A estrutura de grupo das cúbicas não singulares

Pedro Pfarrius Barbassa e Prof. Dr. Marcos Benevenuto Jardim

Palavras-chave: Geometria algébrica, Curvas algébricas, Cúbicas suaves

1 Introdução

Este trabalho de pesquisa faz parte da geometria algébrica, uma área da matemática que junta a geometria e a álgebra. A geometria algébrica tem como foco o estudo de soluções de equações polinomiais, ou seja, queremos estudar o conjunto dos pontos que zeram um polinômio com coeficientes em um corpo algebricamente fechado.

O tópico princial deste trabalho é a estrutura de grupo formada pelos pontos de uma cúbica não singular, também chamada de cúbica suave. Um grupo é uma dupla formada por um conjunto e uma operação, onde a operação satisfaz ser fechada, associativa, possui elemento neutro e inverso. Quando a operação for comutativa chamamos o grupo de abeliano. Para chegarmos ao resultado principal, precisamos de tópicos de curvas no plano, como irredutibilidade, singularidade e o teorema de Bezout.

2 Resultados preliminares

O espaço em que vamos considerar as curvas será o plano projetivo $\mathbb{P}^2_k$, onde k é um corpo algebricamente fechado. O plano projetivo é o conjunto das classes de equivalência da seguinte forma:

$$(x : y : z) \sim (x' : y' : z') \iff \exists\ \lambda \in k^* \text{ tal que } (x, y, z) = \lambda(x', y', z')$$

Assim dois pontos em $\mathbb{P}^2_k$ serão o mesmo, se forem múltiplos um do outro em k^3.

Uma curva plana projetiva será o conjunto dos pontos $(x : y : z) \in \mathbb{P}^2_k$ que zeram um determinado polinômio homogêneo $f \in k[x, y, z]$. Um polinômio ser homogêneo significa que para cada $\lambda \in k$ não nulo, temos $f(\lambda x, \lambda y, \lambda z) = \lambda^d f(x, y, z)$ onde d é o grau do polinômio. Definimos o grau da curva como sendo o grau do polinômio que a define. Para facilitar a notação, vamos sempre denotar uma curva por f, onde f é seu polinômio associado. Como estamos considerando curvas no plano projetivo, o polinômio ser homogêneo é necessário para que os pontos que o anulam estejam bem definidos.

Dizemos que uma curva f é irredutível, se o polinômio que a define for irredutível, ou seja, f não pode ser escrito como produto de dois polinômios não constantes. Uma curva não irredutível é chamada de redutível.

Exemplo:

1) A curva $f(x, y, z) = x^2y - z^3 + y^3$ é uma cúbica (curva de grau 3) irredutível.

2)A curva $g(x, y, z) = xz - yz + z^2 = z(x - y + z)$ é uma cônica (curva de grau 2) redutível.

Dizemos que uma curva f é singular, se existe um ponto $p \in f$, tal que as derivadas parciais se anulam em p, isto é:

$$\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = \frac{\partial f}{\partial z}(p) = 0$$

geometricamente, um ponto ser não singular significa que a reta tangente no ponto é única. Dizemos que uma curva f é não singular (ou suave) se todos os seus pontos forem não singulares.

Exemplo:

1) A curva redutível $g(x, y, z) = xz - yz + z^2$ é singular no ponto $(1 : 1 : 0)$, já que $g(1, 1, 0) = 0$ e calculando sua derivadas parcias temos: $\frac{\partial g}{\partial x}(x, y, z) = z$; $\frac{\partial g}{\partial y}(x, y, z) = z$; $\frac{\partial g}{\partial z}(x, y, z) = x - y + 2z$. Note que o ponto $(1 : 1 : 0)$ zera as derivadas parciais e portanto é um ponto singular. Logo a curva g é singular.

Teorema de Bezout. *Sejam f e g duas curvas projetivas sem componentes em comum. Então existem nm pontos contados com multiplicidade na intercecção de f e g. Aonde n e m são o grau das curvas f e g, respectivamente.*

Note que no teorema de Bezout as curvas não precisam ser irredutíveis, mas o teorema vale para curvas irredutíveis.

Corolário. *Toda curva suave é irredutível.*

Demonstração. Seja f uma curva redutível. Então existem polinômios homogêneos g, h tais que $f = gh$. Podemos supor que g e h não possuem componentes em comun, pois caso contrário teríamos que $g = g_1k$ e $h = h_1k$ e assim $f = gh = k^2g_1h_1 = g_2h_1$, onde $g_2 = k^2g_1$ e h_1 não tem componente em comun. Como g e h não tem componente em comun, pelo teorema de Bezout sabemos que existe pelo menos um ponto $p \in g \cap h$, tal que $g(p) = h(p) = 0$. Disso segue que:

$$\frac{\partial f}{\partial x}(p) = \frac{\partial g}{\partial x}(p)h(p) + \frac{\partial h}{\partial x}(p)g(p) = 0$$

$$\frac{\partial f}{\partial y}(p) = \frac{\partial g}{\partial y}(p)h(p) + \frac{\partial h}{\partial y}(p)g(p) = 0$$

$$\frac{\partial f}{\partial z}(p) = \frac{\partial g}{\partial z}(p)h(p) + \frac{\partial h}{\partial z}(p)g(p) = 0$$

Logo f é uma curva singular, ou seja, uma curva suave não pode ser redutível. Consequentemente toda curva suave é irredutível. □

3 A estrutura de Grupo

A partir de agora vamos considerar C como sendo uma cúbica suave no plano projetivo. Pelo teorema de Bezout, sabemos que toda reta passa por C em até 3 pontos distintos, pelo fato de C ser irredutível, pelo grau de C ser 3 e a da reta 1. Diremos que uma tripla (p, q, r) onde $p, q, r \in C$ é colinear se existe uma reta que passa pelos 3 pontos. A tripla colinear não precisa necessariamente ter pontos distintos, podem ocorrer casos em que (p, p, q) e (p, p, p) são colineares, no último caso p é chamado de ponto de inflexão.

