

Introdução aos Corpos de Funções Algébricas com Exemplos de Códigos Auto-Duais

Ximena Mujica

7 de Agosto de 1997

Introdução aos Corpos de Funções Algébricas com Exemplos de Códigos Auto-Duais

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pela Srta. *Ximena Mujica* e aprovada pela Comissão Julgadora.

Campinas, 16 de Setembro de 1997.

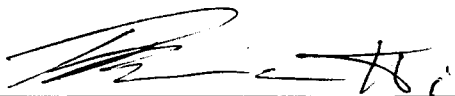
Prof. Dr.


Orientador

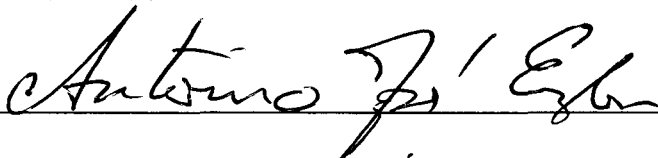
Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em *Matemática*.

Dissertação de Mestrado defendida e aprovada em 16 de setembro de 1997

pela Banca Examinadora composta pelos Profs. Drs.



Prof (a). Dr (a). PAULO ROBERTO BRUMATTI



Prof (a). Dr (a). ANTONIO JOSÉ ENGLER



Prof (a). Dr (a). REGINALDO PALAZZO JÚNIOR

Agradecimentos

Ao prof. P. Brumatti que sempre esteve disponível para tirar as minhas dúvidas, pela dedicação e atenção concedidas.

Ao Diogo, meu companheiro durante todos os seminários, ao estudar a parte mais geral da teoria.

Ao pessoal do SAT que sempre me auxiliou cada vez que eu me atrapalhava com a estação.

À minha família que sempre me deixou estudar com tranquilidade e ao meu pai, por me ceder sua quota de impressão.

A todos aqueles que de alguma maneira me ajudaram a realizar este trabalho.

Sumário

Resumo	v	
Introdução	vi	
I	Corpos de Funções Algébricas	1
I.1	Lugares	1
I.2	Independência de Valorizações	8
I.3	Divisores	12
I.4	O Teorema de Riemann-Roch	19
I.5	Algumas Consequências do Teorema de Riemann-Roch	27
I.6	Componentes Locais dos Diferenciais de Weil	30
II	Códigos Geométricos de Goppa	34
II.1	Códigos	34
II.2	Códigos Geométricos de Goppa	36
II.3	Códigos Geométricos de Goppa Associados com o Corpo de Funções Racionais	43
III	Extensões Algébricas de Corpos de Funções e Códigos Auto-Duais	48
III.1	Extensões Algébricas de Corpos de Funções	48
III.2	Sobre Extensões Integrais de Subanéis de um Corpo de Funções	56
III.3	Alguns Códigos Auto-Duais	72
	Apêndice	80
	Bibliografia	83

Resumo

No Capítulo I desta dissertação introduzimos os conceitos básicos dos corpos de funções algébricas a saber: anéis de valorização, lugares, valorizações discretas, divisores, adeles e os diferenciais de Weil, e obtemos a demonstração de A. Weil do Teorema de Riemann-Roch.

No Capítulo II introduzimos o que são Códigos Lineares, algumas propriedades, Código Dual, a Cota de Singleton e as construções dos Códigos Geométricos de Goppa.

No Capítulo III estudamos Extensões Algébricas de Corpos de Funções e Extensões Integrais de Subanéis de um Corpo de Funções a fim de poder estudar a construção de códigos Auto-Duais numa extensão algébrica F'/F de um corpo de funções racionais. Dentre os resultados a ressaltar estão o Teorema do Diferente de Dedekind e o Teorema das Extensões de Artin-Schreier.

Introdução

Um código corretor de erros é um subespaço vetorial de $\mathbb{F}_q^n$, o espaço vetorial n -dimensional sobre $\mathbb{F}_q$, onde $\mathbb{F}_q$ é um corpo finito. Tais códigos são amplamente utilizados para transmitir informações com mais confiabilidade. Uma forma elementar de se determinar um código C , é considerar um subespaço de $\mathbb{F}_q^n$ e encontrar a sua base; isso nos permite construir uma matriz M denominada matriz geradora do código C ; tais códigos são ditos lineares. Logo, uma forma de construir códigos está relacionada com a construção de matrizes. Mas, se queremos que o código tenha certas propriedades, essa tarefa deixa de ser tão simples.

Em 1983 Goppa mostrou, em seu artigo fundamental [1], como construir códigos por meio de curvas algébricas sobre um corpo finito $\mathbb{F}_q$. Os parâmetros desses códigos podem ser interpretados facilmente, pois possuem um significado geométrico. Tais curvas são geradas por meio de polinômios irredutíveis em duas variáveis sobre um corpo algebricamente fechado K . Mudando o enfoque, esse mesmo polinômio define um corpo de funções sobre o corpo K . Dessa forma, sob um estudo puramente algébrico, podemos construir códigos. A vantagem desta abordagem é que para desenvolvê-la basta ter um conhecimento básico de extensões de corpos algébricas, incluindo Teoria de Galois, e chega-se rapidamente a alguns resultados de grande importância, tais como o teorema de Riemann-Roch.

Nosso objetivo é desenvolver essa teoria e dar alguns exemplos de códigos auto-duais. Inicialmente, fazemos um estudo sobre os conceitos básicos da teoria de corpos de funções. Dentre os vários resultados importantes, mencionamos os dois teoremas de aproximação e o teorema de Riemann-Roch. De posse destas ferramentas, é possível definir os códigos geométricos de Goppa sobre corpos de funções racionais, onde sabemos bem como são seus lugares, divisores e diferenciais.

No entanto, um corpo racional $\mathbb{F}_q(x)$ possibilita a construção de códigos com comprimento no máximo $q + 1$. Mas, numa extensão algébrica $F'/\mathbb{F}_q(x)$, esse número pode ser ampliado consideravelmente. Fazendo um estudo das extensões algébricas de corpos de funções e extensões integrais de subanéis de corpos de funções passamos a ter condições para estudar um código sobre um corpo $F'/\mathbb{F}_q(x)$. Aqui são usados vários resultados da teoria geral de extensões integrais de anéis, os quais são encontrados no Apêndice para maior conveniência do leitor. Finalmente, são apresentados os exemplos de códigos auto-duais. A idéia é encontrar divisores D e G que satisfaçam a condição de auto-dualidade. Como veremos mais adiante, nem sempre é possível encontrar o divisor G necessário, e quando ele existe, por vezes é complicado descrevê-lo explicitamente.

Para encerrar, gostaríamos de dizer que este trabalho foi baseado nas referências [6] e [7].

Capítulo I

Corpos de Funções Algébricas

Neste capítulo iremos introduzir as definições e os conceitos básicos da Teoria dos Corpos de Funções Algébricas, tais como: valorizações, lugares, divisores, gênero de um corpo de funções, adeles e diferenciais de Weil. O principal resultado a ser ressaltado é o Teorema de Riemann-Roch.

I.1 Lugares

I.1.1 Definição Um *corpo de funções algébricas* F/K em uma variável sobre K (corpo arbitrário) é uma extensão de corpos $F \supset K$ tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ o qual é transcendente sobre K . Dizemos que F é um *corpo de funções racionais* se existe $x \in F$ transcendente sobre K tal que $F = K(x)$.

I.1.2 Nota Para simplificar, vamos nos referir a F/K apenas por *corpo de funções*. O conjunto $\tilde{K} := \{z \in F/z \text{ é algébrico sobre } K\}$ é um subcorpo de F , uma vez que a soma, o produto e o inverso de elementos algébricos também são algébricos. $\tilde{K}$ é chamado *corpo das constantes de* F/K . Temos que $K \subseteq \tilde{K} \subseteq F$, e é fácil verificar que $F/\tilde{K}$ é corpo de funções sobre $\tilde{K}$. Dizemos que K é *algébricamente fechado em* F (ou que K é *corpo completo de constantes de* F) se $\tilde{K} = K$.

Para um anel (ou espaço vetorial) A denotaremos por $A^\times$ o conjunto $A \setminus \{0\}$.

I.1.3 Observação Os elementos de F que são transcendentess sobre K podem ser caracterizados como segue: $z \in F$ é transcendente sobre K se e somente se (see) $[F : K(z)] < \infty$.

Agora, iremos introduzir os conceitos de anel de valorização, lugar e valorização discreta; apresentaremos também as suas propriedades e as relações entre os mesmos.

I.1.4 Definição Um *anel de valorização* do corpo de funções F/K é um anel $O \subseteq F$ com as seguintes propriedades:

1. $K \subsetneq O \subsetneq F$
2. $\forall z \in F, z \in O \text{ ou } z^{-1} \in O$

Os resultados I.1.7 e I.1.9 nos dizem que todo anel de valorização é local, i.e., tem um único ideal maximal e este possui elemento primo.

I.1.5 Definição

- (a) Um *lugar* P de F/K é o ideal maximal de um anel de valorização O de F/K ; se $t \in P$ com $P = t.O$, então t é chamado de *elemento primo de* P .
- (b) $\mathbb{P}_F = \{P | P \text{ é lugar de } F/K\}$.

I.1.6 Definição Uma *valorização discreta* de F/K é uma função $v : F \rightarrow \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:

1. $v(x) = \infty \Leftrightarrow x = 0$
2. $v(x.y) = v(x) + v(y), \forall x, y \in F$
3. $v(x + y) \geq \min\{v(x), v(y)\}, \forall x, y \in F$
4. $\exists z \in F$ com $v(z) = 1$
5. $v(a) = 0, \forall a \in K$

I.1.6.1 Nota Neste contexto, o símbolo ∞ se refere a um elemento não pertencente a $\mathbb{Z}$. De 2 e 4 segue que v é sobrejetiva. A propriedade 3 é chamada *Desigualdade Triangular*.

Existem correspondências biunívocas entre os conjuntos dos anéis de valorização, dos lugares e das valorizações discretas. A seguir, veremos suas propriedades e como estes conjuntos estão relacionados. O primeiro resultado que apresentamos tem uma demonstração bastante simples e assim deixaremos de apresentá-la aqui.

I.1.7 Proposição Seja O um anel de valorização do corpo de funções F/K . Então:

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

O lema a seguir é fundamental na prova de que um anel de valorização é principal.

I.1.8 Lema Seja O um anel de valorização do corpo de funções algébricas F/K , P seu ideal maximal e $x \in P$. Sejam $x_1, x_2, \dots, x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$ para $i = 1, 2, \dots, n-1$ então, temos $n \leq [F : K(x)] < \infty$.

Demonstração : Por I.1.3 e I.1.7, segue que $[F : K(x)] < \infty$. Para que $n \leq [F : K(x)]$ basta que $\{x_1, x_2, \dots, x_n\}$ sejam linearmente independentes sobre $K(x)$. Suponha que $\sum_{i=1}^n \varphi_i.x_i = 0$, com algum $\varphi_i \neq 0$ e $\varphi_i \in K(x)$. Como cada φ_i é do tipo $\frac{f_i(x)}{g_i(x)}$ e pertencente a um domínio de integridade, então, podemos supor que $\varphi_i \in K[x], i = 1, 2, \dots, n$ e que x não divide algum deles. Seja $a_i = \varphi_i(0)$ e defina $j \in \{1, 2, \dots, n\}$ tal que $a_j \neq 0$ e $a_i = 0$, se $i > j$. Logo, x/φ_i , para $i > j$. Então, obtemos:

$$-\varphi_j.x_j = \sum_{i \neq j} \varphi_i.x_i \quad (\text{I.1})$$

Como $\varphi_i = b_0 + b_1x + \dots + b_{m_i}x^{m_i} \in K[x] \subset O, \forall i = 1, 2, \dots, n$, para $i < j$, $x_i \in x_jP$ e para $i > j$, $\varphi_i = x.h_i$, onde $h_i(x) \in K[x]$; ao dividir a equação I.1 por x_j , obtemos

$$-\varphi_j = \sum_{i < j} \varphi_i \frac{x_i}{x_j} + \sum_{i > j} \frac{x}{x_j} h_i x_i$$

Logo, $\varphi_j \in P$. Por outro lado, $\varphi_j = a_j + x.g_j$ com $g_j \in K[x] \subset O$ e $x \in P$; logo $a_j = \varphi_j - x.g_j \in P$, mas $P \cap \tilde{K} = \{0\} \Rightarrow a_j = 0$, contradição! Portanto, os $\varphi_i = 0$ e os $\{x_1, x_2, \dots, x_n\}$ são l.i.'s's $\Rightarrow n \leq [F : K(x)]$ $\square$

I.1.9 Teorema *Seja O um anel de valorização do corpo de funções F/K e P seu único ideal maximal. Então:*

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

Demonstração :

- (a) Suponha que P não é principal e escolha $x_1 \in \dot{P}$. Como $P \neq x_1.O$, $\exists x_2 \in P \setminus x_1.O$. Logo, $x_2.x_1^{-1} \notin O \Rightarrow x_2^{-1}.x_1 \in P \Rightarrow x_1 \in x_2.P$. Se $P = x_1.O + x_2.O$, como $x_1 \in x_2.P$ temos $x_1 = x_2.y$, $y \in P$ e portanto, $P = x_2.y.O + x_2.O = x_2.O$. Como P não é principal $\exists x_3 \in P \setminus x_2.O$. Logo, $x_3.x_2^{-1} \notin O \Rightarrow x_3^{-1}.x_2 \in P \Rightarrow x_2 \in x_3.P$. Por indução, obtêm-se uma sequência infinita $x_1, x_2, x_3, \dots \in P$ tal que $x_i \in x_{i+1}.P$, $i \geq 1$, absurdo!, pois por I.1.8, $[F : K(x_1)] < \infty$.

- (b) Como $\forall z \in F$, $z \in O$ ou $z^{-1} \in O$; vamos supor $z \in O$:

- se $z \in O^* \Rightarrow z = t^0.z$
- se $z \in P = O \setminus O^* \Rightarrow z \in t.O = P$

Existe um maximal $m \geq 1$ com $z \in t^m.O$, uma vez que por I.1.8 o comprimento da sequência

$$x_1 = z, x_2 = t^{m-1}, \dots, x_m = t \text{ é finito e } z = t^m.u$$

$$\vdash u \in O^*$$

$$u \notin O^* \Rightarrow u \in P \Rightarrow u = t.w \Rightarrow z = t^{m+1}w, \text{ absurdo!}$$

- (c) Seja $(0) \neq I \subseteq O$ ideal. Se $I = O$, temos $I = t^0.O = O$. Portanto podemos supor $I \subsetneq O$ e neste caso, $I \subseteq P = t.O$. Considere

$A = \{r \in \mathbb{N} / t^r \in I\}$ e $n = \min(A)$, já que $A \neq \emptyset$. Vamos mostrar que $I = t^n.O$:

$$(\supseteq) \quad n = \min(A) \Rightarrow t^n \in I \Rightarrow t^n.O \subseteq I$$

$$(\subseteq) \quad 0 \neq y \in I, y = t^a.u, u \in O^*; \text{ assim } t^a \in I \text{ e } a \geq n = \min(A); \text{ portanto, } y = t^n(t^{a-n}.u) \in t^n.O.$$

□

O resultado a seguir tem uma demonstração muito simples a qual será omitida.

I.1.10 Lema (Desigualdade Triangular Estrita) *Seja v uma valorização discreta de F/K e $x, y \in F$ com $v(x) \neq v(y)$. Então*

$$v(x + y) = \min\{v(x), v(y)\}$$

I.1.11 Definição Para qualquer lugar $P \in \mathbb{P}_F$ podemos definir uma função $v_P : F \rightarrow \mathbb{Z} \cup \{\infty\}$ da seguinte forma: escolha um elemento primo $t \in P$; então todo $z \in \dot{F}$ possui uma representação da forma $z = t^n.u$, $u \in O_P^*$, $n \in \mathbb{Z}$. Defina $v_P(z) = n$ e $v_P(0) = \infty$.

Esta definição depende somente de P , não da escolha de t . De fato, se s é um outro elemento primo de P , então $P = t.O = s.O$; logo, $t = s.w$, $w \in O_P^*$. Portanto, $t^n.u = (s^n.w^n).u = s^n.(w^n.u)$, $w^n.u \in O^*$.

A partir desta definição podemos provar de maneira simples o seguinte resultado:

I.1.12 Teorema *Seja F/K um corpo de funções:*

- (a) *para qualquer lugar $P \in \mathbb{P}_F$, a função v_P definida acima é uma valorização discreta de F/K . Além disso, tem-se*

$$\begin{aligned} O_P &= \{z \in F \mid v_P(z) \geq 0\} \\ O_P^* &= \{z \in F \mid v_P(z) = 0\} \\ P &= \{z \in F \mid v_P(z) > 0\} \end{aligned}$$

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

- (b) *Reciprocamente, suponha que v é uma valorização discreta de F/K . Então o conjunto $P = \{z \in F \mid v_P(z) > 0\}$ é um lugar de F/K , e $O_P = \{z \in F \mid v_P(z) \geq 0\}$ é o anel de valorização correspondente.*
- (c) *Qualquer anel de valorização O de F/K é um subanel próprio maximal de F .*

I.1.13 Nota *Seja P um lugar de F/K e O_P seu anel de valorização. Como P é ideal maximal, o anel das classes residuais O_P/P é um corpo. Para $x \in O_P$ definimos $x(P) \in O_P/P$ como a classe residual de x módulo P ; para $x \in F \setminus O_P$ definimos $x(P) = \infty$ (note que o símbolo ∞ tem aqui um significado distinto daquele na Definição I.1.6). Pela Proposição I.1.7 sabemos que $K \subset O_P$ e $K \cap P = \{0\}$, de modo que a aplicação $O_P \rightarrow O_P/P$ induz uma imersão canônica de K em O_P/P . Assim, vamos sempre considerar K como um subcorpo de O_P/P através desta imersão. Observe que este argumento também se aplica a $\tilde{K}$; logo, podemos considerar $\tilde{K}$ subcorpo de O_P/P .*

I.1.14 Definição *Seja $P \in \mathbb{P}_F$*

- (a) $F_P = O_P/P$ é o *corpo de resíduos do lugar P* . A aplicação $x \rightarrow x(P)$ de F em $F_P \cup \{\infty\}$ é chamada *aplicação de classes residuais com relação a P* . Também usaremos a notação $x + P = x(P)$ para $x \in O_P$.
- (b) $\deg P = [F_P : K]$ é chamado *grau de P* .

I.1.15 Proposição *Se P é um lugar de F/K e $x \in \dot{P}$, então*

$$\deg P \leq [F : K(x)] < \infty$$

Demonstração : Por I.1.3, $[F : K(x)] < \infty$. Observe que basta mostrar que se os elementos $z_1(P), z_2(P), \dots, z_n(P)$ são l.i.'s sobre K então, $z_1, z_2, \dots, z_n$ são l.i.'s sobre $K(x)$, onde $z_i(P) = z_i + P$, para $i = 1, 2, \dots, n$. Supondo que existe uma combinação linear não trivial

$$\sum_{i=1}^n \varphi_i z_i = 0$$

com $\varphi_i \in K(x)$, podemos supor que os φ_i são polinômios em x ($\varphi_i \in K[x]$) e não todos divisíveis por x , i.e., $\exists j \in \{1, 2, \dots, n\}$ tal que $\varphi_j(0) = a_j \neq 0$ (i.e., $\varphi_j = a_j + x.g_j, a_j \in K, g_j \in K[x]$). Usando a aplicação residual módulo P :

$$\begin{aligned} 0 &= \sum_{i=1}^n \varphi_i . z_i \Rightarrow 0(P) = \sum_{i=1}^n \varphi_i(P) . z_i(P) \\ &= \sum_{i=1}^n a_i . z_i(P) \end{aligned}$$

Como os $z_i(P)$ são l.i.'s sobre $K \Rightarrow a_i = 0 \forall i$. Absurdo! Logo, os z_i são l.i.'s sobre $K(x)$. $\square$

I.1.16 Corolário *O corpo $\tilde{K}$ das constantes de F/K é uma extensão finita de K .*

Demonstração : Usaremos o fato que $\mathbb{P}_F \neq \emptyset$ (a ser provado mais adiante). Considere um $P \in \mathbb{P}_F$. Como $\tilde{K}$ está imerso em F_P através da aplicação residual $O_P \rightarrow F_P$, segue que $[\tilde{K} : K] \leq [F_P : K] < \infty$. $\square$

I.1.17 Observação No caso $\deg P = 1$, temos $F_P = K$ e a aplicação das classes residuais leva F em $K \cup \{\infty\}$. Em particular, se K é um corpo algebricamente fechado, qualquer lugar tem grau um, de modo que podemos ver um elemento $z \in F$ como uma função dada por

$$z : \begin{cases} \mathbb{P}_F & \longrightarrow & K \cup \{\infty\} \\ P & \longmapsto & z(P) \end{cases} \quad (I.2)$$

Por isso, F/K é chamado *corpo de funções*. Os elementos de K , interpretados como funções no sentido de (I.2), são funções constantes. Por essa razão K é chamado *corpo de constante* de F .

I.1.18 Definição Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z se e somente se $v_P(z) > 0$; P é um polo de z se e somente se $v_P(z) < 0$. Se $v_P(z) = m > 0$, P é dito ser um zero de z de ordem m ; se $v_P(z) = -m < 0$, P é dito ser um polo de z de ordem m .

I.1.19 Teorema Seja F/K um corpo de funções e R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \subsetneq R$ é um ideal próprio de R . Então existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq O_P$.

Demonstração : Considere o conjunto $\mathcal{F} = \{S \mid S \text{ é subanel de } F \text{ com } R \subseteq S \text{ e } I \cdot S \neq S\}$ e $I \cdot S$ o ideal gerado por I em S . Claramente $\mathcal{F} \neq \emptyset$, pois $R \in \mathcal{F}$.

$\vdash \mathcal{F}$ é indutivamente ordenado pela inclusão

Seja $\mathcal{H} \subseteq \mathcal{F}$ um subconjunto totalmente ordenado; então,

1. $T = \cup_{S \in \mathcal{H}} S$ é um subanel de F com $R \subseteq T$

2. $I \cdot T \neq T$

Suponha que $I \cdot T = T$; assim, temos:

$$1 \in T \Rightarrow 1 \in I \cdot T \Rightarrow \exists a_i \in I, s_i \in T; \sum_{i=1}^n a_i \cdot s_i = 1$$

Como $T = \cup S$ e $S \in \mathcal{H}$, existe $S_0 \in \mathcal{H}$ tal que $s_1, s_2, \dots, s_n \in S_0$ e portanto, $1 = \sum_{i=1}^n a_i \cdot s_i \in I \cdot S_0$. Absurdo! pois, $S_0 \in \mathcal{F}$. Logo, $I \cdot T \neq T$.

T é uma cota superior de $\mathcal{H}$, cadeia totalmente ordenada de $\mathcal{F}$. Logo, pelo Lema de Zorn, $\mathcal{F}$ contém um elemento maximal; isto é existe um anel $O \subseteq F$ tal que $R \subseteq O \subseteq F$, $I \cdot O \neq O$ e O é maximal com essas propriedades: isto é se $O \subsetneq B \subseteq F$ e B é anel, então $I \cdot B = B$.

$\vdash$ Queremos mostrar que O é anel de valorização de F/K . Como $I \neq \{0\}$ e $I \cdot O \neq O$ tem-se, $I \subseteq O \setminus O^*$. Suponhamos que O não é anel de valorização; logo, existe $z \in F$ tal que $z, z^{-1} \notin O$. Então, $O \subsetneq O[z]$ e $O \subsetneq O[z^{-1}]$. Como O é maximal, temos $O[z], O[z^{-1}] \notin \mathcal{F}$, isto é, $I \cdot O[z] = O[z]$ e $I \cdot O[z^{-1}] = O[z^{-1}]$; logo existem $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m \in I \cdot O$ tais que:

$$1 = a_0 + a_1 \cdot z + \dots + a_n \cdot z^n \quad (I.3)$$

$$1 = b_0 + b_1 \cdot z^{-1} + \dots + b_m \cdot z^{-m} \quad (I.4)$$

Como $I \cdot O \neq O$, temos que $a_0 \neq 1$ e $b_0 \neq 1$. Escolhendo as expressões (I.3) e (I.4) com m, n minimais e supondo $n \geq m \geq 1$, usando (I.4), tenho

$$1 \cdot a_n \cdot z^n = a_n(b_0 \cdot z^n + b_1 \cdot z^{n-1} + \dots + b_m \cdot z^{n-m})$$

logo,

$$0 = a_n[(b_0 - 1).z^n + b_1.z^{n-1} + \dots + b_m.z^{n-m}] \quad (I.5)$$

e usando (I.3), temos:

$$1.(b_0 - 1) = (a_0 + a_1 z + \dots + a_n z^n)(b_0 - 1)$$

então

$$0 = (b_0 - 1)[(a_0 - 1) + a_1 z + \dots + a_n z^n]. \quad (I.6)$$

Assim, subtraindo (I.5) de (I.6) temos:

$$\begin{aligned} 0 &= (b_0 - 1)[(a_0 - 1) + a_1.z + \dots + a_n.z^n] - \\ &\quad - a_n[(b_0 - 1).z^n + b_1.z^{n-1} + \dots + b_m.z^{n-m}] \\ &= (b_0 - 1)(a_0 - 1) + (b_0 - 1)(a_1.z + \dots + a_{n-1}.z^{n-1}) - \\ &\quad - a_n(b_1.z^{n-1} + \dots + b_m.z^{n-m}) \\ &= 1 - (a_0 + b_0) + a_0.b_0 + (b_0 - 1)(a_1.z + \dots + a_{n-2}.z^{n-2}) - \\ &\quad - a_n(b_2.z^{n-2} + \dots + b_m.z^{n-m}) + [(b_0 - 1).a_{n-1} - a_n.b_1]z^{n-1} \end{aligned}$$

então

$$\begin{aligned} 1 &= -[a_0.b_0 - (a_0 + b_0) + (b_0 - 1)(a_1.z + \dots + a_{n-2}.z^{n-2}) - \\ &\quad - a_n(b_2.z^{n-2} + \dots + b_m.z^{n-m}) + \\ &\quad + ((b_0 - 1)a_{n-1} - a_n.b_1).z^{n-1}] \in O[z] \end{aligned}$$

Ou seja, n não é minimal; absurdo! Logo, não existe tal z , i.e., O é anel de valorização. Basta considerar $P \subseteq O$ ideal maximal, e portanto lugar, tendo $I \subseteq P$ e $R \subseteq O, P \in \mathbb{P}_F$. $\square$

I.1.20 Corolário *Seja F/K um corpo de funções, $z \in F$ transcendente sobre K . Então z possui pelo menos um zero e um polo. Em particular, $\mathbb{P}_F \neq \emptyset$.*

Demonstração : Considere o anel $R = K[z]$ e o ideal $I = z.K[z]$. Por I.1.19 há um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq O_P$. Logo, P é um zero de z . Analogamente, para z^{-1} , há um lugar $Q \subseteq \mathbb{P}_F$. Logo, Q é um polo de z . Em particular, $\mathbb{P}_F \neq \emptyset$, pois $P, Q \in \mathbb{P}_F$. $\square$

O Corolário I.1.20 pode ser interpretado como segue: todo $z \in F$, com z não pertencente a $\tilde{K}$ de F/K , fornece uma função não constante no sentido de I.1.17.

Estudemos agora o caso específico de um corpo de funções racionais $F = K(x)$, onde x é transcendente sobre K . Dado um polinômio arbitrário mônico e irredutível $p(x) \in K(x)$, considere o anel de valorização

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \right\} \quad (I.7)$$

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

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\} \quad (I.8)$$

No caso particular em que $p(x)$ é linear, i.e., $p(x) = x - \alpha$ com $\alpha \in K$, abreviaremos escrevendo:

$$P_\alpha = P_{x-\alpha} \in \mathbb{P}_{K(x)} \quad (I.9)$$

Existe um outro anel de valorizaçãode $K(x)/K$, a saber

$$O_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) \leq \deg g(x) \right\} \quad (I.10)$$

com ideal maximal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \mid \deg f(x) < \deg g(x) \right\} \quad (I.11)$$

Este é chamado o lugar *infinito* de $K(x)$. Observe que estes rótulos dependem da escolha específica do elemento gerador x de $K(x)$ (por exemplo, $K(x) = K(1/x)$ e o lugar P_∞ com relação a $1/x$ é o lugar P_0 com relação a x).

Para fundamentarmos estas definições, citamos os próximos dois resultados cujas demonstrações serão omitidas pois fogem um pouco do contexto desta dissertação.

I.1.21 Proposição *Seja $F = K(x)$ o corpo das funções racionais:*

- (a) *Seja $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ o lugar definido por (I.8) onde $p(x) \in K[x]$ é um polinômio irredutível. Então $p(x)$ é um elemento primo para P , e a valorização discreta correspondente v_P pode ser descrita como segue: se $z \in K(x) \setminus \{0\}$, então $z = p(x)^n \cdot \frac{f(x)}{g(x)}$ com $f(x), g(x) \in K[x]$, $n \in \mathbb{N}$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. O corpo dos resíduos $K(x)_P = O_P/P$ é isomorfo a $K[x]/p(x)$; um isomorfismo é dado por :*

$$\phi : \begin{cases} K[x]/p(x) & \longrightarrow & K(x)_P \\ f(x) \bmod p(x) & \longmapsto & f(x) \cdot (P) \end{cases}$$

Conseqüentemente, $\deg P = \deg p(x)$.

- (b) *No caso especial $p(x) = x - \alpha$ com $\alpha \in K$, o grau de $P = P_\alpha$ é um e a aplicação de classes residuais é dada por*

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

onde $z(\alpha)$ é definido como segue: escreva $z = \frac{f(x)}{g(x)}$ com polinômios relativamente primos $f(x), g(x) \in K[x]$. Então,

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

- (c) *Finalmente, seja $P = P_\infty$ o lugar infinito de $K(x)/K$ definido por (I.11). Então $\deg P_\infty = 1$. Um elemento primo de P_∞ é $t = 1/x$. A valorização discreta correspondente v_∞ é dada por $v_\infty(f(x)/g(x)) = \deg g(x) - \deg f(x)$, onde $f(x), g(x) \in K[x]$. A aplicação de classes residuais correspondente a P_∞ é determinada por $z(P_\infty) = z(\infty)$ para $z \in K(x)$, onde $z(\infty)$ é definida como segue; se $z = \frac{a_n \cdot x^n + \dots + a_0}{b_m \cdot x^m + \dots + b_0}$ com $a_n, b_m \neq 0$, então*

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

- (d) *K é o corpo completo das constantes de $K(x)/K$.*

Na verdade, devido a um resultado fundamental de Ostrowski, a proposição anterior descreve todos os lugares (e/ou anéis de valorização de $K(x)$).

I.1.22 Teorema *Os únicos lugares no corpo de funções racionais $K(x)/K$ são os lugares $P_{p(x)}$ e P_∞ definidos em (I.8) e (I.11).*

I.2 Independência de Valorizações

O resultado central desta seção é o Teorema de Aproximação Fraca I.2.1 (que é conhecido como o Teorema de Independência). Este Teorema essencialmente estabelece que se $v_1, \dots, v_n$ são valorizações discretas de F/K distintas duas a duas e $z \in F$, e se conhecermos os valores $v_1(z), \dots, v_{n-1}(z)$, nada podemos concluir sobre o valor de $v_n(z)$.

I.2.1 Teorema (da Aproximação Fraca) *Sejam F/K um corpo de funções, $P_1, \dots, P_n \in \mathbb{P}_F$ lugares dois a dois distintos de F/K , $x_1, \dots, x_n \in F$ e $r_1, \dots, r_n \in \mathbb{Z}$. Então, existe algum $x \in F$ tal que*

$$v_{P_i}(x - x_i) = r_i \text{ para } i = 1, \dots, n$$

Demonstração : Para simplificar, seja $v_i = v_{P_i}$. A demonstração deste teorema é construtiva e é feita em vários passos:

Passo 1: $\vdash \exists u \in F : v_1(u) > 0$ e $v_i(u) < 0, i = 2, \dots, n$.

Por indução:

$n = 2$: como os anéis de valorização são maximais, temos que $O_{P_i} \not\subseteq O_{P_j} \forall i \neq j$. Logo, considere $y_1 \in O_{P_1} \setminus O_{P_2}$ e $y_2 \in O_{P_2} \setminus O_{P_1}$. Então $v_1(y_1) \geq 0, v_2(y_1) < 0$ e $v_1(y_2) < 0, v_2(y_2) \geq 0$. Seja $u = y_1/y_2$, então

$$v_i(u) = v_i(y_1)v_i(y_2) \Rightarrow \begin{cases} v_1(u) &= v_1(y_1) - v_1(y_2) &> 0 \\ v_2(u) &= v_2(y_1) - v_2(y_2) &< 0 \end{cases}$$

Agora suponha $n > 2$ e considere y tal que $v_1(y) > 0$ e $v_i(y) < 0, i = 2, \dots, n-1$.

$\vdash \exists u \in F, v_1(u) > 0, v_i(u) < 0, i = 2, \dots, n$.

- se $v_n(y) < 0$, OK!

- se $v_n(y) \geq 0$,

Considere $z \in F, v_1(z) > 0, v_n(z) < 0$ e considere $u = y + z^r$ tal que $r \cdot v_i(z) \neq v_i(y)$ para todo i , logo,

$$v_i(u) = \min\{v_i(y), r \cdot v_i(z)\}$$

Assim, para

$$i = 1, v_1(u) = \min\{v_1(y), r \cdot v_1(z)\} > 0$$

$$i = 2, \dots, n-1, v_i(u) = \min\{v_i(y), r \cdot v_i(z)\} < 0$$

$$i = n, v_n(u) = r \cdot v_n(z) < 0$$

Passo 2: $\vdash \exists w \in F$ tal que $v_1(w-1) > r_1$ e $v_i(w) > r_i, i = 2, \dots, n$.

Considere u do Passo 1 e seja $w = (1 + u^s)^{-1}$ onde $s \in \mathbb{N}$ é grande o bastante para obter:

$$\begin{aligned} v_1(w-1) &= v_1\left(\frac{1}{1+u^s} - 1\right) \\ &= v_1\left(\frac{1 - (1+u^s)}{1+u^s}\right) \\ &= v_1(u^s) - v_1(1+u^s) \\ &= v_1(u^s) - \min\{v_1(1), v_1(u^s)\} \\ &= s \cdot v_1(u) > r_1 \end{aligned}$$

$$\begin{aligned}
v_i(w) &= -v_i(1 + u^s) \\
&= -\min\{v_i(1), s.v_i(u)\} \\
&= r_i
\end{aligned}$$

Passo 3: $\vdash$ dados $y_1, \dots, y_n \in F, \exists z \in F$ com $v_i(z - y_i) > r_i, i = 1, \dots, n$.

Considere $s \in \mathbb{Z}$ tal que $v_i(w_j - 1) \geq s, \forall i, j \in \{1, \dots, n\}$. (Basta considerar $s = \min\{v_i(y_j)/i, j \in \{1, \dots, n\}\}$). Pelo Passo 2, para cada i fixo, existe $w_i \in F$ tal que $v_i(w_i - 1) > r_i - s$ e $v_j(w_i) > r_j - s, j \neq i$. Então $z = \sum_{j=1}^n y_j.w_j$ possui as propriedades desejadas:

$$\begin{aligned}
v_i(z - y_i) &= v_i\left(\sum_{j=1}^n y_j.w_j - y_i\right) \\
&= v_i(y_i(w_i - 1) + \sum_{j \neq i} y_j.w_j) \\
&\geq \min\{v_i(y_i) + v_i(w_i - 1), \min\{v_i(y_j) + v_i(w_j)/j \neq i\}\} \\
&> r_i
\end{aligned}$$

Passo Final: Prova do Teorema

Dados $x_1, \dots, x_n \in F$, pelo Passo 3, $\exists z \in F$ tal que $v_i(z - x_i) > r_i$, para cada $i = 1, \dots, n$. A seguir, escolha $z_i \in F$ tal que $v_i(z_i) = r_i$ (se $t_i \in O_P$ é elemento primo de O_P , considere $z_i = t_i^{r_i}$). Para $z_1, \dots, z_n \in F$, pelo Passo 3, $\exists z' \in F$ tal que $v_i(z' - z_i) > r_i, i = 1, \dots, n$.

Segue que:

$$\begin{aligned}
v_i(z') &= v_i((z' - z_i) + z_i) \\
&= \min\{v_i(z' - z_i), v_i(z_i)\} \\
&= r_i
\end{aligned}$$

Então seja $x = z + z'$:

$$\begin{aligned}
v_i(x - x_i) &= v_i(z + z' - x_i) \\
&= v_i((z - x_i) + z') \\
&= \min\{v_i(z - x_i), v_i(z')\} \\
&= r_i
\end{aligned}$$

□

O resultado a seguir é consequência imediata deste Teorema, e de fato, todo $z \in \bar{F}$ transcendente tem pelo menos um polo.

