UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA APLICADA

Resultantes, Equações Polinomiais e o Teorema de Bezout

por

Fernando Colman Tura

Dissertação submetida como requisito parcial
para a obtenção do grau de

Mestre em Matemática Aplicada

Prof. Dr. Vilmar Trevisan
Orientador

Porto Alegre, Abril de 2006.

CIP - CATALOGAÇÃO NA PUBLICAÇÃO

Colman Tura, Fernando

Resultantes, Equações Polinomiais e o Teorema de Bezout / Fernando Colman Tura.—Porto Alegre: PPGMAp da UFRGS, 2006.

71 p.: il.

Dissertação (mestrado) —Universidade Federal do Rio Grande do Sul, Programa de Pós-Graduação em Matemática Aplicada, Porto Alegre, 2006.
Orientador: Trevisan, Vilmar

Dissertação: Matemática Aplicada
Resultantes, Equações polinomiais e o Teorema de Bezout

Resultantes, Equações Polinomiais e o Teorema de Bezout

por

Fernando Colman Tura

Dissertação submetida ao Programa de Pós-Graduação em Matemática Aplicada do Instituto de Matemática da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de

Mestre em Matemática Aplicada

Linha de Pesquisa: Algoritmos Numéricos e Algébricos

Orientador: Prof. Dr. Vilmar Trevisan

Banca examinadora:

Profa. Dra. Maria de Lourdes Merlini Giuliani
IM/UFSM

Profa. Dra. Ada Maria de Souza Doering
PPGMAT/IM/UFRGS

Prof. Dr. José Afonso Barrionuevo
PPGMAP/IM/UFRGS

Dissertação apresentada e aprovada em
05 de Abril de 2006.

Prof. Maria Cristina Varriale, Ph.D.
Coordenador

SUMÁRIO

LISTA DE ABREVIATURAS

$Res(f, g)$	o resultante de f e g
$\mathbf{V}(f, g)$	variedade afim de f e g
$\mathbf{I}$	o ideal
$\sqrt{I}$	o radical de I
$K[x_1, \ldots, x_n]/I$	a álgebra quociente
$\mathbb{C}^{n+1}$	o espaço vetorial $n+1$ dimensional
$\mathbb{P}^{n+1}(\mathbb{C})$	espaço projetivo n dimensional sobre $\mathbb{C}$
C, D	curvas no plano xy

RESUMO

A presente dissertação aborda uma técnica para determinar as soluções de sistemas de equações polinomiais. Esta técnica que é puramente algébrica, interliga tópicos da Matemática, como a Geometria Algébrica e a Álgebra Computacional.

Mais especificamente, estudamos a teoria de Resultantes e suas aplicações. Começamos com a motivação de encontrar as raízes comuns de dois polinômios a uma variável, em seguida é estendida para o caso mais geral de várias variáveis. Estudamos detalhadamente como obter fórmulas para o cálculo do Resultante, como por exemplo a fórmula de Macaulay e de Poisson.

A técnica para resolver sistemas de equações polinomiais é então apresentada. Terminamos apresentando uma prova de um caso particular do Teorema de Bezout, como aplicação da teoria de Resultantes. Este teorema é muito importante, pois fornece um número de soluções de um sistema de equações polinomiais.

ABSTRACT

The present work presents a classical technique to determine the solutions of systems of polynomial equations. This technique, a purely algebraic one, establish connection topics of the Mathematics, as Algebraic Geometry and Computational Algebra.

More specifically, we study the theory of Resultants and its applications. We start with the motivation to find the common roots of two polynomials of one variable, after that we extend the idea for the case most general of multivariable. We study at great length how to obtain formulas for the calculation of the Resultant, as for example the formula of Macaulay and Poisson.

We then present the tecnique, based on resultants, to find the solution of polinomial system of equations. We finish presenting a proof of a particular case of the Bezout's Theorem, as application of the theory of Resultants. This theorem is considered very important, since it provides the number of solutions of a system of polynomial equations.

AGRADECIMENTOS

Primeiramente agradeço a Deus, por ter me dado força nos momentos mais difíceis. À minha família, em especial aos meus pais e irmãos, que sempre me incentivaram e confiaram em mim. À minha noiva, Mariana de Mello da Silva, por sua compreensão e paciência, que me fortificaram nesses 2 anos de estudos.

E agradeço ao Professor Vilmar Trevisan, meu incentivador e amigo, que com suas sugestões e idéias, fizeram esta dissertação tornar-se um trabalho excepcional.

1 INTRODUÇÃO

O objetivo primordial deste trabalho é apresentar uma técnica para a resolução de sistemas de equações polinomiais. Este tópico é o centro de várias áreas da matemática, não somente pela forte teoria, mas também por suas aplicações. Nos últimos anos, graças a um desenvolvimento explosivo de algoritmos, tem sido possível a resolução de muitos problemas que eram até então considerados como intratáveis. Como exemplo de avanços, a fatoração de polinômios, um subproblema desse tópico de equações polinomiais, alcançou um desenvolvimento incrível, expandindo muito as áreas de aplicações como robótica, estrutura biológica molecular, design computacional, modelagem geométrica, e certamente áreas de estatísticas, otimização, teoria de jogos, e rede biológica. O leitor interessado poderá consultar os artigos [14] e [15] e os trabalhos [7] e [11] para um desenvolvimento mais recente.

Existem várias formas de resolver um sistema de equações polinomiais: a teoria de eliminação de variáveis, a teoria de bases de Gröebner, teoria de autovalores e autovetores, etc. Uma técnica muito interessante e puramente geométrica, que se baseia na teoria de politopos pode ser encontrada no artigo [22] e também nos livros [3] e [5].

A técnica que vamos estudar é puramente algébrica, conhecida como resultante. Esta é uma teoria clássica que retorna ao trabalho de Euler, Bezout, Sylvester e Cayley. A motivação original é como encontrar raízes comuns de n polinômios com n variáveis. No caso de dois polinômios a uma variável, as coisas se mantêm simples e é fácil visualizar. Para um caso mais geral, precisamos utilizar outras ferramentas matemáticas que nos auxiliem a uma maior comprensão.

O motivo de estudar a teoria de resultantes, não é somente pelo fato de ser uma ferramenta na resolução de sistemas de equações polinomiais, mas também, porque o estudo de aspectos de complexidade na resolução desses sistemas pode ser

obtido através da análise do resultante. Desta forma, na última década, renovou-se o interesse por esta teoria, encontrando-se fórmulas explícitas para o seu cálculo.

Além disso, a sua teoria é, por si só, relevante, elegante e matematicamente bonita. De tal forma que esta dissertação dedica considerável espaço ao desenvolvimento da teoria de resultantes, talvez até mais do que ao objetivo original, que é sua aplicação à resolução de sistemas de equações polinomiais.

Iniciamos o capítulo 2 com alguns resultados básicos da Geometria Algébrica, que nos auxiliarão a desenvolver esta teoria de resultantes no capítulo 3.

O cálculo do resultante é um problema que discutimos no capítulo 4. No caso de uma variável, esse processo é bem conhecido, mas no caso de várias variáveis é um problema difícil. Desenvolveremos duas técnicas para o cálculo. Uma das técnicas que iremos apresentar, é conhecida como a fórmula de Macaulay, cujo resultante é explicitado como o quociente de dois determinantes. É um problema instável e a complexidade do resultante pode ser alta na prática. Também apresentaremos a fórmula de Poisson, que necessita de ferramentas mais geométricas do que a fórmula de Macaulay.

No capítulo 5 usaremos a teoria de resultantes para explicitar as soluções de um sistema de equações polinomiais. Ainda no mesmo capítulo usaremos o resultante para provar um caso particular do Teorema de Bezout, para curvas no plano xy. Este é um resultado clássico que dá o número de soluções de um sistema de equações polinomiais. Este teorema está diretamente relacionado com a teoria desenvolvida nos capítulos anteriores.

1.1 Motivação e Histórico

De acordo com [17], suponha que desejamos determinar as raízes comuns de dois polinômios a uma variável com coeficientes reais ou complexos. Sejam os polinômios $a_0 + a_1x$ e $b_0 + b_1x$ de graus 1, procuramos um valor x de modo que satisfaça

$$a_0 + a_1x = 0$$

$$b_0 + b_1x = 0.$$

Resolvendo cada uma dessas equações, temos que $x = \frac{-a_0}{a_1}$ e $x = \frac{-b_0}{b_1}$, respectivamente. Então ambas equações satisfazem simultaneamente

$$\frac{a_0}{a_1} = \frac{b_0}{b_1},$$

que pode também ser escrito como a_0b_1 - $a_1b_0 = 0$.

Formalmente podemos observar isto como um sistema de duas equações lineares de duas variáveis x^0 e x^1, escrita na forma matricial

$$\begin{bmatrix} a_0 & a_1 \\ b_0 & b_1 \end{bmatrix} \begin{bmatrix} x^0 \\ x^1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Então uma solução não trivial exige que o determinante obtido pelos coeficientes da matriz, seja novamente a_0b_1 - $a_1b_0 = 0$.

Agora consideremos dois polinômios de grau 2. Neste caso procuramos um valor x de modo que satisfaça

$$a_0 + a_1x + a_2x^2 = 0$$

$$b_0 + b_1x + b_2x^2 = 0.$$

Como no caso anterior, podemos resolver cada equação o valor de x e igualar os resultados das duas expressões, mas é mais conveniente fazer a forma matricial. De

qualquer modo, este caso temos duas equações lineares de três variáveis x^0, x^1, e x^2. Então podemos multiplicar cada equação por x, obtendo mais duas equações

$$a_0x + a_1x^2 + a_2x^3 = 0$$

$$b_0x + b_1x^2 + b_2x^3 = 0.$$

Da mesma forma que o caso anterior, agora temos quatro equações lineares e quatro variáveis x^0, x^1 , x^2, e x^3, isto é, obtemos o sistema

$$\begin{bmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{bmatrix} \begin{bmatrix} x^0 \\ x^1 \\ x^2 \\ x^3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Novamente, para que os polinômios possuam uma raiz comum, o determinante obtido pelos coeficientes da matriz deve ser nulo, isso implica que

$$(a_0b_2 - a_2b_0)^2 = (a_0b_1 - a_1b_0)(a_1b_2 - a_2b_1) = 0.$$

Mais geralmente, dados dois polinômios $f(x)$ e $g(x)$ de graus m e n, respectivamente, podemos obter um sistema de $m+n$ equações nas variáveis $(x^0, x^1, x^2, \ldots, x^{m+n-1})$. E novamente a condição para que estes dois polinômios possuam uma raiz comum, implica que o determinante obtido pelos coeficientes deste sistema, seja zero. Esse desenvolvimento geral será determinado no capítulo 3 desta dissertação. Esta técnica é conhecida como a teoria do resultante a uma variável. Ela será uma motivação para encontrarmos ferramentas que determinam uma raiz comum, no caso de n polinômios em n variáveis.

1.2 O Resultante e o Teorema de Bezout

Segundo [20], a solução de um sistema de equações lineares, foi desenvolvida na China, cerca de 200 AC, e a aplicação do método de eliminar a variavél x de dois polinômios foi desenvolvido no século 12. Estas técnicas foram utilizadas na Europa por matemáticos somente no século 17, motivados pela geometria de curvas e equações algébricas. O estudo de curvas e seus pontos de intersecção cobriu naturalmente o estudo de polinômios e suas raízes comuns.

Para uma equação representar uma reta contínua de pontos, precisamos de uma equação de duas variáveis. Por exemplo, a reta é representada por um conjunto de pontos (x, y) que satisfaz uma dada equação algébrica da forma $ax + by + c = 0$, onde a, b, c são números reais ou complexos. Um conjunto de diferentes números A, B, C produz uma diferente reta, com coordenadas satisfazendo a equação $Ax + By + C = 0$. Assim cada curva corresponde a um polinômio. A união de duas curvas obviamente corresponde ao produto de dois polinômios. A intersecção entre duas curvas consiste nos pares x, y que satisfazem ambas destas equações.

Em 1620 *Descartes* descobriu algo mais geral: um método de resolver qualquer equação de grau 3 ou 4 através de intersecções de curvas de grau 2, como uma parábola e um círculo. Na verdade não é fácil encontrar uma construção satisfatória para equações de elevado grau. Na procura de uma construção geral, matemáticos têm casualmente assumido que uma curva de grau m intercepta uma curva de grau n em mn pontos. A primeira afirmação deste princípio, que tornou-se conhecido como o Teorema de Bezout, foi feito por Newton.

Para ilustrar, considere o par de equações

$$2x^5 + 7x^4y - 5x^2y^3 - 3y^5 = 0$$

$$9x^3 + xy^2 + y^3 = 0.$$

Os graus desses polinômios são 5 e 3, respectivamente. O Teorema de Bezout afirma que existem 15 pontos na intersecção entre os dois polinômios.

Assim uma de nossas aplicações é usar a teoria de resultantes para demonstrar o Teorema de Bezout de curvas no plano xy.

Para entender a relação do resultante e o Teorema de Bezout, vamos supor que desejamos encontrar as soluções de uma equação de grau 4. De fato existe uma dificuldade algébrica em resolver uma equação polinomial de grau 4. Pensando como *Descartes*, esta equação pode ser o produto de duas equações de grau 2. Assim para determinar as soluções da equação de grau 4, basta determinar os pontos comuns das duas equações de grau 2.

Para exemplificar e ilustrar o método descrito no parágrafo anterior, considere a cônica, isto é, um plano consistindo por todos os pontos com coordenadas x, y de modo que

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

onde $a, b, \ldots, f$ são constantes. Um conjunto diferente de constantes $A, B, \ldots, F$ produz uma cônica diferente, com coordenadas satisfazendo a equação

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0.$$

Para encontrar a intersecção dessas duas curvas, podemos vê-las da forma

$$cy^2 + (bx + e)y + (ax^2 + dx + f) = 0$$

$$Cy^2 + (Bx + E)y + (Ax^2 + Dx + F) = 0.$$

Discutindo esses dois polinômios de grau 2 em y, podemos usar o método do resultante para econtrar uma condição necessária e suficiente para um único valor de y que satisfaz ambas equações. Assim é conveniente definirmos

$$p_0(x) = c \qquad p_1(x) = bx + e \qquad p_2(x) = ax^2 + dx + f$$

$$q_0(x) = C \qquad q_1(x) = Bx + E \qquad q_2(x) = Ax^2 + Dx + F$$

Assim como anteriormente temos um sistema de equações

$$\begin{bmatrix} p_0 & p_1 & p_2 & 0 \\ 0 & p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 & 0 \\ 0 & q_0 & q_1 & q_2 \end{bmatrix} \begin{bmatrix} y^3 \\ y^2 \\ y^1 \\ y^0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Assim o determinante dos coeficientes da matriz deve ser zero

$$(p_0q_2 - p_2q_0)^2 - (p_0q_1 - p_1q_0)(p_1q_2 - p_2q_1) = 0. \tag{1.1}$$

Substituindo por p e q funções, obtemos um polinômios de grau 4 na variavel x. Isto é o resultante de dois polinômios a uma variável.

O número de raízes de (1.1) é exatamente 4. Isto significa que a intersecção entre as duas cônicas é 4 pontos, que está de acordo com o Teorema de Bezout. Naturalmente assumimos, que os polinômios que representam as duas curvas não têm um fator comum, porque se eles compartilham um tal fator, obviamente eles se intersectarão nos infinitos pontos do fator comum. Uma prova rigorosa desse resultado será vista no capítulo 5 deste trabalho.

2 PRÉ-REQUISITOS ALGÉBRICOS

Aqui vamos introduzir algumas definições e fatos básicos de Álgebra e Geometria Algébrica, que usaremos nos próximos capítulos e podem ser encontrados em [2], [3] e [19].

2.1 Ideal, Gerador, Divisores de zero

Definição 2.1.1. *Seja R um anel comutativo com unidade e $\emptyset \neq I \subseteq R$. Então I é chamado ideal em R se:*
i) $a + b \in I$ para qualquer $a, b \in I$, e
ii) $ac \in I$ para todo $a \in I$ e $c \in R$.
I é um ideal próprio se $I \neq \{0\}$ e $I \neq R$. I é um ideal maximal se ele não está contido propriamente em um ideal próprio. I, é um ideal primo se $ab \in I$ implica em $a \in I$ ou $b \in I$.

Exemplo 2.1.1. *O conjunto $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$ de todos inteiros múltiplos de $m \in \mathbb{Z}$ é um ideal do anel $\mathbb{Z}$. Neste caso dizemos que o ideal $m\mathbb{Z}$ é gerado por m.*

Definição 2.1.2. *Um conjunto $B \subseteq R$ é gerador do ideal I se*

$$I = \left\{ \sum_{i=1}^{n} r_i b_i \mid n \in \mathbb{N}, r_1, \ldots, r_n \in R, b_1, \ldots, b_n \in B \right\}$$

Neste caso dizemos que I é um ideal gerado por B, $I = ideal(B) =< B >$. I é finitamente gerado se ele tem um conjunto gerador finito. I é um ideal principal se ele tem um conjunto gerador de cardinalidade 1.

Definição 2.1.3. *Um dividor de zero em um anel comutativo R é um elemento $a \neq 0$ que satisfaz: existe um $b \neq 0 \in R$ tal que $ab = 0$.*

Um domínio de integridade ou simplesmente domínio D é um anel comutativo, com unidade e sem divisores de zero. Dizemos que D é um domínio fatorial se todo elemento não inversível se escreve como produto de fatores irredutíveis.

Exemplo 2.1.2. *Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são anéis sem divisores de zero. Enquanto que o conjunto das matrizes quadradas é um anel com divisores de zero.*

2.2 Corpos e Anéis Polinomiais

Definição 2.2.1. *Seja R um anel comutativo sem divisores de zero. R é chamado de corpo se todo elemento de R diferente de zero tem elemento inverso.*

Exemplo 2.2.1. *Os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são corpos.*

Agora seja R um anel. Um polinômio f de uma variável sobre R é um expressão do tipo

$$f(x) = \sum_{i=1}^{r} f_{n_i} x^{n_i}$$

onde $f_j \in R$ são os coeficientes de x^j do polinômio f e r é um número inteiro tal que $r \geq 0$. O polinômio identicamente nulo, é um $f(x)$ tal que que $f_j = 0$ para todo $j \in \{n_1, n_2, \ldots, n_r\}$.

Definição 2.2.2. *O conjunto de todos polinômios sobre R com as operações usuais de adição e multiplicação de polinômio forma um anel. Representamos o anel dos polinômios sobre R por $R[x]$.*

Muitas propriedades do anel R são herdadas pelo anel dos polinômios $R[x]$. Por exemplo as propriedades, comutativa, unidade, domínio de integridade.

O grau de um polinômio denotado por $grau(f)$, é o máximo dos valores n tal que $f_n \neq 0$. Um polinômio $f(x)$ é dito mônico se o coeficiente do termo $x^{grau(f)}$ é igual a 1.

De forma análoga, um polinômio de $n-$ variáveis sobre um anel R é uma expressão do tipo

$$f(x) = \sum_{i=1}^{r} f_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$$

onde os $f_{i_1,\ldots,i_n} \in R$ e r é um número inteiro tal que $r \geq 0$.

O conjunto de todos os polinômios com $n-$variáveis sobre R forma um anel, $R[x_1, \ldots, x_n]$. O anel polinomial de $n-$variáveis pode ser visto como uma construção sucessivamente de R adjacente ao polinômio de uma variável. De fato, $R[x_1, \ldots, x_n]$ é isomorfo a $R[x_1, \ldots, x_{n-1}][x_n]$.

