A estrutura de grupo de uma cúbica plana irredutível

Palavras-Chave: CÚBICA, CURVA ELÍPTICA, PONTO RAIONAL, GRUPO.

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

1 Introdução

Este projeto de pesquisa visa estudar a estrutura de grupo do conjunto de pontos não-singulares de uma uma cúbica plana irredutível, com enfoque no caso dos pontos racionais, isto é, a coordenadas no corpo $\mathbb{Q}$ dos racionais. Serão abordados resultados clássicos, como os Teoremas de Mordell e Nagell-Lutz; em particular, o primeiro afirma que, no caso racional, todo grupo oriundo de uma cúbica é um grupo abeliano finitamente gerado. Apesar da dificuldade de calcular o grupo explicitamente para uma curva específica, particular relevância será dada ao estudo de exemplos concretos, onde a determinação do grupo pode ser feita explicitamente.

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

3.1 A estrutura de grupo de uma cúbica.

Seja F uma cúbica plana complexa projetiva irredutível, isto é, uma classe de equivalência (a menos de multiplicação por uma constante $\lambda \in \mathbb{C}^*$) de polinômios homogêneos irredutíveis, de grau 3 em $\mathbb{C}[X, Y, Z]$. Considere agora o conjunto S_F dos pontos não singulares de F.

Definição 1. *Sejam P e Q pontos simples em F, seja L a reta que passa por esses dois pontos. Definimos a "operação estrela"entre eles $P \star Q$ como sendo o terceiro ponto R de interseção entre L e a curva F.*

Note que a existência deste terceiro ponto é garantida pelo Teorema de Bézout, e que esta operação é claramente comutativa. Esta operação não é o suficiente para que um grupo seja construído, já que não possui elemento neutro (ou identidade). Vamos agora definir uma nova operação para que isso seja possível.

Definição 2. *Seja $\mathcal{O} \in S_F$ um ponto, que chamaremos de "ponto de base"e $P,\ Q \in S_F$. A soma de P e Q é definida por $P + Q = (P \star Q) \star \mathcal{O}$.*

Lema 1. *S_F é um grupo sob a operação "+"definida a cima, com identidade $\mathcal{O}$ e elemento inverso $-S$ de um elemento S dado por $-S = S \star (\mathcal{O} \star \mathcal{O})$.*

Lema 2. *Seja F uma cúbica não singular. Os grupos $(S_F, +)$ com ponto de base $\mathcal{O} \in F$ e $(S_F, +')$ com ponto de base $\mathcal{O}' \in F$ são isomorfos.*

3.2 Forma Normal de Weierstrass.

A *Forma Normal de Weierstrass*, é caracterizada por uma curva algébrica de grau três da seguinte forma:

$$y^2 = f(x) = x^3 + ax^2 + bx + c \tag{1}$$

Nosso maior interesse ao longo deste projeto serão os pontos racionais, ou seja pontos onde as coordenadas x e y são números racionais, das cúbicas não singulares e, convenientemente, qualquer curva desta forma é birracionalmente equivalente à forma normal de Weierstrass. Ou seja, existe uma transformação racional invertível, cuja inversa também é racional, que nos dá uma equivalência biunívoca entre os pontos racionais da cúbica em questão e os pontos racionais da forma normal de Weierstrass.

A operação aditiva definida anteriormente é invariante sob esse tipo de transformação, fazendo com que a estrutura do grupo S_F seja preservada. Isso nos permite reduzir o estudo sobre os pontos racionais de uma cúbica não singular qualquer ao estudo dos pontos racionais da forma normal de Weierstrass. Provar que transformações birracionais são um homomorfismo está fora do alcance deste projeto, portanto seguiremos apenas tomando isto como verdade.

Homogeneizando a Equação (1) temos a seguinte Equação:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3 \tag{2}$$

Observe que se tomarmos a interseção entre a curva e a reta no infinito $Z = 0$, temos $X^3 = 0$, ou seja, uma raiz tripla $X = 0$, o que significa que a reta no infinito encontra a curva três vezes no mesmo ponto, sendo ele $(0 : 1 : 0)$. Também podemos facilmente verificar que $(0 : 1 : 0)$ é um ponto não singular tomando as derivadas da Equação (2) com relação a cada uma das variáveis.

