



**LUDWIG MONTEIRO ALVARENGA AROUCA**

**CURVAS ALGÉBRICAS E O TEOREMA DE BÉZOUT**

**LAVRAS – MG**

**2019**

**LUDWIG MONTEIRO ALVARENGA AROUCA**

**CURVAS ALGÉBRICAS E O TEOREMA DE BÉZOUT**

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Matemática, para a obtenção do título de Licenciado.

Dr. Fernando Lourenço

Orientador

**LAVRAS – MG**

**2019**

**LUDWIG MONTEIRO ALVARENGA AROUCA**

**CURVAS ALGÉBRICAS E O TEOREMA DE BÉZOUT  
ALGEBRAIC CURVES AND THE BÉZOUT THEOREM**

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Matemática, para a obtenção do título de Licenciado.

APROVADA em 12 de Dezembro.

Dr. Fernando Lourenço	UFLA
Dr. Nelson Antonio Silva	UFLA
Dra. Daiane Alice Henrique Ament	UFLA

Dr. Fernando Lourenço  
Orientador

**LAVRAS – MG  
2019**

*Dedico ao meu pai e minha mãe, por sempre me apoiarem nas minhas escolhas e por não medirem esforços para que eu chegasse a essa etapa da vida.*

## **AGRADECIMENTOS**

Agradeço à Universidade Federal de Lavras (UFLA), em especial, ao Departamento de Ciências Exatas, pela oportunidade concedida para realização desta graduação.

Aos meus professores da UFLA pelos ensinamentos e aos demais servidores com os quais convivi durante o curso.

Ao professor Dr. Fernando Lourenço pela orientação, dedicação e ensinamentos fundamentais para a realização deste trabalho que tanto contribuiu para meu crescimento profissional na área da Matemática.

À Dra. Daiane Alice Henrique Ament e ao Dr. Nelson Antonio Silva que se dispuseram a participar como membros da banca examinadora.

À todos os amigos do curso pelo companheirismo durante esses anos, em especial à Vitória, que foi muito importante para minha formação, me cobrando e incentivando em todos os momentos.

*"Nas questões matemáticas não se compreende a incerteza nem a dúvida, assim como tampouco se podem estabelecer distinções entre verdades médias e verdades de grau superior."  
(Hilbert)*

## RESUMO

O trabalho baseia-se no estudo das curvas algébricas planas. Em um primeiro momento estudamos as curvas em  $\mathbb{C}^2$  e suas propriedades. Com a motivação de resolver um sistema de equações, que geometricamente representa as interseções entre duas curvas, começamos a estudar interseções entre duas curvas algébricas através do método da resultante. Nesse contexto, um resultado importante sobre interseções entre curvas algébricas é o Teorema de Bézout (versão fraca). Tal resultado apresenta uma cota superior para o número de interseção entre duas curvas. Com isso, foi possível estudar algumas aplicações do Teorema de Bézout como, por exemplo, o Teorema de Pappus. Outra aplicação é o Teorema do Hexágono de Pascal, que diz que os pontos de interseção dos lados opostos de um hexágono inscrito numa cônica irredutível são colineares. A continuidade do estudo deste tema foi motivada a partir dos exemplos nos quais o número de interseções que encontrávamos não chegava ao número máximo apresentado pelo Teorema de Bézout (versão fraca). Por exemplo, quando temos uma parábola, de equação  $y = x^2$  e a reta, de equação  $x = 1$ , temos apenas o ponto de interseção  $P = (1, 1)$ . Mas, pelo Teorema de Bézout, o número máximo de pontos seria dois. Com isso, demos sequência aos estudos com os pontos no infinito, o plano projetivo  $\mathbb{P}^2$  e curvas projetivas que, a partir desses conceitos, nos dá condições de encontrar todas as interseções entre duas curvas. Assim, temos: **Teorema de Bézout (versão forte):** *Sejam  $C$  e  $D$  duas curvas projetivas definidas por  $F$  e  $G$ , onde  $\partial F = m$  e  $\partial G = n$ . Suponha que  $C$  e  $D$  não têm componentes em comum, então  $C$  e  $D$  têm exatamente  $mn$  pontos de interseção, ou seja,  $\#C \cap D = mn$ .*

**Palavras-chave:** Teoria de Polinômios. Curvas Algébricas. Plano Projetivo. Teorema de Bézout.

## ABSTRACT

The project is based on the study of plane algebraic curves. At first we study the curves in  $\mathbb{C}^2$  and their properties. With the motivation of solving a system of equations, which geometrically represents the intersections between two curves. We began to study intersections between two algebraic curves using the resulting method. In this context, an important result about intersections between algebraic curves is the Bézout Theorem (weak version). This result has a higher quota for the number of intersection between two curves. Thus, it was possible to study some applications of the Bézout Theorem, such as the Pappus Theorem. Another application is Pascal's Hexagon Theorem, which says that the intersection points on opposite sides of a Hexagon inscribed in an irreducible conic are collinear. The continuity of the study of this theme was motivated from the examples in which the intersections we found did not reach the maximum number presented by the Bézout Theorem. For example, when we have a parable of equation  $y = x^2$  and the line of equation  $x = 1$ , we have only the intersection point  $P = (1, 1)$ . But by the Bézout Theorem, the maximum number of points would be two. Thus, we continued the studies with infinity points and the projective plane  $\mathbb{P}^2$  which, from these concepts, allows us to find all intersections between two curves. So we have: **Bézout Theorem (strong version):** *Let  $C$  and  $D$  be two projective curves defined by  $F$  and  $G$ , where  $\partial F = m$  and  $\partial G = n$ . Suppose  $C$  and  $D$  have no components in common, so  $C$  and  $D$  have exactly  $mn$  intersection points, that is  $\#C \cap D = mn$ .*

**Keywords:** Polynomial theory. Algebraic Curves. Project Plan. Bézout Theorem.

## LISTA DE FIGURAS

Figura 2.1 – Algoritmo da divisão . . . . .	15
Figura 3.1 – Exemplo de curva algébrica . . . . .	18
Figura 3.2 – Gráfico das curvas $C$ e $D$ . . . . .	22
Figura 3.3 – Gráfico das curvas $C$ e $D$ . . . . .	24
Figura 3.4 – Gráfico das curvas $M$ e $N$ . . . . .	25
Figura 3.5 – Curva $C$ - Aplicação 1 do Teorema de Bézout . . . . .	27
Figura 3.6 – Teorema do Hexágono de Pascal . . . . .	28
Figura 3.7 – Teorema de Pappus . . . . .	29
Figura 4.1 – Plano $\pi$ . . . . .	33
Figura 4.2 – Ponto de $\mathbb{P}^2$ . . . . .	33
Figura 4.3 – Relação de igualdade entre dois pontos de $\mathbb{P}^2$ . . . . .	34

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>9</b>
<b>2</b>	<b>TEORIA DE POLINÔMIOS</b>	<b>10</b>
<b>2.1</b>	<b>Polinômio</b>	<b>10</b>
<b>2.2</b>	<b>Grau de Polinômio</b>	<b>12</b>
<b>3</b>	<b>CURVAS ALGÉBRICAS</b>	<b>18</b>
<b>3.1</b>	<b>Interseção entre Curvas Algébricas</b>	<b>19</b>
<b>3.2</b>	<b>Aplicações</b>	<b>25</b>
<b>3.3</b>	<b>Multiplicidades</b>	<b>30</b>
<b>3.3.1</b>	<b>Interseção de uma curva com uma reta</b>	<b>30</b>
<b>3.3.2</b>	<b>Pontos múltiplos</b>	<b>31</b>
<b>4</b>	<b>PLANO PROJETIVO E PONTOS NO INFINITO</b>	<b>33</b>
<b>4.1</b>	<b>Pontos no infinito</b>	<b>33</b>
<b>4.2</b>	<b>Curvas Projetivas</b>	<b>35</b>
<b>4.3</b>	<b>Interseção entre Curvas Projetivas</b>	<b>36</b>
<b>5</b>	<b>CONCLUSÃO</b>	<b>41</b>
	<b>REFERÊNCIAS</b>	<b>42</b>

## 1 INTRODUÇÃO

Um dos campos mais amplos da Matemática é a Álgebra que, ao generalizar a aritmética, introduz variáveis através de símbolos que representam os números. Dentro do estudo da Álgebra, os polinômios ocupam lugar fundamental, pois são expressões algébricas que envolvem as quatro operações básicas da Matemática: adição, subtração, multiplicação e divisão, além da potenciação. Uma das aplicações dos polinômios é o estudo das Curvas Algébricas Planas.

A ideia dessa pesquisa surgiu para dar sequência ao estudo nessa área específica, abordada durante o curso de Graduação em Matemática. Deste modo, este trabalho tem o objetivo de estudar os conceitos dessas curvas no ambiente real, complexo e projetivo, além de apresentar algumas de suas aplicações. A princípio, é apresentada a Teoria dos Polinômios, com o estudo de alguns conceitos indispensáveis para dar sequência ao trabalho com a definição das Curvas Algébricas e exploração de suas propriedades.

No capítulo seguinte, o trabalho concentra-se na definição das Curvas Algébricas, com alguns exemplos para fundamentar o estudo dos pontos de interseções entre Curvas Algébricas e buscar esses pontos, através da utilização do Método da Resultante. Aborda-se, então, o Teorema de Bézout, que relata o número máximo da quantidade de pontos de interseção entre duas curvas. Em sequência, apresenta-se um novo espaço, o Plano Projetivo, com foco nos Pontos no Infinito, elementos que fundamentam a busca pela exatidão no número de interseção de duas curvas.

A relevância desse estudo está na comprovação de que a possibilidade de se encontrar o número exato de pontos de interseção entre duas curvas é real. Comprova-se, então, a importância do Teorema de Bézout para o estudo dos polinômios, para a álgebra e, enfim, para o desenvolvimento matemático da humanidade.

## 2 TEORIA DE POLINÔMIOS

Nesse capítulo vamos trabalhar alguns conceitos sobre polinômios necessários para o desenvolvimento do trabalho, pois a partir desse estudo podemos definir Curvas Algébricas e explorar suas propriedades. Para esse estudo usaremos como referência (LEIMANN, 2003) e (DOMINGUES; IEZZI, 1982) no qual trabalha-se os conceitos sobre anel.

### 2.1 Polinômio

**Definição 2.1.1** *Seja  $A$  um anel comutativo com unidade. Chamamos de Polinômio, com variável  $x$ , a expressão  $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ , onde cada  $a_i \in A$ .*

**Observação 2.1.1** *Denote  $A[x]$  como o conjunto de todos os polinômios sobre a indeterminada  $x$ .*

Dois polinômios são iguais se, e somente se, os coeficientes correspondentes a mesma potência forem iguais.

Definiremos as operações de adição e multiplicação entre dois polinômios. Sejam:

$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m \text{ e}$$

$$q(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n.$$

Temos que,

$$(p + q)(x) := p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_r + b_r)x^r$$

e

$$(pq)(x) := p(x)q(x) = c_0 + c_1x + c_2x^2 + \dots + c_kx^k,$$

onde

$$\begin{cases} c_0 = a_0b_0 \\ c_1 = a_0b_1 + a_1b_0 \\ \vdots \\ c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0, \text{ isto é, } \sum_{i=0}^k a_ib_{k-i}. \end{cases}$$

**Definição 2.1.2** *O polinômio  $0 = 0 + 0x + 0x^2 + \dots + 0x^n$  é chamado de polinômio nulo e o polinômio  $1(x) = 1 + 0x + \dots + 0x^n$  é chamado de polinômio neutro para multiplicação.*

**Teorema 2.1.1** *O conjunto  $A[x]$  é um anel comutativo com unidade.*

**Demonstração:**

Considere os polinômios  $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m$ ,  $q(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$  e  $h(x) = c_0 + c_1x + c_2x^2 + \dots + c_rx^r$  em  $A[x]$ .

