XVIII SEMAT E VIII SEMEST
Universidade Federal de Uberlândia
02 a 05 de outubro de 2018

Semigrupo de Weierstrass

Iván Darío Santamaría Guarín[*1] **e Guilherme Chaud Tizziotti**[†1]

[1]FAMAT - Universidade Federal de Uberlândia

Palavras-chave: *semigrupo de Weierstrass. curvas algébricas. corpo de funções.*

Resumo

Apresentaremos conceitos e resultados básicos da Geometria Algébrica com o intuito de definir o semigrupo de Weierstrass em um ponto racional de uma curva projetiva irredutível definida sobre um corpo finito.

Introdução

Sejam K un corpo e $F(X,Y)$ um polinômio de duas variáveis sobre K. Um ponto $(a,b) \in K^2$ é uma raiz do polinômio $F(X,Y)$ se $F(a,b) = 0$ e todas as raízes de $F(X,Y)$ definem uma *curva afim* sobre K. De fato, consideramos todos os pontos sobre o fecho algébrico de K. No caso em que K é um corpo finito com q elementos $\mathbb{F}_q$, significa que um ponto da *curva afim* é (a,b) com $a,b \in \mathbb{F}_{q^m}$ para algum inteiro positivo m e $F(a,b) = 0$. Pontos da curva com $(a,b) \in K$ são chamados racionais sobre K (ou K-Racionais).

Dado um polinômio homogêneo $F(X,Y,Z)$ sobre K, uma *curva projetiva* definida por $F(X,Y,Z)$ são os pontos $P = (a:b:c)$ no plano projetivo sobre o fecho algébrico de K tal que $F(X,Y,Z) = 0$. Para toda curva projetiva se pode corresponder três curvas afim através de um processo de deshomogenização:

$$F(1,Y,Z) = 0,\ F(X,1,Z) = 0,\ F(X,Y,1) = 0$$

Inversamente, uma curva afim pode ser correspondida com um curva projetiva por meio da homogenização: $Z^d F(X/Z, Y/Z)$ onde d é o grau de F.

Um curva afim (resp. projetiva) é chamada irredutível se $F(X,Y)$ (resp. $F(X,Y,Z)$) não pode ser escrito como o produto de dois polinômios de grau maior que zero. Associando para cada $F(X,Y,Z)$ o polinômio $F(X,Y,1)$, obtemos uma correspondência injetora entre as curvas projetivas irredutíveis e as curvas afim irredutíveis.

Um ponto $P = (a:b:c)$ sobre uma curva projetiva χ definida por $F(X,Y,Z)$ é chamado singular se todas as derivadas F_x, F_y, F_z são zero em P, de outra forma, P é chamado simples. Se todos os pontos são simples, então dizemos que χ é não-singular (ou suave).

Geralmente, para um polinômio F, estabelecer se a curva associada a F é irredutível não é fácil, mas existem vários critérios de irredutibilidade que não vamos mencionar aqui. Deixamos a observação que as curvas suaves são irredutível.

A partir de agora, a palavra *curva* significará curva projetiva não-singular sobre K.

Seja χ uma curva definida por $F(X,Y,Z)$. Uma *função racional* de χ é a razão $f = A(X,Y,Z)/B(X,Y,Z)$ de dois polinômios homogêneos de mesmo grau modulo $F(X,Y,Z)$. Seja I o ideal gerado por F em $K[X,Y,Z]$. Como χ és irredutível, temos que I é um ideal primo, logo $K[X,Y,Z]/I$ é um domínio de integridade. Um elemento g em $K[X,Y,Z]/I$ é de grau d se $g = G + I$, para algum polinômio homogêneo $G \in K[X,Y,Z]$ com $deg(G) = d$. O conjunto de funções racionais de χ é:

$$K(\chi) := \{f = g/h \mid g,h \in K[X,Y,Z]/I \text{ são formas do mesmo grau e } h \neq 0\}$$

O qual é um subcorpo do corpo de funções $K[X,Y,Z]/I$. Dizemos que uma *função racional* f esta *definida* no ponto P, se existe uma representação de $f = A/B$ tal que $B(p) \neq 0$.Neste caso nos podemos estimar a função em P, isto é $f(P) = A(P)/B(P)$. Note que esta avaliação não depende do representante de f.

Dado um ponto P, seja O_p o anelo de todas as funções racionais definido em P. É fácil vê que O_p é um domínio de integridade e $K(\chi)$ é seu corpo de frações. Mais ainda, se pode mostrar que $M_p := \{f \in O_p \mid f(P) = 0\}$ é um ideal principal. Qualquer gerador de M_p é chamado de *parâmetro local* em P.

