UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

INSTITUTO DE CIÊNCIAS EXATAS

CURSO DE GRADUAÇÃO EM MATEMÁTICA

Mateus Gomes Figueira

Curvas Algébricas Planas e o Teorema de Bézout

SEROPÉDICA

2017

Mateus Gomes Figueira

Curvas Algébricas Planas e o Teorema de Bézout

Monografia apresentada à Banca Examinadora da Universidade Federal Rural do Rio de Janeiro, como requisito parcial para obtenção do título de Bacharel em Matemática, sob a orientação do Prof. Dr. Cláudio Cesar Saccomori Júnior.

SEROPÉDICA

2017

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

COORDENAÇÃO DO CURSO DE GRADUAÇÃO EM MATEMÁTICA.

A monografia "CURVAS ALGÉBRICAS PLANAS E O TEOREMA DE BÉZOUT", apresentada e defendida por MATEUS GOMES FIGUEIRA matrícula 201419035-4 foi aprovada pela Banca Examinadora, com conceito "S" recebendo o número 679.

Seropédica, 14 de julho de 2017.

BANCA EXAMINADORA

Prof. Dr. Cláudio César Saccomori Jr.
Orientador

Prof. Dr. André Luiz Martins Pereira

Prof. Dr. Douglas Monsôres de M. Santos

Afinal, quanto maior o saber, maior o sofrimento; e quanto maior o entendimento maior o desgosto.

Eclesiastes 1:18

Agradecimentos

Agradeço ao Eu Sou, pois nada seria sem Ele, e a seu Filho, pela Graça de nos unir novamente ao Pai.

Agradeço a toda minha família, em especial meus pais Alexandre Teixeira Figueira e Rosana Gomes Figueira, por terem me suportado e ajudado durante esses anos, e minha tia Dr. Rejane Gomes Pimentel, pelos conselhos e pela amizade.

Agradeço a meu orientador Dr. Cláudio Cesar Saccomori Júnior, pelo suporte, dedicação e por sempre acreditar em mim.

Agradeço a meus amigos, todos sem exceção, por terem me ajudado e distraído bastante, pois as vezes tudo que precisamos é sair de uma rotina de estudos para aprender de outras formas.

Agradeço a todo o Departamento de Matemática da UFRRJ, pois todos me acolheram de forma carinhosa desde que entrei na universidade, e os levarei como exemplo de profissionalismo e dedicação.

Resumo

Este trabalho tem por fim demonstrar o teorema de Bézout para curvas projetivas planas, isto é, será demonstrado que duas curvas projetivas, sem componentes em comum, de grau m e n respectivamente, sempre se encontram em $m \cdot n$ pontos, contados com multiplicidade. Para isto, será construído toda uma base de Geometria Algébrica começando por conceitos primordiais vindos de um curso de teoria de anéis, passando por definir uma curva algébrica plana, mudança de coordenadas, critérios para determinar a finitude da interseção de duas curvas algébricas planas e como encontrá-las, apresentando o famoso *Nullstellensatz* de Hilbert para o caso de duas variáveis, a resultante, multiplicidade de um ponto de uma curva, e por fim, imergimos no plano projetivo, onde são reapresentados todas as definições e resultados anteriores, porém agora dentro deste novo ambiente que nos dá embasamento para então provarmos o teorema principal.

Palavras-Chave: Geometria Algébrica; Plano projetivo; Curvas planas; Teorema de Bézout.

Sumário

Introdução

"To infinity... and beyond!"[1]

O que acorre "no" infinito? Esta pergunta parece subjetiva, pois o conceito de infinito é amplamente variado e pode ter vários significados. Em Matemática, o conceito de infinito sugere que algo cresce (ou decresce) indefinidamente, ou seja, não podemos fixar uma medida comensurável ou limitada para expressar uma grandeza. Mas será que podemos considerar o infinito um lugar? *Yes, we can*. Daremos um tratamento rigoroso a este conceito de forma que, não só o infinito será um lugar, mas será uma espécie de *Shangri-la* da Matemática, onde as contas dão certo e os teoremas podem ser provados e generalizados.

O objetivo deste trabalho é demonstrar o Teorema de Bézout o qual diz que, duas curvas de graus m e n se encontram em $m \cdot n$ pontos, que podem ser distintos ou não, pois são contados com multiplicidade . Contamos mais de uma vez o mesmo ponto quando as curvas se tangenciam neste ponto ou quando ocorre um fenômeno no qual, intuitivamente, a curva "passar várias vezes" por este ponto. Neste último caso, temos um de ponto múltiplo desta curva.

Para concluir o objetivo, se faz necessário, antes de tudo, tratar sobre conceitos básicos, afim de tornar a leitura mais fácil e menos cansativa. Para isso, o capítulo 1 retorna a conteúdos básicos da disciplina de teoria de anéis, como corpo de frações, lema de Gauss e homomorfismo. Outros resultados que podem facilitar o entendimento e compreensão do texto estão na bibliografia e serão anunciados durante o texto se necessário. Após isso, vemos como se define uma curva e algumas de suas propriedades,

[1] Bordão do personagem Buzz Lightyear na animação *Toy Story*-1995.

como a mudança de referencial. Este é o tema do capítulo 2, que mostrará como é feita a mudança de referencial, através de aplicações denominadas afinidades.

Depois de iniciado o estudo, o capítulo 3 provará que a interseção de duas curvas sem componente em comum é finita. Veremos o Teorema dos Zeros de Hilbert (em uma versão para duas variáveis) que afirma que, se um sistema de equações polinomiais define um ideal próprio do anel de polinômios, então há solução para esse sistema. No fim deste capítulo, analisaremos a resultante, que é uma ferramenta importante para o cálculo dos pontos da interseção de duas curvas.

Quanto à multiplicidade, já citada anteriormente, será abordada no capítulo 4, onde inicialmente veremos como se dá a interseção de uma reta com um curva e que, com essa análise, nos possibilitará defini-la de maneira rigorosa.

Finalmente, o capítulo 5 nos imerge no plano projetivo, onde consideraremos o infinito um "lugar" de fato e veremos qual é o tratamento necessário para que uma curva esteja definida nesse ambiente e as propriedades que isso produz, como é o caso da mudança de coordenadas, vista inicialmente no capítulo 2 para o caso de uma curva no plano afim.

A conclusão de todo esse estudo está no capítulo 6, que apresentará primeiramente os resultados estendidos do capítulo 4, mas agora para o plano projetivo, definindo a multiplicidade de um ponto de uma curva projetiva, demonstrando a finitude da interseção de duas curvas no plano projetivo e culminará no Teorema de Bézout, mostrando exatamente quantos pontos há nessa interseção.

Capítulo 1

Resultados Básicos

Iniciaremos apresentando alguns conceitos preliminares que estão em qualquer curso de teoria de anéis e outros que não, porém podem ser obtidos com certa facilidade pelo leitor e que serão de grande ajuda para o que se sucede nos próximos capítulos. É recomendável que o leitor consulte [2] afim de conhecer conceitos e resultados de assuntos como relação de equivalência, anéis, ideais, anel quociente e domínio de integridade.

1.1 Homomorfismo

Sejam A e A' dois anéis. Para simplificar a notação, denotemos as duas operações desses anéis com os mesmos símbolos $+$ e $\cdot$, porém denotemos por 0 o elemento neutro de A e por $0'$ o elemento neutro de A'. Se ambos os anéis possuírem identidade, denotemos por 1 a unidade de A e por $1'$ a unidade de A'.

Definição 1.1.1. Uma função $f : A \to A'$ diz-se um *homomorfismo* de A em A' se satisfaz as seguintes condições, $\forall x, y \in A$:

1. $f(x + y) = f(x) + f(y)$;
2. $f(x \cdot y) = f(x) \cdot f(y)$.

Se $f : A \to A'$ é um homomorfismo bijetivo dizemos que f é um *isomorfismo* de A sobre A'.

Dizemos que dois anéis A e A' são *isomorfos* se existir um isomorfismo de A sobre A' e escrevemos $A \simeq A'$.

Teorema 1.1.2 (Teorema do homomorfismo)**.** *Sejam A e A' anéis e $f : A \to A'$ um homomorfismo. Então*

1. $Im(f) = \{f(a) \mid a \in A\}$ *é um subanel de A'.*
2. $\ker(f) = \{a \in A \mid f(a) = 0'\}$ *é um ideal de A, e f é injetiva se, e somente se,* $\ker(f) = \{0\}$.
3. *Os anéis $A/\ker(f)$ e $Im(f)$ são isomorfos.*

Demonstração. A demonstração deste teorema pode ser encontrada em [2] páginas 57 e 58. □

Proposição 1.1.3. *Sejam A, B anéis, I ideal de A e J ideal de B. Sejam ainda, os homomorfismos injetivos $\alpha : I \to A$ e $\beta : J \to B$ (inclusões[1]) e os isomorfismos $\mu : I \to J$ e $\phi : A \to B$ tais que o diagrama*

$$\begin{array}{ccc} I & \xrightarrow{\ \mu\ } & J \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A & \xrightarrow{\ \phi\ } & B \end{array}$$

comuta, ou seja, $\beta \circ \mu = \phi \circ \alpha$. Então $A/I \simeq B/J$.

Demonstração. Seja $\overline{\phi}$ definida da seguinte forma:

$$\begin{array}{rccc} \overline{\phi} : & A & \longrightarrow & B/J \\ & a & \longmapsto & \overline{\phi(a)} \end{array}.$$

Tomando $j = \mu(i) \in B$, então $\overline{\phi(i)} = \overline{\phi(\alpha(i))} = \overline{\beta \circ \mu(i)} = \overline{\beta(j)} = \overline{j} = \overline{0}$. Logo $I \subset \ker(\overline{\phi})$. Reciprocamente, seja $a \in \ker(\overline{\phi})$, então $\overline{\phi(a)} = \overline{0}$ e $\phi(a) \in J$. Sendo μ uma bijeção, existe $i \in I$, tal que $\beta \circ \mu(i) = \phi(a)$. Logo, $\phi \circ \alpha(i) = \phi(a)$. Daí $\phi(i) = \phi(a)$,

[1] Se $i \in I$ e $j \in J$, então $\alpha(i) = i$ e $\beta(j) = j$.

portanto $a = i \in I$. Assim $\ker(\overline{\phi}) = I$. Como claramente $\overline{\phi}$ é um homomorfismo sobrejetivo, segue pelo teorema do homomorfismo que $A/\ker(\overline{\phi}) \simeq B/J$, ou seja, $A/I \simeq B/J$. □

1.2 Corpo de Frações

Seja D um domínio de integridade. Denote $D^* = D\backslash\{0\}$. Em $D \times D^*$ definimos a relação:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc, \text{ em } D. \tag{1.1}$$

Proposição 1.2.1. *A relação* (1.1) *é de equivalência.*

Demonstração. Sejam $a, c, e \in D$ e $b, d, f \in D^*$. Note que a relação $\sim$ é:

i) Reflexiva: Como $ab = ba$, pois D é domínio de integridade, vale que $(a, b) \sim (a, b)$.

ii) Simétrica: Se $(a, b) \sim (c, d)$, então $ad = bc$. Pela comutatividade de D, temos que: $cb = da$, então $(c, d) \sim (a, b)$.

iii) Transitiva: Se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, então $ad = bc$ e $cf = de$. Logo, $fad = fbc = bcf = bde = bed$. Daí, $(fa - be)d = 0$. Como $d \neq 0$ e D é domínio, então $fa = be$, ou seja, $af = be$. Portanto, $(a, b) \sim (e, f)$.

Por (i),(ii) e (iii), temos que a relação (1.1) é de equivalência. □

Denota-se a classe de (a, b), relativa a relação $\sim$, por a/b. Assim,

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

Proposição 1.2.2. *Seja* $K = \left\{\frac{a}{b} : a \in D, b \in D^*\right\}$. *Em* K, *se* $\frac{a}{b} = \frac{a'}{b'}$ *e* $\frac{c}{d} = \frac{c'}{d'}$, *então*

$$\frac{ad + cb}{bd} = \frac{a'd' + c'b'}{b'd'} \quad \textit{e} \quad \frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

Demonstração. Como $ab' = ba'$ e $cd' = dc'$ segue-se que

$$b'd'(ad + cb) = b'd'ad + b'd'cb = (b'a)d'd + (cd')b'b.$$

E portanto,

$$b'd'(ad + cb) = (ba')dd' + (dc')bb' = bd(a'd' + c'b').$$

Como D não possui divisores de zero, temos que $bd \neq 0$ e $b'd' \neq 0$. Logo,

$$\frac{ad + cb}{bd} = \frac{a'd' + c'b'}{b'd'}.$$

Analogamente,

$$ac(b'd') = (ab')(cd') = (ba')(dc') = (a'c')(bd).$$

Assim,

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

□

Em vista da proposição anterior, definimos, em K, a soma de frações:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$$

e o produto de frações:

$$\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}.$$

Note que o elemento neutro da soma é $\frac{0}{1} \in K$ e do produto é $\frac{1}{1} \in K$, pois $\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + 0 \cdot b}{b \cdot 1} = \frac{a}{b}$ e $\frac{a}{b} * \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$, para todo $\frac{a}{b} \in K$. Por simplicidade, escrevemos $0 := \frac{0}{1}$ e $1 := \frac{1}{1}$.
É de fácil verificação que $(K, +, *)$ é um anel comutativo. Agora, se $\frac{a}{b} \in K$, com $\frac{a}{b} \neq 0$, então $a \neq 0$ e

$$\frac{a}{b} * \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{1}{1}.$$

Dessa forma $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ e $(K, +, *)$ é na verdade um corpo. Dizemos que K é o *corpo de frações* de D.

Definição 1.2.3. Denota-se por $D^\sharp = \left\{ a^\sharp = \frac{a}{1} \in K : a \in D \right\}$.

É de fácil verificação que $D^\sharp$ é um subanel de K.

Proposição 1.2.4. *Seja*

$$\begin{aligned} \phi : D &\to D^\sharp \\ d &\mapsto d^\sharp \end{aligned}.$$

Então ϕ é um isomorfismo de anéis.

Demonstração. Sejam $a, b \in D$. Então,

$$\phi(a+b) = (a+b)^\sharp = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = a^\sharp + b^\sharp = \phi(a) + \phi(b).$$

Além disso,

$$\phi(ab) = (ab)^\sharp = \frac{ab}{1} = \frac{a}{1} * \frac{b}{1} = a^\sharp * b^\sharp = \phi(a) * \phi(b).$$

Logo ϕ é homomorfismo. Agora, suponha que $a \in \ker\phi$, então $\phi(a) = a^\sharp = \frac{a}{1} = \frac{0}{1} = 0^\sharp$. Logo $a \cdot 1 = 0 \cdot 1$, e assim $a = 0$. Concluímos que $\ker\phi = \{0\}$ e ϕ é injetiva. Finalmente, se $a^\sharp \in D^\sharp$, então $a^\sharp$ é imagem, por ϕ, de $a \in D$. Logo ϕ é sobrejetiva e portanto isomorfismo. □

Em vista da proposição acima, podemos considerar $D \subset K$, identificando cada $a \in D$ com $\frac{a}{1} \in D^\sharp$.

1.3 Polinômios

Denotaremos por $K[X]$ o anel de polinômios em uma variável com coeficientes no corpo K. Um elemento $f \in K[X]$ se escreve de forma única,

$$f = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0,$$

onde os coeficientes a_i são elementos de K. Se $a_n \neq 0$ então f é de grau n e escrevemos

$$\deg(f) = n.$$

Se $a_n = 1$, dizemos que f é *mônico*.

Proposição 1.3.1 (Algoritmo da Divisão)**.** *Sejam $f, g \in K[X], g \neq 0$. Então existem únicos $q, r \in K[X]$, tais que $f = qg + r$, onde $r = 0$ ou $\deg(r) < \deg(g)$.*

Demonstração. Sejam $f = a_n X^n + ... + a_0$ e $g = b_m X^m + ... + b_0$. Se $f = 0$, então basta tomar $q = r = 0$. Se $\deg(f) < \deg(g)$, basta tomar $q = 0$ e $r = f$. Agora, se $n = \deg(f) \geqslant \deg(g) = m$, então faremos a demonstração por indução sobre $\deg(f) = n$:

1. Se $n = 0$, então $f = a_0 \neq 0$, $g = b_0 \neq 0$. Basta tomar $q = b_0^{-1} a_0$ e $r = 0$.

2. Suponha, por indução, a existência provada quando $\deg(f) < n$. Tome $h = -a_n b_m^{-1} X^{n-m} g + f$. Note que $\deg(h) < \deg(f)$. Daí, pela hipótese de indução, existem $q_1, r_1 \in K[X]$, tais que $h = q_1 g + r_1$, onde $r_1 = 0$ ou $\deg(r_1) < \deg(g)$. Como $f = h + a_n b_m^{-1} X^{n-m} g$, então $f = (q_1 + a_n b_m^{-1} X^{n-m}) g + r_1$. Tomando $q = q_1 + a_n b_m^{-1} X^{n-m}$ e $r = r_1$, temos o resultado.

Quanto à unicidade, suponha $f = qg + r = q'g + r'$, onde $r = 0$ ou $\deg(r) < \deg(g)$ e $r' = 0$ ou $\deg(r') < \deg(g)$. Daí vem $(q - q')g = r' - r$. Ora, se $q \neq q'$ então o primeiro membro é um polinômio de grau maior ou igual a m enquanto que o segundo é certamente nulo ou de grau menor que m, o que seria um absurdo. Portanto $q = q'$ e consequentemente $r' = r$. □

Definição 1.3.2. Sejam A um anel comutativo e $a \in A$. O subanel ideal

$$\langle a \rangle := \{ba; b \in A\}$$

é dito subanel ideal *principal* gerado por a.

Proposição 1.3.3. *Todo ideal de $K[X]$ é principal.*

Demonstração. Seja I um ideal de $K[X]$. Se $I = \{0\}$, não há nada a demonstrar. Assim, podemos supor que existe um elemento $f_0 \in I$ de grau mínimo. Vamos mostrar que $I = \langle f_0 \rangle$. Seja $g \in I$. Aplicando o algoritmo da divisão, podemos escrever,

$$g = q f_0 + r,$$

onde $r = 0$ ou $\deg(r) < \deg(f_0)$. Como $r = g - qf_0$ é um elemento do ideal I, se ocorresse $r \neq 0$, produziríamos um elemento em I com grau inferior ao mínimo, o que é absurdo. Portanto, $g = qf_0 \in \langle f_0 \rangle$. □

Definição 1.3.4. Um polinômio não constante $f \in K[X]$ é *redutível* sobre K se existirem polinômios não constantes $g, h \in K[X]$, tais que $f = gh$. Dizemos que f é *irredutível* se não for redutível.

Definição 1.3.5. Seja D um domínio de integridade. Se $a_1, a_2, ..., a_n \in D$, então $d \in D$ é chamado de *máximo divisor comum (MDC)* de $a_1, a_2, ..., a_n$ se:

1. $d \mid a_i$ para $i = 1, 2, ..., n$;

2. se $c \mid a_i$ para $i = 1, 2, ..., n,$ então $c \mid d$.

