IVÁN DARÍO SANTAMARÍA GUARÍN

Semigrupos de Weierstrass em Vários Pontos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2019

IVÁN DARÍO SANTAMARÍA GUARÍN

Semigrupos de Weierstrass em Vários Pontos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria algébrica.

Orientador: Prof. Dr. Guilherme Chaud Tizziotti.

UBERLÂNDIA - MG
2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

S232s 2019

Santamaría Guarín, Iván Darío, 1989-
Semigrupos de Weierstrass em vários pontos [recurso eletrônico] / Iván Darío Santamaría Guarín. - 2019.

Orientador: Guilherme Chaud Tizziotti.
Dissertação (mestrado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://dx.doi.org/10.14393/ufu.di.2019.1008
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. 2. Curvas algébricas. 3. Weierstrass, Pontos de. 4. Semigrupos. 5. Curva Hermitiana. I. Tizziotti, Guilherme Chaud, 1980-, (Orient.). II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU:51

Glória Aparecida – CRB-6/2047

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Iván Darío Santamaría Guarín.

NÚMERO DE MATRÍCULA: 11722MAT001.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Semigrupos de Weierstrass em Vários Pontos.

ORIENTADOR: Prof. Dr. Guilherme Chaud Tizziotti.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 15 de julho de 2019, às 9h30min, pela seguinte Banca Examinadora:

NOME	**ASSINATURA**
Prof. Dr. Guilherme Chaud Tizziotti UFU - Universidade Federal de Uberlândia	
Prof. Dr. Wanderson Tenório UFMT - Universidade Federal de Mato Grosso	
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 15 de julho de 2019.

Dedicatória

Dedico este trabalho aos meus pais Donaldo e Celina, aos meus irmãos Oscar, Nelson e William e ao meu sobrinho Juan Daniel.

Agradecimentos

Primeiro, quero agradecer à minha família pelo apoio incondicional, especialmente aos meus queridos pais, por sua incansável companhia. Quero agradecer à meu orientador Guilherme, por compartilhar comigo todo seu conhecimento e experiência, por sua paciência e disponibilidade para resolver minhas dúvidas ao longo deste processo.

Agradeço ao professor Mário Henrique por seu apoio incondicional à minha chegada ao Brasil. A meus amigos e colegas pelos bons momentos dentro e fora das aulas. Um agradecimento especial a meu amigo Gabriel Dias, por seus aportes e comentários que ajudaram acrescentar esta dissertação. Ao corpo docente do mestrado da faculdade de matemática por sua contribuição na minha formação profissional.

Finalmente, agradeço ao programa de Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES por seu apoio econômico.

SANTAMARÍA GUARÍN, I. D. *Semigrupo de Weierstrass em Vários pontos.* 2019. 43 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho apresentamos um estudo sobre alguns dos resultados mais conhecidos da Teoria de semigrupos de Weierstrass em vários pontos de uma curva algébrica, projetiva não-singular definida sobre um corpo finito. Apresentamos também duas técnicas distintas para se calcular esses semigrupos. A primeira delas, foi estabelecida sobre a curva Hermitiana por meio do cálculo direito de elementos mínimos; a segunda, introduz o conceito de discrepância e foi aplicada numa família de curvas com modelo plano da forma $f(y) = g(x)$.

Palavras-chave: Curvas algébricas, Semigrupo de Weierstrass, curva Hermitiana, discrepância.

SANTAMARÍA GUARÍN, I. D. *Weierstrass semigroup at several points.* 2019. 43 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work we present some results with respect to the Weierstrass semigroups in several points on a non-singular, projective algebraic curve defined over a finite field. We also present two techniques to calculate these semigroups. The first one, was established on the Hermitian curve by means of a direct calculation of minimal elements; the second one, introduces the concept of discrepancy and was applied to a family of curves with plane model of the form $f(y) = g(x)$.

Keywords: Algebraic curves, Weierstrass semigroups, Hermitian curve, discrepancy.

Sumário

Introdução

Um *semigrupo de Weierstrass em um ponto* é uma estrutura algébrica numérica, um semigrupo numérico, que está associada ao estudo clássico das curvas algébricas. Devido à sua proximidade com o espaço Riemann-Roch, os semigrupos de Weierstrass foram inicialmente propostos como uma forma de detectar a "ordem"que um ponto na curva pode ter como *polo*. O conceito de semigrupo de Weierstrass em vários pontos foi inicialmente introduzido por Arbarello, Cornalda, Griffiths e Harris em [3, Pag. 365]. Ali, os autores apresentam uma cota inferior para a cardinalidade do conjunto das lacunas sobre dois pontos de uma curva, o que gerou uma ruptura entre a estrutura do semigrupo de Weierstrass para um ponto e a estrutura do semigrupo de Weierstrass em vários pontos. Em [17], Kim faz um estudo inicial do semigrupo de Weierstrass para dois pontos sobre uma curva com o objetivo de calcular a cardinalidade do conjunto de lacunas para esse caso. Entre os muitos resultados, destacamos dois: a caracterização dos elementos do semigrupo com a *dimensão do espaço Riemann-Roch* associado a divisores com suporte nesses pontos e a correspondência bijetora entre as lacunas associadas a cada ponto, definida por *elementos minimais* no semigrupo. Posteriormente, estes resultados foram complementados por Homma e Kim [14], [15] e Matthews [20].

A motivação para estudar semigrupos Weierstrass em vários pontos remonta-se ao final do século XX com os trabalhos de Goppa [12] na teoria de códigos. Ele estabeleceu técnicas da geometria algébrica para construir códigos sobre curvas algébricas, hoje conhecidos como códigos geométricos Goppa. Garcia, Kim e Lax em [9] e [8] mostraram que os parâmetros de um código Goppa podem ser melhorados (especificamente a distância mínima) de acordo com a distribuição das lacunas num ponto dado da curva. Em [4], Carvalho e Torres estendem as ideias de Kim em [17] para vários pontos sob certa hipótese sobre a cardinalidade do corpo e os pontos a serem considerados sobre o semigrupo. Nesse artigo, eles apresentam uma série de importantes resultados sobre essa estrutura.

Com base nesses fatos, foram estabelecidas técnicas para determinar semigrupos de Weierstrass para um e dois pontos sobre uma curva dada, como são os casos da *curva de Hermitian* [20] e da curva de norma-traço [23]. Naturalmente, esses resultados foram aplicados na teoria de códigos.

Este trabalho pretende sintetizar alguns dos resultados atualmente conhecidos dos semigrupo de Weierstrass sobre vários pontos. Especificamente o trabalho de Carvalho e Torres em [4], os resultados de Matthews em [21] e Castellanos e Tizziotti em [5].

Em [21], Matthews estabelece o semigrupo de Weierstrass em m pontos colineares para uma curva hermitiana, este resultado foi obtido a partir da noção de *conjunto gerador mínimo* para o semigrupo de Weierstrass, introduzido por ela. Em [5], Castellanos e Tizziotti, usam o conceito de *discrepância* para caracterizar os elementos mínimos de um semigrupo de Weierstrass para uma família de curvas com variáveis separáveis com o modelo afim $f(y) = g(x)$.

Antes de apresentar todos esses resultados, introduziremos no Capítulo 1, uma série de conceitos básicos da geometria algébrica clássica de curvas que vão nos ajudar a compreender este texto. Embora os semigrupos de Weierstrass tenham surgido da geometria, eles também podem ser abordados a partir da teoria dos corpos de funções algébricas. Ambas as linguagens são equivalentes, porém pode ser mais interessante trabalhar com esse conceito a partir do

corpo de funções algébricas. Dedicamos a seção 1.4 para introduzir alguns conceitos básicos da teoria dos corpos de funções algébricas.

A base deste trabalho encontra-se no conteúdo do capítulo 2 onde apresentamos todo o conteúdo teórico sobre a estrutura do semigrupo Weierstrass, em um e vários pontos. Na seção 2.2 apresentamos todos os resultados desenvolvidos em [4] e a seção 2.3 é dedicada a construir o conjunto gerador para o semigrupo Weierstrass em vários pontos. Esta construção foi exposta em [21].

O capítulo 3 é dedicado ao cálculo do semigrupo de Weierstrass em dois e vários pontos na curva Hermitiana [21] e [20]. Finalmente, no capítulo 4 vamos expor o trabalho de Castellanos e Tizziotti em [5]. Na seção 4.1, introduzimos o conceito de discrepância e sua relação com os elementos mínimos do semigrupo Weierstrass. Por fim, na seção 4.2, expomos sua implementação para o cálculo explícito do conjunto gerador do semigrupo Weierstrass para uma família de curvas com variáveis separáveis.

Iván Darío Santamaría Guarín
Uberlândia-MG, 15 de julho de 2019.

Capítulo 1

Preliminares

O presente capítulo tem como intuito introduzir alguns dos conceitos básicos da geometria clássica de curvas algébricas, com o objetivo de apresentar as noções de curva algébrica não-singular, divisor sobre uma curva e o espaço de Riemann-Roch associado a um divisor. Muitos dos conceitos da geometria algébrica são motivados pelo estudo de funções de variável complexa, como é o caso, por exemplo, da noção de pontos e curvas não-singulares. Sem entrar em pormenores, pode-se pensar uma curva como o conjunto de zeros de um polinômio irredutível em três variáveis definidas sobre os números complexos, no entanto, tratar este assunto através dos números complexos, não nos possibilita termos uma noção da amplitude deste ramo da matemática. Assim, entre 1920 e 1930, a escola alemã liderada por Hasse, Schimidt e Deuring estendeu essas ideias sobre corpos arbitrários, onde a noção de curva é capturada pelas variedades afins e projetivas.

Sobre as variedades afins (projetivas), os mapas que permitem a interação entre eles, são os morfismos e os mapas racionais, este último de grande interesse nesta área para a classificação de variedades. Associado a uma curva, é possível construir seu modelo não-singular. Aqui, em particular, estamos interessados no corpo de funções racionais da curva. Queremos saber quais são os polos e suas respectivas ordens para funções racionais de uma curva algébrica, dada uma coleção finita de pontos numa curva qualquer. Aqui introduzimos a noção de divisor e espaço Riemann-Roch [13], [7], [11] e [25].

1.1 Variedades Afim e Variedades Projetivas

Seja $\mathbb{K}$ um corpo algebricamente fechado. O *espaço afim* n-dimensional se define como

$$\mathbb{A}^n := \{(a_0 \ldots, a_{n-1}) : a_i \in \mathbb{K}, 0 \leqslant i \leqslant n-1\}.$$

Os elementos de $\mathbb{A}^n$ são geralmente denotados por $P = (x_0, \ldots, x_{n-1})$ e dizemos que $x_0, \ldots, x_{n-1}$ são as coordenadas de P . Este espaço pode ser também dotado de uma topologia, comumente conhecida como *topologia de Zariski*. Os conjuntos fechados na topologia de Zariski são os *conjuntos algébricos* definidos por:

$$\mathcal{X} := \{P \in \mathbb{A}^n : \text{ existe } M \subseteq \mathbb{K}[x_0, \ldots, x_{n-1}] \text{ tal que } f(P) = 0 \text{ para todo } f \in M\},$$

onde $\mathbb{K}[x_1, \ldots, x_n]$ é o anel de polinômios de n variáveis sobre $\mathbb{K}$. Associado a um conjunto algébrico $\mathcal{X}$, define-se o *ideal* de $\mathcal{X}$ por

$$I(\mathcal{X}) := \{f \in \mathbb{K}[x_0, \ldots, x_{n-1}] : f(P) = 0 \text{ para todo } P \in \mathcal{X}\}.$$

O *teorema das bases de Hilbert* garante que $I(\mathcal{X})$ é finitamente gerado por polinômios $f_1, \ldots, f_r \in \mathbb{K}[x_0, \ldots, x_{n-1}]$. Assim, $\mathcal{X}$ pode ser escrito como

$$\mathcal{X} = \{P \in \mathbb{A}^n : f_1(P) = \cdots = f_r(P) = 0\}.$$

Um conjunto algébrico $\mathcal{X}$ é dito *redutível* se $\mathcal{X}$ pode ser escrito como $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, onde $\mathcal{X}_1$ e $\mathcal{X}_2$ são subconjuntos algébricos próprios de $\mathcal{X}$. Caso contrário, $\mathcal{X}$ é chamado de *irredutível*. Os conjunto algébricos irredutíveis são chamados de *variedades afins*.

Proposição 1.1.1. *[7, Proposição 1. Seção 1.5] Um conjunto algébrico $\mathcal{X}$ é uma variedade afim se, e somente se, $I(\mathcal{X})$ é um ideal primo.*

Associado a uma variedade afim $\mathcal{X}$, se define o *anel de coordenadas* de $\mathcal{X}$ por

$$\mathbb{K}[\mathcal{X}] := \mathbb{K}[x_0, \ldots, x_{n-1}]/I(\mathcal{X}).$$

Paralelamente ao caso afim, introduzimos o espaço projetivo.

Considere a coleção de todas as retas em $\mathbb{A}^{n+1}$ que passam pelo origem $(0, \ldots, 0)$ sem incluí-lo. Esta coleção determina uma relação de equivalência $\equiv$ sobre $\mathbb{A}^{n+1}\backslash\{(0, \ldots, 0)\}$. O *espaço projetivo* n-dimensional é definido por

$$\mathbb{P}^n := \mathbb{A}^{n+1}\backslash\{(0, \ldots, 0)\}/\equiv.$$

Os elementos em $\mathbb{P}^n$ são chamados de pontos e serão denotamos por

$$P = (a_0 : \ldots : a_n) = \{\lambda(a_0, \ldots, a_n) \in \mathbb{A}^{n+1} : \lambda \in \mathbb{K}\backslash\{0\}\}$$

e dizemos que $x_0, \ldots, x_n$ são as *coordenadas homogêneas* do ponto P.

Neste caso, os conjuntos *algébricos projetivos* em $\mathbb{P}^n$ são definidos como os zeros de conjuntos de polinômios homogêneos em $\mathbb{K}[x_0, \ldots, x_n]$. Da mesma forma que no caso afim, se pode associar um ideal em $\mathbb{K}[x_0, \ldots, x_n]$, para um conjunto algébrico projetivo, salvo que para este caso, é um ideal de polinômios homogêneos. Também, como no caso afim, os conjuntos algébricos projetivos definem a topologia de Zariski sobre $\mathbb{P}^n$. As noções de *irredutibilidade* e *variedade projetiva* de conjuntos algébricos projetivos são definidas como no caso afim e a Proposição 1.1.1 possui ainda uma versão própria do caso projetivo [7, Seção 4.2].

Para evitarmos conflito de notações, denotamos agora por $\mathcal{X}$ uma variedade projetiva em $\mathbb{P}^n$.

Dada uma variedade projetiva $\mathcal{X} \subseteq \mathbb{P}^n$, denotamos o *anel de coordenadas homogêneo* de $\mathcal{X}$ por

$$\mathbb{K}[\mathcal{X}] := \mathbb{K}[x_0, \ldots, x_n]/I(\mathcal{X}).$$

Um elemento $f \in \mathbb{K}[\mathcal{X}]$ é dito *forma de grau* d se $f = F + I(\mathcal{X})$ para algum polinômio F homogêneo de grau d.

Se $f \in \mathbb{K}[x_0, \ldots, x_n]$ é um polinômio homogêneo, o conjunto de zeros de f é dito *hiperplano*. Em particular, denotamos por H_i o hiperplano gerado por x_i, para $i = 0, \ldots, n$. Seja $U_i = \mathbb{P}^n\backslash H_i$. Então $\mathbb{P}^n$ é coberto pelos abertos U_i. Considere ainda a seguinte função

$$\begin{array}{rccc} \varphi_i : & U_i & \to & \mathbb{A}^n \\ & (a_0 : \ldots : a_n) & \mapsto & (\frac{a_0}{a_i}, \ldots, \frac{a_n}{a_i}) \end{array} \tag{1.1}$$

A função φ_i é bem definida.

Proposição 1.1.2. *Considere U_i com a topologia induzida pela topologia de Zariski. Então a função φ_i é um homeomorfismo de U_i a $\mathbb{A}^n$, para todo $i = 0, \ldots, n$.*

Demonstração. Claramente φ_i é uma bijeção. Portanto, é suficiente provar que os conjuntos fechados em U_i são identificados com os conjuntos fechados de $\mathbb{A}^n$ mediante φ_i. Por conveniência, vamos nos concentrar no caso $i = 0$.

Dado um polinômio homogêneo $f \in \mathbb{K}[x_0, \ldots, x_n]$, identificamos a dês-homogeneização de f por $f_* := f(1, x_1, \ldots, x_n)$. Inversamente, dado um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ de grau d, identificamos a homogeneização de f por $f^* := x_0^d f(x_1/x_0, \ldots, x_n/x_0)$.

Seja $\mathcal{X} \subseteq U_0$ um conjunto fechado e seja $\mathcal{X}_0^*$ o fecho de $\mathcal{X}$ em $\mathbb{P}^n$. Logo existe um ideal homogêneo $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$ tal que $\mathcal{X}_0^* = \{P \in \mathbb{P}^n : f(P) = 0 \text{ para todo } f \in I\}$. Seja $I_* = \{f_* \in \mathbb{K}[x_1, \ldots, x_n] : f \in I\}$. Então, temos que $\varphi_0(\mathcal{X}) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ para todo} f \in I^*\}$. Inversamente, seja $\mathcal{X} \subseteq \mathbb{A}^n$ um fechado, então existe um ideal $I \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $\mathcal{X} = \{P \in \mathbb{A}^n : f(P) = 0 \text{ para todo } f \in I\}$. Tome $I^* = \{f^* \in \mathbb{K}[x_0, \ldots, x_n] : f \in I\}$, portanto $\varphi_0^{-1}(\mathcal{X}) = U_0 \cap \mathcal{X}_0^*$, onde $\mathcal{X}_0^*$ é a variedade gerada por I^*. Assim, φ_0 e φ_0^{-1} são funções fechadas, portanto φ_0 é um homeomorfismo. □

A proposição anterior nos diz que o espaço projetivo $\mathbb{P}^n$ pode ser coberto por n cópias de $\mathbb{A}^n$ e que cada variedade afim pode ser submersa numa variedade projetiva. Se $\mathcal{X} \subseteq \mathbb{A}^n$ é uma variedade afim, a variedade projetiva $\mathcal{X}_i^* \subseteq \mathbb{P}^n$ é a homogenização de $\mathcal{X}$ na variável x_i, comumente chamada de *fecho projetivo* de $\mathcal{X}$.

1.2 Morfismos e Mapas Racionais

Dada uma variedade afim $\mathcal{X}$ em $\mathbb{A}^n$, dizemos que uma função $f : \mathcal{X} \to \mathbb{K}$ é *regular no ponto* $P \in \mathcal{X}$ se existe uma vizinhança A de P com $A \subseteq \mathcal{X}$ e polinômios $g, h \in \mathbb{K}[x_0, \ldots, x_{n-1}]$ tais que $h(P) \neq 0$ para todo ponto $P \in A$ e $f = g/h$. Dizemos que f é *regular* em $\mathcal{X}$ se é regular em todo ponto de $\mathcal{X}$. Para uma variedade projetiva em $\mathbb{P}^n$, uma função regular se define da mesma forma, salvo que neste caso os polinômios $g, h \in \mathbb{K}[x_0, \ldots, x_n]$ são homogêneos do mesmo grau.

Proposição 1.2.1. *[13, Lema 3.1, Observação 3.1.1] Toda função regular é contínua.*

Para duas variedades afins (projetivas) $\mathcal{X}_1$ e $\mathcal{X}_2$, um *morfismo* $\phi : \mathcal{X}_1 \to \mathcal{X}_2$ é uma função contínua tal que para todo aberto $A \subseteq \mathcal{X}_2$ e toda função regular $f : A \to \mathbb{K}$, a função $f \circ \phi : \phi^{-1}(A) \to \mathbb{K}$ é regular. Um *isomorfismo* $\phi : \mathcal{X}_1 \to \mathcal{X}_2$ entre variedades, é um morfismo que admite um morfismo inverso $\psi : \mathcal{X}_2 \to \mathcal{X}_1$ com $\phi \circ \psi = \mathrm{id}_{\mathcal{X}_2}$ e $\psi \circ \phi = \mathrm{id}_{\mathcal{X}_1}$, neste caso dizemos que $\mathcal{X}_1$ e $\mathcal{X}_2$ são isomorfos. Um *automorfismo* é um morfismo de $\mathcal{X}_1$ em $\mathcal{X}_1$.

A seguir, definimos algumas estruturas algébricas associadas a uma variedade afim (projetiva).

Definição 1.2.2. *Seja $\mathcal{X}$ uma variedade afim (projetiva). Denotamos o anel de funções regulares sobre $\mathcal{X}$ por $\mathcal{O}(\mathcal{X})$. Para $P \in \mathcal{X}$, definimos o* anel local *$\mathcal{O}_P$ de $\mathcal{X}$ em P como o conjunto de funções regulares em P. Em outras palavras, um elemento em $\mathcal{O}_P$, é um par $\langle f, U\rangle$, onde U é um aberto em $\mathcal{X}$ contendo P e f é uma função regular sobre U.*

Dois pares $\langle f, U\rangle$, $\langle g, V\rangle$ em $\mathcal{O}_P$ são equivalentes se $f = g$ em $U \cap V$.

Note que realmente $\mathcal{O}_P$ é um anel local, cujo ideal maximal $\mathcal{M}_P$ é o conjunto de funções regulares que se anulam em P.

Definição 1.2.3. *Seja $\mathcal{X}$ uma variedade afim (projetiva). Definimos o corpo de funções $\mathbb{K}(\mathcal{X})$ como o conjunto de classes de equivalência do par $\langle f, U\rangle$, onde U é um conjunto aberto não vazio em $\mathcal{X}$. Os elementos em $\mathbb{K}(\mathcal{X})$ são chamados de* funções racionais *sobre $\mathcal{X}$.*

Teorema 1.2.4. *[13, Teorema 3.2] Seja $\mathcal{X} \subseteq \mathbb{A}^n$ uma variedade afim. Então*

(a) $\mathcal{O}(\mathcal{X}) \cong \mathbb{K}[\mathcal{X}]$.

(b) $\mathcal{O}_P \cong \left\{ f \in \mathbb{K}(\mathcal{X}) : f = \dfrac{g}{h} \text{ com } g, h \in \mathbb{K}[\mathcal{X}] \text{ e } h(P) \neq 0 \right\}$.

(c) Para cada $P \in \mathcal{X}$, seja $M_P \subseteq \mathbb{K}[\mathcal{X}]$ o ideal de todas as funções que se anulam em P. Então a função $\alpha : \mathcal{X} \to \mathcal{P}(\mathbb{K}[\mathcal{X}])$ definida por $\alpha(P) = M_p$ define uma correspondência injetora entre os pontos de P e os ideias maximais de $\mathbb{K}[\mathcal{X}]$.

(d) $\mathbb{K}(\mathcal{X})$ é isomorfo ao corpo quociente de $\mathbb{K}[\mathcal{X}]$ e portanto $\mathbb{K}(\mathcal{X})$ é uma extensão finita sobre $\mathbb{K}$.

Teorema 1.2.5. *[13, Teorema 3.4] Seja $\mathcal{X} \in \mathbb{P}^n$ uma variedade projetiva. Então*

(a) $\mathcal{O}(\mathcal{X}) \cong \mathbb{K}$;

(b) Para cada $P \in \mathcal{X}$,

$$\mathcal{O}_P = \left\{ f \in \mathbb{K}(\mathcal{X}) : f = \frac{g}{h} \text{ com } g, h \in \mathbb{K}[\mathcal{X}], \text{ formas de mesmo grau e } h(P) \neq 0 \right\};$$

(c) $\mathbb{K}(\mathcal{X}) \cong \left\{ \dfrac{g}{h} : g, h \in \mathbb{K}[\mathcal{X}] \text{ são formas de mesmo grau e } h \neq 0 \right\}$.

O seguinte resultado permite introduzir a noção de *mapa racional*.

