

CARLOS HENRIQUE TOGNON

Cotas para a distância mínima de códigos de Goppa envolvendo o piso e o teto de um divisor



UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA

2011

CARLOS HENRIQUE TOGNON

Cotas para a distância mínima de códigos de Goppa envolvendo o piso e o teto de um divisor

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

Área de Concentração: Matemática.

Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG

2011

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

- T645c Tognon, Carlos Henrique, 1985-
Cotas para a distância mínima de códigos de Goppa envolvendo o piso
e o teto de um divisor [manuscrito] / Carlos Henrique Tognon. - 2011.
88 f. : il.
- Orientador: Cícero Fernandes de Carvalho.
- Dissertação (mestrado) – Universidade Federal de Uberlândia, Progra-
ma de Pós-Graduação em Matemática.
Inclui bibliografia.
1. Geometria algébrica - Teses. 2. Códigos de Goppa - Teses. 3.
Riemann-Roch, Teoremas de - Teses. 4. Extensões de corpos (Matemática)
- Teses. I. Carvalho, Cícero Fernandes de. II. Universidade Federal de
Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 514.16

Elaborado pelo Sistema de Bibliotecas da UFU / Setor de Catalogação e Classificação



UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Carlos Henrique Tognon.

NÚMERO DE MATRÍCULA: 100090.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Cotas para a distância mínima de códigos de Goppa envolvendo o piso e o teto de um divisor.

ORIENTADOR: Prof. Dr. Cícero Fernandes de Carvalho.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 03 de Março de 2011, às 16h00min, pela seguinte Banca Examinadora:

NOME

Prof. Dr. Cícero Fernandes de Carvalho
UFU - Universidade Federal de Uberlândia

Prof. Dr. Paulo Roberto Brumatti
UNICAMP - Universidade Estadual de Campinas

Prof. Dr. Alonso Sepúlveda Castellanos
UFU - Universidade Federal de Uberlândia

ASSINATURA

Uberlândia-MG, 03 de Março de 2011.

Dedicatória

Dedico este trabalho aos meus pais, Luiz Carlos Tognon e Dirce Aparecida Tertuliano Tognon, e ao meu irmão, André Luiz Tognon.

Agradecimentos

Primeiramente, agradeço à minha família por sempre estar ao meu lado.

Ao meu orientador Prof. Dr. Cícero Fernandes de Carvalho pela confiança em meu trabalho e por sempre me estimular e me motivar a estudar.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo suporte financeiro concedido neste período de estudos.

Aos professores Paulo Roberto Brumatti e Alonso Sepúlveda Castellanos por terem aceito o convite para comporem a minha banca de defesa da dissertação.

E a todos os demais que fizeram parte deste trabalho de forma direta ou indireta.

TOGNON, C. H. *Cotas para a distância mínima de códigos de Goppa envolvendo o piso e o teto de um divisor*. 2011. 88 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho, estudamos os fundamentos da teoria de corpos de funções algébricas, uma introdução à teoria de códigos, cabendo ressaltar neste ponto o estudo de códigos Geométricos de Goppa juntamente com os conceitos de derivação e forma diferencial, e resultados gerais no que diz respeito ao piso e o teto de um divisor. Este trabalho tem por objetivo apresentar duas cotas para a distância mínima de um código Geométrico de Goppa; estas cotas envolvem o piso de um divisor e fornecem uma boa estimativa para a distância mínima deste código. Além disso, apresentamos uma cota para a distância mínima de um código que envolve o teto de um divisor e, para finalizar, introduzimos alguns códigos sobre determinados corpos de funções algébricas e obtemos cotas para suas distâncias mínimas utilizando o conteúdo exposto no decorrer da dissertação.

Palavras-chave: Corpos de funções algébricas, Semigrupo de Weierstrass, Códigos de Goppa, Distância mínima.

TOGNON, C. H. *Quotas for the minimum distance of Goppa codes involving the floor and ceiling of a divisor*. 2011. 88 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work we study the basics of function field theory and coding theory, including geometric Goppa codes, derivations, differential forms and also results on the ceiling and floor of divisors. We present two bounds for the minimum distance of a geometric Goppa code, both involving the floor of a divisor and yielding good estimates for the true value of the minimum distance. We also present a bound related to the ceiling of a divisor; the work ends with examples dealing with codes over the Hermitian and the Suzuki function fields.

Keywords: Algebraic function fields, Weierstrass semigroup, Goppa codes, Minimum distance.

Sumário

Dedicatória	v
Agradecimentos	vi
Resumo	vii
Abstract	viii
Introdução	1
1 Conceitos Preliminares	3
1.1 Definições e Teoremas	3
2 Fundamentos da Teoria de Corpos de Funções Algébricas	6
2.1 Lugares	6
2.2 O corpo de funções algébricas racional	16
2.3 Independência de Valorizações	19
2.4 Divisores	20
2.5 O Teorema de Riemann-Roch	26
2.6 Algumas consequências do Teorema de Riemann-Roch	32
2.7 Componentes Locais das Diferenciais de Weil	36
3 Códigos Geométricos de Goppa, Derivações e Formas Diferenciais	38
3.1 Códigos	38
3.2 Códigos Geométricos de Goppa	40
3.3 Derivações e Formas Diferenciais	46
4 Sobre o Piso e o Teto de um divisor	53
4.1 O Piso e o Teto de um divisor	53
4.2 As cotas do piso e do piso generalizada	61
Referências Bibliográficas	79

Introdução

Esta dissertação trata do problema de se obter cotas para a distância mínima de um dado código. O trabalho está dividido basicamente em três partes. A primeira começa com definições e teoremas da Álgebra, tais como extensões de corpos, caracterização de extensão finita, elemento algébrico, polinômio minimal, etc. Nesta primeira parte a finalidade é introduzir o leitor no assunto posterior e ao mesmo tempo fazer uma recordação destes conceitos e resultados. Alguns destes resultados foram demonstrados e outros não, mas para estes a demonstração pode ser encontrada em qualquer bom livro de Álgebra, por exemplo, [5]. Dando continuidade a esta primeira parte, introduzimos os fundamentos da teoria de corpos de funções algébricas; entre eles estão os conceitos de valorização discreta, lugares, divisores, gênero e adeles de um corpo de funções algébricas, diferenciais de Weil e o teorema de Riemann-Roch, que nos ajuda a encontrar a dimensão do espaço associado a um divisor. Daremos algumas caracterizações para o gênero em termos da dimensão de certos espaços vetoriais e também usando o teorema de Riemann-Roch. Como um exemplo importante de corpo de funções algébricas veremos o chamado corpo de funções algébricas racional e vamos mostrar que o seu gênero é igual à zero. Não podemos deixar de mencionar que nesta primeira parte da dissertação aparece uma definição crucial para o desenvolvimento do trabalho; nos referimos à definição do chamado semigrupo de Weierstrass de um lugar e ela envolve os conceitos de ordem de pólo e lacuna de um lugar. Com isso chegamos no teorema das Lacunas de Weierstrass, um outro resultado relevante da teoria. Encerramos a primeira etapa com as componentes locais das diferenciais de Weil; esta definição, juntamente com dois resultados que foram colocados, nos auxiliará na segunda parte do trabalho, a qual se refere à teoria de códigos. Neste trabalho vamos considerar apenas códigos lineares. Veremos que um código é um subespaço vetorial de um espaço vetorial de dimensão finita; vamos definir a distância mínima de um código e o peso de cada elemento deste espaço vetorial. Iremos apresentar uma cota que é válida para a distância mínima de qualquer tipo de código, denominada a cota de Singleton, a qual estabelece que a distância mínima de todo código é sempre menor ou igual do que o comprimento menos a dimensão do código somados de um. Nosso principal interesse está em códigos Geométricos de Goppa. É importante colocarmos neste momento uma motivação para a definição de códigos Geométricos de Goppa; para tanto consideremos os chamados códigos Reed Solomon, um espaço vetorial sobre o corpo finito com q elementos $\mathbb{F}_q$. Esta é uma importante classe de códigos bem conhecida na teoria de codificação. Códigos Geométricos de Goppa são uma generalização muito natural

de códigos Reed Solomon. Seja $n = q - 1$ e $\beta \in \mathbb{F}_q$ um elemento gerador do grupo multiplicativo $\mathbb{F}_q \setminus \{0\}$, isto é, β é tal que $\mathbb{F}_q \setminus \{0\} = \{\beta, \beta^2, \dots, \beta^n = 1\}$. Para $k \in \mathbb{Z}$, com $1 \leq k \leq n$, consideremos o $\mathbb{F}_q$ espaço vetorial, k -dimensional, $\mathcal{L}_k := \{f \in \mathbb{F}_q[X] \mid \text{grau}(f) \leq k - 1\}$, e a aplicação avaliação $e_v : \mathcal{L}_k \longrightarrow \mathbb{F}_q^n$ dada por $e_v(f) := (f(\beta), f(\beta^2), \dots, f(\beta^n)) \in \mathbb{F}_q^n$. Note que esta aplicação é $\mathbb{F}_q$ -linear, pois dado $\lambda \in \mathbb{F}_q$ e $f, g \in \mathcal{L}_k$, temos que

$$e_v(f + \lambda g) := ((f + \lambda g)(\beta), \dots, (f + \lambda g)(\beta^n)) = (f(\beta) + \lambda g(\beta), \dots, f(\beta^n) + \lambda g(\beta^n)) = (f(\beta), \dots, f(\beta^n)) + \lambda(g(\beta), \dots, g(\beta^n)) = e_v(f) + \lambda(e_v(g)).$$

Notamos que e_v também é injetora, pois dado um polinômio não nulo $f \in \mathbb{F}_q[X]$ tal que $f \in \mathcal{L}_k$, temos que o $\text{grau}(f) \leq k - 1 \leq n - 1 < n$ e daí f possui uma quantidade de zeros inferior à n e desta forma, $\text{Ker}(e_v) = \{f \in \mathcal{L}_k \mid e_v(f) = 0\} = \{0\}$ e daí e_v é injetora (observe que $\text{Ker}(e_v) = \{0\}$, uma vez que se existisse f não-nulo em $\mathcal{L}_k$ tal que $e_v(f) = 0$, o polinômio f teria as n raízes $\beta, \beta^2, \dots, \beta^n$, o que é absurdo). Portanto, $C_k := \{e_v(f) \mid f \in \mathcal{L}_k\}$ é um código de comprimento n e dimensão k sobre o corpo $\mathbb{F}_q$; este código é chamado código Reed-Solomon. Juntamente com esta introdução à teoria de códigos, definimos os conceitos de derivação e forma diferencial. Neste ponto, o principal resultado que envolve a teoria é o teorema que nos fornece um isomorfismo entre o espaço das formas diferenciais e o espaço das diferenciais de Weil; com isso, muitas vezes será mais fácil utilizarmos uma forma diferencial no lugar de uma diferencial de Weil, principalmente em algumas demonstrações. A terceira parte deste trabalho trata do piso e do teto de um divisor. Nesta parte daremos resultados que são válidos para corpos de funções algébricas arbitrários, no entanto trabalharemos com um específico. Após definirmos o piso e o teto de um divisor, estaremos prontos para demonstrarmos teoremas nos quais vamos obter cotas inferiores para a distância mínima de um código Geométrico de Goppa, haja vista que algumas destas cotas envolvem o piso e outras o teto de um divisor. Finalizamos a dissertação com alguns exemplos de como podemos aplicar a teoria abordada; para tanto vamos definir códigos sobre os corpos de funções algébricas Hermitiano e de Suzuki. Com o auxílio dos teoremas, encontraremos cotas para a distância mínima destes códigos e faremos comparações entre elas, de modo a verificar qual é a melhor. No decorrer destes exemplos usaremos diversos resultados interessantes; em muitos deles omitiremos a demonstração que poderá ser encontrada nas referências bibliográficas.

Capítulo 1

Conceitos Preliminares

O objetivo deste capítulo é introduzir alguns conceitos que usaremos em todo este trabalho.

1.1 Definições e Teoremas

Definição 1.1.1 (i) Se F e K são corpos e $F \supset K$ dizemos que F é uma extensão do corpo K e escrevemos F/K .

(ii) Sejam $u_1, \dots, u_n$ em F e suponha que F é uma extensão de K . A interseção de todos os subanéis de F que contém K e $\{u_1, \dots, u_n\}$ é um subanel de F denotado por $K[u_1, \dots, u_n]$. A interseção de todos os subcorpos de F que contém K e $\{u_1, \dots, u_n\}$ é um subcorpo de F denotado por $K(u_1, \dots, u_n)$.

Dado um corpo K denotaremos o anel de polinômios em n variáveis sobre K por $K[x_1, \dots, x_n]$. Assim é simples concluir que:

Lema 1.1.1 Nas condições da definição acima, temos que:

- (i) $K[u_1, \dots, u_n] = \{f(u_1, \dots, u_n) \in F \mid f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]\}$.
- (ii) $K(u_1, \dots, u_n) = \left\{ \frac{f(u_1, \dots, u_n)}{g(u_1, \dots, u_n)} \in F \mid f, g \in K[x_1, \dots, x_n], g(u_1, \dots, u_n) \neq 0 \right\}$.
- (iii) $K[u_1, \dots, u_{n-1}][u_n] = K[u_1, \dots, u_n]$.
- (iv) $K(u_1, \dots, u_{n-1})(u_n) = K(u_1, \dots, u_n)$.

Definição 1.1.2 Seja F/K uma extensão de corpos e $u \in F$. Dizemos que u é algébrico sobre K se u é raiz de um polinômio não nulo com coeficientes em K . Caso contrário, dizemos que u é transcendente sobre K .

Observação 1.1.1 Na definição acima, se todo elemento $u \in F$ for algébrico sobre K dizemos que a extensão F/K é algébrica.

Teorema 1.1.1 Sejam F/K uma extensão de corpos, $u \in F$ e a aplicação $\phi : K[x] \longrightarrow F$, o homomorfismo avaliação em u dado por $f(x) \longmapsto f(u)$. Então,

- (i) $\text{Im}(\phi) = K[u]$;

- (ii) u é transcendente sobre $K \iff \text{Ker}(\phi) = \{0\}$;
- (iii) Se u é algébrico sobre K então $\text{Ker}(\phi)$ é gerado por um único polinômio irreduzível e mônico logo $\text{Ker}(\phi)$ é ideal maximal;
- (iv) A aplicação $\bar{\phi} : K[x]/\text{Ker}(\phi) \longrightarrow K[u]$ dada por $\bar{\phi}(\bar{f}(x)) = f(u)$, é um isomorfismo; em particular se u é transcendente sobre K então $K[u]$ é isomorfo à $K[x]$ e se u é algébrico sobre K então $K[u] = K(u)$.

Observe que, do teorema acima, temos que se $u \in F \supset K$ é algébrico sobre K então $K[u]$ é um corpo.

Definição 1.1.3 Sejam F , K e ϕ como no teorema acima e seja $u \in F$ um elemento algébrico sobre o corpo K . O gerador mônico de $\text{Ker}(\phi)$ é chamado de polinômio minimal de u sobre K e será denotado por m_u .

Teorema 1.1.2 Seja F/K uma extensão de corpos e $u \in F$ um elemento algébrico sobre K . As seguintes afirmações são equivalentes:

- (i) $f(x)$ é o polinômio minimal de u sobre K ;
- (ii) $f(x)$ possui u como raiz, é mônico e $\text{grau}(f(x)) \leq \text{grau}(g(x))$, para todo polinômio $g(x) \neq 0$ que possui u como raiz;
- (iii) $f(x)$ possui u como raiz, é mônico e é irreduzível.

Definição 1.1.4 Seja F/K uma extensão de corpos e sejam $a_1, \dots, a_n$ elementos de K . Dizemos que $a_1, \dots, a_n$ são algebricamente independentes sobre F se não existe um polinômio não nulo $f(x_1, \dots, x_n)$ pertencente à $F[x_1, \dots, x_n]$ tal que $f(a_1, \dots, a_n) = 0$.

Definição 1.1.5 Seja F/K uma extensão de corpos. Então F é um K -espaço vetorial e sua dimensão, como K -espaço vetorial, é chamada de grau da extensão. Notação: $[F : K]$. Se $[F : K] < \infty$ então dizemos que a extensão F/K é finita. Caso contrário, é uma extensão infinita.

Lema 1.1.2 Seja F/K uma extensão de corpos.

- (i) Seja $u \in F$ algébrico sobre K e seja $n := \text{grau}(m_u)$. Então, $[K[u] : K] = n$; o conjunto $\{1, u, \dots, u^{n-1}\}$ é uma base para $K[u]$ como K -espaço vetorial.
- (ii) Se F/K é uma extensão finita então ela é extensão algébrica.

Demonstração (i) Seja $p(x) := m_u$; temos que $\text{grau}(p(x)) = n$. Seja $f(u) \in K[u]$, onde $f(x) \in K[x]$. Fazendo a divisão euclidiana de f por p obtemos polinômios $q(x)$ e $r(x)$ em $K[x]$ tais que $f(x) = p(x)q(x) + r(x)$, com $r(x) = 0$ ou $\text{grau}(r(x)) < n$, isto é, $r(x) = \sum_{i=0}^{n-1} a_i x^i \in K[x]$. Daí, vem que $f(u) = p(u)q(u) + \sum_{i=0}^{n-1} a_i u^i$ e logo o conjunto $\{1, u, \dots, u^{n-1}\}$ gera $K[u]$ como K -espaço vetorial. Sejam agora $a_0, a_1, \dots, a_{n-1}$ em K tais que $a_0 + a_1 u + \dots + a_{n-1} u^{n-1} = 0$; se não temos todos os coeficientes iguais à zero teríamos que $g(x) = \sum_{i=0}^{n-1} a_i x^i$ seria um

polinômio não nulo que possui u como raiz e tem grau menor do que o grau de m_u , o que é um absurdo. Isto completa a demonstração de que $\{1, u, \dots, u^{n-1}\}$ é uma base.

(ii) Suponha que F/K é uma extensão finita. Seja $n := [F : K]$ e $u \in F$. Temos que o conjunto $\{1, u, \dots, u^{n-1}, u^n\}$ é linearmente dependente, pois possui $n + 1$ elementos. Logo, existem $a_0, \dots, a_n$ não todos nulos tais que $\sum_{i=0}^n a_i u^i = 0$. Isso mostra que $g(x) = \sum_{i=0}^n a_i x^i \in K[x] \setminus \{0\}$ e possui u como raiz, uma vez que $g(u) = 0$. Portanto, u é algébrico sobre K . ■

Teorema 1.1.3 Sejam $K \subset F \subset L$ extensões de corpos tais que $[F : K] < \infty$ e $[L : F] < \infty$. Então, $[L : K] < \infty$. Mais explicitamente, se $\{u_1, \dots, u_n\}$ é uma base de L como F -espaço vetorial e $\{v_1, \dots, v_m\}$ é uma base de F como K -espaço vetorial, então o conjunto constituído pelos elementos da forma $u_i v_j$ tal que $i = 1, \dots, n$ e $j = 1, \dots, m$ é uma base de L como K -espaço vetorial. Em particular, $[L : K] = n.m$.

Corolário 1.1.1 Seja F/K uma extensão de corpos finita e seja $u \in F$. Então, $\text{grau}(m_u)$ divide $[F : K]$.

Demonstração Como $u \in F$ é algébrico sobre K temos que $K[u]$ é um corpo. Considere $K \subset K[u] \subset F$. Observamos então que $[F : K] = [F : K[u]] \cdot [K[u] : K]$, com $\text{grau}(m_u) = [K[u] : K]$. Assim, $\text{grau}(m_u)$ divide o grau da extensão F/K , como queríamos demonstrar. ■

Corolário 1.1.2 Seja F/K uma extensão finita e seja $u \in F$. Temos que, $F = K[u]$ se, e somente se, $\text{grau}(m_u) = [F : K]$.

Demonstração Como F/K é uma extensão de corpos finita, então é algébrica. Sendo $u \in F$ segue que u é algébrico sobre K ; então $K[u]$ é um corpo. Seja $n := \text{grau}(m_u)$. Suponha que $n = [F : K]$. Pelo corolário anterior, temos que $[F : K] = [F : K[u]] \cdot [K[u] : K]$ e então $n = [F : K[u]] \cdot n$, o que acarreta $[F : K[u]] = 1$. Ou seja, a dimensão de F como $K[u]$ -espaço vetorial é igual à um e daí $F = K[u]$. Reciprocamente, se $F = K[u]$ então $[F : K[u]] = 1$ e desta forma $[F : K] = 1 \cdot [K[u] : K]$, donde obtemos que $\text{grau}(m_u) = [F : K]$. ■

Corolário 1.1.3 Sejam $K \subset F \subset L$ extensões de corpos sendo que F/K é extensão algébrica. Se $u \in L$ é algébrico sobre F então é algébrico sobre K .

Demonstração Por hipótese, existe $f(x) = \sum_{i=0}^n a_i x^i \in F[x] \setminus \{0\}$ tal que $f(u) = 0$. Como $a_0, \dots, a_n \in F$, temos que esses elementos são algébricos sobre K . Considere as extensões $K \subset K[a_0] \subset K[a_0, a_1] \subset K[a_0, a_1, a_2] \subset \dots \subset K[a_0, \dots, a_n]$, e observamos que cada inclusão é uma extensão do tipo $M \subset M[\alpha]$, com M um corpo e α um elemento algébrico sobre M . Logo, cada uma dessas extensões é uma extensão finita. Assim, segue que $K[a_0, \dots, a_n]/K$ é extensão finita. Note que u é algébrico sobre $K[a_0, \dots, a_n]$, pois $f(x) \in K[a_0, \dots, a_n][x] \setminus \{0\}$; logo, $K[a_0, \dots, a_n][u]/K[a_0, \dots, a_n]$ é extensão finita e conseqüentemente $K[a_0, \dots, a_n][u]/K$ é extensão finita. Em particular, u é algébrico sobre K . ■

Capítulo 2

Fundamentos da Teoria de Corpos de Funções Algébricas

Neste capítulo vamos introduzir definições básicas e resultados importantes da teoria de Corpos de Funções Algébricas, tais como valorizações, lugares, divisores, o gênero do corpo de funções, adeles, diferenciais de Weil e o teorema de Riemann-Roch. Ao longo de todo este capítulo, K denota um corpo arbitrário.

2.1 Lugares

Definição 2.1.1 Um corpo de funções algébricas F/K em uma variável sobre K é uma extensão de corpos tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ que é transcendente sobre K .

Para abreviar, em certos momentos, vamos simplesmente nos referir a F/K como corpo de funções. Denotaremos por $\tilde{K}$ o conjunto $\tilde{K} := \{z \in F \mid z \text{ é algébrico sobre } K\}$.

O conjunto $\tilde{K}$ é um subcorpo de F , pois somas, produtos e inversos de elementos algébricos também são algébricos e assim $\tilde{K}$ é fechado para a subtração e multiplicação de F e todo elemento não nulo em $\tilde{K}$ possui inverso em $\tilde{K}$. O corpo $\tilde{K}$ é chamado de corpo de constantes de F/K . Já que todo elemento de K é algébrico sobre K , temos que $K \subseteq \tilde{K} \subseteq F$. Observe que F contém $\tilde{K}$ propriamente, pois caso contrário todos os elementos de F seriam algébricos sobre K , o que acarreta que F/K não seria corpo de funções. Dizemos que K é algebricamente fechado em F , ou que K é todo o corpo de constantes de F , se $K = \tilde{K}$.

Afirmção 2.1.1 A extensão de corpos $F \supset \tilde{K}$ é um corpo de funções sobre $\tilde{K}$.

De fato, já temos que a extensão de corpos $F/K(x)$ é extensão algébrica finita, para $x \in F$ um elemento transcendente sobre K , e então como $K(x) \subseteq \tilde{K}(x)$ segue que $[F : \tilde{K}(x)] < \infty$; sendo a extensão $F/\tilde{K}(x)$ finita então ela também é algébrica. Afirmamos que este elemento x é transcendente sobre $\tilde{K}$, uma vez que supondo x algébrico sobre $\tilde{K}$ obtemos que a extensão

$\tilde{K}(x)/\tilde{K}$ é finita e então $[F : \tilde{K}] < \infty$ e como $[\tilde{K} : K] < \infty$ segue que a extensão F/K é finita e portanto algébrica; desta forma x não é transcendente sobre K , o que é absurdo. Portanto, $F/\tilde{K}$ é um corpo de funções sobre $\tilde{K}$.

Observação 2.1.1 Seja F/K um corpo de funções. Os elementos de F que são transcendentos sobre K são caracterizados da seguinte maneira: $z \in F$ é transcendente sobre K se, e somente se, $[F : K(z)]$ é finito.

Exemplo 2.1.1 Um exemplo simples de um corpo de funções algébricas é o corpo de funções racional. O corpo de funções F/K é chamado de racional se $F = K(x)$ para algum $x \in F$ transcendente sobre K . Como temos $K(x) := \left\{ \frac{f(x)}{g(x)} \in F \mid f, g \in K[x], g(x) \neq 0 \right\}$, qualquer elemento $z \in K(x) \setminus \{0\}$ é tal que $z \equiv \frac{f(x)}{g(x)}$ e então z tem uma única representação da forma $z \equiv a \cdot \prod_i p_i(x)^{n_i}$, em que $0 \neq a \in K$, os polinômios $p_i(x) \in K[x]$ são mônicos, distintos dois a dois e irredutíveis com os $n_i \in \mathbb{Z}$.

Definição 2.1.2 Um anel de valorização do corpo de funções algébricas F/K é um anel O do corpo F com as seguintes propriedades:

- (1) $K \subset O \subset F$, e essas inclusões são próprias;
- (2) para todo $z \in F$, temos que $z \in O$ ou $z^{-1} \in O$.

Exemplo 2.1.2 Considere o corpo de funções racional $K(x)/K$ e seja $p(x) \in K[x]$ um polinômio irredutível. Considere o conjunto,

$$O_{p(x)} := \left\{ \frac{f(x)}{g(x)} \in K(x) \mid f(x), g(x) \in K[x], g(x) \neq 0, \text{ com } p(x) \text{ não dividindo } g(x) \right\}.$$

Afirmção 2.1.2 $O_{p(x)}$ é um anel de valorização do corpo de funções $K(x)/K$.

De fato, com as operações herdadas de $K(x)$, temos que $O_{p(x)}$ é um subanel de $K(x)$; logo, é um anel do corpo $K(x)$. Agora, note que:

- (1) Seja $a \in K$; temos $a = \frac{a}{1}$ e $p(x)$ não divide 1, uma vez que se $p(x)$ divide 1 então $1 = p(x) \cdot q(x)$, $q(x) \in K[x]$, e desta forma $\text{grau}(p(x)) = 0$ o que não é possível pois $p(x)$ é irredutível. Assim, $a \in O_{p(x)}$ e portanto $K \subset O_{p(x)}$. Temos que $K \neq O_{p(x)}$, pois $p(x) \in O_{p(x)}$ e não pertence à K . Portanto, $K \neq O_{p(x)}$. Conclusão: $O_{p(x)} \supset K$, propriamente.
- (2) Temos, por definição, que $O_{p(x)} \subset K(x)$. Observe que $\frac{1}{p(x)} \in K(x)$ e não pertence à $O_{p(x)}$, pois $p(x)$ divide $p(x)$. Conclusão: $O_{p(x)} \subset K(x)$, propriamente.
- (3) Seja $\frac{f(x)}{g(x)} \in K(x)$. Se temos que $p(x)$ não divide $g(x)$ então $\frac{f(x)}{g(x)} \in O_{p(x)}$. Agora, se $p(x)$ divide $g(x)$ então $g(x) = p(x) \cdot q(x)$, $q(x) \in K[x]$, e podemos assumir, sem perda de generalidade, que o *m.d.c.* $(f(x), g(x)) = 1$. Assim, $p(x)$ não divide $f(x)$, pois caso contrário teríamos $f(x) = p(x) \cdot s(x)$, $s(x) \in K[x]$, logo $f(x) = \frac{g(x)}{q(x)} s(x)$, ou seja, $g(x)$ divide $f(x)$, o que é uma contradição. Portanto, se $p(x)$ divide $g(x)$ então $p(x)$ não divide $f(x)$ o que acarreta que $\frac{g(x)}{f(x)} \in O_{p(x)}$. Ou seja, o inverso de $\frac{f(x)}{g(x)}$ está em $O_{p(x)}$.

Desta forma, de (1), (2) e (3) temos que $O_{p(x)}$ é um anel de valorização de $K(x)/K$.

Proposição 2.1.1 Seja O um anel de valorização do corpo de funções F/K . Então:

- (a) O é um anel local, isto é, O tem um único ideal maximal, que é $P = O \setminus O^*$, onde $O^* := \{z \in O \mid \text{existe } w \in O \text{ com } z.w = 1\}$ é o grupo de unidades de O .
- (b) Para $0 \neq x \in F$, $x \in P \Leftrightarrow x^{-1} \notin O$.
- (c) Para o corpo $\tilde{K} = \{z \in F \mid z \text{ é algébrico sobre } K\}$ de constantes de F/K temos $\tilde{K} \subseteq O$ e $\tilde{K} \cap P = \{0\}$.

Demonstração (a) Afirmamos que $P = O \setminus O^*$ é um ideal de O . De fato,

(1) P não é vazio, pois O não é vazio. Sejam $x \in P$ e $z \in O$. Se $xz \in O^*$ então existe $w \in O$ tal que $(xz).w = 1$; logo, $(xz).w = 1 \Rightarrow x.(zw) = 1 \Rightarrow x \in O^*$, uma contradição pois $x \in P$. Portanto, $xz \in P$.

(2) Sejam $x, y \in P$; como $\frac{x}{y} \in F$ segue que $\frac{x}{y} \in O$ ou $\frac{y}{x} \in O$, uma vez que O é anel de valorização. Sem perda de generalidade, podemos assumir que $\frac{x}{y} \in O$ e como $1 \in O$, segue que $1 + \frac{x}{y} \in O$. Assim $x + y \in P$, uma vez que $x + y = y \left(1 + \frac{x}{y}\right)$, com $y \in P$.

Conclusão: de (1) e (2), temos que P é um ideal de O .

Também, P é o único ideal maximal. De fato, seja I um ideal de O tal que $P \subset I \subset O$ e $P \neq I$. Assim, existe $z \in I$ tal que $z \in O^*$; como I é ideal de O segue que $z.z^{-1} = 1 \in I$ e então $I = O$. Portanto, P é ideal maximal. Agora, se J é outro ideal maximal de O temos que, se $J \subset P \subset O$ então $P = J$, uma vez que P é maximal ou se $P \subset J \subset O$ então $J = O$ ou $J = P$, pois J é maximal. Portanto, P é o único ideal maximal.

(b) Seja $x \in F \setminus \{0\}$. Assim, se $x \in P$ então $x \notin O^*$ e com isso $x^{-1} \notin O$. Reciprocamente, se $x^{-1} \notin O$ então $x \in O$, pois O é anel de valorização; logo, $x \in O \setminus O^* = P$.

(c) Seja $0 \neq z \in \tilde{K}$ e suponha que $z \notin O$. Como O é anel de valorização temos que $z^{-1} \in O$. Como o inverso de elemento algébrico é algébrico, segue que o inverso de z também é algébrico, logo está em $\tilde{K}$. Então, existe $f(x) \in K[x] \setminus \{0\}$ tal que $f(z^{-1}) = 0$. Sem perda de generalidade, temos que $f(x) = a_r x^r + \dots + a_1 x + 1$. Logo, obtemos que $a_r z^{-r} + \dots + a_1 z^{-1} + 1 = 0$ o que acarreta $z^{-1}(a_r z^{-r+1} + \dots + a_1) = -1$. Portanto, $z = -(a_r z^{-r+1} + \dots + a_1)$ e como $z^{-1} \in O$ segue que $z \in O$, uma contradição. Disto, $\tilde{K} \subseteq O$. Por fim, se $z \neq 0$ está em $\tilde{K}$ o inverso de z também está e então, como $\tilde{K} \subseteq O$, temos que $z, z^{-1} \in O$. Logo, $z \notin P$ e portanto $\tilde{K} \cap P = \{0\}$. ■

Teorema 2.1.1 Seja O um anel de valorização do corpo de funções F/K e $P = O \setminus O^*$ o seu único ideal maximal. Então,

- (a) P é um ideal principal.
- (b) Se $P = tO$ então qualquer $0 \neq z \in F$ tem uma única representação da forma $z = t^n u$, para algum $n \in \mathbb{Z}$, com $u \in O^*$.
- (c) O é um domínio de ideal principal. Mais precisamente, se $P = tO$ e $\{0\} \neq I \subseteq O$ é um ideal então $I = t^n O$, para algum $n \in \mathbb{N}$.

Um anel tendo as propriedades anteriores é chamado um anel de valorização discreta. A demonstração do teorema anterior depende essencialmente do seguinte lema.

Lema 2.1.1 Sejam O um anel de valorização do corpo de funções algébricas F/K , P seu ideal maximal e o elemento não nulo $x \in P$. Sejam $x_1, \dots, x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$, para $i = 1, \dots, n-1$. Então, $n \leq [F : K(x)] < \infty$.

Demonstração Como temos $0 \neq x \in P$ e $\tilde{K} \cap P = \{0\}$ segue que $x \notin \tilde{K}$ e então x é transcendente sobre K . Pela observação 2.1.1. segue que $[F : K(x)] < \infty$. Para provar que $[F : K(x)] \geq n$ é suficiente provar que $x_1, \dots, x_n$ são linearmente independentes sobre $K(x)$, pois assim qualquer conjunto linearmente independente sobre $K(x)$ não terá menos do que n elementos e daí se $x_1, \dots, x_n$ gerarem F teremos $[F : K(x)] = n$, se não gerarem F teremos $[F : K(x)] > n$. Suponha que $x_1, \dots, x_n$ são linearmente dependentes, ou seja, que temos a combinação linear não trivial $\sum_{i=1}^n \Phi_i x_i = 0$, com $\Phi_i \in K(x)$. Podemos supor que todos os Φ_i são expressões polinomiais em x e que x não divide todos os Φ_i , uma vez que se x dividisse todos os Φ_i teríamos $\Phi_i = xg_i \in K(x)$ para todo $i = 1, \dots, n$, e então, $\sum \Phi_i x_i = 0 \Rightarrow \sum x x_i g_i = 0 \Rightarrow x(\sum x_i g_i) = 0 (x \neq 0) \Rightarrow \sum x_i g_i = 0$; basta então substituir Φ_i por g_i . Seja $a_i = \Phi_i(0)$ o termo constante de Φ_i e definindo a_j , para j fixo em $\{1, \dots, n\}$, pela condição $a_j \neq 0$ e $a_i = 0$ para todo $i > j$, obtemos que $\sum \Phi_i x_i = 0$ implica em $\sum_{i \neq j} \Phi_i x_i = -\Phi_j x_j$ com $\Phi_i \in O$, para $i = 1, \dots, n$, uma vez que como $K \subseteq O$ e $x \in O$ segue que $K(x) \subseteq O$. Também, $x_i \in x_j P$ para $j > i$ e para $i > j$, como temos $a_i = 0$, podemos colocar $\Phi_i = xg_i$, onde g_i é uma expressão polinomial em x . Note que como $x_1 \neq 0$ temos, $x_1 \in x_2 P \Rightarrow x_2 \neq 0$; $x_2 \in x_3 P \Rightarrow x_3 \neq 0$; $\dots$; $x_{n-1} \in x_n P \Rightarrow x_n \neq 0$. Logo, existe elemento invertível $x_j \neq 0$ e então, $\sum_{i \neq j} \Phi_i x_i = -\Phi_j x_j \Rightarrow -\Phi_j = \sum_{i < j} \Phi_i \frac{x_i}{x_j} + \sum_{i > j} xg_i \frac{x_i}{x_j}$. Nesta última igualdade todas as parcelas do lado direito pertencem a P , uma vez que $x_i \in P$, $\frac{\Phi_i}{x_j} \in O$, $\frac{x}{x_j} \in O$ e P é ideal de O . Portanto, $\Phi_j \in P$. Por outro lado, observe que $\Phi_j = a_j + xg_j$, com $g_j \in K[x] \subseteq O$ e $x \in P$, onde $a_j = -\sum_{i < j} \Phi_i \frac{x_i}{x_j}$ e $g_j = \sum_{i > j} g_i \frac{x_i}{x_j}$. Logo, $a_j = \Phi_j - xg_j \in P \cap K$. Como $P \cap \tilde{K} = \{0\}$ e $K \subseteq \tilde{K}$, temos $P \cap K = \{0\}$; mas $a_j \neq 0$ está em $P \cap K$, o que é absurdo. Portanto, $x_1, \dots, x_n$ são linearmente independentes sobre $K(x)$ e deste modo $[F : K(x)] \geq n$. ■

Demonstração[Demonstração do Teorema] (a) Suponha que P não é um ideal principal. Escolhemos $x_1 \neq 0$ em P e como P não é principal, podemos supor que $P \neq x_1 O$. Existe então $x_2 \in P \setminus x_1 O$. Então $x_1^{-1} x_2 \notin O$, pois se pertencesse teríamos que $x_2 = x_1 x_1^{-1} x_2 \in x_1 O$, contrariando $x_2 \in P \setminus x_1 O$. Portanto, pela proposição 2.1.1. (b), $x_1 x_2^{-1} \in P$; disto, $x_2^{-1} x_1 = p$ e então $x_1 = x_2 p$. Logo, $x_1 \in x_2 P$. Por indução, obtemos uma sequência infinita $x_1, x_2, \dots$ em P , com $x_i \in x_{i+1} P$, para todo $i \geq 1$, o que contradiz o lema 2.1.1., uma vez que teríamos o grau da extensão $F/K(x)$ não sendo finito. Portanto, P é um ideal principal.

(b) Temos que $P = tO$. Provemos a existência: Sendo $z \in F \setminus \{0\}$, como O é anel de valorização segue que $z \in O$ ou $z^{-1} \in O$. Se z é um elemento invertível de O então $z = t^0 z$. Consideremos agora o caso em que $z \in P$. Seja m um número inteiro, tal que $m \geq 1$ e considere a sequência, $z = x_1, x_2 = t^{m-1}, x_3 = t^{m-2}, \dots, x_m = t$, com os elementos em P e com $x_i \in x_{i+1} P$, para

$i = 1, \dots, m-1$. Logo, $z \in t^{m-1}P = t^{m-1}tO$, ou seja, $z \in t^mO$. Então, $z = t^m u$ com $u \in O$. Podemos tomar este inteiro m sendo o maior valor possível para a formação da sequência anterior, uma vez que pelo lema 2.1.1. o grau da extensão $F/K(x)$ é finito e então m é tomado sendo o maior grau desta extensão. Então o elemento u é uma unidade de O , pois caso contrário temos $u \in P = tO$ e daí $u = tw$, com $w \in O$ e assim $z = t^{m+1}w \in t^{m+1}O$, o que contraria a maximalidade de m . Portanto, $z = t^m u$, $u \in O^*$. Observemos agora a unicidade desta representação: Se $z = t^n u$ e $z = t^m w$, com $u, w \in O^*$, suponha que $n \leq m$; assim, $t^n u = t^m w$ implica que $t^{m-n}(uw^{-1}) = 1$ e com isso $m = n$ e $u = w$.

(c) Como $O \subseteq F$ e F é um corpo, já temos que O é um domínio. Seja $I \neq \{0\}$ um ideal de O e considere o conjunto $A := \{r \in \mathbb{N} \mid t^r \in I\}$. Note que $A \neq \emptyset$, pois se $x \in I$ é um elemento não nulo, como $I \subseteq O$ e $O \subseteq F$, propriamente, segue que $x \in F$ e então pela parte (b) temos $x = t^r u$, com $u \in O^*$, $r \in \mathbb{N}$, e assim segue que $xu^{-1} = t^r \in I$. Sendo A um conjunto de números naturais existe o elemento mínimo de A , digamos $n = \min(A)$. Afirmamos que $I = t^n O$. De fato, como $t^n \in I$ tomamos $p \in O$ e assim $t^n p \in I$. Logo, $t^n O \subseteq I$. Reciprocamente, seja $y \in I \setminus \{0\}$. Pela parte (b) temos que $y = t^s w$, com $w \in O^*$ e $s \geq 0$; logo, $t^s = yw^{-1} \in I$ e $s \geq n$. Daí, $y = t^n t^{s-n} w \in t^n O$ e então $I \subseteq t^n O$. Portanto, $I = t^n O$. ■

Definição 2.1.3 (a) Um lugar P do corpo de funções F/K é o ideal maximal de algum anel de valorização O de F/K . Todo elemento $t \in P$ tal que $P = tO = \{tp \mid p \in O\}$ é chamado um elemento primo para P , também denominado parâmetro local, uniformizante local ou variável uniformizante.

(b) $\mathbb{P}_F := \{P \mid P \text{ é um lugar de } F/K\}$.

Se O é um anel de valorização de F/K e P é seu ideal maximal então O é determinado unicamente por P ; mais explicitamente, $O := \{z \in F \mid z^{-1} \notin P\}$, conforme proposição 2.1.1. (b). Assim, $O_P := O$ é chamado o anel de valorização do lugar P ou o anel de valorização associado ao lugar P . Uma segunda descrição usual de lugares é dada em termos de valorizações.

Definição 2.1.4 Uma valorização discreta de F/K é uma função $v : F \rightarrow \mathbb{Z} \cup \{\infty\}$, possuindo as seguintes propriedades:

- (1) $v(x) = \infty \Leftrightarrow x = 0$.
- (2) $v(xy) = v(x) + v(y)$ para todos $x, y \in F$.
- (3) $v(x+y) \geq \min\{v(x), v(y)\}$ para todos $x, y \in F$.
- (4) Existe um elemento $z \in F$ com $v(z) = 1$.
- (5) $v(a) = 0$ para todo $0 \neq a \in K$.

Neste contexto, o símbolo ∞ representa algum elemento que não é um número inteiro, tal que $\infty + \infty = \infty + n = n + \infty = \infty$ e $\infty > m$ para todos m, n números inteiros.