Denotaremos $d = \text{MDC}(a_1, a_2, ..., a_n)$. Veja que d não é necessariamente único.

Exemplo 1.3.6. Em $\mathbb{R}[X]$ considere $f = x - 1$ e $g_a = ax - a$, com $a \in \mathbb{R} - \{0, 1\}$. Observe que $f \neq g_a$, mas $f|(x^2 - 1)$, $g_a|(x^2 - 1)$, $f|(x^2 - 2x + 1)$ e $g_a|(x^2 - 2x + 1)$. Veja que os outros divisores comuns de $x^2 - 1$ e $x^2 - 2x + 1$ são constantes. Além disso, $f|g_a$ e $g_a|f$. Logo, f e g_a são ambos máximos divisores comuns de $x^2 - 1$ e $x^2 - 2x + 1$.

Proposição 1.3.7. *Se $d \in D$ e $d' \in D$ são MDC de $a_1, a_2, ..., a_n$, então existem $a, b \in D$, tais que $ad = d'$, $bd' = d$ e $ab = 1$.*

Demonstração. Se d e d' são MDC de $a_1, a_2, ..., a_n$ então $d|d'$ e $d'|d$, logo existem $a, b \in D$, tais que $d' = ad$ e $d = bd'$. Com isso, $d = bad$ e assim $d(1 - ba) = 0$. Como $d \neq 0$ então $1 - ba = 0$. O que prova que $ab = 1$. □

Proposição 1.3.8. *Sejam $f, g \in K[X]$ sem fatores irredutíveis em comum. Existem $a, b \in K[X]$, tais que*

$$af + bg = 1.$$

Demonstração. Seja $\langle f \rangle$ o ideal gerado por f. Como $K[X]$ é um domínio de ideais principais, existe $h \in K[X]$, tal que $\langle f, g \rangle = \langle h \rangle$. Assim, podemos tomar $c, d \in K[X]$, tais que $g = hc$ e $f = hd$. Como f, g não tem fatores irredutíveis em comum, então $h \in K$. Portanto, $1 = h^{-1}h \in \langle h \rangle$ e $\langle h \rangle = K[X]$. Como $\langle h \rangle = \langle f, g \rangle$, então existem $a, b \in K[X]$, tais que $1 = af + bg$. □

Lema 1.3.9. *Sejam $p, a, b \in K[X]$ com p irredutível. Então $p|ab$ se, e somente se, $p|a$ ou $p|b$.*

Demonstração. Suponha que $p|ab$, isto é, existe $d \in K[X]$ tal que $pd = ab$. Se $p \nmid a$, então p e a não tem fatores irredutíveis em comum. Logo pela proposição 1.3.8, existem $v, w \in K[X]$ tais que $vp + aw = 1$. Multiplicando os dois lados dessa igualdade por b temos que

$$vpb + w(ab) = b \Leftrightarrow vpb + w(pd) = b \Leftrightarrow p(vb + dw) = b.$$

Isso prova que $p|b$. A reciproca é trivial. □

Proposição 1.3.10 (Fatoração Única)**.** *Todo polinômio f não constante em uma variável e com coeficientes em um corpo, se escreve de maneira única (a menos de ordem dos fatores) na forma*

$$f = c \cdot p_1 \cdot \ldots \cdot p_m,$$

onde c denota uma constante e cada p_i é um polinômio irredutível mônico.

Demonstração. Existência: Se f já é polinômio irredutível, então $f = c \cdot \dfrac{f}{c}$, onde c é o coeficiente líder de f. Se $f = gh$, com $\deg(g), \deg(h) \geqslant 1$, então $\deg(g), \deg(h)$ são ambos menores que $\deg(f)$ e concluímos a prova da existência por indução sobre o grau de f.

Unicidade: Como um produto de polinômios mônicos é mônico, a constante c é bem determinada pois coincide com o coeficiente líder de f. Por outro lado, se

$$p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n \tag{1.2}$$

com cada q_i e cada p_j mônicos e irredutíveis, então, pelo lema 1.3.9, teríamos que p_1 divide algum dos q_i. Reordenando se preciso, podemos supor que $p_1 \mid q_1$. Mas, q_1 é

irredutível e como p_1 e q_1 são mônicos, logo $p_1 = q_1$. Cancelando p_1 e q_1 na igualdade (1.2), concluímos que $p_i = q_i$ e $m = n$ por indução sobre o grau de f. □

1.4 Lema de Gauss

Definição 1.4.1. Um elemento $d \in D$ domínio é dito *invertível* em D ou uma *unidade* de D, se existir $b \in D$, tal que $bd = 1$. Denotaremos de $\mathbb{U}(D)$ o conjunto de todos as unidades de D, isto é

$$\mathbb{U}(D) := \{d \in D : db = bd = 1, \text{para algum } b \in D\}.$$

Definição 1.4.2. Um elemento $a \in D$ é chamado de *elemento irredutível*, se $a \neq 0$, $a \notin \mathbb{U}(D)$ e $a = bc$ implica em $b \in \mathbb{U}(D)$ ou $c \in \mathbb{U}(D)$.

Definição 1.4.3. Um elemento $a \in D$ é dito *primo*, se $a \notin \mathbb{U}(D)$ e toda vez que $a|bc$, então $a|b$ ou $a|c$ para $b, c \in D$.

Exemplo 1.4.4. Um polinômio $f \in K[X]$ é primo se f não é constante e, se $g, h \in K[X]$,

$$f \mid gh \Rightarrow f \mid g \text{ ou } f \mid h.$$

Definição 1.4.5. Um domínio D é dito de *fatoração única (DFU)* se todo elemento se escreve como produto de irredutíveis de forma única a menos de ordem ou de multiplicação por invertível.

Lema 1.4.6. *Seja D um DFU. Então $a \in D$ é irredutível se, e somente se, é primo.*

Demonstração. Sejam $a \in D$ irredutível e $b, c \in D$, tais que $a \mid bc$. Então $bc = ad$, para algum $d \in D$. Como D é DFU e a é irredutível, então a deve figurar no primeiro membro como elemento irredutível na fatoração de b ou c e assim, $a \mid b$ ou $a \mid c$. Reciprocamente, se a é primo e se o exibirmos como produto, $a = bc$, deduzimos que a divide algum dos fatores. Digamos que $b = ab_1$. Substituindo, temos $b = (bc)b_1$ e cancelando[2] b dos dois lados temos $1 = cb_1$, logo c é invertível e concluímos que a é irredutível. □

[2] Se $b - b_1cb = 0$, temos que $b(1 - b_1c) = 0$ e como D é domínio e $b \neq 0$, então $(1 - b_1c) = 0$.

Corolário 1.4.7. *Seja $f \in K[X]$ um polinômio não constante. Então f é primo se, e somente se, é irredutível.*

Demonstração. Pela proposição (1.3.10), $K[X]$ é DFU e o resultado é consequência do lema anterior. □

Pela proposição (1.3.7), quaisquer dois MDC(a, b) são *associados*, ou seja, diferem apenas por uma multiplicação por invertível.

Proposição 1.4.8. *Sejam D um DFU e $a, b \in D$. Então existe MDC(a, b).*

Demonstração. Como D é um domínio de fatoração única, então podemos escrever $a = a_1 \cdot ... \cdot a_k \cdot ... \cdot a_n$ e $b = b_1 \cdot ...b_k \cdot ... \cdot b_m$, onde a_i e b_j são fatores irredutíveis, tais que a_i e b_i são associados para $i \leq k$ e a_i e b_j não são associados $\forall i, j > k$, onde $k \geq 0$. Definimos $d = \prod_{i=1}^{k} a_i$ se $k > 0$ e $d = 1$ se $k = 0$. Segue que d divide a e b. Seja c divisor de a e b. Suponha que $c \nmid d$. Temos que na fatoração de c existe um irredutível f que não divide d, pois D é DFU. Então f divide algum a_i e algum b_j para $i, j > k$. Assim, algum a_i e algum b_j seriam associados, o que é uma contradição. Portanto $c \mid d$ e d é um máximo divisor comum de a e b. □

Esta última proposição nos permite definir, a menos de uma multiplicação por invertível, o conteúdo de um polinômio.

Definição 1.4.9. Seja A um DFU e seja $f = a_n X^n + ... + a_0 \in A[X]$. O *conteúdo* de f é o MDC$(a_1, ..., a_n)$, denotado $c(f)$. Dizemos que f é *primitivo* se $c(f) = 1$.

Proposição 1.4.10. *Sejam A um DFU e $f, g \in A[X]$ polinômios. Se f, g são primitivos, então o seu produto $f \cdot g$ é primitivo. Além disso,*

$$c(f \cdot g) = c(f) \cdot c(g). \tag{1.3}$$

Demonstração. : Sejam $f = a_m X^m + ... + a_0$, $g = b_n X^n + ... + b_0$ e $c_r = \Sigma a_i b_{r-i}$. Note que c_r é o coeficiente de X^r em $f \cdot g$. Seja $d \in A$ irredutível. Como $c(f) = c(g) = 1$, existem índices $0 \leqslant m_0 \leqslant m, 0 \leqslant n_0 \leqslant n$, tais que $d \mid a_i$ para $i < m_0, d \mid b_i$

para $i < n_0$ e $d \nmid a_{m_0} b_{n_0}$. Assim, na expressão $c_{m_0+n_0} = a_{m_0+n_0}b_0 + a_{m_0+n_0-1}b_1 + ... + a_{m_0}b_{n_0} + ... + a_0 b_{m_0+n_0}$, todas as parcelas exceto $a_{m_0}b_{n_0}$ são divisíveis por d. Logo $d \nmid c_{m_0+n_0}$ e sendo d um elemento irredutível arbitrário de A, concluímos que $c(f \cdot g) = 1$ e $f \cdot g$ é primitivo. Quanto à equação (1.3), podemos escrever $f = c(f)f'$ e $g = c(g)g'$, com f' e g' primitivos. Temos então $f \cdot g = c(f)c(g)f'g'$. Com isso, para $d \in A$, tal que $d \mid f \cdot g$, então $d \mid c(f)c(g)$ e assim se conclui que $c(f \cdot g) = c(f) \cdot c(g)$. (É imediato que se $d \mid c(f)c(g)$ então $d \mid f \cdot g$). □

Lema 1.4.11 (Lema de Gauss)**.** *Sejam A um DFU e $K \supseteq A$ seu corpo de frações. Seja ainda $f \in A[X]$ um polinômio primitivo não constante. Se f é redutível em $K[X]$, então também é em $A[X]$. Além disso, se $g \in A[X]$ e $f \mid g$ em $K[X]$, então $f \mid g$ em $A[X]$.*

Demonstração. Sejam $g, h \in K[X]$ não constantes, tais que $f = g \cdot h$. Reduzindo os coeficientes a denominador comum, podemos escrever $g = g_1/d_1, h = h_1/d_2$, com $g_1, h_1 \in A[X]$ e $d_1, d_2 \in A$. Podemos supor que $\mathrm{MDC}(d_1, c(g_1)) = \mathrm{MDC}(d_2, c(h_1)) = 1$. Segue-se que $d_1 d_2 f = g_1 \cdot h_1$ em $A[X]$. Tomando conteúdos, obtemos $d_1 d_2 = c(g_1)c(h_1)$. Logo $d_1 \mid c(h_1)$, $d_2 \mid c(g_1)$ em A e concluímos a relação $f = (g_1/d_2) \cdot (h_1/d_1)$ em $A[X]$. Assim f também é redutível em $A[X]$. Agora, se $g \in A[X]$ e $f \mid g$ em $K[X]$, então $g = f \cdot h$ com $h \in K[X]$. Reduzindo os coeficientes de h a um denominador comum, temos que $h = h_2/d$ com $h_2 \in A[X]$ e $d \in A$. Podemos supor que $\mathrm{MDC}(d, c(h_2)) = 1$ e assim $dg = f \cdot h_2$ em $A[X]$. Tomando conteúdos, obtemos $dc(g) = c(h_2)$. Então $d \mid c(h_2)$ em A e assim $h = h_2/d \in A[X]$. Logo $f \mid g$ em $A[X]$. □

De forma análoga à definição de polinômio em uma variável, podemos dizer que um polinômio em n variáveis $X_1, X_2, ..., X_n$ sobre um anel A é uma soma formal com finitas parcelas da forma

$$f(X_1, X_2, ..., X_n) = \sum_{i_1, i_2, ..., i_n \in \mathbb{N}} a_{i_1, i_2, ..., i_n} X_1^{i_1} \cdot X_2^{i_2} \cdot ... \cdot X_n^{i_n},$$

onde $a_{i_1,i_2,\ldots,i_n} \in A$. Tomamos o grau formal de um polinômio f de n variáveis como

$$deg(f) := \max \left\{ \sum_{j=1}^{n} i_j \mid a_{i_1,i_2,\ldots,i_n} \neq 0 \right\}.$$

Como o anel $K[X]$ de polinômios de uma variável sobre um corpo K é domínio de integridade, podemos considerar por vezes o anel de duas variáveis $K[X,Y]$ como o anel $(K[X])[Y]$, que são os polinômios na variável Y com coeficientes no domínio $K[X]$.

Capítulo 2

Mudança de Coordenadas

Neste capítulo, será introduzido a ideia de mudança de coordenadas cartesianas e com isso, verificaremos o conceito de propriedade independente do referencial, que são propriedades que não dependem da escolha de um particular sistema de coordenadas.

2.1 Coordenadas de um referencial

Definição 2.1.1. Um *referencial* ou *sistema de coordenadas afim* no plano K^2 consiste na escolha de um ponto $O \in K^2$, chamado *origem do referencial*, e de uma base $\{v_1, v_2\}$ do espaço vetorial K^2. O *vetor coordenadas* de um ponto $P \in K^2$, em relação a um referencial

$$R = \{O, \{v_1, v_2\}\},$$

é o par ordenado $(P)_R = (x_1, x_2) \in K^2$ que é a combinação linear dos vetores v_1 e v_2 com coeficientes x_1 e x_2 respectivamente, somando-se a origem, isto é

$$P = O + x_1 v_1 + x_2 v_2. \tag{2.1}$$

Se $R' = \{O', \{v_1', v_2'\}\}$ é outro referencial, obtemos de (2.1), juntamente com $P = O' + x_1' v_1' + x_2' v_2'$, uma forma de representarmos o ponto P do sistema inicial, isto é $(P)_R$, como combinação linear dos novos vetores referenciais somando-se a nova origem, ou seja, $(P)_{R'} = (x_1', x_2')$. Para isso, escreveremos os vetores iniciais e a

nova origem como combinação linear dos novos referenciais: $v_j = a_{1j}v'_1 + a_{2j}v'_2$, $O - O' = a_1v'_1 + a_2v'_2$. Deduzimos por um lado, $P - O' = x'_1v'_1 + x'_2v'_2$ e por outro,

$$\begin{aligned} P - O' &= (O - O') + x_1v_1 + x_2v_2 \\ &= a_1v'_1 + a_2v'_2 + x_1(a_{11}v'_1 + a_{21}v'_2) + x_2(a_{12}v'_1 + a_{22}v'_2) \\ &= (a_1 + a_{11}x_1 + a_{12}x_2)v'_1 + (a_2 + a_{21}x_1 + a_{22}x_2)v'_2. \end{aligned}$$

Dessa forma,

$$\begin{aligned} (x'_1, x'_2) &= (a_1 + a_{11}x_1 + a_{12}x_2, a_2 + a_{21}x_1 + a_{22}x_2) \\ &= (a_1, a_2) + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}. \end{aligned}$$

Exemplo 2.1.2. O *referencial canônico* é dado por

$$O = (0, 0), v_1 = (1, 0), v_2 = (0, 1).$$

Definição 2.1.3. Uma *transformação afim* ou *afinidade* em K^2 é uma aplicação

$$T : K^2 \to K^2$$

composta de uma translação com um isomorfismo linear.

Vale lembrar que um *isomorfismo linear* é uma transformação linear $L : A \to B$, na qual L é uma bijeção linear entre A e B, ou seja, a transformação linear L é injetiva e sobrejetiva, e por consequência, invertível. Além disso, a transformação linear L é um isomorfismo se, e somente se, $\det M \neq 0$, em que M é a matriz da transformação L.

A ordem com que se compõe a translação com o isomorfismo linear na definição 2.1.3 não importa, pois se L é uma aplicação linear e $P_0 \in K^2$, temos $L(P+P_0) = L(P) + L(P_0)$. Ou seja, uma translação seguida de uma aplicação linear tem o mesmo efeito que a (mesma) aplicação linear seguida de uma outra translação.

Toda transformação afim é da forma $T(x_1, x_2) = (y_1, y_2)$, onde

$$\begin{cases} y_1 = a_1 + a_{11}x_1 + a_{12}x_2 \\ y_2 = a_2 + a_{21}x_1 + a_{22}x_2 \quad . \end{cases} \tag{2.2}$$

Como é de fácil verificação, as afinidades formam um grupo $\mathbb{T}$ com a operação de composição de funções, cujo elemento neutro é a função identidade I e, considerando a afinidade dada em (2.2), então sua inversa T^{-1} é da forma

$$\begin{cases} x_1 = \left(\dfrac{a_{12}a_2 - a_{22}a_1}{a_{11}a_{22} - a_{12}a_{21}}\right) + \left(\dfrac{a_{22}}{a_{11}a_{22} - a_{12}a_{21}}\right) y_1 + \left(\dfrac{-a_{12}}{a_{11}a_{22} - a_{12}a_{21}}\right) y_2 \\ x_2 = \left(\dfrac{a_{21}a_1 - a_{11}a_2}{a_{11}a_{22} - a_{12}a_{21}}\right) + \left(\dfrac{-a_{21}}{a_{11}a_{22} - a_{12}a_{21}}\right) y_1 + \left(\dfrac{a_{11}}{a_{11}a_{22} - a_{12}a_{21}}\right) y_2 \end{cases}.$$

De fato, a composta de duas afinidades é uma afinidade, e a inversa de uma afinidade também é. Veremos a seguir como identificar $\mathbb{T}$ como um subgrupo de $\mathbb{GL}_3(K)$, onde $\mathbb{GL}_3(K)$ denota o grupo das matrizes invertíveis 3×3 com coeficientes em K.