- Associatividade da adição:

$$\begin{aligned}
 p(x) + (q(x) + h(x)) &= \\
 &= (a_0 + a_1x + a_2x^2 + \dots) + ((b_0 + c_0) + (b_1 + c_1)x + (b_2 + c_2)x^2 + \dots) = \\
 &= (a_0 + (b_0 + c_0)) + (a_1 + (b_1 + c_1))x + (a_2 + (b_2 + c_2))x^2 + \dots = \\
 &= ((a_0 + b_0) + c_0) + ((a_1 + b_1) + c_1)x + ((a_2 + b_2) + c_2)x^2 + \dots = \\
 &= ((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots) + (c_0 + c_1x + c_2x^2 + \dots) = \\
 &= (p(x) + q(x)) + h(x).
 \end{aligned}$$

- Comutatividade da adição:

$$\begin{aligned}
 p(x) + q(x) &= \\
 &= (a_0 + a_1x + a_2x^2 + \dots + a_mx^m) + (b_0 + b_1x + b_2x^2 + \dots + b_nx^n) = \\
 &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots = \\
 &= (b_0 + a_0) + (b_1 + a_1)x + (b_2 + a_2)x^2 + \dots = \\
 &= (b_0 + b_1x + b_2x^2 + \dots + b_nx^n) + (a_0 + a_1x + a_2x^2 + \dots + a_mx^m) = \\
 &= q(x) + p(x).
 \end{aligned}$$

- Existência do elemento neutro para adição:

Considere o polinômio  $0(x) = 0 + 0x + 0x^2 + \dots + 0x^m$ , temos que:

$$\begin{aligned}
 0(x) + p(x) &= \\
 &= (0 + 0x + 0x^2 + \dots + 0x^m) + (a_0 + a_1x + a_2x^2 + \dots + a_mx^m) = \\
 &= (0 + a_0) + (0 + a_1)x + (0 + a_2)x^2 + \dots + (0 + a_m)x^m = \\
 &= (a_0 + a_1x + a_2x^2 + \dots + a_mx^m) = \\
 &= p(x).
 \end{aligned}$$

- Todo elemento de  $p$  é simetrizável:

Tome o polinômio  $-p(x) = (-a_0) + (-a_1)x + (-a_2)x^2 + \dots + (-a_m)x^m$ . Temos que

$$\begin{aligned}
 p(x) + (-p)(x) &= \\
 &= (a_0 + a_1x + a_2x^2 + \dots + a_mx^m) + ((-a_0) + (-a_1)x + (-a_2)x^2 + \dots + (-a_m)x^m) =
 \end{aligned}$$

$$\begin{aligned}
&= (a_0 + (-a_0)) + (a_1 + (-a_1))x + (a_2 + (-a_2))x^2 + \dots + (a_m + (-a_m))x^m = \\
&= 0 + 0x + 0x^2 + \dots + 0x^m = 0(x).
\end{aligned}$$

Para os próximos itens, considere a seguinte notação :  $p(x) = (a_i)$ ,  $q(x) = (b_j)$ ,  $h(x) = (c_k)$ .

- Associatividade da multiplicação:

Sejam  $q(x)h(x) = (d_l)$ ,  $p(x)(q(x)h(x)) = e_m$ ,  $p(x) \cdot q(x) = f_n$ ,  $(p(x)q(x))h(x) = g_m$ .

$$\begin{aligned}
\text{Assim } (e_m) &= \sum_{i+l=m} a_i d_l = \sum_{i+l=m} a_i \left( \sum_{j+k=l} b_j c_k \right) = \sum_{i+j+k=m} a_i (b_j c_k) = \sum_{i+j+k=m} (a_i b_j) c_k = \sum_{n+k=m} \left( \sum_{i+j} a_i b_j \right) c_k = \\
&\sum_{n+k=m} f_n c_k = g_m.
\end{aligned}$$

- Distributividade:

Sejam  $p(x)q(x) = k_0 + k_1x + \dots + k_nx^n + \dots$ ,  $p(x)h(x) = g_0 + g_1x + \dots + g_nx^n$  e

$$p(x) \cdot (q(x) + h(x)) = e_0 + e_1x + \dots + e_nx^n + \dots$$

$$\text{Assim } (e_n) = \sum_{i=0}^n a_i (b_{n-i} + c_{n-i}) = \sum_{i=0}^n a_i b_{n-i} + a_i c_{n-i} = (k_n) + (g_n).$$

- Comutatividade da multiplicação:

Sejam  $p(x)q(x) = k_0 + k_1x + \dots + k_nx^n + \dots$  e  $q(x)p(x) = e_0 + e_1x + \dots + e_nx^n + \dots$

Assim temos  $(k_n) = \sum_{i=0}^n a_i b_i$ , como  $a_i$  e  $b_i \in A$  então podemos comutar  $a_i$  e  $b_i$ .

$$\text{Logo } \sum_{i=0}^n a_i b_i = \sum_{i=0}^n b_i a_i = (e_n).$$

- Existência do elemento neutro para multiplicação:

Tome  $1(x) = d_0 + d_1x + \dots + d_nx^n \in A[x]$ , onde  $d_0 = 1$  e  $d_i = 0$  para todo  $i = 1, \dots, n$ .

Assim  $1(x)p(x) = e_0 + e_1x + \dots + e_nx^n$ , onde  $e_0 = a_0d_0 = a_0$ ,  $e_1 = a_0d_1 + a_1d_0 = a_1$ ,  $e_2 = a_0d_2 + a_1d_1 + a_2d_0 = a_2$  e  $e_i = a_id_0 = a_i$ .

□

## 2.2 Grau de Polinômio

Nessa seção será definido o grau e a raiz de polinômio seguindo de alguns resultados envolvendo esses conceitos. A definição de grau é indispensável para o desenvolvimento do trabalho, uma vez que será utilizada para encontrar o número de interseções entre duas curvas.

**Definição 2.2.1** Seja  $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_ix^i \in A[x]$  tal que  $a_i \neq 0$  então o grau de  $p$  é  $i$ .

**Notação:**  $\partial p = i$ .

**Observação 2.2.1** O polinômio nulo não tem grau.

Vamos apresentar agora dois resultados sobre o grau de polinômios. Sejam  $p$  e  $q$  polinômios pertencentes a  $A[x]$ , onde  $A$  é um anel, temos:

$$1- \partial(p+q) \leq \max\{\partial(p), \partial(q)\}.$$

**Demonstração:**

Sejam dois polinômios  $p(x) = a_0 + a_1x + \dots + a_ix^i$  e  $q(x) = b_0 + b_1x + \dots + b_jx^j$  tais que  $p, q \in A[x]$ . Assim temos dois casos:

1º: Suponha que  $i > j$ , então:

$$p(x) + q(x) = a_0 + b_0 + (a_1 + b_1)x + \dots + (a_j + b_j)x^j + \dots + a_ix^i$$

$$\text{Logo } \partial(p+q) = i = \max\{\partial(p), \partial(q)\}.$$

2º: Suponha que  $i = j$ , então:

$$\text{Se } a_i + b_i = 0, \text{ temos: } p(x) + q(x) = a_0 + b_0 + (a_1 + b_1)x + \dots + (a_{i-1} + b_{i-1})x^{i-1} + (a_i + b_i)x^i = a_0 + b_0 + (a_1 + b_1)x + \dots + (a_{i-1} + b_{i-1})x^{i-1} + 0x^i = a_0 + b_0 + (a_1 + b_1)x + \dots + (a_{i-1} + b_{i-1})x^{i-1}.$$

$$\text{Logo } \partial(p+q) \leq i-1 < \max\{\partial(p), \partial(q)\}.$$

$$\text{Se } a_i + b_i \neq 0, \text{ temos: } p(x) + q(x) = a_0 + b_0 + (a_1 + b_1)x + \dots + (a_j + b_j)x^j + \dots + (a_i + b_i)x^i.$$

$$\text{Logo } \partial(p+q) = i = \max\{\partial(p), \partial(q)\}.$$

$$\text{Portanto, } \partial(p+q) \leq \max\{\partial(p), \partial(q)\}.$$

$$2- \partial(pq) \leq \partial(p) + \partial(q).$$

Para demonstração desse resultado, veja (LEIMANN, 2003).

□

Para destacar os casos acima temos alguns exemplos.

**Exemplo 2.2.1** Sejam  $f(x) = 2x^3 + 1$  e  $g(x) = -2x^3 + x - 3$  polinômios pertencentes a  $\mathbb{R}[x]$ . Note que  $f(x) + g(x) = (2x^3 + 1) + (-2x^3 + x - 3) = x - 2$  assim  $\partial(f+g) = 1 < \max\{\partial(f), \partial(g)\}$ .

**Exemplo 2.2.2** Considere os seguintes polinômios em  $\mathbb{R}[x]$ :  $p(x) = x^2 - x + 1$  e  $q(x) = x^3 + x - 2$ . A soma entre os dois polinômios é:  $p(x) + q(x) = (x^2 - x + 1) + (x^3 + x - 2) = x^3 + x^2 - 1$  e  $\partial(p+q) = 3 = \max\{\partial(p), \partial(q)\}$ .

**Exemplo 2.2.3** Sejam os polinômios  $a, b \in \mathbb{R}[x]$  da forma  $a(x) = -x + 1$  e  $b(x) = x^2 + x - 2$ .

Temos  $a(x) \cdot b(x) = (-x + 1) \cdot (x^2 + x - 2) = -x^3 - x^2 + 2x + x^2 + x - 2 = -x^3 + 3x - 2$ .

Assim  $\partial(a(x)b(x)) = 3 = 1 + 2 = \partial(a) + \partial(b)$ .

No próximo exemplo usaremos a classe dos restos  $\mathbb{Z}_m$ , onde esse anel é o conjunto dos restos da divisão por  $m$ .

**Exemplo 2.2.4** Considere  $s(x) = \bar{2}x^2 + \bar{3}x + 1$  e  $t(x) = 2x + 2$  polinômios em  $\mathbb{Z}_4[x]$ .

$s(x)t(x) = (2x^2 + 3x + 1) \cdot (2x + 2) = 4x^3 + 4x^2 + 6x^2 + 6x + 2x + 2 = 10x^2 + 8x + 2 = 2x^2 + 2$  e

$\partial(st) = 2 < 3 = 2 + 1 = \partial(s) + \partial(t)$ .

**Teorema 2.2.1** Se  $A$  é um domínio de integridade então  $A[x]$  é domínio de integridade.

**Demonstração:**

Sejam dois polinômios  $p(x) = a_0 + a_1x + \dots + a_i x^i$  e  $q(x) = b_0 + b_1x + \dots + b_j x^j$  com  $a_i \neq 0, b_j \neq 0$  tais que  $p, q \in A[x]$ .

Considere a multiplicação  $p(x)q(x) = c_0 + c_1x + c_2x^2 + \dots + c_{i+j}x^{i+j}$

Como  $A$  é domínio e  $a_i \neq 0, b_j \neq 0$  implica que  $a_i b_j \neq 0$ . Concluimos que  $c_{i+j} \neq 0$ . Logo  $p(x)q(x) \neq 0$ . Portanto  $A[x]$  é domínio.  $\square$

A proposição a seguir diz a respeito à Divisão Euclidiana.

**Proposição 2.2.1** Sejam  $(A, +, \cdot)$  um anel comutativo com unidade e  $A[x]$  o anel de polinômios numa variável sobre  $A$ . Considere  $f(x) = a_0 + a_1x + \dots + a_n x^n$  e  $g(x) = b_0 + b_1x + \dots + b_m x^m$  polinômios em  $A[x]$ , com  $b_m$  inversível em  $A$  e  $n \geq m$ . Então:

i) Existem  $t, r \in A[x]$  tais que  $f(x) = g(x)t(x) + r(x)$ , com  $\partial r < \partial g$  ou  $r = 0$ .

ii) Tais  $t$  e  $r$  podem ser efetivamente calculados.

**Demonstração:**

Vamos dividir em dois casos:

1º caso: Se  $f = 0$  ou se  $\partial f < \partial g$ , tome  $t = 0$  e  $r = f$ .

2º caso: se  $\partial f \geq \partial g = m$ .

Como  $b_m$  é inversível em  $A$ , existe  $\frac{1}{b_m} \in A$  e  $\frac{1}{b_m} a_n x^{n-m} \in A[x]$  sendo  $\frac{1}{b_m} a_n x^{n-m} b_m x^m = a_n x^n$ .

Temos  $f(x) - \frac{1}{b_m} a_n g(x) = (\frac{a_{n-1} - a_n b_{m-1}}{b_m}) x^{n-1} + \dots + (\frac{a_{n-m} - a_n b_0}{b_m}) x^{n-m} + h(x)$  (onde  $h = 0$  ou  $\partial h < n - m$ ) =  $f_1(x) \in A[x]$ . Assim  $f(x) = g(x)(\frac{1}{b_m}) a_n x^{n-m} + f_1(x)$ .

Se  $f_1 = 0$  ou  $\partial f_1 < \partial g = m$ , tome  $t(x) = \frac{1}{b_m} a_n x^{n-m}$  e  $r = f_1$ .

Se  $p = \partial f_1 \geq m$  escreva  $f_1(x) = c_p x^p + \dots + c_0$  com  $n - 1 \geq p \geq m$  e  $c_p \neq 0$  tome  $f_2(x) = f_1(x) - \frac{1}{b_m} c_p x^{p-m} g(x)$  temos  $f(x) = g(x)[\frac{1}{b_m} a_n x^{n-m} + \frac{1}{b_m} c_p x^{p-m}] + f_2(x)$ .

Repete-se esse processo até que  $f_i = 0$  ou  $\partial f_i < m$ . □

**Exemplo 2.2.5** Sejam  $f(x) = 3x^4 - 9x^3 + 7x^2 - 3$  e  $g(x) = 3x^2 - 3x - 2$  polinômio em  $\mathbb{R}[x]$ , calcule a divisão de  $f$  por  $g$ .

Figura 2.1 – Algoritmo da divisão

$$\begin{array}{r}
 f(x) = 3x^4 - 9x^3 + 7x^2 + 2x - 3 \quad \Big| \quad 3x^2 - 3x - 2 = g(x) \\
 \underline{-3x^4 + 3x^3 + 2x^2} \phantom{+ 2x - 3} \\
 -6x^3 + 9x^2 + 2x - 3 \\
 \underline{6x^3 - 6x^2 - 4x} \\
 3x^2 - 2x - 3 \\
 \underline{-3x^2 + 3x + 2} \\
 x - 1 = r(x)
 \end{array}$$

Fonte: Do autor (2019).

