Uma introdução às curvas algébricas planas e ao Teorema de Bézout

Palavras-Chave: CURVA, PONTO SINGULAR, INTERSEÇÃO, TEOREMA DE BÉZOUT

Autores
Bianca Serpa Castanho, IMECC - UNICAMP
Pietro Speziali, (orientador), IMECC - UNICAMP

1 Introdução

Este projeto de pesquisa pretende estudar a teoria introdutória de curvas algébricas planas e desenvolver uma noção das principais propriedades do plano projetivo, o suficiente para que seja possível o estudo e entendimento a respeito de interseções das curvas algébricas neste plano, em especial o Teorema de Bézout.

2 Metodologia

A aluna estudou os materiais citados nas referências, e teve reuniões semanais com o orientador nas quais ela apresentou seminários sobre o conteúdo estudado. Assim, o professor acompanhou consistentemente os resultados dos estudos, podendo auxiliar o aluno sempre que necessário.

3 Estudos realizados

A primeira parte do estudo teve como objetivo entender conceitos básicos a respeito de curvas algébricas no plano afim, começando pela definição.

Definição 1. *Seja $\mathbb{K}$ um corpo. Uma curva algébrica plana afim $\mathcal{C}$ é definida implicitamente por uma equação polinomial em duas variáveis da forma $f(x, y) = 0$:*

$$f(x,y) = \sum_{i,j} a_{ij} x^i y^j$$

Onde $f(x, y)$ pertence ao anel de polinômios em duas indeterminadas $\mathbb{K}[x, y]$.

O grau de uma curva algébrica $\mathcal{C}$ é portanto definido naturalmente como o grau do polinômio $f(x, y)$ que a define.

Outro conceito importantes a ser compreendido é o de ponto singular, mas antes é preciso entender a multiplicidade de interseção de uma curva f e uma reta l em um ponto p que pertence a l, denotado por $I(p, f, l)$. Para isso, vamos lembrar do polinômio de interseção $\psi(t) = f(x(t), y(t)) = f((1 - t)a_1 + tb_1, (1 - t)a_2 + tb_2)$, onde as variáveis x, y são descritas dessa forma por conta da parametrização da reta $l = (1 - t)a + bt$ onde $a = (a_1, a_2)$ e $b = (b_1, b_2)$, com $a, b \in l$ e $t \in \mathbb{K}$.

Definição 2. *Seja f uma curva de grau d em $\mathbb{K}^2$ e $p \in l$ um ponto cujas coordenadas são determinadas pelo parâmetro $t_0 \in \mathbb{K}$. Então o número de interseções $I(p, f, l)$ é dado pela multiplicidade de t_0 como raiz de $\psi(t)$.*

Note que se $I(p, f, l) = 0$ então $p \notin f$ e também que, caso l seja componente de f, então $I(p, f, l) = \infty, \ \forall \, p \in l$. Além disso, o seguinte resultado nos garante a boa definição do número de interseção.

Lema 1. *O número de interseções $I(p, f, l)$ depende apenas de p, f, l, ou seja, não depende da escolha da parametrização de l.*

Um ponto é dito *singular* quando possui multiplicidade ≥ 2, onde essa multiplicidade pode ser calculada de duas formas diferentes, apresentadas nos lemas a seguir.

Lema 2. *Seja $p = (a, b)$ um ponto em uma curva f em $\mathbb{K}^2$. Definimos $g(x, y) = f(a + x, b + y)$. A multiplicidade de p em f é o grau do termo de menor grau em g.*

Prova: Escrevendo $g = G_m + G_{m+1} + \cdots + G_d$ onde cada G_k é um polinômio homogêneo de grau k, e $G_m \neq 0$. Seja (X, Y) um vetor diferente de zero em $\mathbb{K}^2$, e seja $l = l_{X,Y}$ a reta que une os pontos (a, b) e $(a + X, b + Y)$, assim l é parametrizada como $x(t) = a + tX, y(t) = b + tY$. A interseção polinomial associada é, então

$$
\begin{aligned}
\phi_{X,Y}(t) &= f(a + tX, b + tY) \\
&= g(tX, tY) \\
&= G_m(tX, tY) + G_{m+1}(tX, tY) + ... \\
&= t^m G_m(tX, tY) + t^{m+1} G_{m+1}(tX, tY) + ...
\end{aligned}
$$