Observe que a valorização discreta é uma função sobrejetora: de fato, por (1) temos $v(0) = \infty$; agora devido ao item número (4) existe um elemento $z \in F$ tal que $v(z) = 1$ e por (5)

qualquer elemento a não nulo em $K \subseteq F$ é tal que $v(a) = 0$; agora note que para $x \in F \setminus \{0\}$ temos $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$ e então $v(x^{-1}) = -v(x)$; assim para um número inteiro $p > 1$, podemos escrever $p = 1 + 1 + \dots + 1$ e então, por (4), $1 + \dots + 1 = v(z) + \dots + v(z)$ e por (2), $v(z) + \dots + v(z) = v(z^p)$ e portanto, $p = v(z^p)$ e $z^p \in F$ o que mostra que $\mathbb{N} \subseteq v(F)$; com isso $-p = -v(z^p) = -v(z) - \dots - v(z) = v(z^{-1}) + \dots + v(z^{-1}) = v(z^{-p})$ e então $-p = v(z^{-p})$. Logo, a valorização discreta v é uma função sobrejetora.

A propriedade (3) é chamada de desigualdade triangular. Uma versão mais forte desta desigualdade pode ser derivada dos axiomas da definição de valorização discreta e em geral é muito usada.

Lema 2.1.2 (Desigualdade Triangular Estrita) Seja v uma valorização discreta de F/K e $x, y \in F$ com $v(x) \neq v(y)$. Então, $v(x + y) = \min\{v(x), v(y)\}$.

Demonstração Para todo $0 \neq a \in K$, temos, pelos axiomas (2) e (5), que $v(ay) = v(a) + v(y) = 0 + v(y) = v(y)$, para todo $y \in F$. Em particular, para $a = -1$, segue que $v(-y) = v(y)$. Sendo $v(x) \neq v(y)$ assumimos, sem perda de generalidade, que $v(x) < v(y)$. Suponha que $v(x + y) \neq \min\{v(x), v(y)\} = v(x)$. Então, pelo axioma (3), $v(x + y) > \min\{v(x), v(y)\} = v(x)$ para todo $x, y \in F$; logo, $v(x + y) > v(x)$. Assim, por (3), vale o seguinte, $v(x) = v(x + y + (-y)) \geq \min\{v(x + y), v(-y)\} = \min\{v(x + y), v(y)\} > v(x)$. Daí, $v(x) > v(x)$, o que é um absurdo. ■

Podemos generalizar esta desigualdade. É o que veremos a seguir.

Teorema 2.1.2 (Desigualdade Triangular Estrita Generalizada) Seja uma valorização discreta v e consideremos os elementos $x_1, \dots, x_n$ com $v(x_1) < v(x_i)$, para $i = 2, \dots, n$. Então temos que, $v(x_1 + \dots + x_n) = v(x_1)$.

Demonstração Se tivermos x_1 e $x_2 \in F$, com $v(x_1) < v(x_2)$, recaímos no lema 2.1.2.. Suponha que o resultado é válido para $n > 2$. Seja $x_{n+1} \in F$ com $v(x_1) < v(x_{n+1})$. Suponha que $v(x_1 + \dots + x_n + x_{n+1}) \neq v(x_1)$. Dessa forma, temos que $v(x_1 + \dots + x_n + x_{n+1}) > \min\{v(x_1 + \dots + x_n), v(x_{n+1})\} = \min\{v(x_1), v(x_{n+1})\} = v(x_1)$; daí observamos o seguinte fato, $v(x_1) = v(x_1 + \dots + x_n + x_{n+1} - x_{n+1}) \geq \min\{v(x_1 + \dots + x_n + x_{n+1}), v(-x_{n+1})\} > v(x_1)$, o que é um absurdo. ■

Definição 2.1.5 Para qualquer lugar P do corpo de funções algébricas F/K , associamos a função $v_P : F \rightarrow \mathbb{Z} \cup \{\infty\}$, que vamos provar ser uma valorização discreta. Esta função é definida da seguinte maneira: escolha t um elemento primo para P ; pelo teorema 2.1.1., todo elemento z não nulo em F possui uma única representação $z = t^n u$, com $u \in O_P^* = O^*$ e $n \in \mathbb{Z}$. Definimos $v_P(z) := n$ e $v_P(0) := \infty$.

Observe que esta definição depende somente de P e não da escolha de t . De fato, se t' é outro elemento primo para P , então $P = tO = t'O$. Deste modo, $t \in t'O$ e então $t = t'a$,

com $a \in O_P$; como $t' \in tO$ segue que $t' = tb$, com $b \in O_P$. Logo, $t = tba$ e com isso devemos ter $ba = 1$. Portanto, $a \in O_P^*$. Então se temos $P = tO = t'O$ segue que $t = t'w$ para algum $w \in O_P^*$. Consequentemente, $z = t^n u$ com $u \in O_P^*$ implica que, $z = (t'^n w^n) u = t'^n (w^n u)$ com $w^n u \in O_P^*$. Notemos que $w^n u \in O_P^*$, pois como $w^n \in O_P^*$ existe $a_1 \in O_P$ tal que $w^n a_1 = 1$ e como $u \in O_P^*$ existe $a_2 \in O_P$ tal que $ua_2 = 1$, e com isso segue que $w^n a_1 u a_2 = 1$ o que implica $w^n u (a_1 a_2) = 1$, com $a_1 a_2 \in O_P$ e isso acarreta que $w^n u \in O_P^*$. Portanto, a definição de v_P depende somente de P e não da escolha de t .

Para provar que v_P é uma valorização discreta, provemos o seguinte teorema.

Teorema 2.1.3 Seja F/K um corpo de funções.

- (a) Para todo lugar P de F/K , a função v_P definida anteriormente é uma valorização discreta de F/K . Além disso, temos que $O_P = \{z \in F \mid v_P(z) \geq 0\}$, $O_P^* = \{z \in F \mid v_P(z) = 0\}$ e $P = \{z \in F \mid v_P(z) > 0\}$. Um elemento $x \in F$ é primo para P se, e somente se, $v_P(x) = 1$.
- (b) Reciprocamente, suponha que v é uma valorização discreta de F/K . Dessa forma, temos que $P := \{z \in F \mid v(z) > 0\}$ é um lugar de F/K e $O_P := \{z \in F \mid v(z) \geq 0\}$ é o correspondente anel de valorização.
- (c) Todo anel de valorização O de F/K é um subanel próprio maximal de F .

Demonstração (a) Verifiquemos se v_P é uma valorização discreta de F/K .

- (1) Temos que $v_P(0) := \infty$, logo, $v_P(x) = \infty \Leftrightarrow x = 0$.
- (2) Sendo $x, y \in F \setminus \{0\}$, temos $x = t^n u_1$ e $y = t^m u_2$, com $u_1, u_2 \in O_P^*$, $m, n \in \mathbb{Z}$. Assim, $xy = t^{n+m} (u_1 u_2)$, com $u_1 u_2 \in O_P^*$. Por definição, $v_P(xy) = n + m = v_P(x) + v_P(y)$.
- (3) Provemos agora que $v_P(x + y) \geq \min\{v_P(x), v_P(y)\}$. Para tanto, consideremos $x, y \in F$ não nulos, com $v_P(x) = n$ e $v_P(y) = m$. Podemos supor, sem perda de generalidade, que $n \leq m < \infty$ e assim temos $x = t^n u_1$ e $y = t^m u_2$, com $u_1, u_2 \in O_P^*$, onde $P = tO$ e t é um elemento primo para P . Então, $x + y = t^n u_1 + t^m u_2 = t^n (u_1 + t^{m-n} u_2) = t^n z$, com $z = u_1 + t^{m-n} u_2 \in O_P$. Se $z = 0$ então $x + y = 0$ e $v_P(x + y) = \infty > \min\{n, m\}$, pois por definição $\infty > p$, para todo $p \in \mathbb{Z}$. Caso contrário, pelo teorema 2.1.1. (b), temos que $z = t^k u$, com $u \in O_P^*$ e k um número inteiro. Note que se $k < 0$ teremos $z = \frac{1}{t^{-k}} u$ e então $1 = z(u^{-1} t^{-k})$ e desta forma $z^{-1} \in O_P$, de acordo com a proposição 2.1.1., o que não é possível pois já temos que $z \in O_P$ e este é anel de valorização. Logo, $k \geq 0$. Portanto, segue que $v_P(x + y) = v_P(t^n z) = v_P(t^{n+k} u) = n + k \geq n = \min\{v_P(x), v_P(y)\}$.
- (4) Tomando $z = tu$, temos que $v_P(z) = 1$.
- (5) Seja $0 \neq a \in K$ e então, como $K \subseteq O_P$, segue que $a \in O_P^*$. Logo, $a = t^0 a$ e daí $v_P(a) = 0$.

Mostramos assim que v_P é uma valorização discreta de F/K .

Agora, vamos mostrar que $O_P = \{z \in F \mid v_P(z) \geq 0\}$.

De fato, seja $z \neq 0$ em F e O_P o anel de valorização associado ao lugar P . Sendo $P = tO$, $t \neq 0$, temos que $z = t^n w$, com $w \in O_P^*$ e n um número inteiro. Suponha que $z \in O_P$ e mostremos que $n \geq 0$. De fato, note que se $0 \neq t \in P$ então $t^{-1} \notin O_P$, e assim $t^{-2} \notin O_P$, pois caso contrário teríamos $tt^{-2} = t^{-1} \in P$, pois P é ideal, logo 1 está em P e com isso segue que

$P = O_P$, absurdo. Por indução, $t^{-n} \notin O_P$ para qualquer $n \in \mathbb{N}$. Portanto, se em $z = t^n w$ com $w \in O_P^*$ temos $n < 0$, então $zw^{-1} = t^n \in O_P$, contrariando o que foi feito acima. Logo, $n \geq 0$, e disto $v_P(z) = n \geq 0$. Consequentemente, $O_P = \{z \in F \mid v_P(z) \geq 0\}$.

Também, $O_P^* = \{z \in F \mid v_P(z) = 0\}$. De fato, seja z não nulo em O_P^* ; daí, $z = t^0 z$ e então $v_P(z) = 0$. Como $P = O_P \setminus O_P^*$ segue que $P = \{z \in F \mid v_P(z) > 0\}$. Para concluir o item (a) mostremos que $x \in F$ é primo para P se, e somente se, $v_P(x) = 1$. Suponha que $x \in F$ é um elemento primo para P ; segue então que dado z não nulo em F , $z = x^n u$, $u \in O_P^*$ e $n \in \mathbb{Z}$, logo $v_P(z) = n$ e sendo $x^n = zu^{-1}$ temos $v_P(x^n) = v_P(z) + v_P(u^{-1}) = n + 0 = n$. Pelo axioma (2) da definição 2.1.4., temos $v_P(x^n) = nv_P(x)$. Portanto, se $n \neq 0$ temos $nv_P(x) = n$ o que implica $v_P(x) = 1$. Agora, se ocorrer $n = 0$, como $P = tO = xO$, com t elemento primo para P , temos que $x = tp$, com $p \in O_P^*$ e daí, $v_P(x) = 1$. Reciprocamente, suponha que $v_P(x) = 1$. Então, $x = tu$, onde t é elemento primo para P e $u \in O_P^*$. Com isso, segue que $P = tO = (tu)O = xO$ e por conseguinte, x é elemento primo para P .

(b) Suponha que v é uma valorização discreta e seja o conjunto $O_P := \{z \in F \mid v(z) \geq 0\}$. Assim, sejam $x, y, z \in F$, com $v(x), v(y), v(z) \geq 0$. Daí, $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$ e $v(xy) = v(x) + v(y) \geq 0$. Logo, $x+y$ e xy estão em O_P e então O_P é fechado para a adição e multiplicação de F . Seja agora 1_F o elemento neutro para a multiplicação de F . Assim, $v(1_F) = v(1_F \cdot 1_F) = v(1_F) + v(1_F) = 0 + 0 = 0$ e então $1_F \in O_P$. Seja 0_F o elemento neutro para a adição de F ; daí, $v(0_F) = \infty \geq 0$ e então 0_F está em O_P . Sendo $-x$ o oposto aditivo do elemento $x \in O_P$ temos que $v(-x) = v(-1_F) + v(x) = v(x) \geq 0$, mostrando com isso que $-x \in O_P$. Desta forma, O_P é um anel de F . Mostremos agora que O_P é um anel de valorização de F/K .

(1) Temos que para todo a não nulo em K , $v(a) = 0$; consequentemente $K \subseteq O_P$; como existe um elemento $z \in F$ com $v(z) = 1$ segue que $z \in O_P \setminus K$ e desta maneira K está contido em O_P propriamente. Notemos também que tomando $x \in O_P$ com $v(x) > 0$ segue que $0_F = v(1_F) = v(x) + v(x^{-1})$ o que implica que $v(x^{-1}) = -v(x) < 0$ e então $x^{-1} \notin O_P$, mostrando que F contém O_P propriamente.

(2) Suponha que exista $z \in F$ tal que z e $z^{-1} \in F \setminus O_P$. Daí, $v(z) < 0$ e $v(z^{-1}) < 0$ o que acarreta que $0 > v(z) + v(z^{-1}) = v(z z^{-1}) = v(1_F) = 0_F$, o que é absurdo. Portanto, vale que para qualquer $z \in F$, $z \in O_P$ ou $z^{-1} \in O_P$.

De (1) e (2), segue que O_P é um anel de valorização de F/K . Para finalizar este item, vamos mostrar que $P := \{z \in F \mid v(z) > 0\}$ é ideal maximal de O_P , mostrando então que é um lugar de F/K tendo O_P como anel de valorização. Sendo $x \in P$ e $y \in O_P$ temos que $v(xy) = v(x) + v(y) > 0$ e então $xy \in P$. Agora, se x e z estão em P segue que $v(x+z) \geq \min\{v(x), v(z)\} > 0$, e assim $x+z \in P$. Mostramos então que P é um ideal de O_P . Observamos que P é um ideal maximal. De fato, seja I um ideal de O_P tal que P está contido em I propriamente. Desta forma, temos que existe $t \in I$ com $v(t) = 0$. Assim, $t^{-1} \in O_P$, pois do contrário teríamos $v(t^{-1}) < 0$ e então $0 > v(t^{-1}) + v(t) = v(t^{-1}t) = v(1) = 0$, o que é um absurdo. Com isso, segue que $tt^{-1} \in I$ e então $1 \in I$; consequentemente, $I = O_P$.

Logo, P é ideal maximal de O_P . Também, P é o único ideal maximal de O_P . De fato, se existe Q outro ideal maximal de O_P tal que P está contido em Q propriamente, segue que existe $x \in Q$ tal que $v(x) = 0$. Da mesma forma como feito anteriormente, temos que $Q = O_P$.

(c) Seja O qualquer anel de valorização de F/K . Considere P o ideal maximal de O , v_P valorização discreta associada à P e z um elemento em $F \setminus O$. Vamos mostrar que $F = O[z]$. Para este fim, considere um elemento arbitrário $y \in F$. Como $z^{-1} \in O$ e, pelo item (a), $v(z^{-1}) \geq 0$ com $z \in O$, segue que $v(z^{-1}) \neq 0$ e assim $v(z^{-1}) > 0$. Portanto, $z^{-1} \in P = tO$ e então $z^{-1} = tp$, com $p \in O$ e t elemento primo para P . Assim, para $k \geq 0$ suficientemente grande, obtemos que $v_P(yz^{-k}) = v_P(y(tp)^k) = v_P(y) + kv_P(tp) = v_P(y) + k(1 + v_P(p)) \geq v_P(y) + k$, pois $v_P(p) \geq 0$. Chamando $w = yz^{-k}$ temos que $w \in O$ e daí $y = wz^k$ o que implica que $y \in O[z]$. Assim, $F \subset O[z]$ e como $O[z] \subset F$ segue que $F = O[z]$. Portanto, O é anel próprio maximal de F . ■

O teorema 2.1.3. nos diz que lugares, anéis de valorização e valorizações discretas de um corpo de funções algébricas F/K são essencialmente a mesma coisa.

Observação 2.1.2 Sendo O_P um anel, uma relação R sobre O_P é um subconjunto de $O_P \times O_P$. Sendo P um ideal de O_P , este já define uma relação de equivalência sobre O_P , que é a seguinte: $(a, b) \in R \Leftrightarrow b - a \in P$. O anel de classes de resíduos é O_P/P e sendo P ideal maximal, O_P/P é um corpo. Para $a \in O_P$ temos que a classe de equivalência de a é denotada e definida por $\bar{a} := \{b \in O_P \mid (a, b) \in R\} = \{a + x \mid x \in P\}$. Para $x \in O_P$ definimos $x(P) \in O_P/P$ como a classe de resíduos de x módulo P ; agora para $x \in F \setminus O_P$, tomamos $x(P) = \infty$. Note que o símbolo ∞ é definido aqui de uma maneira diferente como usado na definição 2.1.4.. Pela proposição 2.1.1., sabemos que $\tilde{K} \subseteq O_P$ e $\tilde{K} \cap P = \{0\}$, logo $K \cap P = \{0\}$, uma vez que $K \subseteq \tilde{K}$. Também, a aplicação de classes de resíduos $O_P \rightarrow O_P/P$ induz um mergulho de K em O_P/P . Consideramos sempre que K é um subcorpo de O_P/P via este mergulho. Observe que este argumento também se aplica para $\tilde{K}$ em vez de K e então podemos considerar $\tilde{K}$ como subcorpo de O_P/P .

Definição 2.1.6 Seja P um lugar de F/K .

(a) $\mathbb{F}_P := O_P/P$ é o corpo de classes de resíduos de P . A aplicação $x \mapsto x(P)$ de F para $\mathbb{F}_P \cup \{\infty\}$ é chamada de aplicação de classes de resíduos com respeito à P . Às vezes também se usa a notação $x(P) := x + P$, para $x \in O_P$.

(b) $\text{grau}(P) := [\mathbb{F}_P : K]$ é chamado o grau de P .

O grau de um lugar P é sempre finito. Mais precisamente, temos o seguinte resultado.

Proposição 2.1.2 Se P é um lugar de F/K e $0 \neq x \in P$, então $\text{grau}(P) \leq [F : K(x)] < \infty$.

Demonstração Primeiramente, note que como $0 \neq x \in P$ e $\tilde{K} \cap P = \{0\}$, segue que $x \notin \tilde{K}$. Logo, $x \in P$ é transcendente sobre K . Pela observação 2.1.1., temos que $[F : K(x)] < \infty$. Vamos então mostrar que $[O_P/P : K] \leq [F : K(x)]$. Para tanto, é suficiente mostrar que

quaisquer elementos $z_1, \dots, z_n \in O_P$, cujas classes de resíduos $z_1(P), \dots, z_n(P) \in O_P/P$ são linearmente independentes sobre K , são linearmente independentes sobre $K(x)$. Observe que dizer que $z_1(P), \dots, z_n(P)$ são linearmente independentes sobre K , significa que tomando $x_1 \in z_1(P), \dots, x_n \in z_n(P)$, temos que $x_1, \dots, x_n$ são linearmente independentes sobre K . Então como $z_1 \in z_1(P), \dots, z_n \in z_n(P)$ e $z_1, \dots, z_n$ são linearmente independentes sobre K , mostremos que $z_1, \dots, z_n$ são linearmente independentes sobre $K(x)$.

Suponha que $z_1, \dots, z_n$ não são linearmente independentes sobre $K(x)$, ou seja, existe uma combinação linear não trivial de $z_1, \dots, z_n$ igual à zero, digamos $\sum_{i=1}^n \Phi_i z_i = 0$, com Φ_i em $K(x)$. Sem perda de generalidade, assumimos que os Φ_i são expressões polinomiais em x e nem todas elas são divisíveis por x , isto é, $\Phi_i = a_i + xg_i$, com $a_i \in K$, $g_i \in K(x)$, com nem todos os $a_i = 0$ (note que podemos supor isto uma vez que se $\Phi_i = xg_i$, para todo i , temos $\sum_{i=1}^n xg_i z_i = 0$ o que implica $\sum_{i=1}^n g_i z_i = 0$, e assim bastaria substituir Φ_i por g_i). Como $x \in P$ e $g_i \in O_P$, uma vez que $K(x) \subset O_P$, segue que $xg_i \in P$. Logo $\Phi_i - a_i \in P$ e então $\Phi_i(P) = a_i(P) = a_i$. Em $\sum_{i=1}^n \Phi_i z_i = 0$ aplicamos a função de classes de resíduos, obtendo deste modo que $0 = 0(P) = \sum_{i=1}^n \Phi_i(P) z_i(P)$ o que acarreta $\sum_{i=1}^n a_i z_i(P) = 0$. Como, para algum i , temos $a_i \neq 0$ segue que $z_1(P), \dots, z_n(P)$ são linearmente dependentes, o que contraria $z_1, \dots, z_n$ serem linearmente independentes sobre K . Portanto, $z_1, \dots, z_n$ são linearmente independentes sobre $K(x)$ e então $[F : K(x)] \geq [O_P/P : K]$. ■

Corolário 2.1.1 O corpo $\tilde{K} = \{z \in F \mid z \text{ é algébrico sobre } K\}$ de constantes de F/K é uma extensão de corpos finita de K .

Demonstração Usaremos o fato de que o conjunto dos lugares de F/K não é vazio, fato este que será provado no final desta seção. Escolhemos então algum lugar P de F/K . Como dito anteriormente, usando a aplicação de classes de resíduos $O_P \rightarrow O_P/P$, consideramos $\tilde{K}$ como subcorpo de O_P/P . Pelo teorema anterior, temos $[O_P/P : K] \leq [F : K(x)] < \infty$, para x não nulo em P . Dessa forma, temos $[O_P/P : \tilde{K}] < \infty$. Segue disto que $\tilde{K}/K$ é uma extensão de corpos finita. ■

Observação 2.1.3 Para o caso quando $\text{grau}(P) = 1$, temos $O_P/P = K$ e a aplicação de classes de resíduos leva F em $K \cup \{\infty\}$. Em particular, se K é um corpo algebricamente fechado então K não possui extensão algébrica, e assim todo lugar possui grau um. Nesse caso, podemos representar um elemento $z \in F$ como uma função $z : \mathbb{P}_F \rightarrow K \cup \{\infty\}$, $P \mapsto z(P)$. Isto é o porque de F/K ser chamado de corpo de funções. Os elementos de K interpretados como funções no sentido acima, são funções constantes. Por essa razão K é chamado o corpo de funções constantes de F .

Definição 2.1.7 Seja $z \in F$ e P um lugar de F/K . Dizemos que P é um zero de z se, e somente se, $v_P(z) > 0$; P é um pólo de z se, e somente 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 .

Neste momento, é conveniente verificarmos a questão de saber se sempre existem lugares de um corpo de funções algébricas F/K .

Teorema 2.1.4 Seja F/K um corpo de funções algébricas e R um subanel de F , com $K \subseteq R \subseteq F$. Suponha que I é um ideal não nulo próprio de R . Então, existe um lugar P de F/K tal que $I \subseteq P$ e $R \subseteq O_P$, onde O_P é o anel de valorização correspondente.

Demonstração Ver referência [12], Teorema I.1.18.. ■

Corolário 2.1.2 Seja F/K um corpo de funções algébricas e $z \in F$ transcendente sobre K . Então, z possui pelo menos um zero e um pólo. Em particular, $\mathbb{P}_F \neq \emptyset$.

Demonstração Considere o anel $R = K[z]$; assim $I = zK[z]$ é ideal de R . De fato, $I \neq \emptyset$, pois $z \in I$, uma vez que $z = z1$ com $1 \in K \subset K[z]$ e dados $x, y \in I$ temos que $x = zf$ e $y = zg$, $f, g \in K[z]$ e com isso $x + y = z(f + g) \in I$; sendo $x \in I$ e $g \in R$, segue que $x = zf$, com $f \in K[z]$ e $xg = zfg$, com $fg \in K[z]$ logo, $xg \in I$ e disto I é ideal de R . Portanto, temos o anel R de F , com $K \subseteq R \subseteq F$ e I ideal próprio não nulo de R . O teorema 2.1.4. garante que existe um lugar P de F/K tal que $I \subseteq P$ e $R \subseteq O_P$. Como $z \in I$ segue $z \in P$. Pelo teorema 2.1.3. (a), temos $P = \{z \in F \mid v_P(z) > 0\}$, e então P é um zero de z . Sendo z transcendente sobre K , segue que z^{-1} também o é; tomamos então $K[z^{-1}]$ anel de F e $zK[z^{-1}]$ ideal de $K[z^{-1}]$, e assim existe Q um lugar de F/K tal que $z^{-1} \in Q$. Então, $z \notin O_Q = \{x \in F \mid v_Q(x) \geq 0\}$. Logo, $v_Q(z) < 0$ e Q é um pólo de z . ■

2.2 O corpo de funções algébricas racional

Para uma melhor compreensão de valorizações e lugares de um corpo de funções algébricas arbitrário, é indispensável se ter uma idéia precisa para estas noções no caso mais simples. Por esta razão vamos ver estes conceitos no caso do corpo de funções algébricas racional, quando $F = K(x)$, onde x é transcendente sobre K . Dado um polinômio arbitrário $p(x) \in K[x]$, mônico e irredutível, considere o anel de valorização

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in K(x) \mid f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\},$$

de $K(x)/K$ com ideal maximal sendo dado por:

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \text{ divide } f(x), p(x) \text{ não divide } g(x) \right\}.$$

No início da seção 2.1. verificamos que $O_{p(x)}$ é um anel de valorização. No caso particular quando $p(x)$ é um polinômio linear, isto é, $p(x) = x - \alpha$, com $\alpha \in K$, podemos abreviar e escrever $P_\alpha = P_{x-\alpha} \in \mathbb{P}_{K(x)}$. Há um outro anel de valorização de $K(x)/K$, a saber

$$O_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \text{ grau}(f(x)) \leq \text{grau}(g(x)) \right\},$$

com ideal maximal dado por:

$$P_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \text{grau}(f(x)) < \text{grau}(g(x)) \right\}.$$

De fato, O_∞ é um anel de valorização: temos que $K \subset O_\infty$ pois dado $a \in K$ segue que $a = \frac{a}{1} \in O_\infty$ visto que $\text{grau}(a) = 0 = \text{grau}(1)$ e $K \neq O_\infty$ uma vez que $\frac{1}{x} \in O_\infty$ mas não está em K , pois caso contrário teríamos que $x \in K$ o que acarreta que x é algébrico sobre K , contra a hipótese de x ser transcendente sobre K . Também, $O_\infty \neq K(x)$ uma vez que $x \in K(x)$ e não pertence à O_∞ , pois caso contrário teríamos $\text{grau}(1) \geq \text{grau}(x)$. Agora, seja $z = \frac{f(x)}{g(x)} \in K(x)$ e suponha que $z \notin O_\infty$, ou seja, suponha que $\text{grau}(f(x)) > \text{grau}(g(x))$; assim, segue que $z^{-1} = \frac{g(x)}{f(x)} \in O_\infty$, uma vez que $\text{grau}(g(x)) < \text{grau}(f(x))$. Portanto, O_∞ é um anel de valorização. O lugar P_∞ é chamado o lugar infinito de $K(x)$. Observe que estes rótulos dependem da escolha específica do elemento x que origina $K(x)/K$. Por exemplo, $K(x) = K(\frac{1}{x})$, e o lugar infinito com respeito a $\frac{1}{x}$ é o lugar P_0 com respeito a x . Note que $P_\infty := \left\{ \frac{f(\frac{1}{x})}{g(\frac{1}{x})} \mid f(\frac{1}{x}), g(\frac{1}{x}) \in K[\frac{1}{x}], \text{grau}(f(\frac{1}{x})) < \text{grau}(g(\frac{1}{x})) \right\}$ que pode ser visto como,
$$\left\{ \frac{a_0 + a_1 \frac{1}{x} + \dots + a_n (\frac{1}{x})^n}{b_0 + b_1 \frac{1}{x} + \dots + b_m (\frac{1}{x})^m} \mid b_m \neq 0, m > n \right\} = \left\{ \frac{(\frac{1}{x})^n (a_0 x^n + \dots + a_n)}{(\frac{1}{x})^m (b_0 x^m + \dots + b_m)} \mid b_m \neq 0, m > n \right\}.$$

$$\text{Portanto, } P_\infty = \left\{ x^{m-n} \frac{\tilde{f}(x)}{\tilde{g}(x)} \mid x \text{ não divide } \tilde{g}(x), m > n \right\} = P_0.$$

Proposição 2.2.1 Seja $F = K(x)$ e $K(x)/K$ o corpo de funções racional.

(a) Seja $P = P_{p(x)}$ o lugar de $K(x)/K$ dado por

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \text{ divide } f(x), p(x) \text{ não divide } g(x) \right\},$$

onde $p(x) \in K[x]$ é um polinômio irredutível. Então $p(x)$ é um elemento primo para P , e a valorização discreta correspondente v_P pode ser descrita como a seguir: se $z \in K(x) \setminus \{0\}$ é escrito na forma $z = p(x)^n \left(\frac{f(x)}{g(x)} \right)$, com $n \in \mathbb{Z}, f(x), g(x) \in K[x]$ com $p(x)$ não dividindo $f(x)$ e $g(x)$, então definimos $v_P(z) = n$. O corpo de classes de resíduos $\mathbb{F}_P = O_P/P$ é isomorfo a $K[x]/(p(x))$, e o isomorfismo é dado por $\Theta : K[x]/(p(x)) \rightarrow O_P/P, \Theta(f(x) \bmod p(x)) = f(x)(P)$. Consequentemente, o grau do lugar P é igual ao grau de $p(x)$.

(b) No caso especial em que $p(x) = x - \alpha$, com $\alpha \in K$, o grau do lugar $P = P_\alpha$ é igual a um, e a aplicação de classes de resíduos é dada por $z(P) = z(\alpha)$, para $z \in K(x)$, onde definimos $z(\alpha)$ da seguinte maneira: escreva $z = \frac{f(x)}{g(x)}$ com polinômios $f(x), g(x) \in K[x]$ relativamente primos. Então, $z(\alpha) = \frac{f(\alpha)}{g(\alpha)}$, se $g(\alpha) \neq 0$ e $z(\alpha) = \infty$, se $g(\alpha) = 0$.

(c) Finalmente, seja $P = P_\infty$ o lugar infinito de $K(x)/K$ dado por

$$P_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \text{grau}(f(x)) < \text{grau}(g(x)) \right\}.$$

Então o grau de P_∞ é igual a um. Um elemento primo para P_∞ é $t = \frac{1}{x}$. A correspondente valorização discreta v_∞ é dada por $v_\infty \left(\frac{f(x)}{g(x)} \right) = \text{grau}(g(x)) - \text{grau}(f(x))$, onde $f(x), g(x) \in K[x]$. A aplicação de classes de resíduos correspondente para P_∞ é determinada por $z(P_\infty) = z(\infty)$, para $z \in K(x)$, onde $z(\infty)$ é definido como usual: se $z = \frac{a_n x^n + \dots + a_0}{b_m x^m + \dots + b_0}$, com $a_n, b_m \neq 0$

então $z(\infty) = \frac{a_n}{b_m}$, se $n = m$; $z(\infty) = 0$, se $n < m$; $z(\infty) = \infty$, se $n > m$.

(d) K é todo o corpo de constantes de $K(x)/K$.

Demonstração Ver referência [12], Proposição I.2.1.. ■

Teorema 2.2.1 Não há lugares do corpo de funções racional $K(x)/K$ diferentes dos lugares $P_{p(x)}$ e P_∞ , como definidos no início desta seção.

Demonstração Caso 1: Dado um lugar P do corpo de funções algébricas racional tal que $P \neq P_\infty$, mostremos que existe um polinômio irredutível $p(x) \in K[x]$ tal que $O_{p(x)} = O_P$. Assumimos que $x \in O_P$ sendo O_P o anel de valorização de $K(x)/K$ associado ao lugar P . Como $K \subset O_P$ e O_P é um anel, temos $K[x] \subseteq O_P$. Seja $I = K[x] \cap P$ e note que $I \neq \emptyset$, uma vez que $\{0\} \subset I$. Temos que I é um ideal de $K[x]$. De fato, sendo $z, w \in I$ segue $z, w \in P$ e como P é ideal de O_P , $z + w \in P$; logo $z + w \in I$; também para $z \in K[x]$ e $w \in I$, temos que $z \in O_P$ e $w \in P$ e daí $zw \in P$. Portanto, I é ideal de $K[x]$. Além disso, I é um ideal primo de $K[x]$. A aplicação de classes de resíduos que leva $K(x)$ em $O_P/P \cup \{\infty\}$ induz um mergulho de $K[x]$ em O_P/P e consequentemente mergulha $K[x]/I$ em O_P/P . Pela proposição 2.1.2. temos que $[O_P/P : K]$ é finito, logo $[K[x]/I : K]$ também é finito e então $I \neq \{0\}$, uma vez que se $I = \{0\}$ teríamos $K[x]/I = K[x]$ e $[K[x] : K]$ não é finito. Segue que existe, e é determinado unicamente, um polinômio mônico irredutível $p(x) \in K[x]$ tal que $I = K[x] \cap P = p(x)K[x]$. A afirmação anterior decorre do fato de que todo ideal primo de anel de polinômios possui um único gerador mônico irredutível. Qualquer $g(x) \in K[x]$ com $p(x)$ não dividindo $g(x)$ é tal que não pertence à I ; logo devemos ter que $g(x)$ não está em P e disto segue que $\frac{1}{g(x)} \in O_P$, pela proposição 2.1.1.. Concluimos que $O_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in K(x) \mid f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\} \subset O_P$.

Pelo teorema 2.1.3. (c), anéis de valorização são subanéis próprios maximais de $K(x)$; segue então que $O_P = O_{p(x)}$ e consequentemente $P = P_{p(x)}$.

Caso 2: Suponhamos agora que $x \notin O_P$. Pela proposição 2.1.1. temos que $x^{-1} \in P$ e então $x^{-1} \in P \cap K[x^{-1}]$, com $K[x^{-1}] \subseteq O_P$, pois O_P é um anel. Temos também $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$. De fato, temos que $P \cap K[x^{-1}] = p(x^{-1})K[x^{-1}]$, onde $p(x^{-1}) \in K[x^{-1}]$. Como $x^{-1} \in P \cap K[x^{-1}]$, segue que $p(x^{-1}) \mid x^{-1}$. No entanto, os únicos divisores em $K[x^{-1}]$ de x^{-1} são x^{-1} e 1. Se temos $p(x^{-1}) = 1$ então $1 \in P$ e logo $P = O_P$, o que é absurdo. Portanto, devemos ter $p(x^{-1}) = x^{-1}$ e daí, $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$. Todo $g(x^{-1}) \in K[x^{-1}]$, com x^{-1} não dividindo $g(x^{-1})$, não está em I . Assim $g(x^{-1}) \notin P$ e $\frac{1}{g(x^{-1})} \in O_P$, pela proposição 2.1.1.. Então, O_P é tal que contém o seguinte conjunto

$$\left\{ \frac{f(x^{-1})}{g(x^{-1})} \mid f(x^{-1}), g(x^{-1}) \in K[x^{-1}] \text{ com } x^{-1} \text{ não dividindo } g(x^{-1}) \right\},$$

que é igual ao conjunto $\left\{ \frac{a_0 + a_1 x^{-1} + \dots + a_n x^{-n}}{b_0 + b_1 x^{-1} + \dots + b_m x^{-m}} \mid b_0 \neq 0 \right\} = \left\{ \frac{a_0 x^{m+n} + \dots + a_n x^m}{b_0 x^{m+n} + \dots + b_m x^n} \mid b_0 \neq 0 \right\}$, que por sua vez pode ser visto como $\left\{ \frac{u(x)}{v(x)} \mid u(x), v(x) \in K[x], \text{ grau}(u(x)) \leq \text{grau}(v(x)) \right\} = O_\infty$.

Como anéis de valorização são subanéis próprios maximais de $K(x)$, segue que $O_P = O_\infty$ e daí $P = P_\infty$. ■

Corolário 2.2.1 Os lugares de $K(x)/K$ de grau igual a um estão em correspondência biunívoca com $K \cup \{\infty\}$.

Demonstração Pelo teorema 2.2.1., os únicos lugares de $K(x)/K$ são $P_{p(x)}$ e P_∞ . Pela proposição 2.2.1., temos que $\text{grau}(P_\infty) = 1$ e $\text{grau}(P_{x-\alpha}) = 1$, com $\alpha \in K$. Se $P = P_{x-\alpha}$, o item (b) da proposição 2.2.1. diz que $K(x)$ está em correspondência biunívoca com $K \cup \{\infty\}$ e assim $P = P_{x-\alpha}$ também está. Se $P = P_\infty$, o item (c) da proposição 2.2.1. garante que P_∞ está em correspondência biunívoca com $K \cup \{\infty\}$. ■

2.3 Independência de Valorizações

O principal resultado desta seção é o denominado Teorema da Aproximação Fraca, o qual é também referido como Teorema de Independência. Vimos anteriormente que o conjunto dos lugares de F/K não é vazio; daremos uma consequência do Teorema da Aproximação Fraca que é um resultado neste mesmo sentido.

Teorema 2.3.1 (Teorema da Aproximação Fraca) Sejam F/K um corpo de funções e $P_1, \dots, P_n$ lugares dois a dois distintos de F/K ; sejam $x_1, \dots, x_n \in F$ e $r_1, \dots, r_n \in \mathbb{Z}$. Então, existe algum elemento $x \in F$ tal que $v_{P_i}(x - x_i) = r_i$, para $i = 1, \dots, n$.

Demonstração Ver referência [12], Teorema I.3.1.. ■

Corolário 2.3.1 Qualquer corpo de funções possui uma quantidade infinita de lugares.

Demonstração Seja F/K um corpo de funções algébricas e suponha que este possua um número finito de lugares, digamos $P_1, \dots, P_n$. Tome $r_i > 0$ e $x_i = 0$, para todo $i = 1, \dots, n$. Pelo teorema da Aproximação Fraca, existe um elemento $x \in F \setminus \{0\}$ tal que $v_{P_i}(x) = r_i$, para todo $i = 1, \dots, n$. Dessa forma, $v_{P_i}(x) > 0$, para todo $i = 1, \dots, n$; logo este elemento $x \neq 0$ é transcendente sobre K , uma vez que $x \in P_i$ e $P_i \cap \tilde{K} = \{0\}$, $\forall i = 1, \dots, n$. Como x é transcendente, pelo corolário 2.1.2., x possui pelo menos um pólo. Assim, existe um lugar Q tal que $v_Q(x) < 0$. Contradição, pois para todo lugar P de F/K temos que $v_P(x) > 0$. Portanto, todo corpo de funções possui infinitos lugares. ■

Mais adiante, na seção 2.4, provaremos que um elemento $x \in F$ que é transcendente sobre K possui muitos pólos e zeros, já contados sem repetição. Um importante passo na direção deste resultado é a próxima proposição que está no mesmo contexto do lema 2.1.1. e da proposição 2.1.2..

Proposição 2.3.1 Seja F/K um corpo de funções algébricas e $P_1, \dots, P_r$ zeros do elemento $x \in F$. Então, $\sum_{i=1}^r v_{P_i}(x) \cdot \text{grau}(P_i) \leq [F : K(x)]$.

Demonstração Ver referência [12], Proposição I.3.3.. ■

Corolário 2.3.2 Em um corpo de funções algébricas F/K , qualquer elemento $0 \neq x \in F$ possui um número finito de zeros e pólos.

Demonstração Seja $0 \neq x \in F$. Se x é algébrico sobre K temos que $x \in \tilde{K}$. Como $\tilde{K} \cap P = \{0\}$, segue que $x \notin P$. Logo, $v_P(x) \leq 0$. Também temos que $\tilde{K} \subseteq O_P$ e então $x \in O_P$ o que implica que $v_P(x) \geq 0$. Portanto, $0 \leq v_P(x) \leq 0$ e assim $v_P(x) = 0$ o que acarreta que x não possui nem zeros e nem pólos. Se x é transcendente sobre K então $[F : K(x)] < \infty$ e pela proposição 2.3.1. o número de zeros de x é inferior ou igual à $[F : K(x)]$. Portanto, o número de zeros de x é finito. Além disso, o número de zeros de x^{-1} é menor ou igual à $[F : K(x^{-1})] < \infty$, e como os zeros de x^{-1} são pólos de x , segue que x possui um número finito de pólos. ■

2.4 Divisores

O corpo $\tilde{K}$ de constantes do corpo de funções algébricas F/K é uma extensão finita do corpo K , conforme visto no corolário 2.1.1., e $F/\tilde{K}$ é um corpo de funções algébricas de uma variável sobre $\tilde{K}$. Vamos assumir de agora em diante que K é todo o corpo de constantes de F/K , ou seja, assumimos que $K = \{z \in F \mid z \text{ é algébrico sobre } K\}$, isto é, K é algebricamente fechado em F .

Definição 2.4.1 O grupo abeliano livre que possui como base livre os lugares de F/K será denotado por $\mathbb{D}_F$. Ele é chamado de o grupo de divisores de F/K . Os elementos únicos de $\mathbb{D}_F$ são chamados divisores de F/K . Em outras palavras, um divisor é uma soma formal $D = \sum_{P \in \mathbb{P}_F} n_P P$, com $n_P \in \mathbb{Z}$ e quase todos $n_P = 0$, isto é, $n_P \neq 0$ em um número finito de parcelas dessa soma.

O suporte do elemento $D \in \mathbb{D}_F$ é definido por $\text{supp}(D) := \{P \in \mathbb{P}_F \mid n_P \neq 0\}$. Frequentemente é conveniente estabelecer a escrita $D = \sum_{P \in \mathbb{S}} n_P P$, onde $\mathbb{S} \subseteq \mathbb{P}_F$ é um subconjunto finito de $\mathbb{P}_F$, com $\text{supp}(D) \subseteq \mathbb{S}$. Um divisor da forma $D = P$, com P um lugar de F/K é chamado um divisor primo. Dois divisores D e D' , com $D = \sum n_P P$ e $D' = \sum n'_P P$ são somados da seguinte maneira: $D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P$.

