UNIVERSIDADE FEDERAL DE SÃO CARLOS
CCET - CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA

Teoria de Invariantes de Formas Binárias

Aluno: Renato Fehlberg Júnior
Orientador: Prof. Dr. João Nivaldo Tomazella

São Carlos - SP
Março/2010

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CCET - CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA

Teoria de Invariantes de Formas Binárias

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da UFSCar, como parte dos requisitos para obtenção do Título de Mestre em Matemática.

Aluno: Renato Fehlberg Júnior
Orientador: Prof. Dr. João Nivaldo Tomazella

São Carlos - SP
Março/2010

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária da UFSCar

F296ti

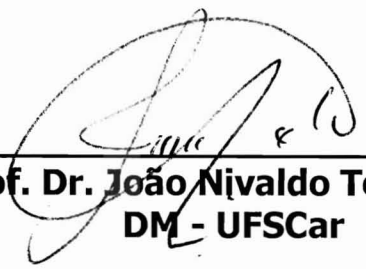
Fehlberg Júnior, Renato.
Teoria de invariantes de formas binárias / Renato Fehlberg Júnior. -- São Carlos : UFSCar, 2010.
82 f.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2010.

1. Álgebra. 2. Covariantes. 3. Operador umbral. 4. Formas canônicas. I. Título.

CDD: 512 (20ª)

Banca Examinadora:



Prof. Dr. João Nivaldo Tomazella
DM - UFSCar

Profa. Dra. Maria Aparecida Soares Ruas
ICMC - USP

Prof. Dr. Eduardo Tengan
ICMC - USP

Agradecimentos

A Deus, por todas as bençãos em minha vida.
À minha família por todo apoio e compreensão e em especial, aos meus pais, que sempre colocam minha vida e meu futuro em primeiro lugar.
Ao meu orientador, por me guiar nestes dois anos de mestrado com competência.
À professora Cidinha, pelos vários seminários que enriqueceram a dissertação.
À Greciane, pela compreensão e por sempre estar ao meu lado.
Ao CNPq, pelo apoio financeiro.
Aos meus amigos, pela companhia.
A todos, os meus sinceros agradecimentos.

Resumo

Neste trabalho, estudamos o artigo [6], que responde as seguintes perguntas: como são todos os covariantes de formas binárias? Quais são e como encontrar as formas canônicas das formas binárias de grau n? Existe um conjunto finito de geradores para os covariantes de formas binárias de grau n? A primeira pergunta será respondida pelo primeiro teorema fundamental, que nos diz que todos os covariantes são avaliações umbral de polinômios colchete, e vice-versa. A segunda questão será respondida usando-se as técnicas de apolaridade, e como aplicação da técnica, mostraremos o resultado para formas binárias de grau baixo. E finalmente, a terceira pergunta será respondida pelo Teorema de Finitude.

Abstract

In this work, we studied article [6], that answers the following questions: how are all covariants of binary forms? What are and how to find the canonical forms of the binary forms of degree n? Is there a finite generating set for the convariants of binary forms of degree n? The first question will be answered by the First Fundamental Theorem. The second question will be answered using the techniques of apolarity. And for application, we will show the results for binary forms of low degree. Finally, the third question will be answered by the Finiteness Theorem.

Sumário

Introdução

Aqui apresentaremos resultados sobre formas binárias usando a velha Teoria de Invariantes, desenvolvida por Hilbert, Boole, Young, Gordan, e outros. A teoria de invariantes para formas binárias será desenvolvida de modo construtivo, de modo que o desenvolvimento da teoria ficará bem claro. Para isso, usaremos a notação umbral, que foi introduzida por Kung e Rota (ver [6]), no lugar da notação simbólica, que pode ser encontrada em [3]. Uma discussão sobre essas notações pode ser encontrada em [4]. A notação umbral será definida e exemplificada no capítulo 1, onde mostraremos rigorosamente como é feito o cálculo umbral. Neste capítulo ainda, definiremos o que é um covariante e daremos vários exemplos do mesmo. Na seção 2, ainda do capítulo 1, demonstraremos o Primeiro e o Segundo Teorema Fundamental, sendo a demonstração do Primeiro Teorema Fundamental, totalmente construtiva, usando-se o algoritmo de ordenação, que é baseado em um syzygy. No capítulo 2, definiremos a álgebra de raízes homogeneizadas, onde obteremos outra representação dos covariantes através de um algoritmo que dará a representação de qualquer covariante em termos de raízes homogeneizadas. Além disso, definiremos os termos diferença simétrico que terão uma certa correspondência com os covariantes homogêneos e isso será usado na demonstração do Teorema de Finitude, no capítulo 5. Na primeira seção do capítulo 3, apenas indicaremos alguns resultados dos capítulos 1 e 2 que podem ser generalizados para covariantes de duas formas binárias, que chamaremos de 2-covariante. A segunda seção é reservada para apresentarmos o covariante apolar. Esta técnica de apolaridade será usada para encontrar a forma canônica de uma forma binária, que é basicamente uma forma mais simples de representar uma forma binária. No capítulo 4, encontraremos as formas canônicas das formas binárias de grau baixo. Finalmente, no capítulo 5 demonstraremos o Teorema de Finitude, que diz que existe um conjunto finito que gera todos os covariantes de formas binárias de grau n, e além disso, explicitaremos um conjunto de geradores para os covariantes das formas cúbicas.

Em uma primeira leitura, recomendamos que na seção 2.2, seja lido apenas o Algoritmo 2.7. Além disso, a Seção 3.1 (com exceção da definição de 2-covariante

e do operador umbral para duplas de formas binárias), assim como a demonstração de todos os Lemas, exceto o Algoritmo de ordenação e o Lema de Hilbert, podem ser deixados para uma segunda leitura. Quanto aos exemplos, eles estão distribuídos em grande número ao longo do texto, para facilitar a visualização dos resultados e definições.

Capítulo 1

Covariantes

1.1 Notação Umbral

Nesta seção, introduziremos a noção de operador umbral, sua ação sobre o espaço umbral e vários exemplos de covariantes.

Definição 1.1. *Uma forma binária $f(x, y)$ de grau n nas variáveis x e y é um polinômio homogêneo de grau n nas variáveis x e y. Escrevemos*

$$f(x, y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}.$$

Os números a_k são chamados coeficientes da forma binária e pertencem a um corpo de característica zero, que denotaremos por $\mathbb{K}$.

Definição 1.2. *Uma mudança linear de variáveis (c_{ij}) é uma transformação das variáveis x e y dada por*

$$x = c_{11}\overline{x} + c_{12}\overline{y}$$

$$y = c_{21}\overline{x} + c_{22}\overline{y}$$

tal que o determinante das entradas, $c_{11}c_{22} - c_{21}c_{12} \neq 0$.

Observação 1.3. *Uma forma binária $f(x, y)$ sob uma mudança linear de variáveis, mais uma expansão e reagrupamento de termos, é transformada em uma outra forma binária nas variáveis $\overline{x}$ e $\overline{y}$, com coeficientes dependendo dos a_i e c_{ij}, que definiremos por*

$$\begin{aligned} \overline{f}(\overline{x}, \overline{y}) &= \sum_{k=0}^{n} \binom{n}{k} a_k (c_{11}\overline{x} + c_{12}\overline{y})^k (c_{21}\overline{x} + c_{22}\overline{y})^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} \overline{a}_k \overline{x}^k \overline{y}^{n-k}. \end{aligned}$$

Definição 1.4. *Seja g um inteiro não negativo. Um polinômio não constante $I(A_0, A_1, ..., A_n, X, Y)$ nas variáveis $A_0, A_1, ..., A_n, X$ e Y, é um covariante de índice g de formas binárias de grau n se, para toda forma binária $f(x, y)$ de grau n e toda mudança linear de variáveis (c_{ij}), temos que*

$$I(\overline{a}_0, \overline{a}_1, ..., \overline{a}_n, \overline{x}, \overline{y}) = (c_{11}c_{22} - c_{21}c_{12})^g I(a_0, a_1, ..., a_n, x, y)$$

Um covariante no qual as variáveis X e Y não aparecem é um *invariante*.

Exemplo 1.5. *Como primeiro exemplo de covariante, vamos considerar o covariante $I(A_0, A_1, X, Y) = A_1X - A_0Y$ de índice $g = 0$ de formas binárias de grau $n = 1$. Seja $f(x, y) = a_1x + a_0y$ uma forma binária de grau um e, $x = c_{11}\overline{x} + c_{12}\overline{y}$ e $y = c_{21}\overline{x} + c_{22}\overline{y}$, uma mudança linear de variáveis, ambas tomadas de modo arbitrário. Sendo $\overline{f}(\overline{x}, \overline{y})$, a forma binária $f(x, y) = a_1x + a_0y$ após a mudança de variáveis, obtemos:*

$$\overline{f}(\overline{x}, \overline{y}) = (a_0c_{21} + a_1c_{11})\overline{x} + (a_0c_{22} + a_1c_{12})\overline{y} = \overline{a}_1\overline{x} + \overline{a}_0\overline{y}.$$

Fazendo um pouco de conta, obtemos $I(\overline{a}_0, \overline{a}_1, \overline{x}, \overline{y}) = I(a_0, a_1, x, y)$.

Definição 1.6. *Um covariante $I(A_0, A_1, ..., A_n, X, Y)$ é homogêneo se ele é homogêneo como polinômio tanto nas variáveis $A_0, A_1, ..., A_n$ quanto nas variáveis X e Y. Se I é um covariante homogêneo, entenderemos por grau de I como o grau de I visto como polinômio nas variáveis $A_0, A_1, ..., A_n$, e chamaremos de ordem de I como o grau de I visto como polinômio nas variáveis X e Y.*

Exemplo 1.7. *Consideremos o discriminante $D = D(A_0, A_1, A_2) = A_0A_2 - A_1^2$, de formas quadráticas binárias. Seja $x = c_{11}\overline{x} + c_{12}\overline{y}$ e $y = c_{21}\overline{x} + c_{22}\overline{y}$, uma mudança linear de variáveis. Fazendo algumas contas, podemos chegar que $D(\overline{a}_0, \overline{a}_1, \overline{a}_2) = (c_{22}c_{11} - c_{12}c_{21})^2 D(a_0, a_1, a_2)$, ou seja, D é um invariante de grau 2, ordem 0, de índice 2 de formas binárias de grau 2.*

Exemplo 1.8. *O discriminante $D(A_0, A_1, A_2, A_3) = -9B_1^2B_2^2 - 54B_1B_2B_3B_0 + 27B_3^2B_0^2 + 108B_2^3B_0 + 4B_1^3B_3$ das formas cúbicas binárias é um invariante de grau 4 e índice 6.*

Exemplo 1.9. *Nos exemplos anteriores, apresentamos apenas covariantes homogêneos. Veremos agora o caso não homogêneo. Consideremos $I(A_0, A_1, A_2, X, Y) = A_2^2A_1X^4 + (A_0A_2^2 + 2A_2A_1^2)X^3Y + 3A_0A_1A_2X^2Y^2 + A_0^2A_2XY^3 + A_1A_2X^2 + A_0A_2XY$. I é um covariante de índice 1 de formas binárias de grau 2, e é não homogêneo. Além disso, se escrevermos $I = I_1 + I_2$, onde $I_1 = A_2^2A_1X^4 + (A_0A_2^2 + 2A_2A_1^2)X^3Y +$*

$3A_0A_1A_2X^2Y^2 + A_0^2A_2XY^3$ *e* $I_2 = A_1A_2X^2 + A_0A_2XY$*, veremos que estes são covariantes homogêneos, de graus* 4 *e* 2 *respectivamente, de índice* 1 *de formas binárias de grau* 2*. Mostrar estas afirmações pela definição pode ser muito cansativo, mas logo veremos que mostrar que esses polinômios são de fato covariantes, será uma tarefa fácil usando o Primeiro Teorema Fundamental.*

Observação 1.10. *Para mais exemplos de covariantes e invariantes clássico, ver [12], [3], [5] e [11].*

Notemos que todo covariante pode ser escrito como uma combinação linear de covariantes homogêneos. Entenderemos por uma *forma binária simples*, como sendo uma n-ésima potência de uma forma linear, ou seja,

$$f(x, y) = (\alpha_1 x + \alpha_2 y)^n.$$

Agora, definiremos o operador umbral e como é sua ação no espaço umbral.

Definição 1.11. *Seja* $\mathscr{A} = \{\alpha, \beta, ..., \omega, u\}$ *um alfabeto consistindo de uma quantidade infinita de letras gregas, seguida de uma única letra romana* u*. As letras em* $\mathscr{A}$ *são chamadas de letras umbral. Para cada letra umbral grega* ζ *e a letra umbral romana* u*, associaremos duas variáveis* ζ_1 *e* ζ_2*. Temos então as variáveis* α_1*,* α_2*,* β_1*,* β_2*, ...,* ω_1*,* ω_2*,* u_1*,* u_2*. O anel de todos os polinômios nestas variáveis será um espaço vetorial de dimensão infinita chamado de espaço umbral* $\mathscr{U}$*.*

Definição 1.12. *Sejam* $n \in \mathbb{N}$*,* $\mathscr{P}$ *o espaço de todos os polinômios nas variáveis* $A_0, A_1, ..., A_n, X$ *e* Y *e* $P(\alpha_1, \alpha_2, ...)$ *um polinômio em* $\mathscr{U}$*. Definiremos o operador umbral*

$$U : \mathscr{U} \to \mathscr{P}$$

para formas binárias de grau n *por:*

$\langle U \,|\alpha_1^k \alpha_2^{n-k}\rangle = A_k$ *para qualquer letra umbral grega* α*;*

$\langle U \,|\alpha_1^j \alpha_2^k\rangle = 0$ *se* $j + k \neq n$ *e* α *é qualquer letra umbral grega;*

$\langle U \,|u_1^k\rangle = (-Y)^k$*;*

$\langle U \,|u_2^k\rangle = X^k$*;*

$\langle U \,|\alpha_1^i \alpha_2^j \beta_1^k \beta_2^l ... u_1^p u_2^q\rangle = \langle U \,|\alpha_1^i \alpha_2^j\rangle \langle U \,|\beta_1^k \beta_2^l\rangle ... \langle U \,|u_1^p\rangle \langle U \,|u_2^q\rangle$ *(chamada lei multiplicativa);*

onde $\langle U \,|P(\alpha_1, \alpha_2, ...)\rangle$ *denota a ação do operador* U *sobre* $P(\alpha_1, \alpha_2, ...) \in \mathscr{U}$*.*

Notemos que por linearidade, o operador umbral U é definido unicamente pelas regras acima.

Exemplo 1.13. *Para ficar mais clara a ação do operador umbral, sejam U o operador umbral para formas binárias de grau 2 e*

$$P = P(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, u_1, u_2) = \alpha_1\alpha_2u_2^2 - \beta_1^2u_1^2 - \gamma_2u_2 + \gamma_1^2\alpha_2^2u_1u_2,$$

um polinômio no espaço umbral $\mathscr{U}$. Então temos, $\langle U\,|P\rangle = A_1X^2 - A_2Y^2 - 0 - A_2A_0XY = A_1X^2 - A_2Y^2 - A_2A_0XY$.

Definição 1.14. *Seja*

$$f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$$

uma forma binária de grau n. Definimos o funcional linear umbral $U(f)$ associado a $f(x,y)$, como o funcional linear sobre $\mathscr{U}$, avaliando o operador umbral U em: $A_i = a_i$, $X = x$ e $Y = y$, para $i = 0, 1, \ldots, n$.

Observação 1.15. *Todo polinômio $I(A_0, A_1, \ldots, A_n, X, Y)$ pode ser escrito como $\langle U\,|Q(\alpha_1, \alpha_2, \ldots)\rangle$, para algum $Q(\alpha_1, \alpha_2, \ldots) \in \mathscr{U}$ (chamaremos o polinômio Q de uma representação umbral de I, e I de uma avaliação umbral de Q). De fato, por linearidade basta considerarmos o caso em que I é um monômio $A_0^{d_o}A_1^{d_1}\ldots A_n^{d_n}X^{e_1}Y^{e_2}$, então, pelas regras do operador umbral U obtemos*

$$I = \langle U|\underbrace{\alpha_1^0\,\alpha_2^n \ldots \gamma_1^0\,\gamma_2^n}_{d_0 vezes}\underbrace{\delta_1^1\,\delta_2^{n-1}\ldots\epsilon_1^1\,\epsilon_2^{n-1}}_{d_1 vezes}\ldots(-u_1^{e_2})\,u_2^{e_1}\rangle,$$

onde as letras umbral $\alpha, \ldots, \gamma, \delta, \ldots, \epsilon, \ldots$ são distintas. Notemos que em geral esta representação não é única.

Exemplo 1.16. *Consideremos o polinômio $I(A_0, A_1, X, Y) = A_1X^2 - A_0Y^3X + A_1A_0$. Temos que uma representação umbral de I é*

$$Q(\alpha_1, \alpha_2, \beta_1, \beta_2, u_1, u_2) = \alpha_1^1\alpha_2^1u_2^2 + \alpha_2^2u_1^3u_2 + \alpha_1^1\alpha_2^1\beta_2^2.$$

Outra representação umbral de I é

$$P(\alpha_1, \alpha_2, \beta_1, \beta_2, u_1, u_2) = \alpha_1^1\alpha_2^1u_2^2 + \beta_2^2u_1^3u_2 + \beta_1^1\beta_2^1\alpha_2^2.$$

Daremos agora, uma notação especial para mudança de variáveis, que facilitará nossa escrita e deixará mais clara a proposição seguinte. Essa proposição nos dará um método de calcular os coeficientes de um polinômio após uma mudança de variável usando sua representação umbral, além de ser usada como ferramenta para provar outros resultados.

Definição 1.17. *Seja (c_{ij}) uma mudança linear de variáveis. Coloquemos*

$$c_2 = c_{11} \quad d_2 = c_{12},$$

$$c_1 = -c_{21} \quad d_1 = -c_{22}.$$

Denotaremos essa mudança de variáveis por (c, d). Se $u = (u_1, u_2)$ e $v = (v_1, v_2)$ são dois vetores (de dimensão dois), definimos o colchete $[u \quad v]$ por $[u \quad v] = u_1v_2 - u_2v_1 = det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}$.

Temos então que $[\alpha \quad \beta] = \alpha_1\beta_2 - \alpha_2\beta_1$ e $[\alpha \quad u] = \alpha_1u_2 - \alpha_2u_1$.

Proposição 1.18. *Sejam $f(x, y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$ uma forma binária de grau n, (c, d) uma mudança de variáveis e $I \in \mathscr{P}$. Sejam então, $\overline{f}(\overline{x}, \overline{y})$ a forma binária obtida de $f(x, y)$ por (c, d) e $I(a_0, a_1, ..., a_n, x, y) = \langle U(f) \,|P(\alpha_1, \alpha_2, \beta_1, \beta_2, ..., u_1, u_2)\rangle$ uma representação umbral de I. Então*

$$I(\overline{a}_0, \overline{a}_1, \dots, \overline{a}_n, \overline{x}, \overline{y}) = \left\langle U(\overline{f}) \,|P(\alpha_1, \alpha_2, \beta_1, \beta_2, \dots, u_1, u_2)\right\rangle$$
$$= \langle U(f) \,|P([\alpha \quad c], [\alpha \quad d], [\beta \quad c], [\beta \quad d], \dots, [u \quad c]/[c \quad d], [u \quad d]/[c \quad d])\rangle .$$

Demonstração: Como o operador umbral é linear e vale a lei associativa, basta provarmos as seguintes identidades:

(a) $\left\langle U(f) \left| [\alpha \quad c]^j [\alpha \quad d]^k \right.\right\rangle = \left\langle U(\overline{f}) \left| \alpha_1^j \alpha_2^k \right.\right\rangle$, $\forall$ letra umbral grega α;

(b) $\langle U(f) \,|[u \quad c]/[c \quad d]\rangle = \left\langle U(\overline{f}) \,|u_1 \right\rangle = -\overline{y}$

(c) $\langle U(f) \,|[u \quad d]/[c \quad d]\rangle = \left\langle U(\overline{f}) \,|u_2 \right\rangle = \overline{x}$

Para provarmos (b) e (c), observemos que da mudança de variáveis temos:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c_2 & d_2 \\ -c_1 & -d_1 \end{pmatrix} \begin{pmatrix} \overline{x} \\ \overline{y} \end{pmatrix},$$

e invertendo, obtemos

$$\begin{pmatrix} \overline{x} \\ \overline{y} \end{pmatrix} = \frac{1}{[c \quad d]} \begin{pmatrix} -d_1 & -d_2 \\ c_1 & c_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

ou seja,

$$\begin{cases} \overline{x} &= (-d_1x - d_2y)/[c \quad d] \\ \overline{y} &= (c_1x + c_2y)/[c \quad d] \end{cases}.$$

Então,

$\langle U(f) \,|[u \quad d]\rangle = \langle U(f) \,|u_1d_2 - u_2d_1\rangle = -yd_2 - xd_1 = \overline{x}\,[c \quad d]$

$\langle U(f) \,|[u \quad c]\rangle = \langle U(f) \,|u_1c_2 - u_2c_1\rangle = -yc_2 - xc_1 = -\overline{y}\,[c \quad d]$

e portanto temos:

$$\langle U(f)\,|[u \quad d]\,/\,[c \quad d]\rangle = \overline{x} = \left\langle U(\overline{f})\,|u_1\right\rangle;$$
$$\langle U(f)\,|[u \quad c]\,/\,[c \quad d]\rangle = -\overline{y} = \left\langle U(\overline{f})\,|u_2\right\rangle.$$

Resta provarmos (a). Para isso, seja α uma letra umbral grega qualquer. Usando a representação umbral temos:

$$\begin{aligned}
\langle U(f)\,|(\alpha_1 u_2 - \alpha_2 u_1)^n\rangle &= \left\langle U(f)\left|\sum_{k=0}^{n}\tbinom{n}{k}(-1)^{n-k}\alpha_1^k u_2^k \alpha_2^{n-k} u_1^{n-k}\right.\right\rangle \\
&= \left\langle U(f)\left|\sum_{k=0}^{n}\tbinom{n}{k}(-1)^{n-k}\alpha_1^k \alpha_2^{n-k} u_2^k u_1^{n-k}\right.\right\rangle \\
&= \sum_{k=0}^{n}\tbinom{n}{k}(-1)^{n-k}\left\langle U(f)\left|\alpha_1^k\alpha_2^{n-k}\right.\right\rangle\left\langle U(f)\left|u_2^k u_1^{n-k}\right.\right\rangle \\
&= \sum_{k=0}^{n}\tbinom{n}{k}a_k(-1)^{n-k}(-y)^{n-k}x^k \\
&= \sum_{k=0}^{n}\tbinom{n}{k}a_k x^k y^{n-k} \\
&= f(x,y),
\end{aligned}$$

e portanto,

$$f(x,y) = \langle U(f)\,|[\alpha \quad u]^n\rangle.$$

Como

$$\begin{aligned}
det\begin{pmatrix}[\alpha & c] & [u & c] \\ [\alpha & d] & [u & d]\end{pmatrix} &= [\alpha \quad c]\,[u \quad d] - [u \quad c]\,[\alpha \quad d] \\
&= [\alpha \quad u]\,[c \quad d],
\end{aligned}$$

e por definição $\overline{f}(\overline{x},\overline{y}) = f(x,y)$, temos que:

$$\begin{aligned}
\overline{f}(\overline{x},\overline{y}) &= \langle U(f)\,|[\alpha \quad u]^n\rangle \\
&= \left\langle U(f)\left|det\begin{pmatrix}[\alpha & u] & [u & c]\,/\,[c & d] \\ [\alpha & d] & [u & d]\,/\,[c & d]\end{pmatrix}^n\right.\right\rangle \\
&= \left\langle U(f)\left|([\alpha \quad u]\,\frac{[u \quad d]}{[c \quad d]} - [\alpha \quad d]\,\frac{[u \quad c]}{[c \quad d]})^n\right.\right\rangle \\
&= \left\langle U(f)\left|\sum_{k=0}^{n}\tbinom{n}{k}[\alpha \quad c]^k\,[\alpha \quad d]^{n-k}\,(-\frac{[u \quad c]}{[c \quad d]})^{n-k}(\frac{[u \quad d]}{[c \quad d]})^k\right.\right\rangle \\
&= \sum_{k=0}^{n}\tbinom{n}{k}\left\langle U(f)\left|[\alpha \quad c]^k\,[\alpha \quad d]^{n-k}\right.\right\rangle\overline{x}^k\overline{y}^{n-k}.
\end{aligned}$$

Comparando o que obtemos com a expressão de $f(x,y) = \overline{f}(\overline{x},\overline{y})$, concluímos que:

$$\left\langle U(f) \left| [\alpha \quad c]^k [\alpha \quad d]^{n-k} \right. \right\rangle = \overline{a}_k = \left\langle U(\overline{f}) \left| \alpha_1^k \alpha_2^{n-k} \right. \right\rangle.$$

Se ocorrer $j + k \neq n$, temos que expandindo $[\alpha \quad c]^i [\alpha \quad d]^j$, os monômios são da forma $\alpha_1^p \alpha_2^q$, onde $p + q = j + k \neq n$, e portanto,

$$\left\langle U(f) \left| [\alpha \quad c]^j [\alpha \quad d]^k \right. \right\rangle = \left\langle U(\overline{f}) \left| \alpha_1^j \alpha_2^k \right. \right\rangle = 0.$$

■

Exemplo 1.19. *Sejam $f(x,y) = 2xy + x^2$ e (c,d) uma mudança linear de variáveis. Neste caso temos: $a_0 = 0$, $a_1 = 1$, $a_2 = 1$, $c = (-1,2)$, $d = (-1,1)$, $x = 2\overline{x} + \overline{y}$ e $y = \overline{x} + \overline{y}$.*

Tomemos $I \in \mathscr{P}$, com $I = I(A_0, A_1, A_2, X, Y) = 5A_0A_1X + 2A_2Y$. Depois da mudança de variáveis, f se torna a forma binária $\overline{f}(\overline{x},\overline{y}) = 8\overline{x}^2 + 10\overline{xy} + 3\overline{y}^2$. Além disso, seja $P(\alpha_1,\alpha_2,\beta_1,\beta_2,x,y) = 5\alpha_2^2\beta_1\beta_2u_2 - 2\alpha_1^2u_1$, uma representação umbral de I. Então temos:

$$I(\overline{a}_0,\overline{a}_1,\overline{a}_2,\overline{x},\overline{y}) = 59x - 43y.$$

Agora, se aplicarmos a Proposição anterior, temos:

$$\begin{aligned} I(\overline{a}_0,\overline{a}_1,\overline{a}_2,\overline{x},\overline{y}) &= \langle U(f) \,|P([\alpha \quad c], [\alpha \quad d], [\beta \quad c], [\beta \quad d], \\ &\qquad [u \quad c] / [c \quad d], [u \quad d] / [c \quad d])\rangle. \end{aligned}$$

Mas, notemos que $[c \quad d] = 1$, então:

$$\begin{aligned} I(\overline{a}_0,\overline{a}_1,\overline{a}_2,\overline{x},\overline{y}) &= \left\langle U(f) \left| 5 [\alpha \quad d]^2 [\beta \quad c] [\beta \quad d] [u \quad d] - 2 [\alpha \quad c]^2 [u \quad c] \right. \right\rangle \\ &= \left\langle U(f) \left| 5(\alpha_1d_2 - \alpha_2d_1)^2(\beta_1c_2 - \beta_2c_1)(\beta_1d_2 - \beta_2d_1) \right. \right. \\ &\quad \left. (u_1d_2 - u_2d_1) - 2(\alpha_1c_2 - \alpha_2c_1)^2(u_1c_2 - u_2c_1) \right\rangle \\ &= \left\langle U(f) \left| 5(\alpha_1 + \alpha_2)^2(2\beta_1 + \beta_2)(\beta_1 + \beta_2)(u_1 + u_2) \right. \right. \\ &\quad \left. -2(2\alpha_1 + \alpha_2)^2(2u_1 + u_2) \right\rangle \\ &= \left\langle U(f) \left| 5(\alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2)(2\beta_1^2 + 3\beta_1\beta_2 + \beta_2^2)(u_1 + u_2) \right. \right. \\ &\quad \left. -2(2\alpha_1^2 + 4\alpha_1\alpha_2 + \alpha_2^2)(2u_1 + u_2) \right\rangle \\ &= 59x - 43y, \end{aligned}$$

como afirma a Proposição.

1.2 Teoremas Fundamentais.

Apresentaremos nesta seção, o Primeiro Teorema Fundamental, que nos dará um método claro para obtermos covariantes e como representá-los umbralmente. Alguns polinômios no espaço umbral que representam covariantes, podem

ter muitos termos redundantes, mas representam o mesmo covariante. O Segundo Teorema Fundamental mostrará que podemos fazer certas operações sobre esses polinômios sem mudar suas avaliações umbral.

Definição 1.20. *Um monômio colchete M no espaço umbral $\mathscr{U}$ é um polinômio não-constante em $\mathscr{U}$ que pode ser escrito como um produto de colchetes, da forma $M = [\alpha \quad \beta]\,[\alpha \quad \delta]\,...\,[\omega \quad u]$, para os colchetes $[\alpha \quad \beta], [\alpha \quad \delta], ..., [\omega \quad u]$.*

Definição 1.21. *Seja M um monômio colchete. O índice de M é o número de colchetes em M contendo somente letras gregas. A ordem de M é o número de colchetes contendo a letra romana u. O tamanho de M é o número total de colchetes que aparecem em M.*

Entenderemos por um *polinômio colchete*, como uma combinação linear de monômios colchete.

Exemplo 1.22. *Qualquer monômio não-constante em $\mathscr{U}$ nas variáveis α_1, α_2, β_1, β_2, ... , u_1, u_2 não é um monômio colchete, e em particular não é um polinômio colchete.*

Inspirados por este exemplo e pela proposição anterior, definimos por $\mathscr{B}$, o conjunto dos polinômios colchete, que é um subespaço do espaço umbral $\mathscr{U}$. Além disso, definimos o subespaço $\mathscr{B}_g$ de $\mathscr{B}$ gerado pelos monômios colchete de índice g. Os elementos de $\mathscr{B}_g$ são chamados de *polinômios colchete de índice g.*

Antes de enunciar os Teoremas Fundamentais, provaremos alguns importantes resultados, sendo um destes, o *Algoritmo de Ordenação.*

Seja $\mathscr{A} = \{\alpha, \beta, \gamma, ...\}$ um alfabeto linearmente ordenado, ou seja, $\alpha < \beta < \gamma < ...$, e seja $M = [\alpha \quad \beta]\,[\alpha \quad \gamma]\,...\,[\delta \quad \epsilon]$ um monômio colchete de tamanho h. Escreveremos M como uma *tabela*, de altura h,

$$M = \begin{bmatrix} \alpha & \beta \\ \alpha & \gamma \\ \vdots & \vdots \\ \delta & \epsilon \end{bmatrix} = [\alpha \quad \beta]\,[\alpha \quad \gamma]\,...\,[\delta \quad \epsilon]\,.$$

Definição 1.23. *Uma tabela é padrão, se as letras em cada linha estão de forma crescente da esquerda para a direita, e as letras em cada coluna estão de forma não-decrescente do topo para baixo. Um monômio colchete é padrão se, por permutação de colchetes ou trocando colchetes $[\alpha \quad \beta]$ por $-[\beta \quad \alpha]$, puder ser escrito como uma tabela padrão.*

Exemplo 1.24. *Seja* $\mathscr{A} = \{\alpha, \beta, \gamma, \delta\}$ *tal que* $\alpha < \beta < \gamma < \delta$. *Notemos que* $P = [\alpha \quad \gamma][\delta \quad \beta]$ *é padrão. Porém,* $Q = [\alpha \quad \delta][\beta \quad \gamma]$ *não é padrão.*

Enunciaremos e demonstraremos agora três lemas que nos ajudarão a demonstrar o próximo teorema.

