Universidade de Brasília
Departamento de Matemática

Dissertação de mestrado

Estimativa para distância mínima de códigos de *Goppa* utilizando as lacunas de *Weierstrass*

Mayra Camelo Madeira de Moura
Orientador: Hemar Godinho

Universidade de Brasília
Departamento de Matemática

Dissertação apresentada ao Instituto de Ciências Exatas da Universidade de Brasília, para a obtenção de Título de Mestre em Ciências, na Área de Matemática.

Estimativa para distância mínima de códigos de Goppa utilizando as lacunas de Weierstrass

Mayra Camelo Madeira de Moura

Orientador: Hemar Godinho

Brasília
Março de 2012

Universidade de Brasília
Departamento de Matemática

Comissão Julgadora:

Prof. Dr.
Cícero Carvalho – UFU

Prof. Dr.
Diego Marques – UnB

Prof. Dr.
Dimas José Gonçalves – UnB (Suplente)

Prof. Dr.
Hemar Godinho – UnB (Orientador)

“Nunca se esqueça de que os santos são pecadores que continuam tentando”

Nelson Mandela

Aos meus pais,
que sempre acreditaram
e nunca me deixaram desistir.

Ao meu avô Macedo,
que com suas empolgantes histórias,
nos fez querer ser brilhantes como ele.

Dois barcos

Quem bater primeiro a dobra do mar
Dá de lá bandeira qualquer
Aponta pra fé e rema
É, pode ser que a maré não vire
Pode ser do vento vir contra o cais
E se já não sinto teus sinais
Pode ser da vida acostumar
Será, Morena?
Sobre estar só, eu sei
Nos mares por onde andei
Devagar
Dedicou-se mais
O acaso a se esconder
E agora o amanhã, cadê?
Doce o mar, perdeu no meu cantar
Só eu sei...

LOS HERMANOS

Agradecimentos

AQUELES QUE PASSARAM PELO MEU CAMINHO, DE ALGUMA FORMA, INFLUENCIARAM EM QUEM EU SOU HOJE. A TODOS VOCÊS, O MEU MUITO OBRIGADA!

Agradeço a Deus, pois tudo que tenho foi provido por Ele;
Aos meus pais, por todo apoio, compreensão e paciência;
À minha irmã Iaiá, pelo companheirismo;
As minhas avós, pelo carinho de sempre;
Aos meus amigos de curso, por todo o suporte;
Aos meus amigos de outros tempos, por me mostrarem o outro lado da vida;
Aos membros da banca, pela especial atenção em revisar este texto;
Ao meu orientador, pela dedicação e coragem de encarar o desafio;
Ao professor Cícero Carvalho, pela imprescindível ajuda;
Ao professor Célius Magalhães, pelo ombro amigo;
Ao professor Nigel Pitt e todos os colegas de seminário, pela atenção e apoio;
A Gretchen Matthews, pelo artigo que nos serviu de base;
Ao CNPq, pelo suporte financeiro.

Resumo

Neste trabalho estudamos as características básicas de corpos de funções algébricas para compreendermos os *códigos de Goppa*. A partir daí, estudamos o conjunto das lacunas de Weierstrass para um par de pontos, com o objetivo de melhorar a cota para distância mínima para esses códigos, especialmente aqueles definidos sobre o corpo de funções hermitiano.

Introdução

Nesta dissertação o nosso objetivo é estudar os corpos de funções, sua associação com curvas algébricas e sua aplicação em códigos de Goppa.

Um código é composto por um alfabeto através do qual transmitimos informações. Um problema frequente é a ocorrência de ruídos no canal de transmissão, alterando o conteúdo original que foi transmitido. Sendo assim, é preciso alguma forma de detectar e corrigir esse erros. É nesse intuito que os códigos corretores de erros foram criados. A Teoria dos Códigos Corretores de Erros foi criada pelo matemático C.E. Shannon, do Laboratório Bell, num trabalho publicado em 1948. Os códigos corretores de erros são utilizados, por exemplo, em comunicações via satélite ou no armazenamento ótico de dados. O mecanismo que esses códigos utilizam para detectar e corrigir falhas na transmissão é a *distância mínima*, d. A medida desse parâmetro nos permite dizer até que ponto um código é capaz de detectar ou mesmo corrigir erros num código. Basicamente, quanto maior a distância mínima, mais erros podem ser detectados e corrigidos. O principal problema é que a medida que o tamanho do código aumenta, essa distância d tende a diminuir. Sendo assim, há uma vasta gama de trabalhos preocupados em obter uma distância mínima grande em relação ao comprimento do código.

Nesta dissertação vamos estudar uma certa classe de códigos corretores de erros, os códigos de Goppa. Isto porque, para essa classe de códigos, Goppa mostrou que é possível obter um código com bons parâmetros, utilizando o teorema de Riemann-Roch, um teorema clássico da geometria algébrica. Em particular, Goppa obteve uma cota inferior para a distância mínima. No artigo [1], Garcia, Kim e Lax construíram um código de Goppa considerando G um certo múltiplo de um ponto P da curva, o chamado código de um ponto. E com isso eles obtiveram uma estrutura na sequência das lacunas de G que lhes permitiu melhorar a cota de Goppa para esse caso. Arbarello, Cornalba, Griffiths e Harris [2] generalizaram a noção de sequência de lacunas estendendo-a para o chamado conjunto de *lacunas de Weierstrass* de um par de pontos numa curva. Isto também foi mostrado por Kim [3] e Homma [4].

Um código é dito ser um código de dois pontos quando G é um divisor efetivo que é uma combinação linear de dois pontos P_1, P_2 da curva. Matthews [5], partindo do resultado de Garcia, Kim e Lax [1] e usando o conhecimento do conjunto das lacunas de Weierstrass do par de pontos (P_1, P_2), obteve um melhoramento da cota de Goppa para códigos de dois pontos. Se

compararmos um código de dois pontos com um código de um ponto sobre a mesma curva e com mesma dimensão, veremos que o código de dois pontos fornece melhores parâmetros com tamanho menor. Isso porque o código de 2 pontos tem tamanho uma unidade a menos e sua distância mínima é maior ou igual a do código de um ponto. Logo temos mais confiabilidade usando menos bits (o comprimento é menor). Por isso temos interesse em estudar códigos de dois pontos.

Esta dissertação pode ser dividida em duas partes. A primeira parte, composta pelos capítulos 1,2 e 3, compõem os pré-requisitos básicos sobre corpos de funções e códigos de Goppa. Nesta parte, nos baseamos muito no Stichtenoth[6], mas também utilizamos alguns resultados de Goldschmidt [7] para diferenciais de Weil, Garcia [8] para curvas algébricas e Hefez e Villela [9] para teoria básica de códigos. A segunda é composta pelo capítulo 4 e nela estudamos Matthews [5]. Nessa parte, explicitamos o conjunto das lacunas Weierstrass de (P_1, P_2), com a ajuda de resultados de Kim [3]. Obtivemos assim uma estimativa melhor para a distância mínima dos códigos de Goppa do que a encontrada por Garcia, Kim e Lax [1], para o caso em que o corpo de funções é Hermitiano. Finalizamos o texto com alguns exemplos dos resultados obtidos.

Sumário

1

Lugares, Valorações e Divisores

1.1 Lugares

Durante todo este capítulo K representa um corpo qualquer.

Definição 1.1.1 (Corpo de Funções)**.** *Um Corpo de Funções Algébricas F/K de uma variável sobre K é uma extensão $F \supseteq K$ tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ que é transcendente sobre K. (Note que a extensão tem que ser feita sobre $K(x)$, pois sobre K essa extensão é infinita.) Chamaremos simplesmente de Corpo de Funções.*

Seja $\widetilde{K} := \{z \in F \mid z \text{ é algébrico sobre } K\}$. Claramente $\widetilde{K}$ é um subcorpo de F já que soma, produto, inverso de algébricos ainda é algébrico. $\widetilde{K}$ é chamado corpo de constantes de F/K.

Temos $K \subseteq \widetilde{K} \subsetneq F$ (já que F é uma extensão de $K(x)$ com x transcendente sobre K) e assim $F/\widetilde{K}$ também é um corpo de funções sobre $\widetilde{K}$.

Em [6] é dada uma maneira de caracterizar os elementos de F transcendentes sobre K:

$$z \in F \text{ é transcendente sobre } K \text{ se e somente se a extensão } F/K(z) \text{ é finita.} \tag{1.1}$$

Exemplo 1.1.2. *Um primeiro exemplo e também o mais simples de corpo de funções é o corpo de funções racionais, isto é, quando $F = K(x)$ para algum $x \in F$ transcendente sobre K. Cada elemento não nulo $z \in K(x)$ tem uma única representação*

$$z = a \cdot \prod_i p_i(x)^{n_i}, \tag{1.2}$$

onde $0 \neq a \in K$*, os polinômios* $p_i(x) \in K[x]$ *são mônicos, dois a dois distintos e irredutíveis e* $n_i \in \mathbb{Z}$*.*

Um corpo de funções é geralmente representado como uma extensão algébrica simples do corpo de funções racionais $K(x)$; i.e.: $F = K(x, y)$ onde $\varphi(y) = 0$ para algum polinômio irredutível $\varphi(T) \in K(x)[T]$.

Quando F não é um corpo de funções racionais, não é tão fácil decompor um elemento $z \in F$ em elementos irredutíveis, como acima, ou mesmo definir o que são elementos irredutíveis em F. De modo a formular esses problemas para um corpo de funções arbitrário, vamos definir anel de valorização e lugares.

Definição 1.1.3 (Anel de valorização)**.** *Um anel de valorização de um corpo de funções é um anel* $\vartheta \subseteq F$ *com as seguintes propriedades:*

1. $K \subsetneq \vartheta \subsetneq F$ *e*
2. *Para todo* $z \in F$ *temos* $z \in \vartheta$ *ou* $z^{-1} \in \vartheta$

A existência de ϑ *será mostrada no teorema (1.1.16)*

A definição de anel de valorização é motivada pela análise do caso $F = K(x)$, pois nesse caso temos: dado $p(x) \in K[x]$ um polinômio mônico e irredutível, considere o conjunto

$$\vartheta_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \not| g(x) \right\}$$

Daí, para qualquer polinômio de $K[x]$, ou ele ou seu inverso estão em $\vartheta_{p(x)}$. De fato, seja $\frac{f(x)}{g(x)} \in K[x]$ e vamos supor que $\frac{f(x)}{g(x)} \notin \vartheta_{p(x)}$. Sem perda de generalidade podemos assumir que mdc$(f, g) = 1$. Como $p(x)|g(x)$ então $p(x) \not| f(x)$, logo $\left(\frac{f(x)}{g(x)}\right)^{-1} = \left(\frac{g(x)}{f(x)}\right) \in \vartheta_{p(x)}$. Observe que se $q(x)$ é outro polinômio mônico irredutível então $\vartheta_{p(x)} \neq \vartheta_{q(x)}$.

Proposição 1.1.4. *Seja* ϑ *o anel de valorização do corpo de funções* F/K*. Então valem as seguintes afirmações:*

(a) ϑ *é um anel local, isto é,* ϑ *possui um único ideal maximal* $P = \vartheta \backslash \vartheta^*$ *onde* $\vartheta^* = \{z \in \vartheta \mid$ *existe um elemento* $\omega \in \vartheta$ *com* $zw = 1 \}$ *é o grupo das unidades de* ϑ*.*

(b) Seja $0 \neq x \in F$*. Então* $x \in P \Leftrightarrow x^{-1} \notin \vartheta$*.*

(c) Para o corpo de constantes $\widetilde{K}$ *de* F/K*temos* $\widetilde{K} \subseteq \vartheta$ *e* $\widetilde{K} \cap P = \{0\}$ *. Em outras palavras, todo elemento não nulo de* P *é transcendente sobre* K*.*

Demonstração. (a) Observe que se I é ideal próprio de ϑ então I não contém nenhuma unidade de ϑ, logo $I \subseteq P$. Assim, basta provar que P é um ideal de ϑ.

1. Seja $x \in \vartheta \backslash \vartheta^*$ e $z \in \vartheta$. Afirmação: $xz \notin \vartheta^*$. De fato, se $xz \in \vartheta^*$ então existe $w \in \vartheta^*$ tal que $xzw = 1$. Mas então $x(zw) = 1$ e como $zw \in \vartheta$ segue que $x \in \vartheta^*$. Absurdo. Logo vale a afirmação.

2. Sejam $x, y \in P$. Pela definição de ϑ, ou x/y ou y/x estão em ϑ. Assim, sem perda de generalidade podemos supor $x/y \in \vartheta$. Daí $1 + x/y \in \vartheta$. E assim $x + y = y(1 + x/y) \in P$ por (1).

Logo P é um ideal.

(b) Note que

$$x \in P \Leftrightarrow x \in \vartheta \text{ e } x \notin \vartheta^* \Leftrightarrow x^{-1} \notin \vartheta$$

(c) Seja $z \in \widetilde{K}$. Assuma que $z \notin \vartheta$. Então $z^{-1} \in \vartheta$. Daí como z^{-1} é algébrico sobre K existem elementos $a_1, \cdots, a_r \in K$ com

$$a_r(z^{-1})^r + \cdots + a_1(z^{-1}) + 1 = 0$$

Daí,

$$\begin{aligned} z^{-1}\left(a_r(z^{-1})^{r-1} + \cdots + a_1\right) &= -1 \\ z = -\left(a_r(z^{-1})^{r-1} + \cdots + a_1\right) &\in K[z^{-1}] \subseteq \vartheta \end{aligned}$$

Isso é uma contradição pois $z \notin \vartheta$. Daí $\widetilde{K} \subseteq \vartheta$. E note que $\widetilde{K} \cap P = \{0\}$, pois $\widetilde{K}$ sendo um corpo contido em ϑ, devemos ter $\widetilde{K} \subseteq \vartheta^*$ □

Lema 1.1.5. *Seja ϑ um anel de valorização de F/K, P seu ideal maximal e $0 \neq y \in P$. Sejam $y_1, \cdots, y_n \in P$ tais que $y_1 = y$ e $y_i \in y_{i+1}P$ para $i = 1, \cdots, n-1$. Então temos*

$$n \leq [F : K(y)] < \infty$$

Demonstração. Seja $y \in P \backslash \{0\}$. Como $P \cap \widetilde{K} = \{0\}$ segue que y é transcendente sobre K, logo por (1.1) temos que $[F : K(y)] < \infty$.

Agora basta mostrar que $y_1, \cdots, y_n$ são linearmente independentes sobre $K(y)$.

Suponha que exista uma combinação linear não trivial tal que

$$\sum_{i=1}^{n} \phi_i(y) y_i = 0, \text{ com } \phi_i(y) \in K(y),$$

Sem perda de generalidade podemos assumir $\phi_i(y) \in K[y]$ e mdc$(\phi_1(y), \cdots, \phi_n(y)) = 1$. Seja a_i o termo constante de $\phi_i(y)$ e defina $j_0 = \max\{i \mid 1 \leq i \leq n \text{ e } a_i \neq 0\}$.

Assim,

$$\sum_{i=1}^{m} \phi_i(y) y_i = 0 \Rightarrow \sum_{i \neq j_0}^{m} \phi_i(y) y_i = -\phi_{j_0}(y) y_{j_0} \tag{1.3}$$

Com $\phi_i(y) \in \vartheta$ (pois $K \subseteq \vartheta$ e $y \in P \subseteq \vartheta$).

Por hipótese, $y_i \in y_{i+1}P$, assim, $\dfrac{y_i}{y_{i+1}} \in P$. Da mesma forma, se $i < j_0$ então $\dfrac{y_i}{y_{j_0}} \in P$. E note que como $y = y_1$ segue que $\dfrac{y}{y_i} \in P$ para todo $i = 1, \cdots, n$.

Dividindo (1.3) por y_{j_0}, temos

$$-\phi_{j_0}(y) = \sum_{i<j_0} \phi_i(y) \frac{y_i}{y_{j_0}} + \sum_{i>j_0} \frac{\phi_i(y)}{y_{j_0}} y_i$$

Como $\dfrac{y_i}{y_{j_0}} \in P$ para $i < j_0$ e $\phi_i(y) \in \vartheta$, temos que

$$\sum_{i<j_0} \frac{y_i}{y_{j_0}} \in P.$$

Agora para $i > j_0$ sabemos que os polinômios $\phi_i(y)$ não tem termo constante, assim podemos escrever

$$\sum_{i>j_0} \frac{\phi_i(y)}{y_{j_0}} y_i = \sum_{i>j_0} \frac{y}{y_{j_0}} g_i(y) y_i$$

e $\dfrac{y}{y_{j_0}} \in P$ e $g_i(y) y_i \in \vartheta$, logo esse somatório também está em P. Portanto, $\phi_{j_0} \in P$.

Por outro lado $\phi_{j_0}(y) = a_{j_0} + y g_{j_0}(y)$ com $a_{j_0} \neq 0$ e $g_{j_0}(y) \in K[y] \in \vartheta$ e $y \in P$. Daí $y g_{j_0}(y) \in P$. E logo, pelo que vimos acima, $a_{j_0} = \phi_{j_0}(y) - y g_{j_0}(y) \in P$. Mas então $a_{j_0} \in P \cap K = \{0\}$. Absurdo, pois $a_{j_0} \neq 0$. Sendo assim, os $y_1, \cdots, y_n$ são linearmente independentes sobre $K(y)$

□

Teorema 1.1.6. *Seja ϑ o anel de valorização do corpo de funções F/K e seja P seu ideal maximal. Então vale:*

(a) P é um ideal principal.

(b) Se $P = t\vartheta$ então cada $0 \neq z \in F$ tem uma única representação na forma $z = t^n u$ para algum $n \in \mathbb{Z}$ e algum $u \in \vartheta^*$

(c) ϑ é um domínio de ideais principais. Mais precisamente: se $P = t\vartheta$ e $\{0\} \neq I \subseteq \vartheta$ é um ideal então $I = t^n\vartheta$ para algum $n \in \mathbb{N}$.

Todo anel com as propriedades acima é chamado *anel de valorização discreta*.

Para demonstrar esse teorema vamos precisar do lema (1.1.5)

Demonstração. (a) Suponha que P não é ideal principal. Então para $x_1 \in P, P \neq x_1\vartheta$. Daí existe $x_2 \in P \backslash x_1\vartheta$ e assim :

$$x_2 x_1^{-1} \notin \vartheta \;\Rightarrow\; (x_2 x_1^{-1})^{-1} = x_1 x_2^{-1} \in \vartheta.$$
$$\text{Logo } x_1 x_2^{-1} \in P \;\Rightarrow\; x_1 \in x_2 P$$

Fazendo isso recursivamente, temos $x_i \in x_{i+1}P$ para todo $i \geq 1$, logo temos uma sequência infinita tal que $x_i \in x_{i+1}P, i \geq 1$. Isso contradiz o lema (1.1.5).

(b) Se $z \in F$ então $z \in \vartheta$ ou $z^{-1} \in \vartheta$. Sem perda de generalidade suponha $z \in \vartheta$. Se $z \in \vartheta^*$ então $z = t^0 \cdot z$. Se $z \in P$ então $z = t \cdot v$. Suponha que exista $n > [F : K(x)]$ tal que $t^n | z$. Fazendo a sequência

$$x_1 \in t^{n-1}P \ , \ t^{n-1} \in t^{n-2}P \cdots$$

$$x_1 = z \ , \ x_2 = t^{n-1} \ , \ x_3 = t^{n-2} \ , \ \cdots \ , \ x_j = t^{n-(j-2)} \ , \ \cdots \ , \ x_{n+1} = t$$

pelo lema (1.1.5) temos $n \leq [F : K(x)]$ o que não ocorre nesse caso. Absurdo. Logo, existe um m máximo tal que $t^{m+1} \nmid z$.

Assim $z \in t^m\vartheta$. Daí $z = t^m \cdot u$, com $u \in \vartheta$. Vamos mostrar que u é uma unidade de ϑ. Se $u \notin \vartheta^*$ então $u \in P = t\vartheta$ e logo $u = t^m \cdot t \cdot u' = t^{m+1} \cdot u'$ com $u' \in \vartheta$. Isso contradiz a maximalidade de m. Logo $u \in \vartheta^*$.

A unicidade da representação segue da maximalidade de m.

(c) Seja $\{0\} \neq I \subseteq \vartheta$ um ideal. O conjunto $A := \{r \in \mathbb{N} \,|\, t^r \in I\}$ é não vazio, pois se $0 \neq x \in I$ então $x = t^r u$ com $u \in \vartheta^*$ e portanto $t^r = xu^{-1} \in I$. Como A é subconjunto dos naturais, existe elemento mínimo, logo seja $n := min(A)$. Queremos mostrar que $I = t^n\vartheta$. Note que $t^n\vartheta \subseteq I$ pois $t^n \in I$. Agora seja $y \in I$. Temos $y = t^s\omega$ com $\omega \in \vartheta^*$ e $s \geq 0$ (pelo item (b)) logo $t^s \in I$ e daí, pela minimalidade de n, $y = t^n \cdot t^{s-n}\omega \in t^n\vartheta$. Assim segue que $I = t^n\vartheta$.

□

Definição 1.1.7 (Lugares)**.** *Um lugar P do corpo de funções F/K é o ideal maximal de algum anel de valorização ϑ de F/K. Todo elemento t tal que $P = t\vartheta$ é chamado elemento primo para P. Denotaremos por $\mathbb{P}_F$ o conjunto de todos os lugares de F/K.*

Se ϑ é um anel de valorização de F/K e P é seu ideal maximal, então ϑ é unicamente determinado por P da seguinte forma: $\vartheta = \{z \in F \,|\, z^{-1} \notin P\}$ (conforme proposição (1.1.4(b))). Daí denotaremos por $\vartheta_P := \vartheta$ o *Anel de valorização do lugar P*.

Outra descrição útil dos lugares é em termos da valorização.

Definição 1.1.8. *Para um lugar $P \in F$ associamos a função $v_p : F \to \mathbb{Z} \cup \{\infty\}$ da seguinte maneira: Escolha um elemento primo t de P. Então todo $0 \neq z \in F$ tem uma única representação $z = t^n u$ com $u \in \vartheta^*$ e $n \in \mathbb{Z}$. Defina $v_P(z) := n$ e $v_P(0) = \infty$. Chamamos essa função de valorização em P.*

Observação: Note que a definição depende somente de P e não da escolha de t. De fato, se $P = t\vartheta = t'\vartheta$ então $t = t'\omega$ para algum $\omega \in \vartheta^*$. Daí $t^n u = (t'^n\omega^n)u = t'^n(\omega^n u)$ com $\omega^n u \in \vartheta^*$.

Teorema 1.1.9. *Seja F/Kum corpo de funções.*

(a) Um elemento $x \in F$ é um elemento primo de P se e só se $v_P(x) = 1$.

(b) Todo anel de valorização ϑ de F/Ké um subanel maximal próprio de F.

Demonstração. (a) Se x é um elemento primo a afirmação segue da definição de v_P. Agora se $v_P(x) = 1$ então $x = tu$ onde t é um elemento primo de P e $u \in \vartheta^*$. Assim $x\vartheta \subseteq P$ e $t = xu^{-1}$. Agora seja $z \in P$ qualquer. Como t é elemento primo de P segue que $z = t\omega = xu^{-1}\omega = x\omega'$ onde $\omega u^{-1} = \omega' \in \vartheta^*$. Logo $z \in x\vartheta$ e assim $P \subseteq x\vartheta$. Portanto $P = x\vartheta$, i.e., x é elemento primo de P.

(b) Seja ϑ um anel de valorização, P seu ideal maximal, v_P a valorização associada a P. Queremos mostrar que se A é um anel tal que $\vartheta \subsetneq A \subseteq F$ então $A = F$.

Vamos supor que $z \in A \backslash \vartheta$, logo $\vartheta \subseteq \vartheta[z] \subseteq A \subseteq F$. Seja $y \in F$ qualquer, por hipótese, $z^{-1} \in \vartheta$ então $v(z^{-1}) = -v(z) > 0$. Note que, $v(yz^{-k}) = v(y) - kv(z)$ e assim existe $k \in \mathbb{N}$ tal que $v(yz^{-k}) \geq 0$, ou seja, $yz^{-k} = w \in \vartheta$. Então, $y = z^k w \in \vartheta[z]$. Logo $F \subseteq \vartheta[z]$, e assim $F = \vartheta[z]$.

□

Observação 1.1.10. *Seja P um lugar de F/Ke seja ϑ_P seu anel de valorização. Como P é um ideal maximal, o anel das classes residuais ϑ_P/P é um corpo. Para $x \in \vartheta_P$ nós definimos $x(P) \in \vartheta_P/P$ como sendo a classe residual de x módulo P, para $x \in F \backslash \vartheta_P$ nós fazemos $x(P) := \infty$ (note que o símbolo ∞ é usado aqui com um sentido diferente do que na definição de valorização). Pela proposição (1.1.4) sabemos que $K \subseteq \vartheta_P$ e que $K \cap P = \{0\}$, então a aplicação $\vartheta_P \to \vartheta_P/P$ induz uma imersão de K em ϑ_P/P. Assim, vamos sempre considerar K como um subcorpo de ϑ_P/P. Como este mesmo argumento se aplica para o corpo de constantes $\widetilde{K}$, da mesma forma podemos considerar $\widetilde{K}$ como um subcorpo de ϑ_P/P.*

Definição 1.1.11 (Grau e corpo residual)**.** *Seja $P \in \mathbb{P}_F$*

(a) O corpo $F_P := \vartheta_P/P$ é chamado o corpo de resíduos (ou de classes) de P. A aplicação $x \mapsto x(P)$ de F para $F_P \cup \{\infty\}$ é chamada aplicação classe residual com respeito a P. Algumas vezes vamos usar a notação $x + P := x(P)$ para $x \in \vartheta_P$.

(b) Dizemos que deg $P = [F_P : K]$ ou $gr\,(P)$ é o grau de P. Um lugar de grau um é também chamado de lugar racional de F/K.

