Cotas Superiores para o Número de Pontos Racionais e Aplicações às Torres de Corpos de Funções

Thiago Filipe da Silva

19 de agosto de 2010

Dados Internacionais de Catalogação-na-publicação (CIP)
(Biblioteca Central da Universidade Federal do Espírito Santo, ES, Brasil)

Silva, Thiago Filipe da, 1987-
S586c Cotas superiores para o número de pontos racionais e aplicações às torres de corpos de funções / Thiago Filipe da Silva. – 2010.
43 f.

Orientador: José Gilvan de Oliveira.
Dissertação (Mestrado em Matemática) – Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Curvas algébricas. 2. Funções algébricas. 3. Weierstrass, Pontos de. I. Oliveira, José Gilvan de. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

Cotas Superiores para o Número de Pontos Racionais e Aplicações às Torres de Corpos de Funções

Thiago Filipe da Silva

Dissertação submetida ao Programa de Pós-Graduação em Matemática da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do grau de Mestre em Matemática.

Aprovada em 19/08/2010 por:

Prof. Dr. Francesco Noseda, UFRJ

Prof. Dr. José Gilvan de Oliveira, UFES - Orientador

Prof. Dr^a Luciane Quoos Conte, UFRJ

Universidade Federal do Espírito Santo
Vitória, Agosto de 2010

Agradecimentos

A Deus

Aos Meus Pais

Ao professor José Gilvan de Oliveira (orientador)

Aos membros externos da Banca examinadora, professor Francisco Noseda e professora Luciane Quoos Conte

Aos amigos do mestrado

À Capes pelo apoio financeiro.

Resumo

O estudo sobre o número de pontos racionais de uma curva algébrica não-singular encontra diversas aplicações em Geometria Algébrica, teoria de códigos corretores de erros e criptografia. O objetivo dessa dissertação é obter cotas superiores para o número desses pontos a partir do trabalho Olav Geil e Ryutaroh Matsumoto [7]. Mostramos como são obtidas essas cotas, que elas dependem dos geradores do semigrupo de Weierstrass de algum ponto racional e que, em alguns casos, essas novas cotas melhoram a cota obtida anteriormente por Lewittes. Apresentamos algumas aplicações desses resultados no estudo de torres de corpos de funções e, finalmente, apresentamos um exemplo de uma torre assintoticamente ótima em característica 3, calculamos os gêneros e alguns semigrupos de Weierstrass nos primeiros níveis da torre.

Abstract

The study on the number of rational points of an nonsingular algebraic curve finds many applications in Algebraic Geometry, Algebraic Geometry Codes and Encryption. The aim of this paper is to obtain upper bounds for the number these points from the paper of Olav Geil and Ryutaroh Matsumoto [7]. We show how these bounds are obtained, depending of the generators of the Weierstrass semigroup of a rational point and that in some cases, the new bound improves the Lewittes's bound. We present some applications of these results in the study of towers of functions fields and, finally, we present an example of an asymptotically optimal tower in characteristic 3, we calculate the genus and some Weierstrass semigroups in the first levels of the tower.

Sumário

Capítulo 1

Introdução

Desde o início do século XX, um objeto de estudo de grande interesse dos matemáticos tem sido o de determinar o número de pontos racionais de uma curva algébrica sobre um corpo finito. Tal interesse tornou-se mais acentuado nas últimas décadas a partir do entendimento de que o conhecimento do número de pontos racionais de uma curva algébrica tem profundas aplicações na teoria dos códigos corretores de erros e na criptografia.

O primeiro resultado geral sobre a quantidade desses pontos foi obtido, em 1930, por Hasse para curvas elípticas. Ele provou o seguinte resultado que havia sido conjecturado por E. Artin em sua tese: Se E é uma curva elíptica definida sobre um corpo K com q elementos então a quantidade $|E(K)|$ de pontos racionais da curva satisfaz a desigualdade $||E(K)| - (q+1)| \leq 2\sqrt{q}$.

Em 1949, Weil fez uma série de conjecturas com alto nível de generalidade a respeito do número de pontos em variedades definidas sobre corpos finitos. Dentre elas destacamos a racionalidade da função Zeta, Equações Funcionais e a Hipótese de Riemann para curvas algébricas. Estas foram provadas por ele mesmo para variedades abelianas e curvas de gênero g qualquer mostrando que, o número N de pontos racionais de uma curva algébrica não-singular de gênero g, definida sobre um corpo finito com q elementos, obedece a desigualdade $|N - (q+1)| \leq 2g\sqrt{q}$. Esse resultado ficou conhecido como o Teorema de Hasse-Weil [5, p.120]. Mais tarde, Serre provou que $|N-(q+1)| \leq g\left\lfloor 2\sqrt{q}\right\rfloor$ [5, p.180]. Finalmente, em 1973, Deligne provou a Hipótese de Riemann.

Em [6], Lewittes exibiu uma cota superior para N usando apenas a multiplicidade do semigrupo de Weierstrass em um único ponto racional, o que serviu de motivação para o nosso trabalho.

O objetivo desta dissertação é obter cotas superiores para o número de pontos racionais de curvas algébricas seguindo [7]. O principal resultado

consiste em obter uma cota que depende de todos os geradores do semigrupo de Weierstrass de um único ponto racional. A partir disso, em alguns casos, será possível melhorar as cotas obtidas por Serre e Lewittes.

Uma outra questão a ser estudada é a seguinte: dado um corpo de constantes $\mathbb{F}_q$ com q elementos e um inteiro não-negativo g, encontrar uma cota superior para o maior número $N_q(g)$ para o qual existe um corpo de funções $F/\mathbb{F}_q$ de gênero g tal que $N(F) = N_q(g)$, onde $N(F)$ é o número de lugares racionais de $F/\mathbb{F}_q$.

A organização deste trabalho é a seguinte. Começamos o Capítulo 2 com uma introdução à Teoria dos Semigrupos Numéricos apresentando alguns resultados e depois estudando algumas propriedades dos chamados semigrupos simétricos e semigrupos telescópicos. No Capítulo 3 fazemos uma introdução à Teoria dos Corpos de Funções Algébricas com o fim de introduzirmos a notação e alguns resultados necessários para a compreensão da linguagem usada nos capítulos seguintes. No Capítulo 4 provamos o teorema principal. A partir de um semigrupo numérico Λ, obtemos uma cota superior para o número de lugares racionais, de um corpo de funções com algum lugar com semigrupo de Weierstrass igual a Λ, dependendo de todos os geradores de Λ e que generaliza um resultado de Lewittes. Finalmente, no Capítulo 5 fazemos algumas aplicações de resultados obtidos anteriormente em torres de corpos de funções. Mostramos que é impossível construir uma torre assintoticamente boa com uma infinidade de corpos de funções que possuem lugares racionais com semigrupos de Weierstrass telescópicos. Finalizamos o trabalho mostrando que a torre definida recursivamente pela equação $x_{n+1}^2 = \frac{1+x_n^2}{2x_n}$ é assintoticamente ótima quando $q = 9 = 3^2$ e explicitamos alguns semigrupos de Weierstrass no caso em que q é ímpar.

Capítulo 2

Semigrupos

Neste capítulo vamos desenvolver alguns resultados da Teoria de Semigrupos Numéricos que serão necessários para a compreensão dos próximos capítulos. Os conceitos de semigrupos simétricos e semigrupos telescópicos serão introduzidos na última seção vamos obter uma fórmula para o gênero de um semigrupo telescópico a partir de uma sequência geradora do semigrupo.

Os resultados obtidos neste capítulo podem ser encontrados em [4].

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

2.1 Semigrupos Numéricos

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

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

Para cada $\lambda \in \mathbb{N}_0$ define-se $\lambda + \Lambda = \{\lambda + x / \ x \in \Lambda\}$.

Proposição 2.1: *Sejam Λ um semigrupo numérico e $\lambda \in \Lambda$. Então*

$$|\Lambda - (\lambda + \Lambda)| = \lambda.$$

Demonstração: Visto que $\mathbb{N}_0 - \Lambda$ é finito então existe c condutor de Λ. Seja $g = |\mathbb{N}_0 - \Lambda|$ e considere os conjuntos $\mathcal{U} = \{t \in \Lambda / \ t < \lambda + c\}$ e $\mathcal{V} = \{v \in \lambda + \Lambda / \ \lambda \leq v < \lambda + c\}$. Logo $|\mathcal{U}| = \lambda + c - g$ e $|\mathcal{V}| = c - g$. Obviamente $\mathcal{V} \subset \mathcal{U}$. Vamos mostrar que $\mathcal{U} - \mathcal{V} = \Lambda - (\lambda + \Lambda)$. Com efeito, dado $t \in \mathcal{U} - \mathcal{V}$ qualquer, segue que $t \in \Lambda$ com $t < \lambda$ ou $t \notin \lambda + \Lambda$. Em qualquer dos casos $t \notin \lambda + \Lambda$. Reciprocamente, dado $t \in \Lambda - (\lambda + \Lambda)$ qualquer segue imediatamente que $t \notin \mathcal{V}$. Como $t \notin \lambda + \Lambda$ e c é o condutor de Λ então $t < \lambda + c$ e assim $t \in \mathcal{U}$.

Portanto, $\mathcal{U} - \mathcal{V} = \Lambda - (\lambda + \Lambda)$ e consequentemente $|\Lambda - (\lambda + \Lambda)| = |\mathcal{U} - \mathcal{V}| = |\mathcal{U}| - |\mathcal{V}| = (\lambda + c - g) - (c - g) = \lambda$. $\square$

Definição: *Dado H subconjunto não-vazio de $\mathbb{N}_0$ define-se o conjunto $\langle H \rangle = \{a_1 x_1 + ... + a_m x_m / \ x_1, ..., x_m \in H, \ a_1, ..., a_m \in \mathbb{N}_0 \ e \ m \in \mathbb{N}\}$ que claramente é um semigrupo de $\mathbb{N}_0$ e é chamado o semigrupo gerado por H. Quando H é finito e é escrito por $H = \{\lambda_1, ..., \lambda_m\}$ então usamos a notação $\langle \lambda_1, ..., \lambda_m \rangle$ para simbolizar $\langle H \rangle$.*

Um semigrupo Λ de $\mathbb{N}_0$ é dito *finitamente gerado* quando existem $m \in \mathbb{N}$ e $\lambda_1, ..., \lambda_m \in \Lambda$ tais que $\Lambda = \langle \lambda_1, ..., \lambda_m \rangle$.

Observação 2.2: *Se Λ é um semigrupo de $\mathbb{N}_0$ e H é um subconjunto não-vazio de Λ então $\langle H \rangle \subset \Lambda$. Isso segue imediatamente do fato de que Λ é fechado para a operação de adição.*

Proposição 2.3: *Se Λ é um semigrupo numérico de $\mathbb{N}_0$ então Λ é finitamente gerado.*

Demonstração: Como $\mathbb{N}_0 - \Lambda$ é finito existe c condutor de Λ. Considere os conjuntos $H = \{t \in \Lambda / \ t < c\}$ e $J = \{c, c+1, ..., c+(c-1)\}$ que são finitos. Segue que $H \cup J \subset \Lambda$ e, pela observação anterior, segue que $\langle H \cup J \rangle \subset \Lambda$. Vamos mostrar que $\Lambda \subset \langle H \cup J \rangle$. De fato, seja $\lambda \in \Lambda$ qualquer. Se $\lambda < c$ então $\lambda \in H$. Se $\lambda = c$ então $\lambda \in J$. Suponha $\lambda > c$. Do algoritmo da divisão de Euclides existem $l, r \in \mathbb{N}_0$ tais que $\lambda = l.c + r$, com $0 \leq r < c$. Visto que $\lambda > c$ então $l \geq 1$, ou seja, $l - 1 \in \mathbb{N}_0$. Assim $\lambda = (l-1).c + (c + r)$ e daí $\lambda \in \langle J \rangle \subset \langle H \cup J \rangle$.