O elemento neutro para a soma do grupo de divisores $\mathbb{D}_F$ é o divisor $0 = \sum_{P \in \mathbb{P}_F} r_P P$, com todo $r_P = 0$. Para Q um lugar e D um divisor de F/K , onde $D = \sum_{P \in \mathbb{P}_F} n_P P$, definimos $v_Q(D) = n_Q$ e portanto, $\text{supp}(D) = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\}$ e $D = \sum_{P \in \text{supp}(D)} v_P(D) P$.

Observação 2.4.1 Uma relação de ordem parcial em $\mathbb{D}_F$ é definida por

$$D_1 \leq D_2 :\Longleftrightarrow v_P(D_1) \leq v_P(D_2), \text{ para todo lugar } P \text{ de } F/K.$$

Um divisor $D \geq 0$, isto é $v_P(D) \geq 0 \forall$ lugar P , é chamado positivo ou efetivo. O grau de um divisor é definido como sendo $\text{grau}(D) = \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \text{grau}(P)$. Pelo corolário 2.3.2. todo elemento não nulo $x \in F$ possui uma quantidade finita de zeros e pólos em $\mathbb{P}_F$. Dessa forma a seguinte definição faz sentido.

Definição 2.4.2 Seja $0 \neq x \in F$ e denotemos por Z , respectivamente N , o conjunto de zeros, e o conjunto de pólos, de x em $\mathbb{P}_F$. Então definimos:

$(x)_0 := \sum_{P \in Z} v_P(x) P$, o divisor de zeros de x ; $(x)_\infty := \sum_{P \in N} -v_P(x) P$, o divisor de pólos de x ; $(x) := (x)_0 - (x)_\infty$, o divisor principal de x .

Como $v_P(x) > 0$ para todo $P \in Z$ segue que $(x)_0 \geq 0$, e como $v_P(x) < 0$ para todo $P \in N$ temos $-v_P(x) > 0$, e então $(x)_\infty \geq 0$; também $(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P$. Os elementos $0 \neq x \in F$ que são constantes são caracterizados por: $x \in K \iff (x) = 0$. De fato, se $x \in K = \tilde{K}$ segue que $x \notin P$, visto que $x \neq 0$ e $\tilde{K} \cap P = \{0\}$; logo $x \in O_P^*$ e portanto, $v_P(x) = 0$ para todo lugar P e disto temos $(x) = 0$. Reciprocamente, se $(x) = 0$ então $v_P(x) = 0$, para todo lugar P de F/K e assim x não é transcendente sobre K , pois se fosse teria pelo menos um zero e um pólo. Logo, $x \in \tilde{K} = K$.

Definição 2.4.3 O conjunto $P_F := \{(x) \mid 0 \neq x \in F\}$, é chamado o grupo de divisores principais de F/K . Este é um subgrupo de $\mathbb{D}_F$, pois para x e $y \in F$, não nulos, note que

$$(x) + (y) = \sum_{P \in \mathbb{P}_F} v_P(x) P + \sum_{P \in \mathbb{P}_F} v_P(y) P = \sum_{P \in \mathbb{P}_F} (v_P(x) + v_P(y)) P = \sum_{P \in \mathbb{P}_F} v_P(xy) P = (xy).$$

O grupo quociente $\mathbb{C}_F := \mathbb{D}_F / P_F$ é chamado de grupo das classes de divisores. Para um divisor $D \in \mathbb{D}_F$, o correspondente elemento no grupo quociente $\mathbb{C}_F$ é denotado por $[D]$, a classe do divisor D . Dois divisores D e D' em $\mathbb{D}_F$ são ditos serem equivalentes, e escrevemos $D \equiv D'$, se $[D] = [D']$, isto é, $D = D' + (x)$ para algum elemento $x \in F \setminus \{0\}$. Temos que, $D \equiv D' \iff [D] = [D']$, é uma relação de equivalência.

A próxima definição é fundamental na teoria de corpos de funções algébricas.

Definição 2.4.4 Para um divisor $A \in \mathbb{D}_F$ definimos, $\mathcal{L}(A) := \{x \in F \mid (x) + A \geq 0\} \cup \{0\}$.

Observação 2.4.2 Seja $A \in \mathbb{D}_F$. Então:

- (a) $x \in \mathcal{L}(A)$ se, e somente se, $v_P(x) + v_P(A) \geq 0$, para todo lugar P de F/K .
- (b) $\mathcal{L}(A) \neq \{0\}$ se, e somente se, existe um divisor $A' \equiv A$, com $A' \geq 0$.

Demonstração (a) Sejam P um lugar de F/K qualquer e $A = \sum_{P \in \text{supp}(A)} v_P(A) P$. Se $v_P(x) + v_P(A) \geq 0$ então $\sum_{P \in \text{supp}(A)} v_P(x) P \geq -\sum_{P \in \text{supp}(A)} v_P(A) P = -A$; assim, obtemos que $\sum_{P \in \mathbb{P}_F} v_P(x) P \geq -A$, ou seja, $(x) + A \geq 0$ e assim $x \in \mathcal{L}(A)$. Reciprocamente, seja $x \in \mathcal{L}(A)$; se $x = 0$, temos $v_P(0) = \infty \geq -n_P = -v_P(A)$, para $n_P \in \mathbb{Z}$, e então $v_P(x) + v_P(A) \geq 0$;

se $x \neq 0$, como $(x) + A \geq 0$ segue que $v_P((x) + A) \geq 0$ e sendo $v_P((x) + A) = v_P(x) + v_P(A)$, concluímos a demonstração.

(b) Se $\mathcal{L}(A) \neq \{0\}$ então existe $0 \neq x \in \mathcal{L}(A)$; logo $(x) + A \geq 0$ e então $A \equiv A'$ com $A' = (x) + A \geq 0$. Reciprocamente, se $A' \equiv A$ com $A' \geq 0$ então $A' = (x) + A \geq 0$, para $x \in F \setminus \{0\}$; segue que $0 \neq x \in \mathcal{L}(A)$ e então $\mathcal{L}(A) \neq \{0\}$, concluindo a demonstração. ■

Lema 2.4.1 Seja $A \in \mathbb{D}_F$. Então temos:

(a) $\mathcal{L}(A)$ é um espaço vetorial sobre o corpo K .

(b) Se A' é um divisor equivalente a A então $\mathcal{L}(A)$ e $\mathcal{L}(A')$ são K -espaços vetoriais isomorfos, e escrevemos $\mathcal{L}(A) \cong \mathcal{L}(A')$.

Demonstração (a) Basta mostrar que $\mathcal{L}(A)$ é um subespaço vetorial de F . Sejam $x, y \in \mathcal{L}(A)$ e $a \in K$, não nulo. Dessa forma, para qualquer lugar P de F/K temos

$$v_P(ax + y) \geq \min\{v_P(ax), v_P(y)\} = \min\{v_P(x), v_P(y)\},$$

uma vez que $v_P(ax) = v_P(a) + v_P(x)$ e como $0 \neq a \in K$ segue que $v_P(a) = 0$. Pela observação 2.4.1. (a), sabemos que $v_P(x) \geq -v_P(A)$ e $v_P(y) \geq -v_P(A)$. Logo, obtemos $\min\{v_P(x), v_P(y)\} \geq -v_P(A)$, o que acarreta que $v_P(ax + y) \geq -v_P(A)$. Novamente pela observação 2.4.1. (a), temos que $ax + y \in \mathcal{L}(A)$ e então $\mathcal{L}(A)$ é um subespaço vetorial de F e assim um espaço vetorial sobre o corpo K .

(b) Por hipótese, $A = A' + (z)$, para algum elemento $0 \neq z \in F$. Considere a aplicação $\Phi : \mathcal{L}(A) \rightarrow F$, dada por $\Phi(x) = xz$. Note que a imagem de Φ está contida em $\mathcal{L}(A')$: de fato, se y está na imagem de Φ , então $y = \Phi(x)$ para algum elemento $x \in \mathcal{L}(A)$; logo, $y = xz$ e $(y) = (xz) = (x) + (z) = (x) + A - A' \geq 0 - A' = -A'$, ou seja, $(y) + A' \geq 0$ e portanto, $y \in \mathcal{L}(A')$ e assim temos provado que a imagem de Φ está contida em $\mathcal{L}(A')$. Também, esta aplicação Φ é K -linear: de fato, sendo x e $y \in \mathcal{L}(A)$ e $\lambda \in K$, temos $\Phi(x + \lambda y) = (x + \lambda y)z = xz + \lambda yz = \Phi(x) + \lambda \Phi(y)$. Da mesma maneira, considere a aplicação K -linear $\Phi' : \mathcal{L}(A') \rightarrow F$, dada por $\Phi'(x) = xz^{-1}$. Temos que a imagem de Φ' está contida em $\mathcal{L}(A)$: de fato, se w está na imagem de Φ' temos $w = \Phi'(x)$, para $x \in \mathcal{L}(A')$; logo, $(w) = (xz^{-1}) = (x) + (z^{-1}) = (x) - (z) = (x) + A' - A \geq 0 - A = -A$, ou seja, $(w) + A \geq 0$ e com isso a imagem de Φ' está contida em $\mathcal{L}(A)$. Tomando então as aplicações $\Phi : \mathcal{L}(A) \rightarrow \mathcal{L}(A')$ e $\Phi' : \mathcal{L}(A') \rightarrow \mathcal{L}(A)$ temos que, $\Phi \circ \Phi' = Id$ sobre $\mathcal{L}(A')$, e $\Phi' \circ \Phi = Id$ sobre $\mathcal{L}(A)$. Assim, Φ e Φ' são inversas uma da outra. Portanto, Φ é um isomorfismo entre $\mathcal{L}(A)$ e $\mathcal{L}(A')$. ■

Lema 2.4.2 (a) $\mathcal{L}(0) = K$.

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

Demonstração (a) Para $0 \neq x \in K$ temos que $(x) = 0$. Logo, $x \in \mathcal{L}(0)$ e então $K \subset \mathcal{L}(0)$. Reciprocamente, se $0 \neq x \in \mathcal{L}(0)$ então $(x) \geq 0$ e com isso $v_P(x) \geq 0$ para todo lugar P ; assim x não possui pólos e então, pelo corolário 2.1.2., x não pode ser transcendente sobre K ; logo,

$x \in \tilde{K} = K$. Portanto, $\mathcal{L}(0) \subset K$. Conclusão: $\mathcal{L}(0) = K$.

(b) Suponha que exista um elemento x não nulo em $\mathcal{L}(A)$, para $A < 0$. Desta maneira, $(x) \geq -A > 0$ e com isso $x \notin K = \tilde{K}$ sendo então transcendente sobre K . Além disso, $(x) > 0$ implica que x não possui pólos, o que é absurdo, visto que todo elemento transcendente possui pelo menos um zero e um pólo. ■

Definição 2.4.5 A dimensão de cada K -espaço vetorial V será denotada por $\ell(V)$.

Nosso próximo objetivo é mostrar que o espaço vetorial $\mathcal{L}(A)$ possui dimensão finita, para todo divisor A de F/K .

Definição 2.4.6 Para $A \in \mathbb{D}_F$, definimos a dimensão do divisor A , e denotamos por $\ell(A)$, como sendo a dimensão do espaço vetorial $\mathcal{L}(A)$, ou seja, $\ell(A) = \ell(\mathcal{L}(A))$.

Lema 2.4.3 Sejam A e B divisores de F/K com $A \leq B$. Então, temos que $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ e $\ell(B) - \ell(A) \leq \text{grau}(B) - \text{grau}(A)$.

Demonstração Ver referência [12], Lema I.4.8.. ■

Proposição 2.4.1 Para todo divisor $A \in \mathbb{D}_F$, o espaço $\mathcal{L}(A)$ é um espaço vetorial sobre K de dimensão finita. Mais precisamente: se $A = A_+ - A_-$, com A_+ e A_- divisores positivos de F/K , então $\ell(A) \leq \text{grau}(A_+) + 1$.

Demonstração Seja $A \in \mathbb{D}_F$. Pelo lema 2.4.1.(a), temos que $\mathcal{L}(A)$ é um espaço vetorial sobre o corpo K . Mostremos que $\mathcal{L}(A)$ tem dimensão finita. Por hipótese, $A_+ = A + A_-$, com A_+ e A_- divisores positivos, então $A \leq A_+$. Pelo lema 2.4.3. segue que $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$. Logo, $\ell(A) \leq \ell(A_+)$, e desta forma é suficiente mostrar que $\ell(A_+) \leq \text{grau}(A_+) + 1$, visto que o grau de qualquer divisor é finito. Agora, como $A_+ \geq 0$, pelo lema 2.4.3. temos que $\ell(A_+) - \ell(0) \leq \text{grau}(A_+) - \text{grau}(0)$, ou seja, $\ell(A_+) - \ell(0) \leq \text{grau}(A_+)$. Temos, pelo lema 2.4.2., que $\mathcal{L}(0) = K$ e então $\ell(0) = 1$. Portanto, $\ell(A_+) \leq \text{grau}(A_+) + 1$. ■

Um dos problemas mais importantes da teoria de corpos de funções algébricas é o de calcular a dimensão de um divisor. O teorema de Riemann-Roch vem nos auxiliar nesta questão.

Teorema 2.4.1 Qualquer divisor principal tem grau zero. Mais precisamente, seja $x \in F \setminus K$, $(x)_0$ o divisor de zeros de x e $(x)_\infty$ o divisor de pólos de x . Então, vale o seguinte:

$\text{grau}((x)_0) = \text{grau}((x)_\infty) = [F : K(x)]$, e portanto temos que:

$$\text{grau}((x)) = \text{grau}((x)_0) - \text{grau}((x)_\infty) = 0.$$

Demonstração Seja $n := [F : K(x)]$ e $B := \sum_{i=1}^r -v_{P_i}(x) P_i$, onde $P_1, \dots, P_r$ são todos pólos de x . Assim, P_i é um zero de x^{-1} .

Pela proposição 2.3.1., observamos que $\text{grau}(B) = \sum_{i=1}^r v_{P_i}(x^{-1}) \text{grau}(P_i) \leq [F : K(x)] = n$. Logo, $\text{grau}(B) \leq n$. Mostremos agora que $\text{grau}(B) \geq n$. Escolhemos $\{u_1, \dots, u_n\}$ uma base para F como $K(x)$ -espaço vetorial, e também um divisor efetivo C de tal forma que $(u_i) \geq -C$, para $i = 1, \dots, n$. Seja $l \geq 0$. Note que $x^t u_j$, para $0 \leq t \leq l$ e $j = 1, \dots, n$, pertence à $\mathcal{L}(lB + C)$. De fato:

$$(u_j) + C \geq 0 \text{ e } t(x)_0 + (l-t)(x)_\infty \geq 0 \Rightarrow (u_j) + C + t(x)_0 + l(x)_\infty - t(x)_\infty \geq 0 \Rightarrow \\ (u_j) + C + lB + t(x) \geq 0 \Rightarrow (u_j) + C + lB + (x^t) \geq 0 \Rightarrow (x^t u_j) + lB + C \geq 0.$$

Portanto, $x^t u_j \in \mathcal{L}(lB + C)$. Como $u_1, \dots, u_n$ são linearmente independentes sobre $K(x)$ segue que são linearmente independentes sobre K e então os elementos $x^t u_j$, $0 \leq t \leq l$ e $1 \leq j \leq n$ são linearmente independentes sobre K . Portanto, $\ell(lB + C) \geq n(l+1)$, para todo $l \geq 0$. Coloquemos $c := \text{grau}(C)$. Pela proposição 2.4.1. segue que $\ell(lB + C) \leq l\text{grau}(B) + c + 1$ e então $n(l+1) \leq \ell(lB + C) \leq l\text{grau}(B) + c + 1$. Assim, para todo $l \geq 0$, temos que $l(\text{grau}(B) - n) \geq n - c - 1$. Tomando l suficientemente grande, devemos ter $\text{grau}(B) \geq n$. Portanto, $n \leq \text{grau}(B) \leq n$ e então $\text{grau}(B) = n$. Provamos então que $\text{grau}((x)_\infty) = [F : K(x)]$. Agora, como $(x)_0 = (x^{-1})_\infty$, concluímos que $\text{grau}((x)_0) = \text{grau}((x^{-1})_\infty) = [F : K(x^{-1})] = [F : K(x)]$. Sendo $(x) = (x)_0 - (x)_\infty$, obtemos que $\text{grau}((x)) = 0$, como queríamos demonstrar. ■

Corolário 2.4.1 (a) Sejam A e A' divisores de F/K com A equivalente à A' . Então, $\ell(A) = \ell(A')$ e $\text{grau}(A) = \text{grau}(A')$.

(b) Se $\text{grau}(A) < 0$ então $\ell(A) = 0$.

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

(1) A é principal.

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

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

Demonstração (a) Como A é equivalente à A' , pelo lema 2.4.1. (b), $\mathcal{L}(A)$ e $\mathcal{L}(A')$ são espaços vetoriais isomorfos sobre o corpo K , logo tem a mesma dimensão. Como, por definição, $\ell(\mathcal{L}(A)) = \ell(A)$ segue que $\ell(A) = \ell(A')$. Por A ser equivalente à A' temos que $A = A' + (x)$, para algum $x \in F \setminus \{0\}$. Pelo teorema 2.4.1., $\text{grau}((x)) = 0$ e então $\text{grau}(A) = \text{grau}(A')$.

(b) Suponha que $\ell(A) > 0$; logo $\mathcal{L}(A) \neq \{0\}$. Pelo lema 2.4.2. (b), temos $A > 0$ e daí $\text{grau}(A) \geq 0$, contra a hipótese. Portanto, $\ell(A) = 0$.

(c) (1) $\Rightarrow$ (2) Suponha que A é um divisor principal. Logo $A = (x)$, para $x \in F \setminus \{0\}$. Como $(x^{-1}) = \sum_{P \in Z} v_P(x^{-1})P - \sum_{P \in N} v_P(x^{-1})P = -\sum_{P \in Z} v_P(x)P + \sum_{P \in N} v_P(x)P = -(x)$, segue que $x^{-1} \in \mathcal{L}(A)$ o que acarreta $\ell(A) \geq 1$.

(2) $\Rightarrow$ (3) Suponha agora que $\ell(A) \geq 1$ e $\text{grau}(A) = 0$. De $\ell(A) \geq 1$ segue que $\mathcal{L}(A) \neq \{0\}$ e então pelo lema 2.4.2. (b), temos que $A \geq 0$. Assim, $A \geq 0$ e $\text{grau}(A) = 0$ implica que $A = 0$. Por consequência, $\ell(A) = \ell(0) = \ell(\mathcal{L}(0)) = \ell(K) = 1$. Portanto, $\ell(A) = 1$.

(3) $\Rightarrow$ (1) Suponha que $\ell(A) = 1$ e $\text{grau}(A) = 0$. Como $\ell(A) = 1$ segue que $\mathcal{L}(A) \neq \{0\}$ e assim podemos escolher um elemento $0 \neq z \in \mathcal{L}(A)$ e temos $(z) + A \geq 0$. Sendo, pelo teorema 2.4.1., $\text{grau}((z)) = 0$ temos que $\text{grau}((z) + A) = 0$, pois $\text{grau}(A) = 0$. De $(z) + A \geq 0$ e $\text{grau}((z) + A) = 0$ segue que $(z) + A = 0$. Logo, $A = -(z) = (z^{-1})$ e então A é um divisor principal. ■

Proposição 2.4.2 Existe uma constante $\gamma \in \mathbb{Z}$ tal que, para todos os divisores $A \in \mathbb{D}_F$, vale o seguinte: $\text{grau}(A) - \ell(A) \leq \gamma$.

Demonstração Para iniciar a demonstração, observemos primeiramente o seguinte fato: sendo A_1 e $A_2 \in \mathbb{D}_F$ temos que, se $A_1 \leq A_2$ então $\text{grau}(A_1) - \ell(A_1) \leq \text{grau}(A_2) - \ell(A_2)$. De fato, pelo lema 2.4.3., segue que $\ell(A_2) - \ell(A_1) \leq \text{grau}(A_2) - \text{grau}(A_1)$ e então temos o resultado. Fixemos agora um elemento $x \in F \setminus K$ e consideremos o divisor específico $B := (x)_\infty$, o divisor de pólos de x . Pela demonstração do teorema 2.4.1., temos que existe um divisor efetivo C de tal forma que $\ell(lB + C) \geq (l+1)\text{grau}(B)$, para todo $l \geq 0$. Por outro lado, pelo lema 2.4.3., temos que $\ell(lB + C) \leq \ell(lB) + \text{grau}(C)$: de fato, $\ell(lB + C) - \ell(lB) \leq \text{grau}(lB + C) - \text{grau}(lB) = \text{grau}(C)$. Desta forma, de $\ell(lB + C) \geq (l+1)\text{grau}(B)$ e $\ell(lB + C) \leq \ell(lB) + \text{grau}(C)$ temos que $\ell(lB) \geq (l+1)\text{grau}(B) - \text{grau}(C) = l\text{grau}(B) + ([F : K(x)] - \text{grau}(C))$ o que acarreta $\ell(lB) \geq \text{grau}(lB) + ([F : K(x)] - \text{grau}(C))$.

Portanto, $\text{grau}(lB) - \ell(lB) \leq \text{grau}(C) - [F : K(x)]$ e com isso $\text{grau}(lB) - \ell(lB) \leq \gamma$, $\forall l \geq 0$, onde $\gamma = \text{grau}(C) - [F : K(x)]$. Resta agora mostrar que $\text{grau}(lB) - \ell(lB) \leq \gamma$ continua valendo quando substituímos lB por qualquer divisor A de F/K . Afirmamos que dado um divisor A de F/K , existem divisores A_1 , D e um inteiro $l \geq 0$ tais que, $A \leq A_1$, A_1 é equivalente à D e $D \leq lB$. De fato, escolha um divisor $A_1 \geq A$, tal que A_1 é um divisor efetivo. Então, pelo lema 2.4.3., obtemos que $\ell(lB - A_1) \geq \ell(lB) - \text{grau}(A_1) \geq \text{grau}(lB) - \gamma - \text{grau}(A_1) > 0$, para l suficientemente grande. Assim, existe algum elemento $z \neq 0$, com $z \in \mathcal{L}(lB - A_1)$. Colocando $D := A_1 - (z)$, obtemos A_1 equivalente à D e $D \leq A_1 - (A_1 - lB) = lB$, como desejado. Utilizando esta afirmação, conseguimos terminar a prova da seguinte maneira: como $A_1 \geq A$ segue, pela observação no início da demonstração, que $\text{grau}(A) - \ell(A) \leq \text{grau}(A_1) - \ell(A_1)$; como A_1 é equivalente à D , temos $\text{grau}(A_1) - \ell(A_1) = \text{grau}(D) - \ell(D) \leq \text{grau}(lB) - \ell(lB) \leq \gamma$. Logo, $\text{grau}(A) - \ell(A) \leq \gamma$, $\forall A \in \mathbb{D}_F$. ■

Devemos observar que a ênfase aqui está no fato que o inteiro γ é independente do divisor A . Esta constante depende somente do corpo de funções algébricas F/K .

Definição 2.4.7 O gênero g de F/K é definido por $g := \max \{ \text{grau}(A) - \ell(A) + 1 \mid A \in \mathbb{D}_F \}$.

Pela proposição 2.4.2., o conjunto $\{ \text{grau}(A) - \ell(A) + 1 \mid A \in \mathbb{D}_F \}$ é limitado superiormente pelo número inteiro $\gamma + 1$. Logo, o gênero g é um número finito e assim a definição anterior faz sentido. O gênero é o invariante mais importante de um corpo de funções.

Observação 2.4.3 O gênero de F/K é um inteiro não negativo.

Demonstração De fato, tomando $A = 0$ temos que $\text{grau}(0) - \ell(0) + 1 = 0 - \ell(K) + 1 = 0 - 1 + 1 = 0$; conseqüentemente $g \geq 0$. ■

Teorema 2.4.2 (Teorema de Riemann) Seja F/K um corpo de funções de gênero g .

- (a) Para todo divisor $A \in \mathbb{D}_F$, $\ell(A) \geq \text{grau}(A) + 1 - g$.
- (b) Existe um inteiro c , dependendo de F/K , tal que $\ell(A) = \text{grau}(A) + 1 - g$, sempre que $\text{grau}(A) \geq c$.

Demonstração (a) Sendo $A \in \mathbb{D}_F$ qualquer, pela definição do gênero de um corpo de funções, segue que $g \geq \text{grau}(A) - \ell(A) + 1$. Logo, obtemos $\ell(A) \geq \text{grau}(A) + 1 - g$.

(b) Escolhemos um divisor A_0 com $g = \text{grau}(A_0) - \ell(A_0) + 1$ e seja $c := \text{grau}(A_0) + 1 - g$. Para A um divisor de F/K , com $\text{grau}(A) \geq c$, pela parte (a) temos que

$$\ell(A - A_0) \geq \text{grau}(A - A_0) + 1 - g = \text{grau}(A) - \text{grau}(A_0) + 1 - g \geq c - \text{grau}(A_0) + 1 - g = 1 + c - c = 1.$$

Logo, $\ell(A - A_0) \geq 1$ e então existe um elemento $0 \neq z \in \mathcal{L}(A - A_0)$. Considere o divisor $A' = A + (z)$, e como $(z) \geq -A + A_0$, temos $A' \geq A_0$. Sendo A equivalente à A' segue pelo corolário 2.4.1. que $\ell(A) = \ell(A')$ e $\text{grau}(A) = \text{grau}(A')$. Com isso, $\text{grau}(A) - \ell(A) = \text{grau}(A') - \ell(A')$. Pelo lema 2.4.3., temos $\text{grau}(A') - \ell(A') \geq \text{grau}(A_0) - \ell(A_0) = g - 1$. Portanto, $\ell(A) \leq \text{grau}(A) - g + 1$. Pelo item (a), $\ell(A) = \text{grau}(A) + 1 - g$. ■

Exemplo 2.4.1 Vamos mostrar que o corpo de funções racional $K(x)/K$ possui gênero $g = 0$. Para este fim, consideremos o lugar P_∞ e conforme visto na proposição 2.2.1., temos que $\text{grau}(P_\infty) = 1$. Considere, para $r \geq 0$, o espaço vetorial $\mathcal{L}(rP_\infty)$. Note que os elementos $1, x, \dots, x^r$ estão em $\mathcal{L}(rP_\infty)$. De fato, para $0 \leq i \leq r$ observamos que $(x^i) + rP_\infty = i(x) + rP_\infty \geq 0$, pois $rP_\infty \geq 0$ e $(x) \geq 0$. Como $1, x, \dots, x^r$ são linearmente independentes em $\mathcal{L}(rP_\infty)$ segue que $r + 1 \leq \ell(rP_\infty) = \text{grau}(rP_\infty) + 1 - g = r + 1 - g$, para r suficientemente grande (teorema de Riemann, item (b)). Desta forma, $r + 1 \leq r + 1 - g$ e então $g \leq 0$. Por outro lado, vimos que $g \geq 0$ para qualquer corpo de funções. Logo, $g = 0$.

Em geral é difícil determinar o gênero de um corpo de funções algébricas.

2.5 O Teorema de Riemann-Roch

Nesta seção, F/K é um corpo de funções algébricas de gênero g .

Definição 2.5.1 Para $A \in \mathbb{D}_F$, definimos $i(A) := \ell(A) - \text{grau}(A) + g - 1$. Este número inteiro é chamado de índice de especialidade do divisor A .

Pelo teorema de Riemann, 2.4.2., temos $\ell(A) \geq \text{grau}(A) + 1 - g$ e então $i(A)$ é um inteiro não negativo. Além disso, $i(A) = 0$ se o $\text{grau}(A)$ é suficientemente grande. Na presente seção forneceremos diversas interpretações para o índice de especialidade de divisores de F/K , como sendo a dimensão de determinados espaços vetoriais. Para este fim, introduziremos a noção de um adele do corpo de funções F/K .

Definição 2.5.2 Um adele de F/K é uma aplicação $\alpha : \mathbb{P}_F \longrightarrow F$, dada por $\alpha(P) = \alpha_P$, tal que $\alpha_P \in O_P$, para quase todos os lugares P de F/K .

De acordo com a definição anterior podemos considerar um adele como uma sequência no corpo F , e portanto utilizamos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou simplesmente $\alpha = (\alpha_P)$. O conjunto $\mathbb{A}_F := \{\alpha \mid \alpha \text{ é um adele de } F/K\}$, é chamado o espaço de adeles de F/K . Este conjunto é um espaço vetorial sobre o corpo K : de fato, sendo $c \in K$ e α, β no espaço de adeles de F/K temos que $(\alpha + c\beta) : \mathbb{P}_F \longrightarrow F$, é tal que $(\alpha + c\beta)(P) = \alpha(P) + c\beta(P) = \alpha_P + c\beta_P \in O_P$, e então $\alpha + c\beta$ é um adele de F/K . O adele principal de um elemento $x \in F$ é o adele cujas componentes são todas iguais à x , e note que $\alpha_P = x \in O_P$, para quase todos os lugares P de F/K faz sentido, uma vez que x não nulo em F tem uma quantidade finita de pólos e zeros. Tomando a aplicação que toma $x \in F$ e leva no seu adele principal, esta é um mergulho de F em $\mathbb{A}_F$, uma vez que é uma aplicação bijetora, e então podemos escrever $F \hookrightarrow \mathbb{A}_F$. Como temos este mergulho, a valorização discreta v_P associada ao lugar P de F/K se estende naturalmente para $\mathbb{A}_F$, colocando $v_P(\alpha) := v_P(\alpha_P)$, sendo que temos α_P a P componente do adele α . Por definição $v_P(\alpha) \geq 0$, para quase todos os lugares P de F/K .

Definição 2.5.3 Para $A \in \mathbb{D}_F$ definimos o seguinte conjunto:

$$\mathbb{A}_F(A) := \{\alpha \in \mathbb{A}_F \mid v_P(\alpha) \geq -v_P(A), \text{ para todo lugar } P \text{ de } F/K\}.$$

Note que este conjunto é um K -subespaço vetorial de $\mathbb{A}_F$: de fato, sendo α, β em $\mathbb{A}_F(A)$ e $0 \neq c \in K$, temos que α e β são adeles de F/K e $v_P(\alpha) \geq -v_P(A)$ e $v_P(\beta) \geq -v_P(A)$, logo, $\alpha + c\beta$ é um adele de F/K e $v_P(\alpha + c\beta) := v_P(\alpha_P + c\beta_P) \geq \min\{v_P(\alpha), v_P(c\beta)\} = \min\{v_P(\alpha), v_P(c) + v_P(\beta)\} = \min\{v_P(\alpha), v_P(\beta)\} \geq -v_P(A)$ e então $\alpha + c\beta$ está em $\mathbb{A}_F(A)$.

Teorema 2.5.1 Para qualquer divisor A de F/K o índice de especialidade é dado por

$$i(A) = \ell(\mathbb{A}_F) - \ell(\mathbb{A}_F(A) + F).$$

Demonstração Ver referência [12], Teorema I.5.4.. ■

Aqui, como usual, as dimensões dos espaços vetoriais são tomadas sendo dimensão como K -espaço vetorial. Como um corolário, obtemos outra caracterização do gênero de F/K .

Corolário 2.5.1 Para qualquer corpo de funções F/K temos, $g = \ell(\mathbb{A}_F) - \ell(\mathbb{A}_F(0) + F)$.

Demonstração Por definição, $i(0) = \ell(0) - \text{grau}(0) + g - 1 = \ell(\mathcal{L}(0)) + g - 1 = g$ e pelo teorema 2.5.1. obtemos que, $i(0) = \ell(\mathbb{A}_F) - \ell(\mathbb{A}_F(0) + F)$. ■

O teorema 2.5.1. pode ser enunciado da seguinte maneira: "Para qualquer $A \in \mathbb{D}_F$, vale que

$$\ell(A) = \text{grau}(A) + 1 - g + \ell(\mathbb{A}_F) - \ell(\mathbb{A}_F(A) + F)."$$

Esta é uma versão preliminar do teorema de Riemann-Roch, que será provado nesta seção, um pouco mais adiante. Introduziremos agora o conceito de diferencial de Weil, o qual conduzirá para uma segunda interpretação do índice de especialidade de um divisor.

Definição 2.5.4 Uma diferencial de Weil de F/K é uma aplicação K -linear $\omega : \mathbb{A}_F \longrightarrow K$, que se anula em $\mathbb{A}_F(A) + F$, para algum divisor $A \in \mathbb{D}_F$. Definimos o módulo de diferencial de Weil de F/K por $\Omega_F := \{\omega \mid \omega \text{ é uma diferencial de Weil de } F/K\}$, e temos que Ω_F é um F -espaço vetorial. Para $A \in \mathbb{D}_F$ seja $\Omega_F(A) := \{\omega \in \Omega_F \mid \omega \text{ se anula em } \mathbb{A}_F(A) + F\}$.

Temos que $\Omega_F(A)$ é um espaço vetorial sobre o corpo K : de fato, se ω_1 se anula sobre $\mathbb{A}_F(A_1) + F$ e ω_2 se anula sobre $\mathbb{A}_F(A_2) + F$, então $\omega_1 + \omega_2$ se anula sobre $\mathbb{A}_F(A_3) + F$, para qualquer divisor A_3 com $A_3 \leq A_1$ e $A_3 \leq A_2$, uma vez que $\mathbb{A}_F(A_3) + F \subset (\mathbb{A}_F(A_1) + F) \cap (\mathbb{A}_F(A_2) + F)$, e então se $\alpha \in \mathbb{A}_F(A_3) + F$, segue que $(\omega_1 + \omega_2)(\alpha) = \omega_1(\alpha) + \omega_2(\alpha) = 0$; também, para $a \in K$ e $\alpha \in \mathbb{A}_F(A_1) + F$ temos que $(a\omega_1)(\alpha) = a\omega_1(\alpha) = 0$; note agora que, para ω_1 e ω_2 em $\Omega_F(A)$, $a \in K$ e $\alpha \in \mathbb{A}_F(A) + F$, temos $(\omega_1 + a\omega_2)(\alpha) = \omega_1(\alpha) + a\omega_2(\alpha) = 0$ e então $\omega_1 + a\omega_2 \in \Omega_F(A)$. Portanto, $\Omega_F(A)$ é subespaço de Ω_F .

Lema 2.5.1 Para A um divisor de F/K temos que $\ell(\Omega_F(A)) = i(A)$.

Demonstração Vamos mostrar que o espaço vetorial $\Omega_F(A)$ é isomorfo ao espaço das transformações lineares de $\mathbb{A}_F/(\mathbb{A}_F(A) + F)$ em K . Seja $\Phi : \Omega_F(A) \longrightarrow \tau(\mathbb{A}_F/(\mathbb{A}_F(A) + F); K)$, onde $\Phi(\omega) = f$, com $f : \mathbb{A}_F/(\mathbb{A}_F(A) + F) \longrightarrow K$, $f(\bar{\alpha}) = \omega(\alpha)$. Note que Φ está bem definida. De fato, sendo $\bar{\alpha}, \bar{\beta}$ em $\mathbb{A}_F/(\mathbb{A}_F(A) + F)$, com $\bar{\alpha} = \bar{\beta}$ segue que $\alpha - \beta \in \mathbb{A}_F(A) + F$ e então $f(\bar{\alpha} - \bar{\beta}) = \omega(\alpha - \beta) = 0$, logo, $f(\bar{\alpha} - \bar{\beta}) = 0$ implica que $f(\bar{\alpha}) - f(\bar{\beta}) = 0$ o que acarreta $f(\bar{\alpha}) = f(\bar{\beta})$. Também, $\Phi(\omega) = 0$ se, e somente se, $\omega(\alpha) = 0$ para todo $\alpha \in \mathbb{A}_F$, isto é, se, e somente se, $\omega \equiv 0$. Portanto, $\text{Ker}(\Phi) = \{0\}$ e Φ é injetora. Temos que Φ é sobrejetora pela própria definição. Logo, Φ é um isomorfismo. Como $\ell(\tau(\mathbb{A}_F/(\mathbb{A}_F(A) + F); K)) = \ell(\mathbb{A}_F) - \ell(\mathbb{A}_F(A) + F)$, segue que $\ell(\Omega_F(A)) = i(A)$. ■

Uma consequência do lema 2.5.1., é que $\Omega_F \neq \{0\}$. De fato, escolhemos um divisor A de modo que o seu grau é menor ou igual à -2 e então como $\ell(\Omega_F(A)) = i(A)$ conseguimos obter que $\ell(\Omega_F(A)) = \ell(A) - \text{grau}(A) + g - 1 \geq 2 - 1 + g + \ell(A) = 1 + g + \ell(A) \geq 1$. Consequentemente, $\Omega_F(A) \neq \{0\}$.

Definição 2.5.5 Para $x \in F$ e $\omega \in \Omega_F$, definimos a diferencial de Weil $x\omega : \mathbb{A}_F \longrightarrow K$ por $(x\omega)(\alpha) := \omega(x\alpha)$.

Verifiquemos se $x\omega$ é uma diferencial de Weil de F/K : se ω se anula sobre $\mathbb{A}_F(A) + F$ então, para $\alpha = \alpha_1 + \alpha_2 \in \mathbb{A}_F(A + (x)) + F$ com $\alpha_1 \in \mathbb{A}_F(A + (x))$ e $\alpha_2 \in F$, teremos que $(x\omega)(\alpha_2) = \omega(x\alpha_2) = 0$, pois $x\alpha_2 \in F$ e ω se anula em $\mathbb{A}_F(A) + F$ e, como $\alpha_1 \in \mathbb{A}_F(A + (x))$ então $v_P(\alpha_1) + v_P(A + (x)) \geq 0$ logo, $v_P(\alpha_1) + v_P(A) + v_P((x)) \geq 0$; assim, $x\alpha_1 \in \mathbb{A}_F(A)$, e então $\omega(x\alpha_1) = 0$. Desta forma, $\omega(x\alpha) = \omega(x\alpha_1 + x\alpha_2) = \omega(x\alpha_1) + \omega(x\alpha_2) = 0$.

Proposição 2.5.1 O módulo de diferencial de Weil Ω_F é um espaço vetorial sobre o corpo F de dimensão um.

Demonstração Como $\Omega_F \neq \{0\}$ escolhemos $\omega_1 \neq 0$ em Ω_F . Temos que mostrar que para qualquer $\omega_2 \in \Omega_F$, existe algum $z \in F$ com $\omega_2 = z\omega_1$. Se $\omega_2 = 0$ basta tomar $z = 0$. Suponha que $\omega_2 \neq 0$. Escolhemos A_1 e A_2 divisores de F/K tais que $\omega_1 \in \Omega_F(A_1)$ e $\omega_2 \in \Omega_F(A_2)$. Para um divisor B , que será especificado posteriormente, considere a aplicação K -linear injetora, $\phi_i : \mathcal{L}(A_i + B) \longrightarrow \Omega_F(-B)$, que a cada x associa o elemento $x\omega_i$, para $i = 1, 2$. Afirmamos que para uma escolha apropriada do divisor B vale que $\phi_1(\mathcal{L}(A_1 + B)) \cap \phi_2(\mathcal{L}(A_2 + B)) \neq \{0\}$.

Prova da afirmação anterior: Começamos com um fato proveniente da Álgebra Linear. O mesmo diz que, se U_1 e U_2 são subespaços de um espaço vetorial V de dimensão finita então $\ell(U_1 \cap U_2) \geq \ell(U_1) + \ell(U_2) - \ell(V)$. Agora, seja $B > 0$ um divisor de grau suficientemente grande tal que $\ell(A_i + B) = \text{grau}(A_i + B) + 1 - g$, para $i = 1, 2$, o que é possível pelo teorema de Riemann. Seja $U_i := \phi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B)$. Temos, $\ell(\Omega_F(-B)) = \ell(-B) - \text{grau}(-B) + g - 1 = \text{grau}(B) - 1 + g$, uma vez que como $\text{grau}(-B) < 0$ segue que $\ell(-B) = 0$. Como ϕ_i é injetora, $i = 1, 2$, segue que $\text{Ker}(\phi_i) = \{0\}$ e então $\ell(\text{Ker}(\phi_i)) = 0$. Pelo Teorema do Núcleo e da Imagem, obtemos que $\ell(A_i + B) = \ell(\text{Ker}(\phi_i)) + \ell(\phi_i(\mathcal{L}(A_i + B)))$ logo, $\ell(A_i + B) = \ell(\phi_i(\mathcal{L}(A_i + B)))$. Portanto, obtemos que:

$$\ell(U_1) + \ell(U_2) - \ell(\Omega_F(-B)) = \text{grau}(A_1 + B) + 1 - g + \text{grau}(A_2 + B) + 1 - g - \text{grau}(B) + 1 - g = \text{grau}(B) + (\text{grau}(A_1) + \text{grau}(A_2) + 3(1 - g)).$$

O termo entre parênteses na igualdade anterior não depende do divisor B ; assim $\ell(U_1) + \ell(U_2) - \ell(\Omega_F(-B)) > 0$, se o grau de B é suficientemente grande. Usando o fato proveniente da Álgebra Linear segue que $U_1 \cap U_2 \neq \{0\}$, o que prova a afirmação. Com isso, escolhemos $x_1 \in \mathcal{L}(A_1 + B)$ e $x_2 \in \mathcal{L}(A_2 + B)$ tais que $x_1\omega_1 = x_2\omega_2 \neq 0$. Então $\omega_2 = (x_2^{-1}x_1)\omega_1$, como desejado. ■

Queremos vincular um divisor para qualquer diferencial de Weil $\omega \neq 0$. Para este fim, considere para uma ω fixada o conjunto $M(\omega) := \{A \in \mathbb{D}_F \mid \omega \text{ se anula sobre } \mathbb{A}_F(A) + F\}$.

Lema 2.5.2 Seja $0 \neq \omega \in \Omega_F$. Então, existe um divisor unicamente determinado $W \in M(\omega)$ tal que $A \leq W$, para qualquer $A \in M(\omega)$.

Demonstração Ver referência [12], Lema I.5.10.. ■

A seguinte definição faz sentido pelo lema precedente.