O grau de um lugar é finito; Mais precisamente vale o seguinte:

Proposição 1.1.12. *Se P é um lugar de F/Ke $0 \neq x \in P$ então*

$$\textit{deg}\, P \leq [F : K(x)] < \infty$$

Demonstração. Note que, como estamos tomando $x \in P$, x é transcendente e daí por (1.1) temos $[F : K(x)] < \infty$.

Para mostrar que deg $P \leq [F : K(x)]$ mostraremos que quaisquer elementos $z_1, \cdots, z_n \in \vartheta_P$, cujas classes residuais $z_1(P), \cdots, z_n(P) \in F_P$ são linearmente independentes sobre K, são independentes sobre $K(x)$.

Suponha que exista uma combinação linear não-trivial

$$\sum_{i=1}^{n} \varphi_i(x) z_i = 0 \tag{1.4}$$

com $\varphi_i(x) \in K(x)$. Sem perda de generalidade podemos assumir que $\varphi_i(x)$ são polinômios em x e nem todos eles divisíveis por x; i.e., $\varphi_i(x) = a_i + x g_i(x)$ com $a_i \in K$ e $g_i(x) \in K[x]$ e nem todos os $a_i = 0$. Como $x \in P$ e $g_i(x) \in \vartheta_P$, segue que $\varphi_i(x)(P) = a_i(P) = a_i$. Usando a aplicação classe residual em (1.4) temos

$$0 = 0(P) = \sum_{i=1}^{n} \varphi_i(x)(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P)$$

onde nem todos os a_i são zero. Mas isso contradiz o fato de que os $z_1(P), \cdots, z_n(P)$ são linearmente independentes sobre K.

□

Corolário 1.1.13. *O corpo das constantes $\widetilde{K}$ de F/Ké uma extensão finita de K.*

Demonstração. Usaremos os fato (que será provado mais adiante em (1.1.17)) de que $\mathbb{P}_F \neq \emptyset$. Tome $P \in \mathbb{P}_F$. Como $\widetilde{K}$ está imerso em F_P via a aplicação classe residual $\vartheta_P \mapsto F_P$ segue que $[\widetilde{K} : K] \leq [F_p : K] \leq [F : K(x)] < \infty$. □

Observação 1.1.14. *Seja P um lugar racional de F/K, i.e., deg $P = 1$. Então temos $F_P = K$ e a aplicação classe residual leva F em $K \cup \{\infty\}$. Em particular, se K é um corpo algebricamente fechado, então $F_P = K$, logo todos os lugares são racionais e assim podemos ver um elemento $z \in F$ como uma função*

$$z : \begin{cases} \mathbb{P}_F & \to & K \cup \{\infty\} \\ P & \mapsto & z(P) \end{cases} \tag{1.5}$$

Esta é a razão pela qual chamamos F/K de Corpo de Funções. Os elementos de K, quando interpretados como funções da forma dada em (1.5) são funções constantes. Por essa razão K é chamado o corpo das constantes de F. A terminologia “zeros”e “pólos”a seguir também é justificada por (1.5).

Definição 1.1.15 (Zeros e Pólos)**.** *Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z se $v_P(z) > 0$; é um pólo se $v_P(z) < 0$. Se $v_P(z) = m > 0$, P é um zero de z de ordem m; se $v_P(z) = m < 0$, P é um pólo de z de ordem $-m$.*

Agora nosso objetivo é saber se existem lugares de F/K e quando existem.

Teorema 1.1.16. *Seja F/K um corpo de funções e seja R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \subsetneq R$ é um ideal próprio de R. Então existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \vartheta_P$.*

Note que este teorema oferece condições para a existência do anel de valorização, dado que o lugar determina univocamente o anel de valorização.

Demonstração. Considere o conjunto

$$\mathcal{F} := \{\, S \mid S \text{ é um subanel de } F \text{ com } R \subseteq S \text{ e } IS \neq S \,\}$$

onde IS é por definição o conjunto de todas as somas finitas $\sum a_\nu s_\nu$ com $a_\nu \in I$ e $s_\nu \in S$. É fácil ver que IS é um ideal de S. Como $R \in \mathcal{F}$ (pois I é um subanel próprio de R) segue que $\mathcal{F}$ é não vazio e além disso $\mathcal{F}$ é indutivamente ordenado por inclusão. De fato, se $\mathcal{H} \subseteq \mathcal{F}$ é um subconjunto totalmente ordenado de $\mathcal{F}$ então

$$T := \bigcup_{S \in \mathcal{H}}$$

é um subanel de F com $R \subseteq T$. Agora nos resta mostrar que $IT \neq T$. Suponha que é falso, então $1 = \sum_{\nu=1}^{n} a_\nu s_\nu$ com $a_\nu \in I, s_\nu \in T$. Como $\mathcal{H}$ é totalmente ordenado, existe um $S_0 \in \mathcal{H}$ tal que $s_1, \cdots, s_n \in S_0$ e assim $1 = \sum_{\nu=1}^{n} a_\nu s_\nu \in IS_0$, o que não ocorre pois $IS_0 \neq S_0$.

Assim, para cada subconjunto totalmente ordenado $\mathcal{H} \subseteq \mathcal{F}$ existe um elemento maximal T em $\mathcal{F}$. Nosso objetivo agora é mostrar que esse conjunto T é o anel de valorização.

Suponha que exista $z \in F$ tal que z e $z^{-1} \notin T$. Daí, como $T[z] \supsetneq T$ então $T[z] = IT[z]$, pois caso contrário, $T[z] \in \mathcal{F}$ e isso contradiria a maximalidade de T. Da mesma forma, $T[z^{-1}] = IT[z^{-1}]$. Assim, podemos encontrar $a_0, \cdots, a_n, b_0, \cdots, b_n \in IT$ com

$$\begin{aligned} 1 &= a_0 + a_1 z + \cdots + a_n z^n \text{ e} \\ 1 &= b_0 + b_1 z^{-1} + \cdots + b_m z^{-m} \end{aligned} \tag{1.6}$$

Claramente $n \geq 1$ e $m \geq 1$ (pois $IT \neq T$). Sem perda de generalidade, suponha $m \leq n$ e que m e n foram tomados de forma minimal em (1.6). Multiplicando a primeira linha de (1.6) por $1 - b_0$ e a segunda linha por $a_n z^n$ obtemos:

$$\begin{aligned} 1 - b_0 &= (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n \text{ e} \\ 0 &= (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}. \end{aligned}$$

Somando as duas equações obtemos $1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}$, com os coeficientes $c_i \in IT$. Mas isso é uma contradição com a minimalidade de n em (1.6). Com isso mostramos que ou z ou $z^{-1} \in T$, para todo $z \in F$ e assim T é um anel de valorização de F/K.

□

Corolário 1.1.17. *Seja F/K um corpo de funções, $z \in F$ transcendente sobre K. Então z tem pelo menos um zero e um pólo. Em particular, $\mathbb{P}_F \neq \emptyset$.*

Demonstração. Considere o anel $R = K[z]$ e o ideal $I = zK[z]$. O teorema (1.1.16) garante que existe um lugar $P \in \mathbb{P}_F$ com $I \subseteq P$, logo $z \in P$ daí P é um zero de z. O mesmo argumento prova que existe um lugar Q tal que Q é um zero de z^{-1} e portanto um pólo de z. □

Para leitores pouco familiarizados com corpos de funções, segue no apêndice um exemplo do corpo de funções mais simples: o corpo de funções racionais.

1.2 Independência das valorizações

O principal resultado desta seção é o Teorema da Aproximação Fraca. Um resultado mais forte será visto adiante.

Essencialmente, o teorema a seguir nos diz que o fato de sabermos a valorização de $z \in F$ para lugares $P_1, \cdots, P_{n-1} \in \mathbb{P}_F$ não nos diz nada a respeito da valoração de z em P_n. Por isso este teorema também é conhecido por Teorema de Independência.

Teorema 1.2.1 (Teorema da Aproximação Fraca)**.** *Seja F/K um corpo de funções, $P_1, ..., P_n \in \mathbb{P}_F$ lugares de F/K dois-a-dois distintos, $x_1, ..., x_n \in F$ e $r_1, ..., r_n \in \mathbb{Z}$. Então existe um $x \in F$ tal que*

$$v_{P_i}(x - x_i) = r_i \quad \textit{para } i = 1, ..., n.$$

Demonstração. A demonstração será feita em vários passos, com o objetivo de construirmos o elemento $x \in F$ que satisfaz a tese do teorema.

Denote v_{P_i} por v_i.

Passo 1: Existe algum $u \in F$ com $v_1(u) > 0$ e $v_i(u) < 0$ para $i = 2, \cdots, n$.

Dem. do passo 1: Vamos mostrar por indução. Para $n = 2$ note que $\vartheta_{P_1} \subsetneq \vartheta_{P_2}$ e $\vartheta_{P_2} \subsetneq \vartheta_{P_1}$ pois anéis de valorização são subanéis maximais próprios de F, conforme (1.1.9). Assim,

existem $y_1 \in \vartheta_{P_1} \backslash \vartheta_{P_2}$ e $y_2 \in \vartheta_{P_2} \backslash \vartheta_{P_1}$ e logo $v_1(y_1) \geq 0, v_2(y_1) < 0, v_2(y_2) \geq 0$ e $v_1(y_2) < 0$. O elemento $u := y_1/y_2$ tem a propriedade $v_1(u) > 0$ e $v_2(u) > 0$ que queríamos.

Agora para $n > 2$ temos que, por hipótese de indução, existe $y \in F$ tal que $v_1(y) > 0$ e $v_i(y) < 0$ para $i = 2, \cdots, n-1$. Se $v_n(y) < 0$, então a demonstração acabou. Se $v_n(y) \geq 0$ então escolha um $z \in F$ tal que $v_1(z) > 0$ e $v_n(z) < 0$ (é fácil ver que tal z existe, basta proceder como no caso n=2) e faça $u := y + z^r$. Aqui, r é escolhido de forma que $r \cdot v_i(z) \neq v_i(y)$ para $i = 1, \cdots, n-1$. Assim, segue que $v_1(u) \geq \min\{v_1(y), r \cdot v_1(z)\} > 0$ e $v_i(u) = \min\{v_i(y), r \cdot v_i(z)\} > 0$ para $i = 2, \cdots, n$ (note que a igualdade vale pois $r \cdot v_i(z) \neq v_i(y)$).

Passo 2: Existe algum $\omega \in F$ tal que $v_1(\omega - 1) > r_1$ e $v_i(\omega) > r_i$ para $i = 2, \cdots, n$.

Dem. do passo 2: Seja u como no passo 1, isto é, $v_1(u) > 0$ e $v_i(u) < 0$ para $i = 2, \cdots, n$. Faça $\omega := (1+u^s)^{-1}$. Temos que $\omega - 1 = \dfrac{1}{1+u^s} - 1 = \dfrac{-u^s}{1+u^s}$. Daí, $v_1(\omega - 1) = v_1(-u^s) - v_1(1+u^s) = s \cdot v_1(u) - v_1(1+u^s)$. E como $v_1(u) > 0$, segue que, para s suficientemente grande, $1 + u^s \notin P_1$ logo $v_1(1+u^s) = 0$ e assim $v_1(\omega - 1) = s \cdot v_1(u) > r_1$ (basta tomar s suficientemente grande tal que $s > \dfrac{r_1}{v_1}$).

E também note que $v_i(\omega) = -v_i(1+u^s)$, e $v_i(1+u^s) = \min\{v_i(1), v_i(u) \cdot s\} = \{0, v_i(u) \cdot s < 0\} = v_i(u) \cdot s$. Logo $v_i(\omega) = -v_i(u) \cdot s$, e para s suficientemente grande, temos $v_i(\omega) > r_i$ (basta tomar $s > \dfrac{r_i}{v_i(u^{-1})}$).

Passo 3: Dados $y_1, \cdots, y_n \in F$, existe um elemento $z \in F$ com $v_i(z - y_i) > r_i$, para $i = 1, \cdots, n$.

Dem. do passo 3: Escolha $s \in \mathbb{Z}$ tal que $v_i(y_j) \geq s,\ i, j \in \{1, \cdots, n\}$. Note que podemos refazer o passo 2 apenas trocando o lugar ao qual queremos que u pertença, isto é, o índice i tal que $v_i(u) > 0$. Dessa forma, podemos refazer o passo 2 para todos os lugares e obtemos então uma generalização do passo 2: existem $\omega_1, \cdots, \omega_n$ tais que $v_i(\omega_i - 1) > r_i - s$ e $v_i(\omega_j) > r_i - s$ para $j \neq i$. Fazendo $z = \sum_{j=1}^{n} y_j \omega_j$ é fácil ver que z tem as propriedades desejadas.

Agora temos condições de finalizar a demonstração do teorema. Por hipótese temos $x_1, \cdots, x_n \in F$ e $r_1, \cdots, r_n \in \mathbb{Z}$. Pelo passo 3, existe $z \in F$ tal que $v_i(z - x_i) > r_i$ para $i = 1, \cdots, n$. Como a valorização é sobrejetiva, existem $z_i \in F$ tal que $v_i(z_i) = r_i, i = 1, \cdots, n$. Novamente, como $z_1, \cdots, z_n \in F$, existe $z' \in F$, pelo passo 3, tal que $v(z' - z_i) > r_i$. Daí segue que $v_i(z') = v_i((z' - z_i) + z_i) = \min\{v_i(z' - z_i) > r_i, v_i(z_i) = r_i\} = r_i$. Fazendo então $x = z' + z$ temos $v_i(x - x_i) = v_i(z' + z - x_i) = \min\{v_i(z') = r_i, v_i(z - x_i) > r_i\} = r_i$. Logo $x = z + z'$ satisfaz o teorema.

□

Corolário 1.2.2. *Todo corpo de funções tem uma quantidade infinita de lugares.*

(Dem. do corolário). Suponha que só exista uma quantidade finita de lugares, digamos $P_1, P_2, \cdots, P_n$. Faça $x_1 = x_2 = \cdots = x_n = 0 \in F$ e $r_1 = \cdots = r_n = 1$ no teorema (1.2.1). Daí segue desse teorema que existe $x \in F$ tal que $v_P(x) = 1 > 0$, para todo $P \in \mathbb{P}_F$; mas então x é transcendente e x só possui zeros. Absurdo pelo corolário (1.1.17).

□

Na próxima seção veremos que se um elemento x é transcendente sobre K então ele tem a mesma quantidade de zeros e pólos. O próximo teorema é um passo importante para mostrar esse resultado.

Teorema 1.2.3. *Seja F/Kum corpo de funções e sejam $P_1, \cdots, P_r$ zeros de um elemento $x \in F$. Então*

$$\sum_{i=1}^{r} v_{P_i}(x) \cdot \deg\, P_i \leq [F : K(x)]$$

Para a demonstração, usamos a seguinte notação: $v_i := v_{P_i}, f_i := \deg P_i, e_i := v_i(x)$ e t_i tal que $v_i(t_i) = 1$ e $v_k(t_i) = 0,\ k \neq i$. O objetivo da prova é mostrar que

$$t_i{}^a \cdot z_{ij} \quad 1 \leq i \leq r;\ 1 \leq j \leq f_i;\ \ 0 \leq a < e_i; z_{ij} \in F$$

são linearmente independentes sobre $K(x)$, pois assim teremos, pelo menos, uma quantidade $\sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i} \cdot \deg P_i$ de elementos linearmente independentes em $F/K(x)$, logo $\sum_{i=1}^{r} v_{P_i} \cdot \deg P_i \leq [F : K(x)]$.

Corolário 1.2.4. *Em um corpo de funções F/K todo elemento $0 \neq x \in F$ tem apenas uma quantidade finita de zeros e pólos.*

(Dem. do corolário). Suponha que x tenha infinitos zeros, $P_1, P_2, \cdots$. Daí tome $n > [F : K(x)]$. Pelo teorema (1.2.3) temos

$$\sum_{i=1}^{n} v_{P_i} \deg\, P_i \leq [F : K(x)]$$

Como P_i é zero de x, $v_{P_i}(x) \geq 1$ e deg $P_i \geq 1$, logo

$$[F : K(x)] \geq \sum_{i=1}^{n} v_{P_i} \deg\, P_i \geq \sum_{i=1}^{n} 1 \cdot 1 = n.$$

uma contradição com o fato de $n > [F : K(x)]$. Logo a quantidade de zeros é finita. O mesmo argumento mostra que a quantidade de zeros de x^{-1} é finita, e logo que a quantidade de pólos de x é finita.

□

1.3 Divisores

Sabemos, pelo corolário (1.1.13) que o corpo das contantes $\widetilde{K}$ de um corpo de funções algébricas F/K é uma extensão finita de K. Além disso, F pode ser visto como um corpo de funções sobre $\widetilde{K}$. Assim o que vamos assumir a partir de agora não acarreta prejuízos a teoria:

Daqui em diante, F/K denotará um corpo de funções algébricas de uma variável tal que K é o corpo de constantes de F/K.

Definição 1.3.1. *Um divisor de F/K é uma soma formal*

$$D = \sum_{P \in \mathbb{P}_F} n_P P$$

tal que o seu suporte, definido como

$$\textit{supp (D)} := \{P \in \mathbb{P}_F \,|\, n_P \neq 0\},$$

é sempre finito.

Seja $Div\, F$ o conjunto de todos os divisores de F. Em $Div\, F$ podemos definir a soma

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_p + n'_p)P$$

e o elemento zero como sendo o divisor tal que $n_p = 0$ para todo $P \in \mathbb{P}_F$. Dessa forma obtemos que $Div\, F$ é um grupo aditivo, chamado o grupo divisor de F/K.

Para cada $Q \in \mathbb{P}_F$ podemos definir uma valorização v_Q sobre $Div\, F$ definida por $v_Q(D) = n_Q$ e reescrever $D = \sum_{P \in \mathbb{P}_F} v_P(D)D$

Uma ordenação parcial em Div (F) é definida como

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \text{ para todo } P \in \mathbb{P}_F$$

Se $D_1 \leq D_2$ e $D_1 \neq D_2$ então dizemos que $D_1 < D_2$. Um divisor $D \geq 0$ é dito positivo (ou efetivo). Note que para um divisor ser não positivo (não efetivo) basta ter um lugar P tal que $v_P(D) < 0$.

O grau de um divisor é definido como

$$\textit{deg}\, D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \textit{deg}\, P,$$

e isso nos dá uma homomorfismo $\textit{deg} : \textit{Div}\,(F) \to \mathbb{Z}$.

Pelo corolário (1.2.4) um elemento não nulo de F tem apenas uma quantidade finita de zeros e pólos em $\mathbb{P}_F$. Sendo assim as definições abaixo fazem sentido:

Definição 1.3.2. *Seja* $0 \neq x \in F$ *e denote por* $\mathcal{Z}$ *(respectivamente* $\mathcal{N}$*) o conjunto dos zeros (resp. dos pólos) de* x *em* $\mathbb{P}_F$*. Então definimos*

$$\begin{aligned}
&(x)_0 := \textstyle\sum_{P \in \mathcal{Z}} v_P(x)P, \text{ o divisor de zeros de } x,\\
&(x)_\infty := \textstyle\sum_{P \in \mathcal{N}} -v_P(x)P, \text{ o divisor de pólos de } x,\\
&(x) := (x)_0 - (x)_\infty \text{ o divisor principal de } x
\end{aligned}$$

Claramente, $(x)_0 \geq 0, (x)_\infty \geq 0$, e

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P \tag{1.7}$$

Os elementos de $0 \neq x \in F$ que são constantes são caracterizados por

$$x \in K \Leftrightarrow (x) = 0$$

conforme o corolário (1.1.17), que nos diz que se x é transcendente então x tem pelo menos um zero e um pólo (lembre-se que estamos assumindo que $\widetilde{K} = K$).

Definição 1.3.3. *O conjunto formado pelos divisores principais*

$$\textit{Princ}\, F := \{(x) \,|\, 0 \neq x \in F\}$$

é chamado o grupo dos divisores principais de F/K*. Este é um subgrupo de Div(F) já que para* $x, y \in F, (xy) = (x) + (y)$ *por (1.7). E o grupo quociente*

$$Cl(F) := \textit{Div}\,(F)/\textit{Princ}\,(F)$$

é chamado o grupo das classes de divisores de F/K*. Para um divisor* $D \in \textit{Div}\,(F)$ *o correspondente elemento no grupo quociente Cl(F) é denotado por* $[D]$*, a classe divisora de* D*. Assim,* $D' \in [D]$ *se, e somente se, existe* $x \in F$ *tal que*
$D' = D + (x)$.

Nossa próxima definição tem um papel muito importante na teoria de corpos de funções algébricas.

Definição 1.3.4. *Para um divisor $A \in Div\,(F)$ definimos o espaço de Riemann-Roch associado à A por*

$$L(A) := \{x \in F \,|\, (x) + A \geq 0\} \cup \{0\}$$

Esta definição tem a seguinte interpretação: Sendo

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

com $n_i > 0, m_j > 0$ então $L(A)$ consiste dos elementos $x \in F$ tais que

- x tem zeros de ordem pelo menos m_j nos lugares Q_j, caso contrário a soma $(x) + A$ não daria ≥ 0.
- x só pode ter pólos nos lugares $P_1, \cdots, P_r$, com a ordem em P_i no máximo n_i, para $i = 1, \cdots, r$.

Lema 1.3.5. *Seja $A \in Div\,(F)$. Então*

(a) $x \in L(A)$ se, e somente se, $v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$.

(b) $L(A) \neq \{0\}$ se, e somente se, existe um divisor $A' \in [A]$ com $A' \geq 0$

Demonstração. (a) $x \in L(A) \Leftrightarrow (x) \geq -A \Leftrightarrow v_P(x) \geq -v_P(a)\ \ \forall P \in \mathbb{P}_F$.

(b) Se $L(A) \neq \{0\}$ então existe $x \in L(A)$ daí $(x) + A \geq 0$, nesse caso, faça $A' = A + (x)$. Agora, se existe $A' \in [A]$ com $A' \geq 0$ então $A' = A + (x) \geq 0$ para algum $x \in F$ e segue que $x \in L(A)$. □

Lema 1.3.6. *(a) L(A) é um espaço vetorial sobre K.*

(b) Se A' é um divisor equivalente a A então $L(A) \cong L(A')$.

Demonstração. (a) Sejam $x, y \in L(A)$ e $a \in K$. Note que $v_P(x+y) = \min\{v_P(x), v_P(y)\} \geq -v_P(A)\ \ \forall P \in \mathbb{P}_F$. Daí, pelo lema (1.3.5) segue que $x+y \in L(A)$. Além disso, $v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(A)$. Logo, $ax \in L(A)$. Assim, $L(A)$ subsepaço vetorial de K.

(b) Como $A \in [A']$ segue que existe $0 \neq z \in F$ tal que $A = A' + (z)$.

Considere a aplicação:

$$\phi : \begin{cases} L(A) & \to & F \\ x & \mapsto & xz \end{cases}$$

Note que ϕ é um homomorfismo sobre K e a imagem de ϕ é $L(A')$, pois $v_P(xz) = v_P(x) + v_P(z) \geq -v_P(A) + v_P(z) = -(v_P(A) - v_P(z))$ $\forall P \in \mathbb{P}_F$ logo $xz \in L(A')$.

Da mesma forma, definimos

$$\phi' : \begin{cases} L(A') & \to & F \\ x & \mapsto & xz^{-1} \end{cases}$$

Note que ϕ' também é homomorfismo sobre K e que a imagem de ϕ' é $L(A)$. Daí, como ϕ e ϕ' são inversas uma da outra então ϕ é um isomorfismo entre $L(A)$ e $L(A')$.

□

Lema 1.3.7. *(a)* $L(0) = K$

(b) Se $A < 0$ *então* $L(A) = \{0\}$.

Demonstração.

(a) Temos $L(0) = \{x \in F \backslash \{0\} \,|\, (x) \geq 0\}$. Mas se $(x) \geq 0$ então $v_P(x) \geq 0$ para todo $P \in \mathbb{P}_F$. Assim, x não pode ser transcendente, já que, nesse caso x teria pólos. Logo x é algébrico e como $\widetilde{K} = K$ segue que $L(0) = K$.

(b) Suponha que exista $x \in L(A), x \neq 0$. Como $A < 0$ segue que $(x) \geq -A > 0$. Assim $(x) > 0$, logo x é transcendente mas não têm pólos, um absurdo. □

Agora nosso próximo objetivo é mostrar que $L(A)$ é espaço de dimensão finita para cada $A \in$ Div (F).

Lema 1.3.8. *Sejam* A, B *divisores de* F/K *com* $A \leq B$. *Então temos* $L(A) \subseteq L(B)$ *e*

$$\textit{dim}\,(L(B)/L(A)) \leq \textit{deg}\, B - \textit{deg}\, A$$

Demonstração. Como $A \leq B$ segue direto que $L(A) \subseteq L(B)$. Para provar a outra afirmação usaremos indução sobre o grau de $B - A$ e para isso vamos assumir $B = A + P_0$ para algum $P_0 \in \mathbb{P}_F$ e mostrar que dim $(L(B)/L(A)) \leq$ deg P_0.

Tome $t \in F$ tal que $v_{P_0}(t) = v_{P_0}(B) = v_{P_0}(A) + 1$ (tal t existe pois v_P é sobrejetiva). Para $x \in L(B)$ nós temos $v_{P_0}(x) \geq -v_{P_0}(B) = -v_{P_0}(t)$. Então $xt \in \vartheta_{P_0}$. Então obtemos a aplicação K-linear

$$\phi : \begin{cases} L(B) & \to & F_{P_0} \\ x & \mapsto & (xt)(P_0) \end{cases}$$

Note que o núcleo de ϕ é $L(A)$. De fato, se $x \in L(A)$ então $v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$, em particular para $P = P_0$. Logo $L(A) \subseteq \ker(\phi)$. Agora se x é tal que $\phi(x) = 0$ então para $P \neq P_0$ temos:

$$v_P(x) \geq -v_P(B) = -v_P(A);$$

Para $P = P_0$, como x está no núcleo de ϕ: $v_{P_0}(xt) > 0$, logo
$v_{P_0}(x) > -v_{P_0}(t) = -v_{P_0}(A) - 1$ e segue que $v_{P_0}(x) \geq -v_{P_0}(A)$ e assim
$\ker(\phi) \subseteq L(A)$.

