Semigrupos Numéricos e Corpos de Funções Algébricas

THIAGO FILIPE DA SILVA

Professor Assistente do Centro de Ciências Exatas da
Universidade Federal do Espírito Santo.

RESUMO

O estudo sobre o número de pontos racionais de uma curva algébrica não-singular encontra diversas aplicações em Geometria Algébrica, teoria de códigos corretores de erros e criptografia. A uma curva algébrica sobre um corpo associamos o que é chamado corpo de funções, que é uma extensão do corpo onde a curva está definida, e que tem algumas propriedades que serão destacadas neste trabalho. Baseado neste fato, faremos uma introdução à teoria de corpos de funções algébricas destacando os principais conceitos e também uma apresentação da teoria de semigrupos numéricos, que estão ligadas através do Teorema das Lacunas de Weierstrass. Finalmente apresentaremos o conceito de torres de corpos de funções com um exemplo de uma torre assintoticamente boa.

ABSTRACT

The study on the number of rational points of an nonsingular algebraic curve finds many applications in Algebraic Geometry, Algebraic Geometry Codes and Encryption. In an algebraic curve over a field we associate what is called functions fields, which is an extension of the field where the curve is defined, and that has some properties that will be highlighted in this work. Based on this fact will make an introduction to the theory of algebraic functions fields highlighting key concepts and also a presentation of the theory of numerical semigroups, which are linked through the Weierstrass Gap Theorem. Finally we present the concept of towers of functions fields with an example of an asymptotically good tower.

Palavras chaves: Corpos de Funções Algébricas, Semigrupos Numéricos, Torres de Corpos.

1. Introdução

O objetivo deste artigo é motivar os alunos concluintes da graduação, ou mesmo ingressantes no mestrado em Matemática, a prosseguirem na carreira acadêmica. Outro objetivo também é mostrar que alguns conceitos, a princípio bem abstratos que são desenvolvidos em um curso de Álgebra, tem grande importância no desenvolvimento de novas teorias.

A Teoria de Corpos de Funções é muita usada na Geometria Algébrica e veremos também como ela esta intimamente ligada a Teoria de Números, mais especificamente a Teoria de Semigrupos Numéricos.

Neste texto evitamos demonstrações, já que o objetivo é divulgar esta área de estudo, e para que a leitura não seja enfadonha.

O leitor dever estar familiarizado com alguns conceitos e resultados básicos de um primeiro curso de Álgebra.

Detalhes das demonstrações dos resultados exibidos: da seção de semigrupos numéricos podem ser encontrados em [1] e [4], da seção de corpos de funções em [2] e da seção de Torre de Corpos de Funções em [2], [3] e [4].

2. Semigrupos Numéricos

Vamos fazer uma revisão de alguns conceitos básicos sobre a teoria de semigrupos numéricos, dada a grande aplicação que existe na teoria de corpos de funções.

Seja $\mathbb{N}_0$ o conjunto dos números inteiros não-negativos e seja $\mathbb{N} \coloneqq \mathbb{N}_0 - \{0\}$.

Um subconjunto Λ de $\mathbb{N}_0$ é chamado um semigrupo quando $0 \in \Lambda$ e para todos $a, b \in \Lambda$ tem-se $a + b \in \Lambda$. O semigrupo Λ é chamado numérico quando $\mathbb{N}_0 - \Lambda$ for finito. Neste caso o número $g = |\mathbb{N}_0 - \Lambda|$ chama-se o gênero de Λ e $\mathbb{N}_0 - \Lambda$ é chamado o conjunto das lacunas de Λ.

No caso em que Λ é um semigrupo numérico, existe um elemento mínimo $c \in \Lambda$ com a propriedade que para todo $x \in \mathbb{N}_0$ com $x \geq c$ tem-se $x \in \Lambda$. Tal elemento c é chamado de *condutor* de Λ.

Dado H subconjunto não-vazio de $\mathbb{N}_0$ define-se o conjunto $\langle H \rangle = \{a_1x_1 + \cdots + a_mx_m / \ x_1, \ldots, x_m \in H, a_1, \ldots, a_m \in \mathbb{N}_0 \ e \ m \in \mathbb{N}\}$ que claramente é

um semigrupo de $\mathbb{N}$ *e é chamado o semigrupo gerado por* H*. Quando* H *é finito e é escrito por* $H = \{\lambda_1, \dots, \lambda_m\}$ *então usamos a notação* $\langle \lambda_1, \dots, \lambda_m \rangle$ *para simbolizar* $\langle H \rangle$*.*

É conhecido que um semigrupo finitamente gerado é numérico se, e somente se, o máximo divisor comum de seus geradores é igual a 1.

