DAS INTEGRAIS ELÍPTICAS ÀS CURVAS ELÍPTICAS

IZABELLA CALAIS FERNANDES
ORIENTADOR: TIAGO JARDIM DA FONSECA

Universidade Estadual de Campinas
Projeto de IC fomentado pela Fundação de Amparo à Pesquisa do Estado de São Paulo - FAPESP - Processo: 2023/09523-8.

Introdução

Este projeto de IC busca estabelecer uma conexão entre integrais elípticas, funções elípticas e curvas elípticas, apresentando brevemente os conceitos importantes que têm sido objetos centrais de estudo em matemática desde o século XVIII. Tais temas continuam relevantes até hoje, assumindo um papel importante nas áreas de análise, geometria algébrica e contribuindo para aplicações em teoria dos números.

1. Integrais Elípticas e Funções Elípticas

Seja $R(x, y) \in \mathbb{C}(x, y)$ uma função racional e $f(x) \in \mathbb{C}[x]$ um polinômio. Nesta seção, estaremos interessados em expressões da forma

$$I = \int R(x, \sqrt{f(x)})dx.$$

Quando o grau de f é 1 ou 2, a integral acima é *elementar*, ou seja, pode ser expressa em termos de funções algébricas, trigonométricas, trigonométricas inversas, exponenciais e logarítmicas. Estas integrais aparecem naturalmente, por exemplo, em problemas geométricos envolvendo o cálculo de comprimento de arco de curvas ou de áreas de figuras bidimensionais, problemas de física clássica, como a descrição de um pêndulo simples, entre outras aplicações diversas.

Como exemplo deste tipo de integral, tomaremos o cálculo do comprimento de arco do círculo unitário, dada por

$$s(t) = \int_0^t \frac{1}{\sqrt{1-x^2}}dx = \arcsin t$$

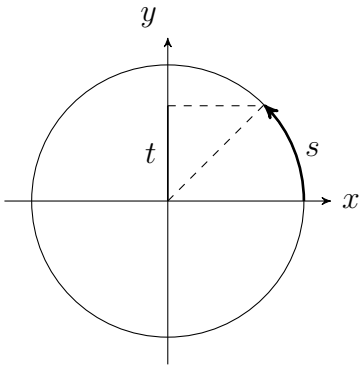

Figura 1. Arco do círculo

Date: 7 de agosto de 2024.

Agora, se o grau de $f(x)$ é maior que dois, a integral nem sempre é elementar. O caso de interesse para este trabalho será em que $f(x)$ é um polinômio de grau 3 ou 4 e não possui raízes múltiplas. A expressão neste caso é chamada de *integral elíptica*. O exemplo que tomaremos ao longo do texto para uma integral elíptica será o comprimento de arco da *lemniscata* (isto é, a curva plana definida pela equação $(x^2+y^2)^2 = (x^2-y^2)$), dado por

$$z(r) = \int_0^r \frac{dx}{\sqrt{1-x^4}}. \tag{1}$$

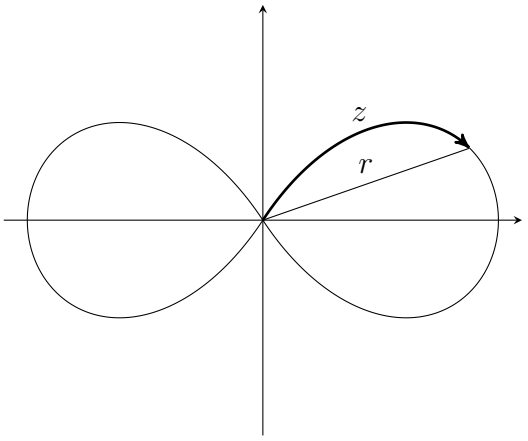

FIGURA 2. Arco da lemniscata

Cada integral elíptica da forma

$$z(r) = \int_0^r R(x, \sqrt{f(x)})dx,$$

possui uma expressão inversa $r(z)$, definindo uma função que é análoga a uma função trigonométrica, com a lemniscata fazendo o papel do círculo. Este tipo de função foi intensamente estudado por Gauss, Euler, Abel e muitos outros matemáticos a partir do século XVIII. Já que são funções que não possuem uma expressão elementar, procuravam-se maneiras de se extrair informações destas funções por outros meios. Uma propriedade surpreendente são as *fórmulas de adição* descobertas inicialmente por Fagnano e posteriormente expandidas por Abel e Euler.

Voltando ao exemplo do comprimento de arco do círculo, ao invertemos a expressão obtemos

$$t(s) = \text{sen}(s),$$

cuja fórmula de adição é bem conhecida:

$$\text{sen}(s+u) = \text{sen}(s)\sqrt{1-\text{sen}(u)^2} + \text{sen}(u)\sqrt{1-\text{sen}(s)^2},$$

Já para o arco da lemniscata, denotaremos a função inversa por $\text{sl}(z) \coloneqq r(z)$. A função sl pode ser estendida para uma função meromorfa sobre todo o plano complexo $\mathbb{C}$, e Fagnano foi capaz de provar a seguinte fórmula de adição.

