))$ em subespaços coordenados V_i de k^n;

3º - Calcular a dimensão de todos os V_i obtidos no segundo passo.

A maior dimensão obtida no 3º passo é a dimensão da variedade $V(I)$.

Os exemplos abaixo serão calculados utilizando a ordem monomial graduada reversa.

Exemplo 1.15. Vamos agora calcular a dimensão da variedade $V(y-x^2, z-x^3) \subset k^3$ (Cúbica reversa afim) utilizando o Singular:

```
> ring S = 0, x(1..3), dp;
> poly f1 = x(2)-x(1)^2;
> poly f2 = x(3)-x(1)^3;
```

```
> ideal I = f1,f2;
> std(I);
```

A base de Gröbner obtida para $< y - x^2,\ z - x^3 >$ é $\{x_2^2 - x_1x_3,\ x_1x_2 - x_3,\ x_1^2 - x_2\}$. Assim, pelo que vimos até agora, precisamos calcular a dimensão de $V(x_2^2,\ x_1x_2,\ x_1^2)$, para deduzirmos a dimensão de $V(I)$. Note que
$V(x_2^2, x_1x_2, x_1^2) = V(x_2^2) \cap V(x_1x_2) \cap V(x_1^2) = V(x_2) \cap (V(x_1) \cup V(x_2)) \cap V(x_1) = V(x_2) \cap V(x_1)$.

Como $V(x_1)$ e $V(x_2)$ são dois planos coordenados de k^3, a sua interseção é uma reta, cuja dimensão é 1. Portanto

$$\dim V(I) = \dim V(\mathrm{in}(I)) = 1.$$

Exemplo 1.16. Iremos calcular a dimensão da variedade dada pelos zeros do ideal

$$I =< x_1^3 + x_2^3 - x_3^3,\ x_2^4 + x_3^4 - x_4^4,\ x_3^5 + x_4^5 - x_1^5 > .$$

```
> ring S = 0, x(1..4), dp;
> poly f1 = x(1)^3+x(2)^3-x(3)^3;
> poly f2 = x(2)^4+x(3)^4-x(4)^4;
> poly f3 = x(3)^5+x(4)^5-x(1)^5;
> ideal I = f1,f2,f3;
> std(I);
```

Obtemos então que

$$\mathrm{in}(I) =< x_1^3,\ x_2^4,\ x_1^2x_2^3,\ x_2^3x_3^3,\ x_1^2x_2x_3^3,\ x_1x_2^3x_3^5,\ x_2^2x_3^6,\ x_1^2x_3^6,\ x_2x_3^8,\ x_1x_3^8,\ x_3^{10} > .$$

Assim,

$$\begin{aligned} V(\mathrm{in}(I)) &= V(x_1^3,\ x_2^4,\ x_1^2x_2^3,\ x_2^3x_3^3,\ x_1^2x_2x_3^3,\ x_1x_2^3x_3^5,\ x_2^2x_3^6,\ x_1^2x_3^6,\ x_2x_3^8,\ x_1x_3^8,\ x_3^{10}) \\ &= V(x_1) \cap V(x_2) \cap V(x_3). \end{aligned}$$

Essa última cadeia de interseções mostra que a única variável livre é x_4. Portanto sua dimensão é 1.

2 Ideal Inicial Genérico

No capítulo anterior vimos uma técnica para o cálculo da dimensão de variedades algébricas afins, e o principal ponto dessa técnica é obter o ideal inicial. Pelos exemplos vistos, percebemos que a obtenção desse ideal depende da ordem monomial adotada e pelo exemplo abaixo veremos que depende também do sistema de coordenadas adotado. Para ficar claro, o sistema de coordenadas é determinado quando especificamos em qual coordenada do vetor formado pelos expoentes ficará o expoente de cada variável. Por exemplo, no caso de três variáveis, quando escrevemos $x < y < z$, significa que o expoente de x ficará na primeira coordenada, o expoente de y ficará na segunda coordenada e o expoente de z na terceira.

Exemplo 2.1. Dado $I =< x^3y^2 + xz + z, x + y + z >$, vamos calcular $\mathrm{in}(I)$ quando $x < y < z$ e $z < y < x$:

```
> ring S = 0, (x,y,z),dp;
> poly f = x^3*y^2+x^3*z^2+z^5;
> poly g = x+y+z;
> ideal I = f,g;
> std(I);
```

Segue que:

- $\mathrm{in}(I) =< y^5, x >$ quando $x < y < z$ e,
- $\mathrm{in}(I) =< y^5, z >$ quando $z < y < x$.

Isso mostra que a escolha do sistema de coordenadas também influencia no resultado do processo de obtenção do ideal inicial.

O nosso objetivo agora será eliminar a dependência da escolha do sistema de coordenadas.

Seja o grupo das matrizes $n \times n$ invertíveis sobre k, $\mathscr{G} := GL(n,k)$. Sejam $g = [g_{ij}] \in \mathscr{G}$ e $p = p(x_1,\ldots,x_n) = \sum_{j=1}^{k} c_j x_1^{a_{j1}} \cdots x_n^{a_{jn}} \in S$ um polinômio. Definimos a aplicação Ψ como

$$\begin{array}{rccl}\Psi: & \mathscr{G}\times S & \to & S\\ & (g,x_j) & \mapsto & g(x_j)=\sum\limits_{i=1}^{n} g_{ij}x_i,\\ & (g,p) & \mapsto & g(p)=p(g(x_1),\ldots,g(x_n)).\end{array}$$

Proposição 2.1. *A aplicação Ψ definida acima é uma ação do grupo $\mathscr{G}$ sobre S.*

Demonstração. Para verificar isso temos que mostrar que $1\cdot p = p$ e $g(h)\cdot p = g(h\cdot p)$ para todo $\forall g,h\in\mathscr{G}$ e $\forall p\in S$.

Observe que cada matriz $g\in\mathscr{G}$ induz um homomorfismo de k-álgebras de S em S:

$$\begin{aligned} g(bp) &= g(b(\sum_{j=1}^{k}[c_jx_1^{a_{j1}}\cdots x_n^{a_{jn}}])) = g(\sum_{j=1}^{k}[bc_jx_1^{a_{j1}}\cdots x_n^{a_{jn}}])\\ &= \sum_{j=1}^{k}[bc_j(g(x_1))^{a_{j1}}\cdots(g(x_n))^{a_{jn}}] = b(\sum_{j=1}^{k}[c_j(g(x_1))^{a_{j1}}\cdots(g(x_n))^{a_{jn}}])\\ &= bg(p),\end{aligned}$$

para todo $b\in k$ e $p\in S$. Com isso temos que verificar apenas se os axiomas de ação de grupos são satisfeitas quando aplicamos nas variáveis.

Segue diretamente da definição de Ψ que é válida a asserção $1\cdot x_i = x_i$. Sejam $g=[g_{ij}]$, $h=[h_{ij}]\in\mathscr{G}$. Considere também o produto $gh=c=[c_{ij}]$, onde $c_{ij}=\sum_{l=1}^{n} g_{il}h_{lj}$. Temos então

$$\begin{aligned}(gh)(x_j) &= \sum_{i=1}^{n} c_{ij}x_i = \sum_{i=1}^{n}(\sum_{l=1}^{n} g_{il}h_{lj})x_i = \sum_{i=1}^{n}\sum_{l=1}^{n} g_{il}h_{lj}x_i = \sum_{l=1}^{n}\sum_{i=1}^{n} g_{il}h_{lj}x_i\\ &= \sum_{l=1}^{n} h_{lj}(\sum_{i=1}^{n} g_{il}x_i) = \sum_{l=1}^{n} h_{lj}(g(x_l)) = g(\sum_{l=1}^{n} h_{lj}x_l) = g(h(x_j)).\end{aligned}$$

$\square$

Seja $g\in\mathscr{G}$. O ideal formado pelos elementos $g(f)$ para todo $f\in I$ será denotado por gI. Se $I=< f_1,\cdots,f_m >$, então $gI=< g(f_1),\cdots,g(f_m) >$, pois g é um isomorfismo e sua ação leva geradores em geradores.

Uma mudança de coordenadas genérica é dada por uma matriz $n\times n$, $h=[h_{ij}]$, cujas entradas h_{ij} são indeterminadas. Quando aplicamos uma mudança de coordenadas, estamos efetivamente mudando o corpo de coeficientes k para $k(h_{11},\ldots,h_{nn})$. Assim, após uma mudança de coordenadas genérica, passamos a ter polinômios em $k(h_{11},\ldots,h_{nn})[x_1,\ldots,x_n]$ e não mais em S.