Definição 2.5.6 (a) O divisor (ω) de uma diferencial de Weil ω não nula é o divisor unicamente determinado de F/K satisfazendo:

- (1) ω se anula sobre $\mathbb{A}_F((\omega)) + F$.
- (2) Se ω se anula sobre $\mathbb{A}_F(A) + F$ então $A \leq (\omega)$.

(b) Para $\omega \in \Omega_F \setminus \{0\}$ e P um lugar de F/K , definimos $v_P(\omega) := v_P((\omega))$.

(c) Um lugar P é dito um zero, respectivamente um pólo, de ω se $v_P(\omega) > 0$, respectivamente $v_P(\omega) < 0$. Dizemos que ω é regular em P se $v_P(\omega) \geq 0$ e ω é denominada regular, ou

holomórfica, se ω é regular para qualquer lugar P de F/K .

(d) Um divisor W é chamado um divisor canônico de F/K se $W = (\omega)$, para alguma ω diferencial de Weil não nula de F/K .

Observação 2.5.1 Segue imediatamente da definição 2.5.6. que:

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

De fato, sendo $\omega \in \Omega_F(A)$ segue que, para $\alpha \in \mathbb{A}_F(A) + F$ temos $\omega(\alpha) = 0$. Observando o item (a) da definição 2.5.6. temos $(\omega) \geq A$. Portanto, $\Omega_F(A) \subset \{\omega \in \Omega_F \mid \omega = 0 \text{ ou } (\omega) \geq A\}$. Agora, se $\omega \equiv 0$ então ω se anula em $\mathbb{A}_F(A) + F$, para qualquer A divisor de F/K ; se $\omega \neq 0$ e $(\omega) \geq A$ temos, para $\alpha \in \mathbb{A}_F(A) + F$, que $v_P(\alpha) \geq -v_P(A)$ o que implica $v_P((\omega)) + v_P(\alpha) \geq v_P((\omega)) - v_P(A) \geq 0$ e com isso, $-\alpha \in \mathbb{A}_F((\omega)) + F$. Desta forma, $\omega(\alpha) = 0$ implica que $\{\omega \in \Omega_F \mid \omega = 0 \text{ ou } (\omega) \geq A\} \subset \Omega_F(A)$. Portanto, temos a igualdade de conjuntos desejada. Temos também que, se $(\omega) \geq 0$ então $v_P((\omega)) \geq 0$, para qualquer lugar P de F/K . Logo, $\Omega_F(0) \subset \{\omega \in \Omega_F \mid \omega \text{ é regular}\}$ e, se ω é regular segue que $\omega \in \Omega_F(0)$. Daí, $\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ é regular}\}$, como queríamos.

Como uma consequência do lema 2.5.1. e da definição 2.5.1. obtemos que $\ell(\Omega_F(0)) = g$. De fato, pelo lema 2.5.1. temos que $\ell(\Omega_F(0)) = i(0)$ e, pela definição 2.5.1., segue que $i(0) = \ell(0) - \text{grau}(0) + g - 1 = 1 + g - 1 = g$.

Proposição 2.5.2 (a) Para $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$ temos que $(x\omega) = (x) + (\omega)$.
 (b) Qualquer par de divisores canônicos de F/K são equivalentes.

Demonstração (a) De acordo com a definição 2.5.5. se ω se anula sobre $\mathbb{A}_F(A) + F$ então $x\omega$ se anula sobre $\mathbb{A}_F(A + (x)) + F$. Pelo item (a) da definição 2.5.6., ω se anula sobre $\mathbb{A}_F((\omega)) + F$ logo, $x\omega$ se anula sobre $\mathbb{A}_F((\omega) + (x)) + F$. Pelo mesmo item da definição citada anteriormente, $(\omega) + (x) \leq (x\omega)$. Da mesma forma, $x\omega$ se anula sobre $\mathbb{A}_F((x\omega)) + F$ e com isso $x^{-1}x\omega$ se anula sobre $\mathbb{A}_F((x\omega) + (x^{-1})) + F$ e então $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. De $(\omega) + (x) \leq (x\omega)$ e $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$, segue que $(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x)$. Portanto, $(x\omega) = (x) + (\omega)$.

(b) Sejam W' e W'' dois divisores canônicos de F/K , ou seja, $W' = (\omega')$ e $W'' = (\omega'')$, para ω' e ω'' diferenciais de Weil de F/K , não nulas. Como Ω_F é um espaço vetorial sobre o corpo F de dimensão um, existe z não nulo em F tal que $\omega'' = z\omega'$. Assim, $W' - W'' = (\omega') - (z\omega') = (\omega') - (z) - (\omega') = (z^{-1})$. Logo, $W' = W'' + (z^{-1})$, onde $z^{-1} \in F \setminus \{0\}$. Então, W' e W'' são divisores equivalentes. ■

Teorema 2.5.2 Sejam A um divisor arbitrário de F/K e $W = (\omega)$ um divisor canônico de F/K . Então, a aplicação $\mu : \mathcal{L}(W - A) \longrightarrow \Omega_F(A)$ dada por $\mu(x) = x\omega$, é um isomorfismo de K -espaços vetoriais. Em particular, $i(A) = \ell(W - A)$.

Demonstração Para $x \in \mathcal{L}(W - A)$ temos que $(x) + W - A \geq 0$. Logo, $(x) + (\omega) \geq A$ implica que $(x\omega) \geq W - (W - A) = A$. Pela observação 2.5.1., $x\omega \in \Omega_F(A)$. Portanto, μ está bem definida. Agora, para $x, y \in \mathcal{L}(W - A)$ e $\lambda \in K$ temos que, $\mu(x + \lambda y) = (x + \lambda y)\omega = x\omega + \lambda y\omega = \mu(x) + \lambda\mu(y)$. Assim, μ é K -linear. Também, μ é injetora: de fato, $\mu(x) = \mu(y) \Rightarrow x\omega = y\omega \Rightarrow (x - y)\omega = 0 \Rightarrow x - y = 0$, uma vez que $\omega \neq 0$. A fim de mostrar que μ é sobrejetora, considere uma diferencial de Weil $\omega' \in \Omega_F(A)$. Pela proposição 2.5.1., $\omega' = x\omega$, para algum $x \in F$. Como, $(x) + W = (x) + (\omega) = (x\omega) = (\omega') \geq A$, obtemos $(x) \geq A - W = -(W - A)$. Logo, $x \in \mathcal{L}(W - A)$ e $\mu(x) = x\omega = \omega'$. Portanto, μ é sobrejetora. Concluimos assim que μ é um isomorfismo de K -espaços vetoriais. Desta forma, $\mathcal{L}(W - A)$ e $\Omega_F(A)$ possuem a mesma dimensão. Pelo lema 2.5.1., obtemos que $\ell(\Omega_F(A)) = i(A)$. Então, $i(A) = \ell(W - A)$, como queríamos demonstrar. ■

Com este resultado demonstraremos o teorema de Riemann-Roch, o qual é um dos teoremas mais importantes da teoria de corpos de funções algébricas.

Teorema 2.5.3 (Teorema de Riemann-Roch) Seja W um divisor canônico do corpo de funções F/K . Então, para qualquer divisor A de F/K , temos que a dimensão de A satisfaz a seguinte igualdade: $\ell(A) = \text{grau}(A) + 1 - g + \ell(W - A)$.

Demonstração Por definição, para qualquer divisor A de F/K temos que $i(A) = \ell(A) - \text{grau}(A) + g - 1$. Pelo teorema 2.5.2., segue que $i(A) = \ell(W - A)$, onde W é um divisor canônico de F/K . Portanto, $\ell(A) = \text{grau}(A) + 1 - g + \ell(W - A)$. ■

Corolário 2.5.2 Para um divisor canônico W , temos que $\text{grau}(W) = 2g - 2$ e $\ell(W) = g$.

Demonstração Tomando A sendo o divisor nulo de F/K , o teorema de Riemann-Roch e o lema 2.4.2. nos fornecem $1 = \ell(K) = 0 + 1 - g + \ell(W - 0)$. Logo, $\ell(W) = g$. Agora, tomemos $A = W$ e assim obtemos, pelo teorema de Riemann-Roch, que $\ell(W) = \text{grau}(W) + 1 - g + 1$. Sendo $g = \ell(W)$ concluímos que $\text{grau}(W) = 2g - 2$. ■

Do teorema de Riemann, já sabemos que existe alguma constante c tal que $i(A) = 0$, sempre que $\text{grau}(A) \geq c$. Podemos agora dar uma descrição mais precisa de como escolher essa constante.

Teorema 2.5.4 Se A é um divisor de F/K , com $\text{grau}(A) \geq 2g - 1$, então vale a seguinte igualdade para a dimensão de A : $\ell(A) = \text{grau}(A) + 1 - g$.

Demonstração Pelo teorema de Riemann-Roch temos $\ell(A) = \text{grau}(A) + 1 - g + \ell(W - A)$, onde W é um divisor canônico de F/K . Já que $\text{grau}(A) \geq 2g - 1$ e, pelo corolário 2.5.2., $\text{grau}(W) = 2g - 2$ segue que $\text{grau}(W - A) = \text{grau}(W) - \text{grau}(A) \leq 2g - 2 - 2g + 1 = -1 < 0$. Do corolário 2.4.1. (b) temos $\ell(W - A) = 0$. Logo, segue que $\ell(A) = \text{grau}(A) + 1 - g$. ■

Observe que a limitação $2g - 1$ neste teorema é a melhor possível. De fato, para um divisor canônico W onde temos $\text{grau}(W) = 2g - 2 < 2g - 1$ obtemos que $\text{grau}(W) + 1 - g = g - 1$, e então $g = \ell(W) > \text{grau}(W) + 1 - g$.

2.6 Algumas consequências do Teorema de Riemann-Roch

Como na seção anterior, F/K é um corpo de funções algébricas de gênero g . Queremos discutir várias consequências do teorema de Riemann-Roch. O nosso primeiro objetivo é mostrar que o teorema de Riemann-Roch fornece uma caracterização para o gênero de um corpo de funções algébricas.

Proposição 2.6.1 Suponha que g_0 , um número inteiro, e W_0 um divisor de F/K satisfazem

$$\ell(A) = \text{grau}(A) + 1 - g_0 + \ell(W_0 - A), \text{ para qualquer divisor } A \text{ de } F/K.$$

Então, $g_0 = g$ e W_0 é um divisor canônico de F/K .

Demonstração Tomamos $A = 0$; com isso temos $1 = \ell(0) = \text{grau}(0) + 1 - g_0 + \ell(W_0)$ e então $\ell(W_0) = g_0$. Tomando agora $A = W_0$, segue que $g_0 = \ell(W_0) = \text{grau}(W_0) + 1 - g_0 + \ell(0)$. Logo, $\text{grau}(W_0) = 2g_0 - 2$. Seja W um divisor canônico de F/K . Escolhemos um divisor A com $\text{grau}(A) > \max\{2g - 2, 2g_0 - 2\}$. Então, pelo teorema 2.5.4., segue que $\ell(A) = \text{grau}(A) + 1 - g$. Como $\text{grau}(W_0 - A) = \text{grau}(W_0) - \text{grau}(A) < 2g_0 - 2 + 2 - 2g_0 = 0$, então pelo corolário 2.4.1. (b) vemos que $\ell(W_0 - A) = 0$. Daí, pela hipótese, $\ell(A) = \text{grau}(A) + 1 - g_0$. Portanto, $\text{grau}(A) + 1 - g_0 = \text{grau}(A) + 1 - g$ o que implica que $g = g_0$. Finalmente, substituímos $A = W$ em $\ell(A) = \text{grau}(A) + 1 - g_0 + \ell(W_0 - A)$ e observamos que:

$$\ell(W) = \text{grau}(W) + 1 - g + \ell(W_0 - W) \Rightarrow g = (2g - 2) + 1 - g + \ell(W_0 - W) \Rightarrow \ell(W_0 - W) = 1.$$

Uma vez que $\text{grau}(W_0 - W) = \text{grau}(W_0) - \text{grau}(W) = 2g_0 - 2 - 2g + 2 = 0$, pelo corolário 2.4.1. (c), temos que $W_0 - W$ é um divisor principal, ou seja, $W_0 - W = (x)$, para $x \in F \setminus \{0\}$. Logo, $W_0 = W + (x)$ e como W é um divisor canônico de F/K , segue que $W = (\omega)$, para alguma $0 \neq \omega \in \Omega_F$. Daí $W_0 = (\omega) + (x)$ e, pela proposição 2.5.2. (a), temos $(\omega) + (x) = (x\omega)$. Assim, $W_0 = (x\omega)$ onde, de acordo com a definição 2.5.5., $x\omega$ é diferencial de Weil de F/K e então W_0 é divisor canônico de F/K . ■

Outra caracterização útil de divisores canônicos é dada a seguir.

Proposição 2.6.2 Um divisor B é canônico se, e somente se, $\text{grau}(B) = 2g - 2$ e $\ell(B) \geq g$.

Demonstração Suponha que $\text{grau}(B) = 2g - 2$ e $\ell(B) \geq g$. Escolhemos um divisor canônico W . Pelo teorema de Riemann-Roch temos que, $g \leq \ell(B) = \text{grau}(B) + 1 - g + \ell(W - B) = g - 1 + \ell(W - B)$. Portanto, $\ell(W - B) \geq 1$ e como $\text{grau}(W - B) = \text{grau}(W) - \text{grau}(B) = 2g - 2 - 2g + 2 = 0$, pelo corolário 2.4.1. (c), $W - B$ é um divisor principal. Logo, existe $x \in F \setminus \{0\}$ tal que $W - B = (x)$ e daí $B = W - (x)$; sendo W um divisor canônico segue que $W = (\omega)$, para alguma $0 \neq \omega \in \Omega_F$. Assim, $B = (x^{-1}\omega)$ e então B é um divisor canônico, uma vez que $x^{-1}\omega$ é uma diferencial de Weil de F/K . Reciprocamente, se B é um divisor canônico então, pelo corolário 2.5.2., observamos que $\text{grau}(B) = 2g - 2$ e $\ell(B) = g$. ■

Em seguida, chegamos a uma caracterização que envolve o corpo de funções racional.

Proposição 2.6.3 Para um corpo de funções F/K as seguintes condições são equivalentes:

- (1) F/K é um corpo de funções racional, isto é, o corpo F é tal que $F = K(x)$, para algum x que é transcendente sobre K .
- (2) F/K possui gênero $g = 0$ e existe algum divisor A de F/K com $\text{grau}(A) = 1$.

Demonstração (1) $\Rightarrow$ (2): Do exemplo 2.4.1. temos que F/K possui gênero $g = 0$ e tomando $A = P_\infty$, do mesmo modo como visto na seção 2.2., segue pela proposição 2.2.1.(c) que $\text{grau}(P_\infty) = 1$.

(2) $\Rightarrow$ (1): Suponha que F/K tenha gênero $g = 0$ e que exista um divisor A de F/K tal que $\text{grau}(A) = 1$. Assim, temos que $\text{grau}(A) \geq 2g - 1$ e então, pelo teorema 2.5.4., obtemos que

$$\ell(A) = \text{grau}(A) + 1 - g = \text{grau}(A) + 1 = 2.$$

Deste modo, $\ell(A) \neq 0$ e então $\mathcal{L}(A) \neq \{0\}$ o que implica que A é um divisor equivalente à A' , para algum divisor efetivo A' , conforme visto na observação 2.4.1.(b). Logo, temos que $\ell(A') = \ell(A) = 2$, conforme corolário 2.4.1.(a), e com isso existe um elemento $x \in \mathcal{L}(A') \setminus K$ e a fortiori $(x) \neq 0$ e $(x) + A' \geq 0$. Pelo corolário 2.4.1.(a), $\text{grau}(A) = \text{grau}(A') = 1$ e como $A' \geq 0$, isto se torna possível somente se $A' = (x)_\infty$, o divisor de pólos de x . Agora, pelo teorema 2.4.1., $[F : K(x)] = \text{grau}((x)_\infty) = \text{grau}(A') = 1$, e assim $F = K(x)$. ■

O próximo teorema reforça o que foi visto no teorema da Aproximação Fraca.

Teorema 2.6.1 (Teorema da Aproximação Forte) Seja $S \subseteq \mathbb{P}_F$ um subconjunto próprio do conjunto dos lugares de F/K e $P_1, \dots, P_r$ elementos de S . Suponha que são dados $x_1, \dots, x_r$ no corpo F e $n_1, \dots, n_r$ números inteiros. Então, existe um elemento $x \in F$ tal que,

$$v_{P_i}(x - x_i) = n_i, \text{ para todo } i = 1, \dots, r \text{ e } v_P(x) \geq 0, \text{ para todo } P \in S \setminus \{P_1, \dots, P_r\}.$$

Demonstração Ver referência [12], Teorema I.6.4.. ■

Neste momento, cabe ressaltarmos que a teoria a seguir é de suma importância para o restante do trabalho.

Proposição 2.6.4 Seja P um lugar de F/K . Então, para todo $n \geq 2g$, existe um elemento $x \in F$ com divisor de pólos $(x)_\infty = nP$.

Demonstração Considere o divisor $(n-1)P$, para n um número natural, $n \geq 2g$. Assim, temos que $\text{grau}((n-1)P) \geq 2g - 1$ e, pelo teorema 2.5.4., temos que $\ell((n-1)P) = (n-1)\text{grau}(P) + 1 - g$. Também, $\text{grau}(nP) \geq 2g > 2g - 1$, uma vez que $g \geq 0$ e, novamente pelo teorema 2.5.4., $\ell(nP) = n\text{grau}(P) + 1 - g$. Portanto, $\mathcal{L}((n-1)P) \subset \mathcal{L}(nP)$, como subespaço próprio. Tomando $x \neq 0$ em $\mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$, temos que $(x) \geq -nP$. Logo, $(x)_0 - (x)_\infty + nP \geq 0$, com $(x)_0, (x)_\infty \geq 0$ e $\text{supp}((x)_0) \cap \text{supp}((x)_\infty) = \emptyset$. Como $x \notin \mathcal{L}((n-1)P)$ temos que $(x)_0 - (x)_\infty < -nP + P$. Desta forma, obtemos o seguinte $-nP \leq (x)_0 - (x)_\infty < -nP + P \Rightarrow (x)_0 + nP \leq (x)_\infty \leq (x)_0 + nP$.

Concluimos então que, $(x)_\infty = nP$. ■

Definição 2.6.1 Seja P um lugar de F/K . Um número inteiro $n \geq 0$ é chamado ordem de pólo do lugar P se, e somente se, existe um elemento $x \in F$ com $(x)_\infty = nP$. Caso contrário, n é chamado uma lacuna de P .

Pela proposição 2.6.4. temos que n é uma ordem de pólo de P se, e somente se, $\ell(nP) > \ell((n-1)P)$. Além disso, o conjunto das ordens de pólo de P é um subsemigrupo do semigrupo aditivo dos números naturais incluindo o zero. De fato, note que se n_1 e n_2 são ordens de pólo de P , então existem elementos x_1 e x_2 em F com $(x_1)_\infty = n_1P$ e $(x_2)_\infty = n_2P$ e daí $(x_1x_2)_\infty = (x_1)_\infty + (x_2)_\infty = n_1P + n_2P = (n_1 + n_2)P$.

Teorema 2.6.2 (Teorema das Lacunas de Weierstrass) Seja F/K corpo de funções de gênero $g > 0$ e seja P um lugar de grau um de F/K . Então existem exatamente g lacunas $i_1 < i_2 < \dots < i_g$ de P . Além disso, temos $i_1 = 1$ e $i_g \leq 2g - 1$.

Demonstração Pela proposição 2.6.4. qualquer lacuna n de P é tal que $n \leq 2g - 1$, e 0 é uma ordem de pólo de P , pois tomando $0 \in F$ observamos que $(0)_\infty = 0 = 0P$.

Temos a seguinte caracterização de uma lacuna:

$$i \text{ é uma lacuna do lugar } P \iff \mathcal{L}((i-1)P) = \mathcal{L}(iP).$$

De fato, se i é uma lacuna de P então não é uma ordem de pólo de P , e assim i não é maior ou igual do que $2g$; daí $\ell((i-1)P) \geq \ell(iP)$ e, como $\mathcal{L}((i-1)P) \subset \mathcal{L}(iP)$, temos a igualdade $\mathcal{L}((i-1)P) = \mathcal{L}(iP)$. Reciprocamente, se vale que $\mathcal{L}((i-1)P) = \mathcal{L}(iP)$, suponha que exista $x \in F$ com $(x)_\infty = iP$; assim segue que $x \in \mathcal{L}(iP)$, pois $(x) + iP = (x)_0 - (x)_\infty + iP = (x)_0 - iP + iP = (x)_0 \geq 0$; no entanto $x \notin \mathcal{L}((i-1)P)$, pois caso contrário teríamos que $(x)_0 - (x)_\infty + iP - P \geq 0$ e então $(x)_0 - P \geq 0$, o que é absurdo uma vez que por P pertencer ao $\text{supp}((x)_\infty)$ segue que $P \notin \text{supp}((x)_0)$; logo, $x \in \mathcal{L}(iP) \setminus \mathcal{L}((i-1)P)$, o que contraria a hipótese. Portanto, i é uma lacuna de P . Considere agora a sequência de espaços vetoriais $K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \dots \subseteq \mathcal{L}((2g-1)P)$, onde $\ell(0) = 1$ e como $\text{grau}((2g-1)P) = 2g-1$, pois $\text{grau}(P) = 1$, pelo teorema 2.5.4. segue que $\ell((2g-1)P) = \text{grau}((2g-1)P) + 1 - g = 2g-1+1-g = g$. Pelo lema 2.4.3., segue que $\ell(iP) - \ell((i-1)P) \leq \text{grau}(iP) - \text{grau}((i-1)P) = i - (i-1) = 1$, para todo $i \geq 0$. Tomando a dimensão de cada espaço vetorial da sequência descrita anteriormente, obtemos $g-1$ números $1 \leq i \leq 2g-1$, com $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$ como subespaço próprio. Os g números $0 \leq i \leq 2g-1$ restantes serão tais que $\mathcal{L}((i-1)P) = \mathcal{L}(iP)$ e, pela caracterização de lacuna, temos que são lacunas de P . Mostremos que 1 é uma lacuna de P . Suponha que 1 é uma ordem de pólo de P . Como as ordens de pólo de P formam um semigrupo aditivo, segue que qualquer número natural n é uma ordem de pólo de P e então não há lacunas. Absurdo, pois $g > 0$ e já vimos que temos g lacunas. Portanto, 1 é uma lacuna. ■

Pelo corolário 2.4.1.(b), para um divisor A tal que $\text{grau}(A) < 0$ temos que $\ell(A) = 0$ e então $\mathcal{L}(A) = \{0\}$. Por outro lado, pelo teorema 2.5.4., se $\text{grau}(A) > 2g-2$ então temos

que $\ell(A) = \text{grau}(A) + 1 - g$. Assim, a dimensão de um divisor A depende somente do grau de A e do gênero do corpo de funções, caso $\text{grau}(A) \geq 2g - 1$. Queremos considerar mais estreitamente o caso em que $0 \leq \text{grau}(A) \leq 2g - 2$. Neste caso a situação é um tanto quanto complicada mas mesmo assim conseguimos alguns resultados gerais.

Definição 2.6.2 Um divisor A do corpo de funções F/K é chamado não especial se o índice de especialidade de A for tal que $i(A) = 0$; caso contrário, A é chamado especial.

Destacamos algumas consequências imediatas desta definição.

Observação 2.6.1 De acordo com a definição 2.6.2., temos que:

- (1) Um divisor A é não especial se, e somente se, $\ell(A) = \text{grau}(A) + 1 - g$.
- (2) $\text{grau}(A) > 2g - 2 \Rightarrow A$ é não especial.
- (3) Se dois divisores são equivalentes então são ambos especiais ou ambos não especiais.
- (4) Divisores canônicos são especiais.
- (5) Qualquer divisor A que tenha dimensão maior do que zero, com $\text{grau}(A) < g$, é especial.
- (6) Se A é um divisor não especial e B é um divisor tal que $B \geq A$ então B é não especial.

Demonstração (1) Pela definição 2.5.1. temos que $i(A) = \ell(A) - \text{grau}(A) + g - 1$. Se A é não especial segue que $i(A) = 0$ e então $\ell(A) = \text{grau}(A) + 1 - g$. Reciprocamente, se $\ell(A) = \text{grau}(A) + 1 - g$ então $\ell(A) - \text{grau}(A) + g - 1 = 0$; logo, $i(A) = 0$.

(2) Se $\text{grau}(A) > 2g - 2$ então, pelo teorema 2.5.4., temos que a dimensão de A é tal que $\ell(A) = \text{grau}(A) + 1 - g$ o que implica que $\ell(A) - \text{grau}(A) + g - 1 = 0$ e assim, $i(A) = 0$. Portanto, A é não especial.

(3) Se o divisor A é equivalente ao divisor A' então temos $\ell(A) = \ell(A')$ e $\text{grau}(A) = \text{grau}(A')$. Logo, $i(A) = i(A')$.

(4) Seja W um divisor canônico. Então, pelo corolário 2.5.2., segue que $\text{grau}(W) = 2g - 2$ e $\ell(W) = g$. Assim, $i(W) = g - 2g + 2 + g - 1 = 1 \neq 0$ e a fortiori W é especial.

(5) Seja A um divisor de F/K com $\ell(A) > 0$ e $\text{grau}(A) < g$. Como $i(A) = \ell(A) - \text{grau}(A) + g - 1$ obtemos que, $1 \leq \ell(A) = \text{grau}(A) + 1 - g + i(A) < i(A) + 1$ o que implica que $i(A) + 1 > 1$ e então $i(A) > 0$. Como consequência, $i(A) \neq 0$ e então A é especial.

(6) Pelo teorema 2.5.1. temos $i(A) = \ell(\mathbb{A}_F) - \ell(\mathbb{A}_F(A) + F)$ e, como $i(A) = 0$, segue que $\mathbb{A}_F = \mathbb{A}_F(A) + F$. Sendo $B \geq A$ então $\mathbb{A}_F(A) \subseteq \mathbb{A}_F(B)$. Logo, $\mathbb{A}_F \subseteq \mathbb{A}_F(B) + F$ e daí $\mathbb{A}_F = \mathbb{A}_F(B) + F$. Desta forma, $i(B) = \ell(\mathbb{A}_F) - \ell(\mathbb{A}_F(B) + F) = 0$. ■

No que diz respeito ao item (5) da observação precedente, o resultado a seguir é interessante.

Proposição 2.6.5 Suponha que T seja um subconjunto do conjunto de lugares do corpo de funções F/K , onde todos os lugares que estão em T são de grau um e o número de elementos de T é tal que $|T| \geq g$. Então, existe um divisor efetivo e não especial B com $\text{grau}(B) = g$ e $\text{supp}(B) \subseteq T$.

Demonstração Ver referência [12], Proposição I.6.10.. ■

Concluimos esta seção com uma desigualdade para a dimensão de um divisor arbitrário de grau menor ou igual à $2g - 2$.

Teorema 2.6.3 (Teorema de Clifford) Para qualquer divisor A do corpo de funções F/K , com $0 \leq \text{grau}(A) \leq 2g - 2$, vale que $\ell(A) \leq 1 + \frac{1}{2}(\text{grau}(A))$.

O principal passo para a demonstração do teorema de Clifford é o resultado que vem a seguir, o qual enunciaremos como um lema.

Lema 2.6.1 Suponha que A e B são divisores com $\ell(A) > 0$ e $\ell(B) > 0$. Então, temos que $\ell(A) + \ell(B) \leq 1 + \ell(A + B)$.

Demonstração Ver referência [12], Lema I.6.12.. ■

Demonstração[Teorema de Clifford] Se $\ell(A) = 0$, como $\text{grau}(A) \geq 0$, segue o resultado. Para W um divisor canônico, com $\ell(W - A) = 0$, pelo teorema de Riemann-Roch temos que:

$$\begin{aligned} \ell(A) &= \text{grau}(A) + 1 - g + \ell(W - A) = \text{grau}(A) + 1 - g = 1 + \frac{1}{2}(\text{grau}(A)) + \frac{1}{2}(\text{grau}(A) - 2g) \leq \\ &1 + \frac{1}{2}(\text{grau}(A)) + \frac{1}{2}(2g - 2 - 2g) = 1 + \frac{1}{2}(\text{grau}(A)) - 1 < 1 + \frac{1}{2}(\text{grau}(A)). \end{aligned}$$

Consideremos agora o caso em que $\ell(A) > 0$ e $\ell(W - A) > 0$. Assim, aplicando o lema 2.6.1., obtemos: $\ell(A) + \ell(W - A) \leq 1 + \ell(W) = 1 + g$. Por outro lado, pelo teorema de Riemann-Roch, temos que $\ell(A) - \ell(W - A) = \text{grau}(A) + 1 - g$. Portanto, somando as duas últimas expressões desenvolvidas anteriormente, conseguimos obter a seguinte desigualdade: $2\ell(A) \leq \text{grau}(A) + 2$. Logo, $\ell(A) \leq 1 + \frac{1}{2}(\text{grau}(A))$. ■

2.7 Componentes Locais das Diferenciais de Weil

Na seção 2.5. consideramos o mergulho $F \hookrightarrow \mathbb{A}_F$ como sendo a aplicação que toma $x \in F$ e leva no correspondente adele principal. Vamos agora introduzir, para qualquer lugar P do corpo de funções F/K , um outro mergulho de F em $\mathbb{A}_F$.

Definição 2.7.1 Seja P um lugar do corpo de funções F/K .

(a) Para $x \in F$ seja $\iota_P(x) \in \mathbb{A}_F$ o adele cuja P -componente é x e todas as outras demais componentes são iguais à zero.

(b) Para uma diferencial de Weil $\omega \in \Omega_F$ definimos a sua componente local como sendo a função $\omega_P : F \rightarrow K$ dada por $\omega_P(x) := \omega(\iota_P(x))$.

Claramente temos que ω_P é uma aplicação K -linear.

Proposição 2.7.1 Seja ω uma diferencial de Weil de F/K e $\alpha = (\alpha_P)$ um adele de F/K . Então $\omega_P(\alpha_P) \neq 0$, para 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 Ver referência [12], Proposição I.7.2.. ■

Para finalizar este capítulo, a proposição a seguir vem nos dizer que uma diferencial de Weil é determinada unicamente por qualquer das suas componentes locais.

Proposição 2.7.2 (a) Seja $\omega \neq 0$ uma diferencial de Weil de F/K e P um lugar. Então,

$$v_P(\omega) = \max \{r \mid r \in \mathbb{Z} \text{ e } \omega_P(x) = 0, \text{ para todo } x \in F \text{ com } v_P(x) \geq -r\}.$$

Em particular, $\omega_P \neq 0$.

(b) Se ω e ω' são diferenciais de Weil de F/K e $\omega_P = \omega'_P$, para algum lugar P de F/K , então $\omega = \omega'$.

Demonstração Ver referência [12], Proposição I.7.3.. ■

Capítulo 3

Códigos Geométricos de Goppa, Derivações e Formas Diferenciais

Neste capítulo descrevemos a teoria de códigos usando corpos de funções algébricas. Começamos com uma breve introdução dos conceitos da teoria de codificação. Em seguida, definimos códigos Geométricos de Goppa e desenvolvemos suas principais propriedades. Também, vamos introduzir os conceitos de Derivações e Formas Diferenciais que, de certa maneira, serão de grande utilidade em nossas discussões posteriores.

3.1 Códigos

Vamos introduzir algumas noções básicas da teoria de codificação. Seja $\mathbb{F}_q$ um corpo finito com q elementos. Consideremos o espaço vetorial n -dimensional $\mathbb{F}_q^n$, cujos elementos são n -uplas da forma $(a_1, \dots, a_n)$, com a_i no corpo $\mathbb{F}_q$, para todo $i = 1, \dots, n$.

Definição 3.1.1 Para $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_n)$ em $\mathbb{F}_q^n$ seja $d(a, b) := |\{i \mid a_i \neq b_i\}|$.

A função $d(a, b)$ apresentada na definição 3.1.1. define uma distância em $\mathbb{F}_q^n$ e $d(a, b)$ é chamada de Distância de Hamming em $\mathbb{F}_q^n$. O peso de um elemento $a \in \mathbb{F}_q^n$ é definido como $\omega(a) := d(a, 0) = |\{i \mid a_i \neq 0\}|$.

Definição 3.1.2 Um código C sobre o alfabeto $\mathbb{F}_q$ é um subespaço vetorial de $\mathbb{F}_q^n$. Os elementos de C são chamados de palavras do código. O número natural n , que aparece em $\mathbb{F}_q^n$, é denominado o comprimento do código C e $\ell(C)$ é a dimensão de C como $\mathbb{F}_q$ -espaço vetorial. Um código de comprimento n e dimensão k é denotado por $[n, k]$. A distância mínima de um código $C \neq \{0\}$ é denotada por $d(C)$ e é definida como

$$d(C) := \min \{d(a, b) \mid a, b \in C \text{ e } a \neq b\}.$$

Como $d(a, b) = |\{i \mid a_i - b_i \neq 0\}| = d(a - b, 0) = \omega(a - b)$ e $a - b \in C$, pois C é um espaço vetorial, segue que a distância mínima é tal que $d(C) := \min \{\omega(c) \mid 0 \neq c \in C\}$. Um

código $[n, k]$ com distância mínima d será referido como um código $[n, k, d]$. A distribuição de peso de um código $[n, k]$ é a $(n+1)$ -upla $(A_0, \dots, A_n)$ de números naturais incluindo o zero, onde cada entrada é dada por $A_i := |\{c \in C \mid \omega(c) = i\}|$. Desta forma, temos que $A_0 = |\{c \in C \mid \omega(c) = 0\}| = 1$, pois o único elemento tal que $\omega(c) = 0$ é o zero. Pela própria definição, resulta também que $A_i = 0$, para $1 \leq i \leq d(C) - 1$.

Definição 3.1.3 Seja C um código $[n, k]$ sobre $\mathbb{F}_q$. Uma matriz geradora de C é uma matriz $k \times n$, cujas linhas formam uma base para C .

Definição 3.1.4 O produto interno canônico sobre $\mathbb{F}_q^n$ é definido por, $\langle a, b \rangle := \sum_{i=1}^n a_i b_i$, para $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_n) \in \mathbb{F}_q^n$.

Definição 3.1.5 Se $C \subseteq \mathbb{F}_q^n$ é um código então $C^\perp := \{u \in \mathbb{F}_q^n \mid \langle u, c \rangle = 0, \forall c \in C\}$ é chamado o código dual de C . O código C é denominado auto-dual, respectivamente auto-ortogonal, se $C = C^\perp$, respectivamente, se $C \subseteq C^\perp$.

Da Álgebra Linear temos que $\mathbb{F}_q^n = C \oplus C^\perp$ e então, $\ell(\mathbb{F}_q^n) = \ell(C) + \ell(C^\perp)$. Logo, $\ell(C^\perp) = n - k$ e portanto o dual de um código $[n, k]$ é um código $[n, n - k]$. Também, $(C^\perp)^\perp = C$. Em particular, a dimensão de um código auto-dual de comprimento n é $\frac{n}{2}$.

Definição 3.1.6 Uma matriz geradora H de $C^\perp$ é dita a matriz de checagem de paridade do código C .

Note que a matriz de checagem de paridade de um código C $[n, k]$, é uma matriz de ordem $(n - k) \times n$, com $(n - k)$ linhas e n colunas. Além disso, temos que $C := \{u \in \mathbb{F}_q^n \mid H \cdot u^t = 0\}$, onde u^t denota a transposta de u . Deste modo, uma matriz de checagem de paridade verifica se um vetor $u \in \mathbb{F}_q^n$ é uma palavra código ou não. Um dos problemas básicos na teoria dos códigos é construir, sobre um alfabeto fixo $\mathbb{F}_q$, códigos tais que a dimensão e a distância mínima são grandes em comparação com o comprimento.

Proposição 3.1.1 (Cota de Singleton) Para um código C , $[n, k, d]$, vale o seguinte:

$$k + d \leq n + 1.$$

Demonstração Considere um subespaço vetorial $W \subseteq \mathbb{F}_q^n$ dado por

$$W := \{(a_1, \dots, a_n) \in \mathbb{F}_q^n \mid a_i = 0, \forall i \geq d\}.$$

Pela própria definição de peso, para qualquer $a \in W$, temos que o peso de a é tal que $\omega(a) \leq d - 1$ uma vez que como $a \in W$, temos $a_i = 0, \forall i \geq d$ e assim se $a_i \neq 0$, segue que $i < d$. Como $d(C) := \min \{\omega(c) \mid 0 \neq c \in C\}$ segue que $W \cap C = \{0\}$, pois se existe $a \neq 0$ nesta interseção segue que $\omega(a) < d$ e então $\min \{\omega(c) \mid 0 \neq c \in C\} < d$, o que é absurdo. Da Álgebra Linear, temos $\ell(C + W) = \ell(C) + \ell(W) - \ell(W \cap C)$, e como $\ell(W \cap C) = 0$ é imediato que $\ell(C + W) = \ell(C) + \ell(W) = k + d - 1$. Por $C + W$ ser subespaço de $\mathbb{F}_q^n$, $\ell(C + W) \leq n$. Logo, concluímos que $k + d - 1 \leq n$ e a fortiori, $k + d \leq n + 1$. ■

Observação 3.1.1 Em geral, obter cotas para a distância mínima de um dado código não é um problema muito fácil. Uma das razões para o interesse em códigos Geométricos de Goppa, a ser definido na próxima seção, é que para esta grande classe de códigos se consegue avaliar uma boa cota para a distância mínima.

3.2 Códigos Geométricos de Goppa

Vamos introduzir a noção de um código Geométrico de Goppa. Antes disso, fixemos algumas notações que serão usadas a partir de agora.

$F/\mathbb{F}_q$ é um corpo de funções algébricas de gênero g .

$P_1, \dots, P_n$ são lugares dois a dois distintos de $F/\mathbb{F}_q$ de grau um.

$D = P_1 + \dots + P_n$.

G é um divisor de $F/\mathbb{F}_q$ tal que $\text{supp}(G) \cap \text{supp}(D) = \emptyset$.

Definição 3.2.1 O código Geométrico de Goppa $C_{\mathcal{L}}(D, G)$, associado com os divisores D e G , é definido por:

$$C_{\mathcal{L}}(D, G) := \{(x(P_1), \dots, x(P_n)) \mid x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Note que esta definição faz sentido: para $x \in \mathcal{L}(G)$, pela observação 2.4.1. (a), segue que $v_{P_i}(x) + v_{P_i}(G) \geq 0$, para todo $i = 1, \dots, n$, e como $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ temos que $v_{P_i}(G) = 0$, logo $v_{P_i}(x) \geq 0$ e assim $x \in \mathcal{O}_{P_i}$, $\forall i = 1, \dots, n$; além disso, de acordo com a definição 2.1.6., a classe de resíduos $x(P_i)$ de x módulo P_i é um elemento do corpo das classes de resíduos de P_i ; como $\text{grau}(P_i) = 1$, pelo item (b) da definição 2.1.6., o corpo das classes de resíduos é $\mathbb{F}_q$ e assim $x(P_i) \in \mathbb{F}_q$, e com isso a definição anterior tem sentido.

O teorema seguinte irá mostrar a razão desses códigos serem tão interessantes: podemos calcular, ou obter uma estimativa muito boa, para os parâmetros n , k e d por meio do teorema de Riemann-Roch, e obtemos uma cota inferior para a distância mínima em uma situação muito geral.

Teorema 3.2.1 $C_{\mathcal{L}}(D, G)$ é um código $[n, k, d]$ com parâmetros satisfazendo o seguinte:

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

Demonstração Seja a aplicação $ev_D : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$ $ev_D(x) = (x(P_1), \dots, x(P_n)) \in \mathbb{F}_q^n$. Como a imagem de ev_D é $C_{\mathcal{L}}(D, G)$ segue que ev_D é uma aplicação linear sobrejetora de $\mathcal{L}(G)$ para $C_{\mathcal{L}}(D, G)$. Observemos que, $\text{Ker}(ev_D) = \{x \in \mathcal{L}(G) \mid x(P_i) = 0, \forall i = 1, \dots, n\}$. Note que, se $x(P_i) = 0$ então $x \in P_i = \{z \in F \mid v_{P_i}(z) > 0\}$ e assim segue que, $v_{P_i}(x) > 0$. Portanto, $\text{Ker}(ev_D) = \{x \in \mathcal{L}(G) \mid v_{P_i}(x) > 0, \forall i = 1, \dots, n\}$.

Seja $x \in \mathcal{L}(G - D)$. Então, pela observação 2.4.1. (a), $v_{P_i}(x) \geq -v_{P_i}(G - D) = -v_{P_i}(G) + v_{P_i}(D) = 0 + v_{P_i}(D)$ o que implica $v_{P_i}(x) \geq v_{P_i}(D) > 0$ e assim, $v_{P_i}(x) > 0$, $\forall i = 1, \dots, n$.

Como $G - D \leq G$, segue do lema 2.4.3., que $\mathcal{L}(G - D) \subseteq \mathcal{L}(G)$; logo, $x \in \mathcal{L}(G)$ e $v_{P_i}(x) > 0$, para todo $i = 1, \dots, n$, ou seja, $x \in \text{Ker}(ev_D)$. Portanto, $\mathcal{L}(G - D) \subseteq \text{Ker}(ev_D)$. Agora, seja $x \in \text{Ker}(ev_D)$. Assim, $x \in \mathcal{L}(G)$ e $v_{P_i}(x) > 0, \forall i = 1, \dots, n$. Além disso, $\{x \in F \mid v_P(x) + v_P(G) - v_P(D) \geq 0, \forall P\} \supseteq \{x \in \mathcal{L}(G) \mid v_{P_i}(x) - v_{P_i}(D) \geq 0 \forall 1 \leq i \leq n\} \supseteq \{x \in \mathcal{L}(G) \mid v_{P_i}(x) > 0, \forall i = 1, \dots, n\}$. Portanto, $x \in \mathcal{L}(G - D)$ e $\text{Ker}(ev_D) \subseteq \mathcal{L}(G - D)$. Concluimos com isso que $\text{Ker}(ev_D) = \mathcal{L}(G - D)$. Pelo Teorema do Núcleo e da Imagem obtemos, $\ell(\text{Ker}(ev_D)) + \ell(C_{\mathcal{L}}(D, G)) = \ell(G)$ o que implica $\ell(C_{\mathcal{L}}(D, G)) = \ell(G) - \ell(G - D)$.