2.1 Definição *Seja* $(a_1, \dots, a_m)$ *uma sequência de números inteiros positivos. Para cada* $i \in \{1, \dots, k\}$ *seja* $d_i = mdc(a_1, \dots, a_i)$*. A sequência* $(a_1, \dots, a_k)$ *é chamada telescópica quando* $d_k = 1$ *e* $\frac{a_i}{d_i} \in \langle \frac{a_1}{d_{i-1}}, \dots, \frac{a_{i-1}}{d_{i-1}} \rangle$*, para todo* $i \in \{2, \dots, k\}$*. Um semigrupo* Λ *de* $\mathbb{N}_0$ *é chamado telescópico quando é gerado por uma sequência telescópica.*

2.2 Exemplos

(1) Seja $\Lambda = \langle 4, 6, 5 \rangle$. Chame $a_1 = 4$, $a_2 = 6$ e $a_3 = 5$. Sendo $d_i = mdc(a_1, \dots, a_i)$, para todo $i \in \{1,2,3\}$, segue que $d_1 = 4$, $d_2 = 2$ e $d_3 = 1$. Observe que $\frac{a_3}{d_3} = 5$, $\frac{a_1}{d_2} = 2$, $\frac{a_2}{d_2} = 3$ e $5 = 1 \cdot 2 + 1 \cdot 3$. Portanto Λ é um semigrupo telescópico.

(2) Seja $\Gamma = \langle 34, 4, 62, 97 \rangle$. Chame $a_1 = 34$, $a_2 = 4$, $a_3 = 62$ e $a_4 = 97$ e $d_i = mdc(a_1, \dots, a_i)$, para todo $i \in \{1, 2, 3, 4\}$. Logo, $d_1 = 34$, $d_2 = 2$, $d_3 = 2$ e $d_4 = 1$. Observe que $\frac{a_4}{d_4} = 97$, $\frac{a_1}{d_3} = 17$, $\frac{a_2}{d_3} = 2$, $\frac{a_3}{d_3} = 31$ e $97 = 1 \cdot 17 + 9 \cdot 2 + 2 \cdot 31$. Temos também que $\frac{a_3}{d_3} = 31$, $\frac{a_1}{d_2} = 17$, $\frac{a_2}{d_2} = 2$ e $31 = 1 \cdot 17 + 7 \cdot 2$. Portanto Γ é um semigrupo telescópico.

2.3 Definição *Seja* Λ *um semigrupo numérico de* $\mathbb{N}_0$ *de gênero* g *e condutor* c*. Dizemos que* Λ *é um semigrupo simétrico quando* $c = 2g$*.*

Sendo Λ um semigrupo numérico com maior lacuna l, é conhecido que Λ é simétrico se, e somente se, para toda lacuna s de Λ tem-se que $l - s$ é uma não lacuna. Daí a nomenclatura "simétrico".

O próximo teorema fornece uma fórmula que expressa o gênero de um semigrupo telescópico em termos de seus geradores, além de provar que todo semigrupo telescópico é simétrico. Esta fórmula será usada na demonstração de um teorema envolvendo torres de corpos de funções.

2.4 Teorema *Sejam* $k \in \mathbb{N}$, $k \geq 2$, $(a_1, \ldots, a_k)$ *uma sequência telescópica,* $\Lambda = \langle a_1, \ldots, a_k \rangle$, $d_i = mdc(a_1, \ldots, a_i)$ *para cada* $i \in \{1, \ldots, k\}$ *e* $g = |\mathbb{N}_0 - \Lambda|$.

a) Se $\Gamma = \langle \frac{a_1}{d_{k-1}}, \ldots, \frac{a_{k-1}}{d_{k-1}} \rangle$ *e* $g' = |\mathbb{N}_0 - \Gamma|$ *então* $g = d_{k-1}g' + \frac{(d_{k-1}-1)(a_k-1)}{2}$;

b) O semigrupo Λ *é simétrico. Em particular*

$$g = \frac{1}{2}\left(1 + \sum_{i=1}^{k}\left(\frac{d_{i-1}}{d_i} - 1\right)a_i\right) \text{ onde } d_0 = 0.$$

Desse modo, os semigrupos telescópicos $\langle 4, 6, 5 \rangle$ e $\langle 34, 4, 62, 97 \rangle$ considerados nos exemplos anteriores têm gênero 4 e 64, respectivamente.