O grau de um $f(x) \in R[x_1, \ldots, x_n]$ é definido por

$$grau(f) := max\{\sum_{j=1}^{n} i_j \mid f_{i_1,\ldots,i_n} \neq 0\}.$$

2.3 Variedade Afim e Álgebra Quociente

Definição 2.3.1. *Seja K um corpo, chamamos o conjunto $K^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in K\}$ de espaço afim n- dimensional sobre K.*

Exemplo 2.3.1. *Seja $K = \mathbb{R}$, temos o espaço Euclidiano $\mathbb{R}^n$ é um espaço afim $n-$dimensional sobre $\mathbb{R}$.*

Definição 2.3.2. *O conjunto do todas as soluções $(a_1, \ldots, a_n) \in K^n$ do sistema de equações*

$$f_1(x_1, \ldots, x_n) = 0$$

$$f_2(x_1, \ldots, x_n) = 0$$

$$\vdots$$

$$f_s(x_1, \ldots, x_n) = 0$$

é conhecido como variedade afim definida por $f_1, \ldots, f_s$, e denotado por $\mathbf{V}(f_1, \ldots, f_s)$.

Exemplo 2.3.2. *A variedade $\mathbf{V}(x^2 + y^2 - 1,\ x - 3y^2) \subset \mathbb{R}^2$ é a intersecção de um circulo $x^2 + y^2 = 1$ e a parábola $x = 3y^2$ no plano xy.*

Exemplo 2.3.3. *A variedade* $\mathbf{V}(x^2 + z^2 - 1)$ *é o cilindro circular definido pela equação*

$$x^2 + z^2 - 1 = 0.$$

A figura abaixo ilustra a variedade em $\mathbb{R}^3$:

Figura 2.1: cilindro circular

Uma variedade afim $\mathbf{V} \subset K^n$ pode representar diferentes sistemas de equações. Note que se $g = p_1 f_1 + \ldots + p_s f_s$, onde $p_i \in K[x_1, \ldots, x_n]$ são polinômios quaisquer, então $g(a_1, \ldots, a_n) = 0$ para cada $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_n)$. Assim dado qualquer conjunto de equações que definem a variedade, podemos sempre adicionar muitos polinômios que se anulam nessa variedade.

Logo faz sentido pensar numa variedade como sendo definida por um ideal em $K[x_1, \ldots, x_n]$, melhor do que um específico sistema de equações. Assim podemos escrever $\mathbf{V}(I)$, onde $I \subset K[x_1, \ldots, x_n]$ é um ideal.

Definição 2.3.3. *Seja* $V \subset K^n$ *uma variedade. Denotamos por* $\mathbf{I}(V)$ *o conjunto* $\{f \in K[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0$ *para todo* $(a_1, \ldots, a_n) \in V\}$.

É fácil ver que $\mathbf{I}$(V) é um ideal. De fato $\mathbf{I}(V)$ é dito ideal de V.

Definição 2.3.4. *Seja $I \subset K[x_1, \ldots, x_n]$ um ideal. O radical de I é o conjunto*

$$\sqrt{I} = \{g \in K[x_1, \ldots, x_n] : g^m \in I \text{ para algum } m \geq 1\}.$$

O ideal I é chamado de ideal radical se $\sqrt{I} = I$.

Proposição 2.3.1. *Se K é um corpo algebricamente fechado e I é um ideal em $K[x_1, \ldots, x_n]$, então $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.*

Esta proposição é conhecida como o Teorema dos zeros de Hilbert. Não vamos fazer aqui uma prova deste teorema, mas sugerimos [2] e [3] para verificar a demonstração.

Definição 2.3.5. *Dados f e $g \in K[x_1, \ldots, x_n]$ e o ideal $I \subset K[x_1, \ldots, x_n]$. Dizemos que f é congruente a g módulo I, denotado por $f \equiv g \ (mod\ I)$, se*

$$f - g \in I.$$

Exemplo 2.3.4. *Seja o ideal I gerado por $< x^2 - y^2, x + y^3 + 1 > \subset K[x, y]$, então $f = x^4 - y^4 + x$ e $g = x + x^5 + x^4y^3 + x^4$ são congruentes módulo I, pois $f - g = x^4 - y^4 - x^5 - x^4y^3 - x^4 = (x^2 + y^2)(x^2 - y^2) - (x^4)(x + y^3 + 1) \in I$.*

Definição 2.3.6. *Dados K um corpo e $I \subset K[x_1, \ldots, x_n]$ um ideal. Seja $f \in K[x_1, \ldots, x_n]$. A classe de equivalência de f, denotada por $[f]$, é o conjunto dos polinômios g tais que $f \equiv g(mod\ I)$, ou seja $[f] = \{g \in K[x_1, \ldots, x_n] : f \equiv g(mod\ I)\}$.*

Definição 2.3.7. *A álgebra quociente de $K[x_1, \ldots, x_n]$ módulo I, denotado por $K[x_1, \ldots, x_n]/I$, é o conjunto das classes de equivalência da congruência módulo I:*

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

Exemplo 2.3.5. *Sejam $K = \mathbb{R}$, $n = 1$ e $I =< x^2 - 2 >$. Podemos indagar se existe uma maneira de determinar todas as classes de equivalência da congruência módulo*

I. Na verdade existe, pelo algoritmo da divisão, todo polinômio $f \in \mathbb{R}[x]$ pode ser escrito como $f = q \cdot (x^2 - 2) + r$, onde $r = ax + b$ para algum $a, b \in \mathbb{R}$. Pela definição, $f \equiv r(mod\ I)$ já que $f - r = q \cdot (x^2 - 2) \in I$. Deste modo, todo elemento de $\mathbb{R}[x]$ faz parte de uma das classes de equivalência $[ax + b]$, e $\mathbb{R}[x]/I = \{[ax + b] : a, b \in \mathbb{R}\}$.

O método descrito no exemplo anterior, pode ser estendido para o caso mais geral, ou seja, para $K[x_1, \ldots, x_n]/I$. Para este caso sugerimos como referência os livros [1, 2, 3].

Pelo fato de $K[x_1, \ldots, x_n]$ ser um anel, e dados quaisquer duas classes $[f], [g] \in K[x_1, \ldots, x_n]/I$, podemos definir as operações de soma e produto sobre as classes, usando as correspondentes operações dos elementos em $K[x_1, \ldots, x_n]$.

$$[f] + [g] = [f + g] \qquad (\ soma\ em\ K[x_1, \ldots, x_n]).$$

$$[f] \cdot [g] = [f \cdot g] \qquad (\ produto\ em\ K[x_1, \ldots, x_n]).$$

Devemos verificar, se estas operações fazem sentido. Para isto, basta mostrar que se escolhermos um diferente $f' \in [f]$ e um $g' \in [g]$, então a classe $[f' + g']$ é a mesma classe de $[f + g]$. Semelhantemente, precisamos verificar que $[f' \cdot g'] = [f \cdot g]$.

Proposição 2.3.2. *As operações sobre as classes de equivalência definidas anteriormente estão bem definidas.*

Prova: Se $f' \in [f]$ e $g' \in [g]$, então $f' = f + a$ e $g' = g + b$, onde $a, b \in I$. Assim

$$f' + g' = (f + a) + (g + b) = (f + g) + (a + b).$$

Como temos $a + b \in I$ (I é um ideal), segue que $f' + g' \equiv f + g(mod\ I)$, então temos que $[f' + g'] = [f + g]$. De forma análoga

$$f' \cdot g' = (f + a) \cdot (g + b) = fg + ag + fb + ab.$$

Já que $a, b \in I$, temos $ag + fb + ab \in I$. Deste modo, $f' \cdot g' \equiv f \cdot g(mod\ I)$, então $[f' \cdot g'] = [f \cdot g]$.

Teorema 2.3.1. (Teorema da Finitude) *Seja $K \subset \mathbb{C}$ um corpo e $I \subset K[x_1, \ldots, x_n]$ um ideal. Então as seguintes afirmações são equivalentes:*
i) $K[x_1, \ldots, x_n]/I$ tem dimensão finita sobre K como espaço vetorial.
ii) A variedade $\mathbf{V}(I) \subset \mathbb{C}^n$ é um conjunto finito.

A prova deste teorema pode ser encontrado em [1]. O ideal que satisfaz qualquer um dos itens do Teorema da Finitude é chamado de ideal zero dimensional.

Uma consequência deste teorema, é que se I é um zero dimensional se e somente existe um polinômio não nulo em $I \cap K[x_i]$ para $i = 1, \ldots, n$.

Dados $A = K[x_1, \ldots, x_n]/I$ e I um ideal zero dimensional. Considere m_i o menor inteiro positivo de modo que o conjunto $\{1, [x_i],$
$[x_i]^2, \ldots, [x_i]^{m_i}\}$ seja linearmente dependente. Então existe uma combinação linear

$$\sum_{j=0}^{m_i} c_j [x_i]^j = [0]$$

em A, onde os $c_j \in K$ e não são todos nulos. Em particular, $c_{m_i} \neq 0$. Pela definição de álgebra quociente, isto equivale dizer que

$$p_i(x_i) = \sum_{j=0}^{m_i} c_j x_i^j \in I. \tag{2.1}$$

A recíproca é imediata.

Proposição 2.3.3. *Seja I um ideal zero dimensional em $\mathbb{C}[x_1, \ldots, x_n]$, e $A = \mathbb{C}[x_1, \ldots, x_n]/I$. Então a dim(A) é maior ou igual ao número de pontos de V(I). A igualdade ocorre se e somente se I é um ideal radical.*

Prova: Seja I um ideal zero dimensional. Pelo teorema da Finitude $V(I)$ é um conjunto finito em $\mathbb{C}^n$. Chamando $V(I) = \{p_1, \ldots, p_m\}$, considere a transformação linear

$$\varphi : \mathbb{C}[x_1, \ldots, x_n]/I \longrightarrow \mathbb{C}^m$$

$$[f] \longrightarrow (f(p_1), \ldots, f(p_m)).$$

Para provar a primeira afirmação do teorema, é suficiente mostrar que φ é sobrejetora. Dado $(\lambda_1, \ldots, \lambda_m) \in \mathbb{C}^m$, seja $f = \sum_{i=1}^{m} \lambda_i g_i$, onde $g_i(x_1, \ldots, x_n)$ tal que $g_i(p_i) = 1$ e $g_i(p_j) = 0$ se $j \neq i$. É fácil ver que $\varphi([f]) = (\lambda_1, \ldots, \lambda_m)$. Então φ é sobrejetora, ou seja, dim(A) $\geq$ m.

Para o seguinte vamos supor que I é radical. Se $[f] \in \mathrm{Ker}(\varphi)$, então $f(p_i) = 0$ para todo i, então por Strong Nullstellensatz, $f \in I(V(I)) = \sqrt{I}$. Deste modo $[f] = [0]$, assim mostramos que f é injetora. Então φ é um isomorfismo, que prova que dim(A) = m se f é um radical. Se $dim(A) = m$, então φ é um isomorfismo já que ele é uma trasformação linear sobrejetora entre espaços vetoriais de mesma dimensão. Consequentemente φ é injetora. Podemos usar isto para provar que I é um ideal radical. A inclusão $I \subset \sqrt{I}$ sempre é válida. Para verificar isto é suficiente para considerar $f \in \sqrt{I} = I(V(I))$ e mostrar que $f \in I$. Se $f \in \sqrt{I}$, então $f(p_i) = 0$ para todo i, que implica que $\varphi([f]) = (0, \ldots, 0)$. Assim φ é injetora e concluimos que $[f] = [0]$, em outra palavras que $f \in I$.

Teorema 2.3.2. *Seja $I \subset \mathbb{C}[x_1, \ldots, x_n]$ um ideal zero dimensional, e seja $f \in \mathbb{C}[x_1, \ldots, x_n]$ e h_f é o polinômio minimal de $m_f : A \longrightarrow A$, onde $A = \mathbb{C}[x_1, \ldots, x_n]/I$. Então, para $\lambda \in \mathbb{C}$, as seguintes afirmações são equivalentes:*
a) λ é uma raiz da equação $h_f(t) = 0$,
b) λ é um autovalor da matriz m_f, e
c) λ é um valor da função f em $\mathbf{V}(I)$.

Prova: A prova deste teorema pode ser encontrada em [3].

2.4 Espaço Projetivo e Coordenadas Homogêneas

Para formalizar " pontos no infinito" precisamos trabalhar no espaço projetivo. A construção usual do espaço projetivo no plano xy, é substituir cada par de coordenandas (x, y) com os raios $\frac{x}{z}$, $\frac{y}{z}$ por algum arbritário z, então cada ponto é representado por três coordenadas (x, y, z).

Para ilustrar, considere a intersecção de duas retas $3x - 2y + 5 = 0$ e $3x - 2y + 1 = 0$. Estas duas retas são paralelas, se eliminarmos y e também x, chegamos a uma condição impossível $4 = 0$, com significado que essas duas retas não têm um ponto em comum no plano xy. De qualquer forma, se substituirmos x e y por $\frac{x}{z}$ e $\frac{y}{z}$, respectivamente, e multiplicarmos por z, a equação das retas será $3x - 2y + 5z = 0$ e $3x - 2y + z = 0$. Essas são as equações homogêneas, e se eliminarmos z obtemos a condição $2y = 3x$, que implica $z = 0$. Consequentemente a intersecção entre as duas retas no espaço projetivo é o ponto $(\frac{2y}{3}, y, 0)$.

Assim temos a seguinte definição:

Definição 2.4.1. *Seja $\mathbb{C}^{n+1}$ o espaço vetorial $n+1$ dimensional sobre um corpo K. O conjunto de retas, isto é, os subespaços de dimensão 1 de $\mathbb{C}^{n+1}$ é chamado de espaço projetivo n dimensional, e denotado por $\mathbb{P}^n(\mathbb{C})$.*

Se introduzirmos coordenadas $\xi_0, \ldots, \xi_n$ em $\mathbb{C}^{n+1}$ então um ponto $\xi \in \mathbb{P}^n(\mathbb{C})$ é obtido por $n+1$ elementos $(\xi_0, \ldots, \xi_n)$ do corpo K, não todos nulos. Dois pontos $(\xi_0, \ldots, \xi_n)$ e $(\eta_0, \ldots, \eta_n)$ são considerados iguais em $\mathbb{P}^n(\mathbb{C})$ se e somente se existe um número complexo $\lambda \neq 0$ de modo que $\eta_i = \lambda \xi_i$ para $i = 0, \ldots, n$.

Definição 2.4.2. *Um conjunto qualquer $(\xi_0, \ldots, \xi_n)$ define um ponto $\xi \in \mathbb{P}^n(\mathbb{C})$, é chamado conjunto de coordenadas homogênenas de ξ.*

Exemplo 2.4.1. *Um ponto p em $\mathbb{P}^2(\mathbb{C})$ é determinado por 3 elementos (ξ_0, ξ_1, ξ_2) de um corpo $\mathbb{C}$, não todos nulos. Se (η_0, η_1, η_2) também determina o mesmo ponto p, então existe $\lambda \neq 0$ de modo que $\xi_0 = \lambda\eta_0, \xi_1 = \lambda\eta_1$ e $\xi_2 = \lambda\eta_2$. Assim qualquer tripla (ξ_0, ξ_1, ξ_2) que define o ponto p é chamado do conjunto de coordenadas homogêneas de p.*

Definição 2.4.3. *Um polinômio $f(x_0, \ldots, x_n)$ sobre um corpo $K[x_0, \ldots, x_n]$, é dito homogêneo de grau $d \in \mathbb{N}$, se para todo $\alpha \in K$*

$$f(\alpha x_0, \ldots, \alpha x_n) = \alpha^d f(x_0, \ldots, x_n).$$

Sejam $(\xi_0, \ldots, \xi_n)$ e $(\eta_0, \ldots, \eta_n)$ dois conjuntos de coordenadas homogêneas para algum ponto $p \in \mathbb{P}^n(\mathbb{C})$. Então existe um número complexo $\lambda \neq 0$ tal que $(\eta_0, \ldots, \eta_n) = \lambda(\xi_0, \ldots, \xi_n)$. Se $f(x_0, \ldots, x_n)$ é um polinômio homogêneo de grau d e $(\eta_0, \ldots, \eta_n) = \lambda(\xi_0, \ldots, \xi_n)$, então

$$f(\eta_0, \ldots, \eta_n) = \lambda^d(\xi_0, \ldots, \xi_n).$$

Definição 2.4.4. *Seja $f(x_0, \ldots, x_n)$ um polinômio homogêneo de grau d.*
A variedade projetiva $\mathbf{V}(f) \subset \mathbb{P}^n(\mathbb{C})$ é o conjunto de pontos de $\mathbb{P}^n(\mathbb{C})$ onde f se anula. Note que $\mathbf{V}(f) \subset \mathbb{P}^n(\mathbb{C})$ é determinado pelas soluções não triviais de $f = 0$.

Proposição 2.4.1. *Seja $f \in \mathbb{C}[x, y, z]$ um polinômio homogêneo não nulo. Então os fatores irredutíveis de f são também homogêneos, e se fatorarmos f em irredutíveis*

$$f = f_1^{a_1} \ldots f_s^{a_s},$$

onde f_i não é uma constante múltipla de f_j para $i \neq j$, então

$$\mathbf{V}(f) = \mathbf{V}(f_1) \cup \ldots \cup \mathbf{V}(f_s)$$

é a menor decomposição de $\mathbf{V}(f)$ em variedades irredutíveis em $\mathbb{P}^2(\mathbb{C})$. Além disso,

$$\mathbf{I}(\mathbf{V}(f)) = \sqrt{< f >} =< f_1 \ldots f_s > .$$

Prova: Primeiramente vamos supor que f fatora-se como $f = gh$, onde $g, h \in \mathbb{C}[x, y, z]$. Afirmamos que g e h devem ser polinômios homogêneos desde que f seja. Para provar esta afirmação, escrevemos $g = g_m + \ldots + g_0$, onde os g_i são homogêneos de grau i, com $g_m \neq 0$. De forma análoga, $h = h_n + \ldots + h_0$. Então

$$f = gh = (g_m + \ldots + g_0)(h_n + \ldots + h_0) = g_m h_n + \textit{outros termos de grau menor.}$$

Desde que f é homogêneo e $\text{grau}(f) = \text{grau}(g) + \text{grau}(h) = m + n$, e como f é homogêneo, então $f = g_m h_n$. Olhando os termos de grau menor de hg, não é difícil de ver que $h_{n-1} = h_{n-2} = \ldots = h_0 = 0$ e $g_{m-1} = g_{m-2} = \ldots = g_0 = 0$, ou seja, $g_m = g$ e $h_n = h$. Então g e h são homogêneos.

Agora considere $f = f_1^{a_1} \dots f_s^{a_s}$. Então $\mathbf{V}(f) = \mathbf{V}(f_1) \cup \dots \cup \mathbf{V}(f_s)$ segue imediatamente do seguinte resultado: Se $f \in \mathbb{C}[x, y, z]$ é irredutível, então $\mathbf{V}(f)$ é irredutível. Para a prova deste resultado sugerimos [2].

A última afirmação é consequência da proposição (2.3.1).

3 RESULTANTES

Neste capítulo vamos introduzir a teoria de resultantes. Surpreendentemente ela é uma ferramenta eficiente para encontrar as soluções de um sistema de equações polinomiais.