I.2.2 Corolário *Todo corpo de funções possui infinitos lugares.*

Já demonstramos que se $x \in \mathbb{F}$ é transcendente sobre K então ele tem zeros e polos. O próximo resultado, que é uma consequência do Teorema da Aproximação Fraca, nos fornece de alguma forma, uma estimativa para o número de zeros (polos) de x .

1.2.3 Proposição Seja F/K um corpo de funções e $P_1, \dots, P_n \in \mathbb{P}_F$ zeros de $x \in F$. Então,

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

Demonstração :

Usaremos a notação seguinte: $v_i = v_{P_i}$, $f_i = \deg P_i$, $e_i = v_i(x)$.

$\vdash$ Para cada $i = \{1, \dots, n\}$, $\exists t_i \in F : v_j(t_i) = \delta_{ij}$.

No Teorema 1.2.1 considere $x_k = 0, \forall k = 1, \dots, n, r_i = 1, r_k = 0, \forall k \neq i$. Então obtemos:

$$\begin{aligned} v_k(t_i - x_k) &= r_k \\ &= \begin{cases} v_i(t_i) = 1 & , \quad k = i \\ v_k(t_i) = 0 & , \quad k \neq i \end{cases} \end{aligned}$$

Para cada i fixo, escolha $s_{i1}, \dots, s_{if_i} \in O_{P_i}$ tais que $s_{i1}(P_i), \dots, s_{if_i}(P_i)$ formam uma base de F_{P_i} sobre K .

$\vdash \exists z_{ij} \in F$ tais que $\forall i, j, v_i(s_{ij} - z_{ij}) > 0$ e $v_k(z_{ij}) \geq e_k$

Fixados i, j , considere $x_i = s_{ij}$ e $x_k = 0, \forall k \neq i$. Aplicando 1.2.1: $\exists z_{ij} \in F$ tal que $v_k(z_{ij} - x_k) = r_k$

$$v_k(z_{ij} - x_k) = \begin{cases} v_i(z_{ij} - s_{ij}) = v_i(s_{ij} - z_{ij}) = 1 > 0 & , \quad k = i \\ v_k(z_{ij} - 0) = v_k(z_{ij}) = e_k \geq e_k & , \quad k \neq i \end{cases}$$

$\vdash \{z_{i1}(P_i), \dots, z_{if_i}(P_i)\}$ é base de $O_{P_i}/P_i \cdot O_{P_i}$ sobre K . $v_i(s_{ij} - z_{ij}) = 1 \Rightarrow s_{ij} - z_{ij} \in O_{P_i} : s_{ij}(P_i)$ é da base $\Rightarrow s_{ij}(P_i) \neq 0(P_i) \Rightarrow s_{ij} \notin P_i : s_{ij} - z_{ij} \in P_i \Rightarrow s_{ij}(P_i) = z_{ij}(P_i)$ é da base.

Afirmamos que os elementos $t_i^a \cdot z_{ij}, 1 \leq i \leq r, 1 \leq j \leq f_i, 1 \leq a < e_i$ são linearmente independentes sobre $K(x)$. Temos um total de $\sum_{i=1}^r e_i \cdot f_i = \sum_{i=1}^r \deg P_i \cdot v_i(x)$ elementos. Sendo estes elementos linearmente independentes, o seu numero é menor ou igual ao de elementos que formam uma base de F sobre $K(x)$, fornecendo o resultado.

$\vdash$ Prova da afirmação:

Vamos supor que os elementos acima são linearmente dependentes, logo, existe uma combinação linear não trivial para o zero sobre $K(x)$; sejam $\varphi_{ija} \in K(x)$ tais que

$$0 = \sum_{i=1}^r \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} \cdot t_i^a \cdot z_{ij} \quad (I.12)$$

Sem perda na generalidade, podemos supor que $\varphi_{ija} \in K[x]$, e nem todo φ_{ija} é divisível por x . Logo, existem índices $k \in \{1, \dots, r\}$ e $c \in \{0, \dots, e_k - 1\}$ tais que

$$\begin{aligned} x | \varphi_{ija} \quad \forall a < c, \quad \forall j \in \{1, \dots, f_k\} \text{ e} \\ x \nmid \varphi_{kjc} \text{ para algum } j \in \{1, \dots, f_k\} \end{aligned} \quad (I.13)$$

Multiplicando (I.12) por t_k^{-c} obtemos:

$$0 = \sum_{i=1}^r \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} \quad (I.14)$$

$$= \sum_{j=1}^{f_k} \sum_{a=0}^{e_k-1} \varphi_{kja} t_k^a t_k^{a-c} z_{kj} + \sum_{i \neq k} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} \quad (I.15)$$

Vamos aplicar a valorização v_k à soma (I.14) (note que $\varphi_{ija} \in K[x]; K \subseteq O_{P_k}, x \in P_k \Rightarrow K[x] \subseteq O_{P_k} \Rightarrow v_k(\varphi - ija) \geq 0$):

- para $i \neq k$:

$$\begin{aligned} v_k(\varphi_{ija} t_i^a t_k^{-c} z_{ij}) &= v_k(\varphi_{ija} + av_k(t_i) - cv_k(t_k) + v_k(z_{ij})) \\ &\geq e_k - c \\ (c \leq e_k - 1 \Rightarrow) &> 0 \end{aligned}$$

- para $i = k$

$$- a < c : x/\varphi_{ija} \Rightarrow v_k(\varphi_{ija} \geq e_k)$$

$$\begin{aligned} v_k(\varphi_{kja} t_k^{a-c} z_{kj}) &= v_k(\varphi_{kja}) + (a-c)v_k(t_k) + v_k(z_{kj}) \\ &\geq e_k + (a-c) + 0 \\ &\geq e_k - c \\ &> 0 \end{aligned}$$

$$- a > c : x \nmid \varphi_{kja} \Rightarrow v_k(\varphi_{kja})$$

$$\begin{aligned} v_k(\varphi_{kja} t_k^{a-c} z_{kj}) &= v_k(\varphi_{kja}) + (a-c)v_k(t_k) + v_k(z_{kj}) \\ &\geq a - c \\ &> 0 \end{aligned}$$

Reescrevendo (I.14) temos:

$$\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} = - \underbrace{\left(\sum_{j=1}^{f_k} \sum_{a \neq c} \varphi_{kja} t_i^{a-c} z_{kj} + \sum_{i \neq k} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} \right)}_S$$

Logo, temos:

$$\begin{aligned} v_k(S) > 0 &\Rightarrow \sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} \in P_k \\ &\Rightarrow \sum_{j=1}^{f_k} \varphi_{kjc}(P_k) z_{kj}(P_k) = 0(P_k) \end{aligned}$$

Mas, sabemos que existe $j \in \{1, \dots, f_k\}$ tal que

$$\varphi_{kjc} = \alpha_0 + \alpha_1.x + \dots + \alpha_n.x^n$$

onde $\alpha_0 \neq 0 \Rightarrow \varphi_{kjc}(P_k) = \alpha_0(P_k) = \alpha_0$. Ou seja, obtivemos uma combinação linear não trivial de elementos da base de $OP_i/P_i.OP_i$ sobre K para o 0, Contradição! Logo, foi errôneo supor que os $t_i^a.z_{ij}$ eram linearmente dependentes, seguindo o resultado. $\square$

I.2.4 Corolário Num corpo de funções F/K , qualquer elemento $x \in F$ possui apenas um número finito de zeros e de polos.

Este resultado é clara consequência da Proposição anterior.

I.3 Divisores

A partir de agora F/K irá denotar um corpo de funções algébricas de uma variável tal que K é algébricamente fechado em F .

I.3.1 Definição O grupo abeliano livre que é gerado pelos lugares de F/K é denotado por $\mathcal{D}_F$, o *grupo divisor* de F/K . Os elementos de $\mathcal{D}_F$ são chamados *divisores* de F/K . Em outras palavras, um divisor é uma soma formal

$$D = \sum_{P \in \mathbb{P}_F} n_P \cdot P \text{ com } n_P \in \mathbb{Z}, \text{ e quase todo } n_P \text{ é nulo}$$

O suporte de D é definido por

$$\text{supp} D = \{P \in \mathbb{P}_F | n_P \neq 0\}$$

Frequentemente será conveniente escrever

$$D = \sum_{P \in S} n_P P, \text{ onde } \text{supp} D \subset S$$

Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ é chamado *divisor primo*. Dois divisores $D = \sum n_P P$ e $D' = \sum n'_P P$ são adicionados coeficiente a coeficiente:

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

O elemento zero do grupo divisor $\mathcal{D}_F$ é o divisor

$$0 = \sum_{P \in \mathbb{P}_F} r_P P, \text{ , } r_P = 0, \forall P$$

Para $Q \in \mathbb{P}_F$ e $D = \sum n_P P \in \mathcal{D}_F$ definimos $v_Q(D) = n_Q$; logo,

$$\text{supp} D = \{P \in \mathbb{P}_F | v_P(D) \neq 0\}$$

e

$$D = \sum_{P \in \text{supp} D} v_P(D) P$$

Uma ordem parcial em $\mathcal{D}_F$ é definida por

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2), \forall P \in \mathbb{P}_F$$

Um divisor $D \geq 0$ é chamado *positivo* (ou *efetivo*). O grau de um divisor é definido por:

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

e fornece um homomorfismo $\deg : \mathcal{D}_F \rightarrow \mathbb{Z}$, $D \mapsto \deg D$.

Pelo Corolário I.2.4 qualquer $x \in \bar{F}$ possui apenas um número finito de zeros e polos em $\mathbb{P}_F$. Logo, faz sentido a seguinte definição:

I.3.2 Definição Seja $x \in \dot{F}$ e denote por Z (respectivamente N) o conjunto dos zeros (respectivamente polos) de x em $\mathbb{P}_F$. Então, definimos:

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

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

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x).P \quad (\text{I.16})$$

Os elementos $x \in F$, que são constantes, são caracterizados por

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

Isto segue imediatamente de I.1.20 e I.1.7.

I.3.3 Definição O conjunto

$$\mathcal{P}_F = \{(x) | x \in \dot{F}\}$$

é chamado *grupo dos divisores principais* de F/K . Este é um subgrupo de $\mathcal{D}_F$, pois por I.16 $(x.y) = (x) + (y)$, $\forall x, y \in F$. O grupo quociente

$$\mathcal{C}_F = \mathcal{D}_F / \mathcal{P}_F$$

é chamado *grupo das classes dos divisores*. Para um divisor $D \in \mathcal{D}_F$ sua classe em $\mathcal{C}_F$ é denotada por $[D]$. Dois divisores D, D' são ditos equivalentes, denotados por $D \sim D'$, se $[D] = [D']$, i.e., $D = D' + (x)$ para algum $x \in \dot{F}$.

I.3.4 Definição Para um divisor $A \in \mathcal{D}_F$ definimos

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

Esta definição tem a seguinte interpretação ; se

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

com $n_i, m_j > 0$, então $\mathcal{L}(A)$ é formado pelos elementos $x \in F$ tais que:

1. x tem zeros de ordem $\geq m_j$ em $Q_j, j = 1, \dots, s$ e
2. x pode ter polos somente nos lugares $P_1, \dots, P_r$ onde a ordem de cada polo em P_i tem cota n_i , para cada $i = 1, \dots, r$.

I.3.5 Observação Seja $A \in \mathcal{D}_F$. Então

- (a) $x \in \mathcal{L}(A)$ se $v_P(x) \geq -v_P(A), \forall P \in \mathbb{P}_F$.
- (b) $\mathcal{L}(A) \neq \{0\}$ se existe $A' \sim A$ com $A' \geq 0$.

A prova de (a) e (b) faz uso da definição anterior.

O lema a seguir tem demonstração bastante simples, a qual será omitida.

I.3.6 Lema *Seja $A \in \mathcal{D}_F$. Então:*

- (a) $\mathcal{L}(A)$ é espaço vetorial sobre K .
- (b) Se $A' \sim A$, então, $\mathcal{L}(A) \simeq \mathcal{L}(A')$ (isomorfos como K -espaços vetoriais).
- (c) $\mathcal{L}(0) = K$.
- (d) Se $A < 0$, então, $\mathcal{L}(A) = \{0\}$.

I.3.7 Lema *Sejam A, B divisores de F/K com $A \leq B$. Então temos*

$$\mathcal{L}(A) \subseteq \mathcal{L}(B) \quad \text{e} \quad \dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg B - \deg A$$

Demonstração : $\vdash \mathcal{L}(A) \subseteq \mathcal{L}(B)$

$$A \leq B \Rightarrow -A \geq -B; x \in \mathcal{L}(A) \Rightarrow (x) \geq -A \geq -B \Rightarrow x \in \mathcal{L}(B)$$

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

$$A \leq B \Rightarrow B = A + D, D = \sum_{P \in \mathbb{P}_F} v_P(D) \cdot P \geq 0$$

Vamos fazer a demonstração por indução:

- Considere $D = Q \in \mathbb{P}_F$

Escolha $t \in F$, com $v_Q(t) = v_Q(B) = v_Q(A) + 1$ (podemos fazer isso pelo Teorema de Independência); logo se considerarmos $x \in F$ com $x \in \mathcal{L}(B)$, temos:

$$v_Q(x) \geq -v_Q(B) = -v_Q(A) - 1$$

Considere a aplicação

$$\begin{array}{ccc} \varphi: \mathcal{L}(B) & \longrightarrow & F_Q = O_Q/Q \cdot O_Q \\ x & \longmapsto & x \cdot t(Q) \end{array}$$

$\vdash \varphi$ é K -linear

Pois é composição de aplicações K -lineares:

$$\begin{array}{ccccc} \mathcal{L}(B) & \longrightarrow & F & \longrightarrow & F_Q \\ x & \longmapsto & x \cdot t & \longmapsto & x \cdot t(Q) \end{array}$$

$$\vdash x \cdot t \in O_Q$$

$$\begin{aligned} v_Q(x \cdot t) &= v_Q(x) + v_Q(t) \\ &= v_Q(x) + v_Q(B) \\ &\geq 0 \end{aligned}$$

$$\vdash \text{Ker} \varphi = \mathcal{L}(A)$$

$$\begin{aligned} x \in \text{Ker} \varphi &\Leftrightarrow x \cdot t \in Q \\ &\Leftrightarrow v_Q(x) + v_Q(t) > 0 \\ &\Leftrightarrow v_Q(x) > -v_Q(t) \\ &\Leftrightarrow v_Q(x) > -v_Q(B) \\ &\Leftrightarrow v_Q(x) > -v_Q(A) - 1 \\ &\Leftrightarrow v_Q(x) \geq -v_Q(A) \\ &\Leftrightarrow x \in \mathcal{L}(A) \end{aligned}$$

pois para $P \neq Q$, $v_P(x) \geq -v_P(B) = -v_P(A)$. Logo, $\mathcal{L}(B)/\mathcal{L}(A) \cong \text{Im}(\varphi) \subseteq F_Q$.

$$\begin{aligned} [F_Q : K] &= \dim F_Q \\ &= \deg Q \\ &= \deg B - \deg A \end{aligned}$$

Logo, $\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq [F_P : K] = \deg B - \deg A$.

- Suponha agora que $B = A + P_1 + \dots + P_n$, e considere o resultado válido para todo $k < n$:

$$\dim(\mathcal{L}(A + P_1 + \dots + P_k)/\mathcal{L}(A)) \leq \deg(P_1) + \dots + \deg(P_k)$$

Lembre que se $U \leq V \leq W$ são espaços vetoriais, então, $(W/U)/(V/U) \cong W/V$ e $\dim(W/V) = \dim(W/U) - \dim(V/U)$. então, considere

$$\begin{aligned} M &= \mathcal{L}(A + P_1 + \dots + P_n)/\mathcal{L}(A) \\ N &= \mathcal{L}(A + P_1 + \dots + P_{n-1})/\mathcal{L}(A) \\ S &= \mathcal{L}(A + P_1 + \dots + P_n)/\mathcal{L}(A + P_1 + \dots + P_{n-1}) \end{aligned}$$

Assim, temos que $\dim M - \dim N = \dim S$. Pela hipótese de indução:

$$\dim S \leq \deg P_n \quad \text{e} \quad \dim N \leq \sum_{i=1}^{n-1} \deg P_i$$

Logo,

$$\dim M \leq \sum_{i=1}^n \deg P_i = \deg B - \deg A$$

□

A próxima proposição fornece uma cota superior para $\dim \mathcal{L}(A)$ em termos do $\deg A_+$

I.3.8 Proposição Para qualquer divisor $A \in \mathcal{D}_F$, o espaço $\mathcal{L}(A)$ é um espaço vetorial finito sobre K . Mais precisamente, se $A = A_+ - A_-$ com divisores positivos A_+ e A_- , então:

$$\dim \mathcal{L}(A) \leq \deg A_+ + 1$$

Para obter o resultado, basta usar o Lema I.3.7.

I.3.9 Definição Para $A \in \mathcal{D}_F$, o inteiro $\dim A = \dim \mathcal{L}(A)$ é chamado *dimensão* do divisor A .

O próximo teorema nos diz, essencialmente, que o número de zeros de $x \in F$ é o mesmo que o número de polos de x (contando com as respectivas ordens).

I.3.10 Teorema Todo divisor principal possui grau zero. Mais precisamente, dado $x \in F \setminus K$

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$$

Demonstração :

Chame $B = (x)_\infty$

$$B = \sum_{P \in N_x} (-v_P(x))P = \sum_{i=1}^r (-v_{P_i}(x))P_i$$

Seja $n = [F : K(x)]$

$\vdash \deg B = n$

($\leq$) Por I.2.3, $\sum_{i=1}^r (-v_{P_i}(x)).deg P_i \leq [F : K(x)]$

($\geq$) Seja $\{u_1, \dots, u_n\}$ uma base de $F/K(x)$ e escolha $C \in \mathcal{D}_F$ tal que $C \geq 0$ e $(u_j) \geq -C, \forall j = 1, \dots, n$; considere $0 \leq t \in \mathbb{Z}$ e considere o conjunto $\mathcal{A} = \{x^i.u_j/0 \leq t, j = 1, \dots, n\}$:

$\vdash$ os elementos de $\mathcal{A}$ são linearmente independentes.

Suponhamos que sejam linearmente dependentes; logo, sem perda na generalidade, existem elementos $\alpha_{ij} \in K[x]$, não todos nulos, tais que:

$$\sum_{j=1}^n \sum_{i=0}^t \alpha_{ij}.x^i.u_j = 0.$$

Como os u_j são linearmente independentes, então é preciso que para cada j tenhamos:

$$\sum_{i=0}^t \alpha_{ij} x^i = 0. \quad (\text{I.17})$$

Cada α_{ij} é do tipo:

$$\alpha_{ij} = \alpha_{ij}(x) = a_{0ij} + a_{1ij}.x + \dots + a_{s_{ij}ij}.x^{s_{ij}}.$$

Logo, I.17 é uma expressão do tipo:

$$\sum_{b=1}^m \gamma_b.x^b = 0 \in K[x]$$

Isso nos diz que x é solução de um polinômio sobre K , absurdo! pois x é transcendente sobre K . Logo, é preciso ter $\alpha_{ij} = 0$, para cada i, j e portanto, os $x^i.u_j$ são linearmente independentes. Temos que $\#\mathcal{A} = (t+1).n$.

Considere agora um lugar arbitrário P e sua respectiva valorização v_P :

$$\begin{aligned} v_P(x^i.u_{ij}) &= i.v_P(x) + v_P(u_j) \\ &= i.(-v_P(B)) - v_P(C) \\ &= -t.v_P(B) - v_P(C) \\ &= -v_P(t.B + C). \end{aligned}$$

Vemos que $x^i.u_{ij} \in \mathcal{L}(tB + C)$. Como os $x^i.u_j$ são linearmente independentes e $\mathcal{L}(tB + C)$ é um K -subespaço vetorial, obtemos:

$$\#\mathcal{A} \leq \dim \mathcal{L}(tB + C). \quad (\text{I.18})$$

Por I.3.8,

$$\begin{aligned} \dim \mathcal{L}(tB + C) &\leq \deg(tB + C) + 1 \\ &\leq t \deg B + \deg C + 1. \end{aligned}$$

Logo, se $c = \deg C$,

$$\begin{aligned} (t+1)n &\leq t.\deg B + c + 1 \\ n - c - 1 &\leq t(\deg B - n). \end{aligned}$$

Assim, para $t \gg 0$,

$$\deg B - n \geq \frac{n - c - 1}{t} \rightarrow 0.$$

Então $\deg B \geq n$. Com isso, $\deg(x)_\infty = [F : K(x)]$. Como $K(x) = K(x^{-1})$ e $(x)_0 = (x)_\infty$, então

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

□

Este teorema traz as seguintes conseqüências.

I.3.11 Corolário

- (a) Sejam A, A' divisores com $A \sim A'$. Então, temos que $\dim A = \dim A'$ e $\deg A = \deg A'$.
- (b) Se $\deg A < 0$, então $\dim A = 0$.
- (c) Para um divisor A de grau zero, as seguintes afirmações são equivalentes:

1. A é principal
2. $\dim A \geq 1$
3. $\dim A = 1$

A demonstração é simples e não será feita. A proposição a seguir nos diz que existe uma cota superior para a diferença $\deg A - \dim A$ que não depende de A . A existência de tal cota é fundamental para definirmos o gênero de um corpo de funções.

I.3.12 Proposição Existe uma constante $\gamma \in \mathbb{Z}$ tal que para todo divisor $A \in \mathcal{D}_F$, vale:

$$\deg A - \dim A \leq \gamma$$

Demonstração : Observe que por I.3.7,

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

e portanto,

$$\deg A_1 - \dim A_1 \leq \deg A_2 - \dim A_2.$$

Fixe $x \in F \setminus K$ e seja $B = (x)_\infty$: como na demonstração de I.3.10, existe $C \geq 0$ divisor (dependendo de x) tal que

$$\dim(tB + C) \geq (t + 1) \cdot \deg B, \quad \forall t \geq 0$$

Por I.3.7

$$\begin{aligned} \dim\left(\frac{\mathcal{L}(tB+C)}{\mathcal{L}(tB)}\right) &\leq \deg(tB + C) - \deg(tB) \\ \Rightarrow \dim(\mathcal{L}(tB + C)) &\leq \dim \mathcal{L}(tB) + \deg C \\ \Rightarrow \dim(tB + C) &\leq \dim(tB) + \deg C. \end{aligned}$$

Combinando as duas desigualdades, obtemos:

$$(t + 1) \deg B \leq \dim(tB + C) \leq \dim(tB) + \deg C,$$

$$\begin{aligned} \dim(tB) &\geq (t+1)\deg B - \deg C \\ &\geq \deg(tB) + ([F : K(x)] - \deg C). \end{aligned}$$

Assim sendo,

$$\deg(tB) - \dim(tB) \leq \deg C - [F : K(x)], \forall t > 0 \quad (\text{I.19})$$

Como C só depende de x , seja $\gamma = \deg C - [F : K(x)]$. Queremos mostrar que (I.19) vale para todo $A \in \mathcal{D}_F$ ao substituir tB por A .

Afirmção:

Dado $A \in \mathcal{D}_F$, $\exists A_1, D \in \mathcal{D}_F$ e um inteiro $l > 0$ tais que $A \leq A_1, A_1 \sim D$ e $D \leq lB$.

⊢ Afirmção: escolha $A_1 = A_+$, então $0 \leq A_1$ e $A \leq A_1$, então, por I.3.7

$$\begin{aligned} \dim(lB) - \dim(lB - A_1) &= \dim\left(\frac{\mathcal{L}(lB)}{\mathcal{L}(lB - A_1)}\right) \leq \deg(lB) - \deg(lB - A_1) \\ &\Rightarrow \dim(lB - A_1) \geq \dim(lB) - \deg A_1 \\ &\text{por I.3.6} \geq \deg(lB) - \gamma - \deg A_1, \end{aligned}$$

e para $l \gg 0$, temos $\dim(lB - A_1)$. Logo, $\exists z \in \mathcal{L}(lB - A_1) \setminus \{0\}$.

Considerando $D = A_1 - (z)$, temos $A_1 \sim D$ e $D = A_1 - (z) \leq A_1(lB - A_1) = lB$

$$\begin{aligned} \deg A - \dim A &\leq \deg A_1 - \dim A_1 \\ &\leq \deg D - \dim D \\ &\leq \deg lB - \dim lB \\ &\leq \gamma \end{aligned}$$

□

I.3.13 Definição O gênero g de F/K é definido por

$$g = \max\{\deg A - \dim A + 1 \mid A \in \mathcal{D}_F\}$$

Esta definição foi bem estabelecida, conforme a Proposição I.3.12.

I.3.14 Observação O gênero de F/K é um inteiro não negativo. De fato, considerando $A = (0)$, temos $\deg A - \dim A + 1 = 0$ e então $g \geq 0$.

I.3.15 Teorema (de Riemann) Seja F/K um corpo de funções de gênero g :

- (a) Para qualquer divisor $A \in \mathcal{D}_F$, $\dim A \geq \deg A + 1 - g$.
- (b) Existe um inteiro c , dependendo de F/K , tal que $\dim A = \deg A + 1 - g$ sempre que $\deg A \geq c$.

Demonstração :

- (a) Pela definição do gênero, $g \geq \deg A - \dim A + 1 \Rightarrow \dim A \geq \deg A + 1 - g$.
- (b) Escolha um divisor A_0 com $g = \deg A_0 - \dim A_0 + 1$ e considere $c = \deg A_0 + g$. Se $\deg A \geq c$, então

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

Logo, existe $z \in \mathcal{L}(A - A_0) \setminus \{0\}$. Considere $A' = A + (z)(\geq A_0)$. Então, temos:

$$\begin{aligned} \deg A - \dim A &= \deg A' - \dim A' \\ &\geq \deg A_0 - \dim A_0 \\ &\geq g - 1 \end{aligned}$$

Logo, $\dim A \leq \deg A + 1 - g$.

□

I.4 O Teorema de Riemann-Roch

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

I.4.1 Definição Para $A \in \mathcal{D}_F$,

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

é chamado *índice de especialidade* de A .

Pelo teorema de Riemann, $i(A) \geq 0$ e $i(A) = 0$ se $\deg A$ for suficientemente grande.

I.4.2 Definição Um *adele* de F/K é uma aplicação:

$$\alpha : \begin{cases} \mathbb{P}_F & \longrightarrow F \\ P & \longmapsto \alpha_P \end{cases}$$

tal que $\alpha_P \in O_P$ para quase todo $P \in \mathbb{P}_F$. O adele é visto como um elemento do produto direto $\prod_{P \in \mathbb{P}_F} F$ e assim, usamos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou ainda $\alpha = (\alpha_P)$. O conjunto

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

é chamado *espaço adélico* de F/K e é visto como um espaço vetorial sobre K (aliás, $\mathcal{A}_F$ também é um anel, mas sua estrutura de anel não será usada).

O *adele principal* de um elemento $x \in F$ é o adele cujas componentes são todas iguais a x :

$$\alpha : \begin{cases} \mathbb{P}_F & \longrightarrow F \\ P & \longmapsto x \end{cases}$$

A definição está bem feita, pois o número de polos de x é finito, e portanto, $x \in O_P$ a menos de um número finito de lugares. Isso nos fornece um mergulho

$$\begin{aligned} F &\hookrightarrow \mathcal{A}_F \\ x &\mapsto (x) = (x, x, x, \dots, x, x, x, \dots) \end{aligned}$$

onde $(x) = (x, x, \dots, x, x, \dots)$ é o *adele principal* de x .

A valorização v_P em F/K se estende naturalmente a $\mathcal{A}_F$ considerando $v_P(\alpha) = v_P(\alpha_P)$, onde α_P é a P -ésima componente do adele α . Pela definição de α , $v_P(\alpha) \geq 0$ para quase todo $P \in \mathbb{P}_F$.

I.4.3 Definição Para $A \in \mathcal{D}_F$ definimos:

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

Obviamente, este é um K -subespaço de $\mathcal{A}_F$.

I.4.4 Teorema Para qualquer divisor A , o índice de especialidade é

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

Demonstração : Este teorema diz que apesar de $\dim \mathcal{A}_F$, $\dim \mathcal{A}_F(A)$ e $\dim F$ serem infinitas como K -espaços, o quociente $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ tem dimensão finita sobre K . A prova deste teorema é feita em várias etapas. Recordemos primeiro o que é uma sequência exata: Dados U, V e W K -espaços vetoriais, dizemos que $0 \longrightarrow U \xrightarrow{\sigma_1} W \xrightarrow{\sigma_2} V \longrightarrow 0$ é uma sequência exata de transformações K -lineares se:

- σ_1 é injetiva
- σ_2 é sobrejetora
- $\text{Ker} \sigma_2 = \text{Im} \sigma_1$

(Passo 1) Sejam $A, B \in \mathcal{D}_F$ com $A \leq B$, então:

- $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$
- $\dim(\mathcal{A}_F(B)/\mathcal{A}_F(A)) = \deg B - \deg A$

$$\vdash \mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$$

$$\gamma \in \mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(A), \forall P \in \mathbb{P}_F\}$$

$$\Rightarrow v_P(\gamma) = v_P(\gamma_P) \geq -v_P(A) \geq -v_P(B)$$

$$\Rightarrow \gamma \in \mathcal{A}_F(B)$$

$$\vdash \dim(\mathcal{A}_F(B)/\mathcal{A}_F(A)) = \deg B - \deg A$$

Esta prova é feita por indução: Suponha $B = A + P$, $P \in \mathbb{P}_F$ e escolha $t \in F$ com $v_P(t) = v_P(A) + 1 = v_P(B)$. Considere a aplicação linear

$$\varphi: \begin{cases} \mathcal{A}_F(B) & \longrightarrow & F_P \\ \alpha & \longmapsto & (t.\alpha_P)(P) = t\alpha_P + P \end{cases}$$

$\vdash \varphi$ é sobrejetiva:

Considere $\bar{x} \in F_P \Rightarrow \bar{x} = x + P$ e considere $\alpha = (\alpha_Q)$ tal que $\alpha_P = t^{-1}.x$ e $\alpha_Q \in \mathcal{L}(B), \forall Q \neq P$, então $\alpha \in \mathcal{A}_F(B)$ e $\varphi(\alpha) = \bar{x}$

$$\varphi(t^{-1}.x) = t.(t^{-1}.x) + P = x + P = \bar{x}$$

$$\vdash \text{Ker} \varphi = \mathcal{A}_F(A)$$

$$\begin{aligned} \alpha \in \text{Ker} \varphi &\Rightarrow t.\alpha_P + P = P \\ &\Rightarrow t.\alpha_P \in P \\ &\Rightarrow v_P(t.\alpha_P) > 0 \\ &\Rightarrow v_P(t) + v_P(\alpha_P) \\ &\Rightarrow v_P(\alpha) > -v_P(t) = -v_P(A) - 1 \\ &\Rightarrow v_P(\alpha) \geq -v_P(A) \end{aligned}$$

Se $\alpha \in \mathcal{A}_F(B)$, então, $v_P(\alpha) \geq -v_Q(B), \forall Q$, em particular, $\forall Q \neq P$. Logo, $\alpha \in \mathcal{A}_F(A)$ e assim, pelo Teorema do Isomorfismo,

$$\mathcal{A}_F(B)/\mathcal{A}_F(A) \cong F_P$$

$$\begin{aligned}
\dim(\mathcal{A}_F(B)/\mathcal{A}_F(A)) &= [F_P : K] \\
&= \deg P \\
&= \deg B - \deg A
\end{aligned}$$

Suponha agora, $B = A + P_1 + \dots + P_n$, $P_i \in \mathbb{P}_F$, $i = 1, \dots, n$ e considere o resultado válido para qualquer $k < n$. Então,

- $\dim(\mathcal{A}_F(B)/\mathcal{A}_F(B - P_n)) = P_n$
- $\dim(\mathcal{A}_F(B - P_n)/\mathcal{A}_F(A)) = \deg P_1 + \dots + \deg P_{n-1}$

Para $U \leq V \leq W$ espaços vetoriais temos:

$$\begin{aligned}
\dim(W/V) &= \dim((W/U)/(V/U)) \\
&= \dim(W/U) - \dim(V/U) \\
\Rightarrow \dim(W/U) &= \dim(W/V) + \dim(V/U)
\end{aligned}$$

Logo, para $U = \mathcal{A}_F(A)$, $V = \mathcal{A}_F(B - P_n)$, $W = \mathcal{A}_F(B)$ temos:

$$\begin{aligned}
\dim(\mathcal{A}_F(B)/\mathcal{A}_F(A)) &= \deg P_1 + \dots + \deg P_n \\
&= \deg B - \deg A
\end{aligned}$$

(Passo 2) Sejam $A, B \in \mathcal{D}_F$ com $A \leq B$. Então:

$$\dim(\mathcal{A}_F(B) + F/\mathcal{A}_F(A) + F) = \quad (I.20)$$

$$(\deg B - \dim B) - (\deg A - \dim A) \quad (I.21)$$

$\vdash 0 \longrightarrow \mathcal{L}(B)/\mathcal{L}(A) \xrightarrow{\sigma_1} \mathcal{A}_F(B)/\mathcal{A}_F(A) \xrightarrow{\sigma_2} \mathcal{A}_F(B) + F/\mathcal{A}_F(A) + F \longrightarrow 0$ é uma sequência exata, onde σ_1 e σ_2 são definidas de forma canônica:

$$\begin{aligned}
\sigma_1 : \begin{cases} \mathcal{L}(B)/\mathcal{L}(A) & \longrightarrow \mathcal{A}_F(B)/\mathcal{A}_F(A) \\ \bar{x} = x + \mathcal{L}(A) & \mapsto \bar{x} = x + \mathcal{A}_F(A), x = (x)_P \end{cases} \\
\sigma_2 : \begin{cases} \mathcal{A}_F(B)/\mathcal{A}_F(A) & \longrightarrow \mathcal{A}_F(B) + F/\mathcal{A}_F(A) + F \\ \bar{\alpha} = \alpha + \mathcal{A}_F(A) & \mapsto \bar{\alpha} = \alpha + (\mathcal{A}_F(A) + F) \end{cases}
\end{aligned}$$

$\vdash \sigma_1$ é injetiva:

$$\sigma_1(\bar{x}) = \bar{0} \Rightarrow x = (x) \in \mathcal{A}_F(A) \Rightarrow v_P(x) \geq -v_P(A), \forall P \in \mathbb{P}_F \Rightarrow x \in \mathcal{L}(A) \Rightarrow \bar{x} = \bar{0}.$$

$\vdash \sigma_2$ é sobrejetiva:

$$\bar{y} \in \mathcal{A}_F(B) + F/\mathcal{A}_F(A) + F \Rightarrow \exists \alpha \in \mathcal{A}_F(B), x_0 \in F \text{ tais que } \bar{y} = \alpha + x + \mathcal{A}_F(A) + F = \alpha + \mathcal{A}_F(A) + F. \text{ Logo, } \sigma_2(\alpha) = \bar{y}.$$

$$\vdash \text{Ker} \sigma_2 \subseteq \text{Im} \sigma_1$$

$$\alpha + \mathcal{A}_F(A) \in \text{Ker} \sigma_2 \Rightarrow \alpha \in \mathcal{A}_F(A) + F \Rightarrow \exists x_0 \in F : \alpha - x_0 \in \mathcal{A}_F(A) \subseteq \mathcal{A}_F(B) \Rightarrow x_0 \in F \cap \mathcal{A}_F(B) = \mathcal{L}(B) \text{ e assim}$$

$$\sigma_1(x_0 + \mathcal{L}(A)) = x_0 + \mathcal{A}_F(A) = \alpha + \mathcal{A}_F(A) \in \text{Im} \sigma_1$$

Mais ainda, temos que $\text{Im} \sigma_1 \subseteq \text{Ker} \sigma_2$. Seja $x + \mathcal{L}(A) \in \mathcal{L}(B)/\mathcal{L}(A)$, então $\sigma_1(x + \mathcal{L}(A)) = x + \mathcal{A}_F(A)$ e $\sigma_2(x + \mathcal{A}_F(A)) = x + \mathcal{A}_F(A) + F = \mathcal{A}_F(A) + F$ e portanto, $x + \mathcal{A}_F(A) \in \text{Ker} \sigma_2$.