Lema 1.25. *(O SYZYGY) Sejam* $\alpha, \beta, \gamma, \delta$ *letras do alfabeto* $\mathscr{A}$ *com* $\alpha < \beta < \gamma < \delta$. *Então*

$$\begin{bmatrix} \alpha & \delta \\ \beta & \gamma \end{bmatrix} = -\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} + \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}.$$

Demonstração: Pela definição

$$\begin{aligned} -\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} + \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} &= [\alpha \quad \beta]\,[\delta \quad \gamma] - [\alpha \quad \gamma]\,[\delta \quad \beta] \\ &= (\alpha_1\beta_2 - \alpha_2\beta_1)(\delta_1\gamma_2 - \delta_2\gamma_1) \\ &- (\alpha_1\gamma_2 - \alpha_2\gamma_1)(\delta_1\beta_2 - \delta_2\beta_1) \\ &= \alpha_1\beta_2\delta_1\gamma_2 - \alpha_1\beta_2\delta_2\gamma_1 - \alpha_2\beta_1\delta_1\gamma_2 \\ &+ \alpha_2\beta_1\delta_2\gamma_1 - \alpha_1\gamma_2\delta_1\beta_2 + \alpha_1\beta_2\delta_2\gamma_1 \\ &+ \alpha_2\beta_1\delta_1\gamma_2 - \alpha_2\beta_1\delta_2\gamma_1 \\ &= (\alpha_1\delta_2 - \alpha_2\delta_1)(\beta_1\gamma_2 - \beta_2\gamma_1) \\ &= [\alpha \quad \delta]\,[\beta \quad \gamma] \\ &= \begin{bmatrix} \alpha & \delta \\ \beta & \gamma \end{bmatrix}. \end{aligned}$$

■

Notemos que o Syzygy acima vale sempre, porém incluímos uma ordenação nas letras por conveniência, para aplicarmos nos próximos resultados.

Dada uma tabela

$$M = \begin{bmatrix} \alpha & \beta \\ \alpha & \gamma \\ \vdots & \vdots \\ \delta & \epsilon \end{bmatrix},$$

associaremos a M, a *linha sequência* $\alpha\beta\alpha\gamma...\delta\epsilon$. Definimos então, no conjunto de todas as tabelas de uma mesma altura, uma relação de ordem total dada por: dadas as tabelas M e N, diremos que $M{>}N$ se a linha sequência de M é lexicograficamente maior que a linha sequência de N. Temos então o seguinte Lema:

Lema 1.26. *(O Algoritmo de Ordenação) Qualquer monômio colchete pode ser escrito como uma combinação linear com coeficientes inteiros de monômios colchete padrão.*

Demonstração: Seja M um monômio colchete. Rescrevamos M como uma tabela tal que as linhas são crescentes e a primeira coluna é não-decrescente (notemos que isso sempre é possível). Se a tabela resultante for padrão, acabou. Suponhamos então que a tabela resultante não está na forma padrão. Procuremos na segunda coluna, de cima para baixo, a primeira violação da padronização. Suponhamos que isto ocorre nas i-ésima e $i+1$-ésima linhas. Na tabela, estas duas linhas correspondem a

$$\begin{bmatrix} \vdots & \vdots \\ \alpha & \delta \\ \beta & \gamma \\ \vdots & \vdots \end{bmatrix},$$

onde $\alpha, \beta, \gamma, \delta$ são letras tais que $\alpha < \beta < \gamma < \delta$. Pelo Lema 1.25, nós temos:

$$M = \begin{bmatrix} \vdots & \vdots \\ \alpha & \delta \\ \beta & \gamma \\ \vdots & \vdots \end{bmatrix} = - \begin{bmatrix} \vdots & \vdots \\ \alpha & \beta \\ \gamma & \delta \\ \vdots & \vdots \end{bmatrix} + \begin{bmatrix} \vdots & \vdots \\ \alpha & \gamma \\ \beta & \delta \\ \vdots & \vdots \end{bmatrix}.$$

Com isso, a linha sequência de ambas as tabelas na lado direito são estritamente lexicograficamente menor que a linha sequência de M. Se as duas tabelas estão na forma padrão, acabou. Caso contrário, nós repetiremos o processo em cada tabela que não estiver na forma padrão. Notemos que este processo termina em um número finito de passos, pois, a partir das letras de M, temos apenas um número finito de tabelas de mesma altura. Então, obtemos uma expressão de M como combinação linear, com coeficientes inteiros, de monômios colchete padrão.

■

Como aplicação do Algoritmo de Ordenação, veja Exemplo 1.41.

Lema 1.27. *Os monômios colchete padrão formam um subconjunto linearmente independente em $\mathscr{B}$.*

Demonstração:

Devemos mostrar que qualquer combinação linear de monômios colchete padrão nula, resulta que os escalares são necessariamente nulos. Seja $\sum_{k=1}^{n} c_k M_k = 0$, uma combinação linear nula, onde M_j é um monômio colchete padrão e c_j é

escalar não-nulo, para $j = 1, \ldots, n$, escolhida dentre todas as possíveis relações de dependência linear, com as seguintes propriedades:

(a) o número de letras distintas em cada M_k é o menor possível;

(b) sujeito a (a), a altura máxima de cada M_k é o menor possível.

Sejam δ e ϵ as duas maiores letras ocorrendo nesta relação, com relação à ordem de $\mathscr{A}$. Por (b), o colchete $[\delta \quad \epsilon]$ não é um fator comum a todos os M_k pois caso isso ocorresse, poderíamos reduzir a altura dos M_k. Trocando δ por ϵ, nem todos os monômios colchete se anularão, e estes que não se anularem continuarão padrão, pela escolha de δ e ϵ. Então, nós obtemos uma combinação linear nula, com coeficientes não-nulos, com um número menor de letras distintas, o que contradiz nossa escolha inicial.

■

De posse destes três lemas temos o seguinte teorema:

Teorema 1.28. *Os monômios colchete padrão formam uma base para o espaço dos polinômios colchete.*

Demonstração: Pelo Lema 1.27, resta mostrar que eles geram o espaço dos polinômios colchete. Mas, do Lema 1.26, qualquer monômio colchete pode ser escrito como combinação com coeficientes inteiros de monômios colchete padrão, e consequentemente, qualquer polinômio colchete.

■

Agora, estabeleceremos as bases para decidir quando dois polinômios no espaço umbral tem mesma avaliação umbral. Este resultado será o *Segundo Teorema Fundamental*.

Definição 1.29. *Sejam P um polinômio no espaço umbral e $\mathscr{C}$ o conjunto de letras umbrais gregas ocorrendo em P(não-trivialmente). O polinômio P é irredundante (para formas binárias de grau n) se, para todo monômio N de P e toda letra umbral grega α em $\mathscr{C}$, o grau total das variáveis α_1 e α_2 é n. Caso exista um monômio em P, com uma letra umbral grega γ, para o qual o grau total de γ_1 e γ_2 não é n ou é* 0*, esse monômio (ou P) é redundante.*

Pelo que foi apresentado na seção anterior, todo polinômio homogêneo $I(A_0, A_1, ..., A_n, X, Y)$ pode ser representado umbralmente por um polinômio irredundante. De fato, sendo I homogêneo, temos que cada monômio N de I tem o mesmo grau. Aplicando o que foi feito na Observação 1.15, obtemos que a representação umbral de I será claramente um polinômio irredundante.

Exemplo 1.30. *Tomemos o polinômio* $I(A_0, A_1, X, Y) = A_0^2XY + A_1A_0X^2$. *Uma representação umbral de* I *é* $I = \langle U\,|Q\rangle$, *onde* $Q = -\alpha_2^2\beta_2^2u_1u_2 + \alpha_1\alpha_2\beta_2^2u_2^2$. *Claramente* Q *é um polinômio irredundante.*

Exemplo 1.31. *Como outro exemplo de polinômio irredundante, podemos considerar* $P(\alpha_1, \alpha_2, \beta_1, \beta_2, u_1, u_2) = \alpha_1^2\beta_1\beta_2u_1 + \alpha_2^2\beta_1^2u_2u_1$, *onde* $\mathscr{C} = \{\alpha, \beta\}$. *Temos que* P *é um polinômio irredundante para formas binárias de grau* 2. *Já o polinômio* $P(\alpha_1, \alpha_2, \beta_1, \beta_2, u_1, u_2) = \alpha_1\beta_1\beta_2u_1 + \alpha_2^2\beta_1^2u_2u_1$ *é redundante.*

Nosso próximo resultado estabelecerá quando a avaliação umbral de um polinômio irredundante é identicamente nula. Mas antes disso, temos a seguinte definição e exemplo:

Definição 1.32. *Sejam* P *um polinômio irredundante em* $\mathscr{U}$, $\mathscr{C}$ *o conjunto de letras umbrais gregas que ocorrem em* P *e* $d = \#\mathscr{C}$. *Se* π *é uma permutação de* $\mathscr{C}$, *o polinômio* $\pi(P)$ *é definido como o polinômio obtido de* P, *pela troca de cada letra* γ *por sua imagem* $\pi(\gamma)$, *sob a permutação* π. *A simetrização* $S(P)$ *do polinômio* P *é o polinômio irredundante definido por* $S(P) = \frac{1}{d!}\sum_\pi \pi(P)$, *onde o somatório ocorre sobre todas as permutações* π *de* $\mathscr{C}$. *Se* $P = S(P)$, *dizemos que* P *é um polinômio simetrizado.*

Exemplo 1.33. *Consideremos o polinômio* $P(\alpha_1, \alpha_2, \beta_1, \beta_2, u_1, u_2) = \alpha_1^2\beta_1\beta_2u_1 + \alpha_2^2\beta_2^2$. *Temos que* P *é polinômio irredundante, com* $\mathscr{C} = \{\alpha, \beta\}$, $\#\mathscr{C} = 2$ *e* $\{\pi, Id\}$ *sendo as únicas permutações do conjunto* $\mathscr{C}$, *onde* π *é dada por* $\pi(\alpha) = \beta$ *e* $\pi(\beta) = \alpha$. *Assim,* $S(P) = \frac{1}{2}[(\alpha_1^2\beta_1\beta_2u_1 + \alpha_2^2\beta_2^2) + (\beta_1^2\alpha_1\alpha_2u_1 + \beta_2^2\alpha_2^2)]$. *Se caso tivéssemos* $P(\alpha_1, \alpha_2, \beta_1, \beta_2, u_1, u_2) = \alpha_1\alpha_2\beta_1\beta_2u_1 + \alpha_2^2\beta_2^2$, *teríamos que* $S(P) = P$, *ou seja,* P *já seria um polinômio simetrizado.*

Lema 1.34. *(A Condição de Simetrização) Seja* P *um polinômio irredundante em* $\mathscr{U}$. *Então,* $\langle U\,|P\rangle = 0 \Leftrightarrow S(P) = 0$ *em* $\mathscr{U}$.

Demonstração:

Suponhamos que $\langle U\,|P\rangle = 0$ e vamos mostrar que $S(P) = 0$ em $\mathscr{U}$. Seja $\mathscr{C}$ o conjunto das letras umbral grega que ocorrem em P. Primeiramente, como P é irredundante, temos que P, visto como polinômio em $k[u_1, u_2]$, onde $k = \mathbb{K}[\alpha_1, \alpha_2, ...]$, tem seus coeficientes como uma combinação linear de termos da forma $\prod_{\alpha\in\mathscr{C}} \alpha_1^{e(\alpha)}\alpha_2^{n-e(\alpha)}$ (que por simplicidade escreveremos assim). Portanto, a condição $\langle U\,|P\rangle = 0$, nos diz que $\left\langle U \left| \prod_{\alpha\in\mathscr{C}} \alpha_1^{e(\alpha)}\alpha_2^{n-e(\alpha)} \right.\right\rangle = 0$. Mais ainda, temos que $\left\langle U(F) \left| \prod_{\alpha\in\mathscr{C}} \alpha_1^{e(\alpha)}\alpha_2^{n-e(\alpha)} \right.\right\rangle = 0$, para toda forma binária F de grau n. Como polinômio em $k[u_1, u_2]$, simetrizar P, é o mesmo que simetrizar cada um de

seus coeficientes, portanto, para mostrarmos que $S(P) = 0$, basta mostrarmos que $\sum_\pi(\prod_{\alpha\in\mathscr{C}} \pi(\alpha)_1^{e(\alpha)}\pi(\alpha)_2^{n-e(\alpha)}) = 0$. O que faremos agora é definir uma F conveniente. Seja $F(x,y) = \sum_{\gamma\in\mathscr{C}} \lambda_\gamma(\gamma_1 x - \gamma_2 y)^n$, uma forma binária de grau n, onde os λ_γ, com $\gamma \in \mathscr{C}$, são novas variáveis.

Fazendo a expansão de cada binômio de $F(x,y)$ e rearranjando os termos, obtemos que o coeficiente de cada $x^i y^{n-i}$ é $\sum_{\gamma\in\mathscr{C}} \lambda_\gamma \gamma_1^i \gamma_2^{n-i}$. Aplicando o funcional umbral $U(F)$ e comparando com a expansão acima, obtemos $\left\langle U(F) \left| \alpha_1^i \alpha_2^{n-i} \right.\right\rangle = a_i = \sum_{\gamma\in\mathscr{C}} \lambda_\gamma \gamma_1^i \gamma_2^{n-i}$. Pela lei multiplicativa,

$$\left\langle U(F) \left| \prod_{\alpha\in\mathscr{C}} \alpha_1^{e(\alpha)} \alpha_2^{n-e(\alpha)} \right.\right\rangle = \prod_{\alpha\in\mathscr{C}} (\sum_{\gamma\in\mathscr{C}} \lambda_\gamma \gamma_1^{e(\alpha)} \gamma_2^{n-e(\alpha)}).$$

Agora, vamos expandir o lado direito da expressão anterior e olhá-lo como um polinômio nas variáveis λ_γ. O coeficiente de $\prod_{\gamma\in\mathscr{C}} \lambda_\gamma$ será

$$\sum_\pi (\prod_{\alpha\in\mathscr{C}} \pi(\alpha)_1^{e(\alpha)}\pi(\alpha)_2^{n-e(\alpha)}),$$

onde o somatório ocorre sobre todas as permutações π de $\mathscr{C}$.

Pela definição de simetrização,

$$\sum_\pi (\prod_{\alpha\in\mathscr{C}} \pi(\alpha)_1^{e(\alpha)}\pi(\alpha)_2^{n-e(\alpha)}) = d! S(\prod_{\alpha\in\mathscr{C}} \alpha_1^{e(\alpha)}\alpha_2^{n-e(\alpha)}).$$

Então, como $\langle U \,|P\rangle = 0$, segue que $\langle U(F) \,|P\rangle = 0$, portanto

$$\sum_\pi (\prod_{\alpha\in\mathscr{C}} \pi(\alpha)_1^{e(\alpha)}\pi(\alpha)_2^{n-e(\alpha)}) = 0,$$

e como queríamos, $S(P) = 0$.

Agora, suponhamos que $S(P) = 0$. Sabemos da definição do operador umbral que $\langle U \,|P\rangle = \langle U \,|\pi(P)\rangle$, $\forall$ permutação π de $\mathscr{C}$.

Assim, $d! \langle U \,|S(P)\rangle = \sum_\pi \langle U \,|\pi(P)\rangle = \sum_\pi \langle U \,|P\rangle = d! \langle U \,|P\rangle$, e portanto $\langle U \,|S(P)\rangle = \langle U \,|P\rangle$

Então, se $S(P) = 0$, segue que $\langle U \,|S(P)\rangle = 0 = \langle U \,|P\rangle$. ■

Exemplo 1.35. *Seja $\mathscr{U}$ o operador umbral para as cúbicas binárias. Consideremos o polinômio colchete irredundante $[\alpha \quad \beta]^3$. Como*

$$[\alpha \quad \beta]^3 = -[\beta \quad \alpha]^3,$$

a simetrização $\frac{1}{2}([\alpha \quad \beta]^3 + [\beta \quad \alpha]^3)$ de $[\alpha \quad \beta]^3$ é identicamente zero. Pelo Lema de Simetrização, a a avaliação umbral de $[\alpha \quad \beta]^3$ é também identicamente zero.

Agora já podemos enunciar e demonstrar os teoremas fundamentais.

Teorema 1.36. *(Segundo Teorema Fundamental) Seja U o operador umbral de formas binárias de grau n e sejam P e Q polinômios no espaço umbral $\mathscr{U}$, tais que $\langle U\,|P\rangle = \langle U\,|Q\rangle$. Então, P pode ser obtido de Q por uma sequência de operações dos seguintes quatro tipos:*

I- *uma aplicação de axiomas de $\mathbb{K}$-álgebras em $\mathbb{K}[\alpha_1, \alpha_2, \beta_1, \beta_2, ..., u_1, u_2]$;*

II- *adicionando um múltiplo escalar de um monômio redundante;*

III- *trocando qualquer monômio M por M', onde M' é obtido de M por troca das variáveis α_1 e α_2, para alguma letra umbral grega α ocorrendo em M, pelas variáveis δ_1 e δ_2, onde δ não ocorre em M;*

IV- *trocando qualquer monômio M por $\pi(M)$, onde π é uma permutação do conjunto de letras umbral ocorrendo em M.*

Demonstração: Primeiramente, podemos fazer algumas restrições sobre P e Q, e ainda manter o mesmo grau de generalidade. Podemos considerar que P e Q não possuem nenhum monômio redundante, pois caso contrário, podemos aplicar (II) e eliminar esses monômios redundantes. Além disso, podemos escrever $P = P_1 + P_2 + ... + P_r$, onde cada P_i, é um polinômio, formado por todos os monômios em P que tem a mesma quantidade i de letras umbrais gregas distintas. Analogamente, escrevemos $Q = Q_1 + Q_2 + ... + Q_s$. Observemos que para qualquer monômio M, o grau de $\langle U\,|M\rangle$ visto como polinômio em $\mathbb{K}[\alpha_1, \alpha_2, \beta_1, \beta_2, ..., u_1, u_2]$, é igual ao número de letras umbral grega distintas ocorrendo em M. Então, como temos por hipótese $\langle U\,|P\rangle = \langle U\,|Q\rangle$, vale por igualdade de polinômio que $\langle U\,|P_i\rangle = \langle U\,|Q_i\rangle$, $\forall\ i = 1, ..., r$. Claramente $r = s$. Resumindo, podemos considerar P e Q como sendo polinômios irredundantes, possuindo o mesmo número de letras umbral grega ocorrendo em cada um deles. Mais ainda, podemos aplicar (III), e assumir que as letras umbrais gregas que ocorrem em P são as mesmas que ocorrem em Q.

Agora podemos de fato começar a demonstração. Temos que $\langle U\,|P\rangle = \langle U\,|Q\rangle$, ou seja, $\langle U\,|P - Q\rangle = 0$. Pelo Lema 1.34, a simetrização $S(P - Q) = S(P) - S(Q) = 0$, e portanto, $S(P) = S(Q)$. Agora, basta notarmos que P pode ser obtido de $S(P)$ aplicando (I) e (IV), pela própria definição de simetrização. E o mesmo vale para Q. Portanto, P pode ser obtido de Q, usando-se (I),(II), (III) e (IV). ■

Exemplo 1.37. *Seja U o operador umbral de formas binárias de grau 2 e sejam $P(\alpha_1, \alpha_2, \beta_1\beta_2, \gamma_1, \gamma_2, u_1, u_2) = \gamma_1^2 u_1^2 + \beta_1\beta_2\alpha_1\alpha_2 u_1 u_2$ e $Q(\alpha_1, \alpha_2, \beta_1\beta_2, \gamma_1, \gamma_2, u_1, u_2) = \beta_1^2 u_1^2 + \alpha_1\alpha_2\gamma_1\gamma_2 u_1 u_2$ polinômios no espaço umbral $\mathscr{U}$. Observemos que $\langle U\,|P\rangle =$*

$\langle U\,|Q\rangle = A_2Y^2 - A_1^2XY$. *Vamos agora aplicar o Segundo Teorema Fundamental e mostrar que podemos obter P a partir de Q. No monômio $\beta_1^2u_1^2$, basta trocarmos a variável β_1, pela variável γ_1 que não ocorre nesse monômio, usando (III), ou, podemos usar (II). Para o monômio $\alpha_1\alpha_2\gamma_1\gamma_2u_1u_2$, podemos aplicar novamente (III).*

Exemplo 1.38. *Seja U o operador umbral para formas binárias de grau 3. Sejam,*

$$P(\alpha_1,\alpha_2,\gamma_1,\gamma_2,\omega_1,\omega_2,u_1,u_2) = \alpha_1^3\gamma_1\gamma_2^2u_2^2 - \gamma_1^2\gamma_2\omega_2^3u_1 + \alpha_1\alpha_2^2\omega_1\omega_2^2\gamma_1^3u_1^2u_2$$

e

$$Q(\alpha_1,\alpha_2,\gamma_1,\gamma_2,\omega_1,\omega_2,u_1,u_2) = \gamma_1^3\omega_1\omega_2^2u_2^2 - \omega_1^2\omega_2\gamma_2^3u_1 + \gamma_1\gamma_2^2\omega_1\omega_2^2\alpha_1^3u_1^2u_2,$$

polinômios em U.

Notemos que $\langle U\,|P\rangle = \langle U\,|Q\rangle$. Vamos agora mostrar que podemos obter P a partir de Q, usando o Segundo Teorema Fundamental.

No primeiro monômio $\gamma_1^3\omega_1\omega_2^2u_2^2$, podemos aplicar (III) duas vezes: primeiro trocamos γ_1 por α_1, e depois ω_1, ω_2 por γ_1,γ_2. No segundo monômio $-\omega_1^2\omega_2\gamma_2^3u_1$, não podemos aplicar (III), mas , como esse monômio é redundante, pois a letra α não aparece, podemos somar $\omega_1^2\omega_2\gamma_2^3u_1$ e subtrair $\gamma_1^2\gamma_2\omega_2^3u_1$, que também são redundantes. Já no terceiro monômio, $\gamma_1\gamma_2^2\omega_1\omega_2^2\alpha_1^3u_1^2u_2$, podemos simplesmente trocá-lo por $\pi(\gamma_1\gamma_2^2\omega_1\omega_2^2\alpha_1^3u_1^2u_2)$, usando (IV), onde π troca α por γ, γ por α e mantém ω fixo. Assim, obtemos o resultado desejado.

Teorema 1.39. *(Primeiro Teorema Fundamental) Se P é um polinômio colchete de índice g, então $\langle U\,|P\rangle$ é um covariante de índice g. Reciprocamente, se I é um covariante de índice g de formas binárias de grau n, então $I = \langle U\,|P\rangle$, para algum polinômio colchete P de índice g.*

Demonstração: ($\Rightarrow$) Como o operador umbral é linear, podemos supor que P é um monômio colchete. Pela demonstração da Proposição 1.18, sabemos que

$$\textbf{(1-1)} \qquad det\begin{pmatrix} [\alpha & c] & [\beta & c] \\ [\alpha & d] & [\beta & d] \end{pmatrix} = [c \quad d]\,[\alpha \quad \beta]$$

$$\textbf{(1-2)} \qquad det\begin{pmatrix} [\alpha & c] & [u & c]\,/\,[c & d] \\ [\alpha & d] & [u & d]\,/\,[c & d] \end{pmatrix} = [\alpha \quad u]$$

Seja $f(x,y)$ uma forma binária qualquer e seja (c,d) uma mudança de variáveis qualquer. Pela Proposição 1.18 e pela igualdade (1-1), temos:

$$\left\langle U(\overline{f})\,|[\alpha \quad \beta]\right\rangle \;=\; \left\langle U(\overline{f})\,|\alpha_1\beta_2 - \alpha_2\beta_1\right\rangle$$

$$\begin{aligned} &= \langle U(f)\,|[\alpha \quad c]\,[\beta \quad d] - [\alpha \quad d]\,[\beta \quad c]\rangle \\ &= \left\langle U(f)\left| det\begin{pmatrix} [\alpha & c] & [\beta & c] \\ [\alpha & d] & [\beta & d] \end{pmatrix}\right.\right\rangle \\ &= \langle U(f)\,|[c \quad d]\,[\alpha \quad \beta]\rangle\,. \end{aligned}$$

Analogamente, pela Proposição 1.18 e pela igualdade (1-2) temos:

$$\left\langle U(\overline{f})\,|[\alpha \quad u]\right\rangle = \langle U(f)\,|[\alpha \quad u]\rangle\,.$$

Portanto,

$$\begin{aligned} \left\langle U(\overline{f})\,|P\right\rangle &= \langle U(f)\,|[c \quad d]^g\,P\rangle \\ &= [c \quad d]^g\,\langle U(f)\,|P\rangle\,, \end{aligned}$$

e assim, $\langle U\,|P\rangle$ é um covariante de índice g.

($\Leftarrow$) Como todo covariante pode ser escrito como uma combinação linear de covariantes homogêneos, podemos supor que I é um covariante homogêneo de grau d, ordem t e índice g. Como I é, em particular, um polinômio homogêneo, ele tem uma representação umbral irredundante $I = \langle U\,|P(\alpha_1, \alpha_2, \beta_1, \beta_2, ..., u_1, u_2)\rangle$. Além disso, $\langle U\,|P\rangle = \langle U\,|S(P)\rangle$, então, pelo Segundo Teorema Fundamental podemos assumir que P é um polinômio simetrizado. Além disso, o Segundo Teorema Fundamental nos diz que o resultado independe da escolha que fazemos de P tal que $\langle U\,|P\rangle = I$.

Seja $f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$ uma forma binária de grau n e seja (c,d) uma mudança de variáveis. Como I é covariante e pela Proposição 1.18, temos

$$[c \quad d]^g\,I(a_0, a_1, \dots, a_n, x, y) = I(\overline{a}_0, \overline{a}_1, \dots, \overline{a}_n, \overline{x}, \overline{y}) =$$

$$= \langle U(f)\,|P([\alpha \quad c]\,,[\alpha \quad d]\,,[\beta \quad c]\,,[\beta \quad d]\,,\dots,[u \quad c]\,/\,[c \quad d]\,,[u \quad d]\,/\,[c \quad d])\rangle\,.$$

Para eliminarmos as frações sob o lado direito, vamos multiplicar ambos os lados da igualdade acima por $[c \quad d]^t$, e teremos a igualdade:

(1-3)

$$[c \quad d]^{g+t}\,I(a_0, a_1, \dots, a_n, x, y) =$$

$$= \langle U(f)\,|P([\alpha \quad c]\,,[\alpha \quad d]\,,[\beta \quad c]\,,[\beta \quad d]\,,\dots,[u \quad c]\,,[u \quad d])\rangle\,.$$

Notemos que ao removermos as frações, o polinômio P continua irredundante e simetrizado. Além disso, (1-3) vale para toda mudança de variável (c,d), então poderemos olhar (1-3) como uma igualdade de polinômios das variáveis c_1, c_2, d_1, d_2.

Nosso objetivo agora, será provar que

$$P([\alpha \quad c]\,,[\alpha \quad d]\,,[\beta \quad c]\,,[\beta \quad d]\,,\dots,[u \quad c]\,,[u \quad d]) = [c \quad d]^{g+t}\,Q(\alpha_1, \alpha_2, \dots, u_1, u_2),$$

onde Q é um polinômio colchete de índice g nas variáveis $\alpha_1, \alpha_2, \ldots, u_1, u_2$, não contendo as variáveis c_1, c_2, d_1, d_2. A partir disso, poderemos cancelar o fator $[c \quad d]^{g+t}$ de ambos os lados de (1-3), e obter o resultado desejado.

Sejam $\mathscr{A}^+ = \{c, d, \alpha, \beta, \ldots, \omega, u\}$ um alfabeto, com a ordenação $c < d < \alpha < \beta < \ldots < \omega < u$, e $\mathscr{B}^+$ o espaço dos polinômios colchete nas letras em $\mathscr{A}^+$. Consideremos $P([\alpha \quad c], [\alpha \quad d], [\beta \quad c], [\beta \quad d], \ldots, [u \quad c], [u \quad d])$ como um polinômio em $\mathscr{B}^+$. Pelo Algoritmo de Ordenação, podemos escrever P, como uma combinação linear $\sum b_k M_k$ de monômios colchete padrão distintos em $\mathscr{B}^+$, com $b_k \neq 0$.

Afirmação 1.40. *O polinômio $P(\alpha_1, \alpha_2, \ldots, u_1, u_2)$ pode ser escolhido de tal forma que cada letra, c e d, ocorram exatamente $g+t$ vezes em cada um dos M_k (ou seja, o colchete $[c \quad d]$ ocorre no máximo $g+t$ vezes em cada M_k).*

De fato. Seja w uma nova variável. Temos que

$$[\alpha \quad (wc)] = w\,[\alpha \quad c],$$

para qualquer letra α. Em (1-3), troque c_1 por wc_1 e c_2 por wc_2, e teremos

$$w^{g+t}\,[c \quad d]^{g+t}\, I(a_0, a_1, \ldots, a_n, x, y) = \left\langle U(f) \,\middle|\, \sum b_k w^{c(k)} M_k \right\rangle,$$

onde $c(k)$ é o número de vezes que c ocorre em M_k. Igualando os coeficientes de w^{g+t}, nós obtemos $[c \quad d]^{g+t}\, I(a_0, a_1, \ldots, a_n, x, y) = \langle U(f) \,|\, \sum' b_k M_k \rangle$, onde a linha no somatório indica que os únicos monômios M_k que aparecem são aqueles tais que $c(k) = g + t$. Repita o processo para d e tome a interseção dos índices tais que $c(k) = g + t$ e $d(k) = g + t$. Finalmente, podemos trocar $P(\alpha_1, \alpha_2, \ldots, u_1, u_2)$ pelo polinômio obtido de $\sum' b_k M_k$ fazendo $c_1 = 1$, $c_2 = 0$, $d_1 = 0$, $d_2 = 1$.

Escrevemos então,

$$M_k = [c \quad d]^{l(k)} \begin{bmatrix} c & \alpha \\ \vdots & \vdots \\ c & \beta \\ d & \gamma \\ \vdots & \vdots \end{bmatrix},$$

onde $l(k)$ é o número de colchetes $[c \quad d]$ que aparecem em M_k. Seja $l = min\{l(k)\}$. Direto da Afirmação anterior, sai que $l \leq g + t$.

Temos duas possibilidades. Se $l = g + t$, então $M_k = [c \quad d]^{g+t}\, M'_k$, segue novamente da Afirmação que as letras c e d não aparecem nos M'_k, então tomemos $Q = \sum b_k M'_k$. Suponhamos que $l < g+t$. Podemos escrever $M_k = [c \quad d]^l\, M'_k$ e então, voltar em (1-3), e obtermos $[c \quad d]^{g+t-l}\, I(a_0, a_1, \ldots, a_n, x, y) = \langle U(f) \,|\, \sum b_k M'_k \rangle$, onde

$g+t-l>0$ e existe pelo menos um monômio colchete padrão M'_j que não contem nenhum colchete $[c \quad d]$. Notemos que a igualdade anterior vale para todo c_1, c_2, d_1 e d_2 em $\mathbb{K}$, tais que $[c \quad d] \neq 0$, e portanto, podemos olhá-la como uma igualdade polinomial nestas variáveis. Façamos $c_1 = d_1$ e $c_2 = d_2$ e teremos $\left\langle U(f) \middle| \sum b_k \widehat{M_k} \right\rangle = 0$, onde os $\widehat{M_k}$ são monômios colchete obtidos de M'_k, fazendo $c = d$. Pela ordem estabelecida, após a troca $c = d$, os monômios colchete que restarem continuam padrão, mais ainda, $\sum b_k \widehat{M_k}$ continua simetrizado.