No Exemplo 2.1, a mudança de coordenadas de $x<y<z$ para $z<y<x$ é realizada pela ação da matriz

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

em $k[x,y,z]$. De fato, temos que $A(x) = z$, $A(y) = y$ e $A(z) = x$, o que mostra o afirmado.

Exemplo 2.2. Sejam $I =< x^2, y^2 >\subset k[x,y]$ e $<$ a ordem lexicográfica. Considere h uma matriz de indeterminadas. Vamos aplicar uma mudança de coordenadas no ideal I:

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Temos que

$$hI =< h(x^2), h(y^2) >=< a^2x^2 + 2acxy + c^2y^2,\ b^2x^2 + 2bdxy + d^2y^2 > . \tag{2.1}$$

Note que $a^2x^2 + 2acxy + c^2y^2,\ b^2x^2 + 2bdxy + d^2y^2 \in k(a,b,c,d)[x,y]$.

A ideia a ser seguida agora é a seguinte: se queremos eliminar a dependência da escolha do sistema de coordenadas, então iremos aplicar uma mudança de coordenadas genérica e, nesse novo ideal, aplicaremos as técnicas vistas no capítulo anterior. Devemos então calcular $\mathrm{in}(hI)$. Ainda, usando a ordem monomial lexicográfica,

```
> ring S = 0,(x,y,a,b,c,d),lp;
> poly f1 = a^2*x^2+2acxy+c^2*y^2;
> poly f2 = b^2*x^2+2bdxy+d^2*y^2;
> ideal hI = f1,f2;
> std(hI);
```

Temos que

$$\mathrm{in}(hI) =< a^2x^2,\ b^2x^2,\ 2ac(ad - bc)xy,\ (ad - bc)^3y^3 > . \tag{2.2}$$

Observe que os coeficientes $a^2,\ b^2,\ 2ac(ad - bc),\ (ad - bc) \in k(a,b,c,d)$, e neste corpo são não nulos, e portanto são inversíveis. Assim, (2.2) pode ser reescrito como

$$\mathrm{in}(hI) =< x^2,\ xy,\ y^3 > .$$

(o que fizemos aqui foi multiplicar cada coeficiente pelo seu inverso multiplicativo e excluir as redundâncias)

Note que o anel original é S, e por isso devemos ter nossa resposta neste anel. Para isso, devemos avaliar quais valores em k as indeterminadas a, b, c e d podem assumir.

Para tal, façamos algumas observações:

i- h deve ser invertível, e daí, $det h = ad - bc \neq 0$;

ii- $a^2, b^2, 2ac$ devem ser não nulos em k, donde $a \neq 0,\ b \neq 0$ e $c \neq 0$.

Com essas observações, temos o seguinte conjunto:

$$U = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} |ad - bc \neq 0,\ a \neq 0,\ b \neq 0 \text{ e } c \neq 0\} \subset \mathrm{GL}(2,k).$$

Esse conjunto é formado pelas matrizes g que satisfazem $\mathrm{in}(gI) = < x^2, xy, y^3 >$. Tal conjunto é um aberto de Zariski em k^4. A saber, esse aberto é o complementar da subvariedade $V((ad - bc)abc)$ em k^4.

O próximo teorema generaliza o que vimos no exemplo acima. Para a demonstração do mesmo serão necessários alguns resultados sobre potência exterior de espaços vetoriais $\bigwedge^t V$, os quais são apresentados no Anexo A.

Teorema 6. *Seja $I \subset S$ um ideal homogêneo. Existe um aberto não vazio de Zariski, $U \subset \mathscr{G}$, e um ideal J, tal que $J = in(gI)$ para todo $g \in U$.*

E mais, para cada $d \geq 0$, se J_d tem dimensão t, então $\bigwedge^t J_d$ é gerado pelo maior monômio de $\bigwedge^t S_d$ que aparece em qualquer elemento $f \in \bigwedge^t gI_d$ com $g \in \mathscr{G}$.

Demonstração. Primeiro, observe que podemos escrever $I = \oplus_{d \geq 1} I_d$, onde cada I_d é o espaço vetorial de todos os elementos de I de grau d. Observe que o I_d é um subespaço de S_d, e como esse último tem dimensão finita sobre k, temos que $\dim_k I_d$ é finito. Sejam $f_1, \ldots, f_t$ uma base para I_d.

Com esse conjunto de geradores, obtemos o gerador $f_1 \wedge \ldots \wedge f_t$ do espaço unidimensional $\bigwedge^t I_d \subset \bigwedge^t S_d$.

Agora façamos uma mudança de coordenadas genérica no gerador de $\bigwedge^t I_d$. Seja $h = (h_{ij})$ uma matriz de indeterminadas h_{ij}. Segue que

$$\wedge^t h(f_1 \wedge \ldots \wedge f_t) = h(f_1) \wedge \ldots \wedge h(f_t).$$

Esta última expressão pode ser desenvolvida para uma combinação linear de monômios de $\bigwedge^t S_d$ cujos coeficientes são polinômios nas indeterminadas h_{ij}, isto é,

$$\wedge^t h(f_1 \wedge \ldots \wedge f_t) = h(f_1) \wedge \ldots \wedge h(f_t) = \sum_i p_{di}(h_{11}, \cdots, h_{tt})\, n_{i,1} \wedge \ldots \wedge n_{i,t}. \tag{2.3}$$

E por padronização de notação, podemos supor que $n_{i,1} \wedge \ldots \wedge n_{i,t} < n_{j,1} \wedge \ldots \wedge n_{j,t}$ para $i < j$. Colocando os termos de (2.3) na forma normal, renomeando o primeiro termo que aparece $n_{i,1} \wedge \ldots \wedge n_{i,t}$ cujo coeficiente é não nulo (monômio líder) por $n_d = n_{d,1} \wedge \ldots \wedge n_{d,t}$ e seja $p_d(h_{11}, \ldots, h_{rr}) \neq 0$ o seu coeficiente.

Definiremos U_d como o conjunto das $g = [g_{ij}] \in \mathcal{G}$ tais que $p_d(g_{11}, \ldots, g_{rr}) \neq 0$. O conjunto U_d assim definido é um aberto não vazio (o conjunto de zeros de um polinômio é um fechado de Zariski, e como U_d é o complementar do conjunto de zeros de p_d, é consequentemente um aberto).

Definiremos J_d como sendo o subespaço de S_d gerado por $n_{d,1}, \ldots, n_{d,t}$. Observe que a parte de grau d do ideal inicial de gI, $\text{in}(gI)$, será $\left(n_{d,1}, \ldots, n_{d,t}\right)$ se, e somente se, $g \in U_d$.

Com isso, temos que para cada d vale

$$J_d = \text{in}(gI). \tag{2.4}$$

Seja

$$J := \oplus J_d. \tag{2.5}$$

O conjunto J acima definido é um ideal. Para verificar tal afirmação é suficiente mostrar que para cada d vale

$$S_1 J_d \subset J_{d+1}. \tag{2.6}$$

Como U_d e U_{d+1} são abertos densos, segue da Proposição 1.3 que existe um elemento $g \in U_d \cap U_{d+1}$. Como vimos acima, temos que $\text{in}(gI)_d = J_d$ e $\text{in}(gI)_{d+1} = J_{d+1}$ (para a mesma matriz g), de onde segue (2.6).

Seja

$$U = \bigcap_{d=1}^{\infty} U_d. \tag{2.7}$$

Mostraremos que U definido em (2.7) é um aberto denso de Zariski em $\mathcal{G}$. Desde que cada U_d é um aberto denso de Zariski, é suficiente mostrar que U é igual a uma interseção finita de U_d. Para verificar isso, suponha que J é gerado por elementos de grau $\leq e$; mostraremos que

$$U = \bigcap_{d=1}^{e} U_d. \tag{2.8}$$

A inclusão $U \subset \bigcap_{d=1}^{e} U_d$ é óbvia.

Para mostrar a outra inclusão, seja $g \in \bigcap_{d=1}^{e} U_d$. Mostramos que $\text{in}(gI)_d = J_d, \forall d \leqslant e$. Logo $\text{in}(gI) \supseteq J$, pois até o grau e já varremos todos os geradores de J.

Desde que $\dim_k J_d = \dim_k I_d = \dim_k (gI)_d$, para todo d, nós vemos que $\text{in}(gI) = J$, ou seja, $g \in U$, como queríamos provar.