3.1 Resultante a uma variável

A definição de resultante se baseia numa matriz conhecida como *matriz Sylvester*. Primeiramente vamos apresentar uma motivação para esta matriz especial. Nosso objetivo é decidir quando dois polinômios f e g têm uma raiz em comum. Para encontrar a resposta desta questão, Euler e Bezout introduziram o clássico resultante que se anula se e somente se isto for verdadeiro. Vamos rever este clássico desenvolvimento a seguir.

Sejam $K[x]$ um anel comutativo e f, g dois polinômios em $K[x]$

$$f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i,$$

de graus n, m respectivamente. Queremos determinar quando o sistema de duas equações lineares

$$f_n x_n + f_{n-1} x_{n-1} + ... + f_1 x_1 + f_0 x_0 = 0,$$

$$g_m x_m + g_{m-1} x_{m-1} + ... + g_1 x_1 + g_0 x_0 = 0$$

de variáveis x_j que seja satisfeito para $x_j = \alpha^j$ para todo j, onde α é uma raíz comum de f, g. Para $n > 1$ existem outras soluções dessas duas equações de várias variáveis, mas *Sylvester* elimina essas soluções desnecessárias adicionando $(m-1)+(n-1)$ equações lineares com as seguintes condições:

$$xf(x) = 0, ..., x^{m-1} f(x) = 0$$

$$xg(x) = 0, ..., x^{n-1} g(x) = 0.$$

Essas equações geram um total de $n+m$ relações lineares juntamente com as variáveis $x_{m+n-1}, ..., x_0$:

$$\begin{array}{ccccccccc}
f_n x_{m+n-1} & + & \dots & + & f_0 x_{m-1} & & & & = 0, \\
 & & \vdots & & & & & & \\
 & & f_n x_n & + & f_{n-1} x_{n-1} & + & \dots + f_0 x_0 & & = 0, \\
g_m x_{m+n-1} & + & \dots & + & g_0 x_{n-1} & & & & = 0, \\
 & & \vdots & & & & & & \\
 & & g_m x_m & + & g_{m-1} x_{m-1} & + & \dots + g_0 x_0 & & = 0.
\end{array}$$

A matriz transposta $(n+m) \times (n+m)$, consiste dos coeficientes de f e g, do sistema acima é chamada de *matriz Sylvester*.

Definição 3.1.1. *A matriz* $(n+m) \times (n+m)$

$$Syl(f,g) = \begin{bmatrix}
f_n & & & & g_m & & & & \\
f_{n-1} & f_n & & & g_{m-1} & g_m & & & \\
\vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & & \\
\vdots & \vdots & & f_n & g_1 & \vdots & & \ddots & \\
\vdots & \vdots & & f_{n-1} & g_0 & \vdots & & & \ddots \\
\vdots & \vdots & & \vdots & & g_0 & & & g_m \\
f_0 & \vdots & & \vdots & & & \ddots & & \vdots \\
 & f_0 & & \vdots & & & & \ddots & \vdots \\
 & & \ddots & \vdots & & & & & \ddots \\
 & & & f_0 & & & & & g_0
\end{bmatrix}$$

é a matriz de Sylvester de f e g, onde os espaços em branco são preenchidos por zero.

Agora vamos a definição formal do resultante.

Definição 3.1.2. *O resultante de f e g, denotado por $Res_{n,m}(f,g)$ é o determinante da matriz Sylvester, ou seja, $Res_{n,m}(f,g) = det(Syl(f,g))$.*

Veremos a seguir que o resultante igual a zero implica na existência de uma raiz comum de f e g. É fácil ver que se fizermos $x_j = \alpha^j$, onde α é uma

raiz comum de f e g, então x_j é uma solução do sistema, portanto o determinante associado a este sistema é zero. O mais importante, no entanto é que a recíproca é essencialmente verdadeira. De fato, a existência de uma solução não nula do sistema de equações implica a existência de um fator comum não trivial de f e g.

Assim a principal propriedade do resultante é o seguinte teorema.

Teorema 3.1.1. *Sejam* $f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i$ *dois polinômios em* $K[x]$ *tais que* $f_n, g_m \neq 0$ *de graus* ≥ 1. *Então as seguintes afirmações são equivalentes:*

i) $Res(f, g) = 0$;

ii) Existem polinômios não nulos $A, B \in K[x]$, *de graus menores que* n *e* m *respectivamente, tais que* $A(x)g(x) = B(x)f(x)$;

iii) f *e* g *têm um fator comum não constante em* $K[x]$;

Prova: *Encontrar polinômios não nulos* $A(x) = \sum_{i=0}^{n-1} c_i x^i$ *e* $B(x) = \sum_{i=0}^{m-1} d_i x^i$ *em* $K[x]$ *tais que* $A(x)g(x) = B(x)f(x)$*é equivalente encontrar uma solução não trivial do seguinte sistema homogêneo de* $n + m$ *equações nas incógnitas* $d_{m-1}, d_{m-2}, \ldots, d_0$, $c_{n-1}, c_{n-2}, \ldots, c_0$:

$$\begin{cases} a_n d_{m-1} - b_m c_{n-1} = 0 \\ a_{n-1} d_{m-1} + a_n d_{m-2} - b_{m-1} c_{n-1} - b_m c_{n-2} = 0 \\ \vdots \\ a_0 d_0 - b_0 c_0 = 0 \end{cases}$$

Isto pode ser observado igualando os coeficientes dos termos de mesmo grau. Existe uma solução não trivial deste sistema se e somente se o determinante da matriz dos coeficientes é nulo. Observa-se que o $Res(f, g)$ *é o determinante da matriz dos coeficientes deste sistema. Consequentemente,* $i)$ *e* $ii)$ *são equivalentes. Mostraremos agora que* $ii)$ *e* $iii)$ *são equivalentes.*

Se existem A e B de graus menores que n e m respctivamente tais que

$$A(x)g(x) = B(x)f(x) \tag{3.1}$$

considere a fatoração em fatores irredutíveis dos dois lados da igualdade (3.1). Os fatores irredutíveis de $g(x)$ têm que dividir o lado direito da igualdade. Como o grau de $B < m$, nem todos os fatores de $g(x)$ podem dividir B. Assim algum fator de g deve dividir f. Logo eles têm um fator comum de grau positivo.
A recíproca, se $\phi(x)$ é um fator comum de grau positivo, então podemos escrever

$$f(x) = \phi(x)A(x), \qquad grau(A) < n$$

$$g(x) = \phi(x)B(x), \qquad grau(B) < m$$

então $A(x)g(x) = A(x)\phi(x)B(x) = B(x)f(x)$. Logo $i)$, $ii)$, e $iii)$ são equivalentes.

Exemplo 3.1.1. *Sejam $f = x^4 - 3x^3 + 2x$ e $g = x^3 - 1$ então o resultante é*

$$Res_{4,3}(f,g) = det \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -3 & 1 & 0 & 0 & 1 & 0 \\ 2 & 0 & -3 & -1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix} = 0.$$

Podemos reescrever $f = x(x-1)(x^2-2x-2)$ e $g = (x-1)(x^2+x+1)$, ou seja, f e g têm um fator em comum $x-1$, que justifica o fato de que o $Res_{4,3}(f,g) = 0$.

3.2 Principais Propriedades do Resultante

Veremos aqui algumas propriedades do resultante de polinômios a uma variável que são bem conhecidas. As mesmas podem ser encontradas em [6], [18] e [23].

Para as seguintes propriedades, sejam f, g dois polinômios em $K[x]$

$$f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i,$$

de graus n, m respectivamente.

Propriedade 3.2.1. *i) O* $Res(f, c) = c^n$, *onde* c *é o polinômio constante não nulo.*

ii) O $Res(f, 0) = 0$, *onde* 0 *é o polinômio identicamente nulo.*

Prova: *i*) Pela definição (3.1.1), os coeficientes do polinômio de f, aparecem distribuídos em colunas exatamente em quantidade igual ao grau do polinômio g. Como g é uma constante c, e o grau de g é zero, então os coeficientes de f não aparecem na matriz Sylvester. De forma análoga para os coeficientes de g. Como f tem grau n, temos por definição que o $Res(f, c)$ é igual a

$$Res_{n,0}(f, c) = det \begin{bmatrix} c & 0 & \dots & & 0 \\ 0 & c & 0 & \dots & 0 \\ \vdots & & \ddots & & \\ 0 & \dots & & 0 & c \end{bmatrix} = c^n.$$

ii) Este resultado é direto por i).

Propriedade 3.2.2. *O* $Res_{n,m}(f, g) = (-1)^{nm} Res_{m,n}(g, f)$.

Prova: Este resultado sai diretamente da definição de resultante. Se permutarmos as colunas da matriz sylvester, o determinante será multiplicado por $(-1)^l$, onde l é a quantidade de permutações. Como o número de permutações é $m(m + n - 1)$, segue que $(-1)^{m(m+n-1)} = (-1)^{nm}$.

Propriedade 3.2.3. *Se $f_i, g_j \in \mathbb{Z}$, com $0 \leq i \leq n$ e $0 \leq j \leq m$ o $Res_{n,m}(f,g)$ é um polinômio inteiro de coeficientes de f, g.*

Prova: Por definição o resultante é um determinante de uma matriz, como os coeficientes desta matriz são inteiros, então o resultante é um inteiro.

Propriedade 3.2.4. *O $Res_{n,m}(f,g)$ pode ser dado também pela seguinte fórmula*

$$Res_{n,m}(f,g) = det \begin{bmatrix} f_n & f_{n-1} & \dots & f_0 & 0 & & \dots & & 0 \\ 0 & f_n & f_{n-1} & \dots & f_0 & 0 & & \dots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & & \dots & 0 & f_n & & & \dots & f_0 \\ g_m & \dots & & g_0 & 0 & & \dots & & 0 \\ 0 & g_m & \dots & & g_0 & 0 & \dots & & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & & \dots & & 0 & g_m & \dots & & g_0 \end{bmatrix}$$

Prova: Usando o fato de que o determinante de uma matriz é igual ao determinante de sua transposta, obtemos o resultado.

Propriedade 3.2.5. *Sejam $\alpha_1, \dots, \alpha_n$ e $\beta_1, \dots, \beta_m$, as raízes respectivamente de f e g. Então podemos mostrar que o Resultante é dado por*

$$Res(f,g) = f_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} g_m^n \prod_{j=1}^{m} f(\beta_j) = f_n^m g_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

Prova: Primeiro vamos mostrar que as expressões segunda e terceira são iguais a quarta. Podemos escrever $f(x) = f_n \prod(x - \alpha_i)$. Assim tomando $x = \beta_j$, temos que $f(\beta_j) = f_n \prod_{i=1}^{n}(\beta_j - \alpha_i)$. Então $g_m^n \prod_{j=1}^{m} f(\beta_j) = g_m^n \prod_{j=1}^{m} f_n \prod_{i=1}^{n}(\beta_j - \alpha_i) = g_m^n f_m^n \prod_{i=1}^{n} \prod_{j=1}^{m}(\beta_j - \alpha_i)$. Logo multiplicando por $(-1)^{mn}$, temos que a terceira expressão é igual a quarta. De forma análoga prova-se que a segunda expressão é igual a quarta.

Para finalizar, basta mostrar que o $Res(f,g)$ é igual a uma dessas expressões. Vamos mostrar que o resultante é equivalente a quarta expressão.

Agora consideremos as raízes de f e g, α_i e β_j como variáveis. Claramente o $Res(f,g)$ é um polinômio de grau n nos coeficientes f_i de f. Similarmente o $Res(f,g)$ é um polinômio de grau m nos coeficientes g_i de g. Como o $Res(f,g)$ se anula para $\alpha_i = \beta_j$, neste caso f e g têm um fator em comum. Consequentemente o $Res(f,g)$ é divisível por $\alpha_i - \beta_j$. Denotando por $S = f_n^m g_m^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$, o $Res(f,g)$ deve ser divisível por S. Sabemos que S é equivalente a

$$S = f_n^m \prod_{i=1}^n g(\alpha_i) = g_m^n \prod_{j=1}^m f(\beta_j).$$

A primeira igualdade implica que S é de grau n, e a segunda igualdade implica que S é de grau m. Mas o $Res(f,g)$ tem o mesmo grau que S e é divisível por S. Deste modo o $Res(f,g)$ deve coincide com S, exceto de um fator constante. Comparando os termos de maior potência do $Res(f,g)$ e S, este fator constante é 1. Logo $S = Res(f,g)$.

Propriedade 3.2.6. *Se f, g podem ser escritas da forma $f = qg + r$ com $grau(r) = v$, então*

$$Res(g,f) = g_m^{n-v} Res(g,r).$$

Prova: Para provarmos esta propriedade, usaremos a propriedade 3.2.5. Podemos escrever $f(x) = q(x)g(x) + r(x)$. Pela proposição anterior temos que

$$Res(g,f) = g_m^n \prod_{j=1}^m f(\beta_j),$$

de forma semelhante

$$Res(g,r) = g_m^v \prod_{j=1}^m r(\beta_j) = g_m^v \prod_{j=1}^m (f(\beta_j - q(\beta_j)g(\beta_j)) = g_m^v \prod_{j=1}^m f(\beta_j).$$

Logo

$$Res(g,f) = g_m^{n-v} Res(g,r).$$

Em geral esta propriedade é provada quando r é o resto da divisão euclidiana de f por g. Este caso particular pode ser encontrado em [18].

Propriedade 3.2.7. *Sejam f, g, então existem polinômios $A(x), B(x) \in K[x]$ de modo que $A(x)f(x)+B(x)g(x) = Res(f,g)$, tal que o grau$(A) < m$ e o grau$(B) < n$.*

Prova: Considere o $Res(f,g)$ definido na propriedade (3.2.4). Denotando por M esta matriz e para $1 \leq i < m+n$, multiplicamos a $i-$ésima coluna da matriz M por x^{n+m-i}, e adicionamos a última coluna. O resultado é uma nova matriz M' cujo o determinante é igual ao determinante de M, e cujas as últimas colunas consistem nos polinômios $x^{m-1}f(x), x^{m-2}f(x), \ldots, f(x), x^{n-1}g(x), x^{n-2}g(x), \ldots, g(x)$, ou seja

$$
\begin{aligned}
x^{m-1}f(x) &= f_n x^{n+m-1} + f_{n-1}x^{n+m-2} + \ldots + f_0 x^{m-1} \\
x^{m-2}f(x) &= \qquad f_n x^{n+m-2} + \ldots \qquad + f_0 x^{m-2} \\
&\vdots \\
f(x) &= \qquad\qquad f_n x^n + \ldots \qquad\qquad + f_0 \\
x^{n-1}g(x) &= g_m x^{n+m-1} + g_{m-1}x^{n+m-2} + \ldots + g_0 x^{n-1} \\
x^{n-2}g(x) &= \qquad g_m x^{n+m-2} + \ldots \qquad + g_0 x^{n-2} \\
&\vdots \\
g(x) &= \qquad\qquad g_m x^m + \ldots \qquad\qquad + g_0
\end{aligned}
$$

Expandindo o determinante de M' com respeito a última coluna, obtemos a identidade $A(x)f(x) + B(x)g(x) = det(M') = det(M) = Res(f,g)$, onde os coeficientes de $A(x), B(x)$ são os cofatores da última coluna de M', e consequentemente de M, e portanto pertencem a $K[x]$.

O que vamos tentar fazer agora, é a generalização do resultante em várias variáveis. O que parece não ser tão trivial. Veremos que para o caso de várias variáveis, o resultante é uma ferramenta para resolução de sistemas de equações polinomiais.

3.3 Resultante a Várias Variáveis

Nessa secção vamos estender a noção do resultante em sistemas de várias variáveis. De fato o melhor caminho para isto é a homogeneização dos polinômios. Assim iniciaremos com uma motivação e em seguida um teorema clássico.

3.3.1 Resultantes Homogêneos

Definição 3.3.1. *Um polinômio f é dito homogêneo se todos os monômios com coeficientes não nulos apresentam o mesmo grau total.*

Exemplo 3.3.1. *O polinômio $f = 4x^3 + 5xy^2 - z^3$ é um polinômio homogêneo de grau total igual a 3 em $K[x, y, z]$, enquanto que $g = 4x^3+5xy^2-z^6$ não é homogêneo.*

Porque trabalhar com Polinômios Homogêneos? Para uma motivação consideramos o sistema linear de duas variáveis

$$f_0(x, y) = x + 2y + 1 = 0$$

$$f_1(x, y) = x + 2y + 2 = 0$$

$$f_2(x, y) = x + 2y + 3 = 0$$

O determinante é zero, mas o sistema é incompatível em $\mathbb{C}^2$, de certa forma contrariando a noção de resultante. Por outro lado, as retas definidas por $f_i(x, y) = 0$ são paralelas e por esta razão podemos argumentar que elas têm um ponto em comum no infinito no espaço projetivo. Podemos fazer este raciocínio com mais precisão passando para o sistema homogêneo

$$F_0(x, y, z) = x + 2y + z = 0$$

$$F_1(x, y, z) = x + 2y + 2z = 0$$

$$F_2(x, y, z) = x + 2y + 3z = 0$$

que têm soluções não nulas da forma $(-2y, y, 0)$, isto é a homogeneização do sistema que tem uma solução no espaço projetivo $\mathbb{P}^2(\mathbb{C})$.

Motivação: Sejam n polinômios homogêneos $F_1 \ldots, F_n$ de n variáveis $(x_1, \ldots, x_n)$, onde o grau total de cada polinômio

$$F_i = \sum_{j_1+j_2+\ldots j_n=d_i} c_{j_1,\ldots j_n} x_1^{j_1} \ldots x_n^{j_n}$$

é d_i, queremos determinar uma solução não trivial para o sistema

$$F_1(x_1, \ldots, x_n) = \ldots = F_n(x_1, \ldots, x_n) = 0. \tag{3.2}$$

Como os F_i são homogêneos de grau total positivo, o sistema (3.2) sempre admite a solução $x_1 = \ldots = x_n = 0$, que é chamada de solução trivial. A questão crucial é quando existe uma solução não trivial. Para o resto do capítulo, trabalharemos sobre os números complexos, então aquela solução não trivial será um ponto em $\mathbb{C}^n$ - $\{(0, \ldots, 0)\}$.

Em geral, a existência de uma solução não trivial depende dos coeficientes dos polinômios $F_1, \ldots, F_n$. Podemos ver facilmente para um caso particular, em que os F_i são equações lineares:

$$\begin{aligned} F_1 &= c_{11}x_1 + \ldots + c_{1n}x_n = 0 \\ &\vdots \\ F_n &= c_{n1}x_1 + \ldots + c_{nn}x_n = 0, \end{aligned}$$

A Álgebra Linear nos fornece que este sistema de equações lineares possui uma solução não trivial se e somente se o determinante dos coeficientes da matriz é zero. Então obtemos uma condição simples $det(c_{ij}) = 0$ para a existência de uma solução não trivial. O que vamos fazer é tentar obter uma condição para um caso mais geral.

Retornando ao sistema (3.2), temos a seguinte questão: Quais são as condições dos coeficientes de $F_1, \ldots, F_n$ para que o sistema (3.2) tenha uma solução não trivial?

Antes de responder esta questão, considere os coeficientes do sistema (3.2). Denotando os coeficientes por (c_{j_i}), com $1 \leq i \leq n$, no total de N coeficientes, estes constituem um espaço afim $\mathbb{C}^N$.