Com isso concluímos que  $3x^4 - 9x^3 + 7x^2 - 3 = (3x^2 - 3x - 2)(x^2 - 2x + 1) + (x - 1)$ .

**Definição 2.2.2** Se  $f(x) = a_0 + a_1 x + \dots + a_n x^n$  é um polinômio não nulo em  $A[x]$  e  $\alpha \in A$  definimos  $f(\alpha) = a_0 + a_1 \alpha + \dots + a_n \alpha^n \in A$ . Dizemos que  $\alpha$  é uma raiz de  $f$  em  $A$  se tivermos  $f(\alpha) = 0$ .

**Proposição 2.2.2** Sejam  $A$  um anel,  $f \in A[x]$  não identicamente nulo e  $\alpha \in A$ , então existe  $q \in A[x]$  tal que  $f(x) = (x - \alpha)q(x) + f(\alpha)$ .

**Demonstração:**

Seja  $(x - \alpha) \in A[x]$ , assim pela Proposição 2.2.1 existem  $q, r \in A[x]$  tais que  $f(x) = q(x)(x - \alpha) + r(x)$  onde  $r = 0$  ou  $\partial r < 1$ , ou seja,  $r \in A$ . Assim temos que  $f(\alpha) = q(\alpha)(\alpha - \alpha) + r$  então  $f(\alpha) = r$ .

Portanto  $f(x) = q(x)(x - \alpha) + f(\alpha)$ . □

**Corolário 2.2.1** Seja  $A$  um anel,  $\alpha \in A$  é raiz de  $f$  se, e somente se,  $(x - \alpha)$  divide  $f$ , ou seja,  $\alpha \in A$ ,  $f(\alpha) = 0$  se, e somente se,  $f(x) = g(x)(x - \alpha)$ , com  $g \in A[x]$ .

**Demonstração:**

( $\rightarrow$ ) Aplicando a proposição anterior temos que  $f(x) = (x - \alpha)g(x) + f(\alpha)$ . Como  $f(\alpha) = 0$ , então  $f(x) = (x - \alpha)g(x) + f(\alpha) = (x - \alpha)g(x) + 0$ .

Portanto  $f(x) = (x - \alpha)g(x)$ .

( $\leftarrow$ ) Nossa hipótese é  $f(x) = g(x)(x - \alpha)$  e pela proposição anterior temos que  $f(x) = (x - \alpha)g(x) + f(\alpha)$ .

Assim  $f(x) = g(x)(x - \alpha) = (x - \alpha)g(x) + f(\alpha)$ . Logo  $f(\alpha) = 0$ .  $\square$

**Definição 2.2.3** *Sejam  $A$  um anel,  $f \in A[x]$  e  $\alpha \in A$ . Dizemos que  $\alpha$  é uma raiz de  $f$  com multiplicidade  $k \geq 1$  se  $(x - \alpha)^k$  divide  $f$  mas  $(x - \alpha)^{k+1}$  não divide  $f$ .*

**Corolário 2.2.2** *Sejam  $A$  um anel,  $f \in A[x]$  e  $\alpha \in A$ . Então as seguintes afirmações são equivalentes:*

i)  $\alpha$  é uma raiz de  $f$  com multiplicidade  $k$ .

ii) Existe  $h \in A[x]$  tal que  $f = (x - \alpha)^k h$  com  $h(\alpha) \neq 0$ .

**Demonstração:**

i)  $\Rightarrow$  ii) Como  $\alpha$  é raiz de  $f$  com multiplicidade  $k$ , então  $(x - \alpha)^k$  divide  $f$ , assim existe  $h \in A[x]$  tal que  $f(x) = (x - \alpha)^k h(x)$ . Suponha  $h(\alpha) \neq 0$ , então existe  $g \in A[x]$  tal que  $h(x) = (x - \alpha)g(x)$ . Substituindo em  $f$  temos  $f(x) = (x - \alpha)^{k+1}g(x)$ . Absurdo! Pois  $(x - \alpha)^{k+1}$  não divide  $f$ .

ii)  $\Rightarrow$  i) Como  $f(x) = (x - \alpha)^k h(x)$  temos que  $\alpha$  é raiz de  $f$  com multiplicidade maior ou igual a  $k$ , assim  $(x - \alpha)^k$  divide  $f$ . Devemos mostrar que  $(x - \alpha)^{k+1}$  não divide  $f$ . Suponha  $(x - \alpha)^{k+1}$  divide  $f$ , assim  $(x - \alpha)^k h(x) = f(x) = (x - \alpha)^{k+1}g(x)$ ,  $g \in A[x]$ . Logo  $(x - \alpha)^k h(x) - (x - \alpha)^{k+1}g(x) = 0$  o que implica em  $(x - \alpha)^k [h(x) - (x - \alpha)g(x)] = 0$ . Assim  $[h(x) - (x - \alpha)g(x)] = 0 \Rightarrow h(x) = (x - \alpha)g(x)$  então  $h(\alpha) = 0$ . Absurdo! Pois, por hipótese,  $h(\alpha) \neq 0$ .  $\square$

**Definição 2.2.4** *Considere  $\mathbb{K}$  um corpo e  $\mathbb{K}[x]$  o conjunto dos polinômios sobre  $\mathbb{K}$  na indeterminada  $x$ . Seja  $f \in \mathbb{K}[x]$  tal que  $\partial f \geq 1$ . Dizemos que  $f$  é polinômio irreduzível sobre  $\mathbb{K}$  se toda vez que  $f(x) = g(x)h(x)$  sendo que  $g, h \in \mathbb{K}[x]$  então  $g(x) = a \neq 0 \in \mathbb{K}$  ou  $h(x) = b \neq 0 \in \mathbb{K}$ . Se  $f$  não for irreduzível sobre  $\mathbb{K}$  dizemos que  $f$  é reduzível sobre  $\mathbb{K}$ .*

**Exemplo 2.2.6** *Considere  $f(x) = x^2 + 3x$ , onde  $f \in \mathbb{R}[x]$ , vamos verificar se esse polinômio é irreduzível ou não.*

*Podemos escrever  $f$  como um produto entre dois polinômios, ou seja,  $f(x) = g(x)h(x)$ , onde  $g(x) = x$  e  $h(x) = x + 3$ . Nesse caso nenhum dos dois polinômios são constantes, portanto  $f$  é um polinômio reduzível sobre  $\mathbb{R}$ .*

Para dar sequência ao trabalho vamos definir anel de polinômio para duas variáveis e uma proposição sobre esse conteúdo.

**Definição 2.2.5** *Seja  $A$  um anel comutativo com unidade. O conjunto  $A[x,y]$  é o conjunto de todos os polinômios sobre as variáveis  $x$  e  $y$ .*

**Definição 2.2.6** *Seja  $p \in A[x,y]$ , o grau de  $p$  é o maior expoente entre os monômios desse polinômio. Em alguns casos temos  $x$  multiplicando  $y$ , então temos que somar os expoentes de cada variável para obter o grau desse monômio.*

**Definição 2.2.7** *Um anel  $A$  é chamado de anel de fatoração única se ele é um anel de integridade tal que:*

- *Todo elemento não nulo de  $A$  que não é uma unidade de  $A$  pode ser decomposto em um produto de irredutíveis.*
- *A decomposição da parte 1 é única além da ordem e multiplicação por unidades.*

Como podemos escrever o anel  $A[x,y]$  como  $A[x]([y])$ , essa definição pode se estender para esse conjunto, que é o conjunto de todos os polinômios sobre as variáveis  $x$  e  $y$ .

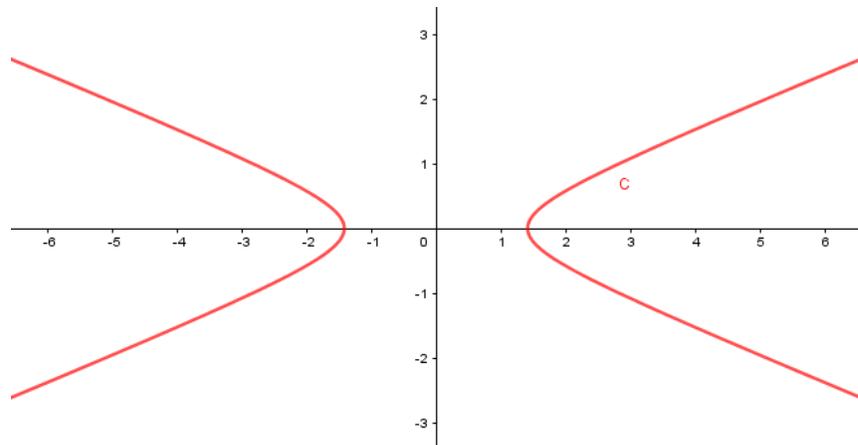
### 3 CURVAS ALGÉBRICAS

Nesse capítulo vamos definir uma curva algébrica através dos conceitos de polinômio, explorando alguns exemplos. Feito isso podemos estudar os pontos de interseções entre curvas algébricas e encontrar esses pontos através do método da resultante. Para esse capítulo veja (GERD, 2001), (FULTON, 2008), (SALEHYAN, 2008) e (VAINSENER, 1996).

**Definição 3.0.1** Considere o anel de polinômio  $\mathbb{K}[x, y]$  em duas variáveis, uma curva algébrica é o conjunto dos zeros de um polinômio qualquer, ou seja, é um conjunto  $C = \{(a, b) \in \mathbb{K}^2 \mid p(a, b) = 0\} \subset \mathbb{K}^2$  onde  $p \in \mathbb{K}[x, y]$ .

**Exemplo 3.0.1** Seja  $f(x, y) = \frac{x^2}{2} - 3y^2 - 1$  um polinômio em  $\mathbb{R}[x, y]$ . Vamos construir o gráfico da curva gerada por esse polinômio. Considere como  $C$  a curva gerada por  $f$ , então  $C = \{(a, b) \in \mathbb{R}^2 \mid f(a, b) = 0\}$ , ou seja,  $C$  tem os pontos que satisfazem a equação  $0 = \frac{x^2}{2} - 3y^2 - 1$ . Assim temos o seguinte gráfico:

Figura 3.1 – Exemplo de curva algébrica



Fonte: Do autor (2019).

**Definição 3.0.2** O grau de uma curva  $D$  gerada pelo polinômio  $p$  é igual ao grau do polinômio, ou seja,  $\partial D := \partial p$ .

Uma motivação para continuar o estudo é o seguinte problema: dadas duas equações  $p(x, y) = 0$  e  $q(x, y) = 0$ , devemos encontrar se estas possuem soluções em comum. Geometricamente estamos verificando se existe interseção entre duas curvas  $C$  e  $D$  geradas pelos polinômios  $p$  e  $q$ .

### 3.1 Interseção entre Curvas Algébricas

Seja  $C$  uma curva definida por  $f \in \mathbb{C}[x, y]$ ,  $f$  admite uma fatoração  $f = f_1^{k_1} + f_2^{k_2} + \dots + f_r^{k_r}$ , com  $f_i$  polinômios irredutíveis. Cada curva  $C_i$  gerada por  $f_i$  é chamada de componente de  $C$ .

**Definição 3.1.1** *Um curva algébrica  $C$  é chamada reduzível se existem curvas algébricas distintas  $C_1$  e  $C_2$  tais que  $C = C_1 \cup C_2$ . Irreduzível significa não reduzível, ou seja, qualquer decomposição  $C = C_1 \cup C_2$  implica  $C_1 = C_2$ .*

**Exemplo 3.1.1** *Considere  $f(x) = x^2 - y^2$  o polinômio que gera a curva  $C$ . Podemos escrever esse polinômio como  $f(x) = (x - y)(x + y)$ , logo a curva  $C$  é reduzível, pois considere  $C_1 = \{x - y\}$  e  $C_2 = \{x + y\}$  sendo  $C = C_1 \cup C_2$ .*

**Teorema 3.1.1** *Qualquer curva algébrica  $C \subseteq \mathbb{C}^2$  admite uma representação única  $C = C_1 \cup C_2 \cup \dots \cup C_r$ , com  $C_i$  irredutível para todo  $i$ .*

**Demonstração:**

Consequência direta do fato que  $\mathbb{C}[x, y]$  é um anel de fatoração única. □

**Lema 3.1.1** *Sejam  $f, g \in \mathbb{C}[x, y]$  polinômios sem fatores irredutíveis em comum. Então existem  $r, s \in \mathbb{C}[x, y]$  e  $t \in \mathbb{C}[x] \setminus \{0\}$  tais que  $rf + sg = t$ .*

**Demonstração:** Para a demonstração veja (SALEHYAN, 2008). □

**Proposição 3.1.1** *O conjunto das soluções de um sistema de duas equações polinomiais a duas variáveis sem fator irredutível comum é finito, ou seja, a interseção de duas curvas algébricas planas sem componente em comum é finita.*

**Demonstração:**

Considere  $C$  e  $D$  curvas sem componentes em comum sendo  $f$  e  $g$  os polinômios que as definem.

Se  $(x_0, y_0) \in C \cap D$  então 
$$\begin{cases} f(x_0, y_0) = 0 \\ g(x_0, y_0) = 0. \end{cases}$$

Pelo Lema 3.1.1 existem  $a, b \in \mathbb{C}[x, y]$  e  $c \in \mathbb{C}[x] \setminus \{0\}$  tais que  $af + bg = c$  o que implica  $a(x_0, y_0)f(x_0, y_0) + b(x_0, y_0)g(x_0, y_0) = c(x_0) \Rightarrow c(x_0) = 0$ .