A última afirmação do teorema segue dos seguintes fatos: J_d tem dimensão t e tem como conjunto de geradores $n_{d,1}, \ldots, n_{d,t}$. Assim, $n_d = n_{d,1} \wedge \ldots \wedge n_{d,t}$ é um gerador para $\bigwedge^t J_d = \bigwedge^t \text{in}(I_d)$. Por definição de $\bigwedge^t \text{in}(I_d)$, como $n_d \in \bigwedge^t \text{in}(I_d)$, então existe $f \in \bigwedge^t I_d$ tal que $\text{in}(f) = n_d$. Como n_d é o maior monômio de f, temos que não pode existir $g \in \bigwedge^t I_d$ tal que $g > f$, pois caso contrário teríamos $\text{in}(g) > \text{in}(f) = n_d$, contrariando a hipótese de que n_d é o maior monômio que aparece em $\bigwedge^t \text{in}(I_d) = \bigwedge^t J_d$. □

Sejam $I \subset S$ um ideal e $g, g' \in \mathscr{G}(n,k)$ duas matrizes. Dizemos que

$$g \sim g' \text{ se } \text{in}(gI) = \text{in}(g'I).$$

É de imediata verificação que a relação " $\sim$ " é uma relação de equivalência.

Cada classe de equivalência induzida pela relação " $\sim$ " é determinada para cada possibilidade de $\text{in}(gI)$. O número dessas classes de equivalência é finito (veja [10, p. 25]). Quando calculamos o conjunto de geradores do ideal inicial de hI, onde $h = [h_{ij}]$ é uma matriz de indeterminadas, vericamos que seus geradores são polinômios nas variáveis originais com coeficientes em $k(h_{11}, \ldots, h_{nn})$. Assim, cada classe de equivalência é determinada determinando quais desses coeficientes é ou não zero.

Quando impomos que todos os coeficientes dos geradores de $\text{in}(hI)$ sejam diferentes de zero, a classe de equivalência associada é a única que também é um aberto de Zariski de $\mathscr{G}(n,k)$ (ou k^{n^2}). Esse aberto é exatamente o aberto enunciado no teorema 6. Com isso, temos a seguinte definição:

Definição 2.1. *O ideal J obtido no Teorema 6 é o* ***ideal inicial genérico*** *de I, e o denotamos por $J = Gin(I)$.*

Exemplo 2.3. Dado $I = < x^2, xy, xz + z^2 > \subset S$ um ideal homogêneo, vamos calcular $\text{Gin}(I)$ usando a ordem monomial lexicográfica graduada reversa. O primeiro passo é aplicar em I uma mudança de coordenadas. Seja h a seguinte matriz mudança de coordenadas:

$$h = \begin{pmatrix} h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 \\ h_7 & h_8 & h_9 \end{pmatrix},$$

onde $h(x) = h_1 x + h_4 y + h_7 z$, $h(y) = h_2 x + h_5 y + h_8 z$ e $h(z) = h_3 x + h_6 y + h_9 z$.

Assim, o ideal

$$\begin{aligned} hI &= < (h_1x+h_4y+h_7z)^2,\ (h_1x+h_4y+h_7z)(h_2x+h_5y+h_8z), \\ &\quad (h_1x+h_4y+h_7z)(h_3x+h_6y+h_9z)+(h_3x+h_6y+h_9z)^2 > . \end{aligned}$$

Agora vamos calcular in(hI):

```
> ring S = 0, (x,y,z,h(1..9)),dp;
> poly hx = h(1)*x+h(4)*y+h(7)*z;
> poly hy = h(2)*x+h(5)*y+h(8)*z;
> poly hz = h(3)*x+h(6)*y+h(9)*z;
> ideal hI = hx^2,hx*hy, hx*hz+hz^2;
> std(hI);
```

Obtemos

$$\begin{aligned} \text{in}(hI) &= < h_1h_3x^2,\ h_1h_2x^2,\ h_1^2x^2,\ h_1h_2h_4xy,\ h_3^3x^2,\ h_2h_3^2x^2,\ h_2h_3^2h_4xy,\ h_1^2h_3h_4xy, \\ &\quad h_1h_3h_4h_5xy^2,\ h_2h_3^2h_4^2y^2,\ h_1h_3h_4^2xy^2,\ h_1h_3h_4h_5h_7xyz,\ h_1h_3^2h_5^2xy^2,\ h_3^3h_4h_5xy^2, \\ &\quad h_3^3h_4^2xy^2,\ h_1h_3^2h_5^2h_7xyz,\ h_3^3h_4h_5h_7xyz,\ h_3^3h_4^2h_5y^3,\ h_3^3h_4^3y^3,\ h_1h_3^2h_5^2h_7^2xz^2, \\ &\quad h_3^3h_4^2h_5h_7y^2z > . \end{aligned}$$

Observe que os geradores de hI pertencem a $k(h_1,\ldots,h_9)[x,y,z]$. Neste caso, para determinar quais são as classes de equivalência induzidas pelo ideal I são obtidas estudando todas as combinações possíveis impondo quais dos coeficientes (pertencentes a $k(h_1,\ldots,h_9)$) são zeros ou não. Como nosso objetivo é obter o ideal inicial genérico, devemos impor que todos são diferentes de zero. Como os coeficientes estão em um corpo, podemos reescrever o conjunto de geradores como

$$\text{in}(hI) = < x^2,\ xy,\ y^2,\ xz^2 > .$$

Agora, para voltar com esse resultado para S, devemos impor algumas condições para quais valores as indeterminadas h_i podem assumir. Observemos:

- Como o único elemento em que aparece o monômio y^2z é $h_3^3h_4^2h_5h_7y^2z$, então a escolha dos valores de $h_3,\ h_4,\ h_5,\ h_7$ devem ser feitas de modo que $h_3^3h_4^2h_5h_7$ seja não nulo em k. Daí, $h_3 \neq 0,\ h_4 \neq 0,\ h_5 \neq 0$ e $h_7 \neq 0$.

- O mesmo raciocínio pode ser aplicado ao monômio y^2. Concluiremos também que $h_2 \neq 0$.

- Depois, analisando o coeficiente do monômio xz^2, obteremos que $h_1 \neq 0$.

Assim,

$$\text{in}(hI) = < x^2,\ xy,\ y^2,\ xz^2 > = \text{Gin}(I).$$

Neste exemplo, o aberto U é:

$$U = \left\{ \begin{pmatrix} h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 \\ h_7 & h_8 & h_9 \end{pmatrix} |\det[h_{ij}] \neq 0,\ h_1 \neq 0,\ h_2 \neq 0,\ h_3 \neq 0,\ h_4 \neq 0,\ h_5 \neq 0 \text{ e } h_7 \neq 0 \right\}.$$

Vimos no capítulo anterior que a dimensão de $V(I)$ é igual a dimensão de $V(\text{in}(I))$, e esse fato nos leva a concluir que se U é o aberto obtido no teorema 6, então

$$\dim V(I) = \dim V(\text{Gin}(I)) = \dim V(\text{in}(gI)) \ \forall g \in U.$$

Isso mostra que a classe de equivalência (induzida pela relação $\sim$ acima descrita) do ideal inicial genérico $\text{Gin}(I)$ tem a dimensão das subvariedades associadas aos elementos dessa classe como um invariante.

2.1 Ideal Borel-fixo

Iremos agora apresentar uma condição necessária (mas não suficiente - Exemplo 2.6) para que um ideal monomial seja um ideal inicial genérico.

Definição 2.2. *O subgrupo B de $\mathscr{G}$ constituído pelas matrizes triangulares superiores invertíveis é chamado de* ***subgrupo de Borel****.*

Seja $\gamma_{ij}^{a_{ij}} = [\gamma_{kl}], i \neq j$ uma matriz elementar $n \times n$ definida por

$$\gamma_{kl} = \begin{cases} 1, & \text{se } k = l; \\ a_{ij}, & \text{se } (i,j) = (k,l); \\ 0, & \text{nos demais casos,} \end{cases}$$

e seja $\gamma_{ii}^{a_{ii}} = [\gamma_{kl}]$ uma matriz elementar $n \times n$ definida por

$$\gamma_{kl} = \begin{cases} 1, & \text{se } k = l \text{ e } (k,l) \neq (i,i); \\ a_{ii}, & \text{se } (k,l) = (i,i); \\ 0, & \text{nos demais casos.} \end{cases}$$

Vamos nos restringir apenas às matrizes $\gamma_{ij}^{a_{ij}}$ que pertençam a B, e para isso basta impor $i \leqslant j$. E mais (como $\gamma_{ij}^{a_{ij}}$ são invertíveis):

(i)- se $i = j \Rightarrow (\gamma_{ii}^{a_{ii}})^{-1} = \gamma_{ii}^{(a_{ii})^{-1}} \in B$, e

(ii)- se $i < j \Rightarrow (\gamma_{ij}^{a_{ij}})^{-1} = \gamma_{ij}^{-a_{ij}} \in B$.