2.2 Representação matricial

Definição 2.2.1. Denotamos por $\mathbb{M}$ o grupo dos isomorfismos lineares de K^3 que deixam o plano $\mathbb{S} = \{(x_1, x_2, x_3) | x_3 = 1\}$ invariante, ou seja:

$$\mathbb{M} = \{M \in \mathbb{GL}_3 \mid M(\mathbb{S}) \subset \mathbb{S}\}.$$

Por abuso de notação, se $M \in \mathbb{M}$, usaremos o mesmo símbolo M para representar sua matriz associada na base canônica de K^3. Note que se M é da forma

$$M = \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{21} & a_{22} & a_2 \\ 0 & 0 & 1 \end{pmatrix}, \tag{2.3}$$

então $M \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11}x + a_{12}y + a_1 \\ a_{21}x + a_{22}y + a_2 \\ 1 \end{pmatrix}$ e portanto, $M \in \mathbb{M}$. Reciprocamente, se $M \in \mathbb{M}$, então M é da forma (2.3). De fato, se $M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, como $P_1 = (1, 0, 1), P_2 = (0, 1, 1), P_3 = (0, 0, 1) \in \mathbb{S}$, então:

$$MP_1 = \begin{pmatrix} a_{11}+a_{13} \\ a_{21}+a_{23} \\ a_{31}+a_{33} \end{pmatrix}, MP_2 = \begin{pmatrix} a_{12}+a_{13} \\ a_{22}+a_{23} \\ a_{32}+a_{33} \end{pmatrix} \text{ e } MP_3 = \begin{pmatrix} a_{13} \\ a_{23} \\ a_{33} \end{pmatrix}.$$

Dessa forma, $a_{33} = 1$ e $a_{31} = a_{32} = 0$, pois M deixa invariante o plano $x_3 = 1$.

Mostraremos que o grupo das afinidades $\mathbb{T}$ pode ser identificado com $\mathbb{M}$. Definimos $\Phi : \mathbb{T} \to \mathbb{M}$, por

$$\Phi(T) = M_T = \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{21} & a_{22} & a_2 \\ 0 & 0 & 1 \end{pmatrix},$$

onde $T(x_1, x_2) = (a_1 + a_{11}x_1 + a_{12}x_2, a_2 + a_{21}x_1 + a_{22}x_2)$.

Proposição 2.2.2 (representação matricial)**.** *Sejam $T \in \mathbb{T}$ e $M_T \in \mathbb{M}$ a matriz associada a afinidade T. Temos que*

(i) $[TP] = M_T[P], \forall P \in K^2$*, onde se* $P = (x, y)$*, escrevemos* $[P] = \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$.

(ii) $M_{TT'} = M_T M_{T'}$ *para todo par de afinidades* T, T'.

(iii) $\Phi : \mathbb{T} \to \mathbb{M}$ *é um isomorfismo de grupos.*

Demonstração. Sejam T uma afinidade, como em (2.2), e $P = (x_1, x_2) \in K^2$, onde $T(x_1, x_2) = (y_1, y_2)$. Por definição, temos que

$$[TP] = [T(x_1, x_2)] = [(y_1, y_2)] = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + a_1 \\ a_{21}x_1 + a_{22}x_2 + a_2 \\ 1 \end{pmatrix}.$$

Por outro lado,

$$M_T[P] = \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{21} & a_{22} & a_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + a_1 \\ a_{21}x_1 + a_{22}x_2 + a_2 \\ 1 \end{pmatrix}.$$

Logo, $[TP] = M_T[P]$, o que prova *(i)*. Sejam agora $P = (x_1, x_2) \in K^2$ e as transformações $T(x_1, x_2) = (y_1, y_2)$, como em (2.2), e $T'(x_1, x_2) = (z_1, z_2)$, tal que

$$T'(x_1, x_2) = \begin{cases} z_1 = b_{11}x_1 + b_{12}x_2 + b_1 \\ z_2 = b_{21}x_1 + b_{22}x_2 + b_2 \end{cases} .$$

Logo

$$T \circ T'(x_1, x_2) = \begin{cases} y_1 = a_{11}z_1 + a_{12}z_2 + a_1 \\ y_2 = a_{21}z_1 + a_{22}z_2 + a_2 \end{cases} =$$

$$= \begin{cases} y_1 = (a_{11}b_{11} + a_{12}b_{21})x_1 + (a_{11}b_{12} + a_{12}b_{22})x_2 + (a_{11}b_1 + a_{12}b_1 + a_1) \\ y_2 = (a_{21}b_{11} + a_{22}b_{21})x_1 + (a_{21}b_{12} + a_{22}b_{22})x_2 + (a_{21}b_2 + a_{22}b_2 + a_2) \end{cases}$$

Assim $M_{TT'}[P] =$

$$= \begin{pmatrix} (a_{11}b_{11} + a_{12}b_{21}) & (a_{11}b_{12} + a_{12}b_{22}) & (a_{11}b_1 + a_{12}b_1 + a_1) \\ (a_{21}b_{11} + a_{22}b_{21}) & (a_{21}b_{12} + a_{22}b_{22}) & (a_{21}b_2 + a_{22}b_2 + a_2) \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ 1 \end{pmatrix}$$

Por outro lado,

$$M_T M_{T'}[P] = \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{21} & a_{22} & a_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_1 \\ b_{21} & b_{22} & b_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} (a_{11}b_{11} + a_{12}b_{21}) & (a_{11}b_{12} + a_{12}b_{22}) & (a_{11}b_1 + a_{12}b_1 + a_1) \\ (a_{21}b_{11} + a_{22}b_{21}) & (a_{21}b_{12} + a_{22}b_{22}) & (a_{21}b_2 + a_{22}b_2 + a_2) \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ 1 \end{pmatrix}$$

Logo $M_T M_{T'}[P] = M_{TT'}[P]$ e como P foi arbitrário, $M_T M_{T'} = M_{TT'}$, e temos *(ii)*. Resta mostrar que Φ é isomorfismo. Suponha que $T \in \mathbb{T}$ é tal que

$$T(x_1, x_2) = \begin{cases} y_1 = a_1 + a_{11}x_1 + a_{12}x_2 \\ y_2 = a_2 + a_{12}x_1 + a_{22}x_2 \end{cases} , \text{ com } \Phi(T) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

Então $a_{11} = 1, a_{12} = 0, a_1 = 0, a_{21} = 0, a_{22} = 1$ e $a_2 = 0$. Logo T é a identidade de $\mathbb{T}$ e com isso $\ker \Phi = \{I\}$. Portanto, Φ é injetiva. Quanto à sobrejetividade, dado

$$M = \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{21} & a_{22} & a_2 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{M},$$

tome $T : K^2 \to K^2$, definida por

$$T(x_1, x_2) = \begin{cases} y_1 = a_1 + a_{11}x_1 + a_{12}x_2 \\ y_2 = a_2 + a_{12}x_1 + a_{22}x_2 \end{cases}.$$

Observe que $0 \neq \det M = \det \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{21} & a_{22} & a_2 \\ 0 & 0 & 1 \end{pmatrix} = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Logo, $T \in \mathbb{T}$. Como $\Phi(T) = M$ e M é arbitrário, temos que Φ é sobrejetiva e com isso Φ é isomorfismo. □

2.3 Transformação associada a um referencial

Escrevendo

$$v_1 = (a_{11}, a_{21}), v_2 = (a_{12}, a_{22}) \text{ e } O = (a_1, a_2),$$

podemos interpretar as equações (2.2) como a mudança de coordenadas de um ponto, isto é,

$$P = (y_1, y_2) \text{ com } (P)_R = (x_1, x_2).$$

E reciprocamente, podemos considerar as relações (2.1) como definindo a afinidade

$$(x_1, x_2) \mapsto O + x_1v_1 + x_2v_2,$$

o que identifica cada afinidade com uma mudança de coordenadas.

Definição 2.3.1. Dizemos que a afinidade T e o referencial R são associados se

$$(T(P)_R) = P \, (\forall P \in K^2).$$

Assim, podemos interpretar essa relação de duas formas diferentes: dada uma afinidade T, podemos olhar a relação

$$(y_1, y_2) = T(x_1, x_2)$$

como a fórmula que nos dá as novas coordenadas de um mesmo ponto em termos das antigas; os pontos ficam e muda-se o sistema de coordenadas. A outra possibilidade, é a de considerar T agindo sobre os pontos do plano: (y_1, y_2) é a nova posição de (x_1, x_2), com as coordenadas todas tomadas em relação ao referencial canônico; o sistema de coordenadas é preservado e os pontos se movem.

Definição 2.3.2. O K-automorfismo do anel de polinômios em 2 variáveis

$$T_\bullet : K[X_1, X_2] \to K[X_1, X_2]$$

associado à afinidade $T : K^2 \to K^2$ é dado por,

$$\forall (x_1, x_2) \in K^2, (T_\bullet f)(x_1, x_2) = f(T^{-1}(x_1, x_2)).$$

Mais precisamente, se

$$T^{-1}(x_1, x_2) = (b_{11}x_1 + b_{12}x_2 + b_1, b_{21}x_1 + b_{22}x_2 + b_2),$$

então

$$(T_\bullet f)(X_1, X_2) = f(b_{11}X_1 + b_{12}X_2 + b_1, b_{21}X_1 + b_{22}X_2 + b_2).$$

Agora, para introduzir o conceito de curva algébrica plana, considere o corpo K algebricamente fechado, isto é, todo polinômio não constate de $K[X]$ tem pelo menos uma solução. Considere também que K tem característica 0, isto é, $n \cdot 1 \neq 0, \forall n \in \mathbb{N}^*$ [1, pg. 8 e 9].

Definição 2.3.3. Uma *curva algébrica plana afim* (o qual chamaremos abreviadamente de *curva*) é uma classe de equivalência de polinômios não constantes $f \in K[X, Y]$, módulo a relação que identifica dois tais polinômios se um é múltiplo do outro por alguma constante em K. Nesse contexto, a *equação* de uma curva é um dos polinômios nessa classe. Dizemos que uma curva *está definida sobre o corpo* K_0, subcorpo de K, se ela admitir uma equação com coeficientes em K_0.

Definição 2.3.4. O *traço* de uma curva é o conjunto das soluções da equação, isto é $f = 0$, $f \in K[X, Y]$. As *componentes irredutíveis* de uma curva f são as curvas definidas pelos fatores irredutíveis de f. O grau de uma curva f é o grau de sua equação e será denotado por $deg(f)$. A *multiplicidade* de uma componente p de f é o expoente com que o fator p ocorre na decomposição de f, quando esta é maior ou igual a 2, dizemos que p é uma *componente múltipla de* f.

Exemplo 2.3.5. Uma das curvas que aparecerão com maior frequência neste trabalho é a reta, normalmente definida por l e tem a seguinte representação:

$$l : aY + bX + c.$$

Veremos, agora, que $T_\bullet$ preserva o traço da curva, ou seja, se P é um ponto do traço de uma curva f, TP é um ponto do traço da curva $T_\bullet f$.

Proposição 2.3.6. *Sejam f uma curva e T uma afinidade. Então o traço de $T_\bullet f$ é igual à imagem do traço de f por T.*

Demonstração. Seja $(x, y) \in V(f)$ onde $V(f)$ é o traço de $f \in K[X, Y]$. Então $T_\bullet f(T(x, y)) = f(T^{-1}T(x, y)) = f(x, y) = 0$. Com isso, $T(V(f)) \subset V(T_\bullet f)$. Reciprocamente, se $(x, y) \in V(T_\bullet f)$, então $T^{-1}(x, y) \in V(f)$ e assim

$$(x, y) = T(T^{-1}(x, y)) \in T(V(f)).$$

Portanto, $V(T_\bullet f) \subset T(V(f))$ e conclui-se que

$$V(T_\bullet f) = T(V(f)),$$

o que completa a demonstração. □

Proposição 2.3.7. *Sejam T uma afinidade e l uma reta de $K[X, Y]$. Temos que T induz um isomorfismo*

$$K[X, Y]/\langle l\rangle \quad \xrightarrow{\sim} \quad K[X, Y]/\langle T_\bullet l\rangle$$

tal que $f + \langle l\rangle$ e $T_\bullet f + \langle T_\bullet l\rangle$ se correspondem.

Demonstração. Se tomarmos as inclusões

$$\alpha : \langle l \rangle \to K[X,Y] \quad \text{e} \quad \beta : \langle T_\bullet l \rangle \to K[X,Y]$$

e os isomorfismos

$$\mu : \langle l \rangle \hookrightarrow \langle T_\bullet l \rangle \qquad \text{e} \qquad T_\bullet : K[X,Y] \hookrightarrow K[X,Y]\,,$$

$$fl \longmapsto T_\bullet(fl) \qquad\qquad f \longmapsto T_\bullet f$$

temos que

$$T_\bullet \circ \alpha(fl) = T_\bullet(fl) = \beta \circ T_\bullet(fl) = \beta \circ \mu(fl), \forall f \in K[X,Y].$$

Logo, pela proposição 1.1.3,

$$K[X,Y]/\langle l \rangle \simeq K[X,Y]/\langle T_\bullet l \rangle,$$

e segue a relação. □

Definição 2.3.8. Sejam T uma afinidade e R o referencial associado. A *equação* de uma curva f em relação ao referencial R é $(T_\bullet)^{-1} f$.

Veja que, para cada $P = (x, y)$ em K^2, temos

$$P \in V(f) \Leftrightarrow \quad f(x,y) = 0 \Leftrightarrow \quad ((T_\bullet)^{-1} f)(T^{-1}(x,y)) = 0$$

e como para algum $a \in K^2$ ocorre $T^{-1}(x,y) = a$, segue que $(T(a)_R) = a$ pois T é associado a R. Logo $(P)_R = T^{-1}(x,y)$. Temos que

$$P \in V(f) \Leftrightarrow \quad ((T_\bullet)^{-1} f)((P)_R) = 0.$$

O que demonstra a naturalidade da definição.

Definição 2.3.9. Dizemos que uma propriedade $\mathcal{P}$ relativa a curvas (ou configurações planas, tais como conjuntos de pontos, retas, etc.) é *invariante* ou *independente do referencial* se, para toda afinidade T, uma curva f (ou configuração C) satisfaz $\mathcal{P}$ se e só se $T_\bullet f$ (ou respectivamente $T(C)$) satisfaz $\mathcal{P}$.

Por exemplo, o grau de uma curva é uma propriedade invariante. As propriedades de três retas serem concorrentes, bem como a de um ponto pertencer a uma curva, são invariantes. Já o requerimento de que dois pontos no plano real sejam equidistantes de um terceiro não é invariante.

Proposição 2.3.10. *Um ponto ser colinear a dois outros é uma propriedade invariante.*

Demonstração. Sejam $(x, y), (u, v)$ e (c, d) pontos do plano. Suponha que estes três pontos sejam colineares, ou seja, o determinante da matriz

$$M = \begin{pmatrix} x & y & 1 \\ u & v & 1 \\ c & d & 1 \end{pmatrix},$$

é zero. Por outro lado, aplicando uma transformação como em (2.2) nos pontos $(x, y), (u, v)$ e (c, d), temos que provar que o determinante da matriz

$$N = \begin{pmatrix} (a_1 + a_{11}x + a_{12}y) & (a_2 + a_{21}x + a_{22}y) & 1 \\ (a_1 + a_{11}u + a_{12}v) & (a_2 + a_{21}u + a_{22}v) & 1 \\ (a_1 + a_{11}c + a_{12}d) & (a_2 + a_{21}c + a_{22}d) & 1 \end{pmatrix}$$

é zero. Observe que

$$\begin{pmatrix} (a_1 + a_{11}x + a_{12}y) & (a_2 + a_{21}x + a_{22}y) & 1 \\ (a_1 + a_{11}u + a_{12}v) & (a_2 + a_{21}u + a_{22}v) & 1 \\ (a_1 + a_{11}c + a_{12}d) & (a_2 + a_{21}c + a_{22}d) & 1 \end{pmatrix} = \begin{pmatrix} x & y & 1 \\ u & v & 1 \\ c & d & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} & 0 \\ a_{12} & a_{22} & 0 \\ a_1 & a_2 & 1 \end{pmatrix}.$$

Como $\det(AB) = \det(A)\det(B)$ e $\det(M) = 0$, então o determinante de N é zero, e portanto, os pontos sobre o novo referencial são colineares. Como a mudança de referencial foi arbitrária, está provado que a propriedade é invariante. □

Capítulo 3

Interseções de Curvas Planas

Quando queremos saber se duas curvas se intersectam e quais os pontos de interseção, precisamos conhecer antes as condições necessárias para que isso ocorra, pois, por exemplo, no caso de duas retas paralelas, isto é, que tem a mesma direção, elas nunca se encontram (após conhecermos o plano projetivo isso não será mais verdade). Mas em contrapartida, veremos que se duas curvas definidas num corpo algebricamente fechado tem uma componente em comum, há uma infinidade de pontos onde as curvas se intersectam. Assim, neste capítulo, veremos condições para que duas curvas tenham interseções finitas e, através do teorema dos zeros de Hilbert, saber que são diferentes de vazio e conheceremos a resultante, que nos dirá em que pontos se situam estas interseções.

3.1 Finitude da Interseção

Para demonstrarmos a finitude de uma interseção, precisamos de um lema muito importante que iremos demonstrar.

Lema 3.1.1. *Sejam $f, g \in K[X, Y]$ polinômios sem fatores irredutíveis em comum. Então existe uma relação*

$$wf + vg = u(X),$$

onde $w, v \in K[X, Y]$, enquanto u é um polinômio apenas na variável X, não nulo.

Resultado análogo vale trocando X por Y.

Demonstração. Denotaremos $A = K[X]$ e $L = K(X)$. Consideremos f, g como elementos de $L[Y]$. Pelo Lema de Gauss, como f, g não admitem fator comum em $A[Y]$, também não o admitem em $L[Y]$. Sendo $L[Y]$ um domínio de ideais principais, temos, pela proposição1.3.8, que existem $s, r \in L[Y]$, tais que

$$rf + sg = 1 \text{ em } L[Y].$$

Como $r = \dfrac{a}{b}$ e $s = \dfrac{c}{d}$ com $b, d \in A - \{0\}$ e $a, c \in A[Y]$, podemos reduzir rf e sg ao mesmo denominador. Assim,

$$rf + sg = \frac{daf + bcg}{db} = 1$$

e multiplicando a igualdade por db, eliminamos os denominadores e temos a relação do lema. Ou seja, se $w = da \in A[Y]$, $v = bc \in A[Y]$ e $u(X) = bd \in A$, então

$$wf + vg = u(X),$$

e temos o resultado. □

Se $f \in K[X]$ é um polinômio não constante, a equação $f(X) = 0$ admite no máximo um número finito de soluções. O próximo resultado é um versão deste fato para polinômios em duas variáveis.

