UNIVERSIDADE ESTADUAL DE CAMPINAS

Tese de Mestrado

Lacunas de Weierstrass e Códigos de Goppa

Diogo Robles

16 de Outubro de 1997

Lacunas de Weierstrass e Códigos de Goppa

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pelo Sr. Diogo Robles e aprovada pela comissão julgadora.

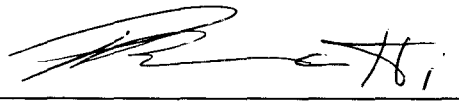
Campinas, 16 de Outubro de 1996

Prof.Dr. Paulo Roberto Brumatti

Dissertação apresentada no Instituto de Matemática, Estátistica e Computação Científica, Unicamp; como requisito parcial para a obtenção do título de Mestre em Matemática.

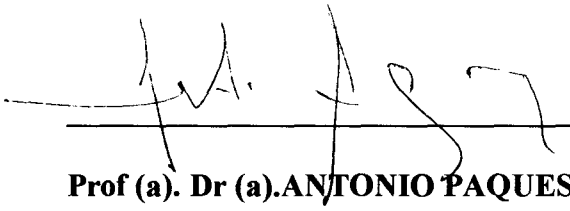
Dissertação de Mestrado defendida e aprovada em 16 de outubro de 1997

pela Banca Examinadora composta pelos Profs. Drs.



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

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



Prof (a). Dr (a).ANTONIO PAQUES

"... minha sabedoria, talvez
resume-se apenas
no conhecimento
de minha ignorância ..."

Aos meus pais,
Gertrudes e Fernando
por tudo.

Agradecimentos

agradecimento. *S.m.***1.** Ato ou efeito de agradecer, mostrar-se grato. **2.** Gratidão, reconhecimento. **3.** Retribuir, recompensar...

Quero agradecer ...

à minha família : Fernando, Gertrudes, Elizabete, Tânia, Rafael, Raquel e Luis pelo apoio incondicional e pela força espiritual,

ao meu orientador Prof. Paulo Roberto Brumatti pela ajuda e motivação,

aos companheiros de república Clevan, Eduardo, Daniel, Escobar, Edson, Júnior e Bina,

à Ximena, Claudio, Ryuichi e a todos os amigos do "predinho"

e ao CNPQ, pela motivação financeira

... e reconhecer que sem eles o caminho seria muito mais difícil .

Índice

Introdução

Um código linear de comprimento n e dimensão k é um subespaço vetorial de dimensão k de $\mathbb{F}_q{}^n$, onde $\mathbb{F}_q$ denota o corpo finito com q elementos. A distância mínima de um código é o número mínimo de lugares em que duas palavras distintas do código diferem.

Neste texto estaremos interessados em um tipo especial de código linear, os códigos de Goppa e no conceito de Lacunas de Weierstrass, estas podendo ser utéis para se estimar a distância mínima destes códigos.

A teoria de códigos possui várias ramificações que utilizam conceitos matemáticos bastantes diversos, como por exemplo, Teoria dos Números, Teoria dos Grupos, Combinatória, Geometrias Finitas e Geometria Algébrica. Os Códigos Geométricos ou códigos de Goppa como são mais conhecidos, combinam Geometria Algébrica e Teoria de Códigos. Este caráter interdisciplinar, que faz isto tão bonito, foi proposto, inicialmente, por *V.D.Goppa* no artigo *Codes associated with divisor- Problems of Information Transmission, 1977* .

A principal ferramenta, para esta combinação tão bem sucedida, são os Corpos de Funções Algébricas F sobre um corpo K, que são , extensões algébricas de grau finito sobre o corpo de Funções Racionais $K(x)$. Os corpos de funções algébricas podem ser estudados de diferentes pontos de vista, mas nossa idéia aqui é dar uma exposição puramente algébrica dos mesmos. Seguindo os passos de [4] começamos, no Capítulo 1, apresentando as definições e os principais resultados sobre Corpos de Funções, que servirão de base para este trabalho. Ainda neste capítulo obteremos o *teorema de Riemann-Roch* objeto básico para estimarmos os parâmetros dos códigos geométricos, básicos também para a obtenção das *lacunas de Weierstrass*, que definimos e apresentamos as principais propriedades no final do capítulo.

Utilizando os divisores de um corpo de funções e o teorema de Riemann-Roch, definimos no Capítulo 2 os códigos de Goppa. Utilizando o corpo de funções racionais $\mathbb{F}_q(x)/\mathbb{F}_q$ apresentamos alguns exemplos dos códigos de Goppa.

Estes códigos geometricos que a partir dos trabalhos de V.D.Goppa, tem encontrado vários adeptos nos meios acadêmicos, possuem "bons" parâmetros e em particular estaremos interessados em encontrar cotas inferiores para a distância mínima. Para isso, seguindo os passos de [2], apresentamos no Capítulo 3, os teoremas principais que mostram como as lacunas de Weierstrass podem ser de grande utilidade no cálculo da distância mínima dos códigos de Goppa .

Apresentamos uma aplicação dos resultados aquí obtidos para uma classe dos códigos de Goppa baseados em curvas Hermitianas, introduzidas por H.Stichtenoth [5].

Gostariamos de mencionar que o estudo básico sobre corpos de funções e códigos de Goppa foi baseado no excelente texto [4]. O estudo relativo às lacunas, para se melhorar os parâmetros de certos códigos de Goppa, foi baseado em [2] .

Campinas, outubro de 1997.

Capítulo 1

Sobre Corpo de Funções Algébricas e o Teorema de Riemann - Roch

1.1 Corpo de Funções e Lugares

Definição 1.1.1 *Um* **corpo de funções algébricas F/K em uma variável sobre K** *(corpo arbitrário) é uma extensão de corpos $K \subseteq F$ tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ transcendente sobre K.*

Observação 1.1.2 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 $K \subset \tilde{K} \subset F$, 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 $\tilde{K} = K$.

Observação 1.1.3 Os elementos de F que são transcendentes sobre K podem ser caracterizados por: $z \in F$ é transcendente sobre K se e somente se $[F : K(z)] < \infty$.

Exemplo 1.1.4 Um exemplo simples de um corpo de funções é o *corpo de funções racionais*; F/K é chamado *racional* se $F = K(x)$ para algum $x \in F$ transcendente sobre K. Qualquer elemento $0 \neq z \in K(x)$ possui uma representação única

$$z = a.\prod_i p_i(x)^{n_i}, \tag{1.1}$$

onde $0 \neq a \in K$, $p_i(x) \in K[x]$ são mônicos, irredutíveis, distintos dois a dois, $i \in \{0, 1, \ldots, n\}$ e $n_i \in \mathcal{Z}$.

Observação 1.1.5 Um corpo de funções arbitrário F/K (não necessariamente racional) é representado em geral como uma extensão (de corpos) algébrica simples de um corpo de funções racionais $K(x)$, isto é , $F = K(x, y)$ onde $\varphi(y) = 0$ para algum polinômio irredutível $\varphi(T) \in K(x)[T]$.

Se F/K é um corpo de funções não racional, não é tão claro, que qualquer elemento $0 \neq z \in F$ admite uma decomposição em irredutíveis análoga à equação (1.1); de fato, nem mesmo sabemos o que é um elemento irredutível de F.

Outro problema relacionado com a representação (1.1) é o seguinte: dados os elementos $\alpha_1, \ldots, \alpha_n \in K$, achar todas as funções racionais $f(x) \in K(x)$ com um número predeterminado de zeros (ou polos) em $\alpha_1, \ldots, \alpha_n$. A fim de formular esses problemas adequadamente, para corpos de funções arbitrários, vamos introduzir as noções de anel de valorização e de lugar.

Definição 1.1.6 *Um* **anel de valorização** *do corpo de funções F/K é um anel $O \subset F$ com as seguintes propriedades:*

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

Observação 1.1.7 Esta definição é motivada pela seguinte observação no caso de um corpo de funções racionais $K(x)$: dado um polinômio irredutível $p(x) \in K[x]$, considere o conjunto:

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

Temos que $O_{p(x)}$ é anel de valorização de $K(x)/K$.[1] Note que se $q(x)$ é um outro polinômio irredutível, então $O_{p(x)} \neq O_{q(x)}$.

A próxima proposição tem uma demonstração bastante simples e deixaremos de apresentá-la aqui.

Proposição 1.1.8 *Seja O um anel de valorização do corpo de funções F/K. Então:*

(a) *O é um anel local, i.e., O possui um único ideal maximal $P = O \backslash O^*$, onde*

$$O^* = \{z \in O \mid \exists w \in O;\ z.w = 1\}$$

é o grupo das unidades de O.

(b) *Para $0 \neq x \in F$, $x \in P \iff x^{-1} \notin O$.*

(c) *Para o corpo $\tilde{K}$ das constantes de F/K temos $\tilde{K} \subseteq O$ e $\tilde{K} \cap P = \{0\}$.*

O Lema abaixo é essencial na demonstração do próximo Teorema.