E portanto ϕ induz uma aplicação K-linear injetiva de $L(B)/L(A)$ em F_P. E dessa forma

$$\dim\left(L(B)/L(A)\right) \leq F_P = \deg P = \deg B - \deg A.$$

O caso geral segue por indução. □

Proposição 1.3.9. *Para cada divisor $A \in Div\,(F)$ o espaço $L(A)$ é um espaço vetorial sobre K de dimensão finita. Mais precisamente: se $A = A_+ - A_-$ com A_+, A_- divisores positivos então*

$$dim\, L(A) \leq deg\, A_+ + 1$$

Demonstração. Como $L(A) \subseteq L(A_+)$ então basta mostrar para $L(A_+)$. Como $0 \leq A_+$, pelo lema (1.3.8) temos $\dim\left(L(A_+)/L(0)\right) \leq \deg\left(A_+\right)$. Assim

$$\dim L(A) \leq \dim L(A_+) \leq \deg\left(A_+\right) + 1$$

□

Definição 1.3.10. *Para $A \in Div\,(F)$ o inteiro $\ell(A) := dim\, L(A)$ é chamado a dimensão do divisor A.*

Um dos problemas mais importantes na teoria de corpos de funções algébricas é determinar a dimensão de $\ell(A)$. Esse problema foi totalmente resolvido pelo Teorema de Riemann-Roch.

Nosso objetivo agora é mostrar que um elemento transcendente tem a mesma quantidade de zeros e pólos.

Teorema 1.3.11. *Todos os divisores principais tem grau zero. Mais precisamente: seja $x \in F\backslash K$ e $(x)_0$ e $(x)_\infty$ o divisor zero e o divisor pólo de x, respectivamente. Então*

$$\textit{deg}\,(x)_0 = \textit{deg}\,(x)_\infty = [F : K(x)].$$

Demonstração. Façamos $n := [F : K(x)]$ e

$$B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i$$

onde $P_1, \cdots, P_r$ são pólos de x. Então, pelo teorema (1.2.3)

$$\deg B = \sum_{i=1}^{r} v_{P_i}(x^{-1}) \cdot \deg P_i \leq [F : K(x)] = n$$

Assim nos resta mostrar que $n \leq \deg B$. Escolha uma base $u_1, \cdots, u_n$ de $F/K(x)$ e um divisor $C \geq 0$ tal que $(u_i) \geq -C$ para $i = 1, \cdots, n$ (é possível escolher tal C pois é uma quantidade finita de u_i's). Agora temos

$$\ell(IB + C) \geq n(I + 1), \text{ para todo } I \geq 0. \tag{1.8}$$

Isso segue do fato que $(x^i u_j) = i(x) + (u_j) \geq -i(x)_\infty - C = (iB + C)$ logo $x^i u_j \in L(IB + C)$ para $0 \leq i \leq I,\ 1 \leq j \leq n$. E note que esses elementos são linearmente independentes sobre K, dado que $u_1, \cdots, u_n$ são linearmente independentes sobre $K(x)$. Fazendo $c := \deg C$ e usando que $IB + C \geq 0$ segue da proposição (1.3.9) que $n(I + 1) \leq \ell(IB + C) \leq \deg(IB + C) + 1 = I\deg B + c + 1$. Então

$$I(\deg B - n) \geq n - c - 1 \tag{1.9}$$

para todo $I \in \mathbb{N}$. Como o lado direito da equação (1.9) independe de I podemos determinar que (1.9) só é possível se $\deg B \leq n$. De fato, se $\deg B - n < 0$ então $n - c - 1 \leq 0$. Mas como a equação (1.9) vale para todo $I \in \mathbb{N}$ então existe I suficientemente grande tal que $I(\deg B - n) < n - c - 1$, uma contradição. Logo $\deg B \leq n$, como queríamos.

Então provamos que deg $(x)_\infty = [F : K(x)]$. Mas como $(x)_0 = (x^{-1})_\infty$, podemos concluir que deg $(x)_0 =$ deg $(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$ □

Corolário 1.3.12. *(a) Sejam A, A' divisores com $A \in [A']$. Então nós temos $\ell(A) = \ell(A')$ e deg $A =$ deg A'.*

(b) Se deg $A < 0$ então $\ell(A) = 0$.

(c) Para um divisor A de grau 0 as seguintes afirmações são equivalentes:

1) A é principal.

2) $\ell(A) \geq 1$.

3) $\ell(A) = 1$.

Demonstração. (a) Como $L(A) \cong L(A')$ segue que $\ell(A) = \ell(A')$. E como $A \sim A'$ segue que existe $0 \neq x \in F$ tal que $A = A' + (x)$. Como deg $(x) = 0$ pelo teorema (1.3.11), segue que deg $A =$ deg A'.

(b) Se $\ell(A) > 0$ então existe $x \in L(A)$, logo $L(A) \neq \{0\}$. Daí existe $A' \geq 0$ tal que $A' \sim A$. Logo $0 \leq$ deg $A' =$ deg A.

(c) Seja $A \in$ Div (F) com deg $A = 0$.

$1) \Rightarrow 2)$ Se A é principal então existe $x \in F \backslash \{0\}$ tal que $A = (x)$. Daí note que $x^{-1} \in L(A)$. Logo $\ell(A) \geq 1$.

$2) \Rightarrow 3)$ Como $\ell(A) \geq 1$ então $L(A) \neq \{0\}$ e daí existe $A' \sim A$ com $0 \leq A'$. Juntando isso com o fato de que deg $A' =$ deg $A = 0$ segue que $A' = 0$. E ao mesmo tempo, $\ell(A) = \ell(A') = \ell(0) = 1$.

$3) \Rightarrow 1)$ Sendo $\ell(A) = 1$, podemos tomar $0 \neq z \in L(A)$. Daí $(z) + A \geq 0$. E como, pelo teorema (1.3.11), deg $((z) + A) = 0$, segue que $(z) + A = 0$. Logo $A = (z^{-1})$ é principal.

□

No exemplo a seguir vamos mostrar como obter um divisor principal usando o corpo de funções mais simples, $F = K(x)$ (ver apêndice).

Exemplo 1.3.13. *Mais uma vez consideraremos o corpo de funções racionais $F = K(x)$, como fizemos na seção 1.2. Seja $0 \neq z \in K(x)$. Temos $z = a \cdot f(x)/g(x)$ com $0 \neq a \in K$ e $f(x), g(x) \in K[x]$ mônicos e relativamente primos. Sejam*

$$f(x) = \prod_{i=1}^{r} p_i(x)^{n_i},\ g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$$

com $p_i(x)$ e $q_j(x) \in K[x]$ irredutíveis, mônicos, 2 a 2 distintos. Daí, como da proposição (A.1.1) sabemos que cada polinômio mônico irredutível é elemento primo de algum lugar de $\mathbb{P}_F$ e pelo teorema (A.1.2) os únicos lugares de $K(x)/K$ são $P_{p(x)}$ e P_∞, segue que

$$(z) = \sum_{i=1}^{r} n_i P_{p_i(x)} - \sum_{j=1}^{s} m_j Q_{q_j(x)} - (\textit{deg}\, g(x) - \textit{deg}\, f(x))P_\infty \tag{1.10}$$

(Basta ver o teorema (A.1.1) itens a) e b)).

Assim, em corpos de funções arbitrários, divisores principais podem ser considerados substitutos para decomposição em polinômios irredutíveis que acontece no caso do corpo de funções racionais.

Vamos fazer uma observação que melhora um pouco a proposição (1.3.9). Nesta proposição vimos que vale

$$\ell(A) \leq 1 + \deg A \tag{1.11}$$

sempre que $A \geq 0$. De fato, essa desigualdade é válida para todo divisor cujo grau é maior ou igual a zero. De fato, suponha $\deg A \geq 0$. Podemos supor $\ell(A) > 0$ já que para $\ell(A) = 0$, (1.11) segue direto de $\deg A \geq 0$. Daí existe $A \sim A'$ para algum divisor $A' \geq 0$ pela observação (1.3.5), e então $\ell(A) = \ell(A') \leq 1 + \deg A' = 1 + \deg A$, pelo corolário (1.3.12).

Agora nosso objetivo é provar a existência de uma cota inferior para $\ell(A)$ da mesma forma que fizemos em (1.11).

Proposição 1.3.14. *Existe uma constante $\gamma \in \mathbb{Z}$ tal que para todos os divisores $A \in Div\,(F)$ vale:*

$$\textit{deg}\, A - \ell(A) \leq \gamma$$

Note que o fato central dessa proposição é que γ independe do divisor A. Ele depende só de F/K.

Demonstração. Inicialmente note que, do lema (1.3.8)

$$A_1 \leq A_2 \Rightarrow l\left(\frac{L(A_2)}{L(A_1)}\right) \leq \text{deg}\, A_2 - \text{deg}\, A_1$$

logo

$$A_1 \leq A_2 \Rightarrow \text{deg}\, A_1 - \ell(A_1) \leq \text{deg}\, A_2 - \ell(A_2) \tag{1.12}$$

Agora fixamos um $x \in F\backslash K$ e consideramos o divisor $B := (x)_\infty$. Como na demonstração de (1.3.11), existe $C \geq 0$ tal que $(u_i) \geq -C$ onde $(u_i)_{i=1}^n$ é uma base para F em $K(x)$ (note que C só depende de x) tal que $\ell(BC + I) \geq (I + 1) \cdot \text{deg}\, B$ para todo $I \geq 0$ (basta ver (1.8)).

Por outro lado, note que, pelo lema (1.3.8) $IB + C \geq IB$ logo $L(IB) \subseteq L(IB + C)$ e assim

$$\dim\left(\frac{L(IB+C}{L(IB)}\right) \leq \text{deg}\,(IB + C) - \text{deg}\,(IB) = \text{deg}\, C$$

portanto $\ell(IB + C) \leq \ell(IB) + \text{deg}\, C$. E assim, juntando as duas desigualdades temos

$$\ell(IB) \geq (I + 1)\text{deg}\, B - \text{deg}\, C = \text{deg}\,(IB) + ([F : K(x)] - \text{deg}\, C).$$

Assim, fazendo $\gamma = (\text{deg}\, C - [F : K(x)])$ a proposição vale para $A = IB$.

Agora vamos mostrar que a proposição vale para todo $A \in \text{Div}\,(F)$ e com o mesmo γ.

Afirmação: Dado um divisor A existem divisores A_1, D e um inteiro $I \geq 0$ tal que $A \leq A_1, A_1 \sim D$ e $D \leq IB$.

Usando essa afirmação a demonstração é imediata pois

$$\begin{aligned}
\text{deg}\, A - \ell(A) &\leq \text{deg}\, A_1 - \ell(A_1) && \text{(por (1.12))} \\
&= \text{deg}\, D - \ell(D) && \text{(pelo corolário (1.3.12))} \\
&= \text{deg}\,(IB) - \ell(IB) && \text{(por (1.12))} \\
&\leq \gamma
\end{aligned}$$

A prova dessa afirmação é relativamente simples:

Escolha $A_1 \geq A$ tal que $A_1 \geq 0$. Então

$$\begin{aligned}
\ell(IB - A_1) &\geq \ell(IB) - \text{deg}\, A_1 && \text{(pelo lema (1.3.8))} \\
&\geq \text{deg}\,\ell(IB) - \gamma - \text{deg}\, A_1 \\
&> 0
\end{aligned}$$

para I suficientemente grande. Então existe um elemento $z \in L(IB - A_1)$. Fazendo $D := A_1 - (z)$, obtemos $A_1 \sim D$ e $D \leq A_1 - (A_1 - IB) = IB$. □

A partir dessa proposição faz sentido falarmos da definição a seguir.

Definição 1.3.15. *O gênero de F/K é definido como*

$$g := \max\{\deg A - \ell(A) + 1 \mid A \in \mathit{Div}\,(F)\}$$

Note que $g \leq \gamma + 1$ pela proposição (1.3.14).

O gênero é um dos invariantes mais importantes de um corpo de funções.

Corolário 1.3.16. *O gênero de F/K é um inteiro não negativo.*

Demonstração. Na definição de gênero, faça $A = 0$. Assim, $g = \deg 0 - \ell(0) + 1 = 0$. Daí $g \geq 0$. □

O próximo teorema é uma versão preliminar do teorema de Riemann-Roch e é um resultado muito útil para os próximos capítulos.

Teorema 1.3.17 (Teorema de Riemann)**.** *Seja F/K um corpo de funções de gênero g. Então temos:*

(a) Para todos os divisores $A \in \mathit{Div}\,(F)$,

$$\ell(A) \geq \deg A + 1 - g$$

(b) Existe um inteiro c, dependendo só do corpo de funções F/K, tal que

$$\ell(A) = \deg A + 1 - g$$

sempre que $\deg A \geq c$.

Demonstração. (a) Segue diretamente da definição de gênero.

(b) Escolha um divisor A_0 tal que $g = \deg A_0 - \ell(A_0) + 1$ e denote por $c := \deg(A_0) + g$.

Por hipótese, $\deg(A) \geq c$. Daí,

$$\begin{aligned} \ell(A - A_0) &\geq \deg(A - A_0) + 1 - g \\ &= \deg(A) - \deg(A_0) + 1 - g \\ &\geq c - \deg(A_0) + 1 - g \\ &= 1 \end{aligned}$$

Logo $L(A - A_0) \neq \{0\}$. Assim, tome $0 \neq z \in L(A - A_0)$. Faça $A' = A + (z)$ e note que $A' \geq A_0$. Assim

$$\begin{aligned}\deg(A) - \ell(A) &= \deg(A') - \ell(A'), \text{ (pelo corolário (1.3.12))} \\ &\geq \deg(A_0) - \ell(A_0) \text{ (pelo lema (1.3.8))} \\ &= g - 1\end{aligned}$$

Daí $\ell(A) \leq \deg(A) + 1 - g$, e a igualdade segue do item (a).

□

No exemplo a seguir vamos, mais uma vez, voltar ao corpo de funções racionais $F = K(x)$ para mostrar que nesse corpo de funções o gênero é nulo.

Exemplo 1.3.18. *Seja P_∞ o pólo divisor de x (conforme vimos em (A.5)). Considere para $r \geq 0$ o espaço vetorial $L(rP_\infty)$. Como o elemento gerador de P_∞) é $1/x$ então $v_\infty(x) = -1, v_\infty(x^2) = -2, \cdots, v_\infty(x^r) = -r$ e para $P \neq P_\infty$, $v_P(x^i) \geq 0$ para todo $i = 1, \cdots, r$. Daí $1, x, x^2, \cdots, x^r \in L(rP_\infty)$. Logo $\ell(rP_\infty) \geq r + 1$.*

Ao mesmo tempo, pelo teorema de Riemann, $\ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$. Daí

$$r + 1 \leq \ell(rP_\infty) \leq r + 1 - g \text{ logo } g \leq 0$$

E como g é sempre não negativo, segue que $g = 0$.

Definição 1.3.19. *Para $A \in Div\,(F)$ o inteiro*

$$i(A) := \ell(A) - \deg(A) + g - 1$$

é chamado índice de especialidade de A.

O teorema de Riemann (1.3.17) afirma que $i(A)$ é um inteiro não negativo e que $i(A) = 0$ para $\deg(A)$ suficientemente grande.

Note que o teorema de Riemann nos diz que $L(A_+) > \deg(A) + g - 1$. O Teorema de Riemann-Roch nos fornece a igualdade para essa inequação.

2

Teorema de Riemann-Roch e aplicações

2.1 Teorema de Riemann-Roch

Neste capítulo F/K denota um corpo de funções de gênero g.

Definição 2.1.1. *Um adele de F/Ké um aplicação*

$$\alpha : \begin{cases} \mathbb{P}_F & \to & F \\ P & \mapsto & \alpha_P \end{cases}$$

tal que $\alpha_P \in \vartheta_P$ para quase todo $P \in \mathbb{P}_F$. Um adele pode ser visto como um elemento do produto direto $\prod_{P\in\mathbb{P}_F} F$, assim, podemos denotar o adele como $\alpha = (\alpha_P)_{P\in\mathbb{P}_F}$, ou ainda $\alpha = (\alpha_P)$. O conjunto

$$\mathcal{A}_F := \{\alpha \,|\, \alpha \text{ é um adele de } F/K\}$$

é chamado o espaço dos adeles de F/K. Podemos ver esse espaço como um subespaço vetorial sobre K da maneira usual (soma e multiplicação por K coordenada a coordenada)

Observe que, dado um $x \in F$, este somente possui um número finito de pólos, portanto $\alpha = (x)_{P\in\mathbb{P}_F}$ também é um adele, chamado de adele principal. Isso nos dá uma imersão $F \hookrightarrow \mathcal{A}_F$. As valorações v_P podem ser naturalmente extendidas até $\mathcal{A}_F$ pela seguine definição: $v_P(\alpha) = v_P(\alpha_P)$, onde α_P é a componente P do adele α. Por definição temos que $v_P(\alpha) \geq 0$ para quase todo $P \in \mathbb{P}_F$.

Definição 2.1.2. *Para $A \in Div\,(F)$ definimos*

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \,|\, v_P(\alpha) \geq -v_P(A) \text{ para todo } P \in \mathbb{P}_F\}.$$

Note que $\mathcal{A}_F(A)$ é um subespaço vetorial de $\mathcal{A}_F$ sobre K.

O lema a seguir é uma importante ferramenta para as próximas seções.

Lema 2.1.3. *Sejam $A_1, A_2 \in Div(F)$ e $A_1 \leq A_2$. Então $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ e*

$$\dim\left(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)\right) = \deg A_2 - \deg A_1 \tag{2.1}$$

Demonstração. Primeiramente, que $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ segue diretamente da definição de $\mathcal{A}_F(A)$. Agora, para a segunda parte, vamos usar indução sobre o grau de $\deg(A_2 - A_1)$. Vamos supor então que $A_2 - A_1 = P'$ com $P' \in \mathbb{P}_F$ e vamos mostrar que $\dim\left(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)\right) = \deg P'$.

Seja t um elemento primo de P' e seja $F_{P'}$ o seu corpo residual. Denote por $e := v_{P'}(A_2)$ e considere a aplicação K-linear

$$\phi : \begin{cases} \mathcal{A}_F(A_2) & \to & \mathbf{F}_{P'} \\ \alpha & \mapsto & t^e \alpha_{P'} + P' \end{cases}$$

Note que o núcleo de ϕ é dado por $\alpha \in \mathcal{A}_F(A_2)$ tais que $v_{p'}(t^e \alpha_{P'}) > 0$, isto é, $v_{p'}(\alpha_{P'}) > -v_{p'}(A_2)$. E como $A_2 = A_1 - P'$ segue que os elementos do núcleo são da forma $v_{p'}(\alpha_{P'}) \geq -v_{p'}(A_1)$. Assim, segue diretamente que $\ker(\phi) = \mathcal{A}_F(A_1)$.

E, além disso, ϕ é sobrejetiva, pois dado $x(P') \in F_{P'}$ existe o adele α da forma $\alpha_{P'} = xt^{-e}$ e $\alpha_P = 0$ para $P \neq P'$, com $\phi(\alpha) = x(P')$.

Dessa forma, podemos usar o teorema do isomorfismo e assim $\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \cong F_P$. □

O teorema a seguir é a essência do teorema de Riemann-Roch e daí sua extrema importância neste estudo.

Teorema 2.1.4. *Para todo divisor A, o índice de especialidade $i(A)$ é*

$$i(A) = \dim\left(\mathcal{A}_F/(\mathcal{A}_F(A) + F)\right)$$

Para demonstrar esse resultado usaremos, além do lema (2.1.3), os seguintes lemas, cujas demonstrações serão omitidas por serem muito técnicas, mas podem ser encontradas em [6].

Lema 2.1.5. *Sejam A_1 e $A_2 \in$ Div (F) e $A_1 \leq A_2$. Então:*

$$\dim(\mathcal{A}_F(A_2)+F)/\dim(\mathcal{A}_F(A_1)+F) = (\deg(A_2)-\ell(A_2))-(\deg(A_1)-\ell(A_1)).$$

Lema 2.1.6. *Se B é um divisor com $\ell(B) = \deg(B)+1-g$, então*

$$\mathcal{A}_F = \mathcal{A}_F(B)+F$$

Dem. do teorema. Considere um divisor arbitrário A. Pelo teorema de Riemann (1.3.17)(b) existe um divisor $A_1 \geq A$ tal que $\ell(A_1) = \deg(A_1)+1-g$. Pelo lema (2.1.6), $\mathcal{A}_F = \mathcal{A}_F(A_1)+F$, e olhando agora para o lema (2.1.5), obtemos

$$\begin{aligned}\dim(\mathcal{A}_F/\mathcal{A}_F(A)+F) &= \dim(\mathcal{A}_F(A_1)+F)/(\mathcal{A}_F(A)+F)\\ &= (\deg(A_1)-\ell(A_1))-(\deg(A)-\ell(A))\\ &= (g-1)+\ell(A)-\deg(A) = i(A)\end{aligned}$$

□

Corolário 2.1.7. $g = dim\,(\mathcal{A}_F/(\mathcal{A}_F(0)+F))$

Demonstração. $i(0) = \ell(0)-\deg(0)+g-1 = 1-0+g-1 = g.$ □

Vamos agora definir os diferenciais de Weil, que vão nos dar uma outra interpretação do índice de especialidade e cujos componentes serão vitais para a construção dos Códigos de Goppa.

Definição 2.1.8. *Um diferencial de Weil de F/K é um funcional K-linear $\omega : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(A)+F$ para algum divisor $A \in$ Div (F). Denotamos por*

$$\Omega_F := \{\omega \,|\, \omega \text{ é um diferencial de Weil de } F/K\}$$

o módulo dos diferenciais de Weil de F/K. Para $A \in$ Div (F) temos

$$\Omega_F(A) := \{\omega \in \Omega_F \,|\, \omega \text{ se anula em } \mathcal{A}_F(A)+F\}$$

Veja que podemos ver Ω_F como um espaço vetorial sobre K da maneira usual (de fato, se ω_1 se anula em $\mathcal{A}_F(A_1)+F$ e ω_2 se anula em $\mathcal{A}_F(A_2)+F$, então $\omega_1+\omega_2$ se anula em $\mathcal{A}_F(A_3)$ para todo divisor A_3 com $A_3 \leq A_2$ e $a\omega_1$ se anula em $\mathcal{A}_F(A_1)+F$ para $a \in K$). E note que $\Omega_F(A)$ é um subespaço vetorial de Ω_F sobre K.

Lema 2.1.9. *Para $A \in$ Div (F) temos $\dim \Omega_F(A) = i(A)$.*

Demonstração. Como $\Omega_F(A)$ é formado pelos funcionais lineares que se anulam em $\mathcal{A}_F(A)+F$, o teorema do homomorfismo induz um isomorfismo natural entre $\Omega_F(A)$ e $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$. E como vimos no teorema (2.1.4) que $\dim \mathcal{A}_F/(\mathcal{A}_F(A)+F) = i(A)$, segue que $\dim \Omega_F(A) = i(A)$. □

Uma consequência simples do lema (2.1.9) é que $\Omega_F \neq 0$. De fato, basta tomar $A \in$ Div (F) tal que $\deg(A) \leq -2$. Daí

$$\dim \Omega_F(A) = i(A) = \ell(A) - \deg(A) + g - 1 \geq 1$$

e assim $\Omega_F(A) \neq 0$.

Definição 2.1.10. *Para $x \in F$ e $\omega \in \Omega_F$ definimos $x\omega : \mathcal{A}_F \to K$ da seguinte forma:*

$$(x\omega)(\alpha) := \omega(x\alpha).$$

Note que $(x\omega)$ é um diferencial de Weil. De fato, se ω se anula em $\mathcal{A}_F(A) + F$ então $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$. Além disso, esta definição, apresenta uma multiplicação de elementos de Ω_F por elementos de F. Isso nos permite ver Ω_F como um espaço vetorial sobre F e não mais só sobre K.

Proposição 2.1.11. *Ω_F é um espaço vetorial de dimensão 1 sobre F.*

Demonstração. Escolha $0 \neq \omega_1 \in \Omega_F$ (existe tal ω_1 pois já sabemos que $\Omega_F \neq 0$). Nosso objetivo é mostrar que para cada $\omega_2 \in \Omega_F$ existe algum $z \in F$ com $\omega_2 = z\omega_1$. Podemos assumir que $\omega_2 \neq 0$.

Tome $A_1, A_2 \in$ Div (F) tais que $\omega_1 \in \Omega_F(A_1)$ e $\omega_2 \in \Omega_F(A_2)$ (existem pois todo $\omega \in \Omega_F$ se anula em $\mathcal{A}_F(D)$ para algum divisor D). Para um divisor B (que será especificado depois), considere a aplicação K-linear

$$\varphi_i : \begin{cases} L(A_i + B) & \to & \Omega_F(-B) \\ x & \mapsto & x\omega_i \end{cases} \qquad (i = 1, 2)$$

Note que φ_i é injetiva.

Agora nossa demonstração segue da seguinte afirmação:

Afirmação. Seja B um divisor cujo grau seja suficientemente grande tal que $\ell(A_j + B) = \deg(A_j+B)+1-g$ para $i = 1, 2$ (a escolha do B é possível pelo teorema de Riemann (1.3.17)), então

$$\varphi_1(L(A_1 + B)) \cap \varphi_2(L(A_2 + B)) \neq \{0\}$$

Pois, sendo válida a afirmação, podemos escolher $x_1 \in L(A_1 + B)$ e $x_2 \in L(A_2 + B)$ de forma que $x_1\omega_1 = x_2\omega_2 \neq 0$. Assim, $\omega_2 = (x_1 x_2^{-1})\omega_1$, como queríamos.