Podemos observar que se um ponto do espaço projetivo em $\mathbb{P}^{n-1}(\mathbb{C})$ tem duas coordenadas homogêneas $(x_1, \ldots, x_n)$ e $(y_1, \ldots, y_n)$, então existe um $\lambda \in \mathbb{C}$ tal que $(y_1, \ldots, y_n) = \lambda(x_1, \ldots, x_n)$. Se $F(x_1, \ldots, x_n)$ é homogêneo de grau d e $(y_1, \ldots, y_n) = \lambda(x_1, \ldots, x_n)$ são dois conjuntos de coordenadas homogêneas para algum ponto $p \in \mathbb{P}^{n-1}(\mathbb{C})$, então

$$F(y_1, \ldots, y_n) = \lambda^d(x_1, \ldots, x_n).$$

Agora podemos responder a nossa questão com o seguinte teorema. A prova deste resultado foi baseada no artigo [21].

Teorema 3.3.1. *Fixando os graus $d_1, ..., d_n \in \mathbb{N}$ então existe um único polinômio irredutível (a menos de um sinal) $Res \in \mathbb{Z}[u]$ que satisfaz as seguintes propriedades:*

i) Se $F_1, \ldots, F_n \in \mathbb{C}[x_1, \ldots, x_n]$ são polinômios homogêneos de grau $d_1, \ldots, d_n$, então a equação (3.2) tem uma solução não trivial em $\mathbb{C}^n$ se e somente se o $Res_{d_1,\ldots,d_n}(F_1, ..., F_n) = 0$.

ii)$Res_{d_1,\ldots,d_n}(F_1, \ldots F_n)$ é irredutível quando visto como um polinômio em $\mathbb{C}[u]$.

Dem: Sejam os polinômios homogêneos $F_1, \ldots, F_n$ de graus $d_1, \ldots, d_n$. Para cada coeficiente $c_{i,\alpha}$, de cada monômio x^α de F_i com grau $\alpha = d_i$, introduzimos um nova variável $u_{i,\alpha}$. Seja $\mathbb{Z}[u]$ o anel dos polinômios com coeficientes inteiros com estas variáveis. O número total destas variáveis em $\mathbb{Z}[u]$ é igual a $N = \sum_{i=1}^{n} \begin{pmatrix} n + d_i - 1 \\ d_i \end{pmatrix}$. Dado um polinômio $P \in \mathbb{Z}[u]$ temos que $P(F_1, \ldots, F_n)$ denota o número obtido pelas substituições de cada variável u_{j_i} pelo correspondente coeficiente c_{j_i}.

Então considere os seguintes polinômios:

$$\mathbf{F}_i = \sum_{|\alpha|=d_i} u_{i,\alpha} x^\alpha.$$

Chamaremos estes polinômios de universais. Note que os coeficientes de x^α são as variáveis $u_{i,\alpha}$. Para determinar uma solução não trivial destes polinômios, usaremos o espaço projetivo $\mathbb{P}^{n-1}(\mathbb{C})$. Considere o seguinte:

i) Seja $x = (x_1, \ldots, x_n)$ com coordenadas homogêneas em $\mathbb{P}^{n-1}(\mathbb{C})$.

ii) Agora considere o produto $\mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C})$. Um ponto $(u_{i,\alpha}, x_1, \ldots, x_n) \in \mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C})$ pode ser visto como n polinômios e um ponto de $\mathbb{P}^{n-1}(\mathbb{C})$. Os polinômios universais $\mathbf{F}_i$ são de fato polinômios em $\mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C})$.

Considere a variedade $W = \mathbf{V}(\mathbf{F}_1, \ldots, \mathbf{F}_n)$. Concretamente, este conjunto é determinado por:

$W = \{(u_{i,\alpha}, x_1, \ldots, x_n) \in \mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C}) : (x_1, \ldots, x_n)$ é uma solução não trivial de $F_1 = \ldots = F_n = 0.\}$

Agora vem a parte interessante: existe uma projeção natural, função tal que

$$\pi : \mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C}) \longrightarrow \mathbb{C}^N$$

definida por $\pi(u_{i,\alpha}, x_1, \ldots, x_n) = (u_{i,\alpha})$, tal que

$\pi(W) = \{(u_{i,\alpha}) \in \mathbb{C}^N :$ existe um $(x_1, \ldots, x_n) \in \mathbb{P}^{n-1}(\mathbb{C})$ de modo que $(u_{i,\alpha}, x_1, \ldots, x_n) \in W\}$

$= \{$ todos os possíveis conjuntos das equações $F_1 = \ldots = F_n = 0$ de graus $d_1, \ldots, d_n$ que tem uma solução não trivial $\}$.

O conteúdo essencial deste teorema é provar que o conjunto $\pi(W)$ é definido por uma única equação irredutível, que é o $Res_{d_1,\ldots,d_n}(F_1, \ldots, F_n) = 0$.

Para provar isto, primeiramente vamos provar que $\pi(W)$ se anula quando $F_1 = F_2 = \ldots = F_n = 0$ tem uma solução não trivial. Provar isto é equivalente a provar que $\pi(W)$ é uma variedade em $\mathbb{C}^N$. Desta forma, pelo seguinte resultado de [19], secção I. 6.3:

Dada uma variedade $W \subset \mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C})$ e uma projeção $\pi : \mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C}) \longrightarrow \mathbb{C}^N$ a imagem $\pi(W)$ é uma variedade em $\mathbb{C}^N$. Consequentemente $\pi(W)$ é definido pelo anulamento de certos polinômios em $\mathbb{C}^N$. Em outras palavras, a existência de uma solução não trivial de $F_1 = \ldots = F_n = 0$ é determinada através do polinômio com condições sobre os coeficientes de $F_1, \ldots, F_n$.

O segundo passo para a prova é mostrar que precisamos somente de um polinômio e que este polinômio é irredutível. A prova requer um certo conhecimento de fatos sobre a dimensão e a irredutibilidade de uma variedade (ver [19], secção I. 6.3). Se aceitarmos uma idéia intuitiva da dimensão, então a idéia básica é mostrar que a variedade $\pi(W) \subset \mathbb{C}^N$ é irredutível (não podemos decompor em pedaços menores que são ainda variedades) de dimensão $N - 1$. Neste caso, a teoria nos mostrará que $\pi(W)$ deve ser definida por exatamente uma equação irredutível, que é o resultante $Res_{d_1,\ldots,d_n}(F_1, \ldots, F_n) = 0$.

Antes de provarmos que $\pi(W)$ é irredutível de dimensão $N-1$, provaremos que a variedade W também é irredutível de dimensão $N-1$. Para isto, considere a projeção

$$\phi : \mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C}) \longrightarrow \mathbb{P}^{n-1}(\mathbb{C})$$

$$(u, x) \longrightarrow x$$

Então $\phi(W) = \mathbb{P}^{n-1}(\mathbb{C})$. Mais precisamente a pré-imagem de $\phi^{-1}(x)$ de qualquer ponto $x \in \mathbb{P}^{n-1}(\mathbb{C})$ pode ser identificado como o conjunto $\{u \in \mathbb{C}^N : (u, x) \in W \}$. Isto é um subespaço de dimensão n em $\mathbb{C}^N$. Para esta situação, novamente aplicaremos um resultado de [19], secção I. 6.3. Ele mostra que W é fechado e uma variedade irredutível do subespaço de dimensão n em $\mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C})$. Por esta razão a $dim(W) = N - 1$.

Retornando à projeção $\pi : \mathbb{C}^N \times \mathbb{P}^{n-1}(\mathbb{C}) \longrightarrow \mathbb{C}^N$, pelo Teorema principal da teoria de eliminação [19], secção I. 6.3, diz que $\pi(W)$ é uma subvariedade irredutível de $\mathbb{C}^N$ que é bem definido sobre $\mathbb{Q}$, todo ponto $c \in \mathbb{C}^N$ pode ser identificado como um sistema polinômial $(F_1, \ldots, F_n)$ de (3.2). Este sistema tem uma

solução não trivial se e somente se c pertence a variedade $\pi(W)$. Para todo c temos

$$dim(\pi(W)) \leq dim(W) = N - 1 \leq dim(\pi^{-1}(c)) + dim(\pi(W))$$

Estas desigualdades podem ser vistas em [19], secção I. 6.3. Agora escolhemos $c = (F_1, \ldots, F_n)$ e $F_1, \ldots, F_{n-1}$ são as equações de (3.2) que têm um número finito de zeros em $\mathbb{P}^{n-1}(\mathbb{C})$. Então escolhendo F_n que se anule exatamente em um destes zeros e chamando de $y \in \mathbb{P}^{n-1}(\mathbb{C})$, temos que $\pi^{-1}(c) = \{(c, y)\}$ é uma varidade zero dimensional. Para esta escolha particular de c ambas desigualdades se mantém com a igualdade. Isto implica que $dim(\pi(W)) = N - 1$. □

3.4 Algumas Propriedades de Resultantes a Várias Variáveis

Agora vamos ver as principais propriedades de resutantes a várias variáveis. As provas têm um nível de tecnalidade usando ferramentas de Geometria Algébrica. Como o nosso objetivo principal é o desenvolvimento do resultante como ferramenta para resolução de sistemas de equações polinomiais, vamos omitir as provas destas propriedades. Para ver as provas destas propriedades sugerimos [10], [12] e [13].

Propriedade 3.4.1. *Para um j fixo entre 1 e n, o $Res_{d_1,\ldots,d_n}(F_1, \ldots, F_n)$ é um polinômio homogêneo nas variáveis $u_{j,\alpha}$, de grau $d_1 d_2 \ldots d_{j-1} d_{j+1} \ldots d_n$ isto é*

$$Res(F_1, \ldots, \lambda F_j, \ldots, F_n) = \lambda^{d_1 \ldots d_{j-1} d_{j+1} \ldots d_n} Res(F_1, \ldots, F_n).$$

Além disso, o grau total do resultante é $\sum_{j=1}^{n} d_1 \ldots d_{j-1} d_{j+1} \ldots d_n$.

Propriedade 3.4.2. *Para $i < j$*

$$Res(F_1, \ldots, F_i, \ldots, F_j, \ldots, F_n) = (-1)^{d_1 \ldots d_n} Res(F_1, \ldots, F_j, \ldots, F_i, \ldots, F_n).$$

Propriedade 3.4.3. *Existem polinômios $A_1, \ldots A_n$ nas variáveis $x_1, \ldots, x_n$ de modo que*

$$Res(F_1, \ldots, F_n) = A_1 F_1 + \ldots + A_n F_n.$$

O nosso próximo problema, é saber como calcular este polinômio que representa o resultante a várias variáveis. De fato existem muitas maneiras de se obter este polinômio. Assim no próximo capítulo apresentaremos duas técnicas.

4 CALCULANDO RESULTANTES

O objetivo deste capítulo é calcular o resultante para o caso de polinômios homogêneos em várias variáveis. Primeiramente vamos apresentar a fórmula de Macaulay, que se baseia na teoria de Geometria Algébrica. Em seguida apresentaremos o algoritmo. Também desenvolveremos a fórmula de Poisson. Para as fórmulas indicamos [3] e [24].

4.1 Como calcular os Resultantes Homogêneos?

Primeiramente vamos ilustrar o resultante para um caso particular. Em seguida partiremos para o caso geral. Assim, considere o seguinte sistema de três equações homogêneas de três variáveis:

$$F_0 = a_1x + a_2y + a_3z = 0$$

$$F_1 = b_1x + b_2y + b_3z = 0$$

$$F_2 = c_1x^2 + c_2y^2 + c_3z^2 + c_4xy + c_5xz + c_6yz = 0.$$

Queremos calcular o $Res_{1,1,2}(F_0, F_1, F_2)$. A idéia é multiplicar cada equação do sistema por um monômio apropriado, então obter uma matriz quadrada cujo determinante, nós podemos calcular. A questão é, quem são estes monômios e como obtê-los?

Tomamos o conjunto dos monômios de grau total igual a 2. Este conjunto é formado por $S = \{\ x^2, xy, xz, y^2, yz, z^2\}$. Agora consideramos os seguintes subconjuntos:
$S_0 = \{$ monômios de grau 2; x divide estes $\} = \{\ x^2, xy, xz\ \}$
$S_1 = \{$ monômios de grau 2; x não divide estes mas y divide $\} = \{y^2, yz\ \}$
$S_2 = \{$ monômios de grau 2; x, y não dividem estes mas z^2 divide $\} = \{z^2\ \}$
Observe que $S = \bigcup S_i$. Agora consideramos o seguinte sistema de equações:

$$x^2/x \cdot F_0 = xy/x \cdot F_0 = xz/x \cdot F_0 = y^2/y \cdot F_1 = yz/y \cdot F_1 = z^2/z^2 \cdot F_2 = 0$$

que podemos reescrever como:

$$\begin{array}{ccccccccccccc}
a_1x^2 & + & 0 & + & 0 & + & a_2xy & + & a_3xz & + & 0 & = 0 \\
0 & + & a_2y^2 & + & 0 & + & a_1xy & + & 0 & + & a_3yz & = 0 \\
0 & + & 0 & + & a_3z^2 & + & 0 & + & a_1xy & + & a_2yz & = 0 \\
0 & + & b_2y^2 & + & 0 & + & b_1xy & + & 0 & + & b_3yz & = 0 \\
0 & + & 0 & + & b_3z^3 & + & 0 & + & b_1xz & + & b_2yz & = 0 \\
c_1x^2 & + & c_2y^2 & + & c_3z^2 & + & c_4xy & + & c_5xz & + & c_6yz & = 0
\end{array}$$

Então obtemos um sistema de 6 equações. Usando o Maple vemos que sistema acima possui uma solução não trivial. Denotando por M a matriz dos coeficientes deste sistema, obtemos que $det(M) = -a_1R$, onde R é um polinômio nas variáveis a_i, b_i, c_i. Como o sistema admite solução, o $det(M) = 0$. Se $a_1 \neq 0$, implica que o polinômio $R = 0$. Por outro lado o $Res_{1,1,2}(F_0, F_1, F_2)$ é um polinômio que se anula nas variáveis a_i, b_i, c_i. Isto implica que R é mútiplo do $Res_{1,1,2}(F_0, F_1, F_2)$. Assim o $det(M)$ é divisível pelo resultante, $det(M) = Res_{1,1,2}(F_0, F_1, F_2) \times fator\ estranho$. No caso geral, provaremos como determinar este $fator\ estranho$ e chegaremos na fórmula desejada.

Passamos agora para o caso geral. Sejam $n+1$ polinômios homogêneos $F_0, \ldots, F_n$ de $n+1$ variáveis $(x_0, \ldots, x_n)$, onde o grau total de cada polinômio é d_i, considere o sistema

$$F_0(x_0, \ldots, x_n) = \ldots = F_n(x_0, \ldots, x_n) = 0. \tag{4.1}$$

Como vimos no caso particular, a idéia é multiplicar cada equação do sistema (4.1) por um monômio apropriado. Então obtemos uma matriz quadrada cujo determinante vai explicitar o resultante a menos de um fator, chamado de $fator\ estranho$. Sejam $F_0, \ldots, F_n \in K[x_0, \ldots, x_n]$, de graus totais $d_0, \ldots, d_n$, respectivamente então seja

$$d = \sum_{i=0}^{n}(d_i - 1) + 1 = \sum_{i=0}^{n} d_i - n$$

e o conjunto S dos monômios $x^\alpha = x_0^{a_0} \ldots x_n^{a_n}$ de grau total d e dividimos então em $n+1$ subconjuntos como segue:

$$S_0 = \{\ x^\alpha : \quad |\,\alpha\,| = d,\ \ x_0^{d_0} \quad \textit{divide}\ \ x^\alpha\}$$
$$S_1 = \{\ x^\alpha : \quad |\,\alpha\,| = d,\ \ x_0^{d_0} \quad \text{não}\ \ \textit{divide}\ \ x^\alpha\ \ \textit{mas}\ \ x_1^{d_1}\textit{divide}\}$$
$$\vdots$$
$$S_n = \{\ x^\alpha : \quad |\,\alpha\,| = d,\ \ x_0^{d_0}, ..., x_{n-1}^{d_{n-1}} \qquad \text{não}\ \textit{dividem}\ \ x^\alpha\ \ \textit{mas}\ \ x_n^{d_n}\textit{divide}\}$$

Observe que por construção, todos estes conjuntos S_i são disjuntos, ou seja, $S = \bigcup_{i=0}^{n} S_i$. Esta construção implica no seguinte resultado.

Proposição 4.1.1. *Todo monômio de grau total d é divisível por um $x_i^{d_i}$ para algum $i \in \{0, \ldots, n\}$.*

Prova: Seja x um monômio de grau total d, $x = x_0^{\beta_0} x_1^{\beta_1} \ldots x_n^{\beta_n}$ tal que $\beta_0 + \beta_1 + \ldots + \beta_n = d$. Vamos supor por absurdo que para todo i, $x_i^{d_i}$ não divide x. Isto implica que todas as potências β_i de x_i em x são menores que d_i. Mas $d = d_1 + d_2 + \ldots + d_n < \beta_1 + \beta_2 + \ldots + \beta_n = d$.

Proposição 4.1.2. *O número de monômios em S_n é exatamente $d_0 \ldots d_{n-1}$.*

Prova: Considere a seguinte afirmação: Dados inteiros $a_0, a_1, \ldots, a_{n-1}$ com $0 \leq a_i \leq d_i - 1$ existe um único a_n de modo que $x_0^{a_0} \ldots x_n^{a_n} \in S_n$. Para provar a existência considere os inteiros $a_0, a_1, \ldots, a_{n-1}$. Existe um inteiro a_n tal que $a_0 + a_1 + \ldots + a_{n-1} + a_n = d$. Segue que $x_0^{a_0} \ldots x_n^{a_n}$ tem grau total d. Pela proposição (4.1.1) ele deve pertencer para algum S_i com $0 \leq i \leq n$. Sabendo que $0 \leq a_i \leq d_i - 1 < d_i$ então $x_0^{d_0}, x_1^{d_1}, \ldots, x_{n-1}^{d_{n-1}}$ não dividem $x_0^{a_0} \ldots x_n^{a_n}$ como este tem grau d implica que $x_0^{a_0} \ldots x_n^{a_n} \in S_n$. Para a unicidade vamos supor que existe a_n' tal que $x_0^{a_0} \ldots x_n^{a_n'} \in S_n$. Como $x_0^{a_0} \ldots x_n^{a_n}$ e $x_0^{a_0} \ldots x_n^{a_n'}$ tem o mesmo grau d então $a_0 + \ldots + a_n = a_0 + \ldots + a_n'$, logo $a_n = a_n'$. Assim, para cada escolha de $a_0, a_1, \ldots, a_{n-1}$ com $0 \leq a_i \leq d_i - 1$, existe um único monômio com grau total d que pertence a S_n. Pelo princípio multiplicativo, existem exatamente $d_0 d_1 \ldots d_{n-1}$ tais escolhas.

Assim reescrevemos o sistema de equações (4.1) por:

$$\begin{cases} x^{\alpha}/x_0^{d_0}.F_0 & = 0 \quad para \quad x^{\alpha} \in S_0 \\ & \vdots \\ x^{\alpha}/x_j^{d_j}.F_j & = 0 \quad para \quad x^{\alpha} \in S_j \\ & \vdots \\ x^{\alpha}/x_n^{d_n}.F_n & = 0 \quad para \quad x^{\alpha} \in S_n \end{cases} \tag{4.2}$$

Proposição 4.1.3. *O sistema (4.2) tem N equações e N variáveis, onde* $N = \begin{pmatrix} d+n \\ n \end{pmatrix}$.