Analogamente existem  $a', b' \in \mathbb{C}[x, y]$  e  $c' \in \mathbb{C}[y] \setminus \{0\}$  tais que  $a'f + b'g = c'$  o que implica em  $c'(y_0) = 0$ .

Logo  $\{(x_0, y_0) | (x_0, y_0) \in C \cap D\} \subseteq \{x_0 | c(x_0) = 0\} \times \{y_0 | c'(y_0) = 0\}$ . Portanto  $C \cap D$  é finito. □

Demonstrada essa proposição, podemos determinar os pontos de interseção entre duas curvas, para isso usaremos o método da resultante. Esse método pode ser encontrado em (TURA, 2006).

Sejam  $f, g \in \mathbb{C}[x, y]$ , vamos escrever  $f$  e  $g$  como polinômios na variável  $y$  com coeficientes em  $\mathbb{C}[x]$ , então temos:  $f(y) = a_0y^m + \dots + a_m$ , com  $m \geq 1$  e  $g(y) = b_0y^n + \dots + b_n$ , com  $n \geq 1$ .

Tentaremos encontrar os valores de  $a$  para os quais  $f(a, y)$  e  $g(a, y)$  admitem raiz em comum. Geometricamente queremos encontrar os valores de  $x$  dos pontos  $C \cap D$ . Para dar sequência ao método usaremos o seguinte teorema.

**Teorema 3.1.2** *Sejam  $f, g \in \mathbb{C}[y] \setminus \mathbb{C}$  com  $\partial f = m, \partial g = n$ . Então  $f$  e  $g$  possuem componentes em comum em  $\mathbb{C}[y]$  se, e somente se, existem  $u, v \in \mathbb{C}[y]$  tais que  $uf = vg$  com  $\partial u < n, \partial v < m$ .*

**Demonstração:**

( $\rightarrow$ ) Seja  $h$  um fator em comum de  $f$  e  $g$ . Assim: 
$$\begin{cases} f = hh_1 \\ g = hh_2 \end{cases}$$

Multiplicando a primeira equação por  $h_2$  e a segunda por  $h_1$  temos: 
$$\begin{cases} fh_2 = hh_1h_2 \\ gh_1 = hh_2h_1 \end{cases}$$

Logo  $fh_2 = gh_1$ . Podemos considerar  $h_2 = u$  e  $h_1 = v$ , assim  $\partial u < \partial g = n$  e  $\partial v < \partial f = m$ .

( $\leftarrow$ ) Se existem  $u, v$  tal que  $\partial u < n, \partial v < m$  e  $uf = vg$  então  $f|vg$  e  $g|uf$ . Como  $\partial v < \partial f$ , logo existe  $h$  tal que  $h|f$  e  $h|g$ . Portanto  $f, g$  possuem componentes em comum.  $\square$

Agora podemos aplicar o Teorema 3.1.2 em  $f, g \in \mathbb{C}[x, y]$  tais que  $f(a, y)$  e  $g(a, y)$  possuem raízes em comum. Escrevemos  $u(y) = c_0y^{n-1} + \dots + c_{n-1}$  e  $v(y) = d_0y^{m-1} + \dots + d_{m-1}$ .

$$\text{Assim } uf = vg \Rightarrow \begin{cases} a_0c_0 = b_0d_0 \\ a_1c_0 + a_0c_1 = b_1d_0 + b_0d_1 \\ \vdots \\ \sum_{i=0}^{n-1} a_i c_{n-1-i} = \sum_{i=0}^{m-1} b_i d_{m-1-i} \end{cases}$$

Em forma matricial temos:

$$\begin{pmatrix} c_0 & \dots & c_{n-1} & -d_0 & \dots & -d_{m-1} \end{pmatrix} \begin{pmatrix} a_0 & a_1 & \dots & a_m & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_m & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_0 & \dots & a_m \\ b_0 & b_1 & \dots & b_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & b_0 & \dots & b_n \end{pmatrix} = 0_{1 \times (m+n)}.$$

Devido a existência de  $u$  e  $v$  temos uma solução não nula para esse sistema, o que é possível somente quando:

$$\det \begin{pmatrix} a_0 & a_1 & \dots & a_m & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_m & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_0 & \dots & a_m \\ b_0 & b_1 & \dots & b_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & b_0 & \dots & b_n \end{pmatrix} = 0.$$

**Definição 3.1.2** *Sejam  $f(y) = a_0y^m + \dots + a_m$  e  $g(y) = b_0y^n + \dots + b_n$  com  $m, n \geq 1$  dois polinômios com coeficientes em  $\mathbb{C}[x]$ . A resultante de  $f$  e  $g$  é:*

$$R_{f,g}(x) = \det \begin{pmatrix} a_0 & a_1 & \dots & a_m & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_m & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_0 & \dots & a_m \\ b_0 & b_1 & \dots & b_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & b_0 & \dots & b_n \end{pmatrix}.$$

Essa resultante é um polinômio na variável  $x$  e suas raízes representam os valores de  $x$  para  $f \cap g$ . Quando encontrado esses valores podemos substituí-los em  $f$  ou  $g$  para descobrir o valor de  $y$  e por fim chegar nas coordenadas dos pontos de interseção. Veja a seguir um exemplo desse cálculo.

**Exemplo 3.1.2** Sejam as curvas  $C$  e  $D$  geradas por  $f(x,y) = xy - 1$  e  $g(x,y) = y^2 + x^2 - 4$ , respectivamente, encontre os pontos de interseção.

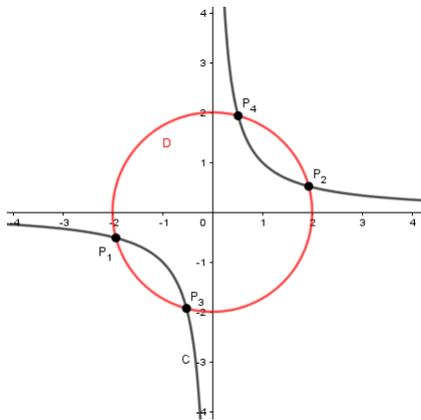
Escrevendo  $f, g$  como polinômios em  $y$ , temos:  $f(y) = xy - 1$  e  $g(y) = y^2 + 0y + x^2 - 4$ . Assim:

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

Calculando o determinante:  $R_{f,g}(x) = \det \begin{bmatrix} 1 & 0 & x^2 - 4 \\ x & -1 & 0 \\ 0 & x & -1 \end{bmatrix} = x^4 - 4x^2 + 1.$

As raízes dessa equação são:  $x_1 = -\sqrt{\sqrt{3}+2}$ ,  $x_2 = \sqrt{\sqrt{3}+2}$ ,  $x_3 = -\sqrt{2-\sqrt{3}}$ ,  $x_4 = \sqrt{2-\sqrt{3}}$ . Aproximadamente, temos:  $x_1 = -1.93$ ,  $x_2 = 1.93$ ,  $x_3 = -0.52$  e  $x_4 = 0.52$ . Substituindo esses valores em  $g(x,y) = 0$ , obtemos os pontos:  $P_1 = (-1.93, -0.52)$ ,  $P_2 = (1.93, 0.52)$ ,  $P_3 = (-0.52, -1.93)$ ,  $P_4 = (0.52, 1.93)$  representados no gráfico a seguir.

Figura 3.2 – Gráfico das curvas  $C$  e  $D$



Fonte: Do autor (2019).

**Definição 3.1.3** Um polinômio homogêneo é um polinômio onde os monômios com coeficientes não nulos têm o mesmo grau.

**Exemplo 3.1.3** Considere os polinômios  $f(x,y) = x^5 - 3x^2y^3 + 2xy^4$  e  $q(x,y) = 4x^3 + x^3 - 2$ . O polinômio  $f$  é homogêneo, pois todos os monômios tem grau 5, já o polinômio  $q$  não é homogêneo, pois o grau de cada monômio é diferente.

**Definição 3.1.4** Seja  $f \in \mathbb{C}[x, y] \setminus \mathbb{C}$  com  $f = f_0 + \dots + f_d$  onde cada  $f_i$  é homogêneo de grau  $i$  e  $f_d \neq 0$ . Cada componente  $ax + by$  de  $f_d$  é chamada de uma direção assintótica de  $f$ .

**Exemplo 3.1.4** Considere os polinômios  $p(x, y) = xy - 1$  e  $q(x, y) = y^2 - x$ . O polinômio  $p$  possui duas direções assintóticas dadas por  $x$  e  $y$ , já o polinômio  $q$  possui uma:  $y$ .

Para os próximos resultados vamos fazer uma breve construção. Sejam  $f, g$  dois polinômios podemos escrevê-los como  $f = \sum_{i=0}^n f_i$  e  $g = \sum_{j=0}^m g_j$ , com  $f_i$  homogêneo de grau  $i$ ,  $f_n \neq 0$  e  $g_j$  homogêneo de grau  $j$ ,  $g_m \neq 0$ . Escrevemos  $f^*(x, y, z) = z^n f_0 + z^{n-1} f_1 + \dots + z f^{n-1} + f_n$ , sendo  $z$  uma nova variável independente de  $x$  e  $y$ . Note que  $f^*$  é um polinômio homogêneo de grau  $n = \partial f$  e  $f^*(x, y, 1) = f(x, y)$ . De forma análoga, fazemos essa construção para  $g$ .

Reescrevemos  $f^*$  e  $g^*$  na forma  $f^*(y) = a_0 y^n + \dots + a_n$  e  $g^*(y) = b_0 y^m + \dots + b_m$ , onde  $a_i, b_j \in \mathbb{K}[x, z]$  são homogêneos com  $\partial a_i = i$  e  $\partial b_j = j$ . Calculando a resultante entre esses dois polinômios, temos:

$$R(x, z) = \det \begin{pmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_0 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & b_0 & \dots & b_m \end{pmatrix}.$$

**Lema 3.1.2** O polinômio  $R(x, z)$  dado pela resultante acima é homogêneo de grau  $nm$ , se não for identicamente nulo.

**Demonstração:** A demonstração desse Lema se encontra em (VAINSENER, 1996). □

**Proposição 3.1.2** O grau da resultante de duas curvas sem direção assintótica em comum é igual ao produto do grau das duas curvas, ou seja,  $\partial R_{f, g} = \partial f \partial g$ .

**Demonstração:**

Seguindo da construção e o lema feitos acima, vamos comparar  $R(x, z)$  com  $R(x)$  e sabemos que  $R(x, 1)$  é a resultante de  $f, g$  considerados polinômios na variável  $y$  de grau  $n, m$ . Note que  $a_0$  é constante em  $f^*$ , sendo nulo se, e somente se,  $y^d$  não ocorre em  $f_d$ , nesse caso  $x$  é um fator de  $f_d$ .

Como  $f, g$  não tem direções assintóticas em comum, segue-se que  $a_0 \neq 0$ . Seja  $j$  o menor índice tal que  $b_j \neq 0$ , desenvolvendo o determinante que define  $R(x, z)$  para  $j$  colunas, temos que  $R(x, 1) = a_0^j R(x)$ . Como  $f, g$  não tem componentes em comum,  $R(x) \neq 0$  e portanto  $R(x, z)$  também é diferente de zero. Então  $\partial R(x, z) = nm$ .  $\square$

**Teorema 3.1.3** (Teorema de Bézout, versão fraca) *Sejam  $C$  e  $D$  duas curvas algébricas definidas por  $f$  e  $g$  pertencentes a  $\mathbb{K}[x, y]$ , onde  $\partial f = m$  e  $\partial g = n$ . Suponha que  $C$  e  $D$  não têm componentes em comum, então  $C$  e  $D$  têm no máximo  $mn$  pontos de interseção, ou seja,*

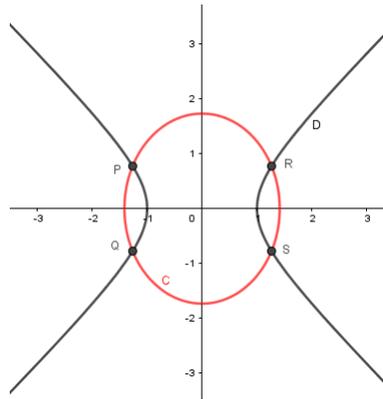
$$\#C \cap D \leq mn.$$

**Demonstração:**

Usando a Proposição 3.1.2 temos que  $\#C \cap D \leq mn$ .  $\square$

**Exemplo 3.1.5** *Sejam  $f(x, y) = \frac{x^2}{2} + \frac{y^2}{3} - 1$  e  $g(x, y) = x^2 - y^2 - 1$  polinômios em  $\mathbb{R}[x, y]$  que geram as curvas algébricas  $C$  e  $D$ , respectivamente. Note que  $\partial f = 2$  e  $\partial g = 2$ . Assim as curvas  $C$  e  $D$  podem ter no máximo quatro interseções como mostra a Figura 3.3.*

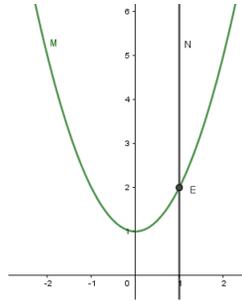
Figura 3.3 – Gráfico das curvas  $C$  e  $D$



Fonte: Do autor (2019).