Portanto, $\Lambda = \langle H \cup J \rangle$ o que conclui a demonstração. $\square$

Proposição 2.4: *Sejam $a, b \in \mathbb{N}$ com $mdc(a,b) = 1$ e $\Lambda = \langle a, b\rangle$. Então para cada $m \in \Lambda$ existem únicos $x, y \in \mathbb{N}_0$ tais que $m = xb + ya$ com $0 \leq x < a$.*

Demonstração: Dado $m \in \Lambda$ existem $x_0, y_0 \in \mathbb{N}_0$ tais que $m = x_0 b + y_0 a$. Do algoritmo da divisão de Euclides existem $q, x \in \mathbb{N}_0$ tais que $x_0 = qa + x$ com $0 \leq x < a$. Definindo $y = qb + y_0$ tem-se que $m = xb + ya$. Suponha que existam $x_1, y_1 \in \mathbb{N}_0$ tais que $m = x_1 b + y_1 a$ com $0 \leq x_1 < a$. Logo $(x - x_1)b = (y_1 - y)a$. Daí a divide $|x - x_1|.b$ e como $mdc(a,b) = 1$ então a divide $|x - x_1|$. Mas, $|x - x_1| < a$ e assim $|x - x_1| = 0$, ou seja, $x = x_1$ e portanto $y_1 = y$. $\square$

2.2 Semigrupos Telescópicos e Simétricos

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

Exemplos de semigrupos telescópicos:

(1) Seja $\Lambda = \langle 4, 6, 5\rangle$. Chame $a_1 = 4$, $a_2 = 6$ e $a_3 = 5$. Sendo $d_i = mdc(a_1, ..., a_i)$, $\forall i \in \{1, 2, 3\}$, segue que $d_1 = 4$, $d_2 = 2$ e $d_3 = 1$. Observe que $\frac{a_3}{d_3} = 5$, $\frac{a_1}{d_2} = 2$ e $\frac{a_2}{d_2} = 3$ e $5 = 1.2 + 1.3$. Portanto Λ é um semigrupo telescópico.

(2) Seja $\Gamma = \langle 34, 4, 62, 97\rangle$. Chame $a_1 = 34$, $a_2 = 4$, $a_3 = 62$ e $a_4 = 97$ e $d_i = mdc(a_1, ..., a_i)$, $\forall i \in \{1, 2, 3, 4\}$. Logo, $d_1 = 34$, $d_2 = 2$, $d_3 = 2$ e $d_4 = 1$. Observe que $\frac{a_4}{d_4} = 97$, $\frac{a_1}{d_3} = 17$, $\frac{a_2}{d_3} = 2$, $\frac{a_3}{d_3} = 31$ e $97 = 1.17 + 9.2 + 2.31$. Temos também que $\frac{a_3}{d_3} = 31$, $\frac{a_1}{d_2} = 17$, $\frac{a_2}{d_2} = 2$ e $31 = 1.17 + 7.2$. Portanto Γ é um semigrupo telescópico.

Observação 2.5: *É imediato verificar que se $(a_1, ..., a_k)$ é uma sequência telescópica com $d_i = mdc(a_1, ..., a_i)$, $\forall i \in \{1, ..., k\}$, então $(\frac{a_1}{d_i}, ..., \frac{a_i}{d_i})$ é uma sequência telescópica, $\forall i \in \{1, ..., k\}$.*

Proposição 2.6: *Sejam* $(a_1, ..., a_k)$ *uma sequência telescópica e* $\Lambda = \langle a_1, ..., a_k \rangle$ *com* $d_i = mdc(a_1, ..., a_i)$, $\forall i \in \{1, ..., k\}$. *Então para cada* $\lambda \in \Lambda$ *existem únicos* $x_1, ..., x_k \in \mathbb{N}_0$ *tais que* $\lambda = x_1a_1 + ... + x_ka_k$ *e* $0 \leq x_i < \frac{d_{i-1}}{d_i}$, $\forall i \in \{2, ..., k\}$.

Demonstração: Por indução sobre k. Para $k = 1$ o resultado é claramente verdadeiro e para $k = 2$ é imediato da Proposição 2.4. Suponha $k \geq 3$ e que o resultado seja válido para $k - 1$. Seja $\Gamma = \left\langle \frac{a_1}{d_{k-1}}, ..., \frac{a_{k-1}}{d_{k-1}} \right\rangle$ que pela Observação 2.5 é telescópico. Como $\lambda \in \Lambda$ existem $\beta_1, ..., \beta_k \in \mathbb{N}_0$ tais que $\lambda = \beta_1a_1 + ... + \beta_ka_k$. Tomando $\sigma = \beta_1\frac{a_1}{d_{k-1}} + ... + \beta_{k-1}\frac{a_{k-1}}{d_{k-1}}$ segue que $\sigma \in \Gamma$ e $\lambda = \beta_ka_k + d_{k-1}\sigma$. Do algoritmo da divisão existem $w, x_k \in \mathbb{N}_0$ tais que $\beta_k = wd_{k-1} + x_k$ com $0 \leq x_k < d_{k-1}$. Logo, $\lambda = x_ka_k + (wa_k + \sigma)d_{k-1}$ e como $wa_k + \sigma \in \Gamma$ então por hipótese de indução existem $x_1, ..., x_{k-1} \in \mathbb{N}_0$ tais que $wa_k + \sigma = x_1\frac{a_1}{d_{k-1}} + ... + x_{k-1}\frac{a_{k-1}}{d_{k-1}}$ e $0 \leq x_j < \frac{D_{j-1}}{D_j}$, $\forall j \in \{2, ..., k-1\}$ onde $D_j = mdc(\frac{a_1}{d_{k-1}}, ..., \frac{a_j}{d_{k-1}})$, $\forall j \in \{1, ..., k-1\}$. É claro que $\frac{D_{j-1}}{D_j} = \frac{d_{j-1}}{d_j}$ para todo $j \in \{2, ..., k-1\}$ e assim $\lambda = x_1a_1 + ... + x_ka_k$ com $0 \leq x_i < \frac{d_{i-1}}{d_i}$, $\forall i \in \{2, ..., k\}$.

Agora suponha que existam $y_1, ..., y_k \in \mathbb{N}_0$ tais que $\lambda = y_1a_1 + ... + y_ka_k$ e $0 \leq y_i < \frac{d_{i-1}}{d_i}$, $\forall i \in \{2, ..., k\}$. Seja $C = \{j \in \{1, ..., k\} / \ x_j \neq y_j\}$ e suponha por absurdo que $C \neq \varnothing$. Tome $l = \max C$. Logo $l > 1$ e $(x_l - y_l)a_l = (y_1 - x_1)a_1 + ... + (y_{l-1} - x_{l-1})a_{l-1}$ donde segue que $\frac{d_{l-1}}{d_l}$ divide $(x_l - y_l)\frac{a_l}{d_l}$. Como $mdc(\frac{a_l}{d_l}, \frac{d_{l-1}}{d_l}) = 1$ então $\frac{d_{l-1}}{d_l}$ divide $x_l - y_l$ e visto que $x_l - y_l \neq 0$ segue que $\frac{d_{l-1}}{d_l} \leq |x_l - y_l|$, absurdo pois $0 \leq x_l, y_l < \frac{d_{l-1}}{d_l}$.

Portanto $C = \varnothing$. $\square$

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

A seguir provaremos um resultado que caracteriza os semigrupos simétricos e que de certa forma justifica sua terminologia.

Proposição 2.7: *Seja* Λ *um semigrupo numérico de* $\mathbb{N}_0$ *de gênero* $g > 0$ *e condutor* c. *Então* $c \leq 2g$. Além disso, Λ *é simétrico se, e somente se, para todo* $s \in \mathbb{N}_0 - \Lambda$ *tem-se que* $c - 1 - s \in \Lambda$.

Demonstração: Considere os conjuntos $S = \{0, 1, ..., c-1\}$, $J = \{(t, c - 1 - t) / \ t \in S\}$, $H = \{(s, c - 1 - s) / \ s \in \mathbb{N}_0 - \Lambda\}$ e $L = \{(c - 1 - s, s) / \ s \in \mathbb{N}_0 - \Lambda\}$. Segue que $|J| = c$ e que $|H| = |L| = g$. Como c é o condutor de Λ então $H \subset J$ e $L \subset J$, ou seja, $H \cup L \subset J$. Afirmamos que $J \subset H \cup L$. De fato, seja $x \in J$ qualquer. Assim existe $t \in S$ tal que $x = (t, c - 1 - t)$.

Como $c-1 \notin \Lambda$ e Λ é um semigrupo de $\mathbb{N}_0$ então $t \notin \Lambda$ ou $c-1-t \notin \Lambda$. Se $t \notin \Lambda$ então $t \in \mathbb{N}_0 - \Lambda \Longrightarrow x \in H$. Suponha que $c-1-t \notin \Lambda$. Tomando $s_0 = c-1-t$ segue que $x = (c-1-s_0, s_0) \in L$. Logo $J \subset H \cup L$ e portanto $J = H \cup L$.

A primeira conclusão a partir disso é que $c = |J| = |H| + |L| - |H \cap L| = 2g - |H \cap L|$. Em particular $c \leq 2g$.

Considere o conjunto $Z = \{(s, c-1-s)/\ s \in \mathbb{N}_0 - \Lambda \text{ e } c-1-s \in \mathbb{N}_0 - \Lambda\}$. É fácil ver que $Z = H \cap L$ e assim:

Λ é simétrico $\Longleftrightarrow c = 2g \Longleftrightarrow Z = \varnothing \Longleftrightarrow$ para todo $s \in \mathbb{N}_0 - \Lambda$ tem-se que $c-1-s \in \Lambda$. $\square$

A seguir enunciamos uma proposição cuja demonstração é análoga à demonstração da Proposição 2.4.

Proposição 2.8: *Sejam $a, b \in \mathbb{N}$ com $mdc(a,b) = 1$. Então para cada $m \in \mathbb{Z}$ existem únicos $x, y \in \mathbb{Z}$ tais que $m = xb + ya$ com $0 \leq y < b$.*

O próximo resultado vai nos garantir que um semigrupo gerado por dois inteiros positivos primos entre si é um semigrupo numérico. Mais adiante vamos mostrar que esse semigrupo é também simétrico.

Proposição 2.9: *Sejam $a, b \in \mathbb{N}$ com $mdc(a,b) = 1$ e $\Lambda = \langle a, b \rangle$. Então:*

a) Para cada $m \in \mathbb{N}_0 - \Lambda$ existem únicos $x, y \in \mathbb{Z}$ tais que $m = xb + ya$ com $x < 0$ e $0 < y < b$;

b) O conjunto $\mathbb{N}_0 - \Lambda$ é finito, ou seja, Λ é um semigrupo numérico.

Demonstração: (a) Isso é consequência imediata da Proposição 2.8.

(b) Dado $m \in \mathbb{N}_0 - \Lambda$ qualquer, do ítem anterior existem $x, y \in \mathbb{Z}$ tais que $m = xb + ya$ com $x < 0$ e $0 \leq y < b$. Se $x < -a$ então $m = xb + ya < (-a)b + ya \leq -ab + (b-1)a = -a < 0$, contradição já que $m \in \mathbb{N}_0$. Logo, $-a \leq x < 0$ e portanto $\mathbb{N}_0 - \Lambda$ é finito. $\square$

Proposição 2.10: *Sejam $a, b \in \mathbb{N}$, com $mdc(a,b) = 1$, $\Lambda = \langle a, b \rangle$, c o condutor de Λ (cuja existência está garantida pela proposição anterior) e $g = |\mathbb{N}_0 - \Lambda|$. Então:*

a) Se $a, b \geq 2$ então $\max(\mathbb{N}_0 - \Lambda) = ab - a - b$. Em particular, $c = (a-1)(b-1)$;

b) O semigrupo Λ é simétrico e $g = \frac{(a-1)(b-1)}{2}$.

Demonstração: (a) Como $a, b \geq 2$ então $(b-1)a-b \geq 0$, ou seja, $(b-1)a-b \in \mathbb{N}_0$. Suponha por absurdo que $(b-1)a-b \in \Lambda$. Da Proposição 2.4 existem $x_0, y_0 \in \mathbb{N}_0$ tais que $-b+(b-1)a = x_0b+y_0a$ com $0 \leq y_0 < b$. Pela Proposição 2.8 segue $-1 = x_0$ e $b-1 = y_0$, contradição. Logo $(b-1)a-b \in \mathbb{N}_0 - \Lambda$. O fato de $(b-1)a-b$ ser o maior elemento em $\mathbb{N}_0 - \Lambda$ decorre imediatamente do ítem (a) da Proposição 2.9.

(b) Vamos mostrar que $c-1-s \in \Lambda$, $\forall s \in \mathbb{N}_0-\Lambda$. De fato, seja $s \in \mathbb{N}_0-\Lambda$ qualquer e suponha por absurdo que $c-1-s \in \mathbb{N}_0-\Lambda$. Pela Proposição 2.9 podemos escrever $s = x_1b+y_1a$ e $c-1-s = x_2b+y_2a$ com $x_1, x_2 \leq -1$ e $0 \leq y_1, y_2 \leq b-1$. Logo, $c-1 = ab-a-b = (x_1+x_2)b+(y_1+y_2)a$ e daí $(-x_1-x_2-1)b = (y_1+y_2-b+1)a$. Sendo $q := (-x_1-x_2-1)b$ positivo temos $q = (y_1+y_2-b+1)a \leq (b-1+b-1-b+1)a = (b-1)a < ab$. Por outro lado, visto que $mdc(a,b) = 1$ então b divide (y_1+y_2-b+1) donde segue que $q \geq ab$, absurdo. Portanto $c-1-s \in \Lambda$ e da Proposição 2.7 concluímos que Λ é um semigrupo simétrico. Assim $g = \frac{(a-1)(b-1)}{2}$. $\square$

A próxima proposição generaliza o resultado obtido no ítem (b) da Proposição 2.9.