Proposição 1.2.6. *[13, Lema 4.1] Sejam $\mathcal{X}_1$ e $\mathcal{X}_2$ variedades afim (projetivas). Sejam ϕ e ψ dois morfismos de $\mathcal{X}_1$ em $\mathcal{X}_2$ e suponha que existe um aberto não vazio em $U \subseteq \mathcal{X}_1$ tal que $\phi \mid_U = \psi \mid_U$, então $\phi = \psi$.*

Então, dadas duas variedades afins (projetivas) $\mathcal{X}_1$ e $\mathcal{X}_2$, um *mapa racional* $\varphi : \mathcal{X}_1 \to \mathcal{X}_2$ é uma classe de equivalência do par $\langle \varphi_U, U \rangle$, onde $U \subseteq \mathcal{X}_1$ é um conjunto aberto não vazio e φ_U é um morfismo de U a $\mathcal{X}_2$. Dizemos que $\langle \varphi_U, U \rangle$ é equivalente a $\langle \varphi_V, V \rangle$, onde $U, V \subseteq \mathcal{X}_1$ se $\phi \mid_{U \cap V} = \psi \mid_{U \cap V}$. Um mapa racional $\varphi : \mathcal{X}_1 \to \mathcal{X}_2$ é um *mapa birracional* se existe um mapa racional $\psi : \mathcal{X}_2 \to \mathcal{X}_1$ tal que $\varphi \circ \psi = id_{\mathcal{X}_2}$ e $\psi \circ \varphi = id_{\mathcal{X}_1}$. Se existe um mapa birracional de $\mathcal{X}_1$ a $\mathcal{X}_2$, dizemos que $\mathcal{X}_1$ e $\mathcal{X}_2$ são *birracionalmente equivalentes*.

Proposição 1.2.7. *[13, Corolário 4.5] Para quaisquer duas variedades afins (projetivas) $\mathcal{X}_1$ e $\mathcal{X}_2$, as seguintes afirmações são equivalentes:*

(a) $\mathcal{X}_1$ e $\mathcal{X}_2$ são birracionalmente equivalentes.

(b) $\mathbb{K}(\mathcal{X}_1) \cong \mathbb{K}(\mathcal{X}_2)$.

Definição 1.2.8. *A dimensão de uma variedade afim (projetiva) $\mathcal{X}$ é o grau de transcendência de $\mathbb{K}(\mathcal{X})$ sobre $\mathbb{K}$.*

Teorema 1.2.9. *[7, Seção 4.3] Seja $\mathcal{X} \subseteq \mathbb{A}^n$ uma variedade afim e $\mathcal{X}_i^* \subseteq \mathbb{P}^n$ seu fecho projetivo. Considere φ_i como em (1.1), então*

(a) Existe um isomorfismo entre $\mathbb{K}(\mathcal{X})$ sobre $\mathbb{K}(\mathcal{X}_i^*)$

(b) Para $P \in \mathcal{X}$, $\mathcal{O}_P(\mathcal{X})$ é isomorfo a $\mathcal{O}_{\varphi_i^{-1}(P)}(\mathcal{X}_i^*)$

1.3 Curvas Algébricas e Corpo de Funções Algébricas

Definição 1.3.1. *Uma* curva algébrica *projetiva (afim) $\mathcal{X}$ é uma variedade projetiva (afim) de dimensão* 1.

Dada uma curva afim $\mathcal{X}$ em $\mathbb{A}^n$ e $0 \leqslant i \leqslant n-1$, a aplicação φ_i em (1.1) nos permite submergir a curva $\mathcal{X}$ em $\mathcal{X}_i^*$. De fato, o Teorema 1.2.9 nos permite determinar que $\mathcal{X}_i^*$ também é uma curva e que, as estruturas algébricas associadas a $\mathcal{X}$ são preservadas mediante φ_i em $\mathcal{X}_i^*$. Portanto, podemos determinar n modelos projetivos de $\mathcal{X}$. De acordo ao modelo que se escolha, chamamos os pontos em $\mathcal{X}_i^* \cap (\mathbb{P}^n \backslash U_i)$ *pontos no infinito de* $\mathcal{X}$, onde U_i é o aberto em $\mathbb{P}^n$ definido pela equação $x_i \neq 0$.

Motivada pelas noções de superfícies sobre os números complexos, a forma mais natural para definir a ideia de não singularidade numa curva algébrica afim envolve o conceito de derivadas. Assim, dada uma curva afim $\mathcal{X} \subseteq \mathbb{A}^n$ definida pelos polinômios $f_1, f_2, \ldots, f_r \in \mathbb{K}[x_0, \ldots, x_{n-1}]$, dizemos que um ponto $P \in \mathcal{X}$ é *não-singular* se o posto da matriz jacobiana $\|(\partial f_i/\partial x_k)(P)\|$ é $n-1$ (ver [13, Pag 31]). A curva $\mathcal{X}$ é *não-singular* se for não-singular em todos seus pontos. Para o caso de curvas arbitrárias, precisa-se introduzir os dois seguintes fatos para estender esse conceito.

Proposição 1.3.2. *[7, Proposição 4, seção 2.5] Seja R um domínio que não é um corpo. Então as seguintes afirmações são equivalentes:*

(a) R é um anel noetheriano e local, cujo ideal maximal é principal.

(b) Existe um elemento irredutível $t \in R$ tal que qualquer elemento $z \neq 0$ em R, pode ser representado de forma única como $z = t^n u$ para algum inteiro não negativo n e u uma unidade de R.

Um anel com as propriedades da proposição anterior é dito de *Anel de valorização discreta.*

Teorema 1.3.3. *[13, Teorema 5.1] Seja $\mathcal{X} \subseteq \mathbb{A}^n$ uma curva afim e P um ponto em $\mathcal{X}$. Então P é um ponto não-singular em $\mathcal{X}$ se, e somente se, o anel local $\mathcal{O}_P$ é um anel de valorização discreta.*

Portanto, podemos dizer que: Um ponto P sobre a curva afim (projetiva) $\mathcal{X}$ é *não-singular* se o anel local $\mathcal{O}_P(\mathcal{X})$ é um anel de valorização discreta. Uma curva $\mathcal{X}$ é chamada *não-singular* se todos seus pontos são não singulares.

Teorema 1.3.4. *([7]. Teorema 1. Seção 7.5) Seja $\mathcal{X}$ uma curva projetiva. Então existe uma curva projetiva não-singular $\mathcal{X}'$ e um morfismo birracional θ' de $\mathcal{X}'$ sobre $\mathcal{X}$. Se existir outra curva não-singular $\mathcal{X}''$ e um morfismo birracional θ'' de $\mathcal{X}''$ sobre $\mathcal{X}$ então existe um único isomorfismo $\theta : \mathcal{X}' \to \mathcal{X}''$ tal que $\theta' = \theta'' \circ \theta$.*

A seguir, apresentamos noções básicas da teoria do corpo de funções algébricas. Neste ponto, auxiliado pelos Teoremas 1.2.4 e 1.2.5, ao invés de utilizarmos uma abordagem geométrica, procuramos introduzir a linguagem do corpo de funções com a intenção de fazer um paralelo entre curvas algébricas e corpo de funções [25].

Definição 1.3.5. *Seja $\mathbb{K}$ um corpo. Um* corpo de funções algébricas $\mathbb{F}/\mathbb{K}$ *de uma variável sobre $\mathbb{K}$ é uma extensão $\mathbb{F} \supseteq \mathbb{K}$ tal que $\mathbb{F}$ é uma extensão algébrica finita de $\mathbb{K}(x)$ para algum $x \in \mathbb{F}$ transcendente sobre $\mathbb{K}$.*

Equivalentemente à Definição 1.3.5, um corpo de funções algébricas $\mathbb{F}$ é um corpo que, em relação a $\mathbb{K}$, tem grau de transcendência igual a um. Comumente um corpo de funções $\mathbb{F}/\mathbb{K}$ é representado como uma extensão algébrica do corpo de funções racionais $\mathbb{K}(x)$, ou ainda $\mathbb{F} = \mathbb{K}(x, y)$, onde y é transcendente em $\mathbb{K}(x)$.

Definição 1.3.6. *Um* anel de valorização *do corpo de funções* $\mathbb{F}/\mathbb{K}$ *é um anel* $\mathcal{O} \subseteq \mathbb{F}$ *com as seguintes propriedades:*

(a) $\mathbb{K} \subsetneq \mathcal{O} \subsetneq \mathbb{F}$

(b) Para todo $z \in \mathbb{F}$*, temos que* $z \in \mathcal{O}$ *ou* $z^{-1} \in \mathcal{O}$*.*

Proposição 1.3.7. *[25, Proposição 1.1.5] Seja* $\mathcal{O}$ *um anel de valorização do corpo de funções* $\mathbb{F}/\mathbb{K}$*. Então* $\mathcal{O}$ *é um anel local cujo ideal maximal* P *pode ser caracterizado da seguinte forma: para* $0 \neq x \in F$*,* $x \in P$ *se, e somente se,* $x^{-1} \notin \mathcal{O}$*.*

Proposição 1.3.8. *[25, Proposição 1.1.6] Seja* $\mathcal{O}$ *um anel local do corpo de funções* $\mathbb{F}/\mathbb{K}$ *e* P *seu único ideal maximal. Então,* $\mathcal{O}$ *é um anel de valorização discreta.*

Um *lugar* P de um corpo de funções $\mathbb{F}/\mathbb{K}$ é o ideal maximal de algum anel de valorização $\mathcal{O}$ de $\mathbb{F}/\mathbb{K}$. Segundo a Proposição 1.3.7 o anel $\mathcal{O}$ está totalmente determinado por P. Portanto, $\mathcal{O}_P := \mathcal{O}$ é dito *anel de valorização do lugar* P. Um elemento $t \in \mathcal{O}_P$ é chamado de *parâmetro local*, se t é um gerador de P.

Sobre $\mathbb{F}$ pode ser definida uma aplicação v_P da seguinte forma: Seja P um lugar e t um parâmetro local de P. Para $0 \neq x \in \mathbb{F}$, temos que $x = t^n u$ com $u \in \mathcal{O}_P$ invertível. Defina $v_P(x) := n$ se $x \neq 0$ e $v_P(0) := \infty$.

Note que v_P está bem definida, pois dado outro parâmetro local t' para P, temos que $t = t'w$ para algum $w \in \mathcal{O}_P$ invertível, logo $x = t^n u = (t'^n w^n u) = t'^n (w^n u)$ com $(w^n u) \in \mathcal{O}_P$ invertível.

Teorema 1.3.9. *[25, Teorema 1.1.13] Seja* $\mathbb{F}/\mathbb{K}$ *um corpo de funções.*

(a) $v_P(x) = \infty$ *se, e somente se,* $x = 0$*.*

(b) $v_P(xy) = v(x) + v(y)$*.*

(c) $v_P(x + y) \geqslant min\{v_P(x), v_P(y)\}$*. A igualdade é satisfeita se* $v_P(x) \neq v_P(y)$*.*

(d) Para cada lugar P *de* $\mathbb{F}/\mathbb{K}$ *temos que*

$$\mathcal{O}_P = \{x \in \mathbb{F} : 0 \leqslant v_P(x)\}$$
$$P = \{x \in \mathbb{F} : 0 < v_P(x)\}$$

(e) Um elemento $t \in \mathbb{F}$ *é um parâmetro local para* P *se, e somente se,* $v_P(t) = 1$*.*

Definição 1.3.10. *Seja* P *um lugar do corpo* $\mathbb{F}/\mathbb{K}$*. a função* v_P *é dita de* valorização discreta de $\mathbb{F}/\mathbb{K}$ *no ponto* P*. Para* $x \in \mathbb{F}$*, o inteiro* $v_P(x)$ *é chamado a* valorização de x no ponto P*.*

É possível fazer uma tradução da linguagem das curvas algébricas ao linguagem de corpo de funções algébricas: Sejam $\mathcal{X}$ uma curva projetiva não-singular e $\mathbb{K}(\mathcal{X})$ seu corpo de funções sobre $\mathbb{K}$. A cada ponto da curva, podemos associar de forma única um lugar de $\mathbb{K}(\mathcal{X})/\mathbb{K}$. Esta correspondência está dada por

$$P \mapsto \mathcal{M}_P.$$

Note que essa correspondência está bem definida pois $\mathcal{O}_P$ é um anel local. correspondência, torna-se possível traduzir definições e resultados do corpo de funções algébricas à linguagem de curvas algébricas e vice-versa. Por exemplo, para um ponto $P \in \mathcal{X}$, temos que:

$$\mathcal{O}_P = \{f \in \mathbb{K}(\mathcal{X}) : v_P(f) \geqslant 0\}$$
$$\mathcal{M}_P = \{f \in \mathbb{K}(\mathcal{X}) : v_P(f) > 0\}$$

onde v_P é a valorização discreta em $\mathbb{K}(\mathcal{X})$ correspondente ao anel de valorização $\mathcal{O}_P$.

Terminamos esta seção introduzindo a noção de curva sobre um corpo finito.

Seja $\mathbb{F}_q$ um corpo finito com q elementos e $\mathbb{K}$ seu fecho algébrico. Para este caso, dizemos que uma curva afim $\mathcal{X} \subseteq \mathbb{A}^n$ está definida sobre $\mathbb{F}_q$ se seu ideal $I(\mathcal{X}) \subseteq \mathbb{K}[x_0, \ldots, x_{n-1}]$ pode ser gerado por polinômios em $\mathbb{F}_q[x_0, \ldots, x_{n-1}]$, semelhantemente, uma curva projetiva $\mathcal{X} \subseteq \mathbb{P}^n$ está definida em $\mathbb{F}_q$ se existem polinômios homogêneos em $\mathbb{F}_q[x_0, \ldots, x_n]$ que geram seu ideal.

Se $\mathcal{X}$ está definida em $\mathbb{F}_q$, um ponto $P \in \mathcal{X} \cap \mathbb{A}^n(\mathbb{F}_q)$ é chamado de *ponto $\mathbb{F}_q$-racional*. No caso projetivo, um ponto $P \in \mathcal{X}$ é dito $\mathbb{F}_q$-racional se existem coordenadas homogêneas de P em $\mathbb{F}_q$.

Seja $\mathcal{X} \subseteq \mathbb{A}^n$ uma curva afim definida sobre $\mathbb{F}_q$. Definimos o ideal

$$I(\mathcal{X}/\mathbb{F}_q) := I(\mathcal{X}) \cap \mathbb{F}_q[x_0, \ldots, x_{n-1}]$$

e seu anel de coordenadas como

$$\mathbb{F}_q[\mathcal{X}] := \mathbb{F}_q[x_0, \ldots, x_{n-1}] \backslash I(\mathcal{X}/\mathbb{F}_q).$$

Neste caso, uma função regular está definida por um quociente de polinômios em $\mathbb{F}_q[x_0, \ldots, x_{n-1}]$. O anel gerado por essas funções regulares é isomorfo a $\mathbb{F}_q[\mathcal{X}]$ e o corpo de funções racionais $\mathbb{F}_q(\mathcal{X})$ de $\mathcal{X}$ é isomorfo ao corpo quociente de $\mathbb{F}_q[\mathcal{X}]$. A dimensão de $\mathcal{X}$ é o grau de transcendência de $\mathbb{F}_q(\mathcal{X})$ sobre $\mathbb{F}_q$, que neste caso, por ser $\mathcal{X}$ uma curva é 1. De forma semelhante, pode-se definir esses conceitos para uma variedade projetiva definida sobre $\mathbb{F}_q$.

1.4 Teorema Riemann-Roch

Na seção anterior, foi estabelecida uma correspondência entre conceitos de curva algébrica e corpo de funções algébricas. Aqui, tomamos como referência [25], adaptando seus resultados à linguagem das curvas. Na presente seção, apresentamos a noção de divisor, divisor de uma função racional, gênero de uma curva e o espaço Riemann-Roch associado a um divisor definido sobre uma curva.

Nesta seção, nos consideramos $\mathcal{X}$ como uma curva projetiva não singular.

Definição 1.4.1. *Seja $\mathcal{X}$ uma curva. Um* divisor *sobre $\mathcal{X}$ é uma soma formal*

$$D = \sum_{P \in \mathcal{X}} n_P P, \text{ onde } n_P \in \mathbb{Z} \text{ e quase todos são } n_P = 0.$$

Notamos por $Div(\mathcal{X})$ o conjunto de divisores sobre $\mathcal{X}$.

Para $Q \in \mathcal{X}$ e $D = \sum_{P \in \mathcal{X}} n_P P$ definimos a ordem *do divisor D no ponto Q por $v_Q(D) := n_Q$. Portanto*

$$D = \sum_{P \in \mathcal{X}} v_P(D) P.$$

O suporte *de D é definido como*

$$Supp(D) := \{P \in \mathcal{X} : v_P(D) \neq 0\}.$$

Um divisor da forma $D = v_P(D)P$ com $P \in \mathcal{X}$ é dito de divisor primo.

O grau de um divisor $D = \sum_{P \in \mathcal{X}} v_P(D) P$ se define por

$$grau(D) := \sum_{P \in \mathcal{X}} v_P(D).$$

Sobre $\mathrm{Div}(\mathcal{X})$ pode-se definir uma estrutura de grupo: Definimos a soma entre dois divisores $D = \sum_{P \in \mathcal{X}} n_P P$ e $D' = \sum_{P \in \mathcal{X}} n'_P P$ de forma natural como

$$D + D' = \sum_{P\in\mathcal{X}}(n_P + n'_P)P.$$

O elemento neutro é o divisor zero

$$0 := \sum_{P\in\mathcal{X}} v_P(0)P \text{ tal que para todo } P, v_P(0) = 0.$$

Também, $\mathrm{Div}(\mathcal{X})$ pode ser dotado de um ordem parcial $\preceq$ definido por

$$D_1 \preceq D_2 \text{ se e somente se } v_P(D_1) \leqslant v_P(D_2) \text{ para todo } P \in \mathcal{X}.$$

Um divisor D é chamado *efetivo* se $0 \preceq D$.

Definição 1.4.2. *Seja $f \in \mathbb{K}(\mathcal{X})$ e $P \in \mathcal{X}$. Dizemos que P é um* zero *de f se $v_P(f) > 0$. Caso em que $v_P(f) < 0$, dizemos que P é um* polo *de f.*

Proposição 1.4.3. *[7, Proposição 1. Seção 8.1] Se $0 \neq f \in \mathbb{K}(\mathcal{X})$, então f tem a mesma quantidade finita de polos e zeros (contando multiplicidades).*

O resultado anterior nos permite apresentar a seguente definição.

Definição 1.4.4. *Seja $0 \neq f \in \mathbb{K}(\mathcal{X})$, denotamos por Z e N o conjunto de zeros e polos de f em $\mathcal{X}$, respectivamente. Definimos*

$$(f)_0 := \sum_{P\in Z} v_P(f)P, \text{ o divisor de zeros de } f,$$

$$(f)_\infty := \sum_{P\in N} (-v_P(f))P, \text{ o divisor de polos de } f,$$

$$(f) := (f)_0 - (f)_\infty, \text{ o divisor de principal de } f.$$

Observe que para qualquer $f \neq 0 \in \mathbb{K}(\mathcal{X})$, $\mathrm{grau}(f) = 0$.

Definição 1.4.5. *Sejam $D, D' \in Div(\mathcal{X})$. Dizemos que D e D' são equivalentes se existe uma função racional $f \in \mathbb{K}(\mathcal{X})$ tal que $(f) = D - D'$. Denotamos esta equivalência por $D \sim D'$.*

A seguinte definição é fundamental para o desenvolvimento deste trabalho.

Definição 1.4.6. *Dado $D \in Div(\mathcal{X})$, definimos o* espaço Riemann-Roch *associado a D por*

$$\mathcal{L}(D) := \{f \in \mathbb{K}(\mathcal{X}) : 0 \preceq (f) + D\} \cup \{0\}.$$

Esta definição tem a seguente interpretação: se

$$D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

com $n_i > 0$ e $m_j > 0$, então $f \in \mathcal{L}(D)$ se

(1) f tem zeros de ordem maior ou igual que m_j em Q_j, para $j = 1, \ldots, S$.

(2) f tem polos somente nos pontos $P_1, \ldots, P_r$, com ordem menor ou igual a n_i, para $i = 1, \ldots, r$.

Observação 1.4.7. *[25, Observação 1.4.5] Seja $D \in Div(D)$. Então*

(i) $f \in \mathcal{L}(D)$ se, e somente se $v_P(f) \geqslant -v_P(D)$ para todo $P \in \mathcal{X}$.

(ii) $\mathcal{L}(D) \neq \{0\}$ se e somente se existe um divisor efetivo D' tal que $D \sim D'$.

A seguir, serão apresentados uma serie de resultado associados ao espaço Riemann-Roch.

Proposição 1.4.8. *[25, Lema 1.4.6] Seja $D \in Div(\mathcal{X})$. Então:*

(a) $\mathcal{L}(D)$ é um espaço vetorial sobre $\mathbb{K}$.

(b) Seja $D' \in Div(\mathcal{X})$ tal que $D \sim D'$, então $\mathcal{L}(D) \simeq \mathcal{L}(D')$.

Proposição 1.4.9. *[25, Lema 1.4.7]*

(a) $\mathcal{L}(0) = \mathbb{K}$.

(b) se $grau(D) < 0$, então $\mathcal{L}(D) = \{0\}$.

Proposição 1.4.10. *[25, Lema 1.4.8] Seja $D, D' \in Div(\mathcal{X})$ com $D \preceq D'$. Então $\mathcal{L}(D) \leqslant \mathcal{L}(D')$ e $\ell(D') - \ell(D) \leqslant grau(D') - grau(D)$.*

Proposição 1.4.11. *[25, Lema 1.4.9] Seja $D \in Div(\mathcal{X})$, então o espaço Riemann-Roch associado a D é um espaço vetorial sobre $\mathbb{K}$ de dimensão finita.*

Definição 1.4.12. *Para $D \in Div(\mathcal{X})$ o inteiro $\ell(D) := dim(\mathcal{L}(D))$ é dito de* dimensão do divisor *D.*

Proposição 1.4.13. *[25, Corolário 1.4.12] Seja $D \in Div(\mathcal{X})$*

(a) Seja $D' \in Div(\mathcal{X})$ tal que $D \sim D'$. Então $\ell(D) = \ell(D')$ e $grau(D) = grau(D')$.

(b) Se $grau(D) < 0$, então $\ell(D) = 0$

(c) Se $grau(D) = 0$, as seguintes afirmações são equivalentes:

(1) D é principal.
(2) $\ell(D) \geqslant 1$.
(3) $\ell(D) = 1$.

Definição 1.4.14. *O* gênero *g da curva $\mathcal{X}$ se define como*

$$g := max\{grau(D) - \ell(D) + 1 : D \in Div(\mathcal{X})\}.$$

Proposição 1.4.15. *[26, Teorema 10.4.6] Seja $\mathcal{X} \subseteq \mathbb{P}^2$ é uma curva não singular projetiva de grau d. Então*

$$g = \frac{1}{2}(d-1)(d-2).$$

Teorema 1.4.16 (Teorema de Riemann)**.** *[25, Teorema 1.4.17] Seja $\mathcal{X}$ uma curva de gênero g. Para $D \in Div(\mathcal{X})$, então $\ell(D) \geqslant grau(D) + 1 - g$. Além disso, existe $c \in \mathbb{Z}$ tal que para qualquer divisor D com $grau(D) \geqslant c$, $\ell(D) = grau(D) + 1 - g$.*

Definição 1.4.17. *Um divisor $W \in Div(\mathcal{X})$ é chamado* canônico *se*

$$grau(W) = 2g - 2 \text{ e } \ell(W) \geqslant g.$$

Teorema 1.4.18 (Teorema de Riemann-Roch)**.** *[25, Teorema 1.5.15] Dado um divisor $D \in Div(\mathcal{X})$, então*

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

onde W é qualquer divisor canônico.

Teorema 1.4.19 (Teorema de Clifford)**.** *[25, Teorema 1.6.13]*

Para todo divisor $D \in Div(\mathcal{X})$ com $0 \leqslant grau(D) \leqslant 2g - 2$ se tem $\ell(D) \leqslant 1 + \frac{1}{2}grau(D)$.