Teorema 1.1 (Fórmula da adição)**.** *Sejam, $z, w \in \mathbb{C}$, e* sl *a função definida como acima, então*

$$\text{sl}(z+w) = \frac{\text{sl}(w)\sqrt{1-\text{sl}(z)^4} + \text{sl}(z)\sqrt{1-\text{sl}(w)^4}}{1+\text{sl}(z)^2\text{sl}(w)^2}. \tag{2}$$

Como um corolário desta fórmula de adição, obtemos a seguinte propriedade da função sl.

Corolário 1.1. *Seja $z \in \mathbb{C}$, então*

$$\text{sl}(z+\lambda) = \text{sl}(z), \qquad \text{sl}(z+i\lambda) = \text{sl}(z), \tag{3}$$

onde

$$\lambda = z(1) = \int_0^1 \frac{dx}{\sqrt{1-x^4}}$$

é a chamada constante de Gauss.

A equação (3) pode ser resumida dizendo que a função sl é uma função duplamente periódica, com períodos λ e $i\lambda$. E com essa propriedade em mãos, podemos reescrever a fórmula (2) em termos das integrais como

$$\int_0^a \frac{dx}{\sqrt{1-x^4}} + \int_0^b \frac{dx}{\sqrt{1-x^4}} = \int_0^c \frac{dx}{\sqrt{1-x^4}} \mod \lambda\mathbb{Z} + i\lambda\mathbb{Z}$$

onde

$$c = \frac{a\sqrt{1-b^4} + b\sqrt{1-a^4}}{1+a^2b^2}.$$

Funções sobre o plano complexo que são meromorfas e duplamente periódicas são chamadas de *funções elípticas* e, como vimos acima, a função sl é o nosso primeiro exemplo de uma função elíptica.

Por fim, vale ressaltar que todos os resultados apresentados acima para a lemniscata possuem análogos para quaisquer polinômios de grau 3 ou 4.

2. As funções $\wp$ de Weierstrass

A abordagem de Weierstrass para o estudo de curvas elípticas foi formalizada através da introdução de funções especiais que serão apresentadas nessa seção, e que possuem uma forte relação com as chamadas curvas elípticas.

Dados dois números complexos não nulos ω_1 e ω_2, $\mathbb{R}$-linearmente independentes, consideramos o reticulado $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ em $\mathbb{C}$, e definimos a *função $\wp$ de Weierstrass* associada ao reticulado Λ da seguinte maneira

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}.$$

Tanto $\wp_\Lambda$ quanto sua derivada $\wp'_\Lambda$ são funções elípticas com períodos ω_1, ω_2.

Exemplo 2.1. A função sl é elíptica com períodos λ e $i\lambda$, e então podemos nos perguntar pela relação entre sl e $\wp_\Lambda$ onde $\Lambda = \lambda\mathbb{Z} + i\lambda\mathbb{Z}$. Acontece que estas funções estão relacionadas pela equação abaixo

$$\wp_\Lambda(z) = \frac{1}{\mathrm{sl}(z)^2}.$$

O próximo teorema é o responsável por fazer a conexão entre as funções $\wp$ de Weiertrass e as curvas elípticas.

Teorema 2.1. *A função $\wp_\Lambda$ é solução para a seguinte equação diferencial*

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2\wp_\Lambda(z) - g_3$$

onde Λ determina unicamente g_2 e g_3 através da série das séries de Eisenstein

$$g_2 = 60\sum_{\substack{\lambda\in\Lambda\\ \lambda\neq 0}} \frac{1}{\lambda^4}, \qquad g_3 = 140\sum_{\substack{\lambda\in\Lambda\\ \lambda\neq 0}} \frac{1}{\lambda^6}.$$

Isso implica que o mapa $z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z))$ é uma parametrização (ou *uniformização*) da curva algébrica plana em $\mathbb{C}^2$ definida pela equação

$$y^2 = 4x^3 - g_2x - g_3. \tag{4}$$

Este tipo de curva é chamado de *curva elíptica*, e apresentaremos mais de suas propriedades na próxima seção.

Observação 2.1. A construção acima é análoga à parametrização do círculo por funções trigonométricas. Se tomarmos $p(x) = \text{sen}(x)$ o mapa $x \mapsto (p(x), p'(x)) = (\text{sen}(x), \cos(x))$ parametriza o círculo $x^2 + y^2 = 1$.

3. Curvas Elípticas

Uma curva elíptica complexa é uma curva algébrica projetiva plana determinada por uma equação (afim) da forma

$$y^2 = f(x),$$

onde $f(x)$ é um polinômio cúbico com três raízes distintas. Por exemplo, as curvas determinadas por uma equação como (4) são curvas elípticas (ditas na *forma canônica de Weierstrass*).