Do fato da sequência ser exata, temos:

$$\begin{aligned}
\dim \frac{\mathcal{A}_F(B) + F}{\mathcal{A}_F(A) + F} &= \dim \frac{\mathcal{A}_F(B)}{\mathcal{A}_F(A)} - \dim \frac{\mathcal{L}(B)}{\mathcal{L}(A)} \\
&= (\deg B - \deg A) - (\dim B - \dim A) \\
&= (\deg B - \dim B) - (\deg A - \dim A)
\end{aligned}$$

(Passo 3) Se $B \in \mathcal{D}_F$ com $\dim B = \deg B + 1 - g$, então $\mathcal{A}_F = \mathcal{A}_F(B) + F$. Considere $C \geq B$, então por I.3.7 temos

$$\begin{aligned} \dim(\mathcal{L}(C)/\mathcal{L}(B)) &\leq \deg C - \deg B \\ \dim C - \dim B &\leq \deg C - \deg B \\ \dim C &\leq \deg C - \deg B + \dim B \\ &\leq \deg C - \deg B + \deg B + 1 - g \\ &\leq \deg C + 1 - g. \end{aligned}$$

Por outro lado, pelo Teorema de Riemann

$$\dim C \geq \deg C + 1 - g$$

Disto segue que

$$\dim C = \deg C + 1 - g, \forall C \geq B. \quad (1.22)$$

Considere $\alpha \in \mathcal{A}_F$. Podemos encontrar $C \geq B$ tal que $\alpha \in \mathcal{A}_F(C)$. Se $P_1, \dots, P_n \in \mathbb{P}_F$ são todos os polos de α , seja $D = \sum_{i=1}^n -v_{P_i}(\alpha).P_i$, então $D \geq 0$. Considere $C = B + D$. Por (I.20) e (1.22):

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

(Prova do teorema) Considere $A \in \mathcal{D}_F$ divisor arbitrário. Pelo Teorema de Riemann, existe $B \geq A$ tal que $\dim B = \deg B + 1 - g$. Pelo Passo 3, $\mathcal{A}_F = \mathcal{A}_F(B) + F$. De I.20, temos

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

□

O Teorema I.4.4 pode ser reescrito como segue:

$$\dim A = \deg A + 1 - g + \dim(\mathcal{A}_F/\mathcal{A}_F(0) + F), \forall A \in \mathcal{D}_F$$

I.4.5 Corolário $g = \dim(\mathcal{A}_F/\mathcal{A}_F(0) + F)$.

Este resultado é consequência imediata do Teorema I.4.5, considerando $A = 0$.

I.4.6 Definição Um *diferencial de Weil* de F/K é uma aplicação K -linear $\omega : \mathcal{A}_F \longrightarrow K$ que se anula em $\mathcal{A}_F(A) + F$ para algum divisor $A \in \mathcal{D}_F$. Chamamos

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

de *módulo diferencial de Weil* de F/K . Para $A \in \mathcal{D}_F$, seja

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

O espaço Ω_F é visto como K -espaço vetorial da forma usual (aliás, se ω_1 se anula em $\mathcal{A}_F(A_1) + F$ e ω_2 se anula em $\mathcal{A}_F(A_2) + F$, então $\omega_1 + \omega_2$ se anula em $\mathcal{A}_F(A_3) + F$ para qualquer $A_3 \leq A_1, A_2$ e $a\omega_1$ se anula em $\mathcal{A}_F(A_1) + F$ para $a \in K$). Claramente, $\Omega_F(A)$ é um subespaço de Ω_F .

I.4.7 Lema Para $A \in \mathcal{D}_F$ temos que $\dim \Omega_F = i(A)$.

Demonstração : O espaço $\Omega_F(A)$ é naturalmente isomorfo ao espaço das formas lineares em $\mathcal{A}_F/\mathcal{A}_F(A) + F$, i.e.,

$$\Omega_F(A) \cong \text{Hom}_K(\mathcal{A}_F/\mathcal{A}_F(A) + F, K).$$

De fato, dado $\omega \in \Omega_F(A)$, ω é um diferencial de Weil que se anula em $\mathcal{A}_F(A) + F$, isto é, ω é uma aplicação K -linear de $\mathcal{A}_F$ em K que se anula em $\mathcal{A}_F(A) + F$; logo, existe $\tilde{\omega}$ tal que:

$$\begin{aligned} \tilde{\omega} : \quad \mathcal{A}_F/\mathcal{A}_F(A) + F &\longrightarrow K \\ \bar{\alpha} = \alpha + (\mathcal{A}_F(A) + F) &\mapsto \tilde{\omega}(\bar{\alpha}) = \omega(\alpha) \end{aligned}$$

Considere $\sigma \in \text{Hom}_K(\mathcal{A}_F/(\mathcal{A}_F(A) + F), K)$, então:

$$\begin{aligned} \sigma : \quad \mathcal{A}_F/\mathcal{A}_F(A) + F &\longrightarrow K \\ \bar{\alpha} = \alpha + \mathcal{A}_F(A) + F &\mapsto \sigma(\bar{\alpha}) \end{aligned}$$

Seja $\phi : \mathcal{A}_F \longrightarrow K$ tal que $\phi(\alpha) = \sigma(\bar{\alpha}) \in K$. Então, ϕ é uma aplicação K -linear e ϕ se anula em $\mathcal{A}_F(A) + F$, pois se $\alpha \in \mathcal{A}_F(A) + F$, então $\bar{\alpha} = \bar{0}$ e $\phi(\alpha) = \sigma(\bar{\alpha}) = \sigma(\bar{0}) = 0$. Logo, $\phi \in \Omega_F(A)$. Assim, podemos definir o seguinte isomorfismo:

$$\begin{aligned} \chi : \quad \Omega_F(A) &\longrightarrow \text{Hom}_K(\mathcal{A}_F/\mathcal{A}_F(A) + F, K) \\ \omega &\mapsto \tilde{\omega} \end{aligned}$$

Logo,

$$\begin{aligned} \dim \Omega_F(A) &= \dim(\mathcal{A}_F/\mathcal{A}_F(A) + F, K) < \infty \\ &= \dim \text{Hom}_K(\mathcal{A}_F/\mathcal{A}_F(A) + F, K) \\ &= \dim(\mathcal{A}_F/\mathcal{A}_F(A) + F) = i(A) \end{aligned}$$

□

Uma conseqüência de I.4.7 é $\Omega_F \neq 0$. Para ver isso, escolho A divisor com $\deg A \leq -2$. Então:

$$\begin{aligned} \dim \Omega_F(A) &= i(A) \\ &= \dim A - \deg A + g - 1 \\ &\geq 0 + 2 + 0 - 1 \\ &\geq 1 \end{aligned}$$

Como $\Omega_F(A) \subseteq \Omega_F$ e $\dim \Omega_F(A) \geq 1$, então, $\Omega_F \neq \emptyset$.

I.4.8 Definição Para $x \in F$ e $\omega \in \Omega_F$ defina $x\omega : \mathcal{A}_F \longrightarrow K$ por

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

É simples verificar que $x\omega$ é novamente um diferencial de Weil de F/K . De fato, se ω se anula em $\mathcal{A}_F(A) + F$, então $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$. Com isso temos que Ω_F é um espaço vetorial sobre F .

I.4.9 Proposição Ω_F é um espaço vetorial unidimensional sobre F .

Demonstração : Por I.4.7 temos que $\Omega_F \neq 0$. Logo, existe $\omega_1 \in \dot{\Omega}_F$. Devemos mostrar que $\forall \omega_2 \in \Omega_F, \exists z \in F : \omega_2 = z\omega_1$. Se $\omega_2 = 0$, basta considerar $z = 0$. Assumindo $\omega_2 \neq 0$, escolha $A_1, A_2 \in \mathcal{D}_F$ tais que $\omega_1 \in \Omega_F(A_1)$ e $\omega_2 \in \Omega_F(A_2)$. Para um divisor B (a ser determinado) considere as aplicações K -lineares injetivas:

$$\phi_i : \begin{cases} \mathcal{L}(A_i + B) & \longrightarrow & \Omega_F(-B) \\ y & \longmapsto & y \cdot \omega_i \end{cases}, i = 1, 2.$$

Afirmção: Para uma escolha apropriada de B , vale:

$$I = \phi_1(\mathcal{L}(A_1 + B)) \cap \phi_2(\mathcal{L}(A_2 + B)) \neq \{0\}$$

Com esta afirmação, temos que se $\omega \in \dot{I}$, então existem $x_i \in \mathcal{L}(A_i + B), i = 1, 2$, tais que $x_1\omega_1 = \omega = x_2\omega_2$ e, portanto, $\omega_2 = x_2^{-1}x_1\omega_1 = z \in F$.

$\vdash$ prova da afirmação:

Seja $B > 0$ um divisor com grau suficientemente grande para ter

$$\dim(A_i + B) = \deg(A_i + B) + 1 - g, i = 1, 2.$$

Considere $U_i = \phi(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B), i = 1, 2$. Como

$$\begin{aligned} \dim \Omega_F(-B) &= i(-B) \\ &= \dim(-B) - \deg(-B) + g - 1 \\ &= \deg B + g - 1 \end{aligned}$$

obtemos

$$\begin{aligned} \dim U_1 + \dim U_2 - \dim \Omega_F(-B) &= \\ &= \deg(A_1 + B) + 1 - g + \deg(A_2 + B) + 1 - g - (\deg B + g - 1) \\ &= \deg B + [\deg(A_1 + B) + \deg(A_2 + B) + 3(1 - g)] \\ &> 0. \end{aligned}$$

logo,

$$\dim U_1 + \dim U_2 - \dim(\Omega_F - B) > 0 \quad (I.23)$$

para B suficientemente grande. De I.23 segue que $\dim(U_1 \cap U_2) > 0$.

□

Considere o seguinte conjunto de divisores:

$$M(\omega) = \{A \in D_F/\omega \text{ se anula em } \mathcal{A}_F(A) + F\}. \quad (I.24)$$

Então temos o seguinte resultado:

I.4.10 Lema *Seja $\omega \in \dot{\Omega}_F$. Então, existe um divisor $W \in M(\omega)$ unicamente determinado tal que $A \leq W, \forall A \in M(\omega)$.*

Demonstração : Pelo Teorema de Riemann, existe $c > 0$ tal que se $D \in \mathcal{D}_F$ com $\deg D \geq c$, então $i(D) = 0$ e $\mathcal{A}_F(D) + F = \mathcal{A}_F$. Supondo que $D \in M(\omega)$ temos que ω se anula em $\mathcal{A}_F(D) = \mathcal{A}_F$ e, portanto $\omega = 0$ absurdo! Logo, $\forall A \in M(\omega), \deg A < c$. Assim, podemos escolher um divisor maximal em $M(\omega)$; seja ele W . Supondo que existe $A_0 \in M(\omega)$ tal que $A_0 \not\leq W$, isto é, existe $Q \in \mathbb{P}_F$ tal que $v_Q(A) > v_Q(W)$:

$\vdash W + Q \in M(\omega)$

Considere $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$; α pode ser escrito como $\alpha = \alpha' + \alpha''$, onde

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

- $v_P(\alpha_P) \geq -v_P(W + Q) = -v_P(W), P \neq Q$
- $v_Q(\alpha_Q) \geq (W + Q) \geq -v_Q(A_0)$

Então,

$$\alpha' \in \mathcal{A}_F(W) \text{ e } \alpha'' \in \mathcal{A}_F(A_0)$$

e assim,

$$\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') \Rightarrow \omega \text{ se anula em } \mathcal{A}_F(W + Q).$$

Mas, $\deg(W + Q) = \deg W + 1$, contradizendo a condição de maximalidade de W . Logo, $A_0 \leq W$ é único

Suponha que existe W' também de grau maximal, logo:

$$\left. \begin{array}{l} W \leq W', \text{ pois } W' \text{ é maximal} \\ W' \leq W, \text{ pois } W \text{ é maximal} \end{array} \right\} \Rightarrow W = W'$$

□

I.4.11 Definição

(a) O divisor (ω) de um diferencial de Weil $\omega \neq 0$ é o único divisor de F/K satisfazendo:

1. ω se anula em $\mathcal{A}_F((\omega)) + F$.
2. Se ω se anula em $\mathcal{A}_F((A)) + F$, então $A \leq (\omega)$.

(b) Para $\omega \in \dot{\Omega}_F$ e $P \in \mathbb{P}_F$ definimos $v_P(\omega) = v_P((\omega))$.

(c) Um lugar P é dito um zero (polo) de ω se $v_P(\omega) > 0$ ($v_P(\omega) < 0$). O diferencial é dito *regular* em P se $v_P(\omega) \geq 0$, e ω é dito *regular* (ou *holomorfo*) se ele for regular em qualquer $P \in \mathbb{P}_F$.

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

I.4.12 Observação Segue imediatamente das definições que

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

Como consequência do Lema I.4.7 e da Definição I.4.1, obtemos

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

I.4.13 Proposição

(a) Para $x \in \dot{F}$ e $\omega \in \dot{\Omega}_F$, temos $(x\omega) = (x) + (\omega)$.

(b) Quaisquer dois divisores canônicos são equivalentes.

Demonstração :

(a) Lembre que ω se anula em $\mathcal{A}_F((\omega)) + F$ e $(x\omega)$ se anula em $\mathcal{A}_F((\omega) + (x))$.

$$\begin{aligned} \omega \text{ se anula em } \mathcal{A}_F((\omega)) + F &\Rightarrow x\omega \text{ se anula em } \mathcal{A}_F((\omega) + (x)) + F \\ &\Rightarrow (x) + (\omega) \in M(x\omega) \\ &\Rightarrow (\omega) + (x) \leq (x\omega) \end{aligned} \tag{I.25}$$

Analogamente,

$$(x\omega) + (x^{-1}) \leq (\omega) \tag{I.26}$$

De (I.25) e (I.26) temos :

$$(\omega) + (x) \leq (x\omega) \leq (\omega) - (x^{-1}) = (\omega) + (x)$$

(b) Sejam (ω) e (v) divisores canônicos. Como $\dim \Omega_F = 1$, existe $x \in F$ tal que $\omega = xv$. Logo, $(\omega) = (xv) = (x) + (v)$.

□

Uma consequência desta proposição é que os divisores canônicos de F/K formam uma única classe $[W]$ no grupo quociente $\mathcal{C}_F$. Esta classe de divisores é chamada a *classe canônica* de F/K .

I.4.14 Teorema *Seja A um divisor arbitrário e $W = (\omega)$ um divisor canônico de F/K . Então a aplicação*

$$\mu : \begin{cases} \mathcal{L}(W - A) & \longrightarrow & \Omega_F(A) \\ x & \longmapsto & x\omega \end{cases}$$

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

Demonstração : Sejam $W = (\omega)$ e $M(\omega)$. Para todo $D \in M(\omega)$, $D \leq W$

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

$$v \in \Omega_F(A) \Rightarrow A \leq (v)$$

$\vdash \mu$ está bem definida:

$$\begin{aligned} x \in \mathcal{L}(W - A) &\Rightarrow (x) \geq -(W - A) \\ &\Rightarrow (x) + (\omega) \geq A \\ &\Rightarrow (x\omega) \geq A \\ &\Rightarrow x\omega \in \Omega_F(A) \end{aligned}$$

$\vdash \mu$ é injetiva:

$$\mu(x) = 0 \Rightarrow x\omega = 0 \Rightarrow \begin{cases} \omega = 0, \text{ absurdo!} \\ \text{ou} \\ x = 0 \end{cases}$$

Logo, $\text{Ker} \mu = \{0\}$.

$\vdash \mu$ é sobrejetiva:

Seja $\gamma \in \Omega_F(A)$; $\dim \Omega_F = 1 \Rightarrow \exists x \in F/x\omega = \gamma \Rightarrow \mu(x) = \gamma$

$\vdash x \in \mathcal{L}(W - A)$

$$\gamma = x\omega \in \Omega_F(A) \Rightarrow (\gamma) = (x\omega) \geq (A) \Rightarrow (x) + (\omega) \geq (A) \Rightarrow (x) \geq -((\omega) - A) \Rightarrow$$

$$x \in \mathcal{L}((\omega) - A) = \mathcal{L}(W - A).$$

□

Acabamos de provar que $\dim \Omega_F(A) = \dim(W - A)$. Como $\dim \Omega_F(A) = i(A)$, então $i(A) = \dim(W - A)$.

I.4.15 Teorema (Riemann-Roch) *Seja W um divisor canônico de F/K . Então para qualquer $A \in \mathcal{D}_F$,*

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

Este resultado é consequência imediata do teorema I.4.14.

I.4.16 Corolário *Para um divisor canônico W , temos*

$$\deg W = 2g - 2 \quad \text{e} \quad \dim W = g$$

A demonstração destes resultados é simples aplicação do Teorema de Riemann-Roch. Disto também segue que $i(\omega) = 1$ (pois $i(\omega) = \dim W - \deg W + g - 1$).

I.4.17 Teorema Se A é um divisor de F/K com grau maior ou igual que $2g - 1$, então

$$\dim A = \deg A + 1 - g$$

Novamente, basta aplicar o Teorema I.4.15.

I.5 Algumas Conseqüências do Teorema de Riemann-Roch

Como anteriormente, F/K denota um corpo de funções algébricas de gênero g . Nosso primeiro objetivo é mostrar que o Teorema de Riemann-Roch caracteriza o gênero e também a classe canônica de F/K .

I.5.1 Proposição Suponha que $g_0 \in \mathbb{Z}$ e $W_0 \in \mathcal{D}_F$ satisfazem

$$\dim A = \deg A + 1 - g_0 + \dim(W_0 - A) \quad (\text{I.27})$$

para qualquer $A \in \mathcal{D}_F$. Então $g_0 = g$, e W_0 é um divisor canônico.

Demonstração :

Para $A = 0$:

$$\dim 0 = \deg 0 + 1 - g_0 + \dim W_0$$

$$1 = 0 + 1 - g_0 + \dim W_0$$

$$\dim W_0 = g_0$$

Para $A = W_0$:

$$\dim W_0 = \deg W_0 + 1 - g_0 + \dim 0$$

$$g_0 = \deg W_0 + 1 - g_0 + 1$$

$$\deg W_0 = 2g_0 - 2$$

Considere W um divisor canônico de F/K e escolha $A \in \mathcal{D}_F$ com $\deg A > \max\{2g - 2, 2g_0 - 2\}$, então:

$$\dim A = \deg A + 1 - g \quad (\text{I.28})$$

$$\deg(W_0 - A) = \deg W_0 - \deg A$$

$$\deg(W_0 - A) < 2g - 2 - \max\{2g - 2, 2g_0 - 2\} \leq 0$$

$$\dim(W_0 - A) = 0, \text{ logo,}$$

$$\dim A = \deg A + 1 - g_0 \quad (\text{I.29})$$

De (I.28) e (I.29), temos $g = g_0$. Considere $A = W$ em (I.27):

$$\dim W = \deg W + 1 - g + \dim(W_0 - W)$$

$$g = 2g - 2 + 1 - g + \dim(W_0 - W)$$

$$1 = \dim(W_0 - W)$$

$$\Rightarrow 0 = \deg(W_0 - W)$$

$$\Rightarrow W_0 - W \text{ é principal}$$

$$\Rightarrow W_0 \sim W$$

$$\Rightarrow W_0 \text{ é canônico}$$

□

I.5.2 Proposição Um divisor B é canônico se $\deg B = 2g - 2$ e $\dim B \geq g$.

Demonstração : Suponha $\deg B = 2g - 2$ e $\dim B \geq g$. Considere um divisor canônico W ; então:

$$g \leq \dim B = \deg B + 1 - g + \dim(W - B)$$

$$g \leq 2g - 2 + 1 - g + \dim(W - B)$$

$$1 \leq \dim(W - B)$$

Agora por I.5.1, $1 \leq \dim(W - B)$ se B é canônico.

□

1.5.3 Proposição Para um corpo de funções, as condições a seguir são equivalentes:

1. F/K é racional, i.e., $F = K(x)$ para algum x transcendente sobre K .
2. F/K tem gênero 0 e existe $A \in \mathcal{D}_F$ com $\deg A = 1$.

Demonstração :

1. $\Rightarrow$ 2. Queremos mostrar que o corpo das funções racionais $K(x)/K$ têm gênero $g = 0$. Afim de provar isto, seja P_∞ o divisor de polos de x . Considere, para $r \geq 0$, o espaço vetorial $\mathcal{L}(rP_\infty)$. Obviamente, os elementos $1, x, \dots, x^r$ estão em $\mathcal{L}(rP_\infty)$.

$$(x) = P_0 - P_\infty \Rightarrow (x) \geq -P_\infty \geq -rP_\infty \Rightarrow x \in \mathcal{L}(rP_\infty)$$

$$v_P(1) = 0, \forall P \in \mathbb{P}_F, 0 \geq -rP_\infty \Rightarrow 1 \in \mathcal{L}(rP_\infty)$$

$$v_P(x^i) = i.v_P(x) \geq v_P(x) \geq -rP_\infty \Rightarrow x^i \in \mathcal{L}(rP_\infty), i = 2, \dots, r.$$

Como os elementos $1, x, \dots, x^r$ são linearmente independentes, temos:

$$\begin{aligned} r+1 &\leq \dim(r.P_\infty) \\ &= \deg(r.P_\infty) + 1 - g, \text{ para } r \gg 0 \\ &= r+1 - g \\ g &\leq 0 \end{aligned}$$

Como $g \geq 0$, então, $g = 0$. Considere $A = P_\infty \in \mathcal{D}_F$; $\deg A = 1$.

2. $\Rightarrow$ 1. $g = 0$ e $\exists A \in \mathcal{D}_F$ com $\deg A = 1$, então:

$$\begin{aligned} 1 = \deg A &\geq 2g - 1 = -1 \Rightarrow \\ &\Rightarrow \dim A = \deg A + 1 - g = 2 \\ &\Rightarrow \mathcal{L}(A) \neq \{0\} \\ &\stackrel{1.3.5(b)}{\Rightarrow} \exists 0 \leq A' \in \mathcal{D}_F, A' \sim A \text{ com } \dim A = \dim A' = 2 \\ &\Rightarrow \exists x \in \mathcal{L}(A') \setminus K \\ &\Rightarrow (x) \neq 0 \text{ e } (x) + A' \geq 0 \end{aligned}$$

Como $A \geq 0$ e $\deg A' = \deg A = 1$, isto só é possível se $A' = (x)_\infty$ (pois caso contrário, x não teria polo). Assim,

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

□

1.5.4 Teorema (da Aproximação Forte) Seja $S \subsetneq \mathbb{P}_F$ um subconjunto próprio de $\mathbb{P}_F$ e $P_1, \dots, P_r \in S$. Suponha que sejam dados $x_1, \dots, x_r \in F$ e $n_1, \dots, n_r \in \mathbb{Z}$. Então, existe um elemento $x \in F$ tal que

$$\begin{aligned} v_{P_i}(x - x_i) &= n_i, \quad i = 1, \dots, r \\ v_P(x) &\geq 0, \quad \forall P \in S \setminus \{P_1, \dots, P_r\} \end{aligned}$$

Demonstração : Considere o adele $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ com

$$\alpha_P = \begin{cases} x_i & , \text{ se } P = P_i \\ 0 & , \text{ caso contrário} \end{cases}$$

Escolha um lugar $Q \in \mathbb{P}_F \setminus S$ e para $m \in \mathbb{N}$ considere

$$D = mQ - \sum_{i=1}^r ((n_i + 1)P_i).$$

Para $m \gg 0$, temos que $\deg D \geq c$, então:

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

Logo, existe $z \in F$ tal que $z - \alpha \in \mathcal{A}_F(D)$. Isto significa que $v_P(z - \alpha) = v_P(z - \alpha_P)$ vale:

$$v_{P_i}(z - x_i) \geq n_i + 1, P = P_i \text{ e } i = 1, \dots, r \quad (I.30)$$

$$v_P(z) \geq 0, \text{ se } P \in S \setminus \{P_1, \dots, P_r\}. \quad (I.31)$$

Escolha $y_1, \dots, y_r \in F$ tais que $v_{P_i}(y_i) = n_i$. Considere $\alpha' = (\alpha'_P)_{P \in \mathbb{P}_F}$ com :

$$\alpha_{P'} = \begin{cases} y_i & , P = P_i \\ 0 & , \text{ caso contrário.} \end{cases}$$

Existe $Q' \in \mathbb{P}_F$ tal que para $m' \gg 0$ e $m' \in \mathbb{N}$

$$\mathcal{A}_F = \mathcal{A}_F(m'Q' - \sum_{i=1}^r (n_i + 1)P_i) + F.$$

Logo, existe $y \in F$ tal que $v_P(y - \alpha') = v_P(y - \alpha'_P)$ e vale:

$$v_{P_i}(y - y_i) > n_i, i = 1, \dots, r \quad (I.32)$$

$$v_P(y) \geq 0, \forall P \notin S. \quad (I.33)$$

Para $i = 1, \dots, r$:

$$\begin{aligned} v_{P_i}(y) &= v_{P_i}((y - y_i) + y_i) \\ &= \min\{v_{P_i}(y - y_i), v_{P_i}(y_i)\} \\ &= n_i. \end{aligned} \quad (I.34)$$

Considere $x = y + z$

$$\begin{aligned} v_{P_i}(x - x_i) &= v_{P_i}(y + (z - x_i)) & v_P(x) &= v_P(z + y) \\ &= \min\{v_{P_i}, v_{P_i}(z - x_i)\} & &\geq \min\{v_P(y), v_P(z)\} \\ &= n_i & &\geq 0 \end{aligned}$$

Logo, foi encontrado $x \in F$ tal que $v_{P_i}(x - x_i) = n_i$ e $v_P(x) \geq 0, P \notin S$. □

I.5.5 Proposição *Seja $P \in \mathbb{P}_F$. Então, para qualquer $n \geq 2g$, existe um elemento $x \in F$ com divisor de polos $(x)_\infty = nP$.*

Demonstração : Pelo Teorema I.4.17 sabemos que se $n - 1 > 2g$, então

$$\dim((n - 1)P) = (n - 1)\deg P + 1 - g \text{ e } \dim(nP) = n\deg P + 1 - g;$$

assim, $\mathcal{L}(nP) \not\subseteq \mathcal{L}((n - 1)P)$ e portanto, $(x)_\infty = nP$. □

I.6 Componentes Locais dos Diferenciais de Weil

I.6.1 Definição Seja $P \in \mathbb{P}_F$

- (a) Para $x \in F$, seja $i_P(x) \in \mathcal{A}_F$ o adele cuja P -componente é x , e as demais são zero.
- (b) Para um diferencial de Weil $\omega \in \Omega_F$ definimos sua *componente local* $\omega_P : F \rightarrow K$ por $\omega_P(x) = \omega(i_P(x))$. Claramente, ω_P é uma aplicação K -linear.

I.6.2 Proposição *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,

$$\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0. \quad (I.35)$$

Demonstração : Dados $\alpha = (\alpha_P) \in \mathcal{A}_F$ e $\omega \in \Omega_F$, queremos mostrar que $\omega_P(\alpha_P) \neq 0$ para no máximo um número finito de lugares .

- $\alpha = (\alpha_P) \in \mathcal{A}_F \mid \Rightarrow \alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$, assim:

$$S_\alpha = \{P \in \mathbb{P}_F / \alpha_P \notin \mathcal{O}_P\} \text{ é finito}$$

- $W = (\omega) \in \mathcal{D}_F \Rightarrow v_P(W) = 0$ para quase todo $P \in \mathbb{P}_F$:

$$S_W = \text{supp} W \text{ é finito}$$

Considere $S = S_\alpha \cup S_W$, então, $\forall P \notin S$, temos

$$P \notin S_W \Rightarrow v_P(W) = 0 \quad \text{e} \quad P \notin S_\alpha \Rightarrow v_P(\alpha_P) \geq 0$$

Seja $\beta = (\beta_P) \in \mathcal{A}_F$ com

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

então

$$v_P(\beta) = \begin{cases} v_P(\alpha_P) \geq 0 = -v_P(W) & , P \notin S \\ v_P(0) = \infty \geq -v_P(W) & , P \in S; \end{cases}$$

logo, $\beta \in \mathcal{A}_F(W)$.

Note que

$$\alpha = \sum_{P \in \mathbb{P}_F} i_P(\alpha_P) \quad \text{e} \quad \beta = \sum_{P \in \mathbb{P}_F} i_P(\beta_P) = \sum_{P \notin S} i_P(\alpha_P);$$

logo, $\alpha = \beta + \sum_{P \in S} i_P(\alpha_P)$ e

$$\begin{aligned} \omega(\alpha) &= \omega(\beta) + \omega\left(\sum_{P \in S} i_P(\alpha_P)\right) \\ &= 0 + \sum_{P \in S} \omega(i_P(\alpha_P)) \\ &= \sum_{P \in S} \omega_P(\alpha_P). \end{aligned}$$

Logo, a soma é finita.

$\vdash \omega_P(\alpha_P) = 0$ para quase todo P .

Se $P \notin S : v_P(\alpha_P) \geq 0, v_P(W) = 0 \Rightarrow i_P(\alpha_P) \in \mathcal{A}_F(W) \Rightarrow \omega_P(\alpha_P) = \omega(i_P(\alpha_P)) = 0$.

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

$1 \in F$ e ω se anula em F e $0 = \omega(1) = \sum_{P \in \mathbb{P}_F} \omega_P(1)$. □

1.6.3 Proposição

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

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

Em particular, $\omega_P \neq 0$.

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

Demonstração :

(a) Dado $\omega \in \Omega_F$, $W = (\omega)$ e $P \in \mathbb{P}_F$, considere

$$S = \{r \in \mathbb{Z} \mid \omega_P(x) = 0 \forall x \in F, v_P(x) \geq -r\}$$

Considere $v_P(\omega)$ e $x \in F$ com $v_P(x) \geq -v_P(\omega)$; o adele $i_P(x) \in \mathcal{A}_F$ é tal que

$$v_Q(i_P(x)) = \begin{cases} v_P(i_P(x)) = v_P(x) & , Q = P \\ \infty & , Q \neq P \end{cases}$$

logo, $v_Q(i_P(x)) \geq -v_Q(\omega)$, $\forall Q \in \mathbb{P}_F$; assim $i_P(x) \in \mathcal{A}_F(W)$ e $\omega_P(x) = \omega(i_P(x)) = 0$; portanto, $v_P(\omega) \in S$. Seja $s = v_P(\omega)$ e suponha que não é elemento máximo de S ; então $s + 1 \in S$; logo, para todo $x \in F$ com $v_P(x) \geq -(s + 1)$ temos $\omega_P(x) = 0$. Considere $\alpha = (\alpha_Q)_{Q \in \mathbb{P}_F} \in \mathcal{A}_F(W + P)$, então, $v_Q(\alpha_Q) \geq -(v_Q(W) + v_Q(P))$, $\forall Q \in \mathbb{P}_F$ e $\alpha = (\alpha - i_P(\alpha_P)) + (i_P(\alpha_P))$.

$\vdash \alpha - i_P(\alpha_P) \in \mathcal{A}_F(W)$

$$\begin{aligned} v_Q(\alpha - i_P(\alpha_P)) &= v_Q(\alpha_Q) - v_Q(i_P(\alpha_P)) \\ &= \begin{cases} v_P(\alpha_P) - v_P(\alpha_P) = 0 \geq -s = -v_P(W) & , Q = P \\ v_Q(\alpha_Q) \geq -(v_Q(W) + v_Q(P)) = -v_Q(W) & , Q \neq P \end{cases} \end{aligned}$$

$\vdash \omega(i_P(\alpha_P)) = 0$

Por hipótese, $\forall x \in F$ se $v_P(x) \geq -(s + 1)$ então $\omega_P(x) = 0$. Para $\alpha \in \mathcal{A}_F(W + P)$ temos $v_P(\alpha) = v_P(\alpha_P) \geq -(s + 1)$ e portanto, $\omega_P(i_P(\alpha_P)) = \omega_P(\alpha_P) = 0$. Logo, temos:

$$\omega(\alpha) = \omega(\alpha - i_P(\alpha_P)) + \omega(i_P(\alpha_P)) = 0,$$

ou seja, ω se anula em $\mathcal{A}_F(W + P)$!Contradição. Logo, $v_P(\omega)$ é maximal.

1.6.3.1 Observação Note que dados $\omega \in \Omega_F$ e $P \in \mathbb{P}_F$ o conjunto

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

só tem máximo para $\omega \neq 0$; pois se $\omega = 0$, $\omega(i_P(x)) = 0$, $\forall x \in F$ e $\forall x \in F, \omega_P(x) = 0$; logo, $\forall r \in \mathbb{Z}$, $v_P(x) \geq -r$ temos $\omega_P(x) = 0$ e $R_{P_\omega} = \mathbb{Z}$.

I.6.3.2 Observação Se $s = \max R_{P_\omega}$, então para todo $t > s$ temos $t \notin R_{P_\omega}$. Considere R_{P_ω} e $S_{P_a} = \{x \in F / v_P(x) \geq -a\}$. Então, se $a \in R_{P_\omega}$, $\omega_P(x) = 0, \forall x \in S_{P_a}$. Considere $b \leq a$, então $\forall x \in S_{P_b}, v_P(x) \geq -b \geq -a \Rightarrow x \in S_{P_a} \Rightarrow S_{P_b} \subseteq S_{P_a}$ e portanto, $b \in R_{P_\omega}$. Logo, $\forall r \geq s+1, r \in R_{P_\omega}$ temos $s+1 \in R_{P_\omega}$; bastou provar (a) para $s+1$.

- (b) $\omega, \omega' \in \Omega_F, \exists P \in \mathbb{P}_F$ tal que $\omega_P = \omega'_P$. Logo, $\forall x \in F, \omega_P(x) = \omega'_P(x)$ isto é, $\omega(i_P(x)) = \omega'(i_P(x))$ e assim $(\omega - \omega')(i_P(x)) = 0$ logo, $(\omega - \omega')(x) = 0$ e $R_{P_{(\omega - \omega')}} = \mathbb{Z}$; logo, pela Observação I.6.3.1, $\omega - \omega' = 0$ ou seja, $\omega = \omega'$.

□

I.6.4 Proposição Para o corpo das funções racionais $F = K(x)$, vale:

- (a) O divisor $-2P_\infty$ é canônico.
(b) Existe um único diferencial de Weil $\eta \in \Omega_{K(x)}$ com $(\eta) = -2P_\infty$ e $\eta_{P_\infty}(x^{-1}) = -1$.
(c) As componentes locais η_{P_∞} e η_{P_a} do diferencial de Weil satisfazem

$$\eta_{P_\infty}((x-a)^n) = \begin{cases} 0 & , n \neq -1 \\ -1 & , n = -1 \end{cases} \quad \text{e} \quad \eta_{P_a}((x-a)^n) = \begin{cases} 0 & , n \neq -1 \\ 1 & , n = -1 \end{cases}$$

Demonstração :

- (a) Lembre que em $K(x)/K$ o gênero é $g = 0$; logo,

$$\left. \begin{aligned} \deg(-2P_\infty) &= -2 = 2g - 2 \\ \dim(-2P_\infty) &= 0 = g, \text{ pois } -2P_\infty < 0 \end{aligned} \right\} \Rightarrow -2P_\infty \text{ é canônico}$$

- (b) Escolha $\omega \in \Omega_F$ com divisor canônico $(\omega) = -2P_\infty$

Como $\dim(\mathcal{A}_F(-P_\infty)/\mathcal{A}_F(-2P_\infty)) = 1$, ω não se anula totalmente em $-P_\infty$ de fato,

$$i_{P_\infty}(x^{-1}) \in \mathcal{A}_F(-P_\infty) \setminus \mathcal{A}_F(-2P_\infty)$$

$$(v_{P_\infty}(i_{P_\infty}(x^{-1}))) = v_{P_\infty}(x^{-1}) = 1 = -v_{P_\infty}(-P_\infty) < -v_{P_\infty}(-2P_\infty) = 2$$

Como $\{i_{P_\infty} + \mathcal{A}_F(-2P_\infty)\}$ é base de $\mathcal{A}_F(-P_\infty)/\mathcal{A}_F(-2P_\infty)$ e ω não se anula em $\mathcal{A}_F(-P_\infty)$, então $\omega_{P_\infty}(x^{-1}) = \omega(i_{P_\infty}(x^{-1})) = c \neq 0$. Considere $\eta = -c^{-1}$:

$$(\eta) = (-c^{-1}\omega) = (-c^{-1}) + (\omega) = -2P_\infty$$

$$\eta_{P_\infty}(x^{-1}) = (-c^{-1}\omega)_{P_\infty}(x^{-1}) = -c^{-1}\omega_{P_\infty}(x^{-1}) = -c^{-1}c = -1$$

$\vdash \eta$ é único

Seja $\eta^* \in \Omega_F$, tal que $(\eta^*) = -2P_\infty$ e $\eta_{P_\infty}^*(x^{-1}) = -1$. Lembramos que $g = 0$ e se $\deg A \geq 2g - 1 = -1 \Rightarrow \mathcal{A}_F = \mathcal{A}_F(A) + F$. Note que $\deg_{P_\infty} = -1$:

$$\forall \alpha \in \mathcal{A}_F(-P_\infty) \setminus \mathcal{A}_F(-2P_\infty), \exists a \in K, \gamma \in \mathcal{A}_F(-2P_\infty)$$

tais que

$$\alpha - ai_{P_\infty}(x^{-1}) = \gamma$$

Logo,

$$\begin{aligned}
(\eta - \eta^*)(\alpha) &= (\eta - \eta^*)(ai_{P_\infty}(x^{-1}) + \gamma) \\
&= a\eta(i_{P_\infty}(x^{-1})) - a\eta^*(i_{P_\infty}(x^{-1})) + \eta(\gamma) - \eta^*(\gamma) \\
&= \eta_{P_\infty}(x^{-1}) - \eta_{P_\infty}^*(x^{-1}) \\
&= -1a - (-1)a \\
&= 0 \\
&\Rightarrow \forall \alpha \in \mathcal{A}_F, (\eta - \eta^*)(\alpha) = 0 \Rightarrow \eta = \eta^*
\end{aligned}$$

(c) Por definição, todo diferencial de Weil de F/K se anula em F e em cada $\alpha \in \mathcal{A}_F, \omega(\alpha) = \sum_{P \in \mathbf{P}_F} \omega_P(\alpha_P)$. Considere $\eta \in \Omega_F$ e $(x-a)^n \in F$.

$$v_{P_\infty}((x-a)^n) = -n, v_{P_a}((x-a)^n) = n \text{ e } v_P((x-a)^n) = 0 \text{ se } P \neq P_a, P_\infty$$

$$\begin{aligned}
v_P(\eta) &= \max\{r \in \mathbb{Z} / \eta_P(x) = 0, \forall x \in F \text{ com } v_P(x) \geq -r\} \\
&\Rightarrow \eta((x-a)^n) = \eta_{P_\infty}((x-a)^n) + \eta_{P_a}((x-a)^n) = 0
\end{aligned} \tag{I.36}$$

- $v_{P_\infty}(\eta) = -2$
 $n \leq -2$: $v_{P_\infty}((x-a)^n) = -n \geq 2 = -v_{P_\infty}(\eta) \Rightarrow \eta_{P_\infty}((x-a)^n) = 0$
 Por (I.36) temos $\eta_{P_a}((x-a)^n) = 0$.