Proposição 2.11: *Sejam $k \in \mathbb{N}$, $k \geq 2$, $a_1, ..., a_k \in \mathbb{N}$ tais que $mdc(a_1, ..., a_k) = 1$ e $\Lambda = \langle a_1, ..., a_k \rangle$. Então $\mathbb{N}_0 - \Lambda$ é finito.*

Demonstração: Para $k = 2$ já foi demonstrado na Proposição 2.9. Suponha por indução que $k \geq 3$ e que o resultado seja válido para $k-1$. Para cada $i \in \{1, ..., k\}$ seja $d_i = mdc(a_1, ..., a_i)$ e considere o semigrupo $\Gamma = \left\langle \frac{a_1}{d_{k-1}}, ..., \frac{a_{k-1}}{d_{k-1}} \right\rangle$. Visto que $mdc(\frac{a_1}{d_{k-1}}, ..., \frac{a_{k-1}}{d_{k-1}}) = 1$, por hipótese de indução segue que $\mathbb{N}_0 - \Gamma$ é finito. Considere os conjuntos $H = \{xd_{k-1} + ya_k / \ x \in \mathbb{N}_0-\Gamma \text{ e } 0 \leq y < d_{k-1}\}$ e $J = \{zd_{k-1}+ya_k / \ -a_k \leq z < 0 \text{ e } 0 \leq y < d_{k-1}\}$ que são finitos. Afirmamos que $\mathbb{N}_0 - \Lambda \subset H \cup J$. Com efeito, seja $t \in \mathbb{N}_0 - \Lambda$ qualquer. Como $mdc(a_k, d_{k-1}) = 1$ então da Proposição 2.8 existem $x, y \in \mathbb{Z}$ tais que $t = xd_{k-1} + ya_k$ com $0 \leq y < d_{k-1}$. Como $t \geq 0$ então $-a_k \leq x$. Se $x < 0$ então $t \in J$. Suponha $x \geq 0$. Se $x \in \Gamma$ então existem $y_1, ..., y_{k-1} \in \mathbb{N}_0$ tais que $x = y_1\frac{a_1}{d_{k-1}} + ... + y_{k-1}\frac{a_{k-1}}{d_{k-1}}$. Daí $xd_{k-1} \in \Lambda$ e assim $t \in \Lambda$, absurdo. Logo $x \in \mathbb{N}_0 - \Gamma$ e desse modo $t \in H$. Portanto $\mathbb{N}_0 - \Lambda$ é finito. $\square$

2.3 O gênero de um Semigrupo Telescópico

Daqui em diante vamos explorar algumas propriedades de um semigrupo telescópico encontrando uma equação que expressa o condutor em função apenas dos geradores do semigrupo. Mais adiante, provaremos que tais semigrupos são simétricos. Isso possibilita também uma equação para o gênero dependendo apenas dos geradores do semigrupo. Isto será usado no Capítulo 5 quando for provado que não é possível construir torres de corpos de funções assintoticamente boas com lugares racionais que tenham semigrupos de Weierstrass telescópicos.

Proposição 2.12: *Sejam* $k \in \mathbb{N}$, $k \geq 2$, $(a_1, ..., a_k)$ *uma sequência telescópica,* $\Lambda = \langle a_1, ..., a_k \rangle$, c *o condutor de* Λ *e* $d_i = mdc(a_1, ..., a_i)$, $\forall i \in \{1, ..., k\}$.

a) Se $\Gamma = \left\langle \frac{a_1}{d_{k-1}}, ..., \frac{a_{k-1}}{d_{k-1}} \right\rangle$ *e* d *é o condutor de* Γ *então*

$$c - 1 = d_{k-1}(d-1) + (d_{k-1} - 1)a_k.$$

b) $c - 1 = \sum_{i=1}^{k} (\frac{d_{i-1}}{d_i} - 1)a_i$, *onde* $d_0 = 0$.

Demonstração: (a) Seja $h = (d-1)d_{k-1} + (d_{k-1} - 1)a_k$. Como $mdc(a_k, d_{k-1}) = 1$ então, da Proposição 2.8, existem únicos $x', y' \in \mathbb{Z}$ tais que $h = x'd_{k-1} + y'a_k$ com $0 \leq y' < d_{k-1}$. Visto que d é o condutor de Γ então $d - 1 \notin \Gamma$. É claro que $h \in \mathbb{N}_0$. Suponha por absurdo que $h \in \Lambda$. Pela Proposição 2.6 existem $x_1, ..., x_k \in \mathbb{N}_0$ tais que $h = x_1a_1 + ... + x_ka_k$ com $x_i < \frac{d_{i-1}}{d_i}$, $\forall i \in \{2, ..., k\}$. Assim $0 \leq x_k < d_{k-1}$ e $h = (x_1\frac{a_1}{d_{k-1}} + ... + x_{k-1}\frac{a_{k-1}}{d_{k-1}})d_{k-1} + x_ka_k$ donde segue que $x' = x_1\frac{a_1}{d_{k-1}} + ... + x_{k-1}\frac{a_{k-1}}{d_{k-1}}$ e $y' = x_k$. Em particular $x' \in \Gamma$. Por outro lado, visto que $h = (d-1)d_{k-1} + (d_{k-1} - 1)a_k$ e $0 \leq d_{k-1} - 1 < d_{k-1}$ então $d - 1 = x'$ e $d_{k-1} - 1 = y'$ e assim $d - 1 \in \Gamma$, contradição. Logo, $h \in \mathbb{N}_0 - \Lambda$. Afirmamos que $h = \max(\mathbb{N}_0 - \Lambda)$. Com efeito, seja $t \in \mathbb{N}_0 - \Lambda$ qualquer. Pela Proposição 2.8 existem $x, y \in \mathbb{Z}$ tais que $t = xd_{k-1} + ya_k$ com $0 \leq y \leq d_{k-1} - 1$. Se $x < 0$ então $t = xd_{k-1} + ya_k < (d-1)d_{k-1} + ya_k \leq (d-1)d_{k-1} + (d_{k-1} - 1)a_k = h$. Suponha que $x \geq 0$. Como $t = xd_{k-1} + ya_k$ e $t \in \mathbb{N}_0 - \Lambda$ então $x \in \mathbb{N}_0 - \Gamma$ e daí $x \leq d-1$. Novamente segue que $t \leq h$. Portanto, $c - 1 = \max(\mathbb{N}_0 - \Lambda) = h = (d-1)d_{k-1} + (d_{k-1} - 1)a_k$.

(b) Pela Proposição 2.10 o resultado é verdadeiro para $k = 2$. Suponha por indução que $k \geq 3$ e que o resultado seja válido para $k - 1$. Temos que o semigrupo $\Gamma = \left\langle \frac{a_1}{d_{k-1}}, ..., \frac{a_{k-1}}{d_{k-1}} \right\rangle$ é telescópico. Sendo $e_j = mdc(\frac{a_1}{d_{k-1}}, ..., \frac{a_j}{d_{k-1}})$,

$\forall j \in \{1, ..., k-1\}$, segue que $d_{k-1}e_j = d_j$, $\forall j \in \{1, ..., k-1\}$. Como d é o condutor de Γ então por hipótese de indução temos que $d - 1 = \sum_{j=1}^{k-1}(\frac{e_{j-1}}{e_j} - 1)\frac{a_j}{d_{k-1}}$. Portanto $c - 1 = d_{k-1}(d-1) + (d_{k-1} - 1)a_k$

$= d_{k-1}(\sum_{j=1}^{k-1}(\frac{e_{j-1}}{e_j} - 1)\frac{a_j}{d_{k-1}}) + (d_{k-1} - 1)a_k = \sum_{i=1}^{k}(\frac{d_{i-1}}{d_i} - 1)a_i$. $\square$

Teorema 2.13: *Sejam $k \in \mathbb{N}$, $k \geq 2$, $(a_1, ..., a_k)$ uma sequência telescópica, $\Lambda = \langle a_1, ..., a_k \rangle$, $d_i = mdc(a_1, ..., a_i)$, $\forall i \in \{1, ..., k\}$ e $g = |\mathbb{N}_0 - \Lambda|$.*

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

b) O semigrupo Λ é simétrico. Em particular

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

Demonstração: (a) Seja $S = \{0, 1, ..., d_{k-1} - 1\}$. Para cada $v \in S$ seja $A(v) = \{va_k + d_{k-1}w / \ w \in \mathbb{N}_0 - \Gamma\}$. Logo $|A(v)| = g'$, $\forall v \in S$. Visto que $mdc(a_k, d_{k-1}) = 1$, a Proposição 2.8 nos diz que $\{A(v) / \ v \in S\}$ é uma coleção de conjuntos dois a dois disjuntos e portanto $\left|\bigcup_{v \in S} A(v)\right| = d_{k-1}g'$. Pelas Proposições 2.6 e 2.8 segue que $A(v) \subset \mathbb{N}_0 - \Lambda$, $\forall v \in S$. Sejam $L = \langle a_k, d_{k-1} \rangle$ e $\mathcal{U} = \{\alpha a_k + \beta d_{k-1} / \ \alpha \in S \text{ e } \beta \in \mathbb{Z} \text{ com } \beta < 0\}$. Assim $\mathcal{U} \subset \mathbb{N}_0 - \Lambda$ e das Proposições 2.4 e 2.8 concluímos que $\mathcal{U} = \mathbb{N}_0 - L$ e $\mathcal{U} \cap A(v) = \varnothing$, $\forall v \in S$. Pela Proposição 2.10 temos que $|\mathcal{U}| = \frac{(d_{k-1}-1)(a_k-1)}{2}$. Disto segue que $|\mathcal{U} \cup (\bigcup_{v \in S} A(v))| = |\bigcup_{v \in S} A(v)| + |\mathcal{U}| = d_{k-1}g' + \frac{(d_{k-1}-1)(a_k-1)}{2}$ e por observações anteriores já sabemos que $\mathcal{U} \cup (\bigcup_{v \in S} A(v)) \subset \mathbb{N}_0 - \Lambda$. Afirmamos que $\mathbb{N}_0 - \Lambda = \mathcal{U} \cup (\bigcup_{v \in S} A(v))$. De fato, seja $t \in \mathbb{N}_0 - \Lambda$ qualquer. Da Proposição 2.8 existem $x, y \in \mathbb{Z}$ tais que $t = ya_k + xd_{k-1}$ com $0 \leq y < d_{k-1}$, logo $y \in S$. Se $x < 0$ então $t \in \mathcal{U}$. Suponha $x \geq 0$. Suponha por absurdo que $x \in \Gamma$. Então existem $x_1, ..., x_{k-1} \in \mathbb{N}_0$ tais que $x = x_1\frac{a_1}{d_{k-1}} + ... + x_{k-1}\frac{a_{k-1}}{d_{k-1}}$, ou seja, $xd_{k-1} = x_1a_1 + ... + x_{k-1}a_{k-1}$. Assim $t \in \Lambda$, contradição. Logo, $x \in \mathbb{N}_0 - \Gamma$

e disto $t \in A(y) \subset \bigcup_{v \in S} A(v)$. Portanto, $\mathbb{N}_0 - \Lambda = \mathcal{U} \cup (\bigcup_{v \in S} A(v))$ e isso implica que $g = |\mathbb{N}_0 - \Lambda| = d_{k-1}g' + \frac{(d_{k-1}-1)(a_k-1)}{2}$.

(b) Para $k = 2$ é resultado imediato da Proposição 2.10. Suponha por indução que o resultado seja válido para $k-1$. Assim $\Gamma = \left\langle \frac{a_1}{d_{k-1}}, ..., \frac{a_{k-1}}{d_{k-1}} \right\rangle$ é simétrico, ou seja, sendo d o condutor de Γ temos que $d = 2g'$. Pela Proposição 2.12 segue que $c - 1 = d_{k-1}(d-1) + (d_{k-1} - 1)a_k$ e assim, pelo que provamos anteriormente concluímos que:

$g = d_{k-1}g' + \frac{(d_{k-1}-1)(a_k-1)}{2} = \frac{d_{k-1}(d-1)+(d_{k-1}-1)a_k+1}{2} = \frac{c}{2}$ e portanto Λ é simétrico.

Em particular, da Proposição 2.12 temos $g = \frac{1}{2}(1 + \sum_{i=1}^{k}(\frac{d_{i-1}}{d_i} - 1)a_i)$. $\square$

Desse modo, os semigrupos telescópicos $\langle 4, 6, 5\rangle$ e $\langle 34, 4, 62, 97\rangle$ considerados no início da seção 2.2 têm gênero 4 e 64, respectivamente.

Capítulo 3

Corpos de Funções Algébricas

Neste capítulo vamos enunciar alguns resultados que serão utilizados no decorrer deste trabalho e introduzir a linguagem básica para a teoria dos corpos de funções algébricas: valorizações, lugares, divisores, gênero e semigrupos de Weierstrass.