A idéia central para provar a afirmação é usar o resultado de álgebra linear que diz que:
Se C_1, C_2 são subespaços vetoriais de um espaço vetorial de dimensão finita V então $\dim C_1 \cap C_2 \geq \dim C_1 + \dim C_2 - \dim V$.
Fazendo $C_j = \varphi_j(L(A_j + B)) \subseteq \Omega_F(-B)$ e usando que $\ell(A_j + B) = \deg(A_j + B) + 1 - g$, obtemos $\dim C_1 + \dim C_2 - \dim \Omega_F(-B) > 0$, o que prova afirmação.

□

Agora queremos associar a cada diferencial de Weil $\omega \neq 0$ um divisor. Com esse fim, defina, para cada $\omega \in \Omega_F, \omega \neq 0$,

$$M(\omega) := \{A \in \text{Div}\,(F) \,|\, \omega \text{ se anula em } \mathcal{A}_F(A) + F\}. \tag{2.2}$$

Lema 2.1.12. *Seja $0 \neq \omega \in \Omega_F$. Então existe um divisor unicamente determinado $W \in M(\omega)$ tal que $A \leq W$ para todo $A \in M(\omega)$.*

Demonstração. Pelo teorema de Riemann (1.3.17) existe uma constante c que depende só de F/K tal que se $\deg(A) \geq c$ então $i(A) = 0$, $A \in \text{Div}\,(F)$. Mas como pelo teorema (2.1.4) $i(A) = \dim(\mathcal{A}_F/\mathcal{A}_F(A) + F)$ então $\deg(A) < c$ para todo $A \in M(\omega)$. Isso porque, se $\dim(\mathcal{A}_F/\mathcal{A}_F(A) + F) = 0$ então $\mathcal{A}_F = \mathcal{A}_F(A) + F$ e ω se anularia em todo $\mathcal{A}_F$, logo $\omega = 0$. Assim, $M(\omega)$ possui um elemento de grau máximo, digamos W.

Agora suponha que W não satisfaz $A \leq W$, para todo $A \in M(\omega)$. Então existe $A_0 \in M(\omega)$ tal que $A_0 \not\leq W$, isto é, existe pelo menos um $Q \in \mathbb{P}_F$ tal que $v_Q(A_0) > v_Q(W)$.

Nosso objetivo será então, para concluir a prova, mostrar que $W + Q \in M(\omega)$, pois isso contrariará a maximalidade do grau de W.

Nesse intuito, considere um adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W+Q)$. Podemos escrever $\alpha = \alpha' + \alpha''$, com

$$\alpha'_P := \begin{cases} \alpha_P & \text{para } P \neq Q \\ 0 & \text{para } P = Q \end{cases} \quad , \quad \alpha''_P := \begin{cases} 0 & \text{para } P \neq Q \\ \alpha_Q & \text{para } P = Q \end{cases}$$

Então é fácil verificar que $\alpha' \in \mathcal{A}_F(W)$ e $\alpha'' \in \mathcal{A}_F(A_0)$ e logo $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$ pois $W, A_0 \in M(\omega)$. Assim, ω se anula em $\mathcal{A}_F(W + Q) + F$ e portanto $W + Q \in M(\omega)$, como queríamos.

Agora vamos mostrar a unicidade. Sejam $W, W' \in M(\omega)$ tal que $A \leq W$ e $A \leq W'$ $\forall A \in M(\omega)$. Mas então $W \leq W'$ e $W' \leq W$, logo $W = W'$. □

A partir do lema (2.1.12) podemos fazer a seguinte definição:

Definição 2.1.13. *(a) O divisor (ω) de um diferencial de Weil é o divisor unicamente determinado (conforme visto no lema (2.1.12)) tal que*

1) ω se anula em $\mathcal{A}_F((\omega)+F)$ e

2) se ω se anula em $\mathcal{A}_F(A)+F$ então $A \leq (\omega)$;

(b) Para $0 \neq \omega \in \Omega_F$ e $P \in \mathbb{P}_F$ definimos $v_P(\omega) := v_P((\omega))$;

*(c) Um lugar P é dito ser um zero (resp. um pólo) de ω se $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$). O diferencial de Weil é dito regular em P se $v_P(\omega) \geq 0$ e é dito **regular** se é **regular** para todo $P \in \mathbb{P}_F$;*

(d) Um divisor W é dito ser divisor canônico de F/K se $W = (\omega)$ para algum $\omega \in \Omega_F$.

Observação 2.1.14. *Segue da definição acima que*

$$\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \text{ ou } (\omega) \geq A\}$$
e
$$\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ é regular } \}$$

E pelo lema (2.1.9) e pela definição (1.3.19) segue que

$$\dim \Omega_F(0) = i(0) = g$$

Proposição 2.1.15. *(a) Para $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$ temos $(x\omega) = (x) + (\omega)$.*

(b) Quaisquer dois divisores canônicos são equivalentes.

Demonstração. (a) Sabemos que, se ω se anula em $\mathcal{A}_F(A) + F$ então $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$. Consequentemente,

$$(x) + (\omega) \leq (x\omega)$$

pois, por definição, ω se anula em $\mathcal{A}_F((\omega))+F$, logo $x\omega$ se anula em $\mathcal{A}_F((\omega)+(x))+F$ e assim $(x)+(\omega) \in M((x\omega))$. E como, por definição $(x\omega)$ é maior ou igual a todo elemento de $M(x\omega)$ segue que $(x) + (\omega) \leq (x\omega)$.

Da mesma forma,

$$(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega), \quad \text{logo} \quad (x\omega) \leq (\omega) + (x)$$

Daí,

$$(x) + (\omega) \leq (x\omega) \leq (\omega) + (x), \quad \text{logo} \quad (x\omega) = (x) + (\omega).$$

(b) Seja $W_1 = (\omega_1)$ e $W_2 = \omega_2$. Queremos mostrar que existe x tal que $(\omega_1) + (x) = (\omega_2)$. Como $\omega_1, \omega_2 \in \Omega_F \backslash \{0\}$, segue da proposição (2.1.11) que existe $x \in F$ tal que $\omega_2 = x\omega_1$. Assim, $(\omega_2) = (x\omega_1) = (x) + (\omega_1)$, como queríamos.

□

Note que a nomenclatura "canônico" no item (d) da definição (2.1.13) faz referência ao que foi mostrado na proposição (2.1.15). Isto porque, ao obtermos um representante da classe dos divisores dos diferenciais de Weil, obtemos todos, já que são todos equivalentes. Essa classe formada pelos divisores canônicos é chamada de *classe canônica*.

O teorema a seguir basicamente conclui a prova do teorema de Riemann-Roch, pois pelo teorema de Riemann (1.3.17) vimos que $\ell(A) \geq \deg(A) - g + 1$. O que esse teorema nos diz é exatamente o que falta para obtermos a igualdade, isto é que $\ell(A) - \deg(A) + g - 1 = \ell(W - A)$.

Teorema 2.1.16 (Teorema da dualidade)**.** *Seja A um divisor arbitrário e $W = (\omega)$ um divisor canônico de F/K. Então a aplicação*

$$\mu : \begin{cases} L(W - A) & \to & \Omega_F(A) \\ x & \mapsto & x\omega \end{cases}$$

é um isomorfismo entre K espaços vetoriais. Em particular,

$$i(A) = \ell(W - A).$$

Demonstração. Para $x \in L(W - A)$ temos

$$(x\omega) = (x) + (\omega) \geq -(W - A) + (\omega) = -(W - A) + W = A$$

Daí $(x\omega) \geq A$ e pela observação (2.1.14), $x\omega \in \Omega_F(A)$, e assim μ é uma aplicação que de fato leva $L(W - A)$ em $\Omega_F(A)$. Note também que μ é linear e injetiva. Para mostrar a

sobrejetividade, tome $\omega_1 \in \Omega_F(A)$. Pela proposição (2.1.11) existe $x \in F$ tal que $\omega_1 = x\omega$, e assim

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A \;\Rightarrow\; (x) \geq -(W - A) \quad \Rightarrow \quad x \in L(W - A)$$

Logo μ é isomorfismo e daí

$$\dim \Omega_F(A) = \ell(W - A)$$

mas como $\dim \Omega_F(A) = i(A)$ pelo lema (2.1.9), segue que $\ell(W - A) = i(A)$. □

E agora sim, vamos obter o Teorema de Riemann-Roch, como uma simples consequência do resultado acima.

Teorema 2.1.17 (Teorema de Riemann-Roch)**.** *Seja W um divisor canônico qualquer de F/K. Então para cada divisor $A \in Div\,(F)$,*

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

Demonstração. Da definição de $i(A)$ temos $\ell(A) = \deg(A) + 1 - g + i(A)$ e pelo teorema (2.1.16) segue que

$$\ell(A) = \deg(A) + 1 - g + \ell(W - A), \quad \text{para algum } W \text{ divisor canônico.}$$

□

Corolário 2.1.18. *Para um divisor canônico W temos*

$$\deg(W) = 2g - 2 \quad \textit{e} \quad \ell(W) = g$$

Demonstração. Para $A = 0$ o teorema de Riemann-Roch nos diz que

$$1 = \ell(0) = \deg(0) + 1 - g + \ell(W - 0) \quad \text{o que implica que} \quad \ell(W) = g$$

E para $A = W$, usando que $\ell(W) = g$, temos

$$g = \ell(W) = \deg(W) + 1 - g + \ell(0) \quad \text{e consequentemente} \quad \deg(W) = 2g - 2$$

□

No Teorema de Riemann vimos que existe uma constante c que só depende de F/K tal que para todo $A \in$ Div (F) com $\deg(A) \geq c$ vale $i(A) = 0$. Agora vamos especificar mais esta constante.

Teorema 2.1.19. *Se A é um divisor de F/K com $\deg(A) \geq 2g-1$ então*

$$\ell(A) = \deg(A) + 1 - g$$

Demonstração. Pelo teorema de Riemann-Roch temos $\ell(A) = \deg(A) + 1 - g + \ell(W - A)$, para algum W divisor canônico. Vimos no corolário (2.1.18) que $\deg(W) = 2g-2$ e como $\deg(A) \geq 2g-1$ temos

$$\deg(W - A) = \deg(W) - \deg(A) \leq (2g-2) - (2g-1) = -1$$

logo $\deg(W - A) < 0$ e daí $\ell(W - A) = 0$, pelo corolário (1.3.12). E o teorema segue. □

Observe que esta cota não pode ser melhorada pois para o divisor canônico, que tem grau uma unidade a menos, vale:

$$\ell(W) > \deg(W) + 1 - g.$$

pelo corolário (2.1.18).

2.2 Consequências do Teorema de Riemann-Roch

Nosso objetivo aqui é mostrar algumas consequências do Teorema de Riemann-Roch. Nosso primeiro resultado apresenta uma caracterização do gênero e da classe canônica de F/K, onde F/K segue sendo o corpo das funções algébricas de gênero g.

Proposição 2.2.1. *Suponha que $g_0 \in \mathbb{Z}$ e $W_0 \in$ Div (F) satisfazem*

$$\ell(A) = \deg(A) + 1 - g_0 + \ell(W_0 - A) \tag{2.3}$$

para todo $A \in$ Div (F). Então $g_0 = g$ e W_0 é divisor canônico.

Demonstração. Fazendo $A = 0$ e $A = W_0$ temos:

$$1 = \ell(0) = 1 - g_0 + \ell(W_0), \quad \text{e portanto} \quad \ell(W_0) = g_0 \quad \text{e}$$
$$g_0 = \deg(W_0) + 1 - g_0, \quad \text{e logo} \quad \deg(W_0) = 2g_0 - 2$$

Agora seja W um divisor canônico de F/K. Escolha uma divisor A tal que $\deg(A) > \max\{2g-2, 2g_0-2\}$. Assim, $\deg(A) \geq 2g-1$ e logo, pelo teorema (2.1.19) segue que $\ell(A) = \deg(A) + 1 - g$.

E ao mesmo tempo $\deg(W_0 - A) < 0$ e assim $\ell(W_0 - A) = 0$, logo $\ell(A) = \deg(A) + 1 - g_0$ e assim $g = g_0$.

Agora fazendo $A = W$ em (2.3) temos $g = \ell(W) = \deg(W) + 1 - g_0 + \ell(W_0 - W)$ e como $g = g_0$ e $\deg(W) = 2g-2$ segue que $\ell(W_0 - W) = 1$. E como $\deg(W_0 - W) = 0$ (pois $\deg(W_0) = 2g_0 - 2 = 2g - 2 = \deg W$) segue que $W_0 = W$, como queríamos. □

A proposição a seguir é uma outra forma de caracterizar os divisores canônicos.

Proposição 2.2.2. *Um divisor B é canônico se, e somente se, $\deg(B) = 2g-2$ e $\ell(B) \geq g$.*

Demonstração. Se B é divisor canônico, a conclusão segue do corolário (2.1.18). Agora suponha que $\deg(B) = 2g-2$ e $\ell(B) \geq g$. Daí, usando o teorema de Riemann-Roch (W divisor canônico qualquer):

$$g \leq \ell(B) = (2g-2) + 1 - g + \ell(W - B) = g - 1 + \ell(W - B) \quad \therefore \quad 1 \leq \ell(W - B)$$

e como $\deg(W - B) = 0$ então $1 \leq \ell(W - B)$ implica que $W - B$ é principal, pelo corolário (1.3.12). Logo $W \sim B$. □

Agora, para exemplificar uma aplicação do Teorema de Riemann-Roch vamos usá-lo para caracterizar o corpo de funções racionais $F = K(x)$.

Proposição 2.2.3. *Para um corpo de funções F/K as seguintes condições são equivalentes:*

(1) F/K é racional, i.e., $F = K(x)$ para algum x que é transcendente sobre o corpo K.

(2) F/K tem gênero 0 e existe um divisor $A \in Div\,(F)$ com $\deg(A) = 1$.

Demonstração. [$(1) \Rightarrow (2)$] No exemplo (1.3.18), no final do capítulo 1, vimos que $g = 0$ para $F = K(x)$. E em (A.1.1)(c) vimos que P_∞ é um divisor de $K(x)$ com $\deg(P_\infty) = 1$.

[$(2) \Rightarrow (1)$] Seja $g = 0$ e $A \in$ Div (F) com $\deg(A) = 1$. Como $\deg(A) = 1 \geq 2g - 1 = -1$, então $\ell(A) = \deg(A) + 1 - g = 2 > 0$. Logo $L(A) \neq \{0\}$ e portanto existe $0 \leq A' \in [A]$. Daí $\ell(A') = \ell(A) = 2 > 0$ e assim existe $x \in L(A') \backslash K$ com $(x) \neq 0$ e logo $(x) + A' \geq 0$. Como $A' \geq 0$ e $\deg(A') = 1$, para que $(x) + A' \geq 0$ ocorra devemos ter $A' = (x)_\infty$. Mas então

$$1 = \deg(A') = \deg(x)_\infty = [F : K(x)]$$

logo $F = K(x)$.

□

Observação 2.2.4. *Existem corpos de funções não racionais de gênero* 0 *(esses corpos não podem conter um divisor de grau 1, conforme a proposição (2.2.3)).*

Contudo se K *é algebricamente fechado ou um corpo finito é possível mostrar que sempre existe um divisor de grau 1. Sendo assim, nesses dois casos vale* $g = 0 \Leftrightarrow F/K$ *é racional.*

Nosso próximo resultado é uma versão mais forte do Teorema (1.2.1) (Aproximação Fraca).

Teorema 2.2.5 (Teorema da Aproximação Forte)**.** *Seja* $S \subsetneq \mathbb{P}_F$ *um subgrupo próprio de* $\mathbb{P}_F$ *e* $P_1, \cdots, P_r \in S$*. Suponha que são dados elementos* $x_1, \cdots, x_r \in F$ *e* $n_1, \cdots, n_r \in \mathbb{Z}$*. Então existe um elemento* $x \in F$ *tal que*

$$\begin{aligned} &v_{P_i}(x - x_i) = n_i && (i = 1, \cdots, r) \text{ e} \\ &v_P(x) \geq 0 && \text{para todo } P \in S \backslash \{P_1, \cdots, P_r\} \end{aligned}$$

Demonstração. Considere o adele $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ da seguinte forma

$$\alpha_P := \begin{cases} x_i & \text{para } P = P_i, \quad i = 1, \cdots, r \\ 0 & \text{caso contrário.} \end{cases}$$

Tome $Q \in \mathbb{P}_F \backslash S$. Para um $m \in \mathbb{N}$ suficientemente grande temos

$$\mathcal{A}_F = \mathcal{A}_F \left(mQ - \sum_{i=1}^{r} (n_i + 1) P_i \right) + F$$

de fato, existe tal m pois, pelo teorema (1.3.17) para um divisor D de grau suficientemente grande vale $0 = i(D)$ o que implica $\mathcal{A}_F = \mathcal{A}_F(D) + F$, pelo lema (2.1.6).

Então existe um elemento $z \in F$ com $z - \alpha \in \mathcal{A}_F \left(mQ - \sum_{i=1}^{r} (n_i + 1) P_i \right)$, isto é

$$v_P(z - \alpha) + v_P(mQ) - \sum_{i=1}^{r} (n_i + 1) v_P(P_i) \geq 0.$$

Daí já podemos concluir que

$$\begin{aligned} &v_{P_i}(z - x_i) > n_i && \text{para} \quad i = 1, \cdots, r \quad \text{e} \\ &v_P(z) \geq 0 && \text{para} \quad P \in S \backslash \{P_1, \cdots, P_r\}. \end{aligned} \tag{2.4}$$

Tome agora $y_1, \cdots, y_r \in F$ com $v_{P_i}(y_i) = n_i$ (existem pois v_{P_i} é sobrejetiva sobre $\mathbb{Z} \cup \{\infty\}$). Da mesma forma que fizemos pra obter z, construímos $y \in F$ com

$$\begin{aligned} v_{P_i}(y - y_i) &> n_i \qquad \text{para} \quad i = 1, \cdots, r \ \text{ e} \\ v_P(y) &\geq 0 \qquad \text{para} \quad P \in S \backslash \{P_1, \cdots, P_r\}. \end{aligned} \tag{2.5}$$

Então temos, para $i = 1, \cdots, r$, pela desigualdade triangular estrita e pela equação (2.5),

$$v_{P_i}(y) = v_{P_i}((y - y_i) + y_i) = \min\{v_{P_i}(y - y_i) > n_i, v_{P_i}(y_i) = n_i\} = n_i$$

Fazendo $x := y + z$ obtemos

$$v_{P_i}(x - x_i) = v_{P_i}(y + (z - x_i)) = \min\{v_{P_i}(y) = n_i, v_P(z - x_i) > n_i\} = n_i,$$

para $i - 1, \cdots, r$.

E para $P \in S \backslash \{P_1, \cdots, P_r\}$, temos $v_P(x) = v_P(y+z) \geq 0$ pelas equações (2.4) e (2.5). □

Agora vamos estudar os casos em que um elemento de F tem apenas um pólo (de multiplicidade qualquer). Os resultados a seguir serão muito importantes para o capítulo 4.

Proposição 2.2.6. *Seja $P \in \mathbb{P}_F$. Então para cada $n \geq 2g$ existe um elemento $x \in F$ com divisor pólo $(x)_\infty = nP$.*

Demonstração. Como $\deg((n-1)P) \geq (2g-1)$ e $\deg(nP) \geq 2g$, pelo teorema (2.1.19) sabemos que $\ell((n-1)P) = (n-1)\deg(P) + 1 - g$ e $\ell(nP) = n\deg(P) + 1 - g$. Assim $\ell((n-1)P) < \ell(nP)$ e portanto $L((n-1)P) \subsetneq L(nP)$.

Assim, se $x \in L(nP) \backslash L((n-1)P)$ então x tem pólo em nP de ordem no máximo n e x não tem pólo de ordem menor ou igual $n-1$. Portanto $(x)_\infty = nP$. □

Definição 2.2.7. *Seja $P \in \mathbb{P}_F$. Um inteiro $n \geq 0$ é chamado de ordem do pólo P se existe um elemento $x \in F$ com $(x)_\infty = nP$. Caso contrário n é chamado uma lacuna de P.*

Note que, da proposição (2.2.6) segue que n é a ordem de um pólo P se, e somente se, $\ell((n-1)P) < \ell(nP)$. E também podemos ver que o conjunto das ordens dos pólos de P é um sub-semigrupo do semigrupo aditivo de $\mathbb{N}$. Para ver isso basta observar que se $(x_1)_\infty = n_1 P$ e $(x_2)_\infty = n_2 P$ então $x_1 x_2$ tem pólo divisor $(x_1 x_2)_\infty = (n_1 + n_2)P$.

O teorema a seguir nos diz exatamente quantas lacunas possui um lugar de grau 1.

Teorema 2.2.8 (Teorema das Lacunas de Weierstrass)**.** *Suponha que F/K tem gênero $g > 0$ e P é um lugar de grau 1. Então existem exatamente g lacunas $i_1 < \cdots < i_g$ de P. E ainda*

$$i_1 = 1 \quad \text{e} \quad i_g \leq 2g - 1$$

Demonstração. Cada lacuna é menor que $2g-1$ pela proposição (2.2.6). E note que se $x \in K$ então $(x)_\infty = 0 = 0P$ para qualquer $P \in \mathbb{P}_F$. Logo 0 é ordem do pólo P para todo $P \in \mathbb{P}_F$.

Sabemos que n é ordem de um pólo P se e somente se $\ell((n-1)P) < \ell(nP)$, logo i é lacuna de P se e só se $L((i-1)P) = L(iP)$.

Agora considere a sequência de espaçoS vetoriais e a sequência formada por suas respectivas dimensões:

$$\begin{array}{ccccccccc} K & = & L(0) & = & L(P) & = & L(2P) & = \cdots = & L((2g-1)P) \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ & & 1 & & j_1 & & j_2 & \cdots & g \end{array}$$

(lembrando que $\ell(0) = 1$ e que, pelo teorema (2.1.19), $\ell((2g-1)P) = \deg((2g-1)P)+1-g = g$ pois $\deg(P) = 1$).

Observe que

$$\dim L(iP) \leq \dim L((i-1)P) + 1 \quad \forall i = 1, \cdots, 2g-1$$

pois $\dim(\ell(iP/(i-1)P)) \leq \deg(iP) - \deg((i-1)P)$, pelo lema (1.3.8). Isto significa que a cada vez que as dimensões j_i, j_{i+1} não são iguais damos um salto de uma unidade de uma dimensão para outra. Mas como nossa sequência tem dimensão máxima igual a g, significa que só podem haver $g-1$ saltos. Como os saltos ocorrem quando $L(iP) \neq L((i-1)P)$ e temos $2g-1$ espaços na sequência, segue que, em exatamente g deles, temos $L(iP) = L((i-1)P)$ e portanto, g lacunas de P.

E note também que, como o conjunto das ordens dos pólos é um semigrupo aditivo, se 1 fosse ordem de algum pólo, então $\mathbb{N}$ estaria contido nesse conjunto, logo todo natural seria ordem de pólo, isto é, não haveriam lacunas, o que é um absurdo pois $g > 0$ e vimos acima que existem exatamente g lacunas de P. □

Observação 2.2.9. *Suponha que K é algebricamente fechado. Então pode-se mostrar que quase todos os lugares de F/K tem a mesma sequência de lacunas (os quais são chamadas de lacunas do corpo de funções F/K). Tais lugares são ditos ordinários. Todo lugar não ordinário é chamado de Ponto de Weierstrass de F/K. Sabe-se também que se o gênero de F/Ké maior ou igual a 2 então existe pelo menos um ponto de Weierstrass.*

Para divisores com $\deg(A) < 0$ vimos que $L(A) = 0$ no corolário (1.3.12). Por outro lado, se $\deg(A) > 2g-2$ então $\ell(A) = \deg(A) + 1 - g$ pelo teorema 2.1.19. E, na maior parte dos casos que vamos utilizar, os divisores terão grau maior ou igual a $2g-1$. Contudo, cabe a

pergunta do que podemos afirmar quando $0 \leq \deg(A) \leq 2g-2$. Para responder essa questão, segue o teorema de Clifford.

Teorema 2.2.10 (Teorema de Clifford)**.** *Para todos os divisores $A \in Div\, F$ com $0 \leq \deg(A) \leq 2g-2$ vale*

$$\ell(A) \leq 1 + \frac{1}{2} \cdot \deg(A)$$

O principal passo para a demonstração desse resultado é o lema a seguir

Lema 2.2.11. *Suponha que A e B são divisores tais que $\ell(A) > 0, \ell(B) > 0$. Então*

$$\ell(A) + \ell(B) \geq 1 + \ell(A + B)$$

A demonstração é direta para $\ell(A) = 0$ e para $\ell(W-A) = 0$ (apenas usando que $\deg(A) = 1/2\deg(A) + 1/2\deg(A)$). Para $\ell(A) > 0$ e $\ell(W - A) > 0$, usando o lema 2.2.11 temos $\ell(A) + \ell(W - A) \geq 1 + \ell(A + W - A) = 1 + \ell(W) = 1 + g$. E somando com a equação que obtemos pelo Teorema de Riemann-Roch segue o resultado.

2.3 Componentes dos diferenciais de Weil

Esta seção é de suma importância para entendermos como são gerados os códigos de Goppa, pois estes códigos tem em suas coordenadas componentes dos diferenciais de Weil.

Na seção 2.1 fizemos uma imersão de $F \hookrightarrow \mathcal{A}_F$ que levava cada $x \in F$ para o correspondente adele principal. Agora vamos definir, para cada lugar $P \in \mathbb{P}_F$ uma nova imersão $\iota_P : F \hookrightarrow \mathcal{A}_F$.

Definição 2.3.1. *Seja $P \in \mathbb{P}_F$.*

(a) Para $x \in F$ seja $\iota_P(x)$ o adele cuja componente P é x e as componentes restantes são iguais a zero.