Proposição 2.2. *O subgrupo de Borel é gerado pelo conjunto* $\mathscr{B} = \{\gamma_{ij}^a | i < j\}$..

Demonstração. Ao multiplicar a matriz g pela matriz elementar γ_{ii}^a (pela direita), o resultado final será uma operação sobre a i-ésima coluna multiplicando-a por a. Assim, se g_{ii} é a i-ésima entrada da diagonal da matriz g, então o produto pela matriz $\gamma_{ii}^{(g_{ii})^{-1}}$ altera apenas a i-ésima coluna de g sendo que o i-ésimo termo da diagonal passa a ser 1, e os elementos logo acima dessa posição passam a ser $(g_{ii})^{-1}g_{ki}$ (os que estavam abaixo continuam sendo 0).

Logo, temos

$$g' = g(\prod_{i=1}^{n} \gamma_{ii}^{(g_{ii})^{-1}}),$$

onde $g'_{ii} = 1$ e $g'_{ij} = (g_{jj})^{-1}g_{ij}$ para $i < j$.

Ao multiplicar a matriz g pela matriz elementar γ_{ij}^a (pela direita) com $i < j$, o resultado final será uma operação sobre a j-ésima coluna trocando-a pela soma da j-ésima coluna com a vezes a i-ésima coluna. Assim, g_{ij} é a (i, j)-ésima entrada da matriz g, então o produto pela matriz $\gamma_{ij}^{-g_{ij}}$(pela direita) irá zerar a entrada (i, j) da matriz g.

Fixando j, se multiplicarmos a matriz g' pelas matrizes $\gamma_{ij}^{-g_{ij}}$ (observando que a cada produto os outros termos não nulos da coluna se alteram, e logo para o próximo produto, deve-se tomar $-g_{ij}$ na nova matriz), teremos como resultado a matriz g' com a j-ésima coluna zerada, a menos da entrada da diagonal principal, que é igual a 1.

Fazendo isso para todos os j possíveis, teremos

$$\mathrm{Id} = g(\prod_{i=1}^{n} \gamma_{ii}^{(g_{ii})^{-1}}) \prod_{l=1}^{k} \gamma_{ij}^{d_l}, \tag{2.9}$$

onde d_l são as entradas selecionadas a cada produto, e k é o número de operações necessárias para zerar todas as entradas acima da diagonal principal. Isso é sempre possível, pois todos os elementos de $\mathscr{B}$ possuem os elementos da diagonal principal não nulos.

Podemos reescrever (2.9) como

$$g = \prod_{l=k}^{1} (\gamma_{ij}^{d_l})^{-1} (\prod_{i=n}^{1} (\gamma_{ii}^{(g_{ii})^{-1}})^{-1}) = \prod_{l=k}^{1} (\gamma_{ij}^{-d_l}) \prod_{i=n}^{1} (\gamma_{ii}^{g_{ii}}).$$

Com isso temos uma decomposição para g em matrizes do tipo $\gamma_{ij}^{g_{ij}}$ com $i \leqslant j$, o que conclui a demonstração. $\square$

Exemplo 2.4. Seja $g \in B \subset \mathrm{GL}(k, 3)$. Temos então que

$$g = \begin{pmatrix} g_{11} & g_{12} & g_{13} \\ 0 & g_{22} & g_{23} \\ 0 & 0 & g_{33} \end{pmatrix}.$$

Utilizando as matrizes elementares acima definidas, temos:

$$\mathrm{Id} = g \cdot \gamma_{11}^{g_{11}^{-1}} \gamma_{22}^{g_{22}^{-1}} \gamma_{33}^{g_{33}^{-1}} \gamma_{23}^{-g_{23}g_{33}^{-1}} \gamma_{13}^{(g_{12}g_{23}g_{22}^{-1}-g_{13})g_{33}^{-1}} \gamma_{12}^{-g_{12}g_{22}^{-1}}.$$

Dessa igualdade, podemos escrever

$$\begin{aligned} g &= (\gamma_{11}^{g_{11}^{-1}} \gamma_{22}^{g_{22}^{-1}} \gamma_{33}^{g_{33}^{-1}} \gamma_{23}^{-g_{23}g_{33}^{-1}} \gamma_{13}^{(g_{12}g_{23}g_{22}^{-1}-g_{13})g_{33}^{-1}} \gamma_{12}^{-g_{12}g_{22}^{-1}})^{-1} \\ &= (\gamma_{12}^{-g_{12}g_{22}^{-1}})^{-1} (\gamma_{13}^{(g_{12}g_{23}g_{22}^{-1}-g_{13})g_{33}^{-1}})^{-1} (\gamma_{23}^{-g_{23}g_{33}^{-1}})^{-1} (\gamma_{33}^{g_{33}^{-1}})^{-1} (\gamma_{22}^{g_{22}^{-1}})^{-1} (\gamma_{11}^{g_{11}^{-1}})^{-1} \\ &= \gamma_{12}^{g_{12}g_{22}^{-1}} \gamma_{13}^{(g_{13}-g_{12}g_{23}g_{22}^{-1})g_{33}^{-1}} \gamma_{23}^{g_{23}g_{33}^{-1}} \gamma_{33}^{g_{33}} \gamma_{22}^{g_{22}} \gamma_{11}^{g_{11}}. \end{aligned}$$

explicitando (no caso 3×3) a decomposição de $g \in B$ em um produto de elementos de $\mathscr{B}$.

Definição 2.3. *Sejam $n_1, \ldots, n_t$ monômios de S.*

1. *Para cada termo $n = an_1 \wedge \ldots \wedge n_t$, definimos o* **peso** *de n como sendo o monômio $w = \prod_i n_i \in S$;*

2. *Definimos $f_w \in \bigwedge^t S_d$ como a soma de todos os termos de f tendo peso w, de modo que temos $f = \sum_w f_w$.*

Exemplo 2.5. Sejam $f_1 = xy + xz + yz$ e $f_2 = x + y + z$. Assim,

$$\begin{aligned} f &= f_1 \wedge f_2 \\ &= (xy + xz + yz) \wedge (x + y + z) \\ &= xy \wedge x + xy \wedge y + xy \wedge z + xz \wedge x + xz \wedge y + xz \wedge z + yz \wedge x + yz \wedge y + yz \wedge z \\ &= n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 + n_9 \end{aligned}$$

onde $n_1 = xy \wedge x,\ n_2 = xy \wedge y,\ n_3 = xy \wedge z,\ n_4 = xz \wedge x,\ n_5 = xz \wedge y,\ n_6 = xz \wedge z,\ n_7 = yz \wedge x,\ n_8 = yz \wedge y$ e $n_9 = yz \wedge z$.

Portanto o peso de n_1, denotado por w_{n_1} é $w_{n_1} = xy \cdot x = x^2y$. Analogamente $w_{n_2} = xy^2$, $w_{n_3} = xyz$, $w_{n_4} = x^2z$, $w_{n_5} = xyz$, $w_{n_6} = xz^2$, $w_{n_7} = xyz$, $w_{n_8} = y^2z$ e $w_{n_9} = yz^2$.

Ainda, temos que $f_{x^2y} = w_{n_1}$, $f_{xy^2} = w_{n_2}$, $f_{x^2z} = w_{n_4}$, $f_{xyz} = w_{n_5} + w_{n_7}$, $f_{xz^2} = w_{n_6}$, $f_{y^2z} = w_{n_8}$ e $f_{yz^2} = w_{n_9}$.

Seguindo ainda a ideia da definição acima, seja w_0 o peso de $\mathrm{in}(f)$. Temos que diferentes termos de f podem possuir o mesmo peso w, mas $\mathrm{in}(f)$ é o único termo tendo peso w_0, pois w_0 é o produto dos maiores monômios envolvidos.

O próximo resultado mostra que ideais iniciais genéricos são especiais entre os ideais monomiais.