**Exemplo 3.1.6** *Sejam  $M$  e  $N$  curvas algébricas geradas pelos polinômios  $h(x, y) = x^2 + 1 - y$  e  $p(x, y) = x - 1$  pertencentes a  $\mathbb{R}[x, y]$ . Note que  $\partial h = 2$  e  $\partial p = 1$ . Assim as curvas  $M$  e  $N$  podem ter no máximo duas interseções. Podemos verificar através da figura 3.4 que apresenta apenas uma interseção.*

Os Exemplos 3.1.5 e 3.1.6 são fundamentais para continuar o estudo da interseção entre duas curvas, pois podemos notar que um deles atingiu a cota máxima dada pelo Teorema de Bézout, já no outro esse fato não acontece.

Figura 3.4 – Gráfico das curvas  $M$  e  $N$ 

Fonte: Do autor (2019).

### 3.2 Aplicações

Nessa seção apresentaremos algumas aplicações do Teorema de Bézout, sendo Proposições e Teoremas cuja demonstração necessitam do auxílio do Teorema de Bézout. Para essas aplicações usamos como referência (LEIMANN, 2003) e (VAINSENER, 1996).

**Definição 3.2.1** Uma *cônica no plano* é definida como o conjunto dos pontos  $P_i = (x_i, y_i)$  que satisfazem a equação  $ax^2 + bxy + cy^2 + dx + ey + f = 0$ , onde  $a, b, c, d, e, f$  são números reais, com  $a, b, c$  não simultaneamente nulos.

**Proposição 3.2.1** Sejam  $P_1, P_2, P_3, P_4, P_5$  cinco pontos distintos em posição geral no plano. Então existe no máximo uma cônica passando por todos eles.

#### Demonstração:

Sejam  $C_1 \neq C_2$  duas cônicas tais que  $\{P_1, P_2, P_3, P_4, P_5\} \subseteq C_1 \cap C_2$ . Pelo Teorema de Bézout  $C_1$  e  $C_2$  apresentam componentes em comum. Assim  $C_1 = L \cap L_1$  e

$C_2 = L \cap L_2$ , onde  $L, L_1, L_2$  são retas. Logo  $C_1 \cap C_2 = L \cup (L_1 \cap L_2)$ , o que implica em  $\{P_1, P_2, P_3, P_4, P_5\} \subset L$ .

Absurdo, pois os pontos estão em posição geral. Portanto existe no máximo uma cônica contendo esses pontos.  $\square$

Podemos trabalhar com um exemplo dessa aplicação, onde dados cinco pontos em posição geral vamos descobrir qual a cônica que passa por todos.

**Exemplo 3.2.1** Sejam os pontos  $P_1 = (1, 0), P_2 = (2, 0), P_3 = (0, 1), P_4 = (0, 2)$  e  $P_5 = (-1, -1)$ . Considere um curva  $C$  gerada pelo polinômio  $f(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$ , nosso objetivo é encontrar os coeficientes de  $f$  tal que  $P_1, P_2, P_3, P_4, P_5 \in C$ .

Por hipótese temos  $P_1, P_2, P_3, P_4, P_5 \in C$ , então se aplicarmos esses pontos em  $f$  temos  $f(x, y) = 0$ ,

assim temos o seguinte sistema:

$$\left\{ \begin{array}{l} a + d + f = 0 \\ 4a + 2d + f = 0 \\ c + e + f = 0 \\ 4c + 2e + f = 0 \\ a + b + c - d - e + f = 0 \end{array} \right. \sim \left\{ \begin{array}{l} a + b + c - d - e + f = 0 \\ a + d + f = 0 \\ 4a + 2d + f = 0 \\ c + e + f = 0 \\ 4c + 2e + f = 0. \end{array} \right.$$

Agora faremos duas operações ( $3^{\text{a}} \text{ linha} - 4 \times 2^{\text{a}} \text{ linha} \rightarrow 3^{\text{a}} \text{ linha}$ ) e ( $5^{\text{a}} \text{ linha} - 4 \times 4^{\text{a}} \text{ linha} \rightarrow 5^{\text{a}} \text{ linha}$ ), ficando:

$$\left\{ \begin{array}{l} a + b + c - d - e + f = 0 \\ a + d + f = 0 \\ -2d - 3f = 0 \\ c + e + f = 0 \\ -2e - 3f = 0. \end{array} \right.$$

Isolando “ $d$ ” na  $3^{\text{a}}$  linha obtemos  $d = \frac{-3f}{2}$  e substituindo na  $2^{\text{a}}$  linha temos  $a = \frac{f}{2}$ . Na  $5^{\text{a}}$  linha podemos isolar “ $e$ ” tendo  $e = \frac{-3f}{2}$  e fazendo a substituição na  $4^{\text{a}}$  linha  $c = \frac{f}{2}$ . Logo  $a = c = \frac{f}{2}$  e  $d = e = \frac{-3f}{2}$ , substituindo esses valores na primeira linha obtemos  $b = -5f$ . Assim todos os coeficientes estão em função de  $f$ , então considerando  $f = 2$ , temos  $a = c = 1$ ,  $b = -10$  e  $d = e = -3$ . Portanto a equação do polinômio é  $f(x, y) = x^2 - 10xy + y^2 - 3x - 3y + 2$  e podemos ver na Figura 3.5 que os cinco pontos pertencem à curva gerada, uma hipérbole.

**Definição 3.2.2** Seja  $C$  uma curva definida por  $f \in \mathbb{K}[x, y]$ . Um ponto  $P \in C$  é chamado de um ponto singular de  $C$ , se  $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$ .

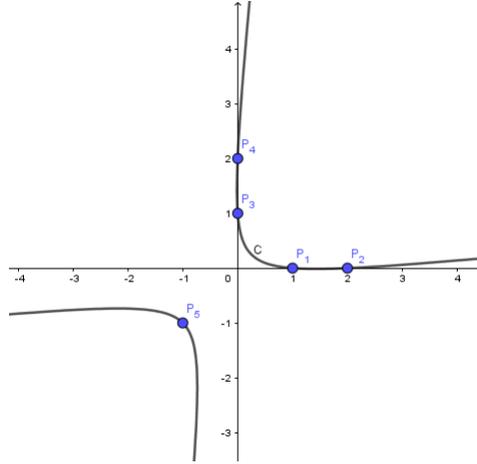
**Observação 3.2.1** O conjunto de todos os pontos singulares de  $C$  é denotado por  $\text{Sing}(C)$ .

**Exemplo 3.2.2** Seja o polinômio  $f(x, y) = x^2 + 2y^2 + 4xy + 4x + 1$  e o ponto  $P = (2, 3)$ , vamos verificar se esse ponto é singular.

Primeiro calculamos as derivadas parciais de  $f$ , assim  $\frac{\partial f}{\partial x}(x, y) = 2x + 4y + 4$  e  $\frac{\partial f}{\partial y}(x, y) = 4y + 4x$ .

Calculando em  $P$  temos  $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 20$ . Podemos afirmar que elas são iguais, mas são diferente de 0, logo  $P$  não é um ponto singular de  $f$ .

Figura 3.5 – Curva C - Aplicação 1 do Teorema de Bézout



Fonte: Do autor (2019).

**Proposição 3.2.2** *Seja  $C$  um curva algébrica. Então  $Sing(C)$  é finito.*

**Demonstração:**

Seja  $f$  o polinômio minimal que gera a curva  $C$ ,  $C_1 = \{P \in C, \frac{\partial f}{\partial x}(P) = 0\}$  e  $C_2 = \{P \in C, \frac{\partial f}{\partial y}(P) = 0\}$ .

Então  $Sing(C) = C \cap C_1 \cap C_2$ . Como uma reta não possui pontos singulares, então  $\partial f \geq 2$  o que implica em  $\frac{\partial f}{\partial x}(x,y) \geq 1$  ou  $\frac{\partial f}{\partial y}(x,y) \geq 1$ .

Suponha  $\frac{\partial f}{\partial x}(x,y) \geq 1$ , então  $C_1$  é uma curva algébrica e sabemos que  $Sing(C) \subset C \cap C_1$ , basta mostrar que  $C \cap C_1$  é finito. Pelo Teorema de Bézout é suficiente mostrar que  $C$  e  $C_1$  possuem componentes em comum.

Seja  $g$  um fator primo comum de  $f$  e  $\frac{\partial f}{\partial x}$ . Então  $f = gh$  e  $\frac{\partial f}{\partial x} = gh_1$ . Derivando  $f = gh$  em relação a  $x$  temos  $\frac{\partial f}{\partial x} = g \frac{\partial h}{\partial x} + h \frac{\partial g}{\partial x}$ , substituindo  $\frac{\partial f}{\partial x}$  por  $gh_1$  e colocando  $g$  em evidência ficamos com  $g(h_1 - \frac{\partial h}{\partial x}) = h \frac{\partial g}{\partial x}$ , portanto  $g$  divide  $h \frac{\partial g}{\partial x}$ .

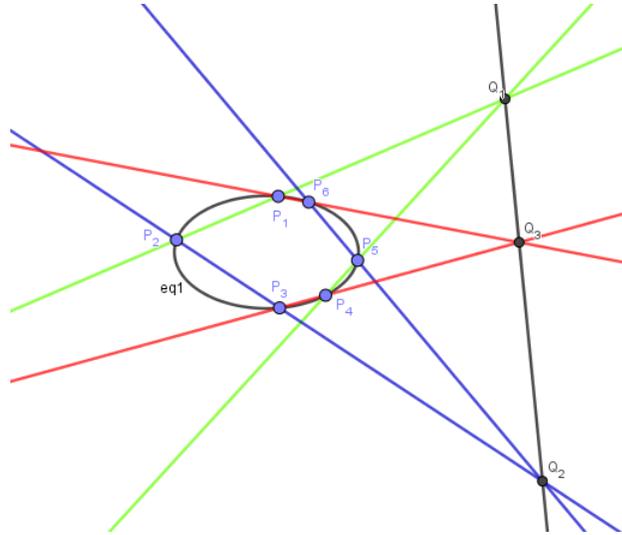
Se  $\frac{\partial g}{\partial x} \neq 0$  então  $g|h$  logo  $g^2|f$  que é absurdo, pois  $f$  é polinômio minimal. Se  $\frac{\partial g}{\partial x} = 0$ , então  $g = y + a$ . Isto é  $C$  possui uma reta paralela ao eixo dos  $x$ . Fazendo uma mudança de coordenadas podemos supor que  $C$  não possui nenhuma reta paralela ao eixos. Portanto pelo Teorema de Bézout,  $Sing(C)$  é finito.

□

Na demonstração dos Teorema 3.2.1 e do Teorema 3.2.2 a seguir usaremos a notação  $M_{h_i}$  para representar o conjunto  $\{(a,b) \in \mathbb{R}, h_i(a,b) = 0\}$ .

**Teorema 3.2.1 (Teorema do Hexágono de Pascal)** Sejam  $\{P_1, P_2, P_3, P_4, P_5, P_6\}$  seis pontos distintos em  $\mathbb{R}^2$  sobre uma cônica irreduzível  $C$ . Se as retas  $P_1P_2$  e  $P_4P_5$  se intersectam em  $Q_1$ , se as retas  $P_2P_3$  e  $P_5P_6$  se intersectam em  $Q_2$  e se as retas  $P_3P_4$  e  $P_6P_1$  se intersectam em  $Q_3$ , então os pontos  $Q_1, Q_2, Q_3$  são colineares.

Figura 3.6 – Teorema do Hexágono de Pascal



Fonte: Do autor (2019).

**Demonstração:**

Sejam  $L_i$  a reta  $P_iP_{i+1}$  com  $i = 1, \dots, 6$  onde  $P_1 = P_7$  e  $l_i(x, y)$  a equação da reta passando pelos pontos  $P_i$  e  $P_{i+1}$ . Escolhe-se um ponto  $A$  sobre  $C$  diferente de  $P_1, P_2, P_3, P_4, P_5, P_6$  com coordenadas  $(\alpha, \beta)$ .

**Afirmção:**  $A \notin L_i$  para todo  $i = 1, \dots, 6$ .

Se  $A \in L_i$ , contradiz o Teorema de Bézout, pois  $\partial L_i = 1$  e  $\partial C = 2$ .

Considere o polinômio  $g(x, y) = l_1l_3l_5 + ul_2l_4l_6$  com  $u \in \mathbb{R}^*$ .

**Afirmção:**  $\partial g = 3$ .

Sabemos que  $\partial g \leq \max \{l_1 + l_3 + l_5, l_2 + l_4 + l_6\}$ . Por outro lado os pontos  $P_1, P_2, Q_1$  estão sobre a curva  $M_g$  determinada por  $g$  e também sobre a reta  $L_1$ . Logo pelo Teorema de Bézout  $\partial g \geq 3$  ou  $l_1$  divide  $g$ .

Se  $l_1$  divide  $g$  então  $l_1$  divide  $ul_2l_4l_6$ . Absurdo, pois  $\mathbb{R}[x, y]$  é um domínio fatorial. Logo  $\partial g = 3$ .