Capítulo 2

Semigrupo de Weierstrass

Neste capítulo, introduzimos noções básicas da teoria de semigrupos de Weierstrass, como semigrupo Weierstrass em um ponto, semigrupo de Weierstrass em vários pontos, elementos minimais e conjunto gerador minimal. No caso de um ponto, a estrutura do semigrupo é bastante simples e suas aplicações na teoria do código de Goppa são bem conhecidas na literatura (ver [25], [26], [12]); para o caso de vários pontos, os resultados aqui apresentados se devem a Carvalho e Torres [4] e Matthews [21]; também, como no caso de um ponto, aplicações enumeráveis na teoria dos códigos Goppa foram obtidas para certo tipo de curvas, ver por exemplo em [22], [23], [4],[20],[15], [14].

2.1 Semigrupo de Weierstrass em um Ponto

Ao longo desta seção, $\mathcal{X}$ denotará uma curva algébrica, projetiva não-singular de gênero g definida sobre um corpo finito $\mathbb{F}_q$ de q elementos.

Definição 2.1.1. *Seja $S \subseteq \mathbb{N}_0$. Dizemos que S é um semigrupo numérico se satisfaz as seguintes condições:*

(i) $0 \in S$,

(ii) $\mathbb{N}_0 \backslash S$ *é finito,*

(iii) Se $a, b \in S$, *então* $a + b \in S$.

Os elementos em $\mathbb{N}_0 \backslash S$ *são chamados* lacunas. *O número* $g := \#\mathbb{N}_0 \backslash S$ *é dito de* gênero *de* S.

Antes de definirmos semigrupo de Weierstrass, precisamos dos seguintes resultados.

Proposição 2.1.2. *Seja $P \in \mathcal{X}$ uma curva sobre $\mathbb{K}$. Para cada $n \geqslant 2g$ existe $f \in \mathbb{K}(\mathcal{X})$ tal que $(f_\infty) = nP$.*

Demonstração. Dado que $\text{grau}(nP) \geqslant 2g$, uma aplicação do Teorema de Riemann-Roch garante que $\ell(nP) = \ell((n-1)P) + 1$. Portanto $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$. Consequentemente, qualquer função $f \in \mathcal{L}(nP) \backslash \mathcal{L}((n-1)P)$ tem divisor de polos nP. □

Definição 2.1.3. *Um número $n \in \mathbb{N}_0$ é chamado de* não-lacuna em $P \in \mathcal{X}$ *se existe uma função $f \in \mathbb{K}(\mathcal{X})$ tal que $(f)_\infty = nP$. Caso contrário n é chamado de* lacuna *em P.*

Teorema 2.1.4 (Teorema de lacunas de Weierstrass)**.** *Sejam $\mathcal{X}$ uma curva projetiva não-singular com gênero $g > 0$ definida sobre $\mathbb{K}$ e $P \in \mathcal{X}$. Então existem exatamente g lacunas $i_1 < i_2 < \ldots < i_g$ com*

$$i_1 = 1 \text{ e } i_g \leqslant 2g-1.$$

Demonstração. Pela Proposição 2.1.2, se n é uma lacuna em P, então $n \leqslant 2g-1$.

Veja a seguinte caracterização óbvia: $n \in \mathbb{N}_0$ é uma não lacuna em P se, e somente se, $\ell(nP) = \ell((n-1)P)+1$. Considere a sequência de $\mathbb{F}_q$-espaços vetoriais

$$\mathbb{F}_q = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \cdots \subseteq \mathcal{L}((2g-2)P) \subseteq \mathcal{L}((2g-1)P).$$

Com $\ell(0) = 1$ e $\ell((2g-1)P) = g$. Pela Proposição 1.4.10 temos

$$\ell(iP) - \ell((i-1)P) \leqslant 1$$

para todo $1 \leqslant i \leqslant 2g-1$. Portanto existem $g-1$ números $1 \leqslant i \leqslant 2g-1$ tais que $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$. Logo existem g lacunas em P.

Finalmente, resta mostrar que 1 é uma lacuna. Suponha que 1 é não lacuna em P, logo existe uma função racional $f \in \mathbb{K}(\mathcal{X})$ tal que $(f)_\infty = P$, pelo Teorema 1.3.9 (b), temos que $(f^n)_\infty = nP$ para todo $n \in \mathbb{N}_0$, logo não existem lacunas em P. Isso é uma contradição, portanto 1 é uma lacuna. □

O Teorema 1.3.9 e o Teorema 2.1.4 garantem a seguinte definição.

Definição 2.1.5. *Seja $P \in \mathcal{X}$. O conjunto*

$$H(P) := \{n \in \mathbb{N}_0 : \exists f \in \mathbb{K}(\mathcal{X}) \text{ tal que } (f)_\infty = nP\},$$

é um semigrupo numérico e é chamado de semigrupo de Weierstrass *em P. O complemento $G(P) := \mathbb{N}_0 \backslash H(P)$ é dito de* conjunto de lacunas *de P.*

Proposição 2.1.6. *Seja $P \in \mathcal{X}$ e $m \in \mathbb{N}_0$. Então $\ell(mP)$ é igual ao número de não-lacunas menores ou iguais a m.*

Demonstração. Note que um número $s \in \mathbb{N}_0$ é uma lacuna se, e somente se, $\ell(sP) = \ell((s-1)P)$. Considere a sequência de $\mathbb{F}_q$-espaços vetoriais $\mathbb{F}_q = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \cdots \subseteq \mathcal{L}(mP)$. Segundo a Proposição 1.4.10, $\ell(iP) - \ell((i-1)P) \leqslant 1$ para todo $1 \leqslant i \leqslant m$. Portanto, temos o resultado. □

Definição 2.1.7. *Seja P um ponto sobre uma curva $\mathcal{X}$ não-singular de gênero g. Dizemos que P é um* ponto Weierstrass *se o conjunto de lacunas $G(P) \neq \{1, 2, \ldots, g\}$. Caso contrário P é chamado de* ponto não-Weierstrass.

2.2 Semigrupo de Weierstrass em Vários Pontos

Nesta seção, introduzimos a noção do semigrupo de Weierstrass em vários pontos. Os resultados aqui desenvolvidos são devidos a Carvalho e Torres em [4].

Definição 2.2.1. *Seja $\mathcal{X}$ uma curva algébrica projetiva, irredutível e não-singular definida sobre o um corpo finito $\mathbb{F}_q$ com q elementos. Sejam $P_1, \ldots, P_m$ pontos $\mathbb{F}_q-$racionais distintos sobre $\mathcal{X}$. O conjunto*

$$H = H(P_1, \ldots, P_m) := \{(n_1, \ldots, n_n) \in \mathbb{N}_0^m : \exists f \in \mathbb{F}_q(\mathcal{X}) \text{ com } (f)_\infty = \textstyle\sum_{i=1}^m n_i P_i\}$$

é dito o semigrupo de Weierstrass *de $\mathcal{X}$ em $P_1, \ldots, P_m$.*

Note que, na Definição 2.2.1, a estrutura do semigrupo de Weierstrass está totalmente determinada pela forma em que os pontos $P_1, \ldots, P_m$ possam ser distribuidos.

Para começar, vamos adotar a seguinte notação:

(i) Para $\boldsymbol{n} := (n_1, \ldots, n_m) \in \mathbb{N}_0^m$ e $i \in \{1, \ldots, m\}$, definimos o conjunto

$$\nabla_i^m(\boldsymbol{n}) := \{(p_1, \ldots, p_m) \in H(P_1, \ldots, P_m) : n_i = p_i \text{ e } p_j \leqslant n_j \forall j \neq i\},$$

(ii) $\boldsymbol{n}_i = \boldsymbol{n} - n_i \boldsymbol{e}_i$, onde $\boldsymbol{e}_i \in \mathbb{N}_0^m$ é o vetor com entrada 1 na i-ésima posição e 0 nas restantes.

(iii) $\mathbf{1} := (1, \ldots, 1) \in \mathbb{N}_0^m$.

(iv) Seja $f \in \mathbb{F}_q(\mathcal{X})$. Para cada $i, 1 \leqslant i \leqslant m$, $v_i(f)$ denota a ordem de f no ponto P_i.

Lema 2.2.2. *Seja $\boldsymbol{n} \in \mathbb{N}_0^m$ e suponha $1 \leqslant i \leqslant m \leqslant \#\mathbb{F}_q$. Então $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i) + 1$ se e somente se $\nabla_i^m(\boldsymbol{n}) \neq \varnothing$.*

Demonstração. Seja $\boldsymbol{n} \in \mathbb{N}_0^m$. Suponha que $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i) + 1$, logo existe $f \in \mathbb{F}_q(\mathcal{X})$ tal que $v_i(f) = -n_i$ e $v_j(f) \geqslant -n_j$ para $j \neq i$, com $1 \leqslant j \leqslant m$. Se $n_i = 0$, então o vetor $\mathbf{0} \in \nabla_i^m(\boldsymbol{n})$. Se $n_i \neq 0$, considere t_j um parâmetro local no ponto P_j, para $1 \leqslant j \leqslant m$. Seja

$$f = a_j t_j^{v_j(f)} + \cdots \in \mathbb{F}_q((t_j))$$

a expansão local de f no ponto P_j. Para satisfazer a implicação, basta tomar $\alpha \in \mathbb{F}_q$ tal que $\alpha + a_j \neq 0$ para todo $1 \leqslant j \leqslant m$ que satisfaz $v_j(f) = 0$. Tome α como o inverso da somatória desses elementos, esse elemento é diferente de zero pelo fato da cardinalidade e $n_i \neq 0$. O elemento $f + \alpha$ garante que $\nabla_i^m(\boldsymbol{n}) \neq \varnothing$. Reciprocamente, suponha que $\nabla_i^m(\boldsymbol{n}) \neq \varnothing$, logo existe $f \in \mathbb{F}_q(\mathcal{X})$ tal que $v_i(f) = n_i$ e $v_j(f) \geqslant -n_j$ para $j \neq i, 1 \leqslant j \leqslant m$, logo $f \in \mathcal{L}(\sum_{j=1}^m n_j P_j) \backslash \mathcal{L}(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i)$, logo $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i) + 1$. □

Seja $D \in \mathrm{Div}(\mathcal{X})$. O conjunto

$$| D | := \{D' : 0 \leq D' \text{ e } D \sim D'\}$$

é chamado de *sistema linear completo*. Um ponto $P \in \mathcal{X}$ é um *ponto base* do sistema linear $| D |$ se $P \in \mathrm{Supp}(D')$ para todo $D' \in | D |$. Um sistema linear que não contém pontos base é chamado *sistema linear livre de ponto base*.

Lema 2.2.3. *Seja $\boldsymbol{n} \in \mathbb{N}_0^m$ e suponha $m \leqslant \#\mathbb{F}_q$. As seguintes afirmações são equivalentes:*

(a) $\boldsymbol{n} \in H(P_1, \ldots, P_m)$.

(b) $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i) + 1$ *para todo* $i, 1 \leqslant i \leqslant m$.

(c) O sistema linear $| n_1 P_1 + \ldots + n_m P_m |$ *é livre de ponto base.*

Demonstração. Primeiramente, vejamos que (a) implica (c). Seja $\boldsymbol{n} \in H(P_1, \ldots, P_m)$, então existe $f \in \mathbb{F}_q(\mathcal{X})$ tal que $(f)_\infty = \sum_{i=1}^m n_i P_i$. Considere o divisor efetivo $(f)_0$, consequentemente $(f)_\infty \sim (f)_0$ e $\mathrm{supp}(f)_\infty \cap \mathrm{supp}(f)_0 = \varnothing$ e portanto o sistema linear $| n_1 P_1 + \ldots + n_m P_m |$ é livre de ponto base.
(c) implica (a). Existe um divisor efetivo D tal que $D \sim \sum_{i=1}^m n_i P_i$ e $\mathrm{supp}(D) \cap \mathrm{supp}(\sum_{i=1}^m n_i P_i) = \varnothing$, logo existe $f \in \mathbb{F}_q(\mathcal{X})$ tal que $(f)_\infty = \sum_{i=1}^m n_i P_i$.
(a) implica (b). Se $\boldsymbol{n} \in H(P_1, \ldots, P_m)$, então $\nabla_i^m(\boldsymbol{n}) \neq \varnothing$ para todo $i \in \{1, \ldots, m\}$. Pelo lema anterior temos que $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i) + 1$ para todo $i \in \{1, \ldots, m\}$.
(b) implica (a). Seja $f_1, \ldots, f_m \in \mathbb{F}_q(\mathcal{X})$ tal que $v_i(f_i) = -n_i$ e $v_j(f_i) \geqslant -n_j$ se $j \neq i$, com $i, j \in \{1, \ldots, m\}$. Vamos provar que existe uma m-tupla $(\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_q^m$ tal que o divisor de polos de $f = \sum_{i=1}^m \alpha_i f_i$ é exatamente $\sum_{i=1}^m n_i P_i$. Considere para cada $i = 1, \ldots, m$ o parâmetro local t_i em P_i e a representação local de f_i em P_i

$$f_i = a_{i,j}t_j^{v_j(f_i)} + \ldots \in \mathbb{F}_q((t_j)).$$

Sem mudar a notação, podemos supor que a representação local de f em P_j é

$$(\sum_{i=1}^m \alpha_i a_{i,j})t_j^{v_j(f_i)} + \ldots \in \mathbb{F}_q(t_i).$$

Logo

$$(f)_\infty = \sum_{i=1}^m n_i P_i \text{ se e somente se } \sum_{i=1}^m \alpha_i a_{i,j} \neq 0. \tag{2.1}$$

Considere para cada $i \in \{1, \ldots, m\}$, o subespaço vetorial A_i gerado pelo conjunto $\{(\beta_1, \ldots, \beta_m) \in \mathbb{F}_q^m : \alpha_i = \beta_i \text{ e } \sum_{i=1}^m \beta_i a_{i,j} = 0\}$, logo $\dim(A_i) = m-1$. Portanto, basta tomar um elemento em $\mathbb{F}_q^m \backslash \cup_{i=1}^m A_i$ para satisfazer (2.1); tal elemento existe pois $\#\mathbb{F}_q \geqslant m$.

□

O seguinte exemplo, foi elaborado por Carvalho e Torres em [4]. Nesse exemplo, eles mostram que a condição sobre a cardinalidade, é realmente necessária para garantir a equivalência entre (a) e (b) no Lema 2.2.3.

Exemplo 2.2.4. *Seja $\mathcal{X}$ uma curva de grau 4 definida sobre $\mathbb{F}_3$ e P_1, P_2, P_3, P_4 pontos colineares sobre a curva $\mathcal{X}$. Logo, $\ell(P_1+P_2+P_3+P_4) = 3$ e $\ell(P_i+P_j+P_k) = 2$ para todo $1 \leqslant i < j < k \leqslant 4$; mas não existe uma função racional $f \in \mathbb{F}_3(\mathcal{X})$ tal que $(f)_\infty = P_1 + P_2 + P_3 + P_4$.*

A partir de agora, assumimos que $\#\mathbb{F}_q \geqslant m$.

Definição 2.2.5. *Sejam $P_1, \ldots, P_m$ pontos $\mathbb{F}_q-$racionais distintos sobre $\mathcal{X}$. Os elementos do conjunto*

$$G(P_1, \ldots, P_m) := N_0^m \backslash H(P_1, \ldots, P_m)$$

são chamados de Lacunas de Weierstrass (ou Lacunas) *nos pontos $P_1, \ldots, P_m$.*

Corolário 2.2.6. *Seja $\boldsymbol{n} \in \mathbb{N}_0^m$. As seguintes afirmações são equivalentes:*

(a) $\boldsymbol{n} \in G(P_1, \ldots, P_m)$.

(b) Existe $1 \leqslant i \leqslant m$ *tal que* $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i)$.

(c) Existe $1 \leqslant i \leqslant m$ *tal que* $\nabla_i^m(\boldsymbol{n}) = \varnothing$.

Demonstração. O Lema 2.2.2 e o Lema 2.2.3 garantem o resultado. □

Observação 2.2.7. *Dado um vetor $\boldsymbol{n} \in \mathbb{N}_0^m$, que $\nabla_i^m(\boldsymbol{n})$ seja vazio, significa que qualquer vetor $\boldsymbol{p} \in \mathbb{N}_0^m$ com $p_i = n_i$ e $0 \leqslant p_j \leqslant n_j$ para todo $j \neq i, 1 \leqslant j \leqslant m$ são também lacunas nos pontos $P_1, .., P_m$.*

Se g é o gênero da curva, o Teorema de Riemann-Roch garante que $\boldsymbol{n} \in H(P_1, \ldots, P_m)$ se $\sum_{i=1}^m n_i \geqslant 2g$. Consequentemente, $G(P_1, \ldots, P_m)$ é um conjunto finito. Algumas cotas superiores para $G(P_1, \ldots, P_m)$ têm sido encontradas em termos do gênero g. Por exemplo, em [17, Teorema 3.2], Kim provou que, se a característica do corpo base for zero, então $\#G(P_1, P_2) \leqslant (3g^2+g)/2$ e que a igualdade é satisfeita se, e somente se, a curva for hiperelíptica e P_1 e P_2 forem pontos Weierstrass; em [16, Teorema 3.9] Ishii mostrou que $\#G(P_1, P_2, P_3) \leqslant g(7g^2 + 6g + 5)/6$ e teremos a igualdade se, e somente se, a curva for hiperelíptica e P_1 e P_2 forem pontos Weierstrass.

Definição 2.2.8. *Seja $\boldsymbol{n} \in \mathbb{N}^m$, dizemos que $\boldsymbol{n}$ é uma* lacuna pura *em $P_1, \ldots, P_m$ se $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i)$ para todo $i \in \{1, \ldots, m\}$. Denotamos o conjunto de lacunas em $P_1, \ldots, P_m$ por $G_0(P_1, \ldots, P_m)$*

A noção de lacunas puras foi introduzida por Homma e Kim em [15]. Observe que cada coordenada de uma lacuna pura é necessariamente um inteiro positivo já que $\mathbf{0} \in \nabla_i^m(\boldsymbol{n}_i)$. Em [15] foi provado que $\#G_0(P_1, P_2) \leqslant g(g-1)/2$ e estudadas propriedades interessantes entre lacunas puras e códigos Goppa num ponto.

Lema 2.2.9. *Seja $\boldsymbol{n} \in \mathbb{N}_0^m$. As seguintes afirmações são equivalentes:*

(a) $\boldsymbol{n} \in G_0(P_1, \ldots, P_m)$.

(b) $\nabla_i^m(\boldsymbol{n}) = \varnothing$ *para todo* $i, 1 \leqslant i \leqslant m$.

(c) $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1}^m (n_j - 1)P_j)$.

Demonstração. (a) implica (b). Definição de $G_0(P_1, \ldots, P_m)$ e Lema 2.2.2.
(b) implica (a). Lema 2.2.2 e contra-recíproca do Lema 2.2.3.
(c) implica (a). Para todo $i, 1 \leqslant i \leqslant m$, temos que $\ell(\sum_{j=1}^m (n_j - 1)P_j) \leqslant \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i) \leqslant \ell(\sum_{j=1}^m n_j P_j)$, logo $\ell(\sum_{j=1}^m (n_j - 1)P_j) = \ell(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i) = \ell(\sum_{j=1}^m n_j P_j)$ para todo $i, 1 \leqslant i \leqslant m$. Portanto $\boldsymbol{n} \in G_0(P_1, \ldots, P_m)$.
(a) implica (c). Por contra-recíproca. Seja $f \in \mathcal{L}(\sum_{j=1}^m n_j P_j) \backslash \mathcal{L}(\sum_{j=1}^m (n_j - 1)P_j)$, então existe $i, 1 \leqslant i \leqslant m$ tal que $v_i(f) = -n_i$ e $v_j(f) \geqslant -n_j$ para $j \neq i, 1 \leqslant j \leqslant m$. Logo $f \in \mathcal{L}(\sum_{j=1}^m n_j P_j) \backslash \mathcal{L}(\sum_{j=1, j\neq i}^m n_j P_j + (n_i - 1)P_i)$. Portanto $\boldsymbol{n} \notin G_0(P_1, \ldots, P_m)$.

□

Definição 2.2.10. *A* gonalidade *de $\mathcal{X}$ é o menor inteiro positivo t tal que existe um sistema linear de grau t com dimensão 1.*

Corolário 2.2.11. *Seja $\boldsymbol{n} \in \mathbb{N}_0^m$.*

(a) Se $\boldsymbol{n} \in G_0(P_1, \ldots, P_m)$, então n_i é uma lacuna em P_i para cada $i, 1 \leqslant i \leqslant m$.

(b) Se $\mathbf{1} \in H(P_1, \ldots, P_m)$, então $G_0(P_1, \ldots, P_m) = \varnothing$.

(c) Seja $\boldsymbol{n} \in \mathbb{N}^m$ tal que a gonalidade de $\mathcal{X}$ sobre $\mathbb{F}_q$ é pelo menos $1 + \sum_{i=1}^m n_i$. Então $\boldsymbol{n} \in G_0(P_1, \ldots, P_m)$.

Demonstração. (a) Seja $\boldsymbol{n} \in G_0(P_1, \ldots, P_m)$. Pela Observação 2.2.7, para qualquer vetor $\boldsymbol{p} \in \mathbb{N}_0^m$ com $p_i = n_i$ e $p_j \leqslant n_j$ se $j \neq i, 1 \leqslant j \leqslant m$, se tem que $\boldsymbol{p} \in G(P_1, \ldots, P_m)$. Em particular $(0, \ldots, n_i, \ldots, 0) \in G(P_1, \ldots, P_m)$, logo $n_i \in G(P_i)$ para todo $i, 1 \leqslant j \leqslant m$.

(b) Suponha $\boldsymbol{n} \in G_0(P_1, \ldots, P_m)$ e seja $n_i = \min\{n_j : 1 \leqslant j \leqslant m\}$. Como $\nabla_i^m(\boldsymbol{n}) = \varnothing$ para todo $i, 1 \leqslant i \leqslant m$, o Lema 2.2.9 garante que $(n_i, \ldots, n_i) \in G(P_1, \ldots, P_m)$; consequentemente, a Observação 2.2.7 e o fato que $n_i \geqslant 1$ garantem que $\mathbf{1} \in G(P_1, \ldots, P_m)$, mas isso contradiz nossa hipótese sobre o vetor $\mathbf{1}$.

(c) Seja $D := \sum_{i=1}^m t_i P_i$ tal que a gonalidade de $\mathcal{X}$ é o grau$(D) = t$. Por hipóteses temos que $\sum_{i=1}^m n_i \leqslant \sum_{i=1}^m n_i + 1 \leqslant t$, e dado que $\ell(D) = 1$, nos devemos ter que $\boldsymbol{n} \in G(P_1, \ldots, P_m)$ ou caso contrario teríamos que a gonalidade de $\mathcal{X}$ é $\sum_{j=1}^m n_j$, logo $\ell(\sum_{j=1}^m n_j P_j) = 1$. Como $n_i \geqslant 1$, obtemos que $\ell(\sum_{j=1}^m (n_j - 1)P_j) = 1$, logo $\ell(\sum_{j=1}^m n_j P_j) = \ell(\sum_{j=1}^m (n_j - 1)P_j)$. Portanto $\boldsymbol{n} \in G_0(P_1, \ldots, P_m)$.

□

Exemplo 2.2.12. *[4, Exemplo 2.7] A cota anterior sobre a gonalidade de uma curva no corolário anterior não pode ser melhorada como mostra o seguinte exemplo. Seja $\mathcal{X}$ a curva de Fermat de grau $r \geqslant 2$,*

$$X^r + Y^r + Z^r = 0$$

definida sobre $\mathbb{F}_q$, tal que $char(\mathbb{F}_q)$ não divide r e $\mathcal{X}(\mathbb{F}_q) \neq \varnothing$. É conhecido que a gonalidade de $\mathcal{X}$ sobre $\mathbb{F}_q$ é $r-1$. Suponha que r divide $q-1$ ou r divide $q+1$, então vamos provar que existem $r-1$ pontos $\mathbb{F}_q$-racionais tais que $\mathbf{1} \in \mathbb{N}_0^{r-1}$ pertence ao semigrupo de Weierstrass de tais pontos.

