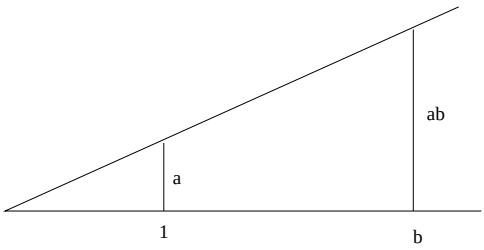
Universidade Estadual Vale do Acaraú
Mini-curso: Introdução às Curvas Algébricas Planas
Prof.: Paulo César Cavalcante de Oliveira - URCA

1. Um pouco de História

A manipulação de expressões do tipo $x^2 + y^2 = 1$ é um fato relativamente recente na história da Matemática, podendo se situar em torno do século XVI. Mas os matemáticos gregos já sabiam efetuar cálculos elaborados, recorrendo a procedimentos geométricos. Por exemplo, para o cálculo do produto de duas quantidades a e b, poderíamos proceder assim:



Neste exemplo, o segmento de comprimento a é traçado perpendicularmente à reta Ob. Esta construção requer somente o desenho de retas e círculos.

Além de retas e círculos, os matemáticos da Antiguidade estudaram outras curvas, geralmente descritas como o lugar geométrico de pontos satisfazendo certas condições. Essas curvas especiais eram o recurso empregado na soluação de vários problemas, para os quais todas as tentativas com régua e compasso fracassaram. Alguns desses têm uma história curiosa, em que lenda e fato se misturam. É o caso dos célebres problemas da duplicação do cubo, da trissecção do ângulo e da quadratura do círculo. Com a ulterior introdução do método da coordenadas, constatou-se que várias curvas conhecidas desde os primórdios da Geometria podiam ser descritas por equações polinomiais.

Definição 1: *Uma curva algébrica plana é o lugar dos pontos cujas coordenadas cartesianas satisfazem uma equação do tipo $f(X, Y) = 0$, onde f é um polinômio não constante.*

Exemplos: 1. O círculo de raio r e centro (a, b) : $(X - a)^2 + (Y - b)^2 = r^2$.

2. A reta que passa pelos pontos $(a, b) \neq (c, d)$. Sua equação é dada por

$$\begin{vmatrix} a & c & X \\ b & d & Y \\ 1 & 1 & 1 \end{vmatrix} = 0 \, .$$

3. A elipse, lugar dos pontos tais que a soma das distâncias a dois pontos fixos é uma constante, isto é

$$\sqrt{(X + c)^2 + Y^2} + \sqrt{(X - c)^2 + Y^2} = 2a \, .$$

Esta equação não é polinomial, mas é possível eliminar os radicais e mostrar que ela se reduz a $\dfrac{X^2}{a^2} + \dfrac{Y^2}{b^2} = 1$, onde $b = \sqrt{a^2 - c^2}$.

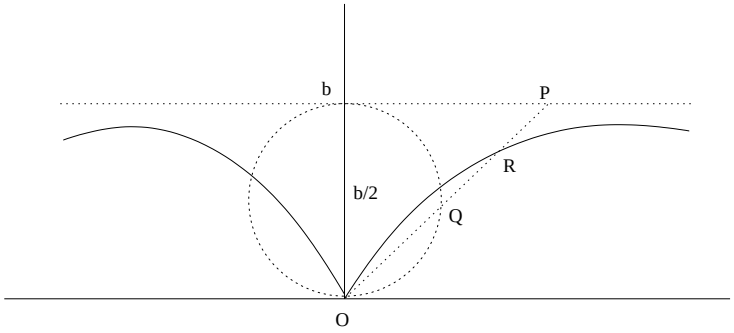
4. A hipérbole, lugar dos pontos cujas distâncias a dois pontos fixos, chamados focos, têm diferença $2a$, isto é,

$$|\sqrt{(X + c)^2 + Y^2} - \sqrt{(X - c)^2 + Y^2}| = 2a \, .$$

Vemos que esta equação não é polinomial, mas é possível eliminar os radicais e mostrar que ela se reduz a $\dfrac{X^2}{a^2} - \dfrac{Y^2}{b^2} = 1$.