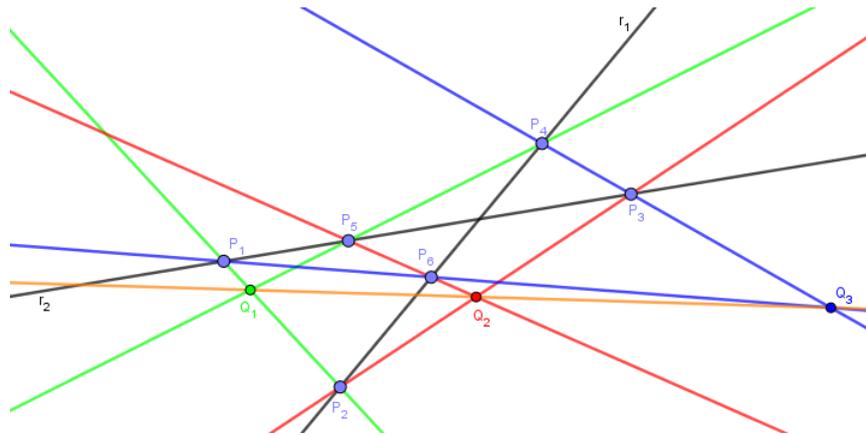
Agora tome  $u$  de maneira que  $A \in M_g$ , ou seja,  $u = \frac{-l_1(\alpha, \beta)l_3(\alpha, \beta)l_5(\alpha, \beta)}{l_2(\alpha, \beta)l_4(\alpha, \beta)l_6(\alpha, \beta)}$ . Note que  $u \in \mathbb{R}^*$  pois  $A \notin L_i$  para todo  $i = 1, \dots, 6$ . Assim  $P_1, P_2, P_3, P_4, P_5, P_6$  e  $A \in C \cap M_g$ . Denote a equação da cônica irreduzível  $C$  por  $f(x, y)$ . Pelo Teorema de Bézout  $\partial g = 3$  e  $\partial f = 2$ , mas existe sete pontos na interseção entre essas duas curvas, logo  $f|g$  então existe  $h(x, y)$  de grau 1 tal que  $g = fh$  o que implica em  $M_g = M_f \cup M_h$ .

**Afirmção:**  $Q_1, Q_2, Q_3$  são colineares ( $Q_1, Q_2, Q_3 \in M_h$ ).

Como  $Q_1, Q_2, Q_3 \in M_g$  basta mostrar que  $Q_1, Q_2, Q_3 \notin M_f = C$ . Suponha que  $Q_1 \in C$ , então  $P_1, P_2, P_4, P_5, Q_1 \in M_{l_1 l_4} \cup C$  contradizendo o Teorema de Bézout, pois  $\partial M_{l_1 l_4} = 2$  e  $\partial C = 2$ . De forma análoga podemos supor  $Q_2, Q_3 \in C$ . Portanto  $Q_1, Q_2, Q_3$  são colineares.  $\square$

**Teorema 3.2.2 (Teorema de Pappus)** *Sejam  $r_1$  e  $r_2$  duas retas concorrentes (pretas),  $P_1, P_3, P_5$  pontos distintos sobre  $r_1$  e  $P_2, P_4, P_6$  pontos distintos sobre  $r_2$ . Se as retas  $P_1 P_2$  e  $P_4 P_5$  (verde) se intersectam em  $Q_1$ , se as retas  $P_2 P_3$  e  $P_5 P_6$  (vermelho) se intersectam em  $Q_2$  e se as retas  $P_3 P_4$  e  $P_6 P_1$  (azul) se intersectam em  $Q_3$ , então  $Q_1, Q_2, Q_3$  são colineares.*

Figura 3.7 – Teorema de Pappus



Fonte: Do autor (2019).

### Demonstração:

Sejam  $h_1(x, y)$  a equação de  $r_1$  e  $h_2(x, y)$  a equação de  $r_2$ ,  $L_i$  a reta  $P_i P_{i+1}$  com  $i = 1, \dots, 6$  onde  $P_1 = P_7$  e  $l_i(x, y)$  a equação da reta  $L_i$ . Considere  $A = (\alpha, \beta)$  a interseção de  $r_1$  e  $r_2$  com  $A \neq P_i$  para todo  $i$ . Note que  $A \notin L_1$ , pois se  $A \in L_1$  então teria dois pontos na interseção entre  $L_1$  e  $r_1$ , o que contradiz o Teorema de Bézout. Analogamente,  $A \notin L_i \forall i = 2, \dots, 6$ .

Considere o polinômio  $g(x, y) = l_1 l_3 l_5 + u l_2 l_4 l_6$  com  $u \in \mathbb{R}^*$ .

**Afirmação:**  $\partial g = 3$ .

Note que  $\partial l_i = 1$  para todo  $i = 1, \dots, 6$ , então pela propriedade de grau do produto de polinômios  $\partial g \leq 3$ . Por outro lado  $P_1, P_2, Q_1 \in M_g$  determinada por  $g$  e  $P_1, P_2, Q_1 \in L_1$ . Logo pelo Teorema de Bézout  $\partial g \geq 3$  ou  $l_1$  divide  $g$ . Suponha  $l_1 | g$ , então  $l_1 | u l_2 l_4 l_6$  o que seria absurdo, pois  $\mathbb{R}[x, y]$  é um domínio fatorial. Logo  $\partial g = 3$ .

Agora tome  $u$  de maneira que  $A \in M_g$ , ou seja,  $u = \frac{-l_1(\alpha, \beta)l_3(\alpha, \beta)l_5(\alpha, \beta)}{l_2(\alpha, \beta)l_4(\alpha, \beta)l_6(\alpha, \beta)}$ . Note que  $u \in \mathbb{R}^*$ , pois  $A \notin L_i$  para todo  $i = 1, \dots, 6$ . Assim  $P_1, P_2, P_3, P_4, P_5, P_6, A$  pertencem a  $(r_1 \cap M_g) \cup (r_2 \cap M_g)$ . Como  $P_1, P_3, P_5, A \in M_g$  e por hipótese  $P_1, P_3, P_5, A$  pertencem a  $h_1(x, y)$ , segue pelo Teorema de Bézout que:  $h_1(x, y) | g(x, y)$  implica  $g(x, y) = h_1(x, y)h(x, y)$ , com  $\partial h(x, y) = 1$ .

De forma análoga  $P_2, P_4, P_6, A \in M_g$  e por hipótese temos que  $A, P_2, P_4, P_6 \in h_2(x, y)$ , logo pelo Teorema de Bézout,  $h_2(x, y) | g(x, y)$  implica  $g(x, y) = h_4(x, y)h(x, y)$ , com  $\partial h_4(x, y) = 1$ . Então  $g(x, y) = h_2(x, y)h_4(x, y) = h_1(x, y)h(x, y)$  o que implica em  $h_1(x, y) = ch_2(x, y)$ , onde  $c$  é uma constante não nula, ou  $h_1(x, y)$  divide  $h_4(x, y)$ . Se ocorresse  $h_1(x, y) = ch_2(x, y)$  então  $r_1 = r_2$  contrariando a hipótese, portanto  $g(x, y) = h_1(x, y)h_2(x, y)h_3(x, y)$ , onde  $h_3(x, y)$  tem grau um e portanto  $M_g = M_{h_1} \cup M_{h_2} \cup M_{h_3}$ .  $\square$

### 3.3 Multiplicidades

#### 3.3.1 Interseção de uma curva com uma reta

Nessa subseção vamos definir o que é multiplicidade de uma reta com uma curva e qual a sua importância no estudo de interseções entre curvas. Para isso começamos estudando sobre uma curva qualquer e uma reta.

Sejam  $C$  uma curva definida por  $f \in \mathbb{K}[x, y]$  e  $L$  uma reta de equação  $y = ax + b$ . Os pontos de  $C \cap L$  podem ser obtidos eliminando  $y$  e resolvendo a equação  $f_L(x) := f(x, ax + b) = 0$ . Nesse caso, podemos ter as seguintes possibilidades:

- $f_L(x)$  é identicamente nulo, caso em que  $L$  é uma componente de  $C$ .
- $f_L(x)$  é uma constante diferente de 0, quando  $C \cap L = \emptyset$ .
- $f_L(x)$  é um polinômio não constante, decompondo-se na forma:  
 $f_L(x) = c \prod (x - x_i)^{m_i}$ , onde  $c$  é uma constante e os  $x_i$  são as abscissas (duas a duas distintas) dos pontos de interseção.

**Lema 3.3.1** *Os inteiros  $m_i$  independem do referencial afim.*

**Demonstração:** Demonstração no livro (VAINSENER, 1996).  $\square$

**Definição 3.3.1** Sejam  $C$  uma curva e  $L$  uma reta, a Multiplicidade de  $L, C$  no ponto  $P$  é dada por:

$$(L, C)_P = \begin{cases} 0, & \text{se } P \notin L \cap C, \\ \infty, & \text{se } P \in L \subset C, \\ m_i, & \text{se } P = (x_i, ax_i + b). \end{cases}$$

Se  $L \subset C$ , chamamos o inteiro  $m_\infty = \partial C - \sum_{i=1}^r m_i$  de multiplicidade no ponto infinito de  $L$ . O significado dessa multiplicidade é que próximo à curva  $C$ , existem curvas do mesmo grau que cortam  $L$  em  $\partial C$  pontos distintos.

**Exemplo 3.3.1** Sejam a curva  $C$  gerada pelo polinômio  $f(x, y) = y - x^2$  e duas retas  $L_1$  e  $L_2$  com equações  $l_1(x, y) = y - 2x + 1$  e  $l_2(x, y) = y - x - 2$ .

Escrevendo as equações das retas na forma  $y = 2x - 1$  e  $y = x + 2$ , podemos calcular  $f_{l_1}(x)$  e  $f_{l_2}(x)$ . Então:  $f_{l_1}(x) = f(x, 2x - 1) = 2x - 1 - x^2 = -1(x - 1)^2$ . Nesse caso a multiplicidade no ponto  $P = (1, 1)$  é dois.

$f_{l_2}(x) = f(x, x + 2) = x + 2 - x^2 = -1(x - 2)(x + 1)$ . Nesse exemplo temos dois pontos de interseção  $P_1 = (-1, 1)$  e  $P_2 = (2, 4)$ , nos dois casos a multiplicidade é um.

### 3.3.2 Pontos múltiplos

**Proposição 3.3.1** Sejam  $C$  uma curva gerada por  $f$  e  $P$  um ponto de  $C$ . Existe um inteiro  $m = m_p(f) \geq 1$  tal que para toda reta  $L$  contendo  $P$ , temos que  $(L, C)_P \geq m$ , ocorrendo a desigualdade estrita para no máximo  $m$  retas e no mínimo uma.

#### Demonstração:

Demonstração no livro (VAINSENER, 1996). □

**Definição 3.3.2** O inteiro  $m = m_p(f)$  descrito na proposição 3.3.1 é a multiplicidade do ponto  $P$  na curva  $C$ . Se  $P \notin C$  convencionamos  $m_p(f) = 0$ . Se  $P = (a, b) \in C$  escrevemos  $f(x + a, y + b) = f_m(x, y) + (\text{termos de grau maior que } m)$ .

O polinômio homogêneo  $f_m(x, y)$  pode ser decomposto da forma

$$\prod (a_i x + b_i y)^{m_i},$$

onde cada  $(a_i x + b_i y)$  são retas distintas. As retas  $l_i = a_i(x - a) + b_i(y - b)$  são retas tangentes a  $f$  em  $P$  e

o expoente  $m_i$  é a multiplicidade da tangente. Na Proposição 3.3.1 tem-se que  $(L, C)_P \geq m = m_P(f)$  para  $L$  sendo uma reta tangente a  $C$  no ponto  $P$ .

Definimos que uma curva  $C$  é lisa em  $P$  se  $m_P(f) = 1$ , se  $m_P(f) \neq 1$  dizemos que é singular. Se  $m_P(f) = 2, 3, \dots, m$ ,  $P$  é dito ponto duplo, triplo,  $\dots$ ,  $m$ -uplo. Um ponto é ordinário se  $f$  admitir  $m$  tangentes diferentes em  $P$ . Temos uma cúspide quando  $P$  é um ponto duplo com tangentes coincidentes e um nó quando temos um ponto duplo ordinário.

**Proposição 3.3.2** *Temos duas consequências da definição de ponto liso:*

- *Um ponto  $P \in C$  é liso se, e somente se, uma das derivadas parciais  $f_x, f_y$  não se anula em  $P$ .*
- *Se  $P = (a, b) \in C$  é liso então a única tangente a  $C$  em  $P$  é dada por  $f_x(P)(x - a) + f_y(P)(y - b) = 0$ .*

**Demonstração:** Consequência direta da fórmula de Taylor de uma função  $f$  dada por:  $f(x + a, y + b) = f(a, b) + f_x(a, b)x + f_y(a, b)y + g(x, y)$  onde todos os termo de  $g$  têm grau maior ou igual a 2.  $\square$

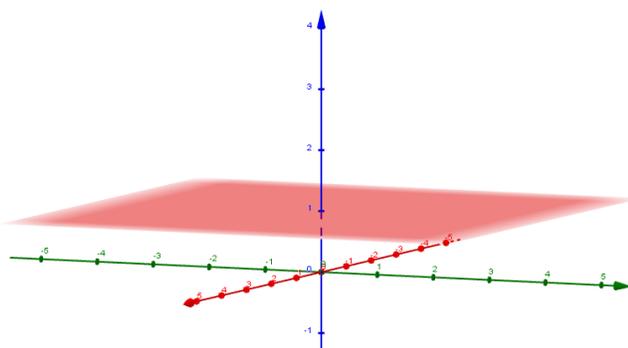
## 4 PLANO PROJETIVO E PONTOS NO INFINITO

Podemos analisar o gráfico de duas retas paralelas e afirmar que não existe interseção entre elas. Pelo Teorema 3.1.3 sabemos que duas retas paralelas podem ter no máximo uma interseção. Então para dar um significado para essa interseção que está faltando vamos estudar sobre os pontos no infinito.

