Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Programa de Pós-Graduação em Matemática

Oscar Jhoan Palacio Marín

Códigos Hermitianos Generalizados

Juiz de Fora
2016

Oscar Jhoan Palacio Marín

Códigos Hermitianos Generalizados

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2016

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Palacio, Oscar.
Códigos Hermitianos Generalizados / Oscar Jhoan Palacio Marín. – 2016.
111 f.

Orientadora: Beatriz Casulari da Motta Ribeiro
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Matemática, 2016.

1. Corpo de Funções. 2. Corpos Finitos. 3. Códigos Corretores de Erros. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Título.

Oscar Jhoan Palacio Marín

Códigos Hermitianos Generalizados

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovada em: 23 de Junho de 2016

BANCA EXAMINADORA

Prof. Dr. Beatriz Casulari da Motta Ribeiro - Orientadora
UFJF

Professor Dr. Frederico Sercio Feitosa
UFJF

Professor Dr. Fernando Eduardo Torres Orihuela
UNICAMP

RESUMO

Nesse trabalho, estamos interessados, especialmente, nas propriedades de duas classes de Códigos Corretores de Erros: os Códigos Hermitianos e os Códigos Hermitianos Generalizados. O primeiro é definido a partir de lugares do corpo de funções Hermitiano clássico sobre um corpo finito de ordem quadrada, já o segundo é definido a partir de uma generalização desse mesmo corpo de funções. Como base para esse estudo, apresentamos ainda resultados da teoria de corpos de funções e outras construções de Códigos Corretores de Erros.

Palavras-chave: Corpos de Funções. Corpos Finitos. Códigos Corretores de Erros. Códigos Hermitianos.

ABSTRACT

In this work we investigate properties of two classes of error-correcting codes, the Hermitian Codes and their generalization. The Hermitian Codes are defined using the classical Hermitian curve defined over a quadratic field. The generalized Hermitian Codes are similar, but uses a generalization of this curve. We also present some results of the theory of function fields and other constructions of error-correcting codes which are important to understand this work.

Key-words: Function Fields. Finite Field. Error-Correcting codes. Hermitian Codes

SUMÁRIO

INTRODUÇÃO

A teoria dos códigos corretores de erros tem a sua origem no ano 1948, com o artigo [13] publicado por Shannon C.E., no Bell System Technical Journal. Os trabalhos de Shannon, em geral, são baseados em probabilidade e somente mostram a existência de bons códigos, mas não como poderiam ser feitos. A construção explícita destes códigos foi necessária a partir de 1970, pelas pesquisas espaciais e a implementação dos computadores. Os trabalhos em álgebra abstrata e teoria dos números de R. Hamming, M. Golay, entre outros, são os primeiros nesse sentido. Na atualidade, cada vez que se deseja transmitir ou armazenar dados de tal maneira que seja garantida sua confiabilidade, é utilizado um código corretor de erros. São exemplos disto as transmissões de dados via satélite e sondas espaciais da NASA, fitas magnéticas dos computadores, sistemas digitais de audio e vídeo (DVD, Blu-Ray), redes ADSL, telefone celular, entre outras.

A finalidade dos códigos corretores de erros é detectar e corrigir a maior quantidade de erros que podem ocorrer durante a transmissão por meio de um canal (canal de radiofrequência, canal de micro-ondas, cabo, circuito integrado, circuito integrado digital, etc.). Exemplos explícitos podem ser encontrados em [3] e [6].

Matematicamente, um código corretor de erros C é um subconjunto próprio de $\mathbb{F}_q^n$, para algum número natural n. No caso em que este subconjunto C é um subespaço linear de $\mathbb{F}_q^n$, o código é dito linear. Um tal código tem parâmetros $[n, k, d]$, onde n é seu comprimento, k é a sua dimensão e $d = \min\{d(a, b) \mid a, b \in C \text{ com } a \neq b\}$ é a sua distância mínima, onde $d(a, b) = \#\{i \mid a_i \neq b_i\}$.

A importância da distância mínima pode ser entendida pela ideia: se v_i são as palavras do código, isto é, v_i são os vetores de C, então recebida uma palavra u, pode-se verificar $d(u, v_i)$ para cada i, e aproximar u pelo v_i mais próximo. Assim, uma distância mínima grande garante que as palavras do código estão mais distantes, o que faz que a correção como explicada seja mais eficiente. O resultado abaixo, cuja prova pode ser encontrada em [6], resume isso formalmente.

Teorema. *Seja C um código com distância mínima d. Então C pode corrigir até $\kappa = [\frac{d-1}{2}]$ erros e detectar até $d - 1$ erros. Onde $[t]$ representa a parte inteira do número real t.*

Assim, é fundamental, para a Teoria dos Códigos, poder calcular d ou pelo menos determinar uma cota inferior para a mesma.

Goppa, em 1977, utilizando conceitos da geometria algébrica, introduziu uma nova forma de construir códigos lineares, a partir de um corpo de funções algébricas $F/\mathbb{F}_q$ de gênero $g \geq 0$. Esta construção também pode ser feita em termos de curvas algébricas, ver [5]. Por tal motivo, o estudo dos códigos de Goppa é uma forte motivação no estudo da geometria algébrica. A chave nas construções de Goppa reside no fato de que pode-se

obter informação dos parâmetros do código em termos da informação do corpo de funções onde foi construído (número de lugares, gênero). O método de Goppa é uma generalização dos códigos de Reed-Solomon, isto será mostrado na seção 2.3.

Para esta construção, deve-se considerar um corpo de funções algébricas $F/\mathbb{F}_q$ de gênero g, n lugares $P_1, P_2, \ldots, P_n$ dois a dois distintos de $F/\mathbb{F}_q$ de grau um, tomando o divisor $D = P_1 + P_2 + \ldots + P_n$ e G outro divisor de $F/\mathbb{F}_q$ tal que $Supp(D) \cap Supp(G) = \emptyset$. O código de Goppa associado aos divisores D e G está definido como a imagem do espaço de Riemann-Roch $\mathcal{L}(G)$ pela função avaliação

$$\begin{array}{rccc} ev_D: & \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n \\ & x & \longmapsto & (x(P_1), x(P_2), \ldots, x(P_n)) \end{array}$$

Fixados os parâmetros n e g, os demais parâmetros do código apenas dependem do grau do divisor G. A escolha mais simples de G e que produz os melhores resultados é quando $G = mQ$, onde Q é um divisor tal que $Q \notin Supp(D)$. Neste caso, o espaço $\mathcal{L}(G)$ esta intrinsecamente relacionado com o semigrupo de Weierstrass em Q.

Um problema natural da teoria de códigos é: fixados n, k, q, determinar d. Ainda, é interesante ter $\frac{d}{n}$ e $\frac{k}{n}$ grandes pois tais taxas determinan a taxa de detecção do código e a quantidade de informação útil recebida. Nesse sentido, os códigos de Goppa, em geral apresentam bons resultados. Por exemplo, em 1982, foi apresentada a primeira aplicação relevante devido a Tsfasman, Vladut e Zink [17], que mostram que é possível uma construção de códigos de Goppa com bons parâmetros que assintóticamente eram melhor que a cota de Gilbert-Varshamov [16], [15].

Neste trabalho, apresentaremos os resultados gerais e mais conhecidos na literatura dos códigos de Goppa e, em particular, dos códigos Hermitianos. Mas ainda, baseados no artigo [8], publicado em 2013, mostraremos resultados gerais dos Códigos Hermitianos Generalizados e também vamos calcular a distância mínima exata destes códigos para alguns valores do semigrupo de Weierstrass em Q.

Apresentamos a seguir a divisão de capítulos que nos conduzirá ao resultado principal.

No Capítulo 1, iniciamos o estudo sobre a teoria geral dos corpos de funções, mostrando resultados clássicos até resultados importantes como o Teorema de Riemann-Roch.

No Capítulo 2, apresentamos as definições gerais e básicas dos códigos corretores de erros. Também a construção dos códigos de Goppa como generalização dos códigos de Reed-Solomon. Além disso, mostramos as propriedades que os mesmos satisfazem em relação aos pesos de Hamming generalizados.

No Capítulos 3, estudamos os fundamentos das extensões de corpos de funções

algébricas. Além disso, definimos e provamos propriedades gerais dos códigos Hermitianos.

No Capítulo 4, definimos os códigos Hermitianos Generalizados. Provamos ainda propriedades destes códigos, algumas delas generalizações das vistas no Capítulo 3 e outras novas. Finalmente, provamos o Teorema 4.2.1 que é o objetivo principal deste trabalho.

1 CONCEITOS PRELIMINARES

Os códigos corretores de erros fazem parte de nossa vida cotidiana: estão presentes, por exemplo, na hora de assistir a um programa na televisão, quando falamos no telefone, ouvimos música ou navegamos pela Internet.

A maioria dos textos introdutórios desta teoria somente apresentam fundamentos matemáticos e seus aspectos mais essenciais de natureza algébrica. Para ter uma melhor abordagem e compreensão dos códigos corretores de erros, precisamos de algumas ferramentas mais fortes da teoria de corpos de funções algébricas.

1.1 LUGARES

Definição 1.1.1. *Um corpo de funções algébricas F/K em uma variável sobre um corpo K é uma extensão F de K, onde F é uma extensão algébrica finita de $K(x)$ para algum $x \in F$ transcendente sobre K*

Notemos que, da definição, o conjunto $\widetilde{K} = \{z \in F \mid \text{ z é algébrico sobre K}\}$ chamado corpo de constante da extensão F/K, é um subcorpo de F que satisfaz $K \subseteq \widetilde{K} \subsetneq F$. Além disso, $F/\widetilde{K}$ é um corpo de funções algébricas sobre $\widetilde{K}$ e K será dito algebricamente fechado em F se $\widetilde{K} = K$.

Utilizaremos também em futuras demonstrações o seguinte resultado muito conhecido da Álgebra abstrata.

Observação 1.1.1. *Um elemento $z \in F$ é transcendente sobre K se, e somente se, a extensão $F/K(z)$ é finita.*

Definição 1.1.2. *Dado um corpo de funções algébricas F/K o anel $\mathcal{O} \subseteq F$ que satisfaz as seguintes propriedades é dito anel de valorização de F/K.*

i) $K \subsetneq \mathcal{O} \subsetneq F$.

ii) Para cada $z \in F$, temos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$

Proposição 1.1.1. *Um anel de valorização $\mathcal{O}$ do corpo de funções algébricas F/K é um anel local.*

Demonstração. Devemos provar que $\mathcal{O}$ possui um único ideal maximal. Definamos o conjunto $P = \mathcal{O} \setminus \mathcal{O}^*$, onde $\mathcal{O}^* = \{z \in \mathcal{O} \mid \ z \text{ é invertível}\}$.

Se $x \in P$ e $z \in \mathcal{O}$, temos que $xz \notin \mathcal{O}^*$, pois, caso contrário, teríamos que $x \in \mathcal{O}^*$, o que seria uma contradição. Portanto, $xz \in P$.

Sejam $x, y \in P \setminus \{0\}$. Claramente, xy^{-1} e yx^{-1} são elementos de F, assim, pela definição de $\mathcal{O}$, temos que $xy^{-1} \in \mathcal{O}$ ou $yx^{-1} \in \mathcal{O}$. Sem perda de generalidade, suponhamos que $xy^{-1} \in \mathcal{O}$. Temos que $1 + xy^{-1} \in \mathcal{O}$ e, por outro lado, pela passagem acima, $x + y = y(1 + xy^{-1}) \in P$. Logo, P é um ideal de $\mathcal{O}$.

Suponha agora que J é outro ideal de $\mathcal{O}$ tal que $P \subsetneq J \subseteq \mathcal{O}$, assim existe um elemento $x \in J$ e $x \notin P$, mas a definição de P implica que $x \in \mathcal{O}^*$, ou seja, $xx^{-1} = 1 \in J$ e daí $J = \mathcal{O}$, consequentemente P é um ideal maximal de $\mathcal{O}$

A unicidade do ideal maximal P se garante pelo fato de que se existe outro ideal maximal N, este não possui elementos invertíveis. Como $N \subseteq P \subsetneq \mathcal{O}$, segue que $N = P$.

✓

Corolário 1.1.1. *Dados um anel de valorização $\mathcal{O}$ do corpo de funções algébricas F/K e seu ideal maximal $P = \mathcal{O} \setminus \mathcal{O}^*$. Então:*

i) Seja $x \in F \setminus \{0\}$. Então $x \in P$ se, e somente se, $x^{-1} \notin \mathcal{O}$

ii) O corpo de constante $\widetilde{K}$ de F/K é um subconjunto de $\mathcal{O}$ e $\widetilde{K} \cap P = \{0\}$

Demonstração. i) Decorre diretamente das definições de P e $\mathcal{O}$

ii) Suponha que existe um elemento $t \in \widetilde{K}$ e $t \notin \mathcal{O}$. Então, pela definição de $\mathcal{O}$ temos que $t^{-1} \in \mathcal{O}$. Além disso, como $\widetilde{K}$ é corpo implica que se t é algébrico sobre K então t^{-1} também é algébrico sobre K, desta forma

$$a_m(t^{-1})^m + \ldots + a_1(t^{-1}) + 1 = 0$$

para $a_i \in K$ com $i = \{1, 2 \ldots, m\}$. Mas ainda,

$$(t^{-1})(a_m(t^{-1})^{m-1} + \ldots + a_1) = -1$$

$$t = -(a_m(t^{-1})^{m-1} + \ldots + a_1) \in K[t^{-1}] \subseteq \mathcal{O}$$

que é uma contradição. Logo $\widetilde{K} \subseteq \mathcal{O}$. Analogamente, podemos mostrar que se $t \in \widetilde{K} \setminus \{0\}$, então $t \in \mathcal{O}$, consequentemente $t \in \mathcal{O}^*$ e daí $\widetilde{K} \cap P = \{0\}$

✓

Lema 1.1.1. *Sejam $\mathcal{O}$ o anel de valorização do corpo de funções algébricas F/K, P seu ideal maximal e $x \in P \setminus \{0\}$. Sejam ainda $x_1, x_2, \ldots, x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$ para cada $i = 1, 2, \ldots, n-1$. Temos que $n \leq [F : K(x)] < \infty$.*

Demonstração. Pela observação 1.1.1 e o corolário 1.1.1, podemos afirmar que a extensão $[F : K(x)]$ é finita. Logo, é suficiente provar que os elementos $x_1, x_2, \ldots, x_n$ são linearmente

independentes sobre $K(x)$. Suponhamos que existe uma combinação linear não trivial

$$\sum_{i=1}^{n} f_i(x)x_i = 0 \quad \text{com} \quad f_i(x) \in K(x).$$

Sem perda de generalidade, temos que $f_i(x) \in K[x]$ e x não divide $f_i(x)$ para algum i. Seja $a_i := f_i(0)$ o termo independente de $f_i(x)$ e fixemos $j \in \{1, 2, \ldots, n\}$ tal que $a_j \neq 0$, mas $a_i = 0$ para cada $i > j$. Assim

$$\sum_{i \neq j} f_i(x)x_i + f_j(x)x_j = 0 \Rightarrow -f_j(x)x_j = \sum_{i \neq j} f_i(x)x_i$$

onde $f_i(x) \in \mathcal{O}$, para cada $i \in \{1, \ldots, n\}$ pois $x = x - i \in P$, além disso $x_i \in x_j P$, para $i < j$ e $f_i(x) = xg_i(x)$, para $i > j$, onde $g_i(x) \in K[x]$. Portanto,

$$-f_j(x)x_j = \sum_{i<j} f_i(x)\frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i(x)x_i = \sum_{i<j} f_i(x)\frac{x_j p_i}{x_j} + \sum_{i>j} \frac{x_j p}{x_j} g_i(x)x_i$$

com $p, p_i \in P$, de modo que a última parcela da igualdade anterior é um elemento de P. Por outro lado, $f_j(x) = a_j + xg_j(x)$, com $g_j(x) \in K[x] \subseteq \mathcal{O}$. Assim, $a_j = f_j(x) - xg_j(x) \in P$ e, como $a_j \in K$ (pois é o termo independente de $f_j(x)$), isto implica que

$$a_j \in P \cap K \subseteq P \cap \widetilde{K} = \{0\}$$

o que é uma contradição, já que $a_j \neq 0$ ✓

O Lema acima é o ingrediente principal para provar o seguinte teorema.

Teorema 1.1.1. *Sejam $\mathcal{O}$ o anel de valorização do corpo de funções algébricas F/K e P seu único ideal maximal. Então*

i) P é um ideal principal.

ii) Se $P = t\mathcal{O}$, então cada elemento $z \in F \setminus \{0\}$ tem uma única representação $z = t^n u$, para algum $n \in \mathbb{Z}$ e u é um elemento invertível de $\mathcal{O}$.

iii) $\mathcal{O}$ é um domínio de ideais principais. Na verdade, se $P = t\mathcal{O}$ e dado um ideal I tal que $\{0\} \subsetneq I \subseteq \mathcal{O}$, então $I = t^n\mathcal{O}$ para algum $n \in \mathbb{Z}$.

Demonstração. i) Suponhamos que P não seja um ideal principal, como nenhum elemento de P é gerador, então tomando $a_1 \in P \setminus \{0\}$ como $P \neq a_1\mathcal{O}$, existe $a_2 \in P \setminus a_1\mathcal{O}$.

Notemos que $a_2 a_1^{-1} \notin \mathcal{O}$ e, pelo corolário 1.1.1, temos que $a_2^{-1}a_1 \in P$. Portanto $a_1 = a_2(a_2^{-1}a_1) \in a_2 P$. Fazendo este mesmo argumento, obtemos uma sequência infinita $a_1, a_2, \ldots, a_n \ldots$ de elemento de P tais que $a_n \in P \setminus a_{n-1}\mathcal{O}$ e $a_{n-1} \in a_n P$, para cada $n \geq 2$ o que é uma contradição pelo lema 1.1.1.

ii) Seja $z \in F \setminus \{0\}$, sem perda de generalidade, suponhamos que $z \in \mathcal{O}$. Se z é invertível então $z = t^0 z$. Resta provar o caso quando $z \in P$. Por hipótese $P = t\mathcal{O}$ e, pelo lema 1.1.1, o comprimento da sequência

$$x_1 = z, \quad x_2 = t^{l-1}, \quad x_3 = t^{l-2} \quad \ldots \quad x_{l-1} = t^2, \quad x_l = t$$

tem que ser finito. Logo, existe um valor máximo $l \geq 1$ tal que $z \in t^l\mathcal{O}$. Agora $z = t^l u$ onde $u \in \mathcal{O}^*$ pois se $u \notin \mathcal{O}^*$ então $u \in P = t\mathcal{O}$ e daí $z \in t^{l+1}\mathcal{O}$, que é uma contradição pela maximalidade de l.

Para provar a unicidade da representação, suponhamos que $z = ut^n = vt^m$, onde $u, v \in \mathcal{O}^*$ e $n \geq m$. Logo $uv^{-1} = t^{n-m}$, e portanto $n = m$ e $uv^{-1} = 1$ consequentemente $n = m$ e $u = v$.

iii) Seja $\{0\} \subsetneq I \subseteq \mathcal{O}$, notemos que se $x \in I \setminus \{0\}$, então $x = t^r u$, onde $u \in \mathcal{O}^*$ logo $t^r = u^{-1}x$, portanto o conjunto $A := \{r \in \mathbb{N} \mid t^r \in I\}$ é não vazio e possui um menor elemento, definamos $n = min(A)$. Resta provar que $I = t^n\mathcal{O}$. De fato, claramente $t^n\mathcal{O} \subseteq I$ pois $t^n \in I$. Agora seja $y \in I$ não nulo, então $y = t^r u$ com $u \in \mathcal{O}^*$ e $r \geq 0$. Mas $t^r = u^{-1}y$ e $n = min(A)$ isto implica que $n \leq r$, portanto $t^n | t^r$ e desse modo $t^n | y$, assim temos que $y \in t^n\mathcal{O}$. Finalmente $I \subseteq t^n\mathcal{O}$ como desejávamos. ✓

Definição 1.1.3. *i) Todo anel que satisfaz o teorema* 1.1.1 *é dito anel de valorização discreta.*

ii) Dado $\mathcal{O}$ o anel de valorização do corpo de funções algébricas F/K, seu ideal maximal P é dito um lugar do corpo de funções algébricas F/K. Além disso cada elemento t tal que $P = t\mathcal{O}$ é chamado elemento primo de P

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

Denotaremos por $\mathcal{O}_P = \mathcal{O}$ o anel de valorização associado ao lugar P. A seguir aplicaremos alguns dos resultados mostrados até agora, em um corpo de funções algébricas particular chamado corpo de funções racionais.

Definição 1.1.4. *Uma valorização discreta do corpo de funções racionais F/K é uma função $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:*

i) $v(x) = \infty$ *se, e somente se,* $x = 0$.

ii) $v(xy) = v(x) + v(y)$, *para cada* $x, y \in F$

iii) $v(x + y) \geq \min\{v(x), v(y)\}$ *para todo* $x, y \in F$

iv) Existe um elemento $z \in F$ *tal que* $v(z) = 1$

v) $v(a) = 0$ *para todo* $a \in K \setminus \{0\}$

Decorre da definição acima que as valorizações discretas são funções sobrejetoras.

Lema 1.1.2 (Desigualdade Triangular Estrita)**.** *Seja v uma valorização discreta do corpo de funções algébricas F/K, então $v(x+y) = \min\{v(x), v(y)\}$ para cada par $x, y \in F$ tal que $v(x) \neq v(y)$.*

Demonstração. Notemos que se $a \in K$ é não nulo e $z \in F$ é um elemento qualquer então $v(az) = v(a) + v(z) = v(z)$. Assim, em particular, $v(-z) = v(z)$ para todo $z \in F$. Por hipótese, podemos supor, sem perda de generalidade, que $v(y) > v(x)$. Suponhamos que $v(x+y) \neq \min\{v(x), v(y)\}$. Por definição, temos então que $v(x+y) > v(x)$. Por outro lado, $v(x) = v((x+y) - y) \geq \min\{v(x+y), v(y)\} > v(x)$, o que é uma contradição. Logo, o lema vale. ✓

Definição 1.1.5. *Definimos a função $v_P : F \to \mathbb{Z} \cup \{\infty\}$ associada a um lugar $P \in \mathbb{P}_F$ da seguinte maneira: dado um elemento primitivo t de P, sabemos, pelo Teorema* 1.1.1*, que cada elemento não nulo $z \in F$ tem uma representação única na forma $z = t^n u$, onde $u \in \mathcal{O}_P^*$ e $n \in \mathbb{Z}$. Assim, definimos $v_P(z) = n$ e $v(0) = \infty$.*

Temos que v_p cumpre $i), ii)$ e $iv)$ da definição 1.1.4, mostremos agora que cumpre as demais propriedades de valorização discreta. De fato,

iii) Consideramos somente o caso não trivial, ou seja, $x, y \in F$ tais que $x = t^n u$, $y = t^m w$, $u, w \in \mathcal{O}_P^*$ e $n \leq M < \infty$. Logo, $x + y = t^n(u + t^{m-n}w) = t^n z$ onde $z \in \mathcal{O}$. Se $z = 0$ $v_P(x+y) + \infty > \min\{n, m\}$, caso contrário $z = t^k v$ com $k \geq$ e $v \in \mathcal{O}_P^*$. Consequentemente

$$v_P(x+y) = v_P(t^{n+k}v) = n + k \geq n = \min\{n, m\} = \min\{v_P(x), v_P(y)\}$$

v) Como $K \setminus \{0\} \subseteq \widetilde{K} \setminus \{0\} \subseteq \mathcal{O}_P^*$, temos que $v_P(a) = v_P(t^0 a) = 0$ para cada $a \in K \setminus \{0\}$

Além disso, notemos que se t' é outro elemento primo de P, temos que $P = t\mathcal{O} = t'\mathcal{O}$, portanto $t = t'w$, onde $w \in \mathcal{O}_P^*$. Consequentemente, $t^n u = (t'^n w^n)u = t'^n(w^n u)$, onde $w^n u \in \mathcal{O}_P^*$. Assim, v_P não depende da escolha do elemento primo t, somente depende do lugar P.

Teorema 1.1.2. *Seja F/K um corpo de funções algébricas.*

i) Sejam $P \in \mathbb{F}_P$ e sua valorização discreta v_P temos que

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

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

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

ii) Um elemento $z \in F$ é um elemento primo de P se, e somente se, $v_P(z) = 1$.

iii) Reciprocamente, seja v uma valorização discreta de F/K. Então, o conjunto

$$P = \{z \in F \mid v(z) > 0\}$$

é um lugar de F/K e

$$\mathcal{O}_P = \{z \in F \mid v(z) \geq 0\}$$

é o anel de valorização correspondente.

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

Demonstração. i) Seja $x \in \{z \in F \mid v_P(z) \geq 0\}$ então $v_P(x) \geq 0$. Se $v_P(x) = \infty$ temos que $x = 0 \in \mathcal{O}_P$. Caso contrário, existem $n \in \mathbb{Z}_+$ e um elemento primitivo t de P tais que $x = t^n u$ com $u \in \mathcal{O}^*$ e $v_P(x) = n \geq 0$. Se $n = 0$ temos que $x = u \in \mathcal{O}^* \subseteq \mathcal{O}$, se $n > 0$ $x \in t\mathcal{O} = P \subseteq \mathcal{O}$. Reciprocamente se $z \in \mathcal{O} \setminus \{0\}$, pelo teorema 1.1.1 temos que $z = t^n u$ para $n \in \mathbb{Z}_+$ e $u \in \mathcal{O}^*$ e assim $v_P(z) \geq 0$. No caso que $z = 0$, implica que $v_P(z) = \infty > 0$. Consequentemente

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

Analogamente podemos provar que

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

e como $P = \mathcal{O} \setminus \mathcal{O}_P^*$ temos que,

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

ii) $\Rightarrow$) Seja z um elemento primo de P temos então que $z = z1$, logo $v_P(z) = 1$.

$\Leftarrow$) Seja $z \in F$ tal que $v_P(z) = 1$, fixando um elemento primo t de P temos que $z = tu$ onde $u \in \mathcal{O}_P^*$. Assim, $P = t\mathcal{O}_P = z\mathcal{O}_P$, portanto z é um elemento primitivo de P.

iii) Mostremos primeiro que $\mathcal{O}_P = \{z \in F \mid v(z) \geq 0\}$ é um subanel de F. De fato, como $v(0) = \infty > 0$ temos que $0 \in \mathcal{O}_P$. Sejam $x, y \in \mathcal{O}_P$ então $v(x) \geq 0$ e $v(y) \geq 0$. Logo,

$$v(x - y) \geq \min\{v(x), v(y)\} \geq 0$$

$$v(xy) = v(x) + v(y) \geq 0.$$

Portanto, temos que $x - y$ e xy são elementos de $\mathcal{O}_P$, onde $\mathcal{O}_P$ é um subanel de F.

Além disso, como uma valorização discreta, em particular, é uma função sobrejetora, temos que existe um elemento $z \in F$ tal que $v(z) = -1$, logo $z \notin \mathcal{O}_P$ o que mostra que $\mathcal{O}_P \subsetneq F$. Ainda, pela definição de v, sabemos que $v(a) = 0$ para todo $a \in K \setminus \{0\}$, portanto

$K \subseteq \mathcal{O}_P$. Novamente pela sobrejetividade de v, existe um $z \in \mathcal{O}_P$ tal que $v(z) = 1$, e daí $K \subsetneq \mathcal{O}_P$.

Por outro lado, se $z \in F \setminus \{0\}$, temos que

$$0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1}) \Longrightarrow v(z) \geq 0 \quad \text{ou} \quad v(z^{-1}) \geq 0$$

consequentemente, $z \in \mathcal{O}_P$ ou $z^{-1} \in \mathcal{O}_P$. Concluímos assim que $\mathcal{O}_P$ é um anel de valorização.

Agora analisaremos os elementos de $\mathcal{O}_P$ que são invertíveis. Seja $z \in \mathcal{O}_P^*$, assim existe um elemento $z^{-1} \in \mathcal{O}_P$ tal que

$$0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1}),$$

mas $v(z) \geq 0$ e $v(z^{-1}) \geq 0$, isto implica que $v(z) = v(z^{-1}) = 0$. Reciprocamente, se $z \in \mathcal{O}_P$ tal que $v(z) = 0$. Então, existe $z^{-1} \in F$ tal que

$$0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1}) = v(z^{-1})$$

isto implica que $v(z^{-1}) = 0$ e daí $z^{-1} \in \mathcal{O}_P$. Assim, um elemento z é invertível em $\mathcal{O}_P$ se, e somente se, $v(z) = 0$. Portanto, $P = \mathcal{O}_P^* \setminus \mathcal{O}_P = \{z \in F \mid v(z) > 0\}$.

iv) Seja A um subanel de F tal que $\mathcal{O} \subsetneq A \subseteq F$, onde $\mathcal{O}$ é um anel de valorização do corpo de funções algébricas F/K, P seu ideal maximal e v_P é a valorização discreta associada a P. Seja $z \in F \setminus \mathcal{O}$, logo pelo corolário 1.1.1 $z^{-1} \in P$ portanto $v(z^{-1}) > 0$. Então, para algum $k \geq 0$ suficientemente grande e $x \in F$ temos que

$$v_P(xz^{-k}) = v_P(x) + v_P(z^{-1}), \ldots, v_P(z^{-1}) \geq 0$$

Assim, $y = xz^{-1} \in \mathcal{O}$ e $x = yz^k \in \mathcal{O}[z]$. Consequentemente, como x é arbitrário, segue que $F = \mathcal{O}[z]$ e daí $A = F$. ✓

Notemos que dados um lugar P de um corpo de funções algébricas F/K e $\mathcal{O}_P$ o anel de valorização correspondente, como P é maximal, então $\mathcal{O}_P/P$ é um corpo. Logo, para cada $x \in \mathcal{O}_P$ podemos definir $x + P \in \mathcal{O}_P/P$ a classe residual de x módulo P. Além disso sabemos, pelo Corolário 1.1.1, que $K \subseteq \mathcal{O}_P$ e $K \cap P = \{0\}$, então o homomorfismo de classes residuais

$$\begin{aligned} \mathcal{O}_P &\longrightarrow \mathcal{O}_P/P \\ x &\longmapsto x + P \end{aligned}$$

induz um mergulho canônico de K em $\mathcal{O}_P/P$. Analogamente para $\widetilde{K}$. De modo que podemos considerar a $\mathcal{O}_P/P$ como sendo uma extensão de K e $\widetilde{K}$.

Definição 1.1.6. *Seja $P \in \mathbb{P}_F$ um lugar de F/K.*

i) $F_P := \mathcal{O}_P/P$ *é o corpo de classes residuais de* P*. A aplicação* $x \longmapsto x + P$ *é chamada mapa das classes residuais com respeito a* P*. Utilizaremos em geral a notação* $x + P = x(P)$*.*

ii) O grau do lugar P *é definido como* $\deg(P) = [F_P : K]$*. Um lugar de grau 1 é dito lugar racional de* F/K*.*

Proposição 1.1.2. *Dado um lugar* P *do corpo de funções algébricas* F/K *e* $x \in P \setminus \{0\}$*, então* $\deg(P) \leq [F : K(x)] < \infty$*.*

Demonstração. Como $x \in P\setminus\{0\}$ e $\widetilde{K} \cap P = \{0\}$, temos que x é um elemento transcendente sobre K, assim a observação 1.1.1 implica que $[F : K(x)] < \infty$.

Por definição, $\deg(P) = [F_P : K]$, então é suficiente mostrar que se $z_1(P), \ldots, z_n(P)$ são linearmente independentes sobre K, então $z_1, \ldots, z_n \in \mathcal{O}_P$ são linearmente independentes sobre $K(x)$ e assim teríamos $\deg(P) \leq [F : K(x)]$.

Suponhamos que existe uma combinação linear não trivial,

$$\sum_{i=1}^{n} f_i(x) z_i = 0,$$

onde $f_1(x), \ldots, f_n(x) \in K(x)$ não são todos nulos. Sem perda de generalidade, podemos supor que $f_i(x) \in K[x]$ e não todos os $f_i(x)$ são divisíveis por x, portanto $f_i(x) = a_i + x g_i(x)$, onde $a_i \in K$, $g_i(x) \in K[x]$ e alguns dos $a_i \neq 0$. Notemos que se $x \in P$ e $g_i(x) \in K[x] \subseteq \mathcal{O}_P$, então $f_i(x)(P) = a_i(P) = a_i$. Consequentemente,

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

o que é uma contradição pois $z_1(P), \ldots, z_n(P)$ são linearmente independentes sobre K. ✓

Observação 1.1.2. *Se* K *é algebricamente fechado, então todos os lugares são racionais, pois* K *não tem uma extensão algébrica própria. Assim, podemos interpretar cada elemento de* $z \in F$ *como a função*

$$z : \begin{cases} \mathbb{P}_F \longrightarrow K \cup \{\infty\} \\ P \longmapsto z(P) \end{cases}$$

Por isto, F/K *é chamado um corpo de funções algébricas. Além disso, a observação justifica a seguinte definição.*

Definição 1.1.7. *Sejam* $P \in \mathbb{P}_F$ *um lugar de* F/K *e* $z \in F$*. Dizemos que* P *é um zero de* z *se* $v_P(z) > 0$*. Ainda,* P *é dito polo de* z *se* $v_P(z) < 0$*. Se* $v_P(z) = m > 0$*, então* P *é dito um zero de ordem* m*. Agora, se* $v_P(z) = -m < 0$*, então* P *é um polo de* z *de ordem* m*.*

Teorema 1.1.3. *Sejam F/K um corpo de funções algébricas e R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \subsetneq R$. Então, existe um lugar $P \in \mathbb{F}_P$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Demonstração. Consideremos o conjunto

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

Notemos que $\mathcal{F}$ é parcialmente ordenado pela relação de inclusão e como $R \in \mathcal{F}$, logo $\mathcal{F} \neq \emptyset$. Seja $\mathcal{C} \subseteq \mathcal{F}$ uma cadeia em $\mathcal{F}$, então $T = \bigcup_{S \in \mathcal{C}} S$ é um subanel de F com $R \subseteq T$. Agora suponha que $T \notin \mathcal{F}$, ou seja, $IT \neq T$. Então $1 = \sum_{i=1}^{n} a_i s_i$, onde $a_i \in I$ e $s_i \in T$, mas sendo $\mathcal{C}$ totalmente ordenado, então existe $S_0 \in \mathcal{C}$ tal que $s_i \in S_0$ para cada $i = 1, \ldots, n$, isto implica que $1 \in S_0$. Logo, $IS_0 = S_0$ o que é uma contradição pois $S_0 \in \mathcal{C} \subseteq \mathcal{F}$. Portanto, $T \in \mathcal{F}$, o que implica que toda cadeia em $\mathcal{F}$ possui limite superior em $\mathcal{F}$, assim pelo lema de Zorn $\mathcal{F}$ tem um elemento maximal. Seja então $\mathcal{O}$ o elemento que satisfaz essas propriedades.

Assim, $\mathcal{O} \subseteq F$, $R \subseteq \mathcal{O} \subseteq F$, $I\mathcal{O} \neq \mathcal{O}$ e $\mathcal{O}$ é maximal. Notemos que se $K = \mathcal{O}$, como, por hipótese, $K \subseteq R$, teríamos que $R = K$ é um corpo e, assim, seus únicos ideais seriam os triviais, o que é uma contradição. Portanto, $K \subsetneq \mathcal{O}$.

Além disso, sabemos que $I \neq \{0\}$ e $I\mathcal{O} \neq \mathcal{O}$. Se $\mathcal{O} = F$, teríamos que $IF = F$ o que é uma contradição, e daí $\mathcal{O} \subsetneq F$

Por outro lado, suponha que exista um elemento $z \in F$ tal que $z \notin \mathcal{O}$ e $z^{-1} \notin \mathcal{O}$. Logo, como $\mathcal{O}$ é um elemento maximal de F temos que $\mathcal{O}[z]$ e $\mathcal{O}[z^{-1}]$ não são elementos de $\mathcal{F}$ e como $R \subseteq \mathcal{O}[z] \subseteq F$ e $R \subseteq \mathcal{O}[z^{-1}] \subseteq F$ obtemos que $I\mathcal{O}[z] = \mathcal{O}[z]$ e $I\mathcal{O}[z^{-1}]$.

Então existem $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in I\mathcal{O}$ tais que

$$1 = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n$$

$$1 = b_0 + b_1 z^{-1} + b_2 z^{-2} + \ldots b_m z^{-1}$$

Como $I\mathcal{O} \neq \mathcal{O}$ temos que $n \geq 1$ e $m \geq 1$. Sejam n e m os valores mínimos que satisfazem as equações acima e suponhamos que $m \leq n$. Multiplicando a primeira equação por $(1 - b)$, a segunda por $a_n z^n$ e somando as novas equações temos que

$$1 = a_0(1 - b_0) + b_0 + a_1(1 - b_0)z + \ldots + [a_{n-1}(1 - b_0) + a_n b_1]z^{n-1},$$

o que é uma contradição pela minimalidade de n. Assim, temos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$ para todo elemento de F. Consequentemente, $\mathcal{O}$ é um anel de valorização de F/K.

Finalmente, provemos que $I \subseteq P$. Se $z \in I$ fosse um elemento invertível em $\mathcal{O}$ teríamos que $z.z^{-1} = 1 \in I\mathcal{O}$, onde $\mathcal{O} = I\mathcal{O}$ que novamente é uma contradição, portanto $I \subseteq P = \mathcal{O} \setminus \mathcal{O}^*$ ✓

Corolário 1.1.2. *Sejam F/K um corpo de funções algébricas e $z \in F$ um elemento transcendente sobre K. Então z possui pelo menos um zero e um polo. Em particular $\mathbb{P}_F \neq \emptyset$.*

Demonstração. Sejam $R = K[z]$ e o ideal $I = zK[z]$. Como $\{0\} \neq I \subsetneq R$, temos que existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$. Daí $z \in I \subseteq P$, donde $v_P(z) > 0$, ou seja, P é um zero de z. Analogamente, existe um zero Q para z^{-1}, isto é, um polo de z. ✓

Corolário 1.1.3. *O corpo de constantes $\widetilde{K}$ do corpo de funções algébricas F/K é uma extensão de corpos finita sobre K.*

Demonstração. Pelo Corolário 1.1.2 sabemos que $\mathbb{P}_F \neq \emptyset$. Escolhamos $P \in \mathbb{P}_F$. Sendo $\widetilde{K}$ um subcorpo de F_P, temos que

$$[\widetilde{K} : K] \leq [F_P : K] = \deg(P) \leq [F : K(x)] < \infty$$

para algum $x \in P \setminus \{0\}$. ✓

1.2 TEOREMA DA APROXIMAÇÃO FRACA

O teorema seguinte essencialmente afirma que se $v_1, \ldots, v_n$ são valorizações discretas de um corpo de funções algébricas F/K e $z \in F$, mesmo conhecendo $v_1(z), \ldots, v_{n-1}(z)$, não podemos concluir nada sobre $v_n(z)$.

Teorema 1.2.1 (Da Aproximação Fraca)**.** *Sejam $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares dois a dois distintos do corpo de funções algébricas F/K, $x_1, \ldots, x_n \in F$ e $r_1, \ldots, r_n \in \mathbb{Z}$. Então, existe $x \in F$ tal que $v_{P_i}(x - x_i) = r_i$ para cada $i = 1, \ldots, n$.*

Demonstração. Para simplificar a notação, escrevamos $v_i = v_{P_i}$.