Pela condição de simetrização, $\sum b_k \widehat{M_k} = 0$. Como os monômios colchete padrão são linearmente independentes, conseguiremos um subconjunto de índices E, que contem o índice j (do monômio M'_j que não contem o colchete $[c \quad d]$), tal que $\sum_{k\in E} b_k \widehat{M_k} = 0$ ainda ocorre e $M'_k \neq M'_j$, mas, $\widehat{M_k} = \widehat{M_j}$ $\forall k \in E$. Como $b_j \neq 0$, existe pelo menos outro índice, digamos $m \neq j$ em E. Do fato que $\widehat{M_j}$ é padrão, segue que ele tem a forma

$$\widehat{M_j} = \widehat{M_m} = \begin{bmatrix} c & * \\ c & * \\ \vdots & \vdots \\ c & * \\ * & * \\ * & * \\ \vdots & \vdots \\ * & * \end{bmatrix},$$

onde c aparece como a primeira letra nas $2(g+t-l)$ primeiras linhas, e os $*$ representam letras umbral grega ou romana. Mas, notemos que M'_j e M'_m diferem de $\widehat{M_j}$ e $\widehat{M_m}$ somente pela troca de c por d, e então, pela Afirmação anterior

$$M'_j = M'_m = \begin{bmatrix} c & * \\ \vdots & \vdots \\ c & * \\ d & * \\ \vdots & \vdots \\ d & * \\ * & * \\ \vdots & \vdots \\ * & * \end{bmatrix},$$

onde c aparece como a primeira letra nas $g+t-l$ primeiras linhas, seguido de d aparecendo nas $g+t-l$ linhas seguintes. Isto contradiz $M'_m \neq M'_j$, e portanto $g+t>l$ não ocorre.

■

Exemplo 1.41. *Vamos ver como a demonstração do teorema anterior, nos dá um algoritmo para expressar qualquer covariante como a avaliação umbral de uma combinação linear de monômios colchete padrão. Consideremos o discriminante* $D = A_0A_2 - A_1^2$, *de formas binárias quadráticas. Tomando* $P(\alpha_1, \alpha_2, \beta_1, \beta_2) = \alpha_2^2\beta_1^2 - \alpha_1\alpha_2\beta_1\beta_2$, *temos que* $\langle U\,|P(\alpha_1, \alpha_2, \beta_1, \beta_2)\rangle$ *é uma representação umbral de* D. *Simetrizando* P, *obtemos* $\frac{1}{2}(\alpha_2^2\beta_1^2 + \alpha_1^2\beta_2^2 - 2\alpha_1\alpha_2\beta_1\beta_2)$.

Agora, troquemos α_1 *por* $[\alpha \quad c]$, α_2 *por* $[\alpha \quad d]$, β_1 *por* $[\beta \quad c]$ *e* β_2 *por* $[\beta \quad d]$, *e escrevemos em forma de tabela, assim obtendo:*

$$\frac{1}{2}\left(\begin{bmatrix}\alpha & d\\ \alpha & d\\ \beta & c\\ \beta & c\end{bmatrix} + \begin{bmatrix}\alpha & c\\ \alpha & c\\ \beta & d\\ \beta & d\end{bmatrix} - 2\begin{bmatrix}\alpha & c\\ \alpha & d\\ \beta & c\\ \beta & d\end{bmatrix}\right).$$

Pela ordem das letras, $c < d < \alpha < \beta < \ldots$, *devemos aplicar o Algoritmo de Ordenação para escrevermos cada um desses monômios como uma combinação linear de monômios padrão (na verdade, aplicaremos aqui apenas o Syzygy não olhando para a ordenação, mas sim, para as tabelas que podem ser canceladas, e obteremos assim o mesmo resultado). Além disso, podemos trocar a ordem das linhas, e inverter o colchete, trocando o sinal. Fazendo esses passos, teremos a seguinte sequência de igualdades:*

$$\frac{1}{2}\left(\begin{bmatrix}\alpha & d\\ \alpha & d\\ \beta & c\\ \beta & c\end{bmatrix} + \begin{bmatrix}\alpha & c\\ \alpha & c\\ \beta & d\\ \beta & d\end{bmatrix} - 2\begin{bmatrix}\alpha & c\\ \alpha & d\\ \beta & c\\ \beta & d\end{bmatrix}\right)$$

$$= \frac{1}{2}\left(\begin{bmatrix}\alpha & d\\ \alpha & d\\ \beta & c\\ \beta & c\end{bmatrix} - \begin{bmatrix}\alpha & c\\ \alpha & \beta\\ d & c\\ \beta & d\end{bmatrix} + \begin{bmatrix}\alpha & c\\ \alpha & d\\ \beta & c\\ \beta & d\end{bmatrix} - 2\begin{bmatrix}\alpha & c\\ \alpha & d\\ \beta & c\\ \beta & d\end{bmatrix}\right)$$

$$= \frac{1}{2}\left(\begin{bmatrix}c & \beta\\ c & \beta\\ \alpha & d\\ \alpha & d\end{bmatrix} - \begin{bmatrix}\alpha & c\\ \alpha & \beta\\ d & c\\ \beta & d\end{bmatrix} + \begin{bmatrix}c & \beta\\ \beta & d\\ \alpha & c\\ \alpha & d\end{bmatrix}\right)$$

$$= -\frac{1}{2}\left(\begin{bmatrix}c & \beta\\ c & \alpha\\ d & \beta\\ \alpha & d\end{bmatrix} + \begin{bmatrix}c & \beta\\ c & d\\ \alpha & \beta\\ \alpha & d\end{bmatrix} - \begin{bmatrix}\alpha & c\\ \alpha & \beta\\ d & c\\ \beta & d\end{bmatrix} + \begin{bmatrix}c & \beta\\ \beta & d\\ \alpha & c\\ \alpha & d\end{bmatrix}\right)$$

$$= \frac{1}{2}\left(\left[\begin{array}{cc} c & \beta \\ c & d \\ \alpha & d \\ \alpha & \beta \end{array}\right] - \left[\begin{array}{cc} \alpha & c \\ \alpha & \beta \\ d & c \\ \beta & d \end{array}\right]\right)$$

$$= \frac{1}{2}\left(-\left[\begin{array}{cc} c & d \\ c & \alpha \\ d & \beta \\ \alpha & \beta \end{array}\right] + \left[\begin{array}{cc} c & d \\ c & d \\ \alpha & \beta \\ \alpha & \beta \end{array}\right] - \left[\begin{array}{cc} \alpha & c \\ \alpha & \beta \\ d & c \\ \beta & d \end{array}\right]\right)$$

$$= \frac{1}{2}\left(\left[\begin{array}{cc} c & d \\ c & d \\ \alpha & \beta \\ \alpha & \beta \end{array}\right]\right).$$

Então, podemos escrever o discriminante em termos de polinômios colchete com a seguinte representação umbral:

$$D = \left\langle U|\frac{1}{2}[\alpha \quad \beta]^2 \right\rangle.$$

Observação 1.42. *Diretamente do Primeiro Teorema Fundamental, se P não é um polinômio colchete de índice g, ou em particular não é um monômio colchete, então $\langle U|P\rangle$ não é um covariante. Portanto, o conjunto dos polinômios cuja avaliação umbral é um covariante de índice g, é justamente o espaço $\mathscr{B}_g$, o subespaço do espaço dos polinômio colchete, gerado pelos monômios colchete de índice g.*

Observação 1.43. *Notemos que o Primeiro Teorema Fundamental nos dá um método para encontrarmos exemplos de covariantes de índice g: basta considerarmos um polinômio colchete de índice g e aplicarmos o operador umbral nesse polinômio.*

Exemplo 1.44. *Para exemplificar isso, voltemos ao exemplo 1.9. Nesse exemplo, tínhamos apenas afirmado que I era um covariante, mas agora, isso fica bem claro se considerarmos o polinômio colchete $P = [\alpha \quad \beta][\alpha \quad u][\beta \quad u][\gamma \quad u]^2 - [\alpha \quad \beta][\alpha \quad u][\beta \quad u]$, de índice 1. Temos que $I = \langle U\,|P\rangle$, e portanto I é um covariante de índice 1 de formas binárias de grau 2, pelo Primeiro Teorema Fundamental.*

Observação 1.45. *Um fato interessante que ocorre quando estamos trabalhando com um covariante homogêneo de formas binárias de grau n, é que podemos obter uma expressão para o seu índice, a partir de seu grau, de sua ordem e de n, além de outras relações. Vejamos como isso ocorre.*

Seja I um covariante homogêneo de grau d, ordem t e índice g de formas binárias de grau n. Seja $I = \langle U\,|\sum b_k M_k\rangle$, uma representação umbral irredundante

de I, por uma combinação linear de monômios colchete, garantida pelo Primeiro Teorema Fundamental. Como é uma representação irredundante, o índice e a ordem de cada M_k é o mesmo de I. Então, todo M_k tem mesma altura $h = g+t$. Notemos que d é o número de letras umbrais gregas em cada M_k (e as mesmas em cada M_k). Como cada colchete tem duas letras, cada letra grega ocorre n vezes e a letra u ocorre t vezes, então $dn = 2g+t$, e em particular, $g = \frac{1}{2}(dn-t)$. Além disso, como $h = g+t$, segue que $2h = dn+t$.

Podemos ainda escrever o Primeiro e Segundo Teorema Fundamental, como o seguinte teorema:

Teorema 1.46. *Seja $\mathscr{I}[n,d,t]$ o espaço vetorial (de dimensão finita) dos covariantes homogêneos de formas binárias de grau n, com grau d, ordem t e índice g, onde $g = \frac{1}{2}(dn-t)$. Seja $\mathscr{U}[n,d,t]$ o subespaço do espaço $\mathscr{B}$ dos polinômios colchete gerados pelos monômios colchete de altura $g+t$ formado com d letras umbrais gregas distintas, cada uma ocorrendo n vezes e a letra romana u ocorrendo t vezes. Finalmente, seja $\mathscr{U}^S[n,d,t]$ o espaço dos polinômios simetrizados em $\mathscr{U}[n,d,t]$. Então*

$$\mathscr{U}^S[n,d,t] \cong \mathscr{I}[n,d,t],$$

onde o isomorfismo é dado pelo operador umbral U de formas binárias de grau n.

Capítulo 2

Covariantes e Raízes.

Nosso objetivo aqui é estudar a álgebra de raízes homogeneizadas e sua relação com o espaço dos covariantes homogêneos. Na primeira seção deste capítulo, daremos as definições básicas e veremos quando um polinômio na álgebra de raízes homogeneizadas é escrito nas funções simétricas elementares. Na segunda seção, descreveremos um algoritmo para calcular a representação de um covariante em termos de raízes homogeneizadas. E finalmente, na seção três, apresentaremos resultados importantes para a demonstração do Teorema de Finitude.

2.1 A Álgebra de Raízes homogeneizadas.

A partir de agora, consideraremos $\mathbb{K}$ um corpo algebricamente fechado.

Seja $f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$, uma forma binária de grau n. Suponha que $a_n \neq 0$. Sejam $\lambda_1, \lambda_2, \dots, \lambda_n$, as raízes do polinômio $f(x,1)$. Podemos escrever $f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k} = a_n(x-\lambda_1 y)(x-\lambda_2 y)...(x-\lambda_n y)$. Expandindo o lado esquerdo da igualdade, e igualando os coeficientes dos polinômios, obtemos:

(2-1) $$\binom{n}{k} a_{n-k} = (-1)^k a_n e_k(\lambda_1, \dots, \lambda_n) = (-1)^k a_n \sum \lambda_{i_1} ... \lambda_{i_k},$$

onde a soma ocorre sobre todo subconjunto de $\{1, 2, \dots, n\}$ com k elementos. Podemos ainda escrever (2-1) da seguinte forma:

(2-2) $$a_{n-k} = (-1)^k \frac{a_n}{n!} k!(n-k)! \sum \lambda_{i_1} ... \lambda_{i_k} = (-1)^k \frac{a_n}{n!} \sum_{\pi} \lambda_{\pi(1)} ... \lambda_{\pi(k)},$$

onde a soma ocorre sobre todas as permutações π de $\{1, 2, \dots, n\}$.

A última igualdade em (2-2), sai do fato que dado qualquer subconjunto com k elementos de $\{1, 2, \dots, n\}$, existem $k!(n-k)!$ permutações π, tais que $\pi(S) = S$. As funções $e_k(\lambda_1, \dots, \lambda_n)$, são as k-ésimas funções simétricas elementares.

A *álgebra de raízes*, é o anel $\mathbb{K}[a_n, \lambda_1, \dots, \lambda_n, x, y]$, de todos os polinômios nas variáveis $a_n, \lambda_1, \dots, \lambda_n, x$ e y.

Definição 2.1. *Definimos o homomorfismo de álgebras*

$$r : \mathbb{K}[A_0, A_1, ..., A_n, X, Y] \longrightarrow \mathbb{K}[a_n, \lambda_1, ..., \lambda_n, x, y]$$

pelas regras:

$$\begin{aligned} A_n &\longmapsto a_n \\ A_{n-k} &\longmapsto (-1)^k \frac{a_n}{n!} \sum_{\pi} \lambda_{\pi(1)} ... \lambda_{\pi(k)} \\ X &\longmapsto x \\ Y &\longmapsto y \end{aligned}$$

Se $I(A_0, A_1, ..., A_n, X, Y)$ é um polinômio, a imagem de I sob r é chamado de representação de I em termos das raízes.

Para raízes homogeneizadas, podemos seguir a mesma linha de raciocínio.

Seja $f(x, y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$ um forma binária de grau n. Podemos expandi-la, não univocamente, como o produto de n formas lineares:

$$f(x, y) = (\mu_1 x - \nu_1 y)(\mu_2 x - \nu_2 y)...(\mu_n x - \nu_n y),$$

onde μ_i, ν_i, são chamados *raízes homogeneizadas de* $f(x, y)$. Analogamente, podemos expandir a expressão acima e igualar os coeficientes, obtendo:

$$\begin{aligned} a_{n-k} &= \frac{(-1)^k}{n!} \sum_{\pi} \nu_{\pi(1)} ... \nu_{\pi(k)} \mu_{\pi(k+1)} ... \mu_{\pi(n)} \\ &= \frac{(-1)^k}{n!} \mu_1 ... \mu_n e_k(\frac{\nu_1}{\mu_1}, ..., \frac{\nu_n}{\mu_n}), \end{aligned}$$

onde a soma ocorre sobre todas as permutações π de $\{1, 2, ..., n\}$.

Definimos também, a *álgebra de raízes homogeneizadas* como sendo o anel $\mathbb{K}[\mu_1, ..., \mu_n, \nu_1, ..., \nu_n, x, y]$, de todos os polinômios nas variáveis μ_1, ... , μ_n, ν_1, ... , ν_n, x e y.

Definição 2.2. *Definimos o homomorfismo de álgebras*

$$h : \mathbb{K}[A_0, A_1, ..., A_n, X, Y] \longrightarrow \mathbb{K}[\mu_1, ..., \mu_n, \nu_1, ..., \nu_n, x, y]$$

pelas regras:

$$\begin{aligned} A_{n-k} &\longmapsto \frac{(-1)^k}{n!} \sum_{\pi} \nu_{\pi(1)} ... \nu_{\pi(k)} \mu_{\pi(k+1)} ... \mu_{\pi(n)} \\ X &\longmapsto x \\ Y &\longmapsto y \end{aligned}$$

Se $I(A_0, A_1, ..., A_n, X, Y)$ é um polinômio, a imagem de I sob h é chamado de representação de I em termos das raízes homogeneizadas.

Definição 2.3. *Seja* $M = \mu_1^{a_1}\mu_1^{a_2}...\mu_n^{a_n}\nu_1^{b_1}\nu_2^{b_2}...\nu_n^{b_n}x^{c_1}y^{c_2}$, *um monômio nas raízes homogeneizadas. Definimos a multiplicidade* m_i *de* i *em* M, *como* $m_i = a_i + b_i$, *para* $i = 1, ..., n$. *Além disso,* M *é regular de grau* d, *se* $m_1 = m_2 = ... = m_n = d$. *Um polinômio nas raízes homogeneizadas é regular de grau* d, *se todo monômio nele é regular de mesmo grau* d.

Denotaremos simplesmente por $R(\mu_i, \nu_i, x, y)$, um elemento da álgebra de raízes homogeneizadas.

Definição 2.4. *Um polinômio* $R(\mu_i, \nu_i, x, y)$ *na álgebra de raízes homogeneizadas é mutuamente simétrico, quando, para toda permutação* π *de* $\{1, 2, ..., n\}$ *vale* $R(\mu_i, \nu_i, x, y) = R(\mu_{\pi(i)}, \nu_{\pi(i)}, x, y)$.

Exemplo 2.5. *Consideremos* $S = \{1, 2, ..., n\}$. *Então, as funções (chamadas de funções simétricas elementares) definidas por*

$$a_k(\mu_i, \nu_i) = \frac{1}{n!}\sum_{\pi} \nu_{\pi(1)}...\nu_{\pi(k)}\mu_{\pi(k+1)}...\mu_{\pi(n)},$$

onde a soma ocorre sobre todas as permutações π *de* S, *são mutuamente simétricas, e mais, são também regulares.*

Veremos agora, que sob certas hipóteses, podemos escrever um polinômio em $\mathbb{K}[\mu_1, ..., \mu_n, \nu_1, ..., \nu_n, x, y]$, em termos das funções simétricas homogeneizadas, ou seja, em termos de $A_0, ..., A_n$ em $\mathbb{K}[A_0, A_1, ..., A_n, X, Y]$.

Proposição 2.6. *Seja* $R(\mu_i, \nu_i, x, y)$ *um polinômio na álgebra de raízes homogeneizadas. Então,* R *é expresso como um polinômio nas funções simétricas homogeneizadas*

$$a_k(\mu_i, \nu_i) = \frac{1}{n!}\sum_{\pi} \nu_{\pi(1)}...\nu_{\pi(k)}\mu_{\pi(k+1)}...\mu_{\pi(n)},$$

(com coeficientes na álgebra $\mathbb{K}[x, y]$*) se, e somente se,* R *é regular e mutuamente simétrico em* μ_i *e* ν_i.

Demonstração: ($\Rightarrow$) Notemos que cada $a_k(\mu_i, \nu_i)$ é mutuamente simétrico e regular pelo exemplo anterior. Além disso, essas propriedade são preservadas sob multiplicação (por elementos de $\mathbb{K}[x, y]$), e a regularidade se mantém na soma, pois em cada a_k o grau de regularidade é o mesmo, pela definição dos a_k. Portanto, R é mutuamente simétrico e regular.

($\Leftarrow$) Seja R regular de grau d. Então, podemos escrever R da seguinte forma:

$$R(\mu_i, \nu_i, x, y) = (\mu_1, ..., \mu_n)^d \widehat{R}(\nu_i/\mu_i, x, y),$$

onde $\widehat{R}$ é um polinômio simétrico nas variáveis $\lambda_i = \nu_i/\mu_i$. Pelo Teorema Fundamental de Funções Simétricas (ver [9]), nós podemos escrever $\widehat{R}$ como um polinômio Q, com coeficientes em $\mathbb{K}[x, y]$, nas funções simétricas elementares $e_k(\nu_i/\mu_i)$. Multiplicando Q por $(\mu_1, \dots, \mu_n)^d$ e distribuindo esses fatores sobre cada função elementar $e_k(\nu_i/\mu_i)$, nós obtemos uma expressão de R em termos das funções simétricas homogeneizadas, como queríamos.

■

2.2 O Algoritmo

Sejam P um polinômio colchete no espaço umbral $\mathscr{U}$ e U o operador umbral para formas binárias de grau n. Então, $h(\langle U\,|P\rangle)$ é um polinômio na álgebra de raízes homogeneizadas. Nossa atenção estará voltada agora, em descrever a função composta $h \circ U$. Nesta seção, apresentaremos o algoritmo que calcula essa representação, e demonstraremos que de fato esse algoritmo funciona. Além disso, vários exemplos serão apresentados no decorrer desta seção.

Algoritmo 2.7. *Sejam T um monômio colchete no espaço umbral $\mathscr{U}$, U o operador umbral de formas binárias de grau n, $\mathscr{A}$ o conjunto de todas letras umbrais gregas que aparecem em T e d a cardinalidade de $\mathscr{A}$. Nós assumiremos que toda letra em $\mathscr{A}$ ocorre exatamente n vezes em T. Caso contrário, $h(\langle U\,|T\rangle) = 0$ e o algoritmo termina.*

Passo 1: Escrevemos T como uma tabela, em alguma ordem fixa:

$$T = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \\ \vdots & \vdots \\ \omega & u \end{bmatrix}$$

Agora, construiremos uma nova tabela a partir dessa particular tabela de T, da seguinte forma: seja α uma letra umbral grega em $\mathscr{A}$. Façamos uma varredura na tabela, começando pela primeira coluna, de cima para baixo, e em seguida repetimos o processo para a segunda coluna, substituindo, a i-ésima ocorrência de α pelo inteiro i. Repetimos esse processo para cada letra umbral em $\mathscr{A}$. Obtemos então, uma tabela $\widehat{T}$, cujas entradas são inteiros do conjunto $\{1, ..., n\}$. Em seguida, coloquemos as tabelas T e $\widehat{T}$, lado a lado,

formando a chamada *tabela dupla*:

$$\left[\begin{array}{cc|cc} \alpha & \beta & i & j \\ \gamma & \delta & k & l \\ \vdots & \vdots & \vdots & \vdots \\ \omega & u & p & u \end{array}\right].$$

Passo 2: Seja Φ, uma função de $\mathscr{A}$ para o conjunto de todas as permutações sobre $\{1, 2, ..., n\}$. Definimos a tabela dupla

$$T[\Phi] = \left[\begin{array}{cc|cc} \alpha & \beta & \Phi(\alpha, i) & \Phi(\beta, j) \\ \gamma & \delta & \Phi(\gamma, k) & \Phi(\delta, l) \\ \vdots & \vdots & \vdots & \vdots \\ \omega & u & \Phi(\omega, p) & u \end{array}\right],$$

onde $\Phi(\alpha, i)$ é a imagem do inteiro i pela permutação $\Phi(\alpha)$.

Passo 3: Consideremos a tabela dupla

$$T[\Phi] = \left[\begin{array}{cc|cc} \alpha & \beta & i' & j' \\ \gamma & \delta & k' & l' \\ \vdots & \vdots & \vdots & \vdots \\ \omega & u & p' & u \end{array}\right].$$

Procederemos agora da seguinte forma: para a linha $[\alpha \quad \beta \,|\, i \quad j]$ na tabela $T[\Phi]$, associamos o polinômio $(\mu_i\nu_j - \nu_i\mu_j)$ nas raízes homogeneizadas, e para a linha $[\alpha \quad u \,|\, i \quad u]$, o polinômio $(\mu_i x - \nu_i y)$, para cada $i, j \in \{1, 2, ..., n\}$ e $\alpha, \beta \in \mathscr{A}$. Os polinômios $(\mu_i\nu_j - \nu_i\mu_j)$ e $(\mu_i x - \nu_i y)$ são chamados de *diferenças*. Construamos agora o polinômio

$$T^h[\Phi] = (\mu_{i'}\nu_{j'} - \nu_{i'}\mu_{j'})(\mu_{k'}\nu_{l'} - \nu_{k'}\mu_{l'})...(\mu_{p'}x - \nu_{p'}y),$$

que é o produto de todas as diferenças, assim obtidas.

Passo 4: Coloquemos

$$h(\langle U\,|T\rangle) = \frac{(-1)^g}{(n!)^d} \sum_{\Phi} T^h[\Phi],$$

onde a soma ocorre sobre todas as funções Φ do conjunto de letras umbral grega $\mathscr{A}$ no conjunto Ω_n das permutações de $\{1, 2, ..., n\}$, e g é o índice do covariante $\langle U\,|T\rangle$, que é o número de colchetes em T não contendo a letra romana u e d é a cardinalidade de $\mathscr{A}$.

■

Notemos que de fato esse algoritmo nos dará a representação de $\langle U\,|T\rangle$, em termos de raízes homogeneizadas, e este será nosso próximo resultado. Mas antes disso, veremos um exemplo utilizando os passos do algoritmo e alguns resultados que serão utilizados na demonstração do principal teorema desta seção.

Exemplo 2.8. *Seja $D = A_0A_2 - A_1^2$ o discriminante de uma forma quadrática binária. Sabemos que D é um invariante. Pelo que já vimos, uma representação umbral de D é $\frac{1}{2}[\alpha \quad \beta]^2$. Temos que $\mathscr{A} = \{\alpha, \beta\}$ e tem cardinalidade 2. Pelo Passo 1 do Algoritmo 2.7, temos apenas uma tabela dupla:*

$$\frac{1}{2}\left[\begin{array}{cc|cc} \alpha & \beta & 1 & 1 \\ \alpha & \beta & 2 & 2 \end{array}\right].$$

Olhando para o passo 2: observemos que $\mathscr{A} = \{\alpha, \beta\}$ e $\Omega_2 = \{id, \pi\}$, onde id é a identidade, e π leva $1 \to 2$ e $2 \to 1$. Então, temos apenas quatro funções de $\mathscr{A}$ em Ω_2 : Φ_1 que leva α na id e β em π, Φ_2 que leva α em π e β na id, Φ_3 que leva ambas na id e finalmente Φ_4, que leva ambas em π. Temos então as tabelas:

$$\begin{array}{cc} \frac{1}{2}\left[\begin{array}{cc|cc} \alpha & \beta & 1 & 1 \\ \alpha & \beta & 2 & 2 \end{array}\right], & \frac{1}{2}\left[\begin{array}{cc|cc} \alpha & \beta & 1 & 2 \\ \alpha & \beta & 2 & 1 \end{array}\right], \\ \frac{1}{2}\left[\begin{array}{cc|cc} \alpha & \beta & 2 & 1 \\ \alpha & \beta & 1 & 2 \end{array}\right], & \frac{1}{2}\left[\begin{array}{cc|cc} \alpha & \beta & 2 & 2 \\ \alpha & \beta & 1 & 1 \end{array}\right]. \end{array}$$

Agora, pelo Passo 3 do algoritmo, temos os seguintes polinômios diferença, respectivamente:

$$0,\ \frac{1}{2}(\mu_1\nu_2 - \nu_1\mu_2)(\mu_2\nu_1 - \nu_2\mu_1),\ \frac{1}{2}(\mu_2\nu_1 - \nu_2\mu_1)(\mu_1\nu_2 - \nu_1\mu_2),\ 0;$$

que na verdade, são apenas:

$$-\frac{1}{2}(\mu_1\nu_2 - \nu_1\mu_2)^2,\ -\frac{1}{2}(\mu_1\nu_2 - \nu_1\mu_2)^2.$$

Finalmente, como $g = d = n = 2$, pelo Passo 4, temos que a representação do discriminante de formas binárias quadráticas, em termos de raízes homogeneizadas é:

$$h(D) = h(\langle U\,|1/2[\alpha \quad \beta]^2\rangle) = -\frac{1}{4}(\mu_1\nu_2 - \nu_1\mu_2)^2.$$

A partir de agora, tudo que fizermos nesta seção será somente para demonstrarmos o Teorema 2.18.

Definição 2.9. *Seja m o número de linhas no monômio colchete T. Rotulemos as linhas em T pelos inteiros $\{1, 2, ..., m\}$. Para cada letra umbral grega γ, ocorrendo*

em T, e cada subconjunto Z de $\{1,2,...,m\}$, definimos os subconjuntos de linhas rotuladas

$$E_1(\gamma,Z)=\{i: i\in Z \text{ e } \gamma \text{ é a primeira letra na } i\text{-ésima linha}\},$$
$$\overline{E}_1(\gamma,Z)=\{i: i\notin Z \text{ e } \gamma \text{ é a segunda letra na } i\text{-ésima linha}\},$$
$$E_2(\gamma,Z)=\{i: i\in Z \text{ e } \gamma \text{ é a segunda letra na } i\text{-ésima linha}\},$$
$$\overline{E}_2(\gamma,Z)=\{i: i\notin Z \text{ e } \gamma \text{ é a primeira letra na } i\text{-ésima linha}\},$$

e definimos também

$$e_1(\gamma,Z)=|E_1(\gamma,Z)|+|\overline{E}_1(\gamma,Z)|,$$
$$e_2(\gamma,Z)=|E_2(\gamma,Z)|+|\overline{E}_2(\gamma,Z)|.$$

Aqui, $|.|$ representa a cardinalidade de um conjunto.

Por hipótese, cada letra umbral grega γ, ocorre n vezes em T, então

$$e_1(\gamma,Z)+e_2(\gamma,Z)=n.$$

Analogamente, definimos os conjuntos $E_1(u,Z)$, $\overline{E}_1(u,Z)$, $E_2(u,Z)$ e $\overline{E}_2(u,Z)$, e os números $e_1(u,Z)$ e $e_2(u,Z)$.

Lema 2.10. *Como um polinômio nas variáveis γ_1, γ_2, u_1, u_2, com $\gamma\in\mathscr{A}$, a tabela T pode ser expandida como*

(2-3) $\qquad T=\sum_Z(-1)^{m-|Z|}M(Z),$

onde

$$M(Z)=\left(\prod_{\gamma\in\mathscr{A}}\gamma_1^{e_1(\gamma,Z)}\gamma_2^{e_2(\gamma,Z)}\right)u_1^{e_1(u,Z)}u_2^{e_2(u,Z)},$$

e a soma ocorre sobre todos os subconjuntos Z do conjunto das linhas rotuladas $\{1,2,\dots,m\}$.

Demonstração: Podemos olhar para a tabela T, como um polinômio nas variáveis $\gamma_1,\gamma_2,\dots,u_1,u_2$, e assim, teremos que T é o produto

$$\prod_{i=1}^{m}(A_i-B_i)=\sum_Z(-1)^{m-|Z|}\prod_{i\in Z}A_i\prod_{j\notin Z}B_j,$$

onde a soma ocorre sobre todo subconjunto Z de $\{1,2,\dots,m\}$ e o termo A_i-B_i representa a expansão do colchete da i-ésima linha de T. Tomemos esse i-ésimo termo, digamos $[\gamma \quad \delta]$, e teremos que $A_i=\gamma_1\delta_2$ e $B_i=\gamma_2\delta_1$. Vamos então olhar para cada um dos termos da igualdade acima. Temos que:

$$\textstyle\prod_{i\in Z}A_i=\left(\prod_\gamma\gamma_1^{p(\gamma)}\gamma_2^{q(\gamma)}\right)u_1^{p(u)}u_2^{q(u)},$$
$$\textstyle\prod_{j\notin Z}B_j=\left(\prod_\gamma\gamma_1^{r(\gamma)}\gamma_2^{s(\gamma)}\right)u_1^{r(u)}u_2^{s(u)},$$

onde, o segundo produto ocorre sobre todos os γ no conjunto $\mathscr{A}$ em ambas as igualdade, e $p(\gamma) = |E_1(\gamma, Z)|$, $q(\gamma) = |E_2(\gamma, Z)|$, $r(\gamma) = |\overline{E}_1(\gamma, Z)|$ e $s(\gamma) = |\overline{E}_2(\gamma, Z)|$. Como $p(\gamma) + r(\gamma) = e_1(\gamma, Z)$ e $q(\gamma) + s(\gamma) = e_2(\gamma, Z)$(analogamente para u), temos

$$\prod_{i\in Z} A_i \prod_{j\notin Z} B_j = \left(\prod_{\gamma\in\mathscr{A}} \gamma_1^{e_1(\gamma,Z)}\gamma_2^{e_2(\gamma,Z)}\right) u_1^{e_1(u,Z)}u_2^{e_2(u,Z)}.$$

Portanto:

$$T = \sum_Z (-1)^{m-|Z|} \prod_{i\in Z} A_i \prod_{j\notin Z} B_j = \left(\prod_{\gamma\in\mathscr{A}} \gamma_1^{e_1(\gamma,Z)}\gamma_2^{e_2(\gamma,Z)}\right) u_1^{e_1(u,Z)}u_2^{e_2(u,Z)}.$$

■

Exemplo 2.11. *Seja*

$$T = \begin{bmatrix} \alpha & \beta \\ \alpha & u \\ \beta & u \end{bmatrix}.$$

A partir de T temos que: $\mathscr{A} = \{\alpha, \beta\}$, $n = 2$, $m = 3$ e $Z \subseteq \{1, 2, 3\}$. Vamos então, seguindo o Lema anterior, expandir T nas variáveis γ_1, γ_2, u_1 e u_2, onde $\gamma \subseteq \mathscr{A}$. Para isso, vamos ver qual a expressão de cada $M(Z)$.