Prova: F_i tem grau total d_i, segue que $x^{\alpha}/x_i^{d_i}.F_i$ tem grau total d. Então cada polinômio do lado esquerdo de (4.2) pode ser escrito como uma combinação linear dos monômios de grau total d. Sabendo que o número de monômios de grau total d em $n+1$ variáveis é o coeficiente binômial $N = \begin{pmatrix} d+n \\ n \end{pmatrix}$, então observe que o número total de equações é o número de elementos de $S_0 \cup \ldots \cup S_n$ que também é N. Assim considerando os monômios de grau total d como variáveis, obtemos um sistema de N equações e N variáveis.

Vamos representar o determinante dos coeficientes da matriz $N \times N$ da equação (4.2) por D_n. O determinante D_n é claramente um polinômio de coeficientes de F_i.

Proposição 4.1.4. *O polinômio D_n é homogêneo de grau $d_0 \ldots d_{n-1}$.*

Prova: Pela proposição (4.1.2) o número de elementos em S_n é exatamente $d_0 \ldots d_{n-1}$. Assim se multiplicarmos cada coeficiente de F_n por $\lambda \in \mathbb{C}$ temos que D_n ficará multiplicado por $\lambda^{d_0 \ldots d_{n-1}}$. Logo D_n é homogêneo.

Proposição 4.1.5. *D_n é divisível pelo resultante, ou seja, $D_n = Res \times fator$ estranho.*

Prova: Primeiramente vamos provar que D_n se anula quando $F_0 = \ldots = F_n = 0$ tem uma solução não trivial. Se os F_i todos se anulam para $(r_0, \ldots, r_n) \neq (0, \ldots, 0)$ então os monômios de grau total d em $(r_0, \ldots, r_n)$ geram uma solução não trivial para o sistema (4.1), logo implica que o determinante D_n se anula. Pensando geometricamente, provamos que o espaço dimensional $\mathbb{C}^N$ formado pelas coordenadas c_{ij} com $1 \leq i, j \leq N$ do polinômio D_n se anula no conjunto $\{ (c_{ij}); 1 \leq i, j \leq N$: (4.1) tem solução não trivial $\} \subset \mathbb{C}^N$. Mas isto é equivalente pelo teorema (3.3.1) no anulamento do $Res_{d_0,\ldots,d_n}(F_0, \ldots, F_n)$, então D_n se anula no conjunto

$$\mathbf{V}(Res_{d_0,\ldots,d_n}(F_0, ..., F_n)) \subset \mathbb{C}^N.$$

Isto significa que $D_n \in \mathbf{I}(\mathbf{V}(Res_{d_0,\ldots,d_n}(F_0, \ldots, F_n) = \sqrt{< Res_{d_0,\ldots,d_n}(F_0, \ldots, F_n) >}$. Esta igualdade é válida pela proposição (2.3.1).
Mas o $Res_{d_0,\ldots,d_n}(F_0, \ldots, F_n)$ é irredutível que implica em

$$\sqrt{< Res_{d_0,\ldots,d_n}(F_0, \ldots, F_n) >} =< Res_{d_0,\ldots,d_n}(F_0, \ldots, F_n) > .$$

Isto prova que $D_n \in< Res_{d_0,\ldots,d_n}(F_0, \ldots, F_n) >$. Isto segue que D_n é um mútiplo do $Res_{d_0,\ldots,d_n}(F_0, \ldots, F_n)$.

Proposição 4.1.6. *Seja $E \in \mathbb{Z}[u]$ irredutível e não constante. Se $F \in \mathbb{Q}[u]$ de modo que $D = E \cdot F \in \mathbb{Z}[u]$, então $F \in \mathbb{Z}[u]$.*

Prova: Podemos encontrar um inteiro positivo m tal que $mF \in \mathbb{Z}[u]$. Então aplicando a fatoração única para $mD = E \cdot mF$, vemos que $m\dfrac{D}{E} = mF$. Já que $E \in \mathbb{Z}[u]$, logo $F = \dfrac{D}{E} \in \mathbb{Z}[u]$.

Proposição 4.1.7. *O fator estranho de (4.1.5) é um polinômio inteiro de coeficientes de $\overline{F}_0, ..., \overline{F}_{n-1}$, onde $\overline{F}_i = F_i(x_0, ..., x_{n-1}, 0)$*

Prova: O determinante D_n é um polinômio em $\mathbb{Z}[u_{i,\alpha}]$, e também sabemos que o $Res \in \mathbb{Z}[u_{i,\alpha}]$. Pela proposição (4.1.5) temos que o fator estranho deve pertencer

a $\mathbb{Q}[u_{i,\alpha}]$, pois dividindo D_n pelo Res obtemos coeficientes racionais. Denotando o fator estranho por E_n, sabemos que o Res é irredutível em $\mathbb{Z}[u_{i,\alpha}]$, assim pela proposição (4.1.6) implica que $E_n \in \mathbb{Z}[u_{i,\alpha}]$. Como o Res e D_n tem o mesmo grau $d_0 \dots d_{n-1}$ nos coeficientes de F_n, segue que E_n tem grau zero nos coeficientes de F_n, então E_n depende somente dos coeficientes de $\overline{F}_0, \dots, \overline{F}_{n-1}$.

Note que a proposição (4.1.5) fornece um método para calcular o resultante. Pois basta fatorar o polinômio D_n em fatores lineares. Os fatores irredutíveis de D_n serão os candidatos ao resultante. Infelizmente, este método é impraticável devido ao fato de que a fatoração de várias variáveis, é um problema muito complexo, especialmente para polinômios grandes como D_n.

Os conjuntos $S_0, \dots, S_n$ e o determinante D_n dependem de como as variáveis $x_0, \dots, x_n$ são ordenadas. De fato, a notação D_n foi escolhida para enfatizar a variável x_n vir a ser a última. Se fixarmos i entre 0 e $n-1$ e ordenar as variáveis então x_i torna-se a última, assim obtemos conjuntos $S_0, \dots, S_n$ levemente diferentes e sistemas da equação (4.2)levemente diferentes. Vamos denotar D_i o determinante deste sistema de equações.

Proposição 4.1.8. *Sejam $F_0, \dots, F_n$ polinômios universais ($F_i \in \mathbb{Z}[u]$). Então o resultante é o máximo divisor comum dos polinômios $D_0, \dots, D_n$ no anel $\mathbb{Z}[u_{i,\alpha}]$, isto é,*

$$Res = MDC(D_0, \dots, D_n).$$

Prova: Para cada i, existe muitas escolhas para D_i (correspondendo a $(n-1)!$ formas de ordenar as variáveis para x_i ser a última). Temos que mostrar que não importa a escolha da ordem para D_i, o $MDC(D_0, \dots, D_n)$ é o resultante. Pela proposição (4.1.5) sabemos que o Res divide D_n, e o mesmo é claramente verdadeiro para $D_0, \dots, D_{n-1}$. Além disso o argumento utilizado na prova mostrou que $D_i = Res.E_i$, onde $E_i \in \mathbb{Z}[c_{i,\alpha}]$, não envolve os coeficientes de F_i. Segue que o

$$MDC(D_0, \dots, D_n) = Res.MDC(E_0, \dots, E_n).$$

Assim cada E_i não envolve as variáveis $u_{i,\alpha}$, o MDC a direita deve ser constante, isto é um inteiro. De qualquer modo já que os coeficientes de D_n são relativamente primos, logo este inteiro deve ser ± 1.

4.2 A Fórmula de Macaulay

Nesta secção vamos determinar o fator estranho da proposição (4.1.5). Esse resultado é devido a Macaulay [16].

Definição 4.2.1. *Sejam $d_0, \ldots, d_n$ os graus de $F_0, \ldots, F_n$ e $d = \sum_{i=0}^{n} d_i - n$.*
i) Um monômio x^α de grau total d é reduzido se $x_i^{d_i}$ divide x^α para exatamente um i.
ii)D'_n é o determinante de uma submatriz de coeficientes da matriz (4.2) obtida por eliminação de todos as linhas e colunas correspondente aos monômios reduzidos x^α.

Exemplo 4.2.1. *O $Res_{1,1,2}(F_0, F_1, F_2)$ no início da secção (4.1), temos que $(d_0, d_1, d_2) = (1, 1, 2)$ e que $n = 2$. D_2 é o determinante dos coeficientes da matriz 6×6. Assim todos os monômios de grau 2 são reduzidos exceto xy. E $D'_2 = a_1$ corresponde a submatriz obtida deletando todas as linhas e colunas exceto a 2 linha e a 4 coluna.*

Uma observação importante, é que podemos representar D'_n como: $D'_n = det \begin{bmatrix} * & E_1 \\ E_2 & 0 \end{bmatrix} = \pm det(E_1) \times det(E_2)$, onde E_1 e E_2 são submatrizes da matriz nos coeficientes definida em (4.2).

A observação de Macaulay [16], é de que o $fator\ estranho$ é exatamente dado por D'_n, ou seja :

Teorema 4.2.1. *Sejam $F_0, ..., F_n$ polinômios universais ($F_i \in \mathbb{Z}[u]$), o resultante é dado por*

$$Res = \frac{D_n}{D'_n}$$

desde que $D'_n \neq 0$, onde D_n e D'_n são bem definidos nas secções (4.1) e (4.2) respectivamente.

Uma prova moderna desse resultado pode ser encontrado em [12]. A seguir esboçamos uma prova algébrica que não precissa de resultados geométricos. Essa prova é baseada no artigo [4].

Dem: Sejam os polinômios homogêneos $F_0, \ldots, F_n$ de graus $d_0, \ldots, d_n$, onde c_{α_i} são os coeficientes de cada monômio x^α de F_i com $\alpha = d_i$. Primeiramente provaremos que D'_n divide D_n. Para isto, usamos o seguinte truque: considere o anel $B = \mathbb{Z}[u_{\alpha_i}]$ com $\alpha_i = d_i$, onde u_{α_i} são variáveis novas dos polinômios

$$F_i = \sum_{\alpha_i = d_i} u_{\alpha_i} x_i^{\alpha_i}.$$

Seja D^u a matriz da transformação linear, que associa cada F_{u_i} com F_i. Considere $A = \mathbb{Z}[c_{\alpha_i}, u_{\alpha_i}]$, e considere a matriz $M(c,u)$ com coeficientes em A dada por:

$$M(c,u) = \begin{bmatrix} * & D \\ D^u & 0 \end{bmatrix}.$$

É fácil de ver aquele $det(M(c,c)) = D_n$, e por causa do lema (4.2.2) abaixo, temos que $\det(E_1)$ divide $\det(M(c,u))$ em A.Transpondo $M(c,u)$ e usando um argumento simétrico, novamente pelo mesmo lema, podemos concluir aquele $\det(E_2^u)$ divide $\det(M(c,u))$ em A. O anel A é um domínio fatorial e $\det(E_1)$ e $\det(E_2^u)$ não têm fatores comuns em A, porque eles dependem de variáveis diferentes. Assim, temos

$$det(M(c,u)) = p(c,u) det(E_1) det(E_2^u)$$

para algum $p \in A$. Agora, especificamos $u_{\alpha_i} \to c_{\alpha_i}$. O fato que $\det(M(c,c))$ é múltiplo do resultante foi demonstrado na proposição (4.1.5) . Por outro lado, desde que o Resultante é irredutível e depende de todos os coeficientes de F_i, enquanto $\det(E_1)$ e $\det(E_2)$ não dependem dos coeficientes de F_n, concluímos que o resultante divide $p(c,c)$. Além disso, o lema (4.2.1)a seguir, diz que eles têm o mesmo grau. Então, a razão deles é um número racional λ. Podemos ver aquele $\lambda = \pm 1$, assim

$$Res = \frac{det(M(c,c))}{det(E_1) \times det(E_2)} = \frac{D_n}{D'_n}$$

□

Exemplo 4.2.2. *Considerando o* $Res_{d_0,d_1,d_2}(F_0, F_1, F_2)$ *do início da secção (4.1), temos que* D_2 *é o determinante do sistema de 6 equações e* $D_2' = a_1$*. Então pelo teorema (4.2.1) o* $Res_{d_0,d_1,d_2}(F_0, F_1, F_2)$ *é igual a* $a_1^2b_2^2c_3 + a_1^2b_3^2c_2 - 2a_1a_2b_1b_2c_3 + a_1a_2b_1b_3c_6 + a_1a_2b_2b_3c_5 - a_1a_2b_3^2c_4 + a_1a_3b_1b_2c_6 - 2a_1a_3b_1b_3c_2 - a_1a_3b_2^2c_5 + a_1a_3b_2b_3c_4 + a_2^2b_1^2c_3 - a_2^2b_1b_3c_5 + a_2^2b_3^2c_1 - a_2a_3b_1^2c_6 + a_2a_3b_1b_2c_5 + a_2a_3b_1b_3c_4 - 2a_2a_3b_2b_3c_1 + a_3^2b_1^2c_2 - a_3^2b_1b_2c_4 + a_3^2b_2^2c_1$.

Lema 4.2.1. *O* $grau(D_n)$ *é igual* $grau(Res)$ *+* $grau(E_1)$ *+* $grau(E_2)$

$$= d_1 \dots d_{i-1}d_{i+1} \dots d_n \ \ + grau(E_1) \ \ + grau(E_2)$$

A prova deste lema é, em linhas gerais, análogo ao lema(5.3.1) do próximo capítulo, com o cuidado de que devemos fazer uma expansão de Laplace para reduzir o problema a 3 variáveis.

Lema 4.2.2. *Seja* A *um anel e* M *uma matriz quadrada com os coeficientes em* A *com a seguinte estrutura:* $M = \begin{bmatrix} M_1 & D \\ M_2 & 0 \end{bmatrix}$*, onde* M_1, M_2 *são matrizes retangulares. Então existe um elemento* $m \in A$ *tal que*

$$det(M) = m\, det(E_1).$$

A prova deste lema será omitida, pelo fato de ser um resultado que pode ser provado usando ferramentas da Álgebra Linear. Sugerimos o artigo [4] para demonstração.

Existem dois fatos importantes deste lema: o primeiro é que D é uma matriz que representa uma transformação linear e E_1 uma submatriz apropriada de D. No nosso caso, D representará o resultante numa base de monômios e o segundo, é que o $det(E_1)$ divide o $\det(M)$.

Aplicando todos estes resultados vamos agora obter um algoritmo para calcular o resultante.

4.2.1 O Algoritmo

Agora vamos apresentar um algoritmo para determinar o resultante de polinômios homogêneos em várias variáveis. Considere $F_0, \ldots, F_n$ polinômios homogêneos de graus $d_0, \ldots, d_n$ nas variáveis $x_0, \ldots, x_n$. Assim de forma análoga a secção (4.1) considere o conjunto $S = \{\ x^\alpha = x_0^{a_0} \ldots x_n^{a_n};\ |\ \alpha\ |= d\ \}$. Onde $d = \sum_{i=0}^{n}(d_i - 1) + 1 = \sum_{i=0}^{n} d_i - n$.

Agora considere os subconjuntos disjuntos de S :

$S_0 = \{\ x^\alpha : \quad |\ \alpha\ |= d,\ \ x_0^{d_0} \quad divide\ \ x^\alpha\}$

$S_1 = \{\ x^\alpha : \quad |\ \alpha\ |= d,\ \ x_0^{d_0} \quad$ não $\ divide\ \ x^\alpha\ \ mas\ \ x_1^{d_1} divide\}$

$\vdots$

$S_n = \{\ x^\alpha : \quad |\ \alpha\ |= d,\ \ x_0^{d_0}, ..., x_{n-1}^{d_{n-1}} \qquad$ não $dividem\ \ x^\alpha\ \ mas\ \ x_n^{d_n} divide\}$.

O algoritmo de Macaulay [24], segue os passos da teoria desenvolvida nas secções anteriores. Portanto, seus passos estão bem justificados pelos resultados provados lá.

Algoritmo Macaulay

1. $T \leftarrow S$, $M = \emptyset$.

2. Para i variando de 0 a n faça:
   2.1 $U \leftarrow \{u \in T : x_i^{d_i} \mid u\}$, $S_i = \{u/x_i^{d_i} : u \in U\}$, $T \leftarrow T \backslash U$;
   2.2 Calcule $M \leftarrow M \bigcup \{uP_i : u \in S_i\}$
   Pare.

3. Para i variando de 0 a n - 1 faça:
   $N_i = \{\ u \in S_i : \exists j, i+1 \leq j \leq n, \ni x_j^{d_j} \mid u\ \}$.
   Pare.

4. Seja $N \leftarrow N_0 \bigcup \ldots \bigcup N_{n-1}$
   Se $N = \emptyset$, então $N \leftarrow (1)$;(N é uma submatriz de M)

5. $R = \dfrac{det(M)}{det(N)}$.

Exemplo 4.2.3. *Considere o seguinte sistema:*

$$F_0 = a_1x_0^2 - a_2x_1^2 = 0$$

$$F_1 = b_1x_0^2 - b_2x_1^2 + b_3x_0x_1 = 0$$

$$F_2 = x_0 - x_1 - x_2 = 0$$

Usando o algoritmo, temos que: $d = d_0 + d_1 + d_2 - n = 2 + 2 + 1 - 2 = 3$. *Assim* $S = \{x^\alpha\ ;|\ \alpha\ |= 3 : x_0^3,\ x_1^3,\ x_2^3,\ x_0x_1^2,\ x_0^2x_1,\ x_0x_2^2,\ x_0^2x_2,\ x_1x_2^2,\ x_1^2x_2,\ x_0x_1x_2\}$.

Os conjuntos S_i *são:*

$S_0 = \{x^\alpha \in S;\ x_0^2\ \textit{divide} : x_0^3,\ x_0^2x_1,\ x_0^2x_2\}$,

$S_1 = \{x^\alpha \in S;\ x_0^2\ \textit{não divide, mas}\ x_1^2\ \textit{divide} : x_1^3,\ x_0x_1^2,\ x_1^2x_2\}$,

$S_2 = \{x^\alpha \in S;\ x_0^2\, e\, x_1^2\ \textit{não dividem, mas}\ x_2\ \textit{divide} :\ x_2^3,\ x_0x_2^2,\ x_1x_2^2,\ x_0x_1x_2\}$.