5. A *cissóide de Diócles*: lugar dos pés das normais traçadas do vértice de uma parábola às suas tangentes. Dada a parábola de equação $X^2 = -4bY$ a tangente num ponto (x_0, y_0) é $-4b(Y - y_0) = 2x_0(X - x_0)$. A reta normal é $Y = \dfrac{2b}{x_0}X$. Assim, temos que o lugar geométrico dos pontos do plano (X, Y) que satisfazem essas condições é $bX^2 - Y(X^2 + Y^2) = 0$.

Em coordenadas polares teremos $r = b\cos\theta\text{cotg}\theta$. Daí, podemos obter uma descrição dinâmica que permite traçar a cissóide: construa o círculo de diâmetro b e centro $(0, \frac{b}{2})$. Considere a reta $Y = b$; para cada um de seus pontos P, trace a reta OP e tome o ponto Q da interseção com o círculo. Finalmente, marque o ponto R tal que $OR = PQ$. Variando P, o ponto R descreve a cissóide.



De fato, notando que o ângulo $\theta = \widehat{OPb} = \widehat{QbO}$, temos

$$\begin{aligned} OR &= PQ = OP - OQ \\ &= \frac{b}{\text{sen}\theta} - b\text{sen}\theta \\ &= b\cos\theta\text{cotg}\theta \end{aligned}$$

A cissóide foi empregada para resolver o problema da duplicação do cubo: dada a aresta de um cubo, construir a aresta de um cubo de volume duplo. Isto é, procuramos resolver a equação $X^3 = 2b^3$, onde b denota o comprimento da aresta conhecida.

Recorrendo à cissóide como *curva auxiliar*, a solução é obtida com o seguinte procedimento: considere a cissóide $(b-Y)X^2 = Y^3$. Determinemos a interseção dela com a reta $b - Y = 2X$ teremos então $Y = \sqrt[3]{2}X$. Fazendo $X = b$, chegamos a quantidade procurada.

2. Equação de uma Curva Algébrica

Uma questão que naturalmente se põe é se a equação polinomial $f = 0$ está bem determinada pela curva a resposta é *não*: $f = 0$ e $f^2 = 0$ admitem as mesmas soluções. Poderíamos arriscar o palpite de que esse seria o único tipo de indeterminação: se tomássemos f com grau mínimo, talvez todas as outras equações definindo a mesma curva fosse do tipo $f^m = 0$. Mas note que as soluções $XY = 0$ e $X^2Y = 0$ são as mesmas. Também $X^2 + Y^2 = 0$ e $2X^2 + Y^2 = 0$ têm as mesmas soluções.

Antes de darmos uma definição mais precisa de curva algébrica, consideraremos, em todo o texto salvo menção contrário, K um corpo algebricamente fechado de característica zero.

Proposição 1: *Sejam f, g polinômios em duas variáveis em $K[X,Y]$. Então $f(X,Y) = 0$ e $g(X,Y) = 0$ têm as mesmas soluções em K^2 se, e somente se, os fatores irredutíveis de f e g são os mesmos.*

Prova: Seja $p \in K[X,Y]$ um fator irredutível de f. Como f e g têm as mesmas soluções $(x,y) \in K^2$ então $p(x,y) = 0 \Rightarrow g(x,y) = 0$. Provaremos que p divide g em $K[X,Y]$.Trocando X por Y se necessário, podemos supor que Y ocorre efetivamente em p. Ponhamos $A = K[X]$ e $L = K(X)$. Assim, pelo Lema de Gauss, $p \in A[Y]$ é irredutível em $L[Y]$. Suponhamos por absurdo, que p não divide g. Então, MDC$(p,g) = 1$. Daí, vem que $ap + bg = 1$, onde $a, b \in L[Y]$. Podemos escrever $a = \frac{a'}{c}$ e $b = \frac{b'}{c}$, onde $a', b' \in A[Y]$ e $c \in A,\ c \neq 0$. Obtemos então $a'p + b'g = c$.