Lema 1.1.9 *Seja O um anel de valorização do corpo de funções algébricas F/K, P seu ideal maximal e $0 \neq x \in P$. Se $x_1, x_2, \ldots, x_n \in P$ são tais que $x_1 = x$ e $x_i \in x_{i+1}P$ para $i = 1, 2, \ldots, n-1$ então, temos $n \leq [F : K(x)] < \infty$.*

Dem. :
Dos resultados (1.1.3) e (1.1.8.(c)), segue que $[F : K(x)] < \infty$. Para que $n \leq [F : K(x)]$ basta mostrar que $\{x_1, x_2, \ldots, x_n\}$ são linearmente independentes sobre $K(x)$. Suponha que $\sum_i \varphi_i . x_i = 0$, 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 estamos num domínio de integridade, então, podemos supor que $\varphi_i \in K[x], \forall i = 1, 2, \ldots, n$ e que x não divide todos eles. Seja $a_i = \varphi_i(0)$ e defina $j \in \{1, 2, \ldots, n\}$ tal que $a_j \neq 0$ e $a_i = 0\ \forall i > j$. Assim, $x/\varphi_i, \forall i > j$. Então, obtemos:

---

[1]

- $K \subsetneq O$: tome $\alpha \in K$, $\alpha = \frac{\alpha}{1} \Longrightarrow \alpha \in O_{p(x)}$; tome $\gamma = \frac{1}{p(x)+1}$; como $p(x) \not| p(x)+1$, então $\gamma \in O_{p(x)} \backslash K$.
- $O_{p(x)} \subsetneq F = K(x)$: $\frac{1}{p(x)} \in K(x) \backslash O_{p(x)}$.
- $\forall\, z \in F,\ z \in O_{p(x)}$ ou $z^{-1} \in O_{p(x)}$: tome $z \in F$, então $z = \frac{f(x)}{g(x)}$ onde $f(x) = p(x)^m \bar{f}(x)$, $g(x) = p(x)^n \bar{g}(x)$ com $p(x) \not| \bar{f}(x)$, $\bar{g}(x)$;logo $z = p(x)^{m-n} \frac{\bar{f}(x)}{\bar{g}(x)}$, então
  - se $m - n \geq 0 \Longrightarrow z \in O_{p(x)}$.
  - se $m - n > 0 \Longrightarrow z^{-1} \in O_{p(x)}$.

$$-\varphi_j x_j = \sum_{i \neq j} \varphi_i x_i \tag{1.2}$$

Como $x = x_1 \in P$ temos $\varphi_i \in O$, $\forall i = 1, 2, \ldots, n$; $x_i \in x_j P$, $i < j$ e $\varphi_i = x h_i$, $i > j$ onde $h_i(x) \in K[x]$, dividindo a equação(1.2) 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 $g_j \in K[x] \subseteq O$ e $x \in P$, logo

$$a_j = \varphi_j - x.g_j \in P \cap K = \{0\}$$

por (1.1.8), então $a_j = 0$, contradição. Portanto, os $\varphi_i = 0$ e os $\{x_1, x_2, \ldots, x_n\}$ são l.i. logo $n \leq [F : K(x)]$

□

Teorema 1.1.10 *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 $P = tO$ então qualquer $0 \neq z \in F$ 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 $P = tO$ e $\{0\} \neq I \subseteq O$ é um ideal, então $I = t^n O$ para algum $n \in \mathbb{N}$.*

Dem. :

(a) Suponha que P não seja principal e escolha $0 \neq x_1 \in P$. Logo $x_1 O \subsetneq P$ e assim existe $0 \neq x_2 \in P \backslash x_1 O$. Logo $x_2 \notin x_1 O$ isto é $x_2.x_1^{-1} \notin O$, por (1.1.8) $x_2^{-1}.x_1 \in P$, ou seja, $x_1 \in x_2 P$. De maneira análoga existe $x_3 \in P \backslash x_2 O$, então $x_3 x_2^{-1} \notin O$, ou seja, $x_3^{-1} x_2 \in P$ logo $x_2 \in x_3 P$; continuando por indução obteremos uma sequência infinita

$$x_1, x_2, x_3, \ldots \in P \backslash \{0\}$$

tal que $x_i \in x_{i+1} P$ para todo i, o que é um absurdo por (1.1.9).

(b) Como para qualquer $z \in F$,

$$z \in O \ \ ou \ \ z^{-1} \in O \ ,$$

basta tomar em cada caso :

$$m = max\{k |\ z \in t^k O \ (ou\ z^{-1} \in t^k O)\ \} \ .$$

(c) É obvio a partir de **(b)** .

□

Definição 1.1.11 (a) *Um* **lugar** *P de F/K é o ideal maximal de um anel de valorização O de F/K.*

(b) *Se $t \in P$, P um lugar de F/K e P é gerado por* **t** *então dizemos que t é* **elemento primo** *de P.*

(c) $\mathbb{P}_F = \{P |\ P$ *é um lugar de* $F/K\}$.

Se O é um anel de valorização de F/K e P um ideal maximal, então O é unicamente determinado por P.[2] Utilizamos a notação O_P para identificar o anel de valorização do lugar P. Uma segunda descrição de lugares é dada através de valorização , para mostrar isto comecemos com a seguinte definição.

Definição 1.1.12 *Uma* **valorização discreta de F/K** *é uma função $v : F \to \mathcal{Z} \cup \{\infty\}$ com as seguintes propriedades:*

1. $v(x) = \infty \iff x = 0$.
2. $v(xy) = v(x) + v(y), \forall x, y \in F$.
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. $v(a) = 0, \forall\ 0 \neq a \in K$.

Observação 1.1.13 Neste contexto, o símbolo ∞ se refere a um elemento não pertencente a $\mathcal{Z}$.[3] De (2) e (4) segue que v é sobrejetiva. A propriedade (3) é chamada *Desigualdade Triangular.*

O seguinte resultado é conhecido como **Desigualdade Triangular Estrita** e tem uma prova bastante simples, que omitimos aqui.

Lema 1.1.14 *Seja v uma valorização discreta de F/K e $x, y \in F$ com $v(x) \neq v(y)$. Então*

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

Definição 1.1.15 *Para qualquer lugar $P \in \mathbb{P}_F$ podemos associar uma função $v_P : F \to \mathcal{Z} \cup \{\infty\}$ dada por: escolha t elemento primo de P; então todo $0 \neq z \in F$ possui uma representação da forma*

$$z = t^n u,\ u \in O_P^*,\ n \in \mathcal{Z}\ .$$

Defina $v_P(z) = n$ e $v_P(0) = \infty$.

Esta definição depende somente de P e não da escolha de t .[4]
O nosso próximo resultado mostra que v_P é uma valorização discreta.

Teorema 1.1.16 *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:*

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

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

[2] De fato, conforme Proposição (1.1.8) $O = \{z \in F | z^{-1} \notin P\}$.
[3] Tal que $\infty + \infty = \infty + n = n + \infty = \infty\ e\ \infty > m;\ \forall\ m, n \in \mathcal{Z}$.
[4] De fato , se s é outro elemento primo de P, então $P = tO = sO$; logo, $t = sw$, *com* $w \in O_P^*$. Portanto, $t^n u = (s^n w^n)u = s^n(w^n u)$, *com* $w^n u \in O^*$.

(b) *Reciprocamente, suponha que v é uma valorização discreta de F/K. Então o conjunto*

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

é um lugar de F/K e

$$O_P = \{z \in F |\ v_P(z) \geq 0\}$$

é o anel de valorização correspondente.

(c) *Qualquer anel de valorização O de F/K é subanel próprio maximal de F.*

Dem. :

As provas de **(a)** e **(b)** são triviais e omitimos aqui.

(c) Seja O um anel de valorização de F/K, P um ideal maximal de O, v_P a valorização discreta associada a P e $z \in F \backslash O$. Mostraremos que $F = O[z]$; para isto, tomemos $\forall\ y \in F$, desde que $z \notin O$ temos $v_P(z^{-1}) > 0$. Logo $v_P(yz^{-k}) \geq 0$, $k \in I\!N$ suficientemente grande. Então , $w = y.z^{-1} \in O$, isto é, $y = w.z^k \in O[z]$.

□

De acordo com o Teorema (1.1.16), um lugar, um anel de valorização e uma valorização discreta são essencialmente a mesma coisa.

Observação 1.1.17 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 $x \in F \backslash O_P$ definimos $v(x) = \infty$ (note que o símbolo ∞ tem aqui um significado distinto daquele na definição(1.1.12)). Pela proposição(1.1.8) sabemos que $K \subseteq O_P$ e $K \cap P = \{0\}$, de modo que a aplicação $O_P \to O_P/P$ 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.

Definição 1.1.18 *Seja $P \in I\!P_F$*

(a) *$F_P = O_P/P$ é o* **corpo de resíduos do lugar P**. *A aplicação $x \longmapsto x(P)$ de F em $F_P \cup \{\infty\}$ é chamada aplicação de classes residuais com relação a P.*[5]

(b) *$[F_P : K]$ é chamado* **grau de P** *e é denotado por deg P.*

O grau de um lugar é sempre finito, para ser mais preciso vale o seguinte.

Proposição 1.1.19 *Se P é um lugar de F/K e $0 \neq x \in P$, então deg $P \leq [F : K(x)] < \infty$.*

Dem. :
Por (1.1.3) temos $[F : K(x)] < \infty$. Agora basta mostrar que $\forall\ z_1, z_2, \ldots, z_n \in O_P$, cujas classes residuais $z_1(P), z_2(P), \ldots, z_n(P) \in F_P$ [6] são l.i. sobre K, são l.i. sobre $K(x)$. Suponha que exista uma combinação linear não trivial

$$\sum_{i=1}^{n} \varphi_i z_i = 0 \tag{1.3}$$

[5] Também usaremos a notação $x + P = x(P)$ para $x \in O_P$.
[6] Onde $z_i(P) = z_i + P, \forall i = 1, 2, \ldots, n$.

com $\varphi_i \in K(x)$. Podemos supor que os φ_i são polinômios em x (isto é, $\varphi_i \in K[x]$) e não todos divisíveis por x, i.e., $\varphi_j = a_j + x.g_j$,com $a_j \in K, g_j \in K[x]$ e $a_j \neq 0$ para algum $j \in \{1,2,\ldots,n\}$ e portanto $\varphi_j \equiv a_j \ mod\ P$. Assim empregando a aplicação residual módulo P em (1.3) temos:

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

Como os $z_i(P)$ são l.i. sobre K, temos $a_i = 0\ \forall i$, o que é uma contradição. Logo, os z_i são l.i. sobre $K(x)$.

□

Corolário 1.1.20 *O corpo $\tilde{K}$ das constantes de F/K é uma extensão de corpo finita sobre K.*

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

□

Observação 1.1.21 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 algébricamente fechado, qualquer lugar tem grau um, de modo que podemos ver um elemento $z \in F$ como uma função

$$z : \begin{array}{ccc} \mathbb{P}_F & \longrightarrow & K \cup \{\infty\} \\ P & \longmapsto & z(P) \ . \end{array} \tag{1.4}$$

Por isso F/K é chamado **corpo de funções**. Os elementos de K, interpretados como funções no sentido de (1.4), são funções constantes. Por essa razão K é chamado **corpo constante** de F.

Definição 1.1.22 *Seja $z \in F$ e $P \in \mathbb{P}_F$.*

(a) Dizemos que P **é um zero de** z *se e so se $m = v_P(z) > 0$, e neste caso diz-se que P é um* **zero de ordem m de z** .