Afirmação 1: Existe $u \in F$ tal que $v_1(u) > 0$ e $v_i(u) < 0$, para cada $i = 2, \ldots, n$.

De fato, faremos a prova por indução. Para $n = 2$, já que os anéis de valorização são subanéis próprios maximais de F, pelo Teorema 1.1.2, temos que $\mathcal{O}_{P_1} \subsetneq \mathcal{O}_{P_2}$. Logo, existem $y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$ e $y_2 \in \mathcal{O}_{P_2} \setminus \mathcal{O}_{P_1}$. De novo pelo Teorema 1.1.2, obtemos que $v_1(y_1) \geq 0$, $v_2(y_1) < 0$, $v_1(y_2) < 0$ e $v_2(y_2) \geq 0$. Agora, definamos o elemento $u = y_1/y_2$ e provemos que é o elemento procurado. Primeiramente

$$v_1(u) = v_1(y_1) + v_1(y_2^{-1}) = v_1(y_1) - v_1(y_2) > 0$$

$$v_2(u) = v_2(y_1) + v_2(y_2^{-1}) = v_2(y_1) - v_2(y_2) > 0$$

Para $n > 2$, por hipótese de indução, temos que existe um elemento y com $v_1(y) > 0$ e $v_i(y) < 0$ para cada $i \in \{2, \ldots, n-1\}$. Se $v_n(y) > 0$, então a prova da afirmação acaba

fazendo $u = y$. Caso contrário, ou seja, se $v_n(y) \geq 0$, escolhemos z tal que $v_1(z) > 0$ e $v_n(z) < 0$ e fazemos $u = y + z^r$, com $r \geq 1$ tal que $rv_i(z) \neq v_i(y)$ para $i = 1, \ldots, n-1$. Consequentemente

$$v_1(u) \geq \min\{v_1(y), rv_1(z)\} > 0 \text{ e } v_i(u) = \min\{v_i(y), rv_i(z)\} < 0 \text{ para } i \in \{2, \ldots, n\}.$$

Afirmação 2: Existe $w \in F$ tal que $v_1(w-1) > r_1$ e $v_i(w) > r_i$ para $i \in \{2, \ldots, n\}$

De fato, escolhamos u como na afirmação 1 e definamos $w = (1 + u^s)^{-1}$. Assim para um s suficientemente grande,

$$\begin{aligned} v_1(w-1) &= v_1\left(\frac{-u^s}{1+u^s}\right) \\ &= v_1(-u^s) + v_1((1+u^s)^{-1}) \\ &= sv_1(u) - v_1(1+u^s) \end{aligned}$$

Claramente $v_1(1) = 0$ e, como u foi definido como na afirmação 1, temos que $v_1(u^s) > 0$ para todo $s \in \mathbb{N}$. Assim, pelo Lema 1.1.2, temos que $v_1(1+u^s) = \min\{v_1(1),\ sv_1(u)\} = 0$. O mesmo resultado vale para v_i para cada $i = \{2, \ldots, n\}$. Logo, $v_1(w-1) = sv_1(u) > r_1$ e

$$\begin{aligned} v_i(w) &= -v_i(w^{-1}) \\ &= v_i(1+u^s) \\ &= -sv_i(u) > r_i \qquad \text{para cada } i = \{2, \ldots, n\}. \end{aligned}$$

Afirmação 3: Dados $y_1, \ldots, y_n \in F$, existe um elemento $z \in F$ com $v_i(z - y_i) > r_i$, para cada $i = \{1, 2, \ldots, n\}$.

De fato, escolhamos $s \in \mathbb{Z}$ tal que $v_i(y_j) \geq s$, para cada, $i, j \in \{1, \ldots, n\}$. Logo, pela afirmação 2, existem $w_1, \ldots, w_n$ tais que $v_i(w_i - 1) > r_i - s$ e $v_j(w_j) > r_j - s$ para $i \neq j$, $i, j \in \{1, \ldots, n\}$.

Seja $z = \sum_{j=1}^{n} y_j w_j$, então

$$\begin{aligned} v_i(z - y_i) &= v_i(y_i(w_i - 1) + \sum_{j \neq i} y_j w_j) \\ &= \min\{v_i(y_i(w_i-1)), v_i(y_1w_1), \ldots, v_i(y_{i-1}w_{i-1}), v_i(y_{i+1}w_{i+1}), \ldots v_i(y_nw_n)\} \\ &> r_i \end{aligned}$$

Finalmente, temos que, pela afirmação 3 podemos encontrar $z \in F$ tal que $v_i(z - x_i) > r_i$ para cada $i = \{1, 2, \ldots, n\}$. Lembrando que v_i é sobrejetora para todo i, podemos encontrar um z_i tal que $v_i(z_i) = r_i$. E, novamente pela afirmação 3, existe z' tal que $v_i(z' - z_i) > r_i$ para cada $i = \{1, 2, \ldots, n\}$. Portanto, para $x = z + z'$, temos que

$$v_i(z') = v_i((z' - z_i) + z_i) = \min\{v_i(z' - z_i), v_i(z_i)\} = r_i \qquad \text{e}$$

$$v_i(x - x_i) = v_i((z - x_i) + z') = \min\{v_i(z - x_i), v_i(z')\} = r_i.$$

✓

Corolário 1.2.1. *Todo corpo de funções algébricas possui um número infinito de lugares.*

Demonstração. Suponhamos que existam somente $P_1, \ldots, P_n$ lugares. Considerando $x_1 = x_2, \ldots, = x_n = 0$ e $r_1, r_2, \ldots, r_n$ no Teorema da Aproximação Fraca 1.2.1, existe um elemento $x \in F\backslash\{0\}$ tal que $v_{P_i} > 0$ $i = \{1, 2, \ldots, n\}$. Logo, x é um elemento transcendente de K que não possui polos, o que é uma contradição com o corolário 1.1.2. ✓

Proposição 1.2.1. *Sejam F/K um corpo de funções algébricas e $P_1, \ldots, P_r$ zeros do elemento $x \in F$. Então*

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

Demonstração. Definamos a seguinte notação $v_i = v_{P_i}$, $f_i = \deg(P_i)$ e $e_i = v_i(x)$.

Pelo Teorema da Aproximação Fraca 1.2.1, para cada i existe $t_i \in F$ tal que $v_i(t_i) = 1$ e $v_k(t_i) = 0$, para $k \neq i$. Sejam $s_{i1}, \ldots, s_{if_i} \in \mathcal{O}_{P_i}$ tais que $s_{i1}(P_i), \ldots, s_{if_i}(P_i)$ são uma base de F_{P_i} sobre K.

Em particular, com uma aplicação mais fraca do Teorema 1.2.1, existem $z_{ij} \in F$ tais que para todos i, j

$$v_i(s_{ij} - z_{ij}) > 0 \text{ e } v_k(z_{ij}) \geq e_n \text{ para } k \neq i.$$

Provemos agora que os elementos $t^a z_{ij}$ com $1 \leq i \leq r$, $1 \leq j \leq f_i$ e $o \leq ia \leq e_i - 1$ são linearmente independentes sobre $K(x)$. Então, suponha que exista uma combinação linear não trivial

$$\sum_{i=1}^{r} \sum_{j=1}^{j_i} \sum_{a=0}^{e_i-1} \varphi_{ija}(x) t_i^a z_{ij} = 0 \tag{1.1}$$

sobre $K(x)$. Sem perda de generalidade, $\varphi_{ija}(x) \in K[x]$ e nem todos os $\varphi_{ija}(x)$ são divisíveis por x. Então, existem índices $k \in \{1, \ldots, r\}$ e $c \in \{0, \ldots, e_k - 1\}$ tais que x divide $\varphi_{kja}(x)$ para todo $a < e$ e para todo $j \in \{1, \ldots, f_k\}$, e x não divide $\varphi_{kjc}(x)$ para algum $j \in \{1, \ldots, f_k\}$. Agora, multiplicando (1.1) por t_k^{-c}, obtemos

$$\sum_{i=1}^{r} \sum_{j=1}^{j_i} \sum_{a=0}^{e_i-1} \varphi_{ija}(x) t_i^a t_k^{-c} z_{ij} = 0. \tag{1.2}$$

Notemos que para $i \neq k$:

$$v_k(\varphi_{ija}(x) t_i^a t_k^{-c} z_{ij}) = v_k(\varphi_{ija}(x)) + v_k(t_i^a) + v_k(t_k^{-c}) + v_k(z_{ij}) \geq -c + e_k > 0.$$

Logo, todas as parcelas de (1.2) estão em P_k.

Para $i = k$ e $a < c$ temos que

$$v_k(\varphi_{kja}(x)t_k^{a-c}z_{kj}) = v_k(\varphi_{kja}(x)) + v_k(t_i^{a-c}) + v_k(z_{kj}) \geq a - c + e_k > -c + e_k > 0.$$

Para $i = k$ e $a > c$ temos que

$$v_k(\varphi_{kja}(x)t_k^{a-c}z_{kj}) \geq e_k + a - c \geq a - c > 0$$

Combinando os casos acima, obtemos

$$\sum_{j=1}^{f_k} \varphi_{kji}(x)z_{kj} \in P_k.$$

Como múltiplos de x pertencem a P_k temos que $\varphi_{kjc}(x)(P_k) \in K$, portanto, no quociente F_{P_k} somente sobra o termo constante. Alem disso, nem todos $\varphi_{kjc}(x)(P_k) = 0$, pois x não divide todos os $\varphi_{kjc}(x)$. Assim temos uma combinação linear não trivial

$$\sum_{j=1}^{f_k} \varphi_{kjc}(x)(P_k).z_{kj}(P_k) = 0$$

sobre K, o que é uma contradição, pois, como $v_i(s_{ij} - z_{ij}) > 0$, então $s_{ij} - z_{ij} \in P_i$, isto implica que $s_{ij}(P_i) = z_{ij}(P_i)$ e, como $\{s_{i1}(P_i), \ldots, s_{if_i}(P_i)\}$ é uma base de F_{P_i} sobre K, consequentemente $\{z_{k1}(P_k), \ldots, z_{kf_k}(P_k)\}$ é uma base de F_{P_i} sobre K.

Concluímos então que os elementos $t^a z_{ij}$ com $1 \leq i \leq r$, $1 \leq j \leq f_i$ e $o \leq ia \leq e_i - 1$, são linearmente independentes sobre $K(x)$. E como o número de elementos dessa forma é igual a

$$\sum_{i+1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i} \deg(P_i),$$

a proposição segue. ✓

Corolário 1.2.2. *Em um corpo de funções algébricas F/K, todo elemento $x \in F \setminus \{0\}$ possui um número finito de zeros e polos.*

Demonstração. Se $x \in \widetilde{K}$ como $\widetilde{K} \cap P = \{0\}$, então x não possui zeros nem polos. Por outro, lado se x é um elemento transcendente sobre K então, pela proposição 1.2.1, o número de zeros de x é no máximo $[F : K(x)]$. Um argumento análogo a esse para x^{-1} implica que x^{-1} tem finitos zeros e, daí, x possui finitos polos. ✓

1.3 DIVISORES E ESPAÇO DE RIEMANN-ROCH

Nesta seção, vamos considerar F/K um corpo de funções algébricas, onde K é algebricamente fechado sobre K, isto é $\widetilde{K} = K$.

Definição 1.3.1. *O grupo dos divisores de F/K é definido como o grupo abeliano livre que é gerado pelos lugares de F/K e é denotado como $Div(F)$. Assim, um divisor $D \in Div(F)$ é uma soma formal*

$$D = \sum_{P \in \mathbb{P}_F} n_p P, \text{ onde } n_p \in \mathbb{Z} \text{ e quase todo } n_P = 0.$$

O suporte de D é definido como

$$supp(D) = \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

Dados dois divisores $D = \sum n_P P$ e $D' = \sum n'_P P$ definimos a soma como

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

E o elemento neutro de $Div(F)$ como

$$0 = \sum_{P \in \mathbb{P}_F} n_P P, \text{ onde } n_p = 0 \text{ para todo } P \in \mathbb{P}_F.$$

Definição 1.3.2. *Nas condições da definição acima:*

i) Sejam $Q \in \mathbb{P}_F$ e $D = \sum n_p P \in Div(F)$, definimos $v_Q(D) = n_Q$. Logo,

$$supp(D) = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\} \text{ e } D = \sum_{P \in supp(D)} v_P(D) P.$$

ii) Em $Div(F)$ definimos uma relação de ordem parcial como segue

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

Ainda se $D_1 \leq D_2$ e $D_1 \neq D_2$, escrevemos $D_1 < D_2$.

iii) O grau de um divisor D é definido como

$$\deg(D) = \sum_{P \in \mathbb{P}_F} v_P(D) \deg(P).$$

Logo, a aplicação $\deg : Div(F) \longrightarrow \mathbb{Z}$ é um homomorfismo de grupos.

Pelo Corolário 1.2.2, a seguinte definição tem sentido.

Definição 1.3.3. *Seja $x \in F \setminus \{0\}$. Sejam $\mathcal{Z}$ e $\mathcal{N}$ o conjunto de zeros e polos de x respectivamente. Então definimos*

i) $(x)_0 = \sum_{P \in \mathcal{Z}} v_P(x) P$, o divisor de zeros de x.

ii) $(x)_\infty = \sum_{P \in \mathcal{N}} -v_P(x) P$, o divisor de polos de x.

iii) $(x) = (x)_0 - (x)_\infty$, *o divisor principal de* x.

Notemos que, da definição 1.3.3, $(x) = \sum v_P(x)P$. Além disso, como K algebricamente fechado em F, pelo Corolário 1.1.2, temos que

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

Definição 1.3.4. *O conjunto de divisores* $Princ(F) = \{(x) \mid 0 \neq x \in F\}$ *é dito o grupo dos divisores principais de* F/K. *O grupo quociente* $Cl(F) = Div(F)/Princ(F)$ *é chamado grupo das classes de divisores de* F/K. *Dado* $D \in Div(F)$, *o elemento correspondente em* $Cl(F)$ *é denotado por* $[D]$

Definição 1.3.5. *Diremos que dois divisores* D *e* D' *são equivalentes e escrevemos* $D \sim D'$ *se* $[D] = [D']$, *isto é, se existe algum* $0 \neq x \in F$ *tal que* $D = D' + (x)$.

Definição 1.3.6. *Dado um divisor* $A \in Div(F)$, *definimos o espaço de Riemman-Roch associado a* A *por*

$$\mathcal{L}(A) = \{x \in F \mid (x) \geq -A\} \cup \{0\}.$$

Afirmação 1.3.1. *Seja* $A \in Div(F)$. *Então:*

i) $x \in \mathcal{L}(A) \Leftrightarrow v_p(x) \geq -v_p(A)$ *para todo* $P \in \mathbb{P}_F$

ii) $\mathcal{L}(A) \neq \{0\} \Leftrightarrow$ *existe* $A' \in Div(F)$ *tal que* $A' \sim A$ *e* $A' \geq 0$.

Demonstração. Claramente, o item (i) decorre das definições. Mostremos então o item (ii):

$$\begin{aligned}\mathcal{L}(A) \neq \{0\} &\Leftrightarrow \exists\, x \in F \setminus \{0\} \text{ tal que } (x) \geq -A \\ &\Leftrightarrow A' = A + (x) \text{ tal que } A' \sim A \text{ e } A' \geq 0 \\ &\Leftrightarrow \exists\, A' \in Div(F) \text{ tal que } A' \sim A \text{ e } A' \geq 0\end{aligned}$$

✓

Lema 1.3.1. *Seja* $A \in Div(F)$. *Então:*

i) $\mathcal{L}(A)$ *é um espaço vetorial sobre* K.

ii) Se A' *é um divisor equivalente a* A, *então* $\mathcal{L}(A') \cong \mathcal{L}(A)$.

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

iv) Se $A < 0$, *então* $\mathcal{L}(A) = \{0\}$.

Demonstração. i) Notemos que $0 \in \mathcal{L}(A)$, assim $\mathcal{L}(A) \neq \emptyset$. Sejam agora $x, y \in \mathcal{L}(A)$ e $a \in K$. Logo, temos que para cada $P \in \mathbb{P}_F$.

$$v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A) \quad \text{e}$$

$$v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(A).$$

Pela Afirmação 1.3.1, temos que $x+y$ e ax são elementos de $\mathcal{L}(A)$. Assim, $\mathcal{L}(A)$ é um espaço vetorial sobre K.

ii) Como $A \sim A'$, então existe $z \in F \setminus \{0\}$ tal que $A = A' + (x)$. Seja agora a aplicação

$$\begin{aligned} \varphi : \mathcal{L}(A) &\longrightarrow F \\ x &\longmapsto xz \end{aligned}$$

Claramente, φ é uma aplicação linear. Mostremos que $\varphi(\mathcal{L}(A)) \subseteq \mathcal{L}(A')$. De fato, se $x \in \mathcal{L}(A) \setminus \{0\}$, então $(x) \geq -A$. Assim, temos que $\varphi(x) = xz \neq 0$. Além disso,

$$(xz) = (x) + (z) = (x) + A - A' \geq -A + A - A' = -A'.$$

Portanto, $\varphi(x) = xz \in \mathcal{L}(A')$. Se $x = 0$, temos que $\varphi(x) = \varphi(0) = 0 \in \mathcal{L}(A')$. Analogamente, podemos verificar que a aplicação $\psi : \mathcal{L}(A') \longrightarrow F$ definida como $x \longmapsto xz^{-1}$ é uma transformação linear cuja imagem está contida em $\mathcal{L}(A)$. Mas ainda, ψ é a inversa de φ. Consequentemente, $\mathcal{L}(A') \cong \mathcal{L}(A)$.

iii) Sabemos que se $x \in K \setminus \{0\}$, então $(x) = 0$, portanto $K \in \mathcal{L}(0)$. Reciprocamente, temos que se $x \in \mathcal{L}(0) \setminus \{0\}$, então $(x) \geq 0$ isto implica que x não possui polos. Logo, pelo Corolário 1.1.2, temos que $x \in K$.

iv) Suponhamos que existe um elemento $x \in \mathcal{L}(A) \setminus \{0\}$. Então, $(x) \geq -A$. Isto implica que x não possui nenhum polo e pelo menos um zero, o que é uma contradição com o Corolário 1.1.2. ✓

Lema 1.3.2. *Sejam $A, B \in Div(F)$, tais que $A \leq B$. Então, $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ e*

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg(B) - \deg(A).$$

Demonstração. Seja $x \in \mathcal{L}(A) \setminus \{0\}$. Então, $v_P(x) \geq -v_P(A)$ para cada $P \in \mathbb{P}_F$. Mas, pela hipótese, como $B \geq A$, temos que $-v_P(A) \geq -v_P(B)$ para cada $P \in \mathbb{P}_F$. Assim, $v_P(x) \geq -v_P(B)$ e daí $x \in \mathcal{L}(B)$, isto mostra que $\mathcal{L}(A) \subseteq \mathcal{L}(B)$.

Agora, podemos assumir $B = A + P$ para algum lugar $P \in \mathbb{P}_F$. O caso geral segue deste por indução. Seja agora $t \in F$ tal que $v_P(t) = v_P(B) = v_P(A) + v_P(P) = v_P(A) + 1$. Para $x \in \mathcal{L}(A)$, temos que $v_P(x) \geq -v_P(B) = -v_P(t)$, consequentemente $v_P(xt) = v_P(x) + v_P(t) \geq 0$, assim $xt \in \mathcal{O}_P$. Logo, podemos definir a aplicação K-linear

$$\begin{aligned} \varphi : \mathcal{L}(B) &\longrightarrow F_P \\ x &\longmapsto (xt)P \end{aligned}$$

Agora notemos que:

$$\begin{aligned} x \in Ker(\varphi) &\Leftrightarrow xt \in P \Leftrightarrow v_P(xt) > 0 \\ &\Leftrightarrow v_P(x) + v_P(t) > 0 \\ &\Leftrightarrow v_P(x) > -v_P(A) - 1 \\ &\Leftrightarrow v_P(x) \geq -v_P(A) \end{aligned}$$

Além disso, para $Q \neq P$ e $x \in \mathcal{L}(B)$ implica que $v_Q(x) \geq -v_Q(B) = -v_Q(A)$. Portanto, $Ker(\varphi) = \mathcal{L}(A)$. Consequentemente, φ induz uma transformação linear injetiva e daí

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \dim(F_P) = \deg(P) = \deg(B) - \deg(A).$$

✓

Proposição 1.3.1. *Para cada divisor A de F/K, o espaço $\mathcal{L}(A)$ é um espaço de dimensão finita sobre K. Mais precisamente, se $A = A_+ - A_-$, onde A_+ e A_- são divisores divisores positivos, então* $\dim(\mathcal{L}(A)) \leq \deg(A_+) + 1$.

Demonstração. Pelo Lema 1.3.1 temos que $\mathcal{L}(0) = K$. Então segue que

$$\dim(\mathcal{L}(A_+)/\mathcal{L}(0)) = \dim(\mathcal{L}(A_+)) - dim(\mathcal{L}(0)) = \dim(\mathcal{L}(A_+)) - 1$$

$$\Rightarrow \dim(\mathcal{L}(A_+)) = \dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1.$$

Por outro lado, como $0 \leq A_+$, aplicando o Lema 1.3.2, temos que

$$\dim(\mathcal{L}(A_+)) \leq \deg(A_+) - \deg(0) + 1 = \deg(A_+) + 1,$$

o que conclui a prova pois como $A \leq A_+$, o Lema 1.3.2 implica que $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$. ✓

Definição 1.3.7. *Dado um divisor de F/K, o inteiro $\ell(A) = \dim(\mathcal{L}(A))$ é dito dimensão do divisor A.*

Teorema 1.3.1. *Todos os divisores principais possuem grau zero. Mais precisamente, se $x \in F \setminus K$, então* $\deg((x)_0) = \deg((x)_\infty) = [F : K(x)]$.

Demonstração. Definamos $n = [F : K(x)]$ e $B = (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i$, onde os P_i com $i = 1, \ldots, r$ são todos os polos de x. Logo, pela Proposição 1.2.1, temos que

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

Provemos agora a desigualdade recíproca.

Sejam $\{u_1, \ldots, u_n\}$ uma base de $F/K(x)$ e um divisor $C \geq 0$ tal que $(u_i) \geq -C$, para cada $i = 1, \ldots, n$. Mostremos que os elementos $x^i u_j$ com $0 \leq i \leq k$, $1 \leq j \leq n$ pertencem a $\mathcal{L}(kB + C)$ e são linearmente independentes sobre K para todo $k \geq 0$.

Com efeito, como $-i \geq -k$ temos que

$$(x^i) = i(x) = i(x)_0 - i(x)_\infty \geq -i(x)_\infty \geq -kB.$$

Por outro lado, $(u_j) \geq -C$ para cada $i = 1, \ldots, n$, então

$$(x^i u_j) = (x^i) + (u_j) \geq -kB - C \Rightarrow x^i u_j \in \mathcal{L}(kB + C).$$

Ainda, se $a_{ij} \in K$ tais que

$$\sum_{j=1}^{n} \sum_{i=1}^{k} a_{ij} x^i u_j = 0 \Longrightarrow \sum_{j=1}^{n} \left(\sum_{i=1}^{k} a_{ij} x^i \right) u_j = 0.$$

Logo, temos que $\sum_k^{i=1} a_{ij} x^i = 0$ para todo $j = 1, \ldots, n$. Mas, como x é um elemento transcendente sobre K, isto implica que $a_{ij} = 0$ para cada $1 = 1, \ldots, k$ e $j = 1, \ldots, n$. Assim, os elementos $x^i u_j$ são linearmente independentes sobre K.

Além disso, notemos que a quantidade deles é $n(k+1)$. Finalmente, pela Proposição 1.3.1, temos que

$$n(k+1) \leq \dim(kB + C) = \deg((KB + C)_+) + 1 = k \deg(B) + \deg(C) + 1$$

Isto implica que $k(\deg(B) - n) \geq n - \deg(C) - 1$ para todo $k \geq 0$. Como o lado direito desta última desigualdade não depende de k, podemos concluir que $\deg(B) \geq n$.

Lembrado que $(x)_0 = (x^{-1})_\infty$ concluímos que

$$\deg(x)_0 = (x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)].$$

✓

Corolário 1.3.1. *Seja A um divisor de F/K.*

i) Se $A' \in Div(F)$ é tal que $A' \sim A$, então $\ell(A) = \ell(A')$ e $\deg(A) = \deg(A')$.

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

iii) Se $\deg(A) = 0$, então são equivalentes:

a) A é um divisor principal.

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

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

Demonstração. *i*) O fato $\ell(A) = \ell(A')$ decorre diretamente do Lema 1.3.1.

Ainda, como $A \sim A'$ então $A = A' + (x)$. Logo, pelo Teorema 1.3.1, temos que

$$\deg(A) = \deg(A') + \deg((x)) = \deg(A').$$

ii) Suponhamos que $\ell(A) > 0$, logo, pela Afirmação 1.3.1, existe $A' \in Div(F)$ tal que $A' \sim A$ e $A' \geq 0$. Mas, pelo item (i), temos que $\deg(A) = \deg(A') \geq 0$, o que é uma contradição pois $\deg(A) < 0$.

iii) $a) \Rightarrow b)$ Se A é principal, então $A = (x)$. Ainda, como $(x^{-1}) = -(x)$, temos que $x^{-1} \in \mathcal{L}(A)$ e daí $\ell(A) \geq 1$.

$b) \Rightarrow c)$ Suponhamos que $\ell(A) \geq 1$. Logo, pela Afirmação 1.3.1 $A' \sim A$ para algum $A' \geq 0$. As condições $A' \geq 0$ e $\deg(A') = \deg(A) = 0$ implicam que $A' = 0$. Consequentemente, temos que $\ell(A) = \ell(A') = \ell(0) = 1$.

$c) \Rightarrow a)$ Suponhamos que $\ell(A) = 1$. Por hipótese, temos que $\deg(A) = 0$. Seja $z \in \mathcal{L}(A) \setminus \{0\}$, então $(z) + A \geq 0$. Ainda, como $\deg((z) + A) = 0$, temos que $(z) + A = 0$. Daí, $A = -(z) = (z^{-1})$ que é um divisor principal. ✓

Proposição 1.3.2. *Existe uma constante $\gamma \in \mathbb{Z}$ tal que para todos os divisores $A \in Div(F)$ temos que* $\deg(A) - \ell(A) \leq \gamma$.

Demonstração. Notemos que dados $A_1, A_2 \in Div(F)$ tais que $A_1 \leq A_2$ então, pelo Lema 1.3.2, temos que

$$\ell(A_2) - \ell(A_1) = \dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \leq \deg(A_2) - \deg(A_1)$$

$$\Rightarrow \deg(A_1) - \ell(A_1) \leq \deg(A_2) - \ell(A_2) \tag{1.3}$$

Fixemos um elemento $x \in F \setminus K$ e seja o divisor $B = (x)_\infty$. Analogamente à demonstração do Teorema 1.3.1, existe um divisor $C \geq 0$ dependendo de x tal que $\ell(kB + C) \geq (k+1)\deg(B)$ para todo $k \geq 0$.

Além disso, novamente pelo Lema 1.3.2, temos que

$$\begin{aligned}\ell(kB + C) - \ell(kB) &= \dim(\mathcal{L}(kB + C)/\mathcal{L}(kB)) \\ &\leq \deg(kB + C) - \deg(kB) = \deg(C)\end{aligned}$$

$$\Rightarrow \ell(kB + C) \leq \ell(kB) + \deg(C) \tag{1.4}$$

Combinando (1.3) e (1.4) mais o fato que $\deg(B) = n = [F : K(x)]$ (pela demonstração do Teorema 1.3.1), temos que

$$\deg(kB) - \ell(kB) \leq \gamma \tag{1.5}$$

para todo $k \geq 0$ e para algum $\gamma \in \mathbb{Z}$, onde $\gamma = [F : K(x)] - \deg(C)$.

Afirmação 1.3.2. *Dado um divisor A, existem divisores A_1, D e um inteiro $k \geq 0$ tais que $A \leq A_1$, $A_1 \sim D$ e $D \leq kB$.*

Prova da Afirmação: Escolhamos um divisor $A_1 \geq A$ tal que $A_1 \geq 0$. Logo, para um k suficientemente grande, temos que

$$\begin{aligned} \ell(kB) - \ell(kB - A_1) &= dim(\mathcal{L}(kB)/\mathcal{L}(kB - A_1)) \\ &\leq \deg(kB) - (\deg(kB - A_1)) \\ \Rightarrow (kB - A_1) &\geq \ell(kB) - \deg(A_1) \\ &\geq \deg(kB) - \gamma - \deg(A_1) \qquad \text{por (1.4)} \\ &> 0 \end{aligned}$$

Logo, existe um elemento $z \in \mathcal{L}(kB - A_1)$. Definindo $D = A_1 - (z)$, obtemos que $A_1 \sim D$ e $D \leq A_1 - (A_1 - kB) = kB$, como desejamos.

Falta mostrar que a desigualdade (1.5) vale mesmo substituindo kB por $A \in Div(F)$. Mas, pela Afirmação 1.3.2, podemos concluir esse resultado pois

$$\begin{aligned} \deg(A) - \ell(A) &\leq \deg(A_1) - \ell(A_1) \\ &= \deg(D) - \ell(D) \quad \text{pelo Corolário 1.3.1} \\ &\leq \deg(kB) - \ell(kB) \\ &\leq \gamma. \end{aligned}$$

✓

Definição 1.3.8. *O gênero g de F/K é definido por*

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

Notemos que o gênero de F/K é um inteiro não negativo. De fato,

$$g \geq \deg(0) - \ell(0) + 1 = 0$$

Teorema 1.3.2 (Teorema de Riemann)**.** *Seja F/K um corpo de funções de gênero g. Então:*

i) Para todos os divisores $A \in Div(F)$, temos $\ell(A) \geq \deg(A) + 1 - g$

ii) Existe um inteiro c, dependendo somente do corpo de funções algébricas F/K, tal que $\ell(A) = \deg(A) + 1 - g$ sempre que $\deg(A) \geq c$.

Demonstração. *i*) Esse item segue da definição do gênero g.

ii) Tomemos um divisor A_0 com $g = \deg(A_0) - \ell(A_0) + 1$ e definamos $c = \deg(A_0) + g$. Se $\deg(A) \geq c$, então

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

Logo, existe um elemento $z \in \mathcal{L}(A - A_0)$. Definamos assim o divisor $A' = A + (z) \geq A_0$. Finalmente, temos que

$$\begin{aligned} \deg(A) - \ell(A) &= \deg(A') - \ell(A') \qquad \text{Pelo Corolário 1.3.1} \\ &\geq \deg(A_0) - \ell(A_0) \qquad \text{Pelo Lema 1.3.2} \\ &= g - 1 \end{aligned}$$

Isto implica que $\ell(A) \leq \deg(A) - g + 1$ e combinando com a desigualdade do item (i) obtemos a igualdade. ✓

Observação 1.3.1. *Notemos que, do item* (ii)*, dado um divisor* A*, podemos sempre encontrar um inteiro* c *dependendo unicamente do corpo de funções* F/K *e um divisor* A' *tal que* $A \leq A'$*,* $\deg(A') \geq c$ *e* $\ell(A') = \deg(A') + 1 - g$

1.4 CORPO DE FUNÇÕES RACIONAIS

Nesta seção, vamos apresentar um caso simples que é o corpo de funções racionais, como exemplo dos resultados apresentados até aqui.

Um corpo de funções algébricas F/K é dito corpo de funções racionais se $F = K(x)$ para algum $x \in F$ que seja transcendente sobre K. Lembremos que

$$K(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], g(x) \neq 0 \right\}.$$

Definamos o conjunto

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}, \tag{1.6}$$

onde $p(x) \in K[X]$ é um polinômio mônico irredutível. Claramente, da definição de $\mathcal{O}_{p(x)}$ e $K(x)$, decorre que $K \subsetneq \mathcal{O}_{p(x)} \subsetneq K(x)$. Além disso, notemos que se $z \in K(x) \setminus \mathcal{O}_{p(x)}$, então, sem perda de generalidade, podemos supor que $z = \frac{f(x)}{g(x)}$ onde $f(x)$ e $g(x)$ não possuem fatores comuns e $p(x) \mid g(x)$. Assim, temos que $g(x) = p(x)q(x)$ para algum

$q(x) \in K[x]$ e $p(x) \nmid f(x)$, logo $z^{-1} = \frac{g(x)}{f(x)} \in \mathcal{O}_{p(x)}$. Podemos então concluir que $\mathcal{O}_{p(x)}$ é um anel de valorização do corpo de funções racionais $K(x)/K$.

Agora, pela demonstração da Proposição 1.1.1, sabemos que $P_{p(x)} = \mathcal{O}_{p(x)} \setminus \mathcal{O}^*_{p(x)}$ é o ideal maximal de $\mathcal{O}_{p(x)}$, ou seja, um lugar do corpo de funções racionais $K(x)/K$. Notemos que se $z \in \mathcal{O}^*_{p(x)}$ então existem $f(x), g(x) \in K[x]$ tais que

$$zz^{-1} = \frac{f(x)}{g(x)}\frac{g(x)}{f(x)}, \quad p(x) \nmid f(x) \quad \text{e} \quad p(x) \nmid g(x).$$

Assim temos que

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\}. \tag{1.7}$$

Além disso, sendo $p(x) \in K[x]$ um polinômio mônico irredutível, podemos ver que $p(x) \in P_{p(x)}$, portanto $p(x)\mathcal{O}_{p(x)} \subseteq P_{p(x)}$. Por outro lado, se $z \in P_{p(x)}$, então existem $f(x), g(x) \in K[x]$ tais que

$$z = \frac{f(x)}{g(x)}, \quad p(x) \mid f(x) \quad \text{e} \quad p(x) \nmid g(x).$$

Como $p(x) \mid f(x)$, temos que existe $q(x) \in K[x]$ tal que $f(x) = q(x)p(x)$. Logo,

$$z = \frac{q(x)}{g(x)}p(x), \quad p(x) \nmid g(x)$$

e, daí, $z \in p(x)\mathcal{O}_{p(x)}$. Isto implica que $p(x)\mathcal{O}_{p(x)} = P_{p(x)}$, ou seja, $p(x)$ é um elemento primo de $P_{p(x)}$.

Finalmente, pelo Teorema 1.1.1, temos que cada $z \in K(x) \setminus \{0\}$ possui uma única representação na forma $z = p(x)^n h(x)$ para algum $n \in \mathbb{Z}$ e $h(x) \in \mathcal{O}^*_{p(x)}$.

Em particular, quando $p(x)$ é um polinômio linear, ou seja, $p(x) = x - \alpha$ com $\alpha \in K$, utilizaremos a notação $P_\alpha; = P_{x-\alpha}$.

Analogamente, podemos provar que

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) \leq \deg g(x) \right\} \tag{1.8}$$

é outro anel de valorização do corpo de funções racionais $K(x)/K$, que define o lugar

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) < \deg g(x) \right\} \tag{1.9}$$

que tem como elemento primo $t = 1/x$. Chamaremos P_∞ de lugar infinito de $K(x)$.

Em seguida, apresentamos alguns resultados sobre o corpo de funções racional.

Proposição 1.4.1. *Seja $K(x)/K$ o corpo de função racional.*

i) Se $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ é o lugar definido em (1.7), onde $p(x) \in K[x]$ é um polinômio mônico irredutível. Então, $p(x)$ é um elemento primo de P, e a valorização correspondente v_P pode ser descrito, como segue: se $z \in K(x) \setminus \{0\}$ é escrito na forma $z = p(x)^n(f(x)/g(x))$ com $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P = n$. O corpo das classes residuais $K(x)_P = \mathcal{O}_P/P$ é isomorfo a $K[x]/\langle p(x)\rangle$. Consequentemente, $\deg P = \deg p(x)$

ii) No caso que $p(x) = x - \alpha$ com $\alpha \in K$, o grau de $P = P_\alpha$ é 1, e o mapa das classe residuais é dado por

$$z(P) = z(\alpha) \ \text{ para } \ z \in K(x),$$

onde $z(\alpha)$ é definido como segue: escreva $z = f(x)/g(x)$ com polinômios primos relativos em $K[x]$, então

$$z(\alpha) : \begin{cases} f(\alpha)/g(\alpha), & \text{se } g(\alpha) \neq 0 \\ \infty, & \text{se } g(\alpha) = 0 \end{cases}$$

iii) Se $P = P_\infty$ é o lugar infinito de $K(x)/K$ definido em (1.9)*, então* $\deg P_\infty = 1$. *O elemento primo para P_∞ é $t = 1/x$. A correspondente valorização discreta v_∞ é dada por*

$$v_\infty\left(\frac{f(x)}{g(x)}\right) = \deg f(x) - \deg g(x),$$

onde $f(x), g(x) \in K[x]$. O mapa das classes residuais correspondente a P_∞ é determinado por $z(P_\infty) = z(\infty)$ para $z \in K(x)$, donde $z(\infty)$ define-se da forma usual: se

$$z = \frac{a_n x^n + \ldots + a_0}{b_m x^m + \ldots + b_0} \ \text{ com } \ a_n, b_m \neq 0,$$

então

$$z(\infty) : \begin{cases} a_n/b_m, & \text{se } n = m, \\ 0, & \text{se } n < m, \\ \infty, & \text{se } n > m. \end{cases}$$

iv) K é o corpo completo de constantes de $K(x)/K$.

Demonstração. A maior parte da prova foi no início da seção, e outras decorrem diretamente da definição 1.1.5, portanto faremos somente os aspectos mais representativos e ainda não feitos da proposição.

i) Consideremos

$$\varphi : K[x] \longrightarrow K(x)_P$$
$$f(x) \longmapsto f(x)(P)$$

Facilmente prova-se que φ é um homomorfismo de anéis. Além disso, $Ker\varphi = \langle p(x)\rangle = P$.

Provemos agora que φ é sobrejetivo. De fato, seja $z \in \mathcal{O}_{p(x)}$, então existem $u(x), v(x) \in K[x]$ tais que $z = f(x)/g(x)$ e $p(x) \nmid v(x)$. Mas ainda, como $p(x)$ é irredutível, $m.d.c.(p(x), v(x)) = 1$, assim $a(x)p(x) + b(x)v(x) = 1$, onde $a(x), b(x) \in K[x]$. Então

$$z = 1.z = a(x)p(x) + b(x)v(x)\frac{u(x)}{v(x)} \Longrightarrow z = \frac{a(x)}{v(x)}p(x) + b(x)u(x).$$

Consequentemente, temos que $\varphi(b(x)u(x)) = (b(x)u(x))P = z(P)$. Finalmente, pelo teorema dos isomorfismos, $K(x)_P$ é isomorfo a $K[x]/\langle p(x)\rangle$.

ii) Pelo item (i) decorre que $\deg P = 1$.

$(*)$ Seja $P = P_\alpha$ com $\alpha \in K$. Se $f(x) \in K[x]$ então $(x - \alpha) \mid (f(x) - f(\alpha))$. Como $p(x) = x - \alpha$, temos que existe $q(x) \in K[x]$ tal que $f(x) - f(\alpha) = p(x)q(x)$ e daí

$$f(x)P = (p(x)q(x))\,(P) + f(\alpha)(P).$$

Lembrando que $\deg P = 1$, ou seja, $K = K(x)_P = \mathcal{O}_P/P$, temos que $f(x)P = f(\alpha)$.