(b) Para um diferencial de Weil $\omega \in \Omega_F$ nós definimos seu componente local $\omega_P : F \to K$ como

$$\omega_P(x) := \omega(\iota_P(x)).$$

Observe que ω_P é uma aplicação K-linear.

Proposição 2.3.2. *Seja $\omega \in \Omega_F$ e $\alpha = (\alpha_P) \in \mathcal{A}_F$. Então $\omega_P(\alpha_P) \neq 0$ para pelo menos uma quantidade finita de lugares P, e*

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P)$$

Em particular

$$\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0$$

Demonstração. Podemos assumir que $\omega \neq 0$ e fazer $W := (\omega)$ o divisor de ω. Sabemos que existe $S \subseteq \mathbb{P}_F$ tal que

$$v_P(W) = 0 \text{ e } \ v_P(\alpha_P) \geq 0 \quad \text{para todo } P \notin S.$$

(basta tomar $S \supseteq \text{supp}(W)$) Defina $\beta = (\beta_P) \in \mathcal{A}_F$ como

$$\beta_P := \begin{cases} \alpha_P & \text{para } \ P \notin S, \\ 0 & \text{para } \ P \in S. \end{cases}$$

Daí $\beta \in \mathcal{A}_F(W)$ pois $v_P(\beta) = v_P(\alpha_P) \geq 0 = -v_P(W)$, para $P \notin S$. E $v_P(\beta) = v_P(0) = 0 \geq -v_P(W)$ pois $v_P(W) \geq 0$ para $P \in S$. Assim, $\omega(\beta) = 0$

E também $\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_P)$. Logo,

$$\omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_P).$$

Para $P \notin S$, $\iota_P(\alpha_P) \in \mathcal{A}_F(W)$ (pois $v_P(\alpha_p) \geq 0 = v_P(W)$) e logo $\omega(\iota_P(\alpha_P)) = \omega_P(\alpha_P) = 0$.

Em particular, como $v_P(1) = 0 \geq -v_P(W)$ para todo $P \in \mathbb{P}_F$ segue que $\omega(1) = 0$. □

O próximo resultado nos mostra que um diferencial de Weil é unicamente determinado pelos seus componentes locais.

Proposição 2.3.3. *(a) Seja $\omega \neq 0$ um diferencial de Weil de F/K e $P \in \mathbb{P}_F$. Então*

$$v_P(\omega) = \max\{r \in \mathbb{Z} \,|\, \omega_P(x) = 0 \ \forall\, x \in F \text{ com } v_P(x) \geq -r\}$$

Em particular ω_P não é identicamente zero.

(b) Se $\omega, \omega' \in \Omega_F$ e $\omega_P = \omega'_P$ para algum $P \in \mathbb{P}_F$ então $\omega = \omega'$.

Antes de iniciarmos a demonstração, vamos entender o que nos diz a proposição. O item (a) nos diz que $v_P(\omega)$ é o maior inteiro r tal que $\omega_P(x) = 0$ para todo x com $v_P(x) \geq -r$. Isso nos diz que $\omega_P \not\equiv 0$. O item (b) afirma que se dois diferenciais de Weil tem pelo menos um componente local em comum então esses diferenciais são iguais.

(Demonstração da proposição). (a) Por definição, $v_P(\omega) = v_P(W)$ onde $W = (\omega)$. Faça $s := v_P(\omega)$. Seja $x \in F$ com $v_P(x) \geq -s = -v_P(\omega)$. Daí temos $\iota_P(x) \in \mathcal{A}_F(W)$, logo $\omega_P(x) = \omega(\iota_P(x)) = 0$. Assim, para todo x que satisfaz $v_P(x) \geq -v_P(\omega)$ temos $\omega_P(x) = 0$. Só falta mostrar que esse valor é o maior possível.

Agora suponha que $\omega_P(x) = 0$ para todo $x \in F$ com $v_P(x) \geq -(s+1)$. Seja $\alpha = (\alpha_Q)_{Q \in \mathbb{P}_F} \in \mathcal{A}_F(W + P)$, onde P é o lugar dado por hipótese. Assim:

$$\alpha = (\alpha - \iota_P(\alpha_P)) + \iota_P(\alpha_P)$$

com $\alpha - \iota_P(\alpha_P) \in \mathcal{A}_F(W)$ (pois estamos retirando justamente a componente P de α) . Daí,

$$\omega(\alpha) = \omega(\alpha - \iota_P(\alpha_P)) + \omega_P(\alpha_P) = 0$$

pois estamos supondo que $\omega_P(x) = 0$ para todo $x \in F$ com $v_P(x) \geq -(s+1)$ e $\alpha_P \in F$ com $v_P(\alpha_P) \geq -(s+1)$. Daí, ω se anula em $\mathcal{A}_F(W+P)$ o que contraria a maximalidade do divisor W (conforme definição (2.1.13)).

(b) Se $\omega_P = \omega'_P$ então $(\omega - \omega')_P = 0$. Daí, como vimos em (a) que um componente local de um diferencial não nulo não pode ser identicamente zero, segue que $\omega = \omega'$.

□

A proposição a seguir é um exemplo de como obter um divisor a partir de um diferencial de Weil e as componentes desse diferencial, usando o corpo de funções mais simples, $F = K(x)$. Vamos usar a notação definida em na seção 1.2: P_∞ denota o pólo divisor de x e P_a denota o lugar associado ao polinômio $x - a$, para $a \in K$.

Proposição 2.3.4. *Para um corpo de funções racionais $F = K(x)$ valem as seguintes afirmações:*

(a) O divisor $-2P_\infty$ é canônico.

(b) Existe um único diferencial de Weil $\eta \in \Omega_{K(x)}$ com $(\eta) = -2P_\infty$ e $\eta_{P_\infty}(x^{-1}) = -1$.

(c) *Os componentes locais η_{P_∞} e resp. η_{P_a} do diferencial de Weil η definido acima satisfazem*

$$\eta_{P_\infty}((x-a)^n) = \begin{cases} 0 & \textit{para } n \neq -1, \\ -1 & \textit{para } n = -1. \end{cases}$$

$$\eta_{P_a}((x-a)^n) = \begin{cases} 0 & \textit{para } n \neq -1, \\ 1 & \textit{para } n = -1. \end{cases}$$

Demonstração. (a) Note que $\deg(-2P_\infty) = -2 = 2g-2$ e que $\ell(-2P_\infty) = 0 = g$ (exemplo (1.3.18) mostra que em $F = K(x)$, $g = 0$). Daí, $-2P_\infty$ é canônico pela proposição (2.2.2).

(b) Tome um diferencial de Weil tal que $(\omega) = -2P_\infty$ (existe pois $-2P_\infty$ é canônico). Então ω se anula em $\mathcal{A}_{K(x)}(-2P_\infty)$ mas não é identicamente nula em $\mathcal{A}_{K(x)}(-P_\infty)$ (pela definição de divisor canônico). Como do lema (2.1.3) temos

$$\dim \mathcal{A}_{K(x)}(-P_\infty)/\mathcal{A}_{K(x)}(-2P_\infty) = \deg(-P_\infty) - \deg(-2P_\infty) = 1$$

e além disso, como

$$\iota_{P_\infty}(x^{-1}) \in \mathcal{A}_{K(x)}(-P_\infty) \backslash \mathcal{A}_{K(x)}(-2P_\infty),$$

segue que

$$\omega_{P_\infty}(x^{-1}) = \omega(\iota_{P_\infty}(x^{-1})) =: c \neq 0.$$

Fazendo $\eta := -c^{-1}\omega$ obtemos $(\eta) = (-c^{-1}) + (\omega) = -2P_\infty$, pois $c \in K$ e $\eta_{P_\infty}(x^{-1}) = -c^{-1}\omega_{P_\infty}(x^{-1}) = -1$.

(c) Como um diferencial de Weil se anula em adeles principais, segue da proposição (2.3.2) que

$$0 = \eta((x-a)^n) = \sum_{P \in \mathbb{P}_F} \eta_P((x-a)^n) \tag{2.6}$$

pois $((x-a)^n)$ é um adele principal.

Para $P \neq P_\infty$ e $P \neq P_a$ temos $v_P((x-a)^n) = 0$, pois caso contrário, existiriam outros polinômios irredutíveis que dividiriam $((x-a)^n)$, o que não ocorre. E como $(\eta) = -2P_\infty$, segue da proposição (2.3.3) que, para $P \neq P_\infty$ e $P \neq P_a$ temos $\eta_P((x-a)^n) = 0$. E observando a equação (2.6) temos

$$\eta_{P_\infty}((x-a)^n) + \eta_{P_a}((x-a)^n) = 0 \tag{2.7}$$

Vejamos as possibilidades para n. Para $n \leq -2$ temos $v_{P_\infty}((x-a)^n) = -n \geq 2 \geq -2 = v_{P_\infty}(\eta)$ e daí por (2.3.3) segue que $\eta_{P_\infty}((x-a)^n) = 0$. E de (2.7) segue que $\eta_{P_a}((x-a)^n) = 0$.

Para $n \geq 0$ temos $v_{P_a}((x-a)^n) = n \geq 0 = v_{P_a}(\eta)$ e assim, da mesma forma que antes, $\eta_{P_a}((x-a)^n) = 0$ e $\eta_{P_\infty}((x-a)^n) = 0$, por (2.7). Assim, só nos resta considerar $n = -1$.

Como, para $n = -1$,

$$\frac{1}{x-a} = \frac{a}{a(x-a)} + \frac{1}{x} \text{ e } \iota_{P_\infty}\left(\frac{a}{x(x-a)}\right) \in \mathcal{A}_{K(x)}(-2P_\infty),$$

temos que $\eta_{P_\infty}((x-a)^{-1}) = \eta_{P_\infty}\left(\frac{a}{x(x-a)}\right) + \eta_{P_\infty}\left(x^{-1}\right) = \eta_{P_\infty}\left(x^{-1}\right) = -1$. E de (2.7) temos $\eta_{P_a}((x-a)^{-1}) = 1$

□

2.4 Curvas algébricas e corpos de Funções

Corpos de funções algébricas e curvas algébricas projetivas não-singulares estão estreitamente relacionados. E essa relação tem sido muito útil para a teoria dos códigos pois possibilita melhorar as cotas existentes para distância mínima.

No capítulo 4 vamos precisar saber o que significa um corpo de funções definido sobre uma curva algébrica. Esta seção é dedicada a fazermos essa transição, que, essencialmente, associa o polinômio que define a curva algébrica ao corpo de funções. Vamos começar definindo o que são curvas algébricas planas.

Definição 2.4.1. *Seja K um corpo e $\widetilde{K}$ seu fecho algébrico. Se $f(X,Y)$ é um polinômio em $K[X,Y]$ então a curva algébrica plana afim associada C_a é dada por*

$$C_a = \{(x,y) \in \widetilde{K} \times \widetilde{K} \mid f(x,y) = 0\}$$

onde $f(X,Y)$ é um polinômio absolutamente irredutível, isto é, irredutível sobre $\widetilde{K}[X,Y]$, e por esse motivo também dizemos que a curva é absolutamente irredutível.

O grau do polinômio f, denotado por $\deg f$, é dado pelo máximo grau dos monômios, onde o grau do monômio $x^i y^j$ é definido como $i+j$.

Podemos associar ao polinômio $f(X,Y)$ o polinômio homogêneo

$$F(X,Y,Z) := Z^d f(X/Z, Y/Z), \text{ onde } d = \deg f.$$

Além disso, vamos definir $(x_1 : y_1 : z_1)$ como a classe de equivalência dada pela relação

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \Leftrightarrow (x_1, y_1, z_1) = \lambda(x_2, y_2, z_2) \text{ para algum } \lambda \in \widetilde{K}.$$

Dito isto, podemos definir curva projetiva.

Definição 2.4.2. *A curva plana projetiva C é definida como*

$$C = \{(x_1 : y_1 : z_1) \in \widetilde{K}^3 \mid F(x_1, y_1, z_1) = 0\}$$

Note que a curva afim C_a está imersa na curva projetiva pela aplicação $(x, y) \mapsto (x, y, 1)$. Para $z = 0$ dizemos que $(x : y : 0)$ é um ponto no infinito e denotamos o conjunto desses pontos por P_∞. Assim, $\#C = \#C_a + \#P_\infty$.

Dizemos que uma curva projetiva é não singular (ou suave) se a seguinte condição é satisfeita

$$F(x, y, z) = F_X(x, y, z) = F_Y(x, y, z) = F_Z(x, y, z) = 0 \ \Rightarrow \ (x, y, z) = 0.$$

Um invariante básico da curva plana C é o seu gênero $g = g(C)$. Esse invariante satisfaz:

$$g \leq \frac{(d-1)(d-2)}{2}, \quad \text{com } d = \deg(f(X, Y)).$$

Quando a curva é não-singular vale a igualdade.

Agora podemos passar a relação existente entre curvas projetivas e corpos de funções. Uma curva projetiva absolutamente irredutível χ está associada a um corpo de funções da seguinte forma: se $f(X, Y) \in K[X, Y]$ é o polinômio irredutível que define χ, seja R o anel residual de $K[X, Y]$ módulo $f(X, Y)$ e seja F o corpo de frações de R; então F é o corpo de funções algébricas associado a χ e denotaremos por $F(\chi)$. Quando χ é não singular, os pontos de χ estão em bijeção com os lugares de seu corpo de funções.

Observação 2.4.3. *Em particular, os lugares de grau 1 estão em bijeção com os pontos da curva projetiva $(a, b) \in K \times K$. Note que a curva χ tem infinitos pontos, assim como o corpo de funções tem infinitos lugares. Dizer que os lugares de grau 1 estão em bijeção com os pontos de $K \times K$ nos diz que, se K é um corpo finito, então a quantidade de lugares de grau 1 é finita.*

No exemplo a seguir vamos usar essa relação entre corpo de funções e curvas algébricas para contar os lugares de grau 1 num corpo de funções Hermitiano. Esse resultado será muito útil no capítulo 4.

Exemplo 2.4.4. *Seja $K = \mathbb{F}_{q^2}$ e considere a curva projetiva absolutamente irredutível χ associada ao polinômio $Y^q + Y = X^{q+1}$. Essa curva é conhecida como a curva de Hermite. Queremos mostrar que a quantidade de lugares de grau 1 em $F(\chi)$ é q^3+1. Para isso, vamos usar a observação (2.4.3) acima, que nos diz que lugares de grau 1 estão em bijeção com os pontos de curva χ em $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$.*

Vamos contar os pontos de $\chi(\mathbb{F}_{q^2})$ a começar da parte afim, $\chi_a(\mathbb{F}_{q^2})$.

$$\begin{aligned}\chi_a(\mathbb{F}_{q^2}) &= \{(x,y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid f(x,y) = 0\} \\ &= \{(x,y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid y^q + y = x^{q+1}\} \\ &= \{(x,y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid \tau(y) = \mathcal{N}(x)\}\end{aligned}$$

onde τ e $\mathcal{N}$ são o Traço e a Norma da extensão $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$. Usando que traço e norma tem como imagem $\mathbb{F}_q$ (pois são aplicações de $\mathbb{F}_{q^2} \to \mathbb{F}_q$) podemos ver que $\tau^{-1}(y) = q$. E sendo que o traço é sobrejetivo e $\mathbb{F}_q$-linear temos

$$\begin{aligned}\#\chi_a(\mathbb{F}_{q^2}) &= \sum_{x \in \mathbb{F}_{q^2}} \#\{y \in \mathbb{F}_{q^2} \mid \tau(y) = x^{q+1}\} \\ &= \sum_{x \in \mathbb{F}_{q^2}} \#\tau^{-1}(x^{q+1}) \\ &= \sum_{x \in \mathbb{F}_{q^2}} q = q \cdot q^2 = q^3\end{aligned}$$

Agora, só nos resta saber quantos são os pontos no infinito.

Seja $F(X,Y,Z) = Y^q Z + Y Z^q - X^{q+1}$ o polinômio $f(X,Y)$ homogenizado. Se $Z = 0$ então $X = 0$. Logo o único ponto no infinito é $(0:Y:0)$ e assim $\#P_\infty = 1$.

Logo $\#\chi(\mathbb{F}_{q^2}) = \#\chi_a(\mathbb{F}_{q^2}) + \#P_\infty = q^3 + 1$.

E da bijeção com os lugares de grau 1 de $F(\chi)$ segue que um corpo de funções sobre uma curva de Hermite tem $q^3 + 1$ lugares de grau 1.

3

Códigos de Goppa

3.1 Códigos de Goppa

Códigos de Goppa foram introduzidos por V.D.Goppa em 1981. Como uma motivação para a construção desses códigos nós primeiro estudaremos os códigos de Reed-Solomon sobre $\mathbb{F}_q$. Essa importante classe de códigos é muito conhecida na teoria de códigos. Os códigos de Goppa são uma generalização muito natural dos códigos de Reed-Solomon.

Leitores pouco familiarizados com teoria básica de códigos podem consultar o apêndice B.

Seja $n = q - 1$ e seja $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^*$, i.e., $\mathbb{F}_q^* = \{\beta, \beta^2, \cdots, \beta^{q-1} = 1\}$. Para um inteiro k com $1 \leq k \leq n$ consideramos o espaço vetorial k-dimensional (considerando que o polinômio nulo tem grau 0):

$$L_k := \{f \in \mathbb{F}_q[X] \mid \deg f \leq k - 1\}$$

e a *aplicação avaliação* ev $: L_k \to \mathbb{F}_q^n$ dada por

$$\text{ev}\,(f) := (f(\beta), f(\beta^2), \cdots, f(\beta^n)) \in \mathbb{F}_q^n. \tag{3.1}$$

Essa aplicação é $\mathbb{F}_q$-linear e é injetiva pois um polinômio não nulo $f \in \mathbb{F}_q$ de grau $\leq k-1 < n$ tem no máximo $k-1 < n$ raízes. Portanto

$$C_k := \{(f(\beta), f(\beta^2), \cdots, f(\beta^n)) \mid f \in L_k\}$$

é um código $[n,k]$ sobre $\mathbb{F}_q$ (a dimensão do código é a dimensão de L_k que é k). Este código é chamado um código RS (*Reed-Solomon*). O peso de uma palavra $0 \neq c = \text{ev}(f) \in C_k$ é dado por

$$\begin{aligned} wt(c) &= n - |\{i \in \{1, \cdots, n\}; f(\beta^i) = 0\}| \\ &\geq n - \deg f \geq n - (k-1). \end{aligned}$$

Logo a distância mínima d de C_k satisfaz a desigualdade $d \geq n+1-k$. Por outro lado, pela cota de Singleton temos $d \leq n+1-k$.

Antes de introduzirmos os códigos de Goppa, vamos definir uma notação que será usada no decorrer da seção.

- $F/\mathbb{F}_q$ é um corpo de funções algébricas de gênero g.
- $P_1, \cdots, P_n$ são lugares dois a dois distintos de $F/\mathbb{F}_q$ de grau 1.
- $D = P_1 + \cdots + P_n$.
- G é um divisor de $F/\mathbb{F}_q$ tal que $\text{supp}(G) \cap \text{supp}(D) = \emptyset$

Definição 3.1.1. *Um código de Goppa $C_L(D,G)$ associado aos divisores D e G é definido como*

$$C_L(D,G) := \{(x(P_1), \cdots, x(P_n)) \mid x \in L(G)\} \subseteq \mathbb{F}_q^n$$

Note que essa definição faz sentido, isto é, $x(P_i) \neq \infty$, para $i = 1, \cdots, n$, pois para $x \in L(G)$ temos $v_{P_i}(x) \geq 0 = -v_{P_i}(G)$ já que $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. A classe residual $x(P_i)$ de x módulo P_i é um elemento do corpo residual de P_i, F_{P_i}. Como $1 = \deg P_i = [F_{P_i} : \mathbb{F}_q]$ segue que $F_{P_i} = \mathbb{F}_q$ logo $x(P_i) \in \mathbb{F}_q$ e assim, $C_L(D,G) \in \mathbb{F}_q^n$.

Como em (3.1), podemos considerar a aplicação avaliação agora definida como $\text{ev}_D := L(G) \to \mathbb{F}_q^n$ dada por

$$\text{ev}_D := (x(P_1), \cdots, x(P_n)) \in \mathbb{F}_q^n.$$

A aplicação avaliação ev_D é $\mathbb{F}_q$-linear e $C_L(D,G)$ é a imagem de $L(G)$ por essa aplicação. Agora fica clara a analogia com códigos de RS.

O próximo teorema nos mostrará porque os códigos de Goppa são interessantes: neles é possível determinar (ou pelo menos estimar) os parâmetros n, k e d através do Teorema de Riemann-Roch . Também podemos obter uma cota inferior não trivial para a distância mínima desse código de uma forma bem geral.

Teorema 3.1.2. *$C_L(D,G)$ é um código $[n,k,d]$ com parâmetros*

$$k = \ell(G) - \ell(G-D) \text{ e } \quad d \geq n - \deg G.$$

Demonstração. Temos que ev_D é uma aplicação linear sobrejetiva de $L(G)$ sobre $C_L(D,G)$ (pela própria definição de $C_L(D,G)$) cujo núcleo é dado por

$$\ker(\text{ev}_D) = \{x \in L(G) \mid v_{P_i}(x) > 0 \text{ para } i = 1, \cdots, n\} = L(G-D).$$

A última igualdade é válida pois, como $x \in L(G)$, então $(x) + G \geq 0$. Mas ao mesmo tempo, $v_{P_i}(x) > 0$, logo $P_1, \cdots, P_n$ são zeros de x, assim ainda podemos retirar $P_1, \cdots, P_n$ de (x) e obter um divisor efetivo, isto é, $(x) + G - D \geq 0$. Assim $k = \dim C_L(D,G) = \dim L(G) - \dim L(G-D) = \ell(G) - \ell(G-D)$.

Para mostrar a afirmação sobre a distância mínima de $C_L(D,G)$ vamos considerar $C_L(D,G) \neq 0$ (não faz sentido falar de distância mínima se isto não ocorre). Seja $x \in L(G)$ com $wt(\text{ev}_D(x)) = d$. Então exatamente $n-d$ lugares são zeros de x, digamos $P_{i_1}, \cdots, P_{i_{n-d}} \in \text{supp}(D)$ e então

$$0 \neq x \in L(G - (P_{i_1} + \cdots + P_{i_{n-d}}))$$

e logo $\ell(G - (P_{i_1} + \cdots + P_{i_{n-d}})) > 0$ e assim pelo corolário (1.3.12) segue que

$$0 \leq \deg(G - (P_{i_1} + \cdots + P_{i_{n-d}})) = \deg G - n + d.$$

E assim, $d \geq n - \deg G$. □

Corolário 3.1.3. *Suponha que o grau de G seja estritamente menor que n. Então $\text{ev}_D : L(G) \to C_L(D,G)$ é injetiva, logo um isomorfismo, e temos*

(a) $C_L(D,G)$ é um código $[n,k,d]$ com

$$d \geq n - \deg G \text{ e } k = \ell(G) \geq \deg G + 1 - g.$$

Daí

$$k + d \geq n + 1 - g \tag{3.2}$$

(b) Se além disso $2g-2 < \deg G < n$ *então* $k = \deg G + 1 - g$.

(c) Se $\{x_1, \cdots, x_k\}$ *é uma base para* $L(G)$ *então a matriz*

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{pmatrix}$$

é a matriz geradora de $C_L(D, G)$.

Demonstração. (a) Como $\deg G < n$ então $\deg(G-D) = \deg G - n < 0$, logo $L(G-D) = 0$. Disso segue que ev_D é injetiva ($\ker(\text{ev}_D) = L(G-D)$) e que $k = \ell(G)$. Além disso, pelo Teorema de Riemann-Roch temos $\ell(G) = \deg G + 1 - g + \ell(W-G) \geq \deg G + 1 - g$.

(b) A hipótese adicional $2g - 2 < \deg G$ nos diz que $\deg(W-G) < 0$ e assim $\ell(W-G) = 0$ e assim o item b segue do Teorema de Riemann - Roch.

(c) Como ev_D é um isomorfismo, a imagem de uma base de $\ell(G)$ é uma base para $C_L(D, G)$.

□

A grande maioria dos códigos que trabalharemos nesse texto satisfarão o item (b). Basicamente, isto significa que para $2g-2 < \deg G < n$ vale $\ell(W-G) = 0$ no Teorema de Riemann-Roch , para W um divisor canônico qualquer.

Observe que a cota inferior (3.2) para a distância mínima é bem parecida com a cota superior de Singleton. Comparando as duas, com $\deg G < n$, temos:

$$n + 1 - g \leq k + d \leq n + 1,$$

e assim podemos ver que se F/K é tal que $g = 0$ então $k + d = n + 1$.

Definição 3.1.4. *O inteiro* $d^* := n - \deg G$ *é chamado de distância designada do código* $C_L(D, G)$.

O teorema (3.1.2) afirma que que a distância mínima d de um código de Goppa é, no mínimo, d^*.

Outro código pode ser associado aos divisores D e G, utilizando os componentes locais dos diferenciais de Weil. Vamos relembrar algumas notações introduzidas no capítulo 2. Para $A \in \text{Div}(F)$, $\Omega_F(A)$ é o espaço dos diferenciais de Weil ω com $\omega \geq A$ e é um espaço vetorial sobre $\mathbb{F}_q$ com dimensão finita e $\dim \Omega_F = i(A)$. Para um diferencial de Weil ω e um lugar $P \in \mathbb{P}_F$, a aplicação $\omega_P : F \to \mathbb{F}_q$ denota a componente local de ω em P.