Por conseguinte, $k = \ell(G) - \ell(G - D)$. A asserção referente à distância mínima d faz sentido somente se $C_{\mathcal{L}}(D, G) \neq \{0\}$. Assim, assumimos que este código não é trivial. Escolha x não nulo em $\mathcal{L}(G)$ com $\omega(ev_D(x)) = d$. Logo, em $ev_D(x) = (x(P_1), \dots, x(P_n))$ temos $n - d$ entradas nulas. Suponha que $x(P_{i_1}) = x(P_{i_2}) = \dots = x(P_{i_{n-d}}) = 0$. Daí, $v_{P_{i_1}}(x) > 0, \dots, v_{P_{i_{n-d}}}(x) > 0$, ou seja, estes $n - d$ lugares de F/K são zeros de x . Assim $0 \neq x$ está em $\mathcal{L}(G - (P_{i_1} + \dots + P_{i_{n-d}}))$ logo, $\ell(G - (P_{i_1} + \dots + P_{i_{n-d}})) \neq 0$ e então, pelo corolário 2.4.1.(b), temos $0 \leq \text{grau}(G - (P_{i_1} + \dots + P_{i_{n-d}})) = \text{grau}(G) - (n - d) = \text{grau}(G) - n + d$.

Conclusão: $d \geq n - \text{grau}(G)$. ■

Corolário 3.2.1 Suponha que o grau de G é estritamente menor do que n . Então, a chamada aplicação avaliação $ev_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D, G)$ é injetora e além disso temos que:

(a) $C_{\mathcal{L}}(D, G)$ é um código $[n, k, d]$ com os parâmetros satisfazendo

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

Consequentemente, $k + d \geq n + 1 - g$.

(b) Se tivermos ainda a hipótese adicional, $2g - 2 < \text{grau}(G) < n$, então $k = \text{grau}(G) + 1 - g$.

(c) Se $\{x_1, \dots, x_k\}$ é uma base de $\mathcal{L}(G)$ então a matriz

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \cdots & x_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{pmatrix}$$

é uma matriz geradora para $C_{\mathcal{L}}(D, G)$.

Demonstração Temos $\text{grau}(G) < n$ e então $\text{grau}(G - D) < 0$. Pelo corolário 2.4.1.(b), segue que se $\text{grau}(G - D) < 0$ então $\ell(G - D) = 0$. Assim, $\mathcal{L}(G - D) = \{0\}$ e como $\mathcal{L}(G - D)$ é o Kernel da aplicação avaliação, temos que $\text{Ker}(ev_D) = \{0\}$ o que acarreta que a aplicação avaliação é injetora. Agora, pelo teorema 3.2.1., temos que $C_{\mathcal{L}}(D, G)$ é um código $[n, k, d]$ com $k = \ell(G) - \ell(G - D)$. Como $\ell(G - D) = 0$ segue que $k = \ell(G)$. Pelo teorema de Riemann, item (a), vemos que $\ell(G) \geq \text{grau}(G) + 1 - g$ e então, $k = \ell(G) \geq \text{grau}(G) + 1 - g$. Também, pelo teorema 3.2.1., temos $d \geq n - \text{grau}(G)$. Daí, $k + d \geq n + 1 - g$. Isto prova o item (a). Se

além das hipóteses anteriores temos que $\text{grau}(G) > 2g - 2$, pelo teorema de Riemann item (b), obtemos que $\ell(G) = \text{grau}(G) + 1 - g$ logo, $k = \text{grau}(G) + 1 - g$. Isto prova o item (b). Provemos agora o item (c). Como o conjunto $\{x_1, \dots, x_k\}$ é base de $\mathcal{L}(G)$ e a aplicação avaliação leva base em base segue que o conjunto $\{ev_D(x_1), \dots, ev_D(x_k)\}$ é uma base de $C_{\mathcal{L}}(D, G)$. Ou seja, as k -linhas de M formam um conjunto linearmente independente em $C_{\mathcal{L}}(D, G)$ que geram este código. Portanto, M é uma matriz geradora de $C_{\mathcal{L}}(D, G)$. ■

Observe que o resultado anterior nos fornece uma outra cota inferior para a distância mínima d , desde que tenhamos $\text{grau}(G) < n$.

Definição 3.2.2 O inteiro $d^* := n - \text{grau}(G)$ é denominado a distância designada do código $C_{\mathcal{L}}(D, G)$.

O teorema 3.2.1. afirma que a distância mínima d de um código Geométrico de Goppa não pode ser menor que a distância designada. A questão se $d^* = d$ ou $d^* < d$, é respondida pela observação seguinte.

Observação 3.2.1 Suponha que $\ell(G) > 0$ e $d^* = n - \text{grau}(G) > 0$. Então, $d^* = d$ se, e somente se, existe um divisor D' satisfazendo, $0 \leq D' \leq D$, $\text{grau}(D') = \text{grau}(G)$ e $\ell(G - D') > 0$.

Demonstração Primeiro assumimos que a distância designada d^* é igual à distância mínima d . Neste caso, tomamos a aplicação avaliação $ev_D : \mathcal{L}(G) \rightarrow C_{\mathcal{L}}(D, G)$ e desta maneira existe x não nulo em $\mathcal{L}(G)$ tal que a palavra código $ev_D(x) = (x(P_1), \dots, x(P_n)) \in C_{\mathcal{L}}(D, G)$ possui precisamente $n - d = n - d^* = \text{grau}(G)$ componentes nulas, uma vez que o mínimo de componentes não nulas é $n - \text{grau}(G)$. Digamos que essas componentes nulas sejam $x(P_{ij}) = 0$, para $j = 1, \dots, \text{grau}(G)$. Tome o divisor $D' := \sum_{j=1}^{\text{grau}(G)} P_{ij}$. Como $n > \text{grau}(G)$ e por definição $D = P_1 + \dots + P_n$ segue que $0 \leq D' \leq D$. Também, $\text{grau}(D') = \text{grau}(G)$, pois P_{ij} , para $j = 1, \dots, \text{grau}(G)$, são lugares de grau um e ainda temos que $x \in \mathcal{L}(G - D') \setminus \{0\}$ e assim segue que, $\ell(G - D') > 0$. Reciprocamente, supondo que exista D' satisfazendo $0 \leq D' \leq D$, $\text{grau}(D') = \text{grau}(G)$ e $\ell(G - D') > 0$; escolhemos y não nulo em $\mathcal{L}(G - D')$ e então temos que $v_P(y) + v_P(G) - v_P(D') \geq 0$ e como $0 \leq D' \leq D$ segue que, $v_P(y) + v_P(G) \geq 0$, ou seja, $y \in \mathcal{L}(G)$ e daí $(y(P_1), \dots, y(P_n)) \in C_{\mathcal{L}}(D, G)$. Suponha que $P_i \in \text{supp}(D')$, para $i = 1, \dots, n$. Assim, $P_i \in \text{supp}(D)$ e como é válido que $v_{P_i}(y) + v_{P_i}(G) - v_{P_i}(D') \geq 0$ e $\text{supp}(G) \cap \text{supp}(D) = \emptyset$, temos que $v_{P_i}(G) = 0$ e então devemos ter $v_{P_i}(y) > 0$. Daí, $y \in P_i$ e assim $y(P_i) = 0$. Com isso o peso da palavra $(y(P_1), \dots, y(P_n))$ é zero e a fortiori $d \leq \omega((y(P_1), \dots, y(P_n))) \leq n - \text{grau}(D') = n - \text{grau}(G) = d^*$. Por outro lado, $d^* \leq d$ e assim podemos concluir que $d = d^*$. ■

Vamos agora definir um outro código associado com os divisores G e D ; este código é definido utilizando componentes locais das diferenciais de Weil. Usaremos algumas notações introduzidas no capítulo 2. Para um divisor A de F/K , $\Omega_F(A)$ é o espaço das diferenciais de

Weil ω com $(\omega) \geq A$. Este é um espaço vetorial de dimensão finita sobre $\mathbb{F}_q$ e de dimensão igual à $i(A)$, o índice de especialidade do divisor A . Para uma diferencial de Weil ω e um lugar $P \in \mathbb{P}_F$, $\omega_P : F \longrightarrow \mathbb{F}_q$ denota a componente local de ω em P .

Definição 3.2.3 Sejam G e $D = P_1 + \dots + P_n$ divisores como antes (isto é, os P_i são lugares dois a dois distintos de grau um e $\text{supp}(G) \cap \text{supp}(D) = \emptyset$). Então, definimos o código $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ por:

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

Nosso primeiro resultado envolvendo este código é análogo ao teorema 3.2.1..

Teorema 3.2.2 $C_\Omega(D, G)$ é um código $[n, k', d']$ com parâmetros satisfazendo o seguinte:

$$k' = i(G - D) - i(G) \text{ e } d' \geq \text{grau}(G) - (2g - 2).$$

Tendo a hipótese adicional $\text{grau}(G) > 2g - 2$ temos que, $k' = i(G - D) \geq n + g - 1 - \text{grau}(G)$. Se, além disso, $2g - 2 < \text{grau}(G) < n$, então $k' = n + g - 1 - \text{grau}(G)$.

Demonstração Seja $P \in \mathbb{P}_F$ um lugar de grau um e ω uma diferencial de Weil com $v_P(\omega) \geq -1$. Afirmamos que $\omega_P(1) = 0$ se, e somente se, $v_P(\omega) \geq 0$. A fim de provar esta afirmação usamos a proposição 2.7.2., a qual afirma que para $r \in \mathbb{Z}$ vale que, $v_P(\omega) \geq r$ se, e somente se, $\omega_P(x) = 0, \forall x \in F$, com $v_P(x) \geq -r$. Suponha que $v_P(\omega) \geq 0$; pela proposição 2.7.2. segue que $\omega_P(x) = 0, \forall x \in F$ com $v_P(x) \geq 0$, e como $v_P(1) = 0$ temos que $\omega_P(1) = 0$. Reciprocamente, suponha que $\omega_P(1) = 0$; seja $x \in F$ com $v_P(x) \geq 0$, e como $\text{grau}(P) = 1$ podemos escrever $x = a + y$, com $a \in \mathbb{F}_q$ e $v_P(y) \geq 1$. Note que $\omega_P(y) = 0$ pois como $v_P(\omega) \geq -1$, pela proposição 2.7.2., isso implica que $\omega_P(x) = 0, \forall x \in F$, com $v_P(x) \geq 1$ e, uma vez que $v_P(y) \geq 1$, temos que $\omega_P(y) = 0$. Então, $\omega_P(x) = \omega_P(a + y) = \omega_P(a) + \omega_P(y) = a\omega_P(1) + 0 = a \cdot 0 = 0$. Assim, $\omega_P(x) = 0$, com $v_P(x) \geq 0$; isso implica, pela proposição 2.7.2., que $v_P(\omega) \geq 0$. Isto prova a afirmação. Considere agora a aplicação $\mathbb{F}_q$ -linear $\varphi_D : \Omega_F(G - D) \longrightarrow C_\Omega(D, G)$, dada por $\omega \longmapsto (\omega_{P_1}(1), \dots, \omega_{P_n}(1))$. Como a imagem de φ_D é igual à $C_\Omega(D, G)$, segue que esta aplicação é sobrejetora.

Note que $\text{Ker}(\varphi_D) = \{\omega \in \Omega_F(G - D) \mid \varphi_D(\omega) = (0, \dots, 0)\}$ é igual ao seguinte conjunto $\{\omega \in \Omega_F \mid (\omega) \geq G - D, v_{P_j}(\omega) \geq 0, \forall j = 1, \dots, n\}$, valendo isso pela afirmação provada no início da demonstração. Assim, $\text{Ker}(\varphi_D) = \Omega_F(G)$. De fato, se $\omega \in \Omega_F(G)$ então $(\omega) \geq G \geq G - D$ e, $v_{P_j}(\omega) \geq v_{P_j}(G) = 0, \forall j = 1, \dots, n$ e então $\omega \in \text{Ker}(\varphi_D)$. Por outro lado, se $\omega \in \text{Ker}(\varphi_D)$ então $(\omega) \geq G - D$; como $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ segue que, $(\omega) \geq G$ e a fortiori $\omega \in \Omega_F(G)$. Portanto, $\text{Ker}(\varphi_D) = \Omega_F(G)$. Assim, pelo Teorema do Núcleo e da Imagem obtemos o seguinte, $\ell(\Omega_F(G - D)) = \ell(\text{Ker}(\varphi_D)) + \ell(\text{Im}(\varphi_D))$ o que implica que $\ell(C_\Omega(D, G)) = \ell(\Omega_F(G - D)) - \ell(\Omega_F(G))$ e assim, $k' = i(G - D) - i(G)$. Observe que esta última igualdade é válida pelo lema 2.5.1., o qual nos fornece que $\ell(\Omega_F(G)) = i(G)$ e $\ell(\Omega_F(G - D)) = i(G - D)$. Agora, vamos provar a asserção referente à distância mínima d' . Seja $\varphi_D(\omega) \in C_\Omega(D, G)$ uma

palavra código de peso $m > 0$. Pela definição de peso temos que $\omega_{P_i}(1) = 0$, para certos índices $i = i_1, \dots, i_{n-m}$. Pela afirmação provada no início da demonstração, segue que $v_{P_{i_j}}(\omega) \geq 0, \forall j = 1, \dots, n - m$. O teorema 2.5.4. nos diz que, se $\ell(\Omega_F(A)) = i(A) \neq 0$ então $\text{grau}(A) \leq 2g - 2$; como temos que $\omega \in \Omega_F\left(G - \left(D - \sum_{j=1}^{n-m} P_{i_j}\right)\right)$ segue que $\text{grau}(G) - (n - (n - m)) \leq 2g - 2$ o que acarreta que $\text{grau}(G) - m \leq 2g - 2$ e então $m \geq \text{grau}(G) - (2g - 2)$.

Sendo $d' = \min\{\omega(c) \mid 0 \neq c \in C_\Omega(D, G)\}$, conseqüentemente a distância mínima d' de $C_\Omega(D, G)$ satisfaz a desigualdade $d' \geq \text{grau}(G) - (2g - 2)$. Suponha agora que $\text{grau}(G) > 2g - 2$. Pelo teorema 2.5.4. obtemos que $i(G) = 0$. Assim, temos que a dimensão k' é tal que $k' = i(G - D) := \ell(G - D) - \text{grau}(G - D) + g - 1 = \ell(G - D) + n + g - 1 - \text{grau}(G)$.

Desta forma, como $\ell(G - D) \geq 0$, segue que $k' \geq n + g - 1 - \text{grau}(G)$. E se tivermos $2g - 2 < \text{grau}(G) < n$ então $\text{grau}(G - D) < 0$ o que implica $\ell(G - D) = 0$; portanto, neste caso, $k' = n + g - 1 - \text{grau}(G)$. ■

Em analogia com a definição 3.2.2., temos que $\text{grau}(G) - (2g - 2)$ é denominada a distância designada do código $C_\Omega(D, G)$. Veremos agora que existe uma relação entre os códigos $C_\mathcal{L}(D, G)$ e $C_\Omega(D, G)$.

Teorema 3.2.3 Os códigos $C_\mathcal{L}(D, G)$ e $C_\Omega(D, G)$ são duais um do outro, isto é, $C_\Omega(D, G) = C_\mathcal{L}(D, G)^\perp$.

Demonstração Ver referência [12], Teorema II.2.8.. ■

Observação 3.2.2 Considere um lugar $P \in \mathbb{P}_F$ de grau um, uma diferencial de Weil ω com $v_P(\omega) \geq -1$ e um elemento $x \in F$ com $v_P(x) \geq 0$. Então, $\omega_P(x) = x(P)\omega_P(1)$.

A fim de provar isto, escrevemos $x = a + y$, com $a = x(P) \in \mathbb{F}_q$ e $v_P(y) > 0$. Como ω_P é linear temos que $\omega_P(x) = \omega_P(a) + \omega_P(y) = a\omega_P(1) + \omega_P(y)$. Observe que, $v_P(\omega) \geq -1$ se, e somente se, $\omega_P(x) = 0, \forall x \in F$ com $v_P(x) \geq 1$. Segue então que $\omega_P(y) = 0$ e daí, $\omega_P(x) = a\omega_P(1) = x(P)\omega_P(1)$.

Nossa próxima finalidade é provar que $C_\Omega(D, G)$ pode ser representado como um código $C_\mathcal{L}(D, H)$, com um divisor H apropriado. Para este propósito necessitamos do seguinte lema.

Lema 3.2.1 Existe uma diferencial de Weil η tal que $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$, para todo $i = 1, \dots, n$.

Demonstração Ver referência [12], Lema II.2.9.. ■

Proposição 3.2.1 Seja η uma diferencial de Weil tal que $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$, para todo $i = 1, \dots, n$. Então, $C_\mathcal{L}(D, G)^\perp = C_\Omega(D, G) = C_\mathcal{L}(D, H)$, com $H := D - G + (\eta)$.

Demonstração Pelo teorema 3.2.3. já sabemos que $C_\mathcal{L}(D, G)^\perp = C_\Omega(D, G)$. Como $v_{P_i}(\eta) = -1, \forall i = 1, \dots, n$, temos que $\text{supp}(H) \cap \text{supp}(D) = \emptyset$. Conseqüentemente, $C_\mathcal{L}(D, H)$ está bem definido. De acordo com o teorema 2.5.2., existe um isomorfismo $\mu : \mathcal{L}((\eta) - (G - D)) \longrightarrow$

$\Omega_F(G - D)$, dado por $\mu(x) = x\eta$. Para $x \in \mathcal{L}(D - G + (\eta))$ temos, conforme a observação 3.2.2., que $(x\eta)_{P_i}(1) = x\eta(\iota_{P_i}(1)) = \eta_{P_i}(x) = x(P_i)\eta_{P_i}(1) = x(P_i)$, pois $\eta_{P_i}(1) = 1$. Desta forma, $C_\Omega(D, G) = C_\mathcal{L}(D, H)$, uma vez que sendo μ isomorfismo temos que é sobrejetor e com isso a imagem de μ é igual à $\Omega_F(G - D)$ e portanto, $x(P_i) \in \Omega_F(G - D)$, para todo $i = 1, \dots, n$. ■

Corolário 3.2.2 Suponha que exista uma diferencial de Weil η satisfazendo o seguinte

$$(\eta) = 2G - D \text{ e } \eta_{P_i}(1) = 1, \text{ para todo } i = 1, \dots, n.$$

Então, o código $C_\mathcal{L}(D, G)$ é auto-dual.

Demonstração A hipótese de que $(\eta) = 2G - D$ significa que $(\eta) = G + G - D$, o que acarreta que $G = D - G + (\eta)$. Lembramos que $\text{supp}(G) \cap \text{supp}(D) = \emptyset$, e assim o código $C_\mathcal{L}(D, D - G + (\eta)) = C_\mathcal{L}(D, G)$ está bem definido. Como $\eta_{P_i}(1) = 1$, para todo $i = 1, \dots, n$, pela proposição 3.2.1., segue $C_\mathcal{L}(D, G)^\perp = C_\mathcal{L}(D, D - G + (\eta)) = C_\mathcal{L}(D, G)$. Portanto, o código $C_\mathcal{L}(D, G)$ é auto-dual. ■

Observação 3.2.3 Utilizando a proposição 3.2.1., podemos reduzir o teorema 3.2.2. ao teorema 3.2.1.; com isso vamos exibir agora uma nova demonstração do teorema 3.2.2..

Demonstração[Outra versão para a prova do teorema 3.2.2.] Queremos mostrar que $C_\Omega(D, G)$ é um código $[n, k', d']$, com parâmetros $k' = i(G - D) - i(G)$ e $d' \geq \text{grau}(G) - (2g - 2)$. Pela proposição 3.2.1., temos que $C_\Omega(D, G) = C_\mathcal{L}(D, D - G + (\eta))$. Pelo teorema 3.2.1., sabemos que $C_\mathcal{L}(D, D - G + (\eta))$ é um código $[n, k, d]$ com parâmetros $k = \ell(D - G + (\eta)) - \ell(D - G + (\eta) - D)$ e $d \geq n - \text{grau}(D - G + (\eta))$. Logo, o parâmetro k' de $C_\Omega(D, G)$ é dado por $k' = \ell(D - G + (\eta)) - \ell(-G + (\eta))$. Pelo teorema 2.5.2., obtemos $i(G) = \ell((\eta) - G)$ e $i(G - D) = \ell((\eta) - G + D)$, e portanto segue que $k' = i(G - D) - i(G)$. Também temos que o parâmetro d' de $C_\Omega(D, G)$ é tal que $d' \geq n - \text{grau}(D - G + (\eta)) = n - \text{grau}(D) + \text{grau}(G) - \text{grau}((\eta))$. Ou seja, $d' \geq n - n + \text{grau}(G) - \text{grau}((\eta)) = \text{grau}(G) - \text{grau}((\eta))$; pelo corolário 2.5.2. sabemos que o $\text{grau}((\eta)) = 2g - 2$ e por consequência $d' \geq \text{grau}(G) - (2g - 2)$. ■

Definição 3.2.4 Dois códigos $C_1, C_2 \subseteq \mathbb{F}_q^n$ são equivalentes se existe um vetor $a = (a_1, \dots, a_n)$ pertencente à $(\mathbb{F}_q \setminus \{0\})^n$ tal que $C_2 = aC_1$, isto é, $C_2 = \{(a_1c_1, \dots, a_nc_n) \mid (c_1, \dots, c_n) \in C_1\}$.

Observamos que códigos equivalentes possuem a mesma dimensão e a mesma distância mínima.

Proposição 3.2.2 (a) Suponha que G_1 e G_2 são dois divisores equivalentes, com $\text{supp}(G_1) \cap \text{supp}(D) = \text{supp}(G_2) \cap \text{supp}(D) = \emptyset$. Então os códigos $C_\mathcal{L}(D, G_1)$ e $C_\mathcal{L}(D, G_2)$ são equivalentes. O mesmo vale para $C_\Omega(D, G_1)$ e $C_\Omega(D, G_2)$.

(b) Reciprocamente, se um código C em $\mathbb{F}_q^n$ é equivalente a um código $C_\mathcal{L}(D, G)$, respectivamente a um código $C_\Omega(D, G)$, então existe um divisor G' equivalente à G tal que $\text{supp}(G') \cap \text{supp}(D) = \emptyset$ e $C = C_\mathcal{L}(D, G')$, respectivamente $C = C_\Omega(D, G')$.

Demonstração Ver referência [12], Proposição II.2.14.. ■

3.3 Derivações e Formas Diferenciais

O conteúdo dessa seção foi elaborado com base no estudo de notas de curso de pós-graduação em Matemática, no nível de Mestrado, realizado no Instituto Nacional de Matemática Pura e Aplicada (IMPA).

Definição 3.3.1 Seja F um corpo. Uma valorização v de F no grupo, ou com grupo, de valores $\mathbb{Z}$ é uma aplicação sobrejetora $v : F \setminus \{0\} \rightarrow \mathbb{Z}$ satisfazendo:

- (i) $v(xy) = v(x) + v(y)$, $\forall x, y \in F \setminus \{0\}$;
- (ii) $v(x + y) \geq \min\{v(x), v(y)\}$, $\forall x, y \in F \setminus \{0\}$ e $x + y \in F \setminus \{0\}$.

Convencionamos que, $v(x) = \infty \iff x = 0$. O par (F, v) é chamado um corpo com valorização.

Observação 3.3.1 Para v uma valorização do corpo F com grupo de valores $\mathbb{Z}$, temos que:

- (1) $v(1) = 0$, pois $v(1) = v(1 \cdot 1) = v(1) + v(1)$.
- (2) $v(-1) = 0$, pois $0 = v(1) = v(-1 \cdot -1) = 2v(-1)$.
- (3) $v(-x) = v(x)$, pois $v(-x) = v(-1) + v(x) = v(x)$, uma vez que $v(-1) = 0$.
- (4) $v(1/x) = -v(x)$, pois $0 = v(1) = v(x \cdot \frac{1}{x}) = v(x) + v(\frac{1}{x})$.

Definição 3.3.2 Seja F/K uma extensão de corpos. Uma valorização v de F/K com grupo de valores $\mathbb{Z}$ é uma valorização de F no grupo de valores $\mathbb{Z}$ que é trivial sobre K , isto é,

- (i) $v(c) = 0$, para cada $c \in K \setminus \{0\}$;
- (ii) $v(xy) = v(x) + v(y)$, $\forall x, y \in F \setminus \{0\}$;
- (iii) $v(x + y) \geq \min\{v(x), v(y)\}$, $\forall x, y \in F \setminus \{0\}$ e $x + y \in F \setminus \{0\}$.

Definição 3.3.3 Seja v uma valorização do corpo F no grupo de valores $\mathbb{Z}$. Um elemento $t \in F$ é chamado um uniformizante local em v se $v(t) = 1$.

Proposição 3.3.1 Seja F/K corpo de funções em uma variável cujo corpo de constantes é algebricamente fechado. Seja v uma valorização de F/K com grupo de valores $\mathbb{Z}$ e seja $x \in F$ tal que $v(x) \geq 0$. Então, existe uma única constante c em K tal que $v(x - c) > 0$.

Definição 3.3.4 O valor c dado na proposição anterior é chamado o valor de x em v e é denotado por $x(v) = c$.

Corolário 3.3.1 Seja F/K um corpo de funções em uma variável cujo corpo de constantes K é algebricamente fechado. Seja v uma valorização de F/K com grupo de valores $\mathbb{Z}$ e t um uniformizante local em v . Então, para cada x em $F \setminus \{0\}$ existe uma única série formal $x = \sum_{n=m}^{\infty} c_n t^n$, onde $m = v(x)$, $c_m \neq 0$ e tal que

$$v\left(x - \sum_{n=m}^j c_n t^n\right) > j, \text{ para cada } j \in \mathbb{Z}, j \geq m.$$

Denotamos por $K((t))$ o conjunto das séries $\sum_{n=m}^{\infty} c_n t^n$ que representam cada elemento x em F , conforme o corolário anterior. Este tipo de série também é conhecida como série de Laurent.

Definição 3.3.5 Seja F/K uma extensão algébrica e $v : F \setminus \{0\} \longrightarrow \mathbb{Z}$ uma valorização de F com grupo de valores $\mathbb{Z}$. Temos que $v(K \setminus \{0\})$ é um subgrupo de $\mathbb{Z}$ que é não nulo. Logo, existe um inteiro positivo $\mathbf{e}$ tal que $v(K \setminus \{0\}) = \mathbb{Z}_{\mathbf{e}} = \{n \cdot \mathbf{e} \mid n \in \mathbb{Z}\}$. Dizemos que $\mathbf{e}$ é o índice de ramificação de v sobre K .

Definição 3.3.6 Seja F um corpo. Uma valorização de posto um de F é uma aplicação $v : F \setminus \{0\} \longrightarrow \mathbb{R}$, não necessariamente sobrejetiva, tal que:

- (i) $v(xy) = v(x) + v(y)$, para todos $x, y \in F \setminus \{0\}$;
- (ii) $v(x + y) \geq \min\{v(x), v(y)\}$, para todos $x, y \in F \setminus \{0\}$, $x + y \in F \setminus \{0\}$.

Definição 3.3.7 Seja F um corpo e v uma valorização de posto um de F . Dizemos que v é uma valorização discreta quando $v(F \setminus \{0\}) = \mathbb{Z}_{\mathbf{r}}$, onde $\mathbf{r}$ é um número real positivo. Dizemos que v é uma valorização normalizada quando $v(F \setminus \{0\}) = \mathbb{Z}$.

Teorema 3.3.1 (Existência de prolongamento) Seja F/K uma extensão finita de corpos e seja v uma valorização discreta de K . Então, existe pelo menos uma valorização discreta de F que prolonga v .

Definição 3.3.8 Seja F/K corpo de funções e v uma valorização normalizada de F . Temos então os seguintes conjuntos:

- (1) $O_v := \{x \in F \mid v(x) \geq 0\}$.
- (2) $U_v := \{x \in F \mid v(x) = 0\}$ é o grupo das unidades de O_v .
- (3) $M_v := \{x \in F \mid v(x) > 0\}$ é o único ideal maximal de O_v .
- (4) $K_v := O_v/M_v$ é o corpo residual em v .

Seja F/K uma extensão finita de corpos, w uma valorização discreta de F e seja $v := w|_K$. Então, $O_v \subseteq O_w$ e $M_v := M_w \cap O_v$. Assim, temos uma imersão $K_v \hookrightarrow K_w$ e com isso vemos K_v como subcorpo de K_w .

Definição 3.3.9 Identificamos $K_v \subseteq K_w$ como subcorpo, de acordo com a imersão anterior, e chamamos $[K_w : K_v]$ o índice de inércia de w sobre F .

Teorema 3.3.2 (Desigualdade Fundamental) Seja F/K uma extensão finita de corpos e considere v uma valorização discreta de K . Se temos $w_1, \dots, w_m$ sendo valorizações discretas de F que prolongam v , $\mathbf{e}_1, \dots, \mathbf{e}_m$ os índices de ramificação e $\mathbf{f}_1, \dots, \mathbf{f}_m$ os índices de inércia, então $\mathbf{e}_1 \mathbf{f}_1 + \dots + \mathbf{e}_m \mathbf{f}_m \leq [F : K]$. Em particular, o número de prolongamentos de v à F é finito.

Derivações

Vimos que as diferenciais de Weil são uma ferramenta muito útil para se estudar corpos de funções algébricas. Agora, vamos introduzir o conceito de formas diferenciais e mostremos como elas se relacionam com as diferenciais de Weil. Porém, antes de fazermos isto introduziremos alguns resultados juntamente com o conceito de derivação.

Definição 3.3.10 Seja $p(x) \in K[x] \setminus K$. Um corpo de raízes para o polinômio $p(x)$ sobre K , é um corpo E que contém K no qual $p(x)$ se fatora como $p(x) = a \prod_{i=1}^n (x - u_i)$, onde $a \in K$ e $E = K(u_1, \dots, u_n)$.

Teorema 3.3.3 Seja $p(x) \in K[x] \setminus K$. Existe um corpo de raízes para $p(x)$.

Definição 3.3.11 Uma extensão algébrica F/K é normal se sempre que um polinômio irreduzível $f(x) \in K[x]$ possui uma raiz em F então ele possui todas as suas raízes em F .

Definição 3.3.12 (i) Um polinômio $f(x)$ em $K[x] \setminus K$ é separável se todas as suas raízes, em um corpo de raízes de f , que existe pelo teorema anterior, têm multiplicidade igual a um.

(ii) Seja F/K uma extensão algébrica e $\alpha \in F$. Dizemos que α é separável sobre K se o polinômio minimal de α sobre K for separável. Dizemos que a extensão algébrica F/K é separável se todo $\alpha \in F$ é separável sobre K .

Definição 3.3.13 Um corpo K é perfeito se toda extensão algébrica F/K é separável.

A partir de agora, consideraremos que K é um corpo perfeito.

Lema 3.3.1 Seja F/K corpo de funções em uma variável sobre K . Então, existe $x \in F$ tal que $F/K(x)$ é extensão finita e separável.

Definição 3.3.14 O elemento x que aparece no lema 3.3.1. é chamado de variável separante.

Definição 3.3.15 Seja F um corpo. Uma F -álgebra é um conjunto U que é um espaço vetorial de dimensão finita sobre F e que admite uma multiplicação associativa e bilinear, isto é, para todos $c, d \in F$ e para todos $\alpha, \beta, \lambda \in U$ temos que:

(i) $\alpha.(\beta\lambda) = (\alpha\beta).\lambda$ (associativa)

(ii) $\alpha.(c\beta + d\lambda) = c.(\alpha\beta) + d.(\alpha\lambda)$, $(c\alpha + d\beta).\lambda = c.(\alpha\lambda) + d.(\beta\lambda)$ (bilinear)

Definição 3.3.16 Dizemos que a F -álgebra U é comutativa e com identidade se, respectivamente, $\alpha.\beta = \beta.\alpha$, $\forall \alpha, \beta$ em U e existe um elemento $1 \in U$ tal que $1.\alpha = \alpha.1 = \alpha$, $\forall \alpha \in U$.

Definição 3.3.17 Seja A uma K -álgebra comutativa e com identidade, onde K é um corpo. Uma K -derivação $D : A \longrightarrow A$ é um homomorfismo de K -espaços vetoriais tal que:

$$D(XY) = XD(Y) + YD(X), \text{ para cada } X, Y \in A.$$

Em particular, sendo F/K corpo de funções e $D : F \longrightarrow F$ K -derivação, dizemos que D é uma K -derivação do corpo de funções F/K .

Exemplo 3.3.1 Se $A = K[x]$, com x transcendente sobre K , então temos que

$$\frac{d}{dx} : K[x] \longrightarrow K[x] \text{ tal que } \sum_j a_j x^j \longmapsto \sum_j j a_j x^{j-1},$$

é uma K -derivação, que admite um único prolongamento a uma K -derivação

$$\frac{d}{dx} : K(x) \longrightarrow K(x), \text{ dada por } \frac{Y}{Z} \longmapsto \frac{1}{Z^2} \cdot \left(Z \frac{dY}{dX} - Y \frac{dZ}{dX} \right).$$

Algumas consequências da definição anterior são listadas no lema a seguir.

Lema 3.3.2 Seja D uma K -derivação do corpo de funções F/K . Então, temos que:

- (a) $D(a) = 0$, para todo $a \in K$.
- (b) $D(z^n) = n z^{n-1} \cdot D(z)$, para todo $z \in F$ e $n \in \mathbb{Z}$.
- (c) Se a característica do corpo K é $p > 0$ então $D(z^p) = 0$, para todo $z \in F$.
- (d) $D(x/y) = (yD(x) - xD(y)) / y^2$, para todos $x, y \in F$, com $y \neq 0$.

Demonstração (a) Observemos primeiro que $D(1) = D(1 \cdot 1) = 1D(1) + 1D(1) = 2D(1)$. Logo, segue que $2D(1) - D(1) = 0$ e então $D(1) = 0$. Tomemos $a \in K$ e como D é K -linear segue que, $D(a) = D(a \cdot 1) = aD(1) = 0$.

(b) Seja $n \in \mathbb{N} \setminus \{0\}$. Vamos fazer uma indução sobre n . Se $n = 1$ então a igualdade vale imediatamente. Suponha então que $D(z^n) = n z^{n-1} \cdot D(z)$. Assim,

$$D(z^{n+1}) = D(z^n z) = zD(z^n) + z^n D(z) = z[n z^{n-1} \cdot D(z)] + z^n D(z) = n z^n D(z) + z^n D(z) = (n+1) z^n \cdot D(z).$$

Logo, a igualdade é válida para $n+1$ e daí o resultado vale para todo $n \in \mathbb{N} \setminus \{0\}$. Agora, observe que temos $0 = D(1) = D(yy^{-1}) = yD(y^{-1}) + y^{-1}D(y)$, $\forall y \in A$ e então $D(y^{-1}) = (-1)y^{-2}D(y)$. Assim, dado $z \in F$ e $n \in \mathbb{N} \setminus \{0\}$ temos que:

$$D(z^{-n}) = D((z^n)^{-1}) = (-1)D(z^n)(z^n)^{-2} = (-1)z^{-2n}[n z^{n-1} \cdot D(z)] = (-n)z^{-(n+1)} \cdot D(z).$$

Desta forma, a igualdade vale para todo $n \in \mathbb{Z}$.

(c) Pelo item (b) temos que $D(z^p) = p z^{p-1} \cdot D(z)$ e então,

$$D(z^p) = z^p(p z^{-1})D(z) = (z^p + \dots + z^p)z^{-1}D(z) = z^p(1 + \dots + 1)z^{-1}D(z) = 0,$$

uma vez que, pela hipótese, $(1 + \dots + 1) = 0$.

(d) Observe que $D(xy^{-1}) = xD(y^{-1}) + y^{-1}D(x) = x(-1)y^{-2}D(y) + y^{-1}D(x) = -xy^{-2}D(y) + y^{-1}D(x) = y^{-2}(yD(x) - xD(y))$, como queríamos. ■

Proposição 3.3.2 Sejam F/K corpo de funções e $x \in F$ variável separante, isto é, a extensão $F/K(x)$ é finita e separável. A K -derivação $\frac{d}{dx} : K[x] \longrightarrow K[x]$ dada por $\sum_j a_j x^j \longmapsto \sum_j j a_j x^{j-1}$ possui um único prolongamento à F , que também será denotado por $\frac{d}{dx}$. Além disso, as K -derivações $D : F \longrightarrow F$ são exatamente da forma $h \frac{d}{dx}$, onde $h \in F$.

Proposição 3.3.3 Sejam F/K corpo de funções, $x \in F$ variável separante e $t \in F$. Então,

$$\frac{dt}{dx} \neq 0 \iff t \text{ é variável separante, isto é, } F/K(t) \text{ é extensão finita e separável.}$$

Corolário 3.3.2 Nas condições da proposição anterior vale que, $\frac{dz}{dx} = \frac{dz}{dt} \cdot \frac{dt}{dx}$.

Demonstração Já sabemos que as K -derivações $D : F \longrightarrow F$ são exatamente da forma $h \frac{d}{dx}$, onde $h \in F$. Então, existe $h \in F$ tal que $\frac{dz}{dt} = h \frac{dz}{dx}$, para cada $z \in F$. Tomando $z = t$ então $1 = h \frac{dt}{dx}$. Logo, obtemos que $\frac{dz}{dx} = \frac{dz}{dx} h \frac{dt}{dx} = \frac{1}{h} \frac{dz}{dt} h \frac{dt}{dx}$ e então $\frac{dz}{dx} = \frac{dz}{dt} \cdot \frac{dt}{dx}$. ■

Observação 3.3.2 O resultado precedente é conhecido como Regra da Cadeia.

Proposição 3.3.4 Seja F/K corpo de funções em uma variável separante cujo corpo K é algebricamente fechado, v valorização de F/K com grupo de valores $\mathbb{Z}$ e t uniformizante local em v . Então, temos que:

(i) t é variável separante.

(ii) Se $h \in F \setminus \{0\}$ é tal que $h = \sum_j c_j t^j$, então $\frac{dh}{dt} = \sum_j j c_j t^{j-1}$.

Formas Diferenciais

Definição 3.3.18 Seja F/K um corpo de funções em uma variável separante. Uma forma diferencial de F/K é uma expressão formal $f dx$, onde $f, x \in F$.

Vejamos que uma forma diferencial é uma classe de equivalência do par $(f, x) \in F \times F$.

De fato, seja $Z := \{(f, x) \in F \times F \mid x \text{ é variável separante}\}$.

Definimos a relação $\approx$ por $(f, x) \approx (h, y) :\iff f dx = h dy :\iff f = h \frac{dy}{dx}$. Se x não é variável separante então definimos assim, $f dx = h dy :\iff h = 0$ ou y não é variável separante. Pela Regra da Cadeia segue que $\approx$ realmente se trata de uma relação de equivalência. Denotamos então por $f dx$ a classe de equivalência de $(f, x) \in Z$, com respeito à $\approx$. Chamamos $f dx$ de uma forma diferencial (ou diferencial) de F/K . A classe de equivalência de $(1, x)$ é simplesmente denotada por dx . Fixemos uma variável separante x ; então cada forma diferencial de F/K se escreve unicamente como $f dx$, onde $f \in F$.

Definição 3.3.19 Definimos $\Omega_{F/K}^1 = \{f dx \mid f, x \in F, \text{ com } x \text{ variável separante}\}$ o conjunto de todas as formas diferenciais de F/K .

Definimos a soma de duas formas diferenciais $f dx$ e $h dy$ em $\Omega_{F/K}^1$ como segue: seja z variável separante; então $f dx = (f \frac{dx}{dz}) dz$ e $h dy = (h \frac{dy}{dz}) dz$ e desta maneira fazemos $f dx + h dy := (f \frac{dx}{dz} + h \frac{dy}{dz}) dz$. Pela Regra da Cadeia esta definição independe da escolha de z . Também definimos, $\omega \cdot (f dx) := (\omega f) dx \in \Omega_{F/K}^1$, para $\omega \in F$ e $f dx \in \Omega_{F/K}^1$.

Com essas operações, $\Omega_{F/K}^1$ é um F -espaço vetorial de dimensão um.

Definição 3.3.20 Seja $\lambda \in \Omega_{F/K}^1$, v uma valorização de F/K com grupo de valores $\mathbb{Z}$ e t uniformizante local em v . Como já vimos, temos que t é uma variável separante e com isso λ se escreve unicamente na forma $\lambda = hdt$, onde $h \in F$. A ordem de λ em v é definida por $v(\lambda) := v(h)$. Temos que a ordem de λ em v independe do uniformizante local t .

Definição 3.3.21 Seja $\lambda \in \Omega_{F/K}^1$ e v valorização de F/K com grupo de valores $\mathbb{Z}$.

- (a) λ possui um zero em $v \iff v(\lambda) > 0$.
- (b) λ possui um pólo em $v \iff v(\lambda) < 0$.

Sendo v valorização de F/K com grupo de valores $\mathbb{Z}$, t uniformizante local em v e $\lambda = hdt$, podemos escrever $h = \sum_j c_j t^j \in K((t))$ e então $\lambda = \sum_j (c_j t^j) dt$, com $v(\lambda) = \min \{j \mid c_j \neq 0\}$.

Definição 3.3.22 Seja $\lambda \in \Omega_{F/K}^1$, v uma valorização de F/K com grupo de valores $\mathbb{Z}$ e t um uniformizante local em v . Se $\lambda = \sum_j (c_j t^j) dt$ então $\text{res}_v(\lambda) = c_{-1}$, que é o chamado resíduo de λ em v . Temos que o resíduo de λ em v independe do uniformizante local em v .

Definição 3.3.23 Seja $h = \sum_j c_j t^j$ um elemento em $K((t))$. O t -resíduo de h é definido por $\text{res}_t(h) = c_{-1}$.