Vamos definir este ponto como sendo nosso ponto de base $\mathcal{O}$ daqui por diante mesmo que estejamos trabalhando no plano afim xy pois, sendo ele o ponto no infinito, é garantido que qualquer reta realmente encontra a cúbica em três pontos.

Observe que a reta no infinito encontra a cúbica no ponto $\mathcal{O}$ três vezes, as retas verticais encontram a cúbica em dois pontos do plano xy e também no ponto $\mathcal{O}$, e as retas não verticais encontram a cúbica em três pontos no plano xy.

3.3 O Teorema de Nagell–Lutz.

Definição 3. *Seja $m > 0$ um inteiro positivo. Um elemento qualquer P de um grupo é dito ter **ordem** m se*

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ vezes}} = \mathcal{O}, \tag{3}$$

*onde $m'P \neq \mathcal{O}$ para todos os inteiros $1 \leq m' < m$. Se tal m existe, então P tem **ordem finita**. Caso contrário, dizemos que P tem **ordem infinita**.*

Teorema 1 (Teorema de Nagell–Lutz)**.** *Seja*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

uma cúbica não singular com coeficientes a, b, c pertencentes ao dos números inteiros, e D o discriminante de $f(x)$

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Seja $P = (x, y)$ um ponto racional de ordem finita. Então x e y são inteiros, e ou $y = 0$, no caso em que P tem ordem 2, ou y divide D.

Este teorema é útil para encontrarmos os pontos racionais de ordem finita em um número finito de etapas. Basta pegar o inteiro D e analisar seus divisores como valores para y. Substituindo esses valores na equação $y^2 = f(x)$. O polinômio f(x) tem coeficientes inteiros, então ele tem pelo menos uma raiz inteira, essa raiz deve dividir o termo constante. Assim, há apenas um número finito de valores possíveis de x para verificar.

Outro ponto importante é destacar que este teorema não é um "se e somente se", logo, é bem possível ter pontos com coordenadas inteiras e com y dividindo D que não são pontos de ordem finita. O teorema de Nagell–Lutz pode ser usado para compilar uma lista de pontos que inclui todos os pontos de ordem finita, mas nunca pode ser usado para provar que qualquer ponto em particular realmente tem ordem finita.

3.4 O Teorama de Mordell

Várias ferramentas são necessárias para chegar de fato no Teorema de Mordell. Vamos começar com uma defin̨ção:

Definição 4. *Seja um ponto $P = (x, y)$, onde $x = m/n$ é um número racional na forma irredutível. A **altura** de P é dada da seguinte forma*

$$H(P) = H(x) = H(m/n) = max\{|m|, |n|\}.$$

*E h é a **função altura** onde $h(P) = logH(P)$.*

Agora podemos enunciar o seguinte teorema, conhecido por "Descent Theorem".

Teorema 2. *Seja Γ um grupo abeliano, e suponha que existe uma função*

$$h : \Gamma \longrightarrow [0, \infty)$$

com as seguintes propriedades:

i) Para todo número real M, o conjunto $P \in \Gamma : h(P) \leq M$ é finito.

ii) Para todo $P_0 \in \Gamma$ existe uma constante k_0 tal que

$$h(P + P_0) \leq 2h(P) + k_0 \; \forall \; P \in \Gamma$$

iii) Existe uma constante k tal que

$$h(2P) \geq 4h(P) - k \; \forall \; P \in \Gamma$$

iv O subgrupo 2Γ é de índice finito em Γ

Então Γ é finitamente gerado.

É possível verificar que tomando o grupo Γ como sendo o grupo dos pontos racionais de uma curva elíptica, ele satisfaz todas as propriedades do teorema anterior, e provando-o, temos basicamente a prova do Teorema de Mordell enunciado a seguir.