$(**)$ Seja $z \in \mathcal{O}_P$, então existem $f(x), g(x) \in K[x]$ tais que $z = f(x)/g(x)$ e $(x - \alpha) \nmid g(x)$. Assim, de forma análoga a $(*)$ temos que $g(x)P = g(\alpha) \neq 0$.

Finalmente de $(*)$ e $(**)$ obtemos

$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha).$$

Logo, se $z = f(x)/g(x)$ com $f(x), g(x) \in K[x]$ e $m.d.c\,(f(x), g(x)) = 1$ temos que

$$z(P) = z(\alpha) : \begin{cases} f(\alpha)/g(\alpha), & \text{se } g(\alpha) \neq 0 \\ \infty, & \text{se } g(\alpha) = 0 \end{cases}$$

iii) Provemos que $1/x$ é um elemento primo de $P_\infty = P$. Claramente, $1/x \in P$ onde, $(1/x) \in \mathcal{O}_\infty \subseteq P$. Reciprocamente, considere $z = f(x)/g(x) \in P$, isto implica que $\deg f < \deg g$. Como $x \neq 0$ então

$$z = \frac{1}{x}\frac{xf(x)}{g(x)}$$

pois $\deg(xf(x)) \leq \deg g(x)$, assim $(xf(x))/g(x) \in \mathcal{O}_\infty$. Portanto, $z \in (1/x)\mathcal{O}_\infty$, onde $P = (1/x)\mathcal{O}_\infty$.

iv) Para provar que K é o corpo de constantes de $K(x)/K$, somente precisamos mostrar que $\widetilde{K} \subseteq K$. Escolhemos então um lugar P_α de grau um com $\alpha \in K$. Agora, sabemos que $\widetilde{K} \subseteq K(x)_P$. Mas ainda $\deg P = 1 = [K(x)_P : K]$, isto implica que $K(x)_P = K$, logo $\widetilde{K} \subseteq K$ ✓

Teorema 1.4.1. *Não existem lugares do corpo de funções racionais $K(x)/K$ além dos lugares $P_{p(x)}$ e P_∞ definidos em* (1.7) *e* (1.9).

Demonstração. Seja P um lugar de $K(x)/K$. Então:

Caso 1 : Suponha que $x \in \mathcal{O}_P$. Então $K[x] \in \mathcal{O}_P$. Definamos o conjunto $I = K[x] \cap P$. Claramente, I é um ideal primo de $K[x]$. Assim, o mapa das classes residuais induz um mergulho $K[x]/I \hookrightarrow K(x)_P$ e, pela Proposição 1.1.2, temos que $I \neq \{0\}$. Segue-se que há um (unicamente determinado) polinômio mônico irredutível $p(x) \in K[x]$ tal que $I = K[x] \cap P = p(x)K[x]$.

Notemos que cada $g(x) \in K[x]$ com $p(x) \nmid g(x)$ não pertence a I. Assim, novamente pelo Corolário 1.1.1, como $g(x) \notin P$, então $g(x)^{-1} = 1/g(x) \in \mathcal{O}_P$. Portanto

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \right\} \subseteq \mathcal{O}_P.$$

Mas, pelo Teorema 1.1.2, sabemos que um anel de valorização é um subanel maximal de $K(x)$, logo $\mathcal{O}_{p(x)} = \mathcal{O}_P$.

Caso 2 : Agora, se $x \notin \mathcal{O}_\mathfrak{p}$, então $x^{-1} \in \mathcal{O}_P$, assim $K[x]^{-1} \subseteq \mathcal{O}_P$. Analogamente ao caso 1, temos que $x^{-1} \in P \cap K[x^{-1}]$, $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$ e

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} \mid f(x^{-1}), g((x^{-1})) \in K^{x^{-1}}, x^{-1} \nmid g(x^{-1}) \right\} \\
&= \left\{ \frac{a_0 + a_1 x^{-1} + \ldots + a_n x^{-n}}{b_0 + b_1 x^{-1} + \ldots + b_m x^{-m}}, \ \ b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0 x^{m+n} + \ldots + a_n x^m}{b_0 x^{m+n} + \ldots + b_m x^n}, \ \ b_0 \neq 0 \right\} \\
&= \left\{ \frac{u(x)}{v(x)} \mid u(x), v(x) \in K[x], \ \ \deg u(x) \leq \deg v(x) \right\} = \mathcal{O}_\infty
\end{aligned}$$

Portanto $\mathcal{O}_P = \mathcal{O}_\infty$ ✓

Para finalizar esta seção exemplo, mostremos que o corpo de funções racionais $K(x)/K$ tem gênero $g = 0$. Seja P_∞ o lugar infinito definido em (1.9). Consideremos $r \geq 0$ um elemento do espaço $\mathcal{L}(rP_\infty)$. Assim, temos que $1, x, \ldots, x^r \in \mathcal{L}(rP_\infty)$. Ainda, como x é transcendente sobre K, então os elementos $1, x, \ldots, x^r$ são linearmente independentes sobre K, donde $r + 1 \leq \ell(rP_\infty)$.

Além disso, pela Proposição 1.4.1 item (iii), sabemos que $\deg P_\infty = 1$. Consequentemente, rP_∞ satisfaz a hipótese (ii) do Teorema de Riemann 1.3.2. Então, para um r suficientemente grande temos que

$$r + 1 \leq \ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g.$$

Assim, $g \leq 0$, mas sabemos que $g \geq 0$ e daí concluímos que $g = 0$.

1.5 O TEOREMA DE RIEMANN-ROCH

Definição 1.5.1. *Para $A \in Div(F)$, o inteiro $i(A) = \ell(A) - \deg(A) + g - 1$ é chamado o índice de especialidade de A.*

Note que, pelo Teorema de Riemann 1.3.2, $i(A) \geq 0$ e, pela Observação 1.3.1, $i(A) = 0$, se $\deg(A)$ for suficientemente grande.

Definição 1.5.2. *Um adele de um corpo de funções algébricas é uma função*

$$\begin{aligned} \alpha : \mathbb{P}_F &\longrightarrow F \\ P &\longmapsto \alpha(P) = \alpha_P \end{aligned}$$

tal que $\alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$. Notemos que também podemos considerar um adele como um elemento do produto direto $\prod_{P \in \mathbb{P}_F} F$, definimos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou simplesmente $\alpha = (\alpha_P)$.

O conjunto $\mathcal{A}_F = \{\alpha \mid \alpha$ é um adele de $F/K\}$ é chamado o espaço de adeles de F/K.

Definição 1.5.3. *Dado $x \in F$, definimos o adele principal de x como*

$$\begin{aligned} \alpha_x : \mathbb{P}_F &\longrightarrow F \\ P &\longmapsto x \end{aligned}$$

Notemos que α_x é um adele pelo Corolário 1.2.2.

Notemos que $\mathcal{A}_F$ com as operações de adição e multiplicação por escalar usuais é um espaço vetorial sobre K. Mais ainda, por meio do adele principal, obtemos um mergulho de F em $\mathcal{A}_F$ como segue

$$\begin{aligned} \varphi : F &\longrightarrow \mathcal{A}_F \\ x &\longmapsto \alpha_x \end{aligned}$$

Além disso, as valorizações discretas v_P de F/K podem-se estender de forma natural para $\mathcal{A}_F$ definindo $v_P(\alpha) := v_P(\alpha_P)$, onde claramente α_P é a componente P do adele α. E, por definição, temos que $v_P(\alpha) \geq 0$ para quase todo $P \in \mathbb{P}_F$.

Definição 1.5.4. *Nas condições acima, definimos o conjunto*

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

que é um subespaço vetorial de $\mathcal{A}_F$.

Lema 1.5.1. *Sejam $A_1, A_2 \in Div(F)$ tais que $A_1 \leq A_2$. Então*

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

Demonstração. A prova pode ser encontrada em [15]. ✓

Lema 1.5.2. *Se B é um divisor com $\ell(B) = \deg(B)+1-g$, então $\mathcal{A}_F = \mathcal{A}_F(B)+F$.*

Demonstração. É suficiente provar que $\mathcal{A}_F \subseteq \mathcal{A}_F(B)+F$. Observemos primeiro que para um divisor $B_1 \geq B$, pelo Lema 1.3.2, temos que

$$\ell(B_1)-\ell(B) = \dim(\mathcal{L}(B_1)/\mathcal{L}(B)) \leq \deg(B_1)-\deg(B)$$
$$\Rightarrow \ell(B_1) \leq \deg(B_1)+\ell(B)-\deg(B) = \deg(B_1)+1-g.$$

Mais ainda, pelo Teorema de Riemann, sabemos que $\ell(B_1) \geq \deg(B_1)+1-g$. Assim temos que cada $B_1 \geq B$ cumpre que $\ell(B_1) = \deg(B_1)+1-g$.

Seja $\alpha \in \mathcal{A}_F$. Se $\alpha \in \mathcal{A}_F(B)$, então não há nada para fazer, pois, neste caso, $\alpha \in \mathcal{A}_F(B)+F$. Caso contrário, definamos o divisor

$$B_1 = \sum_{v_P(\alpha_P) \geq -v_P(B)} v_P(B)P + \sum_{v_P(\alpha_P) < -v_P(B)} -v_P(\alpha_P)P.$$

Como B é um divisor de F/K, sabemos que $v_P(B) = 0$ para quase todo P. Assim da primeira parcela da soma anterior temos que $v_P(\alpha_P) \geq 0$ para quase todo P, isto implica que $v_P(B) \neq 0$ somente para um número finito de lugares P. Ainda, da segunda parcela, temos que $v_P(\alpha_P) < 0$, o que ocorre para um numero finito de lugares P pela definição de α. Se $v_P(B) \neq 0$, temos que $v_P(\alpha_P) < -v_P(B) \neq 0$, o que acontece somente para um número finito de lugares P. Logo, na segunda parcela, também temos um número finito de lugares tais que $v_P(\alpha_P) \neq 0$. Com isto, provamos que o divisor B_1 esta bem definido.

Além disso temos que

$$v_P(B_1) = \begin{cases} v_P(B), & \text{se} \quad v_P(\alpha_P) \geq -v_P(B) \\ -v_P(\alpha_P), & \text{se} \quad v_P(\alpha_P) < -v_P(B). \end{cases}$$

O que implica que $B_1 \geq B$. Logo, pelo Lema 1.5.1, a observação do início da prova e a hipótese, temos que

$$\begin{aligned} \dim((\mathcal{A}_F(B_1)+F)/(\mathcal{A}_F(B)+F) &= (\deg(B_1)-\ell(B_1)) - (\deg(B)-\ell(B)) \\ &= (g-1)-(g-1) = 0 \end{aligned}$$

Isto implica que $\mathcal{A}_F(B_1)+F = \mathcal{A}_F(B)+F$ e como, $\alpha \in \mathcal{A}_F(B_1)$, então $\alpha \in \mathcal{A}_F(B)+F$ e portanto

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

✓

Teorema 1.5.1. *Para cada divisor $A \in Div(F)$, temos que*

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

Demonstração. Seja $A \in Div(F)$. Pela observação do Teorema de Riemann 1.3.1, existe um divisor $A_1 \geq A$ tal que $\ell(A_1) = \deg(A_1) + 1 - g$. Logo, pelo Lema 1.5.2, decorre que $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$, e, do Lema 1.5.1, temos que

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

✓

Corolário 1.5.1. $g = \dim(\mathcal{A}_F/\mathcal{A}_F(0) + F)$.

Demonstração. Decorre diretamente do teorema anterior 1.5.1 e da definição 1.5.1. ✓

Definição 1.5.5. *Um diferencial de Weil do corpo de funções F/K é uma transformação K-linear $w : \mathcal{A}_F \to K$ tal que se anula em $\mathcal{A}_F(A) + F$ para algum divisor $A \in Div(F)$. Definimos o conjunto dos diferenciais de Weil como*

$$\Omega_F = \{w \mid w \text{ é um diferecial de Weil de } F/K\}.$$

Ainda, para cada $A \in Div(F)$, definimos

$$\Omega_F(A) = \{w \in \Omega_F \mid w \text{ se anula em } \mathcal{A}_F(A) + F\}.$$

Além disso, notemos que podemos considerar Ω_F como um espaço vetorial sobre K e $\Omega_F(A)$ um subespaço vetorial de Ω_F.

Lema 1.5.3. *Se $A \in Div(F)$, então* $\dim(\Omega_F(A)) = i(A)$.

Demonstração. Seja $(\mathcal{A}_F/\mathcal{A}_F(A) + F)^* = V^*$ o espaço dual de $\mathcal{A}_F/\mathcal{A}_F(A) + F = V$.

Consideremos a aplicação

$$\varphi : \begin{array}{ccc} \Omega_F(A) & \to & V^* \\ w & \mapsto & \varphi(w) \end{array}, \text{ onde } \varphi(w) : \begin{array}{ccc} V & \to & K \\ \overline{\alpha} & \mapsto & w(\alpha) \end{array}.$$

Mostremos que $\varphi(w)$ e φ estão bem definidas. De fato, se $\overline{\alpha} = \overline{\beta}$, então $\alpha - \beta \in \mathcal{A}_F(A) + F$, donde $w(\alpha - \beta) = 0$ e assim

$$\varphi(w)(\overline{\alpha}) = w(\alpha) = w(\beta) = \varphi(w)(\overline{\beta}),$$

portanto $\varphi(W)$ esta bem definida.

Por outro lado, se $w_1 = w_2$, então $w_1(\alpha) = w_2(\alpha)$, para todo $\mathcal{A}_F$, assim

$$\varphi(w_1)(\overline{\alpha}) = w_1(\alpha) = w_2(\alpha) = \varphi(w_2)(\overline{\alpha}),$$

para cada $\overline{\alpha} \in V$. Consequentemente, $\varphi(w_1) = \varphi(w_2)$, ou seja, φ esta bem definida.

Além disso, notemos que φ e $\varphi(w)$ são lineares pela linearidade de w.

Agora, mostremos que φ é bijetiva. Com efeito, suponhamos que $w_1, w_2 \in \Omega_F(A)$ são tais que $\varphi(w_1) = \varphi(w_2)$. Assim, para cada $\alpha \in \mathcal{A}_F$, $\overline{\alpha} \in V$ temos que

$$w_1(\alpha) = \varphi(w_1)(\overline{\alpha}) = \varphi(w_2)(\overline{\alpha}) = w_2(\alpha).$$

Portanto, $w_1 = w_2$ e φ é injetiva.

Para ver que φ é sobrejetora, dado $g \in V^*$, definimos

$$\begin{array}{rccc} w: & \mathcal{A}_F & \to & K \\ & \alpha & \mapsto & g(\overline{\alpha}). \end{array}$$

Logo, se $\alpha = \beta \in \mathcal{A}_F$, então $\overline{\alpha} = \overline{\beta} \in V$, portanto $w(\alpha) = g(\overline{\alpha}) = g(\overline{\beta}) = w(\beta)$ e daí w esta bem definida, mas ainda w é linear pois g é linear.

Vejamos que $w \in \Omega_F(A)$. De fato, se $\alpha = \alpha_A + f \in \mathcal{A}_F(A) + F$, onde $\alpha_A \in \mathcal{A}_F(A)$ e $f \in F$. Então, $w(\alpha) = g(\overline{\alpha}) = g(\overline{0}) = 0$. Finalmente temos que $\varphi(w)(\overline{\alpha}) = w(\alpha) = g(\overline{\alpha})$, para cada $\overline{\alpha} \in V$, ou seja, $\varphi(w) = g$ e, daí, φ é sobrejetiva.

Em conclusão, mostramos que V^* é isomorfa a $\Omega_F(A)$. Assim pelo Teorema 1.5.1, concluímos que

$$i(A) = \dim(\mathcal{A}/(\mathcal{A}_F(A) + F)) = \dim(V) = \dim(V^*) = \dim(\Omega_F(A)).$$

✓

Observação 1.5.1. *Se escolhemos um divisor A tal que $\deg(A) \leq -2$. Então*

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

Isto implica que $\Omega_F(A) \neq \{0\}$. E, como $\Omega_F(A) \subseteq \Omega_F$, temos que $\Omega_F(A) \neq \{0\}$.

Definição 1.5.6. *Para $x \in F$ e $w \in \Omega_F$, definimos*

$$\begin{array}{rccc} xw: & \mathcal{A}_F & \to & K \\ & \alpha & \mapsto & w(x\alpha) \end{array}$$

Observação 1.5.2. *Nas condições da definição acima, temos que:*

i) $xw \in \Omega_F(A)$. *De fato, sabemos que* w *se anula em* $\mathcal{A}_F(A) + F$. *Seja* $\alpha = \alpha_{Ax} + f$, *onde* $\alpha_{Ax} \in \mathcal{A}_F(A + (x))$ *e* $f \in F$. *Notemos que*

$$\begin{aligned} v_P(x\alpha_{Ax}) &= v_P(x) + v_P(\alpha_{Ax}) \\ &\geq v_P(x) - v_P(A + (x)) \\ &= v_P(x) - v_P(A) - v_P(x)) \\ &= -v_P(A). \end{aligned}$$

Isto implica que $x\alpha_{Ax} \in \mathcal{A}_F(A)$. *Além disso, claramente* $xf \in F$, *logo*

$$x\alpha = x(\alpha_{Ax} + f) = x\alpha_{Ax} + xf \Rightarrow x\alpha \in \mathcal{A}_F(A) + F.$$

Portanto, temos que $xw(\alpha) = w(x\alpha) = 0$, *pois* $w \in \mathcal{A}_F(A) + F$. *Consequentemente,* xw *se anula em* $\mathcal{A}_F(A + (x)) + F$ *e, portanto,* $xw \in \Omega_F(A)$.

ii) $\Omega_F(A)$ *pode ser considerado um espaço vetorial sobre* F, *definindo o produto por escalar como na definição acima.*

Proposição 1.5.1. $\Omega_F(A)$ *é um espaço vetorial de dimensão 1 sobre* F.

Demonstração. Como $\Omega_F(A) \neq \{0\}$, seja $0 \neq w_1 \in \Omega_F(A)$. Basta provar que para todo elemento $w_2 \in \Omega_F(A)$ existe $z \in F$ tal que $w_2 = zw_1$. Notemos que se $w_2 = 0$, tomamos $z = 0$. Suponhamos então o caso onde $w_2 \neq 0$. Pela definição do diferencial de Weil, existem $A_1, A_2 \in Div(F)$ tais que $w_1 \in \Omega_F(A_1)$ e $w_2 \in \Omega_F(A_2)$.

Para cada $B \in Div(F)$, consideremos a transformações lineares injetivas

$$\begin{array}{rccc} \varphi_i : & \mathcal{L}(A_i + B) & \to & \Omega_F(-B) \\ & x & \mapsto & xw_i \end{array}, \text{ para } i = 1, 2.$$

Provemos agora que para a escolha de um divisor apropriado B, teremos que

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

De fato, pelo teorema de Riemann 1.3.1, podemos escolher um divisor $B > 0$ de grau suficientemente grande tal que

$$\ell(A_i + B) = \deg(A_i + B) + 1 - g,$$

Ainda pelo lema 1.5.3, a definição 1.5.1 e o lema 1.3.1 temos que

$$\dim(\Omega_F(-B)) = i(-B) = \ell(-B) - \deg(-B) + g - 1 = \deg(B) + g - 1.$$

Definamos $U_i = \varphi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B)$ (claramente os U_i são subespaços vetorial de $\Omega_F(-B)$). Consequentemente

$$\begin{aligned}\dim(U_1)+\dim(U_2)-\dim(\Omega_F(-B)) &= \sum_{i=1}^{2}\dim(\mathcal{L}(A_i+B))-\deg(B)-g+1\\ &= \sum_{i=1}^{2}\deg(A_i+B)-\deg(B)-3g+3\\ &= \deg(B)+(\deg(A_1)+\deg(A_2)+3(1-g)\end{aligned}$$

Como o termo $\deg(A_1)+\deg(A_2)+3(1-g)$ independe de B, temos que

$$\dim(U_1)+\dim(U_2)-\dim(\Omega_F(-B))>0$$

se $\deg(B)$ for suficientemente grande. Ainda, temos

$$\begin{aligned}\dim(U_1\cap U_2) &= \dim(U_1)+\dim(U_2)-\dim(U_1+U_2)\\ &\geq \dim(U_1)+\dim(U_2)-\dim(\Omega_F(-B))>0.\end{aligned}$$

Onde a desigualdade decorre do fato que $\dim(U_1+U_2)\leq\dim(\Omega_F(-B))$. Portanto, como $\dim(U_1\cap U_2)>0$, concluímos que $U_1\cap U_2\neq\{0\}$.

Assim, podemos escolher $x_i\in\mathcal{L}(A_i+B)$, $i=1,2$ tais que $0\neq x_1w_1=x_2w_2$. Isto implica que

$$w_2=\left(x_2^{-1}x_1\right)w_1$$

como queríamos provar. ✓

Definição 1.5.7. *i) O divisor (w) do diferencial de Weil $w\neq 0$ é o único divisor de F/K satisfazendo:*

a) w se anula em $\mathcal{A}_F((w))+F$.

b) Se w se anula em $\mathcal{A}_F(A)+F$, então $A\leq(w)$.

ii) Para $w\in\Omega_F\setminus\{0\}$ e $P\in\mathbb{P}_F$, definimos $v_P(w)=v_P((w))$.

iii) Um divisor W é chamado divisor canônico de F/K se $W=(w)$, para algum $w\in\Omega_F$.

Observação 1.5.3. *Decorre diretamente das definições que*

$$\Omega_F(A)=\{w\in\Omega_F\mid w=0\ ou\ (w)\geq A\}.$$

Proposição 1.5.2. *Para $x\in F\setminus\{0\}$ e $w\in\Omega_F(A)\setminus\{0\}$, temos que $(xw)=(x)+(w)$.*

Demonstração. Como $w\in\Omega_F(A)\setminus\{0\}$, então existe $A\in Div(F)$ tal que w se anula em $\mathcal{A}_F(A)+F$, e, pela observação 1.5.2, temos que xw se anula em $\mathcal{A}_F(A+(x))+F$. Em particular, w se anula em $\mathcal{A}_F((w))+F$. Isto implica que xw se anula em $\mathcal{A}_F((w)+(x))+F$. Logo, da definição 1.5.7, temos que $(x)+(w)\leq(xw)$. Analogamente, podemos provar

que $(xw) + (x^{-1}) \leq (x^{-1}xw) = (w)$. Assim, das duas desigualdades anteriores podemos ver que

$$(w) + (x) \leq (xw) \leq -(x^{-1}) + (w) = (w) + (x),$$

o que conclui a prova. ✓

Teorema 1.5.2 (Teorema da Dualidade)**.** *Sejam A um divisor quaisquer e $W = (w)$ um divisor canônico, de F/K. Então, a aplicação*

$$\begin{array}{rccc} \kappa: & \mathcal{L}(W-A) & \to & \Omega_F(A) \\ & x & \mapsto & xw \end{array}$$

é um isomorfismo de espaços vetoriais sobre K. Em particular, $i(A) = \ell(W - A)$.

Demonstração. Notemos que se $x \in \mathcal{L}(W - A)$, então $(x) \geq -W + A$. Além disso pela proposição anterior temos que

$$(xw) = (x) + (w) \geq A - W + W = A.$$

Consequentemente, da observação 1.5.3, temos que $xw \in \Omega_F(A)$. Assim, podemos ver que κ é uma aplicação de $\mathcal{L}(W - A)$ em $\Omega_F(A)$.

Além disso, notemos que da observação 1.5.2 decorre que κ é uma transformação linear.

Por outro lado, notemos que se $xw = 0$, com $x \in \mathcal{L}(W - A)$ e $w \neq 0$, temos que $x = 0$, portanto κ é injetiva.

Finalmente, para provar que κ é sobrejetora, pela Proposição 1.5.1, sabemos que dado um diferencial de Weil $w_1 \in \Omega_F(A)$ podemos escrevê-lo como $w_1 = xw$ para algum $x \in F$. Mais ainda,

$$(x) + W = (x) + (w) = (xw) = (w_1) \geq A \Rightarrow (x) \geq A - W,$$

portanto $x \in \mathcal{L}(W - A)$. Assim, temos que $w_1 = \kappa(x) = (xw)$. Portanto, κ é um isomorfismo de espaços vetoriais.

Em particular, pelo Lema 1.5.3, temos que $\ell(W - A) = \dim(\Omega_F(A)) = i(A)$.

✓

Teorema 1.5.3 (Riemann-Roch)**.** *Seja W um divisor canônico de F/K. Então, para cada divisor $A \in Div(F)$,*

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

Demonstração. Da definição 1.5.1, sabemos que $i(A) = \ell(A) - \deg(A) + g - 1$ e, pelo Teorema da Dualidade 1.5.2, temos que $i(A) = \ell(W - A)$. ✓

Corolário 1.5.2. *Para um divisor canônico W, temos* $\deg(W) = 2g - 2$ *e* $\ell(W) = g$.

Demonstração. Para $A = 0$, pelo Teorema de Riemann-Roch e o Lema 1.3.1, temos que $1 = \ell(0) = \deg(0) + 1 - g + \ell(W - A)$, assim $\ell(W) = g$.

Agora sabendo que $g = \ell(W)$ e tomando $A = W$, pelo Teorema de Riemann-Roch, temos que

$$g = \ell(W) = \deg(W) + 1 - g + \ell(0)$$

consequentemente, $\deg(W) = 2g - 2$. ✓

Teorema 1.5.4. *Se A é um divisor de F/K de grau* $\deg(A) \geq 2g - 1$, *então* $\ell(A) = \deg(A) + 1 - g$.

Demonstração. Pelo Teorema de Riemann-Roch, sabemos que

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

onde W é un divisor canônico. Por hipótese, $\deg(A) \geq 2g - 1$ e, pelo Corolário, anterior temos que $\ell(W) = 2g - 2$. Portanto temos que

$$\deg(W) - \deg(A) \leq 2g - 2 - (2g - 1) = -1 < 0.$$

Logo, do Corolário 1.3.1, temos que $\ell(W - A) = 0$, e daí $\ell(A) = \deg(A) + 1 - g$. ✓

Teorema 1.5.5 (Da Aproximação Forte)**.** *Sejam $S \subsetneq \mathbb{P}_F$ e $P_1, \ldots, P_r \in S$. Sejam $x_1, \ldots, x_r \in F$ e $n_1, \ldots, n_r \in \mathbb{Z}$. Então, existe $x \in F$ tal que $v_{P_i}(x - x_i) = n_i$ para cada $i = 1, \ldots, r$ e $v_P(x) \geq 0$ para todo $P \in S \setminus \{P_1, \ldots, P_r\}$.*

Demonstração. Consideremos o adele $\alpha = (\alpha_P)_{p \in \mathbb{P}_F}$, com

$$\alpha : \mathbb{P}_F \longrightarrow F$$

$$P \longmapsto \alpha_P = \begin{cases} x_i, & \text{se } P = P_i,\ i = 1, \ldots, r \\ 0, & \text{caso contrário} \end{cases}$$

Escolhamos um lugar $Q \in \mathbb{P}_F \setminus S$ e definamos o divisor

$$A = mQ - \sum_{i=1}^{r} (n_1 + 1) P_i \quad \text{onde} \quad m \in \mathbb{N}.$$

Notemos que para m suficientemente grande

$$\deg(A) = m \deg(Q) - \sum_{i=1}^{r} (n_i + 1) \deg(P_i) \geq 2g - 1.$$

Assim, pelo Teorema 1.5.4, Teorema da Dualidade 1.5.2, Lema 1.5.3 e Teorema 1.5.1 temos que

$$0 = \ell(W - A) = \dim(\Omega_F(A)) = i(A) = \dim(\mathcal{A}_F / (\mathcal{A}_F(A) + F)).$$

Consequentemente, podemos concluir que $\mathcal{A}_F = \mathcal{A}_F(A) + F$. Esta igualdade implica que existe $z \in F$ tal que $z - \alpha \in \mathcal{A}_F(A)$. Portanto $v_P(z-\alpha) \geq -v_P(A)$ para cada $P \in \mathbb{P}_F$.

Notemos que, pela forma como foram definidos o adele α e o divisor A, obtemos que $v_{P_i}(z - x_i) \geq -v_{P_i}(A) = (n_i + 1)v_{P_i}(P_i) = (n_i + 1) > n_i$ para cada $i = 1, \ldots, r$. Analogamente, $v_P(z - 0) = v_P(z) \geq 0$ para cada $P \in S \setminus \{P_1, \ldots, P_r\}$ pois $Q \in \mathbb{P}_F \setminus S$.

Pelo Teorema da Aproximação Fraca 1.2.1, podemos escolher $y_1, \ldots, y_r \in F$ tais que $v_{P_i}(y_i) = n_i$. Analogamente ao processo feito acima, podemos obter $y \in F$ tal que $v_{P_i}(y - y_i) > n_i$, para cada $i = 1, \ldots, r$ e $v_P(y) \geq 0$ para cada $P \in S \setminus \{P_1, \ldots, P_r\}$

Finalmente, pela Desigualdade Triangular Estrita 1.1.2, temos que

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

Para concluir definamos $x = y + z$. Temos

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

Para cada $P \in S \setminus \{P_1, \ldots, P_r\}$ e $v_P(x) = v_P(y + z) \geq \min\{v_P(y), v_P(z)\} \geq 0$. ✓

Para finalizar essa seção, investigaremos os elementos em F que tem apenas um polo.

Proposição 1.5.3. *Seja $P \in \mathbb{P}_F$. Então para cada $n \geq 2g$ existe um elemento $x \in F$ com um divisor polo, a saber $(x)_\infty = nP$.*

Demonstração. Por hipótese $n \geq 2g$. Logo, $\deg((n-1)P) \geq 2g - 1$ e $\deg(nP) > 2g - 1$ então, pelo Teorema 1.5.4, temos que $\ell((n-1)P) = (n-1)\deg(P) + 1 - g$ e $\ell((n-1)P) = (n-1)\deg(P) + 1 - g$. Assim, pelo Lema 1.3.2, podemos afirmar que $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$, seja $x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P$.

Como $x \in \mathcal{L}(nP)$, temos que $v_P(x) \geq -n$ e $v_Q(x) \geq 0$ para cada $Q \in \mathbb{P}_F \setminus P$. Por outro lado, como $x \notin \mathcal{L}((n-1)P)$, isto implica que $v_P(x) < -(n-1)$, ou seja $v_P(x) \leq -n$. Assim, podemos concluir que $v_P(x) = -n < 0$ e $v_Q(x) \geq 0$ para cada $Q \in \mathbb{P}_F \setminus P$, consequentemente $(x)_\infty = (nP)$. ✓

Definição 1.5.8. *Seja $P \in \mathbb{P}_F$. O inteiro $n \geq 0$ é chamado número polo de P se existe um elemento $x \in F$ tal que $(x)_\infty = (nP)$. Caso contrário, n é dito lacuna de P.*

Claramente, da prova da proposição anterior, temos que n é um número polo de P se é somente se $\ell((n-1)P) < \ell(nP)$. Além disso, o conjunto dos números polo é um subsemigrupo do semigrupo aditivo $\mathbb{N}$. Para ver isto, notemos que se $(x_1)_\infty = n_1P$ e $(x_2)_\infty = n_2P$ então x_1x_2 tem como divisor polo $(x_1x_2) = (n_1 + n_2)P$. Trataremos mais profundamente este assunto no capítulo final.

Teorema 1.5.6 (Das Lacunas de Weierstrass)**.** *Suponha que F/K tem gênero $g > 0$ e P é um lugar de grau um. Então, existem exatamente g lacunas $i_1, \ldots, i_g$ de P. Além disso $i_1 = 1$ e $i_g \leq 2g - 1$.*

Demonstração. Pela Proposição 1.5.3, sabemos que cada lacuna é menor ou igual do que $2g - 1$, 0 é um número polo e

$$i \text{ é uma lacuna de } P \Leftrightarrow \mathcal{L}((i-1)P) = \mathcal{L}(iP).$$

Consideremos a seguinte sequência de espaços vetoriais:

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \ldots \subseteq \mathcal{L}((2g-1)P) \tag{1.10}$$

Claramente $\ell(0) = 1$. Por outro lado $\deg((2g-1)P) = (2g-1)\deg(P) = 2g-1$, já que, por hipótese, $\deg(P) = 1$. Assim, pelo Teorema 1.5.4, temos que

$$\ell((2g-1)P) = \deg((2g-1)P) + 1 - g.$$

Segue que $\ell((2g-1)P) = g$. Além disso, aplicando o Lema 1.3.2, para cada i teremos

$$\ell(iP) - \ell((i-1)P) = \dim(\mathcal{L}(iP)/\mathcal{L}(i-1)P)) \leq \deg(iP) - \deg((i-1)P) = 1$$

$$\Rightarrow \ell(iP) \leq \ell((i-1)P) + 1$$

Assim, na sequência (1.10) existem exatamente $g-1$ números no intervalo $1 \leq i \leq 2g-1$ tais que $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$. Os g números restantes são as lacunas de P.

Finalmente, para provar que 1 é uma lacuna de P, suponhamos que 1 seja um número polo de P. Logo, como os números polo de P formam um semigrupo aditivo, temos que cada $n \in \mathbb{N}$ é um número polo de P, assim não existiriam lacunas de P, o que é uma contradição. ✓

Notemos que dado $A \in Div(F)$, se $\deg(A) < 0$, pelo Corolário 1.3.1, temos que $\ell(A) = 0$. Por outro lado se $\deg(A) > 2g-2$, do Teorema 1.5.4 podemos concluir que $\ell(A) = \deg(A) + 1 - g$. Assim, faltaria somente considerar o caso onde $0 \leq \deg(A) \leq 2g-2$.

Lema 1.5.4. *Sejam $A, B \in Div(F)$ tais que $\ell(A) > 0$ e $\ell(B) > 0$. Então*

$$\ell(A) + \ell(B) \leq 1 + \ell(A + B).$$

Demonstração. Por hipótese $\ell(A) > 0$ e $\ell(B) > 0$. Logo, pela afirmação 1.3.1, existem divisores $A_0, B_0 \geq 0$ tais que $A \sim A_0$ e $B \sim B_0$. Definamos o conjunto

$$X := \{D \in Div(F) \mid D \leq A_0 \text{ e } \ell(D) = \ell(A_0)\},$$

que claramente é não vazio pois $A_0 \in X$. Notemos que, como $\deg(D) \geq 0$ para cada $D \in X$, então existe um divisor D_0 de grau minimal. Segue então que

$$\ell(D_0 - P) < \ell(D_0) \quad \text{para cada} \quad P \in \mathbb{P}_F$$

Provemos agora que

$$\ell(D_0) + \ell(B_0) \leq 1 + \ell(D_0 + B_0) \tag{1.11}$$

Para poder provar 1.11 vamos supor que K é um corpo finito (Na verdade o teorema também é valido no caso que K é infinito, ver Teorema 3.6.3(d) em [15]).

Seja $Supp(B_0) = \{P_1, \ldots, P_r\}$, então $\mathcal{L}(D_0 - P_i) \subsetneq \mathcal{L}(D_0)$ para cada $i = 1, \ldots, r$ ou seja $\mathcal{L}(D_0 - P_i)$ é um subespaço proprio de $\mathcal{L}(D_0)$ para cada $i = 1, \ldots, r$. Como $\mathcal{L}(D_0)$ é um espaço vetorial sobre um corpo infinito, então não pode ser união finita de subespaços próprios, assim existe

$$z \in \mathcal{L}(D_0) \setminus \bigcup_{i=1}^{r} \mathcal{L}(D_0 - P_i).$$

Consideremos a aplicação K-linear:

$$\begin{array}{rccc} \varphi: & \mathcal{L}(B_0) & \to & \mathcal{L}(D_0 + B_0) \setminus \mathcal{L}(A_0) \\ & x & \mapsto & zx \mod \mathcal{L}(A_0) \end{array}$$

Obviamente, $D_0 \leq D_0 + B_0$. Isto implica que $\mathcal{L}(D_0) \subseteq \mathcal{L}(D_0 + B_0)$ e, pela definição do conjunto X, temos que $\mathcal{L}(A_0) \subseteq \mathcal{L}(D_0 + B_0)$. Sabemos que $v_P(xz) = v_P(x) + v_P(z)$ para todo $P \in \mathbb{P}_F$. Por outro lado, como $x \in \mathcal{L}(B_0)$ e $z \in \mathcal{L}(D_0)$, temos que $v_P(x) \geq -v_P(B_0)$ e $v_P(z) \geq -v_P(D_0)$ para cada $P \in \mathbb{P}_F$. Daí $v_P(xz) \geq -v_P(B_0 + D_0)$ para cada $P \in \mathbb{P}_F$. Consequentemente, $xz \in \mathcal{L}(D_0 + B_0)$.

Por definição, sabemos que

$$Ker\, \varphi = \{x \in \mathcal{L}(B_0) \mid xz \in \mathcal{L}(A_0)\} = \{x \in \mathcal{L}(B_0) \mid xz \in \mathcal{L}(D_0)\}.$$

Dado que $x \in \mathcal{L}(B_0)$, isto implica que $v_P(x) \geq -v_P(B_0)$ para cada $P \in \mathbb{P}_F$. Em particular,

$$v_P(x) \geq 0 \quad \text{para cada} \quad P \notin Supp(B_0) \tag{1.12}$$

Como $xz \in \mathcal{L}(D_0)$ temos que

$$v_P(x) \geq -v_P(D_0) - v_P(z) \quad \text{para cada} \quad P \in \mathbb{P}_F \tag{1.13}$$

Ainda, $z \notin \bigcup_{i=1}^{r} \mathcal{L}(D_0 - P_i)$ assim para cada $i \in \{1, \ldots, r\}$ temos que $z \notin \mathcal{L}(D_0 - P_i)$. Logo, existe $Q_{P_i} \in \mathbb{P}_F$ tal que $v_{Q_{P_i}}(z) < -v_{Q_{P_i}}(D_0) + v_{Q_{P_i}}(P_i)$.

Suponhamos que $Q_{P_i} \neq P_i$. Temos que $v_{Q_{P_i}}(z) < -v_{Q_{P_i}}(D_0)$, mas, como $z \in \mathcal{L}(D_0)$, isto implicaria que $v_{Q_{P_i}}(z) < -v_{Q_{P_i}}(D_0) \leq v_{Q_{P_i}}(z)$, o que seria uma contradição. Consequentemente $Q_{P_i} = P_i$, e, portanto,

$$v_{P_i}(z) < -v_{P_i}(D_0) + 1 \quad \Rightarrow \quad v_{P_i}(z) \leq -v_{P_i}(D_0).$$

Novamente, como $z \in \mathcal{L}(D_0)$, então podemos concluir que $v_{P_i}(z) = -v_{P_i}(D_0)$ para cada $P_i \in Supp(B_0)$. Logo, de (1.13) obtemos que

$$v_{P_i}(x) \geq 0 \quad \text{para cada} \quad P_i \in Supp(B_0) \tag{1.14}$$

Assim, de (1.12) e (1.14), podemos concluir que x não possui nenhum polo, e, pelo Corolário 1.1.2, temos que $x \in K$, ou seja, $Ker\,\varphi = K$.