Todas as demonstrações dos resultados aqui enunciados podem ser encontradas em [5].

Em todo este capítulo K é um corpo arbitrário.

3.1 Anéis de Valorização Discreta e Lugares

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

O conjunto $\widetilde{K} := \{z \in F/\ z$ é algébrico sobre $K\}$ é um subcorpo de F que contém K e é chamado o *corpo das constantes de F/K*. Dizemos que K *é algebricamente fechado em F* quando $\widetilde{K} = K$.

Observação: *Os elementos de F que são transcendentes sobre K podem ser caracterizados da seguinte forma: $z \in F$ é transcendente sobre K se, e somente se, a extensão $F/K(z)$ é finita.*

Um exemplo simples de um corpo de funções é o *corpo de funções racional*: F/K é chamado racional se $F = K(x)$ para algum $x \in F$ transcendente sobre K.

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

(1) $K \subsetneq \mathcal{O} \subsetneq F$;

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

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

A seguir enunciamos alguns resultados que nos dão maiores informações sobre um anel de valorização e que vão permitir inserir o conceito de um *lugar* de um corpo de funções.

Proposição 3.1: *Seja* $\mathcal{O}$ *um anel de valorização de um corpo de funções* F/K. *Então:*

a) $\mathcal{O}$ *é um anel local, ou seja,* $\mathcal{O}$ *possui um único ideal maximal* $P = \mathcal{O} - \mathcal{O}^*$ *onde* $\mathcal{O}^*$ *é o grupo das unidades de* $\mathcal{O}$;

b) Seja $x \in F - \{0\}$. *Então:* $x \in P \iff x^{-1} \notin \mathcal{O}$;

c) Para o corpo $\widetilde{K}$ *das constantes de* F/K *temos que* $\widetilde{K} \subset \mathcal{O}$ *e* $\widetilde{K} \cap P = \{0\}$.

Proposição 3.2: *Seja* $\mathcal{O}$ *um anel de valorização de um corpo de funções* F/K *e seja* P *o único ideal maximal de* $\mathcal{O}$. *Então:*

a) P *é um ideal principal;*

b) Se $P = t\mathcal{O}$ *então cada* $z \in F - \{0\}$ *possui uma única representação na forma* $z = t^n u$ *para* $n \in \mathbb{Z}$ *e* $u \in \mathcal{O}^*$;

c) $\mathcal{O}$ *é um domínio de ideais principais. Mais precisamente, se* $P = t\mathcal{O}$ *e* I *é um ideal não-nulo de* $\mathcal{O}$ *então* $I = t^n\mathcal{O}$ *para algum* $n \in \mathbb{N}_0$.

Um anel que possui as propriedades da Proposição 3.2 é chamado um *anel de valorização discreta.*

Definição: *Um lugar P de um corpo de funções F/K é o único ideal maximal de algum anel de valorização $\mathcal{O}$ de F/K. Cada elemento $t \in P$ tal que $P = t\mathcal{O}$ é chamado uniformizante local de P (ou elemento primo de P).*

O conjunto $\mathbb{P}_F := \{P/P$ é um lugar de $F/K\}$ é o *conjunto dos lugares de* F/K.

Se $\mathcal{O}$ é um anel de valorização de F/K e P é o ideal maximal de $\mathcal{O}$ então $\mathcal{O}$ é unicamente determinado por P, a saber $\mathcal{O} = \{z \in F - \{0\}/z^{-1} \notin P\}$ conforme a Proposição 3.1(b). Assim, $\mathcal{O}_P := \mathcal{O}$ é chamado o *anel de valorização associado ao lugar* P.

Exemplo: *Considere novamente o corpo de funções racionais $K(x)/K$. Seja $p(x) \in K[x]$ um polinômio mônico e irredutível. Os conjuntos*

$$\mathcal{O}_{p(x)} = \{\tfrac{f(x)}{g(x)}/f(x), g(x) \in K[x] \text{ e } p(x) \nmid g(x)\} \text{ e}$$

$$\mathcal{O}_\infty = \{\tfrac{f(x)}{g(x)}/f(x), g(x) \in K[x],\ gr(f(x)) \leq gr(g(x))\}$$

são anéis de valorização de $K(x)/K$ cujos ideais maximais são, respectivamente:

$$P_{p(x)} = \{\tfrac{f(x)}{g(x)}/f(x), g(x) \in K[x],\ p(x)|f(x) \text{ e } p(x) \nmid g(x)\} \text{ e}$$

$$P_\infty = \{\tfrac{f(x)}{g(x)}/f(x), g(x) \in K[x] \text{ e } gr(f(x)) < gr(g(x))\}.$$

3.2 Valorizações em Corpos de Funções

Uma outra descrição de lugares pode ser dada em termos de valorizações.

Definição: *Uma valorização discreta, ou simplesmente valorização, de um corpo de funções F/K é uma função $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ que satisfaz as seguintes propriedades:*

(1) $v(x) = \infty \Longleftrightarrow x = 0$*;*

(2) $v(x.y) = v(x) + v(y)$, $\forall x, y \in F$*;*

(3) $v(x + y) \geq \min\{v(x), v(y)\}$, $\forall x, y \in F$*;*

(4) Existe $z \in F$ *tal que* $v(z) = 1$*;*

(5) $v(a) = 0$, $\forall a \in K - \{0\}$.

Nesse contexto o símbolo ∞ é apenas um elemento que não pertence a $\mathbb{Z}$ tal que $\infty + \infty = \infty + n = n + \infty = \infty$ e $\infty > m$, $\forall m, n \in \mathbb{Z}$. Pelas condições (2) e (4) segue imediatamente que $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ é sobrejetiva. A propriedade (3) é chamada *desigualdade triangular*.

O seguinte resultado é rico em aplicações e é comumente chamado *Desigualdade Triangular Estrita*.

Proposição 3.3: *Seja $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ uma valorização discreta em um corpo de funções F/K e sejam $x, y \in F$ com $v(x) \neq v(y)$. Então $v(x + y) = \min\{v(x), v(y)\}$.*

Definição: *Seja P um lugar de um corpo de funções F/K. Define-se uma função $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ da seguinte forma: Tome $t \in P$ um uniformizante local de P. Então cada $z \in F - \{0\}$ possui uma única representação na forma $z = t^n u$ com $u \in \mathcal{O}_P^*$ e $n \in \mathbb{Z}$. Definimos então $v_P(z) = n$ e $v_P(0) = \infty$.*

Vale ressaltar que a definição acima não depende da escolha do uniformizante local t. Com efeito, se $s \in P$ é outro uniformizante local então existe um invertível w em $\mathcal{O}_P$ tal que $t = w.s$. Assim, $z = t^n u = s^n(w^n u)$, onde $w^n u$ é um invertível em $\mathcal{O}_P$.

O teorema a seguir mostra que v_P é uma valorização discreta e expressa uma maneira de obter anéis de valorização e lugares em termos de valorizações e vice-versa.

Teorema 3.4: *Seja F/K um corpo de funções.*

a) Para um lugar P a função v_P definida acima é uma valorização discreta de F/K e mais:

$$\mathcal{O}_P = \{z \in F / v_P(z) \geq 0\};$$

$$\mathcal{O}_P^* = \{z \in F / v_P(z) = 0\};$$

$$P = \{z \in F / v_P(z) > 0\}.$$

Dessa forma, v_P é chamada a valorização correspondente (ou associada) ao lugar P.

b) Um elemento $x \in F$ é um uniformizante local de P se, e somente se, $v_P(x) = 1$.

c) Reciprocamente, suponha que $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ seja uma valorização discreta. Então o conjunto $P := \{z \in F / \ v(z) > 0\}$ é um lugar de F/K com anel de valorização correspondente igual a $\mathcal{O}_P = \{z \in F / v(z) \geq 0\}$.

d) Todo anel de valorização $\mathcal{O}$ de F/K é um subanel maximal próprio de F.

O último resultado nos diz que em um corpo de funções, os conceitos de lugares, anéis de valorização e valorizações discretas essencialmente são iguais.

Seja P um lugar de F/K e $\mathcal{O}_P$ o anel de valorização correspondente a P. Como P é um ideal maximal de $\mathcal{O}_P$ então o anel quociente $F_P = \frac{\mathcal{O}_P}{P}$ é um corpo. Para $x \in \mathcal{O}_P$ define-se $x(P) \in F_P$ como sendo a classe residual de x módulo P e para $x \in F - \mathcal{O}_P$ define-se $x(P) = \infty$ (novamente ∞ denota um elemento que não pertence a F_P). Pela Proposição 3.1 temos que $K \subset \mathcal{O}_P$ e $K \cap P = \{0\}$ donde segue que a aplicação $\varphi_P : K \longrightarrow F_P$, dada por $\varphi_P(x) = x(P)$, é um homomorfismo injetivo. Assim, o corpo K está mergulhado em F_P e de maneira natural temos que F_P é um K-espaço vetorial.

A proposição seguinte mostra que a dimensão de F_P como $K-$espaço vetorial é finita.

Proposição 3.5: *Sejam P um lugar de um corpo de funções F/K e $x \in P - \{0\}$. Então* $\dim_K F_P \leq [F : K(x)]$.

Seja P um lugar de um corpo de funções F/K. O inteiro positivo $\deg P := \dim_K F_P$ é chamado o *grau de P*. Um lugar de grau 1 é dito *lugar racional de F/K*.

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

O próximo teorema é uma aplicação do Lema de Zorn e é útil para responder sobre a existência de lugares de F/K.

Teorema 3.6: *Seja F/K um corpo de funções e R um subanel de F com $K \subseteq R \subseteq F$. Suponha que I seja um ideal não-nulo próprio de R. Então existe um lugar P tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Corolário 3.7: *Sejam F/K um corpo de funções e $z \in F$ transcendente sobre K. Então z possui pelo menos um zero e um pólo. Em particular, o conjunto dos lugares de F/K* não é vazio.

O próximo teorema é um resultado muito forte dentro da teoria de corpos de funções e nos informa sobre a independência de valorizações no seguinte sentido: Se $v_1, ..., v_n$ são valorizações discretas duas a duas distintas em F/K, $z \in F$ e se já conhecemos $v_1(z), ..., v_{n-1}(z)$ então nada podemos concluir a respeito de $v_n(z)$. Esse teorema é muitas vezes chamado de Teorema da Aproximação Fraca.

Teorema 3.8: *Sejam F/K um corpo de funções, $P_1, ..., P_n$ lugares dois a dois distintos, $x_1, ..., x_n \in F$ e $r_1, ..., r_n \in \mathbb{Z}$. Então existe $x \in F$ tal que $v_{P_i}(x - x_i) = r_i$, $\forall i \in \{1, ..., n\}$.*

Corolário 3.9: *Todo corpo de funções possui uma infinidade de lugares.*

O Teorema da Aproximação Fraca tem um importante papel na demonstração do seguinte resultado, que é comumente conhecido como Desigualdade Fundamental.

Teorema 3.10: *Sejam F/K um corpo de funções, $x \in F$ e $P_1, ..., P_r$ zeros de x. Então* $\sum_{i=1}^{r} v_{P_i}(x).\deg P_i \leq [F : K(x)]$.

Corolário 3.11: *Em um corpo de funções F/K, todo elemento $x \in F - \{0\}$ possui uma quantidade finita de zeros e pólos.*

3.3 Divisores e o Teorema de Riemann-Roch

No que segue neste capítulo vamos considerar que F/K é um corpo de funções com corpo de constantes igual a K.

Definição: *O grupo dos divisores de um corpo de funções F/K é definido (escrito aditivamente) como o grupo abeliano livre gerado pelos lugares de F/K e é denotado por $Div(F)$. Os elementos de $Div(F)$ são chamados de divisores de F/K. Em outras palavras, um divisor é uma soma formal $D = \sum_{P \in \mathbb{P}_F} n_P P$ com $n_P \in \mathbb{Z}$, $\forall P \in \mathbb{P}_F$ e $n_P = 0$ para quase todo $P \in \mathbb{P}_F$.*

Dados $D = \sum_{P \in \mathbb{P}_F} n_P P$ e $D' = \sum_{P \in \mathbb{P}_F} n'_P P$ divisores então $D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P)P$. O elemento neutro de $Div(F)$ é o divisor $0 := \sum_{P \in \mathbb{P}_F} r_P P$ com $r_P = 0$, $\forall P \in P_F$. Dados $Q \in \mathbb{P}_F$ e $D = \sum_{P \in P_F} n_P P$ definimos $v_Q(D) := n_Q$.

Uma ordem parcial em $Div(F)$ é definida por: $D_1 \leq D_2 \iff v_P(D_1) \leq v_P(D_2)$, $\forall P \in \mathbb{P}_F$. Se $D, D' \in Div(F)$ com $D \leq D'$e $D \neq D'$ então escrevemos $D < D'$.