Pelo passo 2 do algoritmo, temos que:

$x_0F_0 = x_1F_0 = x_2F_0 = x_1F_1 = x_0F_1 = x_2F_1 = x_2F_2 = x_0x_2F_2 = x_0x_1F_2 = x_1x_2F_2 = 0$,

que implica num sistema de tamanho $N \times N$, *onde* $N = \begin{pmatrix} d+n \\ n \end{pmatrix} = \begin{pmatrix} 3+2 \\ 2 \end{pmatrix} = \frac{5!}{2!3!} = 10$. *Ou seja, temos um sistema de 10 equações e 10 variáveis.*

$$\begin{array}{ccccccccccccc}
a_1x_0^3 & - & a_2x_0x_1^2 & + & 0 & + & \dots & + & 0 & = & 0 \\
a_1x_0^2x_2 & - & a_2x_1^2x_2 & + & 0 & + & \dots & + & 0 & = & 0 \\
a_1x_0^2x_1 & - & a_2x_1^3 & + & 0 & + & \dots & + & 0 & = & 0 \\
b_1x_0^3 & - & b_2x_0x_1^2 & + & b_3x_0^2x_1 & + & \dots & + & 0 & = & 0 \\
b_1x_0^2x_2 & - & b_2x_1^2x_2 & + & b_3x_0x_1x_2 & + & \dots & + & 0 & = & 0 \\
b_1x_0^2x_1 & - & b_2x_1^3 & + & b_3x_0x_1^2 & + & \dots & + & 0 & = & 0 \\
x_0^2x_2 & - & x_0x_1x_2 & - & x_0x_2^2 & + & \dots & + & 0 & = & 0 \\
x_0^2x_1 & - & x_0x_1^2 & - & x_0x_1x_2 & + & \dots & + & 0 & = & 0 \\
x_0x_1x_2 & - & x_1^2x_2 & - & x_1x_2^2 & + & \dots & + & 0 & = & 0 \\
x_0x_2^2 & - & x_1x_2^2 & - & x_2^3 & + & \dots & + & 0 & = & 0
\end{array}$$

Reorganizando este sistema, como um produto matricial, dos coeficientes pelas variáveis $\{x_0^3,\ x_0^2x_2,\ x_0^2x_1,\ x_0x_1^2,\ x_0x_1x_2,\ x_0x_2^2,\ x_1^2x_2,\ x_1^3,\ x_1x_2^2,\ x_2^3\}$, *temos pelo algoritmo que a matriz dos coeficientes é:*

$$M = \left[\begin{array}{cccccccccc} a_1 & 0 & 0 & -a_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 & 0 & 0 & -a_2 & 0 & 0 & 0 \\ 0 & 0 & a_1 & 0 & 0 & 0 & 0 & -a_2 & 0 & 0 \\ b_1 & 0 & b_3 & -b_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b_1 & 0 & 0 & b_3 & 0 & -b_2 & 0 & 0 & 0 \\ 0 & 0 & b_1 & 0 & 0 & b_3 & 0 & -b_2 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \end{array}\right].$$

Os passos 3 e 4 do algoritmo, determinam a submatriz de M, através dos monômios reduzidos. Pela definição os monômios reduzidos são os monõmios de grau 3 que são divisíveis por $x_i^{d_i}$, para exatamente um i, ou seja, são os monômios que têm apenas um dos seguintes divisores: x_0^2, x_1^2 ou x_2. Logo os monômios reduzidos são: $x_0^2x_2$ e $x_1^2x_2$. Então eliminamos todas as linhas e colunas da matriz M, exceto a segunda e quinta linhas com a segunda e sétima colunas. Assim a submatriz N de M é:

$$N = \left[\begin{array}{cc} a_1 & -a_2 \\ b_1 & -b_2 \end{array}\right]$$

Então pelo passo 5 do algoritmo, o resultante é dado por

$$Res_{2,2,1}(F_1, F_2, F_3) = b_2^2a_1^2 - 2a_1b_2a_2b_3 - 2a_1b_2a_2b_1 - a_1a_2b_3^2 + a_2^2b_3^2 + 2a_2^2b_3b_1 + a_2^2b_1^2.$$

4.3 Fórmula de Poisson

Existem muitas maneiras de calcular o resultante em várias variáveis. Na secção anterior apresentamos uma destas maneiras. O que vamos fazer agora é apresentar mais uma fórmula para o cálculo do resultante.

4.3.1 Fórmula de Poisson em uma Variável

Considere f, g dois polinômios em $K[x]$

$$f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i$$

de graus n, m respectivamente. Suponhamos que suas raízes são $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_m$. Então o resultante é dado por

$$Res(f,g) = f_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} g_m^n \prod_{j=1}^{m} f(\beta_j) = f_n^m g_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) \qquad (4.3)$$

Exemplo 4.3.1. *Sejam $f(x) = f_0 x + f_1$ e $g(x) = g_0 x + g_1$, com $f_0, g_0 \neq 0$. Usando a definição do capítulo 3, temos que:*

$$Res(f,g) := det \begin{bmatrix} f_o & g_0 \\ f_1 & g_1 \end{bmatrix} = f_0 g_1 - f_1 g_0.$$

Usando a fórmula de Poisson, reescrevemos o resultante como: $Res(f,g) = f_0 g_1 - f_1 g_0 = f_0 g_0 (\frac{g_1}{g_0} - \frac{f_1}{f_0})$, *onde* $\frac{g_1}{g_0}$ *e* $\frac{f_1}{f_0}$ *são as raízes de f e g respectivamente.*

A prova algébrica deste resultado pode ser vista no capítulo 3. Nesta fórmula fica claro que o resultante de f e g é nulo se e somente se f e g têm uma raiz em comum.

O que vamos fazer agora é esboçar uma prova mais geométrica, para em seguida, entender melhor a fórmula de Poisson em várias variáveis.

Como já provamos a equação (4.3), então provaremos apenas a primeira igualdade. Para entender a fórmula $Res(f,g) = f_n^m \prod_{i=1}^n g(\alpha_i)$, usaremos resultados do capítulo 2.

Deste modo considere a álgebra quociente $A_f = K[x]/ < f >$ e a função definida por: $m_g([h]) = [g]\cdot[h] = [gh] \in A_f$, onde $[h] \in A_f$ é um subconjunto dos $h \in K[x]$. Pensando em termos de resto da divisão por f, então podemos considerar A_f como consistindo por todos os polinômios h de grau $< n$, e sobre esta interpretação, $m_g[h]$ é o resto de gh na divisão por f. Assim temos o seguinte resultado.

Proposição 4.3.1. $Res(f,g) = f_n^m det(m_g : A_f \longrightarrow A_f)$.

Prova: Note que A_f é um espaço vetorial sobre K de dimensão n. Considere $m_g : (A_f \longrightarrow A_f)$ uma transformação linear. Na Álgebra Linear, dizemos que o $det(m_g)$ é definido como o determinante de uma matriz M que representa a transformaçao linear m_g. Desde que M e m_g têm os mesmos autovalores, segue que o $det(m_g)$ é o produto dos autovalores de m_g, incluindo as multiplicidades.

No caso especial quando $g(\alpha_1), \ldots, g(\alpha_n)$ são distintos, podemos provar o nosso resultado usando a teoria do capítulo 2. Sabendo que $\mathbf{V}(f) = \{\alpha_1, \ldots, \alpha_n\}$, segue do teorema (2.3.2) do capítulo 2, que os números $g(\alpha_1), \ldots, g(\alpha_n)$ são os autovalores de m_g. Desde que estes são distintos e A_f tem dimensão n segue que os autovalores têm multiplicidade 1, então $det(m_g) = g(\alpha_1) \ldots g(\alpha_n)$, como desejavamos.

4.3.2 Fórmula de Poisson em Várias Variáveis

A fórmula de Poisson pode ser generalizada pelo seguinte teorema. Sejam os polinômios homogêneos $F_0, \ldots, F_n \in \mathbb{C}[x_0, \ldots, x_n]$ de graus $d_0, \ldots d_n$. Considere a seguinte deshomogeneização:

$$f_i(x_0, \ldots, x_{n-1}) = F_i(x_0, \ldots, x_{n-1}, 1) \;\; \overline{F}_i(x_0, \ldots, x_{n-1}) = F_i(x_0, \ldots, x_{n-1}, 0) \quad (4.4)$$

Note que $\overline{F}_0, \ldots, \overline{F}_{n-1}$ são polinômios em $\mathbb{C}[x_0, \ldots, x_{n-1}]$ de graus $d_0, \ldots d_{n-1}$.

Teorema 4.3.1. (Fórmula de Poisson) *Se o* $Res(\overline{F}_0, \ldots, \overline{F}_{n-1}) \neq 0$, *então o anel quociente* $A = \mathbb{C}[x_0, \ldots, x_{n-1}]/ < f_0, \ldots, f_{n-1} >$ *tem dimensão* $d_0 \ldots d_{n-1}$ *como espaço vetorial sobre* $\mathbb{C}$, *e*

$$Res(F_0, \ldots, F_n) = Res(\overline{F}_0, \ldots, \overline{F}_{n-1})^{d_n} det(m_{f_n} : A \longrightarrow A),$$

Onde $m_{f_n} : A \longrightarrow A$ *é transformação linear dada pela multiplicação por* f_n.

Dem: Primeiramente vamos mostrar que o anel A tem dimensão finita sobre o espaço vetorial $\mathbb{C}$ quando o $Res(\overline{F}_0, \ldots, \overline{F}_{n-1}) \neq 0$. A idéia crucial é pensar em termos do espaço projetivo $\mathbb{P}^n(\mathbb{C})$. Podemos decompor $\mathbb{P}^n(\mathbb{C})$ em dois pedaços usando x_n: o espaço afim $\mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$ definido por $x_n = 1$, e o hiperplano das soluções no infinito $\mathbb{P}^{n-1}(\mathbb{C})$ definido por $x_n = 0$. Notemos que as variáveis $x_0, \ldots, x_{n-1}$ têm duas funções: elas são coordenadas de $\mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$, e elas são coordenadas homogêneas para o hiperplano das soluções no infinito.

As equações $F_0 = \ldots = F_{n-1} = 0$ determinam a variedade projetiva $\mathbf{V} \subset \mathbb{P}^n(\mathbb{C})$. Por (4.4) $f_0 = \ldots = f_{n-1} = 0$ definem a parte afim $\mathbb{C}^n \cap \mathbf{V} \subset \mathbf{V}$ e $\overline{F}_0 = \ldots = \overline{F}_{n-1} = 0$ definem o hiperplano no infinito $\mathbb{P}^{n-1}(\mathbb{C}) \cap \mathbf{V} \subset \mathbf{V}$. Assim por hipotese $Res(\overline{F}_0, \ldots, \overline{F}_{n-1}) \neq 0$ implica que não existem soluções no infinito, em outra palavras, a variedade projetiva $\mathbf{V}$ está contida em $\mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$. Usando um resultado da geometria algébrica:
Se a variedade projetiva em $\mathbb{P}^n(\mathbb{C})$ está contida em um espaço afim $\mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$, então a variedade projetiva deve consistir em um conjunto finito de pontos. Ver [19] (capítulo 1).

Aplicando para $\mathbf{V}$, isto nos diz que $\mathbf{V}$ deve ser um conjunto finito de pontos. Como $\mathbb{C}$ é algebricamente fechado e $\mathbf{V} \subset \mathbb{C}^n$ é definido por $f_0 = \ldots = f_{n-1} = 0$, o Teorema da Finitude do capítulo 2, implica que $A = \mathbb{C}[x_0, \ldots, x_{n-1}]/ < f_0, \ldots f_{n-1} >$ tem dimensão finita sobre $\mathbb{C}$. Assim $det(m_{f_n} : A \longrightarrow A)$ define esta transformação.

Considerando as equações $F_0 = \ldots = F_{n-1} = 0$ com graus $d_0, \ldots, d_{n-1}$, respectivamente e o número finito de soluções em $\mathbb{P}^n(\mathbb{C})$, então, pelo teorema de

Bezout, que nos fornece o número de soluções, a partir dos graus destas equações, logo número de soluções, incluindo multiplicidades é $d_0 \dots d_{n-1}$.
Isto nos diz que $\mathbf{V}$ tem $d_0 \dots d_{n-1}$ pontos, incluindo multiplicidades. Como $\mathbf{V} \subset \mathbb{C}^n$ é definido por $f_0 = \dots = f_{n-1} = 0$, pela proposição(2.3.3) do capítulo 2 implica que o número de pontos de $\mathbf{V}$, incluindo multiplicidades é a dimensão de A. Deste modo, o teorema de Bezout mostra que $dim(A) = d_0 \dots d_{n-1}$.

Agora vamos explicar porque o $Res(\overline{F}_0, \dots, \overline{F}_{n-1})^{d_n} det(m_{f_n})$ comporta-se como o resultante. O primeiro passo é mostrar que $det(m_{f_n})$ anula se e somente se $F_0 = \dots = F_n = 0$ tem uma solução em $\mathbb{P}^n(\mathbb{C})$. Se temos uma solução p, então $p \in \mathbf{V}$ deste modo $F_0(p) = \dots F_n(p) = 0$. Mas $\mathbf{V} \subset \mathbb{C}^n$ então podemos escrever $p = (a_0, \dots a_{n-1}, 1)$, e $f_n(a_0, \dots, a_{n-1}) = 0$ desde $F_n(p) = 0$. Então pelo teorema(2.3.2) do capítulo 2 nos diz que $f_n(a_0, \dots, a_{n-1}) = 0$ é um autovalor de m_{f_n}, que prova que o $det(m_{f_n}) = 0$. Se $det(m_{f_n}) = 0$, então um dos autovalores deve ser zero. Assim os autovalores são $f_n(p)$ para $p \in \mathbf{V}$, novamente pelo teorema (2.3.2) do capítulo 2 temos que $f_n(p) = 0$ para algum p. Escrevendo p da forma $(a_0, \dots, a_{n-1}, 1)$ obtemos uma solução não trivial de $F_0 = \dots F_n = 0$.

Finalmente mostraremos que $Res(\overline{F}_0, \dots, \overline{F}_{n-1})^{d_n} det(m_{f_n})$ tem a propriedade homogênea dada no capítulo 3 na secção(3.4). Substituindo F_j por um λF_j para algum $j < n$ e $\lambda \neq 0$ então $\overline{\lambda F}_j = \lambda \overline{F}_j$, e nem A e nem m_{f_n} são afetados. Assim

$$Res(\overline{F}_0, \dots, \lambda \overline{F}_j, \dots, \overline{F}_{n-1}) = \lambda^{d_0 \dots d_{j-1} d_{j+1} \dots d_{n-1}} Res(\overline{F}_0, \dots, \overline{F}_j, \dots, \overline{F}_{n-1})$$

obtemos a potência desejada de λ por causa do expoente d_n da fórmula do teorema. Por outro lado se substituirmos F_n por λF_n então o $Res(\overline{F}_0, \dots, \overline{F}_{n-1})$ e A são modificados, enquanto que m_{f_n} torna-se λm_{f_n}. Assim $det(\lambda m_{f_n}) = \lambda^{dim(A)} det(M_{f_n})$ isto segue o resultado, pois A tem dimensão $d_0 \dots d_{n-1}$. □

Exemplo 4.3.2. *Sejam* $f(x) = x^3 + x - 1$ *e* $g(x) = 2x^2 + 3x + 7$. *Queremos calcular o* $Res(f, g)$ *usando a fórmula de Poisson. Usando a definição (3.1.2), temos que o resultante é dado por:*

$$Res(f,g) = det \begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 1 & 0 & 7 & 3 & 2 \\ -1 & 1 & 0 & 7 & 3 \\ 0 & -1 & 0 & 0 & 7 \end{bmatrix} = 159.$$

Então temos que obter o mesmo resultado por Poisson. Pela fórmula de Poisson, temos que $Res(f, g) = f_n^m det(m_g : A_f \longrightarrow A_f)$. *Assim o resultante é* $Res(f, g) = (1)^2 det(m_g : A_f \longrightarrow A_f)$. *Sabendo que* $A_f = \mathbb{C}[x]/ < f >= \{c_0 + c_1 x + c_2 x^2 : c_i \in \mathbb{C}\}$ *para determinar o* $det(m_{f_n} : A_f \longrightarrow A_f)$ *basta tomar o resto da divisão de* $(c_0 + c_1 x + c_2 x^2) \times (2x^2 + 3x + 7)$ *por* $x^3 + x - 1$.

Fazendo as contas temos que o resto da divisão é dado por

$$7c_0 + 2c_1 + 3c_2 + (3c_0 + 5c_1 - c_2)x + (2c_0 + 3c_1 + 5c_2)x^2.$$

Assim a transformação que associa

$$(c_0, c_1, c_2) \longrightarrow (7c_0 + 2c_1 + 3c_2, 3c_0 + 5c_1 - c_2, 2c_0 + 3c_1 + 5c_2)$$

é dada pelo

$$det \begin{bmatrix} 7 & 2 & 3 \\ 3 & 5 & -1 \\ 2 & 3 & 5 \end{bmatrix} = 159.$$

Então $Res(f, g) = (1)^2 det(m_g : A_f \longrightarrow A_f) = 159$.

5 APLICAÇÕES

O objetivo deste capítulo é fazer aplicações da teoria de resultantes. Primeiramente vamos resolver sistemas de equações polinomiais usando a teoria de resultantes, em seguida demonstraremos o *Teorema de Bezout* para um caso particular. A prova geral deste teorema pode ser encontrada em [19].

5.1 Sistemas de duas variáveis

Como uma primeira aplicação simples de resultantes, vamos demonstrar como um sistema de duas equações com duas variáveis pode ser resolvido, ou pelo menos reduzido a uma variável. Para esta secção indicamos o livro [5].

Considere $f(x,y) = g(x,y) = 0$, com $f, g \in K[x,y]$. Podemos ocultar a variável y como coeficientes e pensar em $f, g \in K[y][x]$. Denotando n, m os respectivos graus de f, g na variável x. Então, o resultante $Res_{n,m}(f,g)$ na variável x, denotado por $Res(f,g)_x$ vai ser um polinômio em y, que se anulará em todo y_0 se existir um x_0 tal que $f(x_0,y_0) = g(x_0,y_0) = 0$.

Exemplo 5.1.1. *Considere* $f(x,y) = x^2 + y^2 - 10$, $g(x,y) = x^2 + 2y^2 + xy - 16$. *Reescrevemos* $f(x,y) = x^2 + 0x + (y^2 - 10)$, $g(x,y) = x^2 + yx + (2y^2 - 16)$. *Então o resultante de* f, g *é igual*

$$Res_{2,2}(f,g)_x = det \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & y & 1 \\ y^2 - 10 & 0 & 2y^2 - 16 & y \\ 0 & y^2 - 10 & 0 & 2y^2 - 16 \end{bmatrix}$$

$$Res_{2,2}(f,g)_x = -22y^2 + 2y^4 + 36 = 2(y+3)(y-3)(y^2-2).$$

Este polinômio em y, *tem exatamente quatro raízes* $y_0 = -3, 3, \sqrt{2}, -\sqrt{2}$.

Retomamos o sistema inicial:

$$f(x,y) = x^2 + y^2 - 10 = 0$$

$$g(x,y) = x^2 + 2y^2 + xy - 16 = 0$$

e fazendo $f(x,y) - g(x,y) = 0$, *obtemos:*
$y^2 - 10 - 2y^2 - xy + 16 = 0 \longrightarrow -y^2 - xy + 6 = 0 \longrightarrow x = \dfrac{6 - y^2}{y}$. *Então substituindo as raízes* $y_0 = -3, 3, \sqrt{2}, -\sqrt{2}$, *temos* $x_0 = 1, -1, 2\sqrt{2}, -2\sqrt{2}$.

Note que $f(x, y_0) = 0$ também será satisfeito devido ao resultante se anular. Então existe precisamente uma solução x_0 para cada y_0. Assim temos o seguinte resultado.

Teorema 5.1.1. *Sejam* $f(x,y) = \sum_{i=1}^{n} f_i(y)x^i$, $g(x,y) = \sum_{i=1}^{m} g_i(y)x^i$ *polinômios em* $K[x,y]$, *tal que* $f_i, g_i \in K[y]$, *com* f_n *e* g_m *não nulos. Seja* y_0 *uma raiz do resultante* $Res(f,g)_x \in K[y]$. *Se ocorrer de* $f_n(y_0) \neq 0$ *ou* $g_m(y_0) \neq 0$, *existe um* $x_0 \in K$ *de modo que* $f(x_0, y_0) = g(x_0, y_0) = 0$.