- $v_{P_a}(\eta) = 0$
 $n \geq 0$: $v_{P_a}((x-a)^n) = n \geq 0 = -v_{P_a}(\eta) \Rightarrow \eta_{P_a}((x-a)^n) = 0$
 De (I.36) temos $\eta_{P_\infty}((x-a)^n) = 0$

- $n = -1$

$$\frac{1}{x-a} = \frac{x+a-a}{x(x-a)} = \frac{a}{x(x-a)} + \frac{1}{x}$$

$$v_{P_\infty}\left(\frac{a}{x(x-a)}\right) = 2 \geq -v_{P_\infty}(\eta) \Rightarrow \eta_{P_\infty}\left(\frac{a}{x(x-a)}\right) = 0; \eta_{P_\infty}\left(\frac{1}{x}\right) = -1$$

$$\text{Logo, } \eta_{P_\infty}((x-a)^{-1}) = \eta_{P_\infty}(x^{-1}) = -1 \text{ e portanto, de (I.36) } \Rightarrow \eta_{P_a}((x-a)^{-1}) = 1$$

□

Capítulo II

Códigos Geométricos de Goppa

Neste capítulo, descreveremos a construção de códigos corretores de erros proposta por Goppa usando corpos de funções algébricas. Começamos com um breve estudo dos conceitos da Teoria dos Códigos e em seguida definiremos os códigos geométricos de Goppa, desenvolvendo suas propriedades básicas. Finalmente na seção 2.3, discutiremos os códigos construídos por meio de corpos de funções.

II.1 Códigos

Nesta seção iremos introduzir algumas noções básicas da teoria dos códigos. Seja $\mathbb{F}_q$ um corpo finito com q elementos. Consideramos o espaço vetorial n -dimensional $\mathbb{F}_q^n$ cujos elementos são as n -uplas $a = (a_1, \dots, a_n)$ com $a_i \in \mathbb{F}_q$.

II.1.1 Definição Para $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_n)$ em $\mathbb{F}_q^n$ seja

$$d(a, b) = |\{i : a_i \neq b_i\}|$$

Esta função d é chamada *distância de Hamming* em $\mathbb{F}_q^n$. O *peso* de um elemento $a \in \mathbb{F}_q^n$ é definido por

$$\omega(a) = d(a, 0) = |\{i : a_i \neq 0\}|$$

Pode ser verificado facilmente que a distância de Hamming é uma métrica em $\mathbb{F}_q^n$. Em particular, a *Desigualdade Triangular* $d(a, c) \leq d(a, b) + d(b, c)$ vale para todo $a, b, c \in \mathbb{F}_q^n$.

II.1.2 Definição Um *código linear* C (sobre o alfabeto $\mathbb{F}_q$) é um subespaço linear de $\mathbb{F}_q^n$; os elementos de C são chamados *palavras-código*. Chamamos n de *comprimento* de C e $\dim C$ (como $\mathbb{F}_q$ espaço vetorial) a *dimensão* de C . Um $[n, k]$ -código é um código de comprimento n e dimensão k . A *distância mínima* $d(C)$ de um código $C \neq 0$ é definida por

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

Como $d(a, b) = d(a - b, 0) = \omega(a - b)$ e C é um espaço linear, a distância mínima é igual a

$$d(C) = \min\{\omega(c) : c \in C\}$$

Vamos nos referir a um $[n, k]$ -código com distância mínima d por $[n, k, d]$ -código. A *distribuição de peso* de um $[n, k, d]$ -código é a $(n + 1)$ -upla $(A_0, \dots, A_n) \in \mathbb{N}^{n+1}$ dada por

$$A_i = |\{c \in C : \omega(c) = i\}|$$

Evidentemente, $A_0 = 1$ e $A_i = 0$ para $1 \leq i \leq d(C) - 1$. O polinômio

$$W_C(X) = \sum_{i=1}^n A_i X^i \in \mathbb{Z}[X]$$

é chamado o *enumerador de pesos* de C .

Para um código C com distância mínima $d = d(C)$, seja $t = \lfloor (d-1)/2 \rfloor$ (onde $\lfloor x \rfloor$ denota a parte inteira do número real x). Então C é dito *capaz de corrigir até t erros*. A seguinte afirmação é evidente: se $u \in \mathbb{F}_q^n$ e $d(u, c) \leq t$ para algum $c \in C$, então c é a única palavra-código com $d(u, c) \leq t$.

Um modo simples de descrever um código C explicitamente é escrever uma base de C (como espaço espaço vetorial sobre $\mathbb{F}_q^n$).

II.1.3 Definição Seja C um código sobre $\mathbb{F}_q^n$. Uma *matriz geradora* de C é uma matriz $k \times n$ cujas linhas formam uma base de C .

II.1.4 Definição O *produto interno canônico* em $\mathbb{F}_q^n$ é definido por

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

para $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_n)$ em $\mathbb{F}_q^n$. Evidentemente, esta é uma forma bilinear simétrica não degenerada em $\mathbb{F}_q^n$.

II.1.5 Definição Se $C \subseteq \mathbb{F}_q^n$ é um código, então

$$C^\perp = \{u \in \mathbb{F}_q^n \mid \langle u, c \rangle = 0, \forall c \in C\}$$

é chamado o *código dual* de C .

C é chamado *auto-dual* (respec. *auto-ortogonal*) se $C = C^\perp$ (respec. $C \subseteq C^\perp$). A álgebra linear nos diz que o dual de um $[n, k]$ -código é um $[n, n-k]$ -código e $(C^\perp)^\perp = C$. Em particular, a dimensão de um código auto-dual de comprimento n é $n/2$.

II.1.6 Definição Uma matriz geradora H de $C^\perp$ é dita *matriz de verificação de paridade* de C .

Claramente, uma matriz de verificação de paridade de um $[n, k]$ -código é uma matriz H , $(n-k) \times n$ com posto $n-k$ e tem-se

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

(onde u^t denota a transposta de u). Logo, uma matriz de verificação de paridade identifica se um vetor $u \in \mathbb{F}_q^n$ é uma palavra-código ou não.

Um dos problemas básicos na teoria de códigos algébricos é o de construir, sobre um alfabeto fixado $\mathbb{F}_q$, códigos cuja dimensão e distância mínima sejam grandes em comparação com o seu comprimento. Entretanto, há algumas restrições: se a dimensão de um código é grande (com relação ao seu comprimento) então, sua distância mínima é pequena. A cota mais simples é a seguinte.

II.1.7 Proposição (Cota de Singleton) Para um $[n, k, d]$ -código vale

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

Demonstração : Considere o subespaço linear $W \subseteq \mathbb{F}_q^n$ dado por

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

Qualquer $a \in W$ tem peso $\omega(a) \leq d - 1$, logo, $W \cap C = \{0\}$. Como $\dim W = d - 1$, obtemos

$$\begin{aligned} k + (d - 1) &= \dim C + \dim W \\ &= \dim(C + W) + \dim(C \cap W) \\ &= \dim(C + W) \\ &\leq n \end{aligned}$$

□

Códigos com $k + d = n + 1$ são de certa forma ótimos; tais códigos são chamados *códigos MDS* (*maximum distance separable*). Se $n \leq q + 1$, então existem códigos MDS sobre $\mathbb{F}_q$ para toda dimensão $k \leq n$.

II.2 Códigos Geométricos de Goppa

Para introduzirmos a noção de um código geométrico de Goppa, fixemos algumas notações para esta seção:

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

$P_1, \dots, P_n$ lugares de $F/\mathbb{F}_q$ de grau 1, dois a dois distintos

$D = P_1 + \dots + P_n$

G divisor de $F/\mathbb{F}_q$ tal que $\text{supp} G \cap \text{supp} D = \emptyset$

II.2.1 Definição O *código geométrico de Goppa* $C_{\mathcal{L}}(D, G)$ associado aos divisores D e G é definido por

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

II.2.2 Observação A definição está bem feita:

- $x \in \mathcal{L}(G) \Rightarrow v_{P_i}(x) \geq 0 = v_{P_i}(G), \forall i$, pois $\text{supp} D \cap \text{supp} G = \emptyset$.
- a classe residual $x(P_i)$ de x módulo P_i é um elemento do corpo de classes de resíduos de P_i (I.1.14); como $\deg P_i = 1$, o corpo das classes de resíduos é $\mathbb{F}_q$; logo, $x(P_i) \in \mathbb{F}_q$.

Consideremos a aplicação de avaliação

$$\begin{aligned} ev_D : \mathcal{L}(G) &\longrightarrow \mathbb{F}_q^n \\ x &\longmapsto (x(P_1), \dots, x(P_n)) \end{aligned} \quad (\text{II.1})$$

Esta aplicação de avaliação é $\mathbb{F}_q$ -linear e $C_{\mathcal{L}}(D, G)$ é a imagem de $\mathcal{L}(G)$ por ev_D .

II.2.3 Teorema $C_{\mathcal{L}}(D, G)$ é um $[n, k, d]$ -código com parâmetros

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

Demonstração : Considerando $ev_D : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$, sabemos que

$$\mathcal{L}(G)/\text{Ker}(ev_D) \cong \text{Im}(ev_D) = C_{\mathcal{L}}(D, G).$$

Logo,

$$k = \dim G - \dim \text{Ker}(ev_D)$$

Considere $x \in \mathcal{L}(G)$ tal que $ev_D(x) = (0, \dots, 0)$, i.e. $x(P_i) = 0, \forall i$, o que só ocorre se $x \in P_i, \forall i$; daí, temos que $v_i(x) \geq 1, \forall i$, i.e., $v_i(x) \geq v_i(D) > v_i(G) = 0$; logo, $v_P(x) \geq -v_P(G - D) \forall P \in \mathbb{P}_F$, pois se $P \notin \{P_1, \dots, P_n\}$, então $v_P(G - D) = v_P(G)$. Como vale a recíproca de cada uma das implicações, conclui-se que $\text{Ker}(ev_D) = \mathcal{L}(G - D)$, e fica provado que $k = \dim G - \dim(G - D)$. Assumindo $C_{\mathcal{L}}(D, G) \neq 0$, escolha $x \in \mathcal{L}(G)$, com $\omega(ev_D(x)) = d = d(C_{\mathcal{L}}(D, G))$. Então, existem $n - d$ índices $j_1, \dots, j_{n-d} \in \{1, \dots, n\}$ tais que $x(P_{j_i}) = 0$; logo, $x \in \mathcal{L}(G - (P_{j_1} + \dots + P_{j_{n-d}})) \setminus \{0\}$, i.e., $\dim(G - (P_{j_1} + \dots + P_{j_{n-d}})) \geq 1$, ou seja $\deg(G - (P_{j_1} + \dots + P_{j_{n-d}})) \geq 0$. Portanto: $\deg G - (n - d) \geq 0$ e assim concluímos que $d \geq n - \deg G$. $\square$

II.2.4 Corolário *Suponha que o grau de G é estritamente menor do que n . Então, a aplicação de avaliação $ev_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D, G)$ é injetiva e temos:*

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

$$d \geq n - \deg G \quad \text{e} \quad k = \dim G \geq \deg G + 1 - g$$

Logo,

$$k + d \geq n + 1 - g \quad (\text{II.2})$$

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

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

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

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

Demonstração : Como $\deg G < n$ e $\deg(G - D) = \deg G - \deg D < n - n = 0$, então, $\dim(G - D) = 0$, i.e., $\mathcal{L}(G - D) = \text{Ker}(ev_D) = \{0\}$, e portanto, ev_D é uma aplicação injetiva.

(a) Como $k = \dim G$, $d \geq n - \deg G$ e $\dim G \geq \deg G + 1 - g$, então

$$\begin{aligned} k + d &\geq \dim G + n - \deg G \\ &\geq n + 1 - g \end{aligned}$$

(b) Para $2g - 2 < \deg G$, pelo Teorema I.3.15 temos: $k = \dim G = \deg G + 1 - g$.

(c) Como $\{x_1, \dots, x_n\}$ é base de $\mathcal{L}(G)$ e ev_D é injetiva, temos que $\{x(P_1), \dots, x(P_n)\}$ é base de $C_{\mathcal{L}}(D, G)$ e M é uma matriz geradora. $\square$

Observe que a cota inferior (II.2) para a distância mínima é muito parecida com a cota superior de Singleton. Confrontando ambas cotas e com $\deg G < n$, temos

$$n + 1 - g \leq k + d \leq n + 1 \quad (\text{II.3})$$

Note que se F é corpo de funções com gênero $g = 0$, então $k + d = n + 1$, isto é, tem-se um código MDS. Assim, os códigos geométricos de Goppa construídos por meio de um corpo de funções racionais $\mathbb{F}_q(x)$ são sempre MDS. A fim de obter uma distância mínima significativa, geralmente considera-se $\deg G < n$.

II.2.5 Definição O inteiro $d^* = n - \deg G$ é chamado *distância projetada* de $C_L(D, G)$.

O teorema II.2.3 estabelece que a distância mínima de um código geométrico de Goppa não pode ser menor do que sua distância projetada.

II.2.6 Observação Suponha que $\dim G > 0$ e $d = n - \deg G > 0$. Então, $d^* = d$ se e existe um divisor D' com $0 \leq D' \leq D$, $\deg D' = \deg G$ e $\dim(G - D') > 0$.

Demonstração :

($\Rightarrow$) $d^* = d = n - \deg G$

Considere $x \in \mathcal{L}(G)$ tal que $\omega(\text{ev}_D(x)) = d$. Então, $\text{ev}_D(x) = (x(P_1), \dots, x(P_n))$ possui $\deg G = n - d$ coordenadas nulas, sejam elas $x(P_{i_1}), \dots, x(P_{i_{\deg G}})$. Seja $D' = \sum_{j=1}^{\deg G} P_{i_j}$, então $\deg D' = \deg G$, $0 \leq D' \leq D$ e $\dim(G - D') > 0$, pois $x \in \mathcal{L}(G - D')$.

($\Leftarrow$) $\exists 0 \leq D' \leq D$, $\deg D' = \deg G$ e $\dim(G - D') > 0$

Se $\dim(G - D') > 0$, então existe $x \in \mathcal{L}(G - D')$; para $P \in \text{supp } D$, considere $v_P(x)$

$$\begin{aligned} v_P(x) &\geq -v_P(G - D') \\ &\geq -v_P(G) + v_P(D') = \begin{cases} -0 + 1 & , \text{ se } P \in \text{supp } D' \\ -0 + 0 & , \text{ se } P \notin \text{supp } D' \end{cases} \\ \Rightarrow x(P) &= 0 \text{ para pelo menos } \deg D' \text{ lugares} \\ \Rightarrow \omega(\text{ev}_P(x)) &\leq n - \deg D' \\ &\left. \begin{aligned} d &\leq n - \deg G = d^* \\ \text{por II.2.3 } d &\geq n - \deg G \end{aligned} \right\} \Rightarrow d = d^*. \end{aligned}$$

□

Dados os divisores G e D , podemos associar a eles um outro código, por meio das componentes locais de diferenciais de Weil.

II.2.7 Definição Sejam G e $D = P_1 + \dots + P_n$ divisores como anteriormente. Então, defina o código $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ por

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

II.2.8 Teorema $C_\Omega(D, G)$ é um $[n, k', d']$ -código com parâmetros

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

Sob a hipótese adicional $\deg G > 2g - 2$, temos $k' = i(G - D) \geq n + g - 1 - \deg G$. Se além disso $2g - 2 < \deg G < n$, então $k' = n + g - 1 - \deg G$.

Demonstração : Primeiramente, provemos o seguinte:

Afirmção(*): Se $P \in \mathbb{P}_F$ e $\omega \in \Omega_F$ com $v_P(\omega) \geq -1$ e $\deg P = 1$, então:

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

Lembre que por I.6.3

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

($\Rightarrow$) Considere $x \in F$ com $v_P(x) \geq 0$. Como $\deg P = 1$, temos que $x = a + y$ com $a \in \mathbb{F}_q$ e $v_P(y) \geq 1$. Então: $\omega_P(x) = \omega_P(a) + \omega_P(y)$, mas desde que $v_P(y) \geq 1$ e $v_P(\omega) \geq -1$, tem-se por (#) que $\omega_P(y) = 0$ e assim $\omega_P(x) = a \cdot \omega_P(1) = 0$, logo $v_P(\omega) \geq 0$ por (#)

($\Leftarrow$) $v_P(\omega) \geq 0 \xrightarrow{\#} \omega_P(x) = 0, \forall x \in F$ com $v_P(x) \geq 0 \Rightarrow \omega_P(1) = 0$

Agora considere a aplicação $\mathbb{F}_q$ -linear:

$$\begin{aligned} \phi: \Omega(G-D) &\longrightarrow \mathbb{F}_q^n \\ \omega &\longmapsto (\omega_{P_1}(1), \dots, \omega_{P_n}(1)) \end{aligned}$$

então, $C_\Omega(D, G) \cong \Omega(G-D)/\text{Ker}(\phi)$. Primeiro vamos verificar que $\text{Ker} \phi = \Omega_F(G)$. Para isto, considere $\omega \in \text{Ker} \phi$; logo, $\omega_{P_i}(1) = 0$ para $i = 1, \dots, n$. Mas de $\omega \in \Omega_F(G-D)$, temos que $v_{P_i}(\omega) \geq v_{P_i}(G-D) = -v_{P_i}(D) = -1$ e como $\deg P_i = 1, \forall i$, pela afirmação temos $v_{P_i}(\omega) \geq 0, \forall i$; logo, $v_P(\omega) \geq v_P(G), \forall P \in \text{supp} G$, pois se $P \notin \{P_1, \dots, P_n\}$, $v_P(G) = v_P(G-D)$ e $\omega \in \Omega(G-D)$. Agora, se $\omega \in \Omega_F(G) \subseteq \Omega_F(G-D)$, então $(\omega) \geq G$ e portanto, $v_{P_i}(\omega) \geq 0$. De novo, usando (#) tem-se $\omega_{P_i}(1) = 0, \forall i$. Sabendo que $\text{Ker} \phi = \Omega_F(G)$, temos que $k' = \dim \Omega_F(G-D) - \dim \Omega_F(G)$; como $\dim \Omega_F(A) = i(A), A \in \mathcal{D}_F$, então conclui-se que:

$$k' = i(G-D) - i(G)$$

$$\vdash d' \geq \deg G - (2g-2)$$

Considere $(\omega_{P_i}(1), \dots, \omega_{P_i}(1)) = x \in C_\Omega(D, G)$, m o peso x ; então há $n-m$ índices $i = i_1, \dots, i_{n-m}$ tais que $\omega_{P_i}(1) = 0$, então usando (#) de novo temos:

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

$$(\omega) \geq G - (D - \sum_{j=1}^{n-m} P_{i_j}) \Rightarrow \deg(G - (D - \sum_{j=1}^{n-m} P_{i_j})) \leq 2g-2 = \deg((\omega))$$

Logo,

$$\begin{aligned} 2g-2 &\geq \deg(G - (D - \sum_{j=1}^{n-m} P_{i_j})) \\ &\geq \deg G - (n - (n-m)) \\ &\geq \deg G - m \\ \Rightarrow m &\geq \deg G - (2g-2) \end{aligned}$$

Em particular, se d' é a distância mínima, então

$$d' \geq \deg G - (2g-2)$$

- $\deg G > 2g-2$

$$\begin{aligned} \text{Por I.4.17, } i(G) = 0 \text{ e } k' &= i(G-D) = \dim(G-D) - \deg(G-D) - 1 + g \\ &= \dim(G-D) - \deg G + n - 1 + g \\ &\geq n + g - \deg G - 1 \end{aligned}$$

- $2g - 2 < \deg G < n$

$$\deg G < n, \deg D = n \Rightarrow G - D < 0 \Rightarrow \dim(G - D) = 0$$

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

□

A relação entre os códigos $C_{\mathcal{L}}(D, G)$ e $C_{\Omega}(D, G)$ é muito estreita e será apresentada no próximo resultado.

II.2.9 Teorema *Os códigos $C_{\mathcal{L}}(D, G)$ e $C_{\Omega}(D, G)$ são duais entre si, i.e.,*

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

Demonstração : Considere $\text{Im}(ev_D) = C_{\mathcal{L}}(D, G)$ e $\text{Im}\phi = C_{\Omega}(D, G)$, onde

$$\begin{aligned} ev_D : \mathcal{L}(G) &\longrightarrow \mathbb{F}_q^n \\ x &\mapsto (x(P_1), \dots, x(P_n)) \end{aligned}$$

e

$$\begin{aligned} \phi : \Omega(G - D) &\longrightarrow \mathbb{F}_q^n \\ \omega &\mapsto (\omega_{P_1}(1), \dots, \omega_{P_n}(1)) \end{aligned}$$

Primeiro queremos mostrar que $C_{\Omega}(D, G) \subseteq C_{\mathcal{L}}(D, G)^{\perp}$. Para isto, considere $\omega \in \Omega_F(G - D)$ e $x \in \mathcal{L}(G)$. Lembre que ω anula $\mathcal{A}_F(G - D) + F$; assim, $0 = \omega(x) = \sum_{P \in \mathbf{P}_F} \omega_P(x)$. Agora considere $Q \notin \{P_1, \dots, P_n\}$ e observe que $v_Q(x) \geq -v_Q(G)$ e $v_Q(G - D) = v_Q(G)$. Mas, como $\omega \in \Omega_F(G - D)$, tem-se $v_Q(\omega) \geq v_Q(G) \geq -v_Q(x)$. Portanto, $\omega_Q(x) = 0$, pois $v_Q(\omega) = \max\{r \in \mathbb{Z}/\omega_P(x) = 0, \forall x \in F \text{ com } v_Q(x) \geq -r\}$ e assim, $0 = \omega(x) = \sum_{i=1}^n \omega_{P_i}(x)$. Mas, já que $v_{P_i}(x) \geq 0, \forall i$ e $\deg P_i = 1$, tem-se pela afirmação (*) do Teorema anterior que $\omega_{P_i}(x) = x(P_i) \cdot \omega_{P_i}(1)$ e finalmente, conclui-se que:

$$0 = \sum_{i=1}^n x(P_i) \cdot \omega_{P_i}(1) = \langle (x(P_1), \dots, x(P_n)), (\omega_{P_1}(1), \dots, \omega_{P_n}(1)) \rangle.$$

Agora, é preciso mostrar que $\dim C_{\Omega}(D, G) = \dim C_{\mathcal{L}}(D, G)$. Para isso, considere

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

□

Na verdade podemos encontrar um divisor apropriado H para o qual temos $C_{\mathcal{L}}(D, G) = C_{\Omega}(D, H)$. Mas, para isto necessitamos do seguinte lema:

II.2.10 Lema *Existe um diferencial de Weil η tal que*

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

Demonstração : Escolha um diferencial de Weil arbitrário $\omega_0 \neq 0$. Pelo Teorema de Aproximação Fraca, dados $P_1, \dots, P_n$ lugares, $r_i = -v_{P_i}(\omega_0) - 1, i = 1, \dots, n$, existe $z \in F$ tal que

$$v_{P_i}(z) = -v_{P_i}(\omega_0) - 1, i = 1, \dots, n.$$

Considere $\omega = z\omega_0$, então

$$\begin{aligned} v_{P_i}(z\omega_0) &= v_{P_i}(z) + v_{P_i}(\omega_0) \\ &= -v_{P_i}(\omega_0) - 1 + v_{P_i}(\omega_0) \\ &= -1 \end{aligned}$$

Como $v_{P_i}(1) = 0 < 1 = -v_{P_i}(z\omega_0)$, então $\omega_{P_i}(1) \neq 0, \forall i$ (por I.6.3(a)).

Pelo Passo 3 do Teorema de Aproximação Fraca, dados $a_i = \omega_{P_i}(1) \in K, i = 1, \dots, n, \exists y \in F$ tal que $v_{P_i}(y - a_i) > 0, \forall i$. Segue que $y(P_i) = a_i$ e $v_{P_i}(y) = 0, \forall i$. Considere $\eta = y^{-1}\omega$, então,

$$\begin{aligned} v_{P_i}(\eta) &= v_{P_i}(y^{-1}) + v_{P_i}(\omega) & \eta_{P_i}(1) &= (y^{-1}\omega)_{P_i}(1) \\ &= -v_{P_i}(y) + v_{P_i}(\omega) & &= \omega_{P_i}(y^{-1}1) \\ &= 0 + (-1) & \text{e} &= y^{-1}(P_i)\omega_{P_i}(1) \\ & & &= a_i^{-1}a_i \\ & & &= 1 \end{aligned}$$

□

II.2.11 Proposição *Seja η um diferencial de Weil tal que $v_{P_i}(x) = -1$ e $\eta_{P_i}(1) = 1$ para $i = 1, \dots, n$. Então*

$$C_{\mathcal{L}}(D, G)^\perp = C_{\Omega}(D, G) = C_{\mathcal{L}}(D, H) \text{ com } H = D - G + (\eta)$$

Demonstração : Como $v_{P_i}(\eta) = -1, \forall i$, então $(\eta) = -D + N, P_i \notin \text{supp}(N)$. Logo, $\text{supp}(H) = \text{supp}(D - G + (\eta)) = \text{supp}(D - G - D + N)$. Ou seja, $\text{supp}H \cap \text{supp}D = \emptyset$. Então o código $C_{\mathcal{L}}(D, H)$ pode ser definido. Como η é canônico, por I.4.14 posso definir a aplicação

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

a qual é um isomorfismo entre K -espaços vetoriais. Para $x \in \mathcal{L}(D - G + (\eta))$

$$(x\eta)_{P_i} = \eta_{P_i}(x) = x(P_i)\eta_{P_i}(1) = x(P_i).1;$$

logo,

$$\begin{aligned} C_{\Omega}(D, G) &= \{((x\eta)_{P_1}(1), \dots, (x\eta)_{P_n}(1))/x \in \mathcal{L}(D - G + (\eta))\} \\ &= \{(x(P_1), \dots, x(P_n))/x \in \mathcal{L}(H)\} \\ &= C_{\mathcal{L}}(D, H). \end{aligned}$$

□

Como consequência imediata da Proposição II.2.11, podemos fornecer condições suficientes para que um código $C_{\mathcal{L}}(D, G)$ seja auto-dual. Tal fato é expresso no seguinte resultado.

II.2.12 Corolário *Suponha que existe um diferencial de Weil η tal que*

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

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

Demonstração : Assumir que $(\eta) = 2G - D$ equivale a $G = D - G + (\eta)$. Logo, por II.2.11, $C_\Omega(D, G) = C_\mathcal{L}(D, G)$. $\square$

II.2.13 Corolário *Suponha que existe um diferencial de Weil η tal que*

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

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

Demonstração : Por II.2.11, se $H = D - G + (\eta)$, então, $C_\mathcal{L}(D, G)^\perp = C_\mathcal{L}(D, H)$ mas,

$$\begin{aligned} 2G - D &\leq (\eta) \\ G &\leq D - G + (\eta) \\ G &\leq H, \end{aligned}$$

logo, $C_\mathcal{L}(D, G) \subseteq C_\mathcal{L}(D, H) = C_\mathcal{L}(D, G)^\perp$, e portanto, $C_\mathcal{L}(D, G)$ é auto-ortogonal. $\square$

II.2.14 Definição Dois códigos $C_1, C_2 \in \mathbb{F}_q^n$ são ditos *equivalentes* se existe um vetor $a = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ tal que $C_2 = aC_1$, i.e.,

$$C_a = \{(a_1c_1, \dots, a_nc_n) | (c_1, \dots, c_n) \in C_1\}$$

Em direção a esta definição apresentamos o seguinte resultado.

II.2.15 Proposição

- (a) *Suponha G_1 e G_2 divisores, $G_1 \sim G_2$ e $\text{supp}G_i \cap \text{supp}D = \emptyset$. Então, os códigos $C_\Omega(D, G_1)$ e $C_\Omega(D, G_2)$ são equivalentes. O mesmo vale para $C_\mathcal{L}(D, G_1)$ e $C_\mathcal{L}(D, G_2)$.*
- (b) *Reciprocamente, se $C \subseteq \mathbb{F}_q^n$ é um código equivalente a $C_\mathcal{L}(D, G)$ (respec. $C_\Omega(D, G)$), então, existe um divisor $G' \sim G$ tal que $\text{supp}G' \cap \text{supp}G = \emptyset$ e $C = C_\Omega(D, G')$ (respec. $C_\Omega(D, G')$).*

Demonstração :

- (a) $G_1 \sim G_2 \Leftrightarrow \exists y \in F : G_2 = G_1 - (y)$

Agora para $j = 1, 2$ $\text{supp}G_j \cap \text{supp}D = \emptyset$; assim, $v_{P_i}(y) = 0, \forall i = 1, \dots, n$ e então $a = (y(P_1), \dots, y(P_n)) \in \mathbb{F}_q^n$. Como

$$\begin{aligned} \phi: \mathcal{L}(G_1) &\longrightarrow \mathcal{L}(G_2) \\ x &\longmapsto xy \end{aligned}$$

é bijetora, então:

$$\begin{aligned} \bullet \quad C_\mathcal{L}(D, G_2) &= \{(xy(P_1), \dots, xy(P_n)) / x \in \mathcal{L}(G_1)\} \\ &= \{(y(P_1), \dots, y(P_n)) \cdot (x(P_1), \dots, x(P_n)) / x \in \mathcal{L}(G_1)\} \\ &= aC_\mathcal{L}(D, G_1) \\ \bullet \quad C_\Omega(D, G_1) &= \{((y\omega)_{P_1}(1), \dots, (y\omega)_{P_n}(1)) / y\omega \in \Omega_F(G_1 - D)\} \\ &= \{(y(P_1), \dots, y(P_n)), (\omega_{P_1}(1), \dots, \omega_{P_n}(1))\} \\ &= aC_\Omega(D, G_2) \end{aligned}$$

- (b) Seja $C = a.C_L(D, G)$, $a \in \mathbb{F}_q$ e escolha $z \in F$, $z(P_i) = a_i$, $i = 1, \dots, n$; logo, $v_{P_i}(z - a_i) = 1 > 0$ (isso é possível pelo Teorema de Aproximação). Se $G' = G - (z)$, então $C = C_L(D, G')$. Se $C = a.C_\Omega(D, G)$, considere $G' = G + (z)$, então $C = C_\Omega(D, G')$

□

II.2.16 Observação Se G é um divisor tal que $\text{supp}G \cap \text{supp}D \neq \emptyset$, ainda podemos definir $C_L(D, G)$ como segue: escolha $G' \sim G$ com $\text{supp}G' \cap \text{supp}D = \emptyset$ (possível pelo teorema de aproximação) e considere $C_L(D, G) = C_L(D, G')$. Como a escolha de G' não é canônica, $C_L(D, G)$ é bem definido, a menos de equivalências, por II.2.15.

II.3 Códigos Geométricos de Goppa Associados com o Corpo de Funções Racionais

Nesta seção vamos investigar os códigos geométricos de Goppa associados a divisores do corpo de funções racionais. Neste caso, damos de maneira explícita, as matrizes geradora e de verificação de paridade. Na teoria de Códigos, esta classe é conhecida pelo nome de Códigos Generalizados de Reed-Solomon.

II.3.1 Definição Um código Geométrico de Goppa $C_L(D, G)$ associado aos divisores D e G de um corpo de funções racionais $\mathbb{F}_q(x)/\mathbb{F}_q$ é dito ser *racional*.

Observe que o comprimento de $C_L(D, G)$ é limitado por $q + 1$, pois $\mathbb{F}_q(x)$ possui somente $q + 1$ lugares de grau 1, o polo de z , e para cada $\alpha \in \mathbb{F}_q$ o zero P_α de $z - \alpha$.

II.3.2 Proposição Seja $C = C_L(D, G)$ um código geométrico racional de Goppa sobre $\mathbb{F}_q$, e sejam n, k, d os parâmetros de C . Então:

- (a) $n \leq q + 1$.
- (b) $k = 0$ se $\deg G < 0$, e $k = n$ se $\deg G > n - 2$.
- (c) Para $0 \leq \deg G \leq n - 2$, $k = 1 + \deg G$ e $d = n - \deg G$. Em particular, C é um código-MDS.
- (d) $C^\perp$ é também um código geométrico racional de Goppa.

Demonstração : Lembre que neste caso o gênero é zero e utilizando o Teorema II.2.3 e o Corolário II.2.4, temos:

- (a) Como $n = \deg D$, $D = P_1 + \dots + P_n$, P_i lugares de grau um de $\mathbb{F}_q$, distintos dois a dois, e $\mathbb{F}_q$ só possui $q + 1$ lugares de grau um, então $n \leq q + 1$.
- (b) $\vdash k = 0 \Leftrightarrow \deg G < 0$.

É bom lembrar que $n \geq 0$ (caso contrário, ev_D não pode ser definida) e que temos $g = 0$; logo, por I.3.15 vale a igualdade de Riemann para G : $\dim G = \deg G + 1$ (pois, $\deg G = 0 \geq 2g - 1$).

($\Leftarrow$) Se $\deg G < 0$ então $\mathcal{L}(G) = \{0\}$ logo, $\text{Im } ev_D = \{0\}$ e $k = 0$.

($\Rightarrow$) Por contradição; vamos supor que $\deg G \geq 0$. Há dois casos para considerar:

- Se $\deg G < n$; estamos nas condições de II.2.4; então, $k = \dim G = \deg G + 1 \geq 1$.

- Se $\deg G \geq n$; agora $G - D$ também satisfaz a igualdade de Riemann; portanto, $\dim(G - D) = \deg(G - D) + 1$. Então

$$\begin{aligned} k &= \dim G + 1 - \dim(G - D) - 1 \\ &= \deg G + 1 - \deg G + n - 1 \\ &= n \geq 1 \end{aligned}$$

Portanto, obtivemos contradições em ambos casos, e assim, concluímos que se $k = 0$, então $\deg G < 0$.

$$\vdash k = n \Leftrightarrow \deg G > n - 2$$

Como $C_{\mathcal{L}}(D, G)$ é código racional, $g = 0$ e $2g - 1 = -1$, então, $\forall A \in \mathcal{D}_F$ com $\deg A \geq -1$, vale $\dim A = \deg A + 1 - g = \deg A + 1$.

$$(\Rightarrow) k = n$$

Pela cota de Singleton,

$$\left. \begin{array}{l} k + d \leq n + 1 \\ k = n \end{array} \right\} \Rightarrow \left. \begin{array}{l} d \leq 1 \\ d \geq n - \deg G \end{array} \right\} \Rightarrow \deg G \geq n - 1 > n - 2$$

$$(\Leftarrow) \deg G > n - 2$$

Como $n \geq 1$, temos que $n - 2 \geq 1 - 2 = -1 = 2g - 1$. Então, $\dim G = \deg G + 1$. Logo, $\deg(G - D) = \deg G - n \geq n - 1 + n = -1$; assim, $\dim(G - D) = \deg G - n + 1$. Portanto:

$$\begin{aligned} k &= \dim G - \dim(G - D) \\ &= \deg G + 1 - [\deg G - n + 1] \\ &= n \end{aligned}$$

$$(c) \ 0 \leq \deg G \leq n - 2$$

$$\bullet \ k = 1 + \deg G$$

$$\left. \begin{array}{l} \deg G \geq 0 \Rightarrow \dim G = \deg G + 1 \\ \deg G \leq n - 2 \Rightarrow \deg(G - D) < 0 \Rightarrow \dim(G - D) = 0 \end{array} \right\} \Rightarrow k = 1 + \deg G$$

$$\bullet \ d = n - \deg G \text{ por II.2.3.}$$

(d)

$$\begin{aligned} C^{\perp} &= C_{\mathcal{L}}(D, G)^{\perp} \\ &= C_{\Omega}(D, G) \\ &= C_{\mathcal{L}}(D, H), \ H = D - G + (\eta) \text{ por II.2.12.} \end{aligned}$$

□

O próximo resultado determina, de modo explícito, a matriz geradora de um código racional de Goppa.