Agora, como Y ocorre efetivamente em p, segue-se que, exceto para um número finito de valores $x \in K$, a equação $p(x,Y) = 0$ admite solução. Conclui-se que há uma infinidade de valores de x tais que $c(x) = 0$, donde $c = 0$, uma contradição! Logo, $p|g$ em $L[Y]$ e, pelo Lema de Gauss, $p|g$ em $K[X,Y]$. □

Deduzimos da proposição anterior que uma curva algébrica, dada como lugar das soluções de uma equação polinomial não constante $f(X,Y) = 0$, determina(a menos de fator constante) uma equação de grau mínimo: tomar o produto dos fatores irredutíveis de f distintos. Temos então uma definição mais precisa de uma curva.

Definição 2: *Uma curva algébrica plana afim (ou mais abreviadamente, 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.

Dizemos que uma curva *está definida sobre o corpo* K_0, subcorpo de K, se ela admitir uma equação a coeficientes em K_0.

O *traço* de uma curva é o conjunto de soluções da equação. O *grau* de uma curva f é o grau de sua equação, e será denotado por $\deg(f)$. Curvas de grau 1,2,3,... são chamadas *retas, cônicas, cúbicas,....*

Uma curva é *irredutível* se admite uma equação que é um polinômio irredutível. 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 for ≥ 2, dizemos que p é uma *componente múltipla de* f.

Exercícios

Encontre as componentes irredutíveis das curvas abaixo:

a) $f(X,Y) = Y^2 - XY - X^2Y + X^3$ b) $g(X,Y) = X^3 + X - X^2Y - Y$
c) $h(X,Y) = Y^3 - X^3 + X^2Y - XY^2 + X^2 + Y^2 + X - Y - 1$ d) $f(X,Y) = 2X^2Y - 2X^3 + Y^2 - XY + X - Y$

3. Mudança de Coordenadas

Definição 3: *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 referencial canônico é dado por $O = (0,0), v_1 = (1,0)$ e $v_2 = (0,1)$.*

O *vetor de coordenadas* de um ponto $P \in K^2$ em relação a um referencial $\mathcal{R} = \{O, \{v_1, v_2\}\}$ é o par ordenado $(P)_{\mathcal{R}} = (x_1, x_2) \in K^2$ tal que

$$P = O + x_1 v_1 + x_2 v_2 \, . \quad (3)$$

Se $\mathcal{R}' = \{O', \{v_1', v_2'\}\}$ é outro referencial, obtemos da relação acima, juntamente com $P = O' + x_1' v_1' + x_2' v_2'$, uma fórmula que expressa $(P)_{\mathcal{R}}$ em termos de $(x_1', x_2') = (P)_{\mathcal{R}'}$. Para isso, escrevemos $v_j = a_{1j} v_1' + a_{2j} v_2'$, $O - O' = a_1 v_1' + a_2 v_2'$. Deduzimos então

$$\begin{aligned} x_1' v_1' + x_2' v_2' &= P - O' \\ &= a_1' v_1' + a_2 v_2' + x_1(a_{11} v_1' + a_2 1 v_2') + x_2(a_{12} v_1' + a_{22} v_2') \end{aligned}$$

e por fim, $(x_1', x_2') = (a_1 + a_{11}x_1 + a_{12}x_2, a_2 + a_{21}x_1 + a_{22}x_2)$.

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.

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

$$\left\{ \begin{array}{rcl} y_1 &=& a_{11}x_1 + a_{12}x_2 + a_1 \\ y_2 &=& a_{21}x_1 + a_{22}x_2 + a_2 \, , \end{array} \right.$$

com $\det(a_{ij}) \neq 0$.