Definição 3.1.5. *Sejam G e $D = P_1 + P_2 + \cdots + P_n$ divisores onde os P_i's são lugares de grau 1, dois a dois distintos e G e D com suportes distintos. Então definimos o código $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ como*

$$C_\Omega(D, G) := \{(\omega_{P_1}(1), \cdots, \omega_{P_n}(1)) \,|\, \omega \in \Omega_F(G - D)\}.$$

Este código também é chamado de código de Goppa. A relação entre $C_L(D, G)$ e $C_\Omega(D, G)$ ficará clara mais a frente. Nosso primeiro resultado sobre $C_\Omega(D, G)$ é um análogo do teorema (3.1.2). Para demonstrar esse resultado usaremos o lema a seguir:

Lema 3.1.6. *Seja $P \in \mathbb{P}_F$ um lugar de grau 1 e seja ω um diferencial de Weil com $v_P(\omega) \geq -1$. Então*

$$\omega_P(1) = 0 \Leftrightarrow v_P(\omega) \geq 0$$

Demonstração. Para provar esta afirmação usaremos (2.3.3), que nos diz que, para um inteiro $r \in \mathbb{Z}$,

$$v_P(\omega) \geq r \Leftrightarrow \omega_P(x) = 0 \quad \text{para todo } x \in F \text{ com } \quad v_P(x) \geq -r \tag{3.3}$$

Note que, se $v_P(\omega) \geq 0$ então $\omega_P(x) = 0$ para todo $x \in F$ com $v_P(x) \geq 0$; e como $v_P(1) = 0$ segue que $\omega_P(1) = 0$. Assim, a volta é válida.

Agora, suponha que $\omega_P(1) = 0$. Seja $x \in F$ com $v_P(x) \geq 0$. Vamos mostrar que $\omega_P(x) = 0$ pois assim por (3.3) teremos $v_P(\omega) \geq 0$.

Podemos escrever $x = a + y$ onde $a = x(P)$ e $y \in P$, i.e., $v_P(y) \geq 1$; e como $\deg P = 1$, segue que $F_P = \mathbb{F}_q$ logo $a \in \mathbb{F}_q$. Daí,

$$\omega_P(x) = \omega_P(a) + \omega_P(y) = a\omega_P(1) + 0 = 0$$

onde $\omega_P(y) = 0$ pois $v_P(y) \geq 1$ e $\omega \in \Omega_F$ é tal que $v_P(\omega) \geq -1$, logo por (3.3) temos $r = -1$ e $\omega_P(z) = 0$ para todo $z \in F$ com $v_P(z) \geq -1$. E isto conclui a prova do lema.

□

Teorema 3.1.7. *$C_\Omega(D, G)$ é um código $[n, k', d']$ com parâmetros*

$$k' = i(G - D) - i(G) \quad \textit{e} \quad d' \geq \deg G - (2g - 2).$$

Se $\deg G > 2g - 2$ então $k' = i(G - D) \geq n + g - 1 - \deg G$. E se além disso temos $2g - 2 < \deg G < n$ segue que

$$k' = n + g - 1 - \deg G.$$

Demonstração. Considere a aplicação $\mathbb{F}_q$-linear

$$\mu_D := \begin{cases} \Omega_F(G-D) & \to & C_\Omega(D,G), \\ \omega & \mapsto & (\omega_{P_1}(1), \cdots, \omega_{P_n}(1)). \end{cases}$$

Note que μ_D é sobrejetiva (pela definição de $C_\Omega(D,G)$). Além disso, $\ker(\mu_D)$ é formado pelo conjunto dos $\omega \in \Omega_F$ tais que $\omega_{P_i}(1) = 0$ para todo $i = 1, \cdots, n$. Mas pelo lema (3.1.6) isso implica $v_{P_i}(\omega) \geq 0$ e daí $(\omega) - G \geq 0$ ou seja $\ker(\mu_D) = \Omega_F(G)$. Assim

$$k' = \dim \Omega_F(G-D) - \dim \Omega_F(G) = i(G-D) - i(G). \tag{3.4}$$

Agora seja $\mu_D(\omega) \in C_\Omega(D,G)$ uma palavra de peso $m > 0$. Então $\omega_{P_i}(1) = 0$ para exatamente $n-m$ índices, digamos $i = i_1, \cdots, i_{n-m}$ e assim:

$$\omega \in \Omega_F(G - (D - \sum_{j=1}^{n-m} P_{i_j}))$$

pois pelo lema (3.1.6) temos que $\omega_{P_i}(1) = 0$ implica $v_{P_i}(\omega) \geq 0$, logo $(\omega) - (P_{i_1} + \cdots + P_{i_{n-m}}) \geq 0$. E como $\omega \in \Omega_F(G-D)$ a afirmação acima segue.

Assim $\Omega_F(G - (D - \sum_{j=1}^{n-m} P_{i_j})) \neq 0$ e, como pelo teorema (2.1.19) sabemos que se $\Omega_F(A) \neq 0$ então $\deg(A) \leq 2g-2$, segue que $\deg(G - (D - \sum_{j=1}^{n-m} P_{i_j})) \leq 2g-2$. Assim,

$$2g - 2 \geq \deg(G) - (n - (n-m)) = \deg(G) - m \text{ logo, } m \geq \deg(G) - (2g-2)$$

e em particular, como d' é o mínimo dos pesos, $d' \geq \deg(G) - (2g-2)$ □

O teorema a seguir mostra que existe uma ligação muito próxima entre $C_L(D,G)$ e $C_\Omega(D,G)$. É simples perceber que as dimensões são complementares usando o teorema (3.1.2), o lema (3.1.7) e o Teorema de Riemann-Roch, pois

$$\begin{aligned} \dim C_\Omega(D,G) &= i(G-D) - i(G) \\ &= \ell(G-D) + \deg(D) - \ell(G) \\ &= n - k = \dim C_L(D,G)^\perp. \end{aligned}$$

Teorema 3.1.8. *Os códigos $C_L(D,G)$ e $C_\Omega(D,G)$ são duais, i.e.,*

$$C_\Omega(D,G) = C_L(D,G)^\perp.$$

A demostração desse resultado será omitida e pode ser vista em [6]

Vejamos agora um exemplo de um código de Goppa.

Exemplo 3.1.9. *Seja X a curva Hermitiana $y^8 + y = x^9$ sobre $\mathbb{F}_{64}$. Pode-se mostrar que X é não singular. Sejam P_1 e P_2 lugares de grau 1 de $\mathbb{F}_{64}$.*

E assim sendo, façamos $C_\Omega(D, G)$ com $G = 7P_1 + 82P_2$ e D a soma dos $8^3 - 1$ outros pontos racionais de $\mathbb{F}_{64}(X)$ [V, teorema 4.3.4]. Note que $\deg(G) = 89$ e como X é não singular, $g = \frac{(d-1)(d-2)}{2} = \frac{(9-1)(9-2)}{2} = 28$.

Assim $2g - 2 = 54 < \deg(G) < n = 511$, logo, pelo teorema (3.1.7) segue que

$$\dim C_\Omega(D, G) = k = n + g - 1 - \deg(G) = 511 + 28 - 1 - 89 = 449.$$

E pela cota de Goppa,

$$d \geq \deg(G) - 2g + 2 = 89 - 56 + 2 = 35.$$

Logo esse código detecta pelo menos 34 erros e corrige ao menos 17 erros.

4

Códigos de Goppa e o semigrupo Weierstrass para um par de pontos

4.1 Código de dois pontos e Semigrupo de Weierstrass

Seja X uma curva projetiva absolutamente irredutível e não-singular de gênero $g > 1$ sobre $\mathbb{F}_q$ e seja $\mathbb{F}_q(X)$ seu corpo de funções. Conforme visto na seção 2.4, valem todos os resultados mostrados nos capítulos 1 e 2 para esse corpo de funções. Além disso, dada a bijeção entre os lugares de grau 1 e os pontos racionais de X sobre $\mathbb{F}_q$, vamos chamá-los de pontos racionais de $\mathbb{F}_q$.

Retomando o capítulo 3, seja $C_L(D,G) = (f(Q_1), f(Q_2), \cdots, f(Q_n))$ e $C_\Omega(D,G) = (\eta_{Q_1}, \eta_{Q_2}, \cdots, \eta_{Q_n})$ onde $f \in L(G)$, $\eta \in \Omega_F(G-D)$ e $D = Q_1 + \cdots + Q_n$.

Definição 4.1.1. *Se $G = mP$ para algum ponto racional de $\mathbb{F}_q$, $m \in \mathbb{N}$ e D é a soma de todos os outros pontos racionais em X, diremos que $C_L(D,G)$ e $C_\Omega(D,G)$ são códigos de um ponto.*

Se $G = \alpha_1 P_1 + \alpha_2 P_2$ para P_1, P_2 pontos racionais distintos de $\mathbb{F}_q$, $\alpha_1, \alpha_2 \in \mathbb{N}$ e D é a soma de todos os outros pontos racionais de $\mathbb{F}_q$ diremos que $C_L(D,G)$ e $C_\Omega(D,G)$ são códigos de dois pontos.

Note que códigos de dois pontos tem comprimento uma unidade a menos (já que D tem um ponto a menos) que o código de um ponto na mesma curva.

Definição 4.1.2. *Para pontos racionais P_1 e P_2 de $\mathbb{F}_q$, definimos o semigrupo de Weierstrass do ponto P_1 por*

$$\mathcal{H}(P_1) = \{\alpha \in \mathbb{N}_0 \,|\, \exists x \in \mathbb{F}_q(X) \text{ com } (x)_\infty = \alpha P_1\}$$

e o semigrupo de Weierstrass de um par de pontos (P_1, P_2) por

$$\mathcal{H}(P_1, P_2) = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0^2 \,|\, \exists x \in \mathbb{F}_q(X) \text{ com } (x)_\infty = \alpha_1 P_1 + \alpha_2 P_2\},$$

onde $\mathbb{N}_0$ é o conjunto dos inteiros não negativos.

*Definimos o conjunto das **lacunas de Weierstrass** para um ponto racional P_1 como*

$$\mathcal{G}(P_1) = \mathbb{N}_0 \backslash \mathcal{H}(P_1)$$

e o conjunto das lacunas de Weierstrass para um par de pontos (P_1, P_2),

$$\mathcal{G}(P_1, P_2) = \mathbb{N}_0^2 \backslash \mathcal{H}(P_1, P_2)$$

Note que pela proposição (2.2.6), para todo $n \in \mathbb{N}$ com $n \geq 2g$, $n \in \mathcal{H}(P_1)$.

Vamos usar o lema abaixo, de [3], para caracterizar os elementos de $\mathcal{H}(P_1, P_2)$.

Lema 4.1.3. *a) Para $(\alpha_1, \alpha_2) \in \mathbb{N}^2$ temos:*

$(\alpha_1, \alpha_2) \in \mathcal{H}(P_1, P_2) \Leftrightarrow \ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2) + 1 = \ell(\alpha_1 P_1 + (\alpha_2 - 1)P_2) + 1$

b) Seja $\alpha_1 \geq 1$. Então:

$\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2) + 1 \Leftrightarrow \exists \alpha,\ 0 \leq \alpha \leq \alpha_2$ *tal que* $(\alpha_1, \alpha) \in \mathcal{H}(P_1, P_2)$.

Observação 4.1.4. *Suponha que $(\alpha_1, \alpha_2) \in \mathcal{G}(P_1, P_2)$. Então pelo lema (4.1.3), $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$ ou $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell(\alpha_1 P_1 + (\alpha_2 - 1)P_2)$. Então, se $\alpha_1 \geq 1$ sem perda de generalidade podemos assumir $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$. Note que, pelo lema (4.1.3)(b), é isso que ocorre quando $(\alpha_1, \alpha) \in \mathcal{G}(P_1, P_2)$ para todo α tal que $0 \leq \alpha \leq \alpha_2$ (pois não existe α entre 0 e α_2 tal que $(\alpha_1, \alpha) \in \mathcal{H}(P_1, P_2)$). Esta é uma primeira forma de caracterizar os elementos de $\mathcal{G}(P_1, P_2)$.*

4.2 Melhoramento de Matthews para curvas quaisquer

Este teorema, feito por Matthews, que de certa forma generaliza um resultado de Garcia, Kim e Lax [1], é válido para curvas arbitrárias e usa que uma sequência específica de pares

são elementos de $\mathcal{G}(P_1, P_2)$. Mais adiante veremos que se soubermos, explicitamente, quem é $\mathcal{G}(P_1, P_2)$ a cota encontrada neste teorema pode ser melhorada, mas sobre uma curva específica.

Teorema 4.2.1. *Suponha que*

i) $(\alpha_1, \alpha_2) \in \mathcal{G}(P_1, P_2)$ *com* $\alpha_1 \geq 1$ *e* $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$*;*

ii) Existam γ_1, γ_2 *tais que* $(\gamma_1, \gamma_2 - t - 1) \in \mathcal{G}(P_1, P_2)$ *para todo* $t,\ 0 \leq t \leq\ min\{\gamma_2 - 1, 2g - 1 - (\alpha_1 + \alpha_2)\}$*;*

iii) $G = (\alpha_1 + \gamma_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_2$ *e* $D = Q_1 + Q_2 + \cdots + Q_n$*, onde os* Q_i *são pontos racionais distintos, não pertencentes ao suporte de G.*

Se a dimensão de $C_\Omega(D, G)$ *é positiva, então a distância mínima desse código é pelo menos deg* $G - 2g + 3$*.*

Demonstração. Vamos demonstrar por absurdo.

Faça $\omega = \deg G - 2g + 2$. Se existe uma palavra com peso ω,
então existe um diferencial $\eta \in \Omega(G - D)$ com exatamente ω pólos simples, $Q_1, Q_2, \cdots, Q_\omega$ já que, se $\eta_p(1) = 0$ então $v_P(\eta) \geq 0$, pelo lema (3.1.6). Daí

$$(\eta) \geq G - (Q_1 + Q_2 + \cdots + Q_\omega).$$

E como (η) é divisor canônico, segue que

$$\deg(\eta) = 2g - 2 = \deg G - (Q_1 + Q_2 + \cdots + Q_\omega) \text{ daí,}$$

$$(\eta) = G - (Q_1 + Q_2 + \cdots + Q_\omega).$$

Como $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$ então, pelo teorema de Riemann-Roch, segue que

$$\ell(W - (\alpha_1 P_1 + \alpha_2 P_2)) + 1 = \ell(W - ((\alpha_1 - 1)P_1 + \alpha_2 P_2)).$$

Assim, existe $h \in L(W - (\alpha_1 - 1)P_1 + \alpha_2 P_2))\backslash L(W - ((\alpha_1 P_1 + \alpha_2 P_2))$, onde W é um divisor canônico qualquer.

Então,

$$(h) + W - ((\alpha_1 - 1)P_1 + \alpha_2 P_2) \geq 0$$

$$(h) \geq (\alpha_1 - 1)P_1 + \alpha_2 P_2 - W, \quad \text{e portanto}$$

$$(h) = (\alpha_1 - 1)P_1 + \alpha_2 P_2 - W + E$$

onde E é uma divisor efetivo cujo suporte não contém P_1 e tal que deg $E = 2g-1-(\alpha_1+\alpha_2)$ (para que o grau de (h), que é um divisor principal, seja 0).

Repetindo a idéia, escrevamos $E = E' + tP_2$ onde E' é um divisor efetivo cujo suporte não contém P_2 (note que $0 \leq t \leq 2g-1-(\alpha_1+\alpha_2)$, pois não pode ultrapassar o deg E).

Assim

$$(h) = (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 - W + E'.$$

Agora, como quaisquer dois divisores canônicos são equivalentes, segue que $(\eta) \sim W$, e assim temos

$$G - (Q_1 + Q_2 + \cdots + Q_\omega) = (\eta) \sim W \sim (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 + E',$$

e logo

$$G - (Q_1 + Q_2 + \cdots + Q_\omega) \sim (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 + E'$$

Assim, da definição de equivalência temos que existe f função racional tal que (usando que $G = (\alpha_1 + \gamma_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_2$),

$$(f) = -\gamma_1 P_1 - (\gamma_2 - t - 1)P_2 + (Q_1 + Q_2 + \cdots + Q_\omega) + E'.$$

Se $t \leq \gamma_2 - 1$, então f tem pólo divisor $(f)_\infty = \gamma_1 P_1 + (\gamma_2 - t - 1)P_2$ o que contradiz o fato de $(\gamma_1, \gamma_2 - t - 1) \in \mathcal{G}(P_1, P_2)$.

Caso contrário, então $(f)_\infty = \gamma_1 P_1$ o que contraria o fato de γ_1 ser uma lacuna em P_1. Observe que γ_1 é uma lacuna em P_1 porque, se $\gamma_2 - 1 < 2g - 1 - (\alpha_1 + \alpha_2)$ então t assume $\gamma_2 - 1$ e daí $(\gamma_1, 0) \in \mathcal{G}(P_1, P_2)$. □

4.3 Explicitando $\mathcal{G}(P_1, P_2)$ numa curva Hermitiana

Agora, vamos ver alguns resultados de Kim [3] (também pode ser visto em [4]) que serão muito úteis para obter os elementos de $G(P_1, P_2)$.

Lema 4.3.1. *Se* $(\alpha_1, \alpha_2), (\alpha_1', \alpha_2') \in \mathcal{H}(P_1, P_2)$ *então* $(\overline{\alpha_1}, \overline{\alpha_2}) \in \mathcal{H}(P_1, P_2)$ *com* $\overline{\alpha_1} := \max\{\alpha_1, \alpha_1'\}$ *e* $\overline{\alpha_2} := \max\{\alpha_2, \alpha_2'\}$.

Demonstração. Como $(\alpha_1, \alpha_2), (\alpha_1', \alpha_2') \in \mathcal{H}(P_1, P_2)$ segue que existem $f, g \in \mathbb{F}_q(X)$ tais que

$$(f)_\infty = \alpha_1 P_1 + \alpha_2 P_2 \quad \text{e} \quad (g)_\infty = \alpha_1' P_1 + \alpha_2' P_2.$$

E assim, $(f+g)_\infty = \overline{\alpha_1} P_1 + \overline{\alpha_2} P_2$ □

Definição 4.3.2. *Para uma lacuna α_1 em P_1, defina $\beta_{\alpha_1} = min\{\alpha_2 : (\alpha_1, \alpha_2) \in \mathcal{H}(P_1, P_2)\}$. Ou seja, para qualquer $\beta < \beta_{\alpha_1}$ temos $(\alpha_1, \beta) \in \mathcal{G}(P_1, P_2)$.*

O lema a seguir será enunciado sem demonstração, mas esta pode ser vista em [3] ou [4].

Lema 4.3.3. *Para uma lacuna α_1 em P_1, $\alpha_1 = min\{\alpha : (\alpha, \beta_{\alpha_1}) \in \mathcal{H}(P_1, P_2)\}$. Além disso, $\{\beta_{\alpha_1} : \alpha_1 \in \mathcal{G}(P_1)\} = \mathcal{G}(P_2)$*

O lema (4.3.3), juntamente com a definição (4.3.2) nos diz, geometricamente, que no plano $\mathbb{N}_0 \times \mathbb{N}_0$, os segmentos de reta formados por $(\alpha_1, y < \beta_{\alpha_1})$ e $(x < \alpha_1, \beta_{\alpha_1})$ só possuem lacunas do par (P_1, P_2), conforme indica a figura 4.1. Este resultado é fundamental para entendermos a construção de $\mathcal{G}(P_1, P_2)$.

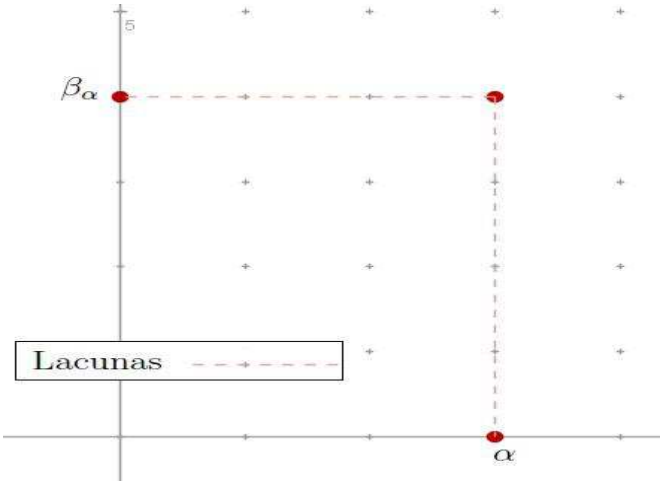

Figura 4.1: Os tracejados são lacunas de $\mathcal{G}(P_1)$ (horizontal) e $\mathcal{G}(P_2)$ (vertical).

Vamos agora determinar o conjunto das lacunas de Weierstrass de um par de pontos de Weierstrass numa curva Hermitiana, $Y^q + Y = X^{q+1}$. E como vamos trabalhar sobre curvas Hermitianas, vamos assumir o seguinte resultado a respeito dessas curvas (uma demonstração completa pode ser encontrada na seção 6.4 de [6]):

Teorema 4.3.4. *Considere o corpo de funções Hermitiano sobre $\mathbb{F}_{q^2}$ definido por*

$$\mathbb{F}_{q^2}(X, Y) \quad com \quad Y^q + Y = X^{q+1}$$

Ele possui as seguintes propriedades:

(a) O gênero de $\mathbb{F}_{q^2}(X, Y)$ é $g = q(q-1)/2$

(b) $\mathbb{F}_{q^2}(X,Y)$ *tem* q^3+1 *lugares de grau 1 sobre* $\mathbb{F}_{q^2}$*, e são eles*

1. P_∞*, o pólo comum de* x *e* y *e*
2. $P_{\alpha,\beta}$ *onde, para cada* $\alpha \in \mathbb{F}_{q^2}$ *existem* q *elementos* $\beta \in \mathbb{F}_{q^2}$ *tais que* $\beta^q+\beta=\alpha^{q+1}$*.*

(c) Para $r \geq 0$*, os elementos* x^iy^j *com* $0 \leq i,\ \ 0 \leq j \leq q-1$ *e* $iq+j(q+1) \leq r$ *formam uma base para* $L(rP_\infty)$*.*

(d) Os divisores de x *e* y *são dados por*

$$(x) = \sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta} - qP_\infty \quad \text{e} \quad (y) = (q+1)(P_{\alpha,\beta} - P_\infty)$$

Note que o item (a) desse teorema segue de definição de gênero, usando o fato da curva Hermitiana ser não singular e seu grau ser $q+1$. O item (b) foi mostrado em (2.4.4).

O teorema a seguir possibilitará o melhoramento do teorema (4.2.1) para o caso de códigos sobre curvas Hermitianas. O (4.3.5), juntamente com o teorema (4.3.6) são o centro do artigo de Matthews [5].

Teorema 4.3.5. *Para quaisquer dois pontos de Weierstrass* P_1 *e* P_2 *na curva Hermitiana* $y^q+y=x^{q+1}$ *sobre* $\mathbb{F}_{q^2}$ *temos que* $(t-j)(q+1)+j$ *é lacuna e*

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

para $1 \leq j \leq t \leq q-1$

Demonstração. Seja $P_1 = P_{0,0}$ e $P_2 = P_\infty$ e lembramos que os divisores de x e y são dados por:

$$(x) = \sum_{\beta^q+\beta=0} P_{0,\beta} - qP_\infty \quad \text{e} \quad (y) = (q+1)(P_{0,0} - P_\infty).$$

Sabendo que uma base para $\ell(mP_2)$ é $\{x^iy^j \,|\, 0 \leq i, 0 \leq j \leq q-1$ com $iq+j(q+1) \leq m\}$ e que as lacunas de P_1 são exatamente os $m's$ para os quais $\ell(mP_2) = \ell((m-1)P_2)$, obtemos que o conjunto das lacunas de Weierstrass é dado por $\{aq+b \,|\, 0 \leq a < b \leq q-1\}$. Explicitamente, todos os elementos de $\mathcal{G}(P_2)$ estão listados abaixo (e $\mathcal{G}(P_1)$ também pois o conjunto das lacunas independe do lugar escolhido).

$$\begin{array}{cccccc} 1 & & 2 & \cdots & q-2 & q-1 \\ (q+1)+1 & & (q+1)+2 & \cdots & (q+1)+(q-2) & \\ \vdots & & \vdots & & \iddots & \\ (q-3)(q+1)+1 & (q-3)(q+1)+2 & & & & \\ (q-2)(q+1)+1 & & & & & \end{array} \tag{4.1}$$

Considere as diagonais de (4.1) começando de baixo para cima, da esquerda para direita, (isto é, na direção $\nearrow$). Numere essas diagonais de 1 a $q-1$ começando do canto superior esquerdo, no caso, do 1. Enumere as colunas (resp. as linhas) de (4.1) da esquerda para direita (resp. de cima para baixo) começando com 1. Então para um t fixo, $1 \leq j \leq t \leq q-1$, os elementos de (4.1) podem ser descritos como $(t-j)(q+1)+j$ onde esse número está na t-ésima diagonal e na j-ésima coluna.

Para $1 \leq j \leq t \leq q-1$,

$$\left(\frac{x^{q-j+1}}{y^{t-j+1}}\right)_\infty = ((t-j)(q+1)+j)P_1 + ((q-t-1)(q+1)+j)P_2 \tag{4.2}$$

Assim, tomando $\alpha = (t-j)(q+1)+j$ queremos mostrar que $\beta_\alpha = (q-t-1)(q+1)+j$. Inicialmente, tome $t = q-1$ e $1 \leq j \leq q-1$. Isso nos dá $((q-1-j)(q+1)+j, j) \in \mathcal{H}(P_1, P_2)$ para $1 \leq j \leq q-1$. Daí, $\beta_{(q-1-j)(q+1)+j} = j$, para $1 \leq j \leq q-1$, pois, pela observação (**??**) segue que se diminuirmos a ordem de P_2 obteremos uma lacuna.

Isso nos dá os β_α para todas as lacunas de P_1 na $(q-1)$-ésima diagonal em (4.1) (Para cada j estamos numa nova coluna e portanto, num novo elemento da diagonal).