Dada uma cúbica suave C e uma tripla colinear (p, q, r), definimos a seguinte operação $* : C \times C \to C$ na qual associa dois pontos ao terceiro ponto da sua tripla colinear, ou seja, $p * q = r$.

Por mais que a operação $*$ seja comutativa, ela não torna C em um grupo pelo seguinte fato: podemos encontrar um ponto de inflexão o tal que (o, o, o) é uma tripla colinear. Com isso pegamos pontos distintos p, q tais que (p, q, o) é uma tripla colinear, disso temos que $o*(p*q) = o*o = o$ e $(o*p)*q = q*q$, se $*$ for associativa, então segue que $q * q = o$ e portanto (q, q, o) é colinear.

Portanto, segue que $p = q * o = q$, o que é um absurdo. Assim por $*$ não ser associativa, temos que $(C, *)$ não forma um grupo.

Teorema. *Dada uma cúbica suave C, vamos fixar um ponto $o \in C$. Com isso, existe uma única operação $+ : C \times C \to C$, que satisfaça:*

- *O ponto o é o elemento neutro, isto é: $p + o = p$, $\forall p \in C$*
- *O trio (p, q, r) é colinear se e somente se $p + q + r$ é constante.*

Demonstração. **Unicidade:** Vamos supor que a estrutura de grupo existe e a partir disso mostrar que é única. Dados $p, q \in C$, seja $p * q = r$ e $r * o = s$, assim obtemos duas triplas colineares (p, q, r) e (r, o, s). Pela segunda propriedade, temos que suas somas são constante, ou seja, são iguais. Portanto:

$$p + q + r = r + o + s \implies p + q = o + s = s \implies p + q = o * r = o * (p * q)$$

Note que apenas cancelamos ambos os lados e usamos o como elemento neutro, pois consideramos a existência da estrutura de grupo. Pela unicidade da operação $*$, obtemos que $+$ é determinado unicamente por $*$.

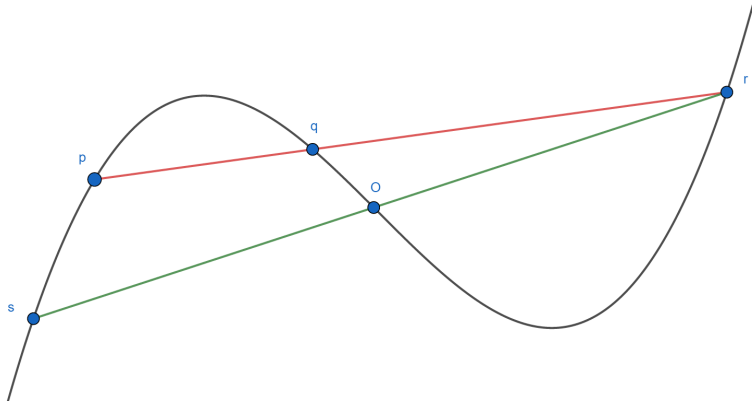

Figura 1: Aonde $p * q = r$ e $p + q = s$

Existência: Agora já temos nossa operação de soma feita: $p + q = o * (p * q)$, $\forall p, q \in C$. Portanto basta mostrarmos as propriedades que tornam C um grupo. Note que essa operação é fechada e que dado (p, q, r), temos que $q * (p * q) = q * r = p$, assim tomando o caso particular $q = o$, temos que: $p + o = o * (p * o) = p$, ou seja, o é de fato elemento neutro. A associatividade por ser bem complicada e extensa não será mostrada aqui, mas uma ideia para demonstra-la seria fixar 3 pontos na curva e considerar todas as possíveis combinações com a operação $+$, com isso montar um diagrama e usar um

lema que diz: dado 8 pontos em posições genéricas, existe um outro ponto x tal que toda cúbica passando pelos 8 pontos passa por x. Utilizando tal lema, iriamos decompor o polinômio que define C e a partir disso mostrar a associatividade. Agora, vamos encontrar o elemento inverso. Para (p, q, r) e (r, o, s), temos $p + q + r = s + r = o * (s * r) = o * o$, como o é fixo, então $o * o$ é constante. Considere a tripla $(p, o * o, (o * o) * p)$, disso segue que

$$p + (o * o) + ((o * o) * p) = o * o \implies p + (o * o) * p = o$$

Logo obtemos que $-p = (o*o)*p$. A comutatividade de $+$ segue diretamente da comutatividade de $*$, já que $p+q = o*(p*q) = o*(q*p) = q+p$. Portanto $(C, +)$ é um grupo abeliano. □

Uma das principais aplicações da estrutura de grupos seria a sua relação com as curvas elípticas, que por sua vez tem papel fundamental na demonstração do último teorema de Fermat. As curvas elípticas também tem uma grande importância na criptografia, que nesse caso é considerado curvas elípticas sobre corpos finitos.

Agradecimentos

Gostaria de agradecer ao prof. Marcos pelo tempo e paciência. Também gostaria de agradecer à PIBIC-CNPQ pelo financiamente deste projeto de pesquisa.