### 4.1 Pontos no infinito

Vamos considerar um plano  $\pi$  no espaço tridimensional  $\mathbb{R}^3$  de equação  $z = 1$ , como representado na figura 4.1.

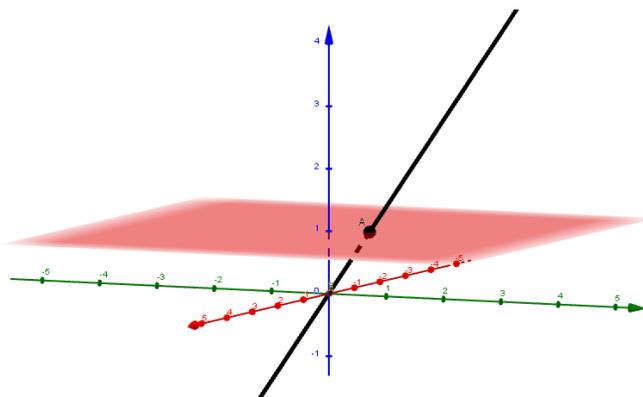
Figura 4.1 – Plano  $\pi$



Fonte: Do autor (2019).

Cada ponto desse plano determina uma reta que passa pela origem e por um ponto dado, como mostrado na figura 4.2.

Figura 4.2 – Ponto de  $\mathbb{P}^2$



Fonte: Do autor (2019).

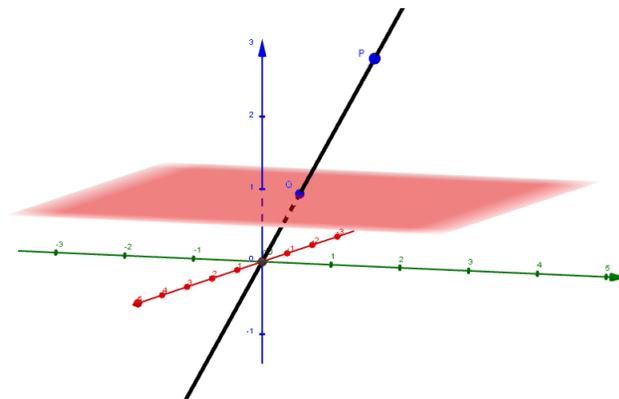
Cada reta de  $\pi$  determina um plano passando pela origem. Dado duas retas  $l, l'$  pertencentes a  $\pi$ , se elas se intersectam, seu ponto de interseção dá origem à reta de interseção dos dois planos associados à  $l, l'$ . Se  $l \cap l' = \emptyset$ , os planos que elas definem ainda se intersectam e definem uma reta contida no plano  $z = 0$  que passa pela origem.

**Definição 4.1.1** O Plano Projetivo denotado por  $\mathbb{P}^2$  é o conjunto das retas no espaço tridimensional passando pela origem.

Pela figura 4.1 podemos afirmar que  $\pi$  é um subconjunto de  $\mathbb{P}^2$ . Os pontos de  $\mathbb{P}^2 - \pi$  serão chamados de pontos no infinito. Denotaremos por  $(x : y : z)$  um ponto de  $\mathbb{P}^2$  que representa a reta ligando a origem ao ponto  $(x, y, z) \neq 0$ . Dizemos que  $x, y, z$  são coordenadas homogêneas do ponto  $(x : y : z)$  relativas à base canônica  $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ .

Podemos definir  $(x : y : z) = (x' : y' : z')$  se, e somente se, existir uma constante  $t$  diferente de zero tal que  $(x, y, z) = t(x', y', z')$ . Essa definição nos diz que dado um ponto não pertencente ao plano  $z = 0$  existe sempre um representante desse ponto no plano  $z = 1$ . A figura 4.3 mostra que o ponto  $P$  tem um representante  $Q$  pertencente ao plano  $\pi$ .

Figura 4.3 – Relação de igualdade entre dois pontos de  $\mathbb{P}^2$



Fonte: Do autor (2019).

**Exemplo 4.1.1** Vamos analisar se os pontos  $P_1 = (2 : 3 : 0)$  e  $P_2 = (10 : 4 : 2)$  pertencentes a  $\mathbb{P}^2$  são pontos no infinito. Observe que o ponto  $P_1$  não pertence ao plano  $z = 1$ , logo ele é um ponto no infinito. O ponto  $P_2 = (10 : 4 : 2)$  é igual a  $(5 : 2 : 1)$  pois  $(10, 4, 2) = 2(5, 2, 1)$ , assim existe um representante de  $P_2$  no plano  $z = 1$ , portanto  $P_2$  não é um ponto no infinito.

Vamos considerar a aplicação  $q : \mathbb{R}^3 - \{0\} \rightarrow \mathbb{P}^2$  definida por  $q(x, y, z) \mapsto (x : y : z)$  para introduzir a topologia quociente em  $\mathbb{P}^2$ . Um conjunto  $U \subset \mathbb{P}^2$  é aberto se  $q^{-1}(U)$  é aberto em  $\mathbb{R}^3 - \{0\}$  com sua topologia usual de  $\mathbb{R}^3$ . Essa definição estabelece uma vizinhança em  $\mathbb{P}^2$ , ou seja, se duas retas formam um ângulo pequeno entre elas então os dois pontos em  $\mathbb{P}^2$  associados a essas retas são considerados próximos.

O conjunto  $\mathbb{A}^2 = \{(x : y : z) / z \neq 0\}$  contido em  $\mathbb{P}^2$  é aberto e denso em  $\mathbb{P}^2$ , pois  $q^{-1}(\mathbb{A}^2)$  é todo o  $\mathbb{R}^3$  exceto o plano  $z = 0$  e podemos afirmar que é aberto e denso em  $\mathbb{R}^3 - \{0\}$ .

Vamos mostrar que a aplicação

$$\begin{aligned} \varphi : \mathbb{R}^2 &\rightarrow \mathbb{A}^2 \subset \mathbb{P}^2 \\ (x, y) &\mapsto (x : y : 1) \end{aligned}$$

é uma bijeção. Primeiro mostraremos que  $\varphi$  é injetora. Seja  $(a, b) \neq (a', b') \in \mathbb{R}^2$ , assim  $\varphi(a, b) = (a : b : 1)$  e  $\varphi(a', b') = (a' : b' : 1)$ . Para  $(a : b : 1)$  ser igual a  $(a' : b' : 1)$  deve existir um  $t \neq 0$  tal que  $(a, b, 1) = t(a', b', 1)$ , ou seja,  $(a, b, 1) = (ta', tb', t)$ . Se  $t = 1$  temos que  $(a, b, 1) = (a', b', 1)$  o que é absurdo, pois  $(a, b) \neq (a', b')$ . Se  $t \neq 1$   $(a, b, 1) \neq (ta', tb', t)$ . Logo a aplicação é injetora.

Agora mostraremos que  $\varphi$  é sobrejetora. Seja  $(x : y : 1) \in \mathbb{A}^2$  então  $z \neq 0$ . Considere  $(\frac{x}{z}, \frac{y}{z}) \in \mathbb{R}^2$ ,  $\varphi(\frac{x}{z}, \frac{y}{z}) = (\frac{x}{z} : \frac{y}{z} : 1)$ . Podemos afirmar que  $(x : y : z) = (\frac{x}{z} : \frac{y}{z} : 1)$  pois tomado  $t = z$  então  $(x, y, z) = z(\frac{x}{z}, \frac{y}{z}, 1)$ . Logo todo elemento do contradomínio está na imagem. Portanto, a aplicação  $\varphi$  é bijeção. Desta forma podemos considerar o plano  $\mathbb{R}^2$  como contido em  $\mathbb{P}^2$ .

## 4.2 Curvas Projetivas

**Proposição 4.2.1** *Sejam  $l = ax + by + c$  (com  $a \neq 0$  ou  $b \neq 0$ ) e  $\bar{l}$  a aderência de  $l$  em  $\mathbb{P}^2$ . Então temos:  $\bar{l} = l \cup \{(b : -a : 0)\} = \{(x : y : z) / ax + by + cz = 0\}$ .*

### Demonstração:

A demonstração está no livro (VAINSENER, 1996). □

**Definição 4.2.1** *Seja  $f = \sum_{i=0}^d f_i$ , onde cada  $f_i \in \mathbb{K}[x, y]$  é homogêneo de grau  $i$ , com  $f_d \neq 0$ . A homogeneização de  $f$  é o polinômio  $f^*$  homogêneo de grau  $d = \partial f$  da forma  $f^*(x, y, z) = \sum_{i=0}^d z^{d-i} f_i(x, y)$ .*

**Exemplo 4.2.1** *Considere os polinômios  $f(x, y) = y - 2x^2 + 3$  e  $g(x, y) = y^3 + x - 1$  vamos calcular sua homogeneização.*

*O polinômio  $f$  homogeneizado é igual a  $f^*(x, y, z) = yz - 2x^2 + 3z^2$  e o polinômio  $g$  homogeneizado é  $g^*(x, y, z) = y^3 + xz^2 - z^3$ .*

**Definição 4.2.2** Uma curva plana projetiva é uma classe de equivalência de polinômios homogêneos não constantes,  $f \in \mathbb{K}[x, y, z]$  módulo a relação que identifica dois tais polinômios  $f, g$  se um for múltiplo constante do outro.

De forma análoga ao Capítulo 3, podemos definir traço, equação, componente irredutível e grau para curvas planas projetivas.

Se  $f$  é um polinômio homogêneo, a relação  $f(tx, ty, tz) = t^{\deg f} f(x, y, z)$  mostra que a condição para que um ponto  $(x : y : z)$  pertença ao traço de uma curva projetiva é independente das coordenadas homogêneas.

Olhando em  $\mathbb{P}^2$  a reta projetiva  $z = 0$  é usualmente chamada de reta no infinito. Mudando a base de  $\mathbb{R}^3$  podemos decretar que qualquer reta de  $\mathbb{P}^2$  previamente estipulada seja a reta no infinito. Seu complementar ( $z \neq 0$ ) é o plano  $\mathbb{A}^2$ , cujos pontos são ditos estarem a distância finita  $\bar{l}$ . O fecho projetivo de uma curva afim  $f$  é a curva projetiva definida pela homogeneização  $f^*$ .

Os pontos a distância finita sobre uma curva  $C$  gerada pelo polinômio  $f$  são dados pela equação  $f(X, Y, 1) = 0$ . O polinômio no primeiro membro desta equação é a desomogeneização de  $f$  com respeito a  $Z$ , denotado por  $f_*$ .

**Exemplo 4.2.2** Considere duas curvas definidas pelos polinômios  $f(x, y) = x^2 - y$  e  $g(x, y) = x - 1$  vamos encontrar suas interseções em  $\mathbb{P}^2$ .

Homogeneizando esses polinômios temos  $F(X, Y, Z) = f^*(X, Y, Z) = X^2 - YZ$  e  $G(X, Y, Z) = g^*(X, Y, Z) = X - Z$ . Igualando as duas funções a zero damos origem às curvas, e pela segunda equação ficamos com  $X = Z$ . Substituindo na primeira equação temos  $X^2 - YX = X(X - Y) = 0$ . Logo se  $X - Y = 0$  temos que  $X = Y = Z$  e fazendo  $X = 1$  obtemos o ponto  $P_1 = (1 : 1 : 1)$ . Se  $X = 0$  implica que  $Z = 0$ , obtendo o ponto  $P_2 = (0, Y, 0)$ . Podemos considerar  $Y = 1$  assim temos o ponto  $P_2 = (0 : 1 : 0)$ . Note que o ponto  $P_1$  está a uma distância finita e o ponto  $P_2$  é o ponto no infinito.

### 4.3 Interseção entre Curvas Projetivas

Na seção anterior podemos ver que, duas curvas, quando olhadas no plano  $\mathbb{P}^2$  sempre se intersectam. Agora veremos que para duas curvas projetivas encontraremos o número exato de interseções entre elas. Para esse estudo começaremos olhando a interseção entre uma reta e uma curva.

Sejam  $L$  uma reta e  $C = \{f = 0\}$  um curva de grau  $d$ . Suponhamos  $L = \{X = 0\}$  então um ponto  $P = (0 : a : b)$  pertence a  $L \cap C$  se, e somente se,  $f(0, a, b) = 0$ . Assim ou o polinômio  $F(0, Y, Z)$  é nulo, caso

onde  $L \subset C$  ou é um polinômio homogêneo de grau  $d$  que pode ser decomposto da seguinte forma:

$$f(0, Y, Z) = \prod (a_i Y - b_i Z)^{m_i},$$

onde  $P_i = (0 : a_i : b_i)$  são dois a dois distintos e pertencem a  $L \cap C$ . O expoente  $m_i$  é chamado de multiplicidade de interseção de  $L, C$  no ponto  $P_i$ . Essas multiplicidades coincidem com as definidas na seção 3.3.