3. **Introdução à Teoria de Corpos de Funções**

A seguir passamos a introduzir a linguagem básica para a teoria dos corpos de funções algébricas: lugares, divisores, gênero e semigrupos de Weierstrass.

Em todo este texto K é um corpo arbitrário.

3.1 Definição *Seja* F/K *uma extensão de corpos. Dizemos que* F/K *é um corpo de funções algébricas ou simplesmente corpo de funções quando existir* $x \in F$ *transcendente sobre* K *tal que a extensão* $F/K(x)$ *é finita.*

Um exemplo simples de um corpo de funções é o *corpo de funções racional* $K(x)/K$, onde $K(x)$ é o corpo de frações do anel de polinômios $K[x]$.

3.2 Definição *Um anel de valorização de um corpo de funções* F/K *é um subanel* $\mathcal{O} \subset F$ *com as seguintes propriedades:*

a) $K \subsetneq \mathcal{O} \subsetneq F$;

b) Para todo $z \in F - \{0\}$ *tem-se* $z \in \mathcal{O}$ *ou* $z^{-1} \in \mathcal{O}$.

3.3 Exemplo Dado um polinômio mônico e irredutível $p(x) \in K[x]$, o conjunto $\mathcal{O}_{p(x)} = \left\{\frac{f(x)}{g(x)} / f(x), g(x) \in K[x] \text{ e } p(x) \nmid g(x)\right\}$ é um anel de valorização de $K(x)/K$. E ainda, se $q(x) \in K[x]$ é outro polinômio mônico e irredutível, então $\mathcal{O}_{q(x)} \neq \mathcal{O}_{p(x)}$.

Qualquer anel de valorização $\mathcal{O}$ de um corpo de funções F/K é um anel local, ou seja, possui um único ideal maximal P, que será chamado um *lugar* do corpo

de funções. Além disso P é um ideal principal, ou seja, existe $t \in \mathcal{O}$ tal que $P = t\mathcal{O}$ (tal elemento t é chamado uniformizante local de P). Desse modo, para cada elemento z em F não-nulo, existe um único inteiro n e um invertível u em $\mathcal{O}$ tal que $z = t^n u$. Tal inteiro não depende da escolha do uniformizante local, e assim é definido como sendo a *valorização* de z por P, e é denotada por $v_P(z)$. Definimos $v_P(0) = \infty$.

O conjunto dos lugares de um corpo de funções F/K é denotado por $\mathbb{P}_F$.

Sendo P o ideal maximal de um anel de valorização $\mathcal{O}$, segue que o anel quociente $\frac{\mathcal{O}}{P}$ é um corpo que contém um subcorpo que é isomorfo a K, logo $\frac{\mathcal{O}}{P}$ é um espaço vetorial sobre K. É conhecido que este espaço vetorial possui dimensão finita, que será denotada por $degP$ e também será chamada *grau de* P. Dizemos que um lugar P é racional quando $degP = 1$.

Um *divisor* em um corpo de funções é uma soma formal $\sum_{P \in \mathbb{P}_F} n_P P$ onde $n_P \in \mathbb{Z}$ para todo lugar P e $n_P \neq 0$ apenas para uma quantidade finita de lugares.

3.4 Definição *Um lugar P é um zero de um elemento $z \in F$ se $v_P(z) > 0$, e P é um polo de z se $v_P(z) < 0$. Se $v_P(z) = m > 0$ então dizemos que P é um zero de z com ordem m. Se $v_P(z) = m < 0$ então dizemos que P é um polo de z com ordem m.*

É conhecido que qualquer elemento não-nulo z em um corpo de funções tem apenas uma quantidade finita de zeros e polos. Assim, sendo $x \in F - \{0\}$, Z o conjunto dos zeros de x e N o conjunto dos polos de x definimos os seguintes divisores:

$(x)_0 \coloneqq \sum_{P \in Z} v_P(x)P$ como sendo o divisor dos zeros de x;

$(x)_\infty \coloneqq \sum_{P \in N} v_P(x)P$ como sendo o divisor dos polos de x e $(x) \coloneqq (x)_0 - (x)_\infty$ como sendo o divisor principal de x.