(b) Dizemos que P **é um polo de** z *se e so se $-m = v_P(z) < 0$, e neste caso diz-se que P é um* **polo de z de ordem m**.

A seguir estaremos preocupados em provar a existência de lugares em F/K.

Teorema 1.1.23 *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 $R \subseteq O_P$.*

Dem. :
Considere o conjunto $\mathcal{F} = \{S |\ S$ é subanel de F com $R \subseteq S$ e $IS \neq S\}$ onde

$$IS = \{ \sum_{finita} a_\nu.s_\nu |\ a_\nu \in I,\ s_\nu \in S\}$$

é um ideal de S.

Afirmamos que $\mathcal{F}$ é não vazio, pois $R \in \mathcal{F}$ e é indutivamente ordenado pela inclusão.
De fato, seja $\mathcal{H} \subseteq \mathcal{F}$ um subconjunto totalmente ordenado; então,

1. $T = \cup\{S | S \in \mathcal{H}\}$ é um subanel de F com $R \subseteq T$; pois, $R \subseteq S$, $\forall\ S \in \mathcal{F}$.

2. $IT \neq T$; de fato, suponhamos $IT = T$; como $1 \in T$ existe $a_i \in I$, $s_i \in T$ tais que

$$\sum_{i=1}^{n} a_i s_i = 1 .$$

Como $\mathcal{H}$ é totalmente ordenado, existe $S_0 \in \mathcal{H}$ tal que $s_1, s_2, \ldots, s_n \in S_0$, logo

$$1 = \sum_{i=1}^{n} a_i . s_i \in IS_0$$

absurdo. Assim $IT \neq T$ e 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 $O \subsetneq F$ tal que $R \subseteq O \subsetneq F$, $IO \neq O$ e O é maximal com essas propriedades, isto é :

$$\begin{cases} Se\ A \in \mathcal{F}, com\ O \subseteq A \subseteq F \text{ então } O = A; \text{ ou} \\ se\ O \subsetneq B \subset F \text{ então } IB = B. \end{cases}$$

Afirmação : O é anel de valorização de F/K. Pois como $I \neq \{0\}$ e $IO \neq O$, tem-se $I \subseteq O \backslash O^*$. 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 em $\mathcal{F}$, tem-se $O[z]$, $O[z^{-1}] \notin \mathcal{F}$, isto é, $IO[z] = O[z]$ e $IO[z^{-1}] = O[z^{-1}]$, ou seja, existem $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in IO$ tais que :

$$1 = a_0 + a_1 z + \ldots + a_n z^n \tag{1.5}$$

$$1 = b_0 + b_1 z^{-1} + \ldots + b_n z^{-m} \tag{1.6}$$

Como $IO \neq O$, tem-se $a_0 \neq 1$ e $b_0 \neq 1$. Tomemos as expressões (1.5) e (1.6) com m, n minimais e suponhamos $n \geq m \geq 1$. Mutiplicando (1.5) por $(1 - b_0)$ e (1.6) por $a_n z^n$ obtemos:

$$(1 - b_0) = (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n \tag{1.7}$$

$$0 = (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m} \tag{1.8}$$

Somando as equações (1.7) e (1.8) chegamos à equação:

$$1 = \underbrace{((1 - b_0)a_0 + b_0)}_{c_0} + \cdots + \underbrace{((1 - b - 0)a_{n-1} + b_1 a_n)}_{c_{n-1}} z^{n-1} + \underbrace{((1 - b_0)a_n + (b_0 - 1)a_n)}_{c_n} z^n$$

Notamos que os $c_i \in IO$, $i \in \{0, 1, \ldots, n\}$ e $c_n = (1 - b_0)a_n + (b_0 - 1)a_n) = 0$.
Assim, $1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1} \in O[z]$, contradizendo a escolha de n em (1.5). Portanto O é um anel de valorização. Basta então tomarmos o ideal maximal $P \subset O$, logo um lugar, onde $I \subseteq P$ e $R \subseteq O_P$.

□

Corolário 1.1.24 *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, $\mathbb{P}_F \neq \emptyset$.*

Dem. :
Consideramos o anel $R = K[z]$ e o ideal $I = zK[z]$. Pelo Teorema (1.1.23) há um lugar $P \in \mathbb{P}_F$, *com* $z \in P$. Logo, P é um zero de z. Analogamente, para z^{-1}, há um lugar $Q \in \mathbb{P}_F$,com $z^{-1} \in Q$. Logo, Q é um polo de z. Em particular,$\mathbb{P}_F \neq \emptyset$, pois P, $Q \in \mathbb{P}_F$.

□

O corolário (1.1.24) pode ser interpretado como segue: Dado $z \in F$,tal que $z \notin \tilde{K}$ de F/K, então z fornece uma função não constante no sentido de (1.1.21).

Para um melhor entendimento de valorização e lugares de um corpo de funções arbitrário damos, no **Apêndice A**, uma idéia precisa destas noções no caso particular de um corpo de funções racional.

1.2 Independência de Valorizações

O principal resultado desta seção é o Teorema (1.2.1) da Aproximação Forma Fraca (que também é conhecido por Teorema de Independência) . Este Teorema desempenha um papel significativo na nossa teoria e principalmente nos resultados desta seção.

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

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

Dem. :
Para simplificar, denotemos $v_i = v_{P_i}$. A demonstração deste teorema é construtiva e por isso à dividimos em vários passos:

Passo 1: Existe $u \in F$ t.q. $v_1(u) > 0$ e $v_i(u) < 0$, $i = 2,\ldots,n$.

De fato, por indução, tomemos $n = 2$; como os anéis de valorização são maximais,[7] temos que $O_{P_1} \not\subset O_{P_2}$ e $O_{P_2} \not\subset O_{P_1}$. Logo, podemos tomar $y_1 \in O_{P_1}\backslash O_{P_2}$ e $y_2 \in O_{P_2}\backslash O_{P_1}$.
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

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

Suponha $n > 2$ e tome, por indução, $y \in F$, tal que:

$$v_1(y) > 0, \; e \; v_i(u) < 0, \text{ para } i = 2,\ldots,n-1. \tag{1.9}$$

- se $v_n(y) < 0$, acabou, tomamos $u = y$.
- suponhamos então que $v_n(y) \geq 0$. Pelo caso $n = 2$, existe

$$z \in F, \; v_1(z) > 0 \; e \; v_n(z) < 0. \tag{1.10}$$

Considere os elementos u da forma $u = y + z^r$, $r \in \mathbb{N}$, tomemos r suficientemente grande tal que $rv_i(z) \neq v_i(y)$, logo por (1.1.14) temos $v_i(u) = min\{v_i(y),\, rv_i(z)\}$. Assim, de (1.9) e (1.10) temos
$i = 1$, $v_1(u) = min\{v_1(y),\, rv_1(z)\} > 0$
$i = 2,\ldots,n$, $v_i(u) = min\{v_i(y),\, rv_i(z)\} < 0$.

Passo 2: Existe $w \in F$ t. q. $v_1(w-1) > r_1$ e $v_i(w) > r_i$, $i = 2,\ldots,n$.

De fato, escolha u como no Passo 1 e tome $w = (1+u^s)^{-1}$ com $s \in \mathbb{N}$. $w - 1 = \frac{1}{1+u^s} - 1 = -u^s.(1+u^s)^{-1}$, logo

$$v_1(w-1) = sv_1(u) - v_1(1+u^s) = sv_1(u).^8$$

Portanto, para s suficientemente grande, $v_1(w-1) > r_1$ e $v_i(w) = -min\{v_i(1), s.v_i(u)\} > r_i$ pois, pelo passo 1, $v_i(u) < 0$ para $i = 2,\ldots,n$.

[7] Teorema (1.1.16).

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

De fato, tomemos $s \in \mathcal{Z}$ tal que $v_i(y_j) \geq s$ para todo i, $j \in \{1, \ldots, n\}$. Basta tomarmos $s = min\{v_i(y_j) \mid i, j \in \{1, \ldots, n\}\}$. Pelo Passo 2, existem $w_1, \ldots, w_n \in F$ t. q. $v_i(w_i - 1) > r_i - s$ e $v_j(w_i) > r_j - s$ para $j \neq i$. Considerando $z = \sum_{j=1}^{n} y_j . w_j$ temos :

$$z - y_i = \sum_{j=1_{j \neq I}}^{n} y_j . w_j + y_i(w_i - 1) \text{ logo}$$

$$\begin{array}{lllll} v_i(y_j w_j) & \geq & s + v_i(w_j) & > & s + r_i - s = r_i \\ v_i(y_i(w_i - 1)) & \geq & s + v_i(w_i - 1) & > & r_i. \end{array}$$

Portanto $v_i(z - y_i) > r_i$ para $i \in \{1, \ldots, n\}$.

Prova do Teorema Dados $x_1, \ldots, x_n \in F$, e $r_1, \ldots, r_n \in \mathcal{Z}$, pelo Passo 3, existe $z \in F$ tal que $v_i(z - x_i) > r_i$, para $i = 1, \ldots, n$. A seguir, escolhemos $z_i \in F$ tal que $v_i(z_i) = r_i$ (se $t_i \in O_P$ é elemento primo de O_P, tomamos $z_i = t_i^{r_i}$). Para $z_1, \ldots, z_n \in F$, ainda pelo Passo 3, existe $z' \in F$ tal que $v_i(z' - z_i) > r_i$ para $i = 1, \ldots, n$. Segue que:

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

Agora, tomemos $x = z + z'$:

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

□

Através deste Teorema obtemos o seguinte Corolário.

Corolário 1.2.2 *Todo corpo de funções possui infinitos lugares.*

Dem. :
Suponhamos que $\mathbb{P}_F = \{P_1, \ldots, P_n\}$. Tome $x_1 = \cdots = x_n = 0$ e $r_1, \ldots, r_n \in \mathcal{Z}$, com $r_i > 0$, $i = 1, \ldots, n$. Pelo Teorema (1.2.1) existe $0 \neq x \in F$ t.q. $v_{P_i}(x) > 0$ para $i = 1, \ldots, n$, ou seja, para todo $P_i \in \mathbb{P}_F$, temos que P_i é zero de x. Logo por (1.1.8) x é transcendente sobre K. Então x é transcendente sobre K e não tem polos. O que é um absurdo pois, pelo corolário (1.1.24) todo transcendente sobre K tem pelo menos um polo e um zero. □

Na seção (1.4) mostraremos que um elemento $0 \neq x \in F$, transcendente sobre K, tem o mesmo numero de zeros e polos, desde que estes sejam contados de maneira conveniente. A nossa próxima proposição é um importante passo para a prova deste resultado.