É evidente que t^m é um fator de $\phi_{X,Y}(t)$ para quaisquer X, Y. Por outro lado, existem X, Y tais que $G_m(X, Y) \neq 0$ e, portanto, t^{m+1} não é um fator de $\phi_{X,Y}(t)$, lembrando que uma forma binária tem uma quantidade finita de zeros. Logo, segue que p é um ponto de multiplicidade m em f. $\square$

Lema 3. *Seja $p = (a, b)$ um ponto de uma curva f em $\mathbb{K}^2$. Então p tem multiplicidade m em f, se e somente se, todas as derivadas parciais de f de ordem $< m$ zerarem em p, e pelo menos uma derivada parcial de ordem m é diferente de zero em p.*

Prova: Definindo $g(x, y) = f(a + x, b + y)$ e escrevendo $g = G_o + ... + G_d$ onde cada G_k é uma forma de grau k. Então pelo Lema 6 o ponto p tem multiplicidade m em f se e somente se $G_o = ... = G_{m-l} = 0$, $G + m \neq 0$. A expansão de Taylor de $g(x, y)$ mostra que essas condições são válidas se e somente se todas as derivadas parciais de g de ordem $< m$ zeram na origem, e pelo menos uma de ordem m é diferente de zero na origem. O resultado segue desde as derivadas parciais de g na origem coincidem com as de f em p. $\square$

A partir do Lema 3 e sua prova podemos observar que é suficiente e necessário para que um ponto $p = (a, b)$ seja singular em uma curva f que $f(p) = 0, \ f_x(p) = 0, \ f(p)_y = 0$.

Exemplo 1. *Para curva a $f = y^2 + 2x^2 - x^4$, é necessário para os pontos singulares que $0 = f, \ 0 = f_x = -4x(-1 + x^2), \ 0 = f_y = 2y$. Então existe um único ponto singular $(0, 0)$, de multiplicidade 2.*

A segunda parte consistiu em estudar o plano projetivo $P\mathbb{K}^2$, e curvas algébricas neste plano, para finalmente estudar suas interseções e o Teorema de Bézout.

Há muitas maneiras equivalentes de definirmos um plano projetivo. Usando uma noção intuitiva, definimos o plano projetivo adicionando vários pontos no infinito a um plano L no $\mathbb{K}^3$ que não passa pela origem O, e um plano L_0 paralelo passando pelo origem O, onde L_0 define a *reta no infinito* associada a L e uma reta no plano projetivo $P\mathbb{K}^2$. O é um único ponto em $P\mathbb{K}^2$ denotado por $(x_1 : x_2 : x_3)$ e diferentemente do caso afim, no caso projetivo podemos trabalhar apenas com polinômios homogêneos (onde um polinômio $F \in K[x, y, z]$ de grau d é homogêneo se, para todo $t \in \mathbb{K}$, tem-se $F(tx, ty, tz) = t^d F(x, y, z)$) para definirmos curvas. Isso acontece porque, para um polinômios homogêneo F o lugar de zeros $V(F) \subset P\mathbb{K}^2$ está bem definido, como explicado a seguir.

No plano projetivo as coordenadas homogêneas não são únicas já que um ponto $A = (a_1, a_2, a_3)$ e um ponto $B = (b_1, b_2, b_3)$ são o mesmo ponto em $P\mathbb{K}^2$ quando existe um escalar $\lambda \neq 0$ tal que $a_1 = \lambda b_1, \ a_2 = \lambda b_2, \ a_3 = \lambda b_3$. Agora podemos definir o conjunto dos zeros de uma curva projetiva F como sendo $V(F)$.

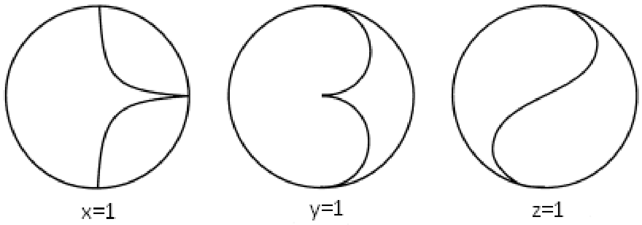

Figura 1: fig. 9.8 da bibliografia [1]

$$V(F) = (x : y : z) \in P\mathbb{K}^2 : F(x, y, z) = 0.$$

Dependendo da escolha do plano afim L na equação $ax + by + cz = d$ e eliminando uma das variáveis x, y, z na relação entre $F(x, y, z) = 0$ e L obtemos diferentes curvas afim f nos planos (x, y), (y, z) ou (x, z), fazendo isso estamos *deshomogeneizando* a curva F. Isso ficará mais claro no exemplo a seguir.