Agora faça $t = q-2$ e $1 \leq j \leq q-2$. Assim $((q-2-j)(q+1)+j, (q+1)+j) \in \mathcal{H}(P_1, P_2)$ para $1 \leq j \leq q-2$, o que, conforme vimos acima, nos diz que $\beta_{(q-2-j)(q+1)+j} = (q+1)+j$ e nos dá todos os β_α para as lacunas $\alpha \in G(P_1)$ na $(q-2)$-ésima diagonal.

Continuando dessa maneira, quando $t = q-i$ e $1 \leq j \leq q-i$ teremos $\beta_{(q-i-j)(q+1)} = (i-1)(q+1)+j$ para $1 \leq j \leq q-i$, o que nos dá todos os β_α para todas as lacunas α em P_1 na $(q-i)$-ésima diagonal.

Finalmente, quando $t = j = 1$ temos $\beta_1 = (q-2)(q+1)+1 = q^2-q-1 = 2g-1$. E assim o teorema é válido para $P_1 = P_{0,0}$ e $P_2 = P_\infty$ (Note que usamos fortemente este fato para construir uma função racional como em (4.2) tal que $(f) = ((t-j)(q+1)+j)P_1 + ((q-t-1)(q+1)+j)P_2$ e logo $((t-j)(q+1)+j, (q-t-1)(q+1)+j) \in \mathcal{H}(P_1, P_2)$). Nosso próximo passo é generalizar essa idéia.

Suponha que $P_1 = P_{a,b}$ e $P_2 = P_\infty$ com $(a,b) \neq (0,0)$. Então, segue de [10] que existe um automorfismo φ que fixa P_∞ e leva $P_{a,b}$ em $P_{0,0}$. Então, podemos voltar na demonstração acima e usar a função racional $\frac{x^{q-j+1}}{y^{t-j+1}} \circ \varphi$ e o restante segue como antes.

Agora, suponha que $P_1 = P_{a,b}$ e $P_2 = P_{c,d}$ com $(a,b) \neq (c,d)$. Então, por [10] existe um automorfismo que deixa $P_{a,b}$ fixado e leva $P_{c,d}$ em P_∞. Na verdade, esse automorfismo é uma composição de dois outros, $\varphi_1 \circ \varphi_2$ onde φ_2 leva $P_{c,d}$ em P_∞ e φ_1 um automorfismo que leva $\varphi_2(P_{a,b})$ em $P_{a,b}$ e deixa P_∞ fixado. Dessa forma, recaímos no caso acima, onde temos $P_1 = P_{a,b}$ e $P_2 = P_\infty$. E assim, vemos que é possível obter uma função racional que gere os β_α, o que prova o teorema. □

Agora vamos interpretar o Teorema (4.3.5), voltando para (4.1), reescrevendo-o de forma que a entrada da j-ésima coluna na linha i da tabela (4.1) seja a entrada da j-ésima coluna na $(q-i)$-ésima diagonal de (4.3).

$$\begin{array}{cccccc}
(q-2)(q+1)+1 & (q-3)(q+1)+2 & \cdots & (q+1)+(q-2) & q-1 \\
(q-3)(q+1)+1 & (q-4)(q+1)+2 & \cdots & q-2 & \\
\vdots & \vdots & \iddots & & \\
(q+1)+1 & 2 & & & \\
1 & & & &
\end{array} \tag{4.3}$$

Note que a $(q-i)$-ésima diagonal de (4.3) é a i-ésima linha de (4.1). Agora, abaixo de cada lacuna de $\mathcal{G}(P_1)$ queremos colocar β_α. Para isso vamos escrever a linha i de (4.1) (em vermelho) imediatamente acima da i-ésima linha de (4.3).

$$\begin{array}{cccccc}
1 & 2 & \cdots & q-2 & q-1 \\
(q-2)(q+1)+1 & (q-3)(q+1)+2 & \cdots & (q+1)+(q-2) & q-1 \\
\\
(q+1)+1 & (q+1)+2 & \cdots & (q+1)+(q-2) & \\
(q-3)(q+1)+1 & (q-4)(q+1)+2 & \cdots & q-2 & \\
\vdots & \vdots & \iddots & & \\
(q-3)(q+1)+1 & (q-3)(q+1)+2 & & & \\
(q+1)+1 & 2 & & & \\
\\
(q-2)(q+1)+1 & & & & \\
1 & & & &
\end{array} \tag{4.4}$$

Assim, se α está na t-ésima diagonal na j-ésima coluna de (4.1), isto é, $\alpha = (t - j)(q + 1) + j$ então β_α é o número em (4.1) na $(q - t + j - 1)$-ésima diagonal na j-ésima coluna. Note que essa construção faz sentido pela observação (**??**).

Com o teorema (4.3.5) vamos descrever todo o $\mathcal{G}(P_1, P_2)$. Nesse intuito, note primeiramente que, sendo $S = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0 \,|\, \alpha_1 + \alpha_2 \leq 2g - 1\}$ temos $\mathcal{G}(P_1, P_2) \subseteq S$. De fato, seja $(\alpha_1, \alpha_2) \in \mathcal{G}(P_1, P_2)$. Daí, pelo lema (4.1.3), temos $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1)P_1 + \alpha_2 P_2)$. Pelo teorema de Riemann-Roch isso significa que, para W um divisor canônico qualquer,

$$\ell(W - (\alpha_1 P_1 + \alpha_2 P_2)) + 1 = \ell(W - ((\alpha_1 - 1)P_1 + \alpha_2 P_2)). \tag{4.5}$$

Mas se $\alpha_1 + \alpha_2 \geq 2g$ segue que deg $(\alpha_1 P_1 + \alpha_2 P_2) = \alpha_1 + \alpha_2 \geq 2g$, logo segue de (1.3.12) que $\ell(W - (\alpha_1 P_1 + \alpha_2 P_2)) = 0$. E da mesma forma, como deg $((\alpha_1 - 1)P_1 + \alpha_2 P_2) = \alpha_1 + \alpha_2 - 1 \geq 2g - 1$ e também por (1.3.12), $\ell(W - ((\alpha_1 - 1)P_1 + \alpha_2 P_2)) = 0$. Assim , de (4.5) segue que $1 = 0$. Absurdo. Logo $\mathcal{G}(P_1, P_2) \subseteq S$.

A seguir usaremos a notação de intervalo $[a, b]$ para denotar $\{c \in \mathbb{N}_0 : a \leq c \leq b\}$ e $[a, b] \times [c, d]$ significando $\{(i, j) \in \mathbb{N}_0^2 : a \leq i \leq b, c \leq j \leq d\}$

Nosso objetivo agora é definir uma série de blocos de pontos de $\mathcal{H}(P_1, P_2)$ de forma que quando olharmos para $\mathbb{N}_0^2 \cap S$ os elementos que não estiverem nesses blocos sejam exatamente os pontos de $\mathcal{G}(P_1, P_2)$. Para garantir que esses pontos estão mesmo em $\mathcal{G}(P_1, P_2)$ usaremos o lema (4.3.3).

Comecemos com $q-1 \in \mathcal{G}(P_1)$. Pelo teorema (4.3.5), $\beta_{q-1} = q-1$. Como $(0, q), (0, q+1) \in \mathcal{H}(P_1, P_2)$ (basta olhar a tabela (4.1) das lacunas), podemos usar o lema (4.3.1) para obter $(q - 1, q), (q - 1, q + 1) \in \mathcal{H}(P_1, P_2)$. Da mesma forma $(q, 0), (q + 1, 0) \in \mathcal{H}(P_1, P_2)$, logo $(q, q-1), (q+1, q-1)$. Outra aplicação do lema (4.3.1) nos diz que $(q, q), (q, q+1), (q+1, q), (q+1, q+1) \in \mathcal{H}(P_1, P_2)$. Isso nos dá um bloco $B_{q-1} = [q - 1, q + 1] \times [q - 1, q + 1] \subseteq \mathcal{H}(P_1, P_2)$.

Agora para $q - 2 \in \mathcal{G}(P_1)$. Note que $\beta_{q-2} = 2q - 1$. Agora, usando que $B_{q-1} \subseteq \mathcal{H}(P_1, P_2)$ e $(q - 2, 2q - 1), (0, 2q), (0, 2q + 1), (0, 2q + 2) \in \mathcal{H}(P_1, P_2)$, aplicando o lema (4.3.1) obtemos o bloco $B_{q-2} = [q - 2, q + 1] \times [2q - 1, 2q + 2] \subseteq \mathcal{H}(P_1, P_2)$, um bloco de tamanho 4×4, de elementos de $\mathcal{H}(P_1, P_2)$.

Continuamos dessa maneira, sempre usando que o bloco anterior está em $\mathcal{H}(P_1, P_2)$ e que os pontos que não aparecem em $\mathcal{G}(P_1)$ estão em $\mathcal{H}(P_1)$. Daí obtemos, para cada lacuna $\alpha = q - i, 1 \leq i \leq q - 3$ de P_1, um bloco B_α com $(i + 2) \times (i + 2)$ elementos de $\mathcal{H}(P_1, P_2)$.

Agora considere $2 \in \mathcal{G}(P_1)$. Do teorema (4.3.5), $\beta_2 = q^2 - 2q - 1$. Aplicando o lema (4.3.1), usando que $B_3 \subseteq \mathcal{H}(P_1, P_2)$, obtemos um bloco de dimensões $((q-2)+2) \times ((q-2)+2)$, isto é

$q \times q$. Mas como estamos interessados só na interseção de $\mathcal{H}(P_1, P_2)$ com S, esse quadrado se restringe a um triângulo, com $\frac{q(q-1)}{2}$ (esse valor vem da soma dos q primeiros valores de 1 a $q-1$, que são os elementos do quadrado que estão em S). Logo, B_2 é um triângulo com $\frac{q(q-1)}{2}$. Como $\beta_1 = 2g-1$ e $(1, 2g-1) \notin S$, não precisamos considerar β_1.

Podemos continuar nesse processo, tomando os β_α para cada α que não esteja na primeira coluna (pois nessa coluna a soma das coordenadas é 2g, logo não estão em S). Para $\alpha = (t-j)(q+1)+j \in \mathcal{G}(P_1)$, $3 \leq j \leq t \leq q-1$ teremos um bloco $B_\alpha \subseteq S$ de elementos do semigrupo de Weierstrass do par (P_1, P_2). Para os α na segunda coluna $(j = 2)$, $\alpha = (t-2)(q+1)-2 \in \mathcal{G}(P_1)$ com $2 \leq t \leq q-1$ obtemos um triângulo $B_\alpha \subseteq S$ com $\frac{q(q-1)}{2}$ elementos de $\mathcal{H}(P_1, P_2)$. Então, pela definição de β_α e pelo lema (4.3.3), todos os elementos de $S \cap \mathbb{N}_0^2$ que não estão em B_α para algum $\alpha \in \mathcal{G}(P_1)$ são elementos de $\mathcal{G}(P_1, P_2)$. E são todos, pois esses blocos cobrem todas as não lacunas de S. Esses fatos podem ser reunidos no seguinte teorema.

Teorema 4.3.6. *Sejam P_1 e P_2 dois pontos distintos de Weierstrass na curva Hermitiana $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$. Então o conjunto das lacunas de Weierstrass do par (P_1, P_2) é*

$$\mathcal{G}(P_1, P_2) = S \backslash \mathbb{H} \cup \mathbb{B}_\alpha,$$

onde $S = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0 \mid \alpha_1 + \alpha_2 \leq 2g-1\}$,
$\mathbb{H} = \{(H(P_1) \times \{0\}) \cup (H(P_2) \times \{0\})$ *e*
$\mathbb{B}_\alpha = \{B_\alpha \mid \alpha = (t-j)(q+1)+j,\ 2 \leq j \leq t \leq q-1\}$*, onde os B_α foram definidos acima.*

Observação 4.3.7. *Note que o cálculo feito para obter β_α é independente da escolha dos pontos de Weierstrass P_1, P_2, e então o conjunto $\mathcal{G}(P_1, P_2)$ também independe dos pontos escolhidos.*

Esse teorema ficará mais claro neste exemplo, apresentado por Mathews em [5].

Exemplo 4.3.8. *Considere a curva $y^8 + y = x^9$ sobre $\mathbb{F}_{64}$. Seja $P_1 = P_{0,0}$ e $P_2 = P_\infty$. Usando o teorema (4.3.5) podemos determinar todas as lacunas α em P_1 e assim, como em (4.4), escrever os respectivos β_α diretamente abaixo de sua lacuna (na cor vermelha).*

$$
\begin{array}{ccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
55 & 47 & 39 & 31 & 23 & 15 & 7 \\
10 & 11 & 12 & 13 & 14 & 15 & \\
46 & 38 & 30 & 22 & 14 & 6 & \\
19 & 20 & 21 & 22 & 23 & & \\
37 & 29 & 21 & 13 & 5 & & \\
28 & 29 & 30 & 31 & & & \\
28 & 20 & 12 & 4 & & & \\
37 & 38 & 39 & & & & \\
19 & 11 & 3 & & & & \\
46 & 47 & & & & & \\
10 & 2 & & & & & \\
55 & & & & & & \\
1 & & & & & &
\end{array}
\tag{4.6}
$$

Vamos obter os blocos e "triângulos"B_α para os elementos da primeira linha de (4.6): Começando com $\alpha = 7$. Note que $\beta_7 = 7$ e que $(0,8), (0,9), (8,0), (9,0) \in \mathcal{H}(P_1, P_2)$ (pois não são lacunas nem de P_1 nem de P_2, conforme (4.6)). Usando (4.3.1) repetidas vezes com esses pontos obtemos:

$$
\begin{array}{ccc}
(7,9) & (8,9) & (9,9) \\
(7,8) & (8,8) & (9,8) \\
(7,7) & (8,7) & (9,7)
\end{array}
\tag{4.7}
$$

Daí, $B_7 = [7,9] \times [7,9]$.

Agora para $\alpha = 6$, temos $\beta_6 = 15$, $B_7 \subseteq \mathcal{H}(P_1, P_2)$ e $(0,16), (0,17), (0,18) \in \mathcal{H}(P_1, P_2)$. Logo, usando (4.3.1) com os pontos de B_7 e com $(6,15) \in \mathcal{H}(P_1, P_2)$, temos:

$$
\begin{array}{cccc}
(6,18) & (7,18) & (8,18) & (9,18) \\
(6,17) & (7,17) & (8,17) & (9,17) \\
(6,16) & (7,16) & (8,16) & (9,16) \\
(6,15) & (7,15) & (8,15) & (9,15)
\end{array}
\tag{4.8}
$$

Assim $B_6 = [6,9] \times [15,18]$.

De um modo geral, para elementos na primeira linha temos

$$B_{q-i} = [q-i, q+1] \times [\beta_{q-i}, \beta_{q-i} + i + 1], \text{ onde é a lacuna } \alpha = (q-i)$$

Desse modo: $B_5 = [5,9] \times [23,27]$, $B_4 = [4,9] \times [31,36]$, $B_3 = [3,9] \times [39,45]$ e B_2 é o triângulo com vértices em $(2,47), (2,53)$ e $(8,47)$ (esses vértices são obtidos somando-se $q-2$ a cada coordenada para termos um triângulo de área $\frac{q(q-1)}{2}$).

Agora para a segunda linha, iniciemos com $\alpha = 15$. Daí, $\beta_{15} = 6$. Usando que $(16,0), (17,0), (18,0) \in \mathcal{H}(P_1, P_2)$ e que $B_7 \subseteq \mathcal{H}(P_1, P_2)$ obtemos $B_{15} = [15,18] \times [6,9]$. Note que ele é o simétrico de B_6, bastando inverter os eixos.

Para $\alpha = 14$, temos $\beta_{14} = 14$ e usando que $B_{15}, B_6 \subseteq \mathcal{H}(P_1, P_2)$ temos $B_{14} = [14,18] \times [14,18]$.

De um modo geral, na segunda linha obtemos:

$$B_{(q+1)+q-i} = [(q+1)+q-i, (q+1)+q-i+i+1] \times [\beta_{(q+1)+q-i}, \beta_{(q+1)+q-i} + i + 1]$$

Assim, $B_{13} = [13,18] \times [22,27]$, $B_{12} = [12,18] \times [30,36]$, e B_{11} é o triângulo com vértices em $(11,38), (11,44), (17,38)$.

Seguindo essa idéia nas próximas linhas obtemos $B_{21} = [21,27] \times [21,27]$ e B_{20} é igual ao triângulo cujos vértices são $(20,29), (26,29), (20,35)$. Note que por simetria podemos determinar $B_{23}, B_{31}, B_{39}, B_{47}, B_{22}, B_{30}, B_{38}$ e B_{29}. Veja a ilustração a 4.2.

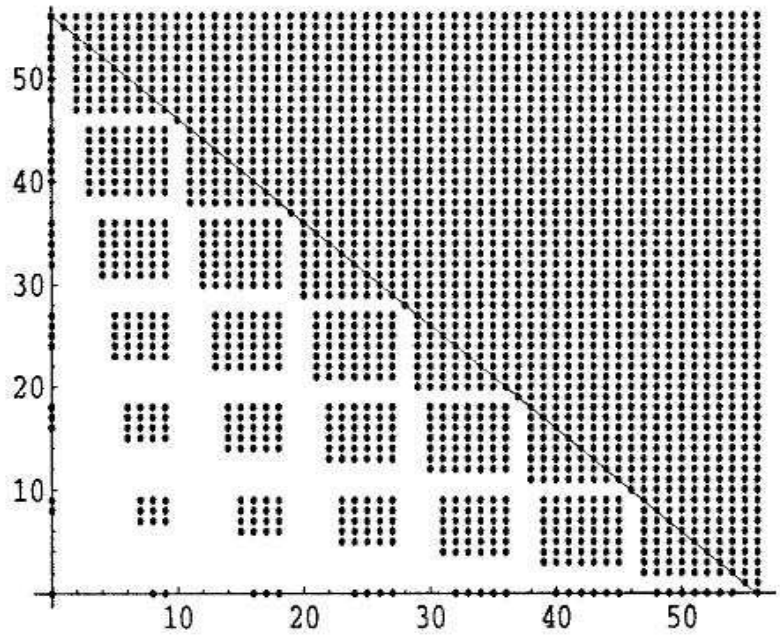

Figura 4.2: Os pontos marcados são $\mathcal{H}(P_1, P_2)$ e os espaços em branco são $\mathcal{G}(P_1, P_2)$. Figura de Matthews [5]

4.4 Melhoramento da cota sobre curvas Hermitianas

Usando o teorema (4.3.5) e as consequências que ele acarreta, podemos melhorar ainda mais a cota do teorema (4.2.1). Nesta seção, χ denota a curva Hermitiana $Y^q + Y = X^{q+1}$ sobre $\mathbb{F}_{q^2}$. Da seção anterior, lembramos que o conjunto das lacunas de Weierstrass de um par de pontos independe da escolha desses pontos.

Teorema 4.4.1. *Considere* $C_\Omega(D,G)$ *em* χ *com* $G = (\alpha_1+\gamma_1-1)P_1+(\alpha_2+\gamma_2-1)P_2$ *e* $D = Q_1+Q_2+\cdots+Q_n$ *onde* $P_1,P_2,Q_1,\cdots,Q_n$ *são pontos racionais distintos de* $\mathbb{F}_{q^2}$.

Suponha que:

i) $(\alpha_1,\alpha_2)\in\mathcal{G}(P_1,P_2), \alpha_1\geq 1$ *e* $\ell(\alpha_1P_1+\alpha_2P_2) = \ell((\alpha_1-1)P_1+\alpha_2P_2)$*;*

ii) $(\gamma_1,\gamma_2-t-1),(\gamma_1+1,\gamma_2-t-1),(\gamma_1+q,\gamma_2-t-1),(\gamma_1,\gamma_2)\in\mathcal{G}(P_1,P_2)$ *para todo* t*,* $0\leq t\leq$ *min*$\{\gamma_2-1, 2g-1-(\alpha_1+\alpha_2)\}$

Se a dimensão do código é positiva, então a distância mínima é pelo menos deg $G-2g+4$*.*

Demonstração. Assuma, inicialmente, $P_1 = P_\infty$. Como aqui valem as hipóteses de (4.2.1), segue que a distância mínima de $C_\Omega(D,G)$ é pelo menos deg $G-2g+3$. Faça $\omega = \deg G - 2g+3$. Se existe uma palavra de peso ω, então existe um diferencial $\eta\in\Omega(G-D)$ com exatamente ω pólos simples, $Q_1+Q_2+\cdots+Q_\omega$. Temos $(\eta)\geq G-(Q_1+Q_2+\cdots+Q_\omega)$, logo $2g-2 = \deg(\eta) = \deg G-\omega+1$ e assim

$$(\eta) = G-(Q_1+Q_2+\cdots+Q_\omega)+A,$$

onde A é um ponto racional de $\mathbb{F}_{q^2}$, $A\neq Q_i$, para $1\leq i\leq\omega$ (só para completar o grau). Como $\ell(\alpha_1P_1+\alpha_2P_2) = \ell((\alpha_1-1)P_1+\alpha_2P_2)$, então pelo teorema de Riemann-Roch existe uma função racional $h\in\mathbb{F}_{q^2}(\chi)$ com divisor

$$(h) = (\alpha_1-1)P_1+(\alpha_2+t)P_2-W+E,$$

onde E é um divisor efetivo cujo suporte não contém P_1 e P_2 e $0\leq t\leq 2g-1-(\alpha_1+\alpha_2)$ (vide demonstração do teorema (4.2.1)). Então

$$G-(Q_1+Q_2+\cdots+Q_\omega)+A = (\eta)\sim W\sim(\alpha_1-1)P_1+(\alpha_2+t)P_2+E$$

implica que existe uma função racional $f\in\mathbb{F}_{q^2}(\chi)$ com divisor

$$(f) = -\gamma_1P_1-(\gamma_2-t-1)P_2-A+(Q_1+Q_2+\cdots+Q_\omega)+E$$

Primeiramente, assuma $t<\gamma_2-1$. Se A está no suporte de E, então A não é pólo de f, logo

$$(f)_\infty = \gamma_1P_1+(\gamma_2-t-1)P_2\ \ \therefore(\gamma_1,\gamma_2-t-1)\in\mathcal{H}(P_1,P_2).$$

O que não ocorre, por hipótese.

Se $A = P_1$, então $(f)_\infty = (\gamma_1+1)P_1+(\gamma_2-t-1)P_2$ e logo $(\gamma_1+1, \gamma_2-t-1) \in \mathcal{H}(P_1, P_2)$, o que não ocorre por hipótese.

Se $A = P_2$, então $(f)_\infty = \gamma_1 P_1+(\gamma_2-t)P_2$ e logo $(\gamma_1, \gamma_2-t) \in \mathcal{H}(P_1, P_2)$, o que não ocorre pois nesse caso, para $t = 0$ teríamos $(\gamma_1, \gamma_2) \in \mathcal{H}(P_1, P_2)$ e por hipótese, $(\gamma_1, \gamma_2) \in \mathcal{G}(P_1, P_2)$.

Só resta então $A = Q_j$, onde $j = \omega+1, \cdots, n$, pois estes são todos os pontos racionais de $\mathbb{F}_{q^2}(\chi)$. Seja $\tilde{f}$ uma função racional em χ com divisor $(\tilde{f}) = (q+1)Q_j - (q+1)P_1$ (Note que podemos encontrar tal $\tilde{f}$ pois $q+1$ é uma não lacuna de P_1). Daí, $(f\tilde{f})_\infty = (\gamma_1+q+1)P_1+(\gamma_2-t-1)P_2$ e isso implica que $(\gamma_1+q+1, \gamma_2-t-1) \in \mathcal{H}(P_1, P_2)$ o que não ocorre por hipótese.

Agora suponha $\gamma_2 - 1 < t \leq 2g-1-(\alpha_1+\alpha_2)$. Observe que, nesse caso, t assume o valor $\gamma_2 - 1$, logo $(\gamma_1+q+1, 0), (\gamma_1, 0)$ e $(\gamma_1+1, 0) \in \mathcal{G}(P_1, P_2)$. Se A está no suporte de E ou $A = P_2$, temos $(f)_\infty = \gamma_1 P_1$. Se $A = P_1$ então $(f)_\infty = (\gamma_1+1)P_1$. Em ambos os casos obtemos uma contradição com o fato de $\gamma_1 \in \mathcal{G}(P_1)$ e $\gamma_1+1 \in \mathcal{G}(P_1)$. Portanto, só nos resta $A = Q_j$, para algum j , $j = \omega+1, \cdots, n$. Então $(f\tilde{f})_\infty = (\gamma_1+q+1)P_1$, contradizendo o fato de que γ_1+q+1 é uma lacuna de P_1. Isto conclui a demonstração para o caso $P_1 = P_\infty$.

Se $P_1 \neq P_\infty$, então existe um automorfismo φ de χ tal que $\varphi(P_1) = P_\infty$ (esse automorfismo é explicitado em [10]). Seja $P_2' = \varphi(P_2)$. Pode-se mostrar que P_2' é novamente um ponto racional de $\mathbb{F}_q$ e assim, como vimos que o conjunto das lacunas de Weierstrass independe dos pontos tomados, $G(P_1, P_2) = G(P_\infty, P_2')$ e daí a prova se reduz ao caso acima.

□

Vamos finalizar vendo um exemplo de um código $C_\Omega(D, G)$ onde a distância mínima é pelo menos $\deg G - 2g + 4$.