Proposição 1.2.3 *Seja F/K um corpo de funções e $P_i, \ldots, P_r \in \mathbb{P}_F$ zeros de $x \in F$. Então:*

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

Dem. :
Simplificaremos a notação denotando: $v_i = v_{P_i}$, $f_i = deg\ P_i = [F_{P_i} : K]$ e $e_i = v_{P_i}(x)$.

1. Para cada $i \in \{1,\ldots,r\}$, existe $t_i \in F$, com $v_i(t_i) = 1$ e $v_k(t_i) = 0$ para $k \neq i$.

   De fato, fixado i, tome no teorema (1.2.1) $x_n = 0$, $n = 1,\ldots,r$; $r_i = 1$ e $r_n = 0$ para $n \neq i$. Assim existe $t_i \in F$ tal que $v_n(t_i - x_n) = r_n$ para $n = 1,\ldots,r$; isto é

$$v_n(t_i) = \begin{cases} v_i(t_i) = 1 & , \ n = i \\ v_n(t_i) = 0 & , \ n \neq i \end{cases} \tag{1.11}$$

   Agora escolhemos, para cada i fixo, $s_{i1},\ldots,s_{if_i} \in O_{P_i}$ tais que $s_{i1}(P_i),\ldots,s_{if_i}(P_i) \in F_{P_i}$ sejam *l.i.* sobre K. Tomando no Teorema (1.2.1) $r_n = e_n > 0$ para $n = 1,\ldots,r$;[9] $x_i = s_{ij}$ e $x_n = 0$ para $n \neq i$ com $j \in \{1,\ldots,f_i\}$. Então existe $z_{ij} \in F$ para cada i fixo e $1 \leq j \leq f_i$ tais que :

$$v_i(z_{ij} - s_{ij}) = e_i > 0 \text{ e } v_n(z_{ij}) = e_n > 0. \tag{1.12}$$

2. **Afirmação**. Os elementos $t_i^a z_{ij} \in F$ para $i = 1,\ldots,r$; $1 \leq j \leq f_i$ e $0 \leq a < e_i$ são *l.i.* sobre $K(x)$.

Logo, fazendo a contagem destes elementos obtemos $\sum_{i=1}^{r} e_i f_i = \sum_{i=1}^{r} v_i(x) deg\ P_i$ elementos de F linearmente dependentes sobre K . Portanto

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

e a Proposição fica demonstrada.

Prova da afirmação :
Por contradição suponhamos que existam $\varphi_{ija}(x) \in K(x)$, não todos nulos, tais que :

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija}(x)\ t_i^a\ z_{ij} = 0 \tag{1.13}$$

Tomando o *m.m.c.* dos $\varphi_{ija}(x) \in K(x)$ podemos supor que $\varphi_{ija}(x) \in K[x]$ e $x \nmid \varphi_{ija}(x)$ para algum (i,j,a). Sem perdas na generalidade, vamos supor que tal tripla seja (k,j,a). Definimos $c \in \{0,1,\ldots,e_k - 1\}$ tal que:

$$x / \varphi_{kja}(x) \quad \text{para } a < c \text{ e } j \in \{1,\ldots,f_k\} \tag{1.14}$$

$$x \nmid \varphi_{kjc}(x) \quad \text{para algum } j \in \{1,\ldots,f_k\} \tag{1.15}$$

Notemos que $\varphi_{ija}(x) \in K[x] \subseteq O_{P_l}$ para todo $l \in \{1,\ldots,r\}$.[10] Logo :

$$v_l(\varphi_{ija}(x)) \geq 0 \text{ para todo } l \in \{1,\ldots,r\}. \tag{1.16}$$

Multiplicando (1.13) por t_k^{-c} temos:

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} = 0$$

[9] Note que $e_n = v_n(x) > 0$ pois os P_n's são zeros de x .
[10] De fato, $x \in P_l \subseteq O_{P_l}$ e $K \subseteq O_{P_l}$, para todo $l \in \{1,\ldots,r\}$.

Podemos escrever a equação acima da seguinte maneira :

$$\sum_{j=1}^{f_i}\sum_{a=0}^{e_i-1}\varphi_{kja}(x)t_k^{a-c}z_{kj}+\sum_{i\neq k}\sum_{j=1}^{f_i}\sum_{a=0}^{e_i-1}\varphi_{ija}(x)t_i^a t_k^{-c}z_{ij}=0 \tag{1.17}$$

Aplicando a valorização v_k em (1.17) temos :

1. para $i \neq k$:

$$v_k(\varphi_{ija}(x)t_i^a t_k^{-c}z_{ij}) = v_k(\varphi_{ija}(x)) + av_k(t_i) - cv_k(t_k) + v_k(z_{ij}) \geq e_k - c > 0.^{11}$$

2. para $i = k$

   (a) $a < c$:

$$v_k(\varphi_{kja}(x)t_k^{a-c}z_{kj}) = v_k(\varphi_{kja}(x)) + (a-c)v_k(t_k) + v_k(z_{kj}) \geq e_k + (a-c) \geq e_k - c > 0.^{12}$$

   (b) $a > c$:

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

Reescrevendo (1.17) temos:

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

Por (1) e (2), temos que $v_k(S) > 0$ então

$$\sum_{j=1}^{f_k}\varphi_{kjc}(x)z_{kj} \in P_K \text{ com isso } \sum_{j=1}^{f_k}\varphi_{kjc}(x)(P_K)\ z_{kj}(P_K) = 0(P_K).$$

Mas $z_{kj} = (z_{kj} - s_{kj}) + s_{kj}$ então $z_{kj}(P_k) = (z_{kj} - s_{kj})(P_k) + s_{kj}(P_k)$, onde $(z_{kj} - s_{kj})(P_k) = 0(P_k)$, pois $v_k(z_{ki} - s_{ki}) > 0$ por (1.12), logo $z_{kj}(P_k) = s_{kj}(P_k)$. Notemos ainda que $\varphi_{kjc}(x)(P_K) = \varphi_{kjc}(0)$, pois $\varphi_{kjc}(x) = q + xg_{kjc}(x)$ onde $q \in K$, $x \in P_k$ e $g_{kjc}(x) \in K[x] \subseteq O_{P_k}$ logo $xg_{kjc}(x) \in P_k$. Portanto

$$\sum_{j=1}^{f_k}\varphi_{kjc}(0)s_{kj}(P_K) = 0 \text{ com } \varphi_{kjc}(0) \neq 0 \text{ para algum } j.^{13}$$

O que é um absurdo! Pois s_{kj} são *l.i.* sobre K.

□

[11] Utilizando os resultados de (1.11), (1.12) , (1.16) e (1.14).

[12] Notemos que, por (1.14) $\varphi_{kja}(x) = xg(x)$, com $g(x) \in K[x] \subseteq O_{P_k}$ logo $v_k(\varphi_{kja}(x) \geq e_k$ e ainda $v_k(z_{kj}) = v_k(z_{kj} - s_{kj} + s_{kj}) \geq min\{v_k(z_{kj} - s_{kj}), v_k(s_{kj})\}$, mas $v_k(s_{kj}) \geq 0$ pois $s_{kj} \in O_{P_k}$ e por (1.12) temos $v_k(z_{kj} - s_{kj}) = r_k > 0$, portanto $v_k(z_{kj}) \geq 0$.

[13] Por (1.14) x não divide $\varphi_{kjc}(x)$ para algum $j \in \{1, \ldots, f_k\}$.

Corolário 1.2.4 *Num corpo de funções F/K, qualquer elemento $0 \neq x \in F$ tem somente um número finitos de zeros e polos.*

Dem. :
Tomemos $0 \neq x \in F$. Se $x \in \tilde{K}$, x não tem zeros nem polos. Se x é transcendente, pela Proposição (1.2.3), seu número de zeros é $\leq [F : K(x)]$. Para os polos, repete-se o mesmo argumento com x^{-1} .
□

1.3 Divisores e o Teorema de Riemann

Pelo Corolário (1.1.20) temos que $\tilde{K}$, o fecho algébrico de K, é uma extensão finita de K. Podemos então considerar F como um corpo de funções algébricas sobre $\tilde{K}$. Por esta razão vamos, a partir de agora, supor que F/K denota um corpo de funções algébricas de uma variável tal que K é algébricamente fechado em F.

Comecemos com algumas definições.

Definição 1.3.1 **(a)** *Um* **divisor** *de F/K é o elemento formal*

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

onde: $n_P \in \mathbb{Z}$ e $n_P = 0$ para quase todo P.[14]

(b) *Seja D um divisor de F/K, definimos como* **suporte de** *D o seguinte conjunto*

$$Supp\ D = \{P \in \mathbb{P}_F \mid n_P \neq 0\}$$

(c) *Um divisor D, da forma*

$$D = P, \text{com } P \in \mathbb{P}_F$$

é chamado de **divisor primo** *de F/K.*

(d) *Para um lugar $Q \in \mathbb{P}_F$ e um divisor $D = \sum_{P \in \mathbb{P}_F} n_P.P$ definimos* **o valor** *de D em Q por:*

$$v_Q(D) := n_Q .$$

(e) *Um divisor D é dito ser* **positivo**, *ou efetivo, se $D \geq 0$, ou seja $v_P(D) \geq 0$ para todo $P \in \mathbb{P}_F$.*

(f) *O* **grau** *de um divisor D é definido por:*

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

Através destas definições formulamos as seguintes observações que não demonstramos aqui pois entendemos que são triviais.

[14] Ou seja, $n_P \neq 0$ para um número finito de lugares $P \in \mathbb{P}_F$.

Observação 1.3.2 1. Dois divisores $D = \sum_{P \in \mathbb{P}_F} n_P.P$ e $D' = \sum_{P \in \mathbb{P}_F} n'_P.P$ podem ser adicionados da seguinte forma:

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

Com esta operação o conjunto

$$\mathcal{D}_F := \{D \mid D \text{ é um divisor de } F/K\}$$

é um grupo abeliano (livre). $\mathcal{D}_F$ é denominado grupo divisor de F/K.