Seja $x := X/Z$ e $y := Y/Z$ funções racionais sobre $\mathcal{X}$. Sejam $b_1, \ldots, b_r$ as raízes de $Y^r + 1 = 0$ e $P_i := (0 : b_1 : 1)$. Então P_i é um ponto $\mathbb{F}_q$-racional de $\mathcal{X}$ para cada $1 \leqslant i \leqslant r$. Segue-se que

$$(x) = \sum_{i=1}^{r} P_i - P_\infty \text{ e } (y - b_i) = rP_i - P_\infty,$$

onde P_∞ é o único ponto no infinito de $\mathcal{X}$. Em particular

$$\left(\frac{y - b_i}{x}\right) = (r-1)P_r - \sum_{i=1}^{r-1} P_i,$$

portanto $\mathbf{1} \in H(P_1 \ldots, P_{r-1})$.

Lema 2.2.13. *Para $\boldsymbol{n}, \boldsymbol{p} \in H(P_1, \ldots, P_m)$, seja $q_i := max\{n_i, p_i\}$ para cada $i, 1 \leqslant i \leqslant m$. Então $\boldsymbol{q} := (q_1, \ldots, q_m) \in H(P_1, \ldots, P_m)$.*

Demonstração. Seja $f, g \in \mathbb{F}_q(\mathcal{X})$ tal que $(f)_\infty = \sum_{i=1}^{m} n_i P_i$ e $(g)_\infty = \sum_{i=1}^{m} p_i P_i$. Para cada $i, 1 \leqslant i \leqslant m$, seja t_i um parâmetro local em P_i e

$$f = a_{i,-n_i} t_j^{-n_i} + \ldots \in \mathbb{F}_q((t_i)),\ g = b_{i,-p_i} t_j^{-p_i} + \ldots \in \mathbb{F}_q((t_i))$$

as representações locais de f e g em P_i. Seja $h = h_{\alpha,\beta} := \alpha f + \beta g$ com $\alpha, \beta \in \mathbb{F}_q$. Então

$$v_i(h) = q_i \text{ se, e somente se, ou } n_i \neq p_i \text{ ou } n_i = p_i \text{ e } \alpha a_{i,-n_i} + \beta b_{i,-p_i} \neq 0. \tag{2.2}$$

A última condição é satisfeita para todo i se $(\alpha, \beta) \in \mathbb{F}_q^2 \setminus \cup_{i=1}^{m} A_i$, onde os A_i são espaços vetoriais de dimensão 1. Dado que $\mathbb{F}_q \geqslant m$, tal (α, β) existe. Portanto tem-se o resultado. □

Corolário 2.2.14. *Seja $\boldsymbol{n} \in \mathbb{N}_0^m$ e $1 \leqslant i \leqslant m$ tais que $\nabla_i^m(\boldsymbol{n}) \neq \varnothing$. Seja $p \in \mathbb{N}_0$ tal que $p < n_i$. Se $\boldsymbol{p} := \boldsymbol{n}_i + p\boldsymbol{e}_i \in H(P_1, \ldots, P_m)$, então $\boldsymbol{n} \in H(P_1, \ldots, P_m)$.*

Demonstração. Existe $\boldsymbol{q} := (q_1, \ldots, q_m) \in H(P_1, \ldots, P_m)$ tal que $q_i = n_i$ e $q_j \leqslant n_j$ para $j \neq i$. Aplicando o Lema 2.2.13 a $\boldsymbol{p}$ e $\boldsymbol{q}$, obtemos o resultado. □

Lema 2.2.15. *Sejam $\boldsymbol{n}, \boldsymbol{p} \in H(P_1, \ldots, P_m)$ e $1 \leqslant j \leqslant m$ tais que $n_j = p_j$. Então existe $\boldsymbol{q} \in H(P_1, \ldots, P_m)$ tal que:*

1. *$q_i = max\{n_i, p_i\}$ se $n_i \neq p_i$ e $i \neq j$, com $1 \leqslant i \leqslant m$.*
2. *$q_i \leqslant n_i$ se $n_i = p_i$ e $i \neq j$, com $1 \leqslant i \leqslant m$.*
3. *$q_j = n_j = 0$ ou $q_j < n_j$.*

Demonstração. Com a notação da demonstração do Lema 2.2.13. Seja $h := b_{j,-p_j} f - a_{j,-n_j} g$ e tome o vetor com coordenadas $q_i := \max\{-v_i(h), 0\}$ para $i = 1, \ldots, m$. □

Corolário 2.2.16. *Sejam $\boldsymbol{n} \in \mathbb{N}_0^m$ e $1 \leqslant i \leqslant m$. Suponha que $\boldsymbol{n}_i \in G(P_1, \ldots, P_m)$ e considere*

$$n := min\{p \in \mathbb{N}_0 : \boldsymbol{n}_i + p\boldsymbol{e}_i \in H(P_1, \ldots, P_m)\}.$$

Então, qualquer vetor $\boldsymbol{p} \in \mathbb{N}_0^m$ com $p_i = n$ e $p_j < n_j$ ou $p_j = n_j = 0$ para $j \neq i, 1 \leqslant j \leqslant m$ também é uma lacuna em $G(P_1, \ldots, P_m)$. Em particular, n é uma lacuna em P_i.

Demonstração. Suponha que existe um vetor $\boldsymbol{p} \in \mathbb{N}_0^m$ com $p_i = n$, $p_j = 0$ ou $p_j < n_j$ para $j \neq i$, com $1 \leqslant j \leqslant m$ tal que $\boldsymbol{p} \in H(P_1, \ldots, P_m)$. Aplicando o Lema 2.2.15 aos vetores $\boldsymbol{p}$ e $\boldsymbol{n}_i + n\boldsymbol{e}_i$, existe $a \in \mathbb{N}_0$ com $a < n$ tal que $\boldsymbol{n}_i + a\boldsymbol{e}_i \in H(P_1, \ldots, P_m)$. Mas isso contradiz a minimalidade de n. □

Corolário 2.2.17. *Sejam $\boldsymbol{n}, i, \boldsymbol{n}_i$ e n como no Corolário 2.2.16. Seja $\boldsymbol{p} \in \mathbb{N}_0^m$ tal que $\boldsymbol{p}_i \in G(P_1, \ldots, P_m)$. Se ou $p_j < n_j$ para todo $j \neq i, 1 \leqslant j \leqslant m$ ou $p_j > n_j$ para todo $j \neq i, 1 \leqslant j \leqslant m$, então*

$$n \neq min\{p \in \mathbb{N}_0 : \boldsymbol{p}_i + p\boldsymbol{e}_i \in H(P_1, \ldots, P_m)\}.$$

Demonstração. Suponha que $n = \min\{p \in \mathbb{N}_0 : \boldsymbol{p}_i + p\boldsymbol{e}_i \in H(P_1, \ldots, P_m)\}$. Então, aplicando o Lema 2.2.15 a $\boldsymbol{n}_i + n\boldsymbol{e}_i$ e $\boldsymbol{p}_i + n\boldsymbol{e}_i$ temos que ou $\boldsymbol{n}_i + q\boldsymbol{e}_i \in H(P_1, \ldots, P_m)$ ou $\boldsymbol{p}_i + q\boldsymbol{e}_i \in H(P_1, \ldots, P_m)$ para algum inteiro positivo $q < n$, contradizendo a escolha de n. □

Para um divisor $D = \sum_{j=1}^m n_j P_j$, a ordem parcial definida em 1.4.1 induz uma ordem parcial $\preceq$ sobre $\mathbb{N}_0^m$, da seguente forma:

$$\boldsymbol{n} \preceq \boldsymbol{p} \Leftrightarrow n_i \leqslant p_i \text{ para todo } 1 \leqslant i \leqslant m.$$

Corolário 2.2.18. *Seja $\boldsymbol{n} \in \mathbb{N}_0^m$ e $1 \leqslant i \leqslant m$ tal que $\boldsymbol{n}$ é um elemento minimal do conjunto $\nabla_i^m(\boldsymbol{n})$ com respeito à ordem parcial $\preceq$. Suponha que $n_i > 0$ e que existe $j \neq i, 1 \leqslant j \leqslant m$, tal que $n_j > 0$. Então*

(a) $\boldsymbol{n}_i \in G(P_1, \ldots, P_m)$.

(b) $n_i := min\{p \in \mathbb{N}_0^m : \boldsymbol{n}_i + p\boldsymbol{e}_i \in H(P_1, \ldots, P_m)\}$; em particular n_i é uma lacuna em P_i

Demonstração. (a) Suponha que $\boldsymbol{n}_i \in H(P_1, \ldots, P_m)$. O Lema 2.2.15 aplicado a $\boldsymbol{n}_i$ e $\boldsymbol{n}$ garante que existe $\boldsymbol{p} \in H(P_1, \ldots, P_m)$ tal que $p_i = n_i$, $p_j < n_j$ e $p_l \leqslant n_l$ para $l \neq i, j$, com $1 \leqslant l \leqslant m$. O último contradiz a minimalidade de $\boldsymbol{n}$.

(b) Por redução ao absurdo, suponha que exista $p < n_i$ tal que $\boldsymbol{n}_i + p\boldsymbol{e}_i \in H(P_1, \ldots, P_m)$. Aplicando o Lema 2.2.15 a $\boldsymbol{n}_i + p\boldsymbol{e}_i$ e $\boldsymbol{n}$, juntamente com a hipótese sobre $j \neq i$, temos que existe $\boldsymbol{q} \in H$ tal que $\boldsymbol{q} \preceq \boldsymbol{n}$ e $\boldsymbol{q} \neq \boldsymbol{n}$ (pois $q_j < n_j$). Isto contradiz a minimalidade de $\boldsymbol{n}$. Portanto $n_i \leqslant p$. Consequentemente, dado que $n_i > 0$ e $\boldsymbol{n} \in H(P_1, \ldots, P_m)$, concluímos que $n_i := \min\{p \in \mathbb{N}_0^m : \boldsymbol{n}_i + p\boldsymbol{e}_i \in H(P_1, \ldots, P_m)\}$. A segunda parte segue-se do Corolário 2.2.16.

□

Lema 2.2.19. *Sejam $\boldsymbol{n}, i, \boldsymbol{n}_i$ e n como no Corolário 2.2.16. Então $\ell(\sum_{j=1}^m n_j P_j + (n - n_i)P_i) \leqslant g + 1$, onde g é o gênero de $\mathcal{X}$*

Demonstração. Se $\sum_{i=1}^m n_j P_j + (n - n_i)P_i$ for um divisor especial, então $\ell(W - (\sum_{i=1}^m n_j P_j + (n - n_i)P_i)) > 0$ para qualquer divisor canônico W. Logo o grau$(\sum_{i=1}^m n_j P_j + (n - n_i)P_i) \leqslant 2g - 2$. Pelo teorema de Clifford obtemos $\ell(\sum_{i=1}^m n_j P_j + (n - n_i)P_i) \leqslant 1 + \frac{1}{2}$grau$(\sum_{i=1}^m n_j P_j + (n - n_i)P_i) \leqslant 1 + \frac{2g-2}{2} = g$.

Se $\sum_{i=1}^{m} n_jP_j + (n-n_i)P_i$ for um divisor não especial, então $\ell(\sum_{i=1}^{m} n_jP_j + (n-n_i)P_i) = \text{grau}(\sum_{i=1}^{m} n_jP_j + (n-n_i)P_i) + 1 - g$. Suponha que $\ell(\sum_{i=1}^{m} n_jP_j + (n-n_i)P_i) \geqslant g+2$, então $\text{grau}(\sum_{i=1}^{m} n_jP_j + (n-n_i)P_i) \geqslant 2g+1$, portanto $\text{grau}(\sum_{i=1}^{m} n_jP_j + (n-n_i-1)P_i - P_j) \geqslant 2g-1$ e pelo teorema de Riemann-Roch $\ell(\sum_{i=1}^{m} n_jP_j + (n-n_i-1)P_i - P_j) = \text{grau}(\sum_{i=1}^{m} n_jP_j + (n-n_i-1)P_i - P_j) + 1 - g$, logo $\ell(\sum_{i=1}^{m} n_jP_j + (n-n_i-1)P_i) = \ell(\sum_{i=1}^{m} n_jP_j + (n-n_i-1)P_i - P_j) + 1$ para todo $j = 1, \ldots, m$. Portanto $\boldsymbol{n}_i + (n-1)\boldsymbol{e}_i \in H$, contradizendo a minimalidade de $\boldsymbol{n}$. □

Observação 2.2.20. *Sejam $m \geqslant 2$ e $i \in \{1, \ldots, m\}$*

(a) Dado que $\ell(\sum_{j=1, j\neq i} n_jP_j) = \ell(\sum_{j=1, j\neq i} n_jP_j - P_i) + 1$, os elementos do semigrupo de Weierstrass em $P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_m$ estão em correspondência injetora com os elementos $\boldsymbol{n}_i \in \mathbb{N}_0^m$ tais que $\boldsymbol{n}_i \in H(P_1, \ldots, P_m)$, respectivamente para lacunas Weierstrass em $P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_m$.

(b) Os Corolários 2.2.16 e 2.2.18 determinam a seguinte função sobrejetora

$$\begin{array}{rccl} \theta_i: & \{\boldsymbol{n}_i \in \mathbb{N}_0^m : \boldsymbol{n}_i \in G(P_1, \ldots, P_m)\} & \to & G(P_i) \\ & \boldsymbol{n}_i & \mapsto & min\{n \in \mathbb{N} : \boldsymbol{n}_i + n\boldsymbol{e}_i \in H(P_1, \ldots, P_m)\}. \end{array}$$

2.3 Conjunto Gerador Minimal

Embora nós saibamos que os elementos do semigrupo de Weierstrass $H(P_1, \ldots, P_m)$ possam ser gerados mediante combinações lineares, essa descrição não resulta ser favorável para descrever um possível conjunto gerador para $H(P_1, \ldots, P_m)$. Assim, o Lema 2.2.13 nos oferece uma alternativa para gerar novos elementos em $H(P_1, \ldots, P_m)$. É neste sentido que, apresentamos, a partir de elementos minimais, como é possível construir um conjunto que gera finitamente o semigrupo de Weierstrass $H(P_1, \ldots, P_m)$. As ideias desta construção foram inicialmente estabelecidas por Kim [17] para o caso $m = 2$ e posteriormente por Matthews [21] para o caso geral.

Proposição 2.3.1. *Seja $\boldsymbol{n} \in \mathbb{N}^m$. As seguintes afirmações são equivalentes:*

(a) $\boldsymbol{n}$ é minimal em $\nabla_i^m(\boldsymbol{n})$ com respeito a $\preceq$ para algum i, $1 \leqslant i \leqslant m$.

(b) $\boldsymbol{n}$ é minimal em $\nabla_i^m(\boldsymbol{n})$ com respeito a $\preceq$ para todo i, $1 \leqslant i \leqslant m$.

Demonstração. Basta só provar (a) implica (b). Suponha que $\boldsymbol{n} \in \mathbb{N}^m$ é minimal em $\nabla_i^m(\boldsymbol{n})$ com respeito a $\preceq$ para algum i, $1 \leqslant i \leqslant m$. Suponha que existe $j \neq i$, $1 \leqslant j \leqslant m$ tal que $\boldsymbol{n}$ não é minimal em $\nabla_j^m(\boldsymbol{n})$. Então existe $\boldsymbol{v} \in H_m$ tal que $\boldsymbol{v} \preceq \boldsymbol{n}, \boldsymbol{v} \neq \boldsymbol{n}$ e $v_j = n_j$. Observe que $v_i < n_i$ pois do contratiro $\boldsymbol{v} \in \nabla_i^m(\boldsymbol{n})$ contradizendo a minimalidade de $\boldsymbol{n}$. Aplicando o Lema 2.2.15 a $\boldsymbol{v}$ e $\boldsymbol{n}$, existe um vetor $\boldsymbol{q} \in H(P_1, \ldots, P_m)$ com $q_i = n_i, q_j < n_j$ e $q_k \leqslant n_k$ para todo $k \neq j, 1 \leqslant k \leqslant m$. Portanto $\boldsymbol{q} \preceq \boldsymbol{n}, \boldsymbol{q} \neq \boldsymbol{n}$ e $\boldsymbol{q} \in \nabla_i^m(\boldsymbol{n})$. Isto contradiz a minimalidade de $\boldsymbol{n}$ em $\nabla_i^m(\boldsymbol{n})$. Portanto $\boldsymbol{n}$ é minimal em $\nabla_i^m(\boldsymbol{n})$ para todo $j, 1 \leqslant j \leqslant m$. □

A partir da proposição anterior, será construído um subconjunto gerador para $H(P_1, \ldots, P_m)$. Para começar, seja $\Gamma_1^+ = H(P_1)$. Para $2 \leqslant l \leqslant m$, definimos

$$\Gamma_l^+ := \{\boldsymbol{n} \in \mathbb{N}^l : \boldsymbol{n} \text{ é minimal em } \nabla_i^l(\boldsymbol{n}) \text{ para algum } i, 1 \leqslant i \leqslant l\}.$$

Como consequência imediata da proposição 2.3.1, tem-se o seguinte resultado.

Lema 2.3.2. *Para $2 \leqslant l \leqslant m$, $\Gamma_l^+ \subseteq G(P_1) \times \cdots \times G(P_l)$.*

Continuando com a construção, a partir dos conjuntos Γ_l^+, serão determinados conjuntos Γ_l, para todo $1 \leqslant l \leqslant m$ da seguinte forma: Para $l = 1$, seja $\Gamma_1 = \Gamma_1^+ = H(P_1)$, para $2 \leqslant l \leqslant m$, seja

$$\Gamma_l := \Gamma_l^+ \cup \left\{ \boldsymbol{n} \in \mathbb{N}_0^l : \begin{array}{c} (n_{i_1}, \ldots, n_{i_k}) \in \Gamma_k^+ \text{ para algum } \{i_1, \ldots, i_m\} = \{1, \ldots, m\} \\ \text{tal que } i_1 < \ldots < i_k \text{ e } n_{i_{k+1}} = \cdots = n_{i_m} = 0 \end{array} \right\}$$

Claramente, Γ_m está determinado por $\{\Gamma_l^+ : 1 \leqslant l \leqslant m\}$.
Dados $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l \in \mathbb{N}_0^m$, definimos a *menor cota superior* de $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l$ por

$$\operatorname{lub}\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l\} = (\max\{u_{1_1}, \ldots, u_{l_1}\}, \ldots, \max\{u_{1_m}, \ldots, u_{l_m}\}) \in \mathbb{N}_0^m$$

Proposição 2.3.3. *Sejam $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l \in H(P_1, \ldots, P_m)$ e $1 \leqslant l \leqslant m$. Então $lub\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l\} \in H(P_1, \ldots, P_m)$.*

Demonstração. Seja $\boldsymbol{q}_2 := \operatorname{lub}\{\boldsymbol{u}_1, \boldsymbol{u}_2\}$. Para $3 \leqslant i \leqslant l$, definimos $\boldsymbol{q}_i := \operatorname{lub}\{\boldsymbol{q}_{i-1}, \boldsymbol{u}_i\}$. De acordo ao Lema 2.2.13, $\boldsymbol{q}_2 \in H(P_1, \ldots, P_m)$. Aplicando repetidamente o Lema 2.2.13 obtemos que $\boldsymbol{q}_i \in H(P_1, \ldots, P_m)$ para todo $i, 2 \leqslant i \leqslant l$. Consequentemente $\boldsymbol{q}_l = \operatorname{lub}\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_l\} \in H(P_1, \ldots, P_m)$. □

O seguinte resultado mostra que Γ_m gera $H(P_1, \ldots, P_m)$.

Teorema 2.3.4. *Se $1 \leqslant m \leqslant \#\mathbb{F}_q$, então*

$$H(P_1, \ldots, P_m) = \{lub\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\} \in \mathbb{N}_0^m : \boldsymbol{u}_1, \ldots, \boldsymbol{u}_m \in \Gamma_m\}.$$

Demonstração. O fato que $\{\operatorname{lub}\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\} \in \mathbb{N}_0^m : \boldsymbol{u}_1, \ldots, \boldsymbol{u}_l \in \Gamma_m\} \subseteq H(P_1, \ldots, P_m)$ segue-se da Proposição 2.3.3.

Suponha que $\boldsymbol{n} \in H(P_1, \ldots, P_m) \backslash \Gamma_m$. Sem perda de generalidade podemos supor que $\boldsymbol{n} \in \mathbb{N}^m$. (De outra forma, existe $(n_{i_1}, \ldots, n_{i_l}) \in \mathbb{N}^l$ para algum $\{i_1, \ldots, i_m\} = \{1, \ldots, m\}$ tal que $i_1 < \cdots < i_l$ e $n_{i_{l+1}} = \cdots = n_{i_m} = 0$ e o mesmo argumento pode se aplicar para $(n_{i_1}, \ldots, n_{i_l})$. Então, de acordo com a Proposição 2.3.1, $\boldsymbol{n}$ não é minimal em $\nabla_i^m(\boldsymbol{n})$ para todo $i, 1 \leqslant i \leqslant m$. Portanto, existe $\boldsymbol{u}_i \in \Gamma_m$ tal que $u_{i_i} = n_i$, $\boldsymbol{u}_i \preceq \boldsymbol{n}$ e $\boldsymbol{u}_i \neq \boldsymbol{n}$ para cada $i, 1 \leqslant i \leqslant m$. Logo $\boldsymbol{n} = \operatorname{lub}\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$, portanto $H(P_1, \ldots, P_m) \subseteq \{\operatorname{lub}\{\boldsymbol{u_1}, \ldots, \boldsymbol{u_m}\} \in \mathbb{N}_0^m : \boldsymbol{u_1}, \ldots, \boldsymbol{u_m} \in \Gamma_m\}$. □

O conjunto Γ_m é comumente chamado de *conjunto gerador minimal*, a motivação principal deste conjunto surgiu pelos estudos feitos por Kim em [17] para o caso $m = 2$.

De acordo com o Teorema 2.3.4 e a definição de Γ_m, o semigrupo de Weierstrass $H(P_1, \ldots, P_m)$ está completamente determinado por $\{\Gamma_l^+ : 1 \leqslant l \leqslant m\}$. Concluímos esta seção com uma caracterização dos elementos de Γ_l^+, $1 \leqslant l \leqslant m$.

Proposição 2.3.5. *Sejam $\boldsymbol{n} \in \mathbb{N}^l$ e $1 \leqslant l \leqslant m$. As seguintes afirmações são equivalentes:*

(a) $\boldsymbol{n} \in \Gamma_l^+$.

(b) $\boldsymbol{n} \in H(P_1, \ldots, P_l)$ *e* $\ell(\sum_{j=1}^l (n_j - 1)P_j) = \ell(\sum_{j=1, j\neq i}^l n_j P_j + (n_i - 1)P_i)$ *para todo* $i, 1 \leqslant i \leqslant l$.

Demonstração. (a) implica (b). Suponha $\boldsymbol{n} \in \Gamma_l^+$. Se $\ell(\sum_{j=1}^l (n_j - 1)P_j) = \ell(\sum_{j=1, j\neq i}^l n_j P_j + (n_i - 1)P_i)$ para algum $i, 1 \leqslant i \leqslant l$, então existe $\boldsymbol{v} \in H(P_1, \ldots, P_l)$ como $\boldsymbol{v} \preceq \boldsymbol{n}$, $v_i \leqslant n_i - 1$ e $v_k = n_k$ para algum $k, 1 \leqslant k \leqslant l$. Mas isto contradiz a minimalidade de $\boldsymbol{n}$ em $\nabla_i^m(\boldsymbol{n})$. Portanto $\ell(\sum_{j=1}^l (n_j - 1)P_j) = \ell(\sum_{j=1, j\neq i}^l n_j P_j + (n_i - 1)P_i)$ para todo $i, 1 \leqslant i \leqslant l$.

(b) implica (a). Suponha $\boldsymbol{n} \in H(P_1, \ldots, P_l)$ e $\ell(\sum_{j=1}^l (n_j - 1)P_j) = \ell(\sum_{j=1, j\neq i}^l n_j P_j + (n_i - 1)P_i)$ para todo $i, 1 \leqslant i \leqslant l$. Isto implica que

$$\mathcal{L}\left(\sum_{j=2}^l n_j P_j + (n_1 - 1)P_1\right) = \mathcal{L}\left(\sum_{j=1}^l (n_j - 1)P_j\right) = \mathcal{L}\left(\sum_{\substack{j=1, \\ j\neq i}}^l n_j P_j + (n_i - 1)P_i\right)$$

para todo $i, 1 \leqslant i \leqslant l$. Se $\boldsymbol{n} \notin \Gamma_l^+$, então existe $\boldsymbol{u} \in H(P_1, \ldots, P_l)$ com $u_1 = n_1, \boldsymbol{u} \preceq \boldsymbol{n}$ e $\boldsymbol{u} \neq \boldsymbol{n}$. Em particular $u_i < n_i$ para algum $i, 2 \leqslant i \leqslant l$. Assim, existe uma função racional $f \in \mathcal{L}(\sum_{j=1, j\neq i}^{l} n_j P_j + (n_i - 1)P_i)$ tal que $f \notin \mathcal{L}(\sum_{j=2}^{l} n_j P_j + (n_1 - 1)P_1)$, contradizendo a hipótese.