- $Z = \{1\}$. *Temos:*

  $e_1(\alpha, Z) = 1 \quad e_2(\alpha, Z) = 1$
  $e_1(\beta, Z) = 0 \quad e_2(\beta, Z) = 2$
  $e_1(u, Z) = 2 \quad e_2(u, Z) = 0.$

  Então, $M(Z) = \alpha_1\alpha_2\beta_2^2u_1^2$.

- $Z = \{2\}$. *Temos,* $M(Z) = \alpha_1\alpha_2\beta_1\beta_2u_1u_2$.

- $Z = \{3\}$. *Temos,* $M(Z) = \alpha_2^2\beta_1^2u_1u_2$.

- $Z = \{1, 2\}$. *Temos,* $M(Z) = \alpha_1^2\beta_2^2u_1u_2$.

- $Z = \{1, 3\}$. *Temos,* $M(Z) = \alpha_1\alpha_2\beta_1\beta_2u_1u_2$.

- $Z = \{2, 3\}$. *Temos,* $M(Z) = \alpha_1\alpha_2\beta_1^2u_2^2$.

- $Z = \{1, 2, 3\}$. *Temos,* $M(Z) = \alpha_1^2\beta_1\beta_2u_2^2$.

Substituindo em T, obtemos:

$$\begin{aligned} T &= (-1)^2\alpha_1\alpha_2\beta_2^2u_1^2 + (-1)^2\alpha_1\alpha_2\beta_1\beta_2u_1u_2 + (-1)^2\alpha_2^2\beta_1^2u_1u_2 \\ &\quad +(-1)\alpha_1^2\beta_2^2u_1u_2 + (-1)\alpha_1\alpha_2\beta_1\beta_2u_1u_2 + (-1)\alpha_1\alpha_2\beta_1^2u_2^2 + (-1)^0\alpha_1^2\beta_1\beta_2u_2^2 \\ &= \alpha_1\alpha_2\beta_2^2u_1^2 + \alpha_1\alpha_2\beta_1\beta_2u_1u_2 + \alpha_2^2\beta_1^2u_1u_2 \\ &\quad -\alpha_1^2\beta_2^2u_1u_2 - \alpha_1\alpha_2\beta_1\beta_2u_1u_2 - \alpha_1\alpha_2\beta_1^2u_2^2 + \alpha_1^2\beta_1\beta_2u_2^2 \end{aligned}$$

Notemos que expandindo T do modo usual, obteremos a mesma expressão acima, que é dada pelo Lema anterior.

Lema 2.12. *$e_2(\alpha, Z) + e_2(\beta, Z) + ... + e_2(\omega, Z) + e_2(u, Z) = m$, onde m é o número de colchetes em T e $\alpha, \beta, ..., \omega$ são todas as letras de $\mathscr{A}$ (o conjunto das letras gregas que aparecem em T) e $Z \subseteq \{1, 2, ..., m\}$ qualquer.*

Demonstração: Primeiramente, notemos que os $E_2(\gamma, Z)$ são dois a dois disjuntos pela própria definição desse conjunto e pelas letras em $\mathscr{A}$ serem duas a duas não equivalentes. Então, basta mostrarmos que

$$E_2(\alpha, Z) \cup E_2(\beta, Z) \cup ... \cup E_2(\omega, Z) \cup E_2(u, Z) = \{1, 2, ..., m\}.$$

Notemos ainda que a inclusão

$$E_2(\alpha, Z) \cup E_2(\beta, Z) \cup ... \cup E_2(\omega, Z) \cup E_2(u, Z) \subseteq \{1, 2, ..., m\},$$

é direta da definição dos conjuntos $E_2(\gamma, Z)$. Para a outra inclusão, seja $i \subseteq \{1, 2, ..., m\}$. Se $i \in Z$, então por definição, $i \in E_2(\gamma, Z)$, e portanto γ é a segunda letra no colchete da i-ésima linha. Se $i \notin Z$, então $i \notin E_2(\gamma, Z)$, mas existe uma letra γ', tal que $i \in E_2(\gamma', Z)$, onde γ' é a primeira letra na i-ésima linha. Portanto, $i \in \{1, 2, ..., m\}$ e o resultado segue.

■

Exemplo 2.13. *Para verificarmos de perto o Lema 2.12, podemos voltar no exemplo anterior. Nele, facilmente vemos que $e_2(\alpha, Z) + e_2(\beta, Z) = 3$, para todo subconjunto $Z \subseteq \{1, 2, 3\}$. Além disso, os passos da demonstração desse Lema podem ser verificados nesse exemplo.*

Definição 2.14. *Seja $\widehat{T}$, a tabela de inteiros construída a partir de T, no Passo 1, do Algoritmo 2.7. Seja $Z \subseteq \{1, 2, ..., m\}$. Definimos então $D_1(\gamma, Z) = \{j : j$ está na primeira entrada na i-ésima linha de $\widehat{T}$, para algum $i \in E_1(\gamma, Z)\}$, ou seja, $D_1(\gamma, Z)$ pode ser construído listando-se todas as linhas de $\widehat{T}$, cujas linhas rotuladas estão em $E_1(\gamma, Z)$, e em seguida, extraímos a primeira entrada de cada linha.*

Notemos que $D_1(\gamma, Z)$ é um subconjunto de $\{1, 2, \dots, m\}$. Analogamente, definimos os conjuntos

$$\begin{aligned}
\overline{D}_1(\gamma, Z) &= \{j : j \text{ está na segunda entrada na } i\text{-ésima linha de } \widehat{T}, \text{ para algum } i \in \overline{E}_1(\gamma, Z)\},\\
D_2(\gamma, Z) &= \{j : j \text{ está na segunda entrada na } i\text{-ésima linha de } \widehat{T}, \text{ para algum } i \in E_2(\gamma, Z)\},\\
\overline{D}_2(\gamma, Z) &= \{j : j \text{ está na primeira entrada na } i\text{-ésima linha de } \widehat{T}, \text{ para algum } i \in \overline{E}_2(\gamma, Z)\}.
\end{aligned}$$

Observação 2.15. *Direto da definição acima, obtemos que: $|D_1(\gamma, Z) \cup \overline{D}_1(\gamma, Z)| = e_1(\gamma, Z)$ e $|D_2(\gamma, Z) \cup \overline{D}_2(\gamma, Z)| = e_2(\gamma, Z)$.*

Exemplo 2.16. *Para esse exemplo, vamos usar a tabela T do Exemplo 2.11. Segundo o primeiro passo do Algoritmo 2.7, temos*

$$\widehat{T} = \begin{bmatrix} 1 & 2 \\ 2 & u \\ 1 & u \end{bmatrix}$$

Então, se $Z = \{1, 2\} \subseteq \{1, 2, 3\}$ e $\alpha \in \mathscr{A}$ temos:

$$\begin{aligned}
D_1(\alpha, Z) &= \{1, 2\}\\
\overline{D}_1(\alpha, Z) &= \emptyset\\
D_2(\alpha, Z) &= \emptyset\\
\overline{D}_2(\alpha, Z) &= \emptyset \quad .
\end{aligned}$$

Além disso,

$$\begin{aligned}
|D_1(\alpha, Z) \cup \overline{D}_1(\alpha, Z)| &= 2 = e_1(\alpha, Z),\\
|D_2(\alpha, Z) \cup \overline{D}_2(\alpha, Z)| &= 0 = e_2(\alpha, Z).
\end{aligned}$$

Lema 2.17. *Seja Φ uma função de $\mathscr{A}$ para o conjunto das permutações sobre $\{1, 2, \dots, n\}$. Como um polinômio em μ_i, ν_i, x e y,*

(2-4)

$$\begin{aligned}
T^h[\Phi] &= \sum_Z (-1)^{m-|Z|} \left[\prod_{\gamma \in \mathscr{A}} \left(\prod_{i \in D_1(\gamma, Z) \cup \overline{D}_1(\gamma, Z)} \mu_{\Phi(\gamma, i)} \right.\right.\\
&\quad \left.\left. \times \prod_{j \in D_2(\gamma, Z) \cup \overline{D}_2(\gamma, Z)} \nu_{\Phi(\gamma, j)} \right) \right] x^{e_2(u, Z)} y^{e_1(u, Z)},
\end{aligned}$$

onde a soma ocorre sobre todos os subconjuntos Z de $\{1, 2, \ldots, m\}$.

Demonstração: Seguiremos as ideias da demonstração do Lema 2.10. Vamos olhar $T^h[\Phi]$, como um polinômio nas variáveis μ_i, ν_i, x e y, na forma

$$\prod_{i=1}^{m}(A_i - B_i) = \sum_{Z}(-1)^{m-|Z|}\prod_{i\in Z}A_i\prod_{j\notin Z}B_j.$$

Porém, olharemos o fator $A_i - B_i$ como a troca do colchete duplo da i-ésima linha de $T^h[\Phi]$ pelo polinômio diferença correspondente, segundo o Passo 3, do algoritmo anterior. Se olharmos a i-ésima linha como sendo $[\gamma \quad \delta|\Phi(\gamma,p) \quad \Phi(\delta,q)]$, então, escrevemos $A_i = \mu_\Phi(\gamma,p)\nu_\Phi(\delta,q)$ e $B_i = \mu_\Phi(\delta,q)\nu_\Phi(\gamma,p)$. Portanto,

$$\prod_{i\in Z}A_i = \prod_{i\in Z}\mu_\Phi(\gamma,p)\nu_\Phi(\delta,q)x^{q(u)}y^{p(u)};$$

$$\prod_{j\notin Z}B_j = \prod_{j\notin Z}\mu_\Phi(\delta,q)\nu_\Phi(\gamma,p)x^{s(u)}y^{r(u)};$$

onde $q(u)$,$p(u)$,$s(u)$ e $r(u)$, são como no Lema 2.10.

Então,a

$$\begin{aligned}\prod_{i\in Z}A_i\prod_{j\notin Z}B_j &= \prod_{i\in Z}\mu_\Phi(\gamma,p)\nu_\Phi(\delta,q)\prod_{j\notin Z}\mu_\Phi(\delta,q)\nu_\Phi(\gamma,p)x^{e_2(u,Z)}y^{e_1(u,Z)}\\ &= \prod_{\gamma\in\mathscr{A}}\left(\prod_{i\in D_1(\gamma,Z)\cup\overline{D}_1(\gamma,Z)}\mu_{\Phi(\gamma,i)}\right.\\ &\quad\left.\times\prod_{j\in D_2(\gamma,Z)\cup\overline{D}_2(\gamma,Z)}\nu_{\Phi(\gamma,j)}\right)x^{e_2(u,Z)}y^{e_1(u,Z)}\end{aligned}$$

■

Teorema 2.18. *O Algoritmo 2.7, calcula a representação do covariante $\langle U\,|T\rangle$, em termos das raízes homogeneizadas.*

Demonstração: Aplicando o operador umbral na igualdade (2-3), do lema 2.10, obtemos:

$$\begin{aligned}\langle U\,|T\rangle &= \sum_{Z}(-1)^{m-|Z|}\langle U\,|M(Z)\rangle\\ &= \sum_{Z}(-1)^{m-|Z|}\left\langle U\right|\left(\prod_{\gamma\in\mathscr{A}}\gamma_1^{e_1(\gamma,Z)}\gamma_2^{e_2(\gamma,Z)}\right)u_1^{e_1(u,Z)}u_2^{e_2(u,Z)}\left\rangle\right..\end{aligned}$$

Então temos:

$$\begin{aligned}\langle U\,|M(Z)\rangle &= \left\langle U\right|\left(\prod_{\gamma\in\mathscr{A}}\gamma_1^{e_1(\gamma,Z)}\gamma_2^{e_2(\gamma,Z)}\right)u_1^{e_1(u,Z)}u_2^{e_2(u,Z)}\left\rangle\right.\\ &= \left(\prod_{\gamma\in\mathscr{A}}A_{e_1(\gamma,Z)}\right)X^{e_2(u,Z)}(-Y)^{e_1(u,Z)},\end{aligned}$$

por aplicação do operador umbral e uso da lei multiplicativa.

Agora, vamos calcular $h\left(\langle U\,|M(Z)\rangle\right)$. Para isso, trocaremos os coeficientes A_k pela respectiva função simétrica nas raízes homogeneizadas, ou seja,

$$\begin{aligned} h\left(\langle U\,|M(Z)\rangle\right) &= \frac{1}{(n!)^d}\prod_{\gamma}(-1)^{e_2(\gamma,Z)} \\ &\quad\times\left[\sum_{\pi}\mu_{\pi(1)}\cdots\mu_{\pi(e_2(\alpha,Z))}\nu_{\pi(e_2(\alpha,Z)+1)}\cdots\nu_{\pi(n)}\right] \\ &\quad\times\left[\sum_{\sigma}\mu_{\sigma(1)}\cdots\mu_{\sigma(e_2(\beta,Z))}\nu_{\sigma(e_2(\beta,Z)+1)}\cdots\nu_{\sigma(n)}\right] \\ &\quad\ldots x^{e_2(u,Z)}\,(-y)^{e_1(u,Z)}, \end{aligned}$$

lembrando que $n-e_2(\alpha,Z)=e_1(\alpha,Z)$, $\forall\alpha\in\mathscr{A}$, ou seja, ao aplicarmos h, tomamos $k=e_2(\alpha,Z)$ em A_{n-k}, e $d=|\mathscr{A}|$.

Fazendo o produto de todos os somatórios, podemos rescrever a expressão anterior em apenas um somatório, que ocorrerá sobre todas as d-uplas $(\pi,\sigma,\ldots)$ de permutações de $\{1,2,\ldots,m\}$, indexadas pelas letras umbrais gregas em $\mathscr{A}$. Separando todos os sinais negativos, obtemos:

$$\begin{aligned} h\left(\langle U\,|M(Z)\rangle\right) &= \frac{1}{(n!)^d}(-1)^{e_2(\alpha,Z)+e_2(\beta,Z)+\ldots+e_2(\omega,Z)+e_1(u,Z)} \\ &\quad\times\sum_{(\pi,\sigma,\ldots)}\mu_{\pi(1)}\cdots\mu_{\pi(e_2(\alpha,Z))}\nu_{\pi(e_2(\alpha,Z)+1)}\cdots\nu_{\pi(n)} \\ &\quad\times\mu_{\sigma(1)}\cdots\mu_{\sigma(e_2(\beta,Z))}\nu_{\sigma(e_2(\beta,Z)+1)}\cdots\nu_{\sigma(n)}\ldots x^{e_2(u,Z)}\,y^{e_1(u,Z)}. \end{aligned}$$

Para sabermos quanto vale $(-1)^{e_2(\alpha,Z)+e_2(\beta,Z)+\ldots+e_2(\omega,Z)+e_1(u,Z)}$, basta olharmos para $e_2(\alpha,Z)+e_2(\beta,Z)+\ldots+e_2(\omega,Z)+e_1(u,Z)\ (mod(2))$. Observemos que do Lema 2.12, $e_2(\alpha,Z)+e_2(\beta,Z)+\ldots+e_2(\omega,Z)+e_2(u,Z)=m$, onde m é o número de colchetes em T e $\mathscr{A}=\{\alpha,\beta,\ldots,\omega\}$. Seja t o número de ocorrências de u em T. Então,

$$\begin{aligned} e_2(\alpha,Z)+e_2(\beta,Z)+\ldots+e_2(\omega,Z)+e_1(u,Z) &= m-e_2(u,Z)+e_1(u,Z) \\ &\equiv m-e_2(u,Z)-e_1(u,Z)\ (mod(2)). \end{aligned}$$

Mas, $t=e_1(u,Z)+e_2(u,Z)$ e $m-t=g$, onde g é o índice do covariante $\langle U\,|T\rangle$, pela Observação 1.45. Então, $(-1)^{e_2(\alpha,Z)+e_2(\beta,Z)+\ldots+e_2(\omega,Z)+e_1(u,Z)}=(-1)^g$.

Agora, podemos substituir cada expressão $h\left(\langle U\,|M(Z)\rangle\right)$ em $h\left(\langle U\,|T\rangle\right)$, e obtemos,

(2-5)

$$h\left(\langle U\,|T\rangle\right) = \frac{(-1)^g}{(n!)^d}\sum_{Z}(-1)^{m-|Z|}$$

$$\times \sum_{(\pi,\sigma,\ldots)} \mu_{\pi(1)}\cdots\mu_{\pi(e_2(\alpha,Z))}\nu_{\pi(e_2(\alpha,Z)+1)}\cdots\nu_{\pi(n)}$$
$$\ldots x^{e_2(u,Z)}\, y^{e_1(u,Z)}.$$

Resta mostrarmos que o polinômio em (2-5), é igual ao polinômio dado pelo Algoritmo 2.7, a dizer,

(2-6)
$$\frac{(-1)^g}{(n!)^d}\sum_{\Phi} T^h[\Phi].$$

Seja $\widehat{T}$ a tabela de inteiros construída a partir de T, no Passo 1 do Algoritmo 2.7.

Substituindo a expressão (2-4), dada pelo Lema 2.17 em (2-6), e teremos:

$$\begin{aligned}\frac{(-1)^g}{(n!)^d}\sum_{\Phi} T^h[\Phi] &= \frac{(-1)^g}{(n!)^d}\sum_{Z}(-1)^{m-|Z|}\\ &\quad\times\sum_{\Phi}\left[\prod_{\gamma\in A}\prod_{i\in D_1(\gamma,Z)\cup\overline{D}_1(\gamma,Z)}\mu_{\Phi(\gamma,i)}\right.\\ &\quad\left.\times\prod_{j\in D_2(\gamma,Z)\cup\overline{D}_2(\gamma,Z)}\nu_{\Phi(\gamma,j)}\right]x^{e_2(u,Z)}y^{e_1(u,Z)}.\end{aligned}$$

Agora, vamos mostrar que o lado direito do polinômio acima e o polinômio em (2-5) são iguais.

Seja Z um subconjunto de $\{1,2,\ldots,m\}$ e seja Ψ uma função de $\mathscr{A}$ no conjunto Ω_n das permutações sobre $\{1,2,\ldots,n\}$, tal que para toda letra γ em $\mathscr{A}$, $\Psi(\gamma)$ leva:

$\{1,2,\ldots,|E_2(\gamma,Z)|\}$ em $D_2(\gamma,Z)$;

$\{|E_2(\gamma,Z)|+1,\ldots,e_2(\gamma,Z)\}$ em $\overline{D}_2(\gamma,Z)$;

$\{e_2(\gamma,Z)+1,\ldots,e_2(\gamma,Z)+|E_1(\gamma,Z)|\}$ em $D_1(\gamma,Z)$;

$\{e_2(\gamma,Z)+|E_1(\gamma,Z)|+1,\ldots,n\}$ em $\overline{D}_1(\gamma,Z)$.

Se Φ é uma função de $\mathscr{A}$ para Ω_n, seja Φ' dada por $\Phi'(\gamma)=\Phi(\gamma)\circ\Psi(\gamma)$, onde $\circ$ é a operação de composição de permutações (lembremos que $\Psi(\gamma)$ e $\Phi(\gamma)$ são permutações do conjunto $\{1,2,\ldots,m\}$). Além disso, notemos que Φ percorre todas as funções de $\mathscr{A}$ para Ω_n, então o mesmo ocorre com Φ' no somatório. Então,

$$\begin{aligned}\sum_{\Phi}\left[\prod_{\gamma\in\mathscr{A}}\prod_{i\in D_1(\gamma,Z)\cup\overline{D}_1(\gamma,Z)}\mu_{\Phi(\gamma,i)}\right. &\times \left.\prod_{j\in D_2(\gamma,Z)\cup\overline{D}_2(\gamma,Z)}\nu_{\Phi(\gamma,j)}\right]x^{e_2(u,Z)}y^{e_1(u,Z)}\\ &= \sum_{\Phi'}\left[\prod_{\gamma\in\mathscr{A}}\prod_{i\in D_1(\gamma,Z)\cup\overline{D}_1(\gamma,Z)}\mu_{\Phi'(\gamma,i)}\right.\\ &\times \left.\prod_{j\in D_2(\gamma,Z)\cup\overline{D}_2(\gamma,Z)}\nu_{\Phi'(\gamma,j)}\right]x^{e_2(u,Z)}y^{e_1(u,Z)}\\ &= \sum_{\gamma\in\mathscr{A}}\mu_{\Phi(\gamma,1)}\cdots\mu_{\Phi(\gamma,e_2(\gamma,Z))}\nu_{\Phi(\gamma,e_2(\gamma,Z)+1)}\\ &\times \quad\cdots\nu_{\Phi(n)}\,x^{e_2(u,Z)}\,y^{e_1(u,Z)}.\end{aligned}$$

Assim, para obtermos a igualdade desejada, basta escrevermos cada Φ, como uma d-upla $(\Phi(\alpha),\Phi(\beta),...)=(\pi,\sigma,...)$, ou seja, teremos

$$\begin{aligned}\sum_{\gamma\in\mathscr{A}}\mu_{\Phi(\gamma,1)}\cdots\mu_{\Phi(\gamma,e_2(\gamma,Z))}\nu_{\Phi(\gamma,e_2(\gamma,Z)+1)} &\times \cdots\nu_{\Phi(n)}\,x^{e_2(u,Z)}\,y^{e_1(u,Z)}\\ &= \frac{(-1)^g}{(n!)^d}\sum_{Z}(-1)^{m-|Z|}\\ &\times \sum_{(\pi,\sigma,...)}\mu_{\pi(1)}\cdots\mu_{\pi(e_2(\alpha,Z))}\nu_{\pi(e_2(\alpha,Z)+1)}\cdots\nu_{\pi(n)}\\ &\times \mu_{\sigma(1)}\cdots\mu_{\sigma(e_2(\alpha,Z))}\nu_{\sigma(e_2(\alpha,Z)+1)}\cdots\nu_{\sigma(n)}\\ &\times \cdots x^{e_2(u,Z)}\,y^{e_1(u,Z)},\end{aligned}$$

como queríamos.

■

2.3 Diferenças.

Vamos a partir de agora, voltar nossa atenção para as relações entre covariantes e diferenças. Nós vimos que as funções simétricas de raízes homogeneizadas, que representam covariantes, podem ser expressadas como polinômios nas diferenças de raízes homogeneizadas, de acordo com o Algoritmo 2.7. Nosso interesse é mostrar que vale a recíproca, como veremos a seguir.

Definição 2.19. *Sejam $\mu_1,...,\mu_n,\nu_1,...,\nu_n$ as raízes homogeneizadas de uma forma binária de grau n. Lembremos que uma diferença é um polinômio na álgebra das raízes homogeneizadas, que pode ser da forma $\mu_i\nu_j-\mu_j\nu_i$ ou $\mu_i x-\nu_i y$. Definimos o monômio diferença N, como o produto de diferenças. Se $i\in\{1,2,...,n\}$, definimos a multiplicidade m_i de i no monômio diferença N, como o número de diferenças em N contendo ν_i. Definimos também, a ordem de N como o número de diferenças em N contendo x, e o índice de N, o número de diferenças em N que não contem as variáveis x ou y. O monômio diferença N é regular de grau d, se $m_1=m_2=...=m_n=d$.*

Definição 2.20. *Sejam*

$$N = (\mu_i\nu_j - \mu_j\nu_i)(\mu_k\nu_l - \mu_l\nu_k)...(\mu_p x - \nu_p y)(\mu_q x - \nu_q y)...,$$

um monômio diferença regular de índice g e π uma permutação de $\{1, 2, ..., n\}$. Definimos

$$\pi(N) := (\mu_{\pi(i)}\nu_{\pi(j)} - \mu_{\pi(j)}\nu_{\pi(i)})(\mu_{\pi(k)}\nu_{\pi(l)} - \mu_{\pi(l)}\nu_{\pi(k)})...(\mu_{\pi(p)}x - \nu_{\pi(p)}y)...$$

Chamaremos de termo diferença simétrico, de índice g, o polinômio $\sum_\pi \pi(N)$, onde a soma ocorre sobre todas as permutações π de $\{1, 2, ..., n\}$. Observemos que o termo diferença simétrico será mutuamente simétrico nas variáveis μ_i e ν_i.

Definição 2.21. *Obtemos $\overline{\mu}$ e $\overline{\nu}$ a partir de μ e ν por uma mudança linear de variáveis.*

Lema 2.22. *Seja (c, d) uma mudança linear de variáveis, de x e y para $\overline{x}$ e $\overline{y}$.*

$$\begin{aligned} \overline{\mu}_i\overline{\nu}_j - \overline{\mu}_j\overline{\nu}_i &= [c \quad d](\mu_i\nu_j - \mu_j\nu_i) \\ \overline{\mu}_i\overline{x} - \overline{\nu}_i\overline{y} &= (\mu_i x - \nu_i y). \end{aligned}$$

Demonstração: Temos que:

$$\begin{aligned} x &= c_2\overline{x} + d_2\overline{y}, \\ y &= -c_1\overline{x} - d_1\overline{y}. \end{aligned}$$

Então:

$$\begin{aligned} \mu_i x - \nu_i y &= \mu_i(c_2\overline{x} + d_2\overline{y}) - \nu_i(-c_1\overline{x} - d_1\overline{y}) \\ &= (\mu_i c_2 + \nu_i c_1)\overline{x} - (-\mu_i d_2 - \nu_i d_1)\overline{y} \\ &= \overline{\mu}_i\overline{x} - \overline{\nu}_i\overline{y}. \end{aligned}$$

Para mostramos a primeira igualdade, vamos usar o valor encontrado para $\overline{\mu}_i$ e $\overline{\nu}_i$. Temos:

$$\begin{aligned} \overline{\mu}_i\overline{\nu}_j - \overline{\mu}_j\overline{\nu}_i &= (\mu_i c_2 + \nu_i c_1)(-\mu_j d_2 - \nu_j d_1) - (\mu_j c_2 + \nu_j c_1)(-\mu_i d_2 - \nu_i d_1) \\ &= -\mu_i c_2\nu_j d_1 - \nu_i c_1\mu_j d_2 + \mu_j c_2\nu_i d_1 + \nu_j c_1\mu_i d_2 \\ &= [c \quad d](\mu_i\nu_j - \mu_j\nu_i). \end{aligned}$$

■

Teorema 2.23. *Seja $R \in \mathbb{K}[\mu_1, ..., \mu_n, \nu_1, ..., \nu_n, x, y]$. Então, R é a representação em termos de raízes homogeneizadas de um covariante I, de índice g de formas binárias de grau n se, e somente se, R é uma combinação linear de termos diferença simétricos, todos de mesmo índice g.*

Demonstração: ($\Rightarrow$) Seja I um covariante, tal que $R = h(I)$. Como I pode ser visto como uma avaliação umbral de algum polinômio no espaço umbral, podemos supor, por linearidade, que $I = \langle U\,|T\rangle$, onde T é um monômio colchete no espaço umbral. Nosso objetivo é mostrar que $h(I)$ é uma combinação linear de termos diferença simétricos.

Sejam $\mathscr{A}$ o conjunto das letras umbrais gregas em T, d a cardinalidade de $\mathscr{A}$ e g o índice de I. Pelo Algoritmo 2.7, nós temos $h\left(\langle U\,|T\rangle\right) = \frac{(-1)^g}{(n!)^d}\sum_{\Phi} T^h[\Phi]$, onde a soma ocorre sobre todas as funções Φ de $\mathscr{A}$ em Ω_n, ou seja, sobre todas as d-uplas $(\Phi(\alpha) : \alpha \in \mathscr{A}) = (\pi, \sigma, ...)$ em $\Omega_n \times \Omega_n \times ... \times \Omega_n$, o produto direto de d cópias de Ω_n. Consideremos $\Omega_n \times \Omega_n \times ... \times \Omega_n$, o produto direto de d cópias do grupo simétrico Ω_n. Seja Δ o subgrupo consistindo de todas as d-uplas das forma $(\pi, \pi, ...)$, onde $\pi \in \Omega_n$, e seja $\mathcal{C}$ o conjunto de todos as classes de representantes à direita de Δ em $\Omega_n \times \Omega_n \times ... \times \Omega_n$. Então,

$$\begin{aligned} h\left(\langle U\,|T\rangle\right) &= \frac{(-1)^g}{(n!)^d}\sum_{\Phi} T^h[\Phi] \\ &= \frac{(-1)^g}{(n!)^d}\sum_{(\pi,\sigma,...)\in\mathcal{C}}\ \sum_{(\pi,\pi,...)\in\Delta} T^h[\pi\sigma, \pi\tau, ...]. \end{aligned}$$

Seja $(\pi, \sigma, ...) \in \mathcal{C}$. Temos que $T^h[\sigma, \tau, ...]$ é um monômio diferença regular de grau d pelo Passo 3 do Algoritmo 2.7. Como π percorre todo o conjunto Ω_n, temos:

$$\begin{aligned} h\left(\langle U\,|T\rangle\right) &= \frac{(-1)^g}{(n!)^d}\sum_{\Phi} T^h[\Phi] \\ &= \frac{(-1)^g}{(n!)^d}\sum_{(\pi,\sigma,...)\in\mathcal{C}}\ \sum_{(\pi,\pi,...)\in\Delta} T^h[\pi\sigma, \pi\tau, ...] \\ &= \frac{(-1)^g}{(n!)^d}\sum_{(\pi,\sigma,...)\in\mathcal{C}}\ \sum_{\pi\in\Omega_n} T^h[\pi\sigma, \pi\tau, ...] \\ &= \frac{(-1)^g}{(n!)^d}\sum_{(\pi,\sigma,...)\in\mathcal{C}}\ \sum_{\pi\in\Omega_n} \pi(T^h[\sigma, \tau, ...]), \end{aligned}$$

e portanto, $h\left(\langle U\,|T\rangle\right)$ é combinação linear de termos diferença simétricos.

($\Leftarrow$) Podemos inicialmente supor que R é apenas um termo diferença simétrico, de índice g, simplesmente por linearidade. Mostraremos que R é a representação em termos de raízes homogeneizadas de um covariante I. Podemos expandir R, como um polinômio nas variáveis μ_i, ν_i, x e y, e teremos que cada monômio na expansão de R é regular e tem o mesmo grau, pela definição de R (ver Definições 2.3, 2.19 e 2.20). Então, R é regular como um polinômio em μ_i e ν_i. Além disso, por definição, R é mutuamente simétrico em μ_i e ν_i. Segue da Proposição 2.6, que existe $I(a_0, ..., a_n, x, y)$ tal que $R = I(a_0(\mu_i, \nu_j), ..., a_n(\mu_i, \nu_j), x, y)$.