Portanto

$$\dim \mathcal{L}(B_0) - 1 \leq \dim \mathcal{L}(D_0 + B_0) - \dim \mathcal{L}(A_0)$$
$$\ell(D_0) + \ell(B_0) \leq 1 + \ell(D_0 + B_0),$$

o que prova (1.11), e finalmente aplicando esta desigualdade a prova do lema é imediata pois,

$$\begin{aligned} \ell(A) + \ell(B) &= \ell(A_0) + \ell(B_0) = \ell(D_0) + \ell(B_0) \\ &\leq 1 + \ell(D_0 + B_0) \leq 1 + \ell(A_0 + B_0) \\ &= 1 + \ell(A + B). \end{aligned}$$

✓

Teorema 1.5.7 (Clifford)**.** *Para cada divisor A tal que $0 \leq \deg(A) \leq 2g - 2$, tem-se*

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

Demonstração. Para $\ell(A) = 0$, não há nada para fazer. Se $\ell(W - A) = 0$ com W um divisor canônio, então

$$\ell(A) = 1 + \frac{1}{2}\deg(A) + \frac{1}{2}(\deg(A) - 2g) < 1 + \frac{1}{2}\deg(A),$$

pois $\deg(A) \leq 2g - 2$.

Agora, somente falta provar os casos onde $\ell(A) > 0$ e $\ell(W - A) > 0$. Aplicando o Lema acima 1.5.4 e o Corolário 1.5.2 obtemos

$$\ell(A) + \ell(W - A) \leq 1 + \ell(W) = 1 + g \tag{1.15}$$

Por outro lado do Teorema de Riemann-Roch

$$\ell(A) - \ell(W - A) = \deg(A) + 1 - g \tag{1.16}$$

Assim de (1.15) e (1.16) podemos concluir que

$$\begin{aligned} \ell(A) &= \deg(A) + 1 - g + \ell(W - A) \\ &\leq \deg(A) + 1 - g + 1 - g - \ell(A) \\ \Rightarrow \ell(A) &\leq \frac{1}{2}\deg(A) + 1 \end{aligned}$$

✓

1.6 COMPONENTES LOCAIS DO DIFERENCIAL DE WEIL

Uma das ferramentas utilizadas na prova do Teorema de Riemann-Roch foi o mergulho diagonal $F \hookrightarrow \mathcal{A}_F$, que leva $x \in F$ no correspondente adele principal. Nesta seção, vamos definir para cada lugar $P \in \mathbb{P}_F$ outro mergulho local $l_P : F \hookrightarrow \mathcal{A}_F$.

Definição 1.6.1. *Seja $P \in \mathbb{P}_F$.*

i) Para $x \in F$, definimos $l_P(x) \in \mathcal{A}_F$ como adele cuja componente P é x e todas as outras componentes são nulas. Ou seja,

$$\begin{aligned} l_P : F &\longrightarrow \mathcal{A}_F \\ x \longmapsto l_P(x) : \ \mathbb{P}_F &\longrightarrow F \\ Q &\longmapsto l_P(x)(Q) = \begin{cases} 0, & \text{se } P \neq Q \\ x, & \text{se } P = Q \end{cases} \end{aligned}$$

ii) Para um diferencial de Weil $\omega \in \Omega_F$ definimos a componente local $\omega_P : F \longrightarrow K$ como

$$\omega_P(x) = \omega(l_P(x)).$$

Observação 1.6.1. *Já que ω é K-linear, então ω_P é uma transformação linear sobre K.*

Proposição 1.6.1. *Sejam $\omega \in \Omega_F$ e $\alpha = (\alpha_P) \in \mathcal{A}_F$. Então, $\omega_P(\alpha_P) \neq 0$ para, no máximo, um número finito de lugares P, e*

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

Em particular, $\sum\limits_{P \in \mathbb{P}_F} w_P(1) = 0$.

Demonstração. Vamos supor que $\omega \neq 0$ e seja $W = (\omega)$ o divisor canônico de ω. Pelo Teorema da Aproximação Forte 1.5.5, existe um conjunto finito $S \subsetneq \mathbb{P}_F$ tal que

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

Definamos $\beta = (\beta_P) \in \mathcal{A}_F$ como

$$\begin{aligned} \beta_P : \mathbb{P}_F &\longrightarrow F \\ P \longmapsto \beta_P(P) &= \begin{cases} \alpha_P, & \text{se} \quad P \notin S \\ 0, & \text{se} \quad P \in S \end{cases} \end{aligned}$$

Mostremos agora que $\beta \in \mathcal{A}_F(W)$. De fato,

$$v_P(\beta) = v_P(\beta_P) = \begin{cases} v_P(\alpha_P), \text{ se } P \notin S \Rightarrow v_P(\alpha_P) \geq -v_P(W) = 0, \text{ se } P \notin S \\ v_P(0), \text{ se } P \in S \Rightarrow v_P(0) = \infty \geq -v_P(W), \text{ se } P \in S \end{cases}$$

Além disso notemos que $\alpha = (\alpha_P)_{P \in \mathbb{P}_F} = (\alpha_P)_{P \notin S} + (\alpha_P)_{P \in S}$. Mais ainda,

$$\begin{aligned} l_P(\alpha_P) : \mathbb{P}_F &\longrightarrow F \\ Q &\longmapsto \begin{cases} 0 & \text{se} \quad Q \neq P \\ \alpha_P & \text{se} \quad P = Q \end{cases} \end{aligned}$$

Portanto, temos que $\alpha = \beta + \sum\limits_{P \in S} l_P(\alpha_P)$

$$\begin{aligned} &\Rightarrow \quad \omega(\alpha) = \omega(\beta) + \sum_{P \in S} \omega(l_P(\alpha_P)) \\ &\Rightarrow \quad \omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_P), \end{aligned}$$

pois $\beta \in \mathcal{A}_F(W) = \mathcal{A}_F((\omega))$ e pela definição de ω_P.

Por outro lado, para $P \notin S$ temos que $l_P(\alpha_P) = \beta_P$. Assim, $l_P(\alpha_P) \in \mathcal{A}_F(W)$ para $P \notin S$ e, portanto, $\omega_P(\alpha_P) = 0$. ✓

Proposição 1.6.2. *i) Seja $\omega \neq 0$ um diferencial de Weil de F/K e $P \in \mathbb{P}_F$. Então $v_P(\omega) = \max\{r \in \mathbb{Z} \mid \omega_P(x) = 0$ para todo $x \in F$ com $v_P(x) \geq -r\}$. Em particular, ω_P não é uma função identicamente nula.*

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

Demonstração. i) Lembremos que, por definição, $v_P(\omega) = v_P(W)$, onde $W = (\omega)$ é o divisor do diferencial de Weil ω. Seja $m := v_P(\omega)$. Para $x \in F$ com $v_P(l_P(x)) = v_P(x) \geq -m$, temos que $l_P(x) \in \mathcal{A}_F(W)$, logo $\omega_P(x) = \omega(l_P(x)) = 0$.

Suponhamos agora que $\omega_P(x) = 0$ para todo $x \in F$, onde $v_P(x) \geq -(m+1)$. Seja $\alpha = (\alpha_Q)_{Q \in \mathbb{P}_F} \in \mathcal{A}_F(W + P)$. Então, $\alpha = (\alpha - l_P(\alpha_P)) + l_P(\alpha_P)$. Mas ainda, como $\alpha \in \mathcal{A}_F(W + P)$, por definição, $v_P(\alpha) \geq -v_P(W) - v_P(P)$ para cada $P \in \mathbb{P}_F$. Consequentemente, $v_Q(\alpha) \geq -m$, se $Q \neq P$ e $v_Q(\alpha) \geq -(m+1)$, se $Q = P$. Daí

$$v_P(\alpha - l_P(\alpha_P)) = \begin{cases} v_P(0) = \infty \geq -v_P(W) \text{ se } P = Q \\ v_Q(\alpha_Q) \geq -m = -v_P(W) \text{ se } P \neq Q \end{cases}$$

Portanto, $\alpha - l_P(\alpha_P) \in \mathcal{A}_F(W)$. Logo,

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

Assim, ω se anula em $\mathcal{A}_F(W + P)$ o que é uma contradição com a definição de W, pois claramente $W \leq W + P$.

ii)

$$\begin{aligned}
\omega_P = \omega'_P &\Rightarrow \omega_P(x) = \omega'_P(x) \quad \text{para cada } x \in F \\
&\Rightarrow \omega(l_P(x)) = \omega'(l_P(x)) \quad \text{para cada } x \in F \\
&\Rightarrow (\omega - \omega')(l_P(x)) = 0 \quad \text{para cada } x \in F \\
&\Rightarrow (\omega - \omega')_P(x) = 0 \quad \text{para cada } x \in F \\
&\Rightarrow (\omega - \omega')_P = 0 \\
&\Rightarrow \omega - \omega' = 0 \quad \text{pelo item (i).}
\end{aligned}$$

✓

2 CÓDIGOS ALGÉBRICOS GEOMÉTRICOS

Neste capítulo, vamos estudar os códigos corretores de erros de V.D. Goppa utilizando os corpos de funções algébricas vistos no capítulo 1. Tais códigos são uma classe de códigos lineares.

2.1 CÓDIGOS LINEARES

Introduziremos as noções básicas da teoria de códigos.

Consideraremos ao longo deste trabalho $\mathbb{F}_q$ um corpo finito com q elementos e $\mathbb{F}_q^n$ o espaço vetorial de dimensão n sobre $\mathbb{F}_q$. Assim, claramente, os elementos de $\mathbb{F}_q^n$ são $n-$uplas da forma $a = (a_1, \ldots, a_n)$ onde $a_i \in \mathbb{F}$ para cada i.

Definição 2.1.1. *Para $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$ elementos de $\mathbb{F}_q^n$ seja*

$$d(a, b) = \#\{i \mid a_i \neq b_i\}.$$

Esta função é dita distância de Hamming para $\mathbb{F}_q^n$. O peso de um elemento $a \in \mathbb{F}_q^n$ é definido como

$$wt(a) = d(a, 0) = |\{i \mid a_i \neq 0\}|.$$

Facilmente podemos ver que a distância de Hamming é uma métrica em $\mathbb{F}_q^n$.

Definição 2.1.2. *Um código linear C sobre um alfabeto $\mathbb{F}_q$ é um subespaço vetorial de $\mathbb{F}_q^n$, os elemento de C são ditos palavras códigos. Chamaremos n o comprimento de C e $k = \dim C$ a dimensão de C (como subespaço de $\mathbb{F}_q^n$). A distância mínima $d(C)$ de $C \neq 0$ é definida como*

$$d = d(C) = \min\{d(a, b) \mid a, b \in C,\ a \neq b\} = \min\{wt(c) \mid 0 \neq c \in C\}.$$

Assim, a notação $[n, k, d]$ representa os parâmetros do código C com comprimento n, dimensão k e distância mínima d.

Por facilidade desde agora, escreveremos código no lugar de código linear.

Definição 2.1.3. *Seja $\mathcal{B} = \{v_1, v_2, \ldots, v_k\}$ uma base ordenada do código C e consideremos a matriz G cujas linhas são os vetores $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$ para $i = 1, 2, \ldots, k$. A matriz G é chamada a matriz geradora de C associada à base $\mathcal{B}$.*

Definição 2.1.4. *Dados $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$ em $\mathbb{F}_q^n$. Definimos o produto interno canônico em $\mathbb{F}_q^n$ como*

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i.$$

Definição 2.1.5. *Seja $C \subseteq \mathbb{F}_q^n$ um código então,*

$$C^{\perp} = \{u \in \mathbb{F}_q \mid \langle u, c\rangle = 0 \text{ para cada } c \in C\}$$

é chamado o código dual de C. O código C é dito auto-dual se $C = C^{\perp}$ e auto-ortogonal se $C \subseteq C^{\perp}$.

Observação 2.1.1. *Um fato conhecido da álgebra linear é que o código dual de um código com parâmetros $[n, k, d]$ possui parâmetros $[n, n-k, d]$ e $(C^{\perp})^{\perp} = C$. Em particular, a dimensão de um código auto-dual de dimensão n é $k = \frac{n}{2}$.*

Definição 2.1.6. *A matriz geradora H de $C^{\perp}$ é dita a matriz teste de paridade de C.*

Claramente a matriz teste de paridade do código C com parâmetros $[n, k, d]$ é uma matriz de ordem $(n-k) \times k$ com posto $n-k$. Portanto

$$C = \{u \in \mathbb{F}_q^n \mid Hu^t = 0\}.$$

Assim, uma matriz teste de paridade "verifica" se um vetor $u \in \mathbb{F}_q^n$ é uma palavra código ou não.

Na teoria dos códigos algébricos, um dos maiores problemas é a construção sobre um alfabeto fixo $\mathbb{F}_q$ de um código cujas dimensão e distância mínima são grandes em comparação com seu comprimento.

Proposição 2.1.1. *Seja H uma matriz teste de paridade de um código C. Então a distancia mínima de C é maior ou igual que m se, e somente se, quaisquer $m-1$ colunas de H são linearmente independentes.*

Demonstração. $\Rightarrow$) Por hipótese $d(C) \geq m$ e suponhamos por absurdo que H tem $m-1$ colunas linearmente dependentes, a saber, $h^{i_1}, h^{i_2}, \ldots, h^{i_{s-1}}$. Logo, existem $c_{i_1}, c_{i_2}, \ldots, c_{i_{m-1}}$ elementos de $\mathbb{F}_q$, não todos nulos, tais que

$$c_{i_1}h^{i_1} + c_{i_2}h^{i_2} + \ldots + c_{i_{m-1}}h^{i_{m-1}} = 0.$$

Consequentemente, temos que $c = (0, \ldots, 0, c_{i_1}, \ldots, c_{i_{m-1}})$ é uma palavra código, assim $wt(c) \leq m-1 < m$, o que seria um absurdo.

$\Leftarrow$) Por hipótese cada conjunto de $m-1$ colunas de H é linearmente independente. Seja $c = c_1 \ldots, c_n$ uma palavra não nula de C, e sejam $h_1, \ldots, h_n$ as colunas de H. Além disso,

$$Hc^t = \sum c_i h^i = 0 \qquad (*)$$

e como $wt(c)$ é o número de componentes não nulas de c, segue que se $wt(c) \leq m-1$, por $(*)$ teríamos uma combinação nula de um número s, onde $1 \leq s \leq m-1$, de colunas de H, o que seria uma contradição. Portanto $wt(c) \geq m$, e daí $d(C) \geq m$. ✓

Teorema 2.1.1. *Seja H uma matriz teste de paridade de um código C. Então, a distância mínima de C é igual a m se, e somente se, quaisquer $m-1$ colunas de H são linearmente independentes e existem m colunas de H linearmente independentes.*

Demonstração. $\Rightarrow$) Suponhamos que $d(C) = m$, logo todo conjunto de $m-1$ colunas de H é linearmente independente. Além disso pela proposição 2.1.1 existem m colunas de H linearmente dependentes, pois caso contrário $d(C) \geq m+1$ o que seria uma contradição.

$\Leftarrow$) Suponhamos que cada conjunto de $m-1$ colunas de H é linearmente independente e existem m colunas linearmente dependentes. Logo, da proposição 2.1.1, temos que $d(C) \geq m$. Mas $d(C)$ não poderia ser maior do que m, pois, nestes caso, novamente pela proposição 2.1.1 teríamos que todo conjunto com m colunas de H é linearmente independente, o que seria uma contradição. ✓

Corolário 2.1.1 (Cota de Singleton)**.** *Dado um código C de parâmetros $[n, k, d]$ então $k + d \leq n + 1$.*

Demonstração. Se H é uma matriz teste de paridade, então tem posto $n-k$. Ainda, pelo Teorema 2.1.1, $d-1$ é menor ou igual ao posto de H, portanto

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

✓

Definição 2.1.7. *Um código é dito MDS (Maximum Distance Separable) se vale a igualdade da cota de Singleton, ou seja, se $k + d = n + 1$.*

2.2 PESOS DE HAMMING GENERALIZADOS DE CÓDIGOS AG

Os conceitos de peso de Hamming e hierarquia de peso de códigos lineares foram introduzidos por V.K.Weil em 1991, provando que a hierarquia de peso de um código linear caracteriza o desempenho do código em um determinado canal.

Definição 2.2.1. *Seja $C \neq 0$ um código com parâmetros $[n, k, d]$ e denotaremos*

$$\chi(C) = \{i \mid c_i \neq 0 \quad \textit{para alguns} \quad (c_1, c_2, \ldots, c_n) \in C\}.$$

Para qualquer r tal que $1 \leq r \leq n$, definimos o $r-$ésimo peso de Hamming generalizado como

$$d_r(C) = \min\{|\chi(V_r)| \mid V_r \textit{ é um subcódigo de } C \textit{ de dimensão } r\},$$

e a hierarquia de pesos de C é o conjunto dos pesos de Hamming generalizados, ou seja

$$\{d_r(C) \mid 1 \leq r \leq n\}.$$

Proposição 2.2.1. *O primeiro peso de Hamming generalizado de C é a distancia mínima de C.*

Demonstração. Por definição temos que o primero peso de Hamming generalizado do código C é definido como

$$d_1(C) = \min\{|\chi(V_1)| \mid V_1 \text{ é um subcódigo de } C \text{ de dimensão } 1\}.$$

Ainda, um subcódigo de dimensão um de C é um subespaço vetorial gerado por um único elemento. Suponhamos então que D seja um subcódigo unidimensional de C tal que $d_1(C) = |\chi(D)|$ onde $D = \langle y \rangle$. Claramente $y \neq 0$.

Suponhamos que d é a distância mínima de C. Se $d_1(C) \leq d$, temos uma contradição pois, em particular, $y \in C$. Por outro lado, se $d \leq d_1(C)$, então existiria $x \in C$ diferente de y com $d \leq d_1(C)$ componentes não nulas e daí

$$|\chi(\langle x \rangle)| \leq |\chi(D)|$$

o que é uma contradição pela mínimalidade de $|\chi(D)|$, assim

$$d = d_1(C).$$

✓

Lema 2.2.1 (Monotonicidade)**.** *Para um código C com parâmetros $[n, k, d]$ temos que*

$$0 < d_1(C) < d_2 < \ldots < d_k(C) \leq n.$$

Demonstração. Seja D um subcódigo de C tal que $|\chi(D)| = d_r(C)$ e $\dim(D) = r$. Para $i \in \chi(D)$ definamos o conjunto

$$D_i = \{x \in D \mid x_i = 0\}.$$

Claramente, $D_i \subsetneq D$. Logo existe $y \in D \setminus D_i$, digamos $y = (y_1, \ldots, y_n)$. Notemos que $y_i \neq 0$.

Provemos que $D = D_i \bigoplus \langle y \rangle$. De fato, se $x = (x_1, \ldots, x_n) \in D$, então existe um $\lambda \in \mathbb{F}_q$ tal que $x_i = \lambda y_i$. Assim, $x = (x - \lambda y) - \lambda y$, onde $(x - \lambda y) \in D_i$ e $\lambda y \in \langle y \rangle$.

Além disso, se $x \in D_i \cap \langle y \rangle$, então $x_i = 0$ e existe $\lambda \in \mathbb{F}_q$ tal que $x = \lambda y$. Isto implica que $0 = x_i = \lambda y_i$ e como $y_i \neq 0$ temos que $\lambda = 0$, portanto $x = 0$ e daí $D_i \cap \langle y \rangle = \{0\}$. Segue que $D = D_i \bigoplus \langle y \rangle$.

Consequentemente, $\dim(D_i) = \dim(D) - 1$. Como D_i é um subcódigo $r - 1$ dimensional de C então

$$d_{r-1}(C) \leq |\chi(D_i)| = |\chi(D)| - 1 = d_r(C) - 1$$

e portanto $d_{r-1}(C) < d_r(C)$. Falta provar que $d_1(C) > 0$ e $d_k(C) \leq n$.

Se D é um subcódigo de C unidimensional, $D \neq \{0\}$ logo existe $0 \neq x \in D$ e portanto $\chi(D) \neq 0$, donde $|\chi(D)| \geq 1$. E, como D é arbitrário, $d_1(C) > 0$. Finalmente, como os elementos de C têm no máximo n elementos, então $d_k(C) \leq n$. ✓

Corolário 2.2.1 (Cota de Singleton Generalizada)**.** *Seja C um código com parâmetros $[n, k, d]$. Para cada r tal que $1 \leq r \leq k$, temos*

$$d_r(C) \leq n - k + r.$$

Demonstração. Primeiro mostremos que para r e t tais que $1 \leq r \leq k$ e $0 \leq t \leq k - r$ então

$$d_r(C) + t \leq d_{t+r}(C).$$

Utilizemos indução em t. Fixando $r \in \{1, 2, \ldots, k\}$ temos que

$$d_r(C) + 0 \leq d_{r+0}(C).$$

Suponhamos que $d_r(C) + t \leq d_{r+t}(C)$ com $t \in \{0, 1, \ldots, k - r - 1\}$. Logo, pelo Lema 2.2.1 temos que

$$d_{r+t+1}(C) \geq d_{r+t}(C) + 1.$$

E pela hipotese de indução $d_{r+t+1}(C) \geq d_r(C) + (t + 1)$. Agora, tomando $t = k - 1$ temos que

$$d_r(C) + k - r \leq d_{r-(k+r)}(C) = d_k(C) \leq n.$$

Onde a última desigualdade também decorre do Lema 2.2.1. Portanto

$$d_r(C) \leq n - k + r.$$

✓

Proposição 2.2.2. *Seja C um código com parâmetros $[n, k, d]$ e $C^{\perp}$ o código dual então*

$$\{1, 2, \ldots, n\} = \{d_r(C) \mid 1 \leq r \leq k\} \cup \{n + 1 - d_r(C^{\perp})\}$$

Demonstração. A prova desta proposição encontra-se em [19]. ✓

2.3 CÓDIGOS DE GOPPA

Os códigos de Goppa foram introduzidos por V.D. Goppa, e são uma generalização natural dos códigos Reed-Solomon [15], que apresentemos a seguir.

Seja $n = q - 1$ e consideremos β um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^*$, isto é, $\mathbb{F}_q^* = \{\beta, \beta^2, \ldots, \beta^n = 1\}$. Para $k \in \mathbb{Z}$ tal que $1 \leq k \leq n$, definimos o espaço vetorial

$$\mathcal{L}_k = \{f \in \mathbb{F}_q[x] \mid \deg f \leq k - 1\}$$

e aplicação

$$\begin{array}{rccc} ev: & \mathcal{L}_k & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & (f(\beta), f(\beta^2), \ldots, f(\beta^n)) \end{array} \tag{2.1}$$

Claramente ev é uma aplicação linear, além disso como um polinômio de grau m possui no máximo m raizes, ainda se $f \in \mathcal{L}_k$, então $\deg f \leq k-1 \leq n-1$. Consequentemente, a quantidade de raízes de f é menor ou igual do que $n-1$. Assim, se $f \in Ker(ev)$, temos que $f = 0$, logo ev é injetiva.

Portanto, o conjunto $C_k = \{(f(\beta), f(\beta^2), \ldots, f(\beta^n)) \mid f \in \mathcal{L}_k\}$ é, na verdade, um código de parâmetros $[n, k, d]$ sobre $\mathbb{F}_q$, chamado código Reed-Solomon ou código RS. Além disso, notemos que uma palavra do código $0 \neq c = ev(f) \in C_k$ tem peso

$$wt(c) = |\{i \in \{1, 2, \ldots, n\} \mid f(\beta^i) \neq 0\}| = n - |\{i \in \{1, 2, \ldots, n\} \mid f(\beta^i) = 0\}|.$$

Como f tem no máximo $k-1$ zeros, concluimos que

$$wt(c) \geq n - \deg f \Rightarrow wt(c) \geq n - k + 1.$$

Por outro lado, pela cota de Singleton (Corolário 2.1.1), sabemos que $wt(c) \leq n - k + 1$, Assim os códigos RS são códigos MDS sobre $\mathbb{F}_q$. Notemos também que se $d = n - k + 1$ e $n = q - 1$ então $d = q - k$ o que implica que o código RS (neste caso) é curto em comparação com o tamanho do alfabeto.

Para continuar com o a análise dos códigos de Goppa, vamos fixar uma notação válida para o resto do capítulo.

$F/\mathbb{F}_q$ é um corpo de funções algébricas de gênero g.
$P_1, P_2 \ldots, P_n$ são lugares dois a dois distintos de $F/\mathbb{F}_q$ de grau um.
$D = P_1 + P_2 + \ldots + P_n$.
G é um divisor de $F/\mathbb{F}_q$ tal que $Supp\, G \cap Supp\, D = \emptyset$.

Se $x \in \mathcal{L}(G)$, então $v_P(x) \geq -v_P(G)$ para cada $P \in \mathbb{P}_F$. Como $Supp\, G \cap Supp\, D = \emptyset$, segue que $v_{P_i}(G) = 0$ para cada $i = 1, 2, \ldots, n$, assim $v_{P_i}(x) \geq 0$ e, consequentemente, $x \in \mathcal{O}_{P_i}$ para cada $i = 1, 2, \ldots, n$. Logo, pela Definição 1.1.6 a clase residual $x(P_i)$ de x módulo P_i é um elemento do corpo de classes residuais de P_i. Por outro lado, sabemos que $[F_{P_i} : \mathbb{F}_q] = \deg P_i = 1$, portanto $x(P_i) \in \mathbb{F}_q$ para cada $i = 1, 2, \ldots, n$.

Finalmente, podemos definir, analogamente como em 2.1, uma aplicação linear, que chamaremos de aplicação avaliação, como segue:

$$\begin{array}{rccc} ev_D: & \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n \\ & x & \longmapsto & (x(P_1), x(P_2), \ldots, x(P_n)) \end{array}$$

Definição 2.3.1. *Definimos o código de Goppa associado aos divisores D e G como:*

$$C_{\mathcal{L}}(D,G) = \{(x(P_1), x(P_2), \ldots, x(P_n)) \mid x \in \mathcal{L}(G)\}.$$

Ou seja, $C_{\mathcal{L}}(D,G)$ é a imagem de $\mathcal{L}(G)$ pela aplicação avaliação.

Teorema 2.3.1. *$C_{\mathcal{L}}(D,G)$ é um código com parâmetros $[n,k,d]$ tais que*

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

Demonstração. Como o código $C_{\mathcal{L}}(D,G)$ é a imagem de $\mathcal{L}(G)$ então ev_D é uma aplicação linear sobrejetora de $\mathcal{L}(G)$ em $C_{\mathcal{L}}(D,G)$. Provemos agora que $Ker(ev_D) = \mathcal{L}(G-D)$. De fato, primeiro notemos que

$$\begin{aligned} Ker(ev_D) =& \{x \in \mathcal{L}(G) \mid x(P_i) = 0 \quad i = 1,2,\ldots,n\} \\ =& \{x \in \mathcal{L}(G) \mid v_{P_i} > 0 \quad i = 1,2,\ldots,n\} \end{aligned}$$

e, por definição, se $x \in \mathcal{L}(G)$ então $v_P(x) \geq -v_P(G)$ para cada $P \in \mathbb{P}_F$.

$\subseteq$) Se $x \in Ker(ev_D)$ temos que $v_{P_i}(x) \geq 1$ e $v_{P_i}(G) = 0$ para cada $i = 1,2,\ldots,n$ assim

$$v_{P_i}(x) \geq -v_{P_i}(G-D) \quad i = 1,2,\ldots,n.$$

Agora, se $P \in \mathbb{P}_F \setminus \{P_1,\ldots,P_n\}$, então $v_P(D) = 0$. Logo, $v_P(x) \geq -v_P(G-D)$. Consequentemente, $x \in \mathcal{L}(G-D)$.

$\supseteq$) Se $x \in \mathcal{L}(G-D)$ por definição temos que

$$v_{P_i} \geq -v_{P_i}(G-D) = -v_{P_i}(G) + -v_{P_i}(D) = 1 \quad \text{para cada} \quad i = 1,2,\ldots,n.$$

Portanto, $v_{P_i}(x) > 0$ para cada $i = 1,2,\ldots,n$ e daí $x \in Ker(ev_D)$.

Finalmente

$$\begin{aligned} k =& \dim C_{\mathcal{L}}(D,G) = \dim(\mathcal{L}(G)/Ker(ev_D)) \\ =& \dim \mathcal{L}(G) - \dim \mathcal{L}(G-D) \\ =& \ell(G) - \ell(G-D). \end{aligned}$$

Assumimos que $C_{\mathcal{L}}(D,G) \neq 0$. Seja $x \in \mathcal{L}(G)$ com $wt(ev_D(x)) = d$, assim existem d componentes não nulas de $ev_D(x)$, consequentemente existe $n-d$ lugares $P_{i_1}, P_{i_2}, \ldots, P_{i_{n-d}}$ no suporte de D que são zeros de x. Isto implica que $v_{P_j}(x) > 0$ para cada $j \in \{i_1, i_2, \ldots, i_{n-d}\}$. Portanto

$$0 \neq x \in \mathcal{L}(G - (P_{i_1} + P_{i_2} + \ldots + P_{i_{n-d}})).$$

Logo, pelo Corolário 1.3.1, temos que $0 < \deg(G - (P_{i_1} + P_{i_2} + \ldots + P_{i_{n-d}})) = \deg(G) - n + d$ e assim $d \geq n - \deg(G)$ como desejamos. ✓

Corolário 2.3.1. *Suponha que o grau de G é estritamente menor do que n. Então a aplicação avaliação $ev_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D,G)$ é injetiva e assim temos que:*

i) $C_{\mathcal{L}}(D,G)$ *é um código com parametros* $[n,k,d]$ *tal que*

$$d \geq n - \deg(G) \quad e \quad k = \mathcal{L}(G) \geq \deg(G) + 1 - g.$$

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

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

iii) Se $\{x_1, x_2, \ldots, x_k\}$ *é uma base de* $\mathcal{L}(G)$ *então a matriz*

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

É uma matriz geradora do código $C_{\mathcal{L}}(D,G)$.

Demonstração. i) Se $\deg(G) < n = \deg(D)$ então $\deg(G - D) < 0$ logo, pelo Corolário 1.3.1, temos que $\dim(G - D) = 0$ e, como $Ker(ev_D) = \mathcal{L}(G - D)$, temos então que aplicação avaliação é injetiva, e pelo Teorema 2.3.1, temos que $k = \ell(G)$. Ainda, pelo Teorema de Riemann-Roch, sabemos que $\ell(G) = \deg(G) + 1 - g + \ell(W - G)$ para algum divisor canônico W, e daí

$$k = \ell(G) \geq \deg(G) + 1 - g.$$

ii) Decorre direitamente do item (i) e do Teorema 1.5.4.

iii) É óbvia.

✓

Definiremos agora um código associado com os divisores G e D utilizando componentes do diferencial de Weil.

Definição 2.3.2. *Sejam G e D divisores (como definidos na página 54), então definimos o código $C_\Omega(D,G) \subseteq \mathbb{F}_q^n$ como*

$$C_\Omega(D,G) = \{(\omega_{P_1}(1), \omega_{P_2}(1), \ldots, \omega_{P_n}(1)) \mid \omega \in \Omega_F(G - D)\}.$$

O código $C_\Omega(D,G)$ também é chamado código de Goppa.

Teorema 2.3.2. *$C_\Omega(D,G)$ é um código com parâmetros $[n,k',d']$ tais que*

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

Com a hipótese adicional de que $\deg(G) > 2g-2$*, temos que* $k' = i(G-D) \geq n+g-1-\deg(G)$*. Além disso, se* $2g-2 < \deg(G) < n$*, então* $k' = n+g-1-\deg(G)$*.*

Demonstração. Sejam $P \in \mathbb{P}_F$ um lugar de grau 1 e ω um diferencial de Weil com $v_P(\omega) \geq -1$. Afirmamos que

$$\omega_P(1) = 0 \Leftrightarrow v_P(\omega) \geq 0 \tag{2.2}$$

De fato, $\Leftarrow$) Decorre direitamente da Proposição 1.6.2 que afirma que $r \in \mathbb{Z}$ satisfaz

$$v_P(\omega) \geq r \Leftrightarrow \omega_P(x) = 0 \quad \forall\, x \in F \quad \text{onde} \quad v_P(x) \geq -r. \tag{2.3}$$

$\Rightarrow$) Suponha que $\omega_P(1) = 0$. Seja $x \in F$ com $v_P(x) \geq 0$ (ou seja, $x \in P$). Como $\deg(P) = 1$, temos que $\mathbb{F}_q = F_P = \mathcal{O}_P/P$, assim podemos escrever $x = a + y$ com $a \in \mathbb{F}_q$ e $y \in P$. Notemos que $v_P(y) \geq 1$, logo, por (2.3) e a hipótese da afirmação, $v_P(\omega) \geq -1$ temos que $\omega_P(y) = 0$. Consequentemente

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

Assim (2.2) é provada.

Agora consideremos a aplicação $\mathbb{F}_q$ linear,

$$\begin{array}{rccc} e_D: & \Omega_F(G-D) & \longrightarrow & C_\Omega(D,G) \\ & \omega & \longmapsto & (\omega_{P_1}(1), \omega_{P_2}(1), \ldots, \omega_{P_n}(1)) \end{array}$$

Claramente, e_D é uma aplicação sobrejetora. Mas ainda, notemos que $\omega \in \Omega_F(G-D)$ se, e somente se, $(\omega) \geq G - D$ o que implica que $v_{P_i}(\omega) \geq -1$ para cada $i = 1, \ldots, n$. Assim, temos que cada P_i e $\Omega_F(G-D)$ satisfaz a afirmação de (2.2).

Mostremos agora que $Ker(e_D) = \Omega_F(G)$. De fato, se $\omega \in \Omega_F(G) \Leftrightarrow (\omega) \geq G \Leftrightarrow v_P(\omega) \geq v_P(G)$ para cada $P \in \mathbb{P}_F$ se, e somente se, $v_{P_i}(\omega) \geq 0$ com $i = 1, \ldots, n \Leftrightarrow \omega_{P_i}(1) = 0$ com $i = 1, \ldots, n$ se, e somente se, $\omega \in Ker(e_D)$.

Assim, temos que

$$k' = \dim(C_\Omega(D,G)) = \dim \Omega_F(G-D) - \dim \Omega_F(G) = i(G-D) - i(G).$$

Seja $e_D(\omega) \in C_\Omega(D,G)$ uma palavra do código de peso $m > 0$. Então $\omega_{P_i}(1) = 0$ para certos índices $i = i_1, i_2, \ldots, i_{n-m}$.

1. Como $\omega \in \Omega_F(G-D)$, temos que $v_P(\omega) \geq v_P(G)$ se $P \in \mathbb{P}_F \setminus \{P_1, P_2, \ldots, P_n\}$ e $v_P(\omega) \geq -1$ se $P = P_i$ para cada $i = 1, 2, \ldots, n$.

2. Para o divisor
$$A = G - \left(D - \sum_{j=1}^{n-m} P_{ij} \right)$$
temos que se $j \in \{i_1, i_2, \ldots, i_{n-m}\}$, então $v_{P_j}(A) = 0$. Mas $\omega_{P_j}(1) = 0$ e pela equação (2.2) temos que $v_{P_j}(\omega) \geq 0$ então $v_{P_j}(\omega) \geq v_{P_j}(A)$.

Assim das afirmações (1) e (2) acima temos que $\omega \in \Omega_F(A)$, ou seja, $\Omega_F(A) \neq 0$. Pelo Lema 1.5.3 sabemos que $\dim(\Omega_F(A)) = i(A)$ e, pelo Teorema de Riemann-Roch, temos que $i(A) = 0$ se $\deg(A) > 2g-2$, consequente $\deg(A) \leq 2g-2$ e daí

$$2g - 2 \geq \deg(G) - (n - (n-m)) = \deg(G) - m.$$

Portanto, a distância mínima d' do código $C_\Omega(D, G)$ cumpre $d' \geq \deg(G) - (2g-2)$.

Agora, suponhamos que $\deg(G) > 2g-2$. Logo, pelo Teorema 1.5.4 temos que $i(G) = 0$. Isto implica que

$$\begin{aligned} k' &= i(G-D) \\ &= \ell(G-D) - \deg(G-D) + g - 1 \\ &= \ell(G-D) - \deg(G) + n + g - 1 \quad (*) \end{aligned}$$

Finalmente $k' = i(G-D) \geq n + g - 1 - \deg(G)$

Além disso, se $\deg(G) < n$, temos que $\deg(G-D) < 0$ e, pelo Corolário 1.3.1, $\ell(G-D) = 0$. Assim de $(*)$ obtemos $k' = n + g - 1 - \deg(G)$. ✓

Teorema 2.3.3. *Os códigos $C_{\mathcal{L}}(D, G)$ e $C_\Omega(D, G)$ são duais entre si, isto é,*

$$C_\Omega(D, G) = C_{\mathcal{L}}(D, G)^\perp.$$

Demonstração. Primeiro, observemos o seguinte fato: consideremos um lugar $P \in \mathbb{P}_F$ de grau 1, o diferencial de Weil ω com $v_P(\omega) \geq -1$ e um elemento $x \in F$ com $v_P(x) \geq 0$. Então

$$\omega_P(x) = x(P)\omega_P(1) \tag{2.4}$$

Para provar isto, podemos escrever $x = a + y$ onde $a = x(P) \in \mathbb{F}_q$ e $v_P(y) > 0$. Então

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

onde a última igualdade decorre da equação (2.3).

Mostremos agora que $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$. Seja $\omega \in \Omega_F(G-D)$ e $x \in \mathcal{L}(G)$, então:

$$\begin{aligned} 0 = \omega(x) &= \sum_{P\in\mathbb{P}_F} \omega_P(x) && (2.5)\\ &= \sum_{i=1}^{n} \omega_{P_i}(x) && (2.6)\\ &= \sum_{i=1}^{n} x(P_i)\omega_{P_i}(1) && (2.7)\\ &= \langle(\omega_{P_i}(1),\ldots,\omega_{P_n}(1)),((x(P_1),\ldots,x(P_n))\rangle. && (2.8) \end{aligned}$$

Onde $\langle , \rangle$ é o produto interno canônico de $\mathbb{F}_q^n$. Justifiquemos agora as igualdades acima.

(2.5) Pela Proposição 1.6.1 e pelo fato que um diferencial de Weil se anular em adeles principais.

(2.6) Para $P \in \mathbb{P}_F \setminus \{P_1,\ldots,P_n\}$ como $\omega \in \Omega_F(G-D)$, então $v_P(\omega) \geq v_P(G)$ e, pela equação (2.3) temos que $\omega_P(x) = 0$ para cada $x \in F$ onde $v_P(x) \geq -v_P(G)$, que é válido pois $x \in \mathcal{L}(G)$.

(2.7) É uma implicação da equação (2.4).

Assim, temos que $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$. Agora, é suficiente provar que os dois códigos tem a mesma dimensão.

$$\begin{aligned} \dim(C_\Omega(D,G)) &= i(G-D) - i(G) \qquad \text{(pelo Teorema 2.3.2)}\\ &= \ell(G-D) - \deg(G-D) + g - 1 - (\ell(G) - \deg(G) + g - 1)\\ &= \ell(G-D) + \deg(D) - \ell(G)\\ &= n - (\ell(G) - \ell(G-D))\\ &= n - \dim(C_\mathcal{L}(D,G)) \qquad \text{(pelo Teorema 2.3.1)}\\ &= \dim(C_\mathcal{L}(D,G)^\perp) \end{aligned}$$

✓

O próximo objetivo desde capítulo é provar que o código $C_\Omega(D,G)$ pode ser representado como um código $C_\mathcal{L}(D,H)$ para um divisor apropriado H.