Proposição 3.1.2. *O conjunto das soluções de um sistema de duas equações polinômiais com duas incógnitas sem fator irredutível em comum é finito.*

Para linguagem geométrica, temos, equivalentemente:

Proposição 3.1.3. *A interseção de duas curvas algébricas planas sem componentes em comum é finita.*

Demonstração. Aplicando o lema anterior aos polinômios $f, g \in K[X, Y]$ que não admitem fator em comum, obtemos relações

$$af + bg = c(X), uf + vg = w(Y),$$

onde a, b, c, u, v, w são polinômios, $c(X), w(Y)$ são não nulos e envolvem só variáveis indicadas. Dessas relações, é evidente que toda solução de $f = g = 0$ tem para abcissa uma raiz de $c(X)$ e para ordenada uma raiz de $w(Y)$, todas em número finito. □

Proposição 3.1.4. *O conjunto de pontos que não anulam um polinômio de n variáveis sobre um corpo algebricamente fechado é infinito.*

Demonstração. Faremos a demonstração por indução. Suponha $n = 1$. Um polinômio em uma variável sobre um corpo algebricamente fechado tem finitas soluções. Logo há infinitos[1] pontos que não anulam o polinômio. Suponha, agora, que a proposição é valida para n variáveis. Se $f \in K[X_1, X_2, ..., X_n, X_{n+1}]$, podemos escrever $f = \sum_{i=0}^{r} g_i(X_1, ..., X_n)X_{n+1}^i$ com cada $g_i(X_1, ..., X_n) \in K[X_1, X_2, ..., X_n]$, sendo r o grau de f em relação a X_{n+1} e $g_r(X_1, ..., X_n) \neq 0$. Pela hipótese de indução, $g_r(X_1, ..., X_n)$ possui infinitos pontos $(x_1, ..., x_n) \in K^n$ tais que $g_r(x_1, ..., x_n) \neq 0$. Para cada um destes pontos, $f(x_1, ..., x_n, X_{n+1})$ é um polinômio em uma variável não constante e assim, admite infinitos pontos que não são solução, o que prova a proposição. □

Proposição 3.1.5. *Sejam um corpo K algebricamente fechado e $f \in K[X_1, X_2, ..., X_n]$, tal que $n \geq 2$ e f é não constante. Então existem infinitos pontos $x_0 = (x_1, x_2, ..., x_n) \in K^n$ onde $f(x_0) = 0$.*

Demonstração. Seja $f \in K[X_1, X_2, ..., X_{n-1}, X_n]$. Podemos escrever

$$f = \sum_{i=0}^{r} g_i(X_1, ..., X_{n-1})X_n^i$$

com cada $g_i(X_1, ..., X_{n-1}) \in K[X_1, X_2, ..., X_{n-1}]$, sendo r o grau de f em relação a X_n e $g_r(X_1, ..., X_{n-1}) \neq 0$. Pela proposição 3.1.4, $g_r(X_1, ..., X_{n-1})$ admite infinitos pontos que não são raízes de g_r, então o conjunto $W := \{(x_1, ..., x_{n-1}) \mid g_r(x_1, ..., x_{n-1}) \neq 0\}$ é infinito. Portanto, para cada $(x_1, ..., x_{n-1}) \in W$ temos que $f(x_1, ..., x_{n-1}, X_n)$ é um polinômio em uma variável não constante e assim, admite um zero em K. Concluímos que, f possui infinitos pontos que o satisfazem. □

[1] Todo corpo K algebricamente fechado possui cardinalidade infinita, pois se fosse finito, digamos $K = \{a_1, ..., a_n\}$, então o polinômio $f(X) = (X - a_1) \cdot .... \cdot (X - a_n) + 1$ de $K[X]$ não teria raiz em K.

Corolário 3.1.6. *Se duas curvas têm componentes não constantes em comum, então existem infinitos pontos na interseção entre elas.*

Demonstração. Pela proposição anterior, basta perceber que o traço das duas curvas contém os mesmos infinitos pontos que anulam a componente em comum delas. □

3.2 O Teorema dos Zeros

Veremos agora, em que tipo de condições um sistema de equações polinomiais admite solução. Para isso, precisamos conhecer o teorema dos zeros de Hilbert (*Nullstellensatz*). Observemos que para um sistema de equações,

$$f_1 = ... = f_n = 0,$$

toda solução é também solução de qualquer equação do tipo

$$g_1 f_1 + ... + g_n f_n = 0,$$

onde os g_i's são polinômios arbitrários. Ora, mas um polinômio desta forma é gerado pelos $f_1, ..., f_n$. Assim denotamos por I o ideal de $K[X, Y]$ gerado por esses polinômios.

Definição 3.2.1. Dizemos que um ponto P é um *zero do ideal* I, se $f(P) = 0$, para todo $f \in I$. Denotamos por $V(I)$ o *conjunto de todos os zeros de* I.

Assim $V(I)$ coincide com o conjunto das soluções do sistema proposto inicialmente. Portanto, se o polinômio constante 1 pertence a I, é evidente que I não admite zero. Reciprocamente o Nullstellensatz afirma:

Teorema 3.2.2 (Nullstellensatz, forma fraca)**.** *Se I é um ideal próprio do anel dos polinômios com coeficientes em um corpo algebricamente fechado, então I admite um zero.*

O leitor interessado pode encontrar a versão forte do Nullstellensatz e sua demonstração em [6, pg. 82]. Para demonstrarmos a forma fraca precisaremos saber como são os ideais máximos de $K[X, Y]$.

Lema 3.2.3. *Seja I um ideal de $K[X,Y]$. Se $(x_0,y_0) \in V(I)$, então $I \subset \mathfrak{m}$, onde $\mathfrak{m} = \langle X - x_0, Y - y_0\rangle$.*

Demonstração. Suponha, por absurdo, que $I \not\subset \mathfrak{m}$. Tome $g \in I$ tal que $g \notin \mathfrak{m}$. Note que $\mathfrak{m} \subsetneqq \langle \mathfrak{m}, g\rangle$, logo $\langle \mathfrak{m}, g\rangle = K[X,Y]$. Portanto, existem $m \in \mathfrak{m}$ e $a, b \in K[X,Y]$, tais que $am + bg = 1$. Agora, $0 = a(x_0,y_0)m(x_0,y_0) + b(x_0,y_0)g(x_0,y_0) = 1$. Absurdo, logo $I \subset \langle X - x_0, Y - y_0\rangle$. □

Proposição 3.2.4. *Seja $(x,y) \in K^2$. Então $\mathfrak{m} = \langle X - x, Y - y\rangle$ é um ideal máximo em $K[X,Y]$.*

Demonstração. Observando o homomorfismo que substitui $X = x$ e $Y = y$, isto é

$$\begin{aligned} h : K[X,Y] &\longrightarrow K \\ f(X,Y) &\mapsto f(x,y), \end{aligned}$$

vemos que o núcleo deste é o ideal $\mathfrak{m}$. De fato, $\mathfrak{m} \subset \ker(h)$ e como $(x,y) \in V(\ker(h))$, pelo lema 3.2.3, $\ker(h) \subset \mathfrak{m}$. Logo, pelo teorema do homomorfismo, existe um isomorfismo $K[X,Y]/\mathfrak{m} \longrightarrow K$ e, sendo K corpo, $K[X,Y]/\mathfrak{m}$ também o é. Ora, mas o anel quociente $K[X,Y]/\mathfrak{m}$ define um corpo se, e só se, $\mathfrak{m}$ é máximo, o que completa a demonstração. □

Sabemos que todo ideal próprio $I \subset K[X,Y]$ está contido em algum ideal máximo. Agora, uma pergunta muito importante: Todo ideal máximo de $K[X,Y]$ é da forma $\mathfrak{m} = \langle X - x, Y - y\rangle$? Se sim, isso nos diz que se I é ideal próprio e $\mathfrak{m} = \langle X - x, Y - y\rangle$ é tal que $I \subset \mathfrak{m}$, então $P = (x,y)$ é um zero de I. Logo o Nullstellensantz é consequência da seguinte proposição que responde a nossa pergunta.

Proposição 3.2.5. *Se K é um corpo algebricamente fechado, então todo ideal máximo $\mathfrak{m}$ de $K[X,Y]$ é do tipo $\langle X - x, Y - y\rangle$ para algum ponto $(x,y) \in K^2$.*

Demonstração. Como $K[X,Y]$ não é corpo, então $\{0\}$ não é máximo. Assim, existe $f \in \mathfrak{m}$ com $f \neq 0$. Note que f não é constante, pois senão, teríamos $\mathfrak{m} = K[X,Y]$. Como $K[X,Y]/\mathfrak{m}$ é corpo, também é domínio de integridade e assim, $\mathfrak{m}$ é um ideal

primo, com isso, podemos supor f irredutível. Pela proposição 3.1.5, existe um ponto $(x_0, y_0) \in K^2$ tal que $f(x_0, y_0) = 0$. Se $(x_0, y_0) \in V(\mathfrak{m})$ então pelo lema 3.2.3, $\mathfrak{m} = \langle X - x_0, Y - y_0 \rangle$ e a proposição já está provada. Senão, existe $g \in \mathfrak{m}$ tal que $g(x_0, y_0) \neq 0$. Em particular, f não divide g. Aplicando o lema 3.1.1, temos que $af + bg = c$, sendo $a, b \in K[X, Y]$ e c um polinômio não constante de uma só variável, X ou Y, à nossa escolha. Escolhemos $c \in K[X]$. Como K é algebricamente fechado, então c pode ser fatorado em fatores lineares e sendo $\mathfrak{m}$ primo, temos que algum fator $X - x$, com $x \in K$, pertence a $\mathfrak{m}$. Analogamente, considerando o caso em que $c \in K[Y]$, temos $Y - y \in \mathfrak{m}$, para algum $y \in K$. Ou seja $\langle X - x, Y - y \rangle \subseteq \mathfrak{m}$. Como $\langle X - x, Y - y \rangle$ é máximo, concluímos que $\langle X - x, Y - y \rangle = \mathfrak{m}$. □

3.3 Resultante

Para acharmos as interseções de duas curvas em duas variáveis, normalmente consideramos uma das variáveis como coeficientes de um anel e que as curvas estão apenas em uma variável, ou seja se $f, g \in K[X, Y]$, consideramos $A = K[X]$ e $f, g \in A[Y]$, e a partir daí tentamos encontrar valores de x tais que $f(x, Y)$ e $g(x, Y)$ admitem raiz comum. Para realizarmos esse processo precisaremos entender uma ferramenta muito importante que se chama resultante.

Definição 3.3.1. Sejam A um anel comutativo (por exemplo, $A = K[X]$), $f = a_d Y^d + ... + a_0$ e $g = b_e Y^e + ... + b_0$, onde $d, e \geqslant 1$, polinômios com coeficientes em A. Definimos a *resultante* de f, g como

$$R = R_{f,g} = \det \begin{pmatrix} a_d & a_{d-1} & ... & a_0 & 0 & 0 & 0 & ... & 0 \\ 0 & a_d & ... & a_1 & a_0 & 0 & 0 & ... & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & ... & 0 & 0 & a_d & ... & & a_0 \\ b_e & b_{e-1} & ... & b_0 & 0 & 0 & 0 & ... & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & ... & 0 & 0 & 0 & b_e & ... & b_0 \end{pmatrix}_{(d+e)\times(d+e)},$$

ou seja, o determinante da matriz com e linhas de a's e d linhas de b's. Na matriz acima, os coeficientes de f figuram nas e primeiras linhas e os de g, nas d últimas linhas.

Veja que para esta definição, os polinômios f, g são considerados respectivamente de graus d e e, apesar de que a_d e b_e possam ser nulos. Porém convencionaremos atribuir o grau do polinômio ao maior grau efetivo em Y. Além disso, podemos considerar que os coeficientes a_i's, b_j's são também polinômios em outras variáveis $X_1, X_2, ..., X_n$.

Proposição 3.3.2. *Seja $\phi : A \to B$ um homomorfismo de anéis e denotemos pelo mesmo símbolo o homomorfismo induzido $A[Y] \to B[Y]$ definido por*

$$\phi\left(\sum a_i Y^i\right) = \sum \phi(a_i) Y^i.$$

Então $\phi(R_{f,g}) = R_{\phi(f),\phi(g)}$ para todo $f, g \in A[Y]$, onde os graus formais atribuídos a $\phi(f)$ e $\phi(g)$ são, respectivamente, os mesmos de f, g.

Demonstração. Basta aplicarmos a fórmula de Leibniz [3, pg. 256] para o cálculo de determinante. De fato, fazendo $n = deg(f) + deg(g)$, temos:

$$\phi(R_{f,g}) = \phi\left(\sum_{\sigma \in S_n} sng(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}\right) = \sum_{\sigma \in S_n} sng(\sigma) \prod_{i=1}^{n} \phi(a_{i,\sigma(i)}) = R_{\phi(f),\phi(g)}.$$

□

Exemplo 3.3.3. Sejam $f = Y^2 + X^2 - 4$ e $g = XY - 1$. Então a resultante de f e g em Y é

$$R_{f,g} = \det \begin{pmatrix} 1 & 0 & X^2 - 4 \\ X & -1 & 0 \\ 0 & X & -1 \end{pmatrix} = X^4 - 4X^2 + 1.$$

Por outro lado, para resolver o sistema

$$\begin{cases} X^2 + Y^2 &= 4 \\ XY &= 1 \end{cases},$$

podemos substituir $Y = 1/X$ na primeira equação e obter

$$X^4 - 4X^2 = -1.$$

O que nos diz que as interseções dessas curvas têm para abcissas as soluções dessa última equação. Não é coincidência que ela seja igual a resultante. Observe o lema e a proposição a seguir que nos mostrarão isso.

Lema 3.3.4. *Sejam $f = a_dY^d + ... + a_0$ e $g = b_eY^e + ... + b_0$ polinômios a coeficientes em um domínio de fatoração única D. Então*

$$R_{f,g} = 0 \Leftrightarrow \begin{cases} a_d = b_e = 0 \\ \textit{ou} \\ f, g \textit{ admitem fator comum não constante.} \end{cases}$$

Demonstração. Se $a_d = b_e = 0$, teremos uma coluna da matriz resultante com coeficientes todos zeros e assim seu determinante é igual a zero. Considere então o caso em que $a_d \neq 0$. Então f, g admitem fator comum h não constante se e só se existirem $p, q \in D[Y]$ ambos não nulos, com $deg(p) \leqslant d - 1$ e $deg(q) \leqslant e - 1$, tais que $f = ph$ e $g = qh$ e assim $fq = phq = pg$ e temos a seguinte relação:

$$qf = pg. \tag{3.1}$$

Visto que $D[Y]$ é fatorial temos, pela proposição 1.3.10, a relação (3.1) acarreta que algum fator irredutível de f ocorre em g. Agora, escrevendo

$$\begin{cases} p = & u_0Y^{d-1} + ... + u_{d-1}, \\ q = & v_0Y^{e-1} + ... + v_{e-1}, \end{cases}$$

a equação (3.1) é equivalente ao sistema linear de $d + e$ equações nas variáveis u_i, v_j obtido comparando os coeficientes de qf com os de pg. Mas especificamente,

$$\begin{cases} a_dv_0 - b_eu_0 & = 0 \\ a_{d-1}v_0 + a_dv_1 - b_{e-1}u_0 - b_eu_1 & = 0 \\ \vdots & \\ a_0v_{e-1} - b_0u_{d-1} & = 0 \end{cases} . \tag{3.2}$$

Ora, este sistema é linear homogêneo e só admite solução não trivial (onde não todos os u_j's e v_h's são nulos) se e só se é nulo o determinante da matriz dos coeficientes, o qual coincide com $R_{f,g}$, a menos de sinal. De fato, a matriz do sistema (3.2) é a transposta da matriz que define a resultante, trocando o sinal dos b_j. □

Agora se f e g são polinômios em várias variáveis temos o seguinte resultado:

Proposição 3.3.5. *Sejam*

$$\begin{cases} f = & a_d(X)Y^d + ... + a_0(X), \\ g = & b_e(X)Y^e + ... + b_0(X), \end{cases}$$

onde a_i, b_j são polinômios nas variáveis $X_1, X_2, ..., X_r$ com coeficientes no corpo K. Então, para cada $x = (x_1, x_2, ..., x_r)$, temos

$$R_{f,g}(x) = 0 \Leftrightarrow \begin{cases} a_d(x) = b_e(x) = 0 \\ \textit{ou} \\ f(x,Y), g(x,Y) \textit{ admitem fator comum não constante.} \end{cases}$$

Demonstração. Para cada $x \in K^r$, defina

$$\begin{array}{rl} \phi_x : K[X_1, X_2, ..., X_r, Y] \to & K[Y] \\ f(X_1, ...X_r, Y) \longmapsto & f(x,Y) \end{array}.$$

Pela proposição 3.3.2, a resultante de $f(x,Y)$ e $g(x,Y)$ é $R_{f,g}$. Por outro lado, $f(x,Y)$ e $g(x,Y)$ admitem uma raiz y em comum se e só se admitem um fator não constante $Y - y$ e como visto no lema 3.3.4 isso ocorre se, e só se, $R_{f,g} = 0$. □

Observemos que $R_{f,g}$ é identicamente nulo se e só se f, g admitem componentes em comum, caso em que $f \cap g$ não é finita. Quando a interseção é finita, podemos estimar o número de suas abcissas, que é limitado pelo grau da resultante $R(X)$. Porém podem ocorrer pontos de interseção com a mesma abcissa, caso onde $R_{f,g}$ tem um fator irredutível com multiplicidade maior que 1, logo nosso procedimento ainda não está muito refinado.

Exemplo 3.3.6. Sejam $f = X^2 + Y^2 - 2X$ (circunferência de raio 1 e centro em $(1,0)$) e $g = Y^2 - X$ (parábola invertida). Sua resultante em Y é $R_{f,g}(X) = X^2(X-1)^2$.

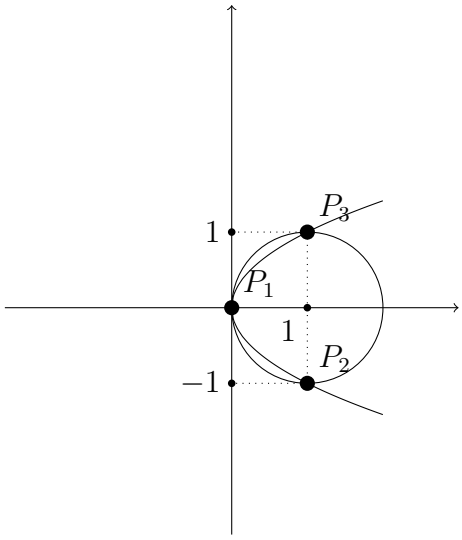

Figura 3.1: Interseção de $X^2 + Y^2 - 2X$ com $Y^2 - X$.

Fonte: O autor.

Note que o grau da resultante não fornece o número exato de interseções. A raiz dupla $x = 1$ é devido ao fato de que há dois pontos de interseção com a mesma abcissa. Porém a multiplicidade da raiz $x = 0$ não significa que há dois pontos distintos de interseção, mas pode ser interpretado como uma tangência entre as duas curvas. Se fizermos a resultante para X teremos

$$R(Y) = Y^2(Y - 1)(Y + 1).$$

Veja que há apenas a multiplicidade em $y = 0$. Isso diz respeito à posição relativa das curvas e não depende do referencial adotado.

Por este exemplo, podemos notar que o grau da resultante não reflete fielmente o número de interseções existentes entre duas curvas, por isso precisamos de ferramentas mais poderosas que veremos depois. Por agora, vejamos outros resultados provenientes desta ferramenta, mas para isso precisaremos de alguns conceitos.