□

Capítulo 3

Semigrupo de Weierstrass na Curva Hermitiana

Neste capítulo, usaremos os resultados obtidos na Seção 2.3 para calcular o conjunto gerador minimal do semigrupo de Weierstrass em m pontos para a curva *Hermitiana* definida pela equação afim $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$. As ideais aqui desenvolvidas são principalmente devidas a Matthews e podem ser encontradas em [20] e [21]. Na Seção 3.1, vamos nos concentrar no caso $m = 2$ e, subsequentemente, na Seção 3.2 estenderemos esses resultados para um caso mais geral.

3.1 Semigrupo de Weierstrass em Dois Pontos da Curva Hermitiana

Seja $\mathcal{X}$ a curva Hermitiana definida pela equação afim $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$. A curva Hermitiana é um curva com $q^3 + 1$ pontos racionais, o que faz dela uma curva maximal, já que atinge a cota de Hasse-Weil, e cujos pontos Weierstrass são exatamente seus pontos $\mathbb{F}_{q^2}$-racionais, veja [9]. Denotamos por $P_\infty := (0 : 1 : 0)$ o ponto no infinito em $\mathcal{X}$ e $P_{ab} := (a : b : 1)$ o zero em comum das funções racionais $x - a$ e $y - b$. Os divisores principais de x e y são:

$$(x) = \sum_{\substack{b \in \mathbb{F}_{q^2} \\ b^q + b = 0}} P_{0b} - qP_\infty \quad e \quad (y) = (q+1)(P_{00} - P_\infty).$$

A partir das funções x e y, e o fato do gênero de $\mathcal{X}$ ser igual a $g = q(q-1)/2$, obtém-se o seguinte resultado.

Teorema 3.1.1. *[9, Theorem 3] O semigrupo de Weierstrass para qualquer ponto $\mathbb{F}_{q^2}$-racional sobre a curva hermitiana é dado por $\langle q, q+1 \rangle$, ou seja,*

$$H(P_\infty) = H(P_{ab}) = \langle q, q+1 \rangle.$$

Como consequência do resultado anterior, o conjunto de lacunas para qualquer ponto $\mathbb{F}_{q^2}$-racional sobre $\mathcal{X}$ é dado por:

$$\begin{array}{cccccc} 1 & 2 & \dots & q-2 & q-1 \\ (q+1)+1 & (q+1)+2 & \dots & (q+1)+(q+2) & & \\ \vdots & \vdots & \iddots & & & \\ (q-3)(q+1)+1 & (q-3)(q+1)+2 & & & & \\ (q-2)(q+1)+1. & & & & & \end{array} \tag{3.1}$$

Esses elementos podem ser descritos da seguinte forma.

Se n é uma lacuna para algum ponto $\mathbb{F}_{q^2}$-racional sobre $\mathcal{X}$, então existem únicos $t, j \in \mathbb{N}$ tais que $n = (t-j)(q+1)+j$ com $1 \leqslant j \leqslant t \leqslant q-1$. Uma demonstração deste fato pode ser obtida a partir da seguinte proposição.

Proposição 3.1.2. *[24, Lema 1] Seja $n \in \mathbb{Z}$. Então $n \notin \langle m, p\rangle$ se, e somente se, existem $j, t \in \mathbb{N}$ tais que $n = mp - jm - tp$.*

Observação 3.1.3. *No diagrama (3.1), considere as diagonais na direção $\nearrow$. Se rotularmos as colunas e as diagonais de 1 ate $q-1$, percorrendo as colunas da esquerda para a direita e as diagonais a partir do canto superior esquerdo, o elemento $n = (t-j)(q+1)+j$ está localizado entre a j-ésima coluna e a t-ésima diagonal.*

Antes de calcular o semigrupo de Weierstrass para dois pontos racionais distintos sobre a curva Hermitiana, precisamo fazer alguns comentários.

Na Observação 2.2.20 (b), vimos que para o caso de vários pontos existe uma correspondência sobrejetora θ_i entre os conjuntos $\{\boldsymbol{n}_i \in \mathbb{N}_0^m : \boldsymbol{n}_i \in G(P_1, \ldots, P_m)\}$ e $G(P_i)$. Para o caso $m = 2$, a função θ_i permite determinar uma função bijetora entre os conjuntos $G(P_1)$ e $G(P_2)$ da seguinte forma: Considere a função

$$\begin{array}{rccc} \gamma: & G(P_1) & \to & G(P_1, P_2) \\ & n & \mapsto & (n, 0) \end{array}$$

O Corolário 2.2.18 garante que γ está bem definida. Definimos agora $\beta := \theta_2 \circ \gamma$

$$\begin{array}{rccl} \beta: & G(P_1) & \to & G(P_2) \\ & n & \mapsto & \beta_n := \min\{p \in \mathbb{N} : (n, p) \in H(P_1, P_2)\}. \end{array}$$

A injetividade de γ e a sobrejetividade de θ_2 garantem que a função β é uma bijeção entre $G(P_1)$ e $G(P_2)$, portanto $G(P_2) = \{\beta_n : n \in G(P_1)\}$ e, ainda mais, $n = \min\{p \in \mathbb{N} : (p, \beta_n) \in H(P_1, P_2)\}$. Se indexamos as lacunas em P_1 e as lacunas em P_2 com o conjunto $\{1, \ldots, g\}$ então, a função β implica a existência de uma permutação σ do conjunto $\{1, \ldots, g\}$ tal que $\beta_{n_i} = \beta_{\sigma(i)}$ para todo $1 \leqslant i \leqslant g$. Denotamos por $\Gamma(P_1, P_2)$ o grafo de β, isso é

$$\Gamma(P_1, P_2) := \{(n_i, \beta_{\sigma(i)}) : 1 \leqslant i \leqslant g\} = \{(n, \beta_n) : n \in G(P_1)\}.$$

Observe que o conjunto $\Gamma(P_1, P_2)$ coincide com a noção de Γ_2^+.

Proposição 3.1.4. *[23, Lema 2] Se existe uma permutação τ de $\{1, \ldots, g\}$ tal que $\{(n_i, \beta_{\tau(i)}) \in G(P_1) \times G(P_2) \cap H(P_1, P_2) : 1 \leqslant i \leqslant g\}$, então $\Gamma(P_1, P_2) = \{(n_i, \beta_{\tau(i)}) \in G(P_1) \times G(P_2) \cap H(P_1, P_2) : 1 \leqslant i \leqslant g\}$.*

De acordo com a função β, mencionada anteriormente, podemos apresentar o seguinte resultado:

Teorema 3.1.5. *Sejam P_1 e P_2 pontos Weierstrass distintos sobre a curva Hermitiana $y^q + y = x^{q+1}$ definida sobre $\mathbb{F}_{q^2}$, então*

$$\beta_{(t-j)(q+1)+j} = (q-t-1)(q+1)+j$$

para $1 \leqslant j \leqslant t \leqslant q-1$.

Demonstração. Para começar, vamos supor que $P_1 = P_{00}$ e $P_2 = P_\infty$. Segundo a Proposição 3.1.4, basta procurar uma permutação τ de $\{1, \ldots, g\}$ tal que $\{(n_i, \beta_{\tau_i}) : 1 \leqslant i \leqslant g\} \subseteq G(P_1) \times G(P_2) \cap H(P_1, P_2)$. Considere o divisor

$$\left(\frac{x^{q-j+1}}{y^{t-j+1}}\right)_\infty = ((t-j)(q+1)+j)P_1 + ((q-t-1)(q+1)+j)P_2,$$

com $1 \leqslant j \leqslant t \leqslant q-1$. Portanto, $((t-j)(q+1)+j, (q-t-1)(q+1)+j) \in H(P_1,P_2)$. Note também que $(q-t-1)(q+1)+j \in G(P_2)$. Consequentemente, $\Gamma(P_1,P_2) = \{((t-j)(q+1)+j, (q-t-1)(q+1)+j) : 1 \leqslant j \leqslant t \leqslant q-1\}$, o que prova o teorema para o caso $P_1 = P_{00}$ e $P_2 = P_\infty$.

Agora, suponha que $P_1 = P_{ab}$ com $P_{ab} \neq P_{00}$ e $P_2 = P_\infty$. Existe um automorfismo φ que fixa P_∞ e leva P_{ab} em P_{00} [20]. Então podemos usar a função racional $\frac{x^{q-j+1}}{y^{t-j+1}} \circ \varphi$ para calcular $\beta_{(t-j)(q+1)+j}$ como no caso anterior.

Novamente, suponha que $P_1 = P_{ab}$ e $P_2 = P_{cd}$, onde $P_{ab} \neq P_{cd}$. Existe um automorfismo ϕ que fixa P_{ab} e leva P_{cd} em P_∞ [20]. Então, como foi feito anteriormente, podemos usar a função racional $\frac{x^{q-j+1}}{y^{t-j+1}} \circ \phi$ para calcular a função β. □

Em concordância com o Teorema 3.1.5, podemos dizer que, para qualquer dois ponto P_1 e P_2 sobre a curva Hermitiana $\mathcal{X}$

$$\Gamma_2^+ := \left\{((t_1-j)(q+1)+j, (t_2-j)(q+1)+j) : \begin{array}{l} 1 \leqslant j \leqslant t_1, t_2 \leqslant q-1, \\ t_1+t_2 = q+j-1 \end{array}\right\}. \tag{3.2}$$

Neste caso, o semigrupo de Weierstrass $H(P_1,P_2)$ está gerado por:

$$\Gamma_2 = \{(n,0) : n \in H(P_\infty)\} \cup \{(0,n) : n \in H(P_\infty)\} \cup \Gamma_2^+.$$

A partir do Teorema 3.1.5, pode ser calculado a cardinalidade de $G(P_1,P_2)$, para isso vamos precisar do seguinte resultado:

Lema 3.1.6. *[14, Teorema 1] Sejam P_1 e P_2 pontos distintos sobre uma curva de gênero $g > 1$. Então*

$$\#G(P_1,P_2) = \sum_{n \in G(P_1)} n + \sum_{m \in G(P_2)} m - \#r(P_1,P_2),$$

onde $r(P_1,P_2) = \{(n,m) \in G(P_1) \times G(P_2) : n < m \text{ e } \beta_n > \beta_m\}$.

Teorema 3.1.7. *Sejam P_1 e P_2 pontos Weierstrass distintos sobre a curva Hermitiana $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$. Então*

$$\#G(P_1,P_2) = \frac{q}{12}(3q^3 - 4q^2 + 3q - 2).$$

Demonstração. Pelo Teorema 3.1.5, temos que:

$$\begin{aligned} \sum_{n \in G(P_1)} n = \sum_{m \in G(P_2)} m &= \sum_{t=1}^{q-1} \sum_{j=1}^{t} (q-t-1)(q+1)+j \\ &= \sum_{t=1}^{q-1} tq^2 - t^2q - t^2 - t + \frac{t(t+1)}{2} \\ &= \frac{1}{6}(q^4 - q^3 - q^2 + q). \end{aligned}$$

Agora, calcularemos $\#r(P_1,P_2)$. Fixados $1 \leqslant j \leqslant t \leqslant q-1$, queremos contar todos os pares (t',j') tais que

$$(t-j)(q+1)+j < (t'-j')(q+1)+j' \tag{3.3}$$

e

$$\beta_{(t-j)(q+1)+j} > \beta_{(t'-j')(q+1)+j'}.$$

Note que $\beta_{(t-j)(q+1)+j} > \beta_{(t'-j')(q+1)+j'}$ é equivalente a

$$(t'-t)(q+1) > j'-j. \tag{3.4}$$

Primeiro, considere o caso $t = t'$. Portanto $(t'-t)(q+1) = 0$, a fim de satisfazer (3.4), deve-se ter que $j > j'$. Portanto existem $j-1$ pares que satisfazem (3.3) e (3.4).

Agora suponha que $t > t'$. Então $(t'-t)(q+1) < 0$. Portanto, para satisfazer (3.4), j' deve satisfazer $j' < j$. Não obstante, $j'-j \geqslant -q+2$ pois $1 \leqslant j, j' \leqslant q-1$ e dado que $1 \leqslant t, t' \leqslant q-1$, obtemos que $(t'-t)(q+1) \leqslant -q^2-q$ o que implica que não pode ser satisfeito (3.4).

Resta considerar o caso $t' > t$. Aqui, (3.4) sempre é satisfeita já que $j'-j \leqslant q-2 < (t'-t)(q+1)$. Se $j' \leqslant j$, então $tq+t-jq < t'q+t'-j'q$ e portanto (3.3) é satisfeita também. Se $j' \geqslant j$, então (3.3) é satisfeita somente se $t-j < t'-j'$. O número de pares com $t' > t$ que satisfazem (3.3) e (3.4) é $\sum_{i=t+1}^{q-1} i - (t-j)(q-1-t)$.

Assim,

$$\begin{aligned}
\#r(P_1,P_2) &= \sum_{t=1}^{q-1}\sum_{j=1}^{t}(t-j+\sum_{i=t+1}^{q-1} i-(t-j)(q-1-t)) \\
&= \sum_{t=1}^{q-1}\sum_{j=1}^{t} t-j+\frac{q(q-1)}{2}-\frac{t(t+1)}{2}-tq+t+t^2+jq-j-jt \\
&= \sum_{t=1}^{q-1}\sum_{j=1}^{t} \frac{q^2}{2}-\frac{q}{2}-\frac{t^2}{2}-\frac{t}{2}-tq+2t+t^2+jq-2j-jt \\
&= \sum_{t=1}^{q-1} t\left(\frac{q^2}{2}-1\right)-t^2\frac{q}{2} \\
&= \left(\frac{q^2}{2}-1\right)\left(\frac{q(q-1)}{2}\right)-\frac{q}{2}\left(\frac{q(q-1)(2q-1)}{6}\right) \\
&= \frac{q}{12}(q^3-7q+6).
\end{aligned}$$

Portanto,

$$\begin{aligned}
\#G(P_1,P_2) &= \sum_{n\in G(P_1)} n+\sum_{m\in G(P_2)} m-\#r(P_1,P_2) \\
&= \frac{1}{3}(q^4-q^3-q^2+q)-\frac{q}{12}(q^3-7q+6) \\
&= \frac{1}{12}(3q^4-4q^3+3q^2-2q).
\end{aligned}$$

□

Na verdade, o Teorema 3.1.5 nos permite, não somente calcular a cardinalidade de $G(P_1,P_2)$, mas também determinar o conjunto $G(P_1,P_2)$. Para começar, vamos fixar a seguinte notação: Para $a, b \in \mathbb{N}_0$, escrevemos o intervalo $[a,b]$ como $\{c \in \mathbb{N}_0 : a \leqslant c \leqslant b\}$ e $[a,b]\times[s,t]$ para denotar $\{\boldsymbol{n} \in \mathbb{N}_0^2 : a \leqslant n_1 \leqslant b \text{ e } s \leqslant n_2 \leqslant t\}$.

Seja $S = \{\boldsymbol{n} \in \mathbb{N}_0^2 : n_1 + n_2 \leqslant 2g-1\}$, portanto $G(P_1, P_2) \subseteq S$. Considere $q-1 \in G(P_1)$. Pelo Teorema 3.1.5, $\beta_{q-1} = q-1$. Dado que $(0,q), (0,q+1) \in H(P_1,P_2)$, podemos aplicar o Lema 2.2.13 para obter $(q-1,q), (q-1,q+1) \in H(P_1,P_2)$. Aplicando novamente o Lema 2.2.13 temos $(q,q), (q,q+1), (q+1,q), (q+1,q+1) \in H(P_1,P_2)$. Assim, o bloco $B_{q-1} = [q-1,q+1]\times[q-1,q+1] \subseteq H(P_1,P_2)$. Agora considere $q-2 \in G(P_1)$, logo $\beta_{q-2} = 2q-1$. Dado que B_{q-1} estão contidos em $H(P_1,P_2)$ e $(q-2,2q-1), (0,2q), (0,2q+1), (0,2q+2) \in H(P_1,P_2)$, o bloco de tamanho 4×4 $B_{q-2} = [q-2,q+1]\times[2q-1,2q+2] \subseteq H(P_1,P_2)$.

Prosseguindo com o processo acima, cada lacuna em P_1 da forma $n = q-i, 1 \leqslant i \leqslant q-3$ gera um bloco B_n de tamanho $(i+2)\times(i+2)$.

Considere agora $2 \in G(P_1)$. Do Teorema 3.1.5, temos $\beta_2 = q^2-2q-1$. Aplicando o Lema 2.2.13 como foi feito anteriormente, temo um "triângulo" B_2 com $q(q-1)/2$ elementos em $H(P_1,P_2)\cap S$. Finalmente, como $\beta_1 = 2g-1$ e $(1,2g-1) \notin S$, não precisamos considerar β_1.

Dando prosseguimento, considere β_n para qualquer lacuna n em P_1 que não esteja na primeira coluna do diagrama (3.1). Para $n = (t-j)(q+1)+j \in G(P_1), 3 \leqslant j \leqslant t \leqslant q-1$, temos um bloco $B_n \subseteq H(P_1,P_2)\cap S$. Para $n = (t-2)(q+1)+2 \in G(P_1), 2 \leqslant t \leqslant q-1$, chegamos em um "triângulo" B_n contido em $S \cap H(P_1,P_2)$ com $q(q-1)/2$ elementos. Então, de acordo com a noção de Γ_2^+ e o Teorema 2.3.4, todos os elementos de $S\cap\mathbb{N}_0^2$ que não estejam em algum bloco B_n para algum $n \in G(P_1)$ são lacunas nos pontos P_1 e P_2.

Teorema 3.1.8. *Sejam P_1 e P_2 dois pontos Weierstrass distintos sobre a curva Hermitiana $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$. Então o conjunto e lacunas em P_1 e P_2 é*

$$G(P_1,P_2) = S\backslash[H(P_1)\times\{0\} \cup \{0\}\times H(P_2) \cup \{B_n : n = (t-j)(q+1)+j, 2 \leqslant j \leqslant t \leqslant q-1\}].$$

Baseados nestes resultados Homman e Kim calculam $G_0(P_1,P_2)$ para qualquer par de pontos P_1 e P_2 sobre uma curva Hermitiana [15, Proposição 4.2].

Exemplo 3.1.9. *Seja $\mathcal{X}$ a curva Hermitiana definida por $y^5+y = x^6$ sobre $\mathbb{F}_{5^2}$. Dado $P \in \mathcal{X}$ $\mathbb{F}_{5^2}$-racional, temos que o conjunto de lacunas em P é:*

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 7 & 8 & 9 & \\ 13 & 14 & & \\ 19 & & & \end{array}$$

Segundo o Teorema 3.1.5, para qualquer dois pontos $\mathbb{F}_{5^2}$-racional distintos P_1 e P_2 em $\mathcal{X}$, temos que

$$\Gamma_2^+ = \{(1,19),(7,13),(2,14),(13,7),(8,8),(3,9),(19,1),(14,2),(9,3),(4,4)\}.$$

Vamos aplicar o Lema 2.2.13 para calcular os blocos e "triângulos" correspondentes para cada lacuna n. Na primeira iteração temos: os blocos $B_4 = [4,6]\times[4,6], B_3 = [3,6]\times[9,12]$ e o "triângulo" B_2 definido pelos vértices $(2,14),(5,14)$ e $(2,17)$; na segunda iteração, obtemos o bloco $B_9 = [9,12]\times[3,6]$ e o " triângulo" B_8 definido pelos vértices $(8,8),(8,11)$ e $(11,8)$ e, finalmente, na terceira iteração, temos o "triângulo" B_{14} com vértices em $(14,2),(14,5)$ e $(17,2)$.

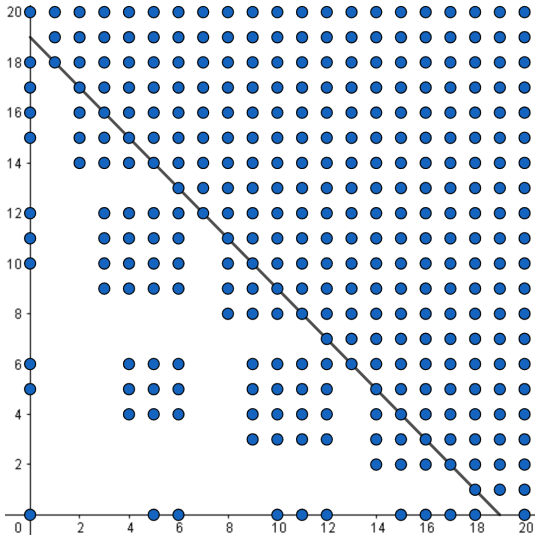

Figura 3.1:

Os pontos na Figura 3.1, representam os elementos do semigrupo de Weierstrass $H(P_1, P_2)$ sobre dois pontos da curva Hermitiana $y^5 + y = x^6$ definida em $\mathbb{F}_{5^2}$ sobre a regão $\{(n_1, n_2) \in \mathbb{N}_0^2 : 0 \leqslant n_1, n_2 \leqslant 20\}$. Os pontos não marcados no gráfico são lacunas em P_1 e P_2. O segmento no gráfico, está definida pela equação $x + y = 19$ com $0 \leqslant x, y \leqslant 19$.

3.2 Semigrupo de Weierstrass em $m$ontos Colineares sobre a Curva Hermitiana

Novamente, seja $\mathcal{X}$ a curva hermitiana definida pela $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$. Nesta seção, vamos calcular o semigrupo de Weierstrass em vários pontos da curva $\mathcal{X}$. Para isso, precisamos fixar algumas ideias.

Para cada $a \in \mathbb{F}_{q^2}$, existem q elementos $b_2, b_3, \ldots, b_{q+1} \in \mathbb{F}_{q^2}$ tais que $b_i^q + b_i = a^{q+1}$ para todo $2 \leqslant i \leqslant q+1$ [25, Lema 6.4.4]. Seja P_{ab} o zero em comum de $x - a$ e $y - b$ e P_∞ o ponto no infinito em $\mathcal{X}$. Considere a notação seguinte $P_1 = P_\infty, P_2 = P_{ab_2}, P_3 = P_{ab_3}, \ldots, P_{q+1} = P_{ab_{q+1}}$. Para $1 \leqslant m \leqslant q+1$, seja $H(P_1, \ldots, P_m)$.

Como na seção anterior, os divisores principais para $x - a$ e y são

$$(x - a) = \sum_{i=2}^{q+1} P_{ab_i} - qP_\infty \quad \text{e} \quad (y) = (q+1)(P_{00} - P_\infty)$$

Considere também, para $2 \leqslant i \leqslant q+1$ as funções racionais $h_{ab_i} := y - b_i - a^q(x - a)$. Segundo [19], o divisor principal de h_{ab_i} é

$$(h_{ab_i}) = (q+1)(P_{ab_i} - P_\infty).$$

Para determinar o semigrupo de Weierstrass sobre os pontos $P_1, P_2, \ldots, P_m$, precisamos estabelecer $\Gamma_m, 1 \leqslant m \leqslant q+1$. Para isso, vamos determinar os conjuntos $\Gamma_l^+, 1 \leqslant l \leqslant m$.

Por definição $\Gamma_1^+ = H(P_1)$. O caso Γ_2^+ foi descrito em (3.2).