Lema 2.3.1. *Existe um diferencial de Weil η tal que*

$$v_{P_i}(\eta) = -1 \quad e \quad \eta_{P_i}(1) = 1 \quad \textit{para cada} \quad i = 1,\ldots,n.$$

Demonstração. Escolhamos um diferencial de Weil $\omega_0 \neq 0$. Pelo Teorema da Aproximação Fraca (Teorema 1.2.1), existe um elemento $z \in F$ tal que $v_{P_i}(z) = -v_{P_i}(\omega_0) - 1$ para cada $i = 1, \ldots, n$. Fazendo $\omega := z\omega_0$ temos que $(\omega) = (z) + (\omega_0)$ e daí $v_{P_i}(\omega) = -1$. Consequentemente, da equação (2.2), $a_i := \omega_{P_i}(1) \neq 0$.

Novamente, pelo Teorema da Aproximação Fraca, $y \in F$ tal que $v_{P_i}(y - a_i) > 0$, portanto temos que $v_{P_i}(y) = 0$ e $y(P_i) = a_i$. Definimos $\eta := y^{-1}\omega$. Logo

$$v_{P_i}(\eta) = v_{P_i}(y^{-1}) + v_{P_i}(\omega) = v_{P_i}(\omega) = -1$$

e

$$\eta_{P_i}(1) = y^{-1}\omega_{P_i}(1) = \omega_{P_i}(y^{-1}) = y^{-1}(P_i)\omega_{P_i}(1) = a_i^{-1}a_i = 1.$$

✓

Proposição 2.3.1. *Se η é um diferencial de Weil tal que $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$ para cada $i = 1, \ldots, n$ então*

$$C_{\mathcal{L}}(D, G)^{\perp} = C_{\Omega}(D, G) = C_{\mathcal{L}}(D, H) \quad \textit{onde} \quad H = D - G + (\eta).$$

Demonstração. Notemos que $Supp(D - G + (\eta)) \cap Supp(D) = \emptyset$ pois $v_{P_i}(\eta) = -1$ para cada $i = 1, \ldots, n$. Portanto, $C_{\mathcal{L}}(D, H)$ está bem definido.

Pelo Teorema da Dualidade (Teorema 1.5.2), existe um isomorfismo

$$\begin{array}{rccc} \mu: & \mathcal{L}((\eta) - (G - D)) & \longrightarrow & \Omega_F(G - D) \\ & x & \longmapsto & x\eta \end{array}$$

Assim, para $x \in ((\eta) - (G - D))$, temos que

$$(x\eta)_{P_i}(1) = \eta_{P_i}(x) = x(P_i)\eta_{P_i}(1) = x(P_i),$$

onde a segunda igualdade decorre da equação 2.4. Portanto, $C_{\Omega}(D, G) = C_{\mathcal{L}}(D, H)$ e, pelo Teorema 2.3.3, sabemos que $C_{\Omega}(D, G) = C_{\mathcal{L}}(D, G)^{\perp}$. ✓

Corolário 2.3.2. *Suponha que existe um diferencial de Weil η tal que*

$$2G - D \leq (\eta) \quad e \quad \eta_{P_i}(1) = 1 \quad para \quad i = 1, \ldots, n.$$

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

$$2G - D = (\eta) \quad e \quad \eta_{P_i}(1) = 1 \quad para \quad i = 1, \ldots, n,$$

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

Demonstração. Suponha que $2G - D \leq (\eta)$ portanto $G \leq D - G + (\eta)$. Logo, pela Proposição 2.3.1, temos que

$$C_{\mathcal{L}}(D, G) \subseteq C_{\mathcal{L}}(D, D - G + (\eta)) = C_{\mathcal{L}}(D, G)^{\perp}.$$

Isto prova que $C_{\mathcal{L}}(D, G)$ é auto-ortogonal.

Agora assumiremos que $2G - D = (\eta)$, ou seja, $G = D - G + (\eta)$, assim

$$C_{\mathcal{L}}(D, G)^{\perp} = C_{\mathcal{L}}(D, D - G + (\eta)) = C_{\mathcal{L}}(D, G).$$

E daí $C_{\mathcal{L}}(D, G)$ é auto-dual. ✓

Corolário 2.3.3. *Se* $\deg(G) > 2g - 2$*, o código* $C_{\mathcal{L}}(D, G)$ *possui*

$$d_r(C_{\mathcal{L}}(D, G)) = n - k + r \quad \textit{para todo} \quad g + 1 \leq r \leq k.$$

Demonstração. Sabemos, pela Proposição 2.3.1, que $C_{\mathcal{L}}(D, G)^{\perp} = C_{\mathcal{L}}(D, H)$ com $H = D - G + (\eta)$, onde η é um diferencial de Weil de F/K com $v_P(\eta) = -1$ e $\eta_{P_i}(1) = 1$ para cada $i = 1, 2, \ldots, n$ e $P_i \in Supp(D)$.

Lembrando que $d_1(C_{\mathcal{L}}(D, H)^{\perp})$ é a distância mínima de $C_{\mathcal{L}}(D, H)$, pelo Teorema 2.3.1 e o Corolário 1.5.2, temos que

$$d_1(C_{\mathcal{L}}(D, G)^{\perp}) \geq \deg(G) - 2g + 2.$$

Ou seja,

$$n + 1 - d_1(C_{\mathcal{L}}(D, G)^{\perp}) \leq n - \deg(G) + 2g - 1.$$

Por outro, lado pelo Lema da Monotonicidade (Lema 2.2.1), sabemos que

$$0 \leq d_1(C_{\mathcal{L}}(D, G)^{\perp}) < d_2(C_{\mathcal{L}}(D, G)^{\perp}) < \ldots < d_{n-k}(C_{\mathcal{L}}(D, G)^{\perp}) < n - k$$

o que implica que

$$n + 1 - d_1(C_{\mathcal{L}}(D, G)^{\perp}) > n + 1 - d_2(C_{\mathcal{L}}(D, G)^{\perp}) > \ldots > n + 1 - d_{n-k}(C_{\mathcal{L}}(D, G)^{\perp}).$$

E pela, Proposição 2.2.2, temos que

$$d_{k-i}(C_{\mathcal{L}}(D, G)^{\perp}) = n - i \quad \text{para cada} \quad i \quad \text{onde} \quad 0 \leq i \leq \deg(G) - 2g.$$

Novamente, pelo Teorema 2.3.1, temos que $k \leq \ell(G)$. Mas, por hipótese, $\deg(G) > 2g - 2$ e assim, pelo Teorema 1.5.4, podemos afirmar que $k \leq \deg(G) + 1 - g$. Isto implica que

$$k - (\deg(G) - 2g) \leq g + 1.$$

✓

Definição 2.3.3. *Seja F/K um corpo de funções algébricas onde $K = \widetilde{K}$. Para cada inteiro $r \geq 1$, definimos o conjunto*

$$\gamma_r = \min\{\deg(A) \mid A \in Div(F) \quad e \quad \ell(A) \geq r\}.$$

A sequência $\{\gamma_r \mid r \geq 1\}$ é chamada sequência de gonalidade de F/K.

Notemos que, pelo Corolário 1.3.1, para um divisor $A \in Div(F)$ de grau zero temos que A é principal se, é somente se, $\ell(A) = 1$. Assim, temos que $\gamma_1 = 0$. Por outro lado, γ_2 é a gonalidade usual, isto é,

$$\gamma_2 = \min\{[F : K(u)] \mid u \in F\}.$$

A prova de γ_2 pode encontra-se em [12].

Seja F/K um corpo de funções com um lugar P de grau um. Sabemos que $r \geq 0$ é um número polo de P se existe $x \in F$ tal que $(x)_\infty = rP$. Além disso, temos que $1, x, x^2, \ldots, x^r \in \mathcal{L}(rP)$ para $r \geq 1$ e estes elementos são linearmente independentes. Consequentemente, $\ell(rP) > r$ e, portanto,

$$\deg(rP) \in \min\{\deg(A) \mid A \in Div(F) \quad \text{e} \quad \ell(A) \geq r\}.$$

E, pela definição de gonalidade, segue que

$$\gamma_r \leq r = \deg(rP).$$

Proposição 2.3.2. *Seja F/K um corpo de funções algébricas de gênero g. Suponhamos que F/K tem um lugar de grau um. Então*

i) $0 = \gamma_1 < \gamma_2 < \ldots < \gamma_r < \gamma_{r+1} < \ldots$

ii) $\gamma_r = r + g - 1$ *para cada* $r > g$.

iii) $\gamma_g = 2g - 2$ *e* $\gamma_r \geq 2(r-1)$ *para cada* $r \geq g$.

Demonstração. i) Seja A um divisor tal que $\deg(A) = \gamma_r$ e $\ell(A) \geq r$. Consideremos agora o divisor $A' = A - P$ onde P é o lugar de grau um. Logo, pelo Lema 1.3.2,

$$\begin{aligned} \ell(A) - \ell(A') &\leq \deg(A) - \deg(A') \\ &= \deg(A) - (\deg(A) - \deg(P)) \\ &= \deg(P) \\ &= 1 \end{aligned}$$

Consequentemente, $\ell(A') \geq r - 1$ e, da definição de gonalidade, temos que $\gamma_{r-1} \leq \deg(A')$ o que implica que

$$\gamma_{r-1} \leq \deg(A) - 1 < \deg(A) = \gamma_r.$$

E, assim, $\gamma_{r-1} < \gamma_r$ como desejamos.

ii) Suponhamos que $r > g$. Seja $A \in Div(F)$ tal que $\deg(A) = r+g-1 > 2g-1$. Logo, pelo Teorema 1.5.4, temos que $\ell(A) = \deg(A) + 1 - g$. Isto implica que $\ell(A) = r$ e, pela definição de gonalidade, obtemos $\gamma_r \leq \deg(A) = r + g - 1$.

Suponhamos que $\gamma_r < r + g - 1$. Consideremos um divisor B tal que $\gamma_r = \deg(B) < r + g - 1$. Assim, existe B' tal que $B \leq B'$ e $\deg(B') = r + g - 2$. Mas, por hipótese, $r > g$ então $\deg(B') > 2g - 2$ e, pelo Teorema 1.5.4, $\ell(B) = \deg(B') + q - 1 = r - 1$. Por outro lado, como $B \leq B'$, pelo Lema 1.3.2 $\ell(B) \leq \ell(B') = r-1 < r$, o que é uma contradição pela definição de gonalidade. Podemos então concluir que $\gamma_r = r+q-1$.

iii) Consideremos o divisor canônico W de F/K. Pelo Corolário 1.5.2, temos que $\deg(W)2g - 2$ e $\ell(W) = g$. Logo, da definição de gonalidade, concluimos que

$$\gamma_g \leq 2g - 2 \quad (*).$$

Ainda pelo item (i) temos que $0 \leq \gamma_r \leq 2g - 2$ para cada $1 \leq r \leq g$. Suponha que A é um divisor tal que $\deg(A) = \gamma_r$ e $\ell(A) \geq r$. Logo, pelo Teorema de Clifford (Teorema 1.5.7), obtemos

$$\gamma \leq \ell(A) \leq 1 + \frac{1}{2}\deg(A) = 1 + \frac{\gamma_r}{2}.$$

Finalmente, da desigualdade anterior, temos que $\gamma_r \geq 2(r-1)$ para cada $1 \leq r \leq g$. Ainda para $r = g$ temos que $\gamma_g \geq 2g - 2$ e, conjuntamente com $(*)$ concluimos que $\gamma_g = 2g - 2$.

✓

O seguinte teorema mostra que a cota inferior para a distância mínima d_1 de códigos de Goppa, tem uma generalização natural para cada d_r que envolve a sequencia de gonalidade $\{\gamma_r \mid r \geq 1\}$ de F/K.

Teorema 2.3.4. *Dado o código $C_{\mathcal{L}}(D, G)$ temos que*

$$d_r(C_{\mathcal{L}}(D, G)) \geq n - \deg(G) + \gamma_r \quad \textit{para cada } r \textit{ tal que} \quad 1 \leq r \leq k,$$

onde k é a dimensão de $C_{\mathcal{L}}(D, G)$.

Demonstração. Seja V_r o subconjunto $r-$dimensional de $C_{\mathcal{L}}(D, G)$ tal que $|\chi(V_r)| = d_r(C_{\mathcal{L}}(D, G))$. Sem perda de generalidade, suponha que V_r é gerado pelas palavras $ev_D(x_1), ev_D(x_2), \ldots, ev_D(x_r)$, onde $x_1, x_2, \ldots, x_r \in \mathcal{L}(G)$ são linearmente independentes sobre $\mathbb{F}_q^n$.

Temos que $|\chi(V_r)| = d_r(C_{\mathcal{L}}(D, G))$ é equivalente a dizer que toda palavra código na base $\{ev_D(x_1), ev_D(x_2), \ldots, ev_D(x_r)\}$ tem exatamente $n - d_r(C_{\mathcal{L}}(D, G))$ lugares distintos,

onde todas as valorizações são zero. Isto pode ser representado em termos de divisores, ou seja, para cada i onde $1 \leq i \leq r$,

$$(x_i) = A + B_i - G_i$$

onde $0 \leq A \leq D$, $\deg(A) = n - d_r(C_{\mathcal{L}}(D,G))$ e $B_i \geq 0$ para $i = 1, 2, \ldots, r$.

Notemos que

$$\left(\frac{x_i}{x_1}\right) = (x_i) - (x_1) = B_i - B_1 \geq -B_1 \quad \text{para cada} \quad i = 1, 2, \ldots, r.$$

Logo, $x_i/x_1, x_i/x_1, \ldots, x_i/x_1 \in \mathcal{L}(B_1)$, além disso esses elementos são linearmente independentes sobre $\mathbb{F}_q$. Consequentemente, $\ell(B_1) \geq r$ e, pela definição de gonalidade, $\gamma_r \leq \deg(B_1)$. Ainda $(x_1) = A + B_1 - G$ e, pelo Teorema 1.3.1, temos que $\deg(B_1) = \deg(G) - \deg(A)$. Finalmente,

$$\gamma_r \leq \deg(B_1) = \deg(G) - n + d_r(C_{\mathcal{L}}(D,G))$$

$$\Rightarrow d_r(C_{\mathcal{L}}(D,G)) \geq \gamma_r + n - \deg(G).$$

✓

Observação 2.3.1. *O Teorema* 2.3.4 *pode ser usado para fornecer uma prova alternativa do Corolário* 2.3.3*, com a hipótese adicional que* $\deg(G) < n$.

Se $2g - 2 < \deg(G) < n = \deg(D)$ *o Corolário* 2.3.1 *implica que* $k = \dim(G) = \deg(G) + 1 - g$. *Pela Proposição* 2.3.2 *e pelo Teorema* 2.3.4*, obtemos*

$$\begin{aligned} d_r(C_{\mathcal{L}}(D,G)) &\geq n - \deg(G) + \gamma_r \\ &= n - \deg(G) + r + g - 1 \\ &= n - (\deg(G) + 1 - g) + r \\ &= n - k + r. \end{aligned}$$

Por outro lado, pelo Corolário 2.2.1 *(Cota de Singleton Generalizada), sabemos que*

$$d_r(C_{\mathcal{L}}(D,G)) \leq n - k + r.$$

Consequentemente, se $2g - 2 < \deg(G) < n$*, então*

$$d_r(C_{\mathcal{L}}(D,G)) = n - k + r \quad \textit{para cada} \quad g + 1 \leq r \leq k.$$

3 CÓDIGOS HERMITIANOS

Os códigos Hermitianos são exemplos interessantes e não triviais dos códigos de Goppa, pois não são curtos em comparação com o tamanho do alfabeto e seus parâmetros k e d são ótimos. Para trabalhar estes códigos, são necessários alguns fundamentos algébricos além dos vistos no Capítulo 1.

3.1 EXTENSÕES DE CORPOS DE FUNÇÕES ALGÉBRICAS

Ao longo desta seção, F/K irá denotar um corpo de funções algébricas, onde K é algebricamente fechado em F é perfeito, isto é, cada $f(x) \in K[x]$ irredutível possui raízes distintas em F. Também consideraremos um corpo de funções algebricas F'/K', onde K' é algebricamente fechado em F', F'/F é uma extensão algébrica e $K \subseteq K'$.

Definição 3.1.1. *i) Um corpo de funções algébricas F'/K' é dito uma extensão algébrica de F/K se $F \subseteq F'$ é uma extensão algébrica e $K \subseteq K'$.*

ii) A extensão algébrica F'/K' de F/K é chamada extensão por constantes se $F' = FK'$, onde FK' é dito o compósito de F e K'.

iii) A extensão algébrica F'/K' de F/K é chamada finita se $[F' : F] < \infty$.

Lema 3.1.1. *Se F'/K' é uma extensão de F/K então:*

i) K'/K é uma extensão algébrica e $F \cap K' = K$.

ii) F'/K' é uma extensão finita de F/K se, e somente se, $[K' : K] < \infty$.

iii) Se $F_1 = FK'$. Então F_1/K' é uma extensão por constantes de F/K e F'/K' é uma extensão finita de F_1/K'.

Demonstração. Pode ser encontrada em [15] Lema 3.1.2. ✓

Definição 3.1.2. *Seja F'/K' uma extensão algébrica de F/K. Um lugar $P' \in \mathbb{P}_{F'}$ é dito uma extensão de $P \in \mathbb{P}_F$ se $P \subseteq P'$ e nesse caso escrevemos, $P'|P$.*

Proposição 3.1.1. *Seja F'/K' uma extensão algébrica de F/K. Sejam $P' \in \mathbb{P}_{F'}$ e $P \in \mathbb{P}_F$, e $\mathcal{O}_{P'} \subseteq F'$ e $\mathcal{O}_P \subseteq F$ os respectivos anéis de valorização. Sejam ainda v_p e $v_{P'}$ as respectivas valorizações discretas. Então, as seguintes afirmações são equivalentes:*

i) $P'|P$.

ii) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

iii) Existe um inteiro $e \geq 1$ tal que $v_{P'}(x) = e \cdot v_P(x)$ para cada $x \in F$.

Mas ainda, se $P'|P$ então $P = P' \cap F$ e $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. Por isto, P é dito a restrição de P' em F.

Demonstração. i) $\Rightarrow$ *ii)* Suponhamos que $P'|P$, mas $\mathcal{O}_P \subsetneq \mathcal{O}_{P'}$. Assim, existe $u \in F$ tal que $v_P(u) \geq 0$ e $v_{P'}(u) < 0$. Mas ainda como, $P \subseteq P'$, então $v_P(u) = 0$.

Tomemos $t \in F$ tal que $v_P(t) = 1$. Logo, $t \in P \subseteq P'$ e $r = v_{P'}(t) > 0$. E daí obtemos as seguintes relações

$$v_P(u^r t) = r \cdot v_P(u) + v_P(t) = 1$$

$$v_{P'}(u^r t) = r \cdot v_{P'}(u) + v_{P'}(t) \leq -r + r = 0.$$

Consequentemente, $u^r t \in P \setminus P'$, o que seria uma contradição pois $P \subseteq P'$.

$(*)$ Mostremos que $\mathcal{O}_P \subseteq \mathcal{O}_{P'} \Rightarrow \mathcal{O}_P = F \cap \mathcal{O}_{P'}$.

Sabemos que $F \cap \mathcal{O}_{P'}$ é um subanel de F e $\mathcal{O}_P \subseteq F \cap \mathcal{O}_{P'}$. Logo pelo Teorema 1.1.2 item (iv), obtemos que $F \cap \mathcal{O}_{P'} = \mathcal{O}_P$ ou $F \cap \mathcal{O}_{P'} = F$. Suponhamos que $F \cap \mathcal{O}_{P'} = F$, isto é, $F \subseteq \mathcal{O}_{P'}$. Escolhendo um elemento $z \in F' \setminus \mathcal{O}_{P'}$, como F'/F é uma extensão algébrica, tem-se

$$z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0 \quad \text{onde} \quad a_i \in F.$$

Portanto, $v_{P'}(z^n) = n \cdot v_{P'}(z) < 0$ pois $z \notin \mathcal{O}_{P'}$. Assim,

$$v_{P'}(a_i z^i) = v_{P'}(a_i) + i \cdot v_{P'}(z) \geq n \cdot v_{P'}(z) = v_{P'}(z^n),$$

para $i = \{1, 2, \ldots, n-1\}$, e $v_{P'}(a_0) \geq 0 > v_{P'}(z^n)$.

Finalmente, pelo Lema da Desigualdade Triangula Estrita (Lema 1.1.2), obtemos que

$$v_{P'}(z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0) = n \cdot v_{P'}(0),$$

o que seria uma contradição e portanto $\mathcal{O}_P = F \cap \mathcal{O}_{P'}$.

ii) $\Rightarrow$ *i)* Suponhamos que $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$. Dado $y \in P$, pelo Corolário 1.1.1, temos que $y^{-1} \notin \mathcal{O}_P$. Por $(*)$, isto nos dá que $y^{-1} \notin \mathcal{O}_{P'}$ e, novamente pelo Corolário 1.1.1, obtemos que $y \in P'$ e daí $P \subseteq P'$.

ii) $\Rightarrow$ *iii)* Seja $u \in F$ um elemento tal que $v_P(u) = 0$. Então, temos que $u, u^{-1} \in \mathcal{O}_{P'}$, uma vez que $u, u^{-1} \in \mathcal{O}_P \subseteq \mathcal{O}_{P'}$. Logo, $v_{P'}(u) = 0$.

Escolhamos $t \in F$ com $v_P(t) = 1$ e coloquemos $e = v_{P'}(t)$. Como $P \subseteq P'$ temos que $e \geq 1$.

Sejam $0 \neq x \in F$ e $v_P(x) = r \in \mathbb{Z}$. Então $v_P(xt^{-r}) = v_P(x) - r \cdot v_P(t) = 0$ e daí

$$v_{P'}(x) = v_{P'}(xt^{-r}) + v_{P'}(t^r) = 0 + r \cdot v_{P'}(t) = r \cdot e = e \cdot v_P(x).$$

iii) $\Rightarrow$ *ii)* Se $x \in \mathcal{O}_P$, então $v_P(x) \geq 0$ e como $v_{P'}(x) = e \cdot v_P(x) \geq 0$ portanto $x \in \mathcal{O}_{P'}$.

$(**)$ Mostremos finalmente que $P'|P \Rightarrow P = P' \cap F$.

De fato, a inclusão $P \subseteq P' \cap F$ segue do fato de $P \subseteq P'$ e $P \subseteq F$. Agora, se $x \in F$ e $v_{P'}(x) > 0$, então $e \cdot v_P(x) = v_{P'}(x) > 0$, portanto $v_P(x) > 0$, pois $e \geq 1$. Isto prova que $P' \cap F \subset P$. ✓

Definição 3.1.3. *Sejam F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$.*

i) O inteiro $e \geq 1$ tal que $v_{P'}(x) = e.v_P(x)$ para cada $x \in F$. Definindo $e := e(P'|P)$ é dito o índice de ramificação de P' sobre P, escrevemos $e = e(P'|P)$. Dizemos que $P'|P$ é ramificado se $e(P'|P) > 1$, e não é ramificado se $e(P'|P) = 1$.

ii) $f(P'|P) := [F'_{P'} : F_P]$ é chamado o grau relativo de P' sobre P.

Notemos que o item (ii) da definição acima faz sentido, pois, como consequência da Proposição 3.1.1, temos que para $P'|P$ existe um homomorfismo canônico injetivo de $F_P = \mathcal{O}_P/P$ em $F_{P'} = \mathcal{O}_{P'}/P'$ dado por

$$x(P) \longmapsto x(P') \quad \text{para cada} \quad x \in \mathcal{O}_P.$$

Logo, podemos considerar F_P como um subcorpo de $F_{P'}$.

Proposição 3.1.2. *Sejam F'/K' é uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$. Então*

i) $f(P'|P) < \infty \Leftrightarrow [F' : F] < \infty$.

ii) Se F''/K'' é uma extensão algébrica de F'/K' e $P'' \in \mathbb{P}_{F''}$ uma extensão de $P' \in \mathbb{P}_{F'}$, então

$$e(P''|P) = e(P''|P') \cdot e(P'|P),$$
$$f(P''|P) = f(P''|P') \cdot f(P'|P).$$

Demonstração. i) Consideremos as inclusões $K \subseteq F_P \subseteq F'_{P'}$ e $K \subseteq K' \subseteq F'_{P'}$, onde $[F_P : K] < \infty$ e $[F'_{P'} : K'] < \infty$. Portanto $[F'_{P'} : F_P] < \infty$ se, e somente se, $[K' : K] < \infty$. Logo pelo item (ii) do Lema 3.1.1, temos que $[F'_{P'} : F_P] < \infty$ se, e somente se, $[F' : F] < \infty$.

ii) Como $v_{P'}(x) = e(P'|P).v_P(x)$, para todo $x \in F$ e $v_{P''}(y) = e(P''|P).v_{P'}(y)$, para todo $y \in F$. Assim temos $v_{P''}(x) = e(P''|P) \cdot e(P'|P)$, para todo $x \in F$, consequentemente $e(P''|P) = e(P''|P') \cdot e(P'|P)$. A outra parte segue do fato de termos $F_P \subseteq F'_{P'} \subseteq F''_{P''}$.

✓

Lema 3.1.2. *Sejam F'/K' é uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$. Então existe $0 \neq z \in F$, com $v_{P'}(z) \neq 0$.*

Demonstração. Suponhamos que o Lema seja falso. Escolhamos $t \in F'$ com $v_{P'}(t) > 0$. Como F'/F é uma extensão algébrica, existe um polinômio

$$c_n t^n + c_{n-1} t^{n-1} + \ldots + c_1 t + c_0 = 0, \text{ onde } c_i \in F, c_0 \neq 0 \text{ e } c_n \neq 0.$$

Por hipótese, temos que

$$v_{P'}(c_o) = 0 \text{ e } v_{P'}(C_i t^i) = v_{P'}(c_i) + i v_{P'}(t) > 0,$$

para cada $i = 1, 2, \ldots, n$, e pelo Lema da Desigualdade Estrita (Lema 1.1.2), obtemos

$$v_{P'}(c_n t^n + \ldots + c_1 t + c_0) = 0,$$

o que é uma contradição. ✓

Proposição 3.1.3. *Seja F'/K' é uma extensão algébrica de F/K.*

i) Para cada lugar $P' \in \mathbb{P}_{F'}$, existe exatamente um lugar $P \in \mathbb{P}_F$ tal que $P'|P$, mais precisamente $P = P' \cap F$.

ii) Reciprocamente, para cada lugar $P \in \mathbb{P}_F$ existe pelo menos uma extensão e, no máximo, um número finito de extensões $P' \in \mathbb{P}_{F'}$.

Demonstração. i) Definamos $\mathcal{O} = \mathcal{O}_{P'} \cap F$ e $P = P' \cap F$.

Primeiro mostremos que $\mathcal{O}$ é um anel de valorização de F/K. De fato, notemos que $K \subseteq K' \subseteq \mathcal{O}_{P'}$ e $K \subseteq F$ e portanto $K \subseteq \mathcal{O}_{P'} \cap F \subseteq F$, ou seja, $K \subseteq \mathcal{O} \subseteq F$.

Vemos que, $K \subsetneq \mathcal{O}$. Com efeito, pelo Lema 3.1.2, existe $0 \neq z \in F$, com $v_{P'}(z) \neq 0$. Assim $z^{-1} \in F$ e $v_{P'}(z) > 0$ ou $v_{P'}(z^{-1}) > 0$. Isso nos dá que $z \in \mathcal{O}_{P'}$ ou $z^{-1} \in \mathcal{O}_{P'}$, ou seja, $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$ e, pela Definição 1.1.4, temos que $z, z^{-1} \notin K$. Isto implica que $K \subsetneq \mathcal{O}$. Por outro lado, tomando o mesmo elemento z acima, temos que $z \in F \setminus \mathcal{O}$ ou $z^{-1} \in F \setminus \mathcal{O}$, assim $\mathcal{O} \subsetneq F$. Podemos então concluir que $K \subsetneq \mathcal{O} \subsetneq F$.

Agora, seja $x \in F$ tal que $x \notin \mathcal{O}$. Então, $x \notin \mathcal{O}_{P'}$, donde $v_{P'}(x) < 0$. Mas isso implica que $x \neq 0$ e $v_{P'}(x^{-1}) > 0$, logo $x^{-1} \in \mathcal{O}_{'P} \cap F = \mathcal{O}$.

Portanto, $\mathcal{O}$ é um anel de valorização de F/K.

Agora, $P = \mathcal{O} \setminus \mathcal{O}^* = P' \cap F$ é o lugar associado ao anel de valorização $\mathcal{O}$, pois $x \in \mathcal{O}^*$ se, e somente se, $x \in F$ e $x \in \mathcal{O}^*_{P'}$.

Além disso, a unicidade do lugar P segue da Proposição 3.1.1.

ii) Seja P um lugar de F/K. Escolhamos $x \in F \setminus K$ de tal forma que seu único zero seja P (a existência deste lugar decorre da Proposição 1.5.3).

Afirmamos que, para cada $P' \in \mathbb{P}'_F$

$$P'|P \text{ se, e somente se, } v_{P'}(x) > 0.$$

Se $P'|P$, então $v_{P'}(x) = e(P'|P)v_P(x) > 0$. Reciprocamente, se $v_{P'}(x) > 0$, seja $Q \in \mathbb{P}_F$ tal que $P'|Q$. Então $v_Q(x) = e(P'|P)^{-1}v_{P'}(x) > 0$. Portanto $P = Q$, pois P é o único zero de x.

Da afirmação acima decorre o resultado desejado, pois x possui no mínimo um e no máximo um número finito de zeros.

✓

Definição 3.1.4. *Seja F'/K' é uma extensão algébrica de F/K. Para cada lugar $P \in \mathbb{P}_F$ definimos sua conorma com respeito a F'/F como*

$$Con_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P'.$$

A função conorma tem uma extensão a um homomorfismo de $Div(F)$ em $Div(F')$ definindo

$$Con_{F'/F}(P)\left(\sum n_P \cdot P\right) := \sum n_P \cdot Con_{F'/F}(P).$$

Proposição 3.1.4. *Seja F'/K' uma extensão algébrica de F/K. Para $0 \neq x \in F$ se $(x)_0^F, (x)_\infty^F, (x)^F, (x)_0^{F'}, (x)_\infty^{F'}, (x)^{F'}$ denotam os divisores de zero, polos e divisor principal de x em $Div(F)$ e $Div(F')$ respectivamente, então*

$$Con_{F'/F}((x)_0^F) = (x)_0^{F'},\ Con_{F'/F}((x)_\infty^F) = (x)_\infty^{F'},\ \text{e } Con_{F'/F}((x)^F) = (x)^{F'}.$$

Demonstração. Aplicando a definição de divisor principal de x, obtemos que

$$\begin{aligned}
(x)^{F'} &= \sum_{P' \in \mathbb{P}_{F'}} v_{P'}P' \\
&= \sum_{P \in \mathbb{P}_F} \sum_{P'|P} v_P(x)P \\
&= \sum_{P \in \mathbb{P}_F} v_P(x) Con_{F'/F}(P) \\
&= Con_{F'/F}\left(\sum_{P \in \mathbb{P}_F} v_P(x)P\right) \\
&= Con_{F'/F}\left((x)^F\right),
\end{aligned}$$

onde a segunda igualdade segue das Proposições 3.1.1 e 3.1.3. O resultado para os divisores polos e divisores zeros decorre das partes positiva e negativa do divisor principal. ✓

Lema 3.1.3. *Se K'/K é uma extensão finita e x é um elemento transcendente sobre K. Então,*

$$[K'(x) : K(x)] = [K' : K].$$

Demonstração. Como K'/K é uma extensão finita, então existem elementos $\alpha_1, \alpha_2, \ldots, \alpha_s \in K'$ tais que $K' = K(\alpha_1, \alpha_2, \ldots, \alpha_s)$.

Assumamos que $K' = K(\alpha)$, $\alpha \in K'$. Assim temos que $K'(x) = K(\alpha)(x) = K(x)K(\alpha)$ o que implica que

$$[K'(x) : K(x)] = \deg(irr(\alpha, K(x))) \leq \deg(irr(\alpha(\alpha, K))) = [K' : K],$$

já que $irr(\alpha, K) \in K[T] \subseteq K(x)[T]$.

Para provar a outra desigualdade basta mostrar que $irr(\alpha, K)$ é um polinômio irredutível sobre $K(x)$. Suponhamos que $irr(\alpha, K)$ é redutível, isto é, $irr(\alpha, K) = g(T)h(T)$, onde $g(T)h(T) \in K(x)[T]$ e são polinomios mônicos, tais que

$$1 \leq \deg(g(T)), \deg(h(t)) < \deg(irr(\alpha, K)).$$

Como $irr(\alpha, K)(\alpha) = 0$, sem perda de generalidade, temos que $g(\alpha) = 0$. Escrevendo

$$g(T) = T^r + \frac{c_{r-1}(x)}{d_{r-1}(x)}T^{r-1} + \ldots + \frac{c_0(x)}{d_0(x)},$$

onde $c_i(x), d_i(x) \in K[x]$ e $r < \deg(irr(\alpha, K))$, isto implica que

$$\alpha^r + \frac{c_{r-1}(x)}{d_{r-1}(x)}\alpha^{r-1} + \ldots + \frac{c_0(x)}{d_0(x)} = 0.$$

Ainda, multiplicando a última igualdade pelo *m.m.c.* de $d_i(x)$, $i = 1, \ldots, r-1$, obtemos que

$$g_r(x)\alpha^r + \ldots + g_1(x)\alpha + g_0(x) = 0,$$

para certos $g_i(x) \in K[x]$ com $i = 1, \ldots, r$. Ainda podemos supor que nem todos os $g_i(x)$ são divisíveis por x. Fazendo $x = 0$, obtemos um polinômio não trivial para α sobre K com grau menor do que $\deg(irr(\alpha, K))$, o que claramente é uma contradição. ✓

Teorema 3.1.1 (Igualdade Fundamental)**.** *Sejam F'/K' uma extensão algébrica finita de F/K, $P \in \mathbb{P}_F$ e $P_1, P_2, \ldots, P_m$ todos os lugares de F'/K' que são extensões de P. Sejam $e_i = e(P_i|P)$ e $f_i = f(P_i)|P$. Então,*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

Demonstração. Pela Proposição 1.5.3, podemos escolher $x \in F$ tal que P seja o único zero de x em F/K. Sejam $r = v_P(x) > 0$. Então pela Afirmação feita na prova da Proposição

3.1.3 item (ii), para cada $P' \in \mathbb{P}'_F$ $P'|P$ se, e somente se, $v_{P'}(x) > 0$, temos que, os lugares $P_1, \ldots, P_m \in \mathbb{P}_F$ são exatamente os zeros de x em F'/K'.

Temos que

$$\begin{aligned}
[F' : K(x)] =& [F' : K'(x)][K'(x) : K(x)] \\
=& \left(\sum_{i=1}^{m} v_{P_i} \deg(P_i) \right) [K' : K] \\
=& \left(\sum_{i=1}^{m} e_i v_P(x) [F'_{P_i} : K'] \right) [K' : K] \\
=& \left(\sum_{i=1}^{m} e_i v_P(x) [F'_{P_i} : K'][K' : K] \right) \\
=& \left(\sum_{i=1}^{m} e_i v_P(x) [F'_{P_i} : K] \right) \\
=& v_P(x) \left(\sum_{i=1}^{m} e_i [F'_{P_i} : F_P][F_P : K] \right) \\
=& r \deg(P) \sum_{i=1}^{m} e_i f_i.
\end{aligned}$$

Onde a segunda igualdade decorre do Teorema 1.3.1 e o Lemma 3.1.3. Por outro lado, $[F' : K(x)] = [F' : F][F : K(x)] = [F' : F] r \deg(P)$ pois $(x)_0^F = rP$. Assim,

$$[F' : F] = \sum_{i=1}^{m} e_i f_i.$$

✓

Corolário 3.1.1. *Se F'/K' é uma extensão algébrica finita de F/K e $P \in \mathbb{P}_F$, então temos que*

i) $|\{P' \in \mathbb{P}_F \mid P' \text{ é uma extensão de } P\}| \leq [F' : F]$.

ii) Se $P' \in \mathbb{P}_F$ é uma extensão de P, então $e(P'|P) \leq [F' : F]$ e $f(P'|P) \leq [F' : F]$.

Definição 3.1.5. *Se F'/K' é uma extensão de F/K de grau $[F' : F] = n$ e $P \in \mathbb{P}_F$.*

i) P se decompõe totalmente em F'/F se existem exatamente n lugares distintos $P' \in \mathbb{P}_{F'}$ tais que $P'|P$.

ii) P é totalmente ramificado em F'/F se existe um lugar $P' \in \mathbb{P}_{F'}$ com $P'|P$ e $e(P'|P) = n$.

Observação 3.1.1. *Notemos que pelo Teorema da Igualdade Fundamental (Teorema* 3.1.1*), temos que se $P \in \mathbb{P}_F$ decompõe completamente em F'/F se, e somente se, $e(P'|P) = f(P'|P) = 1$, para todos os lugares $P'|P$ em F. Se P é totalmente ramificado em F'/F, então existe um único lugar $P' \in \mathbb{P}_{F'}$ com $P'|P$.*

Proposição 3.1.5. *Sejam F/K um corpo de funções e o polinômio*

$$\varphi(T) = a_n T^n + \ldots + a_1 T + a_0 \quad \textit{onde } a_i \in F.$$

Suponha que existe um lugar $P \in \mathbb{P}_F$ tal que cumpre uma das seguintes condições

i) $v_P(a_n) = 0$, $v_P(a_1) \geq v_P(a_0) > 0$ *para* $i = 1, 2, \ldots, n-1$ *e* $m.d.c.(n, v_P(a_0)) = 1$.

ii) $v_P(a_n) = 0$, $v_P(a_i) \geq 0$ *para* $i = 1, 2, \ldots, n-1$, $v_P(a_0) < 0$ *e* $m.d.c.(n, v_P(a_0)) = 1$.

Então $\varphi(T)$ é irredutível em $F[T]$. Se $F' = F(y)$ onde y é uma raiz de $\varphi(T)$ então P tem uma única extensão $P' \in \mathbb{P}_F$ tal que $e(P'|P) = n$ e $f(P'|P) = 1$, isto é, P é totalmente ramificado em $F(y)/F$.