Definição 2.4. *Seja $I \subset S$ um ideal homogêneo. Dizemos que I é um ideal **Borel-fixo** se para todo $g \in B$, tivermos*

$$gI = I.$$

Teorema 7 (Galligo, Bayer e Stillman)**.** *Se $I \subset S$ é um ideal homogêneo então $Gin(I)$ é Borel-fixo.*

Demonstração. Substituindo I por gI para g genérico, assumiremos pelo Teorema 6 que $\mathrm{in}(I) = \mathrm{Gin}(I)$.

Como vimos na Proposição 2.2, o conjunto $\mathscr{B}$ gera o subgrupo de Borel. Portanto, basta provar o teorema para os elementos de $\mathscr{B}$.

Desde que matrizes diagonais estabilizam qualquer ideal monomial, basta mostrar o teorema para as matrizes γ_{ij}^{a}, com $i < j$.

Podemos escrever

$$\gamma_{ij}^{a} = Id_{n\times n} + \alpha_{ij}^{a}, i < j,$$

onde α_{ij}^{a} é uma matriz $n \times n$ tal que a entrada (i, j) é a e as demais são nulas (por simplicidade, sempre que nos referirmos a uma matriz identidade, $\mathrm{Id}_{n\times n}$, a denotaremos por 1 quando não houver risco de confusão com o cardinal 1).

Temos então que verificar para cada grau d que

$$\gamma_{ij}^{a}(\mathrm{in}(I_d)) = (1 + \alpha_{ij}^{a})(\mathrm{in}(I_d)) = \mathrm{in}(I_d)$$

(afim de simplificar a notação, consideraremos abaixo que $\alpha = \alpha_{ij}^{a}$ para algum par arbitrário (i, j) com $i < j$).

Seja $\{f_1, \dots, f_t\}$ uma base para I_d com $\mathrm{in}(f_1) > \cdots > \mathrm{in}(f_t)$. Seja

$$f = f_1 \wedge \ldots \wedge f_t$$

o correspondente gerador do subespaço unidimensional $\bigwedge^t I_d \subset \bigwedge^t S_d$. Temos que $\mathrm{in}(f) = \mathrm{in}(f_1) \wedge \ldots \wedge \mathrm{in}(f_t)$.

Se $(1 + \alpha)(\mathrm{in}(I_d)) \neq \mathrm{in}(I_d)$, então $(1 + \alpha)(\mathrm{in}(f)) \neq \mathrm{in}(f)$. De fato, como α é uma matriz triangular superior, os termos de $(1 + \alpha)(\mathrm{in}(f))$ que não figuram em $\mathrm{in}(f)$ são todos estritamente maiores que $\mathrm{in}(f)$. Seja am um desses termos, onde a é um escalar não nulo e

m é um monômio de $\bigwedge^t S_d$. Vamos mostrar abaixo que, para uma matriz diagonal adequada δ, o monômio m aparece com coeficientes não nulos em $(1+\alpha)\delta f$. Isto contradiz a última afirmação do Teorema 6, o que prova que $(1+\alpha)(\text{in}(I_d)) = \text{in}(I_d)$.

Seja f como citado acima. Pela definição 2.3, podemos escrever:

$$f = \sum_w f_w.$$

Mais ainda, temos que cada f_w pode ser escrito como a seguinte soma:

$$f_w = \sum_{i=1}^{k_w} b_{w,i} n_{w,i},$$

onde $b_{w,i} \in k$ e cada $n_{w,i} \in \bigwedge^t S_d$ é um monômio de f cujo peso é w, e portanto pode ser escrito como

$$n_{w,i} = \prod_{j=1}^{n} x_j^{a_{w,i,1,j}} \wedge \ldots \wedge \prod_{j=1}^{n} x_j^{a_{w,i,t,j}}.$$

E daí temos:

$$f = \sum_w \sum_{i=1}^{k_w} b_{w,i} (\prod_{j=1}^{n} x_j^{a_{w,i,1,j}} \wedge \ldots \wedge \prod_{j=1}^{n} x_j^{a_{w,i,t,j}}).$$

Se δ é uma matriz diagonal então $\delta(x_i) = d_i x_i$ com $d_i \in k^*$, então

$$\begin{aligned}
\delta(f) &= \delta(\textstyle\sum_w \sum_{i=1}^{k_w} b_{w,i}(\prod_{j=1}^{n} x_j^{a_{w,i,1,j}} \wedge \ldots \wedge \prod_{j=1}^{n} x_j^{a_{w,i,t,j}})) \\
&= \sum_w \delta(\sum_{i=1}^{k_w} b_{w,i}(\prod_{j=1}^{n} x_j^{a_{w,i,1,j}} \wedge \ldots \wedge \prod_{j=1}^{n} x_j^{a_{w,i,t,j}})) \\
&= \sum_w \sum_{i=1}^{k_w} b_{w,i} \delta((\prod_{j=1}^{n} x_j^{a_{w,i,1,j}} \wedge \ldots \wedge \prod_{j=1}^{n} x_j^{a_{w,i,t,j}})) \\
&= \sum_w \sum_{i=1}^{k_w} b_{w,i}[\delta(\prod_{j=1}^{n} x_j^{a_{w,i,1,j}}) \wedge \ldots \wedge \delta(\prod_{j=1}^{n} x_j^{a_{w,i,t,j}})] \\
&= \sum_w \sum_{i=1}^{k_w} b_{w,i}[\prod_{j=1}^{n} (d_j x_j)^{a_{w,i,1,j}} \wedge \ldots \wedge \prod_{j=1}^{n} (d_j x_j)^{a_{w,i,t,j}}] \\
&= \sum_w \sum_{i=1}^{k_w} b_{w,i}[\prod_{j=1}^{n} (d_j^{a_{w,i,1,j}} x_j^{a_{w,i,1,j}}) \wedge \ldots \wedge \prod_{j=1}^{n} (d_j^{w,i,t,j} x_j^{a_{w,i,t,j}})] \\
&= \sum_w \sum_{i=1}^{k_w} b_{w,i}(\prod_{j=1}^{n} d_j^{a_{w,i,1,j}} \cdots \prod_{j=1}^{n} d_j^{a_{w,i,t,j}})[\prod_{j=1}^{n} x_j^{a_{w,i,1,j}} \wedge \ldots \wedge \prod_{j=1}^{n} x_j^{a_{w,i,t,j}}] \\
&= \sum_w \sum_{i=1}^{k_w} b_{w,i}(\prod_{l=1}^{t} \prod_{j=1}^{n} d_j^{a_{w,i,l,j}}) n_{w,i}
\end{aligned}$$

$$\delta(f) = \sum_w \sum_{i=1}^{k_w} (\prod_{l=1}^{t} \prod_{j=1}^{n} d_j^{a_{w,i,l,j}}) b_{w,i} n_{w,i}.$$

Observe que a expressão $(\prod_{l=1}^{t} \prod_{j=1}^{n} d_j^{a_{w,i,l,j}})$ é exatamente o monômio w com d_j no lugar de x_j. Com isso, denotando

$$w(d_1,\dots,d_n) = (\prod_{l=1}^{t} \prod_{j=1}^{n} d_j^{a_{w,i,l,j}}),$$

temos:

$$\begin{aligned}
\delta(f) &= \sum_w \sum_{i=1}^{k_w} w(d_1,\dots,d_n) b_{w,i} n_{w,i} \\
&= \sum_w w(d_1,\dots,d_n) \sum_{i=1}^{k_w} b_{w,i} n_{w,i} \\
&= \textstyle\sum_w w(d_1,\dots,d_n) f_w.
\end{aligned}$$

Assim,

$$\begin{aligned}
(1+\alpha)\delta f &= \sum_w (1+\alpha)(w(d_1,\dots,d_n) f_w) = \sum_w w(d_1,\dots,d_n)(1+\alpha) f_w \\
&= w_0(d_1,\dots,d_n)(1+\alpha) f_{w_0} + \sum_{w \neq w_0} w(d_1,\dots,d_n)(1+\alpha) f_w \\
&= w_0(d_1,\dots,d_n)(1+\alpha)\mathrm{in}(f) + \sum_{w \neq w_0} w(d_1,\dots,d_n)(1+\alpha) f_w.
\end{aligned}$$