Para determinar $\Gamma_m^+, 3 \leqslant m \leqslant q+1$, devemos considerar a seguinte notação: Dados $1 \leqslant m \leqslant q+1$, $\boldsymbol{t} \in \mathbb{N}^m$ e $j \in \mathbb{N}$, definimos

$$\boldsymbol{n}_{\boldsymbol{t},j} := ((t_1 - j)(q+1) + j, (t_2 - j)(q+1) + j, \ldots, (t_m - j)(q+1) + j) \in \mathbb{N}_0^m.$$

Note que, se $1 \leqslant j \leqslant t_i \leqslant q-1$ para todo $1 \leqslant i \leqslant m$, então

$$\boldsymbol{n}_{\boldsymbol{t},j} \in G(P_1) \times \cdots \times G(P_m).$$

Procuramos que o conjunto formado pelos $\boldsymbol{n}_{\boldsymbol{t},j}$ realmente determinam o conjunto gerador minimal para o semigrupo de Weierstrass $H(P_1, \ldots, P_m)$.

Teorema 3.2.1. *Sejam $a \in \mathbb{F}_{q^2}$ e $P_1 = P_\infty, P_2 = P_{ab_2}, P_3 = P_{ab_3}, \ldots, P_{q+1} = P_{ab_{q+1}}$, $q+1$ distintos pontos $\mathbb{F}_{q^2}-$racionais sobre a curva Hermitiana $\mathcal{X}$ definida pela equação $y^q + y = x^{q+1}$. Para $2 \leqslant m \leqslant q+1$,*

$$\Gamma_m^+ = \left\{ \boldsymbol{n}_{\boldsymbol{t},j} \in \mathbb{N}^m : \begin{array}{l} \sum_{i=1}^m t_i = q + (m-1)(j-1), \\ 1 \leqslant j \leqslant t_i \leqslant q-1 \text{ para todo } 1 \leqslant i \leqslant m \end{array} \right\}.$$

Em particular, o semigrupo de Weierstrass $H(P_1, \ldots, P_m)$ é gerado por

$$\left\{ \boldsymbol{n} \in \mathbb{N}_0^m : \begin{array}{l} (n_{i_1}, \ldots, n_{i_l}) = \boldsymbol{n}_{\boldsymbol{t},j} \in \Gamma_l^+ \text{ e } n_{i_{l+1}} = \cdots = n_{i_m} = 0 \\ \text{para } l \in \mathbb{N} \text{ e } \{i_1, \ldots, i_m\} = \{1, \ldots, m\} \end{array} \right\}.$$

A demonstração do teorema 3.2.1, é um prova por indução sobre m. Devido a sua extensão, a prova deste teorema será dividida em duas grandes etapas, que por sua vez, serão desmembradas numa série de lemas técnicos. A primeira destas etapas, procura mostrar que $S_m \subseteq \Gamma_m^+$, subsequentemente, na segunda etapa, será provado que $\Gamma_n^+ \subseteq S_m$.

Para começar, vamos estabelecer uma notação. Para $2 \leqslant m \leqslant q+1$ considere o conjunto

$$S_m := \left\{ \boldsymbol{n}_{\boldsymbol{t},j} \in \mathbb{N}^m : \begin{array}{l} \sum_{i=1}^m t_i = q + (m-1)(j-1), \\ 1 \leqslant j \leqslant t_i \leqslant q-1 \text{ para todo } 1 \leqslant i \leqslant m \end{array} \right\}.$$

Para $2 \leqslant i \leqslant q+1$, seja $h_i := h_{ab_i} \in \mathbb{F}_{q^2}(\mathcal{X})$ como anteriormente se definiu, portanto

$$(h_i) = (q+1)(P_i - P_1).$$

***Etapa número* 1**.

Lema 3.2.2. *Seja $\boldsymbol{n}_{\boldsymbol{t},j} \in \mathbb{N}^m$ tal que $\sum_{i=1}^m t_i = q + (m-1)(j-1)$ e $1 \leqslant j \leqslant t_i \leqslant q-1$ para todo $1 \leqslant i \leqslant m$. Suponha $\boldsymbol{u} \in \mathbb{N}_0^m$ tal que:*

(a) $\boldsymbol{u} \preceq \boldsymbol{n}_{\boldsymbol{t},j}$.

(b) $u_1 = (t_1 - j)(q+1) + j$.

(c) Existe $k \in \mathbb{N}, k \geqslant 1$ tal que $j > k$ e $u_m = (t_m - j)(q+1) + j - k$.

Então, os vetores

$$\boldsymbol{v} := ((t_1 + t_m - j - k)(q+1) + k, v_2, \ldots, v_{m-1}) \in \mathbb{N}_0^{m-1},$$

e

$$\boldsymbol{w} := \boldsymbol{n}_{(t_1+t_m-j, t_2-j+1+k, t_3-j+k, \ldots, t_{m-1}-j+k), k} \in \mathbb{N}_0^{m-1}$$

satisfazem que $\boldsymbol{v} \preceq \boldsymbol{w}$ e $\boldsymbol{v} \neq \boldsymbol{w}$ e $\boldsymbol{w} \in S_{m-1}$, onde $v_i = max\{u_i - (j-k), 0\}$ para $2 \leqslant i \leqslant m-1$.

Demonstração. Note que

$$\boldsymbol{v} \preceq \boldsymbol{w} \text{ e } \boldsymbol{v} \neq \boldsymbol{w},$$

pois $w_1 = (t_1+t_m-j-k)(q+1)+k = v_1$, $w_2 = (t_2-j+1)(q+1)+k > (t_2-j)(q+1)+j-(j-k) \geqslant u_2-(j-k)$, e $w_i = (t_i-j)(q+1)+k = (t_i-j)(q+1)+j-(j-k) \geqslant u_i-(j-k)$ para $3 \leqslant i \leqslant m-1$.

Além,

$$\boldsymbol{w} \in S_{m-1},$$

dado que $t_1+t_m-j+t_2-j+1+k+\sum_{i=3}^{m-1}(t_i-j+k) = \sum_{i=1}^{m} t_i-2j+1+k-j\sum_{i=3}^{m-1}1+k\sum_{i=3}^{m-1}1 = q+(m-1)(j-1)-2j+1+k-j(m-3)+k(m-3) = q+(m-1)(j-1)-j(m-1)+k(m-2)+1 = q+k(m-2)-(m-1)+1 = q+(k-1)(m-2)$, como $j > k$, $k \leqslant t_2-j+1+k \leqslant t_2 \leqslant q-1, k \leqslant t_i-j+k \leqslant t_i \leqslant q-1$ para $3 \leqslant i \leqslant m-1$, e $k \leqslant j \leqslant t_1+t_m-j = \sum_{i=1}^{m} t_i - \sum_{i=2}^{m-1} t_i - j \leqslant q+(m-1)(j-1)-(m-2)(j-1)-j = q+(j-1)-j = q-1$. □

Lema 3.2.3. *Seja $m \geqslant 3$ e $\boldsymbol{n}_{\boldsymbol{t},j} \in \mathbb{N}^m$ tal que $\sum_{i=1}^{m} t_i = q+(m-1)(j-1)$ e $1 \leqslant j \leqslant t_i \leqslant q-1$ para todo $1 \leqslant i \leqslant m$. Suponha $\boldsymbol{u} \in \mathbb{N}_0^m$ tal que:*

(a) $\boldsymbol{u} \preceq \boldsymbol{n}_{\boldsymbol{t},j}$.

(b) $u_1 = (t_1-j)(q+1)+j$.

(c) Existe $k \in \mathbb{N}, k \geqslant 1$ tal que $j \leqslant k$ e $u_m = (t_m-j)(q+1)+j-k$.

Então, para o vetor

$$\boldsymbol{v} := ((t_1+t_m-2j)(q+1)+j, u_2, \ldots, u_{m-1}) \in \mathbb{N}_0^{m-1},$$

existe $2 \leqslant i \leqslant m-1$ tal que o vetor

$$\boldsymbol{w} := \boldsymbol{n}_{(t_1+t_m-j,t_2,t_3\ldots,t_{i-1},t_i+1,t_{i+1},\ldots,\ldots,t_{m-1}),j} \in \mathbb{N}_0^{m-1},$$

satisfaz $\boldsymbol{v} \preceq \boldsymbol{w}$ e $\boldsymbol{v} \neq \boldsymbol{w}$ e $\boldsymbol{w} \in S_{m-1}$.

Demonstração. Note que existe $i, 2 \leqslant i \leqslant m-1$, tal que $t_i < q-1$, pois, caso contrário, teríamos que, para todo $1 \leqslant i \leqslant q-1, t_i = q-1$, logo

$$\begin{aligned} 2j < t_1+t_m &= \textstyle\sum_{i=1}^{m} t_i - \sum_{i=2}^{m-1} t_i \\ &= q+(m-1)(j-1)-(q-1)\textstyle\sum_{i=2}^{m-1}1 \\ &= q+(m-1)(j-1)-(q-1)(m-2), \end{aligned}$$

em seguida

$$\begin{aligned} 2j-(m-1)j &\leqslant q-(m-1)-(m-2)q+(m-2) \\ -j(m-3) &\leqslant q-1-(m-2)q \\ -j(m-3) &\leqslant -q(m-3)-1 \\ (q-j)(m-3) &\leqslant -1. \end{aligned}$$

A desigualdade anterior somente é satisfeita se $m < 3$, o que contradiz nossa hipóteses sobre m. Portanto, existe $i, 2 \leqslant i \leqslant m-1$ com $t_i < q-1$. Sem perda de generalidade, podemos supor que $i = 2$, Considere o vetor

$$\boldsymbol{w} := \boldsymbol{n}_{(t_1+t_m-j,t_2+1,t_3,\ldots,t_{m-1}),j}.$$

Note que

$$\boldsymbol{v} \preceq \boldsymbol{w} \text{ e } \boldsymbol{v} \neq \boldsymbol{w},$$

pois $w_1 = (t_1+t_m-2j)(q+1)+j = v_1$, $w_2 = (t_2+1-j)(q+1)+j > (t_2-j)(q+1)+j \geqslant v_2 = u_2$, e $w_i = (t_i-j)(q+1)+j \geqslant u_i = v_i$, para todo $3 \leqslant i \leqslant m-1$.

Note também que

$$\boldsymbol{w} \in S_{m-1}$$

pois $j \leqslant t_1+t_m-j \leqslant q-1$, $(t_1+t_m-j)+(t_2+1)+\sum_{i=3}^{m-1} t_i = \sum_{i=1}^{m} t_i - j + 1 = q+(m-2)(j-1)$, $j \leqslant t_2 \leqslant t_2+1 \leqslant q-1$, e $j \leqslant t_i \leqslant q-1$, para todo $i, 3 \leqslant i \leqslant m-1$. □

Proposição 3.2.4. *Para* $2 \leqslant m \leqslant q+1$, $S_m \subseteq \Gamma_m^+$.

Demonstração. Vamos provar que $S_m \subseteq \Gamma_m^+$ por indução sobre m. Por (3.2) temos

$$\Gamma_2^+ = \{\boldsymbol{n}_{\boldsymbol{t},j} \in \mathbb{N}^2 : t_1 + t_2 = q + j - 1, 1 \leqslant j \leqslant t_1, t_2 \leqslant q-1\} = S_2,$$

o qual resolve o caso $m = 2$. Agora, prosseguimos por indução sobre $m \geqslant 3$. Suponha que $S_l \subseteq \Gamma_l^+$ para todo $2 \leqslant l \leqslant m-1$.

Vejamos que $S_m \subseteq \Gamma_m^+$. Seja $\boldsymbol{n}_{\boldsymbol{t},j} \in S_m$. Então

$$\left(\frac{(x-a)^{q-j+1}}{h_2^{t_2-j+1}h_3^{t_3-j+1}\cdots h_m^{t_m-j+1}}\right)_\infty = \sum_{i=1}^{m}((t_i-j)(q+1)+j)P_i.$$

Portanto $\boldsymbol{n}_{\boldsymbol{t},j} \in H(P_1, \ldots, P_m)$.

Para mostrar que $\boldsymbol{n}_{\boldsymbol{t},j} \in \Gamma_m^+$, é suficiente provar que $\boldsymbol{n}_{\boldsymbol{t},j}$ é minimal em $\nabla_1^m(\boldsymbol{n}_{\boldsymbol{t},j})$. Suponha que não é minimal em

$$\nabla_1^m(\boldsymbol{n}_{\boldsymbol{t},j}).$$

Então existe $\boldsymbol{u} \in H(P_1, \ldots, P_m)$ com $u_1 = (t_1-j)(q+1)+j, \boldsymbol{u} \preceq \boldsymbol{n}_{\boldsymbol{t},j}$ e $\boldsymbol{u} \neq \boldsymbol{n}_{\boldsymbol{t},j}$. Seja $f \in \mathbb{F}_{q^2}(\mathcal{X})$ tal que $(f)_\infty = u_1P_1 + \cdots + u_mP_m$. Dado que $\boldsymbol{u} \neq \boldsymbol{n}_{\boldsymbol{t},j}$, existe $2 \leqslant i \leqslant m$ tal que $u_i < (t_i-j)(q+1)+j$. Sem perder generalidade, podemos supor que $i = m$. Portanto

$$u_m = (t_m-j)(q+1)+j-k$$

Para algum $k \geqslant 1$. Dois casos para considerar:

(1) $j > k$.

(2) $j \leqslant k$.

Caso (1): Suponha $j > k$. Então

$$(fh_m^{t_m-j}(x-a)^{j-k})_\infty = ((t_1+t_m-j-k)(q+1)+k)P_1 + \sum_{i=2}^{m-1}\max\{u_i-(j-k),0\}P_i.$$

Portanto,

$$\boldsymbol{v} := ((t_1+t_m-j-k)(q+1)+k, v_2, \ldots, v_{m-1}) \in H(P_1, \ldots, P_{m-1}),$$

onde $v_i = \max\{u_i-(j-k),0\}$ para $2 \leqslant i \leqslant m-1$. Considere o vetor

$$\boldsymbol{w} := \boldsymbol{n}_{(t_1+t_m-j,t_2-j+1+k,t_3-j+k,\ldots,t_{m-1}-j+k),k}.$$

O Lema 3.2.2, garante que $\boldsymbol{v} \preceq \boldsymbol{w}, v \neq \boldsymbol{w}$ e $\boldsymbol{w} \in S_{m-1}$, Portanto, pela hipóteses de indução, temos que $S_{m-1} \subseteq \Gamma_{m-1}^+$, logo $\boldsymbol{w} \in \Gamma_{m-1}^+$. Pela Proposição 2.3.1, $\boldsymbol{w}$ é minimal em $\nabla_1^{m-1}(\boldsymbol{w})$, e dado que $\boldsymbol{v} \in \nabla_1^{m-1}(\boldsymbol{w})$, temos uma contradição. Portanto o caso (1) não pode acontecer.

Caso (2): Suponha que $j \leqslant k$. Então

$$(fh_m^{t_m-j})_\infty = ((t_1+t_m-2j)(q+1)+j)P_1 + \sum_{i=2}^{m-1}u_iP_i,$$

o que implica que

$$\boldsymbol{v} := ((t_1+t_m-2j)(q+1)+j, u_2, \ldots, u_{m-1}) \in H(P_1, \ldots, P_{m-1}).$$

O Lema 3.2.3 garante que existe $i, 2 \leqslant i \leqslant m-1$ tal que o vetor

$$\boldsymbol{w} := \boldsymbol{n}_{(t_1+t_m-j,t_2,t_3,\ldots,t_{i-1},t_i+1,t_{i+1},\ldots,t_{m-1}),j}$$

satisfaz que $\boldsymbol{v} \preceq \boldsymbol{w}, \boldsymbol{v} \neq \boldsymbol{w}$ e $\boldsymbol{w} \in S_{m-1}$. Pela hipótese de indução, temos que $\boldsymbol{w} \in \Gamma^+_{m-1}$, logo pela proposição 2.3.1 $\boldsymbol{w}$ é minimal em $\nabla_1^{m-1}(\boldsymbol{w})$, mas $\boldsymbol{v} \in \nabla_1^{m-1}(\boldsymbol{w})$ gerando uma contradição. Portanto o caso (2) não pode acontecer.

Dado que os casos (1) e (2) geram ambos uma contradição, concluímos que $\boldsymbol{n}_{\boldsymbol{t},j}$ é minimal em $\nabla_1^m(\boldsymbol{n}_{\boldsymbol{t},j})$. Portanto, pela definição de Γ^+_m, temos que $\boldsymbol{n}_{\boldsymbol{t},j} \in \Gamma^+_m$. Consequentemente

$$S_m \subseteq \Gamma^+_m.$$

□

Etapa número 2.

Para começar, vamos estabelecer a seguinte convenção: Dado $\boldsymbol{v} := (v_1, \ldots, v_m) \in \mathbb{Z}^m$, seja $\boldsymbol{v}^+ := (v_{i_1}, \ldots, v_{i_l}) \in \mathbb{N}^l$ onde $i_1 < \cdots < i_l$ e $v_i > 0$ se, e somente se, $i = i_r$ para todo $1 \leqslant r \leqslant l$; isto é, $\boldsymbol{v}^+$ é o vetor formado por v eliminando cada coordenada de v menor ou igual a zero.

Lema 3.2.5. *Seja* $\boldsymbol{n} := ((t_1 - j_1)(q+1) + j_1, (t_2 - j_2)(q+1) + j_2, \ldots, (t_m - j_m)(q+1) + j_m)$, *com* $1 \leqslant j_i \leqslant q-1$ *para todo* $1 \leqslant i \leqslant m$. *Suponha* $j_m = \max\{j_i : 1 \leqslant i \leqslant m\}$ *e considere* $\boldsymbol{u} \in \mathbb{N}_0^{m-1}$ *tal que:*

(a) $\boldsymbol{u} \preceq (n_1 + (t_m - j_m + 1)(q+1), n_2, \ldots, n_{m-1})$.

(b) $u_1 > n_1$.

(c) $u_1 - (t_m - j_m + 1)(q+1) \geqslant 0$.

(d) $u_2 = n_2$.

(e) Existe $l, 2 \leqslant l \leqslant m-1$ *e algum* $(T_{i_1}, \ldots, T_{i_l})$ *e* j' *satisfazendo* $1 \leqslant j' \leqslant T_{i_r} \leqslant q-1$ *para* $1 \leqslant r \leqslant l$ *e* $\sum_{r=1}^{l} T_{ir} = q + (l-1)(j'-1)$ *tal que*

$$\boldsymbol{u}^+ = \boldsymbol{n}_{(T_{i_1},\ldots,T_{i_l}),j'}.$$

Então o vetor

$$\boldsymbol{v} := (u_1 - (t_m - j_m + 1)(q+1), u_2, u_3, \ldots, u_{m-1}, (t_m - j_m + j_2 - j_2)(q+1) + j_2),$$

satisfaz $\boldsymbol{v} \preceq \boldsymbol{n}$ *e* $\boldsymbol{v}^+ \in S_{l+1}$.

Demonstração. Dado que $u_1 > n_1 > 0$ e $u_2 = n_2 \neq 0$, temos que $i_1 = 1$ e $i_2 = 2$. Consequentemente

$$(T_2 - j')(q+1) + j' = u_{i_2} = u_2 = (t_2 - j_2)(q+1) + j_2$$

o que implica que $(q+1) \mid j_2 - j'$. Como $-(q-1) \leqslant j_k - j' \leqslant q-1$, concluímos que $j_2 = j'$ e portanto $T_2 = t_2$. Logo

$$\boldsymbol{u}^+ = \boldsymbol{n}_{(T_1,T_2,T_{i_3},\ldots,T_{i_l}),j_2}, \tag{3.5}$$

$$u_{i_r} = \begin{cases} (T_{i_r} - j_2)(q+1) + j_2 & se \quad 1 \leqslant r \leqslant l \\ 0 & se \quad l+1 \leqslant r \leqslant m-1 \end{cases},$$

$T_1 + T_2 + T_{i_3} + \cdots + T_{i_l} = q + (l-1)(j_2 - 1)$ e $j_2 \leqslant T_{i_r} \leqslant q-1$ para todo $1 \leqslant r \leqslant l$.

Por (c) temos que $u_1 - (t_m - j_m + 1)(q+1) \geqslant 0$. Como $q+1 \nmid j_2$, segue-se que $u_1 - (t_m - j_m + 1)(q+1) > 0$. Agora, considere o vetor

$$\boldsymbol{v} := (u_1 - (t_m - j_m + 1)(q+1), u_2, u_3, \ldots, u_{m-1}, (t_m - j_m + j_2 - j_2)(q+1) + j_2).$$

Note que $\boldsymbol{v} \preceq \boldsymbol{n}$, pois $u_1 \leqslant n_1 + (t_m + j_m + 1)(q+1)$, então $v_1 \leqslant n_1$, $v_i = u_i$ para todo $i, 2 \leqslant i \leqslant m-1$, e $v_m = (t_m - j_m)(q+1) + j_2 \leqslant (t_m - j_m)(q+1) + j_m = n_m$, pois $j_m = \text{máx}\{j_i : 1 \leqslant i \leqslant m\}$.

Vejamos que $\boldsymbol{v}^+ \in S_{l+1}$. Note que $\boldsymbol{v}^+$ pode-se escreve da forma

$$\boldsymbol{v}^+ = \boldsymbol{n}_{(T_1 - t_m + j_m - 1, T_2, T_{i_3}, \ldots, T_{i_l}, t_m - j_m + j_2), j_2}.$$

Portanto, $(T_1 - t_m + j_m - 1) + T_2 + T_{i_3} + \cdots + T_{i_l} + (t_m - j_m + j_2) = \sum_{r=1}^{l} T_{i_r} + j_2 - 1 = q + (l-1)(j_2 - 1) + (j_2 - 1) = q + l(j_2 - 1)$, $j_2 \leqslant T_{i_r} \leqslant q-1$ para todo $2 \leqslant r \leqslant l$ e, $T_1 - (t_m - j_m) - 1 \leqslant q - 1$. Além disso, se $T_1 - (t_m - j_m) - 1 < j_2$, então $u_1 - (t_m - j_m + 1)(q+1) = (T_1 - j_2 - (t_m - j_m + 1))(q+1) + j_2 < 0$, contradizendo o item (c), logo $j_2 \leqslant T_1 - (t_m - j_m) - 1 \leqslant T_1 \leqslant q - 1$. Portanto $\boldsymbol{v}^+ \in S_{l+1}$.

□

Observação 3.2.6. *A descrição do vetor $\boldsymbol{u}^+$ em (3.5), é uma expressão que constantemente será utilizada no decorrer da etapa número 2. Por isso, enfatizamos nela.*

A partir deste momento, os próximos lemas desta etapa, vão assumir essa expressão sem necessidade de justificativa ou reconstrução.

Lema 3.2.7. *Seja $\boldsymbol{n} := ((t_1 - j_1)(q+1) + j_1, (t_2 - j_2)(q+1) + j_2, \ldots, (t_m - j_m)(q+1) + j_m)$, com $1 \leqslant j_i \leqslant q-1$ para todo $1 \leqslant i \leqslant m$. Suponha $j_m = \text{máx}\{j_i : 1 \leqslant i \leqslant m\}$ e considere $\boldsymbol{u} \in \mathbb{N}_0^{m-1}$ tal que:*

(a) $\boldsymbol{u} \preceq (n_1 + (t_m - j_m + 1)(q+1), n_2, \ldots, n_{m-1})$.

(b) $u_1 > n_1$.

(c) $j_1 < t_1$.

(d) $u_1 - (t_m - j_m + 1)(q+1) < 0$.

(e) $u_2 = n_2$.

(f) Existe $l, 2 \leqslant l \leqslant m-1$ e algum $(T_1, , T_2, T_{i_3}, \ldots, T_{i_l})$ satisfazendo $1 \leqslant j_2 \leqslant T_{i_r} \leqslant q-1$ para $1 \leqslant r \leqslant l$ e $T_1 + T_2 + T_{i_3} + \cdots + T_{i_l} = q + (l-1)(j_2 - 1)$ tal que

$$\boldsymbol{u}^+ = \boldsymbol{n}_{(T_1, T_2, T_{i_3}, \ldots, T_{i_l}), j_2}.$$

Então o vetor

$$\boldsymbol{v} := ((t_1 - j_1 + j_2 - 1 - j_2)(q+1) + j_2, u_2, \ldots, u_{m-1}, (T_1 - t_1 + j_1 - j_2)(q+1) + j_2).$$

satisfaz $\boldsymbol{v} \preceq \boldsymbol{n}, \boldsymbol{v} \neq \boldsymbol{n}$ e $\boldsymbol{v}^+ \in S_{l+1}$.