Definição 3.3.7. Um polinômio *homogêneo* é um polinômio em que todos os seus termos (monômios) não nulos tem o mesmo grau.

Exemplo 3.3.8. O polinômio $x^5 + 2x^4y + 9x^2y^3$ é homogêneo de grau 5.

Proposição 3.3.9. *Seja* $f_m = \sum_{i=0}^{m} = a_i X^i Y^{m-i}$ *um polinômio homogêneo não nulo. Então* f_m *é o produto de* m *fatores lineares homogêneos, ou seja,* $f_m = \Pi(b_i X + c_i Y)$*, onde* b_i, c_i *são constantes não ambas nulas e as razões* b_i/c_i *são bem determinadas.*

Demonstração. Veja que

$$f_m = \sum_{i=0}^{m} a_i X^i Y^{m-i} = Y^m \sum_{i=0}^{c} a_i \left(\frac{X}{Y}\right)^i$$

onde c é o maior índice tal que $a_c \neq 0$. Como $\sum_0^c a_i \left(\frac{X}{Y}\right)^i$ é um polinômio na variável $\left(\frac{X}{Y}\right)$ de grau c então, pelo Teorema Fundamental da Álgebra, é decomposto em c fatores lineares, isto é,

$$\sum_0^c a_i \left(\frac{X}{Y}\right)^i = a_c \left(\frac{X}{Y} - r_o\right)\left(\frac{X}{Y} - r_1\right) ... \left(\frac{X}{Y} - r_c\right),$$

onde as constantes r_i's são raízes de $\sum_0^c a_i \left(\frac{X}{Y}\right)^i$, e com isso

$$\begin{aligned} f_m &= a_c Y^m \left(\frac{X}{Y} - r_o\right)\left(\frac{X}{Y} - r_1\right) ... \left(\frac{X}{Y} - r_c\right) \\ &= a_c Y^{m-c} \left(X - r_o Y\right)\left(X - r_1 Y\right) ... \left(X - r_c Y\right). \end{aligned}$$

□

Definição 3.3.10. Seja o polinômio

$$f = f_0 + f_1 + ... + f_d,$$

onde cada f_i é homogêneo de grau i, e $f_d \neq 0$. Como visto pela proposição 3.3.9, f_d pode ser escrito como produto de fatores lineares. Dizemos que cada componente $aX + bY$ de f_d é uma *direção assintótica* de f.

Intuitivamente, as direções assintóticas são as direções das retas passando pela origem e intersectando pontos da curva que se afastam indefinidamente da origem.

Exemplo 3.3.11. $f = Y^2 - X$ tem apenas direção assintótica Y. Agora, veja que $g = 1 - XY$ tem direções assintóticas X e Y, como se observa na imagem:

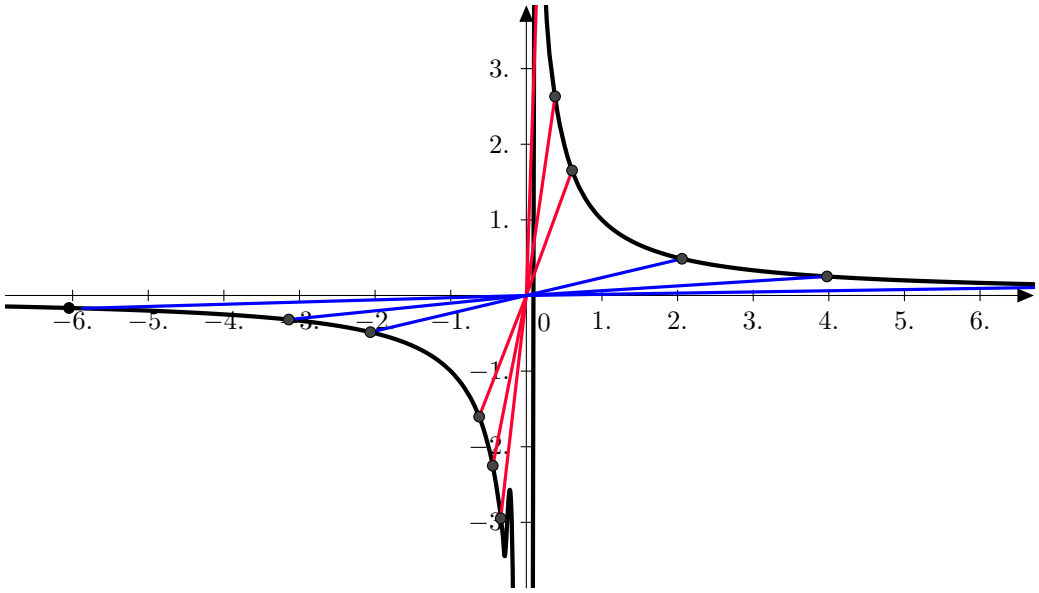

Figura 3.2: direções assintóticas de $g = 1 - XY$.

Fonte: O autor.

Proposição 3.3.12. *Se $f, g \in K[X, Y]$ não tem direção assintótica em comum, então também não tem componentes em comum.*

Demonstração. Suponha por contradição que f, g têm componente em comum $aX + bY$ e que $deg(f) = d$ e $deg(g) = e$. Assim $f = (aX + bY)(f_{d-1} + ... + f_0)$ e $g = (aX + bY)(g_{e-1} + ... + g_0)$ onde f_i, g_j são polinômios homogêneos e $deg(f_i) = i$ e $deg(g_j) = j$. Assim $f = (aX+bY)f_{d-1}+...+(aX+bY)f_0$ e $g = (aX+bY)g_{e-1}+ ... + (aX + bY)g_0$ e portanto, f, g tem direção assintótica em comum. □

Observação 3.3.13. A reciproca desta proposição é falsa, pois se $f = X + 1$ e $g = XY + 1$, observamos que g e f não tem componentes em comum, mas tem direção assintótica X em comum.

Lema 3.3.14. *Um polinômio não nulo $p(X_1, ..., X_n)$ a n variáveis é homogêneo de grau m se e só se vale a identidade*

$$p(TX_1, ..., TX_n) = T^m p(X_1, ..., X_n) \text{ em } K[X_1, ..., X_n, T],$$

onde T é uma nova variável independente.

Demonstração. Sendo p homogêneo, é imediato que a relação vale. Reciprocamente, suponhamos válida a relação e escrevamos

$$p = p_0 + p_1 + ... + p_r,$$

onde o lado direito é soma de polinômios homogêneos com $deg(p_i) = i$, $p_r \neq 0$. Abreviando $X = (X_1, ..., X_n)$, temos

$$p(TX) = p_0 + Tp_1 + ... + T^r p_r = T^m p$$

donde, pela definição de igualdade de polinômios em T, segue-se $m = r$ e $p = p_r$. □

Lema 3.3.15. *Sejam $F, G \in K[X, Y, Z]$ polinômios homogêneos de grau d e e, respectivamente. Então a resultante $R_{F,G}(X, Z)$ é homogêneo de grau $d \cdot e$, se não for identicamente nulo.*

Demonstração. Mostraremos que

$$R(TX, TZ) = T^{de} R(X, Z) \text{ em } K[X, Z, T].$$

Escrevendo $F = A_0 Y^d + ... + A_d$ e $G = B_0 Y^e + ... + B_e$, onde $A_i, B_j \in K[X, Z]$ são homogêneos e $deg(A_i) = i$, $deg(B_j) = j$ obtemos, aplicando T às coordenadas da resultante,

$$R(TX, TZ) = \det \begin{pmatrix} A_0 & TA_1 & ... & T^d A_d & & \\ & A_0 & ... & T^{d-1} A_{d-1} & T^d A_d & \\ \vdots & \vdots & & \vdots & \vdots & \\ B_0 & TB_1 & ... & \vdots & \vdots & T^e B_e \dots \\ \vdots & \vdots & & \vdots & \vdots & \vdots \end{pmatrix}.$$

Multiplicamos a segunda linha por T, a terceira por T^2,..., a e-ésima por T^{e-1}, a segunda linha de B's por T,..., a última por T^{d-1}. Resulta que a 2ª coluna fica divisível por T, a 3ª por T^2, $etc.$ obtemos assim

$$T^N R(TX, TZ) = T^M R(X, Z),$$

onde $N = (1 + \cdots + e - 1) + (1 + \cdots + d - 1)$, $M = 1 + 2 + \cdots + d + e - 1$. Logo, por propriedade de soma de progressão aritmética,

$$M - N = \frac{(d+e)(d+e-1)}{2} - \left(\frac{e(e-1)}{2} + \frac{d(d-1)}{2} \right) = d \cdot e,$$

o que completa a demonstração. □

Proposição 3.3.16. *O grau da resultante de duas curvas sem direção assintótica em comum é igual ao produto dos graus. Ou seja,*

$$deg(R_{f,g}) = (deg(f))(deg(g)).$$

A resultante é tomada atribuindo-se a f, g seus graus efetivos.

Demonstração. Para cada polinômio $f = \sum_0^d f_i$, com f_i homogêneo de grau i e $f_d \neq 0$, ponhamos

$$f^*(X, Y, Z) = Z^d f_0 + Z^{d-1} f_1 + ... + Z f_{d-1} + f_d,$$

onde Z é uma nova variável (independente de X, Y). Observamos que f^* é um polinômio homogêneo de grau $d = deg(f)$, e obviamente $f^*(X, Y, 1) = f(X, Y)$. Reescrevendo f^*, g^* na forma

$$\begin{array}{rl} f^* = & A_0 Y^d + ... + A_d \\ g^* = & B_0 Y^e + ... + B_e \end{array},$$

onde $A_i, B_j \in K[X, Z]$ são homogêneos e $deg(A_i) = i$, $deg(B_j) = j$. Calculemos a resultante

$$R(X, Z) = \det \begin{pmatrix} A_0 & ..... & A_d & & & \\ & & & ..... & & \\ & & & A_0 & ..... & A_d \\ B_0 & ..... & B_e & & & \\ & & & ..... & & \\ & & & B_0 & ..... & B_e \end{pmatrix}.$$

Vamos comparar $R(X,Z)$ com $R_{f,g}(X)$. Veja pela proposição 3.3.2 que $R(X,1)$ é a resultante de f,g considerados *formalmente* como polinômios em Y de graus d,e. Agora observemos que os coeficientes A_0, B_0 de Y^d e Y^e em f^* e g^* são constantes, sendo nulos se e só se Y^d e Y^e não ocorrem em f_d e g_e respectivamente. A condição $A_0 = 0$ é equivalente a X ser fator de f_d. Como f e g não tem direções assintóticas em comum, segue-se que, sem perda de generalidade, $A_0 \neq 0$. Seja j o menor índice tal que $B_j \neq 0$. Assim o determinante pode ser desenvolvido, utilizando o método de Laplace[7, pg. 122], pelas j primeiras colunas, e, obtemos

$$R(X,1) = \det \begin{pmatrix} A_0 & \dots & A_d(X,1) & 0 & & & \dots & & 0 \\ 0 & A_0 & \dots & A_d(X,1) & 0 & & \dots & & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & & \dots & & 0 \\ 0 & \dots & \dots & A_0 & \dots & A_d(X,1) & 0 & \dots & 0 \\ 0 & \dots & \dots & \ddots & \ddots & \ddots & 0 & \dots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & A_0 \dots & A_d(X,1) \\ 0 & \dots & \dots & B_j & \dots & B_e(X,1) & 0 & \dots & 0 \\ 0 & \dots & \dots & 0 & B_j & \dots & B_e(X,1) & 0 \dots & 0 \\ 0 & \dots & \dots & \ddots & \ddots & & \ddots & 0 \dots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & B_j \dots & B_e(X,1) \end{pmatrix}$$

j-colunas $\qquad$ $R_{f,g}(X)$

$$R(X,1) = A_0^j R(X). \tag{3.3}$$

Como f e g não têm direção assintótica em comum então, pela proposição 3.3.12, não têm componente em comum. Logo $R(X) \neq 0$ e portanto $R(X,Z) \neq 0$. Pelo lema 3.3.15, o grau de $R(X,Z)$ é $d \cdot e$. Com isso, $R(X,1)$ tem grau $d \cdot e$, a menos que $R(X,Z)$ seja múltiplo de Z. Mas neste último caso, $R(1,0) = 0$, acarretando que f^* e g^* tem uma interseção, ou seja,

$$f_d(1,y) = f^*(1,y,0) = 0 = g^*(1,y,0) = g_e(1,y)$$

para algum y. Segue-se que f,g admitiriam ambos a direção assintótica $yX - Y$,

proibido por hipótese. Portanto, de fato, $R(X, 1)$ tem grau $d \cdot e$. Assim o resultado segue de (3.3). □

Capítulo 4

Multiplicidade

Neste capítulo, introduziremos o conceito de multiplicidade de um ponto de um curva, que intuitivamente equivale a dizer quantas vezes a curva passa em um mesmo ponto. Para compreender esse conceito, precisamos iniciar nosso estudo averiguando como se dá a interseção de uma curva com uma reta, pois veremos que a questão de multiplicidade de um ponto da curva está relacionada à tangência de uma determinada reta passando por esse ponto.

4.1 Interseção de uma curva com uma reta

Sejam f uma curva e l uma reta de equação $Y = aX + b$. Os pontos de $f \cap l$ podem ser obtidos eliminando Y e resolvendo a equação

$$f_l(X) := f(X, aX + b) = 0.$$

Em função da proposição 3.1.3, temos as seguintes possibilidades:

1. $f_l(X)$ é identicamente nulo, caso em que l é uma componente de f;

2. $f_l(X)$ é uma constante não nula, quando $f \cap l = \emptyset$;

3. $f_l(X)$ é um polinômio não constante, decompondo-se na forma

$$f_l(X) = c\prod_{i=1}^{r}(X - x_i)^{m_i},$$

onde c é uma constante e os x_i são as abcissas (duas a duas distintas) dos pontos de interseção. Procede-se de maneira evidente quando l é da forma $X = cY + d$.

Lema 4.1.1. *Os inteiros m_i independem do referencial afim.*

Demonstração. Seja $\phi : K[X,Y] \to K[X]$ o homomorfismo de anéis onde $\phi(X) = X$ e $\phi(Y) = aX + b$. Ou seja, ϕ é o homomorfismo sobrejetor dado por:

$$\begin{array}{rcl} \phi : K[X,Y] & \longrightarrow & K[X] \\ g & \longmapsto & g(X, aX+b), \end{array}$$

cujo núcleo é o ideal $\langle l \rangle$ gerado por $l = Y - (aX + b)$. Logo, pelo teorema do homomorfismo, obtemos um isomorfismo

$$K[X,Y]/\langle l \rangle \quad \xrightarrow{\sim} \quad K[X]$$

tal que a classe $\overline{f}$ de f módulo $\langle l \rangle$ corresponde a f_l. Visto que $K[X]$ é domínio fatorial, à decomposição $\prod (X - x_i)^{m_i}$ de f_l corresponde uma (única!) decomposição de $\overline{f}$ em fatores irredutíveis, com o mesmo número r de fatores irredutíveis distintos, sendo o i-ésimo fator repetido m_i vezes. Temos, pela proposição 2.3.7, que

$$K[X,Y]/\langle l \rangle \quad \xrightarrow{\sim} \quad K[X,Y]/\langle T_\bullet l \rangle \ ,$$

onde as decomposições em fatores irredutíveis se correspondem e, portanto, os inteiros m_i não dependem do referencial afim. □

Definição 4.1.2. A *multiplicidade* ou *índice de interseção* de l, f no ponto P é dada por

$$(l,f)_P = \begin{cases} 0 & \text{se} \quad P \notin l \cap f \\ \infty & \text{se} \quad P \in l \subset f \\ m_i & \text{se} \quad P = (x_i, ax_i + b) \text{ como no caso (3) acima.} \end{cases}$$

Se $l \not\subset f$, chamamos o inteiro

$$m_\infty := deg(f) - \sum_{i=1}^{r} m_i$$

de *multiplicidade de interseção* de l, f no *ponto impróprio ou ponto de l no infinito*.

Exemplo 4.1.3. Se considerarmos $K = \mathbb{R}$, a curva $f = X^2 - 2X - Y$ e a reta $l = X - 1$ se intersectam apenas no ponto $(1, -1)$. Como $deg(f) = 2$, temos que $m_\infty = 1$. Observe a imagem

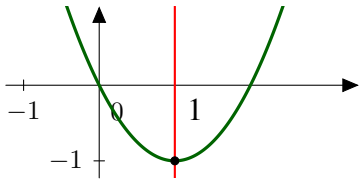

Figura 4.1: Interseção de $X^2 - 2X - Y$ com a reta $X - 1$.

Fonte: O autor.

O significa intuitivo dessas multiplicidades é que, arbitrariamente próximo à curva f, existem curvas do mesmo grau que cortam l em $deg(f)$ pontos distintos, m_i dos quais estão próximos a (x_i, ax_i+b), os m_∞ restantes distanciando-se para ∞ sobre l.

Proposição 4.1.4. *m_∞ é positivo se, e somente se, a direção de $l = Y - (aX + b)$ é uma direção assintótica de f.*

Demonstração. Suponha que $m_\infty > 0$. Definimos $d := deg(f)$ e assim $d > \sum_{i=1}^{r} m_i = deg(f_l(X))$. Escrevendo $f = f_d + ... + f_0$, onde os f_i's são polinômios homogêneos e $deg(f_i) = i$, podemos fatorar f_d da forma $f_d = \prod(e_iX + c_iY)$. Segue que

$$f_l = f_d(X, aX + b) + ... + f_0(X, aX + b),$$

donde $deg(f_d(X, aX + b)) < d$ e, portanto, pelo menos um dos fatores lineares de f_d aplicados a $(X, aX + b)$ é constante α, isto é, para algum fator $cY + eX$ de f_d temos que

$$\alpha = c(aX + b) + dX = X(ca + e) + cb.$$

E com isso $ca + e = 0$, que nos garante $cY + eX = c(Y - aX)$ e portanto, f tem uma direção assintótica igual a direção da reta. Reciprocamente, suponha que $f_d = (aX - Y)g(X, Y)$, com $deg(g(X, Y)) = d - 1$. Então

$$f_d(X, aX + b) = (aX - aX - b)g(X, aX + b) = (-b)g(X, aX + b),$$

logo $deg(f_d(X, aX + b)) \leq d - 1$, e segue que

$$deg(f_l(X)) \leq \max\{d - 1, deg(f_d(X, aX + b)) \leq d - 1.$$

Com isso

$$m_\infty = deg(f) - \sum_{i=1}^{r} m_i = deg(f) - deg(f_l) > 0,$$

e fica demonstrado a proposição. □

4.2 Pontos múltiplos

Vimos como é a questão da multiplicidade da interseção de uma curva com uma reta, mas nesta seção iremos ver a noção de multiplicidade de um ponto sobre uma curva.