Definição 4: *Dizemos que a afinidade T e o referencial $\mathcal{R}$ são associados se $(T(P))_{\mathcal{R}} = P, \ \forall \ P \in K^2$.*

Definição 5: *O K-automorfismo do anel de polinômios em duas variáveis $T_* : K[X_1, X_2] \to K[X_1, X_2]$ associado à afinidade $T : K^2 \to K^2$ é dado por,*

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

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

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

O emprego de T^{-1} na definição acima se justifica em vista da seguinte

Proposição 2: *Sejam f uma curva e T uma afinidade. Então o traço de $T_* f$ é igual à imagem do traço de f por T.*

Prova: Imediata.

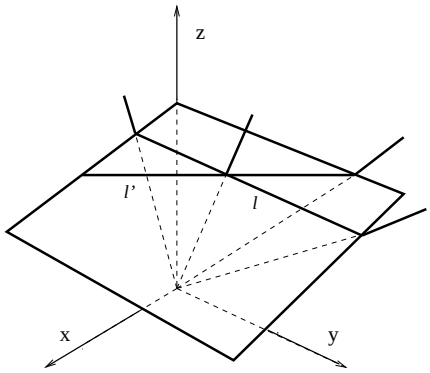
Definição 6: *Sejam T uma afinidade e $\mathcal{R}$ o referencial associado. A equação de uma curva f em relação a um referencial $\mathcal{R}$ é $(T_*)^{-1}f$.*

Definição 7: *Dizemos que uma propriedade $\mathcal{P}$ relativa a curvas é invariante ou independente do referencial se, para toda afinidade T, uma curva f satisfaz $\mathcal{P}$ se, e somente se, T_*f satisfaz $\mathcal{P}$.*

4. O Plano Projetivo

Consideremos o plano afim mergulhado no espaço tridimensional como o plano π de equação $Z = 1$.

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



Definição 8: *O plano projetivo $\mathbb{P}^2$ é o conjunto de retas do espaço tridimensional passando pela origem.*

Os pontos de $\mathbb{P}^2 \setminus \pi$ são chamados de *pontos no infinito*. Denotamos 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 $(x : y : z)$.

5. Espaços Projetivos

Definição 9: *O espaço projetivo $\mathbb{P}(V)$ associado a um espaço vetorial V é o conjunto dos subespaços de V de dimensão 1.*

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 $\{v_0, v_1, \ldots, v_n\}$ de V são as coordenadas $(x_0, x_1, \ldots, x_n)$ de um vetor não nulo do subespaço unidimensional representado por P.

Fixada a base, escrevemos $P = (x_0 : x_1 : \cdots : x_n)$ para indicar um ponto com essas coordenadas homogêneas.

Para cada $i = 0, 1, \ldots, n$, o subconjunto de $\mathbb{P}^n$, $U_i = \{(x_0 : \cdots : x_n);\ x_i \neq 0\}$ pode ser identificado com K^n através da bijeção

$$(x_0 : \cdots : x_n) \longleftrightarrow \left(\frac{x_0}{x_i}, \ldots, \frac{\widehat{x_i}}{x_i}, \ldots, \frac{x_n}{x_i}\right) .$$

Convencionamos escrever $\mathbb{A}^n = U_n$ e 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, $\mathbb{P}^n \setminus \mathbb{A}^n$ identifica-se a um $\mathbb{P}^{n-1}$, que convencionamos chamar *hiperplano no infinito*.

6. Curvas Projetivas

Definição 10: *Seja $\sum_{i=0}^{d} f_i$, 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 $d = degf$,*

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

Definição 11: *Uma curva plana projetiva é uma 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 múltiplo constante do outro.*

Observemos que, 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.

Curvas de grau $1, 2, 3, \ldots$ são, como antes, chamadas *retas, cônicas, cúbicas,* etc.