[*]ivansantamariag@ufu.br
[†]guilhermect@ufu.br

Proposição 1. *Seja $P = (a : b : c)$ um ponto sobre a curva χ definida por $F(X,Y,Z)$. Suponha $c \neq 0$. Seja $f = L_1(X,Y,Z)/L_2(X,Y,Z)$ uma função racional em M_p, tal que $deg(L_1) = deg(L_2) = 1$, $L_2(P) \neq 0$ e L_1 não é um múltiplo de $F_X(P)X + F_Y(p)Y + F_z(P)Z$. Então f é uma parâmetro local em P.*

Dado um ponto P de χ, seja t um parâmetro local em P. então para qualquer $f \in K(\chi)$, $f \neq 0$ existe um inteiro m tal que $f = t^m u$, onde $u \in O_p \setminus M_p$. O inteiro m é chamado *valorização de* f em P e é denotado por $v_p(f)$. Note que os elementos em O_p são caracterizados por $v_p(f) \geq 0$ e M_p consiste das funções com $v_p(f) > 0$.

A valorizações tem as seguentes propriedades:

Proposição 2. *(1) $v_p(fg) = v_p(f) + v_p(g)$ para tudo $P \in \chi$ e para tudo $f, g \in K(\chi)$;*

(2) $v_p(f+g) \geq min\{v_p(f), v_p(g)\}$ para tudo $P \in \chi$ e para tudo $f, g \in K(\chi)$, se $v_p(f) \neq v_p(g)$ então $v_p(f+g) = min\{v_p(f), v_p(g)\}$;

(3) $v_p(a) = 0$ para qualquer $P \in \chi$ e qualquer $a \in K$.

Um ponto P é chamado de zero de multiplicidade m se $v_p(f) = m > 0$. P é chamado de polo de multiplicidade $-m$ se $v_p(f) = m < 0$.

Teorema 3. *Seja $f \neq 0$ em $K(\chi)$. Então f tem as mesma candidate de zeros e polos (contando multiplicidades).*

Semigrupo de Weierstrass

O grupo livre abeliano gerado pelos pontos de χ é chamado de grupo de divisores de χ. Os elementos de esse grupo são chamados *divisores* de χ. Em outras palavras, um divisor $D = \sum_{p \in \chi} n_P P$, quando n_p é um inteiro igual a zero exceto para um número finito de pontos de χ.

O *suporte* de D é definido como Supp$(D) := \{P \in \chi \mid n_p \neq 0\}$. A soma de dois divisores $D = \sum_{p \in \chi} n_P P$ e $D' = \sum_{p \in \chi} n'_P P$ se define de forma natural:

$$(D + D') := \sum_{p \in \chi} (n_P + n'_P) P$$

.

O Elemento zero do grupo divisor é $\sum_{p \in \chi} n_P P$ com $n_p = 0$ para todo ponto $P \in \chi$ e é denotado por 0.

Definimos um ordem parcial sobre o grupo de divisores por:

$$D \leq D' \Leftrightarrow n_p \leq n'_p \text{ para todo } P \in \chi$$

.

Se $n_p \geq 0$ para todo $P \in \chi$, dizemos que D é *positivo* ou *efetivo*. O *grau* de D é deg$(D) = \sum_{P \in \chi} n_P$.

Dada uma função racional f, definimos o divisor de f por $(f) := \sum v_p(f) P$. tal divisor é o divisor zero se e somente se $f \in K$. Para $f \notin K$, (f) pode-se escrever como a diferencia de dois divisores efetivos $(f) = (f)_0 - (f)_\infty$, onde $(f)_0 = \sum_{v_p > 0} v_p P$ é o divisor zero de f e $(f)_\infty = \sum_{v_p < 0} -v_p P$ é o divisor polo de f.

Dois divisores D e D' são equivalentes se existe uma função racional f tal que $D - D' = (f)$. O conjunto que definiremos a seguir, é algo fundamental na construção dos chamados códigos algébricos geométricos. Dado um divisor D, definimos o *espaço vetorial associado* a D por:

$$L(D) := \{f \in K(\chi) \mid (f) \geq -D\} \bigcup \{0\}$$

.

O espaco $L(D)$ também é conhecido como espaco de Riemann-Roch associado a D. Denotaremos a dimensão dim(L(D)) desse espaco por $\ell(D)$.

Note que quando o divisor D é efetivo, $l(D)$ consiste das funções tais que todos os polos estão contidos no Supp(D) e a multiplicidade de cada um de elos não é maior a v_p.

Lema 4. *Seja D e D' divisores.*

(1) Se D' é equivalente a D, então $L(D)$ é isomorfo a $L(D')$ (como $k-$espaço vetorial).

(2) se $deg(D) < 0$ então $L(D) = 0$.

(3) $L(0) = K$.

Demonstração.

(1) Como D e D' são equivalentes, existe $z \in K(\chi)$ tal que $D = D' + (z)$. Defina a função $\varphi : L(D) \longrightarrow K(\chi)$, $x \longmapsto xz$. Claramente φ é $K-$linear e sua imagem esta contida em $L(D')$ pois $v_p(xz) = v_p(x) + v_p(z) \geq -n_p + v_p(z) = n'_p$ para todo $p \in \chi$. Da mesma forma nos definimos $\psi : L(D') \longrightarrow L(D)$, $x \longmapsto xz^{-1}$ e $\varphi \circ \psi = id_{L(D')}$ e $\psi \circ \varphi = id_{L(D)}$.