II.3.3 Proposição *Seja $C = C_{\mathcal{L}}(D, G)$ um código geométrico racional de Goppa sobre $\mathbb{F}_q$ com parâmetros n, k e d .*

- (a) Se $n \leq q$ existem elementos dois a dois distintos $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ e $v_1, \dots, v_n \in \mathbb{F}_q$ (não necessariamente distintos) tais que

$$C = \{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) | f \in \mathbb{F}_q[z] \text{ e } \deg f \leq k-1\}$$

A matriz

$$M = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \dots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \dots & \alpha_n^2 v_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \dots & \alpha_n^{k-1} v_n \end{pmatrix} \quad (\text{II.4})$$

é uma matriz geradora de C .

- (b) Se $n = q + 1$, C possui a matriz geradora

$$M = \begin{pmatrix} v_1 & v_2 & \dots & v_{n-1} & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \dots & \alpha_{n-1} v_{n-1} & 0 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \dots & \alpha_{n-1}^2 v_{n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \dots & \alpha_{n-1}^{k-1} v_{n-1} & 1 \end{pmatrix} \quad (\text{II.5})$$

onde $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_{n-1}\}$ e $v_1, \dots, v_{n-1} \in \mathbb{F}_q$.

Demonstração : Para encontrar a matriz geradora de um código é preciso encontrar uma base do mesmo. Como $C_{\mathcal{L}}(D, G) = ev_D(\mathcal{L}(G))$ é um código sobre $\mathbb{F}_q$, não nulo, por II.3.2, temos :

- (i) $0 < k < n \Rightarrow 0 \leq \deg G \leq n-2$.
(ii) $k = n \Leftrightarrow \deg G > n-2$.

Como estamos num corpo de gênero 0, pelo Teorema I.3.15, temos que para todo divisor G com $\deg G \geq 0$, $\dim G = \deg G + 1$. Agora, neste caso estamos supondo $k = \dim C \geq 1$; logo, por II.3.2, $\deg G \geq 0$ e $\dim G = \deg G + 1$.

- (a) Vamos construir uma base para $C_{\mathcal{L}}(D, G)$. Seja $D = P_1 + \dots + P_n$, P_i lugar de grau 1 com $n \leq q$; como há $q+1$ lugares de grau um em $F/\mathbb{F}_q$, existe $P \notin \text{supp} D$, $\deg P = 1$. Considere $Q = P_1$, e portanto $Q \neq P$. Observe que:

$$\deg(Q - P) = 0 \geq 2g - 1 \Rightarrow \dim(Q - P) = 1$$

Por I.3.11, $Q - P$ é principal, i.e., $\exists z \in \dot{F}$ com $(z) = Q - P$. Logo, $(z)_0 = Q$ e $(z)_{\infty} = P$, mas $[F : \mathbb{F}_q(z)] = \deg(z)_{\infty} = 1$, então, $F = \mathbb{F}_q(z)$ e $P = P_{\infty}$. Se supormos $\deg G \geq n-1$, por II.3.2, $k = n$, i.e., $C_{\mathcal{L}}(D, G) = \mathbb{F}_q^n$ e daí o caso é trivial; suponha agora que $\deg G \leq n-2$; assim, $\deg G = k-1$. Considere o divisor de grau zero $N = (k-1)P_{\infty} - G$; como $\dim N \geq 1$, N é principal; seja $u \in \dot{F}$ tal que $(u) = (k-1)P_{\infty} - G$. Observe agora que $\{u, zu, \dots, z^{k-1}u\} \subseteq \mathcal{L}(G)$, pois para $0 \leq i \leq k-1$:

$$(z^i u) = i(z) + (u) = i(Q - P_{\infty}) + (k-1)P_{\infty} - G = iQ + ((k-1) - i)P_{\infty} - G$$

e portanto, $(z^i u) \geq -G$

Como $F = \mathbb{F}_q(z)$, temos que $\{u, zu, \dots, z^n u\}$ é l.i. sobre $\mathbb{F}_q$ e assim é base para $\mathcal{L}(G)$, i.e.,

$$\mathcal{L}(G) = \{uf(z) | f \in \mathbb{F}_q[z], \text{gr}(f(x)) \leq k-1\}$$

Chamando $\alpha_i = z(P_i)$ e $v_i = u(P_i)$, obtemos:

$$(uf(z))(P_i) = u(P_i)f(z(P_i)) = v_i f(\alpha_i), \text{ para } i = 1, \dots, n.$$

Portanto,

$$(*)C = C_{\mathcal{L}}(D, G) = \{(v_1 \cdot f(\alpha_1)), \dots, (v_n \cdot f(\alpha_n)) | \text{grau}(f(x)) \leq k-1\}$$

Como já sabemos, $k = \deg G + 1$ e por (*):

$$\beta = \{(v_1, \dots, v_n), (\alpha_1 v_1, \dots, \alpha_1 v_n), \dots, (\alpha_1^{k-1} v_1, \dots, \alpha_n^{k-1} v_n)\},$$

gera C , então β é uma base de C e assim M é uma matriz geradora.

- (b) A prova é essencialmente a mesma; neste caso, temos $n = q + 1$ e podemos escolher z tal que $F = \mathbb{F}_q(z)$ e considero $P_n = P_\infty$, onde $P_1, \dots, P_n$ são todos os lugares de grau um de F e $D = P_1 + \dots + P_n$. Como anteriormente, seja $(u) = (k-1)P_\infty - G$ com $u \in F$ e $\{u, zu, \dots, z^{k-1}u\}$ é base de $\mathcal{L}(G)$. Para $1 \leq i \leq n-1 = q$, chame $\alpha_i = z(P_i)$ e $v_i = u(P_i)$ e observe que sendo $P_n = P_\infty = (z)_\infty$, temos para todo $j = 1, \dots, k-2$, $uz^j(P_n) = 0$ (pois $v_{P_n}(uz^j) = k-1-j \geq 1$), mas para $j = k-1$, $v_{P_n}(uz^{k-1}) = 0$, i.e., $\gamma = uz^{k-1}(P_{k-1}) \in \mathbb{F}_q$ e trocando u por $\gamma^{-1}u$ podemos concluir novamente que:

$$\beta = \{(v_1, \dots, v_{n-1}, 0), \dots, (\alpha_1^{k-2}, \dots, \alpha_{n-1}^{k-2} v_{n-1}, 0), (\alpha_1^{k-1} v_1, \dots, \alpha_{n-1}^{k-1} v_{n-1}, 1)\},$$

é base de $C = C_{\mathcal{L}}(D, G)$ e M é a matriz geradora.

□

Vários códigos clássicos dentro da teoria dos códigos são construídos como códigos geométricos de Goppa de corpos de funções racionais; para encerrar o capítulo definiremos vários deles; contudo não será demonstrado o fato que acabamos de citar. Gostaríamos apenas de enfatizar que todos estes códigos são obtidos a partir do corpo de funções racionais.

II.3.4 Definição Seja $\alpha = (\alpha_1, \dots, \alpha_n)$ onde os α_i são elementos distintos de $\mathbb{F}_q$, e seja $v = (v_1, \dots, v_n)$ onde os v_i são elementos não nulos de $\mathbb{F}_q$ (não necessariamente distintos). Então o *Código Reed-Solomon Generalizado*, denotado por $GRS_K(\alpha, v)$ consiste dos vetores

$$(v_1 \cdot f(\alpha_1), \dots, v_n \cdot f(\alpha_n)),$$

com $f(z) \in \mathbb{F}_q[z]$, $\deg f \leq k-1$ (para $k \leq n$ fixo).

Uma definição equivalente de $GRS_K(\alpha, v)$ é o código sobre $\mathbb{F}_q$ com matriz geradora (II.4). No caso em que $\alpha = (\beta, \beta^2, \dots, \beta^n)$ (onde $n = q-1$ e β é raiz primitiva da unidade) e $v = (1, 1, \dots, 1)$, $GRS_K(\alpha, v)$ é um código de Reed-Solomon.

II.3.5 Definição Considere uma extensão de corpo $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$ e um código C sobre $\mathbb{F}_{q^m}$ de comprimento n . Então

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$$

é chamado *subcorpo subcódigo* de C (ou *restrição* de C a $\mathbb{F}_q$).

$C_{\mathbb{F}_q}$ é um código sobre $\mathbb{F}_q$. Sua distância mínima não é menor do que a de C , e para a dimensão de $C|_{\mathbb{F}_q}$ temos a estimativa $\dim C|_{\mathbb{F}_q} \leq \dim C$ (em geral a desigualdade é estrita).

II.3.6 Definição Seja $n|q^m - 1$ e $\beta \in \mathbb{F}_{q^m}$ uma n -ésima raiz primitiva da unidade. Seja $l \in \mathbb{Z}$ e $\delta \geq 2$. Defina um código $C(n, l, \delta)$ sobre $\mathbb{F}_{q^m}$ pela matriz geradora

$$H = \begin{pmatrix} 1 & \beta^l & \beta^{2l} & \dots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \dots & \beta^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \dots & \beta^{(n-1)(l+\delta-2)} \end{pmatrix} \quad (\text{II.6})$$

O código $C = C(n, l, \delta)^\perp|_{\mathbb{F}_q}$ é chamado *BCH código* com distância projetada δ . Em outras palavras,

$$C = \{c \in \mathbb{F}_q^n | H.c^t = 0\}, \quad (\text{II.7})$$

onde H é dado por (II.6).

II.3.7 Definição Seja $L = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$ com $|L| = n$ e seja $g(z) \in \mathbb{F}_{q^m}[z]$ um polinômio de grau t tal que $1 \leq t \leq n-1$ e $g(\alpha_i) \neq 0$ para todo $\alpha_i \in L$.

(a) Definimos um código $C(L, g(z)) \subseteq (\mathbb{F}_{q^m})^n$ pela matriz geradora

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & g(\alpha_2)^{-1} & \dots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \alpha_2 g(\alpha_2)^{-1} & \dots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{i-1} g(\alpha_1)^{-1} & \alpha_2^{i-1} g(\alpha_2)^{-1} & \dots & \alpha_n^{i-1} g(\alpha_n)^{-1} \end{pmatrix} \quad (\text{II.8})$$

(b) O código $\Gamma(L, g(z)) = C(L, g(z))^\perp$ é chamado o *código Clássico de Goppa com polinômio de Goppa $g(z)$* . Ou seja

$$\Gamma(L, g(z)) = \{c \in \mathbb{F}_{q^m}^n | H.c^t = 0\},$$

onde H é dada por (II.8).

Observe que (II.8) é um caso particular de (II.4) onde $v_i = g(\alpha_i)^{-1}$; logo, $C(L, g(z))$ e $\Gamma(L, g(z))$ são códigos Reed-Solomon Generalizados.

Capítulo III

Extensões Algébricas de Corpos de Funções e Códigos Auto-Duais

Vimos nos capítulos anteriores que a descrição dos lugares e valorizações de um corpo de funções racionais é relativamente simples e como consequência podemos descrever os códigos de Goppa destes corpos de maneira explícita. Observando que um corpo de funções algébricas F' é uma extensão algébrica finita de um corpo de funções racionais F , nos parece natural estudar a situação F'/F , a partir do que se sabe em F . Isto é, pretendemos descrever lugares, valorizações, divisores, etc. de F . Tal estudo será realizado nas Seções 3.1 e 3.2. Na Seção 3.3, a partir deste estudo, apresentaremos exemplos de códigos de Goppa auto-duais.

III.1 Extensões Algébricas de Corpos de Funções

Nesta seção vamos estudar extensões algébricas de corpos de funções F'/F dando mais atenção ao comportamento dos lugares e das valorizações.

Fixamos a notação a seguir:

- F/K - corpo de funções algébricas em uma variável com corpo completo de constantes K ;
- K será perfeito; i.e., toda extensão algébrica de K é separável (e.g., K com característica zero, finito ou algebricamente fechado).
- F'/K' - corpo de funções (K' corpo completo das constantes de F') tal que $F' \supseteq F$ é uma extensão algébrica e $K' \supseteq K$.

Por conveniência fixe $\Phi \supseteq F$ algebricamente fechado e considere somente extensões F'/F com $F' \subseteq \Phi$.

III.1.1 Definição

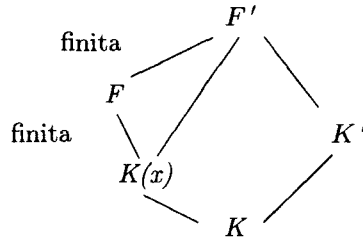
- (a) Um corpo de funções algébricas F'/K' é chamado uma *extensão algébrica* de F/K se $F' \supseteq F$ é uma extensão algébrica e $K' \supseteq K$.
- (b) A extensão algébrica F'/K' de F/K é chamada de *extensão por constantes* se $F' = FK'$, o corpo gerado por F e K' .
- (c) A extensão algébrica F'/K' de F/K é chamada de *extensão finita* se $[F' : F] = n < \infty$.

III.1.2 Lema *Seja F'/K' uma extensão algébrica de F/K . Então, vale o seguinte:*

- (a) K'/K é algébrica e $F \cap K' = K$;
(b) F'/K' é extensão finita de F/K se $[K' : K] < \infty$;
(c) Seja $F_1 = F.K'$. Então F_1/K' é uma extensão por constantes de F/K , e F'/K' é uma extensão finita de F_1/K' (possuindo o mesmo corpo de constantes).

Demonstração :

- (a) Considere $x \in F$ tal que $[F : K(x)] = n < \infty$, i.e., $x \in F$ é transcendente sobre K e considere o diagrama:



Pelo diagrama temos claramente que $F'/K(x)$ é algébrica, e como x é transcendente sobre K , temos que F'/K tem grau de transcendência 1. Mas F'/K' é corpo de funções e $F'/K'(x)$ é algébrica, portanto x é transcendente sobre K' e como $K'(x)/K(x)$ também é algébrica com $K'(x) \subseteq F'$ temos que K'/K é algébrica, pois como já dissemos, F'/K tem grau de transcendência 1.

Por outro lado, $K' \cap F = K$ vem do fato de que estamos supondo K algebricamente fechado em F .

- (b) Considerando o mesmo x da parte (a) e olhando o diagrama temos:

($\Rightarrow$) Se $[F' : F] < \infty$, então $[F' : K(x)] < \infty$ e assim F'/K é corpo de funções. Mas então pelo Corolário I.1.16, considerando $\tilde{K}$ o corpo das constantes de F'/K , temos: $[\tilde{K} : K] < \infty$ e por (a) $K' \subseteq \tilde{K}$, i.e., $[K' : K] < \infty$.

($\Leftarrow$) Suponha $[K' : K] < \infty$; então, pelo diagrama temos $[K'(x) : K(x)] < \infty$. Mas como já havíamos visto que x é transcendente sobre K' e F'/K' é corpo de funções, temos $[F' : K'(x)] < \infty$. Portanto, temos $[F' : K(x)] = [F' : F][F : K(x)] < \infty$ e assim, $[F' : F] < \infty$.

- (c) Observe que ao considerarmos $F_1 = F.K'$ teríamos $F \subseteq F_1 \subseteq F'$, com $K' \subseteq F_1$, e portanto F_1/K' é extensão algébrica de F/K com corpo de constantes K' . Mas então F'/K' é extensão algébrica de F_1/K e $[K' : K] = 1$; assim, por (b) $[F' : F_1] < \infty$.

□

Agora vamos iniciar o estudo da relação entre os lugares de F' e F .

III.1.3 Definição Considere uma extensão algébrica F'/K' de F/K . Um lugar $P' \in \mathbb{P}'_F$ se diz estar sobre $P \in \mathbb{P}_F$ se $P' \supseteq P$. Também dizemos que P' é uma *extensão* de P ou que P está *sob* P' e escrevemos P'/P .

III.1.4 Proposição Seja F'/K' uma extensão algébrica de F/K . Suponha que P (respec. P') é um lugar de F/K (respec. F'/K'), e seja $O_P \subseteq F$ (respec. $O_{P'} \subseteq F'$) o anel de valorização correspondente e v_P (respec. $v_{P'}$) a sua valorização discreta. Então, as afirmações a seguir são equivalentes:

1. P'/P
2. $O_P \subseteq O_{P'}$
3. Existe um inteiro $e \geq 1$ tal que $v_{P'}(x) = ev_P(x)$, $\forall x \in F$.

Mais ainda, se P'/P , então

$$P = P' \cap F \quad \text{e} \quad O_P = O_{P'} \cap F.$$

Por isso, P é chamado a restrição de P' a F .

Demonstração :

- 1 $\Rightarrow$ 2** Suponha que P'/P e $O_P \not\subseteq O_{P'}$. Logo, $\exists u \in F$ tal que $u \in O_P$ e $u \notin O_{P'}$, i. e., $v_P(u) \geq 0$ e $v_{P'}(u) < 0$. Como $P \subseteq P'$, então $v_P(u) = 0$. Escolha $t \in F$ com $v_P(t) = 1$, então $t \in P'$ e $r = v_{P'}(t) > 0$. Conseqüentemente,

$$v_P(u^r t) = rv_P(u) + v_P(t) = 1, v_{P'}(u^r t) = rv_{P'}(u) + v_{P'}(t) < -r + r = 0$$

então, $u^r t \in P$, mas $u^r t \notin P'$. Contradição! Logo, $O_P \subseteq O_{P'}$.

Antes de provar **2 $\Rightarrow$ 3**, provemos que se **2** vale, então $O_P = O_{P'} \cap F$ e $P = P' \cap F$. Observe que de **2** temos $O_P \subseteq O_{P'} \cap F$ e lembre que um anel de valorização é um subanel maximal próprio; então, como $O_{P'} \cap F$ é anel de F , há duas possibilidades: $O_P = O_{P'} \cap F$ ou $F = O_{P'} \cap F$. Se $F = O_{P'} \cap F$, então, $F \subseteq O_{P'}$; considere $z \in F' \setminus O_{P'}$. Como F'/F é algébrica, existe sempre uma equação

$$z^n + c_{n-1}z^{n-1} + \dots + c_1z + c_0 = 0. \quad (\text{III.1})$$

Sabemos que $v_{P'}(0) = \infty$, $v_{P'}(z) < 0$ e que $v_{P'}(c_j) \geq 0$, e portanto:
 $v_P(c_j z^j) = v_P(c_j) + jv_P(z) > nv_P(z)$, logo:

$$v_P(0) = v_{P'}(z^n + c_{n-1}z^{n-1} + \dots + c_0) = nv_{P'}(z) < 0.$$

Assim, tal elemento $z \in F$ não pode existir e, portanto, $O_P = O_{P'} \cap F$. Como $P' \cap F$ é ideal próprio de O_P , necessariamente, temos $P' \cap F \subseteq P$; mas se $x \in P$, temos $x^{-1} \in F \setminus O_P$ e assim $x^{-1} \notin O_{P'}$, i.e. $x \in P'$. Portanto, $P' \cap F = P$.

- 2 $\Rightarrow$ 3** Seja u tal que $v_P(u) = 0$; então, $u, u^{-1} \in O_P \subseteq O_{P'}$ e assim, $v_{P'}(u) = 0$. Seja $t \in O_P$ tal que $v_P(t) = 1$ e fixe $e = v_{P'}(t) \geq 1$. Pelo que mostramos acima, considere um $x \in F$ e seja $r = v_P(x) \in \mathbb{Z}$, então:

$$v_P(xt^{-r}) = v_P(x) - rv_P(t) = r - r \cdot 1 = 0.$$

Logo, $v_{P'}(xt^{-r}) = 0$, então

$$v_{P'}(x) = -v_{P'}(t^{-r}) = -(-r)v_{P'}(t) = ev_P(x).$$

- 3 $\Rightarrow$ 1** De $v_{P'}(x) = ev_P(x)$, $\forall x \in F$, temos:

$$x \in P \Rightarrow v_P(x) \geq 1 \Rightarrow v_{P'}(x) = ev_P(x) \geq 1 \Rightarrow x \in P' \Rightarrow P'/P$$

□

Uma consequência desta proposição é que para P'/P existe uma imersão canônica do corpo das classes de resíduo $F_P = O_P/P$ no corpo das classes de resíduo $F'_{P'} = O_{P'}/P'$, dada por

$$x(P) \mapsto x(P'), \text{ para } x \in O_P$$

Assim, podemos considerar F_P um subcorpo de $F'_{P'}$.

III.1.5 Definição Seja F'/K' uma extensão algébrica de F/K , e seja $P' \in \mathbb{P}_{F'}$ um lugar de F'/K' sobre $P \in \mathbb{P}_F$:

- (a) O inteiro $e(P'/P) = e$ com $v_{P'}(x) = ev_P(x), \forall x \in F$ é chamado *índice de ramificação* de P' sobre P . Dizemos que P'/P é *ramificado* se $e(P'/P) > 1$ e P'/P é *não-ramificado* se $e(P'/P) = 1$.
- (b) $f(P'/P) = [F'_{P'} : F_P]$ é chamado o *grau relativo* de P' sobre P .

Note que $f(P'/P)$ pode ser finito ou infinito, enquanto o índice de ramificação é sempre finito.

III.1.6 Proposição Seja F'/K' uma extensão de F/K e P' um lugar de F'/K' sobre P lugar de F/K . Então

- (a) $f(P'/P) < \infty \Leftrightarrow [F' : F] < \infty$.
- (b) Se F''/K'' é uma extensão algébrica de F'/K' e $P'' \in \mathbb{P}_{F''}$ é uma extensão de P' , então
$$e(P''/P) = e(P''/P').e(P'/P) \quad \text{e} \quad f(P''/P) = f(P''/P').f(P'/P)$$

Demonstração :

- (a) Lembre que $\deg P = [F_P : K] < \infty$ e $\deg P' = [F'_{P'} : K'] < \infty$. Como

$$[F'_{P'} : K] = [F'_{P'} : K'] \cdot [K' : K] = [F'_{P'} : F_P] \cdot [F_P : K]$$

então: $[F'_{P'} : K] < \infty \Leftrightarrow [F'_{P'} : F_P] < \infty \Leftrightarrow [K' : K] < \infty$, por III.1.2(b); i.e.,

$$[K' : K] < \infty \Leftrightarrow [F' : F] < \infty$$

logo, como $f(P'/P) = [F'_{P'} : F_P]$, temos

$$f(P'/P) < \infty \Leftrightarrow [F' : F] < \infty$$

- (b) $x \in F \Rightarrow v_{P'}(x) = e(P'/P) \cdot v_P(x)$

$$\begin{aligned} x \in F \subseteq F' &\Rightarrow v_{P''}(x) = e(P''/P') \cdot v_{P'}(x) \\ &= e(P''/P') \cdot e(P'/P) v_P(x) \end{aligned}$$

Considere $F_P \subseteq F'_{P'} \subseteq F''_{P''}$. Logo, $[F''_{P''} : F_P] = [F''_{P''} : F'_{P'}] \cdot [F'_{P'} : F_P]$.

□

III.1.7 Proposição Seja F'/K' uma extensão algébrica de F/K .

- (a) Para qualquer lugar $P' \in \mathbb{P}_{F'}$ existe exatamente um lugar $P \in \mathbb{P}_F$ tal que P'/P e $P = P' \cap F$.

- (b) Reciprocamente, para um lugar $P \in \mathbb{P}_F$ existe pelo menos um lugar, $P' \in \mathbb{P}_F$ tal que P'/P , e o número de tais lugares é finito.

Demonstração :

- (a) Primeiro provemos que existe algum $z \in \dot{F}$ tal que $v_{P'}(z) \neq 0$. Isso será feito por contradição: Suponha que para todo $z \in \dot{F}$, $v_{P'}(z) = 0$; considere $t \in F'$ e suponha que $v_{P'}(t) > 0$; t é algébrico sobre F ; logo, existem $c_i \in F$, $i = 0, \dots, n$, com $c_0, c_n \in \dot{F}$ tais que

$$c_n t^n + \dots + c_1 t + c_0 = 0.$$

Por hipótese, $v_{P'}(c_i) = 0$; assim,

$$v_{P'}(c_0) = \min\{iv_{P'}(t)/i = 1, \dots, n\} > 0.$$

Contradição! Logo, $P' \cap F \neq \emptyset$.

Por III.1.4 se P'/P , então $P = P' \cap F$. Logo, se $P, Q \in \mathbb{P}_F$ com P'/Q e P'/P , então $Q = P' \cap F = P$.

- (b) Dado $P \in \mathbb{P}_F$, escolha $x \in F/K$ tal que $(x)_0 = P$ (ver Proposição I.5.5). Afirmamos que para $P' \in \mathbb{P}_{F'}$ vale:

$$P'/P \Leftrightarrow v_{P'}(x) > 0 \quad (\text{III.2})$$

$$(\Rightarrow) v_{P'}(x) = ev_P(x) = e > 0$$

$$(\Leftarrow) v_{P'}(x) > 0$$

Seja Q um lugar sob P' , logo $Q = P' \cap F$; então $Q = P$, pois P é o único zero de x em F/K . Por (III.2), P'/P . Agora como o conjunto dos zeros de x em F' é finito, (III.2) garante que temos apenas um número finito P' tais que P'/P .

□

A proposição anterior nos leva à definição de um K -homomorfismo entre os grupos de divisores $\mathcal{D}_F$ e $\mathcal{D}_{F'}$.

III.1.8 Definição Seja F' uma extensão algébrica de F/K . Para um lugar $P \in \mathbb{P}_F$ definimos a sua conorma (com relação a F'/F) por

$$\text{Con}_{F'/F}(P) = \sum_{P'/P} e(P'/P) \cdot P',$$

onde a soma é indexada pelos lugares em F' sobre P . A aplicação conorma se estende a um homomorfismo de $\mathcal{D}_F$ em $\mathcal{D}_{F'}$ da forma seguinte:

$$\text{Con}_{F'/F}\left(\sum_{P \in \mathbb{P}_F} n_P \cdot P\right) = \sum_{P \in \mathbb{P}_F} n_P \cdot \text{Con}_{F'/F}(P)$$

A conorma é uma aplicação bem comportada em relação a torres de corpos de funções $F'' \supseteq F' \supseteq F$; uma consequência imediata de III.1.6(b) é a fórmula

$$\text{Con}_{F''/F}(A) = \text{Con}_{F''/F}(\text{Con}_{F'/F}(A))$$

para qualquer divisor $A \in \mathcal{D}_F$.

Uma outra propriedade fundamental da conorma é que ela leva divisor principal de F em divisor principal de F' . Mais precisamente temos:

III.1.9 Proposição *Seja F'/K' extensão algébrica de F/K corpo de funções. Para $x \in F$ sejam $(x)_0^F, (x)_\infty^F, (x)^F$, respectivamente $(x)_0^{F'}, (x)_\infty^{F'}, (x)^{F'}$ o divisor de zeros, o divisor de polos e o divisor principal de x em $\mathcal{D}_F$, respectivamente em $\mathcal{D}_{F'}$. Então:*

$$\text{Con}_{F''/F}((x)_0^F) = (x)_0^{F'}, \text{Con}_{F''/F}((x)_\infty^F) = (x)_\infty^{F'}, \text{ e } \text{Con}_{F''/F}((x)^F) = (x)^{F'}$$

Demonstração : Por definição, para $x \in F$:

$$\begin{aligned} (x)^{F'} &= \sum_{P' \in \mathbf{P}_{F'}} v_{P'}(x) P' \\ &= \sum_{P \in \mathbf{P}_F} v_P(x) \left(\sum_{P'/P} e(P'/P) P' \right) \\ &= \sum_{P \in \mathbf{P}_F} v_P(x) \text{Con}_{F'/F}(P) \\ &= \text{Con}_{F'/F} \left(\sum_{P \in \mathbf{P}_F} v_P(x) P \right) \\ &= \text{Con}_{F'/F}((x)^F) \end{aligned}$$

Considerando somente a parte positiva (negativa) do divisor principal, obtém-se a demonstração para o divisor de zeros (polos). $\square$

Por esta proposição, a conorma induz um homomorfismo nas classes dos divisores, novamente denotado conorma.

$$\text{Con}_{F'/F} : \mathcal{C}_F \longrightarrow \mathcal{C}_{F'}$$

Geralmente, esta aplicação não é injetiva nem sobrejetiva, enquanto $\text{Con}_{F'/F} : \mathcal{D}_F \longrightarrow \mathcal{D}_{F'}$ é claramente injetiva.

III.1.10 Lema *Seja K'/K extensão finita e x transcendente sobre K . Então*

$$[K'(x) : K(x)] = [K' : K]$$

Demonstração : Podemos assumir que $K' = K(\alpha)$ para algum $\alpha \in K'$. Como $K'(x) = K(x)(\alpha)$, então,

$$[K'(x) : K(x)] \leq [K' : K].$$

Para provar que $[K' : K] \leq [K'(x) : K(x)]$ é preciso mostrar que o polinômio minimal de α em K continua sendo irredutível em $K(x)$. Seja $\phi(T) \in K[T]$ o polinômio minimal de α e suponhamos que é redutível em $K(x)$, isto é, $\exists g(T), h(T) \in K(x)[T]$ polinômios mônicos com grau menor que $\deg \phi$ tais que $\phi(T) = g(T)h(T)$. Como $\phi(\alpha) = 0$, então $g(\alpha) = 0$ ou $h(\alpha) = 0$; suponha que $g(\alpha) = 0$ e $\deg(g) = r$, então:

$$g(T) = T^r + c_{r-1}(x)T^{r-1} + \dots + c_1(x)T + c_0(x)$$

com $c_i(x) \in K(x)$ e $r < \deg \phi$; então

$$\alpha^r + c_{r-1}(x)\alpha^{r-1} + \dots + c_1(x)\alpha + c_0(x) = 0$$

Multiplicando por um denominador comum, obtemos:

$$g_r(x)\alpha^r + g_{r-1}(x)\alpha^{r-1} + \dots + g_1(x)\alpha + g_0(x) = 0 \quad (\text{III.3})$$

onde $g_i(x) \in K[x]$, e podemos assumir que $x \nmid g_i(x)$ para algum $i \in \{1, \dots, r\}$. Considerando $x = 0$ em (III.3) obtemos um polinômio em K , que se anula em α e tem grau menor que $\deg \phi$. $\square$

No caso em que F'/F é finita, podemos encontrar uma relação entre o grau de um divisor A de F e o grau de $\text{Con}_{F'/F}(A)$. Para isto, iniciamos com:

III.1.11 Teorema *Seja F'/K' extensão finita de F/K , P um lugar de F/K e $P_1, \dots, P_n$ os lugares de F'/K que estão sobre P . Sejam $e_i = e(P_i/P)$ e $f_i = f(P_i/P)$. Então*

$$\sum_{i=1}^n e_i \cdot f_i = [F' : F].$$

Demonstração : Pelo Teorema de Aproximação Forte, dados $S \subsetneq \mathbb{P}_F$, $P_1, \dots, P_r \in S$, $x_1, \dots, x_r \in F$ e $n_1, \dots, n_r \in \mathbb{Z}$, $\exists z \in F$ tal que $v_{P_i}(z - x_i) = n_i$, $i = 1, \dots, r$, $v_P(z) \geq 0$, $\forall P \in S \setminus \{P_1, \dots, P_r\}$. Considere $S = \mathbb{P}_F \setminus \{P\}$, $r = 1$, $n_1 = 1$, $x_1 = 0$ e $P_1 \in S$. Então, $\exists z \in F$ tal que $v_{P_1}(z) = 1$, $v_Q(z) \geq 0$, $\forall Q \in S \setminus \{P_1\}$. Assim, $v_P(z) < 0$, i.e., P é o único polo de z .

Logo, considerando $x = z^{-1}$, P é o único zero de x em F . Seja $v_P(x) = s$. Como $v_Q(x) = e(Q/P)v_P(x)$, para todo Q/P , então os P_i/P , $i = 1, \dots, n$ são exatamente os zeros de x em F'/K' . Agora vamos avaliar $[F' : K(x)]$.

$$\begin{aligned} [F' : K(x)] &= [F' : K'(x)] \cdot [K'(x) : K(x)] \\ &= \left(\sum_{i=1}^n v_{P_i}(x) \deg P_i \right) [K' : K] \\ &= \left(\sum_{i=1}^n e_i v_P(x) [F'_{P_i} : K'] \right) [K' : K] \\ &= v_P(x) \left(\sum_{i=1}^n e_i [F'_{P_i} : K'] \right) [K' : K] \\ &= s \left(\sum_{i=1}^n e_i [F'_{P_i} : K] \right) \\ &= s \left(\sum_{i=1}^n e_i [F'_{P_i} : F_P] [F_P : K] \right) \\ &= s \left(\sum_{i=1}^n e_i \cdot f_i \right) \deg P \\ &= v_P(x) \cdot \deg P \left(\sum_{i=1}^n e_i \cdot f_i \right) = [F' : K(x)]. \end{aligned} \tag{III.4}$$

Temos também que $[F' : K(x)] = [F' : F] \cdot [F : K(x)]$. Mas, sendo P o único zero de x em F , temos que

$$[F : K(x)] = v_P(x) \cdot \deg P \tag{III.5}$$

De (III.4) e (III.5) obtemos que $[F' : F] = \sum_{i=1}^n e_i \cdot f_i$. □

III.1.12 Corolário *Seja F'/K' extensão finita de F/K e $P \in \mathbb{P}_F$. Então:*

- (a) $|\{P' \in \mathbb{P}_{F'}; P'/P\}| \leq [F' : F]$.
- (b) Se $P' \in \mathbb{P}_{F'}$ está sobre P , então $e(P'/P) \leq [F' : F]$ e $f(P'/P) \leq [F' : F]$.

Demonstração :

- (a) Seja $m = |\{P' \in \mathbb{P}_{F'}; P'/P\}|$ como $e_i, f_i \geq 1$, então $m \leq \sum_{i=1}^m e_i \cdot f_i = [F' : F]$.

(b) $e_i, f_i \geq 1, \sum e_i \cdot f_i = [F' : F] \Rightarrow e_i, f_i \leq [F' : F]$.

□

III.1.13 Corolário *Seja F'/K' extensão finita de F/K . Então para qualquer divisor $A \in \mathcal{D}_F$,*

$$\deg(\text{Con}_{F'/F}(A)) = \frac{[F' : F]}{[K' : K]} \cdot \deg A$$

Demonstração : Sabendo que $\text{Con}_{F'/F}$ e $\deg$ são homomorfismos de grupos, basta considerar o caso em que $A = P, P \in \mathbb{P}_F$. Assim,

$$\begin{aligned} \deg(\text{Con}_{F'/F}(P)) &= \deg\left(\sum_{P'/P} e(P'/P) \cdot P'\right) \\ &= \sum_{P'/P} e(P'/P) \cdot \deg P' \\ &= \sum_{P'/P} e(P'/P) \cdot [F'_{P'} : K'] \\ &= \sum_{P'/P} e(P'/P) \cdot \frac{[F'_{P'} : K]}{[K' : K]} \\ &= \frac{1}{[K' : K]} \sum_{P'/P} e(P'/P) [F'_{P'} : F_P] [F_P : K] \\ &= \frac{1}{[K' : K]} \left(\sum_{P'/P} e(P'/P) f(P'/P) \right) \deg P \\ &= \frac{[F' : F]}{[K' : K]} \deg P \end{aligned}$$

□

O próximo resultado nos fornece um critério de irreduzibilidade de polinômios para corpos de funções muito útil. Aliás, no caso especial em que $F = K(x)$ é corpo de funções racionais, tal critério é conhecido como Critério de Eisenstein.

III.1.14 Proposição *Considere o corpo de funções F/K e o polinômio*

$$\phi(T) = a_n T^n + a_{n-1} T^{n-1} + \dots + a_1 T + a_0$$

com coeficientes $a_i \in F$. Assuma que existe um lugar $P \in \mathbb{P}_F$ tal que uma das condições a seguir vale:

1. $v_P(a_n) = 0, v_P(a_i) \geq v_P(a_0) > 0$, para $i = 1, \dots, n-1$ e $\text{mdc}(n, v_P(a_0)) = 1$.
2. $v_P(a_n) = 0, v_P(a_i) \geq 0$, para $i = 1, \dots, n-1, v_P(a_0) < 0$ e $\text{mdc}(n, v_P(a_0)) = 1$.