Exemplo 2. *A cúbica projetiva $F = yz^2 - x^3$ em $P\mathbb{R}^2$. Deshomogeneizanda em relação a x, y, z obtemos três vistas afins $f = y - x^3$ no plano (x,y), $g = yz^2 - 1$ no plano (y, z), e $h = z^2 - x^3$ no plano (z, x). E neste caso nenhuma das deshomegeinizações são afim equivalente entre si, ou seja equivalentes sob uma transformação afim.*

É possível de certa forma visualizar que temos diferentes visões afim da curva F do exemplo anterior por meio dos modelos hiperesféricos, se tomarmos os hemisférios resultantes dos planos x = 0, y = 0, Z = 0 em $\mathbb{R}^3$, obtemos as três imagens da FIgura 1.

Outro processo importante envolvendo curvas afim é o processo de homogeneização em relação a forma l, onde se homogeneiza f multiplicando cada monômio pela potência de l necessária para elevar o grau até d. Mais precisamente, dado qualquer curva afim $f(x, y)$ de grau d em $\mathbb{K}^2$, e qualquer plano afim L em $\mathbb{K}^3$ que não passa pela origem, e não é paralelo ao eixo z, existe uma curva projetiva $F(X, Y, Z)$ de grau d em $P\mathbb{K}^2$ com a propriedade de que $F(X, Y, Z) = f(x, y)$ para cada ponto (x, y, z) em L. Na verdade, se L é definido por uma equação $l = 1$, onde $l = ax + by + cz$ com $c \neq 0$, e $f(x, y) = \sum a_{ij} x^i y^j$, precisamos apenas observar que podemos tomar

$$F(x, y, z) = l^d f(\tfrac{x}{z}, \tfrac{y}{z}) = \sum a_{ij} x^i y^j l^{d-i-j}.$$

Assim como no caso afim, para curvas projetivas também definimos um polinômio de interseção Φ. Seja F(x,y,z) uma curva de grau d em $P\mathbb{K}^2$ E seja L uma reta. L é determinado por quaisquer dois pontos distintos, digamos $A = (a_1 : a_2 : a_3)$ e $B = (b_1 : b_2 : b_3)$ então, a reta L pode ser parametrizada como $X_1 = sa_1 + tb_1,\ x_2 = sa_2 + tb_2,\ x_3 = sa_3 + tb_3$. As interseções de F com L são dados por $\Phi(s, t) = 0$, onde Φ é definido por

$$\Phi(s, t) = F(sa_1 + tb_1, sa_2 + tb_2, sa_3 + tb_3),$$

como F(x, y, z) possui grau d, temos que $\Phi(\lambda s, \lambda t) = \lambda^d \Phi(s, t)$ para qualquer escalar λ, então $\Phi(s, t)$ é uma forma binária de grau d.

E assim como no caso afim, I(P, F, L) não depende da parametrização de L. E temos os seguintes lemas.

Lema 4. *Seja F uma curva de grau d em $P\mathbb{C}^2$ e seja L uma reta. Então ou L intersecta F em $\leq$ d pontos, ou L é um componente de F. Assim, para uma curva F sem retas como componentes, o grau d é um limite superior para o número de interseções de F com qualquer reta L.*

Lema 5. *Seja P u ponto de interseção de uma curva F de grau d com uma reta L no plano projetivo $P\mathbb{K}^2$. Deshomogeinizando com respeito à uma das variáveis x, y, z para obter um ponto p, uma curva f e uma reta l no plano afim $\mathbb{K}^2$, temos que I(P,F,L) =I(p,f,l).*

Nas curvas projetivas também temos pontos singulares definidos da mesma forma como no caso afim e podemos encontra-los de forma análoga. Além de termos o seguinte lema.

Lema 6. *Seja P um ponto de uma curva F em $P\mathbb{K}^2$. Deshomogeinizando com respeito a umas das variáveis x, y, z, obtemos um ponto p em uma curva f no plano afim $\mathbb{K}^2$ onde a multiplicidade de P em F é igual a multiplicidade de p em f.*

Agora que as informações mais importantes a respeito de curvas projetivas foram pontuadas podemos finalmente partir para a interseção de duas curvas projetivas, e as informações importantes para sua demonstração do teorema de Bézout.