2. Podemos escrever os elementos de $\mathcal{D}_F$, como:

$$D = \sum_{P \in S} v_P(D).P$$

onde $S \subseteq \mathbb{P}_F$ é um conjunto finito com $Supp D \subseteq S$.

3. Podemos definir uma ordem parcial em $\mathcal{D}_F$ por:

$$D_1 \leq D_2 \iff v_P(D_1) \leq v_P(D_2), \ \forall P \in \mathbb{P}_F \ e \ \forall D_1, \ D_2 \in \mathcal{D}_F \ .$$

4. A aplicação $deg : \mathcal{D}_F \longrightarrow \mathcal{Z}$ é um homomorfismo de grupos.

Pelo Corolário (1.2.4) qualquer elemento não nulo $x \in F$ tem somente um número finito de zeros e polos em $\mathbb{P}_F$. Logo, faz sentido definir :

Definição 1.3.3 *Seja $x \in F$, $x \neq 0$ denotamos por Z (respectivamente N) o conjunto de* **zeros** *(conj. de* **polos** *) de x em $\mathbb{P}_F$. Definimos então :*

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

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

$$(x) = (x)_0 - (x)_\infty, \text{ o } \textbf{divisor principal} \text{ de } x.$$

Notemos que $(x)_0 \geq 0$ *e* $(x)_\infty \geq 0$,[15] portanto podemos escrever

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x).P \tag{1.18}$$

A seguinte observação segue imediatamente da proposição (1.1.8), do corolário (1.1.24) e do fato geral de K ser algebricamente fechado.

Observação 1.3.4 Os elementos $0 \neq x \in F$ que são constantes, ou seja $x \in K$ podem ser caracterizados por :

$$x \in K \iff (x) = \mathbf{0} \ .^{16}$$

---

[15] Pela definição (1.1.22) temos $z \in F, \begin{cases} v_P(z) > 0 & \iff P \in Z \\ v_{P'}(z) < 0 & \iff P' \in N \end{cases}$.

[16] O divisor nulo, denotado por $\mathbf{0}$, é definido naturalmente por $\mathbf{0} := \sum_{P \in \mathbb{P}_F} v_P(\mathbf{0})P$, com $v_P(\mathbf{0}) = 0$ para qualquer $P \in \mathbb{P}_F$.

Definição 1.3.5 *O conjunto*

$$\mathcal{P}_F := \{(x) \mid 0 \neq x \in F\}$$

é chamado **grupo dos divisores principais** *de* F/K.

Observamos que $\mathcal{P}_F$ é um subgrupo de $\mathcal{D}_F$,[17] logo podemos considerar o grupo quociente

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

que é chamado por **grupo das classes dos divisores.**

Para um divisor $D \in \mathcal{D}_F$, o elemento correspondente no grupo quociente $\mathcal{C}_F$ é denotada por $[D]$, a **classe do divisor D**. Com isto vamos definir a seguinte relação de equivalência.

Definição 1.3.6 *Dois divisores* D, D' *são ditos serem* **equivalentes**, *e escrevemos* $D \sim D'$, *se*

$$[D] = [D'],$$

isto é, existe $x \in F \setminus \{0\}$ *tal que* $D = D' + (x)$.

Nossa próxima definição tem uma posição fundamental na teoria de corpos de funções algébricas.

Definição 1.3.7 *Para cada divisor* $A \in \mathcal{D}_F$ *podemos definir o seguinte conjunto :*

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

que é conhecido como **espaço de Riemann-Roch**.

Para um melhor entendimento da definição anterior enunciaremos a seguinte observação.

Observação 1.3.8 Seja $A \in \mathcal{D}_F$. Então os seguintes fatos podem ser provados trivialmente.

(a) 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 $\mathcal{L}(A)$ consiste de todos elementos $x \in F$ tais que:

(i) x tem zeros de ordem pelo menos m_j em Q_j, para $j = 1, \ldots, s$.

(ii) x pode ter polos somente nos lugares $P_1, \ldots, P_r$ e cada possível polo P_i tem ordem limitada por n_i, para $i = 1, \ldots, r$.

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

(c) $\mathcal{L}(A) \neq \{0\}$ se e somente se existe $A' \in \mathcal{D}_F$; t.q. $A' \sim A$ com $A' \geq 0$.[18]

---

[17] De fato,

- $\mathcal{P}_F \neq \emptyset$, pois F/K corpo de funções logo existe $o \neq x \in F$, transcendente sobre K.
- Seja qualquer $x, y \in F$, com $x \neq 0$ e $y \neq 0$ t.q. $(x), (y) \in \mathcal{P}_F$, por (1.18) temos:

$$(x) + (y^{-1}) = \sum_{P \in \mathbb{P}_F} v_P(x)P + \sum_{P \in \mathbb{P}_F} v_P(y^{-1})P = \sum_{P \in \mathbb{P}_F} v_P(xy^{-1})P = (xy^{-1}) \in \mathcal{P}_F .$$

[18] $\mathcal{L}(A) \neq \{0\} \iff \exists\, x \in \mathcal{L}(A)$ *t.q.* $(x) \geq -A \iff \exists\, x \in \mathcal{L}(A)$ *t.q.* $A + (x) \geq 0$, logo e so tomar $A' = A + (x)$.

Lema 1.3.9 *Seja $A \in \mathcal{D}_F$. Então temos :*

(a) *$\mathcal{L}(A)$ é um K-subespaço vetorial de F.*

(b) *Se $A' \sim A$, então , $\mathcal{L}(A) \simeq \mathcal{L}(A')$.*[19].

Dem. :
O item **(a)** é natural e não demonstraremos aqui.

(b) Como $A' \sim A$ existe $z \in F$, t.q. $A' = A + (z)$, definimos então a aplicação:

$$\begin{array}{rccc} \varphi: & \mathcal{L}(A) & \longrightarrow & F \\ & y & \longmapsto & yz \end{array}$$

- φ esta bem definida e é claramente injetora.[20]
- φ é uma transformação linear. De fato, seja $x,\ y \in \mathcal{L}(A)$ *e* $a \in K$, logo
  (i) $\varphi(x+y) = (x+y)z = xz + yz = \varphi(x) + \varphi(y)$.
  (ii) $\varphi(ax) = (ax)z = a(xz) = a\varphi(x)$.

Portanto $\varphi : \mathcal{L}(A) \longrightarrow Im(\varphi)$ é um isomorfismo de espaços vetoriais. Agora seja $x \in \mathcal{L}(A)$, temos por (1.18) e (1.3.6) que

$$(xz) + A' = (x) + (z) + A' = (x) + A \geq 0, \text{ pois } x \in \mathcal{L}(A)$$

então $(xz) + A' \geq 0$ logo $xz = \varphi(x) \in \mathcal{L}(A')$, ou seja $Im(\varphi) \subseteq \mathcal{L}(A')$. Para qualquer $y \in \mathcal{L}(A')$, temos $(y) \geq -A'$, mas $A \sim A'$ logo $(y) \geq -A + (z)$, com $0 \neq z \in F$ então $(y) - (z) = (yz^{-1}) \geq -A$, portanto $yz^{-1} \in \mathcal{L}(A)$ mas $\varphi(yz^{-1}) = (yz^{-1})z = y$, com isso $y \in Im(\varphi)$. Portanto $\mathcal{L}(A') = Im(\varphi)$ e temos o resultado.

□

O Lema abaixo dá uma interpretação dos *Espaços de Riemann-Roch* $\mathcal{L}$, para alguns divisores em particular.

Lema 1.3.10 *Dado um divisor $A \in \mathcal{D}_F$ temos :*

(a) *Se $A = \mathbf{0}$ então $\mathcal{L}(\mathbf{0}) = K$.*

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

Dem. :

(a) Seja $x \in \mathcal{L}(\mathbf{0}) = \{x \in F | (x) \geq \mathbf{0}\}$ pela observação (1.3.8.b) $v_P(x) \geq v_P(\mathbf{0}) = 0$ para todo $P \in \mathbb{P}_F$, logo x não tem polos em $\mathbb{P}_F$, pelo corolário (1.1.24) x é algébrico sobre K, com isso $x \in K$ e temos que $K \subseteq \mathcal{L}(\mathbf{0})$. Agora pela observação (1.3.4), se $0 \neq x \in K$ então $(x) = \mathbf{0}$. Portanto $\mathcal{L}(\mathbf{0}) = K$.

(b) Suponhamos que $\mathcal{L}(A) \neq \{0\}$, logo existe $0 \neq x \in \mathcal{L}(A)$ então $(x) \geq -A > 0$, ou seja $v_P(x) > 0$ para todo $P \in Supp(A)$ e $v_Q(x) \geq 0$ qualquer outro $Q \in \mathbb{P}_F$, por (1.3.4) x é transcendente sobre K, notemos ainda que x não possui polos, o que é impossível por (1.1.24). □

[19] Isomorfismo de espaços vetoriais sobre K.
[20] De fato, seja $x,\ y \in \mathcal{L}(A)$, t.q. $\varphi(x) = \varphi(y) \Longleftrightarrow xz = yz \Longleftrightarrow x = y$.

A seguir vamos trabalhar com varios K-espaços vetorias. A dimensão de cada espaço vetorial E será denotada por $dim\ E$. Nosso próximo objetivo é mostrar que $\mathcal{L}(A)$ tem dimensão finita para qualquer $A \in \mathcal{D}_F$.