Então $\phi(T)$ é irreduzível em $F[T]$. Se $F' = F(y)$ onde y é uma raiz de $\phi(T)$, então P possui uma única extensão $P' \in \mathbb{P}_{F'}$, e tem-se $e(P'/P) = n$ e $f(P'/P) = 1$.

Demonstração : Considere a extensão de corpo $F' = F(y)$ com $\phi(y) = 0$, então $[F' : F] \leq \deg \phi(T) = n$, valendo a igualdade somente se $\phi(T)$ for irreduzível em $F(T)$. Seja $P' \in \mathbb{P}_{F'}$ extensão de P . Como $\phi(y) = 0$, temos:

$$-a_n y^n = a_0 + a_1 y + \dots + a_{n-1} y^{n-1} \quad (\text{III.6})$$

- se vale 1., temos:

$$\begin{aligned}
v_{P'}(-a_n y^n) &= v_{P'}(a_n) + n v_{P'}(y) \\
&= e(P'/P) v_P(a_n) + n v_{P'}(y) \\
&\geq \min\{v_{P'}(a_0), \{v_{P'}(a_i) + i v_{P'}(y)/i = 1, \dots, n-1\}\} \\
&\geq \min\{e(P'/P) v_P(a_0), \{e(P'/P) v_P(a_i) + i v_{P'}(y)/i = 1, \dots, n-1\}\}
\end{aligned}$$

Mas então, $v_{P'}(y) > 0$; caso contrário, teríamos uma contradição e assim, $n.v_{P'}(y) = e.v_P(a_0)$, $e = e(P'/P)$. Como $\text{mdc}(n, v_P(a_0)) = 1$, então $n|e$; logo, $n \leq e$. Mas, como $n = [F' : F] \geq e$, temos que $n = e$, e portanto, $f = 1$ e $\phi(T)$ é irredutível.

- se vale 2., temos:

$$v_{P'}(-a_0) \geq \min\{v_{P'}(a_n y^n), \{v_{P'}(a_i) + i.v_{P'}(y)/i = 1, \dots, n-1\}\}$$

Mas, como $v_P(a_0) < 0$, temos que $v_{P'}(y) < 0$, pois para $i = 1, \dots, n-1$, $v_P(a_i) \geq 0$, e daí $e.v_P(a_0) = n.v_P(y)$ e de novo temos $n|e$, e como em 1. tem-se $n = e$, $f = 1$ e $\phi(T)$ irredutível.

□

III.2 Sobre Extensões Integrais de Subanéis de um Corpo de Funções

III.2.1 Definição Um *subanel* de F/K é um anel R tal que $K \subseteq R \subseteq F$, e R não é um corpo.

III.2.2 Definição Para $\emptyset \neq S \subsetneq \mathbb{P}_F$, seja

$$O_S = \{z \in F | v_P(z) \geq 0, \forall P \in S\}$$

a interseção de todos os anéis de valorização O_P com $P \in S$. Qualquer anel $R \subseteq F$ que é dessa forma é chamado *anel de holomorfia* de F/K .

III.2.3 Definição Seja R um subanel de F/K

(a) Um elemento $z \in F$ é *integral* sobre R se $f(z) = 0$ para algum polinômio mônico $f(X) \in R[X]$. Essa equação é chamada *equação integral* de z em R .

(b) O conjunto

$$ic_F(R) = \{z \in F | z \text{ é integral sobre } R\}$$

é chamado *fecho integral* de R em F .

(c) Seja $F_0 \subseteq F$ o corpo de frações de R . O anel R é dito *integralmente fechado* se $ic_{F_0}(R) = R$.

III.2.4 Teorema Seja R um subanel de F/K e $S(R) = \{P \in \mathbb{P}_F | R \subseteq O_P\}$. Então:

(a) $\emptyset \neq S(R) \subsetneq \mathbb{P}_F$.

(b) O fecho integral de R em F é $ic_F(R) = O_{S(R)}$. Em particular, $ic_F(R)$ é um subanel integralmente fechado de F/K com corpo de frações F .

Demonstração :

(a) Como R não é corpo, existe $I \subsetneq R$ ideal próprio não nulo e por I.1.19 existe $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq O_P$. Logo, $S(R) \neq \emptyset$. Por outro lado, considere $x \in R$ transcendente sobre K . Todo lugar $Q \in \mathbb{P}_F$ que é polo de x não está em $S(R)$, logo $S(R) \neq \mathbb{P}_F$.

(b) $\vdash F$ é o corpo de frações de $O_{S(R)}$.

Considere $x \in F$. Como $\emptyset \neq S(R) \subsetneq \mathbb{P}_F$, pelo Teorema de Aproximação Forte, existe $z \in F$ tal que

$$v_P(z) \geq \max\{0, v_P(x^{-1})\}, \text{ para todo } P \in S(R)$$

já que o número de zeros de x^{-1} em $S(R)$ é finito. Claramente, $z \in O_{S(R)}$, e se tomarmos $y = zx$ temos que $v_P(y) = v_P(z) - v_P(x^{-1}) \geq 0$, para todo $P \in S(R)$ e, portanto $y \in O_{S(R)}$; mas, $x = y \cdot z^{-1}$ e assim, está no corpo de frações de $O_{S(R)}$. Como $O_{S(R)}$ é interseção de anéis de valorização, ele é integralmente fechado (veja III.11).

$$\vdash ic_F(R) = O_{S(R)}$$

($\subseteq$) Como $R \subseteq O_{S(R)}$ e $O_{S(R)}$ é integralmente fechado, então $ic_F(R) \subseteq O_{S(R)}$.

($\supseteq$) Seja $z \in O_{S(R)}$ e suponhamos que não é integral sobre R . Considere o anel $R[z^{-1}]$ e o ideal $I = z^{-1}R[z^{-1}]$. Suponhamos que I é ideal próprio; logo, existe $Q \in \mathbb{P}_F$ tal que $I \subseteq Q$ e $R[z^{-1}] \subseteq O_Q$ e portanto $z^{-1} \in Q$; assim, $z \notin O_Q$, mas $R \subseteq O_Q$ noz diz que $Q \in S(R)$ e portanto que $z \in O_Q$! Logo, I não é ideal próprio. Sendo assim, existem $a_0, \dots, a_s \in R$ tais que

$$1 = z^{-1} \sum_{i=0}^s a_i z^{-i},$$

multiplicando por z^{s+1} , obtemos:

$$z^{s+1} - z^s \sum_{i=0}^s a_i z^{s-i+1} = 0$$

que é uma equação integral para z sobre R ; contradição! Logo, $O_{S(R)} \subseteq ic_F(R)$.

□

Uma consequência imediata desta proposição é:

III.2.5 Corolário Dado um subanel R de F/K tal que F é o corpo de frações de R , então R é integralmente fechado se e só se R é um anel de holomorfia.

A seguir apresentamos uma propriedade fundamental para certos anéis de holomorfia.

III.2.6 Proposição Se $S \subseteq \mathbb{P}_F$ é um conjunto finito e não-vazio de lugares de F/K , então O_S é domínio de ideais principais (DIP).

Demonstração : Considere $S = \{P_1, \dots, P_s\}$ e $\emptyset \neq I \subsetneq O_S$. Para cada $i \in \{1, \dots, s\}$, considere $m_i = \min\{v_{P_i}(u), u \in I\} \in \mathbb{N}$ (m_i existe pois $O_S \subseteq O_{P_i}$ e $I \neq \emptyset$). Agora para cada i escolha $x_i \in I$ com $v_{P_i}(x_i) = m_i$. Pelo Teorema de Aproximação, para cada i , podemos encontrar $z_i \in F$ tal que:

$$v_{P_i}(z_i) = 0 \quad \text{e} \quad v_{P_j}(z_i) > m_i \quad \text{se } i \neq j$$

Portanto, $z_i \in O_S$ e considere $x = \sum_{i=1}^s x_i z_i \in I$. Pela desigualdade triangular estrita, temos $v_{P_i}(x) = m_i$, $i = 1, \dots, s$. Portanto, se mostrarmos que $I \subseteq xO_S$, teremos $I = xO_S$, pois $x \in I$. Considere $z \in I$ e $y = x^{-1}z$, então:

$$v_{P_i}(y) = v_{P_i}(z) - v_{P_i}(x) = v_{P_i}(z) - m_i \geq 0 \quad i = 1, \dots, s.$$

Conseqüentemente, $y \in O_S$ e $z = xy \in xO_S$.

□

Dados F/K corpo de funções e F'/F uma extensão finita e separável, considerando a função traço $Tr_{F'/F} : F' \rightarrow F$, temos por resultado clássico, enunciado no Apêndice III.19, que:

III.2.7 Teorema *Seja R anel integralmente fechado de F/K com corpo de frações F e F'/F extensão finita separável de grau n . Seja $R' = ic_{F'}(R)$. Então:*

- (a) *Para qualquer base $\{x_1, \dots, x_n\}$ de F'/F , existem $a_i \in R$ tais que $a_1x_1, \dots, a_nx_n \in R'$. Conseqüentemente existe uma base de F'/F contida em R' .*
- (b) *Se $\{z_1, \dots, z_n\} \subseteq R'$ é base de F'/F e $\{z_1^*, \dots, z_n^*\}$ é a base dual com relação ao traço*

$$\sum_{i=1}^n Rz_i \subseteq R' \subseteq \sum_{i=1}^n Rz_i^*$$

- (c) *Se além disso R é DIP, então existe $\{u_1, \dots, u_n\}$ base de F'/F tal que*

$$R' = \sum_{i=1}^n Ru_i$$

III.2.8 Observação Lembre que a base $\{z_1^*, \dots, z_n^*\}$ de F'/F é chamada de base dual de $\{z_1, \dots, z_n\}$ em relação ao traço de F'/F .

III.2.9 Corolário *Seja F'/F extensão finita separável de F/K corpo de funções e $P \in \mathbb{P}_F$ um lugar de F/K . Então o fecho integral O'_P de O_P em F' é*

$$O'_P = \cap_{P'/P} O_{P'}.$$

Existe uma base $\{u_1, \dots, u_n\}$ de F'/F tal que

$$O'_P = \sum_{i=1}^n O_P u_i.$$

Tal base $\{u_1, \dots, u_n\}$ é chamada de base integral de O'_P sobre O_P (ou base integral local de F'/F para O_P).

Um importante suplemento para a existência de bases integrais locais é estabelecido no resultado a seguir:

III.2.10 Teorema *Seja F/K corpo de funções, F'/F extensão finita e separável. Então qualquer base $\{z_1, \dots, z_n\}$ de F'/F é base integral para quase todo lugar $P \in \mathbb{P}_F$.*

Demonstração : Considere $\{z_1^*, \dots, z_n^*\}$ base dual de $\{z_1, \dots, z_n\}$. Os polinômios minimais de $z_1, \dots, z_n, z_1^*, \dots, z_n^*$ sobre F envolvem um número finito de coeficientes. Seja $S \in \mathbb{P}_F$ o conjunto dos polos desses coeficientes. Para $P \notin S$ temos

$$z_1, \dots, z_n, z_1^*, \dots, z_n^* \in O'_P, \quad (\text{III.7})$$

onde $O'_P = ic_{F'}(O_P)$. Logo, pelo teorema III.2.6 e já que $\{(z_1^*)^*, \dots, (z_n^*)^*\} = \{z_1, \dots, z_n\}$, temos:

$$\sum O_P z_i \subseteq O'_P \subseteq \sum O_P z_i^* \stackrel{\text{III.7}}{\subseteq} O'_P \stackrel{(\text{III.2.7})}{\subseteq} \sum O_P z_i$$

Logo, $\{z_1, \dots, z_n\}$ é integral para todo $P \notin S$. □

Agora, dadas uma extensão algébrica F'/K' de F/K e um diferencial de Weil de F/K vamos associar um diferencial de Weil de F'/K' . Para isto vamos precisar da noção de divisor Diferente da extensão F'/F . No que segue, estamos sempre supondo que F'/F é separável e finita e, portanto K'/K é finita e separável (lembre que K é perfeito).

III.2.11 Definição Para $P \in \mathbb{P}_F$, seja $O'_P = ic_F(O_P)$ o fecho integral de O_P em F' . Então o conjunto

$$\mathcal{C}_P = \{z \in F' / Tr_{F'/F}(z.O'_P) \subset O_P\}$$

é chamado o *módulo complementar* sobre O_P , onde $Tr_{F'/F}$ denota a aplicação traço de F' em F .

III.2.12 Proposição Com a notação da definição anterior vale o seguinte:

- (a) $\mathcal{C}_P$ é um O'_P -módulo, e $O'_P \subseteq \mathcal{C}_P$.
- (b) Se $\{z_1, \dots, z_n\}$ é uma base integral de O'_P sobre O_P , então

$$\mathcal{C}_P = \sum_{i=1}^n O_P z_i^*$$

onde $\{z_1^*, \dots, z_n^*\}$ é a base dual de $\{z_1, \dots, z_n\}$ com relação ao traço.

- (c) Existe um elemento $t \in F'$ (dependendo de P) tal que $\mathcal{C}_P = t.O'_P$. Mais ainda,

$$v_{P'}(t) \leq 0 \text{ para todo } P'/P,$$

e se $t' \in F'$, então

$$\mathcal{C}_P = t'.O'_P \Leftrightarrow v_{P'}(t') = v_{P'}(t) \text{ para todo } P'/P.$$

- (d) $\mathcal{C}_P = O'_P$ para quase todo $P \in \mathbb{P}_F$.

Demonstração :

- (a) $\mathcal{C}_P$ é um O'_P -módulo pela definição. Como o traço de um elemento $y \in O'_P$ está em O_P , por propriedade do traço (ver III.15), temos $O'_P \subset \mathcal{C}_P$.
- (b) Como $\{z_1^*, \dots, z_n^*\}$ é base de F'/F se $z \in \mathcal{C}_P$ existem $x_1, \dots, x_n \in F$ tais que $z = \sum_{i=1}^n x_i z_i^*$. Como $z_1, \dots, z_n \in O'_P$, segue que $Tr_{F'/F}(zz_j) \in O_P$ para $1 \leq j \leq n$. Logo,

$$Tr_{F'/F}(zz_j) = Tr_{F'/F}\left(\sum_{i=1}^n x_i z_i^* z_j\right) = \sum_{i=1}^n x_i Tr_{F'/F}(z_i^* z_j) = x_j \in O_P$$

Portanto, $z \in \sum_{i=1}^n O_P z_i^*$. Reciprocamente, sejam $z \in \sum_{i=1}^n O_P z_i^*$, $u \in O'_P$ e digamos que $z = \sum_{i=1}^n x_i z_i^*$ e $u = \sum_{j=1}^n y_j z_j$ com $x_i, y_j \in O_P$. Então:

$$\begin{aligned} Tr_{F'/F}(zu) &= Tr_{F'/F}\left(\sum_{i,j=1}^n x_i y_j z_i^* z_j\right) \\ &= \sum_{i=1}^n x_i \sum_{j=1}^n y_j (Tr_{F'/F}(z_i^* z_j)) \\ &= \sum_{i=1}^n x_i y_i \in O_P \end{aligned}$$

Logo, $z \in \mathcal{C}_P$.

- (c) Sabemos por (b) que $\mathcal{C}_P = \sum_{i=1}^n O_P u_i$ para uma escolha apropriada de $u_i's \in F$. Considere $x \in F$ tal que $v_P(x) \geq 0$ e $v_P(x) \geq -v_{P'}(u_i)$, $i = 1, \dots, n$ e para todo P'/P ; então

$$v_{P'}(xu_i) = e(P'/P)v_P(x) + v_{P'}(u_i) \geq 0, \forall P'/P, i = 1, \dots, n$$

Logo, $x\mathcal{C}_P \subseteq O'_{P'}$; ou seja, $x\mathcal{C}_P$ é um ideal de $O'_{P'}$. Assim, $x\mathcal{C}_P = y.O'_{P'}$ para algum $y \in O'_{P'}$, pois $O'_{P'}$ é DIP (por III.2.6). Considere $t = x^{-1}y$; então $\mathcal{C}_P = t.O'_{P'}$. Como $O'_{P'} \subseteq \mathcal{C}_P$, temos que $v_{P'}(t) \leq 0, \forall P'/P$. Agora, considere $t' \in F'$ tal que $\mathcal{C}_P = t'.O'_{P'}$; logo,

$$\begin{aligned} tO'_{P'} &= t'.O'_{P'} \Leftrightarrow t^{-1}t' \in O'_{P'} \text{ e } t'^{-1}t \in O'_{P'} \\ &\Leftrightarrow v_{P'}(t^{-1}.t') \geq 0 \text{ e } v_{P'}(t'^{-1}.t) \geq 0 \\ &\Leftrightarrow v_{P'}(t') = v_{P'}(t), \forall P'/P \end{aligned}$$

- (d) Considere $\{z_1, \dots, z_n\}$ base de F'/F , então por III.2.10 $\{z_1, \dots, z_n\}$ e $\{z_1^*, \dots, z_n^*\}$ são bases integrais para quase todo $P \in \mathbb{P}_F$. Por (b),

$$\mathcal{C}_P = \sum_{i=1}^n O_P z_i^* = O'_{P'} \text{ para quase todo } P \in \mathbb{P}_F$$

□

III.2.13 Definição Considere $P \in \mathbb{P}_F$ um lugar e o fecho integral $O'_{P'}$ de O_P em F' . Seja $\mathcal{C}_P = tO'_{P'}$ o módulo complementar sobre O_P . Então para P'/P definimos o *expoente diferente* de P' sobre P por

$$d(P'/P) = -v_{P'}(t)$$

Pela Proposição anterior $d(P'/P)$ está bem definido e $d(P'/P) \geq 0$. Mais ainda, $d(P'/P) = 0$ para quase todo $P \in \mathbb{P}_F$, já que por (d) da Proposição anterior $\mathcal{C}_P = O'_{P'}$ para quase todo $P \in \mathbb{P}_F$ e portanto podemos definir o

$$Diff(F'/F) = \sum_{P \in \mathbb{P}_F} \sum_{P'/P} d(P'/P) P'$$

o *divisor diferente* de F'/F . Observe ainda que $0 \leq Diff(F'/F) \in \mathcal{D}_F$.

III.2.14 Observação Aqui cabe notar uma caracterização importante do módulo $\mathcal{C}_P$:
 $z \in \mathcal{C}_P \Leftrightarrow v_{P'}(z) \geq -d(P'/P)$ para todo P'/P .

III.2.15 Definição Seja

$$\mathcal{A}_{F'/F} = \{\alpha \in \mathcal{A}_{F'} / \alpha_{P'} = \alpha_{Q'} \text{ sempre que } P' \cap F = Q' \cap F\}$$

Observe que $\mathcal{A}_{F'/F}$ é um F' -subespaço de $\mathcal{A}_{F'}$. Mais ainda, a aplicação traço $Tr_{F'/F} : F' \longrightarrow F$ pode ser estendida a uma aplicação F -linear (também denotada $Tr_{F'/F}$) de $\mathcal{A}_{F'/F}$ em $\mathcal{A}_F$ por:

$$(Tr_{F'/F}(\alpha))_P = Tr_{F'/F}(\alpha_{P'}) \text{ , } \forall \alpha \in \mathcal{A}_{F'/F}$$

onde $P' \in \mathbb{P}_{F'}$, P'/P . Note que como $\alpha_{P'} \in O_{P'}$ para quase todo $P' \in \mathbb{P}_{F'}$, segue que $Tr_{F'/F}(\alpha_{P'}) \in O_P$ para quase todo $P \in \mathbb{P}_F$ e assim, $Tr_{F'/F}(\alpha)$ é realmente um adele de F/K . Claramente o traço de um adele principal $z \in F'$ é um adele principal de F .

O próximo resultado é o que associa um diferencial de Weil de F/K a um diferencial de Weil de F'/K' . Mas antes dele necessitamos de dois lemas:

III.2.16 Lema Para qualquer $C' \in \mathcal{D}_{F'}$, tem-se $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(C')$.

Demonstração : Seja $\alpha = (\alpha_{P'})_{P \in \mathbb{P}_{F'}}$, um adele de F' . Para todo $P \in \mathbb{P}_F$, existe pelo teorema de aproximação, um elemento $x_{P'} \in F'$ com

$$v_{P'}(\alpha_{P'} - x_P) \geq -v_{P'}(C'), \text{ para todo } P'/P$$

Fixe $\beta = (\beta_{P'})_{P \in \mathbb{P}_{F'}}$, com $\beta_{P'} = x_P$ sempre que P'/P . Então $\beta \in \mathcal{A}_{F'/F}$ e $\alpha - \beta \in \mathcal{A}_{F'}(C')$. Como $\alpha = \beta + (\alpha - \beta)$, segue o resultado. $\square$

III.2.17 Lema Seja M/L uma extensão finita e separável de corpos, V um espaço vetorial sobre M e $\mu : V \rightarrow L$ uma aplicação M -linear. Então, existe uma única aplicação M -linear $\mu' : V \rightarrow M$ tal que

$$Tr_{M/L} \circ \mu' = \mu$$

Demonstração : Considere o espaço dos L -funcionais lineares de M , i.e., $M' = \{\lambda : M \rightarrow L, \lambda \text{ é } L\text{-linear}\}$. Lembre que $Tr_{M/L} \in M'$. Agora, dado $y \in M$ defina o L -funcional linear de M dado por $(y.Tr_{M/L})(w) = Tr_{M/L}(y.w)$, para todo $w \in M$.

$\vdash$ Dado $\lambda \in M'$ existe um único $z_\lambda \in M$ tal que $\lambda = z_\lambda.Tr_{M/L}$

De fato, considere $\{z_1, \dots, z_n\}$ uma base de M/L e $\{z_1^*, \dots, z_n^*\}$ sua base dual em relação ao traço. Dado $\lambda \in M'$ defina $z_\lambda = \sum_{i=1}^n \lambda(z_i)z_i^*$ e agora observe que para todo $j = 1, \dots, n$:

$$(z_\lambda.Tr_{M/L})(z_j) = Tr_{M/L}(z_\lambda z_j) = \sum_{i=1}^n \lambda(z_i).Tr_{M/L}(z_i.z_j^*) = \lambda(z_j)$$

Assim, $\lambda = z_\lambda.Tr_{M/L}$, pois são funcionais lineares que coincidem numa base; mais ainda, se $z'_\lambda = \sum_{i=1}^n a_i z_i$ e $\lambda = z'_\lambda.Tr_{M/L}$, teremos $\lambda(z_j) = a_j$ para todo j , i.e., $z'_\lambda = z_\lambda$.

Agora, fixado $v \in V$, defina $\lambda_v : M \rightarrow L$ por $\lambda_v(a) = \mu(av)$; claramente, $\lambda_v \in M'$ e portanto, existe um único $z_\lambda \in M$ tal que $\lambda_v = z_\lambda.Tr_{M/L}$ (*). Defina $\mu' : V \rightarrow M$ por $\mu'(v) = z_v$ e observe que para todo $v \in V$:

$$Tr_{M/L} \circ \mu'(v) = Tr_{M/L}(z_v) = (z_\lambda.Tr_{M/L})(1) = \lambda_v(1) = \mu(v)$$

Que μ' é M -linear e é única segue da igualdade (*) e do fato de que $Tr_{M/L} : M \rightarrow L$ não é o funcional nulo. $\square$

III.2.18 Teorema Usando a notação da Definição III.2.15, para cada diferencial de Weil ω de F/K , existe um único diferencial de Weil ω' de F'/K' tal que

$$Tr_{K'/K}(\omega'(\alpha)) = \omega(Tr_{F'/F}(\alpha)) \quad (\text{III.8})$$

para todo $\alpha \in \mathcal{A}_{F'/F}$. Este diferencial de Weil é chamado cotração de ω em F'/F , e é denotado por $Cotr_{F'/F}(\omega)$. Se $\omega \neq 0$ e $(\omega) \in \mathcal{D}_F$ é o divisor de ω , então

$$(Cotr_{F'/F}(\omega)) = Con_{F'/F}((\omega)) + Diff(F'/F)$$

Demonstração : Queremos provar a existência do cotrção de um diferencial de Weil. Para $\omega = 0$, Basta tomar $\omega' = 0$. Assim, seja então $\omega \neq 0$ e fixe

$$W' = \text{Con}_{F'/F}((\omega)) + \text{Diff}(F'/F) \quad (\text{III.9})$$

Vamos construir ω' por etapas:

Passo 1: A aplicação K -linear $\omega_1 : \mathcal{A}_{F'/F} \longrightarrow K$ dada por $\omega_1 = \omega \circ \text{Tr}_{F'/F}$ tem as seguintes propriedades:

(a₁) $\omega_1(\alpha) = 0$ para todo $\alpha \in \mathcal{A}_{F'/F}(W') + F'$.

(b₁) Se $B' \in \mathcal{D}'_F$ é divisor com $B' \not\leq W'$, então, existe $\beta \in \mathcal{A}_{F'/F}(B')$ com $\omega_1(\beta) \neq 0$.

⊢ (a₁) É claro que ω_1 é linear. Como ω se anula em F , então ω_1 se anula em F' pois $F = \text{Tr}_{F'/F}(F')$. Considere agora, $\alpha \in \mathcal{A}_{F'/F}(W')$ e lembre que para P'/P com $P \in \mathbb{P}_F$ tem-se:

$$v_{P'}(W') = e(P'/P)v_P(\omega) + d(P'/P)$$

Logo, se $x \in F$ com $v_P(x) = v_P(\omega)$, então

$$\begin{aligned} v_{P'}(x\alpha_{P'}) &= v_{P'}(x) + v_{P'}(\alpha_{P'}) \\ &\geq e(P'/P)v_P(\omega) - v_{P'}(W') \\ &\geq -d(P'/P) \end{aligned}$$

ou seja, $x\alpha_{P'} \in \mathcal{C}_P$ e, portanto, $v_P(\text{Tr}_{F'/F}(x\alpha_{P'})) \geq 0$. Assim, $v_P(\text{Tr}_{F'/F}(\alpha_{P'})) \geq -v_P(\omega)$ e portanto, $\text{Tr}_{F'/F}(\alpha) \in \mathcal{A}_{F'/F}((\omega))$ e assim $\omega(\text{Tr}_{F'/F}(\alpha)) = 0$, i.e., $\omega_1(\alpha) = 0$.

⊢ (b₁) Dado $B' \not\leq W'$, existe $P_0 \in \mathbb{P}_F$ tal que para algum P^*/P_0

$$v_{P^*}(\text{Con}_{F'/F}((\omega)) - B') < -d(P^*/P) \quad (\text{III.10})$$

Seja O'_{P_0} o fecho integral de O_{P_0} em F' e $\mathcal{C}_{P_0}$ o módulo complementar de O_{P_0} em F' . Considere o conjunto

$$J = \{z \in F'/v_{P'}(z) \geq v_{P'}(\text{Con}_{F'/F}((\omega)) - B'), \forall P'/P_0\}$$

Pelo Teorema de Aproximação existe $u \in J$ tal que $v_{P'}(u) = v_{P'}(\text{Con}_{F'/F}((\omega)) - B')$ para cada P'/P_0 . Logo, por (III.10), $J \not\subseteq \mathcal{C}_{P_0}$; segue que

$$\text{Tr}_{F'/F}(J) \not\subseteq \mathcal{C}_{P_0}. \quad (\text{III.11})$$

Considere $t \in F$, com $v_{P_0}(t) = 1$; então, para algum $r \geq 0$, temos $t^r J \subseteq O'_{P_0}$; logo, $t^r \text{Tr}_{F'/F}(J) = \text{Tr}_{F'/F}(t^r J) \subseteq O_{P_0}$. Como $t^r \text{Tr}_{F'/F}(J)$ é um ideal de O_{P_0} que é DIP, existe $s \geq 0$ tal que $t^r \text{Tr}_{F'/F}(J) = t^s O_{P_0}$ e assim $\text{Tr}_{F'/F}(J) = t^m O_{P_0}$ com $m \in \mathbb{Z}$; logo, por (III.11), $m \leq -1$ e assim,

$$t^{-1} O_{P_0} \subseteq \text{Tr}_{F'/F}(J) \quad (\text{III.12})$$

Por I.6.3(a) existe $x \in F$ com

$$v_{P_0}(x) = -v_{P_0}(\omega) - 1 \quad \text{e} \quad \omega_{P_0}(x) \neq 0 \quad (\text{III.13})$$

considere $y \in F$ com $v_{P_0}(y) = v_{P_0}(\omega)$; então $v_{P_0}(xy) = -1$ e portanto, $xy \in t^{-1} \cdot O_{P_0}$. Por (III.12) existe $z \in J$ tal que $\text{Tr}_{F'/F}(z) = xy$. Considere $\beta \in \mathcal{A}_{F'/F}$ dado por

$$\beta_{P'} = \begin{cases} 0 & , P' \not\mid P_0 \\ y^{-1}z & , P' \mid P_0 \end{cases}$$

Assim para $P' | P_0$, pela definição de J segue que

$$\begin{aligned} v_{P'}(\beta) &= v_{P'}(y) + v_{P'}(z) \\ &\geq -v_{P'}(\text{Con}_{F'/F}((\omega))) + v_{P'}(\text{Con}_{F'/F}((\omega)) - B') \\ &\geq -v_{P'}(B') \end{aligned}$$

Logo, $\beta \in \mathcal{A}_{F'/F}(B')$ e

$$\omega_1(\beta) = \omega \circ \text{Tr}_{F'/F}(\beta) = \omega(\text{Tr}_{F'/F}(y^{-1}z))$$

mas $\text{Tr}_{F'/F}(y^{-1}z) = y^{-1}\text{Tr}_{F'/F}(z) = x$, i.e., $\omega_1(\beta) = \omega(\text{Tr}_{F'/F}(\beta)) = \omega_{P_0}(x) \neq 0$ por III.2.17.

Passo 2: Defina $\omega_2 : \mathcal{A}_{F'} \rightarrow K$ como segue:

Sabemos pelo Lema III.2.16 que para $\alpha \in \mathcal{A}_{F'}$ existem $\beta \in \mathcal{A}_{F'/F}$ e $\gamma \in \mathcal{A}_{F'}(W')$ tais que $\alpha = \beta + \gamma$. Defina $\omega_2(\alpha) = \omega_1(\beta)$. Esta aplicação está bem definida e é K -linear. De fato, se $\alpha = \beta_1 + \gamma_1 = \beta_2 + \gamma_2$, $\beta_i \in \mathcal{A}_{F'/F}$ e $\gamma_i \in \mathcal{A}_{F'}(W')$, temos $\beta_1 - \beta_2 \in \mathcal{A}_{F'/F}(W') \cap \mathcal{A}_{F'/F}$ e como ω_1 anula $\mathcal{A}_{F'/F}(W')$, temos $\omega(\beta_1) = \omega(\beta_2)$. Que ela é K -linear é óbvio. Mais ainda, por (a_1) e (b_1) ω_2 satisfaz:

$$(a_2) \quad \omega_2(\alpha) = 0, \text{ se } \alpha \in \mathcal{A}_{F'}(W') + F$$

$$(b_2) \quad \text{Se } B' \in \mathcal{D}_F \text{ é divisor com } B' \not\leq W', \text{ existe } \beta \in \mathcal{A}_{F'}(\beta) \text{ com } \omega_2(\beta).$$

Entretanto, procuramos um diferencial de Weil em F' , ou seja uma aplicação K' -linear e ω_2 é somente K -linear.

Passo 3: Por III.2.17 existe $\omega' : \mathcal{A}_{F'} \rightarrow K'$ aplicação K' -linear tal que $\text{Tr}_{K'/K} \circ \omega' = \omega_2$. Das definições de ω_1 e ω_2 obtemos

$$\text{Tr}_{K'/K}(\omega'(\alpha)) = \omega_2(\alpha) = \omega_1(\alpha) = \omega((\text{Tr}_{F'/F})(\alpha))$$

provando (III.8).

Falta mostrar que:

$$(a_3) \quad \omega'(\alpha) = 0 \text{ para todo } \alpha \in \mathcal{A}_{F'/F}(W') + F'.$$

$$(b_3) \quad \text{Se } B' \in \mathcal{D}_F \text{ com } B' \not\leq W', \text{ existe } \beta \in \mathcal{A}_{F'}(W') \text{ com } \omega'(\beta) \neq 0.$$

⊢ (a_3) Como ω' é K' -linear, então a imagem de $\mathcal{A}_{F'}(W') + F'$ por ω' é 0 ou todo K' . Se $\omega'(\mathcal{A}_{F'}(W') + F') = K'$, existe α tal que $\text{Tr}_{K'/K}(\omega'(\alpha)) \neq 0$, pois $\text{Tr}_{F'/F} \neq 0$. Pela construção de ω' , $\omega_2 = \text{Tr}_{F'/F} \circ \omega'$ e portanto $\omega_2(\alpha) \neq 0$, contradizendo (a_2) . Logo, $\omega'(\alpha) = 0$

⊢ (b_3) Por (b_2) existe $\beta \in \mathcal{A}_{F'}(B')$ tal que $\text{Tr}_{K'/K}(\omega'(\beta)) = \omega_2(\beta) \neq 0$. Logo, $(\omega') = W'$. Falta mostrar que ω' é único: seja ω^* diferencial satisfazendo a propriedade (III.8), considere $\eta = \omega' - \omega^*$ e suponha que para todo $\alpha \in \mathcal{A}_{F'/F}$, $\text{Tr}_{K'/K}(\eta(\alpha)) = 0$. Como $\eta \in \Omega_{F'/K'}$, η se anula em $\mathcal{A}'_F(C')$ para algum $C' \in \mathcal{D}_F$. Então, por III.2.16 $\text{Tr}_{K'/K}(\eta(\alpha)) = 0$ para todo $\alpha \in \mathcal{A}'_F$. Logo, $\eta = 0$ e $\omega' = \omega^*$. □

Uma consequência simples do resultado anterior, mas muito importante é o seguinte teorema:

III.2.19 Teorema (de Hurwitz) *Se F/K é um corpo de funções de gênero g e F'/F uma extensão finita e separável com K' o corpo de constantes de F' e g' o gênero de F'/K' . Então temos que :*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \text{Diff}(F'/F)$$

Demonstração : Escolha $W \in \Omega_F$, com $\omega \neq 0$. Segue do Teorema III.2.18

$$(Cotr_{F'/F}(\omega)) = Con_{F'/F}((\omega)) + Diff(F'/F)$$

Lembre que o grau de um divisor canônico é $2g - 2$ (respec. $2g' - 2$) e pelo Corolário III.1.13 temos que:

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + deg Diff(F'/F)$$

□

Observe que qualquer corpo de funções F/K é extensão finita de um corpo de funções racionais ($g = 0$). Se pudermos escolher $x \in F$ tal que $F/K(x)$ seja separável, o teorema precedente é uma arma poderosa para se calcular o gênero g de F/K (sempre podemos escolher x tal que $F/K(x)$ seja separável, mas isso foge ao nosso objetivo). Na verdade, nesta situação o que precisamos calcular é $deg(Diff(F'/F))$, contudo, nem sempre há métodos para realizar este cálculo. Os próximos resultados caminham nessa direção.

Como sempre consideramos F'/K' uma extensão algébrica finita e separável de F/K , com K perfeito. Dados $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com P'/P o próximo teorema nos dá uma relação entre $d(P'/P)$ e $e(P'/P)$. Na prova desse teorema necessitamos de dois lemas bastante técnicos que não serão provados aqui, mas cuja prova se encontra em [4].

III.2.20 Lema *Seja F^*/F extensão de corpo de funções, $P \in \mathbb{P}_F$ e $P^* \in \mathbb{P}_{F^*}$ com P^*/P . Considere um automorfismo σ de F^*/F . Então $\sigma(P^*) = \{\sigma(z)/z \in P^*\}$ é um lugar de F^* e*

(a) $v_{\sigma(P^*)}(y) = v_{P^*}(\sigma^{-1}(y))$, $\forall y \in F^*$

(b) $\sigma(P^*)/P$

(c) $e(\sigma(P^*)/P) = e(P^*/P)$ e $f(\sigma(P^*)/P) = f(P^*/P)$

III.2.21 Lema *Seja $P \in \mathbb{P}_F$ e $P_1, \dots, P_r \in \mathbb{P}_{F'}$ todas as extensões de P em F'/F . Considere os corpos de resíduos $k = O_P/P$, $k_i = O_{P_i}/P_i \supseteq k$ e as aplicações canônicas $\pi : O_P \longrightarrow k$ e $\pi_i : O_{P_i}/P_i \longrightarrow k_i$ ($i = 1, \dots, r$). Então, para todo $u \in O'_P = ic_{F'}(O_P)$*

$$\pi(Tr_{F'/F}(u)) = \sum_{i=1}^r e(P_i/P) Tr_{k_i/k}(\pi_i(u))$$

III.2.22 Teorema (do Diferente de Dedekind) *Para $P \in \mathbb{P}_F$, P'/P , $e(P'/P)$, o índice de ramificação de P' sobre P e $d(P'/P)$ o expoente diferente de P' sobre P , então:*

(a) $d(P'/P) \geq e(P'/P) - 1$

(b) $d(P'/P) = e(P'/P) - 1$ se $char K \nmid e(P'/P)$

Em particular, se $char K = 0$, então $d(P'/P) = e(P'/P) - 1$.