Demonstração. Observe que $\boldsymbol{v} \preceq \boldsymbol{n}$, pois $v_1 = (t_1 - j_1 - 1)(q+1) + j \leqslant (t_1 - j_1 - 1)(q+1) + (q+1) = (t_1 - j_1)(q+1) \leqslant (t_1 - j_1)(q+1) + j_1$, $v_i = u_i \leqslant v_i$ para todo $2 \leqslant i \leqslant m-1$, e dado que $u_1 < (t_m - j_m + 1)(q+1)$, temos que $(T_1 - j_2)(q+1) + j_2 < (t_m - j_m + 1)(q+1)$, logo $(T_1 - j_2)(q+1) < (t_m - j_m + 1)(q+1)$; consequentemente $(T_1 - j_2) < (t_m - j_m + 1)$ e portanto $(T_1 - t_1 + j_1 - j_2)(q+1) + j_2 \leqslant (T_1 - j_2)(q+1) + j_2 \leqslant (t_m - j_m)(q+1) + j_m$, concluindo que $v_m \leqslant n_m$. Logo $\boldsymbol{v} \preceq \boldsymbol{n}$. Além, temos que $n_1 \neq v_1$ pois de outra forma $(t_1 - j_1)(q+1) + j_1 = (t_1 - j_1 - 1)(q+1) + j_2$ e portanto $q+1 \mid j_1 - j_2$, mas isto contradiz o fato que $-(q-1) \leqslant j_1 - j_2 \leqslant q - 1$. Portanto $\boldsymbol{v} \neq \boldsymbol{n}$.

Vejamos que $\boldsymbol{v}^+ \in S_{l+1}$. O fato que $j_1 < t_1$, garante que $v_1 > 0$ e portanto $\boldsymbol{v}^+ \in \mathbb{N}^{l+1}$. Observe que $\boldsymbol{v}^+$ pode-se escrever como

$$\boldsymbol{v}^+ = \boldsymbol{n}_{(t_1-j_1+j_2-1,T_2,T_{i_3},\ldots,T_{i_l},T_1-t_1+j_1),j_2}.$$

Note que $(t_1-j_1+j_2-1)+T_2+\sum_{r=3}^{l} T_{i_r}+(T_1-t_1+j_1) = \sum_{r=1}^{l} T_{i_r}+j_2-1 = q+(l-1)(j_2-1)+(j_2-1) = q+l(j_2-1)$, $j_2 \leqslant T_{i_r} \leqslant q-1$ para todo $2 \leqslant r \leqslant l$, e $T_1-(t_1-j_1) \leqslant T_1 \leqslant q-1$. Além disso, $j_2 \leqslant T_1-t_1+j_1$, caso contraio teríamos $(T_1-t_1+j_1-j_2)(q+1) < 0$; como $-(q-2) \leqslant j_2-j \leqslant q-2$, então $(T_1-t_1+j_1-j_2)(q+1)+j_2-j \leqslant 0$, logo $(T_1-j_2)(q+1)+j_2 \leqslant (t_1-j_1)(q+1)+j$, contradizendo o fato que $n_1 < u_1$. Logo $\boldsymbol{v}^+ \in S_{l+1}$.

□

Lema 3.2.8. *Seja* $\boldsymbol{n} := ((t_1-j_1)(q+1)+j_1, (t_2-j_2)(q+1)+j_2, \ldots, (t_m-j_m)(q+1)+j_m)$, *com* $1 \leqslant j_i \leqslant q-1$ *para todo* $1 \leqslant i \leqslant m$. *Suponha* $j_m = \max\{j_i : 1 \leqslant i \leqslant m\}$ *e considere* $\boldsymbol{u} \in \mathbb{N}_0^{m-1}$ *tal que:*

(a) $\boldsymbol{u} \preceq (n_1+(t_m-j_m+1)(q+1), n_2, \ldots, n_{m-1})$.

(b) $u_1 > n_1$.

(c) $u_1-(t_m-j_m+1)(q+1) < 0$.

(d) $u_2 = n_2$.

(e) Existe $l, 2 \leqslant l \leqslant m-1$ *e algum* $(T_1, , T_2, T_{i_3}, \ldots, T_{i_l})$ *satisfazendo* $1 \leqslant j_2 \leqslant T_{i_r} \leqslant q-1$ *para* $1 \leqslant r \leqslant l$ *e* $T_1+T_2+T_{i_3}+\cdots+T_{i_l} = q+(l-1)(j_2-1)$ *tal que*

$$\boldsymbol{u}^+ = \boldsymbol{n}_{(T_1,T_2,T_{i_3},\ldots,T_{i_l}),j_2}.$$

Então o vetor

$$\boldsymbol{v} := (0, u_2, \ldots, u_{m-1}, (T_{i_1}-j_2)(q+1)+j_2).$$

satisfaz $\boldsymbol{v} \preceq \boldsymbol{n}, \boldsymbol{v} \neq \boldsymbol{n}$ *e* $\boldsymbol{v}^+ \in S_l$.

Demonstração. Novamente, note que $\boldsymbol{v} \preceq \boldsymbol{n}$ e $\boldsymbol{v} \neq \boldsymbol{n}$, já que $v_1 = 0 \leqslant n_1$, $v_i = u_i \leqslant n_i$ para todo $i, 2 \leqslant i \leqslant m-1$, e dado que $u_1 < (t_m-j_m+1)(q+1)$ implica $(T_1-j_2)(q+1) < (t_m-j_m+1)(q+1)$, segue-se que $T_1-j_2 \leqslant (t_m-j_m)$, logo $(T_1-j_2)(q+1)+j_2 \leqslant (t_m-j_m)(q+1)+j_m$.

Vejamos se $\boldsymbol{v}^+ \in S_l$. Observe que $\boldsymbol{v}^+$ pode-se escrever como

$$\boldsymbol{v}^+ := \boldsymbol{n}_{(T_2,T_{i_3}\ldots,T_{i_l},T_1),j_2}.$$

Logo, $j_2 \leqslant T_{i_r} \leqslant q-1$ para todo $r, 1 \leqslant r \leqslant l$ e $\sum_{r=1}^{l} T_{i_r} = q+(l-1)(j_2-1)$. Portanto $\boldsymbol{v}^+ \in S_l$.

□

Proposição 3.2.9. *Para* $2 \leqslant m \leqslant q+1$, $\Gamma_m^+ \subseteq S_m$.

Demonstração. Vamos mostrar que $\Gamma_m^+ \subseteq S_m$ por indução sobre m. Novamente, a expressão (3.2) resolve o caso $m = 2$. Portanto, vamos prosseguimos por indução para $m \geqslant 3$. Suponha $\Gamma_l^+ \subseteq S_l$ para $2 \leqslant l \leqslant m-1$.

Por contradição, suponha que existe $\boldsymbol{n} \in \Gamma_m^+ \backslash S_m$. Portanto existe $f \in \mathbb{F}_{q^2}(\mathcal{X})$ com divisor de polos $(f)_\infty = n_1P_1+\cdots+n_mP_m$. Pelo Lema 2.3.2,

$$\boldsymbol{n} \in \Gamma_m^+ \subseteq G(P_1) \times \cdots \times G(P_m).$$

Assim,

$$\boldsymbol{n} = ((t_1-j_1)(q+1)+j_1, (t_2-j_2)(q+1)+j_2, \ldots, (t_m-j_m)(q+1)+j_m)$$

onde $1 \leqslant j_i \leqslant t_i \leqslant q-1$ para todo $1 \leqslant i \leqslant m$.

Seja $j_r = \text{máx}\{j_i : 1 \leqslant i \leqslant m\}$. Sem perder a generalidade podemos supor que $r = m$. Considere o divisor

$$(fh_m^{t_m - j_m + 1})_\infty = (n_1 + (t_m - j_m + 1)(q+1))P_1 + \sum_{i=2}^{m-1} n_i P_i$$

Logo $(n_1 + (t_m - j_m + 1)(q+1), n_2 \ldots, n_{m-1}) \in H(P_1, \ldots, P_{m-1})$. Então existe $\boldsymbol{u} \in \Gamma_{m-1}$ tal que

$$\boldsymbol{u} \preceq (n_1 + (t_m - j_m + 1)(q+1), n_2 \ldots, n_{m-1})$$

e $u_2 = n_2 = (t_2 - j_2)(q+1) + j_2$. Se $u_1 \leqslant n_1$, então $(u_1, \ldots, u_{m-1}, 0) \preceq \boldsymbol{n}$, o que contradiz a minimalidade de $\boldsymbol{n}$ em $\nabla_2^m(\boldsymbol{n})$. Logo $u_1 > n_1 > 0$. Pela hipóteses de indução,

$$\boldsymbol{u}^+ = \boldsymbol{n}_{(T_{i_1}, \ldots, T_{i_l}), j'} \in \Gamma_l^+ \subseteq S_l$$

para algum $l, 2 \leqslant l \leqslant m-1$ e algum $(T_{i_1}, \ldots, T_{i_l})$ e j' satisfazendo $1 \leqslant j' \leqslant T_{i_r} \leqslant q-1$ para $1 \leqslant r \leqslant l$ e $\sum_{r=1}^{l} T_{i_r} = q + (l-1)(j'-1)$. Portanto, existe um conjunto indexado $\{i_1, \ldots, i_{m-1}\} = \{1, \ldots, m-1\}$ tal que $i_1 < i_2 < \cdots < i_l$ e

$$u_{i_r} = \begin{cases} (T_{i_r} - j')(q+1) + j' & se \quad 1 \leqslant r \leqslant l \\ 0 & se \quad l+1 \leqslant r \leqslant m-1 \end{cases}.$$

Dado que $u_1 > n_1 > 0$ e $u_2 = n_2 \neq 0$, temos que $i_1 = 1$ e $i_2 = 2$. Consequentemente

$$(T_2 - j')(q+1) + j' = u_{i_2} = u_2 = (t_2 - j_2)(q+1) + j_2$$

o que implica que $(q+1) \mid j_2 - j'$. Como $-(q-1) \leqslant j_2 - j' \leqslant q-1$, concluímos que $j_2 = j'$ e portanto $T_2 = t_2$. Logo

$$\boldsymbol{u}^+ = \boldsymbol{n}_{(T_1, T_2, T_{i_3} \ldots, T_{i_l}), j_2},$$

$$u_{i_r} = \begin{cases} (T_{i_r} - j_2)(q+1) + j_2 & se \quad 1 \leqslant r \leqslant l \\ 0 & se \quad l+1 \leqslant r \leqslant m-1 \end{cases},$$

$T_1 + T_2 + T_{i_3} + \cdots + T_{i_l} = q + (l-1)(j_2 - 1)$ e $j_2 \leqslant T_{i_r} \leqslant q-1$ para todo $1 \leqslant r \leqslant l$.

Neste ponto, diferenciamos dois casos:

(1) $u_1 - (t_m - j_m + 1)(q+1) \geqslant 0$.

(2) $u_1 - (t_m - j_m + 1)(q+1) < 0$.

Caso (1): Suponha que $u_1 - (t_m - j_m + 1)(q+1) \geqslant 0$. O Lema 3.2.5, estabelece que o vetor

$$\boldsymbol{v} := (u_1 - (t_m - j_m + 1)(q+1), u_2, u_3, \ldots, u_{m-1}, (t_m - j_m + j_2 - j_2)(q+1) + j_2).$$

satisfaz que $\boldsymbol{v} \preceq \boldsymbol{n}$ e $\boldsymbol{v}^+ \in S_{l+1}$. Segue-se pela Proposição 3.2.4 que $\boldsymbol{v}^+ \in \Gamma_{l+1}^+$, portanto $\boldsymbol{v} \in \Gamma_m$. O fato de que $\boldsymbol{v} \preceq \boldsymbol{n}$ e $\boldsymbol{n} \in \Gamma_m^+$ obriga que $\boldsymbol{n} = \boldsymbol{v}$ ou de outra forma $\boldsymbol{n}$ não seria minimal em $\nabla_2^m(\boldsymbol{n})$, portanto $l+1 = m$ e $\boldsymbol{n} = \boldsymbol{v} = \boldsymbol{v}^+ \in S_m$, mas isto é contraditório, pois $\boldsymbol{n} \in \Gamma_m^+ \backslash S_m$. Portanto o caso (1) não pode acontecer.

Caso (2): Suponha que $u_1 - (t_m - j_m + 1)(q+1) < 0$. Existem dois subcasos:

(a) $j_1 < t_1$.

(b) $j_1 = t_1$.

Subcaso (a): Suponha $j_1 < t_1$. Considere o vetor

$$\boldsymbol{v} := ((t_1 - j_1 + j_2 - 1 - j_2)(q+1) + j_2, u_2, \ldots, u_{m-1}, (T_1 - t_1 + j_1 - j_2)(q+1) + j_2).$$

O Lema 3.2.7 garante que $\boldsymbol{v} \preceq \boldsymbol{n}, \boldsymbol{v} \neq \boldsymbol{n}$ e $\boldsymbol{v}^+ \in S_{l+1}$. Portanto, a Proposição 3.2.4, $\boldsymbol{v}^+ \in S_{l+1} \subseteq \Gamma_{l+1}^+ \subseteq H(P_1, \ldots, P_{l+1})$, logo $\boldsymbol{v} \in H(P_1, \ldots, P_m)$ e $\boldsymbol{v} \in \nabla_2^m(\boldsymbol{n})$. Mas isto contradiz a minimalidade de $\boldsymbol{n}$ em $\nabla_2^m(\boldsymbol{n})$. Portanto não pode acontecer o subcaso (a).

Subcaso (b): Suponha que $j_1 = t_1$. Considere o vetor

$$\boldsymbol{v} := (0, u_2, \ldots, u_{m-1}, (T_1 - j_2)(q+1) + j_2).$$

Uma aplicação do Lema 3.2.8, permite estabelecer que $\boldsymbol{v} \preceq \boldsymbol{n}, \boldsymbol{v} \neq \boldsymbol{n}$ e $\boldsymbol{v}^+ \in S_l$. Novamente, a Proposição 3.2.4 garante que $\boldsymbol{v}^+ \in S_l \subseteq \Gamma_l^+ \subseteq H(P_1, \ldots, P_l)$, logo $\boldsymbol{v} \in H(P_1, \ldots, P_m)$ e $\boldsymbol{v} \in \nabla_2^m(\boldsymbol{n})$. O fato de que $\boldsymbol{v} \neq \boldsymbol{n}$ contradiz a minimalidade de $\boldsymbol{n}$ em $\nabla_2^m(\boldsymbol{n})$. Assim, o subcaso (b) não pode acontecer e consequentemente o caso (2) tampouco. Logo, $\Gamma_m^+ \backslash S_m = \varnothing$. □

Para finalizar, note que a Proposição 3.2.4 e a Proposição 3.2.9 provam o Teorema 3.2.1.

Exemplo 3.2.10. *Considere a curva $\mathcal{X}$ definida pela equação afim $y^5 + y = x^6$ sobre $\mathbb{F}_{5^2}$. Seja P_1, P_2, P_3, P_4 pontos $\mathbb{F}_{5^2}$-racionais de $\mathcal{X}$ distintos, para determinar $H(P_1, P_2, P_3, P_4)$, precisamos determinar $\Gamma_1^+, \Gamma_2^+, \Gamma_3^+, \Gamma_4^+$. Sabemos que $\Gamma_1^+ = \langle 5, 6 \rangle$, e pelo Teorema 3.2.1, temos:*

$$\Gamma_2^+ = \{(1,19), (7,13), (2,14), (13,7), (8,8), (3,9), (19,1), (14,2), (9,3), (4,4)\}.$$

$$\Gamma_3^+ = \{(1,1,13), (1,7,7), (1,13,1), (7,1,7), (7,7,1), (2,2,8), (2,8,2), (13,1,1), (8,2,2), (3,3,3)\}.$$

$$\Gamma_4^+ = \left\{ \begin{array}{l} (1,1,13,1), (1,1,13,7), (1,1,13,13), (1,1,13,19), (1,7,7,1), (1,7,7,7), (1,7,7,13), \\ (1,7,7,19), (1,13,1,1), (1,13,1,7), (1,13,1,13), (1,13,1,19), (7,1,7,1), (7,1,7,7), \\ (7,1,7,13), (7,1,7,19), (7,7,1,1), (7,7,1,7), (7,7,1,13), (7,7,1,19), (2,2,14,2), \\ (2,2,14,8), (2,2,14,14), (2,8,8,2), (2,8,8,8), (2,8,8,14), (2,14,2,2), (2,14,2,8), \\ (2,14,2,14), (13,1,1,1), (13,1,1,7), (13,1,1,13), (13,1,1,19), (8,2,8,2), (8,2,8,8), \\ (8,2,8,14), (8,8,2,2), (8,8,2,8), (8,8,2,14), (3,9,9,3), (3,9,9,9), (14,2,2,2), \\ (14,2,2,8), (14,2,2,14), (9,3,9,3), (9,3,9,9), (9,9,3,3), (9,9,3,9) \end{array} \right\}.$$

Capítulo 4

Semigrupo de Weierstrass em Vários Pontos para Certas Curvas de Variáveis Separáveis

Neste capítulo apresentamos a técnica usada por Castellanos e Tizziotti em [5] para determinar o conjunto Γ_m^+. Paralelamente ao método apresentado no capítulo 3, eles usam o conceito de discrepância introduzido por Duursma e Park em [6], para caracterizar os elementos mínimais em $H(P_1, \ldots, P_m)$ e posteriormente, determinar o conjunto Γ_m^+ para uma família de curvas de variáveis separáveis.

4.1 Discrepância

Definição 4.1.1. *Um divisor $D \in Div(\mathcal{X})$ é chamado de* discrepância *com respeito aos pontos $\mathbb{F}_q-$racionais P e Q sobre $\mathcal{X}$ se $\mathcal{L}(D) \neq \mathcal{L}(D-P) = \mathcal{L}(D-P-Q)$ e $\mathcal{L}(D) \neq \mathcal{L}(D-Q) = \mathcal{L}(D-P-Q)$.*

O seguinte resultado relaciona o conceito de *discrepância* com o conjunto Γ_m^+.

Lema 4.1.2. *Seja $\boldsymbol{n} \in H(P_1, \ldots, P_m)$. Então $\boldsymbol{n} \in \Gamma_m^+$ se, e somente se, o divisor $D = \sum_{j=1}^m n_j P_j$ é* discrepância *com respeito a P_i e P_k para qualquer dois pontos $\mathbb{F}_q-$racionais $P_i, P_k \in \{P_1, \ldots, P_m\}$.*

Demonstração. Seja $\boldsymbol{n} \in \Gamma_m^+$. Para $P_i, P_k \in \{P_1, \ldots, P_m\}$ com $i \neq k$, o Lema 2.2.3 garante que $\mathcal{L}(D) \neq \mathcal{L}(D-P_i)$. Agora, suponha que $\mathcal{L}(D-P_i) \neq \mathcal{L}(D-P_i-P_k)$, logo existe uma função racional $g \in \mathcal{L}(D-P_i) \backslash \mathcal{L}(D-P_i-P_k)$ com divisor de polos $(g)_\infty = \sum_{j=1, j\neq k}^m s_j P_j + n_k P_k$ tal que $s_i < n_i$ e $s_t \leqslant n_t$, para $t \in \{1, \ldots, m\} \backslash \{i, k\}$. Segue-se que $(s_1, \ldots, s_{k-1}, n_k, n_{k+1}, \ldots, s_m) \in \nabla_k^m(\boldsymbol{n})$, mas isto contradiz o fato que $\boldsymbol{n} \in \Gamma_m^+$ é minimal em $\nabla_i^m(\boldsymbol{n})$. De maneira semelhante para o caso $\mathcal{L}(D) \neq \mathcal{L}(D-P_k) = \mathcal{L}(D-P_k-P_i)$. Portanto $D = \sum_{j=1}^m n_j P_j$ é discrepância com respeito a P_i e P_k para qualquer dois pontos $\mathbb{F}_q-$racionais $P_i, P_k \in \{P_1, \ldots, P_m\}$.

Inversamente, suponha que $\boldsymbol{n}$ não é minimal em $\nabla_i^m(\boldsymbol{n})$ e que $D = \sum_{j=1}^m n_j P_j$ é discrepância com respeito a qualquer $P_i, P_k \in \{P_1, \ldots, P_m\}$, com $i \neq k$. Dado que $\boldsymbol{n} \in H(P_1, \ldots, P_m)$, existe $\boldsymbol{s} \in H(P_1, \ldots, P_m)$ tal que $\boldsymbol{s} \in \nabla_i^m(\boldsymbol{n}), \boldsymbol{s} \neq \boldsymbol{n}$ e $\boldsymbol{s} \preceq \boldsymbol{n}$. Consequentemente $n_i = s_i$ e $s_k < n_k$ para algum $k \neq i$. Logo, para qualquer função racional f_i com divisor de polos $(f_i)_\infty = \sum_{j=1}^m s_j P_j$, temos que $f_i \in \mathcal{L}(D-P_k)$ e $f_i \notin \mathcal{L}(D-P_i)$, mas isto contradiz o fato que $\mathcal{L}(D-P_k) = \mathcal{L}(D-P_i) = \mathcal{L}(D-P_i-P_k)$. Portanto $\boldsymbol{n} \in \Gamma_m^+$. □

4.2 Semigrupo de Weierstrass em curvas separáveis

Considere a curva $\mathcal{X}_{f,g}$ definida sobre $\mathbb{F}_q$ pela equação afim $f(y) = g(x)$, em que $f(T), g(T) \in \mathbb{F}_q[T]$, grau$(f(T)) = a$ e grau$(g(T)) = b$ sendo primos relativos. Suponha que $\mathcal{X}_{f,g}$ tenha gênero $g = (a-1)(b-1)/2$ e, suponha ainda que existem pontos $\mathbb{F}_q$-racionais distintos $P_1, P_2, \ldots, P_{a+1}$ sobre a curva tais que:

$$aP_1 \sim P_2 + \cdots + P_{a+1}, \tag{4.1}$$

e

$$bP_i \sim bP_j \text{ para todo } i, j \in \{1, 2, \ldots, a+1\}. \tag{4.2}$$

Esse tipo de curvas serão nosso objeto de estudo nesta seção.

Observamos que pelas suposições acima tem-se que $H(P_1) = \langle a, b\rangle$.

A seguir, apresentamos alguns exemplos de curvas que são do tipo $\mathcal{X}_{f,g}$.

Exemplo 4.2.1. *A curva Hermitiana sobre o corpo $\mathbb{F}_{q^2}$ definida pela equação $y^q + y = x^{q+1}$.*

Exemplo 4.2.2. *A curva Norma-traço definida pela equação afim $y^{q^{r-1}} + \cdots + y^q + y = x^{\frac{q^r-1}{q-1}}$ sobre o corpo $\mathbb{F}_{q^r}$, o gênero desta curva é $g = (q^{r-1}-1)\left(\frac{q^r-1}{q-1} - 1\right)/2$. Esse modelo foi estudado por Geil em [10], o semigrupo de Weierstrass em certo par de pontos foi calculado em [23].*

Exemplo 4.2.3. *A curva maximal definida pela equação $y^{q+1} = \sum_{i=1}^{k} x^{q/2^i}$, com $q = 2^k$ sobre $\mathbb{F}_{q^2}$, ver [2].*

Exemplo 4.2.4. *A curva maximal sobre $\mathbb{F}_{q^{2r}}$ definida pela equação $y^q + y = x^{q^r+1}$, ver [18].*

Exemplo 4.2.5. *A curva extensão de Kummer $y^b = g(x) = \prod_{i=1}^{a}(x - c_i)$, onde $g(x)$ é um polinômio separável e $mdc(a, b) = 1$. Nesse modelo, foram estudadas condições para que um inteiro seja lacuna num ponto da curva em [1].*

A fim de determinar o conjunto Γ_m^+, queremos determinar quais são os elementos minimais do semigrupo de Weierstrass $H(P_1, \ldots, P_m)$, com $1 \leqslant m \leqslant a$. Para isso, vamos descrever certos tipos de divisores. Posteriormente, será mostrado que esses divisores são discrepâncias.