Assim, o coeficiente de m em $(1+\alpha)\delta f$ tem a forma

$$c(d_1,\dots,d_n) := b_{w_0} w_0(d_1,\dots,d_n) + \sum_{w \neq w_0} b_w w(d_1,\dots,d_n),$$

onde os $b_w \in k$ são os coeficientes de m em $(1+\alpha)f_w$. Como o termo $b_{w_0} w_0(d_1,\dots,d_n)$ é não nulo, vemos que o polinômio c também é não nulo. Desde que assumimos que o corpo k é infinito, segue-se que para valores suficientemente gerais de $d_1,\dots,d_n$, o valor $c(d_1,\dots,d_n)$ não é zero, concluindo assim a demonstração do teorema. □

Exemplo 2.6. Seja $I = < x^2, xy, xz + z^2 >$.

```
> ring S = 0,(x,y,z),dp;
> poly f1 = x^2;
> poly f2 = xy;
> poly f3 = xz+z^2;
> ideal I = f1,f2,f3;
> std(I);
```

Temos que

$$\mathrm{in}(I) = < xz, xy, x^2, z^3, yz^2 > .$$

Vamos verificar que $\text{in}(I)$ é Borel-fixo. De fato, seja $g = [g_{ij}] \in B$. Assim, g tem o seguinte aspecto (no caso 3×3):

$$g = \begin{pmatrix} g_{11} & g_{12} & g_{13} \\ 0 & g_{22} & g_{23} \\ 0 & 0 & g_{33} \end{pmatrix}.$$

Observe que g é invertível, e portanto $g_{11} \neq 0$, $g_{22} \neq 0$ e $g_{33} \neq 0$.

Temos neste caso a seguinte ação de g sobre os geradores de $\text{in}(I)$:

$$\begin{array}{rcl}
x & \mapsto & g(x) = g_{11}x \\
y & \mapsto & g(y) = g_{12}x + g_{22}y \\
z & \mapsto & g(z) = g_{13}x + g_{23}y + g_{33}z \\
xz & \mapsto & g(xz) = (g_{11}x)(g_{13}x + g_{23}y + g_{33}z) = g_{11}g_{13}x^2 + g_{11}g_{23}xy + g_{11}g_{33}xz \\
xy & \mapsto & g(xy) = (g_{11}x)(g_{12}x + g_{22}y) = g_{11}g_{12}x^2 + g_{11}g_{22}xy \\
x^2 & \mapsto & g(x^2) = (g_{11}x)^2 = g_{11}^2x^2 \\
z^3 & \mapsto & g(z^3) = (g_{13}x + g_{23}y + g_{33}z)^3 \\
yz^2 & \mapsto & g(yz^2) = (g_{12}x + g_{22}y)(g_{13}x + g_{23}y + g_{33}z)^2
\end{array}$$

donde vemos que os geradores de gI, $g(xz)$, $g(xy)$, $g(x^2)$, $g(z^3)$, $g(yz^2) \in \text{in}(I)$. Logo $g(\text{in}(I)) \subset \text{in}(I)$. Por outro lado, é fácil verificar que xz, xy, x^2, z^3, $yz^2 \in g(\text{in}(I))$, e consequentemente $\text{in}(I) \subset g(\text{in}(I))$. Portanto, $\text{in}(I)$ é um ideal Borel-fixo.

Completando o exemplo, observe que pelo exemplo 2.3 mostramos que

$$\text{Gin}(I) = < x^2, xy, y^2, xz^2 > .$$

Esse fato mostra que a recíproca do Teorema 7 não é válida, ou seja, nem todo ideal Borel-fixo é um ideal inicial genérico.

ANEXO A – Potências Exteriores

Neste anexo apresentaremos todos os resultados relacionados a álgebra multilinear que são necessários para o desenvolvimento desta dissertação. Iniciemos com algumas definições preliminares:

Definição A.1. *Sejam V, $V_1, \ldots,$ V_t e E espaços vetoriais.*

(a) A aplicação

$f : V_1 \times \cdots \times V_t \to E$

é dita ***t-linear*** *(ou* ***multilinear****) se f é linear em cada componente, ou seja, se para cada $i = 1, \ldots,$ t com $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_t$ fixados, temos que a aplicação*

$$\begin{array}{rcl} V_i & \to & E \\ x & \mapsto & f(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_t), \end{array}$$

é linear.

(b) Uma aplicação t-linear $f : V^t \to E$ é dita ***alternada*** *se $f(v_1, \ldots, v_t) = 0$ sempre que existir um índice $1 \leqslant i \leqslant t-1$ tal que $v_i = v_{i+1}$.*

Exemplo A.1. Seja $f : V^t \to E$ uma aplicação t-linear alternada. Temos

$$\begin{array}{rcl} 0 & = & f(v_1, \ldots, v_{i-1}, v+w, v+w, v_{i+2}, \ldots, v_t) \\ & = & f(v_1, \ldots, v_{i-1}, v, v, v_{i+2}, \ldots, v_t) + f(v_1, \ldots, v_{i-1}, v, w, v_{i+2}, \ldots, v_t) \\ & + & f(v_1, \ldots, v_{i-1}, w, v, v_{i+2}, \ldots, v_t) + f(v_1, \ldots, v_{i-1}, w, w, v_{i+2}, \ldots, v_t) \\ & = & f(v_1, \ldots, v_{i-1}, v, w, v_{i+2}, \ldots, v_t) + f(v_1, \ldots, v_{i-1}, w, v, v_{i+2}, \ldots, v_t), \end{array}$$

isso mostra que

$$f(v_1, \ldots, v_{i-1}, v, w, v_{i+2}, \ldots, v_t) = -f(v_1, \ldots, v_{i-1}, w, v, v_{i+2}, \ldots, v_t).$$

Ou seja, ao permutarmos duas componentes adjacentes, a imagem de $(v_1, \ldots, v_t)$ pela aplicação f sofre apenas uma mudança de sinal.

Em geral, dada f uma aplicação t-linear alternada se σ é uma permutação do conjunto $\{1,\ldots,t\}$ e $\varepsilon(\sigma)$[1] o sinal de σ, temos

$$f(v_{\sigma(1)},\ldots,v_{\sigma(t)}) = \varepsilon(\sigma)f(v_1,\ldots,v_t).$$

Vamos agora abordar as principais definições desta seção: Produto Tensorial e Potência Exterior de espaços vetoriais. Daremos aqui uma definição de produto tensorial no contexto de módulos sobre um anel R, e depois nos restringiremos ao caso particular em que o anel R é um corpo, e nesse caso todo R-módulo é um espaço vetorial sobre R.

Sejam M e N módulos sobre o anel comutativo com unidade R. O quociente do $\mathbb{Z}$-módulo livre sobre $M\times N$, $\bigoplus_{(m,n)\in M\times N} R^{M\times N}$, pelo subgrupo gerado pelos elementos da forma

$$\begin{gathered}(m_1+m_2,n)-(m_1,n)-(m_2,n),\\ (m,n_1+n_2)-(m,n_1)-(m,n_2),\\ (rm,n)-(m,rn),\end{gathered}$$

onde $m,m_1,m_2\in M$, $n,n_1,n_2\in N$ e $r\in R$ é um grupo abeliano chamado de **produto tensorial** entre M e N sobre R, denotado por $M\bigotimes_R N$.

Por definição de quociente, os elementos de $M\bigotimes_R N$ satisfazem as relações:

$$\begin{gathered}(m_1+m_2)\otimes n = m_1\otimes n+m_2\otimes n,\\ m\otimes(n_1+n_2) = m\otimes n_1+m\otimes n_2,\\ (rm)\otimes n = m\otimes(rn) = r(m\otimes n),\end{gathered}$$

onde $m,m_1,m_2\in M$, $n,n_1,n_2\in N$ e $r\in R$.

No caso em que $R=k$ é um corpo, M e N são espaços vetoriais sobre k e usaremos a notação $M\bigotimes N$ ao invés de $M\bigotimes_k N$.

Observe que $M\bigotimes N$ é um espaço vetorial sobre k e seus elementos são iguais a somas finitas de parcelas do tipo $m\otimes n$, para $m\in M$ e $n\in N$.