Lema 1.3.11 *Sejam A, B divisores de F/K com $A \leq B$. Então temos $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ e*

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

Dem. :
A demonstração de que $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ é imediata, notando que $A \leq B$ se e so se $-A \geq -B$. Agora, como $A \leq B$ temos que $v_P(A) \leq v_P(B)$ para todo $P \in \mathbb{P}_F$. Observe que por indução basta mostrarmos para o caso em que existe $P' \in \mathbb{P}_F$ t.q. $v_{P'}(B) = v_{P'}(A) + 1$ e que $v_P(B) = v_P(A)$ se $P \neq P'$.[21]

Agora, como $v_P : F \to \mathcal{Z} \bigcup \{\infty\}$ é uma aplicação sobrejetiva, existe $z \in F$ t.q.

$$v_{P'}(z) = v_{P'}(B) = v_{P'}(A) + 1\ .$$

Para todo $x \in \mathcal{L}(B)$ temos $v_P(x) \geq -v_P(B)$ qualquer que seja $P \in \mathbb{P}_F$, em particular para P', $v_{P'}(x) \geq -v_{P'}(B) = -v_{P'}(z)$ então

$$v_{P'}(x) + v_{P'}(z) = v_{P'}(xz) \geq 0\ .$$

Portanto $xz \in O_{P'}$. Com isso podemos definir :

$$\begin{array}{rccc} \psi : & \mathcal{L}(B) & \longrightarrow & F_{P'} = O_{P'}/P' \\ & x & \longmapsto & xz(P') = xz + P' \end{array}$$

(i) ψ é claramente K-linear.[22]

(ii) $Ker(\psi) = \mathcal{L}(A)$. De fato, $x \in Ker(\psi)$ se e so se $\psi(x) = P'$, ou seja $xz \in P'$ logo

$$v_{P'}(xz) = v_{P'}(x) + v_{P'}(z) > 0\ ,$$

mas $v_{P'}(z) = v_{P'}(A) + 1$ portanto $v_{P'}(x) + v_{P'}(A) \geq 0$ ou seja

$$v_{P'}(x) \geq -v_{P'}(A). \tag{1.19}$$

Como $Ker(\psi) \subset \mathcal{L}(B)$, temos $v_P(x) \geq -v_P(B)$ para todo $P \in \mathbb{P}_F$. Por hipótese

$$v_P(B) = v_P(A) \text{ para todo } P \in \mathbb{P}_F \text{ exceto em } P'. \tag{1.20}$$

Por (1.19) e (1.20) temos que $v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$. Logo $Ker(\psi) \subseteq \mathcal{L}(A)$. Agora, seja $x \in \mathcal{L}(A)$, notemos que

$$v_{P'}(xz) = v_{P'}(x) + v_{P'}(z) \geq -v_{P'}(A) + v_{P'}(A) + 1 > 0$$

ou seja $x \in Ker(\psi)$. Com isto $Ker(\psi) = \mathcal{L}(A)$. Então $\mathcal{L}(B)/\mathcal{L}(A) \cong Im(\psi) \subseteq F_{P'}$. E $dim(\mathcal{L}(B)/\mathcal{L}(A)) = dim(Im(\psi)) \leq dim(F_{P'})$, mas

$$dim(F_{P'}) = [F_{P'} : K] = deg\ P' = deg\ B - deg\ A\ .$$

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

[21] Este é o caso mais simples, os outros seguem por indução sobre o numero de P's t.q. $v_P(B) > v_P(A)$.

[22] Lembrando que a soma de dois elementos em $O_{P'}/P'$ é dado por $(x + P') + (y + P') = (x + y) + P'$ e que K é imerso canonicamente em $O_{P'}/P'$.

□

Como consequência imediata deste lema obtemos a seguinte proposição.

Proposição 1.3.12 *Se* $A_1,\ A_2 \in \mathcal{D}_F$, *com* $A_1 \leq A_2$ *então*

$$deg\ A_1 - dim\ \mathcal{L}(A_1) \leq deg\ A_2 - dim\ \mathcal{L}(A_2)\ .$$

Dem. :
Como $A_1 \leq A_2$ pelo lema (1.3.11) temos que $dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \leq deg\ A_2 - deg\ A_1$, mas

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

e portanto vale a proposição.

□

Proposição 1.3.13 *Para qualquer divisor* $A \in D_F$, *o espaço* $\mathcal{L}(A)$ *é um espaço vetorial de dimensão finita sobre* K. *Mais precisamente, se* $A = A_+ - A_-$,[23] *com* A_+ *e* A_- *divisores positivos, então:*

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

Dem. :
Seja $A \in \mathcal{D}_F$ podemos escrever $A = A_+ - A_-$ onde temos sempre que $A \leq A_+$ logo pelo Lema (1.3.11) temos $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$ então $dim\ \mathcal{L}(A) \leq dim\ \mathcal{L}(A_+)$ com isso e suficiente mostrar que

$$dim\ \mathcal{L}(A_+) \leq deg\ A_+ + 1\ .^{24}$$

Agora, como $\mathbf{0} \leq A_+$ o Lema (1.3.11) nos garante que :

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

Por outro lado $dim(\ \mathcal{L}(A_+)/\mathcal{L}(\mathbf{0})\ ) = dim\ \mathcal{L}(A_+) - dim\ \mathcal{L}(\mathbf{0})$, como $\mathcal{L}(\mathbf{0}) = K$ temos que $dim\ \mathcal{L}(\mathbf{0}) = 1$. Portanto $dim\ \mathcal{L}(A_+) \leq deg\ A_+ + 1$. □

A seguir daremos a definição de dimensão de um divisor, o cálculo desta dimensão é um dos mais importantes problemas da teoria de corpos de funções algébricas.

Definição 1.3.14 *Para* $A \in \mathcal{D}_F$, *o número inteiro* $dimA := dim\ \mathcal{L}(A)$ *é chamado* **dimensão do divisor A**.

Daremos agora uma resposta a questão levantada na proposição (1.2.3).

---

[23] Pela observação (1.3.8(a)) podemos escrever

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

com $n_i,\ m_j > 0$, logo $A_+,\ A_- \geq 0$ notemos ainda que sempre $A \leq A_+$ no caso de $A_+ = \mathbf{0}$ teremos ainda que $A \leq A_-$.

[24] Na verdade este fato vale para qualquer $A \in \mathcal{D}_F$ com $deg\ A \geq 0$. Mostraremos este resultado depois do corolário (1.3.16).

Teorema 1.3.15 (Igualdade Fundamental) *Todo divisor principal possui grau zero. Mais precisamente : dado $x \in F\backslash K$ e $(x)_0$ (respect. $(x)_\infty$) denotando os divisores de zeros (respect. de polos) de x. Então :*

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

Dem. :

Seja $x \in F/K$, se $x \in K$ então $(x) = \mathbf{0}$ e o teorema esta provado. Tomemos então $x \in F\backslash K$ pela observação (1.1.3) temos $[F : K(x)] < \infty$. Seja $n = [F : K(x)]$ e tomemos

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

onde $P_1, \ldots, P_r$ são todos os polos de x. Pelo fato de $K(x) = K(x^{-1})$ e da proposição (1.2.3) conseguimos :

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

Agora escolha uma base $\{u_1, \ldots, u_n\}$ de $F/K(x)$ e tomemos um divisor $C \in \mathcal{D}_F$ tal que $C \geq 0$ e $(u_i) \geq -C$, para $i = 1, \ldots, n$ considere o conjunto $\mathcal{A} = \{x^i u_j \mid 0 \leq i \leq t\ e\ j = 1, \ldots, n\}$ logo $\#\mathcal{A} = (t+1)n$.

(i) Afirmamos que os elementos de $\mathcal{A}$ são *l.i.* sobre K. De fato, suponhamos

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

com $\alpha_{ij} \in K$, para $0 \leq i \leq t\ e\ j = 1, \ldots, n$, logo $\alpha_{ij}x^i \in K(x)$, para $0 \leq i \leq t\ e\ j = 1, \ldots, n$ e portanto

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

o que é um absurdo, pois u_j são *l.i.*.

(ii) $\mathcal{A} \subseteq \mathcal{L}(tB + C)$.

De fato, $v_P(x^i u_j) = i v_P(x) + v_P(u_j)$ para todo $P \in \mathbb{P}_F$, mas $v_P(u_j) \geq v_P(C)$ para qualquer $P \in \mathbb{P}_F$ e $v_P(x)\begin{cases} > -v_P(B) = 0 & \text{se } P \text{ é zero de } x \\ = -v_P(B) & \text{se } P \text{ é polo de } x \end{cases}$

então $v_P(x) \geq -v_P(B)$ para todo $P \in \mathbb{P}_F$. Portanto

$$v_P(x^i u_j) \geq -(t v_P(B) + v_P(u_j)) = -v_P(tB + C),\ \forall P \in \mathbb{P}_F\ .$$

Por (1.3.8.(b)) $x^i u_j \in \mathcal{L}(tB + C)$ para $0 \leq i \leq t\ e\ j = 1, \ldots, n$.

Por (i) e (ii) temos $(t+1)n \leq dim\ \mathcal{L}(tB + C)$, mas $dim\ \mathcal{L}(tB + C) \leq deg\ (tB + C) + 1$ por (1.3.13),[25] então $(t+1)n \leq t deg\ B + deg\ C + 1$, tomando $c = deg\ C$ obtemos

$$n - c - 1 \leq t(deg\ B - n)$$

[25] Observe que o divisor $tB + C \geq \mathbf{0}$.

como $n - c - 1$ é fixo e t qualquer a expressão acima só é possível se $deg\ B \geq n$. Portanto temos que $deg\ B = n$. Com isso provamos que $deg\ (x)_\infty = [F : K(x)]$. Agora como $(x)_0 = (x^{-1})_\infty$ concluimos que $deg\ (x)_0 = deg\ (x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$. E o teorema está provado.

□

O corolário a seguir, devido ao teorema (1.3.15), fornece a dimensão de alguns divisores em particular.

Corolário 1.3.16 (a) *Sejam os divisores* $A,\ A' \in \mathcal{D}_F$ *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* $A \in \mathcal{D}_F$ *de grau zero, as seguintes afirmações são equivalentes:*

(i) *A é principal.*

(ii) $dim\ A \geq 1$.

(iii) $dim\ A = 1$.

Dem. :

(a) Se $A,\ A' \in \mathcal{D}_F$ t.q. $A \sim A'$ então existe $x \in F,\ x \neq 0$ tal que $A' = A + (x)$. Pelo lema (1.3.9) temos $\mathcal{L}(A) \cong \mathcal{L}(A')$ então $dim\ A = dim\ A'$. O $deg\ A = deg\ A' + deg\ (x) = deg\ A'$, pois pelo teorema (1.3.15) se (x) é principal então $deg\ (x) = 0$.