Um divisor $D \geq 0$ é chamado *positivo* (ou *efetivo*). O grau de um divisor de D é definido como $\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \deg P$ e a função $\deg : Div(F) \longrightarrow \mathbb{Z}$ é um homomorfismo de grupos.

O Corolário 3.11 diz que um elemento não-nulo em F possui uma quantidade finita de zeros e pólos. Assim, a seguinte definição faz sentido.

Definição: *Seja $x \in F - \{0\}$. Sendo Z o conjunto dos zeros de x e N o conjunto dos pólos de x definimos:*

$(x)_0 := \sum_{P \in Z} v_P(x)P$ *como sendo o divisor dos zeros de x,*

$(x)_\infty := \sum_{P \in N} (-v_P(x))P$ *como sendo o divisor dos pólos de x e*

$(x) := (x)_0 - (x)_\infty$ *como sendo o divisor principal de x.*

Dessa forma, $(x)_0$ e $(x)_\infty$ são divisores efetivos e $(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P$.

Os elementos constantes não-nulos em F são caracterizados por:
$x \in K \iff (x) = 0$.

Proposição 3.12: *Todo divisor principal de F/K possui grau zero. Mais precisamente: Seja $x \in F - K$.* Então $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$.

Definição: *O conjunto $\mathcal{P}(F) := \{(x)/x \in F - \{0\}\}$ é chamado o grupo dos divisores principais de F/K. É claro que $\mathcal{P}(F)$ é um subgrupo de $Div(F)$ pois para $x, y \in F - \{0\}$ temos $(x) + (y) = (x.y)$ e $-(x) = (x^{-1})$.*

Para um divisor $A \in Div(F)$ definimos o *espaço de Riemann-Roch associado a A* por $\mathcal{L}(A) := \{x \in F - \{0\}/\ (x) \geq -A\} \cup \{0\}$.

A próxima proposição é uma reunião de alguns dos principais resultados a respeito do espaço de Riemann-Roch associado a um divisor de F/K.

Proposição 3.13: *Seja F/K um corpo de funções.*

a) $\mathcal{L}(A)$ é um espaço vetorial sobre K, $\forall A \in Div(F)$;

b) $\mathcal{L}(0) = K$;

c) Para cada divisor $A \in Div(F)$ o espaço $\mathcal{L}(A)$ possui dimensão finita como $K-$espaço vetorial, representada por $l(A)$.

Um dos problemas mais importantes na teoria de corpos de funções algébricas é calcular a dimensão $l(A)$. A resposta para essa questão é dada em um dos resultados mais importantes dessa teoria, a saber, o Teorema de Riemann-Roch.

O próximo resultado vai nos permitir definir o que vem a ser o gênero de um corpo de funções.

Proposição 3.14: *Existe uma constante* $\gamma \in \mathbb{Z}$ *tal que* $\deg A - l(A) \leq \gamma$, $\forall A \in Div(F)$.

Definição: *O gênero* g *de um corpo de funções* F/K *é definido por* $g := \max\{\deg A - l(A) + 1 / A \in Div(F)\}$.

Visto que $\mathcal{L}(0) = K$, o gênero de um corpo de funções sempre é um inteiro não-negativo.

Definição: *Um divisor* W *de um corpo de funções* F/K *é dito canônico quando* $\deg W = 2g - 2$ *e* $l(W) \geq g$.

A definição de divisor canônico dada acima é equivalente à definição feita em [5] (confira a Proposição 1.6.2 em [5]). Com isso podemos enunciar o Teorema de Riemann-Roch.

Teorema 3.15 (Riemann-Roch): Seja W um divisor canônico de F/K. Então, para todo $A \in Div(F)$ vale que $l(A) = \deg A + 1 - g + l(W - A)$.

O próximo resultado é comumente chamado de Teorema da Aproximação Forte e é uma consequência do Teorema de Riemann-Roch.

Teorema 3.16: *Sejam* $S \subsetneq \mathbb{P}_F$ *e* $P_1, ..., P_r \in S$, *com* $r \in \mathbb{N}$. *Sejam* $x_1, ..., x_r \in F$ *e* $n_1, ..., n_r \in \mathbb{Z}$. *Então existe um elemento* $x \in F$ *tal que* $v_{P_i}(x - x_i) = n_i$, $\forall i \in \{1, ..., r\}$ *com* $v_P(x) \geq 0$, $\forall P \in S - \{P_1, ..., P_r\}$.

Sejam F/K um corpo de funções e F'/F uma extensão de corpos. Seja $v' : F' \longrightarrow \mathbb{Z} \cup \{\infty\}$ uma valorização discreta. Como $v'(F - \{0\})$ é um subgrupo de $\mathbb{Z}$ então existe um inteiro positivo e tal que $v'(F - \{0\}) = e\mathbb{Z}$. Desse modo, a função $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ definida por $v(z) = \frac{1}{e}v'(z)$ é uma valorização discreta em F/K. Sendo $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ os correspondentes lugares de v e v', respectivamente, o inteiro positivo $e(P'|P) := e$ é chamado *indice de ramificação de* P' sobre P.

Teorema 3.17 (Riemann-Hurwitz): *Sejam* F/K *um corpo de funções de gênero* g *e* F'/F *uma extensão finita separável. Sejam* K' *o corpo das constantes de* F' *e* g' *o gênero de* F'/K'. *Se* $e(P'|P)$ *não é divisível por* $car(K)$ *para todos* $P \in \mathbb{P}_F$ *e* $P' \in \mathbb{P}_{F'}$ *com* $P'|P$ *então*

$$2g' - 2 = \frac{[F':F]}{[K':K]}(2g - 2) + \sum (e(P'|P) - 1).$$

3.4 O Teorema das Lacunas de Weierstrass

Definição: *Seja $P \in \mathbb{P}_F$. O conjunto $N(P) := \{n \in \mathbb{N}_0 /$ existe $x \in F - \{0\}$ tal que $(x)_\infty = nP\}$ é chamado o semigrupo de Weierstrass de P.*

É claro que, de fato $N(P)$ é um semigrupo de $\mathbb{N}_0$ pois se $x_1, x_2 \in F - \{0\}$ e $(x_1)_\infty = n_1 P$, $(x_2)_\infty = n_2 P$ então $(x_1.x_2)_\infty = (x_1)_\infty + (x_2)_\infty = (n_1 + n_2)P$.

O conjunto $N(P)$ também é chamado *conjunto das não-lacunas de P* e o conjunto $\mathbb{N}_0 - N(P)$ é chamado *conjunto das lacunas de P*. Uma outra maneira de descrever o conjunto das não-lacunas de um lugar P é observar que um inteiro não-negativo n pertence $N(P)$ se, e somente se, $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$.

O próximo resultado nos diz que o semigrupo de Weierstrass de um lugar é um semigrupo numérico, ou seja, o conjunto das lacunas de P é finito.

Proposição 3.18: *Sejam $P \in \mathbb{P}_F$ e g o gênero de F/K. Então para todo $n \geq 2g$ existe um elemento $x \in F$ tal que $(x)_\infty = nP$.*

Finalizamos o capítulo enunciando um teorema que será fundamental nos capítulos seguintes.

Teorema 3.19 *(Teorema das Lacunas de Weierstrass): Sejam F/K um corpo de funções com gênero $g > 0$ e P um lugar racional. Então P possui exatamente g lacunas.*

Capítulo 4

Cotas Superiores para o Número de Pontos Racionais

Anteriormente estudamos algumas propriedades de semigrupos numéricos e revisamos alguns resultados básicos da teoria de corpos de funções algébricas. O leitor assim terá maior familiaridade com certos conceitos que serão apresentados a seguir.

Nosso objetivo neste capítulo consiste em obter cotas superiores para o número de lugares racionais de um corpo de funções sobre um corpo finito. Isto será feito a partir de um tipo especial de semigrupo numérico, que são os semigrupos de Weierstrass.

4.1 O Teorema Principal

Seja $F/\mathbb{F}_q$ um corpo de funções sobre um corpo finito $\mathbb{F}_q$ com q elementos. Por questões técnicas vamos sempre assumir que o corpo das constantes de $F/\mathbb{F}_q$ é o corpo $\mathbb{F}_q$. Denotamos por $N(F)$ o número de lugares racionais de $F/\mathbb{F}_q$.

Para cada inteiro g não-negativo define-se $N_q(g)$ como sendo o maior número para o qual existe um corpo de funções $F/\mathbb{F}_q$ de gênero g tal que $N_q(g) = N(F)$.

Neste capítulo Λ é um semigrupo numérico de $\mathbb{N}_0$ com um número finito g de lacunas e é finitamente gerado por $\lambda_1, ..., \lambda_m$, com $0 < \lambda_1 < ... < \lambda_m$. O inteiro positivo λ_1 é chamado a multiplicidade de Λ.

Se existe um corpo de funções sobre $\mathbb{F}_q$ possuindo um lugar racional tal que seu semigrupo de Weierstrass é exatamente Λ então define-se $N_q(\Lambda) = \max\{N(F)/\ F$ é um corpo de funções sobre $\mathbb{F}_q$ com semigrupo de Weierstrass igual a Λ em algum lugar racional$\}$. Se tal corpo de funções não existe então define-se $N_q(\Lambda) = 0$.

Lewittes mostrou em [6] que se λ_1 é a multiplicidade de um semigrupo de Weierstrass de algum lugar racional de $F/\mathbb{F}_q$ então $N(F) \leq q\lambda_1 + 1$.

O principal teorema nesse capítulo consiste em obter uma cota superior para $N(F)$ dependendo não apenas da multiplicidade λ_1 mas também de todos os demais geradores de Λ. Veremos também que o resultado de Lewittes será uma consequência direta desse teorema.

Teorema 4.1: *Se $F/\mathbb{F}_q$ é um corpo de funções tal que existe $P \in \mathbb{P}_F$ racional com semigrupo de Weierstrass igual a Λ então*

$$N(F) \leq \left| \Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda)) \right| + 1.$$

Em particular tem-se

$$N_q(\Lambda) \leq \left| \Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda)) \right| + 1 \leq q\lambda_1 + 1.$$

Demonstração: Sejam $N = N(F)$ e $P_1, ..., P_{N-1}, P$ todos os lugares racionais de $F/\mathbb{F}_q$. Defina $L_t = \mathcal{L}(tP)$ o espaço de Riemann-Roch associado ao divisor tP para todo $t \in \mathbb{N}_0 \cup \{-1\}$ e $L = \bigcup_{t=0}^{\infty} L_t$. Em particular $L_{-1} = \{0\}$. Como Λ é o semigrupo de Weierstrass de P então $L_t = L_{t-1}$ se $t \in \mathbb{N}_0 - \Lambda$ e $\dim L_t = \dim L_{t-1} + 1$, se $t \in \Lambda$. Aqui, $\dim V$ denota a dimensão do espaço vetorial V sobre $\mathbb{F}_q$. Considere a função linear $\varphi : L \longrightarrow \mathbb{F}_q^{N-1}$ dada por $\varphi(f) = (f(P_1), ..., f(P_{N-1}))$ e defina $E_t = \varphi(L_t)$, para todo $t \in \mathbb{N}_0 \cup \{-1\}$.

Segue que $E_{-1} = \{0\}$ e $\dim E_t = \dim E_{t-1}$, para todo $t \in \mathbb{N}_0 - \Lambda$. Para $t \in \Lambda$ temos que $E_t = E_{t-1}$ ou $\dim E_t = \dim E_{t-1} + 1$.

Vamos mostrar que φ é sobrejetiva. Com efeito, seja $u \in \mathbb{F}_q^{N-1}$ qualquer. Então podemos escrever $u = (z_1(P_1), ..., z_{N-1}(P_{N-1}))$ com $z_j \in \mathcal{O}_{P_j}$, $\forall j \in \{1, ..., N-1\}$. Seja $S = \mathbb{P}_F - \{P\}$. Como $P_1, ..., P_{N-1} \in S$, pelo Teorema da Aproximação Forte concluímos que existe $z \in F$ tal que $v_{P_j}(z - z_j) = 1$,

$\forall j \in \{1, ..., N-1\}$ e $v_Q(z) \geq 0$, $\forall Q \in S - \{P_1, ..., P_{N-1}\}$. Daí $z \in L$ e $z(P_j) = z_j(P_j)$, $\forall j \in \{1, ..., N-1\}$ e consequentemente
$u = \varphi(z)$. Portanto, φ é sobrejetiva e para t suficientemente grande temos que $\dim E_t = N - 1$.

Considere o conjunto $J = \{t \in \Lambda / \dim E_t = \dim E_{t-1} + 1\}$. Como $\dim E_t = N - 1$ para t suficientemente grande então $|J| = N - 1$.