O semigrupo de Weierstrass de um lugar P é o conjunto $N(P) \coloneqq \{n \in \mathbb{N}_0 / (x)_0 = nP \ para \ algum \ x \in F - \{0\}\}$. É possível mostrar que este conjunto é um semigrupo numérico, ou seja, é fechado para a soma e tem um número finito de lacunas. Não pretendemos dar a definição de *gênero* de um corpo de funções neste texto, mas o Teorema das Lacunas de Weierstrass afirma que o gênero de um corpo de funções é exatamente o gênero do semigrupo de Weierstrass de um lugar racional.

4. Torre de Corpos de Funções

Adiante, passamos a estudar um novo conceito que é muito utilizado na Teoria de Códigos Corretores de Erros que são as torres de corpos de funções. Para a construção de códigos com bons parâmetros, é desejável trabalhar em corpos de funções com um grande número de lugares racionais. Daí se justifica o estudo do comportamento assintótico de torres, a fim de saber se em uma sequência de corpos de funções é possível encontrar um que tenha o número adequado de lugares racionais.

Uma sequência $(F^{(1)}/K, F^{(2)}/K, \dots)$ de corpos de funções é chamada *torre* se $F^{(i)} \subset F^{(i+1)}$, para todo $i \in \mathbb{N}$. Denotamos o corpo finito com q elementos por $\mathbb{F}_q$. É conhecido que um corpo de funções $F/\mathbb{F}_q$ sobre um corpo finito tem uma quantidade finita de lugares racionais. Tal quantidade será denotada por $N(F)$.

Dada uma torre $(F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \dots)$ escrevemos $N^{(i)} = N(F^{(i)})$ e $g^{(i)} = g(F^{(i)})$ (gênero de $F^{(i)}/K$). Dizemos que uma torre de corpos de funções é *assintoticamente boa* quando $\lim_{i\to\infty} g^{(i)} = \infty$ e $\lim_{i\to\infty} inf\, \frac{N^{(i)}}{g^{(i)}} = k > 0$. Esta segunda condição satisfeita nos diz que o número de lugares racionais é grande em relação ao gênero, que já explode para o infinito à medida que se aumenta o nível da torre.

O próximo resultado faz uma associação entre o conceito de semigrupos telescópicos e a busca por torres assintoticamente boas.

4.1 Teorema *Seja* $(F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \dots)$ *uma torre de corpos de funções tal que para uma infinidade de índices* i *tem-se que* $F^{(i)}$ *possui um lugar racional* $P^{(i)}$ *com semigrupo de Weierstrass telescópico igual a* $\Lambda^{(i)}$. *Então a torre* $(F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \dots)$ *não é assintoticamente boa.*

4.2 Exemplo Sejam $q = l^2$, onde l é uma potência de um primo ímpar, (x_n) uma sequência tal que $x_{n+1}^2 = \frac{1+x_n^2}{2x_n}$ e $F^{(n)} = \mathbb{F}_q(x_0, \dots, x_n)$, para todo $n \in \mathbb{N}_0$, com x_0 transcendente sobre $\mathbb{F}_q$.

Então a torre $\mathcal{F} = (F^{(0)}/\mathbb{F}_q, F^{(1)}/\mathbb{F}_q, \dots)$ é assintoticamente boa.

Referências Bibliográficas

[1] Hoholdt, T., van Lint, J. e Pellikaan, R., *Algebraic Geometry Codes*, V.S. Pless, W. C. huffman (Eds.), Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, 1998, pp.871-961. (Chapter 10).

[2] Stichtenoth, H., *Algebraic Function Fields and Codes*, (Universitext)(Springer 2009).

[3] Geil, O. e Matsumoto, R., *Bounding the Number of rational places using Weierstrass Semigroups*, Journal of Pure and Applied Algebra, 213, (6), 2009, pp.1152-1156.

[4] da Silva, T. F, *Cotas Superiores para o Número de Pontos Racionais e Aplicações às Torres de Corpos de Funções*, Dissertação de Mestrado, 2010 - UFES

Universidade Federal do Espírito Santo, Vitória - ES, Brasil
E-mail address: thiago.filipe@hotmail.com
URL: www.ufes.br