Proposição 4.2.1. *Seja f uma curva e seja P um ponto de f. Existe um inteiro $m = m_P(f) \geqslant 1$, tal que, para toda reta l passando por P, temos*

$$(l, f)_P \geqslant m,$$

ocorrendo a desigualdade estrita para no máximo m retas e no mínimo uma.

Demonstração. Pelo lema 4.1.1, o índice de interseção não depende do referencial abordado, então suporemos, sem perda de generalidade, $P = O$ e com isso, pelo *Nullstellensatz* $f \in \langle X, Y \rangle$, ou seja, todos os seus termos tem grau maior ou igual a 1. Assim, podemos escrever

$$f = f_m + ... + f_d, \tag{4.1}$$

com f_i homogêneo de grau i para $m \leqslant i \leqslant d$, e $\deg(f_m) > 0$. Mudando coordenadas se necessário, podemos supor que $X \nmid f_m$. Veja que, $f_i(0, Y) = f_i(0, 1)Y^i$, e portanto, podemos fazer

$$f(0, Y) = Y^m(f_m(0, 1) + ... + f_d(0, 1)Y^{d-m}),$$

em que $f_m(0, 1) \neq 0$. Daí vem que $(X, f)_O = m$, ou seja, a multiplicidade do ponto P da interseção de f com a reta $l : X = 0$ é m, pois $f(0, Y)$ tem exatamente m raízes

$Y = 0$. Para as demais retas passando por O, ponhamos $l_t = Y - tX$. Se escrevermos $f(X, tX)$, podemos deduzir que cada fator se escreve da forma

$$f_i(X, tX) = X^i f_i(1, t).$$

Temos então,

$$f(X, tX) = X^m(f_m(1, t) + f_{m+1}(1, t)X + ... + f_d(1, t)X^{d-m}).$$

Deduzimos que

$$(l_t, f)_O \geqslant m,$$

ocorrendo igualdade se e só se $f_m(1, t) \neq 0$. Como $X \nmid f_m$, segue-se que $f_m(1, t)$ é um polinômio em t de grau $m(\geqslant 1)$ e que portanto se anula para ao menos um e no máximo m valores de t distintos. □

Para todo ponto $P = (x_0, y_0)$ de uma curva f podemos aplicar uma afinidade T, da forma

$$\begin{array}{rccc} T: & K^2 & \longrightarrow & K^2 \\ & (X, Y) & \longrightarrow & (X - x_0, Y - y_0) \end{array},$$

para transladarmos o ponto P para origem. Assim, o K-automorfismo associado a T aplicado a f é escrito como

$$T_\bullet f(X, Y) = f(T^{-1}(X, Y)) = f(X + x_0, Y + y_0).$$

Ou seja, para mudarmos o referencial, em vista de transladarmos o ponto $P = (x_0, y_0)$ de uma curva f para a origem, devemos aplicar $X = X + x_0$ e $Y = Y + y_0$. Note que $T_\bullet f$ é da forma (4.1), onde $m = m_p(f)$. Agora que sabemos como fazer essa mudança de coordenadas, podemos definir a multiplicidade de um ponto de uma curva.

Definição 4.2.2. O inteiro $m = m_P(f)$ descrito na proposição acima é a *multiplicidade do ponto P na curva f* ou *multiplicidade de f em P*. Se $P \notin f$, convencionamos $m_P(f) = 0$, e se $P = (x, y) \in f$, escrevemos

$$f(X + x, Y + y) = f_m(X, Y) + (\text{ termos de grau } > m).$$

O polinômio homogêneo $f_m(X, Y)$ pode ser decomposto de maneira única,

$$f_m = \prod (a_i X + b_i Y)^{e_i},$$

onde os fatores lineares $a_i X + b_i Y$ são retas distintas. As retas

$$l_i = a_i(X - x) + b_i(Y - y)$$

são denominadas as *retas tangentes* de f em P. O expoente e_i é a *multiplicidade da tangente* l_i.

A demonstração da proposição 4.2.1 mostra que $(l, f)_P > m = m_P(f)$ justamente para l igual a uma das retas tangentes a f em P.

Dizemos que um ponto P de uma curva f é *liso*, ou *não singular* ou *simples* em f e que f é *lisa*, ou *não singular* ou *simples* em P se $m_P(f) = 1$; singular caso contrário. A curva f é *lisa* ou *não singular* se $m_P(f) = 1$ para cada $P \in f$. Se $m_P(f) = 2, 3, ..., m$, P é dito um ponto *duplo, triplo,..., m-uplo*. Um ponto *m-uplo* $P \in f$ é *ordinário* se f admitir m tangentes distintas no ponto P. Uma *cúspide* é um ponto duplo com tangente coincidentes. Um *nó* é um ponto duplo ordinário.

Exemplo 4.2.3. A curva $X^2 - Y(Y^2 + X^2)$ tem uma cúspide na origem com tangente vertival $X = 0$.

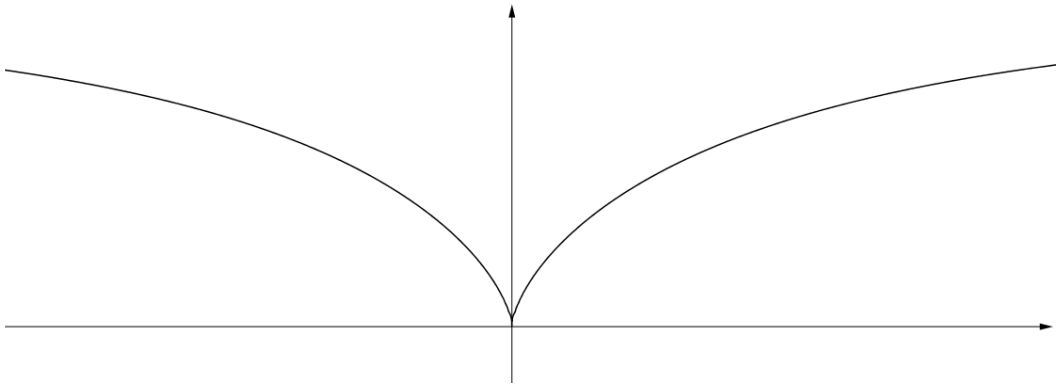

Figura 4.2: Curva $X^2 - Y(Y^2 + X^2)$.

Fonte: O autor.

Exemplo 4.2.4. A curva $(X^2+Y^2)^2 = X^2 - Y^2$ tem um nó na origem, com tangentes $Y = \pm X$.

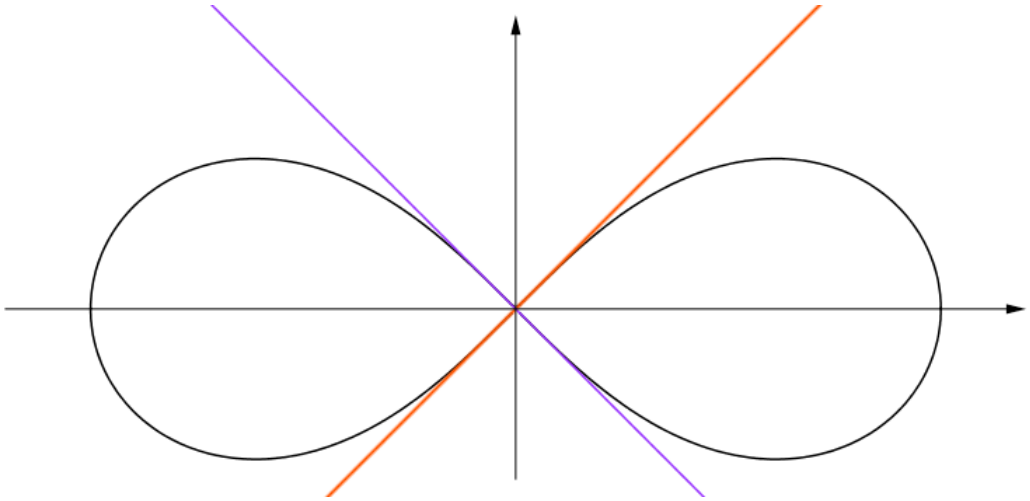

Figura 4.3: Curva $(X^2 + Y^2)^2 = X^2 - Y^2$.

Fonte: O autor.

Capítulo 5

Pontos no Infinito

Ao estudarmos a interseção de curvas algébricas, verificamos que em alguns casos há um espécie de paralelismo entre curvas, isto é, como no caso de retas, as curvas seguem a mesma direção (direção assintótica) e parecem nunca se tocar. Assim temos a sensação de que "faltam" interseções que nunca ocorrerão. Por esse desconforto que sentimos nessa sensação de "falta" de interseções vamos construir um espaço onde existem pontos no infinito, isto é, pontos onde curvas com mesma direção assintótica se tocam. Para isso precisamos definir esse novo espaço, que no final das contas, trataremos os pontos no infinito da mesma forma que tratamos os pontos que não estarão no infinito, o qual estamos acostumados a trabalhar.

5.1 Topologia quociente

Para trabalharmos nesse novo espaço, precisamos de noções topológicas para adentrar de maneira sólida neste novo ambiente. Assim, nesta seção, definiremos a topologia quociente a qual iremos utilizar na definição de espaço projetivo.

Definição 5.1.1. Dada uma aplicação $f : A \to B$, dizemos que o conjunto $f(A) = \{f(x) : x \in A\}$, dos elementos $f(x) \in B$ tal que $x \in A$, é chamado a *imagem da aplicação*.

Definição 5.1.2. Dado a aplicação $f : A \to B$, consideremos um subconjunto $Z \subset B$.

A *imagem inversa* de Z por f é o conjunto $f^{-1}(Z)$ dos elementos de A que se aplicam por f em elementos de Z. Isto é:

$$f^{-1}(Z) = \{x \in A; f(x) \in Z\}.$$

As imagens inversas se comportam bem relativamente às operações com conjuntos. São válidas as seguintes propriedades, onde Z e W indicam subconjuntos de B e $(B_\lambda)_{\lambda \in M}$ uma família qualquer de subconjuntos de B:

$$\begin{aligned} f^{-1}(\cup_{\lambda \in M} B_\lambda) &= \cup_{\lambda \in M} f^{-1}(B_\lambda); \\ f^{-1}(Z \cap W) &= f^{-1}(Z) \cap f^{-1}(W); \\ f^{-1}(Z - W) &= f^{-1}(Z) - f^{-1}(W); \\ Z \subseteq W &\Rightarrow f^{-1}(Z) \subseteq f^{-1}(W); \\ f^{-1}(B) &= A; \\ f^{-1}(\emptyset) &= \emptyset. \end{aligned}$$

Definição 5.1.3. Seja R uma relação de equivalência num conjunto A. Para cada elemento $x \in A$ indiquemos com C_x o conjunto de todos os elementos $y \in A$ que são equivalentes a x segundo a relação R:

$$C_x = \{y \in A;\ yRx\}.$$

Definição 5.1.4. O *conjunto quociente* de um conjunto A por uma relação de equivalência R é o conjunto A/R, cujos elementos são as classes de equivalência dos elementos de A segundo a relação R:

$$A/R = \{C_x;\ x \in A\}.$$

Nas condições definidas acima, existe uma aplicação natural $\pi : A \to A/R$, definida por $\pi(x) = C_x$. A aplicação π é chamada de *aplicação canônica* de A sobre A/R.

Definição 5.1.5. Uma *topologia* num conjunto X é uma coleção τ de subconjuntos de X, chamados os *subconjuntos abertos* (segundo a topologia τ) satisfazendo às seguintes condições:

1. X e o subconjunto vazio $\emptyset$ são abertos;

2. a reunião de uma família qualquer de subconjuntos abertos é um subconjunto aberto;

3. a interseção de uma família finita de subconjuntos abertos é um subconjunto aberto.

Observação 5.1.6. É equivalente, em vez 3., afirmar apenas que a interseção de *dois* abertos é um aberto, pois para n abertos, $n \in \mathbb{N}$, podemos concluir por indução.

Definição 5.1.7. Um *espaço topológico* é um par (X, τ) onde X é um conjunto e τ uma topologia em X.

Normalmente nos referiremos apenas a "espaço topológico X"sem mencionar o τ. Só o mencionamos quando for necessário.

Exemplo 5.1.8.

1. Seja qualquer conjunto X. Podemos definir uma topologia τ_0 em X tomando *todos* os subconjuntos de X como abertos. τ_0 chama-se *topologia discreta*.

2. Para qualquer conjunto X podemos tomar também uma topologia τ_1 em X, na qual os únicos abertos são X e o conjunto vazio $\emptyset$, também chamada de *topologia caótica*.

3. No caso dos números reais, usamos a topologia τ_2 usual sobre $\mathbb{R}$, na qual os abertos de $\mathbb{R}$ são os conjuntos A tal que $A = int(A)$, a saber, $int(A)$ é o conjunto dos pontos interiores [4, pg. 35] de A.

Definição 5.1.9. Se (X, τ) é um espaço topológico, $x \in X$ e $V \subset X$, diz-se que V é uma *vizinhança* de x se V contém algum aberto A tal que $x \in A$.

Definição 5.1.10. Sejam X e X' espaços topológicos e $a \in X$. Diz-se que uma função $f : X \to X'$ é *contínua em* a se, para cada vizinhança V de $f(a)$, $f^{-1}(V)$ for uma vizinhança de a. Caso contrário, diz-se que f é *descontínua* em a.

Definição 5.1.11. Sejam X e X' espaços topológicos. Diz-se que $f : X \to X'$ é *contínua* se, para cada aberto A de X', $f^{-1}(A)$ for um aberto de X. Caso contrário, diz-se que f é *descontínua*.

Antes de definirmos topologia quociente, vamos nos utilizar de uma forma mais geral de topologia que abrange também a topologia quociente.

Proposição 5.1.12. *Sejam X um espaço topológico, Q um conjunto qualquer e $\phi : X \to Q$ uma aplicação de X em Q. Indiquemos por τ a coleção dos subconjuntos $B \subset Q$ tais que $\phi^{-1}(B)$ é aberto em X. Então τ é uma topologia sobre Q.*

Demonstração. Por propriedades de imagem inversa, temos

1. $\phi^{-1}(Q) = X$ e $\phi^{-1}(\emptyset) = \emptyset$ são abertos de X, pois este é espaço topológico. Assim, Q e $\emptyset$ são abertos de Q;

2. se $(A_\lambda)_{\lambda \in M}$ é uma família qualquer de abertos de Q então vale que

$$\phi^{-1}(\cup_{\lambda \in M} A_\lambda) = \cup_{\lambda \in M} \phi^{-1}(A_\lambda)$$

   que é um subconjunto aberto de X, pois é a união de uma família de abertos do espaço topológico X. Logo $\cup_{\lambda \in M} A_\lambda$ é um aberto de Q;

3. se $Z, W \in Q$ são abertos, então $f^{-1}(Z \cap W) = f^{-1}(Z) \cap f^{-1}(W)$ que é um subconjunto aberto de X, pois é a interseção finita de abertos. Logo $Z \cap W$ é um aberto de Q.

Por 1., 2. e 3. fica provado que τ é uma topologia. □

Definição 5.1.13. Chamamos a topologia acima descrita como *topologia co-induzida*.

Agora considere o seguinte: seja X um espaço topológico e E uma relação de equivalência em X. No conjunto $Q = X/E$, quociente de X pela relação E, consideramos a topologia co-induzida pela aplicação canônica $\sigma : X \to X/E$, que associa a cada $x \in X$ a classe de equivalência $\sigma(x)$ que o contém. Esta é a *topologia quociente* de X/E. A aplicação σ chama-se *aplicação quociente*. Para mais informações sobre Topologia, pode-se consultar [5].

5.2 O plano projetivo

Seja K um corpo. Consideremos o plano afim K^2 mergulhado no espaço tridimensional K^3 como $\pi : Z = 1$.

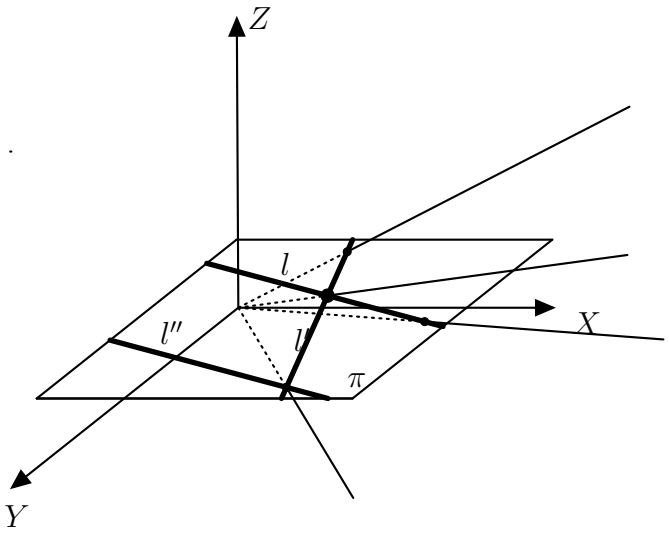

Figura 5.1: Plano projetivo.

Fonte: o autor.

Cada ponto do plano π determina uma reta passando por ele e pela origem. Cada reta de π determina um plano com a origem. Se as retas $l, l' \subset \pi$ se encontram, seu ponto de interseção dá lugar à reta de interseção dos dois planos associados a l, l'. Se as retas $l, l'' \subset \pi$ são paralelas então os planos que elas definem ainda se cruzam. Esta interseção é feita ao longo de uma reta passando pela origem e contida no plano $Z = 0$.

Definição 5.2.1. O *plano projetivo* $\mathbb{P}^2(K)$ é o conjunto das retas do espaço tridimensional K^3 passando pela origem.

Por abuso de notação, as vezes denotaremos apenas por $\mathbb{P}^2$ o plano projetivo e cada reta será dita um ponto do plano projetivo.

Note que o plano π se identifica naturalmente com um subconjunto de $\mathbb{P}^2$ que também denotaremos por π. Os pontos de $\mathbb{P}^2 \setminus \pi$ são chamados de *pontos no infinito*. Denotaremos por $(x : y : z)$ o ponto de $\mathbb{P}^2$ que representa a reta ligando a origem O a

um ponto $(x, y, z) \neq O$. Dizemos que x, y, z são *coordenadas homogêneas* do ponto (x, y, z) relativas à base canônica $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. Por definição temos

$$(x : y : z) = (x' : y' : z') \Leftrightarrow \text{ existe contante } t \neq 0 \text{ tal que } (x, y, z) = t(x', y', z').$$

Em geral, fixada uma base qualquer no espaço tridimensional, as coordenadas de um ponto não nulo relativas a essa base são chamadas de *coordenadas homogêneas* do ponto correspondente de $\mathbb{P}^2$. Coordenadas homogêneas de um ponto de $\mathbb{P}^2$(relativas a uma base prefixada) só estão bem definidas a menos de um fator escalar não nulo.