Exemplo 4.4.2. *Seja a curva Hermitiana $y^4+y = x^5$ de gênero $g = 6$ sobre $\mathbb{F}_{16}$, $P_1 = P_{0,0}$ e $P_2 = P_\infty$. Seja $(\alpha_1, \alpha_2) = (6, 5)$, $(\gamma_1, \gamma_2) = (3, 2)$ e $G = (\alpha_1+\gamma_1-1)P_1+(\alpha_2+\gamma_2-1)P_2 = 8P_1+6P_2$. Note que $(6, \alpha) \in \mathcal{G}(P_1, P_2)$ para todo $0 \leq \alpha \leq 5$. Vamos verificar as hipóteses de (4.4.1) (Note que $\gamma_2 - 1 = 1$ e $2g-1-(\alpha_1+\alpha_2) = 0$ e como $0 \leq t \leq 0$ segue que $t = 0$):*

i) $(\gamma_1, \gamma_2-1) = (3, 1) \in \mathcal{G}(P_1, P_2)$ *pela definição de* β_α*;*

ii) $(\gamma_1+1, \gamma_2-1) = (4, 1) \in \mathcal{G}(P_1, P_2)$ *pois para* $\beta_\alpha = 1$ *segue que* $\alpha = 11 = 2g-1$ *e* $4 < \alpha$ *e daí segue;*

iii) $(\gamma_1+q+1, \gamma_2-1) = (8, 1) \in \mathcal{G}(P_1, P_2)$ *pelo mesmo argumento do item anterior; ´*

iv) $\ell(\alpha_1 P_1+\alpha_2 P_2) = \ell((\alpha_1-1)P_1+\alpha_2 P_2)$ *pelo lema 1.1, pois* $(\alpha_1, \alpha_2) \in \mathcal{G}(P_1, P_2)$.

Daí estão satisfeitas as hipóteses de (4.4.1) e logo a distância mínima de $C_\Omega(D, G)$ *é pelo menos deg* $(G) - 2g + 4 = 6$.

A figura abaixo ilustra a forma como obtemos os elementos de $\mathcal{H}(P_1, P_2) \cap S$, *onde* S *é o conjunto dos inteiros não-negativos menores ou iguais a* $2g - 1$. *A reta* r *da figura é dada por* $x + y = 12$.

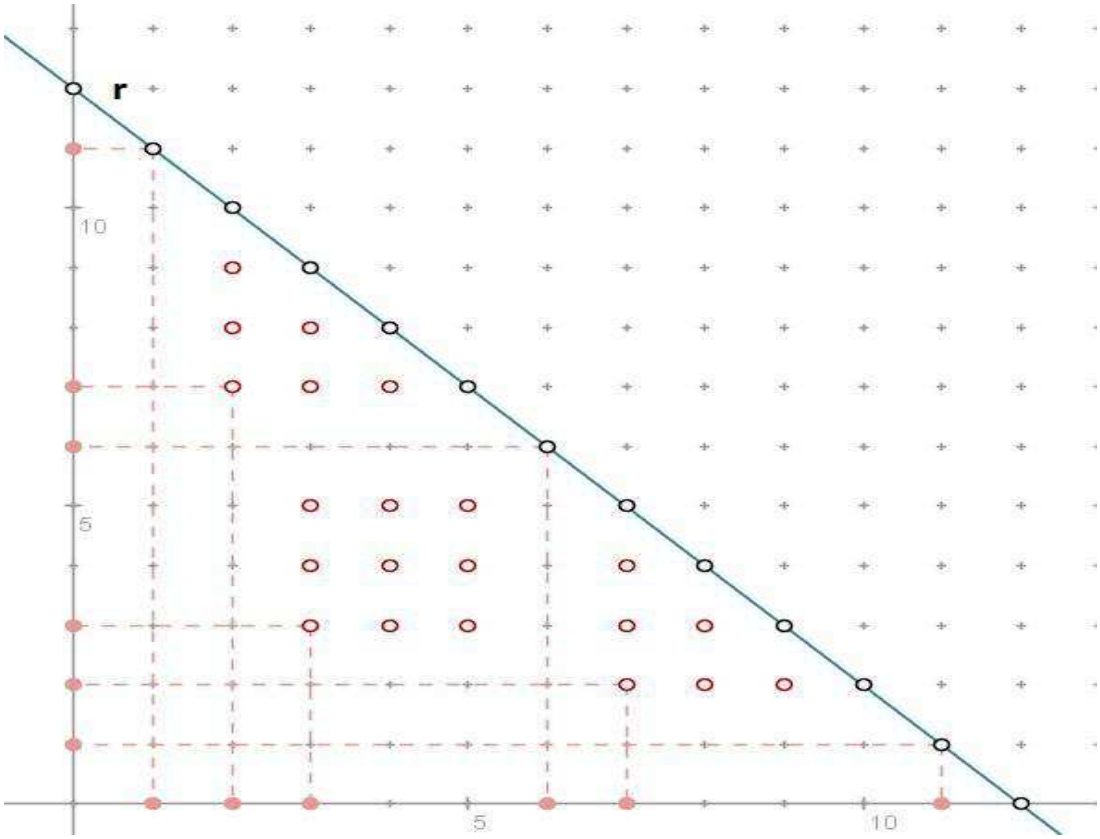

Figura 4.3: Os tracejados são $\mathcal{G}(P_1, P_2)$. Observe os blocos do teorema (4.3.6)

A

Corpo de Funções Racionais

A.1 Um exemplo de corpo de funções: o corpo de funções racionais

Para entendermos melhor os conceitos de valorização e lugares em um corpo de funções arbitrário, é muito útil estudarmos o caso mais simples: $F = K(x)$, onde x é transcendente sobre K. Dado um polinômio mônico irredutível $p(x) \in K[x]$, consideremos o anel de valorização

$$\vartheta_{p(x)} := \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], p(x) \not| g(x) \right\}, \tag{A.1}$$

de $K(x)/K$ com ideal maximal

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], p(x) | f(x), p(x) \not| g(x) \right\} \tag{A.2}$$

No caso particular onde $p(x)$ é linear, i.e., $p(x) = x - \alpha$ com $\alpha \in K$, abreviaremos a notação para

$$P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}. \tag{A.3}$$

Há também um outro anel de valorização:

$$\vartheta_\infty := \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], \text{deg } f(x) \leq \text{deg } g(x) \right\}, \tag{A.4}$$

com ideal maximal

$$P_\infty := \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], \text{deg } f(x) < \text{deg } g(x) \right\}. \tag{A.5}$$

Esse lugar é chamado o *lugar infinito (ou ponto no infinito)* de $K(x)$.

Proposição A.1.1. *Seja $F = K(x)$ o corpo de funções racionais.*

(a) Seja $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ o lugar definido como em (A.2), onde $p(x) \in K[x]$ é um polinômio irredutível. Então $p(x)$ é um elemento primo de P, e a correspondente valorização v_P pode ser descrita como segue: se $z \in K(x)\backslash\{0\}$ é escrito da forma $z = p(x)^n \cdot (f(x)/g(x))$, com $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. O corpo de resíduos $K(x)_P = \vartheta_P/P$ é isomorfo a $K[x]/(p(x))$; um isomorfismo é dado por

$$\phi : \begin{cases} K[x]/(p(x)) & \to \quad K(x)_P \\ f(x) \, mod \, P & \mapsto \quad f(x)(P) \end{cases}$$

Consequentemente, deg $P =$ deg $p(x)$.

(b) No caso particular $p(x) = x - \alpha$ com $\alpha \in K$, o grau de $P = P_\alpha$ é 1 e a aplicação classe residual é dada por

$$z(P) = z(\alpha) \quad \text{para } z \in K(x),$$

onde $z(\alpha)$ é definida como segue: escreva $z = f(x)/g(x)$ com $f(x), g(x) \in K[x]$ polinômios relativamente primos. Então:

$$z(\alpha) = \begin{cases} f(\alpha)/g(\alpha) & \text{se } g(\alpha) \neq 0; \\ \infty & \text{se } g(\alpha) = 0; \end{cases}$$

(c) Faça $P = P_\infty$ o lugar no infinito de $K(x)/K$ definido por (A.5). Então deg $P_\infty = 1$. Um elemento primo de P_∞ é $t = 1/x$. A valorização discreta v_∞ correspondente a esse lugar é dada por:

$$v_\infty(f(x)/g(x)) = \text{deg } g(x) - \text{deg } f(x),$$

onde $f(x), g(x) \in K[x]$. A aplicação classe residual correspondente a P_∞ é determinada por $z(P_\infty) = z(\infty)$ para $z \in K(x)$, onde $z(\infty)$ é definido como:

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0} \text{ com } a_n, b_m \neq 0,$$

então

$$z(\infty) = \begin{cases} a_n/b_m & \text{se } n = m \\ 0 & \text{se } n < m \\ \infty & \text{se } n > m \end{cases}$$

(d) K é todo o corpo de contantes do corpo de funções racionais $K(x)/K$.

Demonstração. (a) Seja $P = P_{p(x)}$, $p(x) \in K[x]$ irredutível. O ideal $P_{p(x)} \subseteq \vartheta_{p(x)}$ é gerado por $p(x)$ pois $p(x)$ é irredutível. Assim, $p(x)$ é um elemento primo de P.

Para mostrar a afirmação sobre o corpo resíduos, considere o isomorfismo:

$$\varphi : \begin{cases} K[x] & \to & K(x)_P \\ f(x) & \mapsto & f(x)(P) \end{cases}$$

Note que o núcleo de φ é $(p(x))$, i.e., o ideal gerado por $p(x)$. Além do mais, φ é sobrejetiva. De fato, se $z \in \vartheta_P$ então $z = u(x)/g(x)$ com $u(x), v(x) \in K[x]$, tal que $p(x) \not| v(x)$, isto é, mdc$(p(x), v(x)) = 1$. Assim, existem $a(x), b(x) \in K(x)$ tais que $a(x)p(x) + b(x)v(x) = 1$, portanto

$$z = 1 \cdot z = \frac{a(x)u(x)}{v(x)} p(x) + b(x)u(x)$$

e $z(P) = (b(x)u(x))(P)$ está na imagem de φ. Assim, φ induz um isomorfismo ϕ de $K[x]/(p(x))$ em $K(x)_P$. E assim, deg $P = [K(x)_P : K] = [K[x]/(p(x)) : K] =$ deg $p(x)$.

(b) Agora $P = P_\alpha$ com $\alpha \in K$. Se $f(x) \in K[x]$ então $(x - \alpha)|(f(x) - f(\alpha))$, daí $f(x)(P) = (f(x) - f(\alpha))(P) + f(\alpha)(P) = f(\alpha)$. Um elemento arbitrário $z \in \vartheta_P$ pode ser escrito como $z = f(x)/g(x)$ com $f(x), g(x) \in K[x]$ e $(x - \alpha) \not| g(x)$. Assim, $g(x)(P) = g(\alpha) \neq 0$ e

$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha).$$

(c) Vamos mostrar que $1/x$ é elemento primo de P_∞. Claramente $1/x \in P_\infty$, logo $(1/x)\vartheta_\infty \subseteq P_\infty$. Considere um elemento $z = f(x)/g(x) \in P_\infty$, i.e., deg $f <$ deg g. Então

$$z = \frac{1}{x} \cdot \frac{xf}{g}, \text{ com deg } (xf) \leq \text{deg } g.$$

Isso nos mostra que $z \in (1/x)\vartheta_\infty$ e assim, $P_\infty \subseteq (1/x)\vartheta_\infty$. Daí, $1/x$ gera o ideal P_∞, logo é um elemento primo de P_∞.

Note que deg $P_\infty = 1$ pois $1 \leq \deg(P_\infty) = [F_{P_\infty} : K] \leq [K(x) : K(x)] = 1$. Logo, $\deg(P_\infty) = 1$.

Agora vamos definir a valorização. Note que em ϑ_∞ as unidades são do tipo $f(x)/g(x)$ tal que deg $f =$ deg g. Daí, se $z \in K(x)$ então podemos escrever $z = (1/x)^m \dfrac{f(x)}{g(x)}$ onde deg $f =$ deg g. Daí, $v_\infty(z) = m$.

Para o corpo de resíduos, note que, se

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}$$

então para $n = m$ temos

$$z = \frac{a_n + \cdots + a_0/x^n}{b_m + \cdots + b_0/x^m} \ \therefore z(P) = \frac{a_n}{b_n}$$

pois $(1/x) \in P_\infty$; Para $n > m$ temos:

$$z = \frac{a_n + \cdots + a_0/x^n}{b_m/x^{n-m} + \cdots + b_0/x^n} \ \therefore z(P) = \infty.$$

E para $n < m$ temos:

$$z = \frac{a_n/x^{m-n} + \cdots + a_0/x^m}{b_m + \cdots + b_0/x^m} \ \therefore z(P) = 0.$$

(d) Tome um lugar P de $K(x)/K$ de grau 1 (por exemplo $P = P_\alpha$, com $\alpha \in K$). O corpo $\widetilde{K}$ das constantes de $K(x)$ está imerso no corpo de resíduos $K(x)_P$ e assim $K \subseteq \widetilde{K} \subseteq K(x)_P = K$, pois deg $P = [K(x)_P : K] = 1$.

□

Teorema A.1.2. *Não há outro tipo de lugares no corpo de funções racionais além de $P_{p(x)}$ e P_∞, definidos por (A.2) e por (A.5)*

Demonstração. :

Seja $K \subseteq \vartheta \subseteq K(x)$ um anel de valorização de $K(x)/K$. Queremos mostrar que $\vartheta = \vartheta_{p(x)}$ ou $\vartheta = \vartheta_\infty$. Suponha $\vartheta \neq \vartheta_\infty$.

Tome $x \in \vartheta$. Daí $K[x] \subseteq \vartheta$. Seja $P = \vartheta \backslash \vartheta^*$ e $I = K[x] \cap P$. Note que I é ideal (segue de P ser ideal) de $K[x]$ e na verdade é um ideal primo. De fato, se $f \cdot g \in I$ e $f \notin I$ então $f \notin P$ pois $f, g \in K[x]$, e assim $f \in \vartheta^*$. Logo, $g \in P$.

Note que, como $K[x] \subseteq \vartheta$ então $K[x]/P \subseteq \vartheta/P$. Agora faça :

$$\phi : \begin{cases} K[x] & \to & K[x]/P \\ g & \mapsto & g + P \end{cases}$$

Daí o núcleo de ϕ é dado pelos elementos de $K[x] \cap P = I$. E ϕ é claramente sobrejetora. Assim, temos que $K[x]/I \cong K[x]/P \subseteq \vartheta/P = K(x)_P$. Logo, $K[x]/I \hookrightarrow K(x)_P$. Mas como P é um lugar de grau 1, deg $P = [K(x)_P : K] = 1 \ \therefore K(x)_P = K$. Assim, $K[x]/I \hookrightarrow K$ e logo $I \neq \{0\}$.

Assim segue que existe um polinômio mônico irredutível unicamente determinado $p(x) \in K(x)$ tal que $I = K[x] \cap P = p(x) \cdot K[x]$ (Note que $p(x)$ é irredutível pois I é ideal primo).

Logo, todo $g(x) \in K[x]$ com $p(x) \nmid g(x)$ não está em I, logo $g(x) \notin P$, e assim $1/g(x) \in \vartheta$.

Dessa forma, todo elemento do tipo $\dfrac{f(x)}{g(x)}$ onde $f(x), g(x) \in K[x]$ estão em ϑ. Portanto, $\vartheta_{p(x)} \subseteq \vartheta$.

E como anéis de valorização são subanéis maximais próprios de $K(x)$, temos $\vartheta = \vartheta_{p(x)}$.

□

Note que repetindo o mesmo raciocínio para $x \in \vartheta$, temos uma descrição exata de ϑ_∞.

Se $x \notin \vartheta$ então $x^{-1} \in \vartheta$. Daí, $K[x^{-1}] \subseteq \vartheta$, e faça $I = K[x^{-1}] \cap P$. Note que $x^{-1} \in P$ (pois $x \notin \vartheta$) daí $x^{-1} \in I$. E ao mesmo tempo, se $z \in K[x^{-1}] \cap P$ então z não é inversível e

$$\begin{aligned} & z = a_m(x^{-1})^m + \cdots + a_1(x^{-1}) + a_0 \\ & z - a_m(x^{-1})^m + \cdots + a_1(x^{-1}) = a_0 \in P \\ & \therefore a_0 \in K \cap P \ \therefore \ a_0 = 0 \\ & \therefore z \in x^{-1}K[x^{-1}] \end{aligned}$$

Assim, $I = P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$, e daí para todo $g(x^{-1}) \in K[x^{-1}]$ tal que $x^{-1} \nmid g(x^{-1})$ não estão em I, logo $\dfrac{1}{g(x^{-1})} \in \vartheta$. Logo,

$$
\begin{aligned}
\vartheta &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} \,|\, f(x^{-1}), g(x^{-1}) \in K[x^{-1}] \text{ com } x^{-1} \not| g(x^{-1}) \right\} \\
&= \left\{ \frac{a_m(x^{-1})^m + \cdots + a_0}{b_r(x^{-1})^r + \cdots + b_0} \,|\, \text{ com } b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_m x^r + \cdots + a_0 x^{m+r}}{b_r x^m + \cdots + b_0 x^{m+r}} \,|\, \text{ com } b_0 \neq 0 \right\} \\
&= \left\{ \frac{f(x)}{g(x)} \,|\, \text{deg } f \leq \text{deg } g \right\} \text{ pois } b_0 \neq 0 \\
&= \vartheta_\infty
\end{aligned}
$$

E pela maximalidade dos aneis de valorização segue que $\vartheta = \vartheta_\infty$.

Corolário A.1.3. *Os lugares de $K(x)/K$ de grau 1 estão em 1-1 correspondência com $K \cup \{\infty\}$.*

Demonstração. Da proposição (A.1.1) segue que os lugares P_α e P_∞ estão em 1-1 correspondência com $K \cup \{\infty\}$ através da aplicação classe residual, explicitada nos itens (b) e (c) da proposição (A.1.1). E como do teorema (A.1.2) só existem esses lugares de grau 1, o corolário segue. □

B

Teoria Básica sobre Códigos

B.1 Teoria básica sobre códigos

Sejam $\mathbb{F}_q$ um corpo finito com q elementos. Consideremos o espaço vetorial n-dimensional $\mathbb{F}_q^n$ cujos elementos são n-uplas $a = (a_1, \cdots, a_n)$ com $a_i \in \mathbb{F}_q$. O corpo sobre o qual o código é escrito é chamado de alfabeto.

A definição a seguir é um parâmetro de extrema importância para teoria de códigos. O grande interesse nesse parâmetro é maximizá-lo em relação ao tamanho do código.

Definição B.1.1. *Para $a = (a_1, \cdots, a_n)$ e $b = (b_1, \cdots, b_n) \in \mathbb{F}_q^n$ seja*

$$d(a, b) := |\{i; a_i \neq b_i\}|$$

isto é, a quantidade de dígitos onde a, b diferem.

Esta função d é chamada distância de Hamming em $\mathbb{F}_q^n$.

O peso de um elemento $a \in \mathbb{F}_q^n$ é definido como

$$wt(a) := d(a, 0) = |\{i; a_i \neq 0\}|$$

isto é, a quantidade de dígitos não nulos de a.

É possível mostrar que a distância de Hamming é uma métrica em $\mathbb{F}_q^n$. Em particular, vale a desigualdade triangular, $d(a, c) \leq d(a, b) + d(b, c)$.

Definição B.1.2. *Um código C (sobre o alfabeto $\mathbb{F}_q^n$) é um subespaço linear de $\mathbb{F}_q^n$; os elementos de C são chamados de palavras. Denotamos por n o comprimento de C e $\dim C$ (visto como subespaço vetorial sobre $\mathbb{F}_q$) a dimensão do código. Um código $[n, k]$ é um código de comprimento n e dimensão k.*

A distância mínima $d(C)$ de um código $C \neq 0$ é definida como

$$d(C) := \min\{d(a,b) \,|\, a,b \in C \, e \, a \neq b\} = \min\{wt(c) \,|\, 0 \neq c \in C\}$$

Um código $[n,k]$ com distância mínima d será denotado por um código $[n,k,d]$.

Observação B.1.3. *Mais geralmente podemos definir códigos em subconjuntos não-vazios arbitrários $C \subseteq A^n$ onde $A \neq \emptyset$ é um conjunto finito. Se $A = \mathbb{F}_q$ e $C \subseteq \mathbb{F}_q^n$ é subespaço linear, C é dito um código linear. Vamos trabalhar somente com códigos lineares, logo não vamos nos referir a eles como lineares.*

Lema B.1.4. *Se $u \in \mathbb{F}_q^n$ e $d(u,c) \leq t$ para algum $c \in C$, então c é a única palavra com $d(u,c) \leq t$.*

Demonstração. Se existisse $c' \in C$ tal que $d(c',u) \leq t$ então

$$d(c,c') \leq d(c,u) + d(u,c') \leq 2t \leq d-1 < d$$

o que não o ocorre pois d é a distância mínima entre palavras do código. □

Para entender a importância deste parâmetro veremos o teorema a seguir, de [9].

Teorema B.1.5. *Seja C um código com distância mínima d. Então C pode corrigir até $t = [\frac{d-1}{2}]$ erros e detectar até $d-1$ erros.*

Demonstração. Suponha que ao transmitirmos uma palavra **c** do código cometemos x erros com $x \leq t$, obtendo a palavra **r**. Então $d(\mathbf{r},\mathbf{c}) = x \leq t$. E como afirma o lema (B.1.4), todas as outras palavras do código tem distância maior que t de **r**. Isso determina **r** univocamente, possibilitando assim a correção desses erros.

Por outro lado, dada uma palavra, podemos introduzir nela até $d-1$ erros sem gerar uma nova palavra (pois a distância entre essa nova palavra, com erros, e a original será menor que d, e logo não poderá ser uma palavra do código), possibilitando assim a detecção do erro. □

Sendo assim, quanto maior a distância mínima, mais erros de transmissão no código podem ser detectados e corrigidos.

Um jeito simples de descrever um código explicitamente é descrever sua base.

Definição B.1.6. *Seja C um código $[n,k]$ sobre $\mathbb{F}_q$. Uma matriz geradora de C é uma matriz $k \times n$ cujas linhas são uma base de C como subespaço vetorial sobre $\mathbb{F}_q$.*

O produto interno canônico de $\mathbb{F}_q^n$ é definido por

$$< a, b > := \sum_{i=1}^{n} a_i b_i$$

onde $a = (a_1, \cdots, a_n)$ e $b = (b_1, \cdots, b_n) \in \mathbb{F}_q^n$.

Note que $<, >$ é uma forma simétrica bilinear não-degenerada.

Definição B.1.7. *Se $C \subseteq \mathbb{F}_q^n$ é um código então*

$$C^{\perp} := \{u \in \mathbb{F}_q^n \mid \ < u, c > = 0, \, \forall c \in C\}$$

é chamado o dual de C. O código é chamado de auto-dual (resp. auto-ortogonal) se $C = C^{\perp}$ (resp. $C \subseteq C^{\perp}$).

Segue de um resultado de duais de álgebra linear que o dual de um código $[n, k]$ é um código $[n, n-k]$ e $(C^{\perp})^{\perp} = C$. Em particular a dimensão de um código auto-dual é $n/2$.

Definição B.1.8. *Uma matriz H geradora de $C^{\perp}$ é dita ser a matriz teste de paridade de C.*

Claramente uma matriz teste de paridade H de um código $[n, k]$ é uma matriz $(n-k) \times n$ de posto $n-k$ e temos

$$C = \{u \in \mathbb{F}_q^n \mid H \cdot u^t = 0\}$$

onde $u^t = u$ transposto.

Note que a matriz teste de paridade de fato verifica quando um vetor $u \in \mathbb{F}_q^n$ é uma palavra do código ou não.

Um dos problemas mais básicos em teoria de códigos algébricos é construir - sobre um alfabeto fixado $\mathbb{F}_q$ - códigos cuja dimensão e distância mínima são grandes em comparação com seu comprimento. Contudo existem algumas restrições. *Grosso modo*, se a dimensão do código é grande (em comparação com seu comprimento), então a distância mínima é pequena.

Proposição B.1.9 (Cota de Singleton)**.** *Para um código C $[n, k, d]$ vale*

$$k + d \leq n + 1$$

Demonstração. Considere um subespaço linear $E \subseteq \mathbb{F}_q^n$ dado por

$$E := \{(a_1, \cdots, a_n) \in \mathbb{F}_q^n \mid a_i = 0 \ \forall \ i \geq d\}$$

Todo $a \in E$ tem peso no máximo $d-1$, daí $E \cap C = 0$. E como $\dim E = d-1$ segue que

$$\begin{aligned} k + (d-1) &= \dim C + \dim E \\ &= \dim(C+E) + \dim C \cap E = \dim(C+E) \leq n \end{aligned}$$

□

Em geral é um problema bem mais complicado obter cotas inferiores para a distância mínima de um dado código. Apenas para uma pequena classe de códigos sabemos determinar uma cota inferior. Uma das razões porque vamos estudar os códigos de Goppa é que para essa classe de códigos existe uma boa cota inferior para a distância mínima.

Referências Bibliográficas

[1] S.J. Kim A. Garcia and R.F.Lax. Consecutive Weierstrass gaps and the minimum distance of Goppa codes. *J. Pure Appl. Algebra*, 84:199–207, 1993.

[2] P. Griffiths E.Arbarello, M.L.T. Cornalba and J Harris. *Geometry of Algebraic Curves*. Springer-Verlag, 1985.

[3] S.J. Kim. On the index of the Weierstrass semigroup of a pair of points on a curve. *Arch. Math.*, 62:73–82, 1994.

[4] M. Homma. The Weierstrass semigroup of a pair of points on a curve. *Arch. Math.*, 67:337–348, 1996.

[5] Gretchen Matthews. Weierstrass Pairs and Minimum Distance of Goppa Codes. *Designs, Codes and Cryptography*, 22:107–121, 2001.

[6] H. Stichtenoth. *Algebraic Function Fields and Codes,2nd Edition*. Springer, 2008.

[7] D.M.Goldschmidt. *Algebraic Function ande Projective Curves,2nd Edition*. Springer, 2002.

[8] A.Garcia. *Pontos racionais em curvas sobre corpos finitos*. IMPA, 1995.

[9] M. Villela A.Hefez. *Codigos Corretores de Erros*. IMPA, 2002.

[10] H. Stichtenoth. Uber die Automorphismengruppe eines algebraischen Funktionenkorpers von Primzahlcharakteristik II. *Arch. Math.*, 24:615–631, 1973.