Estabelecida a definição de produto tensorial, podemos considerar a aplicação

$$\begin{array}{rccc} i: & M\times N & \to & M\bigotimes N\\ & (m,n) & \mapsto & m\otimes n.\end{array}$$

Note que, se $m_1,m_2\in M$ e $n\in N$, temos

$$i(m_1+m_2,n) = (m_1+m_2)\otimes n = m_1\otimes n+m_2\otimes n = i(m_1,n)+i(m_2,n)$$

[1]Para mais detalhes sobre sinal de permutações veja seção 3.5 de [4]

Isso mostra que i é linear na primeira coordenada. Analogamente, mostra-se que é linear na segunda coordenada. Logo i é 2-linear (também usamos dizer bilinear). Essa aplicação i é especial, como evidencia a seguinte proposição:

Proposição A.1. *Sejam V_1 e V_2 espaços vetoriais sobre um corpo k. Considere $V_1 \bigotimes V_2$ o produto tensorial entre V_1 e V_2 e a aplicação*

$$\begin{array}{rrcl} i: & V_1 \times V_2 & \to & V_1 \bigotimes V_2 \\ & (v_1, v_2) & \mapsto & v_1 \otimes v_2. \end{array}$$

Se $\phi : V_1 \times V_2 \to W$ é uma aplicação bilinear, então existe uma única aplicação linear $\Phi : V_1 \bigotimes V_2 \to W$ tal que $\phi = \Phi \circ i$, ou seja, o seguinte diagrama comuta

$$\begin{tikzcd} V_1 \times V_2 \arrow[r, "\phi"] \arrow[dr, "i"'] & W \\ & V_1 \bigotimes V_2 \arrow[u, "\Phi"'] \end{tikzcd}$$

A prova da proposição acima pode ser encontrada em [4] (Corolário 12, p.368). Temos ainda que vale a associatividade para produtos tensoriais (veja [4], p.372), ou seja

$$(V_1 \bigotimes V_2) \bigotimes V_3 \cong V_1 \bigotimes (V_2 \bigotimes V_3).$$

Com isso podemos omitir os parênteses da expressão acima e tomar o produto tensorial de t fatores da seguinte forma

$$V_1 \bigotimes \cdots \bigotimes V_t,$$

essa expressão indica que estamos operando os conjuntos dois a dois sem dar importância a ordem em que a operação é realizada.

A propriedade obtida na Proposição A.1 é dita **Propriedade Universal de Produtos Tensoriais** e pode ser estendida para produtos tensoriais de mais de dois termos, como veremos abaixo.

$$\begin{array}{rrcl} i: & V_1 \times \cdots \times V_t & \to & V_1 \bigotimes \cdots \bigotimes V_t \\ & (v_1, \ldots, v_t) & \mapsto & v_1 \otimes \cdots \otimes v_t. \end{array}$$

Se $\phi : i : V_1 \times \cdots \times V_t \to E$ é uma aplicação t-linear, então existe uma única aplicação linear $\Phi : i : V_1 \bigotimes \cdots \bigotimes V_t \to E$ tal que $\phi = \Phi \circ i$, ou seja, o seguinte diagrama comuta

$$\begin{tikzcd}
V_1 \times \cdots \times V_t \arrow[r, "\phi"] \arrow[dr, "i"'] & E \\
& V_1 \bigotimes \cdots \bigotimes V_t \arrow[u, "\Phi"']
\end{tikzcd}$$

A prova desse resultado se dá pela combinação da propriedade associativa do produto tensorial com a Proposição A.1.

Seja V um espaço vetorial sobre k. Denotaremos para $t \geqslant 1$

$$T^t(V) = \underbrace{V \bigotimes \cdots \bigotimes V}_{t \text{ fatores}},$$

e definimos que $T^0(V) = k$.

Seja $A^t(V)$ o subespaço de $T^t(V)$ gerado por todos os elementos $v_1 \otimes \cdots \otimes v_t \in T^t(V)$ tais que $v_i = v_j$ para algum par $i \neq j$.

Definição A.2. *Sejam $T^t(V)$ e $A^t(V)$ como acima. O quociente*

$$\bigwedge^t V = \frac{T^t(V)}{A^t(V)}$$

*é dito a t-ésima **potência exterior** de V.*

Denotamos $v_1 \otimes \cdots \otimes v_t \mod A^t(V)$ é um elemento de $\bigwedge^t V$ o qual denotaremos por $v_1 \wedge \cdots \wedge v_t$.

Veremos a seguir uma propriedade para potências exteriores semelhante a propriedade universal para produtos tensoriais.

$$\begin{array}{rccc}
j: & V \times \cdots \times V & \to & \bigwedge^t V \\
& (v_1, \ldots, v_t) & \mapsto & v_1 \wedge \cdots \wedge v_t.
\end{array}$$

Note que por construção, a aplicação j definida acima é alternada. Além disso, a aplicação j atende a seguinte propriedade: se $\phi : V^t \to E$ é uma aplicação t-linear alternada, então existe uma única aplicação linear $\Phi : \bigwedge^t V \to E$ tal que o diagrama comuta (veja [4], p. 447):

$$\begin{tikzcd}
V \times \cdots \times V \arrow[rr, "\phi"] \arrow[drr, "i"'] & & E \\
& & \bigwedge^t V \arrow[u, "\Phi"']
\end{tikzcd}$$

Tal propriedade é conhecida como propriedade universal para aplicações multilineares alternadas.

Estabeleceremos a seguir algumas propriedades para $\bigwedge^t V$. Por construção, são válidas as seguintes propriedades:

i - $v_1 \wedge \ldots \wedge v_t = 0$ se $v_j = v_i$ para algum par (i, j) com $i \neq j$ e $i, j \in \{1, \ldots, t\}$;

ii - $\ldots \wedge v_i \wedge (v+w) \wedge v_{i+2} \wedge \ldots = \ldots \wedge v_i \wedge v \wedge v_{i+2} \wedge \ldots + \ldots \wedge v_i \wedge w \wedge v_i + 2 \wedge \ldots$;

iii - $v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(t)} = \text{sgn }(\sigma)(v_1 \wedge \cdots \wedge v_t)$;

A propriedade [i] segue por construção do quociente que define a potência exterior. As propriedades [ii] e [iii] seguem do fato de j ser uma aplicação t-linear alternada.

Exemplo A.2. Seja $\bigwedge^2 V$. Por definição do quociente, temos que se $v_1 = v_2$ então $v_1 \wedge v_2 = 0$. Assim temos,

$$\begin{aligned}
0 &= (v+w) \wedge (v+w) \\
&= v \wedge v + w \wedge v + v \wedge w + w \wedge w \\
&= 0 + w \wedge v + v \wedge w + 0.
\end{aligned}$$

donde vemos que $w \wedge v = -v \wedge w$.

Exemplo A.3. Seja $V = \mathbb{R}^2$ e sua base canônica $\{e_1, e_2\}$. Então, $\bigwedge^t \mathbb{R}^2$ consiste de soma finitas de elementos da forma $(a_{11}e_1 + a_{12}e_2) \wedge \cdots \wedge (a_{t1}e_1 + a_{t2}e_2)$.

No caso em que $t = 2$, temos:

$$\begin{aligned}
(a_{11}e_1 + a_{12}e_2) \wedge (a_{21}e_1 + a_{22}e_2) &= (a_{11}e_1) \wedge (a_{21}e_1) + (a_{11}e_1) \wedge (a_{22}e_2) \\
&+ (a_{12}e_2) \wedge (a_{21}e_1) + (a_{12}e_2) \wedge (a_{22}e_2) \\
&= a_{11}a_{21}(e_1 \wedge e_1) + a_{11}a_{22}(e_1 \wedge e_2) \\
&+ a_{12}a_{21}(e_2 \wedge e_1) + a_{12}a_{22}(e_2 \wedge e_2) \\
&= a_{11}a_{22}(e_1 \wedge e_2) + a_{12}a_{21}(e_2 \wedge e_1) \\
&= a_{11}a_{22}(e_1 \wedge e_2) - a_{12}a_{21}(e_1 \wedge e_2) \\
&= (a_{11}a_{22} - a_{12}a_{21})(e_1 \wedge e_2).
\end{aligned}$$

Isso mostra que $\bigwedge^2 \mathbb{R}^2$ é gerado pelo elemento $e_1 \wedge e_2$. Notação: $< e_1 \wedge e_2 >$.