Demonstração. Consideremos a extensão de corpos $F' = F(y)$ onde $\varphi(y) = 0$. O grau de F'/F é $[F' : F] \leq \deg \varphi(T) = n$, onde vale a igualdade se, e somente se, $\varphi(T)$ é irredutível sobre $F[T]$. Escolhendo uma extensão $P' \in \mathbb{P}_{F'}$ de P, como $\varphi(y) = 0$, então

$$-a_n y^n = a_0 + a_1 y + \ldots + a_{n-1} y^{n-1}. \tag{3.1}$$

Primeiro assumamos (i). Sejam $v'_P(a_n) = 0$ e $v'_P(a_i) > 0$ para $i = 1, \ldots, n-1$, além disso notemos que $v'_P(y) > 0$. Definamos $e := e(P'|P)$, temos que

$$v'_P(a_0) = e \cdot v_P(a_0) \text{ e } v'_P(a_i y^i) = e \cdot v_P(a_i) + i \cdot v'_P(y) > e \cdot v_P(a_0)$$

para cada $i = 1, \ldots, n-1$. Logo, pela Desigualdade Triangular (Lema 1.1.2) em (3.1) obtemos

$$n \cdot vP'(y) = e \cdot v_P(a_0).$$

Como por hipótese $m.d.c(n, v_P(a_0)) = 1$, conclui-se que $n|e$ e portanto $n \leq e$. Por outro lado, pelo Corolário 3.1.1, temos que $e \leq [F' : F] \leq n$. Assim, obtemos

$$n = e = [F' : F].$$

Finalmente o item (i) decorre do Teorema 3.1.1 e a igualdade acima. A prova do item (ii) é análoga ao item (i). ✓

Proposição 3.1.6. *Se $\varphi(T) = T^n + f_{n-1}(x)T^{n-1} + \ldots + f_0(x) \in K(x)[T]$ o polinômio irredutível sobre o corpo de funções racionais $K(x)$. Considere o corpo de funções $K(x, y)/K$, onde y satisfaz a equação $\varphi(y) = 0$, e o elemento $\alpha \in K$ tal que $f_j(\alpha) \neq \infty$ para cada, $0 \leq j \leq n-1$. Denotemos por $P_\alpha \in \mathbb{P}_{K(x)}$ o zero de $x - \alpha$ em $K(x)$. Suponha que o polinômio*

$$\varphi_\alpha(T) := T^n + f_{n-1}(\alpha)T^{n-1} + \ldots + f_0(\alpha) \in K[T]$$

tem a seguinte decomposição no anel de polinômios $K[T]$:

$$\varphi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T),$$

onde $\psi_i(T) \in K[T]$ são polinômios mônicos irredutíveis dois a dois distintos. Então

i) Para cada $i = 1, 2, \ldots, r$ existe um lugar unicamente determinado $P_i \in \mathbb{P}_{K(x,y)}$ tal que $x - \alpha \in P_i$ e $\psi(y) \in P_i$. O elemento $x - \alpha$ é um elemento primo de P_i, isto é, $e(P_i|P_\alpha) = 1$, e o corpo de classe residual de P_i é um K-isomorfismo sobre $K[T]/(\psi_i(T))$. Consequentemente, $f(P_i|P_\alpha) = \deg(\psi_i(T))$.

ii) Se $\deg(\psi_i(T)) = 1$ para pelo menos um $i \in \{1, 2, \ldots, r\}$, então K é algebricamente fechado sobre $K(x, y)$.

iii) Se $\varphi_\alpha(T)$ tem $n = \deg(\varphi(T))$ raízes distintas $\beta \in K$, então existe para cada β tal que $\varphi_\alpha(\beta) = 0$ um único lugar $P_{\alpha,\beta} \in \mathbb{P}_{K(x,y)}$ tal que

$$x - \alpha \in P_{\alpha,\beta} \quad e \quad y - \beta \in P_{\alpha,\beta},$$

onde $P_{\alpha,\beta}$ é um lugar de $K(x, y)$ de grau um.

Demonstração. A prova encontra-se em [15] Corolário 3.3.8. ✓

3.2 O DIFERENCIAL

Ao longo desta subseção F'/F representará uma extensão finita separável, onde F'/K' e F/K são corpos de funções algébricas com corpos de constantes K' e K respectivamente.

Definição 3.2.1. *Seja R um subanel de F/K.*

i) Um elemento $z \in F$ é dito integral sobre R se $f(z) = 0$ para algum polinômio mônico $f(T) \in R[T]$, isto é, se existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

$$z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0.$$

Uma tal equação é chamada equação integral para z sobre R.

ii) O conjunto $ic_F(R) = \{z \in F \mid z \text{ é integral sobre } R\}$ é chamado fecho integral de R em F.

iii) Seja $F_0 \subseteq F$ o corpo de frações de R. O anel R é chamado integralmente fechado se $ic_{F_0}(R) = R$, isto é, todo elemento $z_0 \in F$ que é integral sobre R pertence a R.

Definição 3.2.2. *Sejam $P \in \mathbb{P}_F$ e $\mathcal{O}'_P := ic_{F'}(\mathcal{O}_P)$. Então, o conjunto*

$$\mathcal{C}_P := \{z \in F' \mid Tr_{F'/F}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

é chamado o módulo complementar sobre $\mathcal{O}_P$.

Definição 3.2.3. *Sejam $P \in \mathbb{P}_F$ um lugar e $\mathcal{O}'_P$ o fecho integral de $\mathcal{O}_P$ em F'. Seja $\mathcal{C} = t \cdot {}'O_P$ o módulo complementar sobre $\mathcal{O}_P$. Então, definimos para $P'|P$ o expoente diferencial de P' sobre P como $d(P'|P) := -v_{P'}(t)$.*

Teorema 3.2.1. *Suponha que $F' = F(y)$ é uma extensão finita separável do corpo F de grau $[F' : F] = n$. Seja $P \in \mathbb{P}_F$ tal que o polinômio minimal $\varphi(T)$ de y sobre F tem coeficientes em $\mathcal{O}_P$ e se $P_1, P_2, \ldots, P_r \in \mathbb{P}_{F'}$ são todas as extensões de P. Então*

i) $d(P_i|P) \leq v_{P_i}(\varphi'(y))$ para cada $1 \leq i \leq r$.

ii) $\{1, y, y^2, \ldots y^{n-1}\}$ é uma base inteira de F'/F para o lugar P se, e somente se, $d(P_i|P) = v_{P_i}(\varphi'(y))$ para cada $1 \leq i \leq r$, onde $\varphi'(T)$ denota a derivada de $\varphi(T)$ no anel de polinômios $F'[T]$.

Demonstração. Ver Proposição 3.5.10, [15]. ✓

3.3 EXTENSÕES CICLICAS DO CORPO DE FUNÇÕES RACIONAIS

Estudaremos agora o corpo de funções $F = K(x, y)$ definido pela equação

$$y^n = a \prod_{i=1}^{s} p_i(x)^{n_i}, \tag{3.2}$$

onde $s > 0$, $p_i(x) \in K[x]$ são polinômios mônicos irredutíveis dois a dois distintos, $0 \neq a \in K$ e $0 \neq n_i\mathbb{Z}$. Além disso vamos considerar as seguintes condições até o final da seção.

$$char(k) \nmid n \text{ e } m.d.c.(n, n_i) = 1 \text{ para } 1 \leq i \leq s. \tag{3.3}$$

Definição 3.3.1. *Uma extensão cíclica é uma extensão de Galois onde o grupo de Galois é cíclico.*

Proposição 3.3.1. *Suponhamos que $F = K(x, y)$ seja como definido em (3.2) e (3.3). Então*

i) K é um corpo algébricamente fechado em F e $[F : K(x)] = n$. Se K contém uma raiz primitiva da unidade, então $F/K(x)$ é uma extensão de corpos cíclica.

ii) Se P_i e P_∞ denotam um zero de $p_i(x)$ e um polo de x, respectivamente, em $K(x)$, então os lugares $P_1, \ldots, P_s$ são totalmente ramificados em $F/K(x)$. Alem disso, todos os lugares $Q_\infty \in \mathbb{P}_F$ onde $Q_\infty | P_\infty$ tem índice de ramificação $e(Q_\infty|P_\infty) = n/d$ onde

$$d := m.d.c. \left(n, \sum_{i=1}^{s} n_i \deg(p_i(x)) \right).$$

E Não existem lugares além de $P_1, \ldots, P_s, P_\infty$ ramificados em $F/K(x)$.

iii) O gênero de F/K é

$$g = \frac{n-1}{2} \left(-1 + \sum_{i=1}^{s} \deg(p_i(x)) \right) - \frac{d-1}{2},$$

onde d é definido como no item (ii).

Demonstração. Ver Proposição 6.3.1, [15]. ✓

Exemplo 3.3.1. *Seja $F = K(x, y)$ onde*

$$y^n = \frac{x^m - b}{x^m - c},$$

com $b, c \in K \setminus \{0\}$, $b \neq c$ e $char(K) \nmid mn$.

Claramente, este corpo de funções cumpre as hipóteses da Proposição 3.3.1*, onde $n_1 = 1$, $n_2 = -1$, $p_1(x) = x^m - b$ e $p_2(x) = x^m - c$.*

Assim, do item (i) temos que $[F : K(x)] = n$. Por outro lado do item (ii) obtemos

$$\begin{aligned} d :&= m.d.c \left(n, \sum_{i=1}^{2} n_i \deg(p_i(x)) \right) \\ &= m.d.c.(n, (1)m + (-1)m) = n \end{aligned}$$

Finalmente o item (iii) implica em

$$\begin{aligned} g &= \frac{n-1}{2} \left(-1 + \sum_{i=1}^{s} \deg(p_i(x)) \right) - \frac{d-1}{2} \\ &= \frac{n-1}{2}(-1 + 2m) - \frac{n-1}{2} \\ &= (n-1)(m-1) \\ &= ([F : K(x)] - 1)\,(m-1). \end{aligned}$$

Notemos que $K(y, x) \cong K(x, y) = F$. Então, tomando $F = K(x, y)$ onde

$$x^m = \frac{y^n - b}{y^n - c},$$

com $b, c \in K \setminus \{0\}$, $b \neq c$ *e* $char(K) \nmid mn$, *temos que* $[F : K(y)] = m$. *Consequentemente,*

$$g = ([F : K(x)] - 1)([F : K(y)] - 1).$$

Proposição 3.3.2. *Consideremos o corpo de funções* $F = K(x, y)$ *onde*

$$y^q + \mu y = f(x) \in K[x],$$

com $p = char(K)$, $q = p^s > 1$ *e* $0 \neq \mu \in K$. *Suponha que* $\deg(f) := m > 0$ *e todas as raízes de* $T^q + \mu T = 0$ *são elementos de* K. *Então*

i) $[F : K(x)] = q$ *e* K *é um corpo algebricamente fechado em* F.

ii) $F/K(x)$ *é de Galois. O conjunto* $A := \{\gamma \in K \mid \gamma^q + \mu\gamma = 0\}$ *é um subgrupo de ordem* q *do grupo aditivo de* K. *Para cada* $\sigma \in Gal(F/K(x))$ *existe um único* $\gamma \in A$ *tal que* $\sigma(y) = y + \gamma$, *e o mapa*

$$\begin{array}{ccc} Gal(F/K(x)) & \longrightarrow & A \\ \sigma & \longmapsto & \gamma \end{array}$$

é um isomorfismo.

iii) O polo $P_\infty \in \mathbb{P}_{K(x)}$ *de* x *em* $K(x)$ *tem uma única extensão* $Q_\infty \in \mathbb{P}_F$, *e* $Q_\infty | P_\infty$ *é totalmente ramificada, isto é,* $e(Q_\infty | P_\infty) = q$. *Consequentemente,* Q_∞ *é um lugar de grau um de* F/K.

iv) P_∞ *é o único lugar de* $K(x)$ *que se ramifica em* $F/K(x)$.

v) O gênero de F/K *é* $g = (q-1)(m-1)/2$.

vi) O divisor do diferencial dx *é* $(dx) = (2g-2)Q_\infty = ((q-1)(m-1)-2)Q_\infty$.

vii) Os divisores polo de x *e* y *são* $(x)_\infty = qQ_\infty$ *e* $(y)_\infty = mQ_\infty$ *respectivamente.*

viii) Se $r \geq 0$, *então os elementos* $x^i y^j$ *onde* $0 \leq i$, $0 \leq j \leq q-1$ *e* $qi + mj \leq r$ *são uma base de* $r\mathcal{L}(Q_\infty)$ *sobre* K.

ix) Cada $\alpha \in K$ *satisfaz um dos seguintes casos*

1. *A equação* $T^q + \mu T = f(\alpha)$ *tem* q *raízes distintas em* K.
2. *A equação* $T^q + \mu T = f(\alpha)$ *não tem raízes em* K.

No primero caso, para cada β *tal que* $\beta^q + \mu\beta = f(\alpha)$, *existe um único lugar* $P_{\alpha,\beta} \in \mathbb{P}_F$ *tal que* $P_{\alpha,\beta} | P_\alpha$ *e* $y(P_{\alpha,\beta}) = \beta$.

No segundo caso, todas as extensões de P_α *em* F *são de grau maior do que um.*

Demonstração. Ver Proposição 6.4.1, [15]. ✓

Proposição 3.3.3. *Se t é um elemento de F tal que $v_{P_i}(t) = 1$ para $i = 1, 2, \ldots, n$, então*

i) O diferencial $\eta := dt/t$ satisfaz $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$ para cada $i = 1, 2, \ldots, n$.

ii) $C_\Omega(D, G) = C_\mathcal{L}(D, D - G + (dt) - (t))$.

Demonstração. Ver Proposição 6.1.2, [15]. ✓

3.4 CORPO DE FUNÇÕES HERMITIANO

Definição 3.4.1. *O corpo de funções $F/\mathbb{F}_q$ de gênero g é dito maximal se*

$$N = q + 1 + 2gq^{1/2},$$

onde N é o número de lugares em F de grau um, ou seja, $N := |\{P \in \mathbb{P}_F \mid \deg(P) = 1\}|$.

Definição 3.4.2. *Seja $\mathbb{F}_{q^2}$ um corpo finito. O corpo de funções $H = \mathbb{F}_{q^2}(x, y)$ definido como*

$$H = \mathbb{F}_{q^2}(x, y) \quad \textit{onde} \quad y^q + y = x^{q+1},$$

é dito o corpo de funções Hermitiano $H/\mathbb{F}_{q^2}$ sobre $\mathbb{F}_{q^2}$.

Notemos que, da Proposição 3.3.2, itens (v) e (vi), o gênero g e o divisor do diferencial dx do corpo de função Hermitiano são, respectivamente,

$$g = \frac{q(q-1)}{2} \quad \text{e} \quad (dx) = (q(q-1) - 2)Q_\infty,$$

onde Q_∞ é o divisor polo comum de x e y tal que $(x)_\infty = qQ_\infty$ e $(y)_\infty = (q+1)Q_\infty$. Ainda, novamente pela Proposição 3.3.2, itens (iii) e (ix), os lugares de grau um de $H/\mathbb{F}_{q^2}$ são como segue:

i) O lugar Q_∞.

ii) Extensões de algum lugar $P_\alpha \in \mathbb{P}_{\mathbb{F}_{q^2}(x)}$. Logo, temos que contar os elementos $\alpha \in \mathbb{F}_{q^2}$ tais que a equação

$$T^q + T = \alpha^{q+1} \tag{3.4}$$

tem raízes $\beta \in \mathbb{F}_{q^2}$. Sabemos que a aplicação traço

$$\begin{array}{ccc} \mathbb{F}_{q^2} & \longrightarrow & \mathbb{F}_q \\ \beta & \longmapsto & \beta^q + \beta \end{array}$$

é uma aplicação sobrejetora. Logo, a equação (3.4) tem raízes em $\mathbb{F}_{q^2}$ se, e somente se, $\alpha^{q+1} \in \mathbb{F}_{q^2}$. Seja $u^* \subset \mathbb{F}_{q^2}^*$ o subgrupo de ordem $(q-1)(q+1)$. Então, para $\alpha \in \mathbb{F}_{q^2}$ temos que

$$\alpha^{q+1} \in \mathbb{F}_q \Leftrightarrow \alpha \in u^* \cup \{0\} = u.$$

Assim, temos que o numero $q|u|$ representa a quantidade de lugares de grau um distintos de Q_∞.

Portanto, o número de lugares de grau um em $H/\mathbb{F}_{q^2}$ é

$$N = q|u| + 1 = q^3 + 1.$$

Ainda, como o gênero de $H/\mathbb{F}_{q^2}$ é $g = q(q-1)/2$, então, o corpo de funções Hermitiano satisfaz a Definição 3.4.1 pois

$$\begin{aligned} q^2 + 1 + 2g\left(q^2\right)^{1/2} &= q^2 + 1 + 2\left(\frac{q(q-1)}{2}\right)q \\ &= 1 + q^3 \\ &= N. \end{aligned}$$

Assim, $H/\mathbb{F}_{q^2}$ é um corpo de função maximal.

Sejam agora $P_{\alpha,\beta}$ os zeros comuns de $x-\alpha$ e $y-\beta$ sempre que $\alpha \in u$, $\beta \in \mathbb{F}_{q^2}$ tais que $\beta^q + \beta = \alpha^{q+1}$. Para qualquer $\alpha, \beta \in \mathbb{F}_{q^2}$ os divisores de $x-\alpha$ e $y-\beta$ são

$$(x-\alpha) = \begin{cases} \sum\limits_{\substack{\beta \in \mathbb{F}_{q^2} \\ \beta^q+\beta=\alpha^{q+1}}} P_{\alpha,\beta} - qQ_\infty & \text{se } \alpha \in u \\ R_\alpha - qQ_\infty & \text{se } \alpha \in K \setminus u \end{cases}$$

onde R_α é um divisor de grau q em $H/\mathbb{F}_{q^2}$ dependendo de α tal que $supp(R_\alpha)$ não contém nenhum lugar de grau um e

$$(y-\beta) = \begin{cases} (q+1)P_{\alpha,\beta} - (q+1)Q_\infty & \text{se } \beta^q + \beta = 0 \\ \sum\limits_{\substack{\alpha \in K \\ \beta^q+\beta=\alpha^{q+1}}} P_{\alpha,\beta} - (q+1)Q_\infty & \text{se } \beta^q + \beta \neq 0 \end{cases}$$

Isto implica que, para cada $\alpha \in \mathbb{F}_{q^2}$, existem q elementos $\beta \in \mathbb{F}_{q^2}$ tais que $\beta^q + \beta = \alpha^{q+1}$ e, para cada par (α, β), existe um único lugar $P_{\alpha,\beta} \in \mathbb{P}_H$ de grau um com $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$.

Finalmente, a construção feita até agora e a Proposição 3.3.2, item (*viii*), mostram o seguinte Lema.

Lema 3.4.1. *O corpo de funções Hermitiano sobre* $\mathbb{F}_{q^2}$

$$H = \mathbb{F}_{q^2}(x, y) \quad onde \quad y^q + y = x^{q+1}$$

cumpre com as seguintes propriedades:

i) O gênero de H *é* $g = q(q-1)/2$.

ii) H *tem* $q^3 + 1$ *lugares de grau um sobre* $\mathbb{F}_{q^2}$*, a saber,*

1. *O polo* Q_∞ *comum de* x *e* y.
2. *Para cada* $\alpha \in \mathbb{F}_{q^2}$ *existem* q *elementos* $\beta \in \mathbb{F}_{q^2}$ *tais que* $\beta^q + \beta = \alpha^{q+1}$*, e para cada par* (α, β)*, existe um único lugar* $P_{\alpha,\beta} \in \mathbb{P}_H$ *de grau um com* $x(P_{\alpha,\beta}) = \alpha$ *e* $y(P_{\alpha,\beta}) = \beta$.

iii) $H/\mathbb{F}_{q^2}$ *é um corpo de funções maximal.*

iv) O divisor do diferencial dx *é* $(dx) = (q(q-1) - 2)Q_\infty$.

v) Para $m \geq 0$*, os elementos* $x^i y^j$ *com* $0 \leq i$*,* $0 \leq j \leq q-1$ *e* $iq + j(q+1) \leq m$ *são uma base de* $\mathcal{L}(mQ_\infty)$.

vi) Os divisores polo de x *e* y *são* $(x)_\infty = qQ_\infty$ *e* $(y)_\infty = (q+1)Q_\infty$ *respectivamente.*

Proposição 3.4.1. *O corpo de funções Hermitiano sobre* $\mathbb{F}_{q^2}$ *definido como*

$$H = \mathbb{F}_{q^2}(x, y) \quad onde \quad y^q + y = x^{q+1}$$

pode ser representado por $\mathbb{F}_{q^2}(u, v)$ *onde* $u^{q+1} + v^{q+1} = 1$.

Demonstração. Sejam $a, b, c \in \mathbb{F}_{q^2}$ em $\mathbb{F}_{q^2}$ com $u^{q+1} + v^{q+1} = 1$ tais que $a^{q+1} = 1$, $b^q + b = 1$ e $c = -ab^q$, temos que

$$\begin{cases} ab^q + c = 0 \\ a^q b + c^q = (ab^q + c)^q = 0 \\ 1 = -a^{q+1}(b + b^q) = a(-a^q b) + a^q(-ab^q) = ac^q + a^q c \end{cases} \tag{3.5}$$

Sejam

$$x = \frac{1}{u + av} \quad \text{e} \quad y = \frac{bu + cv}{u + av} \quad \text{sobre } \mathbb{F}_{q^2}.$$

Então

$$y^q + y = x^{q+1} \Rightarrow (u + av)^{q+1}(y^q + y) = 1.$$

Por outro lado

$$\begin{aligned} 1 = (u+av)^{q+1}(y^q+y) &= (u+av)^{q+1}\left(\frac{bu+cv}{u+av}\right)^q + (u+av)^{q+1}\left(\frac{bu+cv}{u+av}\right) \\ &= u^{q+1}(b^q+b) + u^q v(ab^q+c) + uv^q(c^q+a^q b) + v^{q+1}(ac^q+a^q c) \\ &= u^{q+1} + v^{q+1} \end{aligned}$$

onde a última igualdade decorre de (3.5). ✓

3.5 CÓDIGOS HERMITIANOS

Do Lema 3.4.1, temos que, para cada $\alpha \in \mathbb{F}_{q^2}$, existem q elementos distintos $\beta \in \mathbb{F}_{q^2}$ tais que $\beta^q + \beta = \alpha^{q+1}$. Consequentemente, o número de lugares $P_{\alpha,\beta}$ de grau um é q^3.

Definição 3.5.1. *Para $m \in \mathbb{Z}$, definimos o código*

$$C_m = C_{\mathcal{L}}(D, mQ_\infty) \quad \textit{onde} \quad D = \sum_{\substack{\alpha \in K \\ \beta^q+\beta=\alpha^{q+1}}} P_{\alpha,\beta}$$

é a soma formal dos lugares de grau um, exceto Q_∞, do corpo de funções Hermitiano $H/\mathbb{F}_{q^2}$. O código C_m é dito código Hermitiano.

Notemos que os códigos Hermitiamos tem comprimento q^3 sobre $\mathbb{F}_{q^2}$. Além disso, é claro que, para $r \leq m$ então $C_r \subseteq C_m$.

Observemos alguns casos de códigos Hermitianos. Para $m < 0$ temos que $\deg(mQ_\infty) < 0$ logo, $\mathcal{L}(mQ_\infty) = 0$ e, portanto, $C_m = 0$. Ainda para

$$m > q^3 + q^2 - q - 2 = q^3 + (2g-2),$$

temos que $\deg(mQ_\infty) \geq 2q-1$ e, pelos Teoremas 2.3.1 e 1.5.4, temos que

$$\begin{aligned} \dim(C_m) &= \ell(mQ_\infty) - \ell(mQ_\infty - D) \\ &= (m+1-g) - (m-q^3+1-g) \\ &= q^3 \end{aligned}$$

Consequentemente, $C_m = \mathbb{F}_{q^2}^{q^3}$. Portanto, resta analizar os códigos Hermitianos onde $0 \leq m \leq q^3+q^2-q-2$.

Proposição 3.5.1. *O código dual de C_m é $C_m^\perp = C_{q^3+q^2-q-2-m}$. Ainda, C_m é auto-ortogonal se $2m \leq q^3+q^2-q-2$ e C_m é auto-dual para $m = (q^3+q^2-q-2)/2$.*

Demonstração. Consideremos o elemento $t := \prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha) = x^{q^2} - x$. Pela construção feita do código Hermitiano temos que $(t)_0 = D$. Além disso,

$$\begin{aligned} v_{Q_\infty}(x^{q^2} - x) &= v_{Q_\infty}(x(x^{q^2-1} - 1)) \\ &= Q_\infty(x) + Q_\infty(x^{q^2-1} - 1) \\ &= Q_\infty(x) + \min\{(q^2-1)Q_\infty(x), 0\} \\ &= q^2 Q_\infty(x) \\ &= -q^3, \end{aligned}$$

onde a última igualdade decorre do fato que $(x)_\infty = qQ_\infty$, pelo Lema 3.4.1. Assim $(t)_\infty = q^3 Q_\infty$. Consequentemente, o divisor principal de t é

$$(t) = D - q^3 Q_\infty.$$

Ainda, $dt = d(x^{q^2} - x) = -dx$ e pelo Lema 3.4.1 item (iv) obtemos

$$(dt) = (dx) = (q^2 - q - 2)Q_\infty.$$

Por outro lado, para cada lugar $P_{\alpha,\beta} \in supp(D)$ temos que

$$v_{P_{\alpha,\beta}}(t) = v_{P_{\alpha,\beta}}\left(\prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha)\right) = \sum_{\alpha \in \mathbb{F}_{q^2}} v_{P_{\alpha,\beta}}(x - \alpha) = 1.$$

Assim, pelo Teorema 2.3.3, o item (ii) da Proposição 3.3.3 e as passagens acima concluímos o resultado, pois

$$\begin{aligned} C_m^\perp = C_\Omega(D, mQ_\infty) &= C_{\mathcal{L}}(D, D - mQ_\infty + (dt) - (t)) \\ &= C_{\mathcal{L}}(D, (q^3 + q^2 - q - 2 - m)Q_\infty) \\ &= C_{q^3+q^2-q-2-m}. \end{aligned}$$

✓

Consideremos I o conjunto dos número polo de Q_∞, ou seja,

$$I = \{n \geq 0 \mid \text{existe um elemento } z \in H \text{ tal que } (z)_\infty = nQ_\infty\}.$$

Proposição 3.5.2. *O conjunto dos números polo de Q_∞ satisfaz a seguinte igualdade*

$$I = \{n = iq + (q+1)j \mid i \geq 0, 0 \leq j \leq q-1\}.$$

Demonstração. Primeiro mostremos que $n = iq + (q+1)j$ onde $i \geq 0$ e $0 \leq j \leq q-1$ é um número polo de Q_∞. Seja $z = x^i y^j$ tal que $i \geq 0$ e $0 \leq j \leq q-1$, temos que

$$\begin{aligned} (z)_\infty &= i(x)_\infty + j(y)_\infty \\ &= iqQ_\infty + j(q+1)Q_\infty \quad \text{pelo Lema 3.4.1 item } (vi) \\ &= (iq + (q+1)j)Q_\infty \\ &= nQ_\infty \end{aligned}$$

Daí, n é um número polo de Q_∞.

Agora provemos que I é gerado por q e $q+1$. Seja $\varphi(T) = T^q + T - x^{q+1}$ o polinômio minimal de y sobre $\mathbb{F}_{q^2}$. Como o único lugar que é ramificado em H (Proposição 3.3.2 item (iv)) é Q_∞, pelo Teorema 3.2.1 item (ii), temos que

$$\{y^j \mid 0 \leq j \leq q-1\}$$

é uma base inteira de $H/\mathbb{F}_{q^2}$. Agora se $n \in I$, então existe $z \in H$ tal que $(z)_\infty = nQ_\infty$. Suponhamos que

$$z = \sum_{j=0}^{q-1} z_j y^j \quad \text{onde} \quad z_j \in \mathbb{F}_{q^2}[x].$$

Rescrevendo z como

$$z = \sum_{j=0}^{q-1} \sum_{i \geq 0} a_{ij} x^i y^j \quad \text{com} \quad a_{ij} \in \mathbb{F}_{q^2}.$$

Mas ainda,

$$\begin{aligned} -n = v_{Q_\infty}(z) &= \min\{v_{Q_\infty}(a_{ij}x^i y^j) \mid a_{ij} \neq 0\} \\ &= \min\{v_{Q_\infty}(a_{ij}) + i v_{Q_\infty}(x) + j v_{Q_\infty}(y) \mid a_{ij} \neq 0\} \\ &= \min\{iq + j(q+1)\}, \end{aligned}$$

onde a última igualdade decorre do Lema 3.4.1 item (vi) e da Definição 1.1.4 item (v). Logo, n é uma combinação linear de q e $q+1$. ✓

Proposição 3.5.3. *Sejam $m \geq 0$ e $I(m)$ o conjunto dos números polo de Q_∞ menores do que m, ou seja,*

$$I(m) = \{l \leq m \mid l = iq + j(q+1),\ i \geq 0,\ 0 \leq j \leq q-1\}.$$

Então $\ell(mQ_\infty) = |I(m)|$.

Demonstração. Consideremos a sequência

$$\mathbb{F}_{q^2} = \mathcal{L}(0) \subseteq \mathcal{L}(Q_\infty) \subseteq \mathcal{L}(2Q_\infty) \subseteq \ldots \subseteq \mathcal{L}(mQ_\infty).$$

Pelo Lema 1.3.2, temos que para cada $k \geq 0$, $\ell(kQ_\infty) \leq \ell((k-1)Q_\infty) + 1$. Por outro lado pela consequência da Proposição 1.5.3 e a Definição 1.5.8, temos que $k \geq 0$ é um número polo de Q_∞ se, e somente se,

$$\ell(kQ_\infty) > \ell((k-1)Q_\infty)$$

isto é $\ell(kQ_\infty) \geq \ell((k-1)Q_\infty) + 1$. Consequentemente, temos que

$$\ell(kQ_\infty) = \ell((k-1)Q_\infty) + 1.$$

Mas ainda, como $0 \in I(m)$ e $\ell(0) = 1$ então dimensão da sequência aumenta de acordo com a quantidade de elementos do conjunto $I(m)$, ou seja $\ell(mQ_\infty) = |I(m)|$. ✓

Observação 3.5.1. *Notemos que se* $m > 2g-2$*, então* $\deg(mQ_\infty) \geq 2g-1$*. Assim, pelo Teorema* 1.5.4*, temos que*

$$|I(m)| = \ell(mQ_\infty) = \deg(mQ_\infty) + 1 - g = m + 1 - g.$$

Proposição 3.5.4. *Suponha que* $0 \leq m \leq q^3 + q^2 - q - 2$*. Então*

i) A dimensão de C_m *é dada por*

$$\dim C_m = \begin{cases} |I(m)| & \text{para} \quad 0 \leq m \leq q^3 \\ q^3 - |I(s)| & \text{para} \quad q^3 \leq m \leq q^3 + q^2 - q - 2 \end{cases}$$

onde $s := q^3 + q^2 - q - 2 - m$ *e* $I(m) = \{n \in I \mid n \leq m\}$*.*

ii) Se $q^2 - q - 2 < m < q^3$ *então* $\dim C_m = m + 1 - g$*.*

iii) A distância mínima de C_m *satisfaz* $d \geq q^3 - m$*. Se* $0 \leq m < q^3$*. Além disso, se* m *e* $q^3 - m$ *são números polo de* Q_∞ *então,* $d = q^3 - m$*.*

Demonstração. Lembremos que os códigos Hermitiamos são códigos de comprimento q^3 sobre $\mathbb{F}_{q^2}$.

i) Se $0 \leq m < q^3$, pelo Corolário 2.3.1, temos que

$$\dim C_m = \ell(mQ_\infty) = |I(m)|.$$

Ainda, se $s := q^3 + q^2 - q - 2 - m$ e $q^3 \leq m \leq q^3 + q^2 - q - 2$, notemos que

$$\begin{cases} m \leq q^3 + q^2 - q - 2 & \Rightarrow s \leq 0 \\ q^3 \leq m & \Rightarrow s \leq q^2 - q - 2 < q^3, \end{cases}$$

o que implica que $0 \leq s < q^3$, isto garante que $C_s \subseteq \mathbb{F}_{q^2}^{q^3}$. Por outro lado, como $s = q^3 + q^2 - q - 2 - m$, então, pela Proposição 3.5.1, temos que $C_m^\perp = C_s$. Além disso, pela observação ao início da prova podemos concluir que

$$\begin{aligned} \dim C_m &= q^3 - \dim C_m^\perp \\ &= q^3 - \dim C_s \\ &= q^3 - |I(s)|. \end{aligned}$$

ii) Do Lema 3.4.1, sabemos que o gênero de H é $g = q(q-1)$, donde

$$q^2 - q - 2 = q(q-1) - 2 = 2g - 2.$$

Logo, da hipótese, obtemos $2g - 2 < m < q^3$. Além disso, $m = \deg(mQ_\infty)$. Finalmente, pelo Corolário 2.3.1, obtemos que

$$\dim C_m = \deg(mQ_\infty) + 1 - g = m + 1 - g.$$

iii) A desigualdade $d \geq q^3 - m$ é imediata pelo Teorema 2.3.1. Para provar que $d \leq q^3 - m$ quando m e $q^3 - m$ são números polo de Q_∞, faremos por casos.

Caso 1. Seja $m = q^3 - q^2$. Escolhamos $k = q^2 - q$ elementos distintos $\alpha_1, \alpha_2 \ldots, \alpha_k \in \mathbb{F}_{q^2}$. Pelo item (ii) do Lema 3.4.1, para cada α_i existem q elementos $\beta \in \mathbb{F}_{q^2}$ tais que para cada par (α_i, β) existe um único lugar $P_{\alpha_i,\beta} \in \mathbb{P}_H$ de grau um. Ou seja, P_{α_i} tem q extensões distintas $P_{\alpha_i,\beta}$ em $H/\mathbb{F}_{q^2}(x)$ de grau um para $i = 1, 2 \ldots, q^2 - q$. Logo o elemento $\prod_{i=1}^{k}(x - \alpha_i) \in P_{\alpha_i,\beta}$ para cada $i = 1, 2, \ldots, k$. Portanto, z tem exatamente $qk = q(q^2 - q) = m$ zeros distintos $P_{\alpha_i,\beta}$ de grau um. Além disso como

$$z = x^{q^2-q} + \ldots + \alpha_1\alpha_2 \ldots \alpha_{q^2-q},$$

pelo item (v) do Lema 3.4.1, temos que $z \in \mathcal{L}(mQ_\infty)$. Consequentemente,

$$wt(ev_D(z)) = q^3 - m \Rightarrow d \leq q^3 - m.$$

Caso 2. Seja $m < q^3 - q^2$. Como m é um número polo de Q_∞, podemos escrever $m = iq + j(q+1)$ como $i \geq 0$ e $0 \leq j \leq q-1$. Notemos que se $i > q^2 - q - 1$, então $r \geq q^3 - q^2$, o que seria uma contradição. Assim, $0 \leq i \leq q^2 - q - 1$.

Fixando $0 \neq \gamma \in \mathbb{F}_q$, definimos o conjunto $A = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^{q+1} \neq \gamma\}$. Consequentemente, $|A| = q^2 - (q+1) \geq i$. Escolhemos $\alpha_1, \alpha_2, \ldots, \alpha_i \in A$. Assim o elemento

$$z_1 = \prod_{\nu=1}^{i}(x - \alpha_\nu)$$

possui iq zeros distintos $P_{\alpha,\beta} \leq D$.

Por outro lado, podemos escolher j elementos distintos $\beta_1, \beta_2, \ldots, \beta_j \in \mathbb{F}_{q^2}$ onde $\beta_j^q + \beta_j = \gamma$ e

$$z_2 = \prod_{\mu=1}^{j}(y - \beta_\mu)$$

tem $j(q+1)$ zeros distintos $P_{\alpha\beta} \leq D$.

Além disso, notemos que, pela construção, $\beta_j^q + \beta_j = \gamma \neq \alpha_\nu^{q+1}$, para cada $\nu = 1, 2, \ldots, i$ e $\mu = 1, 2, \ldots, j$, logo os zeros de z_1 e z_2 são todos distintos. Finalmente, e pelos mesmos argumentos do caso 1, temos que o elemento

$$z = z_1 z_2 \in \mathcal{L}((iq + j(q+1))Q_\infty) = \mathcal{L}(mQ_\infty),$$

tem $m = iq + j(q+1)$ zeros distintos $P_{\alpha,\beta} \leq D$. Portanto a palavra código $ev_D(z)$ tem peso $wt(z) = q^3 - m$, consequentemente $d \leq q^3 - m$.

Caso 3. Seja $q^3 - q^2 < m < q^3$. Para $s = q^3 - m$, temos que $0 < s < q^2 \leq q^3 - q^2$ e, por hipótese, s é um número polo de Q_∞. Pelo Caso 2, existe um elemento $z \in H$ com divisor principal $(z) = D' - sQ_\infty$ onde $0 \leq D' \leq D$ e $\deg(D') = s$. Além

disso, o elemento $u := x^{q^2} - x \in H$ tem como divisor principal $(u) = D - q^3 Q_\infty$, consequentemente,

$$\begin{aligned}(z^{-1}u) &= (z^{-1}) + (u) = -(z) + (u) \\ &= -D' + sQ_\infty + D - q^3 Q_\infty \\ &= D - D' - (q^3 - s)Q_\infty \\ &= D - D' - mQ_\infty \\ &\geq -mQ_\infty\end{aligned}$$

Portanto, $z^{-1}u \in \mathcal{L}(mQ_\infty)$ e, assim, a palavra código $ev_D(z^{-1}u) \in C_m$, donde $d \leq q^3 - m$.

✓

A partir das Proposições 1.1.2 e 3.5.3 e do Lema 3.4.1, podemos facilmente obter a matriz geradora do código C_m. Para isto, temos que fixar uma ordem no conjunto

$$T := \{(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid \beta^q + \beta = \alpha^{q+1}\}.$$

Para $s = iq + j(q+1)$ com $i \geq 0$ e $0 \leq j \leq q-1$ definimos o vetor

$$u_s := \left(\alpha^i \beta^j\right)_{(\alpha,\beta)\in T} \in (\mathbb{F}_{q^2})^{q^3}.$$

Obtemos o seguinte resultado:

Teorema 3.5.1. *Suponha que $0 \leq m < q^3$. Se $0 = s_1 < s_2 < \ldots < s_K \leq m$ são números polo de mQ_∞, então a matriz M_m cujas linhas são $u_{s_1}, u_{s_2}, \ldots, u_{s_k}$ é uma matriz geradora do código C_m.*

Demonstração. Pelo item (v) do Lema 3.4.1, os elementos $\{\alpha^i \beta^j\}$ onde $i \geq 0$ e $0 \leq j \leq q-1$ são uma base de $\mathcal{L}(mQ_\infty)$. Logo, como $m < q^3$ então, pelo Corolário 2.3.1, temos que

$$M_m = \begin{pmatrix} u_{S_1} \\ u_{S_2} \\ \vdots \\ u_{S_k} \end{pmatrix}$$

é a matriz geradora do código C_m. ✓

Corolário 3.5.1. *Para $q^2 - q - 2 < m \leq q^3 + q^2 - q - 2$, a matriz $M_{q^3+q^2-q-2-m}$ (definida como no Teorema 3.5.1) é a matriz teste de pariedade de C_m.*

Demonstração. Sabemos que a matriz geradora de $C_m^{\perp}$ é a matriz teste de paridade de C_m, por outro lado da Proposição 3.5.1 sabemos que

$$C_m^{\perp} = C_{q^3+q^2-q-2-m}.$$

Chamemos $m^{\perp} = q^3 + q^2 - q - 2 - m$. Como por hipótese $q^2 - q - 2 < m \leq q^3 + q^2 - q - 2$ isto implica que $0 \leq m^{\perp} < q^3$. E, analogamente ao Teorema 3.5.1, temos que $M_{m^{\perp}}$ é a matriz geradora de $C_{m^{\perp}}$. ✓

Observação 3.5.2. *i) As linhas da matriz M_m também geram o código M_m para $m \geq q^3$. Porem, já não são linearmente independentes. Por exemplo*

$$u_{q^2,0} = \left(\alpha^{q^2}\beta^0\right) = \left(\alpha^{q^2}\right) = (\alpha) = \left(\alpha\beta^0\right) = u_{1,0}.$$

ii) O Teorema 3.5.1 *e o Corolário* 3.5.1 *mostram que é mais conveniente utilizar os geradores x y y de F em vez de u, v (ver Proposição* 3.4.1*) uma vez que as matrizes geradora e teste de paridade podem ser expressadas de maneira muito mais simples.*

4 CÓDIGOS HERMITIANOS GENERALIZADOS

Neste capítulo, generalizaremos alguns resultados obtidos no capítulo 3, calculando distâncias mínimas exatas para alguns valores do conjunto de números polo. Finalmente, empregaremos estes resultados para obter informações sobre os pesos generalizados de Hamming dos códigos Hermitianos generalizados.