A reta $Z = 0$ é usualmente chamada de *reta no infinito.* O *fecho projetivo* de uma curva afim f é a curva projetiva definida pela homogeneização f^*.

7. Curvas Maximais

Seja C uma curva algébrica projetiva não-singular definida sobre um corpo finito $K = \mathbb{F}_q$. Por um resultado devido a Weil temos que

$$\#C(\mathbb{F}_q) \leq 1 + q + 2g\sqrt{q}, \qquad (1)$$

onde g é o gênero da curva e $\#C(\mathbb{F}_q)$ denota o número de pontos racionais de C.

Curvas para as quais a desigualdade em (1) é uma igualdade(neste caso $q = p^{2n},\ n \in \mathbb{N}$) são chamadas de *curvas maximais*(sobre $\mathbb{F}_q$). Por um resultado devido a Ihara, temos que o gênero g de uma curva maximal satisfaz

$$g \leq \frac{\sqrt{q}(\sqrt{q}-1)}{2}\ .$$

Exemplo:(Curva de Hermite) Considere a curva projetiva $\mathcal{H}$ associada ao polinômio $f(X,Y)$ abaixo:

$$f(X,Y) = Y^{p^n} + Y - X^{1+p^n} \in K[X,Y],$$

onde K é o corpo finito de cardinalidade $q = p^{2n}$, com $n \in \mathbb{N}$.

O polinômio homogêneo associado $F(X,Y,Z)$ é dado por

$$F(X,Y,Z) = ZY^{p^n} + Z^{p^n}Y - X^{1+p^n}\ .$$

Temos que $\mathcal{H}$ é não-singular. Assim, o gênero g da curva $\mathcal{H}$ é dado por

$$g = \frac{(d-1)(d-2)}{2} = \frac{p^n(p^n-1)}{2} = \frac{\sqrt{q}(\sqrt{q}-1)}{2}\ .$$

Calculemos agora o número de pontos racionais de $\mathcal{H}$.

Seja $(x,y) \in \overline{K} \times \overline{K}$ um ponto da curva afim, isto é: $y^{p^n} + y = x^{1+p^n}$. Suponha $x \in K$, i.e., temos $x^{p^{2n}} = x$. Assim,

$$\begin{aligned} y^{p^{2n}} + y^{p^n} &= (y^{p^n} + y)^{p^n} \\ &= (x^{1+p^n})^{p^n} = x^{1+p^n} \\ &= y^{p^n} + y\ . \end{aligned}$$

Assim, $y^{p^n} = y$, logo $y \in K$.

Para cada $x \in K$, existem exatamente p^n soluções no fecho algébrico de K para a equação polinomial $Y^{p^n} + Y = x^{1+p^n}$.

Os argumentos acima mostram que qualquer solução $y \in \overline{K}$ é racional sobre K, i.e., $y \in K$. Para cada $x \in K$, existem p^n elementos $y \in K$ tais que o par (x,y) pertencem a curva.

Observando que $(0:1:0)$ é o único ponto do infinito de $\mathcal{H}$, temos então $\#\mathcal{H}(K) = 1 + p^{3n}$.

Um cálculo direto mostra que $1 + q + 2g\sqrt{q} = 1 + p^{3n}$. Segue que $\mathcal{H}$ é uma curva maximal.

Referências

[1] Vainsencher, Israel, *Introdução às Curvas Algébricas Planas*, Col. Mat. Universitária, IMPA, 2a. edição, Rio de Janeiro, 2005.

[2] Garcia, Arnaldo, *Pontos Racionais em Curvas sobre Corpos Finitos*, 20° Colóquio Brasileiro de Matemática, IMPA, Rio de Janeiro, 1995.

[3] Fulton, William, *Algebraic Curves: An Introduction to Algebraic Geometry*, W.A. Benjamin, Inc., New York, 1969.