Vamos mostrar que $(\bigcup_{i=1}^{m}(q\lambda_i + \Lambda)) \subset \Lambda - J$. De fato, se $i \in \{1, ..., m\}$ e $t \in q\lambda_i + \Lambda$ então existe $\lambda \in \Lambda$ tal que $t = q\lambda_i + \lambda$. Considere $x_i \in L$ tal que $v_P(x_i) = -\lambda_i$. Temos que $E_t \subset E_{t-1}$. Com efeito, seja $f \in L_t$ qualquer. Se $f \in L_{t-1}$ nada a provar. Suponha que $f \notin L_{t-1}$. Tomando $g = x_i^{-q}.f$, temos que $g \in L_\lambda - L_{\lambda-1}$ e assim $f = x_i^q.g \in L_t - L_{t-1}$. Como $(x_i g)_\infty = (\lambda_i + \lambda)P$ então $x_i g \in L_{t-1}$. Logo $\varphi(f) = \varphi(x_i^q.g) = \varphi(x_i.g) \in E_{t-1}$ donde segue que $E_t \subset E_{t-1}$. Visto que $E_{t-1} \subset E_t$ então $E_t = E_{t-1}$, ou seja, $t \in \Lambda - J$. Portanto $(\bigcup_{i=1}^{m}(q\lambda_i + \Lambda)) \subset \Lambda - J$ e consequentemente $J \subset \Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))$.

Como $|J| = N(F) - 1$ então $N(F) \leq \left|\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))\right| + 1$.

Mas também $\left|\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))\right| \leq |\Lambda - (q\lambda_1 + \Lambda)|$ e pela Proposição 2.1 temos $|\Lambda - (q\lambda_1 + \Lambda)| = q\lambda_1$ donde segue a outra desigualdade. $\square$

4.2 Comparando Cotas Superiores

A cota de Serre implica que se Λ tem gênero g então $N_q(\Lambda) \leq g\left\lfloor 2\sqrt{q}\right\rfloor + q + 1$. Observe que a cota de Lewittes é melhor do que a cota de Serre se e somente se $\frac{\lambda_1 - 1}{g} < \frac{\left\lfloor 2\sqrt{q}\right\rfloor}{q}$. Esta última desigualdade ocorre sempre que o corpo $\mathbb{F}_q$ tem $2, 3$ ou 4 elementos. De fato, como a multiplicidade de um semigrupo numérico não pode exceder $g + 1$ então $\frac{\lambda_1 - 1}{g} \leq \frac{g}{g} = 1$. Mas, $\frac{\left\lfloor 2\sqrt{2}\right\rfloor}{2} = \frac{3}{2} > 1$, $\frac{\left\lfloor 2\sqrt{3}\right\rfloor}{3} = \frac{4}{3} > 1$ e $\frac{\left\lfloor 2\sqrt{4}\right\rfloor}{4} = \frac{5}{4} > 1$.

Exemplo: Seja $q = 2$ e considere o semigrupo numérico $\Lambda = \langle 8, 9, 20\rangle$.

Assim, $\lambda_1 = 8$, $\lambda_2 = 9$, $\lambda_3 = 20$ e $\Lambda = \{0, 8, 9, 16, 17, 18, 20, 24, 25, 26, 27, 28, 29, 32, 33, 34, 35, 36, 37, 38, 40, 41, ...\}$.

Logo, $2\lambda_1 + \Lambda = \{16, 24, 25, 32, 33, 34, 35, 36, 40, 41, 42, 43, 44, 45, 48, 49, 50, 51, 52, 53, 54, 56, ...\}$. Disto segue que $S := \Lambda - (2\lambda_1 + \Lambda) = \{0, 8, 9, 17, 18, 20, 26, 27, 28, 29, 35, 37, 38, 46, 47, 55\}$.

Observe que $2\lambda_2 + \Lambda = \{18, 26, 27, 34, 35, 36, 38, 42, 43, 44, 45, 46, 47, 50, 51, 52, 53, 54, 55, 56, 58, ...\}$ e daí $T := S - (2\lambda_2 + \Lambda) = \{0, 8, 9, 17, 20, 28, 29, 37\}$.

Como todos os elementos de T são menores do que 40 então $T-(2\lambda_3+\Lambda) = T - (40 + \Lambda) = T$.

Mas, $\Lambda - ((2\lambda_1 + \Lambda) \cup (2\lambda_2 + \Lambda) \cup (2\lambda_3 + \Lambda)) = T - (2\lambda_3 + \Lambda) = T$ e desse modo $|\Lambda - ((2\lambda_1 + \Lambda) \cup (2\lambda_2 + \Lambda) \cup (2\lambda_3 + \Lambda))| = 8$. Portanto, a nova cota obtida nesse caso é $8+1 = 9$ enquanto que a cota de Lewittes é $2\lambda_1 + 1 = 17$.

Nas tabelas abaixo constam outros exemplos comparando a cota de Lewittes com a nova cota obtida no Teorema 4.1, onde x é a cota de Lewittes e y é a nova cota obtida.

$\Lambda = \langle 8, 9, 20\rangle$
$g = 20$

q	x/y
2	17/9
3	25/16
4	33/25
8	65/65
9	73/73
16	129/129

$\Lambda = \langle 13, 14, 20\rangle$
$g = 42$

q	x/y
2	27/9
3	40/17
4	53/33
8	105/95
9	118/102
16	209/195

$\Lambda = \langle 10, 11, 20, 22\rangle$
$g = 45$

q	x/y
2	21/5
3	31/10
4	41/17
8	81/65
9	91/82
16	161/141

A seguinte proposição nos dá mais informações sobre o quanto pode ser boa a cota obtida no Teorema 4.1 e mostra que sua diferença com a cota de Lewittes não excede o gênero g.

Proposição 4.1: *Se* $\Lambda = \langle \lambda_1, ..., \lambda_m\rangle$ *é um semigrupo numérico então* $q\lambda_1 + 1 - g \leq \left|\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))\right| + 1 \leq \min\{q\lambda_1 + 1, q^m + 1\}$.

Demonstração: A primeira desigualdade decorre do fato que existem no máximo $q\lambda_1 - g$ elementos em Λ que são menores do que $q\lambda_1$ e que esses elementos pertencem a $\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))$. Para a última desigualdade, do Teorema 4.1, já temos que $\left|\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))\right| + 1 \leq q\lambda_1 + 1$. Considere o conjunto $L = \{b_1\lambda_1 + ... + b_m\lambda_m / \ 0 \leq b_i < q, \forall i \in \{1, ..., m\}\}$. Afirmamos que $\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda)) \subset L$. De fato, seja $t \in \Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))$ qualquer. Como

$t \in \Lambda$, então existem $a_1, ..., a_m \in \mathbb{N}_0$ tais que $t = a_1\lambda_1 + ... + a_m\lambda_m$. Suponha por absurdo que exista $j \in \{1, ..., m\}$ tal que $a_j \geq q$. Consequentemente existe $d \in \mathbb{N}_0$ de maneira que $a_j = q+d$ e $t = a_j\lambda_j + w$ onde $w = \sum_{k \neq j} a_k\lambda_k \in \Lambda$. Sendo $u = d\lambda_j + w$ concluímos que $u \in \Lambda$ e $t = a_j\lambda_j + w = (q+d)\lambda_j + w = q\lambda_j + (d\lambda_j + w) = q\lambda_j + u \in q\lambda_j + \Lambda$, contradição. Logo, $0 \leq a_i < q$, $\forall i \in \{1, ..., m\}$ donde segue que $t \in L$.

Portanto, $\left|\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))\right| \leq q^m$ o que conclui a prova da proposição. □

A seguir apresentamos um corolário do Teorema 4.1 que, sob certas condições, consegue melhorar efetivamente a cota de Lewittes.

Corolário 4.1: *Seja* $B = \{\lambda \in \Lambda \ / \ \lambda \in [\lambda_1 + 1, \lambda_1 + \left\lceil \frac{\lambda_1}{q} \right\rceil - 1]\}$. *Se* $t = |B|$ *então* $N_q(\Lambda) \leq q\lambda_1 - t + 1$.

Demonstração: Se $B = \varnothing$ então $t = 0$ e a desigualdade é verdadeira pelo Teorema 4.1. Suponha $B \neq \varnothing$. Para cada $\lambda \in B$ temos que $q\lambda \neq q\lambda_1 + \eta$ para qualquer $\eta \in \Lambda$ já que não existe um elemento não-nulo $\eta \in \Lambda$ com $\eta < \lambda_1$. Logo, $q\lambda \notin (q\lambda_1 + \Lambda)$ e visto que $\lambda \geq \lambda_1 + 1$ então $q\lambda \in q\lambda_j + \Lambda$, para algum $j \in \{1, ..., m\}$. Daí $q\lambda \in (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda)) - (q\lambda_1 + \Lambda)$. Assim, se J é o conjunto dos elementos $q\lambda$ com $\lambda \in B$ então $J \subset (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda) \cap (\Lambda - (q\lambda_1 + \Lambda))$ e $|J| = t$. Desse modo, a união disjunta $(\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))) \cup J$ está contida em $\Lambda - (q\lambda_1 + \Lambda)$ e daí $\left|\Lambda - (\bigcup_{i=1}^{m}(q\lambda_i + \Lambda))\right| \leq q\lambda_1 - t$. Pelo Teorema 4.1 concluímos que $N_q(\Lambda) \leq q\lambda_1 - t + 1$. □

No caso em que $\lambda_1 = g+1$ temos $\Lambda = \{0, g+1, g+2, ...\}$ e o número t do Corolário 4.1 é exatamente $\left\lceil \frac{g+1}{q} \right\rceil - 1$. Logo, $N_q(\Lambda) \leq q(g+1) + 2 - \left\lceil \frac{g+1}{q} \right\rceil$.

Observação: *Seja* c *o condutor de* Λ. *É claro que a nova cota coincide com a cota de Lewittes sempre que* $q\lambda_1 + c \leq q\lambda_2$. *Isso ocorre quando* $q\lambda_1 + 2g \leq q\lambda_2$ *já que* $c \leq 2g$.

Como a multiplicidade de um semigrupo Λ não pode exceder $g+1$ então pela cota de Lewittes temos $N_q(g) \leq q(g+1) + 1$. No próximo resultado

vamos explorar uma implicação do Teorema 4.1 para obter uma nova cota para o número $N_q(g)$.

Proposição 4.2: *Se $q \in \mathbb{N}$ é potência de um primo e g é um inteiro não-negativo então $N_q(g) \leq (q - \frac{1}{q})g + q + 2 - \frac{1}{q}$.*

Demonstração: Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero de g e $P \in \mathbb{P}_F$ racional. Seja Λ o semigrupo de Weierstrass de P. Pelo Teorema das Lacunas de Weierstrass temos que $|\mathbb{N}_0 - \Lambda| = g$ e assim Λ é finitamente gerado. Tome $\lambda_1, ..., \lambda_m \in \Lambda$ geradores de Λ com $0 < \lambda_1 < ... < \lambda_m$. Temos que $\lambda_1 \leq g + 1$. Seja $B = \{\lambda \in \Lambda \ / \ \lambda \in [\lambda_1 + 1, \lambda_1 + \left\lceil \frac{\lambda_1}{q} \right\rceil - 1]\}$ e $t = |B|$. Do Corolário 4.1 segue que $N(F) \leq q\lambda_1 - t + 1$. Considere o conjunto $J = \{h \in \mathbb{N}_0 \ / \ h \in [\lambda_1 + 1, \lambda_1 + \left\lceil \frac{\lambda_1}{q} \right\rceil - 1]\}$ que possui $|J| = \left\lceil \frac{\lambda_1}{q} \right\rceil - 1$ elementos. Sendo $M = \{l \in \mathbb{N}_0 - \Lambda \ / \ l > \lambda_1\}$, como não existem elementos não-nulos de Λ menores do que λ_1 então $|M| = g - (\lambda_1 - 1)$. Visto que J está contido na união disjunta $B \cup M$ então $\left\lceil \frac{\lambda_1}{q} \right\rceil - 1 \leq t + g - (\lambda_1 - 1)$ e assim $-t \leq -(\frac{\lambda_1}{q} + \lambda_1 - g - 2)$ donde concluímos que $N(F) \leq (q - \frac{1}{q})g + q + 2 - \frac{1}{q}$. Portanto, $N_q(g) \leq (q - \frac{1}{q})g + q + 2 - \frac{1}{q}$. $\square$

Uma aplicação direta da Proposição 4.2 é que $N_2(g) \leq \frac{3}{2}g + \frac{7}{2}$, $N_3(g) \leq \frac{8}{3}g + \frac{14}{3}$ e $N_4(g) \leq \frac{15}{4}g + \frac{23}{4}$ que são cotas muito melhores do que a cota de Serre para esses casos e, para gênero pequeno, competem até mesmo com a cota de Ihara.

Capítulo 5

Torres de Corpos de Funções

Neste capítulo vamos estudar um novo conceito que é muito utilizado na Teoria de Códigos Corretores de Erros que são as torres de corpos de funções.