Teorema 3. *Teorama de Mordell*
Seja C uma cúbica não singular dada pela equação

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c$$

onde a e b são inteiros, então o grupo de pontos racionais $C(\mathbb{Q})$ é um grupo abeliano finitamente gerado.

De um jeito mais simples podemos dizer que existem geradores $P_1, \cdots, P_r, Q_1, \cdots, Q_s \in C(\mathbb{Q})$ de forma que para to do $P \in C(\mathbb{Q})$

$$P = n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \cdots + m_sQ_s.$$

Aqui, os inteiros n_i são unicamente determinados por P, enquanto os inteiros m_j são determinados módulo $p_j^{\nu_j}$.

Pela estrutura do teorema temos que

$$C(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \; vezes} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}}$$

O inteiro r é chamado de *posto* (ou *rank*) de $C(\mathbb{Q})$. O grupo $C(\mathbb{Q})$ é finito se, e somente se, ele tem posto $r = 0$. O subgrupo

$$\mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}$$

corresponde aos elementos de ordem finita em $C(\mathbb{Q})$.

O posto da r curva pode ser calculado a partir da fórmula

$$2^r = \frac{(\Gamma : \psi(\bar{\Gamma}) \cdot (\Gamma : \phi(\bar{\Gamma})}{4}.$$

onde $\phi : \Gamma \to \bar{\Gamma}$ e $\psi : \Gamma \to \bar{\Gamma}$ são homomorfismos definidos da seguinte forma:

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & \text{se } P = (x,y) \neq \mathcal{O}, T, \\ \mathcal{O}, & \text{se } P = \mathcal{O} \text{ ou } P = T. \end{cases}$$

$$\psi(\overline{P}) = \begin{cases} \left(\frac{\overline{y}^2}{\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{\overline{x}^2}\right), & \text{se } \overline{P} = (\overline{x},\overline{y}) \neq \overline{\mathcal{O}}, \overline{T}, \\ \mathcal{O}, & \text{se } \overline{P} = \overline{\mathcal{O}} \text{ ou } \overline{P} = \overline{T}. \end{cases}$$

E a composição $\psi \circ \phi : C \to C$ é a multiplicação por dois, isto é, $\psi \circ \phi(P) = 2P$.
Podemos também introduzir um mapa α de Γ para $\mathbb{Q}^*/\mathbb{Q}^{*2}$ definida por:

$$\alpha(\mathcal{O}) = 1 \mod \mathbb{Q}^{*2},$$

$$\alpha(0,0) = b \mod \mathbb{Q}^{*2},$$

$$\alpha(x,y) = x$$

Depois de algumas contas, podemos afirmar que

$$2^r = \frac{(\Gamma : \phi(\overline{\Gamma})) \cdot (\overline{\Gamma} : \phi(\Gamma))}{4} = \frac{\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma})}{4}.$$

Assim temos as ferramentas para tentar calcular explicitamente o posto de curvas elípticas.

4 Conclusões

Apresentamos a estrutura de grupo associada aos pontos racionais de cúbicas planas não singulares, equivalentemente, nas curvas elípticas definidas sobre os racionais. Com base nos teoremas de Mordell e Nagell–Lutz, exploramos como essas curvas admitem uma estrutura de grupo abeliano finitamente gerado, e vimos que é possível determinar explicitamente sua parte de torção e, em alguns casos, seu posto.

Referências

[1] J. W. S. Cassels, *Lectures on Elliptic curves*, London Mathematical Society Student Texts, Cambridge University press, 1991.

[2] C. G. Gibson, , *Elementary Geometry of Algebraic Curves, An Undergraduate Introduction*, Cambridge University Press Ed. 1, 2001.

[3] A. Machì, *Groups. An Introduction to Ideas and Methods of the Theory of Groups*, Springer-Verlag Italia, 2012.

[4] J. H. Silverman, J.T. Tate, *Rational points on elliptic curves*, Second Edition, Undergraduate Texts in Mathematics, Springer, 2015.