(2) Suponha que existe $x \in L(D)$ com $x \neq 0$. Então $D' = D + (x)$ é um divisor efetivo e equivalente a D, logo $0 \leq deg(D') = deg(D)$, mas isso é uma contradição.

(3) Claramente $K \subseteq L(0)$. por outra parte, cada elemento de $L(0)$ não tem polos, por tanto são constantes.

■

Seja χ uma curva definida por $F(X, Y, Z)$ e seja d o grau de χ. Introduzimos o valor $g = (d-1)(d-2)/2$, o qual é chamado de *genus* de χ. Também definimos o divisor canônico como qualquer divisor W tal que $deg(W) = 2g - 2$ e $\ell(W) = g$.

Teorema 5 (Teorema de Riemann-Roch)**.** *Dado um divisor D,*

$$l(D) = deg(D) + 1 - g + \ell(W - D)$$

onde W é qualquer divisor canônico.

Corolário 6. *Para qualquer divisor D tal que $deg(D) \geq 2g - 1$,*

$$\ell(D) = deg(D) + 1 + g$$

Demonstração. Pelo teorema de Riemann-Roch temos que $\ell(D) = deg(D) + 1 + g + \ell(W - D)$, onde W é um divisor canonic. Como $deg(D) \geq 2g - 1$ e $deg(W) = 2g - 2$, temos que $deg(W - D) < 0$, logo por o lema anterior $\ell(W - D) = 0$, logo se satisfaz a igualdade. ■

Considere o divisor $D = mP$, onde P é um ponto $K-$racional de χ e $m > 0$. Os elementos de $L(D)$ sao as funções tais que $(f)_\infty = lP$ com $l \leq m$. Considere o conjunto

$$H(P) := \{l \in \mathbb{N} \mid \text{ Existe } f \in K(\chi) \text{ com } (f)_\infty = lP\}$$

.

Os Elementos de $H(P)$ são chamados de *não-lacunas* e os elementos em $\mathbb{N} \setminus H(P)$ são chamados de *lacunas*. Utilizando a Proposicão 2 mostra-se que $H(P)$ é um semigrupo, ou seja,
i) $0 \in H(P)$;
ii) se $\ell_1, \ell_2 \in H(P)$, então $\ell_1 + \ell_2 \in H(P)$;
iii) $\mathbb{N}_0 \setminus H(P)$ é finito.
Por ser um semigrupo, $H(P)$ é chamado de semigrupo de Weierstrass de χ em P.

Proposição 7. *A dimensão de $L(mP)$ é igual ao número de não-lacunas em P que são menores ou iguais a m.*

Demonstração. Note que s é um gap se e somente se $L((s-1)P) = L(sP)$. considere la seguinte cadeia $L(0) \subseteq L(P) \subseteq L(2P) \subseteq \cdots \subseteq L(mP)$. Para qualquer i, $0 \leq i \leq m$, temos $l(iP) - l((i-1)P) \leq 1$: qualquer dois $f_1, f_2 \in L(iP) \setminus L((i-1)P)$ são linearmente dependentes sobre K por tanto f_1/f_2 não tem polos, logo f_1/f_2 é um elemento de K. logo por o lema anterior temos que $Dim(L(0) = 1)$ e por tanto se satisfaz a proposição. ■

Pelo Teorema de Riemann-Roch, $L((s-1)P) = L(sP)$ se, e somente se, $\ell(W - (s-1)P) = \ell(W - sP) + 1$, em que W é um divisor canônico. Pelo item (2) do Lema 4 isso não é possível quando $s \geq 2g$. Assim, temos que:

(•) para qualquer $P \in \chi$, se s é um inteiro tal que $s \geq 2g$, então s é uma nã-lacuna.

Mais ainda, temos o seguinte resultado.

Proposição 8. *Existem exatamente g lacunas para cada $P \in \chi$.*

Demonstração. Pelo Corolário 6, temos que $\ell(2gP) = g + 1$. Pela Proposicão 7, o número de não-lacunas em P as quais são menores do que ou iguais a $2g$ é $g + 1$. Assim, por (•) acima, temos o número de lacunas em P é igual a g. ■

Corolário 9. *Se $g \geq 1$, existe ao menos um gap para qualquer $P \in \chi$. Como $H(P)$ é um semigrupo, 1 é um gap para qualquer ponto $P \in \chi$.*

Nas últimas décadas o interesse na teoria de semigrupos de Weierstrass aumentou muito devido às muitas aplicacões, especialmente na teoria de códigos. Como exemplo dessas aplicacões, se $C(D, G)$ é um código algébrico geométrico com $G = mP$, a estrutura da sequência de lacunas em P permite dar uma melhor cota inferior para a distância mínima para $C(D, G)$, algo muito importante no estudo de códigos.

Referências

[1] Giulietti, M. (2003). Notes on algebraic-geometric codes. Department of Mathematics, Royal Institute of Technology.

[2] Stichtenoth, H. (2009). Algebraic function fields and codes (Vol. 254). Springer Science & Business Media.