Demonstração :

(a) Seja $O'_P = ic_{F'}(O_P)$ e $\mathcal{C}_P$ o módulo complementar de O_P em F' . Na verdade pela Observação III.2.14, queremos provar que para qualquer $t \in F'$ com

$$v_{P'}(t) = 1 - e(P'/P), \forall P'/P \quad (\text{III.14})$$

tem-se $Tr_{F'/F}(tO'_P) \subseteq O_P$. Considere então uma extensão Galoisiana F^*/F tal que $F^* \supseteq F' \supseteq F$ e considere $n = [F' : F]$ F -automorfismos $\sigma_1, \dots, \sigma_n$ de F^*/F cujas restrições a F' sejam duas a duas distintas. Para $z \in O'_P$ temos:

$$Tr_{F'/F}(tz) = \sum_{i=1}^n \sigma_i(tz) \quad (\text{III.15})$$

Fixe P^* lugar de F^* sobre P e fixe $P_i^* = \sigma_i^{-1}(P^*)$ e $P_i' = P_i^* \cap F'$. Como z é integral sobre O_P temos $v_{P_i}(\sigma_i(z)) \geq 0$. Então

$$\begin{aligned} v_{P^*}(\sigma_i(tz)) &= v_{P^*}(\sigma_i(t)) + v_{P^*}(\sigma_i(z)) \\ &\geq v_{P^*}(\sigma_i(t)) = v_{P_i^*}(t) \text{ por III.2.20} \\ &= e(P_i^*/P_i')(1 - e(P_i'/P)) \text{ por III.14} \\ &> -e(P_i^*/P_i').e(P_i'/P) \\ &= -e(P_i^*/P) = -e(P^*/P) \text{ por III.2.20} \end{aligned}$$

Usando (III.15), concluímos que

$$-e(P^*/P) < v_P^*(Tr_{F'/F}(tz)) = e(P^*/P)v_P(Tr_{F'/F}(tz))$$

Isto implica que $v_P(Tr_{F'/F}(tz)) \geq 0$, seguindo o resultado.

- (b) Utilizaremos a notação usada em III.2.21 e abreviaremos $e_i = e(P_i/P)$. Seja $P' = P_1$ e $e = e(P'/P)$. Temos por objetivo mostrar que

$$d(P'/P) = e - 1 \Leftrightarrow \text{char } K \nmid e \quad (\text{III.16})$$

($\Leftarrow$) Supondo que $\text{char } K \nmid e(P'/P)$ e que $d(P'/P) \geq e$. Logo, existe algum $w \in F'$ tal que

$$v_{P'}(w) \leq -e \quad \text{e} \quad Tr_{F'/F}(w.O_P') \subseteq O_P \quad (\text{III.17})$$

Como K é perfeito, a extensão k_1/k é separável e podemos encontrar $y_0 \in O_{P'}$ com $Tr_{k_1/k}(\pi_1(y_0)) \neq 0$. Pelo Teorema de Aproximação, existe um elemento $y \in F'$ tal que

$$v_{P'}(y - y_0) > 0 \quad , \quad \text{i.e.,} \quad \pi_1(y) = \pi_1(y_0)$$

e

$$v_{P_i}(y) \geq \max\{1, e_i + v_{P_i}(w)\} \quad \text{para} \quad 2 \leq i \leq r \quad (\text{III.18})$$

em particular, $\pi_i(y) = 0$ para $i = 2, \dots, r$ Então, $y \in O_P'$ e pelo Lema III.2.21,

$$\begin{aligned} \pi(Tr_{F'/F}(y)) &= e.Tr_{k_1/k}(\pi_1(y)) + \sum_{i=2}^r e_i.Tr_{k_i/k}(\pi_i(y)) \\ &= e.Tr_{k_1/k}(\pi_1(y_0)) \neq 0 \end{aligned}$$

isto é, $Tr_{F'/F}(y) \in O_P'$. (Aqui foi usado que $\text{char } K \nmid e$, e portanto, $e \neq 0$ em k .) E concluímos que

$$v_P(Tr_{F'/F}(y)) = 0$$

Agora escolhemos $x \in F$ com $v_P(x) = 1$. Então

$$(Tr_{F'/F}(x^{-1}y)) = x^{-1}(Tr_{F'/F}(y)) \notin O_P \quad (\text{III.19})$$

Por outro lado, $x^{-1}yw^{-1} \in O_P'$ pois

$$v_{P'}(x^{-1}yw^{-1}) = -e + v_{P'}(y) - v_{P'}(w) \geq 0$$

e

$$v_{P_i}(x^{-1}yw^{-1}) = v_{P_i}(y) - (e_i + v_{P_i}(w)) \geq 0$$

para $i = 2, \dots, r$ por (III.17) e (III.18). Segue que $x^{-1}y \in wO_P'$ e $Tr_{F'/F}(x^{-1}y) \in O_P$ por (III.17), contradizendo (III.19).

($\Rightarrow$) Agora suponha que $\text{char} K | e$. A fim de mostrar que $d(P'/P) \geq e$, seja $u \in F'$ tal que

$$v_{P'}(u) = -e \text{ e } v_{P_i}(u) \geq -e_i + 1 \quad (i = 2, \dots, r) \quad (\text{III.20})$$

Como antes, $x \in F$ denota um elemento P -primo. Para qualquer $z \in O'_P$ temos

$$v_{P'}(xuz) \geq 0 \text{ e } v_{P_i}(xuz) > 0 \quad (i = 2, \dots, r)$$

Logo, $xuz \in O'_P$ e por III.2.21

$$\pi(\text{Tr}_{F'/F}(xuz)) = e \cdot \text{Tr}_{k_1/k}(\pi(xuz)) + \sum_{i=2}^r e_i \text{Tr}_{k_i/k}(\pi(xuz)) = 0$$

Concluindo que $x \text{Tr}_{F'/F}(uz) = \text{Tr}_{F'/F}(xuz) \in P = xO_P$, e assim, $\text{Tr}_{F'/F}(uz) \in O_P$ para qualquer $z \in O'_P$. Logo, $u \in C_P$ e portanto, $-e = v_{P'}(u) \geq -d(P'/P)$.

□

Em condições especiais sobre F'/F e $P \in \mathbb{P}_F$ podemos dar um limite superior para $d(P'/P)$ ou mesmo dar uma fórmula explícita para $d(P'/P)$. Os próximos resultados seguem nessa direção.

III.2.23 Teorema *Suponha que $F' = F(y)$ é uma extensão finita e separável de um corpo de funções de grau $[F' : F] = n$. Seja $P \in \mathbb{P}_F$ tal que o polinômio minimal de $\varphi(T)$ de y sobre F tem os coeficientes em O_P (i.e. y é integral sobre O_P), e sejam $P_1, \dots, P_r \in \mathbb{P}_F$ todos os lugares de F' sobre P . Então vale o seguinte:*

- (a) $d(P_i/P) \leq v_{P_i}(\varphi'(y))$ para $1 \leq i \leq r$.
- (b) $\{1, y, \dots, y^{n-1}\}$ é uma base integral de F'/F no lugar P se e $d(P_i/P) = v_{P_i}(\varphi'(y))$ para $1 \leq i \leq r$.

(Aqui $\varphi'(T)$ denota a derivada de $\varphi(T)$ no anel de polinômios $F[T]$.)

Demonstração : Nestas condições sabemos que $\alpha = \{1, y, \dots, y^{n-1}\}$ é F -base de F' e mais ainda, por hipótese, $\alpha \subseteq O_P$. Assim, α' , a base dual de α com relação ao traço exerce um papel importante no cálculo de $d(P_i/P)$, $i = 1, \dots, r$. Um resultado de teoria de Galois (veja [4], Proposição VIII.5.1) nos garante que: se $\varphi(T) = (T - y) \cdot (c_{n-1}T^{n-1} + \dots + c_1T + c_0)$ com $c_0, c_{n-1} \in F$ e $c_{n-1} = 1$, então $\alpha' = \{ \frac{c_0}{\varphi'(y)}, \dots, \frac{c_{n-1}}{\varphi'(y)} \}$ e $\sum_{i=0}^{n-1} O_P y^i = \sum_{i=0}^{n-1} O_P c_i$ (lembre que $\varphi(T) \in O_P[x]$).

- (a) Como sempre C_P denota o módulo complementar e O'_P o fecho integral de O_P em F' . Agora observe que para mostrar que $d(P_i/P) \leq v_{P_i}(\varphi'(y))$, basta mostrarmos que (por III.2.14)

$$z \in C_P \Rightarrow v_{P_i}(z) \geq -v_{P_i}(\varphi'(y))$$

Portanto, considere $z \in C_P$; como α' é base de F'/F , temos: $z = \sum_{i=0}^{n-1} r_i \frac{c_i}{\varphi'(y)}$, $r_i \in F$.

Desde que para $0 \leq l \leq n-1$, $y^l \in O'_P$ e $z \in C_P$, temos $\text{Tr}_{F'/F}(zy^l) \in O_P$. Mas,

$$\text{Tr}_{F'/F}(zy^l) = \text{Tr}_{F'/F}(\sum_{i=0}^{n-1} r_i \frac{c_i}{\varphi'(y)} y^l) = r_l \text{ pois } \alpha' \text{ é base dual de } \alpha \text{ e, portanto, } r_l \in O_P.$$

Assim, temos:

$$z = \frac{1}{\varphi'(y)} \sum_{i=0}^{n-1} r_i c_i \in \frac{1}{\varphi'(y)} \sum_{i=0}^{n-1} O_P y^i \subseteq \frac{1}{\varphi'(y)} O'_P$$

Portanto, $v_{P_i}(z) \geq -v_{P_i}(\varphi'(y))$ para $i = 1, \dots, r$.

(b) Sabemos que:

$$\sum_{i=0}^{n-1} O_P y^i = \sum_{i=0}^{n-1} O_P c_i$$

Agora suponha que $\alpha = \{1, y, \dots, y^{n-1}\}$ é base integral para O'_P e então α' é base livre do O_P -módulo C_P (por III.2.3) e assim:

$$\begin{aligned} C_P &= \sum_{i=0}^{n-1} O_P \frac{c_i}{\varphi'(y)} = \frac{1}{\varphi'(y)} \sum_{i=0}^{n-1} O_P c_i \\ &= \frac{1}{\varphi'(y)} \sum_{i=0}^{n-1} O_P y^i = \frac{1}{\varphi'(y)} O'_P \end{aligned}$$

Conseqüentemente $d(P_i/P) = -v_{P_i}(\varphi'(y))$, pela definição III.2.13. Para a recíproca suponha que:

$$d(P_i/P) = -v_{P_i}(\varphi'(y)) \quad i = 1, \dots, r$$

Assim pela Proposição III.2.3 (b), $C_P = \frac{1}{\varphi'(y)} O'_P$. considere $z \in O'_P$ e escreva $\sum_{i=0}^{n-1} t_i y^i$, $t_j \in F$. Para $0 \leq j \leq n-1$, temos:

$$\text{Tr}_{F'/F} \left(\frac{1}{\varphi'(y)} c_j z \right) = t_j \in O_P$$

pois, $c_j \in O'_P$ e $\frac{z}{\varphi'(y)} \in C_P$. Portanto, concluímos que $z \in \sum_{i=0}^{n-1} O_P y^i$, ou seja, $O'_P \subseteq \sum_{i=0}^{n-1} O_P y^i \subseteq O'_P$ e $\{1, y, \dots, y^{n-1}\}$ é base integral de O'_P .

□

III.2.24 Corolário Seja $F' = F(y)$ uma extensão finita e separável de corpos de funções de grau $n = [F' : F]$, e seja $\varphi(T) \in F[T]$ o polinômio mínimo de y sobre F . Suponha que $P \in \mathbb{P}_F$ satisfaz

$$\varphi(T) \in O_P[T] \quad \text{e} \quad v_{P'}(\varphi'(y)) = 0$$

para todo $P' \in \mathbb{P}_{F'}$ com P'/P . Então P'/P é não-ramificado em F'/F , e $\{1, y, \dots, y^{n-1}\}$ é uma base integral de F'/F em P .

Demonstração : Por III.2.23,

$$0 \leq d(P'/P) \leq v_{P'}(\varphi'(y)) = 0$$

para todo P'/P . O corolário segue imediatamente do Teorema de Dedekind e de III.2.23(b). □

III.2.25 Proposição Seja F'/F uma extensão finita separável de corpos de funções, $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com P'/P . Suponha que $e(P'/P) = [F' : F] = n$ (P'/P é totalmente ramificado). Seja $t \in F'$ um elemento P' -primo e considere o polinômio minimal $\varphi(T) \in F[T]$ de t sobre F . Então $d(P'/P) = v_{P'}(\varphi'(t))$, e $\{1, t, \dots, t^{n-1}\}$ é uma base integral de O'_P sobre O_P .

Demonstração : Primeiro observamos que $\{1, t, \dots, t^{n-1}\}$ é l.i. sobre F , pois se temos:

$$\sum_{i=0}^{n-1} r_i t^i = 0 \quad \text{com} \quad r_i \in F \quad \text{e nem todo} \quad r_i = 0$$

para $r_i \neq 0$ tem-se:

$$v_{P'}(r_i t^i) = i + e(P'/P) \cdot v_P(r_i) = i + n \cdot v_P(r_i) \equiv i \pmod{n}$$

Assim $v_{P'}(r_i t^i) \neq v_{P'}(r_j t^j)$ sempre que $0 \leq i, j \leq n-1$, $r_i, r_j \neq 0$. Pela desigualdade triangular estrita segue:

$$v_{P'}(r_i t^i) = \min\{v_{P'}(r_i t^i)/r_i \neq 0\} < \infty$$

o que é uma contradição e assim $\{1, t, \dots, t^{n-1}\}$ é base de F'/F . Agora, de $e(P'/P) = n = [F' : F]$, temos que P' é o único lugar acima de P e portanto, $O'_P = O_{P'}$. Mas $t \in O_{P'}$; portanto, $\sum_{i=0}^{n-1} O_P t^i \subseteq O_{P'} = O'_P$. Considere $z \in O_{P'}$ e escreva $z = \sum_{i=0}^{n-1} x_i t^i$, $x_i \in F$. Como $0 \leq v_{P'}(z) = \min\{n \cdot v_P(x_i) + i/0 \leq i \leq n-1\}$, pelo argumento usado anteriormente. Assim temos que $v_P(x_i) \geq 0$ para todo i e $z \in \sum_{i=0}^{n-1} O_P t^i$, i.e., $O'_P = \sum_{i=0}^{n-1} O_P t^i$ como queríamos. Agora que $d(P'/P) = v_{P'}(\varphi'(t))$ segue de modo imediato do Teorema III.2.23. $\square$

Os próximos dois lemas são usados na prova que utilizamos de forma fundamental para a construção de códigos de Goppa auto-duais.

III.2.26 Lema *Se F/K é corpo de funções (K algebricamente fechado em F) e $\alpha \in \Phi$ um fecho algébrico de K , então $[F(\alpha) : F] = [K(\alpha) : K]$.*

Demonstração : É evidente que $[F(\alpha) : F] \leq [K(\alpha) : K]$. Na verdade queremos mostrar que se $\varphi(T) \in K[T]$ é polinômio mínimo de α sobre K , então $\varphi(T)$ é irredutível em $F[T]$. Suponha que não, i.e., $\varphi(T) = h(T) \cdot g(T)$ com $h(T), g(T) \in F[T]$ e $\text{gr}(h(T)), \text{gr}(g(T)) \geq 1$. Mas, observe que qualquer raiz de $h(T)$ e $g(T)$ é raiz de $\varphi(T)$ também, e portanto é algébrica sobre K , e assim os coeficientes de $h(T)$ e $g(T)$ são algébricos sobre K e estão em F , mas K é algebricamente fechado em F e portanto $h(T), g(T) \in K[T]$ o que é uma contradição. $\square$

III.2.27 Lema *Seja F/K corpo de funções algébricas com característica $p > 0$. Dado um elemento $u \in F$ e um lugar $P \in \mathbb{P}_F$, vale o seguinte:*

- (a) *existe um elemento $z \in F$ tal que $v_P(u - (z^p - z)) \geq 0$,*
- (b) *ou para algum $z \in F$,*

$$v_P(u - (z^p - z)) = -m < 0, \quad \text{com } m \not\equiv 0 \pmod{p}$$

No segundo caso, o inteiro m é unicamente determinado por u e por P , a saber

$$-m = \max\{v_P(u - (w^p - w))/w \in F\} \quad (\text{III.21})$$

Demonstração : Considere a afirmação a seguir: Assuma que $x_1, x_2 \in F$ e $v_P(x_1) = v_P(x_2)$. Então existe algum $y \in F$ com

$$v_P(y) = 0 \quad \text{e} \quad v_P(x_1 - y^p x_2) > v_P(x_1) \quad (\text{III.22})$$

De fato, a classe residual de $(x_1/x_2)(P) \in O_P/P$ é não nula; daí, $(x_1/x_2)(P) = (y(P))^p$ para algum $y \in O_P \setminus P$ (aqui é essencial que O_P/P seja perfeito). Isto implica $v_P(y) = 0$ e $v_P(x_1/x_2 - y^p) > 0$, seguindo $v_P(x_1 - y^p x_2) > v_P(x_1)$. A seguir mostramos que: se $v_P(u - (z_1^p - z_1)) = -lp < 0$, então existe um elemento $z_2 \in F$ com

$$v_P(u - (z_2^p - z_2)) > -lp \quad (\text{III.23})$$

A fim de provar isto, escolhemos $t \in F$ com $v_P(t) = -l$; então $v_P(u - (z_1^p - z_1)) = v_P(t^p)$. Por (III.22) podemos encontrar $y \in F$ com $v_P(y) = 0$

$$v_P(u - (z_1^p - z_1) - ((yt)^p - yt)) > -lp;$$

considerando $z_2 = z_1 + yt$, satisfazemos (III.23). A partir de (III.23) segue imediatamente a existência de um elemento que satisfaz (a) (respec. (b)). No caso (b) ainda falta provar a caracterização de m dada por (III.21). Por hipótese temos $v_P(u - (z^p - z)) = -m < 0$ com $m \not\equiv 0 \pmod{p}$. Para qualquer $w \in F$ vale $p \cdot v_P(w - z) \neq -m$; logo, podemos considerar os casos:

Caso 1: $p \cdot v_P(w - z) > -m$. Então $v_P((w - z)^p - (w - z)) > -m$ e $v_P(u - (w^p - w)) = v_P(u - (z^p - z) - ((w - z)^p - (w - z))) = -m$ (utilizamos a desigualdade triangular estrita).

Caso 2: $p \cdot v_P(w - z) < -m$. Neste caso, obtemos $v_P(u - (w^p - w)) = v_P(u - (z^p - z) - ((w - z)^p - (w - z))) < -m$

Em ambos casos $v_P((w - z)^p - (w - z)) \geq -m$, provando (III.21). □

III.2.28 Teorema (Extensões de Artin-Schreier) *Seja F/K um corpo de funções algébricas com característica $p > 0$. Suponha que $u \in F$ é um elemento que satisfaz a condição a seguir:*

$$u \neq w^p - w \quad \text{para todo } w \in F \quad (\text{III.24})$$

Seja

$$F' = F(y) \quad \text{com} \quad y^p - y = u \quad (\text{III.25})$$

Tal extensão F'/F é chamada extensão Artin-Schreier de F . Para $P \in \mathbb{P}_F$ definimos o inteiro m_P por

$$m_P = \begin{cases} m & \text{se existe um elemento } z \in F \text{ satisfazendo} \\ & v_P(u - (z^p - z)) = -m < 0 \text{ e } m \not\equiv 0 \pmod{p}, \\ -1 & \text{se } v_P(u - (z^p - z)) \geq 0 \text{ para algum } z \in F. \end{cases}$$

Logo, temos:

- (a) F'/F é extensão cíclica Galoisiana de grau p . Os automorfismos de F'/F são dados por $\sigma(y) = y + \nu$, com $\nu = 0, 1, \dots, p-1$.
- (b) P é não-ramificado em F'/F se $m_P = -1$.
- (c) P é totalmente ramificado em F'/F se $m_P > 0$. Denote por P' o único lugar de F' sobre P . Então $d(P'/P) = (p-1)(m_P + 1)$.
- (d) Se pelo menos um lugar $Q \in \mathbb{P}_F$ satisfaz $m_Q > 0$, então K é algebricamente fechado em F' ,
e

$$g' = p \cdot g + \frac{p-1}{2}(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg P),$$

onde g' (respec. g) é o gênero de F'/K (respec. F/K).

Demonstração :

- (a) É um resultado clássico da Teoria de Galois (veja [5]).
- (b) Primeiro considere o caso $m_P = -1$, i.e. $v_P(u - (z^p - z)) \geq 0$ para algum $z \in F$. Seja $y_1 = y - z$ e $u_1 = u - (z^p - z)$; então, $F' = F(y_1)$ e $\varphi_1(T) = T^p - T - u_1$ é o polinômio minimal de y_1 sobre F . Como $v_P(u_1) \geq 0$, y_1 é integral sobre o anel de valorização O_P , e o expoente diferente $d(P'/P)$ de qualquer extensão P' de P em F satisfaz

$$0 \leq d(P'/P) \leq v_{P'}(\varphi'(y_1)) = 0$$

pois, $\varphi'(T) = -1$ (ver III.2.23). Logo, $d(P'/P) = 0$ e P'/P é não ramificado pelo Teorema do Diferente de Dedekind.

- (c) A seguir, assumamos $m_P > 0$. Escolha $z \in F$ tal que $v_P(u - (z^p - z)) = -m_P$. Considere o elemento $y_1 = y - z$ e $u_1 = u - (z^p - z)$. Como anteriormente, temos $F' = F(y_1)$, e $\varphi_1(T) = T^p - T - u_1$ é o polinômio minimal de y_1 sobre F . Seja $P' \in \mathbb{P}_F$ uma extensão de P em F' . Como $y_1^p - y_1 = u_1$, obtemos:

$$v_{P'}(u_1) = e(P'/P) \cdot v_P(u_1) = -m_P \cdot e(P'/P)$$

e

$$v_{P'}(u_1) = v_{P'}(y_1^p - y_1) = p \cdot v_{P'}(y_1)$$

Como p e m_P são relativamente primos e $e(P'/P) \leq [F' : F] = p$, então

$$e(P'/P) = p \quad \text{e} \quad v_{P'}(y_1) = -m_P$$

em particular, P é totalmente ramificado em F'/F . Seja $x \in F$ um elemento P -primo. Escolha inteiros $i, j \geq 0$ tais que $1 = ip - jm_P$ (lembre que p e m_P são relativamente primos). Então o elemento $t = xy_1^j$ é P -primo, pois $v_{P'}(t) = iv_{P'}(x) + jv_{P'}(y_1) = ip - jm_P = 1$. Pela Proposição III.2.25, o expoente diferente é dado por

$$d(P'/P) = v_{P'}(\psi'(t))$$

onde $\psi(T) \in F'[T]$ é o polinômio mínimo de t sobre F . Seja $G = \text{Gal}(F'/F)$ o grupo de Galois de F'/F . Claramente

$$\psi(T) = \prod_{\sigma \in G} (T - \sigma(t)) = (T - t) \cdot h(T)$$

com

$$h(T) = \prod_{\sigma \neq id} (T - \sigma(t)) \in F'[T]$$

Logo, $\psi'(T) = h(T) + (T - t) \cdot h'(T)$ e $\psi'(t) = h(t)$. Concluimos que

$$d(P'/P) = v_{P'} \left(\prod_{\sigma \neq id} (t - \sigma(t)) \right) = \sum_{\sigma \neq id} v_{P'}(t - \sigma(t)) \quad (\text{III.26})$$

(a soma percorre os $\sigma \in G$ com $\sigma \neq id$). Qualquer $\sigma \in G \setminus \{id\}$ é da forma $\sigma(y_1) = y_1 + \mu$ para algum $\mu \in \{1, \dots, p-1\}$; assim

$$t - \sigma(t) = xy_1^j - x(y_1 + \mu)^j = -x_i \cdot \sum_{l=1}^j \binom{j}{l} y_1^{j-l} \mu^l$$

Como $v_{P'}(y_1^{j-1}) < v_{P'}(y_1^{j-l})$ para $l > 2$, a desigualdade triangular estrita nos diz

$$\begin{aligned} v_{P'}(t - \sigma(t)) &= v_{P'}(x) + v_{P'}(j\mu y_1^{j-1}) \\ &= ip + (j-1) \cdot (-m_P) \\ &= ip - jm_P + m_P = m_P + 1 \end{aligned} \quad (\text{III.27})$$

(utilizamos que $j \neq 0 \in K$; isso segue de $1 = ip - jm_P$). Substituindo (III.27) em (III.26), obtemos $d(P'/P) = (p-1)(m_P+1)$.

- (d) Considere $Q \in \mathbb{P}_F$ tal que $m_Q > 0$; por (c) Q é totalmente ramificado em F' . Chame K' o fecho algébrico de K em F' e suponha que $[K' : K] > 1$. Considere Q' o único lugar de F' sobre Q ; logo, $e(Q'/Q) = n = [F' : F]$ (*).

$\vdash K$ é algebricamente fechado em F .

Por contradição: seja K' o fecho algébrico de K em F e $[K' : K] > 1$; temos que $F \subsetneq F'_1 = F.K'$, considere $Q_1 = Q' \cap F_1$. Por (*) segue que $e(Q'/Q_1) = 1$, pois se tomamos $K' = K(\alpha)$ temos $F_1 = F(\alpha)$ e neste caso $[F_1 : F] = [K' : K]$ (por III.2.26). Considerando $\varphi(T) \in K[T]$ e o polinômio mínimo de α sobre K , pelo teorema III.2.23, já que $\varphi(T) \in O_Q[T]$, temos que $0 \leq d(Q_1/Q)v_Q(\varphi'(\alpha))$; mas $\varphi(\alpha) \in K$ e assim $d(Q_1/Q) = 0$ e pelo Teorema do Diferente de Dedekind temos $e(Q_1/Q) = 1$! Absurdo, pois $e(Q'/Q) = e(Q'/Q_1).e(Q_1/Q) = 1$. A fórmula

$$g' = pg + \frac{p-1}{2}(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1).deg P)$$

é consequência de (b) e (c) e da fórmula de Hurwitz.

□

O próximo teorema tem uma prova análoga ao teorema anterior e assim não faremos tal demonstração aqui. Mas ele será importante na obtenção de um exemplo de código de Goppa auto-dual.

III.2.29 Teorema Considere um corpo de funções algébricas F/K com corpo de constantes K de característica $p > 0$ e um polinômio aditivo separável $a(T) \in K[T]$ de grau p^n com todas as raízes em K . Seja $u \in F$; suponha que para qualquer $P \in \mathbb{P}_F$ existe um elemento $z \in F$ (dependendo de P) tal que

$$v_P(u - a(z)) \geq 0 \quad (III.28)$$

ou

$$v_P(u - a(z)) = -m \quad \text{com } m > 0 \quad \text{e } m \not\equiv 0 \pmod{p} \quad (III.29)$$

Defina $m_P = -1$ para o caso (III.28) e $m_P = m$ no caso (III.29). Então m_P é um inteiro bem definido. Considere a extensão de corpo $F' = F(y)$ de F onde y satisfaz a equação

$$a(y) = u$$

Se existe pelo menos um lugar $Q \in \mathbb{P}_F$ com $m_Q > 0$, então vale o seguinte:

- (a) F'/F é Galoisiana, $[F' : F] = p^n$ e o grupo de Galois de F'/F é isomorfo ao grupo aditivo $\{\alpha \in K/a(\alpha) = 0\}$, e assim é isomorfo a $(\mathbb{Z}/p\mathbb{Z})^n$. (tal grupo é dito ser abeliano elementar de expoente p ; logo, F'/F é chamada extensão elementar abeliana de expoente p e grau p^n .)
- (b) K é algebricamente fechado em F' .
- (c) Qualquer $P \in \mathbb{P}_F$ com $m_P = -1$ é não-ramificado em F'/F .
- (d) Qualquer $P \in \mathbb{P}_F$ com $m_P > 0$ é totalmente ramificado em F'/F , e o expoente diferente $d(P'/P)$ da extensão P' de P em F' é

$$d(P'/P) = (p^n - 1)(m - 1)$$

- (e) Seja g' (respec. g) o gênero de F (respec. F'). Então

$$g' = p^n + \frac{p^n - 1}{2} \left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1).deg P \right).$$

III.3 Alguns Códigos Auto-Duais

Nosso objetivo agora, é construir alguns exemplos de códigos auto-duais; para tal, faremos uso de vários dos resultados vistos anteriormente. Um código $C_L(D, G)$ num corpo de funções F'/K é dito auto-dual se existe um diferencial de Weil $\eta \in \Omega_{F'}$ tal que $2G - D = (\eta)$ e $\eta_Q(1) = 1$ para $Q \in \text{supp} D$. Assim, nos exemplos a seguir, estaremos à procura de tais divisores e diferencial apropriados.

Dado um corpo de funções $F' = F(y)$, começaremos por encontrar os seus lugares com grau um, a partir dos lugares de $F = \mathbb{F}_q(x)$ corpo racional e do polinômio $\varphi(T) \in F[T]$ que define F' (y é raiz de $\varphi(T)$). Assim, podemos construir D . Para encontrar um diferencial de Weil em F' , vamos tomar o cotraço de um diferencial de Weil em F e calcular o seu divisor em F' ; para isso é necessário calcular o expoente diferente de todos os lugares Q/P de F' , com $P \in \mathbb{P}_F$ (para calcular $\text{Diff}(F'/F)$). Nesta altura, podemos encontrar o gênero g' de F' , pois se W é divisor canônico de F' , então $2g' - 2 = \deg W$. Com isso, podemos encontrar um G satisfazendo $2G - D = (\eta)$; mas, é preciso ter $\eta_{Q_i}(1) = 1$ para cada $Q_i \in \text{supp} D$. Usando o Teorema de Aproximação, é possível encontrar $z \in F'$ tal que o diferencial $z^{-1}\eta$ satisfaz a propriedade desejada; se existir $u \in F'$ tal que $u^2 = z$, então considerando $G' = G - (u)$ obtemos um código auto-dual. Nos exemplos encontram-se indicados os resultados utilizados. Estaremos trabalhando com $\mathbb{F}_q$, corpo finito com q elementos.

III.3.1 Exemplo Seja $q = 2^e$ e $F' = \mathbb{F}_q(x, y)$ com F' definido pela equação

$$y^2 + y = f(x), \quad f(x) \in \mathbb{F}_q[x], \quad \deg(f(x)) = m \not\equiv 0 \pmod{2}$$

Considere $F = \mathbb{F}_q(x)$, $\varphi(T) = T^2 + T - f(x) \in F[T]$ e P_∞ o polo de x em $F = \mathbb{F}_q(x)$. Como $v_\infty(1) = 0$ e $v_\infty(f(x)) = -m < 0$, estamos na condição (2) de III.1.14; logo, $\varphi(T)$ é polinômio irredutível sobre $F[T]$ e define o corpo $F' = F(y)$, onde y é uma raiz de $\varphi(T)$. Além disso, pela mesma proposição, P_∞ tem uma única extensão em F' , $Q_\infty \in \mathbb{P}_{F'}$ satisfazendo

$$e(Q_\infty/P_\infty) = 2 \quad \text{e} \quad f(Q_\infty/F_\infty) = 1$$

e assim, $Q_\infty = 2P_\infty$.

A fim de saber quem são os demais lugares de grau um em F' , devemos estudar as extensões dos lugares de grau um em F ; considere o conjunto a seguir:

$$M = \{\alpha \in \mathbb{F}_q / \exists \beta \in \mathbb{F}_q : \beta^2 + \beta = f(\alpha)\}$$

Para $\alpha \in M$, vamos estudar o divisor dos zeros de $x - \alpha$ em F' . Considere $\beta \in \mathbb{F}_q$ tal que $\beta^2 + \beta = f(\alpha)$; então:

$$\begin{aligned} y^2 + y - f(x) &= \beta^2 + \beta - f(\alpha) \\ y^2 + y - \beta^2 - \beta &= f(x) - f(\alpha) \\ (y - \beta)^2 + (y - \beta) &= f(x) - f(\alpha) \\ (y - \beta)(y + \beta) + (y - \beta) &= f(x) - f(\alpha) \\ (y - \beta)(y + \beta + 1) &= (x - \alpha)g(x) \end{aligned}$$

pois $(x - \alpha) | (f(x) - f(\alpha))$.

Logo, se v_α é a valorização correspondente ao lugar P_α , então $v_\alpha(f(x) - f(\alpha)) > 0$. Seja $Q \in \mathbb{P}_{F'}$ com Q/P_α , então

$$v_Q((y - \beta)(y + \beta + 1)) = v_Q(y - \beta) + v_Q(y + \beta + 1) > 0$$

Podemos escrever $y + \beta + 1 = (y - \beta) + 1$ e $y - \beta = (y + \beta + 1) - 1$. Se $v_Q(y - \beta)$ é negativo, então:

$$v_Q(y + \beta + 1) = \min\{v_Q(y - \beta), v_Q(1)\} < 0$$

chegando a uma contradição. Logo, $v_Q(y - \beta)$ ou $v_Q(y + \beta + 1)$ é positivo.

- Se $v_Q(y - \beta) > 0$, então $v_Q(y + \beta + 1) = \min\{v_Q(y - \beta), 0\} = 0$
- Se $v_Q(y + \beta + 1) > 0$, temos $v_Q(y - \beta) = \min\{v_Q(y + \beta + 1), 0\} = 0$

Logo, há pelo menos duas extensões de P_α em F' . Por III.1.11, segue que há exatamente duas extensões Q_α^1 e Q_α^2 e que $e(Q_\alpha^i/P_\alpha) = 1$ e $f(Q_\alpha^i/P_\alpha) = 1$, pois $[F' : F] = 2$. O Teorema III.2.28 nos diz de forma simples que, a menos de Q_∞/P_∞ , todos os lugares Q/P de F' são não-ramificados; no entanto, é interessante ver que é possível encontrar a extensão de um lugar sem ter que utilizar resultados mais fortes.

A fim de construir um código auto-dual é preciso encontrar divisores $D, G \in \mathcal{D}_{F'}$ tais que $2G - D$ seja um divisor canônico, i.e., que exista um diferencial de Weil $\eta \in \Omega_{F'}$ tal que $(\eta) = 2G - D$ e que $\eta_{Q_\alpha}(1) = 1$ (ver II.2.12). Por III.2.18 tendo um diferencial de Weil de F , sabemos como encontrar seu cotraço em F' e calcular seu divisor. Como F é corpo de funções racionais, então $-2P_\infty$ é divisor canônico; seja ω seu diferencial de Weil e passemos ao cálculo de (ω') , o divisor do seu cotraço:

$$(\omega') = \text{Con}_{F'/F}((\omega)) + \text{Diff}(F'/F)$$

$$\begin{aligned} \text{Con}_{F'/F}((\omega)) &= \text{Con}_{F'/F}(-2P_\infty) = -2 \sum_{Q/P_\infty} e(Q/P_\infty) \cdot Q \\ &= -2 \cdot 2 \cdot Q_\infty = -4Q_\infty \end{aligned}$$

Para o cálculo do diferente precisamos estudar o valor de $d(Q/P)$ para todo $Q \in \mathbb{P}_{F'}$; usaremos o Teorema III.2.28. Como o polinômio $\varphi(T) = T^2 + T - f(x)$ é irredutível, estamos nas condições de tal Teorema.

Para $P \in \mathbb{P}_F$ vamos calcular m_P ; temos $p = \text{char } \mathbb{F}_q = 2$

- $P = P_\infty$ e $z = 1$, então $v_P(f(x) - (1^2 - 1)) = v_P(f(x)) = -m < 0$

Logo, $m_{P_\infty} = m$ e por III.2.28(c) P_∞ é totalmente ramificado e se Q_∞/P_∞ , então

$$d(Q_\infty/P_\infty) = (p - 1)(m_{P_\infty} + 1) = m + 1$$

- $P \neq P_\infty$ e $z = 1$: $v_P(f(x) - (1^2 - 1)) = v_P(f(x)) \geq 0$, $\forall P \neq P_\infty$.

Assim, $m_P = -1$ para todo $P \in \mathbb{P}_F \setminus \{P_\infty\}$ e por III.2.28(b) todo $P \neq P_\infty$ é não-ramificado: $e(Q/P) = 1$; mas 2 $\nmid 1$ e assim, por III.2.22 (b), para todo $P \neq P_\infty$, $d(Q/P) = e(Q/P) - 1 = 0$.