Resta demostrarmos que $I(A_0, ...A_n, X, Y)$ é covariante. Para isso, seja g o número de diferenças do tipo $\mu_i\nu_j - \mu_j\nu_i$ em um monômio em R. Como esse número g é o mesmo em cada monômio, segue do Lema 2.22, que

$$R(\overline{\mu_i}, \overline{\nu_j}, \overline{x}, \overline{y}) = [c \quad d]^g R(\mu_i, \nu_j, x, y).$$

Então, para qualquer forma binária $f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$ com raízes homogeneizadas μ_i e ν_i, e qualquer mudança de variáveis (c,d), temos:

$$\begin{aligned} I(\overline{a}_0, ..., \overline{a}_n, \overline{x}, \overline{y}) &= I(\overline{a}_0(\overline{\mu}_i, \overline{\nu}_j), ..., a_n(\overline{\mu}_i, \overline{\nu}_j), \overline{x}, \overline{y}) \\ &= R(\overline{\mu_i}, \overline{\nu_j}, \overline{x}, \overline{y}) \\ &= [c \quad d]^g R(\mu_i, \nu_j, x, y) \\ &= [c \quad d]^g I(a_0(\mu_i, \nu_j), ..., a_n(\mu_i, \nu_j), x, y) \\ &= [c \quad d]^g I(a_0, ..., a_n, x, y) \end{aligned}$$

■

Notação 2.24. *Escrevemos* $[i \quad j] = \mu_i\nu_j - \mu_j\nu_i$ *e* $[i \quad u] = \mu_i x - \nu_i y$.

Definição 2.25. *Seja* $\mathscr{V}$ *a subalgebra gerada pelos colchetes dados acima, na álgebra de raízes homogeneizadas. Definimos o operador simetrização* S *sobre* $\mathscr{V}$ *por* $\langle S\,|[i \quad j][k \quad l]...[p \quad u]\rangle = \sum_\pi [\pi(i) \quad \pi(j)][\pi(k) \quad \pi(l)]...[\pi(p) \quad u]$, *onde a soma ocorre sobre todas as permutações* π *de* $\{1, 2, ..., n\}$, *e então estendemos por linearidade para polinômios.*

Observação 2.26. *Nesta notação, um termo diferença simétrico é a imagem de um monômio colchete, na álgebra de raízes homogeneizadas, sob o operador simetrização.*

A Proposição seguinte nos explicitará um importante isomorfismo, que nos dará uma outra forma de vermos o espaço dos covariantes, e será uns dos passos principais na demonstração do Teorema de Finitude.

Proposição 2.27. *Seja* $\mathscr{V}^S[n,d,t]$ *o espaço de todos os monômios colchete simetrizados formados com os* n *inteiros* $\{1, 2, ..., n\}$, *cada um ocorrendo* d *vezes e a letra romana* u *ocorrendo* t *vezes. Então,*

$$\mathscr{I}[n,d,t] \cong \mathscr{V}^S[n,d,t],$$

onde o isomorfismo é dado pela restrição do homomorfismo h *a* $\mathscr{I}[n,d,t]$, *onde* $\mathscr{I}[n,d,t]$ *é o espaço dos covariantes de grau* d *e ordem* t *de formas binárias de grau* n.

Demonstração: Notemos que a sobrejetividade sai direto da Observação anterior. Para mostrarmos a injetividade, seja $I \in \mathscr{I}[n,d,t]$ e suponhamos que $h(I)=0$. Mas, pela definição de h, temos que ter necessariamente $I=0$.

■

Notemos que este resultado nos diz que a simetrização de um monômio diferença M representa um covariante se, e somente se, M é regular. Esse resultado poderá ser estabelecido com a notação de colchetes, como mostra a seguinte proposição:

Proposição 2.28. *Seja M um polinômio colchete não-constante em $\mathscr{V}$. Então, $\langle S\,|M\rangle$ é a representação em termos de raízes homogeneizadas de um covariante I de grau d e ordem t de formas binárias de grau n se, e somente se, as seguintes condições são satisfeitas: Sejam*

$$\begin{aligned} m_{ij} &= \textit{número de ocorrências do colchete } [i \quad j] \textit{ ou } [j \quad i] \textit{ em } M, \\ t_i &= \textit{número de ocorrências do colchete } [i \quad u] \textit{ ou } [u \quad i] \textit{ em } M. \end{aligned}$$

Então:

A. *Para todo i e j, $m_{ij}=m_{ji}$ e $m_{ii}=0$;*

B. *para todo i, $t_i+m_{i1}+m_{i2}+...+m_{in}=d$;*

C. $t_1+t_2+...+t_n=t$;

D. *a soma de todos os $t_i's$ e $m_{ij}'s$ é par.*

Inversamente, qualquer covariante pode ser representado em termos de raízes homogeneizadas, como uma combinação linear de termos diferença simétrico $\langle S\,|M\rangle$, onde M satisfaz as condições anteriores.

Para um exemplo de aplicação da proposição anterior, vamos mostrar quais são todos os invariantes das cúbicas binárias.

Exemplo 2.29. *([6] pág. 58) Seja $\langle S\,|M\rangle$ um termo diferença simétrico representando um invariante das cúbicas binárias. Então, as entradas não nulas m_{ij}, com $i\neq j$ e $i,j=1,2,3$, satisfazem as seguintes equações diofantinas:*

$$m_{ij}=m_{ji},$$

$$m_{12}+m_{13}=m_{21}+m_{23}=m_{31}+m_{32}=d,$$

$$m_{12}+m_{13}+m_{21}+m_{23}+m_{31}+m_{32}=2h.$$

Resolvendo estas equações, obtemos:

$$m_{12} = m_{13} = m_{23}.$$

Assim,

$$M = ([1 \quad 2][1 \quad 3][2 \quad 3])^k,$$

para algum inteiro positivo k.

Como,

$$([\pi(1) \quad \pi(2)][\pi(1) \quad \pi(3)][\pi(2) \quad \pi(3)])^k = sgn(\pi)([1 \quad 2][1 \quad 3][2 \quad 3])^k,$$

$\langle S\,|M\,\rangle$ é zero se k é impar. Assim,

$$\langle S\,|M\,\rangle = ([1 \quad 2][1 \quad 3][2 \quad 3])^k,$$

onde k é par, são os únicas termos diferença simétricos não nulos representado invariantes das cúbicas.

Para $k = 2$,

$$([1 \quad 2][1 \quad 3][2 \quad 3])^2 = ((\mu_1\nu_2 - \mu_2\nu_1)(\mu_1\nu_3 - \mu_3\nu_1)(\mu_2\nu_3 - \mu_3\nu_2))^2,$$

que é um múltiplo constante do discriminante das cúbicas. Portanto, todo invariante não nulo das cúbicas binárias é um múltiplo constante de uma potência do discriminante.

Para mostrar o quão fortes são os resultados anteriores, daremos uma simples demonstração da Lei de Reciprocidade de Hermite.

Teorema 2.30. *(Lei de Reciprocidade de Hermite) Seja $c(n, d, t)$ a dimensão do espaço vetorial dos covariantes de grau d e ordem t de formas binárias de grau n. Então*

$$c(n, d, t) = c(d, n, t).$$

Demonstração: Seja $\mathscr{U}^S[n, d, t]$ o espaço vetorial gerado por todos os monômios colchete simetrizados formado com d letras gregas distintas $\alpha, \beta, \ldots, \omega$, cada uma ocorrendo n vezes e a letra romana u ocorrendo t vezes. Seja ainda, $\mathscr{V}^S[d, n, t]$ o espaço vetorial gerado por todos os monômios colchete simetrizados, formados com os inteiros $1, 2, \ldots, d$, cada um ocorrendo n vezes e a letra romana u ocorrendo t vezes.

Esta demonstração é feita olhando-se para os covariantes de duas formas diferentes: primeiro, representamos umbralmente os covariantes de grau d e ordem t, de formas binárias de grau n. Segue então do Teorema 1.46 que

$$c(n, d, t) = \dim \mathscr{U}^S[n, d, t].$$

Depois, podemos representar os covariantes por raízes homogeneizadas, e teremos pela Proposição 2.27 que

$$c(d,n,t) = \dim \mathscr{V}^S[d,n,t].$$

Agora, resta notarmos que vale

$$\mathscr{U}^S[n,d,t] \cong \mathscr{V}^S[d,n,t],$$

usando a seguinte identificação: $\alpha \mapsto 1$, $\beta \mapsto 2$, ... , $\omega \mapsto d$. ■

Capítulo 3

Mutuamente Covariante

Neste capítulo mostraremos os principais resultados sobre covariantes de várias formas binárias, chamados de mutuamente covariantes. Para nossos objetivos, definiremos apenas covariantes de duas formas binárias, que chamaremos de 2-covariante. Um desses 2-covariantes, de grande importância, é o covariante apolar.

3.1 2-Covariante

Aqui apresentaremos alguns resultados e definições para 2-covariantes e deixaremos indicados quais resultados apresentados nas seções anteriores, podem ser generalizados para 2-covariante. Para mais detalhes, ver [6] e [3].

Definição 3.1. *Seja g um inteiro não negativo. Um polinômio não constante $I(A_{10}, A_{11}, \dots, A_{1n}, A_{20}, A_{21}, \dots, A_{2n}, X, Y)$ nas variáveis A_{10}, A_{11}, ... , A_{1n}, A_{20}, A_{21}, ... , A_{2n}, X e Y, é um 2-covariante de índice g de duplas de formas binárias $f_1(x, y)$ e $f_2(x, y)$ de graus $n(1)$ e $n(2)$ respectivamente se, para toda mudança linear de variáveis (c, d) e toda dupla $f_1(x, y)$ e $f_2(x, y)$ de formas binárias de graus $n(1)$ e $n(2)$ respectivamente, valem*

$$I(\overline{a}_{10}, \dots, \overline{a}_{1n}, \overline{a}_{20}, \dots, \overline{a}_{2n}, \overline{x}, \overline{y}) = (c_{11}c_{22} - c_{21}c_{12})^g I(a_{10}, \dots, a_{1n}, a_{20}, \dots, a_{2n}, x, y).$$

Um 2-invariante de $f_1(x, y)$ e $f_2(x, y)$, é um 2-covariante no qual não aparecem as variáveis X e Y.

Definição 3.2. *O operador umbral do espaço das duplas $f_1(x, y)$ e $f_2(x, y)$ de graus $n(1)$ e $n(2)$ respectivamente, é definido como segue: particionemos o conjunto das letras umbrais gregas em 2 subconjuntos infinitos disjuntos $\mathscr{A}_1$ e $\mathscr{A}_2$, e indiquemos as letras umbrais gregas no i-ésimo subconjunto $\mathscr{A}_i$ para a i-ésima forma $f_i(x, y)$. Se duas letras são indicadas para a mesma forma $f_i(x, y)$, elas são equivalentes. O*

operador umbral U é o operador linear definido do espaço umbral $\mathscr{U}$ para o espaço dos polinômios nas variáveis $A_{10}, A_{11}, \ldots, A_{1n}, A_{20}, A_{21}, \ldots, A_{2n}, X$ e Y pelas regras:

$\langle U|\alpha_1^k\alpha_2^{n(i)-k}\rangle = A_{ik}$ *se* α *está em* $\mathscr{A}_i$*;*
$\langle U\,|\alpha_1^j\alpha_2^k\,\rangle = 0$ *se* $j+k \neq n(i)$ *e* α *está em* $\mathscr{A}_i$*;*
$\langle U\,|u_1^k\,\rangle = (-Y)^k$*;*
$\langle U\,|u_2^k\,\rangle = X^k$*;*

e a lei multiplicativa estendida aqui, vale se as letras umbral são atribuídas para formas diferentes.

Observação 3.3. *Os dois teoremas fundamentais e suas demonstrações são de modo direto estendidas para duas formas binárias. As definições do início da Seção 2-1 e a Proposição 2.6 são também estendidos para duas formas binárias, de modo totalmente análogo.*

Um Corolário importante dos Teoremas Fundamentais é o seguinte:

Corolário 3.4. *Seja $I(A_0, A_1, \ldots, A_n, X, Y)$ um polinômio homogêneo de grau d e ordem l. Então, $I(A_0, A_1, \ldots, A_n, X, Y)$ é um covariante de índice g de formas binárias de grau n se, e somente se, o polinômio $I(A_0, A_1, \ldots, A_n, S, -T)$, obtido pondo-se $X = S$ e $Y = -T$, é um 2-invariante de índice $g + l$ de formas binárias de grau n e formas lineares $tx + sy$.*

Agora, vamos mostrar uma extensão do Algoritmo 2.7 para duas formas binárias. Sejam $f_1(x, y)$ e $f_2(x, y)$ formas binárias de graus $n(1)$ e $n(2)$ respectivamente, e $\mu_1^i, \ldots, \mu_{n(i)}^i, \nu_1^i, \ldots, \nu_{n(i)}^i$ as raízes homogeneizadas de $f_i(x, y)$, $i = 1, 2$.

Algoritmo 3.5. *Seja $\mathscr{A}_i$ o conjunto das letras umbrais gregas pertencentes a $f_i(x, y)$ aparecendo em T e seja d_i a cardinalidade de $\mathscr{A}_i$. Assumiremos que toda letra em $\mathscr{A}_i$ ocorre exatamente $n(i)$ vezes. Se não, $h(\langle U\,|T\rangle) = 0$ e o algoritmo termina.*

Passo 1: Construamos a tabela $\widehat{T}$ repetindo o Passo 1 do Algoritmo 2.7 para $\mathscr{A}_i$, $i = 1, 2$;

Passo 2: seja Φ uma função de $\mathscr{A}_1 \cup \mathscr{A}_2$ para o conjunto das permutações tais que se $\alpha \in \mathscr{A}_i$, então $\Phi(\alpha)$ é uma permutação do conjunto $\{1, 2, \ldots, n(i)\}$. Definimos então a tabela $T[\Phi]$ como no Passo 2 do Algoritmo 2.7;

Passo 3: para cada linha de $T[\Phi]$, associamos um polinômio nas raízes homogeneizadas de acordo com as seguintes regras: se $\alpha \in \mathscr{A}_p$ e $\beta \in \mathscr{A}_q$, então

$$\begin{aligned} [\alpha \quad \beta|i \quad j] &\leftarrow \mu_i^{(p)}\nu_j^{(q)} - \nu_i^{(p)}\mu_j^{(q)}; \\ [\alpha \quad u|i \quad u] &\leftarrow \mu_i^{(p)}x - \nu_i^{(p)}y. \end{aligned}$$

O polinômio $T^h[\Phi]$ é o produto de todas as diferenças obtidas.

Passo 4: ponhamos

$$h(\langle U\,|T\rangle) = \left((-1)^g/\prod_{i=1}^{r}(n(i)!)^{d_i}\right)\sum_{\Phi}T^h[\Phi],$$

onde g é o índice do covariante $\langle U\,|T\rangle$ e a soma ocorre sobre todas as funções Φ do tipo definido no Passo 2.

■

Podemos também estender para duas formas binárias o conceito de diferenças. Sejam $f_1(x,y)$ e $f_2(x,y)$ formas binárias de graus $n(1)$ e $n(2)$ respectivamente e sejam $\mu_i^{(k)}$, $\nu_i^{(k)}$, com $i = 1, 2, \ldots, n(k)$, as raízes homogeneizadas da k-ésima forma binária $f_k(x,y)$. Uma *diferença* é um polinômio na álgebra $\mathbb{K}[\mu_i^{(k)}, \nu_i^{(k)}, x, y]$ de raízes homogeneizadas, da forma,

$$\mu_i^{(k)}\nu_j^{(l)} - \mu_j^{(l)}\nu_i^{(k)} \text{ ou } \mu_i^{(k)}x - \nu_i^{(k)}y,$$

e um *monômio diferença* é o produto de diferenças. A multiplicidade $m_i^{(k)}$ de i relativo a k-ésima forma binária em um monômio diferença N é o número de diferenças em N contendo as variáveis $\mu_i^{(k)}$. Um monômio diferença é regular de grau (d_1, d_2) se a multiplicidade de i relativa a k-ésima forma binária são todas iguais a d_i. Com isso, podemos estender o Teorema 2.23 e a Proposição 2.27 para duas formas binárias.

Exemplo 3.6. *Consideremos as formas binárias*

$$f(x,y) = a_2x^2 + 2a_1xy + a_0y^2$$

e

$$g(x,y) = b_3x^3 + 3b_2x^2y + 3b_1xy^2 + b_0y^3.$$

A partir delas, temos o polinômio conhecido como Resultante de Sylvester da forma quadrática f e da forma cúbica g, dado por: $R(A_0,A_1,A_2,B_0,B_1,B_2,B_3) = B_0^2A_2^3 - 6B_0A_2^2B_2A_0 + 6B_0A_2B_3A_0A_1 - 6B_2A_0^2B_3A_1 - 6A_1B_1A_2^2B_0 - 18A_1B_1A_2B_2A_0 + 9B_2^2A_0^2A_2 + 12A_1^2B_1B_3A_0 + 12A_1^2B_2A_2B_0 - 8A_1^3B_3B_0 + 9A_0B_1^2A_2^2 - 6A_0^2B_1A_2B_3 + A_0^3B_3^2$.

O polinômio R é um 2-invariante.

Exemplo 3.7. *Para criarmos mais exemplos de 2-covariantes, basta aplicarmos a versão do Primeiro Teorema Fundamental para duas formas binárias, de maneira análoga feita para uma forma binária. Um desses exemplos é o covariante apolar, que será apresentado na próxima seção. Outros exemplos ainda podem ser encontrados em [12] e [5].*

3.2 Apolaridade

Nesta seção, introduziremos a noção de covariante apolar e alguns resultados que servirão para classificar formas binárias, no sentido que queremos encontrar as formas canônicas para as formas binárias de um certo grau. Na *Seção 4.2*, veremos as formas canônicas de formas binárias de grau baixo, que servirão como exemplo da aplicação de importantes resultados dessa seção.

Definição 3.8. *Consideremos duas formas binárias*

$$f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k} = \langle U(f,g) \,|[\alpha \quad u]^n \rangle \,,$$

$$g(x,y) = \sum_{k=0}^{m} \binom{m}{k} b_k x^k y^{m-k} = \langle U(f,g) \,|[\beta \quad u]^m \rangle \,,$$

onde $f(x,y)$ e $g(x,y)$ tem graus respectivamente n e m, com $n \geq m$, e α é uma letra umbral ocorrendo em f e β ocorrendo em g. Definimos umbralmente o covariante apolar $\{f,g\}$, de f e g, como a forma binária de grau $n-m$ dada por

$$\{f,g\} = \left\langle U(f,g) \,\middle|[\alpha \quad \beta]^m [\alpha \quad u]^{n-m} \right\rangle .$$

Exemplo 3.9. *Sejam $f(x,y) = a_0y^2 + 2a_1xy + a_2x^2 = \langle U(f,g) \,|[\alpha \quad u]^2 \rangle$ e $g(x,y) = b_0y + b_1x = \langle U(f,g) \,|[\beta \quad u] \rangle$ duas formas binárias, de graus $n = 2$ e $m = 1$ respectivamente. Então, o covariante da f e g é $\{f,g\} = \langle U(f,g) \,|[\alpha \quad \beta][\alpha \quad u] \rangle = (b_0a_2 - b_1a_1)x + (b_0a_1 - b_1a_0)y$. Notemos, após fazer algumas contas, que o polinômio $I(A_0, A_1, A_2, B_0, B_1, X, Y) = (B_0A_2 - B_1A_1)X + (B_0A_1 - B_1A_0)Y$, é um 2-covariante de índice $g = 1$ de formas binárias quadráticas e formas binárias lineares.*

Temos que a expressão geral do covariante apolar é dada por

$$\{f,g\} = \sum_{l=0}^{n-m} \binom{n-m}{l} \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} b_{m-k} a_{k+l} x^l y^{n-m-l}.$$

Observação 3.10. *Pelo Primeiro Teorema Fundamental, para 2-covariante, temos que o polinômio $I = I(A_i, B_i, X, Y)$ definido por*

$$I = \sum_{l=0}^{n-m} \binom{n-m}{l} \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} B_{m-k} A_{k+l} X^l Y^{n-m-l},$$

é um 2-covariante de índice $g = m$ de formas binárias de graus n e m.

Lema 3.11. *Seja $\mathscr{F}_n$ o espaço vetorial de todas as formas binárias de grau n. Então, o covariante apolar $\{f,g\}$ é uma aplicação bilinear de $\mathscr{F}_n \times \mathscr{F}_m$ para $\mathscr{F}_{n-m}$ que é 2-covariante em f e g. Inversamente, qualquer aplicação bilinear 2-covariante de $\mathscr{F}_n \times \mathscr{F}_m$ para $\mathscr{F}_{n-m}$ é um múltiplo constante de $\{f,g\}$.*

Além dessas representações do covariante apolar de f e g, podemos encontrar sua representação em termos de raízes homogeneizadas. Sejam

$$f(x,y) = a(\mu_1 x - \nu_1 y)(\mu_2 x - \nu_2 y)...(\mu_n x - \nu_n y),$$

$$g(x,y) = b(\epsilon_1 x - \eta_1 y)(\epsilon_2 x - \eta_2 y)...(\epsilon_m x - \eta_m y)$$

a fatoração de $f(x,y)$ e $g(x,y)$ em formas lineares. Diremos que duas formas $\mu_i x - \nu_i y$ e $\mu_j x - \nu_j y$ na fatoração de $f(x,y)$ são distintas, se $\mu_i x - \nu_i y \neq c\mu_j x - \nu_j y$ para toda constante c. Pelo Algoritmo 3.5, obtemos a expressão de $\{f,g\}$ em termos dos coeficientes μ_i, ν_i, ϵ_i e η_i, das formas lineares ocorrendo em ambas as fatorações, que é:

$$\begin{aligned}\{f,g\} \;= \tfrac{(-1)^{n-m}ab}{m!n!} \;& \sum_{\pi,\sigma} (\mu_{\pi(1)}\eta_{\sigma(1)} - \nu_{\pi(1)}\epsilon_{\sigma(1)}) \\ & ...(\mu_{\pi(m)}\eta_{\sigma(m)} - \nu_{\pi(m)}\epsilon_{\sigma(m)}) \\ & \times(\mu_{\pi(m+1)}x - \nu_{\pi(m+1)}y)...(\mu_{\pi(n)}x - \nu_{\pi(n)}y),\end{aligned}$$

onde a soma ocorre sobre todas as permutações π de $\{1,2,...,n\}$ e σ de $\{1,2,...,m\}$, $g = n - m$ e $d_1 = d_2 = 1$.

Lema 3.12. *Sejam $f(x,y)$ uma forma binária de grau n, $g(x,y)$ uma forma binária de grau m_1 e $h(x,y)$ uma forma binária de grau m_2, com $m_1 + m_2 \leq n$. Então, $\{f, gh\} = \{\{f,g\},h\}$.*

Demonstração: É apenas uma questão de fazer contas, portanto, será omitida. ■

Como uma consequência direta do Lema anterior temos:

Corolário 3.13. *Sob as mesmas hipóteses do Lema anterior, se $\{f,g\} = 0$, então $\{f, gh\} = 0$.*

A grande motivação desta seção é a seguinte definição:

Definição 3.14. *Duas formas binárias $f(x,y)$ e $g(x,y)$ são apolares, se o covariante apolar delas é a forma identicamente nula.*

Exemplo 3.15. *Consideremos as formas binárias $f(x,y) = 6x^2y + 2y^3$ e $g(x,y) = x^2 - y^2$, de graus 3 e 2 respectivamente. Elas são apolares.*

A partir dessa definição, e sendo dada uma forma binária de grau s e um inteiro positivo t, queremos saber qual é a dimensão do espaço vetorial de todas as formas binárias de grau t apolares a dada forma binária, e quem sabe encontrarmos uma base para este espaço. Mais ainda, queremos saber o que essa informação nos diz sobre a forma binária dada.

Precisaremos analisar dois casos:

A. $t \geq s$;

B. $t < s$.

O caso A, é facilmente respondido pela:

Proposição 3.16. *Seja $g(x,y)$ uma forma binária não-nula de grau m, e seja n um inteiro positivo tal que $n \geq m$. Então, a dimensão do espaço vetorial de todas as formas de grau n apolares a $g(x,y)$ é igual a m. Mais precisamente, se*

$$g(x,y) = a(\mu_1 x - \nu_1 y)^{m_1}(\mu_2 x - \nu_2 y)^{m_2}...(\mu_p x - \nu_p y)^{m_p}$$

é a fatoração de $g(x,y)$ em formas lineares distintas, então as formas binárias

$$(\mu_i x - \nu_i y)^{n-m_i+1} x^j y^{m_i-j-1},$$

com $i = 1, 2, ..., p$ e $j = 0, 1, ..., m_i - 1$, formam uma base para o espaço vetorial de todas as formas de grau n apolares a $g(x,y)$.

Demonstração: Seja $g(x,y) = \sum_{k=0}^{m} \binom{m}{k} b_k x^k y^{m-k}$ uma forma binária de grau m. Se $f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$ é apolar a g, ou seja, $\{f,g\} = 0$, teremos usando a forma expandida de $\{f,g\}$, $n - m + 1$ equações lineares que tem que ser satisfeitas pelos coeficientes a_k de $f(x,y)$. Assim temos:

$$\begin{array}{lllll}
\binom{m}{0} b_m a_0 & -\binom{m}{1} b_{m-1} a_1 & +\binom{m}{2} b_{m-2} a_2 - ... & \pm \binom{m}{m} b_0 a_m & = 0 \\
\binom{m}{0} b_m a_1 & -\binom{m}{1} b_{m-1} a_2 + & ... & \pm \binom{m}{m} b_0 a_{m+1} & = 0 \\
 & \vdots & & & \\
 & \binom{m}{0} b_m a_{n-m} + & ... & \pm \binom{m}{m} b_0 a_n & = 0.
\end{array}$$

Como $g(x,y)$ é não-nulo, estas equações lineares são linearmente independentes. Além disso, observemos que existem $n - m + 1$ equações e $n + 1$ incógnitas, portanto, estas equações determinam um subespaço do espaço vetorial de todas as formas binárias de grau n, de dimensão igual a $(n+1) - (n - m + 1) = m$.

Suponhamos que $g(x,y) = a(\mu_1 x - \nu_1 y)^{m_1}(\mu_2 x - \nu_2 y)^{m_2}...(\mu_p x - \nu_p y)^{m_p}$. Queremos mostrar que cada $(\mu_i x - \nu_i y)^{n-m_i+1} x^j y^{m_i-j-1}$ é apolar a $g(x,y)$, além disso, que estas formas binárias são linearmente independentes, e então, concluirmos que são uma base. Para isso, seja $\mu_i x - \nu_i y$, uma forma linear ocorrendo com multiplicidade m_i na fatoração de $g(x,y)$. Seja

$$h(x,y) = (\mu_i x - \nu_i y)^{n-m_i+1} x^j y^{m_i-j-1}.$$

Então, pelo que foi feito anteriormente, temos

$$\begin{aligned}
\{h,g\} \quad = \tfrac{(-1)^{n-m} a}{m!n!} \quad & \sum_{\pi,\sigma} (\kappa_{\pi(1)} \eta_{\sigma(1)} - \lambda_{\pi(1)} \xi_{\sigma(1)}) \\
& ...(\kappa_{\pi(m)} \eta_{\sigma(m)} - \lambda_{\pi(m)} \xi_{\sigma(m)}) \\
& \times (\kappa_{\pi(m+1)} x - \lambda_{\pi(m+1)} y)...(\kappa_{\pi(n)} x - \lambda_{\pi(n)} y),
\end{aligned}$$

onde κ_i, λ_i são os coeficientes das formas lineares na fatoração de $h(x,y)$ e ξ_i, η_i são os coeficientes das formas lineares na fatoração de $g(x,y)$. Observe que os coeficientes μ_i e ν_i ocorrem com multiplicidade $n-m_i+1$ entre os κ_i e λ_i, e com multiplicidade m_i entre os ξ_i e η_i. Como $m_i+(n-m_i+1) = n+1 > n$, e temos exatamente n fatores em cada soma na igualdade anterior, pelo Principio da Casa dos Pombos, existe um fator da forma $(\mu_i\nu_j - \nu_i\mu_j)$, que é nulo em cada soma. Portanto, $\{h,g\} = 0$ e $h(x,y)$ é apolar a $g(x,y)$. Portanto, todas as formas

$$(\mu_i x - \nu_i y)^{n-m_i+1} x^j y^{m_i-j-1},$$

onde $i = 1,2,...,p$ e $j = 0,1,...,m_i-1$, são apolares a g. Como temos $m = m_1 + ... + m_p$ destas formas e elas são linearmente independentes, pela maneira como foram definidas, elas formam uma base para o subespaço (de dimensão m) das formas binárias de grau n apolares a $g(x,y)$. ■

Para responder o caso B, não temos um resultado direto como fizemos em A e nem resolveremos todos os casos, porém, temos alguns importantes resultados para alguns valores de t e s.

Proposição 3.17. *Seja $f(x,y)$ uma forma binária de grau n e seja m um inteiro positivo tal que $\frac{n}{2} \leq m \leq n$. Então, o subespaço de todas as formas binárias de grau m apolares a $f(x,y)$ tem dimensão maior ou igual que $2m-n$.*

Demonstração: Seja dada uma forma binária $f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$. A condição $\{f,g\} = 0$, ou seja, f e g são apolares, onde $g(x,y) = \sum_{k=0}^{m} \binom{m}{k} b_k x^k y^{m-k}$, produz $n-m+1$ equações lineares sobre os coeficientes b_i, de $g(x,y)$, que é:

(3-1) $\sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} a_{k+l} b_{m-k} = 0,$

onde $l = 0,1,...,n-m$. Notemos que estas equações podem ser linearmente dependentes, assim, a dimensão do espaço vetorial de todas as formas binárias de grau m apolar a f, tem dimensão no mínimo $m+1-(n-m+1) = 2m-n$, que é positivo pela limitação do valor de m.

■

Quando soubermos o posto do sistema (3-1), o seguinte corolário nos dará precisamente a dimensão do espaço das formas binárias de grau m, apolares a forma f de grau n dada.

Corolário 3.18. *Sob as mesmas hipóteses da proposição anterior, o espaço das formas binárias de grau m apolar a $f(x,y)$ tem dimensão $m-r+1$, onde r é o posto do sistema (3-1) de equações lineares.*

Demonstração: Se o sistema (3-1) tem posto r, então esse sistema nos dá $n - m + 1 = r$ equações linearmente independentes. Assim, a dimensão do espaço de todas as formas binárias de grau m apolares a $f(x, y)$ é igual a $m + 1 - r$, como queríamos.

■

A partir de agora, faremos certas restrições sobre os valores de n e m. Analizaremos os casos quando n é par ou ímpar, impondo ao mesmo tempo uma restrição ainda maior ao valor de m. Começaremos apresentando o Teorema de Sylvester, que nos dará um importante e clássico resultado quando n é ímpar.