Dem: Observe que os polinômios f e g, são vistos como polinômios na variável x. Como o $Res(f,g)_x$ é um polinômio em y e existe um y_0 tal que

$$Res(f,g)_x(y_0) = 0.$$

Então substituindo y_0 em f e g, e como $f_n(y_0) \neq 0$ ou $g_m(y_0) \neq 0$, segue pelo teorema (3.1.1) que f e g têm um fator não constante em comum. Que implica na existência de um x_0 de modo que $f(x_0, y_0) = g(x_0, y_0) = 0$. □

5.2 Resolvendo Equações via Resultantes

A idéia básica é utilizar o $u - Resultante$, teoria desenvolvida por *van der Waerden*.

Sejam $F_1, \ldots, F_n$ polinômios homogêneos de graus $d_1, \ldots, d_n$, respectivamente, nas variáveis $x_0, \ldots, x_n$. Queremos encontrar uma solução não trivial para o sistema de equações

$$F_1 = \ldots = F_n = 0 \tag{5.1}$$

Considerando o sistema (5.1), vamos adicionar a este sistema outra equação polinômial homogênea $F_0 = 0$, assim obtemos $n+1$ equações homogêneas em $n+1$ variáveis, onde

$$F_0 = u_0x_0 + \ldots + u_nx_n \tag{5.2}$$

tais que, $u_0, \ldots, u_n$ são variáveis independentes. Assim podemos calcular o resultante $Res_{1,d_1,\ldots,d_n}(F_0, F_1, \ldots, F_n)$ que é chamado de $u - Resultante$. Antes da teoria geral de $u - Resultante$ vamos fazer um exemplo.

Exemplo 5.2.1. *Sejam*

$$F_1 = x_1^2 + x_2^2 - 10x_0^2 = 0$$

$$F_2 = x_1^2 + x_1x_2 + 2x_2^2 - 16x_0^2 = 0$$

Este sistema é a interseção de um círculo e uma elipse em $\mathbb{P}^2(\mathbb{C})$. *Sabemos, pelo teorema de Bezout, que será demonstrado na próxima secção, que existem 4 soluções. Para encontrarmos vamos adicionar a equação*

$$F_0 = u_0x_0 + u_1x_1 + u_2x_2 = 0$$

Assim calculando o $Res_{1,2,2}(F_0, F_1, F_2) = (2u_0^4 + 16u_1^4 + 36u_2^4 - 80u_1^3u_2 + 120u_1u_2^3 - 18u_0^2u_1^2 - 22u_0^2u_2^2 + 52u_1^2u_2^2 - 4u_0^2u_1u_2)$. *Fatorando este polinômio, usando o Maple podemos reescrever o resultante como:* $Res_{1,2,2}(F_0, F_1, F_2) = (u_0+u_1-3u_2)(u_0-u_1+3u_2)(u_0^2-8u_1^2-2u_2^2-8u_1u_2) = (u_0+u_1-3u_2)(u_0-u_1+3u_2)(u_0+2\sqrt{2}u_1+\sqrt{2}u_2)(u_0-2\sqrt{2}u_1-\sqrt{2}u_2)$. *Os coeficientes dos fatores lineares do* $Res_{1,2,2}(F_0, F_1, F_2)$ *são dados por 4 pontos:* $(1,1,-3)(1,-1,3)(1,2\sqrt{2},\sqrt{2})(1,-2\sqrt{2},-\sqrt{2})$ *em* $\mathbb{P}^2(\mathbb{C})$. *Estes*

4 pontos são as soluções de $F_1 = F_2 = 0$. *Note que há mais soluções em* $\mathbb{C}^3$, *pelo fato de que estamos determinando todas as soluções no espaço afim* $\mathbb{C}^2 \subset \mathbb{P}^2(\mathbb{C})$, *definidas por* $x_0 = 1$. *Assim poderiamos definir* $x_0 = 2$ *e as soluções determinadas por este espaço também serão soluções, pois são coordenadas homogênenas da soluções definidas por* $x_0 = 1$.

Agora vamos generalizar a idéia de $u - Resultante$. Assim como podemos homogeneizar as equações polinomiais, também podemos deshomogeneizar pela substituição de $x_0 = 1$. Assim definimos:

$$f_i(x_1, \ldots, x_n) = F_i(1, x_1, \ldots, x_n) \quad \overline{F}_i(x_1, \ldots, x_n) = F_i(0, x_1, \ldots, x_n) \tag{5.3}$$

Note que cada f_i tem grau no máximo d_i, com $0 \leq i \leq n$. Dentro de $\mathbb{P}^n(\mathbb{C})$ temos o espaço afim $\mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$ definido por $x_0 = 1$, e as soluções do sistema de equações

$$f_1 = \ldots = f_n = 0 \tag{5.4}$$

são precisamente as soluções de (5.1) que pertencem a $\mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$. Similarmente, uma solução não trivial das equações homogêneas

$$\overline{F}_1 = \ldots = \overline{F}_n = 0$$

pode ser considerada como solução que pertence ao ∞ . Nós dizemos que (5.3) não tem solução no ∞, se $\overline{F}_1 = \ldots = \overline{F}_n = 0$ não tem solução não trivial. Pelo teorema(3.3.1) do capítulo 3 é equivalente afirmar que o $Res(\overline{F}_1, \ldots, \overline{F}_n) \neq 0$.

Proposição 5.2.1. *Sejam* $f_1 = \ldots = f_n = 0$ *definidas em (5.3) de graus total no máximo* $d_1, \ldots, d_n$, *sem soluções no* ∞, *e todas soluções de multiplicidade 1. Se* $f_0 = u_0 + u_1x_1 + \ldots + u_nx_n$, *é a deshomogeneização de (5.2)*$(x_0 = 1)$, *tais que,* $u_0, \ldots, u_n$ *são variáveis independentes, então existe uma constante não nula C tal que*

$$Res_{1,d_1,\ldots,d_n}(f_0, f_1, \ldots, f_n) = C \prod_{p \in V(f_1,\ldots,f_n)} f_0(p).$$

Dem: O teorema é uma adaptação da fórmula de Poisson.
Seja $C = Res_{d_1,\ldots,d_n}(\overline{F}_1,\ldots,\overline{F}_n)$, que não é nulo por hipótese. Como os coeficientes de f_0 são as variáveis $u_0,\ldots,u_n$, precisamos trabalhar sobre o corpo $K = \mathbb{C}[u_0,\ldots,u_n]$ de funções racionais em $u_0,\ldots,u_n$. Consequentemente, nesta prova, trabalharemos sobre K mais propriamente do que sobre $\mathbb{C}$.

Adaptando a fórmula de Poisson para a situação de (5.3) produz

$$Res_{1,d_1,\ldots,d_n}(f_0,f_1,\ldots,f_n) = Cdet(m_{f_0}),$$

onde $m_{f_0} : A \longrightarrow A$ é uma transformação linear dada pela multiplicação por f_0 sobre o anel quociente $A = K[x_1,\ldots,x_n]/ < f_1,\ldots,f_n >$. Pelo teorema de Bezout, A é um espaço vetorial sobre K de dimensão $d_1 \ldots d_n$ e pelo teorema (2.3.2) do capítulo 2 implica que os autovalores de m_{f_0} são os valores de $f_0(p)$ para $p \in \mathbf{V}(f_1,\ldots,f_n)$. Como todas multiplicidades são 1, existem $d_1 \ldots d_n$ pontos p, correspondendo a $f_0(p)$ pontos distintos já que $f_0 = u_0 + u_1x_1 + \ldots + u_nx_n$ e $u_0,\ldots,u_n$ são variáveis independentes. Deste modo m_{f_0} tem $d_1 \ldots d_n$ autovalores distintos $f_0(p)$, então isto

$$det(m_{f_0}) = \prod_{p \in V(f_1,\ldots,f_n)} f_0(p).$$

□

Para ver mais claramente o que a proposição quer dizer, sejam os pontos de $\mathbf{V}(f_1,\ldots,f_n)$ denotados por p_i para $1 \leq i \leq d_1 \ldots d_n$. Se escrevermos cada ponto como $p_i = (a_{i1},\ldots,a_{in}) \in \mathbb{C}^n$, então $f_0 = u_0 + u_1x_1 + \ldots + u_nx_n$ implica

$$f_0(p_i) = u_0 + a_{i1}u_1 + \ldots + a_{in}u_n,$$

assim pela proposição (5.2.1), o $u - Resultante$ é dado por

$$Res_{1,d_1,\ldots,d_n}(f_0,\ldots,f_n) = C \prod_{i=1}^{d_1\ldots d_n} (u_0 + a_{i1}u_1 + \ldots + a_{in}u_n) \tag{5.5}$$

Vemos claramente que o $u - Resultante$ é um polinômio em $u_0,\ldots,u_n$. Além disso, obtemos o seguinte método para encontrar as soluções de (5.4): calcular $Res_{1,d_1,\ldots,d_n}(f_0,\ldots,f_n)$, fatore em fatores lineares, então lêia as soluções.

Assim temos que o $u - Resultante$, que resolve (5.4), é reduzido para o problema de fatoração de várias variáveis.

Para calcular o $u - Resultante$, usamos a fórmula de Macaulay ou Poisson do capítulo 4.

Exemplo 5.2.2. *Agora considere o seguite sistema:*

$$f_1 = x_0^2 + x_1^2 - 2 = 0$$

$$f_2 = x_0^2 + 6x_1^2 - 3 = 0$$

Vamos determinar os pontos comuns do círculo e da elipse usando de u- Resultante. Assim transformando as equações para forma homogênea a adicionando a equação $F_0 = u_0x_0 + u_1x_1 + u_2x_2 = 0$, *temos o seguinte sistema*

$$F_0 = u_0x_0 + u_1x_1 + u_2x_2 = 0$$

$$F_1 = x_0^2 + x_1^2 - 2x_2^2 = 0$$

$$F_2 = x_0^2 + 6x_1^2 - 3x_2^2 = 0$$

Usando o algoritmo de Macaulay

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & -2 \\ 1 & 0 & 0 & 6 & 0 & -3 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 6 & 0 & -3 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 6 & 0 & -3 \\ 0 & u_o & 0 & u_1 & u_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_0 & 0 & u_1 & u_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & u_0 & 0 & 0 & u_1 & u_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & u_0 & 0 & 0 & u_1 & u_2 \end{bmatrix}$$

e N a submatriz de M é:

$$N = \begin{bmatrix} 1 & 1 \\ 1 & 6 \end{bmatrix}$$

Logo o

$$Res_{1,2,2}(F_0, F_1, F_2) = 81u_0^4 - 18u_0^2u_1^2 - 90u_0^2u_2^2 - 10u_2^2u_1^2 + 25u_2^4 + u_1^4.$$

Fatorando este polinômio usando o Maple podemos reescrever como:

$$Res_{1,2,2}(F_0, F_1, F_2) = (3u_0+u_1+\sqrt{5}u_2)(-u_1+\sqrt{5}u_2+3u_0)(3u_0+u_1+\sqrt{5}u_2)(-u_1+\sqrt{5}u_2-3u_0)$$

Assim obtemos as coordenadas dos pontos de intersecção

$$(\frac{3}{\sqrt{5}}, \frac{1}{\sqrt{5}}), (\frac{3}{\sqrt{5}}, \frac{-1}{\sqrt{5}}), (\frac{-3}{\sqrt{5}}, \frac{1}{\sqrt{5}}), (\frac{-3}{\sqrt{5}}, \frac{-1}{\sqrt{5}})$$

5.3 O Teorema de Bezout

O Teorema de Bezout foi citado em quase todo o desenvolvimento da teoria de resultantes. Vimos que este teorema fornece uma cota superior para o número de soluções de um sistema de equações polinomiais, através do produto dos graus destes polinômios. Deste modo, nessa última secção, iremos explorar o que acontece quando duas curvas se interceptam no plano. Estamos particularmnete interessados no número de pontos da intersecção. E como uma aplicação, demonstraremos o Teorema de Bezout, usando a teoria de resultantes.

Considere o seguinte exemplo, que ilustra porque a questão é especialmente bonita quando trabalhamos com curvas no espaço projetivo sobre os números complexos $\mathbb{P}^2(\mathbb{C})$.

Exemplo 5.3.1. *Primeiramente considere a intersecção de uma parábola com uma elipse. Sejam* $y = x^2$ *e* $x^2 + 4(y - \lambda)^2 = 4$, *onde* λ *é um parâmetro que podemos variar. Quando* $\lambda = 0$ *e* 2, *obtemos as seguintes figuras:*

Figura 5.1: $\lambda = 0$ *e* $\lambda = 2$

Sobre os $\mathbb{R}$, *obtemos números diferentes na intersecção. Isto fica claro, se observarmos as figuras, o parâmetro* λ *determina o deslocamento da elipse no eixo y. Assim tomando* $\lambda \leq -2$, *implica que as curvas têm intersecção vazia. Isto justifica que existem valores de* λ *para os quais as curvas não têm ponto em comum.*

O que é mais interessante é trabalhar sobre $\mathbb{C}$, *no qual obtemos 4 pontos na intersecção, ou seja* $4 =$ *grau(parábola)*$\times$ *grau(elipse), em ambos os casos de* $\lambda = 2$ *ou* $\lambda = 0$.

Para $\lambda = 0$, *podemos eliminar* x *de* $y = x^2$ *e* $x^2 + 4y^2 = 4$ *para obter* $y + 4y^2 = 4$, *cujas raízes são:*

$$y = \frac{-1 \pm \sqrt{65}}{8}.$$

E os correspondentes valores de x *são:*

$$x = \pm\sqrt{\frac{-1 \pm \sqrt{65}}{8}}.$$

O que nos fornece 4 pontos da intersecção, 2 reais e 2 complexos. Para o caso $\lambda = 2$, *sobre o* $\mathbb{C}$ *obtemos o mesmo número de pontos na intersecção.*

Exemplo 5.3.2. *Seja* $\mathbb{P}^2(\mathbb{C})$, *e considere as duas curvas* $C = \mathbf{V}(x^2 - z^2)$ *e* $D = \mathbf{V}(x^2y - xz^2 - xyz + z^3)$. *É fácil checar que* $(1, b, 1) \in C \cap D$ *para qualquer* $b \in \mathbb{C}$, *então esta intersecção* $C \cap D$ *é infinita. Para ver como isto acontece, considere a fatoração de:*

$$x^2 - z^2 = (x - z)(x + z), \quad x^2y - xz^2 - xyz + z^3 = (x - z)(xy - z^2).$$

Assim C é a união de duas retas projetivas e D é a união de uma reta e uma cônica. Agora vemos onde o problema ocorre: C e D têm uma componente irredutível em comum $(x - z)$, então naturalmente sua intersecção é infinita.

Estes exemplos explicam porque queremos trabalhar em $\mathbb{P}^2(\mathbb{C})$. Agora considere o seguinte resultado sobre a irredutibilidade de polinômios.

Proposição 5.3.1. *Seja $f \in \mathbb{C}[x, y, z]$ um polinômio homogêneo não nulo. Então os fatores irredutíveis de f são também homogêneos, e se fatorarmos f em irredutíveis*

$$f = f_1^{a_1} \dots f_s^{a_s},$$

onde f_i não é uma constante múltipla de f_j para $i \neq j$, então

$$\mathbf{V}(f) = \mathbf{V}(f_1) \cup \dots \cup \mathbf{V}(f_s)$$

é a menor decomposição de $\mathbf{V}(f)$ em componentes irredutíveis em $\mathbb{P}^2(\mathbb{C})$. Além disso,

$$\mathbf{I}(\mathbf{V}(f)) = \sqrt{< f >} =< f_1 \dots f_s > .$$

Prova: A prova deste resultado pode ser vista no capítulo 2.

Uma consequência desta proposição é de que toda curva $C \subset \mathbb{P}^2(\mathbb{C})$ tem uma equação polinomial definida. Se $C = \mathbf{V}(f)$ para algum polinômio homogêneo, então a proposição implica que $\mathbf{I}(C) =< f_1 \dots f_s >$, onde $f_1, \dots, f_s$ são os fatores irredutíveis distintos de f. Deste modo, qualquer outro polinômio que define C é múltiplo de $f_1 \dots f_s$, então $f_1 \dots f_s = 0$, define a equação de grau mínimo. Esta equação chamamos de equação reduzida de C.

Assim se considerarmos a intersecção de duas curvas C e D em $\mathbb{P}^2(\mathbb{C})$, e assumirmos que C e D não têm componentes irredutíveis em comum, então os polinômios que definem estas curvas não têm fatores em comum.

Nosso objetivo é relacionar o número de pontos de $C \cap D$ com os graus das equações que definem estas curvas. Para isto considere os seguintes lemas.

Lema 5.3.1. *Sejam $F, G \in \mathbb{C}[x, y, z]$ polinômios homogêneos de graus total respectivamente m, n. Se $F(0, 0, 1)$ e $G(0, 0, 1)$ são não nulos, então o resultante $Res(F, G)$ na variável z é homogêneo em x e y de grau total mn.*

Dem: Primeiramente, vamos representar o $Res(f, g)$ na variável z por $Res(f, g)_z$. Agora escrevemos F e G como polinômios em z :

$$F = a_0 z^m + \ldots + a_m$$

$$G = b_0 z^n + \ldots + b_n$$

Observe que F é homogêneo de grau total m, e que cada $a_i \in \mathbb{C}[x, y]$ deve ser homogêneo de grau i. Além disso, $F(0, 0, 1) \neq 0$ implica que a_0 é uma constante não nula. De forma análoga, b_i é homogêneo de grau i, e $b_0 \neq 0$.

Assim pela secção 1 do capítulo 3, podemos considerar o $Res(F, G)_z$, como o determinante da matriz $(m + n) \times (m + n)$:

$$Res(F,G) = det \begin{pmatrix}
a_0 & & & & b_0 & & & & & \\
a_1 & a_0 & & & b_1 & b_0 & & & & \\
\vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & & & \\
\vdots & \vdots & & a_0 & b_{n-1} & \vdots & & \ddots & & \\
\vdots & \vdots & & a_1 & b_n & \vdots & & & \ddots & \\
\vdots & \vdots & & \vdots & & b_n & & & & b_0 \\
a_m & \vdots & & \vdots & & & \ddots & & & \vdots \\
 & a_m & & \vdots & & & & \ddots & & \vdots \\
 & & \ddots & \vdots & & & & & \ddots & \vdots \\
 & & & a_m & & & & & & b_n
\end{pmatrix}$$

Para mostrar que o $Res(F, G)_z$ é homogêneo de grau mn, seja c_{ij} a $ij-$ésima entrada da matriz. Do padrão acima, podemos ver que as entradas não nulas são: $c_{ij} = \begin{cases} a_{i-j} & se\ \ j \leq n \\ b_{n+i-j} & se\ \ j > n. \end{cases}$

Assim, os c_{ij} não nulos são homogêneos de grau total $i-j$ (se $j \leq n$) ou $n+i-j$ (se $j > n$). Como o resultante é dado pelo determinante, podemos escrever o $Res(F,G)_z$ como um somátorio de um produto:

$$\pm \prod_{i=1}^{m+n} c_{i\sigma(i)}$$

onde σ é uma permutação de $\{1,\ldots,m+n\}$. Podemos assumir que cada $c_{i\sigma(i)}$ é não nulo. Se escrevermos o produto como

$$\pm \prod_{\sigma(i)\leq n} c_{i\sigma(i)} \quad \prod_{\sigma(i)>n} c_{i\sigma(i)}$$

então, este produto é um polinômio homogêneo de grau

$$\prod_{\sigma(i)\leq n} (i-\sigma(i)) + \quad \prod_{\sigma(i)>n} (n+i-\sigma(i)).$$

Assim σ é uma permutação de $\{1,\ldots,m+n\}$, o primeiro somátorio tem n termos e o segundo tem m, e todo o i entre 1 e $m+n$ aparecem precisamente uma vez. Assim podemos reorganizar o somátorio para obter

$$mn + \prod_{i=1}^{m+n} i - \quad \prod_{i=1}^{m+n} \sigma(i) = mn,$$

que prova que o $Res(F,G)_z$ é um somátorio de um polinômio homogêneo de grau mn. □

Lema 5.3.2. *Seja $h \in \mathbb{C}[x,y]$ um polinômio homogêneo não nulo. Então h pode ser escrito da forma*

$$h = c(s_1x - r_1y)^{m_1} \ldots (s_tx - r_ty)^{m_t},$$

onde $c \neq 0$ em $\mathbb{C}$ e $(r_1,s_1),\ldots,(r_t,s_t)$ são pontos distintos em $\mathbb{P}^1(\mathbb{C})$. Além disso,

$$\mathbf{V}(h) = \{(r_1,s_1),\ldots,(r_t,s_t)\} \subset \mathbb{P}^1(\mathbb{C}).$$

Prova: Este lema segue como consequência da proposição (5.3.1).