(b) Suponhamos que $dim\ A > 0$ então $\mathcal{L}(A) \neq \{0\}$, pela observação (1.3.8.(c)) existe $A' \in \mathcal{D}_F$ com $A \sim A'$ e $A' \geq 0$, por (a) $deg\ A = deg\ A' \geq 0$ o que é um absurdo.

(c) Seja $A \in \mathcal{D}_F$, com $deg\ A = 0$.

(i) $\Longrightarrow$ **(ii)** Suponhamos que A seja principal, logo $A = (x)$, onde $0 \neq x \in F$ temos que $(x^{-1}) = -(x) = -A$ então $x^{-1} \in \mathcal{L}(A)$ e portanto $dim\ A \geq 1$.

(ii) $\Longrightarrow$ **(iii)** Suponhamos que $dim\ A \geq 1$, logo $\mathcal{L}(A) \neq \{0\}$ pela observação (1.3.8.(c)) existe $A' \in \mathcal{D}_F$ com $A' \sim A$ *e* $A' \geq \mathbf{0}$. Por (a), $deg\ A' = deg\ A = 0$, como $A' \geq \mathbf{0}$ e $deg\ A' = 0$ então $A' = \mathbf{0}$ logo $A \sim \mathbf{0}$, pelos lemas (1.3.9.(b)) e (1.3.10) temos $\mathcal{L}(A) \cong \mathcal{L}(\mathbf{0}) = K$, portanto $dim\ A = dim\ K = 1$.

(iii) $\Longrightarrow$ **(ii)** Suponhamos $dim A = 1$, logo existe $0 \neq z \in \mathcal{L}(A)$ por definição $(z) + A \geq \mathbf{0}$, como $deg\ ((z) + A) = deg\ (z) + deg\ A = 0$ pois (z) é principal e o $deg\ A = 0$ por hipótese, temos $(z) + A = \mathbf{0}$, ou seja $A = (z^{-1})$ é portanto principal.

□

Observação 1.3.17 Como mencionamos na proposição (1.3.13) temos que

$$dim\ A \leq deg\ A + 1, \text{ para qualquer } A \in \mathcal{D}_F \text{ com } deg\ A \geq 0\ .$$

De fato, se $dim\ A = 0$, acabou. Então suponhamos que $dim\ A > 0$, logo por (1.3.8.(c)) $A \sim A'$ para algum $A' \geq \mathbf{0}$, portanto por (1.3.16) temos, $dim\ A = dim\ A' \leq 1 + deg\ A' = 1 + deg\ A$.

Consideremos no exemplo a seguir o corpo de funções racional $F = K(x)$ que é apresentado no Apêndice A.

Exemplo 1.3.18 Para $0 \neq z \in K(x)$ tem-se $z = a\frac{f(x)}{g(x)}$, com $a \in K\backslash\{0\}$, $f(x), g(x) \in K[x]$ mônicos e relativamente primos. Sejam

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

com $p_i(x), q_j(x) \in K[x]$ polinômios mônicos irredutíveis distintos dois a dois. Então o divisor principal de z em $\mathcal{D}_{K(x)}$ aparece da seguinte forma :

$$(z) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (deg\ g(x) - deg\ f(x))P_\infty\ ,$$

onde P_i (respect. Q_j) são lugares correspondentes para $p_i(x)$ (respect. $q_j(x)$) conforme Apêndice A.

Além do mais, em corpos de funções arbitrário, os divisores principais servem como substitutos da decomposição em polinômios irredutíveis que ocorrem em corpos de funções racionais.

A seguir mostraremos a existência de uma cota inferior para dimensão de um divisor.

Proposição 1.3.19 *Existe uma constante $\gamma \in \mathcal{Z}$ tal que, para todo divisor $A \in \mathcal{D}_F$, vale o seguinte :*

$$deg\ A - dim\ A \leq \gamma\ .^{26}$$

Dem. :
Pelo corolário (1.3.12) temos que

$$deg\ A_1 - dim\ A_1 \leq deg\ A_2 - dim\ A_2 \tag{1.21}$$

para todo $A_1, A_2 \in \mathcal{D}_F$, com $A_1 \leq A_2$.

Agora, pela prova do teorema (1.3.15) podemos fixar $x \in F\backslash K$ e tomar $B = (x)_\infty$, logo existe $C \in \mathcal{D}_F$ com $C \geq \mathbf{0}$ tal que

$$dim\ (tB + C) \geq (t+1).deg\ B \tag{1.22}$$

para $t \geq 0$. Notemos ainda que por (1.3.11) vale

$$dim\ (tB + C) - dim\ tB = dim\ (\mathcal{L}(tB + C)/\mathcal{L}(tB) \leq deg\ (tB + C) - deg\ (tB) = deg\ C$$

ou seja

$$dim\ (tB + C) \leq dim\ (tB) + deg\ C \tag{1.23}$$

Portanto por (1.22) e (1.23) temos $dim\ (tB) + deg\ C \geq (t+1)deg\ B = tdeg\ B + deg\ B$ mas $deg\ C = c$ e $deg\ B = [F : K(x)]$ são números inteiros fixos. Tomando $\gamma = c - [F : K(x)] \in \mathcal{Z}$ temos

$$deg\ tB - dim\ (tB) \leq \gamma,\ \forall\ t > 0. \tag{1.24}$$

[26] Um fato importante aqui é que γ independe do divisor A, este depende somente do corpo de funções F/K.

Afirmação : Dado $A \in \mathcal{D}_F$, existem A_1, $D \in \mathcal{D}_F$ e um inteiro $t > 0$ tais que, $A \leq A_1$, $A_1 \sim D$ e $D \leq (tB)$.

Desta afirmação resulta a proposição, pois de (1.21) temos $deg\ A - dim\ A \leq deg\ A_1 - dim\ A_1$ e $deg\ D - dim\ D \leq deg\ (tB) - dim\ (tB)$. Por (1.24) $deg\ (tB) - dim\ (tB) \leq \gamma$. Mas como $A_1 \sim D$ temos por (1.3.16) $deg\ A_1 - dim\ A_1 = deg\ D - dim\ D$. Portanto $deg\ A - dim\ A \leq \gamma$, com $\gamma \in \mathcal{Z}$.

Prova da Afirmação
Podemos sempre escolher $A_1 \in \mathcal{D}_F$ t.q. $A \leq A_1$ e $A_1 \geq \mathbf{0}$. Então pelo lema (1.3.11) temos

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

Então $dim\ (tB) - deg\ A_1 \leq dim\ (tB - A_1)$, mas por (1.24), $dim\ (tB) \geq tdeg\ B - \gamma$, logo podemos tomar t suficientemente grande tal que $dim(tB - A_1) > 0$, portanto existe $0 \neq z \in \mathcal{L}(tB - A_1)$. Considerando $D = A_1 - (z)$, obtemos $A_1 \sim D$ e $D = A_1 - (z) \leq A_1 - (A_1 - tB) = tB$.

□

Definiremos a seguir um dos mais importantes valores invariantes de um corpo de funções.

Definição 1.3.20 *O* **gênero g** *de F/K é definido por*

$$g := max\{\ degA - dimA + 1 |\ A \in D_F\ \}$$

Note pela proposição (1.3.19), que esta definição faz sentido.

Observação 1.3.21 *O gênero de F/K é um inteiro não negativo.*

Dem. :
Na definição de g tome $A = \mathbf{0}$, logo $g \geq deg\ \mathbf{0} - dim\ \mathbf{0} + 1 = 0$. □

Teorema 1.3.22 (Teorema de Riemann) *Seja F/K um corpo de funções de gênero g. Então :*

(a) *Para qualquer divisor $A \in \mathcal{D}_F$, temos $dimA \geq deg\ A + 1 - g$.*

(b) *Existe um inteiro c, dependendo de F/K, tal que $dimA = deg\ A + 1 - g$ sempre que $deg\ A \geq c$.*

Dem. :

(a) Pela definição do gênero, temos $g \geq deg\ A - dimA + 1$ então $dimA \geq deg\ A + 1 - g$.

(b) Escolha um divisor $A_0 \in \mathcal{D}_F$ com $g = deg\ A_0 - dimA_0 + 1$ e tome $c := degA_0 + g$. Seja $A \in \mathcal{D}_F$ t.q. $deg\ A \geq c$, pela parte (a) temos

$$dim\ (A - A_0)\ \geq\ deg\ (A - A_0) + 1 - g\ =\ deg\ A - c + 1; \geq 1\ .$$

Logo, existe $0 \neq z \in \mathcal{L}(A - A_0)$, ou seja $(z) \geq -A + A_0$. Considere $A' = A + (z)$, é claro que $A' \geq A_0$. Temos, pelo lema (1.3.11) e pelo corolário (1.3.16) que

$$deg\ A - dim\ A = deg\ A' - dim\ A' \geq degA_0 - dim\ A_0 = g - 1$$

Portanto $deg\ A - g + 1 \geq dim\ A$ e a parte (a) garante a igualdade. □

Vamos dar um exemplo do gênero de um corpo de funções para o caso onde $F = K(x)$, ou seja F é um corpo de funções racionais.

Exemplo 1.3.23 O corpo de funções racionais $K(x)/K$ têm gênero $g = 0$. Afim de provar isto, seja P_∞ o divisor de polos de x, definido em (A.4). Considere, para $r \geq 0$, o espaço vetorial $\mathcal{L}(rP_\infty)$. Afirmamos que os elementos $1, x, \ldots, x^r$ estão em $\mathcal{L}(rP_\infty)$, pois :

Pelo teorema (A.1.2) $(x) = P_0 - P_\infty$, logo

$$v_P(x) = \begin{cases} 1 & \text{se } P = P_0 \\ -1 & \text{se } P = P_\infty \\ 0 & \text{para qualquer outro } P \in \mathbb{P}_F \end{cases}$$

Então $v_P(x^i) = iv_P(x) \geq -rv(P_\infty)$, para $0 \leq i \leq r$. Como os elementos $1, x, \ldots, x^r$ são linearmente independentes, temos:

$$r + 1 \quad \leq \quad dim\,(rP_\infty) = deg\,(r.P_\infty) + 1 - g, \text{ para } r \text{ suficientemente grande.}$$

Por (A.1.1) $deg\ P_\infty = 1$, portanto $r + 1 \leq r + 1 - g$. Como $g \geq 0$ pela observação(1.3.21), então $g = 0$.