Para começar, seja $m \in \mathbb{N}$. Considere a igualdade

$$t + \sum_{j=2}^{m} s_j = a + 1 - m, \tag{4.3}$$

onde $t, s_2, \ldots, s_m \in \mathbb{Z}$. Das equações 4.1 e 4.2 temos que

$$(tb - ia)P_1 + \sum_{j=2}^{m}(s_j b + i)P_j \sim \sum_{j=m+1}^{a+1}(b - i)P_j, \tag{4.4}$$

com $i \in \mathbb{N}_0$. Note que os coeficientes em (4.4) são positivos se

$$0 < ai < tb \text{ e } 0 \leqslant s_j \text{ para todo } 2 \leqslant j \leqslant m. \tag{4.5}$$

Note também que $0 < t \leqslant a, 0 < i < b$ e $1 \leqslant m \leqslant a$.

Lema 4.2.6. *Sejam $a, b, i, m \in \mathbb{N}$ tais que $0 < t \leqslant a, 0 < i < b$ e $1 \leqslant m \leqslant a$. Considere o divisor*

$$D = (b - i)(aP_1 - \sum_{j=2}^{m} P_j). \tag{4.6}$$

Então,

$$D' = ((a+1-m)b - ia)P_1 + i(\sum_{j=2}^{m} P_j) \tag{4.7}$$

é um divisor efetivo e $D \sim D'$.

Demonstração. Seja $D = (b-i)(aP_1 - \sum_{j=2}^{m} P_j)$ e $D' = ((a+1-m)b-ia)P_1 + i(\sum_{j=2}^{m} P_j)$. Se $1 \leqslant m \leqslant a$, então, por (4.3) $ai < tb < (a+1-m)b$, portanto $D' = ((a+1-m)b-ia)P_1 + i(\sum_{j=2}^{m} P_j)$ é um divisor efetivo. Agora, da equação (4.1) temos que $D \sim (b-i)\sum_{j=m+1}^{a+1} P_j$, Usando (4.2) temos

$$D' \sim \sum_{j=m+1}^{a+1}(b-i)P_j$$

Portanto $D' \sim D$.

□

No decorrer desta seção, vamos assumir $a, b, t, i, s_2, \ldots, s_m$ como em (4.1)-(4.5).

Redistribuindo $a+1-m = s+t$ sobre P_1 e P_2, os divisores em (4.4), com $s = \sum_{j=2}^{m} s_j$, tem a seguinte representação

$$(tb - ia)P_1 - (sb + i)P_2 + i\sum_{j=3}^{m} P_j \sim \sum_{j=m+1}^{a+1} (b-i)P_j. \tag{4.8}$$

Com os mesmos parâmetros t, s e i, outros divisores são obtidos de (4.8) distribuindo s em todas as formas possíveis sobre $P_2, \ldots, P_{m+1}$ tal que $s = \sum_{j=2}^{m} s_j$. Para nosso seguinte resultado, precisamos introduzir os seguintes fatos:

Definição 4.2.7. *Um semigrupo é dito* simétrico *se sua última lacuna é* $2g-1$*, onde* g *é o gênero do semigrupo.*

Proposição 4.2.8. *[26, Proposição 5.11] Sejam* $a, b \in \mathbb{N}$ *tais que* $mdc(a,b) = 1$*. O semigrupo gerado por* a *e* b *é simétrico e a última lacuna é* $ab - a - b$*.*

Lema 4.2.9. *[7, Noether's Reduction Lemma] Seja* $D \in Div(\mathcal{X})$*,* $P \in \mathcal{X}$*, e seja* K *um divisor canônico em* $\mathcal{X}$*. Se* $\ell(D) > 0$ *e* $\ell(K - D - P) \neq \ell(K - D)$*, então* $\ell(D + P) = \ell(D)$*.*

Proposição 4.2.10. *O divisor* $D = (b-i)(aP_1 - \sum_{j=2}^{m} P_j)$ *é discrepância com respeito a* P_i *e* P_k *para qualquer dois pontos distintos* $P_i, P_k \in \{P_1, \ldots, P_m\}$*.*

Demonstração. Pelo Lema 4.2.6 existe uma função racional $f \in \mathcal{L}(D')$ tal que $(f)_\infty = D'$. Portanto $\mathcal{L}(D') \neq \mathcal{L}(D' - P_i)$ para qualquer ponto $P_i \in \{P_1, \ldots, P_m\}$. Para mostrar que $\mathcal{L}(D' - P_i) = \mathcal{L}(D' - P_i - P_k)$ considere o divisor $K = (ab - a - b - 1)P_1$. A Proposição 4.2.8 e o fato que $\text{grau}(K) = 2g - 2$, garantem que K é um divisor canônico. Logo

$$\begin{aligned} K + P_i + P_k - D' &= (ab - a - b - 1)P_1 + P_i + P_k - ((a+1-m)b - ia)P_1 - i(\textstyle\sum_{j=2}^{m} P_j) \\ &= ((i-1)a + (m-2)b - 1)P_1 + P_i + P_k - i(\textstyle\sum_{j=2}^{m} P_j) \end{aligned}$$

Considere o caso $P_1 \in \{P_i, P_k\}$. Sem perda de generalidade podemos supor que $i = 1$ e $k = 2$. Sejam $f_1, \ldots, f_m$ funções como divisores

$$(f_j) = \begin{cases} -aP_1 + \sum_{j=2}^{a+1} & j = 2 \\ b(P_j - P_1) & j > 2 \end{cases}$$

Então $f_2^{i-1}f_3\cdots f_m \in \mathcal{L}(K+P_1+P_2-D')\backslash\mathcal{L}(K+P_2-D')$. Consequentemente, pelo Lema 4.2.9, temos $\mathcal{L}(D'-P_2)=\mathcal{L}(D'-P_1-P_2)$. Segue que $\mathcal{L}(D')\neq\mathcal{L}(D'-P_2)=\mathcal{L}(D'-P_1-P_2)$ e $\mathcal{L}(D')\neq\mathcal{L}(D'-P_1)=\mathcal{L}(D'-P_2-P_1)$.

Considere o caso $P_1\notin\{P_i,P_k\}$. Novamente, sem perda de generalidade podemos supor que $i=2$ e $k=3$. Como no caso anterior, concluímos que $f_2^{i-1}f_4\cdots f_m\in\mathcal{L}(K+P_2+P_3-D')\backslash\mathcal{L}(K+P_3-D')$ e portanto $\mathcal{L}(D'-P_3)=\mathcal{L}(D'-P_2-P_3)$. Dado que $D\sim D'$, concluímos que $\mathcal{L}(D)\neq\mathcal{L}(D-P_3)=\mathcal{L}(D-P_2-P_3)$ e $\mathcal{L}(D)\neq\mathcal{L}(D-P_2)=\mathcal{L}(D-P_3-P_2)$.

□

Corolário 4.2.11. *O divisor $(tb-ia)P_1+\sum_{j=2}^m(s_jb+i)P_j$ é discrepância com respeito a P_i e P_k para qualquer dois pontos distintos $P_i,P_k\in\{P_1,\ldots,P_m\}$.*

Demonstração. Segue-se do resultado anterior e do fato

$$(tb-ai)P_1+\textstyle\sum_{j=2}^m(s_jb+i)P_j\sim\sum_{j=m+1}^{a+1}P_j\sim D\sim D'.$$

□

Teorema 4.2.12. *Seja $\mathcal{X}$ uma curva irredutível definida pela equação afim $f(y)=g(x)$, onde $f(T),g(T)\in\mathbb{F}_q[T]$, grau$(f(y))=a$ e grau$(g(x))=b$, com mcd$(a,b)=1$ e* gênero $g=(a-1)(b-1)/2$. *Sejam $P_1,P_2,\ldots,P_{a+1}$ pontos $\mathbb{F}_q-$racionais distintos sobre a curva $\mathcal{X}$. Para $2\leqslant m\leqslant a+1$, considere o conjunto*

$$S_m=\left\{(tb-ia,s_2b+i,\ldots,s_mb+i):\begin{array}{l}t+\sum_{j=2}^m s_j=a+1-m,0<ia<tb,\\ 0\leqslant s_j\ \textit{para todo}\ j,2\leqslant j\leqslant m.\end{array}\right\}.$$

Então $\Gamma_m^+=S_m$.

Demonstração. Pelo Corolário 4.2.11 o divisor $(tb-ia)P_1+\sum_{j=2}^m(s_j+i)P_j$ é discrepância com respeito a P_i e P_k para qualquer dois pontos distintos $P_i,P_k\in\{P_1,\ldots,P_m\}$. Portanto, pelo Lema 4.1.2 segue-se que $S_m\subseteq\Gamma_m^+$.

Por conseguinte, será provado que $\Gamma_m^+\subseteq S_m$. Seja $\boldsymbol{n}\in\Gamma_m^+$. Pelo Lema 2.3.2, $\boldsymbol{n}\in G(P_1)\times\cdots\times G(P_m)$.

Como $H(P_1)=\langle a,b\rangle$, a Proposição 3.1.2 garante que existem $i_1,j_1\in\mathbb{N}$ tais que $n_1=ab-i_1a-j_1b=(a-j_1)b-i_1a$. Seja $\lambda=a-j_1$. Note que $0<ai_1<b\lambda$ e $0<j_1<a$.

Pela equação (4.2), $b\in H(P_l)$ para todo $l,2\leqslant l\leqslant m$, portanto $n_l=s_lb+i_l$, onde $0<i_l<b$ e $s_l\geqslant 0$.

Seja $i=\min\{i_l:2\leqslant l\leqslant m\}$. Por (4.2), para cada $2\leqslant l\leqslant m$ existe um função racional h_l tal que $(h_l)=bP_1-bP_l$. Por (4.1) existe uma função racional g tal que $(g)=\sum_{j=2}^{a+1}P_j-aP_1$.

Seja $f=g^{b-i}\prod_{l=2}^m h_l^{s_l+1}$. Então, $(f)_\infty=((a-\sum_{l=2}^m(s_l+1))b-ai)P_1+\sum_{l=2}^m(s_lb+i)P_l$. Tomando $t=a-\sum_{l=2}^m(s_l+1)$, o Corolário 4.2.11 garante que $(f)_\infty$ é discrepância com respeito a P_i e P_k para qualquer dois pontos distintos $P_i,P_k\in\{P_1,\ldots,P_m\}$. Portanto, pelo Lema 4.1.2, $\boldsymbol{w}=(tb-ia,s_2b+i,\ldots,s_mb+i)\in\Gamma_m^+$. Além disso, sabemos que $i=i_t$ para algum $t,1\leqslant t\leqslant m$. Então $\boldsymbol{w}\in\nabla_t^m(\boldsymbol{n})$ e pela minimalidade de $\boldsymbol{w}$ e $\boldsymbol{n}$, segue-se que $\boldsymbol{w}=\boldsymbol{n}$ e portanto $\Gamma_m^+\subseteq S_m$.

□

Exemplo 4.2.13. *Seja $y^{q+1}=\sum_{i=1}^k x^{q/2^i}$, com $q=2^k$ sobre $\mathbb{F}_{q^2}$. Esta curva tem um único ponto no infinito $P_\infty=(1:0:0)$. Seja $P_1=(0:0:1)$ e considere funções racionais x e y em $\mathbb{F}_q(\mathcal{X})$, logo*

$$(x)=\textstyle\sum_{i=1}^{q^{k-1}}P_i-(2^{k-1})P_\infty\quad e\quad (y)=(q+1)(P_1-P_\infty).$$

Tome $k=3,q=2$, logo $a=9$ e $b=4$. Pelo Teorema 4.2.12, Γ_4^+ está composto pelos vetores:

$4(6,0,0,0)+i(-3,1,1,1), i=1,2,$
$4(5,0,0,1)+i(-3,1,1,1), i=1,2,$
$4(5,0,1,0)+i(-3,1,1,1), i=1,2,$
$4(5,1,0,0)+i(-3,1,1,1), i=1,2,$
$4(4,0,0,2)+(-3,1,1,1),$
$4(4,0,2,0)+(-3,1,1,1),$
$4(4,0,1,1)+(-3,1,1,1),$
$4(4,1,0,1)+(-3,1,1,1),$
$4(4,1,1,0)+(-3,1,1,1),$
$4(3,0,0,3)+(-3,1,1,1),$
$4(3,0,3,0)+(-3,1,1,1),$
$4(3,3,0,0)+(-3,1,1,1),$
$4(3,0,1,2)+(-3,1,1,1),$
$4(3,0,2,1)+(-3,1,1,1),$
$4(3,1,0,2)+(-3,1,1,1),$
$4(3,2,0,1)+(-3,1,1,1),$
$4(3,1,2,0)+(-3,1,1,1),$
$4(3,2,1,0)+(-3,1,1,1),$
$4(3,1,1,1)+(-3,1,1,1).$

Exemplo 4.2.14. *Seja $y^b = g(x) = \prod_{i=1}^{a}(x-c_i)$ um extensão de Kummer , onde $g(x)$ é um polinômio separável sobre $\mathbb{F}_q$ de grau a e $mdc(a,b)=1$. Seja $P_1 = P_\infty$ o ponto no infinito da curva e $P_2,\ldots,P_{a+1}$ pontos racionais. Então*

$$(x-c_i) = b(P_i - P_1) \text{ para todo } 2 \leqslant i \leqslant a+1 \quad e \quad (y) = \sum_{i=2}^{a+1} -P_1.$$

Para $a=6$ e $b=5$, temos:

$$\Gamma_2^+ = \left\{ \begin{array}{l} (27,1),(19,2),(11,3),(3,4),(22,6),(14,7),(6,8), \\ (17,11),(9,12),(1,13),(12,16),(4,17),(7,21),(2,26) \end{array} \right\}.$$

$$\Gamma_3^+ = \left\{ \begin{array}{l} (22,1,1),(14,2,2),(6,3,3),(17,1,6),(9,2,7), \\ (1,3,8),(12,1,11),(4,2,12),(7,1,16),(2,1,21), \\ (17,6,1),(9,7,2),(1,8,3),(12,6,6),(4,7,7), \\ (7,6,11),(2,6,16),(12,11,1),(4,12,2),(7,11,6), \\ (2,11,11),(7,16,1),(2,16,6),(2,21,1) \end{array} \right\}.$$

$$\Gamma_4^+ = \left\{ \begin{array}{l} (17,1,1,1),(9,2,2,2),(1,3,3,3),(12,1,1,6),(4,2,2,7), \\ (7,1,1,11),(2,1,1,16),(12,1,6,1),(4,2,7,2),(7,1,6,6), \\ (2,1,6,11),(7,1,11,1),(2,1,11,6),(2,1,16,1),(12,6,1,1), \\ (4,7,2,2),(7,6,1,6),(2,6,1,11),(7,6,6,1),(2,6,6,6), \\ (2,6,11,1),(7,11,1,1),(2,11,1,6),(2,11,6,1),(2,16,1,1) \end{array} \right\}.$$

Exemplo 4.2.15. *considere a curva Norma-traço definida pela equação afim $y^{q^{r-1}} + \cdots + y^q + y = x^{\frac{q^r-1}{q-1}}$ sobre o corpo $\mathbb{F}_{q^r}$. Seja $P_\infty = (0:1:0)$ o ponto no infinto sobre a curva Norma-traço. Seja P_{ab} o zero em comum de $x-a$ e $y-b$, onde $a,b \in \mathbb{F}_{q^r}$. Denotamos por $P_1 = P_\infty, P_2 = P_{00}, P_3 = P_{0b_2}, \ldots, P_{q^{r-1}+1} = P_{0b_{q^{r-1}}}$, com $b_i^{q^{r-1}} + \cdots + b_i^q + b_i = 0, b_i \in \mathbb{F}_{q^r}$ para todo $2 \leqslant i \leqslant q^{r-1}$. Os divisores principais de x e y são:*

$$(x) = \sum_{i=2}^{q^{r-1}+1} P_i - q^{r-1}P_1, \quad (y) = \frac{q^r-1}{q-1}(P_{00} - P_1)$$

Tome $q=2, r=3$ e $m=4$, portanto $a=4$ e $b=7$. Pelo Teorema 4.2.12, temos que Γ_4^+ contém exatamente os seguintes elementos:

$13(6,0,0,0)+i(-9,1,1,1), i=1,\ldots,8,$
$13(5,1,0,0)+i(-9,1,1,1), i=1,\ldots,7,$
$13(5,0,1,0)+i(-9,1,1,1), i=1,\ldots,7,$
$13(5,0,0,1)+i(-9,1,1,1), i=1,\ldots,7,$
$13(4,2,0,0)+i(-9,1,1,1), i=1,\ldots,5,$
$13(4,0,2,0)+i(-9,1,1,1), i=1,\ldots,5,$
$13(4,0,0,2)+i(-9,1,1,1), i=1,\ldots,5,$
$13(4,1,1,0)+i(-9,1,1,1), i=1,\ldots,5,$
$13(4,1,0,1)+i(-9,1,1,1), i=1,\ldots,5,$
$13(4,0,1,1)+i(-9,1,1,1), i=1,\ldots,5,$
$13(3,3,0,0)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,0,3,0)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,0,0,3)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,1,2,0)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,1,0,2)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,0,1,2)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,2,1,0)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,2,0,1)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,0,2,1)+i(-9,1,1,1), i=1,\ldots,4,$
$13(3,1,1,1)+i(-9,1,1,1), i=1,\ldots,4,$

$13(2,4,0,0)+i(-9,1,1,1), i=1,2,$ $13(1,5,0,0)+(-9,1,1,1),$
$13(2,0,4,0)+i(-9,1,1,1), i=1,2,$ $13(1,0,5,0)+(-9,1,1,1),$
$13(2,0,0,4)+i(-9,1,1,1), i=1,2,$ $13(1,0,0,5)+(-9,1,1,1),$
$13(2,2,2,0)+i(-9,1,1,1), i=1,2,$ $13(1,4,1,0)+(-9,1,1,1),$
$13(2,2,2,0)+i(-9,1,1,1), i=1,2,$ $13(1,4,0,1)+(-9,1,1,1),$
$13(2,2,0,2)+i(-9,1,1,1), i=1,2,$ $13(1,1,0,4)+(-9,1,1,1),$
$13(2,0,2,2)+i(-9,1,1,1), i=1,2,$ $13(1,1,4,0)+(-9,1,1,1),$
$13(2,1,1,2)+i(-9,1,1,1), i=1,2,$ $13(1,0,1,4)+(-9,1,1,1),$
$13(2,1,2,1)+i(-9,1,1,1), i=1,2,$ $13(1,0,4,1)+(-9,1,1,1),$
$13(2,2,1,1)+i(-9,1,1,1), i=1,2,$ $13(1,0,3,2)+(-9,1,1,1),$
$13(2,0,1,3)+i(-9,1,1,1), i=1,2,$ $13(1,0,3,2)+(-9,1,1,1),$
$13(2,1,0,3)+i(-9,1,1,1), i=1,2,$ $13(1,0,2,3)+(-9,1,1,1),$
$13(2,0,3,1)+i(-9,1,1,1), i=1,2,$ $13(1,2,0,3)+(-9,1,1,1),$
$13(2,1,3,0)+i(-9,1,1,1), i=1,2,$ $13(1,2,3,0)+(-9,1,1,1),$
$13(2,3,1,0)+i(-9,1,1,1), i=1,2,$ $13(1,3,0,2)+(-9,1,1,1),$
$13(2,3,0,1)+i(-9,1,1,1), i=1,2,$ $13(1,3,2,0)+(-9,1,1,1),$

$13(1,1,1,3)+(-9,1,1,1),$ $13(1,1,2,2)+(-9,1,1,1),$
$13(1,1,3,1)+(-9,1,1,1),$ $13(1,2,1,2)+(-9,1,1,1),$
$13(1,3,1,1)+(-9,1,1,1),$ $13(1,2,2,1)+(-9,1,1,1).$

Referências Bibliográficas

[1] M. Abdón, H. Borges, and L. Quoos. Weierstrass points on Kummer extensions. *Advances in Geometry*, 2015.

[2] M. Abdón and F. Torres. On maximal curves in characteristic two. *Manuscripta Mathematica*, 99(1):39–53, 1999. https://doi.org/10.1007/s002290050161.

[3] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves: volume I*, volume 267. Springer Science & Business Media, 1985. https://doi.org/10.1007/978-1-4757-5323-3.

[4] C. Carvalho and F. Torres. On Goppa codes and Weierstrass gaps at several points. *Designs, Codes and Cryptography*, 35(2):211–225, 2005. https://doi.org/10.1007/s10623-005-6403-4.

[5] A. Castellanos and G. Tizziotti. On Weierstrass semigroup at m points on curves of the form $f(y) = g(x)$. *Journal of Pure and Applied Algebra*, 222(7):1803–1809, 2018. https://doi.org/10.1016/j.jpaa.2017.08.007.

[6] I. M. Duursma and S. Park. Delta sets for divisors supported in two points. *Finite Fields and Their Applications*, 18(5):865–885, 2012. https://doi.org/10.1016/j.ffa.2012.06.005.

[7] W. Fulton. Algebraic curves. *An introduction to Algebraic Geometry*, 2008.

[8] A. Garcia and R. Lax. Goppa codes and Weierstrass gaps. In *Coding theory and algebraic geometry*, pages 33–42. Springer, 1992. https://doi.org/10.1007/BFb0087991.

[9] A. Garcia and P. Viana. Weierstrass points on certain non-classical curves. *Archiv der Mathematik*, 46(4):315–322, 1986. https://doi.org/10.1007/BF01200462.

[10] O. Geil. On codes from norm–trace curves. *Finite Fields and Their Applications*, 9(3):351–371, 2003. https://doi.org/10.1016/S1071-5797(03)00010-8.

[11] D. Goldschmidt. *Algebraic functions and projective curves*, volume 215. Springer Science & Business Media, 2006.

[12] V. D. Goppa. *Geometry and codes*. Springer, 1988. https://doi.org/10.1007/978-94-015-6870-8.

[13] R. Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[14] M. Homma. The Weierstrass semigroup of a pair of points on a curve. *Archiv der Mathematik*, 67(4):337–348, 1996. https://doi.org/10.1007/BF01197599.

[15] M. Homma and S. J. Kim. Goppa codes with Weierstrass pairs. *Journal of Pure and Applied Algebra*, 162(2-3):273–290, 2001. https://doi.org/10.1016/S0022-4049(00)00134-1.

[16] N. Ishii. A certain graph obtained from a set of several points on a Riemann surface. *Tsukuba Journal of Mathematics*, 23(1):55–89, 1999. https://doi.org/10.21099/tkbjm/1496163776.

[17] S. J. Kim. On the index of the Weierstrass semigroup of a pair of points on a curve. *Archiv der Mathematik*, 62(1):73–82, 1994. https://doi.org/10.1007/BF01200442.

[18] S. Kondo, T. Katagiri, and T. Ogihara. Automorphism groups of one-point codes from the curves $y^q + y = x^{q^r+1}$. *IEEE Transactions on Information Theory*, 47(6):2573–2579, 2001. https://doi.org/10.1109/18.945272.

[19] H. Maharaj, G. L. Matthews, and G. Pirsic. Riemann–Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences. *Journal of Pure and Applied Algebra*, 195(3):261–280, 2005. https://doi.org/10.1016/j.jpaa.2004.06.010.

[20] G. L. Matthews. Weierstrass pairs and minimum distance of Goppa codes. *Designs, Codes and Cryptography*, 22(2):107–121, 2001. https://doi.org/10.1023/A:1008311518095.

[21] G. L. Matthews. The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve. In *International Conference on Finite Fields and Applications*, pages 12–24. Springer, 2003. https://doi.org/10.1007/978-3-540-24633-6_2.

[22] G. L. Matthews. Weierstrass semigroups and codes from a quotient of the Hermitian curve. *Designs, Codes and Cryptography*, 37(3):473–492, 2005. https://doi.org/10.1007/s10623-004-4038-5.

[23] C. Munuera, G. C. Tizziotti, and F. Torres. Two-point codes on Norm-Trace curves. In *Coding Theory and Applications*, pages 128–136. Springer, 2008. https://doi.org/10.1007/978-3-540-87448-5_14.

[24] J. Rosales. Fundamental gaps of numerical semigroups generated by two elements. *Linear Algebra and its Applications*, 405:200–208, 2005. https://doi.org/10.1016/j.laa.2005.03.014.

[25] H. Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[26] J. H. van Lint. Introduction to coding theory, volume 86 of. *Graduate Texts in Mathematics*, 1998. https://doi.org/10.1007/978-3-642-58575-3.