Curvas elípticas se notabilizam na teoria das curvas algébricas por possuírem uma estrutura natural de grupo abeliano. A lei de grupo é dada pela construção seguinte. Seja E uma curva elíptica e $P, Q \in E$ dois pontos. A reta $\overline{PQ}$ intersecta E em um terceiro ponto, que denotaremos por $P * Q$. Agora, seja $\mathcal{O} \in E$ o ponto no infinito. Para dois pontos $P, Q \in E$ quaisquer, definimos

$$P + Q = \mathcal{O} * (P * Q). \tag{5}$$

É possível provar geometricamente que o conjunto E munido com a operação $+$ definida acima é um grupo abeliano em que $\mathcal{O}$ é o elemento neutro. As figuras abaixo apresentam visualmente essas construções.

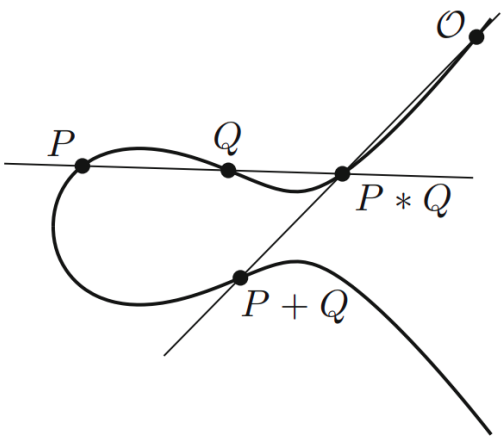

Figura 3. Lei de Grupo

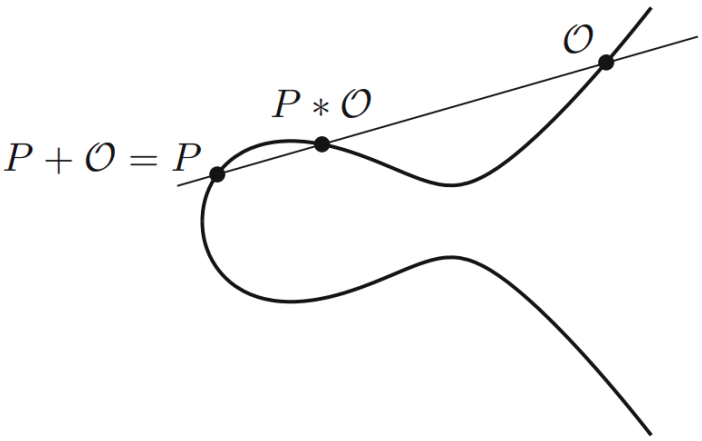

Figura 4. Elemento neutro $\mathcal{O}$

A estrutura de grupo das curvas elípticas tem uma ampla gama de aplicações, destacando-se na teoria dos números. A existência da estrutura de grupo abeliano em uma curva elíptica pode ser interpretada como uma manifestação geométrica das fórmulas de adição para integrais ou funções elípticas.

Considere, por exemplo, a integral $z(r)$ definida na equação (1). Fazendo a mudança de variáveis $t = 1/x^2$ obtemos:

$$z(r) = \int_{\infty}^{\frac{1}{r^2}} \frac{dx}{\sqrt{4x^3 - 4x}}.$$

A integral acima, por sua vez, pode ser vista como a integral da forma diferencial $\omega = dx/y$ em E de um caminho que liga a origem $\mathcal{O}$ ao ponto P correspondente a $1/r^2$:

$$\int_{\mathcal{O}}^{P} \frac{dx}{y}$$

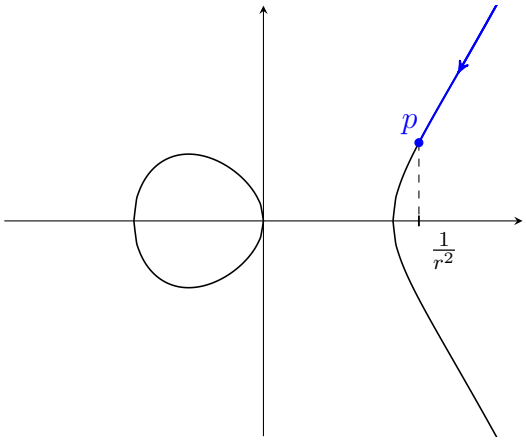

FIGURA 5. Curva após a mudança de variável

Em geral, pode-se mostrar que as integrais elípticas fornecem um isomorfismo de grupos e de superfícies de Riemann

$$E \to \mathbb{C}/\Lambda, \qquad P \mapsto \int_{\mathcal{O}}^{P} \frac{dx}{y}$$

que corresponde ao inverso da parametrização de Weierstrass. A compatibilidade com a lei de grupo é equivalente à fórmula

$$\int_{\mathcal{O}}^{P_1+P_2} \omega = \int_{\mathcal{O}}^{P_1} \omega + \int_{\mathcal{O}}^{P_2} \omega \mod \Lambda$$

que é nada mais que a fórmula de adição para integrais elípticas.

REFERÊNCIAS

[MM97] Henry MacKean and Victor Moll. *Elliptic curves: Function theory, geometry, arithmetic*. Cambridge Univ. Press, 1997.

[Nek04] Jan Nekovar. Elliptic functions and elliptic curves, a classical introduction, 2004.

[ST15] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Springer International Publishing, 2015.