Lema 3.3.3 Sejam $h \in F \setminus \{0\}$ e v valorização de F/K com grupo de valores $\mathbb{Z}$. Então, $\text{res}_v\left(\frac{dh}{h}\right) = v(h) \cdot 1_K$.

Demonstração Sejam $m := v(h)$ e t um uniformizante local em v . Então $h = c_m t^m + c_{m+1} t^{m+1} + \dots$, com $c_m \neq 0$. Deste modo, $dh = (m c_m t^{m-1} + (m+1) c_{m+1} t^m + \dots) dt$. Daí, $\frac{dh}{h} = (m t^{-1} + \dots) dt$. Logo, $\text{res}_v\left(\frac{dh}{h}\right) = m = v(h) \cdot 1_K$. ■

Teorema 3.3.4 (Teorema dos resíduos) Seja F/K corpo de funções em uma variável e K algebricamente fechado. Então $\sum_v \text{res}_v(\lambda) = 0$, para cada $\lambda \in \Omega_{F/K}^1$, onde v é valorização de F/K com grupo de valores $\mathbb{Z}$.

Aplicando o teorema dos resíduos à forma diferencial $\frac{dh}{h}$, onde $h \in F \setminus \{0\}$, obtemos $\sum_v \text{res}_v\left(\frac{dh}{h}\right) = 0$. Pelo lema anterior temos que, $\text{res}_v\left(\frac{dh}{h}\right) = v(h) \cdot 1_K$ e então $\sum_v v(h) = 0$.

Tomemos agora $\mathbb{A} = \mathbb{A}_{F/K}$ o espaço dos adeles:

$\{(z_v) \mid z_v \in F, \forall v \text{ valorização de } F/K \text{ com grupo de valores } \mathbb{Z} \text{ e } z_v \in O_v, \text{ para quase toda } v\}$.

Vamos identificar $F \hookrightarrow \mathbb{A}$ por $h \mapsto (z_v)$, onde $z_v = h$, para toda v . Suponhamos K algebricamente fechado. Cada forma diferencial $\lambda = hdx \in \Omega_{F/K}^1$ define uma função K -linear $\mu : \mathbb{A} \rightarrow K$, que está bem definida, dada por $(z_v) \mapsto \sum_v \text{res}_v(z_v \lambda)$. Temos que μ é uma diferencial de Weil, isto é, vale que:

- (i) μ se anula sobre F ;
- (ii) existe um divisor D tal que μ se anula sobre $\mathbb{A}(D)$, onde

$\mathbb{A}(D) = \{(z_v) \in \mathbb{A} \mid v(z_v) \geq -n_v, \forall v \text{ valorização de } F/K \text{ com grupo de valores } \mathbb{Z}\}.$

Teorema 3.3.5 Suponha que K é algebricamente fechado. A aplicação canônica:

$\Psi : \Omega_{F/K}^1 \longrightarrow \Omega_F$ dada por $\lambda \longmapsto \mu$, onde $\mu : \mathbb{A} \longrightarrow K$ é tal que $\mu((z_v)) = \sum_v \text{res}_v(z_v \lambda)$,

é um isomorfismo de F -espaços vetoriais.

Demonstração Vamos mostrar que essa aplicação é um isomorfismo do espaço das formas diferenciais no espaço das diferenciais de Weil. Temos que $\dim_F(\Omega_{F/K}^1) = 1 = \dim_F(\Omega_F)$. Logo, esses espaços vetoriais sobre o corpo F possuem a mesma dimensão finita. A aplicação Ψ é uma transformação linear. De fato, dados $\lambda_1, \lambda_2 \in \Omega_{F/K}^1$ e $c \in F$ temos que $\Psi(\lambda_1 + c\lambda_2) = \mu$, onde temos $\mu : \mathbb{A} \longrightarrow K$ de tal forma que $(z_v) \longmapsto \sum_v \text{res}_v(z_v(\lambda_1 + c\lambda_2))$. Como $z_v \in F, \forall v$ e $\lambda_1 = h_1 dx$, temos $z_v \lambda_1$ forma diferencial e então $z_v \lambda_1 = \sum_j (c_j t^j) dt$ e da mesma forma temos que $z_v c\lambda_2 = \sum_i (a_i t^i) dt$. Assim, $\text{res}_v(z_v \lambda_1) = c_{-1}$ e $\text{res}_v(z_v c\lambda_2) = a_{-1}$. Note que, se temos $z_v \lambda_1 + z_v c\lambda_2 = \sum_j (a_j t^j + c_j t^j) dt$ então o resíduo da forma diferencial $z_v \lambda_1 + z_v c\lambda_2$ é tal que, $\text{res}_v(z_v \lambda_1 + z_v c\lambda_2) = a_{-1} + c_{-1} = \text{res}_v(z_v \lambda_1) + \text{res}_v(z_v c\lambda_2)$.

Logo, $\sum_v \text{res}_v(z_v(\lambda_1 + c\lambda_2)) = \sum_v \text{res}_v(z_v \lambda_1 + z_v c\lambda_2) = \sum_v [\text{res}_v(z_v \lambda_1) + \text{res}_v(z_v c\lambda_2)]$, e esta última expressão é igual à $\sum_v \text{res}_v(z_v \lambda_1) + \sum_v \text{res}_v(z_v c\lambda_2)$. Portanto, $\Psi(\lambda_1 + c\lambda_2) = \Psi(\lambda_1) + c\Psi(\lambda_2)$ e então Ψ é linear.

Conclusão: $\Omega_{F/K}^1$ e Ω_F são F -espaços vetoriais isomorfos. ■

Observação 3.3.3 Como consequência do teorema anterior, podemos identificar o espaço das diferenciais de Weil de F/K com o espaço das formas diferenciais. Assim, sendo $\omega \neq 0$ em Ω_F , v uma valorização de F/K com grupo de valores $\mathbb{Z}$ e t um uniformizante local em v podemos escrever $\omega = z dt$, com $z \in F$. Deste modo, para uma forma diferencial $\lambda = z dx \neq 0$, com x variável separante e $z \in F$, definimos o divisor de λ por $(\lambda) = (z dx) := (z) + (dx)$.

Capítulo 4

Sobre o Piso e o Teto de um divisor

Dado um divisor A de um corpo de funções algébricas, existe um único divisor de grau mínimo que define o mesmo espaço vetorial $\mathcal{L}(A)$ e existe um único divisor de grau máximo que define o mesmo espaço vetorial $\Omega_F(A)$. Estes divisores são chamados, respectivamente, o piso e o teto do divisor A . Há um método para encontrar tanto o piso como o teto de um divisor e estes divisores também estabelecem limites para a distância mínima de códigos. É o que veremos a seguir.

4.1 O Piso e o Teto de um divisor

Ao longo desta seção, $F/\mathbb{F}_q$ é um corpo de funções algébricas sobre o corpo finito $\mathbb{F}_q$ que possui q elementos. Dado um divisor A , consideraremos divisores A' que definem o mesmo espaço vetorial de diferenciais de Weil que A , ou seja, divisores A' tais que temos $\Omega_F(A) = \Omega_F(A')$. Vamos também considerar divisores A' tais que $\mathcal{L}(A) = \mathcal{L}(A')$. Em particular, nosso interesse está nos divisores A' que satisfazem as igualdades de espaços vetoriais colocadas anteriormente e que possuem um grau tão grande quanto for possível e um grau tão pequeno quanto for possível.

Definição 4.1.1 Dados dois divisores A e A' de $F/\mathbb{F}_q$, o máximo divisor comum de A e A' é o divisor $m.d.c.(A, A') := \sum_{P \in \mathbb{P}_F} \min\{v_P(A), v_P(A')\} P$ e o mínimo múltiplo comum entre os divisores A e A' é o divisor $m.m.c.(A, A') := \sum_{P \in \mathbb{P}_F} \max\{v_P(A), v_P(A')\} P$.

Proposição 4.1.1 Seja G um divisor do corpo de funções $F/\mathbb{F}_q$ com $\ell(G) > 0$. Suponha que G' é um divisor de $F/\mathbb{F}_q$ de grau mínimo tal que $\mathcal{L}(G) = \mathcal{L}(G')$. Então, $G \geq G'$. Consequentemente, G' é o único divisor que respeita esta propriedade.

Demonstração Pela hipótese, temos que $\mathcal{L}(G) = \mathcal{L}(G') \cap \mathcal{L}(G)$. Assim, $\mathcal{L}(G') \cap \mathcal{L}(G) = \mathcal{L}(m.d.c.(G', G))$: de fato, se $0 \neq x \in \mathcal{L}(G') \cap \mathcal{L}(G)$ então $(x) + G' \geq 0$ e $(x) + G \geq 0$. Logo, $\min\{v_P((x) + G'), v_P((x) + G)\} = \min\{v_P((x)) + v_P(G'), v_P((x)) + v_P(G)\} \geq 0, \forall P \in \mathbb{P}_F$. Por outro lado, é visto que o valor mínimo do conjunto dado anteriormente é o seguinte,

$v_P(x) + \min\{v_P(G'), v_P(G)\}$. Portanto, $\sum_P (v_P(x) + \min\{v_P(G'), v_P(G)\}) P \geq 0$ para todo $P \in \mathbb{P}_F$, ou seja, $(x) + m.d.c.(G', G) \geq 0$. Desta maneira, $x \in \mathcal{L}(m.d.c.(G', G))$. Conclusão: $\mathcal{L}(G') \cap \mathcal{L}(G) \subseteq \mathcal{L}(m.d.c.(G', G))$. Seja agora $x \in \mathcal{L}(m.d.c.(G', G))$. Sendo então $\min\{v_P(G), v_P(G')\} \leq v_P(G)$, $\forall P \in \mathbb{P}_F$, segue que:

$$\sum_P \min\{v_P(G), v_P(G')\} P \leq \sum_P v_P(G) P \Rightarrow 0 \leq (x) + m.d.c.(G, G') \leq (x) + G \Rightarrow x \in \mathcal{L}(G) = \mathcal{L}(G') \Rightarrow x \in \mathcal{L}(G) \cap \mathcal{L}(G').$$

Conclusão: $\mathcal{L}(m.d.c.(G', G)) \subseteq \mathcal{L}(G') \cap \mathcal{L}(G)$.

Chegamos então a conclusão final de que $\mathcal{L}(G) = \mathcal{L}(G) \cap \mathcal{L}(G') = \mathcal{L}(m.d.c.(G', G))$. Desta forma, segue da minimalidade do grau de G' que, $\text{grau}(G') \leq \text{grau}(m.d.c.(G', G))$.

Como $\min\{v_P(G'), v_P(G)\} \leq v_P(G')$ para todo lugar P , obtemos a seguinte desigualdade $\sum_P \min\{v_P(G'), v_P(G)\} P \leq \sum_P v_P(G') P$ e então temos que $m.d.c.(G', G) \leq G'$. Portanto, temos as seguintes relações: $\text{grau}(G') \leq \text{grau}(m.d.c.(G', G))$ e $m.d.c.(G', G) \leq G'$. Assim, $\text{grau}(m.d.c.(G', G)) \leq \text{grau}(G')$ e com isso temos $\text{grau}(G') = \text{grau}(m.d.c.(G', G))$; logo, sendo $m.d.c.(G', G) \leq G'$ podemos concluir que, $G' = m.d.c.(G', G)$. Por conseguinte, $G' \leq G$, visto que $m.d.c.(G', G) \leq G$. Suponha agora que G' e G'' são dois divisores de $F/\mathbb{F}_q$ de grau mínimo tais que, $\mathcal{L}(G) = \mathcal{L}(G')$ e $\mathcal{L}(G) = \mathcal{L}(G'')$. De G'' divisor de grau mínimo tal que $\mathcal{L}(G') = \mathcal{L}(G'')$ segue, do feito anteriormente, que $G' \geq G''$ e de G' divisor de grau mínimo tal que $\mathcal{L}(G'') = \mathcal{L}(G')$, temos que $G'' \geq G'$. Portanto, $G' = G''$. Por consequência, existe um único divisor G' de $F/\mathbb{F}_q$ de grau mínimo satisfazendo $\mathcal{L}(G) = \mathcal{L}(G')$. ■

Definição 4.1.2 Dado um divisor G do corpo de funções $F/\mathbb{F}_q$ com $\ell(G) > 0$, o piso de G é o único divisor G' de $F/\mathbb{F}_q$ de grau mínimo tal que $\mathcal{L}(G) = \mathcal{L}(G')$. O piso de G será denotado por $\lfloor G \rfloor$.

Corolário 4.1.1 Sejam G_1 e G_2 divisores do corpo de funções $F/\mathbb{F}_q$ com $\ell(G_1) > 0$ e $\ell(G_2) > 0$. Então, $\mathcal{L}(G_1) = \mathcal{L}(G_2)$ se, e somente se, $\lfloor G_1 \rfloor = \lfloor G_2 \rfloor$.

Demonstração Suponha que $\mathcal{L}(G_1) = \mathcal{L}(G_2)$. Pela definição do piso de um divisor segue que $\mathcal{L}(G_1) = \mathcal{L}(\lfloor G_1 \rfloor)$ e $\mathcal{L}(G_2) = \mathcal{L}(\lfloor G_2 \rfloor)$. Assim, pela hipótese, segue $\mathcal{L}(\lfloor G_1 \rfloor) = \mathcal{L}(\lfloor G_2 \rfloor)$. Desta forma, $\lfloor G_1 \rfloor$ é divisor de grau mínimo tal que $\mathcal{L}(\lfloor G_2 \rfloor) = \mathcal{L}(\lfloor G_1 \rfloor)$; logo, $\lfloor G_2 \rfloor \geq \lfloor G_1 \rfloor$. Também, $\lfloor G_2 \rfloor$ é divisor de grau mínimo tal que $\mathcal{L}(\lfloor G_1 \rfloor) = \mathcal{L}(\lfloor G_2 \rfloor)$; então, $\lfloor G_1 \rfloor \geq \lfloor G_2 \rfloor$. Conclusão: $\lfloor G_1 \rfloor = \lfloor G_2 \rfloor$. Reciprocamente, suponha que $\lfloor G_1 \rfloor = \lfloor G_2 \rfloor$. Nesse caso, pela definição, segue que $\mathcal{L}(G_1) = \mathcal{L}(\lfloor G_1 \rfloor) = \mathcal{L}(\lfloor G_2 \rfloor) = \mathcal{L}(G_2)$. ■

Os próximos três resultados ajudam a encontrar o piso de um divisor. Cada um deles tem sua importância, mas em especial o que diz que se um divisor G é efetivo e existe um outro divisor D tal que $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ então $\text{supp}(\lfloor G \rfloor) \cap \text{supp}(D) = \emptyset$, é frequentemente usado.

Proposição 4.1.2 Seja G um divisor de $F/\mathbb{F}_q$ com $\ell(G) > 0$. Definimos o divisor efetivo E como sendo $E := m.d.c.(G + (x) \mid x \in \mathcal{L}(G) \setminus \{0\})$. Então, $\lfloor G \rfloor = G - E$.

Demonstração Observe que para qualquer lugar P de $F/\mathbb{F}_q$ temos que

$$-v_P(G - E) = \min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\}.$$

De fato, $-v_P(G - E) = -v_P(G) + v_P(E) = -v_P(G) + v_P(\sum_P \min \{v_P(G + (x))\} P)$. Também, $\min \{v_P(G + (x)) \mid x \in \mathcal{L}(G) \setminus \{0\}\} = v_P(G) + \min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\}$. Portanto, $-v_P(G - E) = -v_P(G) + v_P(\sum_P (v_P(G) + \min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\}) P)$. Logo, $-v_P(G - E) = -v_P(G) + v_P(\sum_P v_P(G) P) + v_P(\sum_P \min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\} P)$, que por sua vez é o mesmo que $-v_P(G) + v_P(G) + v_P(\sum_P \min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\} P)$. Por fim, obtemos que $-v_P(G - E) = -v_P(G) + v_P(G) + \min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\}$.

Então, para qualquer x não nulo em $\mathcal{L}(G)$ vale a desigualdade $v_P(x) \geq -v_P(G - E)$, ou seja, $v_P(x) + v_P(G - E) = v_P((x) + G - E) \geq 0$, $\forall$ lugar P . Podemos concluir assim que $(x) + G - E \geq 0$ e então $x \in \mathcal{L}(G - E)$. Desta forma, $\mathcal{L}(G) \subseteq \mathcal{L}(G - E)$. Agora, tome $x \in \mathcal{L}(G - E)$. Sendo $G - E \leq G$, temos que $0 \leq (x) + G - E \leq G + (x)$ e daí $(x) + G \geq 0$, o que implica que $x \in \mathcal{L}(G)$. Daí, temos que $\mathcal{L}(G - E) \subseteq \mathcal{L}(G)$. Concluimos disto que $\mathcal{L}(G) = \mathcal{L}(G - E)$. Como $\mathcal{L}(G) = \mathcal{L}(\lfloor G \rfloor)$ e o piso de G é o único divisor de grau mínimo tal que isso ocorre, segue pela proposição 4.1.1. que $G - E \geq \lfloor G \rfloor$. Suponha que $G - E > \lfloor G \rfloor$. Então existe um lugar P tal que $G - E > G - E - P \geq \lfloor G \rfloor$. Logo, $(x) + G - E > (x) + G - E - P \geq (x) + \lfloor G \rfloor \geq 0$ o que acarreta que $\mathcal{L}(G) = \mathcal{L}(\lfloor G \rfloor) \subseteq \mathcal{L}(G - E - P) \subseteq \mathcal{L}(G - E)$. Como $\mathcal{L}(G) = \mathcal{L}(G - E)$ segue que $\mathcal{L}(G - E) = \mathcal{L}(G - E - P)$. Sendo $-v_P(G - E) = \min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\}$, existe um elemento $0 \neq x_0 \in \mathcal{L}(G) = \mathcal{L}(G - E)$ tal que $v_P(x_0) = -v_P(G - E)$. Se $x_0 \in \mathcal{L}(G - E - P)$ então $(x_0) + G - E - P \geq 0$. Ou seja, $v_P(x_0) \geq -v_P(G - E - P)$ logo, $-v_P(G - E) \geq -v_P(G - E - P)$, o que contraria $v_P(G - E) > v_P(G - E - P)$. Assim, $x_0 \notin \mathcal{L}(G - E - P)$, o que é uma contradição com $\mathcal{L}(G - E) = \mathcal{L}(G - E - P)$. Portanto, $v_P(G - E) = v_P(\lfloor G \rfloor)$ para todos os lugares P de $F/\mathbb{F}_q$, e consequentemente $G - E = \lfloor G \rfloor$. ■

Teorema 4.1.1 Se G é um divisor efetivo de $F/\mathbb{F}_q$ então o piso de G também é um divisor efetivo. Em particular, se G é um divisor efetivo então o suporte de $\lfloor G \rfloor$ é um subconjunto do suporte de G .

Demonstração Como $G \geq 0$, os elementos de $\mathbb{F}_q$ pertencem à $\mathcal{L}(G)$. Logo, vale a desigualdade $-\min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\} \geq 0$. Seja $E := m.d.c. (G + (x) \mid x \in \mathcal{L}(G) \setminus \{0\})$; pela proposição 4.1.2. segue que $\lfloor G \rfloor = G - E$. Logo, $v_P(\lfloor G \rfloor) = -\min \{v_P(x) \mid x \in \mathcal{L}(G) \setminus \{0\}\}$ o que implica que $v_P(\lfloor G \rfloor) \geq 0$, $\forall P \in \mathbb{P}_F$. Assim, $\lfloor G \rfloor$ é um divisor efetivo. Como $G \geq \lfloor G \rfloor$, segue que $v_P(G) \geq v_P(\lfloor G \rfloor)$, $\forall P \in \mathbb{P}_F$, e por conseguinte o suporte do piso de G está contido no suporte de G . ■

Teorema 4.1.2 Seja G um divisor de $F/\mathbb{F}_q$ e sejam $b_1, \dots, b_t$ em $\mathcal{L}(G)$ formando um conjunto gerador para este espaço vetorial. Então, $\lfloor G \rfloor = -m.d.c. ((b_i) \mid i = 1, \dots, t)$.

Demonstração Como $b_1, \dots, b_t$ geram $\mathcal{L}(G)$ temos que $\ell(G) > 0$. Tomamos então o divisor efetivo $E := m.d.c.(G + (x) \mid x \in \mathcal{L}(G) \setminus \{0\})$. Para todo $x \in \mathcal{L}(G) \setminus \{0\}$ existem $c_1, \dots, c_t$ em $\mathbb{F}_q$ tais que $x = c_1 b_1 + \dots + c_t b_t$, com $c_i \neq 0$ para pelo menos um índice $i = 1, \dots, t$. Assim, $G + (x) = G + (c_1 b_1 + \dots + c_t b_t) \geq G + \sum_P \min\{v_P(c_1) + v_P(b_1), \dots, v_P(c_t) + v_P(b_t)\} P$.

Como $v_P(c_i) = 0, \forall i = 1, \dots, t$, segue que $G + (x) \geq G + \sum_P \min\{v_P(b_1), \dots, v_P(b_t)\} P$, e temos $m.d.c.(G + (b_i) \mid i = 1, \dots, t) = \sum_P v_P(G) P + \sum_P \min\{v_P(b_i) \mid i = 1, \dots, t\} P$.

Portanto, para $x \in \mathcal{L}(G) \setminus \{0\}$ temos que $G + (x) \geq m.d.c.(G + (b_i) \mid i = 1, \dots, t)$. Desta forma, $E \geq m.d.c.(G + (b_i) \mid i = 1, \dots, t)$. Suponha que $E > m.d.c.(G + (b_i) \mid i = 1, \dots, t)$.

Tomamos então os divisores $G + (b_1), \dots, G + (b_t)$ e $G + (x)$ para $x \neq b_i, \forall i = 1, \dots, t$. Se os mínimos dos coeficientes dos lugares destes divisores estão todos nos divisores da forma $G + (b_i), i = 1, \dots, t$, então temos que $E = m.d.c.(G + (b_i) \mid i = 1, \dots, t)$, o que é uma contradição. Se pelo menos um dos mínimos dos coeficientes dos lugares está nos divisores da forma $G + (x)$, com $x \neq b_i \forall i = 1, \dots, t$, então não vale $E > m.d.c.(G + (b_i) \mid i = 1, \dots, t)$, o que é absurdo. Portanto, $m.d.c.(G + (b_i) \mid i = 1, \dots, t) = E$. Pela proposição 4.1.2., temos $[G] = G - E$; assim, obtemos $[G] = G - E = G - G - \sum_P \min\{v_P(b_i) \mid i = 1, \dots, t\} P = -m.d.c.((b_i) \mid i = 1, \dots, t)$. ■

Proposição 4.1.3 Seja A um divisor do corpo de funções $F/\mathbb{F}_q$, com $i(A) > 0$. Suponha que A' é um divisor de $F/\mathbb{F}_q$ de grau máximo tal que $\Omega_F(A) = \Omega_F(A')$. Então, $A \leq A'$. Consequentemente, A' é o único divisor que respeita esta propriedade.

Demonstração Pela hipótese segue que, $\Omega_F(A) = \Omega_F(A) \cap \Omega_F(A')$. Mostremos que $\Omega_F(A') \cap \Omega_F(A) = \Omega_F(m.m.c.(A', A))$. Seja $0 \neq \omega \in \Omega_F(A') \cap \Omega_F(A)$. Portanto, para qualquer lugar P , $v_P(\omega) \geq \max\{v_P(A'), v_P(A)\}$. Logo, $\sum_P v_P(\omega) P \geq \sum_P \max\{v_P(A'), v_P(A)\} P$, o que acarreta $(\omega) \geq m.m.c.(A', A)$ e então $\omega \in \Omega_F(m.m.c.(A', A))$. Portanto, temos $\Omega_F(A') \cap \Omega_F(A) \subseteq \Omega_F(m.m.c.(A', A))$. Agora, se $\omega \in \Omega_F(m.m.c.(A', A))$ então, por definição, $(\omega) - \sum_P \max\{v_P(A'), v_P(A)\} P \geq 0$, para qualquer lugar P de $F/\mathbb{F}_q$. Com isso, se $-\max\{v_P(A'), v_P(A)\} \leq -v_P(A)$ então $0 \leq (\omega) - \sum_P \max\{v_P(A'), v_P(A)\} P \leq (\omega) - A \forall P$, donde obtemos que $(\omega) - A \geq 0$. Portanto, $\omega \in \Omega_F(A) = \Omega_F(A') \cap \Omega_F(A)$.

Assim, $\Omega_F(m.m.c.(A', A)) \subseteq \Omega_F(A') \cap \Omega_F(A)$. Por consequência, $\Omega_F(m.m.c.(A', A)) = \Omega_F(A') \cap \Omega_F(A)$. Segue da maximalidade do grau de A' que $\text{grau}(A') \geq \text{grau}(m.m.c.(A', A))$. Por outro lado, temos que $m.m.c.(A', A) \geq A'$; logo, $\text{grau}(m.m.c.(A', A)) \geq \text{grau}(A')$. Obtemos então que $\text{grau}(A') = \text{grau}(m.m.c.(A', A))$. Isso e o fato de que $A' \leq m.m.c.(A', A)$ acarreta que $A' = m.m.c.(A', A)$. Como $m.m.c.(A', A) \geq A$, segue que $A' \geq A$. Agora, suponha que A' e A'' são dois divisores de $F/\mathbb{F}_q$ de grau máximo tais que $\Omega_F(A) = \Omega_F(A')$ e $\Omega_F(A) = \Omega_F(A'')$. Desta maneira, $\Omega_F(A') = \Omega_F(A'')$. Do fato de A'' ser um divisor de $F/\mathbb{F}_q$ de grau máximo tal que $\Omega_F(A') = \Omega_F(A'')$, do feito acima, isso implica que $A' \leq A''$. Similarmente, segue que $A'' \leq A'$, uma vez que A' é um divisor de $F/\mathbb{F}_q$ de grau máximo tal que $\Omega_F(A'') = \Omega_F(A')$. Portanto, $A' = A''$. Consequentemente, existe um único divisor A' de $F/\mathbb{F}_q$ de grau máximo satisfazendo $\Omega_F(A) = \Omega_F(A')$. ■

Definição 4.1.3 Dado um divisor A do corpo de funções $F/\mathbb{F}_q$, com $i(A) > 0$, o teto de A é o único divisor A' de $F/\mathbb{F}_q$ de grau máximo tal que $\Omega_F(A) = \Omega_F(A')$. O teto de A será denotado por $\lceil A \rceil$.

Corolário 4.1.2 Sejam A_1 e A_2 divisores do corpo de funções $F/\mathbb{F}_q$, com $i(A_1) > 0$ e $i(A_2) > 0$. Então, $\Omega_F(A_1) = \Omega_F(A_2) \iff \lceil A_1 \rceil = \lceil A_2 \rceil$.

Demonstração Suponha que vale $\Omega_F(A_1) = \Omega_F(A_2)$. Seja A' o teto de A_1 . Então, A' é o único divisor de $F/\mathbb{F}_q$ de grau máximo tal que ocorre $\Omega_F(A') = \Omega_F(A_1)$. Como $\Omega_F(A_1) = \Omega_F(A_2)$, temos que $\Omega_F(A') = \Omega_F(A_2)$. Desta maneira, A' é o teto de A_2 . Portanto, $\lceil A_1 \rceil = \lceil A_2 \rceil$. Reciprocamente, suponha que $\lceil A_1 \rceil = \lceil A_2 \rceil$. Assim, $\Omega_F(A_1) = \Omega_F(\lceil A_1 \rceil) = \Omega_F(\lceil A_2 \rceil) = \Omega_F(A_2)$. ■

Os próximos dois resultados nos mostram como se faz para encontrar o teto de um divisor.

Proposição 4.1.4 Seja A um divisor de $F/\mathbb{F}_q$, com $i(A) > 0$. Definimos o divisor E da seguinte maneira $E := m.d.c.((\omega) \mid \omega \in \Omega_F(A) \setminus \{0\})$. Então, $\lceil A \rceil = E$.

Demonstração Pela definição de máximo divisor comum, observamos que para qualquer lugar P de $F/\mathbb{F}_q$ segue que $\min\{v_P(\omega) \mid \omega \in \Omega_F(A) \setminus \{0\}\} = v_P(E)$. Então, para qualquer $\omega \in \Omega_F(A) \setminus \{0\}$ temos que, $v_P(\omega) \geq v_P(E)$ logo, $(\omega) \geq E$. Desta forma $\omega \in \Omega_F(E)$ e por conseguinte $\Omega_F(A) \subseteq \Omega_F(E)$. Note agora que $E \geq A$. De fato, tomando quaisquer elementos ω em $\Omega_F(A) \setminus \{0\}$, temos que $v_P(\omega) \geq v_P(A)$, para todo lugar P , e então $\min\{v_P(\omega) \mid \omega \in \Omega_F(A) \setminus \{0\}\} \geq v_P(A)$ e desta forma $E \geq A$. Logo, sendo $\eta \in \Omega_F(E)$ temos $(\eta) \geq E \geq A$ e assim $\eta \in \Omega_F(A)$. Portanto, $\Omega_F(E) \subseteq \Omega_F(A)$. Consequentemente, $\Omega_F(E) = \Omega_F(A)$. Pela definição, temos que $\lceil A \rceil$ é o único divisor de grau máximo de $F/\mathbb{F}_q$ tal que vale o seguinte $\Omega_F(A) = \Omega_F(\lceil A \rceil)$. Logo, $\Omega_F(E) = \Omega_F(\lceil A \rceil)$. Pela proposição 4.1.3., ocorre que $E \leq \lceil A \rceil$. Suponha que $E < \lceil A \rceil$. Assim, existe um lugar P tal que $v_P(E) < v_P(\lceil A \rceil)$ e então $E + P \leq \lceil A \rceil$. Com isso, $\Omega_F(\lceil A \rceil) \subseteq \Omega_F(E + P)$ e como $E < E + P$ segue que $\Omega_F(E + P) \subseteq \Omega_F(E)$. Portanto, $\Omega_F(A) = \Omega_F(\lceil A \rceil) \subseteq \Omega_F(E + P) \subseteq \Omega_F(E)$. Sendo $\Omega_F(A) = \Omega_F(E)$ segue que $\Omega_F(E) = \Omega_F(E + P)$. Como temos $v_P(E) = \min\{v_P(\omega) \mid \omega \in \Omega_F(A) \setminus \{0\}\}$, existe $0 \neq \omega_0 \in \Omega_F(A)$ tal que $v_P(\omega_0) = v_P(E)$. Note que $\omega_0 \in \Omega_F(E)$, visto que $\Omega_F(A) = \Omega_F(E)$. Mostremos que $\omega_0 \notin \Omega_F(E + P)$. De fato, se ocorre o contrário temos que $(\omega_0) \geq E + P$ e assim, se $(\omega_0) \geq E + P$ então $v_P(\omega_0) \geq v_P(E + P)$ donde vemos que $v_P(E) \geq v_P(E) + v_P(P)$. Logo, $0 \geq 1$, o que é absurdo.

Portanto, $\omega_0 \notin \Omega_F(E + P)$, o que é uma contradição, uma vez que $\Omega_F(E) = \Omega_F(E + P)$. Desta maneira, $v_P(E) = v_P(\lceil A \rceil)$ para todos os lugares P de $F/\mathbb{F}_q$, e assim obtemos que $E = \lceil A \rceil$. ■

Teorema 4.1.3 Seja A um divisor de $F/\mathbb{F}_q$ com índice de especialidade positivo e seja o conjunto $\{\eta_1, \dots, \eta_t\} \subseteq \Omega_F(A) \setminus \{0\}$, um conjunto de geradores para o F -espaço vetorial $\Omega_F(A)$. Então, $\lceil A \rceil = m.d.c.((\eta_i) \mid i = 1, \dots, t)$.

Demonstração Seja $E := m.d.c.((\eta_i) \mid i = 1, \dots, t)$. Para cada $i = 1, \dots, t$, temos que $\eta_i \in \Omega_F(A) = \Omega_F(\lceil A \rceil)$; logo, $(\eta_i) \geq \lceil A \rceil$, $\forall i = 1, \dots, t$. Com isso, para qualquer lugar P , obtemos que $v_P(\eta_i) \geq v_P(\lceil A \rceil)$ e deste modo $\lceil A \rceil \leq m.d.c.((\eta_i) \mid i = 1, \dots, t) = E$. Da proposição anterior temos que $\lceil A \rceil = m.d.c.((\eta) \mid \eta \in \Omega_F(A) \setminus \{0\})$. Seja agora P um lugar de $F/\mathbb{F}_q$ e escolhamos η em $\Omega_F(A) = \Omega_F(\lceil A \rceil)$ tal que $v_P(\eta) = v_P(\lceil A \rceil)$. Escolhemos um elemento $x \in F$ tal que x é um uniformizante local para P , isto é, $v_P(x) = 1$ e então temos que x é variável separante para o corpo de funções $F/\mathbb{F}_q$. Já que $\Omega_{F/\mathbb{F}_q}^1$ é isomorfo à $\Omega_{F/\mathbb{F}_q}$, podemos encarar $\eta_i \forall i = 1, \dots, t$, como uma forma diferencial e então η_i se escreve unicamente na forma $\eta_i = x_i dx$, onde $x_i \in F$. Sendo $\{\eta_1, \dots, \eta_t\}$ um conjunto gerador para o K -espaço vetorial $\Omega_F(A)$, existem $a_i \in \mathbb{F}_q$ não nulos tais que $\eta = a_1 x_1 dx + a_2 x_2 dx + \dots + a_t x_t dx$, e então obtemos que $(\eta) = (a_1 x_1 + a_2 x_2 + \dots + a_t x_t) dx$. Por definição temos $v_P(\eta) = v_P(a_1 x_1 + a_2 x_2 + \dots + a_t x_t)$. Assim, é imediato que $v_P(\eta) \geq \min\{v_P(x_i) \mid a_i \neq 0, \forall i\} = \min\{v_P(\eta_i) \mid a_i \neq 0, \forall i\}$. Uma vez que o máximo divisor comum entre dois divisores é o divisor cujos coeficientes dos lugares é o mínimo entre os coeficientes dos lugares dos dois divisores, segue que:

$$\min\{v_P(\eta_i) \mid a_i \neq 0, \forall i\} = v_P(m.d.c.((\eta) \mid a_i \neq 0)) \geq v_P(m.d.c.((\eta_i) \mid i = 1, \dots, t)).$$

Portanto, $v_P(\lceil A \rceil) \geq v_P(E)$, para todo lugar P , e então $\lceil A \rceil \geq E$.

Conclusão: $\lceil A \rceil = E$. ■

Dado um divisor A de $F/\mathbb{F}_q$ e um conjunto gerador $\{\eta_1, \dots, \eta_t\}$ para $\Omega_F(A)$, como F -espaço vetorial, o teorema anterior mostra que o suporte do teto de A está contido na união dos suportes de $(\eta_1), \dots, (\eta_t)$.

Proposição 4.1.5 Seja A um divisor de $F/\mathbb{F}_q$ com $i(A) > 0$. Se W é um divisor canônico de $F/\mathbb{F}_q$ com a propriedade de que $W \geq A$, então $W \geq \lceil A \rceil$.

Demonstração Como W é um divisor canônico temos que $W = (\eta)$ para alguma diferencial de Weil $\eta \in \Omega_F \setminus \{0\}$. Então, $W \geq A$ implica que $(\eta) \geq A$ e assim $\eta \in \Omega_F(A) = \Omega_F(\lceil A \rceil)$. Desta forma, segue que $(\eta) \geq \lceil A \rceil$, ou seja, $W \geq \lceil A \rceil$. ■

O resultado a seguir estabelece uma relação entre o piso e o teto de um divisor, e também nos mostra como computar o teto de um divisor.

Teorema 4.1.4 Sejam A um divisor e W um divisor canônico de $F/\mathbb{F}_q$.

(a) Se $i(A) > 0$ então $W - \lceil A \rceil = \lfloor W - A \rfloor$.

(b) Se $\ell(A) > 0$ então $W - \lfloor A \rfloor = \lceil W - A \rceil$.

Demonstração (a) Sendo W um divisor canônico existe uma diferencial de Weil $0 \neq \eta \in \Omega_F$ tal que $W = (\eta)$. Pelo teorema 2.5.2. temos que $\mathcal{L}(W - A)$ é isomorfo à $\Omega_F(A)$. Temos também que $\mathcal{L}(W - A) = \mathcal{L}(\lfloor W - A \rfloor)$ e $\Omega_F(A) = \Omega_F(\lceil A \rceil)$. Por conseguinte $\mathcal{L}(\lfloor W - A \rfloor)$ é isomorfo à $\Omega_F(\lceil A \rceil)$. Agora, tomemos a aplicação $\phi : \Omega_F(\lceil A \rceil) \longrightarrow \mathcal{L}(W - \lceil A \rceil)$ dada por $\phi(\omega) = \frac{\omega}{\eta}$. Observe que $(\omega/\eta) + W - \lceil A \rceil = (\omega) - (\eta) + W - \lceil A \rceil = (\omega) - W + W - \lceil A \rceil = (\omega) - \lceil A \rceil \geq 0$,

pois $\omega \in \Omega_F(\lceil A \rceil)$. Logo, ϕ é bem definida e é F -linear. Temos que ϕ é sobrejetora: de fato, dado $x \in \mathcal{L}(W - \lceil A \rceil)$ temos então que $(x) + W - \lceil A \rceil \geq 0$ o que acarreta $(x) + (\eta) - \lceil A \rceil \geq 0$, ou seja, $(x\eta) \geq \lceil A \rceil$ e desta maneira $x\eta \in \Omega_F(\lceil A \rceil) = \Omega_F(A)$; daí basta tomar $x\eta \in \Omega_F(A)$ que teremos $\phi(x\eta) = x$. Também, ϕ é injetora: de fato, $\phi(\omega) = \phi(\lambda) \Rightarrow \frac{\omega}{\eta} = \frac{\lambda}{\eta} \Rightarrow \omega = \lambda$. Portanto, segue disto que ϕ é isomorfismo. Por outro lado, já vimos que o isomorfismo entre $\mathcal{L}(W - A)$ e $\Omega_F(A)$ é dado por $x \mapsto x\eta$; logo, sendo μ este isomorfismo temos que, $(\phi \circ \mu)(x) = \phi(x\eta) = x$ e $(\mu \circ \phi)(x) = \mu\left(\frac{x}{\eta}\right) = \omega$.

Assim, a composta destas aplicações é a aplicação identidade.

Isto implica que $\mathcal{L}(W - \lceil A \rceil) = \mathcal{L}(\lfloor W - A \rfloor) = \mathcal{L}(W - A)$. Por definição, $\lfloor W - A \rfloor$ é o único divisor de grau mínimo tal que $\mathcal{L}(\lfloor W - A \rfloor) = \mathcal{L}(W - \lceil A \rceil)$; por sua vez $\lfloor W - A \rfloor$ é o único divisor de grau mínimo tal que $\mathcal{L}(\lfloor W - A \rfloor) = \mathcal{L}(W - A)$. Como $\mathcal{L}(W - A) = \mathcal{L}(W - \lceil A \rceil)$ temos que $\lfloor W - A \rfloor$ satisfaz $\mathcal{L}(\lfloor W - A \rfloor) = \mathcal{L}(W - \lceil A \rceil)$; assim, $\lfloor W - A \rfloor = \lfloor W - A \rfloor$. Sendo $W - \lceil A \rceil \geq \lfloor W - A \rfloor$, obtemos que $W - \lceil A \rceil \geq \lfloor W - A \rfloor$. Suponha que ocorra a desigualdade estrita. Então, existe um lugar P tal que $W - \lceil A \rceil \geq \lfloor W - A \rfloor + P$; logo, $W - \lceil A \rceil - P \geq \lfloor W - A \rfloor$. Assim, $\mathcal{L}(\lfloor W - A \rfloor) \subseteq \mathcal{L}(W - \lceil A \rceil - P)$, ou seja, $\mathcal{L}(W - \lceil A \rceil) \subseteq \mathcal{L}(W - \lceil A \rceil - P)$. Também, $W - \lceil A \rceil \geq W - \lceil A \rceil - P$ e então $\mathcal{L}(W - \lceil A \rceil - P) \subseteq \mathcal{L}(W - \lceil A \rceil)$. Portanto, $\mathcal{L}(W - \lceil A \rceil - P) = \mathcal{L}(W - \lceil A \rceil)$. Temos, pelo teorema 2.5.2., que $\mathcal{L}(W - \lceil A \rceil - P)$ é isomorfo à $\Omega_F(\lceil A \rceil + P)$ e $\mathcal{L}(W - \lceil A \rceil)$ é isomorfo à $\Omega_F(\lceil A \rceil)$. Como temos a igualdade de espaços vetoriais, $\mathcal{L}(W - \lceil A \rceil - P) = \mathcal{L}(W - \lceil A \rceil)$ segue que $\Omega_F(\lceil A \rceil + P)$ é isomorfo à $\Omega_F(\lceil A \rceil)$. Assim, esses espaços vetoriais sobre o corpo F possuem a mesma dimensão finita. Como $\lceil A \rceil + P \geq \lceil A \rceil$ temos $\Omega_F(\lceil A \rceil + P) \subseteq \Omega_F(\lceil A \rceil)$. Concluimos com isso que $\Omega_F(\lceil A \rceil + P) = \Omega_F(\lceil A \rceil) = \Omega_F(A)$. Sendo $\text{grau}(\lceil A \rceil + P) > \text{grau}(\lceil A \rceil)$ temos uma contradição com o fato de que $\lceil A \rceil$ é o único divisor de grau máximo tal que $\Omega_F(\lceil A \rceil) = \Omega_F(A)$. Então, $W - \lceil A \rceil = \lfloor W - A \rfloor$.