**Definição 4.3.1** A aplicação  $T : \mathbb{P}^2 \rightarrow \mathbb{P}^2$  é chamada de projetividade ou mudança projetiva de coordenadas em  $\mathbb{P}^2$ , tal que para  $T_\bullet f(x, y, z) = f(t^{-1}(x, y, z))$ .

**Proposição 4.3.1** Sejam  $L$  uma reta e  $C$  uma curva com grau  $d$ . Se  $L \not\subset C$  então  $L \cap C = \{P_1, \dots, P_r\}$  onde  $P_i \neq P_j$  se  $i \neq j$  e existem inteiros  $m \geq 1$  bem determinados pela seguinte condição: se  $T$  é uma projetividade tal que  $T_\bullet L = X$  então  $(T_\bullet C)(0, Y, Z) = \prod_1^r (a_i Y - b_i Z)^{m_i}$ , onde  $TP_i = (0 : a_i : b_i)$  para  $i = 1, \dots, r$ .

**Demonstração:** Para a demonstração dessa proposição, veja (VAINSENER, 1996) □

**Definição 4.3.2** A multiplicidade da reta  $L$  com a curva  $C$  no ponto  $P$  é definida por:

$$(L, C)_P = \begin{cases} 0, & \text{se } P \notin L \cap C \\ \infty, & \text{se } P \in L \subset C \\ m_i, & \text{se } P = P_i \text{ nas condições da Proposição 4.3.1.} \end{cases}$$

Podemos reescrever a Proposição 4.3.1 dizendo que a interseção entre uma reta  $L$  e uma curva  $C$  tem  $\partial C$  pontos contados com multiplicidade. Esse exemplo é um caso particular do Teorema de Bézout e o caso geral será apresentado mais adiante.

A mesma proposição revela, que com o emprego de um projetividade conveniente, podemos supor, para o cálculo de  $(L, C)_P$ , que  $P$  se encontra a distância finita e que  $L, C$  são distintos da reta no infinito. Nestas circunstâncias, é imediato que

$$(L, C)_P = (L_*, C_*)_P,$$

onde o segundo membro é a multiplicidade de interseção definida no caso afim.

Assim, os resultados apresentados na Seção 3.3 podem ser estudados para curvas projetivas. Um desses resultados é o seguinte.

**Proposição 4.3.2** Sejam  $C$  uma curva projetiva e  $P$  um ponto de  $C$ . Existe um inteiro  $m = m_P(C) \geq 1$  tal que, para toda reta  $C$  passando por  $P$ ,  $(L, C)_P \geq m$ , ocorrendo desigualdade estrita para no máximo  $m$  retas e no mínimo uma.

**Demonstração:** Podemos mover  $C$  e  $P$  com uma projetividade para que a reta no infinito não contenha  $P$ . Assim chegamos ao caso da curva algébrica seguindo a demonstração da Proposição 3.3.1.  $\square$

**Definição 4.3.3** O inteiro  $m_P(C)$  descrito na Proposição 4.3.2 é a multiplicidade de  $C$  em  $P$ . Se  $P \notin C$ , definimos  $m_P(C) = 0$ .

De forma análoga ao capítulo anterior podemos definir ponto liso, singular, duplo, triplo e  $m$ -uplo. Se  $C$  é uma curva afim gerada por  $f$  e  $D$  uma curva gerada por  $F = f^*$ , podemos afirmar que  $m_P(C) = m_P(D)$  para cada ponto  $P \in \mathbb{A}^2$ . Portanto, as definições dadas acima são consistentes com as do capítulo 3.

**Lema 4.3.1** *Sejam  $C, D$  curvas planas projetivas. Então  $C \cap D$  é finita se, e somente se,  $C, D$  não admitem componentes em comum.*

**Demonstração:**

( $\leftarrow$ ) Suponha que  $F$  e  $G$  possuem componente em comum, logo existe  $H \in \mathbb{K}[X, Y, Z]$  tal que  $F = H_1 H$  e  $G = H_2 H$ . Assim a interseção entre  $F$  e  $G$  possuem infinitos pontos, que são os pontos que zeram o polinômio  $H$ .

( $\rightarrow$ ) Pela hipótese se  $C, D$  não admitem componentes em comum em  $\mathbb{K}[X, Y, Z]$  então  $F_*, G_*$  também não admitem em  $\mathbb{K}[X, Y]$ . Logo podemos escrever  $F_* = fh$  e  $G_* = gh$ , com  $f, g, h \in \mathbb{K}[X, Y]$  e  $h$  não constante. Então  $F = (F_*)^* = f^* h^*$  e  $G = (G_*)^* = g^* h^*$ , ou seja,  $F, G$  tem  $h$  em comum, o que contradiz a hipótese. Assim segue que  $F \cap Z$  ou  $G \cap Z$  é finita, portanto  $F \cap G$  é finita.  $\square$

**Definição 4.3.4** *Sejam  $P_i = (x_i : y_i : z_i), i = 1, \dots, r$  pontos distintos de  $F \cap G$ .  $F, G$  estão em boa posição ou bem posicionados se  $P_0 \notin F \cap G$  e se, para cada  $P_i, P_j \in F \cap G, P_0, P_i, P_j$  são não colineares.*

Agora, vamos supor que  $F, G$  não possuem componente em comum. Escrevemos

$F(Y) = A_0 Y^m + A_1 Y^{m-1} + \dots + A_m$  e  $G(Y) = B_0 Y^n + \dots + B_n$ , onde  $A_i, B_j \in \mathbb{K}[X, z]$  são homogêneos de grau  $i, j$ .

**Definição 4.3.5** A Multiplicidade de  $F, G$  no ponto  $P$  é definida por:

$$(F, G)_P = \begin{cases} 0, & \text{se } P \notin L \cap C \\ m_i, & \text{se } P = P_i \text{ nas condições anteriores.} \end{cases}$$

Podemos observar que o somatório de  $m_i$  é igual ao produto do grau de  $F$  e  $G$ , chegando assim ao próximo resultado.

**Teorema 4.3.1** (Teorema de Bézout, versão forte) *Dadas duas curvas projetivas  $C, D$  sem componentes em comum geradas por  $f, g$  pertencentes a  $\mathbb{K}[x, y]$ , respectivamente, onde  $\partial C = m$  e  $\partial D = n$ . Então a interseção entre  $C$  e  $D$  tem exatamente  $mn$  pontos, ou seja,*

$$\#C \cap D = mn.$$

**Demonstração:**

Suponha que  $C$  e  $D$  não têm componentes em comum. Escrevemos  $f(Y) = a_0 Y^m + a_1 Y^{m-1} + \dots + a_d$  e  $g(Y) = b_0 Y^n + \dots + b_n$  com  $a_i, b_j \in \mathbb{K}[X, Z]$  são homogêneos de grau  $i, j$ .

Podemos afirmar que  $(0 : 1 : 0)$  pertence a  $C$  se, e somente se,  $a_0 = 0$ . Logo estando  $C$  e  $D$  bem posicionadas temos  $a_0 = 0$  ou  $b_0 = 0$ . Pelo lema 3.1.2, a resultante  $R(X, Z)$  é homogênea de grau  $mn$ . Como  $a_0 \neq 0$  ou  $b_0 \neq 0$  para  $(x : z) \in \mathbb{P}^1$  temos  $R(X, Z) = 0$  se, e somente se  $(x : y : z) \in C \cap D$ .

Suponha  $C, D$  muito bem posicionadas, então podemos escrever  $R(X, Z) = c \prod_{i=1}^r (c_i X - a_i Z)^{m_i}$ , onde  $c$  é uma constante diferente de zero,  $m_i$  são inteiros maiores ou iguais a um com somatório de  $m_i$  é igual a  $mn$  e  $P_i = (a_i : b_i : c_i)$ , com  $i = 1, \dots, r$ , são os pontos de  $C \cap D$ . Portanto  $\#C \cap D = mn$ .  $\square$

**Exemplo 4.3.1** *Retomando o Exemplo 3.1.6 onde encontramos apenas uma interseção para as curvas  $M$  e  $N$  geradas pelos polinômios  $h(x, y) = x^2 + 1 - y$  e  $p(x, y) = x - 1$ , respectivamente. Vamos encontrar todas as interseções para  $h(X, Y)$  e  $p(X, Y)$ , agora polinômios em  $\mathbb{P}^2$ .*

*Primeiro vamos homogeneizar os dois polinômios, obtendo:  $h^*(X, Y, Z) = X^2 + Z^2 - ZY$  e  $p^*(X, Y, Z) = X - Z$ . Igualando os dois polinômios a zero temos  $X^2 + Z^2 - ZY = 0$ ,  $X - Z = 0$  e da segunda equação podemos afirmar que  $X = Z$ . Substituindo na primeira equação ficamos com  $X^2 + X^2 - XY = 0$ , logo  $X(2X - Y) = 0$ . Então temos dois casos:*

- *Se  $2X - Y = 0$ , temos  $Y = 2X$ , assim encontramos o ponto  $P_1 = (X : 2X : X)$ , fazendo  $X = 1$ , temos  $P_1 = (1 : 2 : 1)$ . Note que a coordenada  $Z$  desse ponto é 1, então esse ponto pertence a  $\mathbb{R}^2$ , ou seja, não está no infinito.*
- *Se  $X = 0$ , obtemos o ponto  $P_2 = (0 : 1 : 0)$ , nesse caso  $Z = 0$ , logo esse ponto está no infinito.*

*Portanto encontramos os dois pontos de interseção entre as curvas  $C$  e  $D$ , previsto pelo Teorema de Bézout, uma vez que  $\partial M = 2$  e  $\partial N = 1$ , logo  $\#M \cap N = 2$ .*

Sabemos que não existe interseção entre duas retas em  $\mathbb{R}^2$ . Mas pelo Teorema de Bézout, se tomarmos duas curvas em  $\mathbb{P}^2$  o número de interseções entre elas será igual ao produto de seus graus. Assim como

o grau de uma reta é um, tomados duas retas em  $\mathbb{P}^2$  temos que encontrar um ponto de interseção. Nesse caso encontraremos um ponto no infinito, como mostra o exemplo a seguir.

**Exemplo 4.3.2** Considere duas retas  $L_1$  e  $L_2$  pertencentes a  $\mathbb{P}^2$  de equações  $l_1(X, Y) = Y - 2X + 6$  e  $l_2(X, Y) = Y - 2X + 12$ , respectivamente. Encontraremos todos os pontos de  $L_1 \cap L_2$ .

Homogeneizando as duas retas, temos:  $l_1^*(X, Y, Z) = Y - 2X + 6Z$  e  $l_2^*(X, Y) = Y - 2X + 12Z$ . Para determinar a interseção entre as duas retas devemos resolver o seguinte sistema:

$$\begin{cases} 0 = Y - 2X + 6Z \\ 0 = Y - 2X + 12Z. \end{cases}$$

Isolando  $Y$  nas duas equações temos  $Y = 2X - 6Z$  e  $Y = 2X - 12Z$ , assim  $2X - 6Z = 2X - 12Z$  o que implica que  $6Z = 0$ , logo  $Z = 0$ . Substituindo o valor de  $Z$  em uma das equações obtemos  $Y = 2X$ . Portanto temos o ponto  $P = (X : 2X : 0)$  e tomando  $X = 1$  temos  $P = (1 : 2 : 0)$  sendo o ponto de interseção entre as duas retas paralelas  $L_1$  e  $L_2$ .

## 5 CONCLUSÃO

Este estudo apresentou conceitos das Curvas Algébricas, algumas aplicações e exploração de suas propriedades. Assim, pôde-se comprovar a real possibilidade de se encontrar o número exato de pontos de interseção entre duas curvas. Bézout é criador de várias proposições matemáticas, que são utilizadas nos estudos matemáticos, em especial, na área da Álgebra. Contudo, o Teorema de Bézout abordado neste trabalho não é frequente nos cursos de graduação. Diante disso, recomenda-se que mais pesquisadores dediquem seus estudos a esse tema, dada a importância do Teorema de Bézout no estudo da Teoria dos Números e para a Matemática, em geral.

**REFERÊNCIAS**

DOMINGUES, H. H.; IEZZI, G. Álgebra moderna. **Atual Editora**, 1982.

FULTON, W. Algebraic curves. **An Introduction to Algebraic Geom**, 2008.

GERD, F. Plane algebraic curves, volume 15 of student mathematical library. **American Mathematical Society, Providence, RI**, 2001.

LEIMANN, K. R. F. Teorema do hexágono de pascal teorema de pappus. 2003.

SALEHYAN, P. Curvas algébrica, uma leva introdução. 2008.

TURA, F. C. Resultantes, equações polinomiais e o teorema de bezout. 2006.

VAINSENER, I. **Introdução às curvas algébricas planas**. [S.l.]: Instituto de Matemática Pura e Aplicada, 1996.