Considere $K = \mathbb{R}$. Seja, agora, a aplicação

$$\begin{array}{rcl} q : \mathbb{R}^3 - \{0\} & \to & \mathbb{P}^2 \\ (x, y, z) & \mapsto & (x : y : z) \end{array}.$$

Dizemos que um subconjunto $U \subset \mathbb{P}^2$ é *aberto* se $q^{-1}(U)$ é aberto em $\mathbb{R}^3 - 0$ com sua topologia usual. Estabelecemos assim em $\mathbb{P}^2$ uma noção de vizinhança, segundo a qual dois pontos de $\mathbb{P}^2$ estão "próximos" se as retas associadas em $\mathbb{R}^3$ formam um ângulo "pequeno". O subconjunto de $\mathbb{P}^2$,

$$\mathbb{A}^2 = \{(x : y : z) \mid z \neq 0\},$$

é aberto e denso em $\mathbb{P}^2$, pois $q^{-1}(\mathbb{A}^2)$ é o complementar do plano $z = 0$ em $\mathbb{R}^3$ e é evidentemente aberto e denso em $\mathbb{R}^3 - \{0\}$. Pode-se mostrar que a aplicação

$$\begin{array}{rcl} \mathbb{R}^2 & \to & \mathbb{A}^2 \subset \mathbb{P}^2 \\ (x, y) & \to & (x : y : 1) \end{array}$$

é uma bijeção contínua, com inversa também contínua. Desta maneira, passamos a considerar o plano afim $\mathbb{R}^2$ como contido em $\mathbb{P}^2$, identificando-o com $\mathbb{A}^2$.

5.3 Espaços projetivos

Para um espaço vetorial V de dimensão arbitrária sobre um corpo K, podemos usar a mesma lógicas que fizemos até então para definirmos espaços projetivos associados.

Definição 5.3.1. O *espaço projetivo* $\mathbb{P}(V)$ associado a um espaço vetorial V é o conjunto dos subespaços de V de dimensão 1.

No caso de $\mathbb{P}(\mathbb{R}^3)$, o conjunto de subespaços $\mathbb{R}^3$ são as retas passando pela origem. Se $V = K^{n+1}$, escrevemos $\mathbb{P}^n_K = \mathbb{P}(V)$, ou simplesmente $\mathbb{P}^n$.

As *coordenadas homogêneas* de um ponto $P \in \mathbb{P}(V)$ relativas a uma base $\{v_0, ..., v_n\}$ de V são as coordenadas $(x_0, ..., x_n)$ de um vetor não nulo do subespaço unidimensional representado por P, módulo a multiplicação por escalar diferente de zero. Assim,

$$(x_0 : ... : x_n) = (y_0 : ... : y_n) \Leftrightarrow \exists \lambda \neq 0 \text{ tal que } y_i = \lambda x_i,\ i = 1, ..., n.$$

Fixada a base, $i = 0, ..., n$, o subconjunto de $\mathbb{P}^n$

$$U_i = \{(x_0 : \cdots : x_n) \mid x_i \neq 0\}$$

pode ser identificado com K^n através da bijeção

$$(x_0 : \cdots : x_n) \longleftrightarrow (\frac{x_0}{x_i}, ..., \frac{x_n}{x_i}) \qquad (\text{omitir } \frac{x_i}{x_i}).$$

Convencionamos escrever $\mathbb{A}^n = U_n$; salvo menção contrário, identificamos K^n com $\mathbb{A}^n \subset \mathbb{P}^n$.

O complementar de $\mathbb{A}^n$ em $\mathbb{P}^n$ consiste em pontos da forma $(x_0 : \cdots : x_{n-1} : 0)$. Desta maneira, $\mathbb{P}^n \backslash \mathbb{A}^n$ identifica-se a um $\mathbb{P}^{n-1}$, que convencionamos chamar *hiper plano no infinito*.

Exemplo 5.3.2. $\mathbb{P}^0$ consiste em um só ponto.

Exemplo 5.3.3. $\mathbb{P}^1$, a *reta projetiva*, é a reta usual $\mathbb{A}^1$ com um ponto extra no infinito. Quando $K = \mathbb{R}$, podemos visualizar a reta projetiva real $\mathbb{P}^1(\mathbb{R})$ como a circunferência, com o ponto no infinito indicado na figura:

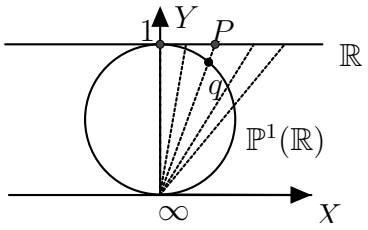

Figura 5.2: Reta projetiva.

Fonte: O autor

Cada ponto de $\mathbb{R}$ é identificado com um ponto q da circunferência pertencente à reta que contém P e o ponto ∞.

5.4 Curvas projetivas

Para trabalharmos nesse novo espaço, precisamos dar um novo tratamento às nossas curvas, isto é, devemos saber como nossas curvas afins se comportam nesse novo ambiente.

Definição 5.4.1. Seja $f = \sum_{0}^{d} f_i$, onde cada $f_i \in K[X,Y]$ é homogêneo de grau i, $f_d \neq 0$. A *homogeneização* de f é o polinômio homogêneo de grau $d = deg(f)$,

$$f^*(X,Y,Z) = \sum Z^{d-i} f_i(X,Y).$$

Exemplo 5.4.2. A homogeneização de $f = X^3Y^4 + 5X^5 + Y^2 + 8$ é o polinômio $f^* = X^3Y^4 + 5X^5Z^2 + Y^2Z^5 + 8Z^7$.

Definição 5.4.3. Uma *curva plana projetiva* é a classe de equivalência de polinômios homogêneos não constantes, $F \in K[X,Y,Z]$, módulo a relação que identifica dois tais polinômios, F, G, se um for múltiplo constante do outro.

Neste contexto, as definições de *traço, equação, componente irredutível* e *grau* feitas em 2.3.3 e 2.3.4, se aplicam as curvas projetivas, ou seja:

Definição 5.4.4. A *equação* de uma curva projetiva é um dos polinômios nessa classe. O *traço* de uma curva é o conjunto das soluções da equação, isto é $F = 0$, $F \in$

$K[X, Y, Z]$. O grau de uma curva F é o grau de sua equação e será denotado por $deg(F)$. As *componentes irredutíveis* de uma curva F são as curvas definidas pelos fatores irredutíveis de F. A *multiplicidade* de uma componente p de F é o expoente com que o fator p ocorre na decomposição de F; quando é maior ou igual a 2, dizemos que p é *componente múltipla de* F.

Se F é um polinômio homogêneo de grau d, a relação

$$F(tx, ty, tz) = t^d F(x, y, z)$$

mostra que a condição para que um ponto (x, y, z) pertença ao traço de uma curva projetiva é independente das coordenadas homogêneas, ou seja, está bem definido o traço de F em $\mathbb{P}^2$.

A reta $Z = 0$ é usualmente chamada de *reta no infinito*. No entanto, mudando a base de K^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*.

O *fecho projetivo* de uma curva afim f é a curva projetiva definida pela homogeneização f^*. Os pontos a distância finita sobre uma curva F são dados pela equação $F(X, Y, 1) = 0$. Definimos a *desomogeneização de F com respeito a Z*, por $F_* = F(X, Y, 1) \in K[X, Y]$.

Se F_* é constante, significa que F é um polinômio apenas na variável Z, isto é, o traço de F está contido na reta no infinito. Observe que, podemos desomogeneizar uma curva F em respeito Y e X, porém consideraremos o plano no infinito sendo $Y = 1$ e $X = 1$, respectivamente.

Exemplo 5.4.5. Se $F = ZX^2Y + Z^3Y + 4X^3Z$, então sua desomogeneização em relação a Z é $F_* = X^2Y + Y + 4X^3$. Observe que a curva definida pela homogeneização de F_*, a saber $(F_*)^* = X^2Y + YZ^2 + 4X^3$, é diferente de F. Isso ocorre pois Z é uma componente de F.

Convenção 5.4.6. De agora em diante, as curvas algébricas planas afins $f(X, Y) = 0$

serão consideradas implicitamente como a parte que se acha a distância finita sobre a curva projetiva $f^*(X, Y, Z) = 0$.

Proposição 5.4.7. *Sejam f e g polinômios em $K[X, Y]$ e F e G polinômios homogêneos em $K[X, Y, Z]$. Então as seguintes fórmulas são válidas:*

1. $(fg)^* = f^*g^*$;
2. $(FG)_* = F_*G_*$;
3. $(f^*)_* = f$;
4. $Z^n(F_*)^* = F$, *onde* $n = deg(F) - deg(F_*)$.

Demonstração. Escrevemos $f = \sum_{i=0}^{d} f_i$ e $g = \sum_{j=0}^{e} g_j$. Temos que

1. $(fg)^* = \left(\sum_{i=0}^{d} f_i \sum_{j=0}^{e} g_j\right)^* = \left(\sum_{i=0}^{d}\sum_{j=0}^{e} f_i g_j\right)^*$ que é um polinômio em que cada fator $f_i g_j$ é homogêneo de grau $i + j$ e assim $(fg)^* = \sum_{i=0}^{d}\sum_{j=0}^{e} Z^{e+d-(i+j)} f_i g_j = \sum_{i=0}^{d}\sum_{j=0}^{e} Z^{d-i} f_i Z^{e-j} g_j = \sum_{i=0}^{d} Z^{d-i} f_i \sum_{j=0}^{e} Z^{e-j} g_j = f^*g^*$.
2. $(FG)_* = (FG)(X, Y, 1) = F(X, Y, 1)G(X, Y, 1) = F_*G_*$.
3. $(f^*)_* = \left(\sum_{i=0}^{d} Z^{d-i} f_i\right)_* = \left(\sum_{i=0}^{d} Z^{d-i} f_i\right)(X, Y, 1) = \sum_{i=0}^{d} f_i = f$.
4. Colocando em evidência o máximo de componentes possíveis Z em F de maneira que não haja variáveis Z no denominador, podemos escrever $F = Z^n F'$ onde F' é homogêneo, $deg(F') = deg(F) - n$ e há termos de F' sem a componente Z. Assim $(F_*)^* = ((Z^n F')(X, Y, 1))^* = (F'(X, Y, 1))^*$. Por construção, $(F'(X, Y, 1))^* = F'$ e assim $Z^n(F_*)^* = Z^n F' = F$.

□

5.5 Mudança de coordenadas projetivas

Veremos agora como se comportam as equações de uma curva projetiva quando estas passam por uma mudança de coordenadas projetivas.

Definição 5.5.1. Seja $T : K^3 \to K^3$ uma aplicação linear bijetiva. Visto que uma tal aplicação preserva retas de K^3 passando pela origem, temos definida uma bijeção natural, ainda designada por $T : \mathbb{P}^2 \to \mathbb{P}^2$, chamada uma *projetividade* ou *mudança de coordenadas projetivas* em $\mathbb{P}^2$.

Temos também induzido um K-isomorfismo

$$T_\bullet : K[X, Y, Z] \to K[X, Y, Z]$$

tal que, para todo $(x, y, z) \in K^3$ e todo polinômio f,

$$(T_\bullet f)(x, y, z) = f(T^{-1}(x, y, z)).$$

Mais explicitamente, escrevendo $X = X_1$, $Y = X_2$, $Z = X_3$ e designando por (a_{ij}) a matriz de T^{-1} relativa à base canônica de K^3, temos

$$(T_\bullet f)(X_1, X_2, X_3) = f(\Sigma a_{1j}X_j, \Sigma a_{2j}X_j, \Sigma a_{3j}X_j).$$

Definição 5.5.2. A *imagem de uma curva projetiva* F por uma projetividade T é a curva definida por $T_\bullet F$. As curvas F e $T_\bullet F$ são ditas *congruentes*.

Dizemos que uma propriedade $\mathcal{P}$ relativa à curva F é *invariante* ou *independente das coordenadas* se F satisfaz $\mathcal{P}$ somente se $T_\bullet F$ a satisfaz para toda projetividade T. São exemplos de propriedades invariantes o grau de uma curva projetiva, a redutibilidade de uma curva, e várias outras.

Exemplo 5.5.3. Duas retas em $\mathbb{P}^2$ sempre se encontram porque dois planos passando pela origem em K^3 sempre contêm uma reta em comum. Observe por exemplo, que duas retas paralelas $aX + bY + c = 0$ e $aX + bY + c' = 0$ com $c \neq c'$ se cruzam no infinito, no ponto $(b : -a : 0)$.

Capítulo 6

Interseção de Curvas Projetivas

Agora que adentramos neste novo ambiente, vamos verificar como se comportam as curvas projetivas. Iniciaremos, como no caso afim, verificando como se dá a interseção de uma reta com uma curva para então definirmos multiplicidade. Em seguida, vermos o caso geral de interseções de duas curvas projetivas que será finalizado com a demonstração de uma proposição que completa o teorema de Bézout.

6.1 Interseção de reta e curva no espaço projetivo

Seja L uma reta e seja F uma curva de grau d. Observe que, se $L = X$, temos então:

$$P = (0 : y : z) \in X \cap F \Leftrightarrow F(0, y, z) = 0.$$

O polinômio $F(0, Y, Z)$ ou é identicamente nulo, caso em que $X \subset F$, ou é homogêneo de grau d, decompondo-se na forma

$$F(0, Y, Z) = \prod (z_i Y - y_i Z)^{m_i},$$

onde os pontos $P_i = (0 : y_i : z_i)$ são dois a dois distintos e constituem $X \cap F$. Chamamos naturalmente o expoente m_i de *multiplicidade de interseção de* X, F *em* P_i. Ora, se definimos multiplicidade da interseção para a reta X com a curva F, por que não o fazemos para uma reta L qualquer, apenas aplicando uma projetividade que leve a reta L a se identificar com a reta X?

Proposição 6.1.1. *Sejam L uma reta e F uma curva de grau d. Se $L \nsubseteq F$ então*

$$L \cap F = \{P_1, ..., P_r\},$$

onde $P_i \neq P_j$ para $i \neq j$ e existem inteiros $m_i \geq 1$ bem determinados pela seguinte condição: Se T é qualquer projetividade tal que $T_\bullet L = X$, então

$$(T_\bullet F)(0, Y, Z) = \prod_{i=1}^{r} (z_i Y - y_i Z)^{m_i},$$

onde $TP_i = (0 : y_i : z_i)$ para $i = 1, ..., r$. Em particular, $\sum m_i = d$.

Demonstração. Consideremos os isomorfismos

$$\mu : \langle L \rangle \xrightarrow{\sim} \langle X \rangle \qquad \text{e} \qquad T_\bullet : K[X, Y, Z] \xrightarrow{\sim} K[X, Y, Z].$$

Como $\langle X \rangle$ e $\langle L \rangle$ são ideais de $K[X, Y, Z]$, pela proposição 1.1.3, existe um isomorfismo

$$\begin{array}{rcl} \overline{T_\bullet} : K[X, Y, Z]/\langle L \rangle & \xrightarrow{\sim} & K[X, Y, Z]/\langle X \rangle \\ G + \langle L \rangle & \mapsto & T_\bullet G + \langle X \rangle \end{array},$$

mas como existe o isomorfismo $\phi : K[X, Y, Z]/\langle X \rangle \xrightarrow{\sim} K[Y, Z]$, de maneira que $\phi(H + \langle X \rangle) = H(0, Y, Z)$. Compondo $\overline{T_\bullet} \circ \phi$, temos o isomorfismo

$$\begin{array}{rcl} \widetilde{T}_\bullet : K[X, Y, Z]/\langle L \rangle & \xrightarrow{\sim} & K[Y, Z] \\ G + \langle L \rangle & \mapsto & T_\bullet G(0, Y, Z) \end{array}.$$

Consideremos, agora, o diagrama de homomorfismos de anéis

$$\begin{array}{ccc} K[X, Y, Z] & \xrightarrow{T_\bullet} & K[X, Y, Z] \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ K[X, Y, Z]/\langle L \rangle & \xrightarrow[\widetilde{T}_\bullet]{} & K[Y, Z] \end{array} \tag{6.1}$$

onde a primeira das flechas verticais é a aplicação quociente $\alpha : g \mapsto \overline{g} = g + \langle L \rangle$; e a segunda é dada por

$$\beta : g(X, Y, Z) \mapsto g(0, Y, Z).$$

Afirmamos que o diagrama acima é comutativo. De fato, se $F \in K[X, Y, Z]$, temos

$$\beta \circ T_\bullet(F) = (T_\bullet F)(0, Y, Z) = \widetilde{T}_\bullet\,(F + \langle L \rangle) = \widetilde{T}_\bullet\,(\overline{F}) = \widetilde{T}_\bullet \circ \alpha(F).$$

Sendo $K[X,Y,Z]/\langle L\rangle$ isomorfo ao domínio fatorial $K[Y,Z]$, $\overline{F} \in K[X,Y,Z]/\langle L\rangle$ admite fatoração única, ou seja,

$$\overline{F} = p_1^{m_1} \cdots p_s^{m_s},$$

onde os p_i's são irredutíveis distintos e cada expoente m_i é maior ou igual a 1. Note que os m_i's não dependem de T, dependem apenas de $\overline{F}$. Portanto, estão univocamente determinados por $\overline{F}$. Além disso, sendo $\widetilde{T}_\bullet$ um isomorfismo e lembrando que todo polinômio homogêneo se fatora em homogêneos de grau 1, segue que

$$(T_\bullet F)(0,Y,Z) = \widetilde{T}_\bullet\,(\overline{F}) = \prod_{i=1}^{r}(z_iY - y_iZ)^{m_i}.$$

Finalmente, como TP_i está na interseção $T_\bullet L \cap T_\bullet F = T_\bullet F(0,Y,Z)$, então é imediato que TP_i é da forma $(0,y_i,z_i)$. □

Definição 6.1.2. A *multiplicidade* ou *índice de interseção* da reta L com uma curva F no ponto P é definida por

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

A proposição anterior nos diz que $L \cap F$ consiste em $deg(F)$ pontos contados com multiplicidades; é o caso particular do teorema de Bézout que diz que o número de interseção de duas curvas projetivas consiste no produto de seus graus, o qual veremos mais adiante. Outra coisa que a proposição nos revela é que, com o emprego de uma projetividade conveniente, podemos sempre supor, para o cálculo de $(L,F)_P$, que P se encontra a distância finita e que L e F são distintos da reta no ∞. Nessas circunstâncias, é imediato que

$$(L,F)_P = (L_*,F_*)_P,$$

onde o segundo membro é a multiplicidade de interseção definida no caso afim. Assim, os resultados do capítulo sobre multiplicidade podem ser transcritos para as curvas projetivas. Veremos isso agora.

Proposição 6.1.3. *Seja F uma curva projetiva e seja P um ponto de F. Então existe um inteiro $m = m_P(F) \geq 1$ tal que, para toda reta L passando por P, vale*

$$(L, F)_P \geq m,$$

ocorrendo desigualdade estrita para no máximo m retas e no mínimo uma.

Demonstração. Movendo F e P com uma projetividade, podemos supor que a reta no infinito não contém P. Assim, reduzimos ao caso afim, quando então o enunciado é consequência da proposição 4.2.1 do capítulo sobre multiplicidades. □

Definição 6.1.4. As *retas tangentes* a F em P são as retas distinguidas na proposição anterior.