Teorema 3.19. *(Sylvester) Seja $f(x, y)$ uma forma binária de grau ímpar $n = 2j + 1$. Então, existe uma forma não-nula $g(x, y)$ de grau $m = j + 1$ apolar a $f(x, y)$. Se, em adição, existir uma tal forma $g(x, y)$ com m fatores lineares distintos $\mu_1 x - \nu_1 y, ..., \mu_m x - \nu_m y$, então existirão escalares c_i, tais que*

$$f(x, y) = \sum_{i=1}^{m} c_i(\mu_i x - \nu_i y)^n.$$

Demonstração: Segue diretamente da Proposição anterior, que o espaço de todas as formas de grau m apolares a f, tem dimensão no mínimo $2m-n = 2(j+1)-(2j+1) = 1$, e portanto existe pelo menos uma forma binária de grau m, digamos $g(x, y)$, apolar a f. Agora, suponhamos que essa forma, $g(x, y)$, tem m fatores lineares distintos, ou seja, $g(x, y) = (\mu_1 x - \nu_1 y)...(\mu_m x - \nu_m y)$. Então, pondo $m_i = 1$ na Proposição 3.16, existirão constantes c_i tais que,

$$f(x, y) = \sum_{i=1}^{m} c_i(\mu_i x - \nu_i y)^n.$$

■

Exemplo 3.20. *Consideremos as formas binárias $f(x, y) = 6x^2y + 2y^3$ e $g(x, y) = x^2 - y^2$, de graus 3 e 2 respectivamente. Já sabemos que f e g são apolares e como $g(x, y) = (x - y)(x + y)$, segue do Teorema de Sylvester que $f(x, y) = c_1(x - y)^3 + c_2(x + y)^3$, para algum c_1 e c_2. Abrindo a expressão da f e igualando, nós obtemos que $c_1 = -1$ e $c_2 = 1$.*

Usando a Proposição 3.17 e a Proposição 3.16, podemos enunciar o seguinte teorema:

Teorema 3.21. *Seja $f(x, y)$ uma forma binária de grau ímpar $n = 2j + 1$ e seja $g(x, y)$ uma forma não-nula de grau $m = j + 1$ apolar a $f(x, y)$. Se*

$$g(x, y) = (\mu_1 x - \nu_1 y)^{m_1}(\mu_2 x - \nu_2 y)^{m_2}...(\mu_p x - \nu_p y)^{m_p}$$

é a fatoração de $g(x,y)$ em p formas lineares distintas, então existem formas $h_i(x,y)$ de grau $m_i - 1$ tais que

$$f(x,y) = \sum_{i=1}^{p} h_i(x,y)(\mu_i x - \nu_i y)^{n-m_i+1}.$$

A demonstração desse Teorema é feita observando-se que de fato existe uma forma binária g apolar a f, de grau $j+1$. Em seguida, aplicamos a Proposição 3.16.

Quando o posto do sistema linear dado na Proposição anterior é m, saberemos como são todas as formas binárias apolares a uma dada forma binária. Mais ainda, essas formas serão um múltiplo de um covariante, como veremos no seguinte Lema:

Lema 3.22. *Seja $f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$ uma forma binária de grau ímpar $n = 2j+1$ e $m = j+1$. Seja J o covariante dado umbralmente por*

$$J = \left\langle U(f) \left| \prod_{\delta<\epsilon} [\delta \quad \epsilon]^2 \prod_{\delta} [\delta \quad u] \right. \right\rangle,$$

onde $\{\alpha, \beta, \ldots, \omega\}$ é o conjunto de m letras umbrais linearmente ordenadas de $f(x,y)$, o primeiro produto é sobre todos os pares (δ, ϵ) de letras umbrais tais que $\delta < \epsilon$, e o segundo produto é sobre todas as letras umbrais δ. Então, $J(a_0, a_1, \ldots, a_n, x, y)$ é apolar a $f(x,y)$, e se $J(a_0, a_1, \ldots, a_n, x, y) \neq 0$, toda forma de grau m apolar a $f(x,y)$, é um múltiplo constante de $J(a_0, a_1, \ldots, a_n, x, y)$.

Demonstração: Seja

$$g(x,y) = \sum_{k=0}^{m} \binom{m}{k} b_k x^k y^{m-k},$$

uma forma binária de grau m apolar a $f(x,y)$, ou seja, $\{f, g\} = 0$. Dessa igualdade temos o seguinte sistema, onde os coeficientes $b_i's$, o satisfazem:

$$\begin{gathered}
(-1)^m a_0 b_m + (-1)^{m-1} \binom{m}{1} a_1 b_{m-1} + \ldots + a_m b_0 = 0 \\
(-1)^m a_1 b_m + (-1)^{m-1} \binom{m}{1} a_2 b_{m-1} + \ldots + a_{m+1} b_0 = 0 \\
\vdots \\
(-1)^m a_{m-1} b_m + (-1)^{m-1} \binom{m}{1} a_m b_{m-1} + \ldots + a_{2m-1} b_0 = 0.
\end{gathered}$$

Resolvemos este sistema para $b_0, \ldots, b_m$, usando a regra de Cramer, substituindo em g e reagrupando os termos em um determinante (notemos que os denominadores dos $b_i's$, quando usamos a regra de Cramer, serão cancelados). Obtemos:

$$g(x,y) = (-1)^m \begin{vmatrix} a_0 & -\binom{m}{1} a_1 & \binom{m}{2} a_2 & ... & a_m \\ a_1 & -\binom{m}{1} a_2 & \binom{m}{2} a_3 & ... & a_{m+1} \\ a_2 & -\binom{m}{1} a_3 & \binom{m}{2} a_4 & ... & a_{m+2} \\ \vdots & & & & \\ a_{m-1} & -\binom{m}{1} a_m & \binom{m}{2} a_{m+1} & ... & a_{2m-1} \\ x^m & \binom{m}{1} x^{m-1}y & \binom{m}{2} x^{m-2}y^2 & ... & y^m \end{vmatrix}.$$

Podemos expressar $g(x,y)$ umbralmente por:

$$\begin{aligned} g(x,y) &= \left[\prod_{k=1}^{n} (-1)^{m-k} \binom{m}{k}\right] \\ &\times \left\langle U(f)| \begin{vmatrix} \alpha_2^n & \alpha_1\alpha_2^{n-1} & \alpha_1^2\alpha_2^{n-2} & ... & \alpha^m\alpha_2^{m-1} \\ \beta_1\beta_2^{n-1} & \beta_1^2\beta_2^{n-2} & \beta_1^3\beta_2^{n-3} & ... & \beta_1^{m+1}\beta_2^{m-2} \\ \gamma_1^2\gamma_2^{n-2} & \gamma_1^3\gamma_2^{n-3} & ... & & \\ \vdots & & & & \\ \omega_1^{m-1}\omega_2^m & \omega_1^m\omega_2^{m-2} & ... & & \\ u_2^m & u_2^{m-1}u_1 & u_2^{m-2}u_1^2 & ... & u_1^m \end{vmatrix} \right\rangle \end{aligned}$$

onde $\alpha, \beta, ..., \omega$, são m letras umbrais gregas de $f(x,y)$ ordenadas linearmente tais que $\alpha < \beta < ... < \omega$. Seja Δ o determinante dentro da representação umbral de $g(x,y)$. Fatorando a primeira entrada de cada linha de Δ, nós obtemos:

$$\begin{aligned} \Delta &= \alpha_2^n\beta_1\beta_2^{n-1}\gamma_1^2\gamma_2^{n-2}...\omega_1^{m-1}\omega_2^m u_2^m \\ &\times \begin{vmatrix} 1 & \alpha_1/\alpha_2 & (\alpha_1/\alpha_2)^2 & ... & (\alpha_1/\alpha_2)^{m-1} \\ 1 & \beta_1/\beta_2 & (\beta_1/\beta_2)^2 & ... & (\beta_1/\beta_2)^{m-1} \\ 1 & \gamma_1/\gamma_2 & ... & & \\ \vdots & & & & \\ 1 & \omega_1/\omega_2 & ... & & \\ 1 & u_1/u_2 & (u_1/u_2)^2 & ... & (u_1/u_2)^{m-1} \end{vmatrix}. \end{aligned}$$

A menos de um fator, o determinante Δ é um determinante de Vandermonde e nós temos:

$$\Delta = \alpha_2^n\beta_1\beta_2^{n-1}\gamma_1^2\gamma_2^{n-2}... \omega_1^{m-1}\omega_2^m u_2^m \prod_{\delta<\epsilon}\left(\frac{\delta_1}{\delta_2} - \frac{\epsilon_1}{\epsilon_2}\right)\prod_{\delta}\left(\frac{\delta_1}{\delta_2} - \frac{u_1}{u_2}\right).$$

Notemos que

$$\frac{\delta_1}{\delta_2} - \frac{\epsilon_1}{\epsilon_2} = \frac{\delta_1\epsilon_2 - \delta_2\epsilon_1}{\delta_2\epsilon_2} = \frac{[\delta \quad \epsilon]}{\delta_2\epsilon_2},$$

e analogamente, fazemos para o segundo produto. Além disso, como temos m letras, cada variável γ_2 e u_2 aparecerão m vezes no denominador após substituirmos essa

expressão em Δ. Assim, restará em α_2, por exemplo , o expoente $n-m=2j+1-(j+1)=j=m-1$. Obtemos então:

$$\Delta=\alpha_2^{m-1}\beta_1\beta_2^{m-2}\gamma_1^2\gamma_2^{m-3}...\,\omega_1^{m-1}\prod_{\delta<\epsilon}[\delta\quad\epsilon]\prod_{\delta}[\delta\quad u].$$

Vejamos ainda que Δ não é um polinômio colchete, mas podemos usar a simetrização, que vimos na *Seção 1.2*, para contornarmos esse problema e obtermos um polinômio colchete. Seja π uma permutação do conjunto $\{\alpha,\beta,...,\omega\}$. Aplicando π em Δ, obtemos:

$$\pi(\Delta)=\pi(\alpha)_2^{m-1}\pi(\beta)_1\pi(\beta)_2^{m-2}\pi(\gamma)_1^2\pi(\gamma)_2^{m-3}...\,\pi(\omega)_1^{m-1}\prod_{\delta<\epsilon}[\pi(\delta)\quad\pi(\epsilon)]\prod_{\delta}[\pi(\delta)\quad u].$$

Notemos que o produto $\prod_\delta[\delta\quad u]$, não é alterado após aplicarmos uma permutação, mas o produto $\prod_{\delta<\epsilon}[\delta\quad\epsilon]$ é alterado. Para voltarmos a essa mesma expressão, basta trocarmos a ordem de cada colchete que não tiver suas duas letras obedecendo a ordem dada. Fazendo isso, aparecerá em Δ um $sgn(\pi)$, resultando na seguinte expressão:

$$\pi(\Delta)=sgn(\pi)\pi(\alpha)_2^{m-1}\pi(\beta)_1\pi(\beta)_2^{m-2}\pi(\gamma)_1^2\pi(\gamma)_2^{m-3}...\,\pi(\omega)_1^{m-1}\prod_{\delta<\epsilon}[\delta\quad\epsilon]\prod_{\delta}[\delta\quad u].$$

Como as letras $\alpha,\beta,...,\omega$ são todas equivalentes, no sentido que após aplicarmos o operador umbral obtemos o mesmo resultado, temos:

$$\langle U(f)\,|\pi(\Delta)\rangle=\langle U(f)\,|\Delta\rangle\,.$$

Então, aplicando o funcional linear umbral sobre todas as $m!$ permutações do conjunto $\{\alpha,\beta,...,\omega\}$, obtemos:

$$\begin{aligned}
m!\,\langle U(f)\,|\Delta\rangle &= \langle U(f)|\sum_\pi\pi(\Delta)\rangle\\
&= \sum_\pi\langle U(f)\,|\pi(\Delta)\rangle\\
&= \Bigg\langle U(f)|\sum_\pi sgn(\pi)\pi(\alpha)_2^{m-1}\pi(\beta)_1\pi(\beta)_2^{m-2}\\
&\quad ...\,\pi(\omega)_1^{m-1}\prod_{\delta<\epsilon}[\delta\quad\epsilon]\prod_{\delta}[\delta\quad u]\Bigg\rangle.
\end{aligned}$$

Mas, temos:

$$\sum_\pi sgn(\pi)\pi(\alpha)_2^{m-1}\pi(\beta)_1\pi(\beta)_2^{m-2}\pi(\gamma)_1^2\pi(\gamma)_2^{m-3}...\,\pi(\omega)_1^{m-1}$$

$$= \begin{vmatrix} \alpha_2^{m-1} & \alpha_1\alpha_2^{m-2} & ... & \alpha_1^{m-1} \\ \beta_2^{m-1} & \beta_1\beta_2^{m-2} & ... & \beta_1^{m-1} \\ \vdots & & & \\ \omega_2^{m-1} & \omega_1\omega_2^{m-2} & ... & \omega_1^{m-1} \end{vmatrix}$$
$$= \prod_{\delta<\epsilon} [\delta \quad \epsilon].$$

Portanto,

$$g(x,y) = (\left[\prod_{k=1}^{n} (-1)^{m-k} \binom{m}{k}\right] /m!) \left\langle U(f) \left| \prod_{\delta<\epsilon} [\delta \quad \epsilon]^2 \prod_{\delta} [\delta \quad u] \right. \right\rangle,$$

ou seja, $J = \left\langle U(f) \left| \prod_{\delta<\epsilon} [\delta \quad \epsilon]^2 \prod_{\delta} [\delta \quad u] \right. \right\rangle$ é um múltiplo constante de $g(x,y)$, e portanto, apolar a $f(x,y)$.

Agora, se $J(a_0, a_1, ..., a_n, x, y) \neq 0$, então um de seus coeficientes é não nulo e o sistema linear inicial é linearmente independente, ou seja, tem posto máximo m. Então, pelo Corolário 3.18, a dimensão do espaço vetorial de todas as formas binárias de grau m apolar a $f(x,y)$ é $m+1-m=1$, ou seja, toda forma de grau m apolar a $f(x,y)$, é um múltiplo constante de $J(a_0, a_1, ..., a_n, x, y)$.

■

Veremos agora como tratar o caso de formas binárias de grau par.

Definição 3.23. *Seja $f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k}$ uma forma binária de grau par $n = 2j$. O Cataleticante de $f(x,y)$ é definido como o determinante*

$$cat(f) = \begin{vmatrix} a_0 & a_1 & a_2 & ... & a_j \\ a_1 & a_2 & a_3 & ... & a_{j+1} \\ a_2 & a_3 & a_4 & ... & a_{j+2} \\ \vdots & & & & \\ a_j & a_{j+1} & a_{j+2} & ... & a_{2j} \end{vmatrix}.$$

Lema 3.24. *O Cataleticante tem a representação umbral*

$$\left\langle U(f) \left| \frac{1}{(j+1)!} \prod_{\gamma<\delta} [\gamma \quad \delta]^2 \right. \right\rangle,$$

onde $\mathscr{A} = \{\alpha, \beta, ..., \omega\}$ é o conjunto das $j+1$ letras umbrais linearmente ordenadas de $f(x,y)$ e o produto ocorre sobre todos os pares (γ, δ) de letras umbrais tais que $\gamma < \delta$.

Demonstração: Seguiremos os mesmos passos da demonstração do Lema 3.22. Podemos expressar o cataleticante umbralmente por:

$$cat(f) = \left\langle U(f)\right| \begin{vmatrix} \alpha_2^n & \alpha_1\alpha_2^{n-1} & \alpha_1^2\alpha_2^{n-2} & ... & \alpha_1^j\alpha_2^j \\ \beta_1\beta_2^{n-1} & \beta_1^2\beta_2^{n-2} & \beta_1^3\beta_2^{n-3} & ... & \beta_1^{j+1}\beta_2^{j-1} \\ \gamma_1^2\gamma_2^{n-2} & \gamma_1^3\gamma_2^{n-3} & & ... & \\ \vdots & & & & \\ \omega_1^j\omega_2^j & \omega_1^{j+1}\omega_2^{j-1} & & ... & \omega_1^n \end{vmatrix} \left| \right\rangle .$$

Seja Δ o determinante dentro da representação umbral de $cat(f)$. Fatorando a primeira entrada de cada linha de Δ, obtemos:

$$\begin{aligned} \Delta &= \alpha_2^n\beta_1\beta_2^{n-1}\gamma_1^2\gamma_2^{n-2}...\,\omega_1^j\omega_2^j \\ &\times \begin{vmatrix} 1 & \alpha_1/\alpha_2 & (\alpha_1\alpha_2)^2 & ... & (\alpha_1/\alpha_2)^j \\ 1 & \beta_1/\beta_2 & (\beta_1/\beta_2)^2 & ... & (\beta_1/\beta_2)^j \\ 1 & \gamma_1/\gamma_2 & & ... & \\ \vdots & & & & \\ 1 & \omega_1/\omega_2 & & ... & (\omega_1\omega_2)^j \end{vmatrix} . \end{aligned}$$

Novamente, a menos de um fator, temos um determinante de Vandermonde:

$$\Delta = \alpha_2^n\beta_1\beta_2^{n-1}\gamma_1^2\gamma_2^{n-2}...\,\omega_1^j\omega_2^j \prod_{\gamma<\delta}\left(\frac{\gamma_1}{\gamma_2} - \frac{\delta_1}{\delta_2}\right).$$

Pelo mesmo argumento dado na demonstração do Lema 3.22, temos:

$$\Delta = \alpha_2^j\beta_1\beta_2^{j-1}\gamma_1^2\gamma_2^{j-2}...\,\omega_1^j \prod_{\gamma<\delta}[\gamma \quad \delta].$$

Seja π uma permutação do conjunto $\{\alpha, \beta, ..., \omega\}$, que tem $j+1$ letras umbrais gregas. Aplicando π em Δ, obtemos:

$$\pi(\Delta) = \pi(\alpha)_2^j\pi(\beta)_1\pi(\beta)_2^{j-1}\pi(\gamma)_1^2\pi(\gamma)_2^{j-2}...\,\pi(\omega)_1^j \prod_{\gamma<\delta}[\pi(\gamma) \quad \pi(\delta)],$$

e então,

$$\pi(\Delta) = sgn(\pi)\pi(\alpha)_2^j\pi(\beta)_1\pi(\beta)_2^{j-1}\pi(\gamma)_1^2\pi(\gamma)_2^{j-2}...\,\pi(\omega)_1^j \prod_{\gamma<\delta}[\gamma \quad \delta].$$

Como

$$\langle U(f)\,|\pi(\Delta)\rangle = \langle U(f)\,|\Delta\rangle\,,$$

temos,

$$\begin{aligned} (j+1)!\,\langle U(f)\,|\Delta\rangle &= \sum_{\pi}\langle U(f)\,|\pi(\Delta)\rangle \\ &= \left\langle U(f)\right| \sum_{\pi} sgn(\pi)\pi(\alpha)_2^j\pi(\beta)_1\pi(\beta)_2^{j-1} \\ &\quad ...\,\pi(\omega)_1^j \prod_{\gamma<\delta}[\gamma \quad \delta] \left| \right\rangle . \end{aligned}$$

onde a soma ocorre sobre todas as permutações π do conjunto $\{\alpha, \beta, ..., \omega\}$.

Então,

$$\sum_{\pi} sgn(\pi)\pi(\alpha)_2^j\pi(\beta)_1\pi(\beta)_2^{j-1}\pi(\gamma)_1^2\pi(\gamma)_2^{j-2}...\,\pi(\omega)_1^j$$

$$\begin{aligned} &= \begin{vmatrix} \alpha_2^j & \alpha_1\alpha_2^{j-1} & ... & \alpha_1^j \\ \beta_2^j & \beta_1\beta_2^{j-1} & ... & \beta_1^j \\ \vdots & & & \\ \omega_2^j & \omega_1\omega_2^{j-1} & ... & \omega_1^j \end{vmatrix} \\ &= \prod_{\gamma<\delta} [\gamma \quad \delta]. \end{aligned}$$

Portanto,

$$cat(f) = \left\langle U(f) \left| \frac{1}{(j+1)!} \prod_{\gamma<\delta} [\gamma \quad \delta]^2 \right. \right\rangle.$$

■

Teorema 3.25. *Seja $f(x, y)$ uma forma binária de grau par $n = 2j$. Então, existe uma forma não-nula $g(x, y)$ de grau j apolar a $f(x, y)$ se, e somente se, o cataleticante de $f(x, y)$ é zero. Além disso, se existir uma forma $g(x, y)$ com j fatores lineares distintos, $\mu_1 x - \nu_1 y, ..., \mu_j x - \nu_j y$, então*

$$f(x, y) = \sum_{i=1}^{j} c_i(\mu_i x - \nu_i y)^n.$$

Demonstração: Seja dada

$$f(x, y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^k y^{n-k},$$

uma forma binária de grau $n = 2j$ e seja $g(x, y) = \sum_{k=0}^{m} \binom{m}{k} b_k x^k y^{m-k}$, uma forma binária qualquer de grau $m = j$. Seja r o posto do sistema linear de equações

$$\sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} a_{k+l} b_{j-k} = 0,$$

com $l = 0, 1, ..., j$. Notemos que esse é o posto da matriz

$$\begin{pmatrix} a_0 & a_1 & a_2 & ... & a_j \\ a_1 & a_2 & a_3 & ... & a_{j+1} \\ a_2 & a_3 & a_4 & ... & a_{j+2} \\ \vdots & & & & \\ a_j & a_{j+1} & a_{j+2} & ... & a_{2j} \end{pmatrix}.$$

Além disso, o cataleticante de f é justamente o determinante dessa matriz. Então, $r < j+1$ se, e somente se, o cataleticante de f é nulo. Mais ainda, $r < j+1$ se, e somente se, o espaço de todas as formas de grau j apolares a $f(x, y)$ tem dimensão pelo menos 1, pelo Corolário 3.18. Portanto, $cat(f) = 0$ se, e somente se, o espaço de todas as formas binárias de grau j apolares a $f(x, y)$ tem $dim \geq 1$, ou seja, existe g de grau j apolar a f. Agora, suponha que $g(x, y) = (\mu_1 x - \nu_1 y)...(\mu_j x - \nu_j y)$, com grau j. Tomando $m_i = 1$ para $i = 1, ..., j$, segue da Proposição 3.16 que $f(x, y) = \sum_{i=1}^{j} c_i(\mu_i x - \nu_i y)^n$. ■

Capítulo 4

Classificação de Formas Binárias

A classificação de objetos matemáticos é um capítulo importante em várias teorias, assim como na teoria de invariantes. Um problema clássico em teoria de invariantes é o chamado Waring's Problem. Para formas binárias esse problema é: dada uma forma binária f de grau n, queremos saber qual é o número mínimo s, tal que podemos escrever f como a soma de s n-ésimas potências de formas lineares. Esse problema foi resolvido explicitamente por Gundelfinger em 1885 para o caso complexo. A classificação de formas binárias pode ser encontrada em [6], de onde extraímos a classificação das cúbicas e quínticas; em [5] e [11], podemos encontrar a classificação das formas binárias de graus 2, 3 e 4; ou uma longa discussão sobre as quárticas em [1]. Em [2] e [10], podemos encontrar alguns interessantes resultados sobre classificação de formas binárias, e também, resultados mais gerais para formas com n variáveis. O que estamos propondo aqui, é apresentarmos a classificação das formas binárias de grau baixo, através da obtenção das possíveis formas canônicas para o dado grau. Para essa classificação, usaremos as técnicas de apolaridade, onde analisaremos o espaço das formas binárias de um certo grau, apolares à forma dada. Além disso, usaremos os invariantes e covariantes clássicos das formas binárias. Para saber as características algébricas da classificação das formas binárias de graus 2, 3 e 4, veja [5].

Antes disso, vamos apresentar a Hessiana de uma forma binária, que é um importante covariante de formas binárias. Serão mostrados também, alguns resultados clássicos sobre a Hessiana, que serão de grande ajuda na classificação das formas binárias. Destacamos que neste capítulo continuaremos a trabalhar sobre um corpo algebricamente fechado.

4.1 A Hessiana

Definição 4.1. *A Hessiana $H(x,y)$ de uma forma binária de grau n é definida umbralmente por*

$$H(x,y) = \frac{1}{2}n^2(n-1)^2 \left\langle U(f) \left| [\alpha \quad \beta]^2 [\alpha \quad u]^{n-2} [\beta \quad u]^{n-2} \right\rangle \right.,$$

onde α e β são letras de $f(x,y)$.

O Lema a seguir apresenta uma forma mais interessante de ver a Hessiana (para fazer contas), que também pode ser encarada como uma definição.

Lema 4.2.

$$H(x,y) = det \begin{pmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} \end{pmatrix}.$$

Demonstração: Primeiramente, notemos que valem as seguintes relações:

$$\frac{\partial}{\partial x} U(f) = U(f) \frac{\partial}{\partial u_2}$$

$$\frac{\partial}{\partial y} U(f) = -U(f) \frac{\partial}{\partial u_1}$$

Agora, vamos simplesmente aplicar as relações acima em $f(x,y) = \langle U(f) \left| [\gamma \quad u]^n \right\rangle$, onde γ é uma letra umbral de f. Temos então:

$$\begin{array}{rcccl} \frac{\partial^2 f}{\partial x^2} & = & \left\langle U(f) \left| \frac{\partial^2}{\partial u_2^2} [\gamma \quad u]^n \right\rangle \right. & = & \left\langle U(f) \left| n(n-1)\gamma_1^2 [\gamma \quad u]^{n-2} \right\rangle \right., \\ \frac{\partial^2 f}{\partial x \partial y} & = & \left\langle U(f) \left| \frac{\partial^2}{\partial u_2 \partial u_1} [\gamma \quad u]^n \right\rangle \right. & = & \left\langle U(f) \left| n(n-1)\gamma_1\gamma_2 [\gamma \quad u]^{n-2} \right\rangle \right., \\ \frac{\partial^2 f}{\partial y^2} & = & \left\langle U(f) \left| \frac{\partial^2}{\partial u_1^2} [\gamma \quad u]^n \right\rangle \right. & = & \left\langle U(f) \left| n(n-1)\gamma_2^2 [\gamma \quad u]^{n-2} \right\rangle \right.. \end{array}$$

Substituindo temos:

$$\begin{array}{rcl} det \begin{pmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} \end{pmatrix} & = & det \begin{pmatrix} \frac{\partial^2}{\partial x^2} \langle U(f) \left| [\alpha \quad u]^n \right\rangle & \frac{\partial^2}{\partial x \partial y} \langle U(f) \left| [\beta \quad u]^n \right\rangle \\ \frac{\partial^2}{\partial x \partial y} \langle U(f) \left| [\alpha \quad u]^n \right\rangle & \frac{\partial^2}{\partial y^2} \langle U(f) \left| [\beta \quad u]^n \right\rangle \end{pmatrix} \\ & = & n^2(n-1)^2 \left\langle U(f) \left| (\alpha_1^2\beta_2^2 - \alpha_1\alpha_2\beta_1\beta_2) \right.\right. \\ & \times & [\alpha \quad u]^{n-2} [\beta \quad u]^{n-2} \left.\right\rangle. \end{array}$$

Como α e β são letras umbrais em f, podemos trocar na expressão acima $\alpha_1^2\beta_2^2[\alpha \quad u]^{n-2}[\beta \quad u]^{n-2}$ por $\frac{1}{2}(\alpha_1^2\beta_2^2 + \alpha_2^2\beta_1^2)[\alpha \quad u]^{n-2}[\beta \quad u]^{n-2}$, pois tem a mesma avaliação umbral. Notemos agora que, $\alpha_1^2\beta_2^2 + \alpha_2^2\beta_1^2 - \alpha_1\alpha_2\beta_1\beta_2 = \frac{1}{2}[\alpha \quad \beta]^2$, e por substituição, obtemos a expressão desejada. ■

Observação 4.3. *Notemos que a Hessiana é um covariante de índice 2, pelo Primeiro Teorema Fundamental. Para mais detalhes, veja [12].*

Lema 4.4. *A expressão da Hessiana em termos de raízes homogeneizadas μ_i e ν_i é dada por:*

$$\begin{aligned} H(x,y) &= \frac{1}{2((n-2)!)^2}\sum_{(\pi,\sigma)}(\mu_{\pi(1)}\nu_{\sigma(1)}-\mu_{\sigma(1)}\nu_{\pi(1)})(\mu_{\pi(2)}\nu_{\sigma(2)}-\mu_{\sigma(2)}\nu_{\pi(2)}) \\ &\quad\times\prod_{i=3}^{n}(\mu_{\pi(i)}x-\nu_{\pi(i)}y)(\mu_{\sigma(i)}x-\nu_{\sigma(i)}y). \end{aligned}$$

Demonstração: Escrevamos

$$\begin{aligned} T &= [\alpha \quad \beta]^2[\alpha \quad u]^{n-2}[\beta \quad u]^{n-2} \\ &= \begin{bmatrix} \alpha & \beta \\ \alpha & \beta \\ \alpha & u \\ \vdots & \vdots \\ \alpha & u \\ \beta & u \\ \vdots & \vdots \\ \beta & u \end{bmatrix}. \end{aligned}$$

Como $\mathscr{A} = \{\alpha, \beta\}$, temos que as funções Φ do conjunto $\{\alpha, \beta\}$ para Ω_n, podem ser trocadas pelos pares de permutações (π, σ) de $\Omega_n \times \Omega_n$. Então, pelo Algoritmo 2.7, temos

$$\begin{aligned} H(x,y) &= \frac{n^2(n-1)^2(-1)^2}{2n!^2}\sum_{\Phi}T^h[\Phi] \\ &= \frac{1}{2(n-2)!^2}\sum_{(\pi,\sigma)}(\mu_{\pi(1)}\nu_{\sigma(1)}-\mu_{\sigma(1)}\nu_{\pi(1)})(\mu_{\pi(2)}\nu_{\sigma(2)}-\mu_{\sigma(2)}\nu_{\pi(2)}) \\ &\quad\times\prod_{i=3}^{n}(\mu_{\pi(i)}x-\nu_{\pi(i)}y)(\mu_{\sigma(i)}x-\nu_{\sigma(i)}y). \end{aligned}$$

■

A proposição seguinte nos dará uma importante propriedade da Hessiana.

Proposição 4.5. *A Hessiana da forma binária $f(x, y)$ de grau n é identicamente nula se, e somente se, a forma binária é uma n-ésima potência de uma forma linear.*

Demonstração: ($\Leftarrow$) Se $f(x, y)$ é a n-ésima potência de uma forma linear, pelo Lema 4.2 segue que $H(x, y) = 0$.

($\Rightarrow$) Suponhamos que $H(x,y) = 0$. Expandindo a representação da Hessiana dada pelo Lema 4.2 e igualando a zero, obtemos:

$$\begin{aligned} a_n a_{n-2} - a_{n-1}^2 &= 0, \\ a_{n-3}a_n - a_{n-2}a_{n-1} &= 0, \\ (n-3)a_n a_{n-4} - (n-1)a_{n-2}^2 + 2a_{n-1}a_{n-3} &= 0, \\ &\vdots \end{aligned}$$

Suponhamos que $a_n \neq 0$. Escrevendo $a_n = a$ e $a_{n-1} = a\lambda$, segue que $a_{n-2} = a\lambda^2$. Continuando esse processo, obtemos: $a_{n-3} = a\lambda^3$, ..., $a_0 = a\lambda^n$. Então, $f(x,y) = a(x+\lambda y)^n$. Agora, suponha que $a_n = 0$. Substituindo na primeira igualdade, obtemos que $a_{n-1} = 0$. Substituindo novamente na terceira igualdade, obtemos que $a_{n-2} = 0$. Procedendo desta forma, obtemos que $a_n = ... = a_1 = 0$, ou seja, $f(x,y) = a_0 y^n$.

■

Exemplo 4.6. *Consideremos a forma binária*

$$f(x,y) = 8x^3 + 36x^2y + 54xy^2 + 27y^3.$$

Vamos usar o Lema anterior para encontrar a expressão da Hessiana. Calculando as derivadas parciais de f, obtemos que a Hessiana é:

$$H(f) = (48x + 72y)(108x + 162y) - (72x + 108y)^2 = 0.$$

Portanto, pela Proposição 4.5, f é uma potência de uma forma linear. De fato, temos que $f(x,y) = (2x+3y)^3$.

Podemos finalmente, começar a classificação das formas binárias.

4.2 Formas Quadráticas Binárias

A classificação das quadráticas é extremamente simples, como veremos a seguir.