4.1 CORPO DE FUNÇÕES HERMITIANO GENERALIZADO

Sejam q uma potência de um número primo p e $\mathbb{F}_{q^r}$ um corpo finito com q^r elementos, onde $r \geq 2$. Definimos o corpo de funções $GH = \mathbb{F}_{q^r}(x, y)$ sobre $\mathbb{F}_{q^r}$ por

$$\sum_{i=0}^{r-1} y^{q^i} = p(x) := x^{1+q} + \ldots + x^{1+q^{r-1}} + x^{q+q^2} + \ldots + x^{q+q^{r-1}} + \ldots + x^{q^{r-2}+q^{r-1}}. \quad (4.1)$$

Notemos que a equação definida acima é equivalente a

$$s_{r,1}\left(y, y^q + \ldots + y^{q^{r-1}}\right) = s_{r,2}\left(x, x^q + \ldots + x^{q^{r-1}}\right), \quad (4.2)$$

onde $s_{r,1}(y)$ e $s_{r,2}(x)$ são o primeiro e o segundo polinômios simétricos em r respectivamente.

No caso $r = 2$, temos o corpo de funções Hermitiano estudado no capítulo 3. Para $r > 2$ obtemos os corpos de funções Hermitianos generalizados [4]. Uma das propriedades básicas do corpo de funções Hermitiano generalizado é a existência de um único divisor polo das funções x e y. No Lema abaixo, apresentamos outras propriedades desse corpo de funções.

Lema 4.1.1. *O corpo de funções Hermitiano generalizado GH sobre $\mathbb{F}_{q^r}$ definido acima possui as seguintes propriedades.*

i) *Gênero $g = q^{r-1}(q^{r-1} - 1)/2$ e $q^{2r-1} + 1$ lugares de grau um.*

ii) $(x)_\infty = q^{r-1}Q_\infty$ *e* $(y)_\infty = (q^{r-1} + q^{r-2})\,Q_\infty$, *onde Q_∞ é o único divisor polo das funções x e y de grau um.*

iii) *Se* $z := x^{q+1} - y^q + y^{q-1}y$, *então* $(z)_\infty = (q^r + 1)Q_\infty$.

iv) *Para cada* $\alpha \in \mathbb{F}_{q^r}$, $D_\alpha = (x - \alpha)_0 \leq D$ *e* $\deg(D_\alpha) = q^{r-1}$, *onde D é o divisor de todos os lugares de grau um, distintos de Q_∞.*

v) $D \sim q^{2r-1}Q_\infty$.

Demonstração. Para a prova dos itens (i) e (ii) apresentaremos as condições gerais que deve satisfazer o corpo de funções Hermitiano generalizado para que o resultado seja satisfeito. Os detalhes da demonstração estão em [4].

i) Seja $GH = \mathbb{F}_{q^r}(x, y)$ a extensão de corpos tal que x e y satisfaz a equação (4.1). Primeiro mostra-se que se χ é uma curva algébrica plana sobre $\mathbb{F}_{q^r}$ definida pela equação (4.1), então é absolutamente irredutível, ou seja $[GH : \mathbb{F}_{q^r}(x)] = q^{r-1}$. Para isto, é suficiente provar que $\mathbb{F}_{q^{r-1}} \subseteq GH$ contém $(q^{r-1} - 1)/(p - 1)$ corpos intermediários dois a dois distintos E_i tais que a extensão $E_i/\mathbb{F}_{q^r}(x)$ é cíclica de grau $p = char(\mathbb{F}_{q^r})$.

   Agora, para cada E_i temos que o gênero é

$$g(E_i) = \frac{q^{r-1}(p-1)}{2}$$

   e o polo de x é totalmente ramificado em $E_i/\mathbb{F}_{q^2}(x)$. Logo, a curva χ tem o mesmo gênero do corpo de funções GH sobre $\mathbb{F}_{q^r}$

$$g = g(GH) = \left(\frac{q^{r-1}-1}{p-1}\right)\left(\frac{q^{r-1}(p-1)}{2}\right) = \frac{q^{r-1}\left(q^{r-1}-1\right)}{2}.$$

   Finalmente, para cada $\alpha \in \mathbb{F}_{q^r}$ temos que

$$\alpha^{q+1} + \alpha^{q^2+1} + \ldots + \alpha^{q^{r-2}+q^{r-1}} = \beta \in \mathbb{F}_q.$$

   Consequentemente, existem q^{r-1} elementos distintos $\lambda \in \mathbb{F}_{q^r}$ tais que

$$\lambda^{q^{r-1}} + \ldots + \lambda^q + \lambda = \beta.$$

   Assim, temos que GH tem exatamente

$$q^r\left(q^{r-1}+1\right) = 1 + q^{2r-1},$$

   lugares de grau um.

ii) Do item (i), sabemos que $[GH : \mathbb{F}_{q^r}(x)] = q^{r-1}$. Então, o polo P_∞ de x em $\mathbb{F}_{q^r}(x)$ tem uma única extensão $Q_\infty \in \mathbb{P}_{GH}$ e $e(Q_\infty|P_\infty) = q^{r-1}$. Logo, Q_∞ é um lugar de grau um em $GH/\mathbb{F}_{q^r}$. Portanto, temos que $(x)_\infty = q^{r-1}Q_\infty$. Ainda, pela definição de χ, temos que x e y têm os mesmos polos, portanto, Q_∞ é o único polo de y. Finalmente,

$$\begin{aligned} v_{Q_\infty}\left(y^{q^{r-1}}\right) &= v_{Q_\infty}\left(x^{q^{r-2}+q^{r-1}}\right) \\ q^{r-1}v_{Q_\infty}(y) &= \left(q^{r-2}+q^{r-2}\right)v_{Q_\infty}(x) \\ (y)_\infty &= \left(q^{r-1}+q^{r-2}\right)Q_\infty. \end{aligned}$$

iii) Suponha que $z := x^{q+1} - y^q + y^{q-1}y$. Então,

$$z^{q^{r-1}} = x^{q^r+q^{r-1}} - y^{q^r} + x^{q^r-q^{r-1}}y^{q^{r-1}} \tag{4.3}$$

Seja $h(x) := p(x) - p(x)^q + x^{q^r+q^{r-1}} + x^{q^r-q^{r-1}}p(x)$, onde $p(x)$ é definido em (4.1). Notemos que $p(x)$ definido em (4.1) é tal que

$$p(x) = x^{1+q} + \ldots + x^{1+q^{r-1}} + x^{q+q^2} + \ldots + x^{q+q^{r-1}} + \ldots + x^{q^{r-2}+q^{r-1}} \tag{4.4}$$

$$p(x) = \sum_{i=0}^{r-2} \left(x^{q^{r-1}+q^i} + \ldots + x^{q^{i+1}+q^i} \right) \tag{4.5}$$

Logo, por (4.4) obtemos,

$$p(x) - p(x)^q = \sum_{i=1}^{r-1} x^{q^i+1} - \sum_{i=1}^{r-2} x^{q^r+q^i} - x^{q^{r-1}+q^r} \tag{4.6}$$

Agora, de (4.5) e (4.6) temos que

$$h(x) = \underbrace{\sum_{i=1}^{r-1} x^{q^i+1} - \sum_{i=1}^{r-2} x^{q^r+q^i}}_{(1)} + \underbrace{x^{q^r+q^{r-1}} \sum_{i=0}^{r-2} \left(x^{q^{r-1}+q^i} + \ldots + x^{q^{i+1}+q^i} \right)}_{(2)}.$$

Ainda, da equação acima notemos que

$$(1) = x^{q+1} + \ldots + x^{1+q^{r-1}} - x^{q+q^r} - x^{q^2+q^r} - \ldots - x^{q^r+q^{r-3}} - x^{q^r+q^{r-2}}.$$

$$\begin{aligned}(2) = {} & x^{q^r-q^{r-1}+q+1} + x^{q^r-q^{r-1}+q^2+1} + \ldots + x^{q^r-q^{r-1}+q^{r-2}+1} + x^{q^r+1} \\ & + x^{q^r-q^{r-1}+q^2+q} + x^{q^r-q^{r-1}+q^3+q} + \ldots + x^{q^r-q^{r-1}+q^{r-2}+q} + x^{q^r+q} \\ & + x^{q^r-q^{r-1}+q^3+q^2} + \ldots + x^{q^r-q^{r-1}+q^{r-2}+q^2} + x^{q^r+q^2} \\ & + x^{q^r-q^{r-1}+q^4+q^3} + \ldots + x^{q^r-q^{r-1}+q^{r-2}+q^{r-3}} + x^{q^r+q^{r-3}} + x^{q^r+q^{r-2}}.\end{aligned}$$

Assim, podemos reescrever $h(x)$ como

$$\begin{aligned}h(x) = {} & x^{q+1} + \ldots + x^{1+q^{r-1}} + x^{q^r-q^{r-1}+q+1} + \ldots + x^{q^r-q^{r-1}+q^{r-2}+1} + x^{q^r+1} \\ & + x^{q^r-q^{r-1}+q^2+q} + x^{q^r-q^{r-1}+q^3+q} + \ldots + x^{q^r-q^{r-1}+q^{r-2}+q} \\ & + x^{q^r-q^{r-1}+q^3+q^2} + \ldots + x^{q^r-q^{r-1}+q^{r-2}+q^2} \\ & + x^{q^r-q^{r-1}+q^4+q^3} + \ldots + x^{q^r-q^{r-1}+q^{r-2}+q^{r-3}}.\end{aligned}$$

E daí podemos concluir que $\deg(h(x)) = q^r + 1$.

Mostremos agora que

$$z^{q^{r-1}} = h(x) - x^{q^r - q^{r-1}} \sum_{i=0}^{r-2} y^{q^i} - y. \tag{4.7}$$

Com efeito,

$$h(x) - x^{q^r - q^{r-1}} \sum_{i=0}^{r-2} y^{q^i} - y = x^{q^r - q^{r-1}} \left(p(x) - \sum_{i=0}^{r-2} y^{q^i} \right) + (p(x) - p(x)^q) - y + x^{q^r + q^{r-1}}.$$

Por outro, lado de (4.1), temos que

$$p(x) = y + y^r + y^{r^2} + \ldots + y^{r-1}.$$

Isto implica que

$$\begin{aligned} h(x) - x^{q^r - q^{r-1}} \sum_{i=0}^{r-2} y^{q^i} - y &= x^{q^r - q^{r-1}} \left(y^{q^{r-1}} \right) + \left(y - y^{q^r} \right) - y + x^{q^r + q^{r-1}} \\ &= x^{q^r + q^{r-1}} - y^{q^r} + x^{q^r - q^{r-1}} y^{q^{r-1}} \\ &= z^{q^{r-1}}, \end{aligned}$$

onde a última igualdade decorre de 4.3. Por outro lado, observemos que

$$\deg \left(\sum_{i=0}^{r-2} y^{q^i} \right) = q^{r-2} + q^{r-3} \quad \text{e} \quad \deg \left(x^{q^- r q^{r-1}} \right) = q^r - q^{r-1}.$$

Finalmente, seja $v = v_{Q_\infty}$ a valorização em Q_∞, temos que

$$\begin{aligned} v\left(z^{q^{r-1}} \right) &= v \left(h(x) - x^{q^r - q^{r-1}} \sum_{i=0}^{r-2} y^{q^i} - y \right) \\ &= min \left\{ (q^r + 1)\, v(x),\ \left(q^r + q^{r-1} \right) v(x) + \left(q^{r-2} + q^{r-3} \right) v(x),\ v(y) \right\} \\ &= min \left\{ (q^r + 1)(-q^{r-1}), (q^r - q^{r-1} + q^{r-2} + q^{r-3})(-q^{r-1}), -(q^{r-1} + q^{r-2}) \right\} \\ &= (q^r + 1)(-q^{r-1}). \end{aligned}$$

Isto implica que $v(z) = -(q^r + 1)$. Consequentemente, $(z)_\infty = (q^r + 1)Q_\infty$.

iv) Primeiro, provaremos a seguinte afirmação: Para cada $\alpha \in \mathbb{F}_{q^r}$, a reta $x = \alpha$ intersecta a curva χ em q^{r-1} pontos racionais distintos (ou seja, lugares de grau um em $GH/\mathbb{F}_{q^r}$). Para isto, é suficiente provar que, para cada $\alpha \in \mathbb{F}_{q^r}$, existem q^{r-1} elementos $\beta \in \mathbb{F}_{q^r}$ tais que

$$\beta^{q^{r-1}} + \ldots + \beta^q + \beta = \alpha^{1+q} + \alpha^{1+q^2} + \ldots + \alpha^{q^{r-2} + q^{r-1}} := f(\alpha),$$

e para todo par (α, β) existe um único lugar $P_{\alpha,\beta} \in \mathbb{P}_{GH}$ de grau um com $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$.

Seja

$$Tr(y) = x^{1+q} + x^{1+q^2} + \ldots + x^{q^{r-2}+q^{r-1}}.$$

Para $x = \alpha$, temos que $Tr(y) = \beta$. E, portanto, $T^{q^{r-1}} + \ldots + T^{q^r} + T = f(\alpha) = \beta$ tem q^{r-1} raízes distintas em $\mathbb{F}_{q^r}$. Pelo Corolário 3.1.6, para cada raiz $\beta_i \in \mathbb{F}_{q^r}$ onde $i = 1, 2, \ldots, q^{r-1}$, existe um único lugar $P_{\alpha_i,\beta_i} \in \mathbb{P}_{GH}$ tal que $P_{\alpha_i,\beta_i} | P_{\alpha_i}$, $y - \beta_i \in P_{\alpha_i,\beta_i}$ e $\deg(P_{\alpha_i,\beta_i}) = 1$. Logo, $x(P_{\alpha_i,\beta_i}) = \alpha$ e $y(P_{\alpha_i,\beta_i}) = \beta$.

Pela construção feita acima, para o elemento

$$t := \prod_{\alpha \in \mathbb{F}_{q^r}} (x - \alpha) = x^{q^r} - x,$$

temos que $(t)_0 = D$, onde $D := \sum_{\alpha \in \mathbb{F}_{q^r}} D_\alpha$, com $D_\alpha (x - \alpha)_0$. Por outro lado,

$$\begin{aligned} v_{Q_\infty}(t) =& v_{Q_\infty}(x) + v_{Q_\infty}\left(x^{q^r-1} - 1\right) \\ =& v_{Q_\infty}(x) + min\left\{(q^r - 1)\, v_{Q_\infty}(x), v_{Q_\infty}(1) = 0\right\} \\ =& v_{Q_\infty}(x) + (q^r - 1)\, v_{Q_\infty}(x) \\ =& -(q^{r-1})(q^r) = -q^{2r-1}. \end{aligned}$$

Portanto $(t)_\infty = q^{2r-1} Q_\infty$. Consequentemente, $(t) = D - q^{2r-1} Q_\infty$.

v) Do item (iv) temos que $(t) = D - q^{2r-1} Q_\infty$ o que implica, $D = (t) + q(2r-1)Q_\infty$ e portanto $D \sim q(2r-1)Q_\infty$.

✓

Para continuar, vamos definir alguns conceitos dos semigrupos telescópicos, que podem ser encontrados em [7].

Definição 4.1.1 (4.1 em [7]). *O conjunto $S \subseteq \mathbb{Z}^+$ é um semigrupo se para cada $x, y \in S$, então $x + y \in S$ e o conjunto $\mathbb{Z}^+ \setminus S$ é finito. Chamaremos os elementos de $\mathbb{Z}^+ \setminus S$ de lacunas de S e os elementos de S serão ditos números polo de S. Denotaremos a quantidade de lacunas como $g(S)$. No contexto do semigrupo de números polo de um ponto racional de uma curva algébrica $g = g(S)$ é o gênero da curva (ver Teorema das lucunas de Weierstrass, Teorema 1.5.6). Ainda, podemos enumerar as lacunas de S na ordem $l_1 < l_2 < \ldots < l_g$. Definimos $l_g = l_g(S)$ como a maior lacuna de S.*

Definição 4.1.2 (4.3 em [7]). *Um semigrupo é simétrico se $l_g(S) = 2g(S) - 1$.*

Definição 4.1.3 (6.1 em [7]). *Seja $a_1, \ldots, a_k$ uma sequência de inteiros positivos com m.d.c. igual a um. Definimos*

$$d_i = m.d.c.(a_1, \ldots, a_i) \quad e \quad A_i = \left\{ \frac{a_1}{d_i}, \ldots \frac{a_i}{d_i} \right\},$$

para $i = 1, 2, \ldots, k$. Definimos ainda $d_0 = 0$. Seja S_i o semigrupo gerado por A_i. Se $a_i/d_i \in S_{i-1}$ para $i = 2, 3, \ldots, k$, então a sequência $(a_1, a_2, \ldots, a_k)$ é chamada telescópica. Um semigrupo é chamado telescópico se ele é gerado por uma sequência telescópica.

Lema 4.1.2 (6.5 em [7]). *Seja S_k o semigrupo gerado pela sequência telescópica $(a_1, a_2, \ldots, a_k)$. Então,*

$$l_g(S_k) = d_{k-1}\left(l_g(S_{k-1}) - 1\right) + (d_{k-1} - 1)\, a_k = \sum_{i=1}^{k} \left(\frac{d_{i-1}}{d_i} - 1 \right) a_i$$

$$g(S_k) = d_{k-1} g(S_{k-1}) + (d_{k-1} - 1)\frac{a_k - 1}{2} = \frac{l_g(S_k) + 1}{2}.$$

Ainda, da fórmula do gênero para o semigrupo telescópico, temos que os semigrupos telescópicos são simétricos.

O semigrupo de Weierstrass para o divisor polo Q_∞ é definido como

$$\begin{aligned} H(Q_\infty) &= \left\{ t \in \mathbb{Z}^+ \mid t \text{ é um número polo de } Q_\infty \right\} \\ &= \left\{ t \in \mathbb{Z}^+ \mid \text{existe } x \in GH \text{ tal que } (x)_\infty = tQ_\infty \right\}. \end{aligned}$$

Proposição 4.1.1. *O semigrupo de Weierstrass para o divisor polo Q_∞ é*

$$H(Q_\infty) = \langle q^{r-1}, q^{r-1} + q^{r-2}, q^r + 1 \rangle.$$

Em particular $H(Q_\infty)$, é simétrico.

Demonstração. Pelo Lema 4.1.1, temos que $(x)_\infty = q^{r-1}$, $(y)_\infty = q^{r-1} + q^{r-2}$ e $(z)_\infty = q^r + 1$, onde $z := x^{q+1} - y^q + y^{q-1}y$. Isto implica que q^{r-1}, $q^{r-1} + q^{r-2}$, $q^r + 1$ são números polo de Q_∞. Consequentemente,

$$\langle q^{r-1}, q^{r-1} + q^{r-2}, q^r + 1 \rangle \subseteq H(Q_\infty).$$

Para provar a igualdade, pela Definição 4.1.1, basta provar que os dois semigrupos têm o mesmo gênero. Obviamente, o semigrupo $\langle q^{r-1}, q^{r-1} + q^{r-2}, q^r + 1 \rangle$ é gerado pela sequência $(q^{r-1},\ q^{r-1} + q^{r-2}\ , q^r + 1)$. Claramente, esta sequência cumpre as condições da definição 4.1.3, assim o semigrupo $\langle q^{r-1}, q^{r-1} + q^{r-2}, q^r + 1 \rangle = S$ é telescópico.

Logo, pelo Lema 4.1.2, temos que

$$\begin{aligned} l_g(S) &= (0-1)q^{r-1} + \left(\frac{q^{r-1}}{q^{r-2}} - 1\right)\left(q^{r-1}+q^{r-2}\right) + \left(q^{r-2}-1\right)(q^r+1) \\ &= q^{2r-2} - q^{r-1} - 1 \\ &= q^{r-1}\left(q^{r-1}-1\right) - 1. \end{aligned}$$

Ainda, como S é simétrico, então, da definição 4.1.2, concluímos que

$$g(S) = \frac{l_g(S)-1}{2} = \frac{q^{r-1}\left(q^{r-1}-1\right)}{2} = g,$$

onde a última igualdade decorre do Lema 4.1.1 . ✓

Observação 4.1.1. *Como Corolário, temos que a curva χ definida pela equação* (4.1) *é uma curva Castle (veja [11] e [10]).*

Corolário 4.1.1.

$$H(Q_\infty) = \left\{ iq^{r-1} + j\left(q^{r-2}+q^{r-1}\right) + k\left(q^r+1\right) \mid i \geq 0,\ 0 \leq j < q \ \text{ e } \ 0 \leq k < q^{r-2} \right\}.$$

Demonstração. Pela proposição anterior é suficiente provar que

$$H(Q_\infty) \subseteq \left\{ iq^{r-1} + j\left(q^{r-2}+q^{r-1}\right) + k\left(q^r+1\right) \mid i \geq 0,\ 0 \leq j < q \text{ e } 0 \leq k < q^{r-2} \right\}.$$

Seja $x \in H(Q_\infty)$, então, pela Proposição 4.1.1, existem $s \geq 0$, $t \geq 0$ e $u \geq 0$ tais que

$$x = sq^{r-1} + t\left(q^{r-2}+q^{r-1}\right) + u\left(q^r+1\right).$$

Pelo algoritmo da divisão, existem $u, w \in \mathbb{Z}^+$, tais que $u = vq^{r-2} + w$ onde $0 \leq w < q^{r-2}$. Assim,

$$\begin{aligned} x &= sq^{r-1} + t\left(q^{r-2}+q^{r-1}\right) + \left(vq^{r-2}+w\right)\left(q^r+1\right) \\ &= sq^{r-1} + t\left(q^{r-2}+q^{r-1}\right) + vq^{2r-2} + vq^{r-2} + w\left(q^r+1\right) \\ &= \left(s + vq^{r-1} - v\right)q^{r-1} + (t+v)\left(q^{r-2}+q^{r-1}\right) + w\left(q^r+1\right). \end{aligned}$$

Novamente, pelo algoritmo da divisão, existem $m, n \in \mathbb{Z}^+$ tais que $t+v = mq+n$ onde $0 \leq n < q$.

$$\begin{aligned} x &= \left(s + vq^{r-1} - v\right)q^{r-1} + (mq+n)\left(q^{r-2}+q^{r-1}\right) + w\left(q^r+1\right) \\ &= \left(s + vq^{r-1} - v + m + mq\right)q^{r-1} + n\left(q^{r-2}+q^{r-1}\right) + w\left(q^r+1\right). \end{aligned}$$

Como $s + vq^{r-1} - v + m + mq \geq 0$, $0 \leq n < q$ e $0 \leq w < q^{r-2}$, concluimos a prova. ✓

Definamos agora o conjunto $H_m(Q_\infty) = \{n \in H(Q_\infty) \mid n \leq m\}$. Pelo Corolário anterior temos que

$$H_m(Q_\infty) = \left\{n \leq m \mid n = iq^{r-1} + j\left(q^{r-2} + q^{r-1}\right) + k\left(q^r + 1\right) \mid i \geq 0,\ 0 \leq j < q \text{ e } 0 \leq k < q^{r-2}\right\}$$

Lema 4.1.3. *Sejam z a função definida no Lema 4.1.1 e $m \in \mathbb{Z}$. Então*

$$\left\{x^i y^j z^k \mid iq^{r-1} + j\left(q^{r-2} + q^{r-1}\right) + k\left(q^r + 1\right) \leq m,\ \ i \geq 0,\ \ 0 \leq j < q \ \ e\ 0 \leq k < q^{r-2}\right\}$$

é uma base de $\mathcal{L}(mQ_\infty)$.

Demonstração. Seja $t = x^i y^j z^k$ onde $i \geq 0,\ 0 \leq j < q\ ,\ 0 \leq k < q^{r-2}$ e z a função definida no Lema 4.1.1. Assim, temos que

$$\begin{aligned}(t) &\geq -(t)_\infty = -(x^i y^j z^k)_\infty \\ &= -(iq^{r-1} + j\left(q^{r-2} + q^{r-1}\right) + k\left(q^r + 1\right))Q_\infty \qquad \text{pelo Lema 4.1.1} \\ &\geq -mQ_\infty,\end{aligned}$$

onde a última desigualdade decorre da hipótese. Isto mostra que $x^i y^j z^k \in \mathcal{L}(mQ_\infty)$, onde $i \geq 0,\ \ 0 \leq j < q\ \ ,\ \ 0 \leq k < q^{r-2}$. Resta provar que os elementos são linearmente independentes.

Suponha que $\sum\limits_{i,j,k} a_{ijk} x^i y^j z^k = 0$, onde $a_{ijk} \in \mathcal{L}(mQ_\infty)$ e nem todo $a_{ijk} = 0$. Se $v = v_{Q_\infty}$ representa a valorização de Q_∞, temos que

$$v\left(\sum_{i,j,k} a_{ijk} x^i y^j z^k\right) = v(0) = \infty \tag{4.8}$$

Por outro lado,

$$\begin{aligned}v\left(\sum_{i,j,k} a_{ijk} x^i y^j z^k\right) &= \min\left\{v\left(a_{ijk}\right) + iv(x) + jv(y) + kv(z) \mid a_{ijk} \neq 0\right\} \\ &= \min\left\{v(a_{ijk}) - \left(iq^{r-1} + j\left(q^{r-1} + q^{r-2}\right) + k\left(q^r + 1\right)\right) \mid a_{ijk} \neq 0\right\}.\end{aligned}$$

Para simplifica a notação, escrevemos $n_{ijk} = iq^{r-1} + j\left(q^{r-1} + q^{r-2}\right) + k\left(q^r + 1\right)$. Ainda, como $a_{ijk} \in \mathcal{L}(mQ_\infty)$, então $v(a_{ijk}) \geq -v(mQ_\infty) = -m$ e, como por hipótese,

$$n_{ijk} = iq^{r-1} + j\left(q^{r-2} + q^{r-1}\right) + k\left(q^r + 1\right) \leq m.$$

Podemos concluir que

$$v(a_{ijk}) - n_{ijk} \geq -2m$$

para $a_{ijk} \neq 0$. Além disso, é claro que

$$v(a_{ijk}) - n_{ijk} \geq \min\left\{v(a_{ijk}) - n_{ijk} \mid a_{ijk} \neq 0\right\}.$$

Isto implica que

$$\min\{v(a_{ijk}) - n_{ijk} \mid a_{ijk} \neq 0\} - 2m \leq 2\,(v(a_{ijk}) - n_{ijk})\,.$$

Mais ainda, como Q_∞ é o único divisor polo de x e y de grau um e $a_{ijk} \in \mathcal{L}(Q_\infty)$, então $v(a_{ijk}) \leq 0$. Além disso, como $n_{ijk} \geq 0$, temos que

$$v(a_{ijk}) - n_{ijk} \leq 0,$$

o que implica que $\min\{v(a_{ijk}) - n_{ijk} \mid a_{ijk} \neq 0\} \leq 2m$. Assim, de (4.8), teríamos que

$$\infty = v(0) = v\left(\sum_{i,j,k} a_{ijk}x^i y^j z^k\right) = \min\{v(a_{ijk}) - n_{ijk} \mid a_{ijk} \neq 0\} \leq 2m,$$

o que seria uma contradição. Consequentemente, os elementos $x^i y^j z^k \in \mathcal{L}(mQ_\infty)$ onde $i \geq 0,\ 0 \leq j < q\ ,\ 0 \leq k < q^{r-2}$, são linearmente independentes. ✓

Corolário 4.1.2. *Dado*

$$H(Q_\infty) = \left\{iq^{r-1} + j\left(q^{r-2} + q^{r-1}\right) + k\,(q^r + 1) \mid i \geq 0,\ 0 \leq j < q \ \ e\ \ 0 \leq k < q^{r-2}\right\},$$

então $|H_m(Q_\infty)| = \ell(mQ_\infty)$.

Demonstração. Análoga à prova da Proposição 3.5.3. ✓

4.2 CÓDIGOS HERMITIANOS GENERALIZADOS

A partir das ferramentas obtidas na seção anterior, em particular do Lema 4.1.1 e sua prova, definimos os códigos Hermitianos Generalizados como

$$CH_m = C_{\mathcal{L}}(\chi, D, mQ_\infty), \ \text{ onde } \ D = \sum_{\beta^{q^{r-1}} + \ldots + \beta = \alpha^{1+q} + \ldots + \alpha^{q^{r-2} + q^{r-1}}} P_{\alpha,\beta}$$

é a soma de todos os lugares grau um, exceto Q_∞, do corpo de funções $GH/\mathbb{F}_{q^r}$, e χ é a curva algébrica plana sobre $\mathbb{F}_{q^r}$ que satisfaz a equação (4.1). Claramente, do Lema 4.1.1, temos que o comprimento deste código é $n = q^{2r-1}$ e $CH_m \subseteq CH_{m'}$ para $m \leq m'$.

Proposição 4.2.1. *O código dual de* CH_m *é* $CH_m^\perp = CH_{n+2g-2-m}$.

Demonstração. Consideremos o elemento

$$t = \prod_{\alpha \in \mathbb{F}_{q^r}} (x - \alpha) = x^{q^r} - x.$$

Sabemos da prova do Lema 4.1.1 item (iv) que o divisor principal de t é $(t) = D - q^{2r-1}Q_\infty$. Logo, $v_{P_{\alpha,\beta}}(t) = v_{P_{\alpha,\beta}}(D) = 1$ para cada $P_{\alpha,\beta} \in supp(D)$.

Por outro lado, $dt = d(x^{q^r} - x) = -dx$, já que $d(x^{q^r}) = 0$ pois $char(\mathbb{F}_{q^r}) = p > 0$ com p primo.

Ainda, pelo Lema 4.3 em [2] temos que $(dx) = (2g-2)Q_\infty$. Consequentemente,

$$(dx) = (dt) = (2g-2)Q_\infty$$

Finalmente, do Teorema 2.3.3, do item (ii) da Proposição 3.3.3 e das passagens acima concluímos o resultado, pois

$$\begin{aligned} CH_m^\perp &= CH_\Omega(D, mQ_\infty) = CH_\mathcal{L}(D, D - mQ_\infty + (dt) - (t)) \\ &= CH_\mathcal{L}(D, (n + 2g - 2 - m)Q_\infty) \\ &= CH_{n+2g-2-m}. \end{aligned}$$

✓

Notemos que, para o caso $r = 2$, esta proposição é a primeira parte da proposição 3.5.1. O resto da proposição vale somente em alguns casos, para isto temos o seguinte corolário.

Corolário 4.2.1. *Seja CH_m um código Hermitiano generalizado que possui comprimento $n = q^{2r-1}$. Então*

i) CH_m é auto-dual se $2m < n + 2g - 2$.

ii) CH_m é auto-ortogonal se $2m = n - 2g - 2$, somente se q é uma potência de 2.

Demonstração. Decorre diretamente da Proposição acima e da definição de auto-dual e auto-ortogonal. ✓

Agora, observemos os casos triviais para a dimensão dos códigos Hermitianos generalizados, cujo raciocínio é análogo ao caso estudado para os códigos Hermitianos.

i) Para $m < 0$, temos que $\deg(mQ_\infty) < 0$, donde, $\mathcal{L}(mQ_\infty) = 0$ e, portanto $CH_m = 0$.

ii) Para $m > q^{2r-1} + q^{2r-2} - q^{r-1} - 2 = n + 2g - 2$, ou seja, $m - n \geq 2g - 1$, temos que $\deg(mQ_\infty) > \deg(mQ_\infty - D) = m - n \geq 2g - 1$. Assim, pelos Teoremas 2.3.1 e 1.5.4, temos que

$$\begin{aligned} \dim(CH_m) &= \ell(mQ_\infty) - \ell(mQ_\infty - D) \\ &= (m + 1 - g) - (m - q^{2r-1} + 1 - g) \\ &= q^{2r-1} = n \end{aligned}$$

Consequentemente, $CH_m = \mathbb{F}_{q^2}^n$. Portanto, resta analizar os códigos Hermitianos generalizados onde $0 \leq m \leq n + 2g - 2$.

Observação 4.2.1. *Notemos que para $m \geq 2g-1$ o Teorema de Riemann-Roch garante que*

$$\ell(mQ_\infty) = \deg(mQ_\infty) + 1 - g = m + 1 - g.$$

Ainda, pelo Corolário 4.1.2*, temos que $|H_m(Q_\infty)| = m + 1 - g$.*

Proposição 4.2.2. *Suponhamos que $0 \leq m \leq n + 2g - 2$, então*

i) A dimensão de CH_m é dada por

$$\dim(CH_m) = \begin{cases} |H_m(Q_\infty)| & \text{para } 0 \leq m \leq n. \\ n - |H_s(Q_\infty)| & \text{para } n \leq m \leq n + 2g - 2 \end{cases}$$

onde $s = n + 2g - 2 - m$.

ii) Para $2g - 2 < m < n$, então $\dim(CH_m) = m + 1 - g$

iii) A distância mínima d_m do código CH_m satisfaz $d_m \geq n - m$.

Demonstração. i) Para $0 \leq m < n$, pelo Corolário 2.3.1 temos que

$$\dim(CH)_m = \ell(mQ_\infty) = |H_m(Q_\infty)|.$$

Agora, se $n \leq m \leq n + 2g - 2$ e $s = n + 2g - 2 - m$, então $0 \leq s < n$ o que implica que $\dim(CH_s) = |H(Q_\infty)|$. Por outro lado, pela Proposição 4.2.1, temos que $CH_m^\perp = CH_s$. Assim,

$$\begin{aligned} \dim(CH_m) &= n - \dim(CH_m^\perp) \\ &= n - \dim(CH_s) \\ &= n - |H_s(Q_\infty)| \end{aligned}$$

ii) Notemos que $\deg(mQ_\infty) = m$. Logo, se $2g - 2 < \deg(mQ_\infty) < n$, pelo Corolário 2.3.1, podemos concluir que $\dim(CH_m) = m + 1 - g$.

iii) A desigualdade $d_m \geq n - m$ é imediata pelo Teorema 2.3.1. ✓

Proposição 4.2.3. *Seja d_m a distância mínima do código CH_m. Temos:*

i) Se $m = aq^{r-1}$ com $0 \leq a < q^r$, então $d_m = n - m$.

ii) Se $m = aq^{r-1} + b\,(q^{r-1} + q^{r-2})$ com $0 \leq a \leq q^r - q^{r-1} - q^{r-2}$ e $0 \leq b < q^{r-1}$, então $d_m = n - m$.

iii) Se $m = q^{2r-1} - q^{r-1} + b$ com $0 \leq b \leq q^{r-1}$, então $d_m = q^{r-1}$.

Demonstração.

i) Escolhamos a elementos distintos em $\mathbb{F}_{q^r}$, a saber, $\alpha_1, \alpha_2, \ldots, \alpha_a$. Como a aplicação traço de $\mathbb{F}_{q^r}$ em $\mathbb{F}_q$ é linear e sobrejetora, então o divisor canônico de $x - \alpha_i$, tem exatamente q^{r-1} zeros distintos $P_{\alpha,\beta}$ de grau um em $\mathbb{P}_{GH}$. Logo,

$$z = \prod_{i=1}^{a} (x - \alpha_i),$$

possui exatamente aq^{r-1} zeros distintos $P_{\alpha,\beta}$ de grau um.

Por outro lado, $z = x^a + \ldots + \alpha_1\alpha_2 \ldots \alpha_a$ com $0 \leq a < q^r$. Assim, pelo Lema 4.1.3, temos que $z \in \mathcal{L}(mQ_\infty)$. Consequentemente,

$$wt(ev_D(z)) = q^{2r-1} - aq^{r-1} = n - m.$$

Isto implica que $d_m \leq n - m$. E, pela Proposição 4.2.2 item (iii), podemos concluir que $d_m = n - m$.

ii) Fixemos um elemento $0 \neq \gamma \in \mathbb{F}_q^*$ e definamos o conjunto $A = \{\alpha \in \mathbb{F}_{q^r} \mid p(\alpha) \neq \gamma\}$, onde

$$p(\alpha) = \alpha^{1+q} + \ldots + \alpha^{1+q^{r-1}} + \alpha^{q+q^2} + \cdots + \alpha^{q+q^{r-1}} + \ldots + \alpha^{q^{r-2}+q^{r-1}}.$$

Temos que $|A| \geq q^r - q^{r-1} - q^{r-2} \geq a$. Logo, podemos escolher a elementos distintos $\alpha_1, \alpha_2, \ldots, \alpha_a$ em A. Assim,

$$f_1 = \prod_{\mu=1}^{a} (x - \alpha_\mu),$$

possui aq zeros distintos $P_{\alpha,\beta} \in supp(D)$. Também podemos escolher q^{r-1} elementos distinto $\beta \in \mathbb{F}_{q^r}$, tais que

$$\beta^{q^{r-1}} + \beta^{q^{r-2}} + \ldots + \beta = \gamma \in \mathbb{F}_{q^r}^*.$$

Assim, para $0 \leq b < q^{r-1}$, temos que

$$f_2 = \prod_{\nu}^{b} (y - \beta),$$

tem $b\,(q^{r-1} + q^{r-2})$ zeros distintos $P_{\alpha,\beta} \in supp(D)$. Além disso, pela construção

$$\beta_\nu^{q^{r-1}} + \beta_\nu^{q^{r-2}} + \ldots + \beta_\nu = \gamma \neq \alpha_\mu \text{ para } \nu = 1, 2, \ldots, b \text{ e } \mu = 1, 2, \ldots, a.$$

Consequentemente,

$$f = f_1 f_2 \in \mathcal{L}\left(\left(aq^{r-1} + b\left(q^{r-1} + q^{r-2}\right)\right) Q_\infty\right) = \mathcal{L}(mQ_\infty).$$

Portanto, f tem $aq^{r-1} + b\,(q^{r-1} + q^{r-2}) = m$ zeros distintos $P_{\alpha,\beta} \in supp(D)$. E daí, $wt(ev_D(f)) = q^{2r-1} - m$, assim $d_m \leq n - m$. Pela Proposição 4.2.2 item (iii), podemos concluir que $d_m = n - m$.

iii) Notemos primeiro que $n - q^{r-1} = q^{2r-1} - q^{r-1} = q^{r-1}(q-1)$ e $0 \leq q-1 < q^r$. Logo, pelo item (i), temos que

$$d_{n-q^{r-1}} = n - (n - q^{r-1}) = q^{r-1}.$$

Por outro lado, da hipótese, temos que $m = n - q^{r-1} + b$, $0 \leq b < q^{r-1}$. Portanto $m \geq n - q^{r-1}$. Pois, caso contrário,

$$m < n - q^{r-1} \Rightarrow n - q^{r-1} + b < n - q^{r-1} \Rightarrow b < 0,$$

o que seria uma contradição. Agora, se $n - q^{r-1} \leq m$, temos que

$$d_m \leq d_{n-q^{r-1}} = q^{r-1} \;\; \Rightarrow \;\; d_m \leq q^{r-1}.$$

Finalmente, lembrando que $q^{2r-1}Q_\infty - D$ é um divisor principal de grau zero, então pelo Corolário 1.3.1, temos que $\ell(q^{2r-1}Q_\infty - D) = 1$.