Definição 6.1.5. O inteiro $m_P(F)$ descrito acima é a *multiplicidade* de F *em* P ou *multiplicidade* de P *em* F. Se $P \notin F$, convencionamos $m_P(F) = 0$. Dizemos que P é um ponto *simples* ou *não singular* ou *liso* de F, e que F é *simples* ou *não singular* ou *lisa* em P se $m_P(F) = 1$; P é *múltiplo* ou *singular* se $m_P(F) \geq 2$. Se $m_p(F) = 2, 3, ..., m$, dizemos que P é um ponto *duplo, triplo,...,m-uplo*. A curva F é *lisa* ou *não singular* se o for em cada um de seus pontos.

Se f é uma curva afim e $F = f^*$, é imediato que $m_P(F) = m_P(f)$ para cada ponto $P \in \mathbb{A}^2$. Portanto, as definições acima são consistentes com as dadas no capítulo sobre as multiplicidades afins. Ainda neste contexto, para a determinação de $m_p(F)$ e das retas tangentes, reduzimos ao caso afim, desomogeneizando F com relação a uma variável que não se anula no ponto P.

6.2 Teorema de Bézout

Emfim, chegamos aos últimos passos para demonstrar o tão aguardado teorema supracitado. Vamos a isso!

Lema 6.2.1. *Sejam F, G curvas planas projetivas. Então $F \cap G$ é finita se, e somente se, F, G não admitem componente em comum.*

Demonstração. Afirmamos que se F, G não admitem fator em comum em $K[X, Y, Z]$ então F_*, G_* também não o admitem em $K[X, Y]$. De fato, se $F_* = fh$ e $G_* = gh$, com $f, g, h \in K[X.Y]$ e h não constante, então $(F_*)^* = f^*h^*$ e $(G_*)^* = g^*h^*$. Daí se seguiria que h^* é fator de F, G, o que é uma contradição. Como F_*, G_* não tem componente comum e $F = Z^n(F_*)^*$ e $G = Z^m(G_*)^*$, segue-se que F e G tem interseção finita, a distância finita. Como $F \cap Z$ ou $G \cap Z$ é finita, (senão Z seria componente comum) temos que $F \cap G$ é finita. A reciproca é consequência da contrapositiva do corolário 3.1.6. □

Agora que sabemos a finitude da interseção de duas curvas projetivas, vamos calcular o seu número de pontos. Observemos que não podemos afirmar que a interseção não é vazia, em geral. Isso será uma consequência do teorema de Bézout.

Definição 6.2.2. Sejam $P_i = (x_i : y_i : z_i), \quad i = 1, ..., r$ os distintos pontos de $F \cap G$. Diremos que F, G estão em *boa posição* ou *bem posicionadas* se $P_0 = (0 : 1 : 0) \notin F \cap G$. Diremos que F, G estão em *muito boa posição* ou *muito bem posicionadas* se $P_0 \notin F \cap G$ e se, para cada par $P_i, P_j \in F \cap G$, então P_0, P_i, P_j são não colineares.

Observe que, se considerarmos $P_i = (x_i : y_i : z_i)$ e $P_j = (x_j : y_j : z_j)$, então P_0, P_i, P_j são colineares se, e só se, a determinante da matriz que tem as linhas definidas por P_0, P_i, P_j é igual a zero, ou seja

$$\det \begin{pmatrix} 0 & 1 & 0 \\ x_i & y_i & z_i \\ x_j & y_j & z_j \end{pmatrix} = 0 \Leftrightarrow z_i x_j = x_i z_j.$$

Vejamos que, se $x_j = 0$, então z_j não pode ser zero, pois teríamos $P_j = P_0$. Dessa forma, $z_i x_j = x_i z_j$ nos diz que se $x_j = 0$, então $x_i = 0$. Analogamente, se $x_i = 0$, então $x_j = 0$. E neste caso, teremos $(0 : z_i) = (0 : z_j)$. Agora, se $x_i \neq 0$, temos que

$$z_i x_j = x_i z_j \Leftrightarrow \frac{z_i}{x_i} = \frac{z_j}{x_j} \Leftrightarrow (x_i : z_i) = (x_j : z_j).$$

Portanto, a condição de P_0, P_i, P_j serem não colineares, equivale a $(x_i : z_i) \neq (x_j : z_j)$, se $i \neq j$.

Daqui em diante, consideraremos que as curvas projetivas F, G não têm componente em comum. Escrevemos

$$\begin{cases} F &= A_0Y^d + A_1Y^{d-1} + ... + A_d, \\ G &= B_0Y^e + B_1Y^{e-1} + ... + B_e, \end{cases}$$

onde $A_i, B_j \in K[X, Z]$ são homogêneos de graus i, j.

Observe que, $(0 : 1 : 0) \in F$ se, e só se, $A_0 = 0$. Portanto, estando F, G bem posicionadas, temos A_0 ou $B_0 \neq 0$. Lembrando o lema 3.3.15, a resultante $R = R(X, Z)$ de F, G com respeito a Y é homogênea de grau $d \cdot e$. Por outro lado, levando em conta que A_0 ou $B_0 \neq 0$, pela proposição 3.3.5, para cada $(x : z) \in \mathbb{P}^1$ temos que

$$R(x, z) = 0 \Leftrightarrow \exists (x : y : z) \in F \cap G,$$

ou seja, a resultante só se anula no ponto $(x : z) \in \mathbb{P}^1$ se existe um ponto $(x : y : z)$ na interceção de F com G. É claro que, supondo F, G muito bem posicionadas, concluímos que R, por ser homogêneo, escreve-se na forma

$$R(X, Z) = c \prod_{i=1}^{r} (z_iX - x_iZ)^{m_i}$$

onde

- c é uma constante diferente de 0,
- $P_i = (x_i : y_i : z_i), \quad i = 1, ..., r$, são os distintos pontos de $F \cap G$,
- os expoentes m_i são inteiros ≥ 1 e $\Sigma m_i = d \cdot e$.

Adotaremos, então, a seguinte definição:

Definição 6.2.3. A *multiplicidade* ou *índice de interseção* de F, G no ponto P é dado por

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

Observe que, para o caso em que F, G estão bem posicionadas, $\Sigma m_i = deg(R) = deg(F) \cdot deg(G)$, que pode ser enunciado pelo seguinte teorema

Teorema 6.2.4 (Teorema de Bézout)**.** *Se F, G são curvas planas projetivas sem componentes em comum então o número de pontos na interseção $F \cap G$, contados com multiplicidade, é igual a $deg(F) \cdot deg(G)$.*

Para o caso geral, precisamos definir o índice $(F, G)_P$ sem a hipótese de bom posicionamento.

Proposição 6.2.5. *Sejam F e G duas curvas projetivas sem componentes em comum. Existe uma projetividade T tal que $T_\bullet F$ e $T_\bullet G$ estão muito bem posicionadas.*

Demonstração. Seja $P_0 = (0 : 1 : 0)$. Observemos que $F \cap G$ é finito, pois F e G não têm componentes em comum. Escrevendo $F \cap G = \{P_i = (x_i : y_i : z_i),\ i = 1, ..., r\}$, podemos tomar um ponto $V_0 \neq P_0$, tal que V_0 não está contido nas retas $\overleftrightarrow{P_i P_j}$, com $i, j = 1, ...r$ e $i \neq j$. Tome T uma projetividade tal que

$$T(V_0) = P_0.$$

Note que $P_0 \notin T_\bullet F \cap T_\bullet G$ pois, sendo T uma bijeção, então $T(P_i) \neq P_0$, para todo $i = 1, ..., r$. Agora, suponha por absurdo, que existam $P_i, P_j \in F \cap G$, para $i \neq j$, tais que $T(P_i)$ e $T(P_j)$ sejam colineares com P_0. Como colinearidade é uma propriedade preservada por qualquer aplicação linear bijetiva, então, aplicando a projetividade inversa T^{-1}, P_i e P_j são colineares com $T^{-1}(P_0) = V_0$. O que é absurdo, por construção de V_0. Assim $T_\bullet F$ e $T_\bullet G$ estão em muito boa posição. □

Pela proposição anterior, podemos, agora, definir a multiplicidade para duas curvas sem componentes em comum, utilizando sempre uma projetividade T tal que $T_\bullet F, T_\bullet G$ estão em muito boa posição.

Definição 6.2.6. O *índice* ou *multiplicidade de interseção* de curvas projetivas F, G sem componentes em comum no ponto $P \in \mathbb{P}^2$ é

$$(F, G)_P = (T_\bullet F, T_\bullet G)_{TP}$$

onde T denota uma projetividade tal que $T_\bullet F, T_\bullet G$ estejam muito bem posicionadas, de maneira que o segundo membro pode ser calculada como na definição 6.2.3.

Observe que, não provamos que a multiplicidade em um ponto da interseção é sempre o mesmo, não importando se tomarmos duas projetividades T, T' diferentes em que, as curvas F e G estejam muito bem posicionadas. Para que nossa definição tenha consistência, precisamos averiguar este fato.

Proposição 6.2.7. *Sejam F, G curvas muito bem posicionadas. Seja T uma projetividade tal que $T_\bullet F, T_\bullet G$ também estão muito bem posicionadas. Então*

$$(F, G)_P = (T_\bullet F, T_\bullet G)_{TP} \qquad \forall P \in \mathbb{P}^2.$$

Demonstração. Para esta demonstração, a ideia é provar a igualdade quando T é uma *projetividade genérica*. Sejam $W_{ij}(i, j = 1, 2, 3)$ nove indeterminadas, e seja

$$L = \overline{K(W_{ij})},$$

o fecho algébrico [1, pg. 43] do corpo de funções racionais nessas novas variáveis. O plano projetivo $\mathbb{P}^2_K$ se identifica a um subconjunto de $\mathbb{P}^2_L$ (o plano projetivo a coordenadas no corpo L). Note que F, G definem curvas em $\mathbb{P}^2_L$, que denotaremos por $\overline{F}, \overline{G}$. O fato importante a observar é que, mesmo considerando pontos com coordenadas em $L \supset K$, temos ainda

$$\overline{F} \cap \overline{G} = F \cap G = \{P_1, ..., P_r\}.$$

Com efeito, as coordenadas de um ponto de $\overline{F} \cap \overline{G}$ provêm das raízes da resultante de F, G com relação a uma variável conveniente, e portanto satisfazem uma equação algébrica a coeficientes em K. Sendo este corpo algebricamente fechado, vemos que os pontos comuns a $\overline{F}, \overline{G}$ em $\mathbb{P}^2_L$ são os que já conhecíamos, em $F \cap G$.

A projetividade genérica W é a projetividade de P^2_L definida por

$$W(x_1 : x_2 : x_3) = (\Sigma W_{1j} x_j : \Sigma W_{2j} x_j : \Sigma W_{3j} x_j).$$

Consideremos agora os "transladados genéricos", $W_\bullet \overline{F}, W_\bullet \overline{G}$. Temos, por definição,

$$(W_\bullet \overline{F})(X, Y, Z) = \overline{F}(W^{-1}(X, Y, Z)).$$

Como $W^{-1} = \dfrac{1}{det(W_{ij})} adj(W_{ij})$ onde $adj(W_{ij})$ é a matriz adjunta de W [3, pg. 261], podemos eliminar os denominadores da expressão acima, definindo

$$F^W(X,Y,Z) = (det(W_{ij}))^d \overline{F}(W^{-1}(X,Y,Z)), \qquad (d = deg(F)).$$

Assim, F^W é um polinômio a coeficientes em $K[\{W_{ij}\}]$, anel dos polinômios nas variáveis W_{ij}. É claro que F^W e $W_\bullet \overline{F}$ definem a mesma curva em $\mathbb{P}^2_L$, pois diferem por um múltiplo constante. Para cada projetividade T definida por uma matriz (t_{ij}) com coeficientes em K, é evidente que o resultado da substituição $W_{ij} \to t_{ij}$ em F^W é $T_\bullet F$. Dizemos que *especializamos* W_{ij} para t_{ij}. Note ainda que para cada ponto $Q \in F^W \cap G^W$, existe $P = (x_1 : x_2 : x_3) \in F \cap G$ tal que $W(P) = Q$, a saber, $Q = (\Sigma W_{1j}x_j : \Sigma W_{2j}x_j : \Sigma W_{3j}x_j)$.

Afirmação. *F^W, G^W estão muito bem posicionadas.*

Demonstração da Afirmação. Suponha, por absurdo, que $P_0 = (0 : 1 : 0) \in F^W \cap G^W$. Então

$$P_0 = W(P) \tag{6.2}$$

para algum $P \in F \cap G$. Especializando (W_{ij}) para a matriz identidade, segue-se que $P_0 \in F \cap G$, o que é proibido por hipótese. Da mesma forma, se existissem pontos distintos $Q, Q' \in F^W \cap G^W$ colineares com P_0, concluiríamos a existência de $P, P' \in F \cap G$ colineares com P_0. Basta notar que se $Q = W(P)$,$Q' = W(P')$ são colineares com P_0, o determinante da matriz com linhas Q, Q' e P_0 é um polinômio que se anula para toda especialização $W_{ij} \to t_{ij}$[1]. Se especializarmos W_{ij} pela matriz identidade, este determinante coincide com a determinante da matriz com linhas P, P' e P_0, o que mostra que estes serão colineares. Portanto, F^W, G^W estão muito bem posicionadas, o que prova nossa afirmação. □

Agora que sabemos que F^W, G^W estão muito bem posicionadas, vamos calcular a resultante entre elas. Encontramos

$$R((W), X, Z) = c(W) \prod_{i=1}^{r} (z_i(W)X - x_i(W)Z)^{n_i},$$

[1] O determinante de uma matriz quadrada se anula se, e só se, algum dos vetores desta matriz é linearmente dependente dos outros, isto é, pelo menos um é combinação linear dos outros.

onde $c(W)$ é um polinômio não nulo, cada n_i é um inteiro $\geqslant 1$ e

$$x_i(W) = W_{11}x_i + W_{12}y_i + W_{13}z_i,$$

$$z_i(W) = W_{31}x_i + W_{32}y_i + W_{33}z_i,$$

são coordenadas homogêneas do i-ésimo ponto, $W(x_i : y_i : z_i)$, de $F^W \cap G^W$.

A expressão para a resultante está correta porque, por um lado, sabemos que $R((W), X, Z) \in K[\{W_{ij}\}][X, Z]$ (um polinômio com variáveis X, Z com coeficientes em $K[\{W_{ij}\}]$) pode se escrever na forma

$$R = c(W) \cdot \overline{R}((W), X, Z),$$

onde $\overline{R}$ é a resultante de $W_\bullet\overline{F}$ e $W_\bullet\overline{G}$, não divisível por $c(W)$ e que, em $L[X, Y]$, $\overline{R}$ é completamente decomponível nos fatores lineares $z_i(W)X - x_i(W)Z$, correspondentes aos pontos de $W_\bullet\overline{F} \cap W_\bullet\overline{G}$ e, portanto, também aos pontos de $F^W \cap G^W$.

Precisamos verificar que, se especializarmos (W_{ij}) para qualquer (t_{ij}), com coeficientes em K, associada a projetividade T tal que $T_\bullet F$, $T_\bullet G$ estejam muito bem posicionadas, $R((W), X, Z)$ se especializa na resultante de $T_\bullet F$, $T_\bullet G$. De fato, pela proposição 3.3.2, como a função especialização é um homomorfismo e denotando-a por E, temos

$$E(R((W), X, Z)) = E(R_{F^W,G^W}) = R_{E(F^W),E(G^W)} = R_{T_\bullet F,T_\bullet G}.$$

Finalmente, a condição de bom posicionamento garante que para $i \neq j$ os fatores $z_i(T)X - x_i(T)Z$ e $z_j(T)X - x_j(T)Z$ permanecem distintos, ou seja, cada fator $z_i(W)X - x_i(W)Z$ se transforma no fator correspondente ao ponto TP_i. Segue que os expoentes n_i não dependem de t_{ij}, e em particular,

$$(T_\bullet F, T_\bullet G)_{TP} = (F, G)_P,$$

e a proposição está provada. □

Portanto, demonstramos o teorema de Bézout e concluímos o objetivo deste trabalho.

Considerações Finais

Este trabalho teve por fim demonstrar o Teorema de Bézout para interseção de curvas projetivas, um resultado de suma importância para a Geometria Algébrica, que conta o número de pontos de interseção de duas curvas projetivas. Para isso, foi usado como base para a construção deste trabalo o livro *Introdução às Curvas Algébrica Planas* de Israel Vainsencher [8], que pode ser consultado como forma de ampliar e dar seguimento aos resultados aqui apresentados. Começamos esta construção desde resultados básicos de teoria de anéis e seguimos introduzindo ao leitor a definição de uma curva algébrica plana e algumas propriedades desta, como a mudança de referencial, a multiplicidade de seus pontos e por fim vimos como se dá a interseções entre duas delas. Após isso, adentramos num novo ambiente, o plano projetivo, e observamos como as curvas, agora projetivas, se comportam nesse novo âmbito que tem muitas propriedades boas, como é o caso do nosso teorema principal.

A motivação por esse tema adveio do interesse do autor em seguir na carreira acadêmica no ramo da álgebra abstrata e aprender cada vez mais sobre essa área que tanto assusta os alunos dos cursos de graduação, mas que se vista com outros olhos, é um manancial de conhecimento que tangência a toda matemática por qualquer seguimento. Assim, este trabalho trouxe uma experiência significativa, abastecendo o conhecimento, instigando a curiosidade e aprendendo a lidar com as dificuldades que, ao concluir o curso, só aumentarão em um mestrado e doutorado, porém o aprendizado e a maturidade para lidar com as adversidades também acompanharão o crescimento dessa caminhada.

Referências Bibliográficas

[1] ENDLER, Otto, *Teoria dos Corpos*, Publicações Matemáticas, IMPA, RJ, 2012.

[2] GONÇALVES, Adilson, *Introdução à álgebra*, 5a edição. Rio de Janeiro, IMPA, 2006.

[3] LIMA, Elon Lages, *Álgebra Linear*, 9a edição, IMPA, Rio de Janeiro, 2016.

[4] LIMA, Elon Lages, *Curso de análise*, vol. 2, 11a edição, IMPA, Rio de Janeiro, 2015.

[5] LIMA, Elon Lages, *Elementos de Topologia Geral*, Editora Ao Livro Técnico S.A., Rio de Janeiro, 1970.

[6] MUKAI, Shigeru , *An Introduction to Invariants and Moduli*, Cambridge studies in advanced mathematics, CAMBRIDGE UNIVERSITY PRESS, United Kingdom, 2003.

[7] PARGA, Paulo, *Álgebra Linear básica com geometria analítica*, Editora Edur-UFRRJ, 2011.

[8] VAINSENCHER, Israel, *Introdução às Curvas Algébricas Planas*, 3a Edição, Coleção Matemática Universitária, IMPA, RJ, 2009.