Consideremos a forma binária quadrática

$$f(x,y) = a_2x^2 + 2a_1xy + a_0y^2.$$

Seja $cat(f)$, o cataleticante da f, dado por:

$$cat(f) = \begin{vmatrix} a_0 & a_1 \\ a_1 & a_2 \end{vmatrix} = a_0a_2 - a_1^2.$$

Neste caso, dizer que a Hessiana é nula, é dizer que $cat(f) = 0$ (ou que o discriminante é nulo), então pelo Teorema 3.25, existe uma forma $g(x, y) = \mu x - \nu y$ apolar a f, e portanto,

$$f(x, y) = c(\mu x - \nu y)^2.$$

Se $cat(f) \neq 0$, podemos concluir que

$$f(x, y) = c_1(\mu_1 x - \nu_1 y)^2 + c_2(\mu_2 x - \nu_2 y)^2.$$

Para vermos isso, podemos proceder de duas maneiras: primeiro, notemos que se f não é apolar a nenhuma forma de grau 1, temos garantido que existe uma forma binária g de grau 2 apolar a f. Neste caso, temos necessariamente que g tem dois fatores lineares distintos (ver [8], pág. 164, Proposição 2.3), e portanto f tem a forma canônica anterior. Outro modo, podemos usar o resultado conhecido como Teorema de Gundelfinger (ver [7] e [8]), para concluir que f, neste caso, pode ser escrita como soma de dois quadrados de formas lineares e não como apenas o quadrado de uma forma linear. A demonstração do Teorema de Gundelfinger pode ser encontrada em [8]. Isso termina a classificação das quadráticas.

4.3 Formas Cúbicas Binárias

Consideremos a forma cúbica binária

$$f(x, y) = a_3x^3 + 3a_2x^2y + 3a_1xy^2 + a_0y^3.$$

Seja $H(x, y)$ a Hessiana da f. Se H é identicamente nula, segue da Proposição 4.5, que

$$f(x, y) = (\mu x - \nu y)^3.$$

Seja $J = \langle U(f) \,|[\alpha \quad \beta]^2[\alpha \quad u][\beta \quad u]\rangle$ um covariante de formas binárias de grau 2. Pela definição umbral da Hessiana, temos que a Hessiana da cúbica f, é um múltiplo do covariante J. Então, pelo Lema 3.22, H é apolar a f. Suponhamos que $H(x, y) \neq 0$. Se $H(x, y) = (\mu x - \nu y)^2$, então, pela Proposição 3.16,

$$f(x, y) = (ax + by)(\mu x - \nu y)^2.$$

Se H tem dois fatores lineares distintos $\mu_1 x - \nu_1 y$ e $\mu_2 x - \nu_2 y$, então, novamente pela Proposição 3.16, temos que

$$f(x, y) = a(\mu_1 x - \nu_1 y)^3 + b(\mu_2 x - \nu_2 y)^3.$$

Notemos que ao invés de usar a Proposição 3.16, poderíamos ter usado de modo mais explícito o Teorema de Sylvester e o Teorema 3.21. E portanto, temos a classificação das cúbicas.

4.4 Formas Quárticas Binárias

A classificação das quárticas binárias, assim como os casos anteriores, é um resultado clássico, já conhecido a muitas décadas, e podemos encontrar em [5], [11] e [1], e é feita olhando-se para as raízes da forma binária quártica ou para os seus principais invariantes e covariantes. O que faremos aqui, é uma tentativa de encontrar as formas canônicas das quárticas binárias usando a teoria de apolaridade descrita na Seção 3.2. Pelas Proposições 3.17 e 3.16, temos que uma forma binária quártica sempre pode ser escrita como soma de três quarta-potências de formas lineares, mas isso não ajuda muito na classificação (veja [7]). O problema de simplesmente olharmos para o espaço das cúbicas apolares a quártica dada, é que esse espaço tem dimensão maior ou igual a dois, pela Proposição 3.17, ou seja, não temos uma única forma canônica neste caso. O ideal, é que consigamos olhar para o espaço das formas apolares à quártica dada, sempre tendo dimensão 1. Neste caso das quárticas, faremos menção às raízes dela, para enxergarmos que de fato obtemos todas as formas canônicas, e mais, que elas tem um significado geométrico. Outra coisa que faremos, é usar as formas canônicas das binárias quadráticas e cúbicas.

A classificação a seguir, foi uma tentativa de classificar as quárticas usando a teoria de apolaridade. O grande problema do que será feito a seguir, é que quando supomos que o cataleticante é não nulo, não temos teoremas para trabalhar, e assim, na tentativa de olharmos para as cúbicas, perdemos a unicidade, como já foi mencionado.

Consideremos a forma quártica binária

$$f(x,y) = a_4x^4 + 4a_3x^3y + 6a_2x^2y^2 + 4a_1xy^3 + a_0y^4.$$

Se $H(x,y)$, a Hessiana de f, é identicamente nula, então,

$$f(x,y) = (\mu x - \nu y)^4,$$

pela Proposição 4.5.

Se $H(x,y)$ é não nula, consideremos o cataleticante da f, a dizer $cat(f)$. Se $cat(f) = 0$, segue do Teorema 3.25 que existe uma forma binária quadrática $Q(x,y)$ apolar a f. Se $Q(x,y) = (\mu_1 x - \nu_1 y)(\mu_2 x - \nu_2 y)$, então pela Proposição 3.16, segue que

$$f(x,y) = a(\mu_1 x - \nu_1 y)^4 + b(\mu_2 x - \nu_2 y)^4.$$

Caso $Q(x,y) = (\mu_1 x - \nu_1 y)^2$, segue da mesma Proposição que

$$f(x,y) = (ax + by)(\mu_1 x - \nu_1 y)^3.$$

Agora, suponhamos $cat(f) \neq 0$. Neste caso, não temos uma g de grau 1 ou 2, tal que $\{f, g\} = 0$. Mas, a Proposição 2.6, garante que existe uma forma binária g, de grau 3, apolar a f. Se $g(x, y) = (\mu_1 x - \nu_1 y)(\mu_2 x - \nu_2 y)(\mu_3 x - \nu_3 y)$, então,

$$f(x, y) = a(\mu_1 x - \nu_1 y)^4 + b(\mu_2 x - \nu_2 y)^4 + c(\mu_3 x - \nu_3 y)^4.$$

Se $g(x, y) = (\mu_1 x - \nu_1 y)^2(\mu_2 x - \nu_2 y)$, então, existe uma forma binária linear $h(x, y) = ax + by$, tal que

$$f(x, y) = (ax + by)(\mu_1 x - \nu_1 y)^3 + c(\mu_2 x - \nu_2 y)^4.$$

Finalmente, se $g(x, y) = (\mu x - \nu y)^3$, temos que existe uma forma binária quadrática $h(x, y) = ax^2 + 2bxy + cy^2$, tal que

$$f(x, y) = (ax^2 + 2bxy + cy^2)(\mu x - \nu y)^2.$$

O que propomos agora, é classificar as quárticas usando a classificação das quadráticas e das cúbicas. O que destacaremos também, é que como na classificação clássica, diremos qual a relação da forma canônica com as raízes da forma quártica.

Para não nos perdermos em coeficientes e seus índices, abreviaremos a notação das formas binárias.

Escrevamos $f(x, y) = Q_1 Q_2$, onde Q_1 e Q_2 são duas formas binárias quadráticas. Consideremos D_1 e D_2 os discriminantes de Q_1 e Q_2 respectivamente. Notemos que neste caso, das quadráticas, o discriminante coincide com o cataleticante.

Primeiramente, suponhamos que D_1 e D_2 são ambos não nulos e que f tem quatro raízes distintas. Neste caso, pela classificação das quadráticas, temos que $Q_1 = \alpha_1 L_1^2 + \alpha_2 L_2^2$ e $Q_2 = \beta_1 \tilde{L}_1^2 + \beta_2 \tilde{L}_2^2$. Por uma transformação linear, podemos levar a reta $\tilde{L}_1$ na reta L_1 e $\tilde{L}_2$ na reta L_2. Então, podemos considerar $Q_2 = \beta_1 L_1^2 + \beta_2 L_2^2$. Temos então:

$$\begin{aligned} f(x, y) &= Q_1 Q_2 \\ &= (\alpha_1 L_1^2 + \alpha_2 L_2^2)(\beta_1 L_1^2 + \beta_2 L_2^2) \\ &= \alpha_1\beta_1 L_1^4 + \alpha_2\beta_2 L_2^4 + (\alpha_1\beta_2 + \alpha_2\beta_1) L_1^2 l_2^2 \\ &= L_1^4 + L_2^4 + \gamma L_1^2 L_2^2 \\ &= L_1^4 + L_2^4 + 6\lambda L_1^2 L_2^2 \end{aligned}$$

onde $\lambda \neq \pm\frac{1}{3}$, pela escolha inicial.

Assim,

$$f(x, y) = L_1^4 + L_2^4 + 6\lambda L_1^2 L_2^2.$$

Agora, suponhamos que $D_1 \neq 0$ e $D_2 = 0$, e que f tem três raízes distintas, sendo uma de multiplicidade dois. Pela classificação das quadráticas temos que $Q_1 = \alpha_1 L_1^2 + \alpha_2 L_2^2$ e $Q_2 = \alpha L^2$. Por uma transformação linear, podemos fixar L_2 e levar L em L_1. Então temos:

$$\begin{aligned} f(x,y) &= Q_1 Q_2 \\ &= (\alpha_1 L_1^2 + \alpha_2 L_2^2)(\alpha L_1^2) \\ &= \alpha_1 \alpha L_1^4 + \alpha_2 \alpha L_1^2 l_2^2 \\ &= L_1^4 + \gamma L_1^2 L_2^2. \end{aligned}$$

Assim,

$$f(x,y) = L_1^4 + L_1^2 L_2^2.$$

E finalmente, suponhamos que D_1 e D_2 são ambos nulos. Esse é o caso quando temos duas raízes de multiplicidade 2. Novamente pela classificação, temos direto que:

$$f(x,y) = L_1^2 L_2^2.$$

Os três casos acima, correspondem a f ter cataleticante não nulo (exceto quando $\lambda = 0$). Resta-nos olhar mais dois casos.

O primeiro, é o caso da Hessiana nula. Esse é o caso quando temos apenas uma raiz de multiplicidade quatro. Como foi feito anteriormente,

$$f(x,y) = L^4.$$

Por último, olharemos para o cataleticante sendo nulo. Aqui teremos o caso de uma raiz de multiplicidade três. Podemos simplesmente podemos considerar o que foi feito anteriormente e assim já teremos a classificação, ou olhar da seguinte forma: escreva $f = Cl$, onde l é uma forma binária linear e C é uma forma binária cúbica. Olharemos agora para a classificação das cúbicas. Mas, como é esperado, precisamos olhar apenas para o caso quando $C = L^3$ e l não é um múltiplo de L. Os outros casos recaem no que já foi feito anteriormente. Temos então:

$$f(x,y) = L^3 l.$$

E isso encerra a classificação das quárticas.

4.5 Formas Quínticas Binárias

Na classificação das quínticas, usaremos somente a teoria de apolaridade. Notemos que quando olhamos para o sistema gerado por considerar uma forma

linear, quadrática ou cúbica, apolar a quíntica, o espaço dessas formas tem sempre dimensão 1, ou seja, temos unicidade na representação da forma binária.

Consideremos a forma quíntica binária

$$f(x,y) = a_5x^5 + 5a_4x^4y + 10a_3x^3y^2 + 10a_2x^2y^3 + 5a_1xy^4 + a_0y^5,$$

com $a_5 \neq 0$. Para encontramos todas as formas canônicas das quínticas, vamos olhar para o espaço de todas as cúbicas binárias $g(x,y) = b_3x^3 + 3b_2x^2y + 3b_1xy^2 + b_0y^3$ apolares a $f(x,y)$. Pela demonstração do Lema 3.22, devemos resolver o seguinte sistema linear nas indeterminadas b_0, b_1, b_2 e b_3:

$$\begin{aligned} -a_0b_3 + 3a_1b_2 - 3a_2b_1 + a_3b_0 &= 0 \\ -a_1b_3 + 3a_2b_2 - 3a_3b_1 + a_4b_0 &= 0 \\ -a_2b_3 + 3a_3b_2 - 3a_4b_1 + a_5b_0 &= 0. \end{aligned}$$

Se este sistema de equações lineares é linearmente independente, então todas as cúbicas apolares a f são um múltiplo constante do covariante J, onde $J = J(a_0,...,a_5,x,y) = \langle U(f)\,|[\alpha\quad\beta]^2[\beta\quad\gamma]^2[\gamma\quad\alpha]^2[\alpha\quad u][\beta\quad u][\gamma\quad u]\rangle$, dado pelo Lema 3.22. Se J tem três fatores distintos $\mu_1x - \nu_1y$, $\mu_2x - \nu_2y$ e $\mu_3x - \nu_3y$, então pelo Teorema de Sylvester, segue que

$$f(x,y) = a(\mu_1x - \nu_1y)^5 + b(\mu_2x - \nu_2y)^5 + c(\mu_3x - \nu_3y)^5.$$

Se $J = (\mu_1x - \nu_1y)^2(\mu_2x - \nu_2y)$, então pelo Teorema 3.21, segue que

$$f(x,y) = (ax + by)(\mu_1x - \nu_1y)^4 + c(\mu_2x - \nu_2y)^5.$$

E por último, se $J = (\mu x - \nu y)^3$, segue novamente do Teorema 3.21 que

$$f(x,y) = (ax^2 + bxy + cy^2)(\mu x - \nu y)^3.$$

Suponhamos agora que o sistema anterior não é linearmente independente. Isto ocorre se, e somente se, $J = 0$. Vamos olhar para o posto do sistema.

Se o sistema tem posto 2, podemos por $b_3 = 0$, e resolver o sistema para b_0, b_1 e b_2. Neste caso, podemos encontrar uma forma quadrática não-nula $Q(x,y)$, unicamente determinada por um múltiplo constante, apolar a $f(x,y)$, da seguinte maneira: montemos um outro sistema como se procurássemos uma forma quadrática Q apolar a f. Chamaremos esse de sistema II. Como o sistema original tem posto 2, podemos eliminar uma das linhas desse sistema. Esse linha eliminada no sistema original, também será eliminada no sistema II, que ficará com apenas três equações e três incógnitas. O que precisamos concluir agora, para mostramos que existe

uma tal Q quadrática (não-nula) apolar a f, é que o sistema II tenha posto 2 (isso significa que teremos $m - r + 1 = 3 - r = 1$). Mas, isso é claro se lembrarmos que como o sistema original tem posto 2, então existe pelo menos um subsistema de duas equações e duas incógnitas que é linearmente independente e, além disso, o sistema II, a menos de um múltiplo escalar, possui um desses subsistemas do sistema original. Resta mostrarmos que o sistema II não tem posto 3. Mas, olhando novamente para o sistema original no começo, temos que todo subsistema $3x3$ é linearmente dependente, o que resulta, a menos de múltiplo, que o sistema II tem todos seus subsistemas $3x3$ também linearmente dependente. Portanto, juntando essas duas informações, concluímos que o sistema II tem posto 2.

Vamos analisar a decomposição da Q. Se $Q(x, y)$ tem dois fatores lineares distintos $\mu_1 x - \nu_1 y$ e $\mu_2 x - \nu_2 y$, então, pela Proposição 3.16,

$$f(x, y) = a(\mu_1 x - \nu_1 y)^5 + b(\mu_2 x - \nu_2 y)^5.$$

Se caso, $Q(x, y) = (\mu x - \nu y)^2$, novamente pela Proposição 3.16,

$$f(x, y) = (ax + by)(\mu_1 x - \nu_1 y)^4.$$

Nosso último caso, é quando o sistema acima tem posto 1. Quando isso ocorre, podemos escolher $b_3 = b_2 = 0$ e resolver o sistema para b_1 e b_0, e de maneira análoga à feita para o caso de posto 2, obtemos uma forma linear não-nula $l(x, y) = \mu x - \nu y$, apolar a $f(x, y)$. Novamente pela Proposição 3.16,

$$f(x, y) = a(\mu x - \nu y)^5.$$

Isso encerra a classificação das quínticas.

Capítulo 5

O Teorema de Finitude

Neste capítulo, mostraremos que existe um conjunto finito de covariantes que gera o espaço dos covariantes de formas binárias de grau n. Para mostrarmos este resultado, conhecido como *Teorema de Finitude*, apresentaremos uma demonstração que usará *O Algoritmo de Ordenação Circular*. Esta demonstração nos dará um método explícito de calcular um conjunto de geradores de covariantes. Existe uma segunda demonstração usando o Lema de Gordan que pode ser encontrada em [6], pág. 79, ou em [12], pág.129, ou ainda em [3], pág.101.

Definição 5.1. *Um conjunto $\mathscr{S}$ de covariantes de formas binárias de grau n é um conjunto de geradores se, para todo covariante I, existe um polinômio $P(X_1, \ldots, X_s)$ tal que $I = P(C_1, \ldots, C_s)$, onde $C_1, \ldots, C_s$ são covariantes em $\mathscr{S}$.*

Teorema 5.2. *(O Teorema de Finitude) Existe um conjunto finito de geradores para os covariantes de formas binárias de grau n.*

5.1 A Demonstração.

Para essa demonstração, começaremos com novas definições, como a de polinômios colchete ciclicamente padrão, e apresentaremos resultados importantes, como o Lema de Kempe e o Lema de Hilbert.

Definição 5.3. *Seja $\mathscr{A} = \{\alpha, \beta, \gamma, \delta, \ldots\}$ um alfabeto. Uma ordem cíclica Γ sobre o alfabeto $\mathscr{A}$ é uma relação, denotada por $\alpha \Rightarrow \beta$, satisfazendo: para toda letra $\beta \in \mathscr{A}$ existe uma única letra $\alpha \in \mathscr{A}$ tal que $\alpha \Rightarrow \beta$ e uma única γ tal que $\beta \Rightarrow \gamma$. A letra α é chamada de o predecessor de β e a letra γ é chamada de sucessor de β.*

Podemos visualizar a ordem cíclica Γ como um grafo direcionado, também denotado por Γ, sobre o conjunto de vértices $\mathscr{A}$ tal que existe uma linha direcionada

de α para β se, e somente se, $\alpha \Rightarrow \beta$. Este grafo direcionado é um ciclo direcionado e existe um único caminho simples (que é um caminho sem qualquer repetição de vértices) de qualquer vértice α para qualquer outro vértice δ.

Definição 5.4. *Diremos que β está entre α e δ, e escrevemos $\alpha \to \beta \to \delta$, se β é um vértice distinto, de α e δ, sobre um único caminho simples de α para δ. Se $\mathscr{A}'$ é um subconjunto de $\mathscr{A}$, a restrição de Γ a $\mathscr{A}'$ é a ordem cíclica definida por: $\alpha \Rightarrow \beta$ se toda letra entre α e β não está em $\mathscr{A}'$.*

Definição 5.5. *Seja $\mathscr{U}$ o espaço umbral formado com as letras do alfabeto $\mathscr{A}$ e seja $\mathscr{B}$ o espaço dos monômios colchete. Seja M um monômio colchete em $\mathscr{B}$. Dois colchetes, $[\alpha \quad \gamma]$ e $[\beta \quad \delta]$ em M formam um par cruzado se $\alpha \to \beta \to \gamma \to \delta$. Diremos que um monômio colchete é ciclicamente padrão se ele é não-nulo e nenhum par de colchetes em M formam um par cruzado.*

Se colocarmos as letras de $\mathscr{A}$ sobre um círculo, de acordo com a ordem cíclica, e olharmos o colchete $[\alpha \quad \gamma]$ como uma linha ligando α e γ, podemos ver a definição de par cruzado, como o cruzamento das linhas de dois colchetes.

Exemplo 5.6. *Consideremos o alfabeto $\mathscr{A} = \{\alpha, \beta, \gamma, \delta, ...\}$ com a ordem cíclica natural, ou seja, $\alpha \to \beta \to \gamma \to \delta \to ....$ Notemos que o monômio colchete $M = [\alpha \quad \beta][\beta \quad \gamma][\gamma \quad \delta]$ é um monômio colchete ciclicamente padrão.*

Lema 5.7. *(O Algoritmo de Ordenação Circular) Todo monômio colchete pode ser escrito como uma combinação linear com coeficientes inteiros de monômios ciclicamente padrão.*

Demonstração: Seja M um monômio colchete e seja $\mathscr{C}$ uma lista (com devidas multiplicidades) dos pares cruzados de colchetes de M. O comprimento $|\mathscr{C}|$ de $\mathscr{C}$ é chamado de número de cruzamento de M. Suponha que M não é ciclicamente padrão. Sejam $[\alpha \quad \gamma]$ e $[\beta \quad \delta]$, um par cruzado de M, e escreva $M = [\alpha \quad \gamma][\beta \quad \delta]M'$. Pelo Lema 1.25,

$$M = [\alpha \quad \gamma][\beta \quad \delta]M' = [\alpha \quad \beta][\gamma \quad \delta]M' + [\alpha \quad \delta][\beta \quad \gamma]M'.$$

Afirmamos que ambos os monômios colchete sobre o lado direito tem o número de cruzamentos estritamente menor que $|\mathscr{C}|$. De fato, sejam $[\xi \quad \eta]$ e $[\zeta \quad \omega]$, um par cruzado em $[\alpha \quad \beta][\gamma \quad \delta]M'$. Se $[\xi \quad \eta]$ e $[\zeta \quad \omega]$ estão ambos no monômio M', então o par, $[\xi \quad \eta]$ e $[\zeta \quad \omega]$, está também em $\mathscr{C}$, e temos o resultado. Se $[\xi \quad \eta] = [\alpha \quad \beta]$, então nós temos $\alpha \to \zeta \to \beta \to \omega$. Neste caso, temos duas possibilidade: se ω está entre β e δ, então $\zeta \to \beta \to \omega \to \delta$ e portanto, $[\zeta \quad \beta]$, $[\omega \quad \delta]$,

é um par cruzado de colchetes em $\mathscr{C}$. Mas, se $\omega = \delta$ ou ω está entre δ e α, então $\zeta \to \gamma \to \omega \to \alpha$ e portanto, $[\zeta \quad \omega]$, $[\alpha \quad \gamma]$, é um par cruzado de colchetes em $\mathscr{C}$. Analogamente, fazemos os mesmos argumentos para $[\xi \quad \eta] = [\gamma \quad \delta]$. Portanto, todo par cruzado de colchetes no monômio colchete $[\alpha \quad \beta][\gamma \quad \delta]M'$ está associado, de modo injetivo, a um par cruzado de colchetes em $\mathscr{C}$. Entretanto, o par $[\alpha \quad \gamma][\beta \quad \delta]$ em $\mathscr{C}$, não está associado com qualquer par cruzado em $[\alpha \quad \beta][\gamma \quad \delta]M'$. Portanto, o número cruzado de $[\alpha \quad \beta][\gamma \quad \delta]M'$ é estritamente menor que $|\mathscr{C}|$. Analogamente, o número cruzado de $[\alpha \quad \delta][\beta \quad \gamma]M'$ é estritamente menor que $|\mathscr{C}|$.

Continuando esse processo, nós podemos escrever o monômio colchete M como uma combinação linear (com coeficientes inteiros) de monômios colchete cujo número cruzado são zero, que é, um monômio colchete ciclicamente padrão. ■

Lema 5.8. *Os monômios colchete ciclicamente padrão formam um conjunto linearmente independente.*

Demonstração: Suponhamos que são linearmente dependente. De todas as possíveis relações de dependência linear não-trivial entre monômios colchete ciclicamente padrão, escolha uma, $\sum_{k=1}^{m} c_k M_k = 0$, em que:

(a) $c_k \neq 0$ para todo k;

(b) o número de letras distintas é o menor possível;

(c) sujeito a (b), o número máximo de colchetes em um monômio M_k ocorrendo na relação linear é o menor possível.

Seja $\mathscr{A}'$ o conjunto de todas as letras ocorrendo na relação linear, ciclicamente ordenado pela restrição da ordem cíclica sobre $\mathscr{A}$. Seja δ e ϵ duas letras em $\mathscr{A}'$, tais que $\delta \Rightarrow \epsilon$ na ordem restrita. Pela condição (c), o colchete $[\delta \quad \epsilon]$ não é um fator comum a todos os monômios colchete M_k. Assim, colocando δ igual a ϵ, nem todos os monômios M_k se anularão. Pela escolha de δ e ϵ, os monômios restantes continuarão ciclicamente padrão. Obtemos assim, uma combinação linear não trivial com uma quantidade estritamente menor de letras distintas, contradizendo nossa escolha inicial. ■

Teorema 5.9. *Os monômios colchete ciclicamente padrão formam uma base para o espaço $\mathscr{B}$ dos polinômios colchete.*

Demonstração: Esse teorema sai diretamente dos Lemas 5.7 e 5.8. ■

Definição 5.10. *Sejam α e ϵ letras em $\mathscr{A}$. Definimos o segmento (α, ϵ) como o conjunto de todas as letras estritamente entre α e ϵ, ou seja,*

$$(\alpha, \epsilon) = \{\gamma : \alpha \to \gamma \to \epsilon\}.$$

Notemos que os segmentos (α, ϵ) e (ϵ, α) são distintos, pois $\mathscr{A} = (\alpha, \epsilon) \cup (\epsilon, \alpha) \cup \{\epsilon, \alpha\}$.

Definição 5.11. *Seja M um monômio colchete. Um colchete $[\gamma \quad \delta]$ é diagonal se ambas as condições $\gamma \Rightarrow \delta$ e $\delta \Rightarrow \gamma$ não ocorrem. Denotemos por $\mathscr{A}_M$, o conjunto de todas as letras ocorrendo em M ordenadas ciclicamente pela restrição da ordem cíclica sobre $\mathscr{A}$. Além disso, um segmento não-vazio (α, ϵ) em $\mathscr{A}_M$ é um segmento exterior de M se para toda letra γ em (α, ϵ), não existem colchetes diagonais em M contendo γ. Um segmento exterior é maximal se ele não está contido estritamente em outro segmento exterior.*

Exemplo 5.12. *Seja $\mathscr{A} = \{\alpha, \beta, \gamma, \delta, \sigma, \epsilon, \omega\}$, com a ordem cíclica natural. Sejam $M = [\alpha \quad \delta][\gamma \quad \epsilon][\alpha \quad \epsilon]$ e $\mathscr{A}_M = \{\alpha, \gamma, \delta, \epsilon\}$, com a ordem cíclica induzida. Temos que $(\alpha \quad \delta)$ é um segmento exterior de M e $(\alpha \quad \epsilon)$ é um segmento exterior maximal de M.*

Proposição 5.13. *Seja M um monômio colchete ciclicamente padrão. Então, M não tem colchetes diagonal ou existem no mínimo dois segmentos exteriores maximais de M.*

Demonstração: Seja $\mathscr{A}$ o conjunto das letras ocorrendo em M. Vamos demonstrar essa Proposição, usando indução sobre $|\mathscr{A}|$.

Suponhamos que M tem colchetes diagonais. Se $[\alpha \quad \epsilon]$ é um colchete, entenderemos como a distância de $[\alpha \quad \epsilon]$ pelo comprimento do menor caminho não direcionado entre α e ϵ (o número de setas contadas no caminho entre as letras). Agora, dentre todos os colchetes diagonais de M, escolhemos um, $\pm[\alpha \quad \epsilon]$, para o qual a distancia é mínima e é alcançada pelo caminho direcionado de α para ϵ. Como M é ciclicamente padrão, então M não tem par cruzado de colchetes, o que significa que (α, ϵ) é um segmento exterior maximal. De fato, se existisse uma letra γ em (α, ϵ) tal que γ estivesse em algum colchete diagonal, digamos $[\gamma \quad \delta]$, teríamos que: se $\delta \in (\alpha, \epsilon)$, então $\pm[\alpha \quad \epsilon]$ não seria minimal, o que contradiz nossa hipótese inicial; caso $\delta \in (\alpha, \epsilon)$, $[\alpha \quad \epsilon]$ e $[\gamma \quad \delta]$ seria um par cruzado, o que não ocorre pois M é ciclicamente padrão. Além disso, é maximal pois se (α, ϵ) estivesse contido estritamente em um segmento exterior, teríamos que α (ou ϵ) seria uma letra nesse segmento, que é uma letra do colchete diagonal $[\alpha \quad \epsilon]$, o que seria um absurdo.

Resta agora encontrarmos o segundo segmento exterior maximal. Para isso, vamos primeiro observar que os colchetes em M podem ser separados em 3 blocos:

- os colchetes contendo somente letras de $\{\alpha, \epsilon\} \cup (\alpha, \epsilon)$;
- os colchetes iguais a $[\alpha \quad \epsilon]$;

- os colchetes contendo somente letras de $\{\alpha, \epsilon\} \cup (\epsilon, \alpha)$.

Consideremos o sub-monômio M' de M, consistindo de todos os colchetes em M do segundo e terceiro blocos. Como M é ciclicamente padrão e $|\mathscr{A}'_M| < |\mathscr{A}_M|$, por hipótese de indução, M' não tem colchete diagonal, segundo a ordem cíclica induzida da ordem de $\mathscr{A}$, ou M' tem dois segmentos exterior maximais.

No primeiro caso, teremos que (ϵ, α) será segmento exterior maximal de M. De fato, se caso existisse uma letra γ em (ϵ, α) que está contido em algum colchete diagonal, esse colchete teria, além da letra γ, outra letra que pertenceria a $\mathscr{A}_M - \mathscr{A}'_M$, digamos μ, então o colchete $[\gamma \quad \mu]$ (ou $-[\gamma \quad \mu]$), seria um colchete diagonal de M, e portanto, teríamos que $\pm[\gamma \quad \mu]$ e $[\alpha \quad \epsilon]$ seria um par cruzado de M, o que é um absurdo pois M é ciclicamente padrão. A maximalidade de (ϵ, α), sai do fato de que se isso não ocorresse, teríamos que α (ou ϵ) seria uma letra nesse segmento que estaria contida no colchete diagonal $[\alpha \quad \epsilon]$, o que seria um absurdo.

No segundo caso, temos que um dos segmentos exterior maximal de M' não contem o subconjunto $\{\alpha, \epsilon\}$. De fato, se caso os dois segmentos contivessem $\{\alpha, \epsilon\}$, então teríamos um absurdo pois $[\alpha \quad \epsilon]$ é diagonal. Portanto, o segmento exterior que não contem o conjunto $\{\alpha, \epsilon\}$, também é um segmento exterior maximal de M. Seja (ψ, ω) esse segmento exterior maximal de M'. De fato, por construção, esse segmento exterior não contêm letras de (α, ϵ), e portanto não está contido em (α, ϵ). Como ele não contem o conjunto $\{\alpha, \epsilon\}$, segue que esse segmento exterior está contido em (ϵ, α). Agora, suponhamos que ele não é exterior maximal de M. Portanto, existe $\gamma \in (\psi, \omega)$, tal que $[\gamma \quad \eta]$ é diagonal, com $\eta \in \mathscr{A}_M$. Se $\eta \in \mathscr{A}'_M$, absurdo pois (ψ, ω) é exterior em M'; se $\eta \in \mathscr{A} - \mathscr{A}'_M$, teríamos que $\eta \in (\alpha, \epsilon)$, o que também é um absurdo pois (α, ϵ) é exterior e $[\gamma \quad \eta]$ é diagonal. Isto encerra a demonstração.

■

Exemplo 5.14. *Para a proposição anterior ficar mais clara, vamos mostrá-la em um exemplo. Sejam* $M = [\alpha \quad \delta][\alpha \quad \beta][\beta \quad \delta][\beta \quad \gamma][\epsilon \quad \alpha]$ *um monômio colchete ciclicamente padrão e* $\mathscr{A} = \{\alpha, \beta, \gamma, \delta, \epsilon\}$*, o conjunto das letras aparecendo em* M *não trivialmente. Consideremos em* $\mathscr{A}$ *a ordem cíclica padrão. Temos que* M *tem dois colchetes diagonais, a dizer* $[\alpha \quad \delta]$ *e* $[\beta \quad \delta]$*. Escolhemos o colchete* $[\beta \quad \delta]$*, de comprimento mínimo. Temos que* (β, δ) *é um segmento exterior, pois* γ *está em* (β, δ) *e está também em* $[\beta \quad \gamma]$*, porém este colchete não é diagonal. Mais ainda,* (β, δ) *é segmento exterior maximal, pois* (α, ϵ)*,* (β, ϵ)*,* (β, α) *e* (α, δ)*, são os únicos segmentos na qual* (β, δ) *está contido estritamente, porém, nenhum deles é exterior. Portanto,* (β, δ) *é segmento exterior maximal.*

Se fizéssemos os mesmo argumentos, poderíamos mostrar que (δ, α) é um segmento exterior maximal, porém, vamos fazer isso usando a Proposição anterior. Vamos então procurar o segundo segmento exterior maximal. Notemos que de fato ele existe pela Proposição anterior. Separando os colchetes de M nos 3 blocos, segundo a demonstração da Proposição anterior, temos:

- $[\beta \quad \gamma]$;
- $[\beta \quad \delta]$;
- $[\epsilon \quad \alpha]$,$[\alpha \quad \beta]$,$[\alpha \quad \delta]$.