Logo, pelo Corolário 2 em [9], temos que

$$d_m = d_1(CH_m) \geq n - \deg(mQ_\infty) + \gamma_2,$$

onde $\gamma_2 = \min\{\deg(A) \mid A \in Div(GH) \text{ e } \ell(A) \geq 2\}$ (Definição 2.3.3). Ainda, γ_2 é a gonalidade usual (ver [12]), isto implica que, $\gamma_2 = [GH : \mathbb{F}_{q^r}(x)]$.

Por outro lado, da prova do Lema 4.1.1, sabemos que $[GH : \mathbb{F}_{q^r}(x)] = q^{r-1}$.

Consequentemente, $d_m \geq n - m + q^{r-1}$. E como por hipótese $m \leq n$, temos que $n - m + q^{r-1} \geq q^{r-1}$, portanto

$$d_m \geq q^{r-1},$$

o que conclui a prova. ✓

Para concluir este trabalho, estudaremos os casos $n \leq m \leq n+2g-2$ onde podemos calcular a distância mínima exata do código CH_m.

Lema 4.2.1. *Todo inteiro não negativo m tem uma única representação na forma*

$$m = aq^{r-1} + bq^{r-2} + c,$$

onde $a \geq 0$, $0 \leq b < q$ e $0 \leq c < q^{r-2}$. Além disso, $m \in H(Q_\infty)$ se, somente se, $a \geq b + cq$.

Demonstração. Suponhamos que $a_1q^{r-1} + b_1q^{r-2} + c_1 = m = a_2q^{r-1} + b_2q^{r-2} + c_2$, onde $a_1, a_2 \geq 0$, $0 \leq b_1, b_2 < q$ e $0 \leq c_1, c_2 < q^{r-2}$. Isto implica que

$$(a_1 - a_2)q^{r-1} + (b_1 - b_2)q^{r-2} = c_1 - c_2,$$

ou seja,

$$q^{r-2}\left((b_1 - b_2) + (a_1 - a_2)q\right) = c_1 - c_2$$

Portanto $q^{r-2}|(c_1 - c_2)$, mas $0 \leq c_1, c_2 < q^{r-2}$ e daí, $c_1 = c_2$. Consequentemente,

$$(a_1 - a_2)q^{r-1} + (b_1 - b_2)q^{r-2} = 0.$$

Analogamente, podemos provar que $a_1 = a_2$ e $b_1 = b_2$, assim a representação de m é única.

Finalmente, provemos que $m \in H(Q_\infty)$ se, somente se, $a \geq b + cq$.

$\Rightarrow$) Por hipótese $m \in H(Q_\infty)$. Então, do Corolário 4.1.1, temos que

$$m = iq^{r-1} + j\left(q^{r-2} + q^{r-1}\right) + k\left(q^r + 1\right),$$

onde $i \geq 0$, $0 \leq j < q$ e $0 \leq k < q^{r-2}$. Ainda, rescrevendo m, temos que

$$m = (i + j + kq)q^{r-1} + jq^{r-2} + k.$$

Mas ainda, já mostramos que m tem uma única representação, assim $b = j$, $c = k$ e $a = i + b + cq$. Notemos que se $a < b + cq$, isto implicaria que $a + i < a$, o que seria uma contradição, pois $i \geq 0$. Assim, $a \geq b + cq$.

$\Leftarrow$) Seja $m = aq^{r-1} + bq^{r-2} + c$, onde $a \geq 0$, $0 \leq b < q$ e $0 \leq c < q^{r-2}$. Suponhamos que $a \geq b + cq$, ou seja, $a - b - cq \geq 0$. Logo, pelo Lema 4.1.3, temos que

$$h = x^{a-b-cq}y^b z^c \in \mathcal{L}(mQ_\infty).$$

Por outro lado,

$$\begin{aligned} v_{Q_\infty}(h) &= (a - b - cq)v_{Q_\infty}(x) + bv_{Q_\infty}(y) + cv_{Q_\infty}(z) \\ &= -(a - b - cq)q^{r-1} - b\left(q^{r-2} + q^{r-1}\right) - c\left(q^r + 1\right) \\ &= -\left(aq^{r-1} - bq^{r-1} - cq^r + bq^{r-2} + bq^{r-1} + cq^r + c\right) \\ &= -\left(aq^{r-1} + bq^{r-2} + c\right) \\ &= -m \end{aligned}$$

Consequentemente, $(h)_\infty = mQ_\infty$, donde $m \in H(Q_\infty)$. ✓

Observação 4.2.2. *Para $0 \leq m \leq n + 2g - 1$, definimos $m^\perp = n + 2g - 2 - m$. Pela Proposição 4.2.1, sabemos que $CH_{m^\perp}$ é o código dual do código CH_m.*

Além disso, se $n \leq m \leq n + 2g - 2$ então $m \in H(Q_\infty)$ e $0 \leq m^\perp < 2g - 2$. Com efeito, pelo Lema 4.2.1 temos que m tem uma representação única na forma

$$m = aq^{r-1} + bq^{r-2} + c, \text{ tal que } a \geq 0,\ 0 \leq b < q \text{ e } 0 \leq c < q^{r-2}$$

e $m \in H(Q_\infty)$ se, e somente se, $a \geq b + cq$.

Suponhamos pelo absurdo que $m \notin H(Q_\infty)$*, isto é,* $a < b + cq$*. Assim,*

$$\begin{aligned} n \leq m &= aq^{r-1} + bq^{r-2} + c \\ &< (b + cq)q^{r-1} + bq^{r-2} + c \\ &= bq^{r-1} + cq^r + bq^{r-2} + c \\ &< qq^{r-1} + q^{r-2}q^r + qq^{r-2} + q^{r-2} \\ &= q^r + q^{2r-2} + q^{r-1} + q^{r-2}. \end{aligned}$$

Lembrando que para os códigos Hermitianos generalizados $n = q^{2r-1}$*, teríamos que* $q^{2r-1} < q^r + q^{2r-2} + q^{r-1} + q^{r-2}$*, o que implicaria* $q^{r+1} < q^r + q^2 + q + 1$*, o que seria uma contradição pois* $q, r \geq 3$*. Consequentemente,* $m \in H(Q_\infty)$*. A prova que* $0 \leq m^\perp < 2g - 2$ *é óbvia.*

Ainda, se $m^\perp$ *é um número polo de* Q_∞ *e* $t^\perp$ *é o maior número polo de* Q_∞*, tal que* $t^\perp \leq m^\perp$*, pelo Lema* 4.1.3*, temos que* $\mathcal{L}(t^\perp Q_\infty) = \mathcal{L}(m^\perp Q_\infty)$*, portanto* $CH_{t^\perp} = CH_{m^\perp}$*. Assim, podemos considerar* m*, onde* $m^\perp$ *é um número polo de* Q_∞*. Logo, nas condições do Lema* 4.2.1*, podemos escrever*

$$m^\perp = aq^{r-1} + bq^{r-2} + c, \text{ tal que } 0 \leq b < q, \ 0 \leq c < q^{r-2} \text{ e } a \geq b + cq.$$

E como $m^\perp \leq 2g - 2$*, teremos que* $0 \leq b + cq \leq q^{r-1} - 2$*. Com efeito,*

$$m^\perp \leq 2g - 2 = q^{r-1}\left(q^{r-1} - 1\right) - 2,$$

por outro lado, $m^\perp = aq^{r-1} + bq^{r-2} + c$*. Logo,*

$$aq^{r-1} \leq aq^{r-1} + bq^{r-2} + c \leq q^{r-1}\left(q^{r-1} - 1\right) - 2 < q^{r-1}\left(q^{r-1} - 1\right).$$

Isto implica que $a \leq q^{r-1} - 2$ *e, como* $a \geq b + cq$*, então* $b + cq \leq q^{r-1} - 2$*.*

Observação 4.2.3. *Na prova do Lema* 4.2.1*, mostramos que o elemento*

$$h = x^{a-b-cq}y^b z^c,$$

onde $a \geq b + cq$*,* $0 \leq b < q$*,* $0 \leq c < q^{r-2}$ *e* $0 \leq b + cq \leq q^{r-2} - 2$*, é um elemento básico de* $\mathcal{L}(mQ_\infty)$*, com* $m = aq^{r-1} + bq^{r-2} + c$*. Por outro lado, o elemento*

$$t = x^{a-b-cq+q}y^b z^{c-1}$$

onde $a \geq b + cq$*,* $0 \leq b < q$*,* $0 \leq c < q^{r-2}$ *e* $0 \leq b + cq \leq q^{r-2} - 2$*, também é um elemento de base de* $\mathcal{L}(mQ_\infty)$*. De fato,*

$$\begin{aligned} &(a - b - cq + q)q^{r-1} + b\left(q^{r-1} + q^{r-2}\right) + (c - 1)\left(q^r + 1\right) \\ &= q^r + aq^{r-1} - bq^{r-1} - cq^r + bq^{r-1} + bq^{r-2} + cq^r + c - q^r - 1 \\ &= aq^{r-1} + bq^{r-2} + c - 1 \\ &= m - 1 < m. \end{aligned}$$

Logo, pelo Lema 4.1.3*, obtemos o resultado. Além disso, é fácil provar que*

$$x^{a-b-cq+q+1}y^b z^c, x^{a-b-cq+q+1}y^b z^{c-1} \notin \mathcal{L}(mQ_\infty).$$

Consequentemente, temos que

$$\left\{x^i y^j z^k \mid 0 \leq i \leq a-b-cq+q,\ 0 \leq j \leq b,\ 0 \leq k \leq c\right\}$$

é uma base de $\mathcal{L}(mQ_\infty)$*, onde* m *é definido como*

$$m = aq^{r-1} + bq^{r-2} + c,\ \textit{tal que}\ 0 \leq b < q,\ 0 \leq c < q^{r-2}\ \textit{e}\ a \geq b + cq.$$

Lema 4.2.2. *Sejam* $t^\perp = aq^{r-1} + bq^{r-2} + c$ *nas condições do* 4.2.1*, onde* $a = b + cq$*, e* H *a matriz geradora do código* $CH_{t^\perp}$*. Então, quaisquer* $a+1$ *colunas de* H *são linearmente independentes.*

Demonstração. Da Observação 4.2.3, temos que uma base para

$$\begin{aligned}\mathcal{L}(t^\perp Q_\infty) &= \mathcal{L}\left(\left(aq^{r-1} + bq^{r-2} + c\right)Q_\infty\right)\\ &= \mathcal{L}\left(\left((b+cq)q^{r-1} + bq^{r-2} + c\right)Q_\infty\right)\\ &= \mathcal{L}\left(\left(b\left(q^{r-1} + q^{r-2}\right) + c\left(q^r + 1\right)\right)Q_\infty\right)\end{aligned}$$

é $\{x^i y^j z^k \mid 0 \leq i \leq q,\ 0 \leq j \leq b,\ 0 \leq k \leq c\}$, ou seja,

$$\begin{aligned}&\{1, x, y, x^2, xy, y^2, \ldots, x^{q-1}, x^{q-2}\ldots, y^{q-1}, x^q, z, x^{q-1}y, \ldots, x^q y,\\ &\ yz, x^{q-1}y^2, \ldots, x^a, \ldots x^q y^b z^{c-1}, y^b z^c\}\end{aligned}$$

Lembremos que cada coluna da matriz H é da forma $x^i y^j z^k(P_{\alpha,\beta})$, onde $x^i y^j z^k$ são elementos da base de $\mathcal{L}(t^\perp Q_\infty)$ e $P_{\alpha,\beta}$ são todos os lugares de grau um distintos de Q_∞. Por notação, chamemos $u_{ijk} = x^i y^j z^k$. Consideremos agora uma submatriz A de H, correspondente à escolha de $a+1$ colunas distintas de H, reordenando as colunas de A a partir dos α, temos que

$$\begin{aligned}A = \Big(&u_{ijk}\left(P_{\alpha_1,\beta_{1,1}}\right), u_{ijk}\left(P_{\alpha_1,\beta_{1,2}}\right), \ldots, u_{ijk}\left(P_{\alpha_1,\beta_{1,b_1}}\right),\\ &u_{ijk}\left(P_{\alpha_2,\beta_{2,1}}\right), u_{ijk}\left(P_{\alpha_2,\beta_{2,2}}\right)\ldots, u_{ijk}\left(P_{\alpha_2,\beta_{2,b_2}}\right), \ldots\\ &, u_{ijk}\left(P_{\alpha_l,\beta_{l,1}}\right), u_{ijk}\left(P_{\alpha_l,\beta_{l,2}}\right), \ldots u_{ijk}\left(P_{\alpha_l,\beta_{l,b_l}}\right)\Big),\end{aligned}$$

onde os α_i são dois a dois distintos, $b_1 \geq b_2 \geq \ldots \geq b_l \geq 1$ e $b_1 + b_2 + \ldots + b_l = a+1$. Mostremos agora que os elementos

$$x^{i-1}y^{k_i}z^{t_i}\ \text{com}\ 0 \leq k_i + t_i q \leq b_i - 1,\ 0 \leq k_i < q\ \text{e}\ 0 \leq i \leq l, \tag{4.9}$$

são elementos básicos de $\mathcal{L}(t^{\perp}Q_{\infty})$. Com efeito,

$$\begin{aligned}(i-1)q^{r-1}+k_i\left(q^{r-2}+q^{r-1}\right)+t_i\left(q^r+1\right) &= q^{r-1}\left(i-1+k_i+t_iq\right)+k_iq^{r-2}+t_i\\ &\leq q^{r-1}\left(i+b_i-2\right)+k_iq^{r-2}+t_i.\end{aligned}$$

Ainda, pela escolha dos b_i, temos que $b_i+i-2\leq a$ para $i=1,2,\ldots,l$. Por outro lado,

$$k_i+t_iq\leq b_i-1<a=b+cq.$$

Isto implica que, $k_i<b$ e $t_i<c$. Logo,

$$\begin{aligned}(i-1)q^{r-1}+k_i\left(q^{r-2}+q^{r-1}\right)+t_i\left(q^r+1\right) &< aq^{r-1}+k_iq^{r-2}+t_i\\ &< aq^{r-1}+bq^{r-2}+c=t^{\perp}\end{aligned}$$

E assim, pelo Lema 4.1.3, obtemos os resultado.

Agora, reordenamos os elementos definidos em (4.9) como segue

$$\begin{aligned}1,y,\ldots,y^{q-1},z,yz,\ldots y^{r_1}z^{s_1}\ ;\ x,xy,\ldots,xy^{q-1},xz,xyz,\ldots,xy^{r_2}z^{s_2}\ ;\\ x^2,x^2y,\ldots,x^2y^{q-1},x^2z,x^2yz,\ldots,x^2y^{r_3}z^{s_3}\ ;\ \ldots\\ ;\ x^{l-1},x^{l-1}y,\ldots,x^{l-1}y^{q-1},x^{l-1}z,x^{l-1}yz,\ldots,x^{l-1}y^{r_l}z^{s_l}.\end{aligned}\tag{4.10}$$

Mostremos agora que cada parcela definida na expressão (4.10), ou seja,

$$x^{i-1},x^{i-1}y,\ldots,x^{i-1}y^{q-1},x^{i-1}z,x^{i-1}yz,\ldots,x^{i-1}y^{r_i}z^{s_i}\tag{4.11}$$

onde $r_i+qs_i=b_i-1$, tem b_i elementos, para $i=1,2,\ldots,l$. Com efeito, pela definição de (4.9), temos que o máximo valor que pode ter r_i é $q-1$. Por outro lado, podemos rescrever (4.11) em duas parcelas da forma

$$\begin{aligned}x^{i-1}y^0z^0,x^{i-1}yz^0,x^{i-1}y^2z^0,\ldots,x^{i-1}y^{q-1}z^0\ ;\\ x^{i-1}y^0z,x^{i-1}yz,\ldots,x^{i-1}y^{q-1}z,\ldots,x^{i-1}y^0z^2,\ldots,\\ x^{i-1}y^{q-1}z^2,\ldots,x^{i-1}y^0z^{s_i},x^{i-1}yz^{s_i},\ldots,x^{i-1}y^{q-1}z^{s_i}.\end{aligned}$$

Notemos que a primeira parcela tem q elementos e a segunda parcela tem qs_i elementos. Consequentemente, a expressão (4.11) possui $q+qs_i$ elementos. Lembrando, novamente que o máximo valor de r_i é $q-1$. Então, (4.11) contém

$$q+qs_i=(r_i+1)+qs_i=b_i,$$

elementos, para $i=1,2,\ldots,l$. E, pela construção dos b_i, podemos concluir que (4.10) possui $a+1$ elementos. Assim, podemos escolher um submatriz B de A de tamanho $(a+1)\times(a+1)$, definida como segue

$$B=\left(\upsilon_{(i-1)k_it_i}\left(P_{\alpha_1,\beta_{1,1}}\right),\ldots,\upsilon_{(i-1)k_it_i}\left(P_{\alpha_1,\beta_{1,b_1}}\right),\ldots,\upsilon_{(i-1)k_it_i}\left(P_{\alpha_l,\beta_{l,b_l}}\right)\right),$$

onde os $v_{(i-1)k_it_i}$ são elementos definidos em (4.10).

Observemos, por exemplo, que B contém uma submatriz de ordem $b_2 \times b_3$, a saber, para $r_2 + s_2q = b_2 - 1$, temos

$$B_{2,3} = \begin{pmatrix} x\left(P_{\alpha_3,\beta_{3,1}}\right) & x\left(P_{\alpha_3,\beta_{3,2}}\right) & \cdots & x\left(P_{\alpha_3,\beta_{3,b_3}}\right) \\ xy\left(P_{\alpha_3,\beta_{3,1}}\right) & xy\left(P_{\alpha_3,\beta_{3,2}}\right) & \cdots & xy\left(P_{\alpha_3,\beta_{3,b_3}}\right) \\ \vdots & \vdots & \cdots & \vdots \\ xy^{q-1}\left(P_{\alpha_3,\beta_{3,1}}\right) & xy^{q-1}\left(P_{\alpha_3,\beta_{3,2}}\right) & \cdots & xy^{q-1}\left(P_{\alpha_3,\beta_{3,b_3}}\right) \\ xz\left(P_{\alpha_3,\beta_{3,1}}\right) & xz\left(P_{\alpha_3,\beta_{3,2}}\right) & \cdots & xz\left(P_{\alpha_3,\beta_{3,b_3}}\right) \\ \vdots & \vdots & \cdots & \vdots \\ xy^{r_2}z^{s_2}\left(P_{\alpha_3,\beta_{3,1}}\right) & xy^{r_2}z^{s_2}\left(P_{\alpha_3,\beta_{3,2}}\right) & \cdots & xy^{r_2}z^{s_2}\left(P_{\alpha_3,\beta_{3,b_3}}\right) \end{pmatrix}$$

Lembrando que $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$, então $B_{2,3} = \alpha D_{2,3}$, onde

$$D_{2,3} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_{3,1} & \beta_{3,2} & \cdots & \beta_{3,b_3} \\ \vdots & \vdots & \cdots & \vdots \\ \beta_{3,1}^{q-1} & \beta_{3,2}^{q-1} & \cdots & \beta_{3,b_3}^{q-1} \\ z\left(P_{\alpha_3,\beta_{3,1}}\right) & z\left(P_{\alpha_3,\beta_{3,2}}\right) & \cdots & z\left(P_{\alpha_3,\beta_{3,b_3}}\right) \\ \vdots & \vdots & \cdots & \vdots \\ \beta_{3,1}^{r_2}z^{s_2}\left(P_{\alpha_3,\beta_{3,1}}\right) & \beta_{3,2}^{r_2}z^{s_2}\left(P_{\alpha_3,\beta_{3,2}}\right) & \cdots & \beta_{3,b_3}^{r_2}z^{s_2}\left(P_{\alpha_3,\beta_{3,b_3}}\right) \end{pmatrix}$$

Por outro lado, como $z = x^{q+1} - y^q + x^{q-1}y$, então $z(P_{\alpha,\beta}) = \alpha^{q+1} - \beta^q + \alpha^{q-1}\beta$. Assim, com operações elementares entre linhas, temos que a matriz $D_{2,3}$ é equivalente à matriz $\overline{D}_{2,3}$, onde

$$\overline{D}_{2,3} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_{3,1} & \beta_{3,2} & \cdots & \beta_{3,b_3} \\ \vdots & \vdots & \cdots & \vdots \\ \beta_{3,1}^{q-1} & \beta_{3,2}^{q-1} & \cdots & \beta_{3,b_3}^{q-1} \\ -\beta_{3,1}^{q} & -\beta_{3,2}^{q} & \cdots & -\beta_{3,b_3}^{q} \\ \vdots & \vdots & \cdots & \vdots \\ (-1)^{s_2}\beta_{3,1}^{b_2-1} & (-1)^{s_2}\beta_{3,2}^{b_2-1} & \cdots & (-1)^{s_2}\beta_{3,b_3}^{b_2-1} \end{pmatrix}$$

Assim, indutivamente, temos que $B = [B_{ij}]$, $i, j = 1, 2, \ldots, l$, onde cada B_{ij} são matrizes de ordem $b_i \times b_j$ e cada entrada (u, v) é

$$\alpha_j^{i-1}\beta_{j,v}^{u_1}z^{u_2}\left(P_{\alpha_j,\beta_{j,v}}\right), \qquad u_1 + u_2q = u - 1.$$

Assim, $B_{ij} = \alpha_j^{i-1} D_{ij}$, onde

$$D_{ij} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_{j,1} & \beta_{j,2} & \cdots & \beta_{j,b_j} \\ \vdots & \vdots & \cdots & \vdots \\ \beta_{j,1}^{q-1} & \beta_{j,2}^{q-1} & \cdots & \beta_{j,b_j}^{q-1} \\ z\left(P_{\alpha_j,\beta_{j,1}}\right) & z\left(P_{\alpha_j,\beta_{j,2}}\right) & \cdots & z\left(P_{\alpha_j,\beta_{j,b_j}}\right) \\ \vdots & \vdots & \cdots & \vdots \\ \beta_{j,1}^{r_i} z^{s_i}\left(P_{\alpha_j,\beta_{j,1}}\right) & \beta_{j,2}^{r_i} z^{s_i}\left(P_{\alpha_j,\beta_{j,2}}\right) & \cdots & \beta_{j,b_j}^{r_i} z^{s_i}\left(P_{\alpha_j,\beta_{j,b_j}}\right) \end{pmatrix}$$

tal que $r_i + s_i q = b_i - 1$. Além disso, D_{ij} é equivalente à matriz $\overline{D}_{ij}$ onde

$$\overline{D}_{ij} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_{j,1} & \beta_{j,2} & \cdots & \beta_{j,b_j} \\ \vdots & \vdots & \cdots & \vdots \\ \beta_{j,1}^{q-1} & \beta_{j,2}^{q-1} & \cdots & \beta_{j,b_j}^{q-1} \\ -\beta_{j,1}^{q} & -\beta_{j,2}^{q} & \cdots & -\beta_{j,b_j}^{q} \\ \vdots & \vdots & \cdots & \vdots \\ (-1)^{s_i}\beta_{j,1}^{b_i-1} & (-1)^{s_i}\beta_{j,2}^{b_i-1} & \cdots & (-1)^{s_i}\beta_{j,b_j}^{b_i-1} \end{pmatrix}$$

Finalmente, usando o método de eliminação de Gauss e por indução, temos que

$$\det(B) = \left(\prod_{i=1}^{l} \det(D_{ii})\right)\left(\prod_{j=2}^{l} \mu_j^{b_j}\right) = \left(\prod_{i=1}^{l} \det(\overline{D}_{ii})\right)\left(\prod_{j=2}^{l} \mu_j^{b_j}\right),$$

onde $\mu_j = \prod_{i=1}^{j-1} (\alpha_j - \alpha_i)$, com $j = 2, 3, \ldots, l$. Ainda, como os α_i são dois a dois distintos para $i = 1, 2, \ldots, l$, temos que $\mu_j \neq 0$, para cada $j = 2, 3, \ldots, l$. Por outro lado, os B_{ij} são dois a dois distintos para cada $i = 1, 2, \ldots, l$, então $\det(D_{ii}) = \det(\overline{D}_{ii}) \neq 0$.

Consequentemente, $\det(B) \neq 0$. Assim, $a + 1 = Posto(B) \leq Posto(A) \leq a + 1$. Portanto, quaisquer $a + 1$ colunas de A são linearmente independentes. ✓

Teorema 4.2.1. *Para $n \leq m \leq n + 2g - 2$, seja $t^{\perp} \leq m^{\perp} = n + 2g - 2$ o maior inteiro tal que $t^{\perp} = aq^{r-1} + b^{r-2} + c$, como foi definido no Lema 4.2.1, com $a \geq b + cq$. Então, a distância mínima d_m de CH_m cumpre*

i) $d_m = a + 2$ se $a = b + cq$.

ii) $d_m = a + 2$ se $a > b + cq$ com $a = b' + c'q$ para $b', c' \in \mathbb{Z}$, e $b' < b$.

iii) $d_m = a + 1$ se $a > b + cq$ com $a = b' + c'q$ para $b', c' \in \mathbb{Z}$, e $b' \geq b$.

Demonstração. Pela observação 4.2.2, sabemos que $\mathcal{L}(m^{\perp}Q_{\infty}) = \mathcal{L}(t^{\perp}Q_{\infty})$. Além disso, a matriz teste de paridade do código CH_m é a matriz geradora do código dual $CH_m^{\perp}$, mas das hipótese e pela Proposição 4.2.1, temos que $CH_m^{\perp} = CH_{m^{\perp}} = CH_{t^{\perp}}$.

Por outro lado, pela Proposição 2.1.1, sabemos que a distância mínima de um código é d se, e somente se, na matriz teste de paridade quaisquer $d-1$ colunas são linearmente independentes e existem d colunas linearmente dependentes.

i) Seja $a = b + cq$. Da prova do Lema 4.2.2, temos que uma base para $\mathcal{L}(t^{\perp}Q_{\infty})$ é dada por

$$\{1, x, y, x^2, xy, y^2, \ldots, x^{q-1}, x^{q-2}\ldots, y^{q-1}, x^q, z, x^{q-1}y, \ldots, x^q y,$$
$$yz, x^{q-1}y^2, \ldots, x^a, \ldots x^q y^b z^{c-1}, y^b z^c\}$$

Logo, a matriz teste da paridade do código CH_m é

$$H = \begin{pmatrix} 1\,(P_{\alpha,\beta}) \\ x\,(P_{\alpha,\beta}) \\ y\,(P_{\alpha,\beta}) \\ \vdots \\ x^{q-1}\,(P_{\alpha,\beta}) \\ x^{q-2}\,(P_{\alpha,\beta})\,y\,(P_{\alpha,\beta}) \\ \vdots \\ y^{q-1}\,(P_{\alpha,\beta}) \\ x^q\,(P_{\alpha,\beta}) \\ z\,(P_{\alpha,\beta}) \\ x^{q-1}\,(P_{\alpha,\beta})\,y\,(P_{\alpha,\beta}) \\ \vdots \\ x^a\,(P_{\alpha,\beta}) \\ \vdots \\ y^b\,(P_{\alpha,\beta})\,z^c\,(P_{\alpha,\beta}) \end{pmatrix}$$

Consideremos agora o conjunto

$$\{P_i = P_{0,\beta_i} \mid P_i \in Supp(D),\ \ i = 1, 2, \ldots, q^{r-1},\ \ \beta_i \neq \beta_j \text{ para } i \neq j\}.$$

Além disso, do final da Observação 4.2.2, temos que $a + 2 \leq q^{r-1}$.

Consideremos a submatriz B de H cujas colunas sejam as classes correspondentes a $P_1, P_2, \ldots, P_{a+2}$. Assim,

$$B = \begin{pmatrix} 1\,(P_1) & \cdots & 1\,(P_{a+1}) \\ x\,(P_1) & \cdots & x\,(P_{a+1}) \\ y\,(P_1) & \cdots & y\,(P_{a+1}) \\ \vdots & \cdots & \vdots \\ x^{q-1}\,(P_1) & \cdots & x^{q-1}\,(P_{a+1}) \\ x^{q-2}\,(P_1)\,y\,(P_1) & \cdots & x^{q-2}\,(P_{a+1})\,y\,(P_{a+1}) \\ \vdots & \cdots & \vdots \\ y^{q-1}\,(P_1) & \cdots & y^{q-1}\,(P_{a+1}) \\ x^{q}\,(P_1) & \cdots & x^{q}\,(P_{a+1}) \\ z\,(P_1) & \cdots & z\,(P_{a+1}) \\ x^{q-1}\,(P_1)\,y\,(P_1) & \cdots & x^{q-1}\,(P_{a+1})\,y\,(P_{a+1}) \\ \vdots & \cdots & \vdots \\ x^{a}\,(P_1) & \cdots & x^{a}\,(P_{a+1}) \\ \vdots & \cdots & \vdots \\ y^{b}\,(P_1)\,z^{c}\,(P_1) & \cdots & y^{b}\,(P_{a+1})\,z^{c}\,(P_{a+1}) \end{pmatrix}$$

Por outro lado, como $x\,(P_{\alpha,\beta}) = \alpha$, $y\,(P_{\alpha,\beta}) = \beta$ e $z = x^{q+1} - y^q + x^{q-1}y$. Então, $x(P_i) = 0$ e $z(P_i) = -\,(\beta_i)^q$. Logo, usando propriedades das matrizes, temos que B é equivalente a

$$B = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{a+2} \\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \cdots & \beta_{a+2}^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \beta_1^{q-1} & \beta_2^{q-1} & \beta_3^{q-1} & \cdots & \beta_{a+2}^{q-1} \\ -\beta_1^{q} & -\beta_2^{q} & -\beta_3^{q} & \cdots & -\beta_{a+2}^{q} \\ -\beta_1^{q+1} & -\beta_2^{q+1} & -\beta_3^{q+1} & \cdots & -\beta_{a+2}^{q+1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ (-1)^c\beta_1^{a} & (-1)^c\beta_2^{a} & (-1)^c\beta_3^{a} & \cdots & (-1)^c\beta_{a+2}^{a} \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Consequentemente, B contém uma submatriz de ordem $(a+1) \times (a+1)$ com determinante não nulo, pois os β_i são dois a dois distintos. Portanto, o posto de B é $a+1$, e daí H possui $a+2$ colunas linearmente dependentes. Finalmente, pelo Lema 4.2.2, sabemos que quaisquer $a+1$ colunas de H são linearmente independentes, ou seja, $d_m = a+2$.

ii) Suponha que $a > b + cq$, $a = b' + c'q$ e $b' < b$. Notemos que

$$\begin{aligned} & b' \leq b - 1 \\ \Rightarrow \;& b'q^{r-2} \leq bq^{r-2} - q^{r-2} \\ \Rightarrow \;& b'q^{r-2} + c' \leq bq^{r-2} - q^{r-2} + c' < bq^{r-2} \leq bq^{r-2} + c. \end{aligned}$$

Isto implica que $b'q^{r-2} + c' \leq bq^{r-2} + c$.

Agora, provemos que os elementos $y^{b'}z^{c'}$ onde $a = b' + c'q \leq q^{r-1} - 2$, com $0 \leq b, b' \leq q$ e $0 \leq c, c' \leq q^{r-2}$ são elementos básicos de $\mathcal{L}(t^{\perp}Q_{\infty})$. Com efeito,

$$\begin{aligned} b'\left(q^{r-2} + q^{r-1}\right) + c\left(q^r + 1\right) &= b'q^{r-2} + b'q^{r-1} + c'q^r + c' \\ &= q^{r-1}\left(b' + c'q\right) + q^{r-2}b' + c' \\ &= aq^{r-1} + b'q^{r-2} + c' \\ &\leq aq^{r-1} + bq^{r-2} + c = t^{\perp}. \end{aligned}$$

Além disso, notemos que a quantidade de elementos desta forma é $qq^{r-2} = q^{r-1}$.

Como $a + 2 \leq q^{r-1}$, analogamente ao item (i), podemos encontrar uma submatriz B', da matriz teste de paridade H de CH_m, da mesma forma que a matriz B do item (i) que tem posto $a + 1$. Logo, a matriz H tem $a + 2$ colunas linearmente dependentes. Consequentemente,

$$d_m \leq a + 2. \tag{4.12}$$

Finalmente, se definimos

$$k = n + 2g - 2 - b'\left(q^{r-2} + q^{r-1}\right) - c\left(q^r + 1\right),$$

temos que

$$k^{\perp} = b'\left(q^{r-2} + q^{r-1}\right) + c\left(q^r + 1\right),$$

onde $0 \leq b + cq \leq a = b' + c'q \leq q^{r-1} - 2$. Logo, pelo item (i), obtemos que a distância mínima do código CH_k é $d_k = a + 2$.

Mas ainda,

$$\begin{aligned} k^{\perp} &= b'\left(q^{r-2} + q^{r-1}\right) + c\left(q^r + 1\right) \\ &= aq^{r-1} + b'q^{r-2} + c' \\ &\leq aq^{r-1} + bq^{r-2} + c = t^{\perp}. \end{aligned}$$

Assim, se $k^{\perp} \leq t^{\perp}$, então $t < k$. Consequentemente, $d_m = d_t \geq d_k = a + 2$, ou seja,

$$d_m \geq a + 2. \tag{4.13}$$

Podemos assim concluir, de (4.12) e (4.13) que, $d_m = a + 2$.

iii) É analoga à prova do item (ii).

✓

Observação 4.2.4. *Os parâmetros do código CH_m também podem ser calculados utilizando-se o fato que a curva χ dada pela equação* (4.1) *é Castle, para resultados sobre isso veja [10] e [11].*

Exemplo 4.2.1. *Para $q = 2$ e $r = 3$, temos o corpo de funções $\mathbb{F}_8(x, y)$ definido por $y^4 + y^2 + y = x^3 + x^5 + x^6$. Aplicando o Lema* 4.1.1*, obtemos que a quantidade de lugares de grau um é $N = 33$ e o gênero $g = 6$. Ainda, pela Proposição* 4.1.1*, concluimos que o semigrupo de Weierstrass para o divisor polo Q_∞ é $H(Q_\infty) = \langle 4, 6, 9\rangle$.*

Além disso, notemos que os números

$$\{4, 6, 8, 10, 12, 16, 18, 20, 22, 24, 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42\}$$

são números polo de Q_∞ que satisfazem as hipóteses das Proposições 4.2.2*,* 4.2.3*, e do Teorema* 4.2.1*. Assim, podemos calcular os parâmetros dos códigos CH_m listados na seguinte tabela.*

m	[n,k,d]	m	[n,k,d]	m	[n,k,d]
4	[32,2,28]	24	[32,19,8]	35	[32,29,3]
6	[32,3,26]	26	[32,21,6]	36	[32,29,3]
8	[32,4,24]	28	[32,23,4]	37	[32,30,2]
10	[32,6,22]	29	[32,24,4]	38	[32,30,2]
12	[32,7,20]	30	[32,25,4]	39	[32,31,2]
16	[32,11,16]	31	[32,26,4]	40	[32,31,2]
18	[32,13,14]	32	[32,26,4]	41	[32,31,2]
20	[32,15,12]	33	[32,27,4]	42	[32,31,2]
22	[32,17,10]	34	[32,28,3]		

Tabela 1 – Parâmetros para o código CH_m.

REFERÊNCIAS

[1] BARRERO, A. I.; MUNERA, C. The Weight Hierarchy of Hermitian Codes. *SIAM J. Discrete Math*, v. 13, n. 1, p. 79-104.

[2] BULYGIN, S. V. Generalized Hermitian codes over GF(2^r). *IEEE Transactions on information theory*, v. 52, p. 4664-4669, 2006.

[3] COUTINHO, M. *Corpos finitos e códigos corretores de erros.* Trabalho de Conclusão de Curso do Bacharelado em Matemática, Universidade Federal de Juiz de Fora, 2014.

[4] GARCIA, A.; STICHTENOTH, H. A class of polynomials over finite fields. *Finite Fields Appl*, v. 5, p. 424-435, 1999.

[5] GOPPA, V. Codes on algebraic curves. *Sov. Math.-Dokl*, v. 24, p. 170-172, 1981.

[6] HEFEZ, A.; VILLELA, M.L. *Códigos Corretores de Erros. 2 ed.* Rio de Janeiro: IMPA, 2008.

[7] KIRFEL, C.; PELLIKAAN, R. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE, Transactions on information theory*, v. 41, p. 1720-1732, 1995.

[8] MUNUERA, C.; SEPÚLVEDA, A.; TORRES, F. Generalized Hermitian Codes. *Des. Codes Cryptogr*, v. 69, n. 69, p. 123-130, 2013. DIO 10.100/s10623-012-9627-0.

[9] MUNUERA, C. On the generalized Hamming weights of geometric Goppa codes. *IEEE Transactions on information theory*, v. 40, p. 2094-2099, 1994.

[10] MUNERA, C.; SEPÚLVEDA, A.; TORRES, F. Algebraic geometry codes from castle curves. *Coding Theory an Applications*, p. 117-127. Springer, Heidelberg 2008.

[11] MUNERA, C.; SEPÚLVEDA, A.; TORRES, F. Castle curves and codes. *Adv. Math. Commun*, v. 3, no 4, p. 399-408, 2009.

[12] PELLIKAAN, R. On the gonality of curves, abundant codes and decoding. STICHTENOTH, H. and TSFASMAN, eds., *Lecture Notes in Mathematics, vol. 1518, Coding Theory and Algebraic Geometry*, Springer-Verlag, p. 132-144, 1992.

[13] SHANNON, C. A mathematical theory of communication. *Bell System Technical Journal*, v. 27, p. 656-716, 1948.

[14] STICHTENOTH, H. A Note on Hermitian Codes Over GF(q^2). *IEEE Transactions on information theory*, v. 34, n. 5, p. 1345-1348, sep. 1988.

[15] STICHTENOTH, H. *Algebraic Function Fields and Codes. 2 ed.* New York: Springer-Verlag, 2009.

[16] TSFASMAN, M.A.; VLADUT S.G.; ZINK T. Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilberth bound.*Math. Nachr.*, v. 109, p. 21-28, 1982.

[17] TSFASMAN, M.A.; VLADUT S.G. Algebraic-Geometric Codes. *Kluwer Academic Publisher*, Dordrecht-Boston-London, 1991.

[18] VAN LINT, J. *Introduction to Coding Theory*, 2 ed. Springer-Verlag, 1992.

[19] WEIL, V. K. Generalized Hamming Weights for Linear Codes. *IEEE Transactions on information theory*, v. IT-37, p. 1412-1418, sep. 1991.

[20] YANG, P. KYEONGCHEOL.; KUMAR, V.; STICHTENOTH, H. On the Weight Hierarchy of Geometric Goppa Codes. *IEEE Transactions on information theory*, v. 40, n. 3, p. 913-920, may. 1994.