Assim,

$$\text{Diff}(F'/F) = \sum_{P \in \mathbb{P}_F} \sum_{Q/P} d(Q/P) \cdot Q = (m + 1) \cdot Q_\infty$$

e

$$(\omega') = -4Q_\infty + (m + 1)Q_\infty = (m - 3)Q_\infty$$

é divisor canônico em F' . Logo, já podemos calcular o gênero de F' , pois sabemos que o seu grau é $2g' - 2$, onde g' é o gênero de F' ; disto, temos:

$$\begin{aligned} \deg(\omega') &= (m - 3) \cdot \deg Q_\infty \\ 2g' - 2 &= m - 3 \\ g' &= \frac{m - 1}{2} \end{aligned}$$

Considere $U \subseteq M$, $|U| = s$, $n = 2s$ e o polinômio $\varphi(x) = \prod_{\alpha_i \in U} (x + \alpha_i)$; o divisor $D = (\varphi(x))_0 = Q_1 + \dots + Q_n$ onde para $j = 1, 2$, $Q_{\alpha_i}^j = Q_{i+(j-1)s}$ são os lugares sobre P_{α_i} .

$$(1/\varphi(x)) = nQ_\infty - D$$

é divisor principal, e portanto se $\eta = \omega'/\varphi(x)$,

$$(\eta) = (\omega') - (\varphi(x)) = (n + m - 3)Q_\infty - D = 2\left(s + \frac{m-3}{2}\right)Q_\infty - D$$

é divisor canônico. Considerando $G = (s + \frac{m-3}{2})Q_\infty$, temos que $2G - D = (\eta)$ é divisor canônico. Isso garante que $(\eta)_{Q_i}(1) \neq 0$ (por 1.6.3) mas, queremos encontrar $\eta' \in \Omega_{F'}$ tal que $\eta'_{Q_i}(1) = 1$.

Dado $\alpha_i \in U$, seja $\beta_i \in \mathbb{F}_q$ tal que $(y - \beta_i)(y + \beta_i + 1) = f(x) - f(\alpha_i)$; denotaremos

$$f_i = (y - \beta_i) = \widehat{f}_{i+s} \quad \text{e} \quad f_{i+s} = (y + \beta_i + 1) = \widehat{f}_i, \quad 1 \leq i \leq s$$

temos que $v_k(f_k) > 0$ e $v_k(\widehat{f}_k) = 0$, onde $v_k = v_{Q_k}$. Seja

$$l_k = \frac{\varphi(x)}{(x - \alpha_i)} \cdot \widehat{f}_k \quad \text{para } k = 1, \dots, n = 2s, \quad k \equiv i \pmod{s}.$$

Temos que ($k \neq i, i + s$):

$$\begin{aligned} v_i(f_i) &> 0 & v_{i+s}(f_i) &= 0 & v_k(f_i) &\geq 0 \\ v_i(\widehat{f}_i) &= 0 & v_{i+s}(\widehat{f}_i) &> 0 & v_k(\widehat{f}_i) &\geq 0 \\ v_i((x - \alpha_i)) &= 1 & v_{i+s}((x - \alpha_i)) &= 1 & v_k((x - \alpha_i)) &= 0 \\ v_i(l_i) &= 0 & v_{i+s}(l_i) &> 0 & v_k(l_i) &> 0 \end{aligned}$$

Agora, considere

$$z_k = \frac{l_k}{f_k + (x - \alpha_i) + l_k}, \quad k \equiv i \pmod{s}$$

e avaliando:

$$\begin{aligned} v_{i+s}(z_i) &= v_{i+s}(l_i) - \min\{v_{i+s}(f_i), v_{i+s}((x - \alpha_i)), v_{i+s}(l_i)\} > 0 \\ v_k(z_i) &= v_k(l_i) - \min\{v_k(f_i), v_k((x - \alpha_i)), v_k(l_i)\} > 0 \end{aligned}$$

e para $z_i - 1$,

$$v_i(z_i - 1) = v_i(f_i + (x - \alpha_i)) - v_i(f_i + (x - \alpha_i) + l_i) > 0$$

Lembremos que estamos trabalhando num corpo $\mathbb{F}_q$ com característica dois, $q = 2^e$; logo, para todo $a \in \mathbb{F}_q$, $\exists b \in \mathbb{F}_q$ com $a = b^2$. Assim, para cada $a_i = \eta_{Q_i}(1) \in \mathbb{F}_q$, existe $b_i \in \mathbb{F}_q$ com $a_i = b_i^2$. Além disso,

$$v_i((z_i - 1)^2) > 0, \quad v_{i+s}(z_i) > 0, \quad v_k(z_i) > 0.$$

Seja $z = \sum_{k=1}^n b_k \cdot z_k$; então,

$$z^2 = \left(\sum_{k=1}^n b_k \cdot z_k\right)^2 = \sum_{k=1}^n b_k^2 \cdot z_k^2 = \sum_{k=1}^n a_k \cdot z_k^2.$$

Avaliando $z^2 - a_i$:

$$\begin{aligned}
v_i(z^2 - a_i) &= v_i(a_i(z_i^2 - 1) + \sum_{i \neq k=1}^n a_k \cdot z_k^2) \\
&\geq \min\{v_i(a_i(z_i^2 - 1)), v_i(\sum_{i \neq k=1}^n a_k \cdot z_k^2)\} > 0.
\end{aligned}$$

Logo, $v_i(z^2) = 0$, $z^2 \in O_{Q_i} \setminus Q_i$ e $z^2(Q_i) = a_i$. Considerando $\eta' = z^{-2} \cdot \eta$, obtemos:

$$\eta'_{Q_i}(1) = \eta_{Q_i}(z^{-2} \cdot 1) = z^{-2}(Q_i) \cdot \eta_{Q_i}(1) = a_i^{-1} \cdot a_i = 1$$

Seja $G' = G - (z)$: $2G' - D = 2G - D - 2(z) = (\eta) + (z^{-2}) = (\eta')$

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

A questão se podemos construir desta forma códigos auto-duais de comprimento n grande é, portanto, de particular interesse. Usando a cota clássica de Hasse-Weil, o código que acabamos de descrever tem cota

$$n \leq q + 2gq^{\frac{1}{2}} = q + (m-1)q^{\frac{1}{2}}$$

Mas, se considerarmos o caso particular $q = t^2$, $t = 2^h$ e $f(x) = x^{t+1}$, i.e., estamos considerando $F' = \mathbb{F}_q(x, y)$ com $y^2 + y = x^{t+1}$, tal cota é atingida. Neste caso o conjunto $M = \{\alpha \in \mathbb{F}_q / \exists \beta \in \mathbb{F}_q : \beta^2 + \beta = f(\alpha)\}$ é o próprio $\mathbb{F}_q$ (vamos provar o fato mais abaixo) e assim o conjunto U escolhido poderia ser o próprio $\mathbb{F}_q$ e $\varphi(x) = X^q - X$. Considere $\alpha \in \mathbb{F}_q$; então $1 = \alpha^{q-1} = \alpha^{(t-1)(t+1)}$ e, portanto, $\alpha^{t(t+1)} = \alpha^{t+1}$ e assim $\alpha^{t+1} \in \mathbb{F}_t \subseteq \mathbb{F}_q$. Agora considere o polinômio $g(T) = T^2 + T - \alpha^{t+1} \in \mathbb{F}_t$. Se $g(t)$ tem raiz $\beta \in \mathbb{F}_t$, já temos $\beta \in \mathbb{F}_q$ tal que $\beta^2 + \beta = \alpha^{t+1}$ e assim $\alpha \in M$. Se $g(t)$ não tem raiz em $\mathbb{F}_t$, i.e., $g(t)$ é irredutível, considerando β raiz de $g(t)$ em ϕ fecho algébrico, teremos $[\mathbb{F}_t(\beta) : \mathbb{F}_t] = 2$, i.e., $|\mathbb{F}_t(\beta)| = t^2$, e portanto, $\mathbb{F}_t(\beta) = \mathbb{F}_q$ e de novo $\alpha \in M$.

Mais ainda, a diferencial $\eta = \frac{\omega'}{X^q - X}$ satisfaz: para todo Q_i , $\eta_{Q_i}(1) = 1$, e portanto, o código $C_{\mathcal{L}}(D, G)$, onde $D = Q_1, \dots, Q_{2q}$ e $G = (s + \frac{m-3}{2})Q_{\infty} = (\frac{q}{2} + t + 1 - 3)Q_{\infty} = (\frac{q}{2} + t - 2)Q_{\infty}$ é auto-dual.

$\vdash \eta_{Q_i}(1) = 1$ para todo $i = 1, \dots, n$.

Lembre que $\omega' = \text{Cotr}(\omega)$, $\omega \in \Omega_F$ e $(\omega) = -2P_{\infty}$ e assim, por I.6.4(c) $\omega_{P_i}((x - \alpha_i)^{-1}) = 1$ e $\omega_{P_i}(1) = 0$, para todo $i = 1, \dots, q$. ($M = \{\alpha_i \in \mathbb{F}_q, \exists \beta_i : \beta_i^2 + \beta_i = \alpha_i^{t+1}\}$).

Se $\gamma \in F'$, $\gamma = a(x) + yb(x)$, com $a(x), b(x) \in F = \mathbb{F}_q(x)$; da definição de cotração e da noção de componente local de um diferencial, temos: $\omega_{P_i}(Tr_{F'/F}(\gamma)) = Tr_{K'/\mathbb{F}_q}(\omega'_{Q_i}(\gamma) + \omega'_{Q_{i+s}}(\gamma))$. Como $K' = \mathbb{F}_q$, então $Tr_{K'/\mathbb{F}_q}(\gamma) = \gamma$; como $\text{char}(\mathbb{F}_q) = 2$, $Tr_{F'/F}(y) = y + y + 1 = 1$ e para todo $z \in F$, $Tr_{F'/F}(z) = z + z = 0$. Logo, $Tr_{F'/F}(\gamma) = Tr_{F'/F}((a(x) + yb(x))) = a(x)Tr_{F'/F}(1) + b(x)Tr_{F'/F}(y) = b(x)$.

1. Se $a(x) \in F$, então $\omega'_{Q_i}(a(x)) = \omega'_{Q_{i+s}}(a(x))$

Prova: $Tr_{F'/F}(a(x)) = 0$; logo, $\omega_{P_i}(Tr_{F'/F}(a(x))) = \omega_{P_i}(0) = 0$ e $\omega'_{Q_i}(a(x)) = -\omega'_{Q_{i+s}}(a(x)) = \omega'_{Q_{i+s}}(a(x))$, e portanto, $\omega'_{Q_i}(a(x)) = \omega'_{Q_{i+s}}(a(x))$

2. $\vdash \omega'_{Q_i}\left(\frac{1}{x^q - x}\right) = 1 = \omega'_{Q_{i+s}}\left(\frac{1}{x^q - x}\right)$

Prova: $\vdash \omega\left(\frac{1}{x^q - x}\right) = 1 = \omega\left(\frac{1}{x - \alpha_i}\right)$.

$$x^q - x = (x - \alpha_i)^q - (x - \alpha_i) = (x - \alpha_i) \cdot ((x - \alpha_i)^{q-1} - 1)$$

chamando $g(x) = (x - \alpha_i)^{q-1} - 1$, temos que:

$$\frac{1}{x^q - q} + \frac{1}{(x - \alpha_i)} = \frac{1 + g(x)}{(x - \alpha_i) \cdot g(x)} = \frac{(x - \alpha_i)^{q-1}}{(x - \alpha_i) \cdot g(x)} = \frac{(x - \alpha_i)^{q-2}}{g(x)} \in P_{\alpha_i}$$

pois $q = t^2 = 2^{2h}$, $h \geq 1$ e assim, $\omega_{P_{\alpha_i}}(\frac{1}{x^q - q} + \frac{1}{(x - \alpha_i)}) = \omega_{P_{\alpha_i}}(\bar{0}) = 0$, isto é,

$$\omega_{P_{\alpha_i}}(\frac{1}{x^q - q}) = \omega_{P_{\alpha_i}}(\frac{1}{(x - \alpha_i)}) \stackrel{I.6.4}{=} 1$$

Como $Tr_{F'/F}(\frac{y - \beta_i}{x^q - x}) = \frac{1}{x^q - x}$, então

$$1 = \omega'_{P_i}(\frac{1}{x^q - x}) = \omega'_{Q_i}(\frac{y - \beta_i}{x^q - x}) + \omega'_{Q_{i+s}}(\frac{y - \beta_i}{x^q - x})$$

Se $\gamma = \frac{y - \beta_i}{x^q - x}$ e $\gamma' = \frac{y + \beta_i + 1}{x^q - x}$, então temos $v_{Q_i}(\gamma) \geq 0$ e $v_{Q_{i+s}}(\gamma') \geq 0$; logo, como $v_{Q_i}(\omega') = 0$, por I.6.3 que $\omega'_{Q_i}(\gamma) = 0 = \omega'_{Q_{i+s}}(\gamma')$ e assim, $1 = \omega_{P_i}(\frac{1}{x^q - x}) = \omega'_{Q_{i+s}}(\gamma)$. Como $\gamma = \frac{y + \beta_i + 1}{x^q - x} + \frac{1}{x^q - x} = \gamma' + \frac{1}{x^q - x}$, então

$$1 = \omega'_{Q_{i+s}}(\gamma) = \omega'_{Q_{i+s}}(\gamma') + \omega'_{Q_{i+s}}(\frac{1}{x^q - x}) = \omega'_{Q_{i+s}}(\frac{1}{x^q - x})$$

De 1. segue que

$$1 = \omega'_{Q_i}(\frac{1}{x^q - x})$$

Como $\eta = \frac{\omega'}{x^q - x}$, segue de 2. que:

$$\eta_{Q_i}(1) = \omega'_{Q_i}(\frac{1}{x^q - x}) = 1 = \omega'_{Q_{i+s}}(\frac{1}{x^q - x}) = \eta_{Q_{i+s}}(1)$$

III.3.2 Exemplo Dado $\mathbb{F}_q$ com $q = p^h$, p um primo arbitrário, considere o corpo de funções $F' = \mathbb{F}_q(x, y)$, onde $y^e = f(x)$. Assuma que:

- (a) $f(x) = q_1(x) \dots q_r(x)$, $q_i(x) \in \mathbb{F}_q[x]$ onde os $q_i(x)$ são irredutíveis e co-primos dois a dois; $\deg(q_i(x)) = m_i$ e $m = \deg(f(x)) = m_1 + \dots + m_r$.
- (b) $\text{mdc}(e, m) = 1$ e $q \equiv 1 \pmod{e}$.

Nestas condições, por III.1.14, $\varphi(T) = T - f(x) \in f[T]$ é irredutível, onde $F = \mathbb{F}_q(x)$, e portanto $[F' : F] = e$ e os lugares $P_\infty, P_i = (q_i(x))_0$ com $i = 1, \dots, r$ são totalmente ramificados. Mostra-se também que:

1. Se Q_∞/P_∞ , então $d(Q_\infty/P_\infty) = e - 1$.

Prova: Como Q_∞/P_∞ é totalmente ramificado, $e(Q_\infty/P_\infty) = e$; como $\text{char}(\mathbb{F}_q) = p$ e $q \equiv 1 \pmod{e}$, então $\text{mdc}(p, e) = 1$, ou seja, $\text{char}(\mathbb{F}_q) \nmid e(Q_\infty/P_\infty)$; logo, pelo Teorema do diferente de Dedekind, $d(Q_\infty/P_\infty) = e - 1$

2. Para cada $i = 1, \dots, r$ considere o lugar $Q_i/P_i = (q_i(x))_0$ de F' ; então como $e(Q_i/P_i) = e - 1$, novamente pelo Teorema de Dedekind, $d(Q_i/P_i) = e - 1$.

3. Se $P \in \mathbb{P}_F \setminus \{P_\infty, P_1, \dots, P_r\}$ e $Q \in \mathbb{P}_{F'}$ com Q/P , então $d(Q/P) = 0$.

Prova: P é tal que $v_P(f(x)) = 0$ e portanto, $\varphi(T) = T^e - f(x) \in \mathcal{O}_P[T]$. Logo, por III.2.23 temos $0 \leq d(Q/P) \leq v_Q(\varphi'(y))$. Observe que $e \cdot v_Q(y) = v_Q(f(x)) = e(Q/P) \cdot v_P(f(x)) = 0$; assim, $v_Q(\varphi'(y)) = v_Q(e) + (e - 1) \cdot v_Q(y) = 0$, pois por (b), $e \in \mathbb{F}_q$. Logo, $d(Q/P) = 0$.

De 1, 2 e 3 ,temos que: $Diff(F'/F) = (e-1)(Q_\infty + Q_1 + \dots + Q_r)$

Considerando $\omega \in \Omega_F$ com $(\omega) = -2P_\infty$ divisor canônico de F , seja $\omega' = Cotr_{F'/F}(\omega)$. Como

$$Con_{F'/F}(-2P_\infty) = -2e Q_\infty,$$

temos

$$(\omega') = Con_{F'/F}(\omega) + Diff(F'/F) = (e-1)(Q_1 + \dots + Q_r) - (e+1)Q_\infty.$$

Como (ω') é divisor canônico, já podemos calcular o gênero de F' :

$$\begin{aligned} 2g' - 2 &= deg((e-1)(Q_1 + \dots + Q_r) - (e+1)Q_\infty) \\ &= (e-1)(m_1 + \dots + m_r) - (e+1).1 \\ &= (e-1)m - (e+1) \\ g' &= \frac{m(e-1) - (e+1)}{2} \\ &= \frac{(e-1)(m-1)}{2}. \end{aligned}$$

Queremos achar os demais lugares de grau um de F' . Para isso, considere o conjunto

$$M = \{\alpha \in \mathbb{F}_q / f(\alpha) \neq 0 \text{ e } \exists \beta \in \mathbb{F}_q : \beta^e = f(\alpha)\}.$$

Para $\alpha \in M$, se $P_\alpha = (x - \alpha)$ sabemos que se Q/P_α , então $e(Q/P_\alpha) = 1$ (por III.2.24) e P_α tem e extensões distintas $Q_{\alpha i}/P_\alpha$ com $f(Q_{\alpha i}/P_\alpha) = 1$. Agora considere o conjunto $U \subseteq M$ com $|U| = s \geq 1$ e seja

$$\varphi(x) = \prod_{\alpha \in U} (x - \alpha)$$

Logo,

$$(1/\varphi(x)) = e.s Q_\infty - \sum_{\alpha \in U} \sum_{i=1}^e Q_{\alpha i} = e.s Q_\infty - (Q'_1 + \dots + Q'_{e.s}).$$

Note que

$$\begin{aligned} v_Q(y^e) &= v_Q(f(x)) = e(Q/P).v_P(f(x)) \\ &= \begin{cases} e.(-m) & , Q = Q_\infty \\ e.1 & , Q = Q_i, i = 1, \dots, r \\ 0 & , \text{ caso contrário} \end{cases} \end{aligned}$$

Logo,

$$(1/y^{e-1}) = (e-1)m Q_\infty - (e-1)(Q_1 + \dots + Q_r).$$

Considere o divisor canônico a seguir:

$$\begin{aligned} (\eta) = \left(\frac{\omega'}{y^{e-1}\varphi(x)} \right) &= (e-1)(Q_1 + \dots + Q_r) - (e+1)Q_\infty \\ &\quad - [(e-1)(Q_1 + \dots + Q_r) - (e-1)m Q_\infty] \\ &\quad - [(Q'_1 + \dots + Q'_{e.s}) - e.s Q_\infty] \\ &= [-(e+1) + (e-1).m + e.s]Q_\infty - [(Q'_1 + \dots + Q'_{e.s})] \\ &= [2g' - 2 + e.s]Q_\infty - [(Q'_1 + \dots + Q'_{e.s})] \\ &= [2g' - 2 + e.s]Q_\infty - D. \end{aligned}$$

Se $n = e.s$ é par, (basta tomar s par, ou se e for par esse cuidado é desnecessário), considerando $r = g' - 1 + \frac{n}{2}$ e $G = rQ_\infty$, obtemos que

$$(\eta) = 2G - D$$

Isso nos garante que $v_{Q'_i}(\eta) = -1$ e assim $\eta_{Q'_i}(1) = a_i \neq 0$. Pelo Teorema de aproximação existe $x \in F'$ tal que $v_{Q'_i}(z - a_i) > 0$; logo, $z(Q'_i) = a_i$ e assim se $\eta' = z^{-1}.\eta$

$$\eta'_{Q'_i}(1) = \eta_{Q'_i}(z^{-1}.1) = z^{-1}(Q'_i).\eta_{Q'_i}(1) = a_i^{-1}.a_i = 1$$

Se existir $u \in F'$ tal que $u^2 = z$, então considerando $G' = G - (u)$ obtemos o código auto-dual $C_L(D, G')$; se a característica de $\mathbb{F}_q$ for par esse elemento sempre existe (no exemplo anterior foi possível construí-lo). Caso contrário, obtemos, na melhor das hipóteses, um código auto-ortogonal, considerando $H \in \mathcal{D}_{F'}$ tal que $2H \leq (\eta') + D$. O código $C_L(D, H)$ é auto-ortogonal.

III.3.3 Exemplo Considere o corpo arbitrário finito $\mathbb{F}_q$ com $\text{char}(\mathbb{F}_q) = p$. Defina o corpo $F' = \mathbb{F}_q(x, y)$ pela equação:

$$h(y) = f(x) \quad \text{com} \quad h(y) \in \mathbb{F}_q[y], \quad f(x) \in \mathbb{F}_q[x].$$

Assuma também que:

1. $h(y)$ é o polinômio de grau p^ν dado por

$$h(y) = \sum_{i=0}^{\nu} c_i y^{p^i}, \quad c_i \in \mathbb{F}_q, \quad c_0 \neq 0, \quad c_\nu \neq 0$$

o qual é separável e se decompõe em fatores lineares em $\mathbb{F}_q$ e seus zeros formam um subgrupo aditivo de $\mathbb{F}_q$ de ordem p^ν .

2. $\deg(f(x)) = m \not\equiv 0 \pmod{p}$.

Usando III.1.14, com o lugar $P_\infty \in \mathbb{P}_F$ e $F = \mathbb{F}_q(x)$ prova-se que o polinômio

$$\varphi(T) = h(T) - f(x) \in F[T]$$

é irredutível sobre F , e que P_∞ é totalmente ramificado em F' : Q_∞/F_∞ com $e(Q_\infty/F_\infty) = p^\nu$ e $f(Q_\infty/F_\infty) = 1$. Para encontrar as demais extensões dos lugares de grau um de F , usamos o conjunto

$$M = \{\alpha \in \mathbb{F}_q / \exists \beta \in \mathbb{F}_q : h(\beta) = f(\alpha)\}.$$

Para cada $\alpha \in M$ o elemento $(x - \alpha)$ tem p^ν zeros distintos em F' . A seguir, apresentamos o cálculo do expoente diferente de cada lugar Q/P , $P \in \mathbb{P}_F$; pela Proposição III.2.29 temos que:

$$d(Q_\infty/P_\infty) = (p^\nu - 1)(m + 1)$$

e que todo $P \neq P_\infty$ é não-ramificado, i.e., $e(Q/P) = 1$ e por III.2.22, obte-se que

$$d(Q/P) = 0, \quad \forall Q/P, \quad P \in \mathbb{P}_F \setminus \{P_\infty\}.$$

Considere $-2P_\infty$ o divisor canônico de F , e seja $\eta \in \Omega_F$ o seu diferencial de Weil, i.e., $(\eta) = -2P_\infty$. Calculemos o divisor do cotraço de η :

$$\begin{aligned}
(\eta') &= \text{Con}(-2P_\infty) + \text{Diff}(F'/F) \\
&= -2e(Q_\infty/P_\infty)Q_\infty + d(Q_\infty/P_\infty) \\
&= [-2p^\nu + (p^\nu)(m+1)]Q_\infty \\
&= (p^\nu m - p^\nu - m - 1)Q_\infty.
\end{aligned}$$

Com isso, podemos calcular o gênero g' de F' , pois, $\deg((\eta')) = 2g' - 2$:

$$\begin{aligned}
2g' - 2 &= p^\nu m - p^\nu - m - 1 \\
g' &= 1/2(p^\nu m - p^\nu - m + 1) \\
g' &= \frac{(p^\nu - 1)(m - 1)}{2}.
\end{aligned}$$

Agora, prossigamos com a construção dos divisores D e G ; seja $U \subseteq M$, $|U| = s > 0$, e seja:

$$\varphi(x) = \prod_{\alpha \in U} (x - \alpha) = D - (p^\nu s)Q_\infty.$$

Queremos encontrar G tal que $2G - D$ seja canônico. Para isso, considere o diferencial de Weil ω de F' dado por:

$$\omega = \frac{\eta'}{\varphi(x)}.$$

Então,

$$\begin{aligned}
(\omega) &= (p^\nu m - p^\nu - m - 1)Q_\infty + p^\nu s Q_\infty - D \\
&= (2g' - 2 + p^\nu s)Q_\infty - D.
\end{aligned}$$

Desse modo, encontramos um diferencial tal $v_Q(\omega) = -1$ para $Q \in \text{supp}D$, o que garante que $\omega_Q(1) = a_i \neq 0$. Pelo Teorema de Aproximação podemos encontrar $z \in F'$ tal que $v_Q(z - a_i) > 0$ para cada $Q \in \text{supp}D$. O diferencial $\omega' = z^{-1}\omega$ satisfaz as condições desejadas: $v_Q(\omega') = -1$ e $\omega'_q(1) = 1$. Agora, se existir $u \in F'$ tal que $u^2 = z$, então, se $p^\nu \cdot s$ for par considerando $G = (g' - 1 + \frac{p^\nu \cdot s}{2})Q_\infty - (u)$, obtemos o código auto-dual $C_{\mathcal{L}}(D, G)$.

Se alguma dessas condições falhar, considerando H tal que $2H \leq (2g' - 2 + p^\nu \cdot s) - (z)$ obtemos um código auto-ortogonal $C_{\mathcal{L}}(D, H)$.

Apêndice

Extensões Integrais de Anéis

Para facilidade de referência apresentaremos neste apêndice os conceitos básicos, definições e resultados mais importantes (sem demonstrações) sobre os vários pontos da teoria geral de extensões integrais de anéis comutativos com identidade utilizados neste trabalho. Neste texto, sempre que falarmos em extensões de anéis, estamos nos referindo a extensões de anéis comutativos com identidade. As principais referências para este apêndice são [4] e [5].

Iniciamos lembrando que se S/K é uma extensão de anéis com K corpo, denotaremos por $[S : K]$ a dimensão do K -espaço vetorial S .

III.1 Definição Sejam S/R uma extensão de anéis e $y \in S$. Dizemos que y é *integral* (ou *inteiro*) sobre R se existe um polinômio mônico $f(x) \in R[X]$ tal que $f(y) = 0$ (i.e., y é raiz de $f(x)$).

Um primeiro resultado que caracteriza um elemento integral sobre um anel R é dado pela seguinte proposição :

III.2 Proposição *Dados uma extensão de anéis S/R e $y \in S$, as seguintes condições são equivalentes:*

1. y é integral sobre R .
2. O anel $R[y] = \{f(y); f(X) \in R[X]\}$ é um R -módulo finitamente gerado.
3. Existe um sub-anel B de S tal que $R \subseteq B$, B é R -módulo finitamente gerado e $y \in B$.

III.3 Observação Observe que quando R é um corpo o conceito de elemento integral sobre R é o mesmo que de elemento algébrico sobre R . Assim, todos os conceitos e resultados que descrevermos em termos de extensões integrais podem ser vistas no contexto de extensões algébricas de corpos.

Como consequência natural da Proposição III.2 podemos obter o seguinte resultado mais geral:

III.4 Proposição *Sejam S/R extensões de anéis e $y_1, \dots, y_n \in S$. Então $y_1, \dots, y_n$ são integrais sobre R se e só se o anel $R[y_1, \dots, y_n]$ é um R -módulo finitamente gerado.*

A partir desta proposição obtém-se que:

III.5 Corolário *Seja S/R uma extensão de anéis. Então:*

1. Se $y, z \in S$ são integrais sobre R , então $x \pm y$ e $x.y$ também são.
2. $ic_S(R) = \{y \in S; y \text{ é integral sobre } R\}$ é subanel de S .

O Corolário III.5 nos leva às definições:

III.6 Definição Seja S/R extensão de anéis; o anel $ic_S(R)$ é chamado *fecho integral de R em S* . Se R é domínio e $S = K$ é o corpo de frações de R , então, $ic_K(R)$ é chamado *fecho integral de R* . Se todo elemento de S é integral sobre R dizemos que S/R é uma *extensão integral*.

Uma propriedade fundamental a respeito de extensões integrais é dada pela seguinte proposição:

III.7 Proposição (transitividade) Se S/B e B/R são extensões integrais, então, S/R também é integral.

Uma relação entre extensões integrais e extensões algébricas de corpos pode ser vista no seguinte resultado:

III.8 Proposição Se S/R é uma extensão integral de anéis sendo S um domínio, então: S é corpo se e só se R é corpo e nesse caso S/R é extensão algébrica de corpo.

III.9 Definição Dado um domínio R , dizemos que R é integralmente fechado se $ic_K(R) = R$, onde K é o corpo de frações de R .

A seguir, apresentamos alguns exemplos de domínios integralmente fechados:

III.10 Exemplo Todo domínio fatorial é integralmente fechado. Em particular, os domínios principais são integralmente fechados, e portanto, os anéis de valorizações de corpos de funções algébricas são integralmente fechados.

III.11 Exemplo Se S é um domínio e $\mathcal{F}$ é uma família de subanéis de S que são integralmente fechados, então $B = \bigcap_{A \in \mathcal{F}} A$ é integralmente fechado. Em particular, os anéis de holomorfia de um corpo de funções (Definição III.2.2) são integralmente fechados.

Agora, estamos interessados em introduzir a função traço de uma extensão algébrica finita de corpos L/K . Para isto, considere $y \in L$ e $\{v_1, \dots, v_n\} \subseteq L$ uma K -base do espaço vetorial L . Considere agora a aplicação K -linear determinada por y e definida por:

$$\begin{aligned} m_y : L &\longrightarrow L \\ x &\longmapsto yx \end{aligned}$$

Como $\alpha = \{v_1, \dots, v_n\}$ é base de L , temos que para todo j , $1 \leq j \leq n$, $yv_j = \sum_{i=1}^n a_{ij}v_i$, $a_{ij} \in K$ e assim determinamos a matriz $a = (a_{ij})$, chamada de matriz de representação de m_y na base α e denotada por $[m_y]_\alpha$.

III.12 Definição Dados L/K uma extensão algébrica com $[L : K] = n$, $\alpha = \{v_1, \dots, v_n\} \subseteq L$ uma K -base de L e $y \in L$, definimos o traço de $y \in L$ em K por $Tr_{L/K}(y) = Tr[m_y]_\alpha = \sum_{i=1}^n a_{ii}$, onde $[m_y]_\alpha = (a_{ij}) \in M_n(K)$.

III.13 Observação Pela álgebra linear, sabemos que a definição da função traço não depende da escolha da base α .

As primeiras propriedades da função traço podem ser dadas no seguinte resultado:

III.14 Proposição Seja L/K uma extensão finita de corpo. Então a aplicação $Tr : L \longrightarrow K$ é um K -funcional linear que satisfaz: se $a \in K$, então $Tr_{L/K}(a) = na$, $n = [L : K]$.

Agora lembre que uma extensão algébrica de corpos L/K é dita separável se todo elemento $y \in L$ é separável sobre K , i.e., se o polinômio mínimo de y sobre K , $p_{y/K}(X)$, só tem raízes de multiplicidade um em algum fecho algébrico de K (e portanto em todo fecho algébrico $\bar{K}$ de K). Para extensões separáveis a aplicação traço tem propriedades fundamentais, que descrevemos em seguida:

III.15 Proposição *Seja L/K uma extensão de corpos separável e finita. Se $y \in L$ e $x_1, \dots, x_m$ são as raízes do polinômio mínimo de y sobre K num fecho algébrico de K , então temos $\text{Tr}_{L/K}(y) = s(x_1 + \dots + x_m)$, onde $s = [L : K(y)]$.*

III.16 Observação Nas condições acima, uma outra versão da Proposição III.15 pode ser vista da seguinte maneira. Se consideramos o conjunto

$$\text{Iso}_K(L, \bar{K}) = \{\sigma : L \longrightarrow \bar{K}, \sigma \text{ é um } K\text{-homomorfismo de } L \text{ num fecho algébrico } \bar{K} \text{ de } K\}$$

sabemos que: $\text{Iso}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$, onde $n = [L : K]$ e então $\text{Tr}_{L/K}(y) = \sum_{i=1}^n \sigma_i(y)$.

Na verdade pode-se provar que se L/K é extensão finita e separável então a forma bilinear φ definida (a partir do traço) por $\varphi(x, y) = \text{Tr}_{L/K}(x \cdot y)$, $x, y \in L$ é não-degenerada e então tem-se o seguinte resultado:

III.17 Proposição *Se L/K é uma extensão separável e finita de corpos e $\alpha = \{v_1, \dots, v_n\}$ é uma K -base de L , então existe uma outra K -base de L , $\beta = \{v_1^*, \dots, v_n^*\}$, tal que para quaisquer i, j com $1 \leq i, j \leq n$ tem-se $\text{Tr}(v_i \cdot v_j^*) = \delta_{ij}$, onde δ_{ij} é o símbolo de Kronecker. Neste caso dizemos que β é a base dual de α em relação ao traço.*

Na verdade, neste apêndice estamos especialmente interessados no estudo da seguinte situação:

(*) Seja R um domínio integralmente fechado, K seu corpo de frações e L/K uma extensão de corpos finita e separável. Considerando $R' = ic_L(R) = \{y \in L, y \text{ integral sobre } R\}$ o que podemos dizer de R' a partir de R em termos da aplicação traço e do próprio R .

Observando que se $\sigma : L \longrightarrow \bar{K}$ é um K -isomorfismo de L em $\bar{K}$ (um fecho algébrico de K) e $y \in R'$, então $\sigma(y) \in R'$ e podemos obter a partir da versão dada pela Observação III.16 para o traço que:

III.18 Lema *Na situação (*), se $y \in R'$, então $\text{Tr}_{L/K}(y) \in R$; mais ainda, $p_{y/K}(X) \in R[X]$, onde $p_{y/K}(X)$ é o polinômio minimal de y sobre K .*

Agora usando a definição de $ic_L(R)$ e os resultados III.17 e III.18 obtem-se o seguinte teorema geral:

III.19 Teorema *Sejam R um domínio integralmente fechado, K seu corpo de frações, L/K uma extensão de corpos finita e separável e $R' = ic_L(R)$. Então:*

1. L é o corpo de frações de R' e R' é integralmente fechado.
2. Se $\alpha = \{v_1, \dots, v_n\}$ é uma K -base de L , então existem $a_1, \dots, a_n \in R$ tal que $\alpha' = \{a_1 v_1, \dots, a_n v_n\} \subseteq R'$ e α' é K -base de L .
3. Se $\beta = \{u_1, \dots, u_n\}$ é uma K -base de L com $\beta \subseteq R'$, então $R' \subseteq Ru_1^* \oplus \dots \oplus Ru_n^*$, onde $\{u_1^*, \dots, u_n^*\}$ é base dual de β com relação ao traço (ver III.17).

III.20 Definição Se S/R é uma extensão de anéis tal que S é um R -módulo livre de posto n e $\alpha = \{v_1, \dots, v_n\} \subseteq S$ é uma R -base livre de S , então dizemos que α é uma base integral de S/R .

Para concluir, lembrando o teorema de módulos sobre domínios principais e usando a parte 3 do teorema III.19, obtemos o seguinte resultado fundamental:

III.21 Corolário *Se no Teorema III.19 supormos que R é domínio principal, então, R' é um R -módulo livre de posto n , onde $n = [L : K]$ e portanto R'/R admite uma base integral.*

Bibliografia

- [1] Goppa, V. D.: Algebraico-geometric codes. Math. USSR-Izv. 21 (1)(1983) 75-91
- [2] Hefez, A.: Introdução à Teoria dos Códigos, XIII Escola de Álgebra, 1994.
- [3] Lint, J. H.: Introduction to Coding Theory and Algebraic Geometry. (DMV Seminar, vol. 12.) Birkhaeuser, Basel-Boston-Berlin, 1988.
- [4] Lang, S.: Algebra. Addison Wesley, Reading, Massachusetts, 1965.
- [5] Samuel, P.: Algebraic Theorie of Numbers. Kershaw Publ. Co. 1972 (tradução original do francês Théorie Algébrique des Nombres. Hermann Paris 1967).
- [6] Stichtenoth, H.: Algebraic Function Fields and Codes. (Universitext) Springer-Verlag, 1993.
- [7] Stichtenoth, H.: Self-Dual Goppa Codes, Journal of Pure and Applied Algebra 55 (1988)199-211, North-Holland.