(b) Seja $\tilde{A}$ um divisor qualquer de $F/\mathbb{F}_q$ com $\ell(\tilde{A}) > 0$. Tome $A = W - \tilde{A}$. Note que $i(A) > 0$. De fato, $i(A) = i(W - \tilde{A})$ e, por definição, $i(W - \tilde{A}) = \ell(W - \tilde{A}) - \text{grau}(W - \tilde{A}) + g - 1 = \ell(W - \tilde{A}) - (2g - 2) + \text{grau}(\tilde{A}) + g - 1 = \ell(W - \tilde{A}) - g + 1 + \text{grau}(\tilde{A})$; pelo teorema de Riemann-Roch temos que $\ell(W - \tilde{A}) = \ell(\tilde{A}) - \text{grau}(\tilde{A}) - 1 + g$; assim, $i(W - \tilde{A}) = \ell(\tilde{A}) - \text{grau}(\tilde{A}) - 1 + g - g + 1 + \text{grau}(\tilde{A}) = \ell(\tilde{A}) > 0$. Logo, $i(A) > 0$. Pelo item (a) temos que $W - \lceil A \rceil = \lfloor W - A \rfloor$ e daí segue que $W - \lceil W - \tilde{A} \rceil = \lfloor W - W + \tilde{A} \rfloor$, isto é, $W - \lceil W - \tilde{A} \rceil = \lfloor \tilde{A} \rfloor$ e então, $\lceil W - \tilde{A} \rceil = W - \lfloor \tilde{A} \rfloor$, como queríamos demonstrar. ■

Observação 4.1.1 Seja W um divisor canônico e A um divisor com $i(A) > 0$. Como mencionado na demonstração do teorema anterior, existe um isomorfismo entre $\Omega_F(A)$ e $\mathcal{L}(W - A)$. Consequentemente, de acordo com a definição de teto de um divisor, segue que o teto do divisor A é o único divisor tal que:

$$\mathcal{L}(W - \lceil A \rceil) = \mathcal{L}(W - A) \text{ e } \text{grau}(\lceil A \rceil) = \max \{ \text{grau}(A') \mid \mathcal{L}(W - A) = \mathcal{L}(W - A') \}.$$

Observamos também que como $W - A$ é um divisor de $F/\mathbb{F}_q$ com $\ell(W - A) > 0$, tomando $E_{W-A} := m.d.c.(W - A + (x) \mid x \in \mathcal{L}(W - A) \setminus \{0\})$ segue que $\lfloor W - A \rfloor = W - A - E_{W-A}$. Pelo item (a) do teorema anterior, temos que $\lfloor W - A \rfloor = W - \lceil A \rceil$; logo, $W - \lceil A \rceil = W - A - E_{W-A}$ o que nos fornece a igualdade $\lceil A \rceil = A + E_{W-A}$.

Em seguida, vamos exibir alguns divisores que são iguais a seus pisos ou tetos e também mostrar algumas relações entre o piso e o teto.

Corolário 4.1.3 Seja z um elemento não nulo de F , A um divisor e W um divisor canônico de $F/\mathbb{F}_q$.

- (a) Se $i(A) > 0$ então $\lceil A + (z) \rceil = \lceil A \rceil + (z)$.
- (b) Se $\ell(A) > 0$ então $\lfloor A + (z) \rfloor = \lfloor A \rfloor + (z)$.
- (c) $\lfloor (z) \rfloor = (z)$, $\lfloor (z)_0 \rfloor = (z)_0$ e $\lfloor (z)_\infty \rfloor = (z)_\infty$.
- (d) $\lceil W - (z)_0 \rceil = W - (z)_0$; $\lceil W - (z)_\infty \rceil = W - (z)_\infty$ e $\lceil W - (z) \rceil = W - (z)$.

Demonstração (a) Seja $x \in F$ um elemento separável. Então, como o divisor de uma forma diferencial é um divisor canônico segue que tomando a forma diferencial dx e sabendo que o divisor de uma forma diferencial é o divisor da correspondente diferencial de Weil associada por ela temos que $\lfloor (dx) - ((z) + A) \rfloor = (dx) - \lceil (z) + A \rceil$, valendo isso pelo teorema anterior. Também, $\lfloor ((dx) - (z)) - A \rfloor = (dx) - (z) - \lceil A \rceil$, pois $(dx) - (z)$ é um divisor canônico. Desta forma, obtemos por comparação que $\lceil (z) + A \rceil = (z) + \lceil A \rceil$.

(b) Seja $x \in F$ um elemento separável. Então, tomamos a forma diferencial de $F/\mathbb{F}_q$, dx , e como o divisor de uma forma diferencial é um divisor canônico, temos que $\lceil (dx) - ((z) + A) \rceil = (dx) - \lfloor (z) + A \rfloor$, pelo teorema anterior, item (b) e também que $\lceil (dx) - (z) - A \rceil = (dx) - (z) - \lfloor A \rfloor$. Logo, $\lfloor A + (z) \rfloor = \lfloor A \rfloor + (z)$.

(c) Da parte (b), tomando $A = 0$ temos $\lfloor (z) \rfloor = \lfloor A + (z) \rfloor = \lfloor 0 \rfloor + (z) = (z)$. Agora, seja $A = (z)_\infty$. Então, como $(z) + (z)_\infty \geq 0$ segue que $z \in \mathcal{L}(A)$, de modo que $\mathcal{L}(A) \neq \{0\}$ e daí $\ell(A) > 0$. Pela parte (b), temos que $\lfloor (z)_\infty + (z) \rfloor = \lfloor (z)_\infty \rfloor + (z)$; daí $\lfloor (z)_\infty + (z)_0 - (z)_\infty \rfloor = \lfloor (z)_\infty \rfloor + (z)_0 - (z)_\infty$. Logo, $\lfloor (z)_0 \rfloor = \lfloor (z)_\infty \rfloor + (z)_0 - (z)_\infty$ de modo que, $\lfloor (z)_0 \rfloor - (z)_0 = \lfloor (z)_\infty \rfloor - (z)_\infty$. Temos que se A é um divisor efetivo então o suporte do piso de A está contido no suporte de A . Como $(z)_0 \geq 0$, segue que o suporte de $\lfloor (z)_0 \rfloor$ está contido no suporte de $(z)_0$ e como $(z)_\infty \geq 0$ também obtemos que o suporte de $\lfloor (z)_\infty \rfloor$ está contido no suporte de $(z)_\infty$. Os divisores de zeros e de pólos de z possuem suporte disjunto e então o mesmo é verdade para os divisores $\lfloor (z)_0 \rfloor$ e $\lfloor (z)_\infty \rfloor$. Mas, como visto logo acima, temos que $\lfloor (z)_0 \rfloor - (z)_0 - \lfloor (z)_\infty \rfloor + (z)_\infty = 0$. Daí, $(z)_0 = \lfloor (z)_0 \rfloor$ e $(z)_\infty = \lfloor (z)_\infty \rfloor$.

(d) Observe que $W - (z)_0 \leq W$ logo, $-\text{grau}(W - (z)_0) \geq -\text{grau}(W)$ e então,

$$\ell(W - (z)_0) - \text{grau}(W - (z)_0) + g - 1 \geq \ell(W) - \text{grau}(W) + g - 1 = g - (2g - 2) + g - 1 = -g + 2 + g - 1 = 1 > 0, \text{ ou seja, } i(W - (z)_0) > 0.$$

De forma completamente análoga temos que, $i(W - (z)_\infty) > 0$.

Agora, seja $A = W - (z)_0$; pela parte (a) segue que $\lceil W - (z)_0 + (z) \rceil = \lceil W - (z)_0 \rceil + (z)$. Mas, $\lceil W - (z)_0 + (z) \rceil = \lceil W - (z)_\infty \rceil$, pois $(z) = (z)_0 - (z)_\infty$. Como $\ell((z)_\infty) > 0$ segue pelo teorema anterior, item (b), que $\lceil W - (z)_\infty \rceil = W - \lfloor (z)_\infty \rfloor$. Pelo item (c) deste corolário vemos o seguinte $\lfloor (z)_\infty \rfloor = (z)_\infty$ logo, $\lceil W - (z)_0 + (z) \rceil = W - (z)_\infty$. Desta forma, $\lceil W - (z)_0 \rceil + (z) = W - (z)_\infty$ e conseqüentemente, $\lceil W - (z)_0 \rceil + (z)_0 - (z)_\infty = W - (z)_\infty$ implica que $\lceil W - (z)_0 \rceil = W - (z)_0$. Mostremos agora que $\lceil W - (z)_\infty \rceil = W - (z)_\infty$. Note que $W = (\eta)$, para $\eta \in \Omega_F \setminus \{0\}$. Assim, $(\eta) + (z) = (z\eta)$ é um divisor canônico, pois na definição 2.5.5. vimos que $z\eta$ é uma diferencial de Weil. Logo, em $\lceil W - (z)_0 \rceil = W - (z)_0$ substituímos W por $W + (z)$ e então $\lceil W + (z) - (z)_0 \rceil = W + (z) - (z)_0$, o que implica $\lceil W - (z)_\infty \rceil = W - (z)_\infty$. Provemos agora que $\lceil W - (z) \rceil = W - (z)$. Tomemos $\tilde{z}$ um elemento não nulo de $\mathbb{F}_q$; daí segue que $(\tilde{z}) = 0$. Dessa forma, $\ell((\tilde{z})) = \ell(0) = 1 > 0$. Pelo item (b) do teorema 4.1.4. temos que $\lceil W - (\tilde{z}) \rceil = W - \lfloor (\tilde{z}) \rfloor$ e então, $\lceil W \rceil = W$. É visto que $W - (z)$ também é um divisor canônico, pois $W - (z) = W + (z^{-1}) = (z^{-1}\eta)$ e, como vimos na definição 2.5.5., $z^{-1}\eta$ é uma diferencial de Weil. Assim, aplicando o item (b) do teorema 4.1.4. obtemos que $\lceil W - (z) \rceil = W - (z)$. ■

4.2 As cotas do piso e do piso generalizada

A principal motivação para o estudo das noções de piso e teto de um divisor é que elas nos levam a uma melhor avaliação da distância mínima de códigos. Veremos duas cotas para a distância mínima muito importantes envolvendo o piso de um divisor que, de uma certa forma, nos levarão a uma cota para esta mesma distância com o auxílio do teto de um divisor. Vamos agora introduzir o teorema da cota do piso, que daremos uma generalização denominada cota do piso generalizada. Em seguida, daremos alguns exemplos onde vamos aplicar esta cota para estimar melhorias da distância mínima de alguns códigos.

Teorema 4.2.1 (Cota do piso) Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g . Seja $D := P_1 + \dots + P_n$, onde $P_1, \dots, P_n$ são lugares dois a dois distintos de $F/\mathbb{F}_q$, que possuem todos grau igual à um, e seja $G := H + \lfloor H \rfloor$, um divisor de $F/\mathbb{F}_q$ tal que H é um divisor efetivo cujo suporte não contém quaisquer dos lugares $P_1, \dots, P_n$. Seja $E_H := H - \lfloor H \rfloor$. Então, $C_\Omega(D, G)$ é um código $[n, k, d]$ cuja distância mínima satisfaz:

$$d = d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(E_H) = 2\text{grau}(H) - (2g - 2).$$

Demonstração Como H é um divisor efetivo, temos que $\lfloor H \rfloor$ é efetivo e $\text{supp}(\lfloor H \rfloor) \subseteq \text{supp}(H)$. Assim, $G := H + \lfloor H \rfloor$ é um divisor efetivo e como os suportes dos divisores H e D são disjuntos, segue que os suportes dos divisores G e D também são disjuntos. Escolhemos uma diferencial de Weil $\eta \in \Omega_F(G - D)$ tal que a palavra código $c_0 := (\eta_{P_1}(1), \dots, \eta_{P_n}(1))$ é de peso mínimo. Por definição, a distância mínima de um código é o mínimo do conjunto dos pesos das palavras código não nulas; assim, podemos assumir, sem perda de generalidade, que as primeiras d -coordenadas de c_0 são não nulas e que as coordenadas restantes são nulas. Então,

sendo $D' := P_1 + \dots + P_d$ obtemos que $(\eta) \geq G - D'$, uma vez que como $\text{supp}(D') \subseteq \text{supp}(D)$ e $(\eta) \geq G - D$ segue que $v_Q(\eta) \geq v_Q(G - D)$, para todo lugar Q de $F/\mathbb{F}_q$ que pertence ao suporte de D e então, em particular, isso vale para todo lugar que pertence ao suporte de D' . Deste modo, existe um divisor efetivo A tal que $(\eta) = G - D' + A$ e cujo suporte não contém quaisquer dos lugares $P_1, \dots, P_d$. Na igualdade $(\eta) = G - D' + A$, tomamos o grau dos divisores em ambos os lados, e por consequência temos que $\text{grau}((\eta)) = \text{grau}(G) - d + \text{grau}(A)$, e como $\text{grau}((\eta)) = 2g - 2$, pois (η) é divisor canônico, segue que $2g - 2 = \text{grau}(G) - d + \text{grau}(A)$, donde $d = \text{grau}(G) - (2g - 2) + \text{grau}(A)$. A fim de provar a afirmação sobre a cota da distância mínima, é suficiente mostrar que $\text{grau}(A) \geq \text{grau}(E_H)$. Observe que $\text{grau}(A) \geq \ell(H + A) - \ell(H) = \ell(H + A) - \ell(\lfloor H \rfloor) \geq \ell(H + A) - \ell(\lfloor H \rfloor + A)$. De fato,

(1) $\text{grau}(A) \geq \ell(H + A) - \ell(H)$, pois como $A \geq 0$ temos que $H + A \geq H$ e então, pelo lema 2.4.3., segue que $\ell(H + A) - \ell(H) \leq \text{grau}(H + A) - \text{grau}(H) = \text{grau}(A)$. Portanto, $\text{grau}(A) \geq \ell(H + A) - \ell(H)$.

(2) $\ell(H + A) - \ell(H) = \ell(H + A) - \ell(\lfloor H \rfloor)$, pois como $\mathcal{L}(H) = \mathcal{L}(\lfloor H \rfloor)$, temos $\ell(H) = \ell(\lfloor H \rfloor)$ e daí segue a igualdade desejada.

(3) $\ell(H + A) - \ell(\lfloor H \rfloor) \geq \ell(H + A) - \ell(\lfloor H \rfloor + A)$, uma vez que como $\lfloor H \rfloor \leq \lfloor H \rfloor + A$ segue que $\mathcal{L}(\lfloor H \rfloor) \subseteq \mathcal{L}(\lfloor H \rfloor + A)$; logo, $\ell(\lfloor H \rfloor) \leq \ell(\lfloor H \rfloor + A)$ e então $-\ell(\lfloor H \rfloor) \geq -\ell(\lfloor H \rfloor + A)$ e somando $\ell(H + A)$ de ambos os lados desta desigualdade temos o resultado.

Mostremos agora que $\text{grau}(E_H) = \ell(H + A) - \ell(\lfloor H \rfloor + A)$. Temos $W = G - D' + A$ divisor canônico. Tomando o divisor $H + A$ e o divisor $\lfloor H \rfloor + A$, pelo teorema de Riemann-Roch obtemos as seguintes igualdades:

$$(i) \ell(H + A) = \text{grau}(H + A) + 1 - g + \ell(W - H - A) \text{ e}$$

$$(ii) \ell(\lfloor H \rfloor + A) = \text{grau}(\lfloor H \rfloor + A) + 1 - g + \ell(W - \lfloor H \rfloor - A).$$

Assim, $\ell(H + A) - \ell(\lfloor H \rfloor + A) = \text{grau}(H) + \ell(W - H - A) - \text{grau}(\lfloor H \rfloor) - \ell(W - \lfloor H \rfloor - A)$. Portanto, $\ell(H + A) - \ell(\lfloor H \rfloor + A) = \text{grau}(H - \lfloor H \rfloor) + \ell(W - H - A) - \ell(W - \lfloor H \rfloor - A) = \text{grau}(E_H) + \ell(W - H - A) - \ell(W - \lfloor H \rfloor - A)$. Como $W - A = G - D'$ e $G = H + \lfloor H \rfloor$, obtemos a expressão final:

$$\ell(H + A) - \ell(\lfloor H \rfloor + A) = \text{grau}(E_H) + \ell(\lfloor H \rfloor - D') - \ell(H - D').$$

Para completar a demonstração, mostremos que $\mathcal{L}(\lfloor H \rfloor - D') = \mathcal{L}(H - D')$. Como $H - D' \leq H$, segue que $\mathcal{L}(H - D') \subseteq \mathcal{L}(H)$ e então $\mathcal{L}(H - D') \subseteq \mathcal{L}(\lfloor H \rfloor)$, donde $\mathcal{L}(H - D') = \mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor)$. Mostremos que $\mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor) = \mathcal{L}(m.d.c.(H - D'; \lfloor H \rfloor))$. Tome $0 \neq x \in \mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor)$ logo, $(x) + H - D' \geq 0$ e $(x) + \lfloor H \rfloor \geq 0$ e então para todo lugar P vemos que $v_P((x) + H - D') \geq 0$ e $v_P((x) + \lfloor H \rfloor) \geq 0$ e assim,

$$\min \{v_P((x) + H - D'); v_P((x) + \lfloor H \rfloor)\} = v_P((x)) + \min \{v_P(H - D'); v_P(\lfloor H \rfloor)\} \geq 0,$$

para todo lugar P de $F/\mathbb{F}_q$. Com isso, $\sum_P (v_P((x)) + \min \{v_P(H - D'); v_P(\lfloor H \rfloor)\}) P \geq 0$. Portanto segue que, $(x) + m.d.c.(H - D'; \lfloor H \rfloor) \geq 0$ e então $x \in \mathcal{L}(m.d.c.(H - D', \lfloor H \rfloor))$. Deste modo, $\mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor) \subseteq \mathcal{L}(m.d.c.(H - D', \lfloor H \rfloor))$.

Se $0 \neq x \in \mathcal{L}(m.d.c.(H - D', \lfloor H \rfloor))$ por definição temos que, $(x) + m.d.c.(H - D', \lfloor H \rfloor) \geq 0$. Temos que, $\min \{v_P(H - D'), v_P(\lfloor H \rfloor)\} \leq v_P(H - D'), \forall$ lugar P . Desta maneira é visto o seguinte, $0 \leq (x) + m.d.c.(H - D', \lfloor H \rfloor) \leq (x) + (H - D')$; logo $x \in \mathcal{L}(H - D') \subseteq \mathcal{L}(\lfloor H \rfloor)$ e daí $x \in \mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor)$. Portanto, vale a inclusão $\mathcal{L}(m.d.c.(H - D', \lfloor H \rfloor)) \subseteq \mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor)$. Assim, chegamos à igualdade desejada $\mathcal{L}(m.d.c.(H - D', \lfloor H \rfloor)) = \mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor)$. Por hipótese, $\text{supp}(H) \cap \text{supp}(D) = \emptyset$ e sendo D' um divisor efetivo tal que $D' \leq D$ temos que $\text{supp}(H) \cap \text{supp}(D') = \emptyset$ e como $\text{supp}(\lfloor H \rfloor) \subseteq \text{supp}(H)$ segue que $\text{supp}(\lfloor H \rfloor) \cap \text{supp}(D') = \emptyset$. Pela definição, o máximo divisor comum entre $H - D'$ e $\lfloor H \rfloor$ é o divisor cujos coeficientes dos lugares são os mínimos dos coeficientes dos lugares de $H - D'$ e $\lfloor H \rfloor$, e sendo $H \geq \lfloor H \rfloor$ concluimos que $m.d.c.(H - D', \lfloor H \rfloor) = \lfloor H \rfloor - D'$. Isto implica que $\mathcal{L}(m.d.c.(H - D', \lfloor H \rfloor)) = \mathcal{L}(\lfloor H \rfloor - D')$ e, como $\mathcal{L}(m.d.c.(H - D', \lfloor H \rfloor)) = \mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor) = \mathcal{L}(H - D')$, pois $\mathcal{L}(H - D') \subseteq \mathcal{L}(\lfloor H \rfloor)$, obtemos que $\mathcal{L}(\lfloor H \rfloor - D') = \mathcal{L}(H - D')$. Segue então que:

$$d = d(C_\Omega(D, G)) = \text{grau}(G) - (2g - 2) + \text{grau}(A) \geq \text{grau}(G) - (2g - 2) + \text{grau}(E_H) = \text{grau}(H) + \text{grau}(\lfloor H \rfloor) - (2g - 2) + \text{grau}(H) - \text{grau}(\lfloor H \rfloor) = 2\text{grau}(H) - (2g - 2).$$

■

Corolário 4.2.1 (da Cota do piso) Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g . Seja $D := P_1 + \dots + P_n$, onde $P_1, \dots, P_n$ são lugares dois a dois distintos de grau um de $F/\mathbb{F}_q$ e seja o divisor $G := H + A$, onde H e A são divisores efetivos tal que o suporte de H não contém quaisquer dos lugares $P_1, \dots, P_n$ e $\lfloor H \rfloor \leq A \leq H$. Então, $C_\Omega(D, G)$ é um código $[n, k, d]$ cuja distância mínima d satisfaz a desigualdade:

$$d = d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(H - A).$$

Demonstração Note que, pela hipótese, $H + \lfloor H \rfloor - D \leq H + A - D$ e isto implica que $C_\Omega(D, H + A) \subseteq C_\Omega(D, H + \lfloor H \rfloor)$. De fato, sendo $\omega \in \Omega_F(H + A - D) \setminus \{0\}$ segue que $(\omega) \geq H + A - D \geq H + \lfloor H \rfloor - D$ e então $\omega \in \Omega_F(H + \lfloor H \rfloor - D)$ e assim, $\Omega_F(H + A - D) \subseteq \Omega_F(H + \lfloor H \rfloor - D)$. Visto isso, seja $(\eta_{P_1}(1), \dots, \eta_{P_n}(1)) \in C_\Omega(D, H + A)$. Desta forma, temos que a diferencial de Weil η é tal que $\eta \in \Omega_F(H + A - D) \subseteq \Omega_F(H + \lfloor H \rfloor - D)$ e logo $(\eta_{P_1}(1), \dots, \eta_{P_n}(1)) \in C_\Omega(D, H + \lfloor H \rfloor)$. Portanto, $C_\Omega(D, H + A) \subseteq C_\Omega(D, H + \lfloor H \rfloor)$. Desta maneira segue que, $d(C_\Omega(D, H + A)) \geq d(C_\Omega(D, H + \lfloor H \rfloor))$. Pelo teorema da cota do piso, aplicado ao código $C_\Omega(D, H + \lfloor H \rfloor)$, temos que:

$$d(C_\Omega(D, H + \lfloor H \rfloor)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(E_H),$$

ou seja, $d(C_\Omega(D, H + \lfloor H \rfloor)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(H) - \text{grau}(A)$, uma vez que se $\lfloor H \rfloor \leq A$ então $-\text{grau}(\lfloor H \rfloor) \geq -\text{grau}(A)$. Como $d(C_\Omega(D, H + A)) \geq d(C_\Omega(D, H + \lfloor H \rfloor)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(H - A)$, podemos concluir que:

$$d(C_\Omega(D, H + A)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(H - A).$$

Ou seja, $d(C_\Omega(D, H + A)) \geq d^* + \text{grau}(H) - \text{grau}(A)$. ■

Teorema 4.2.2 (Cota do piso generalizada) Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g . Sejam $P_1, \dots, P_n$ lugares dois a dois distintos de $F/\mathbb{F}_q$, de grau um. Definindo $D := P_1 + \dots + P_n$, sejam A, B, G e Z divisores com o suporte disjunto do suporte de D tal que Z é efetivo e vale que $\ell(A) = \ell(A - Z)$, $\ell(B) = \ell(B + Z)$ e $G = A + B$. Então, a distância mínima d do código $C_\Omega(D, G)$ é tal que satisfaz a desigualdade:

$$d = d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(Z).$$

Demonstração Seja $\eta \in \Omega_F(G - D)$, tal que a palavra código $c_0 := (\eta_{P_1}(1), \dots, \eta_{P_n}(1))$ é de peso mínimo não nulo. Como a distância mínima d de $C_\Omega(D, G)$ é tal que

$$d(C_\Omega(D, G)) = \min \{ \omega(c) \mid 0 \neq c \in C_\Omega(D, G) \},$$

podemos assumir, sem perda de generalidade, que $c_i \neq 0$, para $1 \leq i \leq d$ e $c_i = 0$, para $d < i \leq n$. Seja $D' := P_1 + \dots + P_d$. Por hipótese, temos que $\text{supp}(G) \cap \text{supp}(D) = \emptyset$, pois $G = A + B$ e A e B são divisores com suporte disjunto do suporte de D . Como $\text{supp}(D') \subseteq \text{supp}(D)$ segue que $\text{supp}(G) \cap \text{supp}(D') = \emptyset$. Sendo $v_Q(\eta) \geq v_Q(G - D)$, para todo lugar Q de $F/\mathbb{F}_q$, tal que $Q \in \text{supp}(D)$ segue, em particular, que isso é válido para todo $Q \in \text{supp}(D')$. Portanto, devemos ter $(\eta) \geq G - D'$. Desta forma, existe um divisor efetivo E , com suporte disjunto do suporte de D' , de modo que $W := (\eta) = G - D' + E$, e assim observamos que W é um divisor canônico e com isso $\text{grau}(W) = 2g - 2$. Tomamos o grau dos divisores de ambos os lados da igualdade $W := G - D' + E$ e obtemos que, $2g - 2 = \text{grau}(G) - d + \text{grau}(E)$ e isso implica que $d = \text{grau}(G) - (2g - 2) + \text{grau}(E)$.

Observe que $\text{grau}(E) \geq \ell(A + E) - \ell(A) = \ell(A + E) - \ell(A - Z)$. De fato, pelo lema 2.4.3., temos que $\ell(A + E) - \ell(A) \leq \text{grau}(A + E) - \text{grau}(A) = \text{grau}(E)$, e desta forma $\text{grau}(E) \geq \ell(A + E) - \ell(A)$; como, por hipótese, $\ell(A) = \ell(A - Z)$ é imediato que $\ell(A + E) - \ell(A) = \ell(A + E) - \ell(A - Z)$. Logo, $\text{grau}(E) \geq \ell(A + E) - \ell(A - Z)$. Sendo E um divisor efetivo segue que, $A + E - Z \geq A - Z$ e daí, $\mathcal{L}(A - Z) \subseteq \mathcal{L}(A + E - Z)$. Desta forma, $\ell(A - Z) \leq \ell(A + E - Z)$, o que implica $-\ell(A - Z) \geq -\ell(A + E - Z)$. Portanto, $\text{grau}(E) \geq \ell(A + E) - \ell(A + E - Z)$. Aplicando o teorema de Riemann-Roch aos divisores $A + E$ e $A + E - Z$, obtemos as seguintes relações:

- (i) $\ell(A + E) = \text{grau}(A + E) + 1 - g + \ell(W - (A + E))$,
- (ii) $\ell(A + E - Z) = \text{grau}(A + E - Z) + 1 - g + \ell(W - (A + E - Z))$.

Assim, conseguimos obter a seguinte igualdade:

$$\ell(A + E) - \ell(A + E - Z) = \ell(W - (A + E)) - \ell(W - (A + E - Z)) + \text{grau}(Z) = \text{grau}(Z) + \ell(W - A + G - D' - W) - \ell(W + Z - A + G - D' - W),$$

e então, $\ell(A + E) - \ell(A + E - Z) = \text{grau}(Z) + \ell(B - D') - \ell(B + Z - D')$. Agora, como $B + Z - D' \leq B + Z$ temos que $\mathcal{L}(B + Z - D') \subseteq \mathcal{L}(B + Z)$. Sendo Z efetivo, $B + Z \geq B$ e daí $\mathcal{L}(B) \subseteq \mathcal{L}(B + Z)$; por hipótese temos, $\ell(B) = \ell(B + Z)$ e assim segue a igualdade dos espaços vetoriais, $\mathcal{L}(B) = \mathcal{L}(B + Z)$. Portanto, $\mathcal{L}(B + Z - D') \subseteq \mathcal{L}(B)$ e então $\mathcal{L}(B + Z - D') = \mathcal{L}(B + Z - D') \cap \mathcal{L}(B)$.

Mostremos que $\mathcal{L}(B + Z - D') = \mathcal{L}(m.d.c.(B + Z - D'; B))$. Seja $x \in \mathcal{L}(B + Z - D') = \mathcal{L}(B + Z - D') \cap \mathcal{L}(B)$. Então $(x) + B + Z - D' \geq 0$ e $(x) + B \geq 0$. Assim, para todo lugar P de $F/\mathbb{F}_q$, temos que $v_P((x) + B + Z - D') \geq 0$ e $v_P((x) + B) \geq 0$, e então obtemos a seguinte desigualdade $v_P((x)) + \min\{v_P(B + Z - D'); v_P(B)\} \geq 0$; com isso $x \in \mathcal{L}(m.d.c.(B + Z - D'; B))$ e daí $\mathcal{L}(B + Z - D') \subseteq \mathcal{L}(m.d.c.(B + Z - D'; B))$. Agora, se $x \in \mathcal{L}(m.d.c.(B + Z - D'; B))$ temos $\min\{v_P(B + Z - D'); v_P(B)\} \leq v_P(B + Z - D')$, $\forall$ lugar P de $F/\mathbb{F}_q$, donde vemos o seguinte, $0 \leq (x) + m.d.c.(B + Z - D'; B) \leq (x) + B + Z - D'$. Logo, $x \in \mathcal{L}(B + Z - D') = \mathcal{L}(B + Z - D') \cap \mathcal{L}(B)$. Com isso temos a inclusão, $\mathcal{L}(m.d.c.(B + Z - D'; B)) \subseteq \mathcal{L}(B + Z - D')$.

Conclusão: $\mathcal{L}(B + Z - D') = \mathcal{L}(m.d.c.(B + Z - D'; B))$.

Temos que $\text{supp}(D') \subseteq \text{supp}(D)$ logo, $\text{supp}(B) \cap \text{supp}(D') = \emptyset$ e $\text{supp}(Z) \cap \text{supp}(D') = \emptyset$. Sendo Z efetivo, $B + Z \geq B$ e então $m.d.c.(B + Z - D'; B) = B - D'$. Desta maneira, obtemos $\mathcal{L}(B + Z - D') = \mathcal{L}(B - D')$ e então $\ell(B + Z - D') = \ell(B - D')$. Assim, $\text{grau}(E) \geq \ell(A + E) - \ell(A + E - Z) + \text{grau}(Z)$ o que implica $\text{grau}(E) \geq \ell(B - D') - \ell(B + Z - D') + \text{grau}(Z) = \text{grau}(Z)$. Assim, temos que $\text{grau}(E) \geq \text{grau}(Z)$. Logo, $d = d(C_\Omega(D, G)) = \text{grau}(G) - (2g - 2) + \text{grau}(E) \geq \text{grau}(G) - (2g - 2) + \text{grau}(Z)$. ■

Em seguida, vamos obter mais uma cota para a distância mínima de um código do tipo $C_\Omega(D, G)$. Esta cota está relacionada com o teto de um determinado divisor.

Teorema 4.2.3 Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero g e o divisor $D := P_1 + \dots + P_n$, onde $P_1, \dots, P_n$ são lugares dois a dois distintos e de grau um. Seja G um divisor tal que o suporte do divisor $[G - D] + D$ não contém quaisquer dos lugares $P_1, \dots, P_n$. Então, $C_\Omega(D, G)$ é um código $[n, k, d]$ cuja distância mínima d satisfaz a desigualdade:

$$d = d(C_\Omega(D, G)) \geq \text{grau}([G - D]) + n + g - 1 = \text{grau}(G) - (2g - 2) + \text{grau}(E_{W-G+D}),$$

onde W é qualquer divisor canônico tal que $E_{W-G+D} = W - G + D - [W - G + D]$.

Demonstração Sendo W um divisor canônico temos que $[W - (G - D)] = W - [G - D]$, ou seja, $[W - G + D] = W - [G - D]$. Observemos o seguinte fato:

$$G - D + E_{W-G+D} = G - D + W - G + D - [W - G + D] = W - W + [G - D] = [G - D].$$

Com isso, $\Omega_F(G - D) = \Omega_F([G - D]) = \Omega_F(G - D + E_{W-G+D})$. Agora, seja $\eta \in \Omega_F(G - D)$ tal que a palavra código $c_0 := (\eta_{P_1}(1), \dots, \eta_{P_n}(1))$ é de peso mínimo. Pela definição da distância mínima d , podemos assumir que as primeiras d coordenadas de c_0 são não nulas e as coordenadas restantes são nulas. Então, sendo $D' := \sum_{i=1}^d P_i$, como $\Omega_F(G - D) =$

$\Omega_F(G - D + E_{W-G+D})$ temos que, $\eta \in \Omega_F(G - D + E_{W-G+D})$. Disto e do fato que $D \geq D'$ segue que $(\eta) \geq G - D' + E_{W-G+D}$. Assim, existe um divisor efetivo A cujo suporte não contém quaisquer dos lugares $P_1, \dots, P_d$, e tal que $(\eta) = G - D' + E_{W-G+D} + A$. Tomando o grau dos divisores de ambos os lados da igualdade acima, obtemos que:

$$2g - 2 = \text{grau}(G) - d + \text{grau}(E_{W-G+D}) + \text{grau}(A).$$

Portanto, $d = \text{grau}(G) - (2g - 2) + \text{grau}(E_{W-G+D}) + \text{grau}(A)$.

Como $\text{grau}(A) \geq 0$ temos então que $d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(E_{W-G+D}) = \text{grau}(\lceil G - D \rceil) + n + g - 1$. ■

Proposição 4.2.1 Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g . Seja $D := P_1 + \dots + P_n$, onde $P_1, \dots, P_n$ são lugares dois a dois distintos de grau um de $F/\mathbb{F}_q$, e seja G um divisor tal que o suporte do piso de G não contém quaisquer dos lugares $P_1, \dots, P_n$. Então, $C_\Omega(D, \lceil G \rceil)$ é um código $[n, k, d]$ cuja distância mínima d satisfaz a desigualdade:

$$d = d(C_\Omega(D, \lceil G \rceil)) \geq \text{grau}(\lceil G \rceil) - (2g - 2) = \text{grau}(G) - (2g - 2) + \text{grau}(\lceil G \rceil - G).$$

Demonstração Temos que a distância designada do código $C_\Omega(D, \lceil G \rceil)$ é dada por

$$d^*(C_\Omega(D, \lceil G \rceil)) = \text{grau}(\lceil G \rceil) - (2g - 2).$$

Por outro lado, a distância mínima deste mesmo código é maior ou igual do que a distância designada. Logo, $d(C_\Omega(D, \lceil G \rceil)) \geq d^*(C_\Omega(D, \lceil G \rceil))$, como queríamos demonstrar. ■

Observação 4.2.1 Note que a demonstração do teorema da cota do piso generalizada assume que o código $C_\Omega(D, G)$ é não trivial, ou seja, o referido código não é o espaço vetorial nulo e consequentemente possui uma palavra código de peso não nulo. Se o código é trivial, a questão da cota para a distância mínima dada no respectivo teorema não é muito interessante.

A partir de agora, vamos dar alguns exemplos que ilustram como a cota do piso e a cota do piso generalizada podem ser aplicadas.

Exemplo 4.2.1 (Código Hermitiano de um lugar) Um código Hermitiano é um código sobre o corpo de funções Hermitiano. Um corpo de funções F/K , onde $K = \mathbb{F}_{q^2}$ com q uma potência de algum número primo p e $F = K(x, y)$, com equação dada por $y^q + y = x^{q+1}$, é dito um corpo de funções Hermitiano. De acordo com [12] Lema VI.4.4., este tal corpo de funções possui gênero $g = \frac{q(q-1)}{2}$ e $q^3 + 1$ lugares de grau um.

Seja então o corpo finito com 16 elementos $\mathbb{F}_{16}$ e considere o corpo de funções $\mathbb{F}_{16}(x, y)/\mathbb{F}_{16}$ com equação definida por $y^4 + y = x^5$. Neste caso, temos $q = 4$ e então o corpo de funções descrito anteriormente é um corpo de funções Hermitiano. Assim, o gênero g desse corpo de funções é $g = 6$ e ele possui $q^3 + 1 = 65$ lugares de grau um. Denotemos estes lugares por $P_0, P_1, \dots, P_{63}, P_\infty$ onde, de acordo com [12] Lema VI.4.4., P_∞ é o único pólo em comum de x e de y . Vamos tomar o semigrupo de Weierstrass do lugar P_∞ , isto é, o conjunto das ordens de pólo de P_∞ :

$$H(P_\infty) := \{n \in \mathbb{N}_0 \mid \text{existe } x \in F \text{ com } (x)_\infty = nP_\infty\},$$

onde $\mathbb{N}_0$ denota o conjunto dos números inteiros não-negativos. Com isso, definimos o conjunto das lacunas de Weierstrass do lugar P_∞ por $G(P_\infty) := \mathbb{N}_0 \setminus H(P_\infty)$. Temos que o semigrupo de Weierstrass do lugar P_∞ é tal que $H(P_\infty) \supset \langle 4, 5 \rangle = \{0, 4, 5, 8, 9, 10, 12, 13, 14, \dots\}$, uma vez que pela referência [12] Proposição VI.4.1. temos $(x)_\infty = qP_\infty$ e $(y)_\infty = (q+1)P_\infty$, com $q = 4$.

Pelo teorema das lacunas de Weierstrass temos que P_∞ possui exatamente $g = 6$ lacunas, que serão denotadas aqui por n_1, n_2, n_3, n_4, n_5 e n_6 , com $n_1 < n_2 < n_3 < n_4 < n_5 < n_6$ e, ainda pelo teorema citado, $n_1 = 1$ e $n_i \leq 2g - 1 = 11$, para todo $i = 1, \dots, 6$. Vamos mostrar que $n_2 = 2, n_3 = 3, n_4 = 6, n_5 = 7$ e $n_6 = 11$. Suponha que $n_6 < 11$. Poderíamos então ter $n_6 = 10, 9$ ou 8 , mas isto não é possível, pois $8, 9$ e 10 pertencem à $\langle 4, 5 \rangle \subset H(P_\infty)$. Então, tome $n_6 = 7$. Neste caso, na melhor das hipóteses teremos que $n_2 = 2, n_3 = 3, n_4 = 6$ e assim não há valores possíveis para n_5 , o que é absurdo. Portanto, não podemos ter $n_6 = 7$. Agora, se $n_6 = 6$, na melhor das hipóteses temos que $n_2 = 2, n_3 = 3$ e então não temos valores para n_4 e n_5 , o que é absurdo. Se $n_6 = 3$, então na melhor das hipóteses teremos $n_2 = 2$ e com isso n_3, n_4 e n_5 não recebem valor algum, o que é absurdo. Se $n_6 = 2$ não existem valores para n_2, n_3, n_4 e n_5 , o que é absurdo. Podemos então concluir que $n_6 = 11$ e desta maneira devemos ter $n_2 = 2, n_3 = 3, n_4 = 6$ e $n_5 = 7$. Portanto, $\{1, 2, 3, 6, 7, 11\}$ é o conjunto das lacunas de P_∞ e consequentemente $\mathbb{N}_0 \setminus \{1, 2, 3, 6, 7, 11\}$ é o conjunto das ordens de pólo de P_∞ . Logo, segue que $H(P_\infty) = \mathbb{N}_0 \setminus \{1, 2, 3, 6, 7, 11\}$.

Conclusão: $H(P_\infty) = \langle 4, 5 \rangle$.

Recordemos que, na demonstração do teorema das lacunas de Weierstrass, caracterizamos uma lacuna pelo seguinte:

i é uma lacuna de um lugar de grau um Q se, e somente se, $\mathcal{L}((i-1)Q) = \mathcal{L}(iQ)$.

Assim, visto que 11 é uma lacuna de P_∞ obtemos que $\mathcal{L}(11P_\infty) = \mathcal{L}(10P_\infty)$ e sendo 7 também uma lacuna de P_∞ segue que $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$. Tomemos os divisores $A = 11P_\infty$, $B = 6P_\infty$ e $Z = P_\infty$ e coloquemos $G = A + B = 17P_\infty$ e $D := P_0 + P_1 + \dots + P_{63}$. Consideremos o código $C_\Omega(D, G)$.

Definição 4.2.1 Seja F/K um corpo de funções. Se $G = mP$, para algum lugar P de grau um, $m \in \mathbb{N}$ e D é um divisor que é a soma de todos os outros lugares de grau um de F/K , nos referimos ao código $C_\Omega(D, G)$ como código de um lugar sobre F/K .

De acordo com a definição anterior temos que $C_\Omega(D, G)$ é um código de um lugar sobre o corpo de funções Hermitiano, ou seja, é um código Hermitiano de um lugar. Portanto, temos A, B, G e Z divisores cujo suporte é disjunto do suporte de D , Z é efetivo, $G = A + B$ e $\ell(A) = \ell(A - Z)$, pois $\mathcal{L}(11P_\infty) = \mathcal{L}(10P_\infty)$ e $\ell(B) = \ell(B + Z)$, uma vez que $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$. Pelo teorema da cota do piso generalizada segue que:

$$d = d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(Z) = 17 - 10 + 1 = 8.$$

Sabemos que a distância designada de $C_\Omega(D, G)$ é $d^* = \text{grau}(G) - (2g - 2) = 17 - 10 = 7$. Como $d(C_\Omega(D, G))$ é pelo menos 8, obtemos uma melhoria de pelo menos um para a distância mínima de $C_\Omega(D, G)$ em relação à distância designada.