Para melhor estabelecer se dois polinômios possuem fatores comuns, damos agora o conceito de resultante. Sejam

$$f(t) = a_0 + a_1 t + ... + a_p t^p \quad (a_p \neq 0)$$
$$g(t) = b_0 + b_1 t + ... + b_q t^q \quad (b_q \neq 0).$$

A partir dos coeficientes a_i, b_j construimos a matriz A de ordem $(p+q)$ definida por

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_p & 0 & 0 & \cdots \\ 0 & a_0 & a_1 & a_2 & \cdots & a_p & 0 & \cdots \\ 0 & 0 & a_0 & a_1 & a_2 & \cdots & a_p & \cdots \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \\ b_0 & b_1 & b_2 & \cdots & b_q & 0 & 0 & \cdots \\ 0 & b_0 & b_1 & b_2 & \cdots & b_q & 0 & \cdots \\ 0 & 0 & b_0 & b_1 & b_2 & \cdots & b_q & \cdots \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \end{pmatrix}$$

O Resultante $R(f,g)$ é definido como o determinante da matriz A acima. Valem os seguintes resultados, de importância central no nosso estudo.

Lema 7. *Os polinômios $f,\ g$ têm um fator não constante em comum se, e somente se, $R(f,g) = 0$.*

Lema 8. *Sejam F, G polinômios em z de grau m, n, a coeficientes no domínio $K[x,y]$ definido pelas fórmulas*

$$F(x,y,z) = A_m + A_{m-1}z + \cdots + A_0 z^m \quad (A_0 \neq 0)$$
$$G(x,y,z) = B_n + B_{n-1}z + \cdots + B_0 z^m \quad (B_0 \neq 0)$$

onde para todo k, A_k, B_k são formas em x, y de grau k. Então o determinante $R(x,y)$ de F, G é zero ou um polinômio homogêneo de grau mn.

Prova: O resultante R(x,y) é dado por um determinante de ordem (m + n). E como $A_k,\ B_k$ são formas de grau k, o resultante R(tx, ty) é obtido multiplicando cada entrada $A_k,\ B_k$ por t^k. Multiplicando a primeira linha de A por t^n, o segundo por t^{n-1} e assim por diante até que o n-ésimo seja multiplicado por t. então o determinante é multiplicado por t^N, onde $N = \frac{1}{2}n(n+1)$, a soma dos primeiros n números naturais. Da mesma forma, multiplicamos a primeira linha de B por t^m, o segundo por t^{m-1}, e assim por diante, até que o m-ésimo seja multiplicado por t. Isso se multiplica o determinante por t^M onde $M = \frac{1}{2}m(m+1)$. Agora retiramos um fator de t^{m+n} da primeira coluna, um fator de t^{m+n-1} da segunda coluna, e assim por diante até finalmente retirarmos um fator de t da última coluna. Isso divide o determinante por t^W onde $W = \frac{1}{2}(m+n)(m+n+1)$. O resultado disso é dividir o determinante por $t^{W-N-M} = t^{mn}$. Por isso $R(tx,ty) = t^{mn}R(x,y)$. $\square$

Teorema 1. (Teorema de Bézout) *Sejam F, G curvas em $P\mathbb{C}^2$ de grau m, n sem componentes em comum. Então a soma do número de intersecções $I(P,F,G)$ nos pontos de intersecção P, é mn. Em particular, F e G se intersectam em pelo menos um ponto.*

Prova: A soma da da multiplicidade dos zeros de R(x, y) é exatamente mn, o grau de R. $\square$

Esta demostração do teorema de Bézout, usando a noção de resultante é a mais antiga e clássica. Porém hoje em dia já temos demonstrações melhor construídas deste teorema, que nos dão uma profundidade e possuem uma riqueza de detalhes algébricos muito maior, assim como as demostrações presentes em diferentes bibliografias a respeito do assunto, como nas referências 2 e 3.

4 Conclusões

Durante o desenvolvimento do projeto foi possível desenvolver grande conhecimento a respeito das curvas algébricas planas bem como resultados clássicos a respeito destas, a respeito de seus pontos singulares e interseções com outras curvas, assim como seu comportamento no plano projetivo.

Houve um foco principal em compreender a interseção de duas curvas algébricas projetivas sobre um corpo algebricamente fechado e sem componentes em comum, nos levando por ao estudo do Teorema de Bézout que tem grande relevância nesta área de estudos, e nos da como caso particular o fato de que uma reta intersecta uma curva em exatamente d pontos, onde d é o grau da curva em questão.

Referências

[1] C. G. Gibson, *Elementary Geometry of Algebraic Curves: an Undergraduate Introduction*, Cambridge Univ. Press, 1998.

[2] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves Over a Finite Field*, Princeton Univ. Press, Princeton, (2008).

[3] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, 2008.