Assim, $M' = [\epsilon \quad \alpha][\alpha \quad \beta][\beta \quad \delta][\alpha \quad \delta]$. Como M' tem colchete diagonal, a dizer $[\alpha \quad \delta]$, M' tem dois segmentos exterior maximal, (α, δ) e (δ, α). O segmento (δ, α) satisfaz o que queremos.

Vamos agora olhar para os monômios colchetes elementares e ver um dos principais resultados desta seção: o Lema de Kempe. Com ele, poderemos escrever qualquer monômio colchete regular como uma combinação linear de produtos de monômios colchete elementares. Mas antes, algumas definições e exemplos.

Definição 5.15. *Seja $\mathscr{B}$ o espaço dos polinômios colchete formado com o alfabeto $\mathscr{A} = \{\alpha, \beta, ..., \epsilon, u\}$ consistindo de um número finito de letras gregas e uma letra romana u. Lembremos que um monômio colchete M é regular de grau d se para toda letra umbral grega α em $\mathscr{A}$, o número de ocorrências de α em M é igual a d; o número de ocorrências da letra romana u é chamada de ordem de M, e não precisa ser igual a d. Definimos o monômio colchete elementar como um monômio colchete regular de grau um, ou um monômio colchete regular de grau dois que não é o produto de dois monômios colchete regular de grau um.*

Exemplo 5.16. *Seja $\mathscr{A} = \{\alpha, \beta, \gamma, \delta, \epsilon, u\}$. Os monômios $[\alpha \quad \beta][\gamma \quad \delta][\epsilon \quad u]$, $[\alpha \quad \beta][\gamma \quad u][\delta \quad u][\epsilon \quad u]$ e $[\alpha \quad \beta][\beta \quad \gamma][\gamma \quad \delta][\delta \quad \epsilon][\epsilon \quad \alpha]$, são todos monômios colchete elementares.*

Definição 5.17. *Sejam $\mathscr{A} = \{\alpha, \beta, \dots, \epsilon, u\}$ e $\mathscr{E}$ um outro alfabeto de letras gregas. Seja $e : \mathscr{E} \to \mathscr{A} - \{u\}$ uma função. Duas letras ξ e η são equivalentes (à γ), se $e(\xi) = e(\eta) = \gamma$. Um monômio colchete M formado com letras de $\mathscr{E} \cup \{u\}$ é um monômio colchete com letras equivalentes. Seja M um monômio colchete com letras equivalentes, nós diremos que M é regular, se o monômio colchete $e(M)$, ou seja, o monômio colchete M tomando a imagem de cada letra η de M pela função e, é regular. Analogamente, definimos se M é ciclicamente padrão.*

Observação 5.18. *Os resultados que temos sobre monômios colchete regular (ou ciclicamente padrão), também valem para monômios colchete regular (ou ciclicamente padrão) com letras equivalentes, pois esses resultados são todos provados exibindo-se um algoritmo construtivo.*

Proposição 5.19. *(Lema de Kempe) Todo monômio colchete regular formado com o alfabeto $\mathscr{A} = \{\alpha, \beta, ..., \epsilon, u\}$ pode ser escrito como uma combinação linear com coeficientes inteiros de produtos de monômios colchete elementares.*

Demonstração: A prova desse Lema será apresentada da seguinte forma: primeiro melhoraremos o enunciado, usando a Definição 5.17 e a Observação 5.18, ou seja, não trabalharemos com monômios colchete, mas sim, com monômios colchete com letras equivalentes. Então, procederemos usando indução sobre o número de letras gregas de $\mathscr{A}$, ou seja, sobre $|\mathscr{A}| - 1$. Os três primeiros casos serão feitos explicitamente, assim, poderemos tratar apenas do problema quando temos mais que três letras gregas. No passo indutivo, verificaremos que existem dois segmentos exterior maximais em M. Existirá então uma letra grega em algum seguimento exterior, daí então analisaremos o caso quando o sucessor e o antecessor dessa letra grega são letras gregas, e o caso quando isso não ocorre.

Vamos analisar o primeiro passo da indução. Se $|\mathscr{A}| - 1 = 1$, temos que $\mathscr{A} = \{\alpha, u\}$, e portanto temos apenas $[\alpha \quad u]$ como monômio colchete elementar, e assim, claramente a afirmação é verdadeira. Se $|\mathscr{A}| - 1 = 2$, temos que $\mathscr{A} = \{\alpha, \beta, u\}$, e portanto, temos somente dois monômios colchete elementar (a menos de permutação das letras gregas ou inversão de alguns colchete), a dizer $[\alpha \quad u][\beta \quad u]$ e $[\alpha \quad \beta]$, ambos de grau 1. Neste caso, a afirmação também é verdadeira. Para último caso particular, vamos analisar quando $|\mathscr{A}| - 1 = 3$, ou seja, $\mathscr{A} = \{\alpha, \beta, \gamma, u\}$. Aqui temos, a menos de permutação das letras gregas ou inversão de colchetes, os seguintes monômios colchete elementar: $[\alpha \quad u][\beta \quad u][\gamma \quad u]$ e $[\alpha \quad \beta][\gamma \quad u]$, ambos de grau 1 e, $[\alpha \quad \beta][\beta \quad \gamma][\gamma \quad \alpha]$ e $[\alpha \quad \beta][\beta \quad \gamma][\gamma \quad u][\alpha \quad u]$ são os de grau 2. Além disso, notemos que de fato qualquer monômio colchete regular formado com o alfabeto $\mathscr{A} = \{\alpha, \beta, \gamma, u\}$, pode ser escrito como uma combinação linear com coeficientes inteiros dos monômios colchete elementar que apresentamos.

Para o passo indutivo, assumiremos como hipótese de indução, que existe um algoritmo para escrevermos qualquer monômio colchete regular com letras equivalentes como uma combinação linear com coeficientes inteiros de produtos de monômios colchete elementar com letras equivalentes, se $\mathscr{A}$ tem $n - 1$ ou menos, letras gregas.

Seja $\mathscr{A}$ um alfabeto consistindo de n letras gregas e uma letra romana u, com a ordem cíclica padrão. Seja ainda, M um monômio colchete regular sobre $\mathscr{A}$,

e mais, suponhamos que M não é elementar, pois caso contrário, não há o que fazer. Como os monômios colchete ciclicamente padrão formam uma base para o espaço dos polinômios colchete, podemos supor que M é ciclicamente padrão. Agora, como M é ciclicamente padrão, temos pelo Teorema 5.13 que M não tem colchetes diagonais ou existem pelo menos dois segmentos exterior maximal de M. No primeiro caso, M será produto de potências de monômios colchete elementar. Vamos então supor que M tem pelo menos um colchete diagonal. Como existem dois segmentos exterior maximal em M, temos que existe uma letra β em um segmento exterior. Temos dois casos:

I. existe uma tal letra grega β tal que ambos, o predecessor α e o antecessor γ, são letras gregas;

II. para toda letra grega, o predecessor ou o antecessor é a letra romana u.

Para analisarmos o caso I, podemos trocar M por um monômio mais específico, que mostraremos na seguinte afirmação:

Afirmação 5.20. *O monômio colchete M pode ser escrito como uma combinação linear com coeficientes inteiros de monômios colchete N (que podem não ser ciclicamente padrão) tais que β está ainda em um segmento exterior e $[\alpha \quad \gamma]$ não aparece como um colchete em N, isto é,*

$$N = [\alpha \quad \beta]^{d-k}[\beta \quad \gamma]^k N',$$

onde N' é um monômio colchete que não contém a letra β e o colchete $[\alpha \quad \gamma]$.

De fato, suponhamos que M tem grau d (de regularidade), ordem t e contenha r colchetes iguais a $[\alpha \quad \gamma]$. Como estamos no primeiro caso, ou seja, temos que $\alpha \Rightarrow \beta$ e $\beta \Rightarrow \gamma$ ocorrem, e M tem um fator $[\alpha \quad \gamma]^r$, segue que não podemos ter em M um colchete da forma $[\beta \quad x]$, com $x \neq \alpha$ e $x \neq \gamma$, pois M é ciclicamente padrão. Portanto, temos em M, d colchetes da forma $[\beta \quad x]$, com $x = \alpha$ ou $x = \gamma$. Então, tínhamos inicialmente $3d$ letras (α, β e γ) e tiramos $2d$ letras, dos colchetes $[\beta \quad x]$, e mais $2r$ letras, dos colchetes $[\alpha \quad \gamma]$. Restou assim, $d - 2r$ letras, entre as letras α e γ, que nos darão exatamente $d - 2r$ colchetes, pois α e γ não podem estar mais em um mesmo colchete por suposição. Portanto, temos $d + r + d - 2r = 2d - r$ colchetes contendo α, γ ou β. Pela Observação 1.45, temos em M $\frac{1}{2}dn + \frac{1}{2}t$ colchetes. Portanto, existem $\frac{1}{2}dn + \frac{1}{2}t - (2d - r) = r + \frac{1}{2}t + \frac{1}{2}d(n-4)$ colchetes em M não contendo as letras α, γ ou β. Como já mostramos os casos para $n = 1, 2, 3$, podemos supor $n \geq 4$, e assim temos que existem pelo menos r colchetes em M não contendo as letras α, γ ou β.

Seja $[\delta \quad \epsilon]$ um colchete em M não contendo α, γ ou β. Pelo Syzygy (Lema 1.25), temos:

$$[\delta \quad \epsilon][\alpha \quad \gamma] = [\alpha \quad \epsilon][\delta \quad \gamma] - [\alpha \quad \delta][\epsilon \quad \gamma].$$

Portanto, se escrevermos $M = [\delta \quad \epsilon][\alpha \quad \gamma]M'$, após aplicar o Syzygy, temos

$$M = [\alpha \quad \epsilon][\delta \quad \gamma]M' - [\alpha \quad \delta][\epsilon \quad \gamma]M' = M_1 - M_2,$$

onde M_1 e M_2 são monômios colchetes contendo $r-1$ colchetes iguais a $[\alpha \quad \epsilon]$ e pelo menos $r-1$ colchetes não contendo α, γ ou β. Além disso, note que M_1 e M_2 não são necessariamente ciclicamente padrão, porém, continuam sendo regulares de mesmo grau d. Podemos então continuar esse processo até que não reste nenhum monômio colchete na expansão de M com o colchete $[\alpha \quad \gamma]$. Mais ainda, ao usar o Syzygy, nós não alteramos os colchetes contendo a letra β, portanto, temos que cada monômio colchete na expansão de M, pode ser escrito da forma que queremos.

Isto encerra a prova da nossa afirmação.

Podemos então provar o resultado desse Lema, supondo que

$$M = N = [\alpha \quad \beta]^{d-k}[\beta \quad \gamma]^k N',$$

onde N' não contem colchetes da forma $[\alpha \quad \gamma]$ e nem a letra β. Note ainda, que como o grau de N é d, temos que o número total de ocorrências de α e γ em N' é exatamente d.

Definimos então que α e γ são letras equivalentes a uma nova letra ζ, ou seja, $e(\alpha) = e(\gamma) = \zeta$, onde e é uma função que sai de $\mathscr{A} - \{u\}$ e chega em $\mathscr{E} - \{u\}$, com $\mathscr{E} = (\mathscr{A} - \{\alpha, \beta, \gamma\}) \cup \{\zeta\}$. A partir disso, temos que N' é um monômio colchete regular com letras equivalentes, para o alfabeto $\mathscr{E}$. Como $\mathscr{E}$ tem $n-1$ letras, segue por hipótese de indução, que podemos escrever N' da forma

$$N' = \sum_i b_i E_{i1} E_{i2} \ldots E_{ik(i)},$$

onde os $b_i's$ são números inteiros e E_{ij} são monômios colchete elementar com letras equivalentes.

Portanto,

$$N = \sum_i b_i [\alpha \quad \beta]^{d-k}[\beta \quad \gamma]^k E_{i1} E_{i2} \ldots E_{ik(i)}.$$

Mas, nós queremos obter o resultado para monômios colchete elementar com letras no alfabeto $\mathscr{A}$, e não com letras equivalentes. Para isso, vamos distribuir os colchetes $[\alpha \quad \beta]$ e $[\beta \quad \gamma]$ nos monômios E_{ij}, de modo que isso ocorra.

A distribuição será feita do seguinte modo:

I. se E_{ij} é de grau dois e contem duas ocorrências de α (ou γ), então colocaremos $\widehat{E}_{ij} = [\beta \quad \gamma]^2 E_{ij}$ (ou $[\alpha \quad \beta]^2 E_{ij}$);

II. se E_{ij} é de grau dois e contem uma ocorrência cada de α e γ, então colocaremos $\widehat{E}_{ij} = [\alpha \quad \beta][\beta \quad \gamma] E_{ij}$;

III. se E_{ij} é de grau um e contem uma ocorrência de α (ou γ), então colocaremos $\widehat{E}_{ij} = [\beta \quad \gamma] E_{ij}$ (ou $[\alpha \quad \beta] E_{ij}$).

Como E_{ij} é elementar com letras equivalentes, é fácil ver que $\hat{E}_{ij}$ é elementar, pelo descrito em I, II e III. Além disso, o número de colchetes $[\alpha \quad \beta]$ e $[\beta \quad \gamma]$ é a quantidade exata para tornar todos os E_{ij} elementares, pela regularidade de N.

Portanto,

$$N = \sum_i b_i \hat{E}_{i1} \hat{E}_{i2} ... \hat{E}_{ik(i)},$$

onde $\hat{E}_{ij}$ são monômios colchete elementar.

Vamos agora tratar do caso II. Para isso, sem perda de generalidade, fixemos que $\beta \Rightarrow u$.

Primeiramente, notemos que este caso só ocorre se existem exatamente dois segmentos exterior maximal e eles são da forma (α, u) e (u, γ). De fato, suponhamos que um desses segmentos exterior maximal, digamos (u, γ), é da forma (ω, γ). Seja $\delta \in (\omega, \gamma)$, então, existe ξ tal que $[\delta \quad \xi]$ é um colchete em M e, $\delta \Rightarrow \xi$ ou $\xi \Rightarrow \delta$, ocorre. Suponhamos que ocorra $\delta \Rightarrow \xi$, sem perda de generalidade. Então, $\xi \in (\omega, \gamma)$ ou $\xi = \gamma$ ocorre. Se $\xi \in (\omega, \gamma)$ ocorrer, então necessariamente temos $\xi = u$, pois qualquer outro caso já é um absurdo, pela hipótese de que o sucessor ou o antecessor de cada letra em um segmento exterior é u. Ora, $u \in (\omega, \gamma)$ e (α, u) é segmento exterior, então $\omega \in (\alpha, u)$, pois caso contrário, (α, u) não seria maximal. Absurdo, pois temos que para ω em (α, u), não ocorre $\omega \Rightarrow u$ nem $u \Rightarrow \omega$. Agora, se ocorrer $\xi = \gamma$, então necessariamente temos $u \Rightarrow \delta$. Chegamos novamente em um absurdo, seguindo o raciocínio anterior. O caso em que os dois segmentos exterior maximal são da forma (α, ω) e (δ, γ), trivialmente não ocorre.

Como os dois segmentos exterior maximal são da forma (α, u) e (u, γ), então cada um deles tem necessariamente apenas um elemento (a hipótese inicial prova direto essa afirmação), digamos $(\alpha, u) = \{\beta\}$ (pois $\beta \Rightarrow u$) e $(u, \gamma) = \{\delta\}$. Assim, nós temos $\alpha \to \beta \to u \to \gamma \to \delta$, na ordem cíclica. Com isso, afirmamos o seguinte:

Afirmação 5.21. *Sob estas condições,* $[\zeta \quad u]$ *é um colchete em* M *para toda letra grega* ζ *em* $\mathscr{A}$*.*

De fato, suponhamos que $[\zeta \quad u]$ não é um colchete em M, para algum $\zeta \in \mathscr{A}$. Então, pela ordem cíclica, $\zeta \neq \beta$ e $\zeta \neq \gamma$. Como ζ não está em um

segmento exterior, pois caso contrário ele estaria em algum dos maximais, segue que existe uma letra grega η, tal que $[\zeta \quad \eta]$ é diagonal. Vamos escolher um η tal que a distância até ζ seja minimal. Pela mesma ideia usada na demonstração da Proposição 5.13, concluímos que o segmento (ζ, η) ou (η, ζ), é exterior. Suponhamos (ζ, η). Como, (ζ, η) não é maximal, pois é diferente dos dois iniciais e só existem dois segmento exterior maximal, temos que esse segmento está contido em algum dos maximais, e mais, sendo não vazio, ele é necessariamente igual a um deles. Como $\zeta \neq u$, então temos que ter $\zeta = \alpha$ e $\eta = u$, o que contradiz nossa suposição inicial. E isso mostra nossa afirmação.

Então, direto dessa afirmação, temos que

$$M = (\prod_{\zeta \in \mathscr{A}} [\zeta \quad u])M'.$$

Como $\prod_{\zeta \in \mathscr{A}} [\zeta \quad u]$ é um monômio colchete elementar de grau 1, então M' é regular de grau $d-1$, e portanto, podemos repetir esse processo inteiro para M'. Obtemos assim o resultado desejado.

■

Antes de mostramos o último resultado necessário para concluirmos o Teorema de Finitude, vamos olhar para o que já temos, para ver que de fato, o Lema de Hilbert é de fato essencial. Pela Proposição 2.27, todo covariante de formas binárias de grau n pode ser expresso como uma combinação linear de termos diferença simétricos $\langle S \,|M\rangle$, onde M é um monômio colchete regular, que é escrito no alfabeto $\{1, 2, ..., n, u\}$. Se olharmos os números $1, 2, ..., n$ como letras gregas, podemos usar o Lema de Kempe para escrever M como uma combinação linear de produtos de monômios colchete elementares, ou seja, o conjunto dos monômios colchete elementar é um conjunto gerador para os monômios colchete regular. Porém, as simetrizações desses monômios colchetes elementares não formam (exceto quando $n = 1$) um conjunto de geradores para os termos diferença simétricos. O Lema de Hilbert nos dará esse conjunto de geradores.

Lema 5.22. *(Hilbert) Seja $r = n!$ e seja $\{E_1, ..., E_m\}$ um conjunto de geradores para o conjunto de monômios colchete regular sobre o alfabeto $\{1, 2, ..., n, u\}$. Então o conjunto de termos diferença simétrico*

$\langle S \,|E_1^{e_1} E_2^{e_2} ... E_m^{e_m}\rangle$, $0 \leq e_i \leq r-1$, $e_i \neq 0$ *para algum i;*

$\langle S \,|E_i^r\rangle$, $0 \leq i \leq m$,

é um conjunto de geradores para o conjunto de termos diferença simétrico.

Demonstração: Sejam $\pi \in \Omega_n$ e $E_i \in \{E_1, ..., E_m\}$. Vamos escrever o produto de $(S - \pi(E_i))$, para todo $\pi \in \Omega_n$, e depois desenvolve-lo. Desse modo temos:

$$\prod_{\pi \in \Omega_n} (S - \pi(E_i)) = S^r - a_1(\pi(E_i))S^{r-1} + a_2(\pi(E_i))S^{r-2} + ... \pm a_r(\pi(E_i)),$$

onde, $a_j(\pi(E_i))$ são as funções simétricas elementares nos monômios colchete $\pi(E_i)$.

Como por construção E_i é raiz desse polinômio, temos a seguinte relação, ao substituirmos E_i na expressão acima, e isolarmos o termo E_i^r:

$$E_i^r = a_1(\pi(E_i))E_i^{r-1} - a_2(\pi(E_i))E_i^{r-2} + ... \pm a_r(\pi(E_i))$$

Multiplicando a expressão anterior por $k - r$, para $k \geq r$, obtemos:

$$E_i^k = a_1(\pi(E_i))E_i^{k-1} - a_2(\pi(E_i))E_i^{k-2} + ... \pm a_r(\pi(E_i))E_i^{k-r}.$$

Lembrando que as funções simétricas elementares são invariantes pelas permutações $\pi \in \Omega_n$, e sendo M um monômio colchete, temos:

$$\langle S \,|a_j(\pi(E_i))M\rangle = \sum_{\pi \in \Omega_n} a_j(\pi(E_i))\pi(M) = a_j(\pi(E_i)) \langle S \,|M\rangle .$$

Para $k \geq r$, obtemos então:

$$\begin{aligned} \left\langle S \left| E_1^{e_1} ... E_i^k ... E_m^{e_m} \right. \right\rangle &= a_1(\pi(E_i)) \left\langle S \left| E_1^{e_1} ... E_i^{k-1} ... E_m^{e_m} \right. \right\rangle \\ &\quad - ... \pm a_r(\pi(E_i)) \left\langle S \left| E_1^{e_1} ... E_i^{k-r} ... E_m^{e_m} \right. \right\rangle . \end{aligned}$$

Notemos que os expoente dos E_i no lado direito da expressão acima, são estritamente menor que r. Repetindo esse processo, podemos reduzir o expoente dos E_i, até ficarem estritamente menor que r, e obtemos:

$$\langle S \,|M\rangle = \left\langle S \left| \sum_i b_i E_1^{i1} E_2^{i2} ... E_m^{im} \right. \right\rangle$$

como uma combinação linear de produtos de $a_j(\pi(E_i))$ e $\langle S \,|b_i E_1^{e_1} E_2^{e_2} ... E_m^{e_m}\rangle$.

Resta agora eliminarmos os $a_j(\pi(E_i))$, de modo a obtermos o resultado desejado. Para isso, vamos trocar esses funções simétricas por outras funções simétricas convenientes.

Relembremos que as funções simétricas elementares $a_j(\pi(E_i))$ podem ser escritas em termos de soma de potências das funções simétricas $h_j(\pi(E_i))$, onde

$$h_j(\pi(E_i)) = \sum_{\pi \in \Omega_n} \pi(E_i)^j = \left\langle S \left| E_i^j \right. \right\rangle .$$

■

Demonstração: (Teorema de Finitude)

Pela Proposição 2.27, basta encontrarmos um conjunto finito de geradores para os termos diferença simétricos. Mas, a existência de tal conjunto é garantida pela Lema de Hilbert, e isso encerra a demonstração.

■

O Teorema de Finitude pode ser escrito ainda, da seguinte forma mais explicita, bastando aplicar o Lema de Hilbert para o conjunto dos monômios colchete elementar, como segue:

Teorema 5.23. *Seja* $\{E_1, \dots, E_m\}$ *o conjunto dos monômios colchete elementar formados com o alfabeto* $\{1, 2, \dots, n, u\}$. *O conjunto dos covariantes cuja representação em termos de raízes homogeneizadas são dadas por*

$\langle S \,|E_1^{e_1} E_2^{e_2} \dots E_m^{e_m}\rangle$, $0 \leq e_i \leq n! - 1$, $e_i \neq 0$ *para algum* i;

$\left\langle S \,\middle|E_i^{n!}\right\rangle$, $0 \leq i \leq m$,

é um conjunto de geradores finito para o conjunto dos covariantes de formas binárias de grau n.

5.2 Conjuntos de Geradores

Nesta seção, calcularemos explicitamente um conjunto de geradores para os covariantes das cúbicas binárias, como aplicação do Teorema de Finitude, mais ainda, explicitaremos um conjunto minimal de geradores. Para os invariantes de cúbicas binárias, temos uma solução mais simples. No Exemplo 2.29, é mostrado que todos os invariantes não-nulos das cúbicas binárias são um múltiplo constante de uma potência do discriminante das cúbicas binárias.

Vamos então mostrar explicitamente esse conjunto. Considere o alfabeto $\mathscr{A} = \{1, 2, 3, u\}$.

Primeiramente, listaremos todos os monômios colchetes elementares formados com esse alfabeto. Olhando para a ordem de cada monômio, temos a seguinte lista:

- ordem 0: $[1 \quad 2][2 \quad 3][3 \quad 1]$;
- ordem 1: $[1 \quad 2][3 \quad u]$, $[1 \quad 3][2 \quad u]$, $[2 \quad 3][1 \quad u]$;
- ordem 3: $[1 \quad u][2 \quad u][3 \quad u]$.

Notemos que não existem monômios colchete elementar de ordem 2, pois os monômios colchete regulares de ordem 2, são da forma $[1 \quad 2][2 \quad 3][3 \quad u][1 \quad u]$, e eles são produto de dois monômios colchete elementar de ordem 1. Além disso, todos os monômios colchete regular de grau maior que 3, não são elementar.

A lista acima pode ser reduzida um pouco se observarmos que:

$$[2 \quad 3][1 \quad u] = [1 \quad 3][2 \quad u] - [1 \quad 2][3 \quad u].$$

Temos então que: $A = [1 \quad 2][2 \quad 3][3 \quad 1]$, $B = [1 \quad 2][3 \quad u]$, $C = [1 \quad 3][2 \quad u]$ e $D = [1 \quad u][2 \quad u][3 \quad u]$, é um conjunto de geradores para os monômios colchete regulares.

Pelo Lema de Hilbert, um conjunto de geradores para os covariantes das cúbicas é:

$(*)$ $\left\langle S \left| A^a B^b C^c D^d \right.\right\rangle$, $0 \leq a, b, c, d \leq 5$,

$\langle S \,|A^6\rangle$, $\langle S \,|B^6\rangle$, $\langle S \,|C^6\rangle$, $\langle S \,|D^6\rangle$.

Porém, neste conjunto, existem elementos em excesso. Vamos mostrar que podemos reduzir esse conjunto e deixá-lo com apenas quatro elementos. Mostraremos que esses elementos são:

$$\Delta = \langle S \,|A^2\rangle,\ f = \langle S \,|D\rangle,\ -H = \langle S \,|B^2\rangle,\ T = \langle S \,|B^2C\rangle,$$

onde, Δ é o discriminante, f é a própria forma cúbica, H a Hessiana e T, o jacobiano da f e da H.

Esses covariantes são dados umbralmente por:

$$\begin{aligned}
\Delta &= \frac{27}{2}\left\langle U \left| [\alpha \quad \beta]^2[\alpha \quad \gamma][\beta \quad \delta][\gamma \quad \delta]^2 \right.\right\rangle, \\
f &= \left\langle U \left| [\alpha \quad u]^3 \right.\right\rangle, \\
H &= 18\left\langle U \left| [\alpha \quad \beta]^2[\alpha \quad u][\beta \quad u] \right.\right\rangle, \\
T &= 108\left\langle U \left| [\alpha \quad \beta]^2[\alpha \quad \gamma][\beta \quad u][\gamma \quad u]^2 \right.\right\rangle.
\end{aligned}$$

Vamos mostrar que todos os termos diferença simétricos em $(*)$, podem ser escritos em termos de Δ, f, H e T. Primeiramente, vamos fazer algumas observações. Temos que o monômio colchete elementar D é invariante sob permutações do conjunto $\{1, 2, 3\}$, e então temos que

$$\langle U \,|DM\rangle = \sum_{\pi \in \Omega_n} D\pi(M) = D\,\langle U \,|M\rangle\,.$$

Então, todo termo diferença simétrico em $(*)$, que tiver D como um fator, exceto $\langle U \,|D\rangle$, pode ser descartado.

Para A^2 podemos aplicar o mesmo raciocínio aplicado a D, e eliminar todos os termos diferença simétrico em $(*)$ que tiverem A^2 como fator. Restaram então os termos:

$\left\langle S \left| A^a B^b C^c \right.\right\rangle$, $0 \leq b, c \leq 5$ e $0 \leq a \leq 1$,

$\langle S \,|A^2\rangle$, $\langle S \,|B^6\rangle$, $\langle S \,|C^6\rangle$, $\langle S \,|D\rangle$.

Vamos verificar os termos restantes. Para esses termos, a verificação é feita caso a caso. Aqui, apenas indicaremos o que é feito, e daremos alguns exemplos de como eliminamos alguns desses termos diferença simétricos.

Começaremos olhando os termos diferença simétricos da forma $\left\langle S \left| B^b C^c \right.\right\rangle$, ou seja, $a = 0$. Desses termos separamos $-H$ e T, e analisamos os termos restantes. Para esses termos, temos duas possibilidades: eles são nulos ou são expressos em termos de Δ, f, H e T. Como exemplos para os termos diferença simétricos nulos temos: $\langle S \,|B\rangle$, $\langle S \,|B^3\rangle$, $\langle S \,|B^5\rangle$, $\langle S \,|B^4C\rangle$. Como exemplos de termos não nulos que são expressos em termos de Δ, f, H e T, temos: $\langle S \,|BC\rangle = -\frac{1}{2}H$, $\langle S \,|B^4\rangle = \frac{1}{8}H^2$, $\langle S \,|B^6\rangle = \frac{1}{32}H^3 + 4\Delta f^2$, $\langle S \,|BC^2\rangle = T$. Para os termos diferença simétrico da forma $\left\langle S \left| AB^b C^c \right.\right\rangle$, temos a mesma análise. Como exemplos desses termos que são nulos temos: $\langle S \,|A\rangle$, $\langle S \,|AB\rangle$ e $\langle S \,|AC\rangle$. Além disso temos: $\langle S \,|AB^2C\rangle = \frac{3}{2}\Delta^2 f$.

Isso encerra a verificação.

Referências Bibliográficas

[1] Davis, C.S., *The Minimum of a Binary Quartic Form(I)*, Cambridge.

[2] Ehrenborg, R., Rota, G.C., *Apolarity and Canonical Forms for Homogeneous Polynomials*, Europ. J. Combinatorics, 14, pag.157-181 (1993).

[3] Grace, J.H., Young, A., *The Algebra of Invariants*, Cambridge Univ. Press, Cambridge (1903).

[4] Grosshans, F.D., *The work of Gian-Carlo Rota on invariant theory*, Algebra univers., 49, pag.213-258 (2003).

[5] Gurevich, G.B., *Foundations of the Theory of Algebraic Invariants*, Noordhoff, Groningen, pag.246-294 (1964).

[6] Kung, J.P.S., Rota, G.C., *The Invariant Theory of Binary Forms*, Bulletin (New Series) of the American Mathematical Society, vol 10, pag.27-85 January (1984).

[7] Kung, J.P.S., *Canonical Forms for Binary Forms of Even Degree*, Lecture Notes in Mathematics, Invariant Theory, N°1278, pag.52-61 (1987).

[8] Kung, J.P.S., *Gundelfinger's Theorem on Binary Forms*, Studies in Applied Mathematics, N°75, pag.163-170 (1986).

[9] Lang, S., *Algebra*, Graduate Texts in Mathmatics, Springer, 3ªEd., pag.190-192 (2002).

[10] Mourrain, B., Comon, P., *Decomposition of quantics in sums of powers of linear forms*, Signal Processing, 53, pag.93-107 (1996).

[11] Olver, P.J., *Classical Invariant Theory and the Equivalence Problem for Particle Lagrangians I. Binary Forms*, Advances in Mathmatics, Vol.80, pag.51-72 (1990).

[12] Sturmfels, B., *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation, Spring-Verlag, pag.117-135 (1993).