Caso $t = 3$, temos
$(a_{11}e_1 + a_{12}e_2) \wedge (a_{21}e_1 + a_{22}e_2) \wedge (a_{31}e_1 + a_{32}e_2)$
$= (a_{11}e_1) \wedge (a_{21}e_1) \wedge (a_{31}e_1) + (a_{11}e_1) \wedge (a_{21}e_1) \wedge (a_{32}e_2) + (a_{11}e_1) \wedge (a_{22}e_2) \wedge (a_{31}e_1)$
$+ (a_{11}e_1) \wedge (a_{22}e_2) \wedge (a_{32}e_2) + (a_{12}e_2) \wedge (a_{21}e_1) \wedge (a_{31}e_1) + (a_{12}e_2) \wedge (a_{21}e_1) \wedge (a_{32}e_2)$
$+ (a_{12}e_2) \wedge (a_{22}e_2) \wedge (a_{31}e_1) + (a_{12}e_2) \wedge (a_{22}e_2) \wedge (a_{32}e_2)$
$= 0.$

Isso mostra que $\bigwedge^3 \mathbb{R}^2 = 0$. Esse fato irá também ocorrer para todo $t \geqslant 3$.

Com isso, podemos listar:

$t = 0 : \bigwedge^t \mathbb{R}^2 = \mathbb{R};$

$t = 1 : \bigwedge^t \mathbb{R}^2 = \mathbb{R}^2;$

$t = 2 : \bigwedge^t \mathbb{R}^2 =< e_1 \wedge e_2 >;$

$t \geqslant 3 : \bigwedge^t \mathbb{R}^2 = 0.$

O exemplo acima pode ser generalizado pelo seguinte resultado.

Proposição A.2. *Seja V um espaço vetorial sobre k tal que $dim_k V = l$. Se*

i - $t > l$, então $\bigwedge^t V = 0$;

ii - $1 \leqslant t \leqslant l$, então $dim_k(\bigwedge^t V) = \begin{pmatrix} l \\ t \end{pmatrix}$.

Além disso, se $\{v_1, \ldots, v_l\}$ é uma base para V, então

$$\{v_{i_1} \wedge \cdots \wedge v_{i_t} \mid \forall v_{i_1}, \ldots, v_{i_t} \in \{v_1, \ldots, v_l\} \; com \; \leqslant l1 \leqslant v_{i_1} < v_{i_2} < \cdots < v_{i_t} \leqslant l\}$$

é uma base para $\bigwedge^t V$.

A prova dessa proposição é uma generalização do Exemplo A.3. Em particular, se V tem dimensão t, e se $\{v_1, \ldots, v_t\}$ for uma base para V, então $\{v_1 \wedge \ldots \wedge v_t\}$ é uma base para o espaço unidimensional $\bigwedge^t V$.

Se h é uma aplicação linear do espaço vetorial V em W, temos uma aplicação induzida de $\bigwedge^t V$ em $\bigwedge^t W$ definida naturalmente pela ação de h em cada entrada do produto exterior, ou seja,

$$\wedge^t h(f_1 \wedge \cdots \wedge f_t) = h(f_1) \wedge \cdots \wedge h(f_t)$$

$f_1, \ldots, f_t \in V$ e $h(f_1), \ldots, h(f_t) \in W$.

Agora, façamos algumas observações para o caso em que $V = S_{\leqslant d} = \{f \in S | \deg(f) \leqslant d\}$. Sejam $m_1, \cdots, m_t$ monômios de $S_{\leqslant d}$, então $m_1 \wedge \cdots \wedge m_t$ é um monômio de $\bigwedge^t S_{\leqslant d}$. Um termo de $\bigwedge^t S_{\leqslant d}$ é do tipo $\alpha m_1 \wedge \cdots \wedge m_t$, onde $\alpha \in k$ e $m_1 \wedge \cdots \wedge m_t$ é um monômio.

Seja $<$ uma ordem monomial definida em $S_{\leqslant d}$. Assim, temos a ordem monomial induzida em $\bigwedge^t S_{\leqslant d}$ como

$$m_1 \wedge \cdots \wedge m_r < n_1 \wedge \cdots \wedge n_r \Rightarrow m_i < n_i$$

para o menor índice i tal que $m_i \neq n_i$, onde m_i, n_i são monômios em $S_{\leqslant d}$.

Dados $f_1, \cdots, f_r \in S_{\leqslant d}$, então

$$f_1 \wedge \cdots \wedge f_r = (\text{in}(f_1) + resto(f_1)) \wedge \cdots \wedge (\text{in}(f_r) + resto(f_r)) = \text{in}(f_1) \wedge \cdots \wedge \text{in}(f_r) + resto.$$

O monômio $\text{in}(f_1) \wedge \cdots \wedge \text{in}(f_r)$ assim obtido é o monômio líder de $f_1 \wedge \cdots \wedge f_r$, ou seja, $in(f_1 \wedge \cdots \wedge f_r) = in(f_1) \wedge \cdots \wedge in(f_r)$.

Dizemos que um monômio em $\bigwedge^t S_{\leqslant d}$ é dito estar na forma normal se $m = m_1 \wedge \cdots \wedge m_r \Rightarrow m_1 > \cdots > m_r$, onde $m_1, \cdots, m_r$ são monômios em $S_{\leqslant d}$.

Se $f_1, \cdots, f_t \in S_{\leqslant d}$ são polinômios, então o elemento de $\bigwedge^t S_{\leqslant d}$ pode ser escrito como uma soma de monômios de $\bigwedge^t S_{\leqslant d}$.

Dizemos que um elemento de $m_1 + \cdots + m_r \in \bigwedge^t S_{\leqslant d}$ é dito estar na forma normal se $m_1 > \cdots > m_r$, onde $m_1, \cdots, m_r \in \bigwedge^t S_{\leqslant d}$ são monômios.

Exemplo A.4. Sejam $f_1 = x^2 + y^2, f_2 = xy + z^2$. A ordem monomial adotada é a lexicográfica reversa graduada e $x < y < z$. Sabemos que $x^2 > xy > y^2 > z^2$. Daí,

$$\begin{aligned}
f_1 \wedge f_2 &= (x^2 + y^2) \wedge (xy + z^2) \\
&= x^2 \wedge (xy + z^2) + y^2 \wedge (xy + z^2) \text{ linearidade na primeira coordenada.} \\
&= (x^2 \wedge xy + x^2 \wedge z^2) + (y^2 \wedge xy + y^2 \wedge z^2) \text{ linearidade na segunda coordenada.} \\
&= x^2 \wedge xy + x^2 \wedge z^2 + y^2 \wedge xy + y^2 \wedge z^2 \\
&= x^2 \wedge xy + x^2 \wedge z^2 - xy \wedge y^2 + y^2 \wedge z^2 \text{ colocando os monômios na forma normal.}
\end{aligned}$$

Portanto $f_1 \wedge f_2 = x^2 \wedge xy + x^2 \wedge z^2 - xy \wedge y^2 + y^2 \wedge z^2$ e $\text{in}(f_1 \wedge f_2) = x^2 \wedge xy = \text{in}(f_1) \wedge \text{in}(f_2)$.

Referências

[1] BAYER, D.; STILLMAN, M. A theorem on refining division orders by the reverse lexicographic orders. **Duke Mathematical Journal**. v.55. p. 321-328.

[2] COX, D.; LITTLE, J.; O'SHEA, D. **Ideals, Varieties, and Algorithms:** An Introduction to Computational Algebraic Geometry and Commutative Algebra. 3rd ed. New York: Springer, 2007.

[3] DECKER, W. et al. **Singular 3-1-2:** A computer algebra system for polynomial computations. 2010. Disponível em: < http://www.singular.uni-kl.de>. Acesso em: 02 jan. 2011.

[4] DUMMIT, D. S.; FOOTE, R. M. **Abstract Algebra** 3rd ed. John-Wiley and Sons Inc., 2004.

[5] EISENBUD, D. **Commutative Algebra with a View Toward Algebraic Geometry**. New York: Springer, 2004.

[6] GALLIGO, A. A propos du théorème de préparation de Weierstrass. In Fonctions des Plusieurs Variables Complexes. **Lecture Notes in Mathematics**. v.409. New York: Springer-Verlag, 1974. p. 543-579.

[7] HASSETT, B. **Introduction to Algebraic Geometry**. New York: Cambridge University Press, 2007.

[8] KREUZER, M.; ROBBIANO, L. **Computational Commutative Algebra 2**. New York: Springer-Verlag, 2005.

[9] LIU, Q. **Algebraic Geometry and Arithmetic Curves**. New York: Oxford University Press, 2002.

[10] MILLER, E.; STURMFELS, B. **Combinatorial Commutative Algebra**. New York: Springer, 2005.

[11] SANTOS, J.P.O.; MELLO, M.P.; MURANI, I.T.C. **Introdução à Análise Combinatória**. Campinas: Unicamp, 1995.