5.1 Torres com Semigrupos Telescópicos

Uma sequência $(F^{(1)}/\mathbb{F}_q,\ F^{(2)}/\mathbb{F}_q, ...)$ de corpos de funções é chamada *torre* se $F^{(i)} \subset F^{(i+1)}$, $\forall i \in \mathbb{N}$. Escrevemos $N^{(i)} = N(F^{(i)})$ e $g^{(i)} = g(F^{(i)})$ (gênero de $F^{(i)}/\mathbb{F}$). Dizemos que uma torre de corpos de funções é assintoticamente boa quando $\lim\limits_{i\to\infty} g^{(i)} = \infty$ e $\lim\limits_{i\to\infty} \inf \frac{N^{(i)}}{g^{(i)}} = \kappa > 0$.

A seguir apresentamos um resultado que é uma consequência do Teorema 4.1 e da Proposição 4.1.

Proposição 5.1: *Seja* $(F^{(1)}/\mathbb{F}_q,\ F^{(2)}/\mathbb{F}_q, ...)$ *uma torre assintoticamente boa. Seja* $(P^{(1)}, P^{(2)}, ...)$ *uma sequência tal que* $P^{(i)}$ *é um lugar racional de* $F^{(i)}/\mathbb{F}_q$ *para cada* $i \in \mathbb{N}$. *Seja* $\lambda_1^{(i)}$ *a multiplicidade do semigrupo de Weierstrass* $\Lambda^{(i)}$ *de* $P^{(i)}$ *e* m_i *o número de geradores em alguma descrição de* $\Lambda^{(i)}$. *Então* $\lim\limits_{i\to\infty} \inf \frac{\lambda_1^{(i)}}{g^{(i)}} \geq \frac{\kappa}{q}$ *e* $\lim\limits_{i\to\infty} m_i = \infty$, *onde* $\lim\limits_{i\to\infty} \inf \frac{N^{(i)}}{g^{(i)}} = \kappa$.

Demonstração: Como $\lim\limits_{i\to\infty} g^{(i)} = \infty$ então $\lim\limits_{i\to\infty} \frac{1}{qg^{(i)}} = 0$. Do Teorema 4.1 temos que $N^{(i)} \leq q\lambda_1^{(i)} + 1$, $\forall i \in \mathbb{N}$, e assim $\frac{N^{(i)}}{qg^{(i)}} \leq \frac{\lambda_1^{(i)}}{g^{(i)}} + \frac{1}{qg^{(i)}}$, $\forall i \in \mathbb{N}$. Logo, $\lim\limits_{i\to\infty} \inf \frac{N^{(i)}}{qg^{(i)}} \leq \lim\limits_{i\to\infty} \inf(\frac{\lambda_1^{(i)}}{g^{(i)}} + \frac{1}{qg^{(i)}})$, ou seja, $\lim\limits_{i\to\infty} \inf \frac{\lambda_1^{(i)}}{g^{(i)}} \geq \frac{\kappa}{q}$.

Para a segunda parte, visto que $\kappa > 0$, então podemos tomar $\varepsilon \in \mathbb{R}$ com $0 < \varepsilon < \kappa$. Como $\kappa = \lim\limits_{i\to\infty} \inf \frac{N^{(i)}}{g^{(i)}}$ então existe $i_0 \in \mathbb{N}$ tal que $\kappa - \varepsilon < \frac{N^{(i)}}{g^{(i)}}$, para todo $i > i_0$. Da Proposição 4.1 temos que $N^{(i)} \leq q^{m_i} + 1$, $\forall i \in \mathbb{N}$. Logo,

para cada $i \in \mathbb{N}$ com $i > i_0$ tem-se $\kappa - \varepsilon < \frac{N^{(i)}}{g^{(i)}} \leq \frac{q^{m_i+1}}{g^{(i)}}$ donde segue que $q^{m_i} > (\kappa - \varepsilon)g^{(i)} - 1$. Assim, $\lim_{i\to\infty} q^{m_i} = \infty$ já que $\kappa - \varepsilon > 0$ e $\lim_{i\to\infty} g^{(i)} = \infty$. Portanto, $\lim_{i\to\infty} m_i = \infty$. $\square$

Para a construção de códigos geométricos de Goppa com bons parâmetros, além de encontrar uma base $\{f_1,\ f_2, ...\}$ do espaço vetorial $\mathcal{L}(iP)$ tal que $v_p(f_i) > v_P(f_{i+1})$, também é necessário calcular $f_i(P_j)$, o que geralmente é difícil mesmo quando se tem um conjunto de equações explicitamente dado. S. Miura em [1] e R. Pellikaan em [2], independentemente e simultaneamente, propuseram uma forma padrão de definir equações para curvas algébricas afins para que $f_i(P_j)$ pudesse ser calculado de maneira simples. Porém, J. Suzuki em [3] mostrou que o número de equações na forma padrão proposta por Miura e Pellikaan é mínimo se, e somente se, o semigrupo de Weierstrass de P é telescópico. Com isso, seria desejável encontrar torres de corpos de funções assintoticamente boas com semigrupos de Weierstrass telescópicos. O que vamos mostrar a seguir é que não existe tal torre.

Proposição 5.2: *Seja $(F^{(1)}/\mathbb{F}_q,\ F^{(2)}/\mathbb{F}_q, ...)$ uma torre de corpos de funções tal que para uma infinidade de índices i tem-se que $F^{(i)}$ possui um lugar racional $P^{(i)}$ com semigrupo de Weierstrass telescópico igual a $\Lambda^{(i)}$. Então a torre $(F^{(1)}/\mathbb{F}_q,\ F^{(2)}/\mathbb{F}_q, ...)$ não é assintoticamente boa.*

Demonstração: Seja $(\gamma_1^{(i)}, ..., \gamma_{m_i}^{(i)})$ uma sequência telescópica que gera $\Lambda^{(i)}$ com m_i menor possível com essa propriedade. Por [1] temos que $\{\gamma_1^{(i)}, ..., \gamma_{m_i}^{(i)}\}$ é um conjunto minimal gerador de $\Lambda^{(i)}$. Sendo $d_j^{(i)} = mdc(\gamma_1^{(i)}, ..., \gamma_j^{(i)})$ para todo $j \in \{1, ..., m_i\}$ segue da Proposição 2.6 que $\frac{d_{j-1}^{(i)}}{d_j^{(i)}} \geq 2$, $\forall j \in \{2, ..., m_i\}$.

Suponha por absurdo que a torre $(F^{(1)}/\mathbb{F}_q,\ F^{(2)}/\mathbb{F}_q, ...)$ seja assintoticamente boa. Para cada i seja $\lambda_1^{(i)} = \min\{\gamma_1^{(i)}, ..., \gamma_{m_i}^{(i)}\}$. Pela Proposição 5.1 existe $\kappa > 0$ tal que $\liminf_{i\to\infty} \frac{\lambda_1^{(i)}}{g^{(i)}} \geq \frac{\kappa}{q}$ e $\lim_{i\to\infty} m_i = \infty$. A partir da expressão obtida no Teorema 2.13 para $g^{(i)}$ concluímos que $m_i < \frac{2g^{(i)}}{\lambda_1^{(i)}} + 2$.

Seja $d = \liminf_{i\to\infty} \frac{\lambda_1^{(i)}}{g^{(i)}}$. Visto que $d \geq \frac{\kappa}{q} > 0$ então se pode tomar $\varepsilon > 0$ com $\varepsilon < d$. Daí existe $i_0 \in \mathbb{N}$ tal que $\frac{\lambda_1^{(i)}}{g^{(i)}} \geq d - \varepsilon$ para todo $i > i_0$. Como $d - \varepsilon > 0$ então $\frac{g^{(i)}}{\lambda_1^{(i)}} \leq \frac{1}{d-\varepsilon}$ para todo $i > i_0$. Portanto $m_i < \frac{2}{d-\varepsilon} + 2$, para todo $i > i_0$, o que contradiz o fato de que $m_i \longrightarrow \infty$ quando $i \longrightarrow \infty$. $\square$

5.2 Uma Torre Assintoticamente Ótima

Vamos estudar nesta seção um exemplo de uma torre de corpos de funções sobre o corpo $\mathbb{F}_q$, definida de maneira recursiva, que provaremos ser assintoticamente ótima no caso $q = 9$.

Uma torre $\mathcal{F}$ sobre o corpo finito $\mathbb{F}_q$ é assintoticamente ótima se $\lambda(\mathcal{F}) = \lim_{n\longrightarrow\infty} \frac{N(F^{(n)})}{g^{(n)}}$ atinge a chamada *constante de Ihara* $A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$.

O próximo teorema pode ser encontrado em [5, Teorema 7.1.3].

Teorema (A cota de Drinfeld-Vladut): *A constante de Ihara satisfaz*

$$A(q) \leq \sqrt{q} - 1.$$

Sejam $q = l^2$, onde l é uma potência de um primo ímpar, (x_n) uma sequência tal que $x_{n+1}^2 = \frac{1+x_n^2}{2x_n}$ e $F^{(n)} = \mathbb{F}_q(x_0, ..., x_n)$, $\forall n \in \mathbb{N}_0$, com x_0 transcendente sobre $\mathbb{F}_q$.
Considere a torre $\mathcal{F} = (F^{(0)}/\mathbb{F}_q, F^{(1)}/\mathbb{F}_q, ...)$ e seja $g^{(n)}$ o gênero de $F^{(n)}/\mathbb{F}_q$, $\forall n \in \mathbb{N}_0$.

Dado $\lambda \in \mathbb{F}_q \cup \{\infty\}$, considere a valorização $v_\lambda : F^{(0)} \longrightarrow \mathbb{Z} \cup \{\infty\}$ tal que $v_\infty(x_0) = -1$ e $v_\lambda(x_0 - \lambda) = 1$ se $\lambda \neq \infty$, e seja P_λ o correspondente lugar de v_λ em $F^{(0)}$. Se $v_\lambda^{(1)} : F^{(1)} \longrightarrow \mathbb{Z} \cup \{\infty\}$ é uma valorização acima de v_λ, com índice de ramificação $e_\lambda^{(1)}$ e correspondente lugar $P_\lambda^{(1)}$ em $F^{(1)}/\mathbb{F}_q$, então

$$v_\lambda^{(1)}(x_1) = \frac{e_\lambda^{(1)}}{2}(v_\lambda(1 + x_0^2) - v_\lambda(x_0)).$$

Vamos mostrar que são verdadeiras as seguintes afirmações:

(a) $F^{(n+1)}/F^{(n)}$ *é uma extensão separável de grau* 2 *para todo* $n \in \mathbb{N}_0$;

(b) $\mathbb{F}_q$ *é o corpo das constantes de* $F^{(n)}/\mathbb{F}_q$, $\forall n \in \mathbb{N}_0$.

Com efeito, pela equação $x_{n+1}^2 = \frac{1+x_n^2}{2x_n}$ e do fato da característica do corpo de base ser ímpar, temos que $[F^{(n+1)} : F^{(n)}] \leq 2$ e $F^{(n+1)}/F^{(n)}$ é separável para todo $n \in \mathbb{N}_0$. Seja P_∞ o polo de x_0. Tome $P_\infty^{(1)} \in \mathbb{P}_{F^{(1)}}$ tal que $P_\infty^{(1)}|P_\infty$ e seja $e_\infty^{(1)}$ o índice de ramificação de $P_\infty^{(1)}$ sobre P_∞. Observe que $v_\infty^{(1)}(x_1) = \frac{e_\infty^{(1)}}{2} v_\infty(\frac{1+x_0^2}{2x_0}) = -\frac{e_\infty^{(1)}}{2}$. Logo, $e_\infty^{(1)} = 2$ e $v_\infty^{(1)}(x_1) = -1$.

Prosseguindo indutivamente construímos uma sequência de lugares $P_\infty^{(n)} \in \mathbb{P}_{F^{(n)}}$ tal que $P_\infty^{(n+1)}|P_\infty^{(n)}$ e o índice de ramificação de $P_\infty^{(n+1)}$ sobre $P_\infty^{(n)}$ é $e_\infty^{(n+1)} = 2$, $\forall n \in \mathbb{N}_0$. Por [5, Teorema 3.1.11] temos que $[F^{(n+1)} : F^{(n)}] \geq e_\infty^{(n+1)} = 2$ donde segue que $[F^{(n+1)} : F^{(n)}] = 2$, $\forall n \in \mathbb{N}_0$. Portanto, (a) e (b) decorrem de [5, Proposição 7.2.15].

Visto que $q = l^2$ então existe $i \in \mathbb{F}_q$ tal que $i^2 = -1$.

O que faremos agora é explicitar alguns semigrupos de Weierstrass de $F^{(1)}/\mathbb{F}_q$, $F^{(2)}/\mathbb{F}_q$ e $F^{(3)}/\mathbb{F}_q$ calculando os correspondentes gêneros.

Vamos mostrar inicialmente que o semigrupo de Weierstrass de $P_\infty^{(1)}$ é $\Lambda^{(1)} = \langle 2, 3\rangle$ e que $g^{(1)} = 1$.