Enquanto a cota do piso generalizada fornece esta melhoria a cota do piso não fornece, uma vez que não existe nenhuma maneira de escrever o divisor $G = 17P_\infty$ como $G = H + \lfloor H \rfloor$, onde H é um divisor efetivo cujo suporte é disjunto do suporte de D . De fato, suponha que $G = 17P_\infty$ possa ser escrito da maneira descrita anteriormente. Assim, H é da forma $H = aP_\infty$ e sendo H um divisor efetivo temos que o piso de H também é efetivo e $\text{supp}(\lfloor H \rfloor) \subseteq \text{supp}(H)$. Se H fosse igual à $0P_\infty, 1P_\infty, 2P_\infty, 3P_\infty, 4P_\infty, 5P_\infty, 6P_\infty, 7P_\infty$ ou $8P_\infty$ deveríamos ter, respectivamente, $\lfloor H \rfloor$ igual à $17P_\infty, 16P_\infty, 15P_\infty, 14P_\infty, 13P_\infty, 12P_\infty, 11P_\infty, 10P_\infty$ e $9P_\infty$; em todos esses casos se contraria o fato de que $\lfloor H \rfloor \leq H$. Se $H = 9P_\infty$ então devemos ter $\lfloor H \rfloor = 8P_\infty$ e assim $\mathcal{L}(9P_\infty) = \mathcal{L}(8P_\infty)$, o que implica que 9 é uma lacuna, o que é um absurdo. Se $H = 10P_\infty$ então devemos ter $\lfloor H \rfloor = 7P_\infty$; se isso ocorre então $\mathcal{L}(10P_\infty) = \mathcal{L}(7P_\infty)$ e como 7 é uma lacuna segue que $\mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty)$ e daí $\lfloor 10P_\infty \rfloor \neq 7P_\infty$, pois o piso de H é o divisor de grau mínimo tal que $\mathcal{L}(H) = \mathcal{L}(\lfloor H \rfloor)$ e neste caso temos $\text{grau}(6P_\infty) < \text{grau}(7P_\infty)$. Se $H = 11P_\infty$ então, visto que G se escreve como a soma de H com o piso de H , devemos ter $\lfloor H \rfloor = 6P_\infty$; logo temos $\mathcal{L}(11P_\infty) = \mathcal{L}(6P_\infty) = \mathcal{L}(5P_\infty)$ e daí $\lfloor 11P_\infty \rfloor \neq 6P_\infty$, pelo mesmo motivo explicado anteriormente. Se $H = 12P_\infty$, devemos ter $\lfloor H \rfloor = 5P_\infty$; com isso segue a igualdade $\mathcal{L}(12P_\infty) = \mathcal{L}(5P_\infty) = \mathcal{L}(6P_\infty) = \mathcal{L}(7P_\infty)$ e daí $\lfloor 12P_\infty \rfloor = 5P_\infty$ e portanto dois divisores diferentes possuem o mesmo piso, o que é absurdo. Se $H = 13P_\infty$ devemos ter $\lfloor H \rfloor = 4P_\infty$; no entanto 13 é ordem de pólo e assim $\mathcal{L}(13P_\infty) \neq \mathcal{L}(12P_\infty)$ e daí, se vale que $\mathcal{L}(13P_\infty) = \mathcal{L}(4P_\infty)$ devemos ter $\mathcal{L}(4P_\infty) = \mathcal{L}(12P_\infty)$, pois $4P_\infty \leq 12P_\infty$, logo $\mathcal{L}(13P_\infty) = \mathcal{L}(12P_\infty)$, o que é absurdo; portanto, $\lfloor 13P_\infty \rfloor \neq 4P_\infty$. Se $H = 14P_\infty$, devemos ter $\lfloor H \rfloor = 3P_\infty$ e então $\mathcal{L}(14P_\infty) = \mathcal{L}(3P_\infty)$, e como 3 é lacuna segue que, $\mathcal{L}(3P_\infty) = \mathcal{L}(2P_\infty)$ e assim temos um divisor cujo grau é menor do que o grau de $3P_\infty$ e $\mathcal{L}(2P_\infty) = \mathcal{L}(14P_\infty)$; segue disto que não podemos ter $\lfloor 14P_\infty \rfloor = 3P_\infty$. Se $H = 15P_\infty$ devemos então ter $\lfloor H \rfloor = 2P_\infty$; no entanto 2 é lacuna e desta forma $\mathcal{L}(H) = \mathcal{L}(2P_\infty) = \mathcal{L}(1P_\infty)$ e com isso o piso de H não pode ser $2P_\infty$. Se $H = 16P_\infty$ então seu piso deve ser $1P_\infty$; no entanto, 1 é lacuna e assim, pelo mesmo argumento anterior, não podemos ter que $\lfloor H \rfloor = 1P_\infty$. Finalmente, se $H = 17P_\infty$ então devemos ter $\lfloor H \rfloor = 0P_\infty$; assim $\mathcal{L}(17P_\infty) = \mathcal{L}(0) = \mathbb{F}_{16}$, o que é absurdo.

Conclusão: G não se escreve como $G = H + \lfloor H \rfloor$, onde H é um divisor efetivo cujo suporte é disjunto do suporte de D .

Observação 4.2.2 Mostremos que $C_\Omega(D, 17P_\infty) = C_\mathcal{L}(D, 57P_\infty)$. De fato, pela referência [12] Proposição VII.4.2., temos que $C_\mathcal{L}(D, 57P_\infty)^\perp = C_{q^3+q^2-q-2-57} = C_{17} = C_\mathcal{L}(D, 17P_\infty)$. Pelo teorema 3.2.3. temos que $C_\mathcal{L}(D, G)$ e $C_\Omega(D, G)$ são códigos duais. Logo, $C_\mathcal{L}(D, 17P_\infty)^\perp = C_\Omega(D, 17P_\infty)$. No entanto, note que $C_\mathcal{L}(D, 17P_\infty)^\perp = \left(C_\mathcal{L}(D, 57P_\infty)^\perp\right)^\perp = C_\mathcal{L}(D, 57P_\infty)$.

Portanto, $C_\Omega(D, 17P_\infty) = C_\mathcal{L}(D, 57P_\infty)$, como queríamos.

Desta forma, por [4], temos que a distância mínima deste código é exatamente 8.

Para os exemplos posteriores necessitamos, neste momento, de alguns conceitos e resultados, cuja finalidade é fazer com que tenhamos melhor compreensão e entendimento do assunto aqui abordado.

Definição 4.2.2 Sejam P_1 e P_2 dois lugares distintos de grau um do corpo de funções F/K . O semigrupo de Weierstrass do par de lugares (P_1, P_2) é definido por:

$$H(P_1, P_2) = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid \text{existe } x \in F \text{ com } (x)_\infty = \alpha_1 P_1 + \alpha_2 P_2\}.$$

O conjunto das lacunas de Weierstrass é então dado por $G(P_1, P_2) = \mathbb{N}_0^2 \setminus H(P_1, P_2)$.

Vamos enunciar uma caracterização muito útil de elementos que estão em $H(P_1, P_2)$; este resultado é encontrado na referência [3] Lema 2.1..

Afirmção 1: Para $(\alpha_1, \alpha_2) \in \mathbb{N} \times \mathbb{N} \setminus \{0, 0\}$ são equivalentes:

- (i) $(\alpha_1, \alpha_2) \in H(P_1, P_2)$.
- (ii) $\ell(\alpha_1 P_1 + \alpha_2 P_2) - \ell((\alpha_1 - 1) P_1 + \alpha_2 P_2) = 1$ e $\ell(\alpha_1 P_1 + \alpha_2 P_2) - \ell(\alpha_1 P_1 + (\alpha_2 - 1) P_2) = 1$.

Em outras palavras, a afirmação anterior nos diz o seguinte:

$(\alpha_1, \alpha_2) \in H(P_1, P_2)$ se, e somente se, vale $\mathcal{L}(\alpha_1 P_1 + \alpha_2 P_2) \setminus \mathcal{L}((\alpha_1 - 1) P_1 + \alpha_2 P_2) \neq \emptyset$ e $\mathcal{L}(\alpha_1 P_1 + \alpha_2 P_2) \setminus \mathcal{L}(\alpha_1 P_1 + (\alpha_2 - 1) P_2) \neq \emptyset$.

Um resultado que utilizaremos bastante no que vem a seguir, e é também encontrado em [3] Lema 2.3., é o seguinte:

Afirmção 2: Seja $\alpha_1 \geq 1$. Então, $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell((\alpha_1 - 1) P_1 + \alpha_2 P_2) + 1$ se, e somente se, existe α , $0 \leq \alpha \leq \alpha_2$, tal que $(\alpha_1, \alpha) \in H(P_1, P_2)$. Analogamente, seja $\alpha_2 \geq 1$; então, $\ell(\alpha_1 P_1 + \alpha_2 P_2) = \ell(\alpha_1 P_1 + (\alpha_2 - 1) P_2) + 1$ se, e somente se, existe α , $0 \leq \alpha \leq \alpha_1$, tal que $(\alpha, \alpha_2) \in H(P_1, P_2)$.

Tendo isso em mãos, voltemos aos nossos exemplos.

Exemplo 4.2.2 (Código Hermitiano de dois lugares) Consideraremos neste exemplo o mesmo corpo de funções Hermitiano do exemplo precedente.

Definição 4.2.3 Seja F/K um corpo de funções. Se um divisor G é tal que $G = \alpha_1 P_1 + \alpha_2 P_2$, para distintos lugares de grau um P_1 e P_2 , $\alpha_1, \alpha_2 \in \mathbb{N}$ e D um divisor que é a soma de todos os outros lugares de grau um de F/K , nos referimos ao código $C_\Omega(D, G)$ como um código de dois lugares sobre F/K .

Assim, consideremos o divisor $G = 2P_0 + 8P_\infty$ e $D = P_1 + P_2 + \dots + P_{63}$ e tome, de acordo com a definição anterior, o código Hermitiano de dois lugares $C_\Omega(D, G)$. Na referência [10] Exemplo 5.2. é computado o semigrupo de Weierstrass do par de lugares (P_0, P_∞) . Mais precisamente, como anteriormente, seja $\mathbb{N}_0$ denotando o conjunto dos inteiros não negativos; a tabela 4.1. retrata $H(P_0, P_\infty) \cap \mathbb{N}_0^2$. Nesta tabela, o lugar marcado por um $\times$ representa o ponto cuja primeira coordenada é dada pelo número que está na horizontal e a segunda coordenada é dada pelo número que está na vertical.

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	×				×	×			×	×	×		×
1												×	×
2								×	×	×	×	×	×
3				×	×	×		×	×	×	×	×	×
4	×			×	×	×		×	×	×	×	×	×
5	×			×	×	×		×	×	×	×	×	×
6							×	×	×	×	×	×	×
7			×	×	×	×	×	×	×	×	×	×	×
8	×		×	×	×	×	×	×	×	×	×	×	×
9	×		×	×	×	×	×	×	×	×	×	×	×
10	×		×	×	×	×	×	×	×	×	×	×	×
11		×	×	×	×	×	×	×	×	×	×	×	×
12	×	×	×	×	×	×	×	×	×	×	×	×	×

Tabela 4.1: $H(P_0, P_\infty) \cap (\mathbb{N}_0 \times \mathbb{N}_0)$

Como vimos, $H(P_0, P_\infty) = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0^2 \mid \text{existe } x \in F \text{ tal que } (x)_\infty = \alpha_1 P_0 + \alpha_2 P_\infty\}$.

Vejamos que $\mathcal{L}(2P_0 + 6P_\infty) = \mathcal{L}(5P_\infty)$ e $\mathcal{L}(2P_0 + 3P_\infty) = \mathcal{L}(2P_\infty)$. De fato, tomemos $\alpha_1 = 2$ e $\alpha_2 = 6$ e observando a tabela 4.1. vemos que não existe $0 \leq \alpha \leq 6$ tal que $(2, \alpha) \in H(P_0, P_\infty)$. Segue então, de acordo com a afirmação 2, que $\mathcal{L}(2P_0 + 6P_\infty) = \mathcal{L}(1P_0 + 6P_\infty)$ e, de acordo com a tabela 4.1., temos para $\alpha_1 = 1, \alpha_2 = 6$ que não existe $0 \leq \alpha \leq 6$ tal que $(1, \alpha) \in H(P_0, P_\infty)$; logo, $\mathcal{L}(1P_0 + 6P_\infty) = \mathcal{L}(6P_\infty)$. Para $(\alpha_1, \alpha_2) = (0, 6)$ temos, observando a tabela 4.1., que $(0, 6)$ é uma lacuna; segue, pela afirmação 2, que $\mathcal{L}(0P_0 + 6P_\infty) = \mathcal{L}(0P_0 + 5P_\infty)$. Portanto, $\mathcal{L}(2P_0 + 6P_\infty) = \mathcal{L}(5P_\infty)$. Também, temos que para $(\alpha_1, \alpha_2) = (2, 3)$ não existe $0 \leq \alpha \leq 3$ tal que $(2, \alpha)$ é uma ordem de pólo e então, $\mathcal{L}(2P_0 + 3P_\infty) = \mathcal{L}(1P_0 + 3P_\infty)$. Além disso, o mesmo raciocínio se aplica para $(\alpha_1, \alpha_2) = (1, 3)$ e assim $\mathcal{L}(1P_0 + 3P_\infty) = \mathcal{L}(3P_\infty)$; para $(\alpha_1, \alpha_2) = (0, 3)$ temos, pela tabela 4.1., que $(0, 3)$ é lacuna e então, pela afirmação 2, segue que $\mathcal{L}(0P_0 + 3P_\infty) = \mathcal{L}(0P_0 + 2P_\infty)$. Portanto, $\mathcal{L}(2P_0 + 3P_\infty) = \mathcal{L}(2P_\infty)$. Vamos então aplicar a cota do piso generalizada a este código de dois lugares. Para tanto, sejam os divisores A, B, G e Z tais que $A = 2P_0 + 6P_\infty, B = 2P_\infty, G = A + B = 2P_0 + 8P_\infty$ e $Z = 2P_0 + P_\infty$. Desta forma, esses divisores possuem suporte disjunto do suporte de $D = \sum_{i=1}^{63} P_i$, Z é efetivo e como $A - Z = 5P_\infty$ e $\mathcal{L}(A) = \mathcal{L}(5P_\infty)$ segue que $\ell(A) = \ell(A - Z)$ e sendo $B + Z = 2P_0 + 3P_\infty$ e $\mathcal{L}(B) = \mathcal{L}(2P_0 + 3P_\infty)$ segue que $\ell(B) = \ell(B + Z)$. Estamos nas hipóteses do teorema da cota do piso generalizada; logo a distância mínima d de $C_\Omega(D, G)$ é tal que:

$$d = d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(Z) = 10 - 10 + 3 = 3.$$

Como a distância designada deste código é tal que $d^* = \text{grau}(G) - (2g - 2) = 10 - 10 = 0$, temos que a diferença entre a distância mínima e a distância designada é de no mínimo 3. Conclusão: obtemos uma melhoria de no mínimo 3 para a distância mínima em relação à distância designada.

Usando divisores efetivos, a cota do piso não atinge essa melhoria. A melhor escolha de um divisor H para a cota do piso é $H = 2P_0 + 4P_\infty$, com $\lfloor H \rfloor = 4P_\infty$ (note que neste caso temos $G = H + \lfloor H \rfloor = 2P_0 + 8P_\infty$ e suporte de H é disjunto do suporte de D). Seja $E_H = H - \lfloor H \rfloor$. Assim, de acordo com o teorema da cota do piso, o código $C_\Omega(D, G)$ possui distância mínima d satisfazendo a desigualdade:

$$d = d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(E_H) = 2.$$

Desta forma, a cota do piso faz com que a distância mínima tenha uma diferença de no mínimo 2 para a distância designada. Portanto, para este código Hermitiano de dois lugares $C_\Omega(D, G)$ com $G = 2P_0 + 8P_\infty$, a cota do piso generalizada fornece uma melhoria superior em relação à cota do piso para a distância mínima em relação à distância designada.

Observação 4.2.3 De acordo com a referência [11] temos o seguinte resultado:

”Seja $G = aP_0 + bP_\infty$ com $a = a_0(q + 1) + a_1$, $0 \leq a_1 \leq q$, e $b = b_0(q + 1) + b_1$, $0 \leq b_1 \leq q$. Suponha que G satisfaça uma ou outra das seguintes condições:

- (1) $\text{grau}(G) < \text{grau}(W)$, para W um divisor canônico ou
- (2) $\text{grau}(W) \leq \text{grau}(G) \leq \text{grau}(W) + q$, com G equivalente a sP_0 ou equivalente a tP_∞ , para $s, t \in \mathbb{Z}$ e W um divisor canônico.

Então, $d(C_\Omega(D, G)^\perp) = a_0 + b_0 + 2$.”

Como $G = 2P_0 + 8P_\infty$, podemos escrever $2 = 0(4 + 1) + 2$ (e então $a_0 = 0$ e $a_1 = 2$) e $8 = 1(4 + 1) + 3$ (e então $b_0 = 1$ e $b_1 = 3$). Também para qualquer divisor canônico W temos $\text{grau}(W) = 2g - 2 = 2(6) - 2 = 10$ e assim G satisfaz a condição 2 dada no resultado anterior. Temos então que $d(C_\Omega(D, G)^\perp) = a_0 + b_0 + 2 = 0 + 1 + 2 = 3$. Sendo, pelo teorema 3.2.3., $C_\Omega(D, G)^\perp = C_\Omega(D, G)$ segue que neste caso $d(C_\Omega(D, G)) = 3$.

Exemplo 4.2.3 (Código de Suzuki de dois lugares) Da mesma forma como no caso de um código Hermitiano, um código de Suzuki é um código sobre o corpo de funções de Suzuki.

Definição 4.2.4 Seja $\mathbb{F}_q(x, y)/\mathbb{F}_q$ um corpo de funções algébricas com equação dada da seguinte forma, $y^q - y = x^{q_0}(x^q - x)$, onde $q_0 = 2^n$ e $q = 2^{2n+1}$, para algum inteiro positivo n . Este corpo de funções é chamado de corpo de funções de Suzuki e, de acordo com a referência [9], ele possui exatamente $q^2 + 1$ lugares de grau um e o gênero g é dado por $g := q_0(q - 1)$.

Consideremos então o corpo de funções $\mathbb{F}_8(x, y)/\mathbb{F}_8$, com equação dada por $y^8 - y = x^2(x^8 - x)$. Assim, temos que $q_0 = 2^1$ e $q = 2^{2 \cdot 1 + 1} = 8$ e então, de acordo com a definição

anterior, $\mathbb{F}_8(x, y)/\mathbb{F}_8$ é um corpo de funções de Suzuki. Portanto, o gênero g desse corpo de funções é $g = 2 \cdot (8 - 1) = 14$ e ele possui exatamente $q^2 + 1 = 65$ lugares de grau um. Denotamos estes lugares por $P_0, P_1, \dots, P_{63}, P_\infty$ onde, segundo a referência [9], P_∞ é o único pólo em comum de x e y .

A fim de encontrarmos o semigrupo de Weierstrass do par de lugares (P_0, P_∞) é necessário entender como isso é feito no caso de um corpo de funções de Suzuki qualquer. Seja então o corpo de funções $\mathbb{F}_q(x, y)/\mathbb{F}_q$ com equação dada por $y^q - y = x^{q_0}(x^q - x)$ tal que este é um corpo de funções de Suzuki qualquer. Sejam P_1 e P_2 quaisquer dois lugares desse corpo de funções de Suzuki distintos e de grau um. Para $a_1, a_2, \dots, a_k$ pertencentes à $\mathbb{N}$ vamos denotar por $\langle a_1, \dots, a_k \rangle$ o subsemigrupo dos inteiros não negativos gerado por $a_1, \dots, a_k$ e temos que $\langle a_1, \dots, a_k \rangle := \left\{ \sum_{i=1}^k c_i a_i \mid c_i \in \mathbb{N}_0 \right\}$. De acordo com a referência [9] Lema 3.1. obtemos que o semigrupo de Weierstrass do lugar P_1 é dado por $H(P_1) := \langle q, q + q_0, q + q/q_0, q + q/q_0 + 1 \rangle$. Também por [9] Lema 3.2., para determinarmos $H(P_1, P_2)$ precisamos somente encontrar o conjunto $\Gamma(P_1, P_2) := \{(\alpha, \beta_\alpha) \mid \alpha \in G(P_1)\}$, onde definimos o inteiro não negativo β_α por $\beta_\alpha := \min \{\beta \in \mathbb{N}_0 \mid (\alpha, \beta) \in H(P_1, P_2)\}$ e, de acordo com a referência [2], β_α é uma lacuna do lugar P_2 .

Dados $u = (u_1, u_2)$ e $v = (v_1, v_2)$ em $\mathbb{N}_0 \times \mathbb{N}_0$, definimos a menor cota superior de u e v por $\text{lub}\{u, v\} = (\max\{u_1, v_1\}, \max\{u_2, v_2\}) \in \mathbb{N}_0^2$. Como mencionado em [9] no Lema 3.2. temos que o semigrupo de Weierstrass do par de lugares (P_1, P_2) é dado por $H(P_1, P_2) = \{\text{lub}\{\gamma_1, \gamma_2\} \mid \gamma_1, \gamma_2 \in \mathbb{S}\}$, onde $\mathbb{S} := \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))$.

Voltemos agora a trabalhar com o corpo de funções de Suzuki considerado neste exemplo.

Utilizando o que foi descrito anteriormente vemos que $H(P_0) = H(P_\infty) = \langle 8, 10, 12, 13 \rangle$, uma vez que $q = 8$ e $q_0 = 2$. Como dado em [9] Exemplo 3.4., o conjunto das lacunas de Weierstrass do lugar P_0 é $G(P_0) = \{1, 2, 3, 4, 5, 6, 7, 9, 11, 14, 15, 17, 19, 27\}$ e o conjunto $\Gamma(P_0, P_\infty) = \{(\alpha, \beta_\alpha) \mid \alpha \in G(P_0)\}$, com $\beta_\alpha = \min \{\beta \in \mathbb{N}_0 \mid (\alpha, \beta) \in H(P_0, P_\infty)\}$, é formado pelos seguintes elementos:

$(1, 27), (2, 19), (3, 11), (4, 17), (5, 9), (6, 15), (7, 7), (27, 1), (19, 2), (11, 13), (17, 4), (9, 5), (15, 6)$ e $(14, 14)$.

Com esses dados, podemos então concluir, como descrito anteriormente, que o semigrupo de Weierstrass do par de lugares (P_0, P_∞) é o seguinte $H(P_0, P_\infty) = \{\text{lub}\{\gamma_1, \gamma_2\} \mid \gamma_1, \gamma_2 \in \mathbb{S}\}$, com $\mathbb{S} = \Gamma(P_0, P_\infty) \cup (\langle 8, 10, 12, 13 \rangle \times \{0\}) \cup (\{0\} \times \langle 8, 10, 12, 13 \rangle)$. Tomamos o código $C_\Omega(D, G)$ sobre o corpo de funções de Suzuki, com $G = 5P_0 + 28P_\infty$ e D a soma dos outros 63 lugares de grau um. Desta forma, $C_\Omega(D, G)$ é um código de Suzuki de dois lugares. Vamos encontrar uma cota inferior para a distância mínima deste código. Novamente vamos usar a afirmação 2, dada anteriormente.

Tomemos $(\alpha_1, \alpha_2) = (2, 15)$ e observamos, pelo semigrupo de Weierstrass, que não existe $0 \leq \alpha \leq 15$ tal que $(2, \alpha) \in H(P_0, P_\infty)$; logo, $\mathcal{L}(2P_0 + 15P_\infty) = \mathcal{L}(1P_0 + 15P_\infty)$. Para $(\alpha_1, \alpha_2) = (1, 15)$ é visto que não existe $0 \leq \alpha \leq 1$ tal que $(\alpha, 15) \in H(P_0, P_\infty)$ e então $\mathcal{L}(1P_0 + 15P_\infty) = \mathcal{L}(1P_0 + 14P_\infty)$. O mesmo argumento anterior vale para $(\alpha_1, \alpha_2) = (1, 14)$

e daí, $\mathcal{L}(1P_0 + 14P_\infty) = \mathcal{L}(1P_0 + 13P_\infty)$. Portanto, $\mathcal{L}(2P_0 + 15P_\infty) = \mathcal{L}(1P_0 + 13P_\infty)$.

Mostremos agora que $\mathcal{L}(4P_0 + 15P_\infty) = \mathcal{L}(3P_0 + 13P_\infty)$. De fato, para $(\alpha_1, \alpha_2) = (4, 15)$, procedendo de modo análogo aos argumentos anteriores temos que não existe $0 \leq \alpha \leq 15$ tal que $(4, \alpha) \in H(P_0, P_\infty)$ e então $\mathcal{L}(4P_0 + 15P_\infty) = \mathcal{L}(3P_0 + 15P_\infty)$. Agora, para $\alpha_1 = 3$ e $\alpha_2 = 15$, não existe $0 \leq \alpha \leq 3$ de forma que $(\alpha, 15) \in H(P_0, P_\infty)$ e assim $\mathcal{L}(3P_0 + 15P_\infty) = \mathcal{L}(3P_0 + 14P_\infty)$. Por fim, não existe $0 \leq \alpha \leq 3$ tal que $(\alpha, 14)$ é ordem de pólo, logo, $\mathcal{L}(3P_0 + 14P_\infty) = \mathcal{L}(3P_0 + 13P_\infty)$. Portanto, $\mathcal{L}(4P_0 + 15P_\infty) = \mathcal{L}(3P_0 + 13P_\infty)$.

Visto isto, tomamos os divisores $A = 2P_0 + 15P_\infty$, $B = 3P_0 + 13P_\infty$ e $Z = 1P_0 + 2P_\infty$ e temos então que $G = A + B = 5P_0 + 28P_\infty$, o divisor Z é efetivo e A , B , G e Z possuem suporte disjunto do suporte de D . Além disso,

- (i) $\ell(A) = \ell(2P_0 + 15P_\infty) = \ell(1P_0 + 13P_\infty) = \ell(A - Z)$ e
- (ii) $\ell(B) = \ell(3P_0 + 13P_\infty) = \ell(4P_0 + 15P_\infty) = \ell(B + Z)$.

Logo, as hipóteses do teorema da cota do piso generalizada estão satisfeitas. Desta forma obtemos que a distância mínima d do código $C_\Omega(D, G)$ é tal que:

$$d = d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(Z),$$

ou seja, temos que $d(C_\Omega(D, G)) \geq 33 - 26 + 3 = 10$. Sendo a distância designada $d^* = \text{grau}(G) - (2g - 2) = 33 - 26 = 7$, segue que a cota do piso generalizada prevê uma melhoria de pelo menos 3 da distância mínima em relação à distância designada.

Observação 4.2.4 No teorema 3.2.2., observamos que o código $C_\Omega(D, G)$ possui dimensão $k = i(G - D) - i(G)$. Porém, neste caso do exemplo, temos $(2g - 2) = 26 < \text{grau}(G) = 33 < n = 63$ e assim, por este mesmo teorema, a dimensão k é tal que $k = n + g - 1 - \text{grau}(G) = 43$.

Exemplo 4.2.4 (Código atingindo uma melhor cota usando divisores não efetivos)

Vamos considerar o código de Suzuki de dois lugares como dado no exemplo anterior, tomando agora o divisor $G = 0P_0 + 32P_\infty = 32P_\infty$ e $D = P_1 + P_2 + \dots + P_{63}$.

Nos exemplos anteriores, computamos a cota do piso generalizada para escolhas de divisores efetivos A e B e vimos que isto fornece uma boa melhoria da distância mínima em relação à distância designada. No entanto, a escolha de divisores efetivos A e B para computar a cota do piso generalizada nem sempre fornece a melhor melhoria, ou seja, podemos obter uma diferença maior entre as distâncias mínima e designada, na cota do piso generalizada, tomando divisores A e B onde pelo menos um deles não é efetivo. É o que veremos a seguir.

Do semigrupo de Weierstrass, usado no exemplo anterior aqui abordado, conseguimos obter que $\mathcal{L}(5P_0 + 15P_\infty) = \mathcal{L}(5P_0 + 13P_\infty)$ e $\mathcal{L}(8P_0 + 6P_\infty) = \mathcal{L}(8P_0 + 4P_\infty)$.

De fato, vamos usar a afirmação 2 para $(\alpha_1, \alpha_2) = (5, 15)$ e, de acordo com o semigrupo de Weierstrass do par de lugares (P_0, P_∞) , não existe $0 \leq \alpha \leq 5$ tal que $(\alpha, 15) \in H(P_0, P_\infty)$; desta maneira $\mathcal{L}(5P_0 + 15P_\infty) = \mathcal{L}(5P_0 + 14P_\infty)$. De modo completamente análogo, aplicamos este raciocínio para $(\alpha_1, \alpha_2) = (5, 14)$ e obtemos que $\mathcal{L}(5P_0 + 14P_\infty) = \mathcal{L}(5P_0 + 13P_\infty)$.

Como no parágrafo anterior, fazemos o mesmo raciocínio para $(\alpha_1, \alpha_2) = (8, 6)$ e depois para $(\alpha_1, \alpha_2) = (8, 5)$, obtendo as igualdades de espaços vetoriais, $\mathcal{L}(8P_0 + 6P_\infty) = \mathcal{L}(8P_0 + 5P_\infty)$ e $\mathcal{L}(8P_0 + 5P_\infty) = \mathcal{L}(8P_0 + 4P_\infty)$.

Da referência [9], o divisor principal de y é tal que $(y) = 13P_0 - 13P_\infty$; a partir disso se nota que $8P_0 + 6P_\infty - (y) = -5P_0 + 19P_\infty$. Logo, $\mathcal{L}(8P_0 + 6P_\infty - (y)) = \mathcal{L}(-5P_0 + 19P_\infty)$ e disto vemos que $\ell(-5P_0 + 19P_\infty) = \ell(8P_0 + 6P_\infty - (y))$. Agora, note que se $x \in \mathcal{L}(8P_0 + 6P_\infty - (y))$ então $(x) \geq -8P_0 - 6P_\infty + (y)$ e daí $(xy^{-1}) \geq -8P_0 - 6P_\infty$ o que acarreta que $(xy^{-1}) \in \mathcal{L}(8P_0 + 6P_\infty) = \mathcal{L}(8P_0 + 4P_\infty)$ e daí $(x) \geq -8P_0 - 4P_\infty + (y)$. Assim, $x \in \mathcal{L}(8P_0 + 4P_\infty - (y))$ e com isso vemos que $\mathcal{L}(8P_0 + 6P_\infty - (y)) \subset \mathcal{L}(8P_0 + 4P_\infty - (y))$. Por outro lado, se $z \in \mathcal{L}(8P_0 + 4P_\infty - (y))$ segue que $(zy^{-1}) \geq -8P_0 - 4P_\infty$ e então $(zy^{-1}) \in \mathcal{L}(8P_0 + 4P_\infty) = \mathcal{L}(8P_0 + 6P_\infty)$. Logo, $(z) \geq -8P_0 - 6P_\infty + (y)$ e por consequência $z \in \mathcal{L}(8P_0 + 6P_\infty - (y))$. Desta forma, $\mathcal{L}(8P_0 + 4P_\infty - (y)) \subset \mathcal{L}(8P_0 + 6P_\infty - (y))$. Portanto, $\mathcal{L}(8P_0 + 4P_\infty - (y)) = \mathcal{L}(8P_0 + 6P_\infty - (y))$. Assim, $\ell(-5P_0 + 19P_\infty) = \ell(8P_0 + 6P_\infty - (y)) = \ell(8P_0 + 4P_\infty - (y)) = \ell(-5P_0 + 17P_\infty)$.

Conclusão: $\ell(-5P_0 + 19P_\infty) = \ell(-5P_0 + 17P_\infty)$ e $\ell(5P_0 + 15P_\infty) = \ell(5P_0 + 13P_\infty)$.

Tomando então os divisores $A = 5P_0 + 15P_\infty$, $B = -5P_0 + 17P_\infty$ e $Z = 2P_\infty$ teremos que $G = A + B = 32P_\infty$, Z é efetivo e os suportes dos divisores A , B , G e Z são disjuntos do suporte do divisor D . Além disso,

- (i) $\ell(A) = \ell(5P_0 + 15P_\infty) = \ell(5P_0 + 13P_\infty) = \ell(A - Z)$ e
- (ii) $\ell(B) = \ell(-5P_0 + 17P_\infty) = \ell(-5P_0 + 19P_\infty) = \ell(B + Z)$.

Aplicando o teorema da cota do piso generalizada, obtemos que a distância mínima d do código $C_\Omega(D, G)$ satisfaz a seguinte desigualdade:

$$d = d(C_\Omega(D, G)) \geq \text{grau}(G) - (2g - 2) + \text{grau}(Z) = 8.$$

Como a distância designada deste código é, por definição, $d^* = \text{grau}(G) - (2g - 2) = 6$, temos uma melhoria de pelo menos $\text{grau}(Z) = 2$ para a distância mínima em relação à d^* .

Observação 4.2.5 É importante mencionar que, de acordo com a referência [1], temos que a distância mínima do código apresentado neste exemplo é exatamente igual à 8. Observamos também que neste cálculo feito para a distância mínima tomamos o divisor B sendo não efetivo. De acordo com a tabela 4.4., a melhor escolha de divisores efetivos A e B para o cálculo da cota para a distância mínima, neste caso em que $G = 0P_0 + 32P_\infty$, fornece a distância mínima do código maior ou igual à 7. Assim, como $d^* = 6$, temos uma melhoria de pelo menos 1 para a distância mínima em relação à distância designada. Visto isto, podemos concluir que a escolha de divisores efetivos A e B forneceu uma melhoria inferior para a distância mínima em relação à distância designada comparada com a melhoria obtida para a escolha de A e B não ambos efetivos.

Cabe ressaltarmos que a cota do piso generalizada não é totalmente exata, uma vez que não atinge a distância mínima real de um código em todos os casos. Para obtermos uma perspectiva mais global, vamos considerar como a cota do piso generalizada se aplica para alguns códigos Hermitianos de dois lugares sobre $\mathbb{F}_{16}$, isto é, códigos da forma $C_\Omega(D, aP_0 + bP_\infty)$ com $a, b \in \mathbb{Z}$ e $D = \sum_{i=1}^{63} P_i$, como no exemplo 4.2.1., ou seja, forneceremos cotas para a distância mínima de tais códigos. Vamos também fazer a mesma análise aplicando a cota do piso. No exemplo 4.2.1. temos que o gênero g é tal que $g = 6$. Restringimos nossa atenção para códigos com $G = aP_0 + bP_\infty$ um divisor efetivo e com $\text{grau}(G) \geq 2g - 2 = 10$, onde a distância designada é não negativa. Podemos mostrar que $(y) = 5P_0 - 5P_\infty$. Deste modo, restringimos ainda mais a nossa atenção para códigos com $0 \leq a < 5$, uma vez que qualquer outro código é equivalente a um com valor de a neste intervalo, pois para um valor de $r \in \mathbb{N}$ apropriado temos que $G + (y^r) = aP_0 + bP_\infty + r5P_0 - r5P_\infty = (a + r5)P_0 + (b - r5)P_\infty$, com $0 \leq a + r5 < 5$. Logo, G e $(a + r5)P_0 + (b - r5)P_\infty$ são divisores equivalentes e assim, conforme a proposição 3.2.2., $C_\Omega(D, G)$ e $C_\Omega(D, (a + r5)P_0 + (b - r5)P_\infty)$ são códigos equivalentes e então possuem as mesmas distâncias mínima e designada.

Usamos o semigrupo de Weierstrass $H(P_0, P_\infty)$ como no exemplo 4.2.1. e calculamos para cada $G = aP_0 + bP_\infty$ com $0 \leq a < 5$ a melhor escolha de divisores efetivos para as cotas do piso e do piso generalizada. As duas tabelas a seguir nos fornecem o que foi descrito anteriormente. Na tabela 4.2. computamos cotas para a distância mínima, de acordo com o teorema da cota do piso. Desta forma, se $G = H + [H] = aP_0 + bP_\infty$, escrevemos na posição (a, b) o valor $d^* + \text{grau}(H) - \text{grau}([H])$ que é a cota para a distância mínima d que o teorema da cota do piso fornece. Na tabela 4.3. listamos as cotas para a distância mínima, conforme o teorema da cota do piso generalizada. Portanto, o valor na posição (a, b) é $d^* + \text{grau}(Z)$, de acordo com as hipóteses do teorema da cota do piso generalizada.

Observação 4.2.6 Na tabela 4.4. listamos as cotas para a distância mínima de alguns códigos de Suzuki de dois lugares sobre $\mathbb{F}_8$, usando divisores efetivos A e B , obtidas pelo teorema da cota do piso generalizada. A computação é análoga à realizada na tabela 4.3.. As informações desta tabela foram obtidas usando o corpo de funções de Suzuki que foi dado no exemplo 4.2.3. e os códigos sobre este corpo de funções são códigos de dois lugares. Então novamente restringimos nossa atenção para códigos da forma $C_\Omega(D, G)$, onde $G = aP_0 + bP_\infty$, $\text{grau}(G) \geq 2g - 2 = 26$ (no exemplo 4.2.3. temos que $g = 14$) e G é efetivo. Como observado no exemplo 4.2.4. temos $(y) = 13P_0 - 13P_\infty$ e assim podemos restringir nossa atenção para códigos com $0 \leq a < 13$.

$0 \leq a \leq 4, 6 \leq b \leq 21$	0	1	2	3	4
6					
7					
8			2	2	
9			2		
10		2	4	4	
11	2	4	6	6	6
12	4	6	6	6	
13	4	6	6		
14		6			
15					
16		8			
17					
18		10			
19					
20		12			
21	12				

Tabela 4.2: Nesta tabela a primeira linha fornece o valor de a e a primeira coluna, o valor de b ; os demais números que aparecem no cruzamento de uma linha com uma coluna são cotas inferiores para a distância mínima de códigos, do tipo $C_{\Omega}(D, G)$, sobre o corpo de funções Hermitiano dado no exemplo 4.2.1. com o divisor G sendo $G = aP_0 + bP_{\infty}$, fornecidas pelo teorema da cota do piso. Os valores destacados em negrito são a distância mínima exata do código, de acordo com a referência [11].

$0 \leq a \leq 4, 6 \leq b \leq 21$	0	1	2	3	4
6					2
7				3	3
8			3	3	3
9		2	3	3	
10		2	4	4	
11	2	4	6	6	6
12	4	6	6	6	7
13	4	6	6		
14		6	7		
15		7	8		
16	7	8	9	10	11
17	8	9			
18		10			
19		11			
20		12			
21	12				

Tabela 4.3: Nesta tabela a primeira linha fornece o valor de a e a primeira coluna, o valor de b ; os demais números que aparecem no cruzamento de uma linha com uma coluna são cotas inferiores para a distância mínima de códigos, do tipo $C_\Omega(D, G)$, sobre o corpo de funções Hermitiano dado no exemplo 4.2.1. com o divisor G tal que $G = aP_0 + bP_\infty$, fornecidas pelo teorema da cota do piso generalizada. Os valores destacados em negrito são a distância mínima exata do código, de acordo com a referência [11].

$0 \leq a \leq 12, 14 \leq b \leq 40$	0	1	2	3	4	5	6	7	8	9	10	11	12
14													2
15												3	4
16											3	3	5
17										3	4	4	6
18									3	4	5	5	6
19								4	4	5	6	6	7
20							4	4	5	6	6	7	7
21						3	4	5	5	6	6	7	
22					3	4	5	6	6	7	7	8	9
23				3	4	5	6	6	6	7		9	
24			3	3	4	5	6	7	7	8	9	10	11
25		2	4	5	6	6	7	7		9		11	
26		2	4	5	6	7	8	8		10		12	
27	2	4	6	6	7	8	9	10	10	12	12	14	14
28	4	6	8	8	9	10	10	12	12	13	14	14	15
29	4	6	8	8	9	10	10	12	12	13	14		
30	5	7	9	9	10	11	12	13	13	14	15	16	17
31	6	8	10	10	11	12	12	13	14				
32	7	9	10	10	12	12	14	14	15	16	17	18	19
33	8	10	12	12	13	13	14						
34		10	12	12	13	14	15						
35	10	12	13	13	14		16						
36		12	14	14	15		17						
37	12	14	14		16		18						
38		14	15		17		19						
39		15	16		18		20						
40	15	16	17	18	19	20	21	22	23	24	25	26	27

Tabela 4.4: Nesta tabela a primeira linha fornece o valor de a e a primeira coluna, o valor de b ; os demais números que aparecem no cruzamento de uma linha com uma coluna são cotas inferiores para a distância mínima de códigos, do tipo $C_\Omega(D, G)$, sobre o corpo de funções de Suzuki dado no exemplo 4.2.3. com o divisor $G = A + B = aP_0 + bP_\infty$ onde A e B são divisores efetivos, fornecidas pelo teorema da cota do piso generalizada.

Referências Bibliográficas

- [1] Chen, Chien-Yu and Duursma, I. M., *Geometric Reed-Solomon codes of length 64 and 65 over $\mathbb{F}_8$* , IEEE Transactions on Information Theory, vol. 49, pp. 1351-1353, 2003.
- [2] Homma, M., and Kim, S. J., *Goppa codes with Weierstrass pairs*, Journal of Pure and Applied Algebra, vol. 162, pp. 273-290, 2001.
- [3] Kim, S. J., *On the index of the Weierstrass semigroup of a pair of points on a curve*, Archiv der Mathematik, vol. 62, pp. 73-82, 1994.
- [4] Kumar, P. V., Stichtenoth, H., and Yang, K., *On the Weight Hierarchy of Geometric Goppa Codes*, IEEE Transactions on Information Theory, vol. 40, pp. 913-920, 1994.
- [5] Lang, S., *Algebra*, Springer, 3rd. ed., 2002.
- [6] Lundell, B., and McCullough, J., *A generalized floor bound for the Minimum Distance of Geometric Goppa Codes*, Journal of Pure and Applied Algebra, vol. 207, pp. 155-164, 2006.
- [7] Maharaj, H., and Matthews, G. L., *On the floor and the ceiling of a divisor*, Finite Fields and their Applications, vol.12, pp. 38-55, 2006.
- [8] Maharaj, H., Matthews G. L., and Pirsic, G., *Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences*, Journal of Pure and Applied Algebra, vol. 195, pp. 261-280, 2005.
- [9] Matthews, G. L., *Codes from the Suzuki function field*, IEEE Transactions on Information Theory, vol. 50, pp. 3298-3302, 2004.
- [10] Matthews, G. L., *Weierstrass Pairs and Minimum Distance of Goppa Codes*, Designs, Codes and Cryptography, vol. 22, pp. 107-121, 2001.
- [11] Park, Seungkook, *Minimum distance of Hermitian two-point codes*, Designs, Codes and Cryptography, vol. 57, pp. 195-213, 2009.
- [12] Stichtenoth, H., *Algebraic Function Fields and Codes*, Berlin Heidelberg New York: Springer-Verlag, 1993.