Proposição 5.3.2. *Dados $f, g \in \mathbb{C}[x, y, z]$. Escrevendo f e g como polinômios na variável x temos*

$$f = a_0 x^l + \ldots + a_l$$

$$g = b_0 x^m + \ldots + b_m,$$

onde $a_0, b_0 \in \mathbb{C}[y, z]$. Se o $Res(f, g)_x \in \mathbb{C}[y, z]$ se anula em $(c_2, c_3) \in \mathbb{C}^2$ então ocorre um dos seguintes itens:
i) a_0 ou b_0 se anulam em (c_2, c_3) ou
ii) existe um $c_1 \in \mathbb{C}$ de modo que f e g se anulam em $(c_1, c_2, c_3) \in \mathbb{C}^3$.

Prova: Sejam $c = (c_2, c_3)$, $f(x, c) = (x, c_2, c_3)$ e $g(x, c) = (x, c_2, c_3)$. Isto é suficiente para mostrar que $f(x, c)$ e $g(x, c)$ têm um fator comum quando $a_0(c)$ e $b_0(c)$ são não nulos. Para provar isto, escrevemos

$$f(x, c) = a_0(c)x^l + \ldots + a_l(c)$$

$$g(x, c) = b_0(c)x^m + \ldots + b_m(c).$$

Por hipótese, $h = Res(f, g)_x$ se anula em c. Assim se calcularmos o determinante dado por h no ponto c, obtemos

$$0 = h(c) = det \begin{pmatrix} a_0(c) & & & b_0(c) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_0 c & \vdots & & b_0(c) \\ a_l(c) & & \vdots & b_m(c) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l(c) & & & b_m(c) \end{pmatrix}$$ assim o resultante de $f(x, c)$ e $g(x, c)$ é exatamente o determinante acima, logo segue que

$$0 = h(c) = Res(f(x, c), g(x, c))_x.$$

Então pelo teorema (3.1.1) do capítulo 3 implica que $f(x, c)$ e $g(x, c)$ tem uma raiz em comum.

A partir destes resultados, mostraremos como limitar o número de pontos da intersecção de duas curvas usando os graus de suas equações reduzidas.

Teorema 5.3.1. *Sejam C e D curvas projetivas em $\mathbb{P}^2(\mathbb{C})$ sem componentes irredutíveis em comum. Se os graus das equações reduzidas C e D são m e n respectivamente, então $C \cap D$ é finita e tem no máximo mn pontos.*

Dem: Suponha que $C \cap D$ tem mais do que mn pontos. Escolhendo $mn+1$ pontos, que representaremos por $p_1, \ldots, p_{mn+1}$, e para $1 \leq i < j \leq mn+1$, sejam L_{ij} as retas que ligam os pontos p_i e p_j. Considere um ponto $q \in \mathbb{P}^2(\mathbb{C})$ de modo que

$$q \notin C \cup D \cup \bigcup_{i<j} L_{ij}. \tag{5.6}$$

Este ponto existe pelo fato de que se considerarmos um polinômio não nulo $f \in \mathbb{C}[x,y,z]$, o conjunto $\mathbb{C}^2 - \mathbf{V}(f)$ é não vazio. Agora considere uma função $A : \mathbb{P}^2(\mathbb{C}) \longrightarrow \mathbb{P}^2(\mathbb{C})$, de modo que $A(q) = (0,0,1)$. Se considerarmos A em novas coordenadas para $\mathbb{P}^2(\mathbb{C})$, então o ponto q tem coordenas $(0,0,1)$ neste novo sistema. Então podemos assumir que $q = (0,0,1)$ em (5.6).

Agora suponhamos que $C = \mathbf{V}(f)$ e $D = \mathbf{V}(g)$, onde f e g são as equações reduzidas de graus m e n respectivamente. Então (5.6) implica que $f(0,0,1) \neq 0$ já que $(0,0,1) \notin C$, e $g(0,0,1) \neq 0$ já que $(0,0,1) \notin D$. Deste modo pelo lema (5.3.1), o resultante de $Res(f,g)_z$ é um polinômio homogêneo de grau mn em x, y. Como f e g têm grau positivo em z e não têm fatores em comum em $\mathbb{C}[x,y,z]$, pelo teorema (3.1.1) do capítulo 3, o $Res(f,g)_z$ é um polinômio não nulo.

Sejam $p_i = (u_i, v_i, w_i)$, então já que o resultante é um ideal gerado por f e g, temos

$$Res(f,g)_z(u_i, v_i) = 0. \tag{5.7}$$

Note que a reta que une o ponto $q = (0,0,1)$ com $p_i = (u_i, v_i, w_i)$ intersecta $z = 0$ nos pontos $(u_i, v_i, 0)$. Por esta razão, (5.7) nos diz que o $Res(f,g)_z$ se anula para os pontos obtidos pela projeção dos $p_i \in C \cap D$ de $(0,0,1)$ na reta $z = 0$.
Por (5.6), $(0,0,1)$ pertence a uma das retas que liga p_i e p_j, que implica que os pontos $(u_i, v_i, 0)$ são distintos para $i = 1, \ldots, mn+1$. Se considerarmos $z = 0$ como uma cópia de $\mathbb{P}^1(\mathbb{C})$ com coordenadas homogêneas x, y, então obtemos distintos

pontos $(u_i, v_i) \in \mathbb{P}^1(\mathbb{C})$, e o polinômio homogêneo $Res(f, g)_z$ se anula para todos $mn + 1$ deles. Pelo lema (5.3.2), isto é impossível pois o $Res(f, g)_z$ é não nulo de grau mn. □

Note que $C \cap D \neq \emptyset$. Pelo fato de que C e D são curvas no espaço projetivo $\mathbb{P}^2(\mathbb{C})$, logo sempre possuem um ponto em comum.

Agora que temos um critério para $C \cap D$ ser finito, o próximo passo é definir a multiplicidade de um ponto $p \in C \cap D$. Antes de definir a multiplicidade de um ponto de uma intersecção, retornamos ao exemplo (5.3.1), que considera a intersecção de uma parábola $y = x^2$ com uma elipse $x^2 + 4(y - \lambda)^2 = 4$.

Tomando $\lambda = 1$, observe a figura abaixo

Figura 5.2: $\lambda = 1$

Vemos facilmente que existe somente 3 pontos na intersecção. Isto é verdadeiro, mesmo que trabalhando sobre $\mathbb{C}$. Mas isso não contraria o Teorema de Bezout? Na verdade não. Pois o ponto da origem (0, 0), que pertence a intersecção da parábola com a elipse, tem multiplicidade 2. E os outros 2 pontos da intersecção têm cada um multiplicidade 1. Assim se adicionarmos as multiplicidades dos pontos obtemos que o número total na intersecção é 4, que está de acordo com o Teorema de Bezout.

A importância deste exemplo, implica na seguinte definição.

Definição 5.3.1. *Sejam C e D curvas em $\mathbb{P}^2(\mathbb{C})$ sem componentes em comum e suas equações reduzidas $f = 0$ e $g = 0$. Escolhendo coordenadas para $\mathbb{P}^2(\mathbb{C})$, de modo que satisfaça*

$$(0,0,1) \notin C \cup D \cup \bigcup_{p \neq q \in C \cap D} L_{pq}. \tag{5.8}$$

Então, dado $p = (u, v, w) \in C \cap D$, a multiplicidade $I_p(C, D)$ é definida como o expoente de $vx - uy$ da fatoração do $Res(f, g)_z$.

Exemplo 5.3.3. *Considere os seguintes polinômios em $\mathbb{C}[x, y, z]$:*

$$f = x^3 + y^3 - 2xyz,$$

$$g = 2x^3 - 4x^2y + 3xy^2 + y^3 - 2y^2z.$$

Estes polinômios definem curvas cúbicas $C = \mathbf{V}(f)$ e $D = \mathbf{V}(g)$ em $\mathbb{P}^2(\mathbb{C})$. Para analizar a intersecção destas curvas, primeiramente vamos calcular o resultante na variável z :

$$Res(f, g)_z = -2y(x - y)^3(2x + y).$$

Assim para determinarmos os pontos de $C \cap D$, basta fazer $Res(f, g)_z = 0$, isto é equivalente $y = 0$, $x - y = 0$ ou $2x + y = 0$. Deste modo $C \cap D$ consiste em 3 pontos:

$$p = (0,0,1), \quad q = (1,1,1), \quad r = (4/7, -8/7, 1).$$

Isto mostra em particular que C e D não têm componentes em comum.

Como $(0,0,1) \in C$, pois é um ponto de intersecção, isto contraria (5.8). Então devemos fazer uma mudança de coordenadas. Para isso considere:

$$(0,1,0) \notin C \cup D \cup L_{pq} \cup L_{pr} \cup L_{qr}.$$

Agora devemos encontrar uma transformação A, de modo que a mudança de coordenadas satisfaça $A(0,1,0) = (0,0,1)$. Isto não é difícil de fazer, seja $A(x, y, z) = (z, x, y)$. Então

$$(0,1,0) \notin A(C) \cup A(D) \cup L_{A(p)A(q)} \cup L_{A(p)A(r)} \cup L_{A(q)A(r)}.$$

Para encontrar a equação que define $A(C)$, note que $(u,v,w) \in A(C) \Leftrightarrow A^{-1}(u,v,w) \in C \Leftrightarrow f(A^{-1}(u,v,w)) = 0$. Deste modo, $A(C)$ é definida pela equação $f \circ A^{-1}(x,y,z) = f(y,z,x) = 0$, e de forma análoga, $A(D) = g(y,z,x) = 0$. Então pela definição (5.3.1), o resultante $Res(f(y,z,x), g(y,z,x))$ determina as multiplicidades para $A(p) = (1,0,0), A(q) = (1,1,1)$ e $A(r) = (1, 4/7, -8/7)$. O resultante é

$$Res(f(y,z,x), g(y,z,x))_z = 8y^5(x-y)^3(4x-7y),$$

então as multiplicidades dos pontos p, q, e r são

$$I_p(C,D) = 5, \quad I_q(C,D) = 3, \quad I_r(C,D) = 1.$$

Agora, finalmente podemos provar o Teorema de Bezout.

Teorema 5.3.2. (Teorema de Bezout) *Sejam C e D curvas em $\mathbb{P}^2(\mathbb{C})$ sem componentes em comum, e sejam m e n os graus de suas equações reduzidas, respectivamente. Então*

$$\sum_{p \in C \cap D} I_p(C,D) = mn,$$

onde $I_p(C,D)$ é a multiplicidade do ponto $p \in C \cap D$.

Dem: Sejam $f = 0$ e $g = 0$ as equações reduzidas de C e D, e assumimos que as coordenadas foram sido escolhidas, de modo que satisfaça

$$(0,0,1) \notin C \cup D \cup \bigcup_{p \neq q \in C \cap D} L_{pq}.$$

Escrevendo $p \in C \cap D$ como $p = (u_p, v_p, w_p)$. Então afirmamos que

$$Res(f,g)_z = c \sum_{p \in C \cap D} (v_p x - u_p y)^{I_p(C,D)} \tag{5.9}$$

onde c é uma constante não nula. Para cada p, está claro que $(v_p x - u_p y)^{I_p(C,D)}$ é a potência exata de $v_p x - u_p y$ que divide o resultante, isto segue da definição de $I_p(C,D)$. Precisamos verificar se isto ocorre para todas as raízes do resultante. Mas se $(u,v) \in \mathbb{P}^1(\mathbb{C})$ satisfaz $Res(f,g)_z(u,v) = 0$, então pela proposição (5.3.2), implica que existe algum $w \in \mathbb{C}$ de modo que f e g se anula para (u,v,w). Isto é

porque se escrevermos $(u, v, w) \in C \cap D$, e nossa afirmação está provada. Assim pelo lema (5.3.1), $Res(f, g)_z$ é um polinômio homogêneo não nulo de grau mn. Então o Teorema de Bezout segue pela comparação do grau de cada termo do outro lado da equação (5.9). □

Assim pelo exemplo (5.3.3) o número de pontos em comum de f e g é $5 + 3 + 1 = 9 = 3 \times 3 = grau(f) \times grau(g)$.

Exemplo 5.3.4. *Sejam $f = y^2 - 3$ e $g = 6y - x^3 + 9x$. Queremos determinar o número de pontos de $f \cap g$, através das multiplicidades dos pontos da intersecção. Então homogeneizando, temos:*

$$F = y^2 - 3z^2 = 0$$

$$G = 6yz^2 - x^3 + 9xz^2 = 0,$$

Calculando o resultante de F e G na variável z, temos:

$$Res(F, G)_z = 9(x - 2y)^2(x + y)^4.$$

Assim os pontos (-2, 1, 1) tem multiplicidade 2 e (1, 1, 1) multiplicidade 4. Assim $f \cap g$ tem 6 pontos.

6 CONCLUSÃO

Neste trabalho foi apresentado uma técnica clássica para a resolução de sistemas de equações polinomiais. O desenvolvimento desta teoria, conhecida como resultantes, foi intensamente motivador tanto pela sua elegância algébrica como suas aplicações.

Para desenvolvermos este trabalho, a motivação original era de encontrar uma condição simples para que dois polinômios a uma variável tivessem uma raiz em comum. Essa motivação é classicamente generalizada para o caso de polinômios em várias variáveis. Esta extensão é não trivial, pois são necessários alguns resultados fortes da Geometria Algébrica, como exemplo, a irredutibilidade e dimensão de variedades.

Em relação ao cálculo do resultante, vimos que, em alguns casos pode não ser viável. Por exemplo, a fórmula de Macaulay, que é dada pelo quociente de dois determinantes, é impraticável quando estes são de grandes tamanhos.

No caso de $u-$ Resultante, técnica que apresentamos no capítulo 5 para determinar as soluções de um sistema de equações, ele tranfere o problema para a fatoração de polinômios, que é por si só uma tarefa complicada, principalmente no caso de muitas variáveis.

Também apresentamos no capítulo 5, uma prova de um caso particular do Teorema de Bezout usando a teoria de resultantes. Este resultado é um teorema clássico da Geometria Algébrica, pois determina uma cota para o número de soluções de um sistema de equações polinomiais.

Uma importância da técnica de resultantes, é que ela tem uma variedade de aplicações. Como exemplo, o cálculo do MDC de dois polinômios via resultantes pode ser encontrado nos seguintes trabalhos [8] e [9]. Esta aplicação não foi feita,

pois estávamos interessados em estudar uma técnica para determinar as soluções de um sistema de equações polinomiais.

Temos ainda que o resultante pode ser determinado de forma mais analítica, através da teoria de resíduos, que pode ser encontrado em [5]. Ainda no mesmo [5], podemos encontrar uma técnica para calcular facilmente números algébricos usando resultantes. Desta forma podemos ver que o resultante é uma teoria, por si só, relevante, elegante e matematicamente bonita com diversas aplicações.

Talvez a principal utilidade da técnica de resultantes não seja seu uso como uma ferramenta prática para a resolução de sistema de equações polinomiais, mas sim ainda como uma ferramenta teórica para análise dos sistemas de equações polinomiais. Por isso o fato de ter dado considerável importância para a parte teórica do resultante, exibindo suas propriedades e resultados. Através do resultante, pode-se estudar o comportamento do espaço solução de sistemas genéricos.

BIBLIOGRAFIA

[1] Adams, W., and Loustaunau, P. *An Introduction to Gröbner Bases.* AMS, Providence RI, 1994.

[2] Cox, D., Little, J., and O'Shea, D. *Ideals, Varieties and Algorithms.* Springer, 1996.

[3] Cox, D., Little, J., and O'Shea, D. *Using Algebraic Geometry.* Springer, 2004.

[4] Dickenstein, A. Explicits formulas for the multivariate resultant. *J. of Pure and Applied Algebra 164* (2001), 59–86.

[5] Dickenstein, A. Solving polynomial equations. *Algorithms and Computation in Mathematics 14* (2004).

[6] Dilcher, K., and Stolarsky, K. B. Resultants and discriminants of chebyshev and related polynomials. *Transactions of the AMS 357* (2005), 965–981.

[7] Gao, S. Factoring multivariate polynomials via partial differential equations. *Mathematics of Computation 72* (2003), 801–822.

[8] Gathen, J. V. Z., and Gerhard, J. *Modern Computer Algebra.* Cambridge University Press, 1999.

[9] Gathen, J. V. Z., and Lücking, T. Subresultants revisited. *Theoretical Computer Science 297* (2003), 199–239.

[10] Gelfand, I., Kapranov, M., and Zelevinsky, A. *Discriminants, Resultants and Multidimensional Determinants.* Birkhäuser, 1994.

[11] Hoppen, C. *Uma Generalização do Algoritmo de Gao para Fatoração de Polinômios.* Dissertação de Mestrado - PPG Matemática Aplicada - UFRGS - http://www.biblioteca.ufrgs.br/bibliotecadigital/, 2004.

[12] Jouanolou, J. Le formalisme du résultant. *Advances in Mathematics 90* (1991), 117–263.

[13] Jouanolou, J. Formes d'inertie et résultant: un formulaire. *Advances in Mathematics 126* (1997), 119–250.

[14] Kaltofen, E. *Polynomial factorization 1982-1986*, vol. 125 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, Inc., 1990, pp. 285–309.

[15] Kaltofen, E. *Polynomial factorization 1987-1991*, vol. 583 of *Lecture Notes in Computer Science*. Springer Verlag, 1992, pp. 294–313.

[16] Macaulay, F. On some formulas in elimination. *Journal Mathematics Society 3-27* (1902), 3.

[17] mathpages. *http://www.mathpages.com/home/kmath544/kmath544.htm*.

[18] Mignotte, M. *Mathematics for computer algebra*. Springer- Verlag, 1992.

[19] Shafarevich, I. *Basic Algebraic Geometry*. Springer-Verlag, Berlin-Heidelberg-New York, 1977.

[20] Stillwell, J. *Mathematics and history*. Springer-Verlag, 1989.

[21] Sturmfels, B. Introduction to resultants. *Proccedings of Symposia in Applied Mathematics 53* (1998), 25–39.

[22] Sturmfels, B. Polynomial equations and convex polytopes. *The American Mathematical Monthly 105* (1998), 907.

[23] van der Waerden, B. *Modern Algebra*. Springer-Verlag, 1950.

[24] Wang, W., and Lian, X. Computations of multi-resultants with mecanization. *Applied Mathematics and Computation* (2005).