Com efeito, analogamente ao que fizemos anteriormente temos que $e_0^{(1)} = 2$ e $v_0^{(1)}(x_1) = -1$. Logo $v_0^{(1)}(x_0) = 2$ e $v_\infty^{(1)}(x_0) = -2$. Pela desigualdade triangular estrita temos $v_i(x_0) = \min\{v_i(x_0 - i), v_i(i)\} = 0$ e $v_i(x_0 + i) = \min\{v_i(x_0 - i), v_i(2i)\} = 0$. De maneira análoga $v_{-i}(x_0) = v_{-i}(x_0 - i) = 0$. Desse modo, $v_i^{(1)}(x_1) = \frac{e_i^{(1)}}{2}(v_i(x_0 - i) + v_i(x_0 + i)) = \frac{e_i^{(1)}}{2}$ e portanto $e_i^{(1)} = 2$ e $v_i^{(1)}(x_1) = 1$. Analogamente $e_{-i}^{(1)} = 2$, $v_{-i}^{(1)}(x_1) = 1$ e $v_\lambda^{(1)}(x_1) \geq 0$ para $\lambda \in \{0, \infty, i, -i\}$. Então podemos concluir que os divisores das funções x_0 e x_1 em $F^{(1)}$ são:

$$(x_0)^{(1)} = 2P_0^{(1)} - 2P_\infty^{(1)}$$

$$(x_1)^{(1)} = P_i^{(1)} + P_{-i}^{(1)} - P_0^{(1)} - P_\infty^{(1)}.$$

Dessa forma, $(x_0x_1)^{(1)} = P_i^{(1)} + P_{-i}^{(1)} + P_0^{(1)} - 3P_\infty^{(1)}$ e assim $2, 3 \in \Lambda^{(1)}$. Daí $g^{(1)} \leq 1$. Pela fórmula do gênero de Riemann-Hurwitz temos $2g^{(1)} - 2 \geq 2(-2) + 4 = 0$ o que implica $g^{(1)} \geq 1$. Portanto, $g^{(1)} = 1$ e $\Lambda^{(1)} = \langle 2, 3\rangle$. Além disso, os únicos lugares ramificados na extensão $F^{(1)}/F^{(0)}$ são P_∞, P_0, P_{-i} e P_i. Neste caso, a cota obtida no Teorema 4.1 para o número de lugares racionais de $F^{(1)}/\mathbb{F}_q$ é $2q + 1$.

Vamos mostrar que o gênero de $F^{(2)}/\mathbb{F}_q$ é $g^{(2)} = 3$ e que o semigrupo de Weierstrass do lugar $P_\infty^{(2)}$ em $F^{(2)}$ acima de $P_\infty^{(1)}$ é $\Lambda^{(2)} = \langle 3, 4\rangle$.

De fato, para cada $\lambda \in \mathbb{F}_q \cup \{\infty\}$, seja $v_\lambda^{(2)} : F^{(2)} \longrightarrow \mathbb{Z} \cup \{\infty\}$ uma valorização acima de v_λ com índice de ramificação $e_\lambda^{(2)}$ e correspondente lugar $P_\lambda^{(2)}$ em $F^{(2)}/F^{(1)}$. Então, de maneira análoga ao caso anterior concluímos

que $e_\lambda^{(2)} = 2$ se $\lambda \in \{\infty, 0, -i, i\}$, $v_{-1}^{(2)}(x_2) = e_{-1}^{(2)}$ e $v_\lambda^{(2)}(x_2) \geq 0$ se $\lambda \notin \{\infty, 0, -i, i, -1\}$.

Então podemos concluir que os divisores das funções x_0, x_1 e x_2 em $F^{(2)}$ são:

$$(x_0)^{(2)} = 4P_0^{(2)} - 4P_\infty^{(2)},$$

$$(x_1)^{(2)} = 2P_{-i}^{(2)} + 2P_i^{(2)} - 2P_0^{(2)} - 2P_\infty^{(2)} \text{ e}$$

$$(x_2)^{(2)} = \sum_{P_{-1}^{(2)}|P_{-1}} P_{-1}^{(2)} - P_0^{(2)} - P_\infty^{(2)} - P_i^{(2)} - P_{-i}^{(2)}.$$

Desse modo, $4 \in \Lambda^{(2)}$. Visto que $x_{n+1}^2 = \frac{1+x_n}{2x_n}$ então $(\frac{1+x_0}{x_2})^2 = 4x_0x_1$. Assim, $2(\frac{1+x_0}{x_2})^{(2)} = (x_0x_1)^{(2)} = 2P_{-i}^{(2)} + 2P_i^{(2)} + 2P_0^{(2)} - 6P_\infty^{(2)}$.

Logo, $(\frac{1+x_0}{x_2})^{(2)} = P_{-i}^{(2)} + P_i^{(2)} + P_0^{(2)} - 3P_\infty^{(2)}$ e daí $3 \in \Lambda^{(2)}$. Disto segue que $g^{(2)} \leq 3$. Pela fórmula do gênero de Riemann-Hurwitz temos que $2g^{(2)} - 2 \geq 2(2.1 - 2) + 4$ o que implica que $g^{(2)} \geq 3$. Portanto, $g^{(2)} = 3$ e $\Lambda^{(2)} = \langle 3, 4 \rangle$. Além disso os únicos lugares ramificados na extensão $F^{(2)}/F^{(1)}$ são $P_\infty^{(1)}$, $P_0^{(1)}$, $P_{-i}^{(1)}$ e $P_i^{(1)}$. Neste caso, a cota obtida no Teorema 4.1 para o número de lugares racionais de $F^{(2)}/\mathbb{F}_q$ é $3q + 1$.

Agora vamos motrar que $g^{(3)} = 9$ e que o semigrupo de Weierstrass do lugar $P_\infty^{(3)}$ em $F^{(3)}$ acima de $P_\infty^{(2)}$ é $\Lambda^{(3)} = \langle 6, 8, 11, 15 \rangle$.

Para isso, para cada $\lambda \in \mathbb{F}_q \cup \{\infty\}$, seja $v_\lambda^{(3)} : F^{(3)} \longrightarrow \mathbb{Z} \cup \{\infty\}$ uma valorização acima de v_λ com índice de ramificação $e_\lambda^{(3)}$ e correspondente lugar $P_\lambda^{(3)}$ em $F^{(3)}/F^{(2)}$. Então de maneira análoga aos casos anteriores concluímos que $e_\lambda^{(3)} = 2$ se $\lambda \in \{\infty, 0, -i, i, -1\}$ e $v_\lambda^{(3)}(x_3) \geq 0$ se $\lambda \notin \{\infty, 0, -i, i, -1\}$.

Desse modo, $(x_0)^{(3)} = 8P_0^{(3)} - 8P_\infty^{(3)}$. Observe que $v_\infty^{(3)}(\frac{1+x_0}{x_2}) = -6$ e, como $v_\lambda^{(3)}(\frac{1+x_0}{x_2}) \geq 0$ se $\lambda \neq \infty$, então $(\frac{1+x_0}{x_2})_\infty^{(3)} = 6P_\infty^{(3)}$.

Temos que $v_\infty^{(3)}(\frac{x_0(x_1+1)}{x_3}) = v_\infty^{(3)}(x_0) + 4v_\infty^{(1)}(x_1 + 1) - v_\infty^{(3)}(x_3) = -8 - 4 - (-1) = -11$ e, como $v_\lambda^{(3)}(\frac{x_0(x_1+1)}{x_3}) \geq 0$ se $\lambda \neq \infty$, então $(\frac{x_0(x_1+1)}{x_3})_\infty^{(3)} = 11P_\infty^{(3)}$.

Vemos também que $v_\infty^{(3)}(\frac{(x_0-1)^2}{x_3}) = 16v_\infty(x_0-1) - v_\infty^{(3)}(x_3) = -16-(-1) = -15$ e, como $v_\lambda^{(3)}(\frac{(x_0-1)^2}{x_3}) \geq 0$ se $\lambda \neq \infty$, então $(\frac{(x_0-1)^2}{x_3})_\infty^{(3)} = 15P_\infty^{(3)}$. Assim,

6, 8, 11, 15 $\in \Lambda^{(3)}$ e dessa forma $g^{(3)} \leq 9$. Mas, pela fórmula do gênero de Riemann-Hurwitz temos que $2g^{(3)} - 2 \geq 2(2.3 - 2) + 8 = 16$ donde segue que $g^{(3)} \geq 9$. Portanto, $g^{(3)} = 9$ e $\Lambda^{(3)} = \langle 6, 8, 11, 15 \rangle$. Além disso os únicos lugares ramificados na extensão $F^{(3)}/F^{(2)}$ são $P_{\infty}^{(2)}$, $P_0^{(2)}$, $P_{-i}^{(2)}$, $P_i^{(2)}$ e os quatro lugares acima de P_{-1}. Neste caso, a cota obtida pelo Teorema 4.1 para o número de lugares racionais de $F^{(3)}/\mathbb{F}_q$ é $6q + 1$.

Agora vamos analisar o caso $q = 3^2$ e mostrar que neste caso a torre $\mathcal{F}$ é assintoticamente ótima.

Visto que $g^{(2)} > 2$ então também da fórmula do gênero de Riemann-Hurwitz segue que $g^{(n)} \longrightarrow \infty$ quando $n \longrightarrow \infty$.

O corpo $\mathbb{F}_9$ pode ser representado por $\mathbb{F}_9 = \mathbb{F}_3(i)$ e assim
$\mathbb{F}_9 = \{0, \pm 1, \pm i, \pm(i+1), \pm(i-1)\}$. Neste caso o conjunto
$\Sigma = \{\pm(i+1), \pm(i-1)\}$ satisfaz as condições de [5, Corolário 7.2.21] e portanto a taxa de decomposição $\nu(\mathcal{F}/F^{(0)}) = \lim_{n\to\infty} \frac{N(F^{(n)})}{[F^{(n)}:F^{(0)}]}$ de $\mathcal{F}$ sobre $F^{(0)}$ satisfaz $\nu(\mathcal{F}/F^{(0)}) \geq |\Sigma| = 4$.

O conjunto Λ_0 de [5, Proposição 7.2.23] é dado por $\Lambda_0 = \{\infty, 0, \pm i\}$ como uma consequência direta de [5, Proposição 3.7.3]. Considere agora o conjunto $\Lambda = \{0, \infty, \pm 1, \pm i\} \subset \overline{\mathbb{F}_9} \cup \{\infty\}$. Observe que para todo $\beta \in \Lambda$, todas as soluções $\alpha \in \overline{\mathbb{F}_9} \cup \{\infty\}$ da equação $\frac{1+\alpha^2}{2\alpha} = \beta^2$ estão em Λ. Isso se verifica facilmente como segue:

Se $\beta = \infty$ então $\alpha = 0$ ou $\alpha = \infty$;
Se $\beta = 0$ então $\alpha = \pm i$;
Se $\beta = \pm 1$ então $\alpha = 1$;
Se $\beta = \pm i$ então $\alpha = -1$.

Além disso, por [5, Teorema 7.2.10(b)], o gênero da torre
$\gamma(\mathcal{F}/F^{(0)}) = \lim_{n\to\infty} \frac{g^{(n)}}{[F^{(n)}:F^{(0)}]}$ satisfaz $\gamma(\mathcal{F}/F^{(0)}) \leq -1 + \frac{|\Lambda|}{2} = -1 + 3 = 2$.

Portanto, por [5, Proposição 7.2.23] temos que $\lambda(\mathcal{F}) = \frac{\nu(\mathcal{F}/F^{(0)})}{\gamma(\mathcal{F}/F^{(0)})} \geq \frac{4}{2} = 2 = \sqrt{9} - 1$ atinge a cota de Drinfeld-Vladut e consequentemente a torre $\mathcal{F}$ é assintoticamente ótima.

Em [8], Garcia e Stichtenoth mostraram que a torre $\mathcal{F}$ é assintoticamente ótima para $q = p^2$ onde p é um primo ímpar qualquer.

Referências Bibliográficas

[1] Miura, S., *Linear codes on affine algebraic curves*,Trans. IEICE J81-A (1998) 1398-1421 (in Japanese).

[2] Pellikaan, R.,*On the existence of order functions*, J. Statist. Plann. Inference 94 (2001) 287-301.

[3] Suzuki, J., *Miura conjecture on affine curves*, Osaka J. Math 44 (2007) 187-196.

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

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

[6] Lewittes, J., *Places of degree one in Functions Fields over finite fields*, J. Pure Appl. Algebra 69 (1990) 177-183.

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

[8] Garcia, A., Stichtenoth, H., *On Tame Towers over Finite Fields*, J. Reine Angew. Math. 557 (2003), 53-80.

[9] Garcia, A., Stichtenoth, H., *Topics in Geometry, Coding Theory and Cryptography*, Algebra and Applications, Springer, 2007.