1.4 O Teorema de Riemann-Roch

Ainda interessados na dimensão de divisores vamos nesta seção ao encontro do *Teorema de Riemann-Roch*, que é um dos mais importantes teoremas da teoria de corpos de funções algébricas.

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

Definição 1.4.1 *Para $A \in \mathcal{D}_F$, definimos*

$$i(A) = dim(A) - degA + g - 1$$

como **índice de especialidade de A**.[27]

Através do Teorema de Riemann (1.3.22) a seguinte observação é natural.

Observação 1.4.2 **(a)** $i(A)$ é um inteiro não negativo, para todo divisor $A \in \mathcal{D}_F$.

(b) $i(A) = 0$ se *deg* A for suficientemente grande.

Ainda neste seção provaremos varias interpretações para $i(A)$ como dimensão de certos espaços vetorias. Para isto introduziremos a noção de *adele*.

Definição 1.4.3 *Um* **adele**[28] **de F/K** *é uma aplicação :*

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

tal que $\alpha_P \in O_P$ para quase todo[29] $P \in \mathbb{P}_F$.

[27] Observe que, pela definição do gênero, $i(A)$ é um número finito.

[28] Notemos que na literatura em geral um adele pode ter outro interpretação que não esta aqui apresentada.

[29] Ou seja a menos de um numero finito de P's.

Com esta definição observamos que os adeles tem um número finito de polos, mas podem ter um número infinito de zeros.

Um adele pode ser visto como um elemento do produto direto

$$\prod_{P \in \mathbb{P}_F} F ,$$

logo usamos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou $\alpha = (\alpha_P)$.

Definição 1.4.4 *O conjunto* $\mathcal{A}_F = \{ \alpha | \ \alpha$ *é um adele de* $F/K \}$ *é chamado o* **espaço adélico** *de* F/K.

Observação 1.4.5 $\mathcal{A}_F$ é um espaço vetorial sobre K.[30]

Dem. :
De fato, podemos definir uma adição e uma multiplicação por escalar em $\mathcal{A}_F$, da seguinte maneira : Para $\alpha, \ \beta \in \mathcal{A}_F$; $k \in K$, com $\alpha = (\alpha_P)$ e $\beta = (\beta_P)$ definimos :

$$\alpha + \beta \ = \ (\alpha_P + \beta_P) \ \ e \ \ k\alpha \ = \ (k\alpha_P) \, .$$

□

Pelo corolário (1.2.4), qualquer $0 \neq x \in F$ tem um número finito de polos, logo faz sentido definir :

Definição 1.4.6 (a) *O* **adele principal** *de um elemento* $x \in F$ *é o adele cujas componentes são todas iguais a* x, *ou seja :*

$$\begin{array}{rccc} \alpha_x : & \mathbb{P}_F & \longrightarrow & F \\ & P & \longmapsto & \alpha_P = x \end{array} .$$

(b) *Dado* $P \in \mathbb{P}_F$, *para* $x \in F$, *podemos considerar* $i_P(x) \in \mathcal{A}_F$ *como o adele cujo* P*-componente é* x, *e os demais são zero, isto é* $i_P(x) = (\alpha_Q)$, *onde* $\alpha_Q = \begin{cases} x & se \ \ Q = P \\ 0 & se \ \ Q \neq P \end{cases}$ *para todo* $Q \in \mathbb{P}_F$.

Observamos que cada ítem da definição (1.4.6) fornece uma imersão de $F \hookrightarrow \mathcal{A}_F$ diferente. Mas aqui, fora menção contrária, quando falarmos da imersão $F \hookrightarrow \mathcal{A}_F$ estaremos nos referindo à do itém **(a)** .

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

Definição 1.4.7 *Para* $A \in \mathcal{D}_F$ *definimos:*

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

Claramente, $\mathcal{A}_F(A)$ é um K-subespaço de $\mathcal{A}_F$, para cada $A \in \mathcal{D}_F$. Observamos ainda que, pela definição de $\mathcal{L}(A)$ e $\mathcal{A}_F(A)$, temos $\mathcal{L}(A) = \mathcal{A}_F(A) \cap F$.

Vamos mostrar agora alguns resultados, sobre espaços adélicos, que serão usados mais adiante.

Proposição 1.4.8 *Sejam* $A, \ B \in \mathcal{D}_F$ *com* $A \leq B$, *então:*

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

[30] O conjunto $\mathcal{A}_F$ ainda pode ser observado como um anel, mas sua estrutura não será usada aqui.

Dem. :

Seja $\alpha \in \mathcal{A}_F(A)$ logo

$$v_P(\alpha) = v_P(\alpha_P) \geq -v_P(A), \text{ para qualquer } P \in \mathbb{P}_F$$

mas $-v_P(A) \geq -v_P(B)$ para todo $P \in \mathbb{P}_F$, pois $A \leq B$ então $v_P(\alpha) \geq -v_P(B)$ para qualquer $P \in \mathbb{P}_F$, ou seja $\alpha \in \mathcal{A}_F(B)$ e temos $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$.

Agora, para o outro resultado, usando a mesma idéia do lema (1.3.11), provaremos para $B = A + P$, com $P \in \mathbb{P}_F$. Escolha $t \in F$ tal que $v_P(t) = v_P(A) + 1 = v_P(B)$ e consideremos a seguinte aplicação K-linear :

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

Afirmamos que φ é sobrejetiva e que $ker\ \varphi = \mathcal{A}_F(A)$.

De fato, seja $\bar{y} \in F_P$, ou seja $\bar{y} = y + P$, com $y \in O_P$. Consideremos o adele $\alpha = (\alpha_Q)$ tal que

$$\alpha_Q = \begin{cases} t^{-1}y & se \quad Q = P \\ max\{0,\ -v_Q(B)\} & se \quad Q \neq P \end{cases}$$

Então $\alpha \in \mathcal{A}_F(B)$ e $\varphi(\alpha) = t(\alpha_P) + P = t(t^{-1}y) + P = \bar{y}$. Portanto φ é sobrejetora.

Seja agora $\alpha \in Ker\varphi \subset \mathcal{A}_F(B)$, logo $\varphi(\alpha) = (t\alpha_P) + P = P$ ou seja $t\alpha_P \in P$ então $v_P(t\alpha_P) = v_P(t) + v_P(\alpha_P) > 0$, mas $v_P(t) = v_P(A) + 1$, então $v_P(\alpha_P) + v_P(A) \geq 0$. Como $\alpha \in \mathcal{A}_F(B)$ e $B = A + P$ então $v_Q(\alpha_Q) \geq -v_Q(A)$ para qualquer $Q \neq P$. Portanto $\alpha \in \mathcal{A}_F(A)$. A inclusão contrária é natural, logo $ker\ \varphi = \mathcal{A}_F(A)$. Pelo teorema do homomorfismo temos,

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

ou seja

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

□

Para a próxima proposição necessitamos da definição de sequência exata curta.
Dados U, V e W espaços vetoriais e σ_1, σ_2 aplicações K-lineares como abaixo

$$0 \longrightarrow U \xrightarrow{\sigma_1} W \xrightarrow{\sigma_2} V \longrightarrow 0$$

Dizemos que tal sequência é exata curta se σ_1 é injetora, σ_2 é sobrejetora e $Ker(\sigma_2) = Im(\sigma_1)$.

Neste caso um resultado elementar de álgebra linear nos garante que :

$$dim(V) = dim(W) - dim(U)\ .$$

Proposição 1.4.9 *Sejam A, $B \in \mathcal{D}_F$ com $A \leq B$. Então :*

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

Dem. :

Consideremos a seguinte sequência de aplicações lineares

$$0 \longrightarrow \mathcal{L}(B)/\mathcal{L}(A) \xrightarrow{\sigma_1} \mathcal{A}_F(B)/\mathcal{A}_F(A) \xrightarrow{\sigma_2} \mathcal{A}_F(B) + F/\mathcal{A}_F(A) + F \longrightarrow 0$$

onde σ_1 e σ_2 são definidas de forma canônica:

$$\begin{array}{rccc} \sigma_1: & \mathcal{L}(B)/\mathcal{L}(A) & \longrightarrow & \mathcal{A}_F(B)/\mathcal{A}_F(A) \\ & \bar{x} = x + \mathcal{L}(A) & \longmapsto & \bar{x} = \alpha_x + \mathcal{A}_F(A) \end{array}$$

notemos que σ_1 tem sentido, pois $\mathcal{L}(A) = \mathcal{A}_F(A) \cap F$ e α_x denota o adele principal de x.

$$\begin{array}{rccc} \sigma_2: & \mathcal{A}_F(B)/\mathcal{A}_F(A) & \longrightarrow & \mathcal{A}_F(B) + F/\mathcal{A}_F(A) + F \\ & \bar{\alpha} = \alpha + \mathcal{A}_F(A) & \longmapsto & \bar{\alpha} = \alpha + (\mathcal{A}_F(A) + F) \end{array}$$

Afirmamos que esta sequência de aplicações é uma sequência exata curta de K-espaços vetoriais.

De fato :

(i) σ_1 é injetiva , pois : seja $\bar{x} \in Ker(\sigma_1)$ então $\sigma_1(\bar{x}) = \alpha_x + \mathcal{A}_F(A) = \mathcal{A}_F(A)$, ou seja $\alpha_x \in \mathcal{A}_F(A)$ por definição $v_P(\alpha_x) \geq -v_P(A)$, para todo $P \in \mathbb{P}_F$ portanto $x \in \mathcal{L}(A)$ para todo $P \in \mathbb{P}_F$. Portanto $Ker(\sigma_1) = \mathcal{L}(A) = \{0\}$.

(ii) σ_2 é sobrejetiva, de fato : Para todo $\bar{\alpha} \in \mathcal{A}_F(B) + F/\mathcal{A}_F(B) + F$ existe $\alpha \in \mathcal{A}_F(B)$ *e* $z \in F$ tais que $\bar{\alpha} = \alpha + z + \mathcal{A}_F(A) + F = \alpha + \mathcal{A}_F(A) + F$. Logo, $\sigma_2(\alpha) = \bar{\alpha}$.

(iii) $Ker(\sigma_2) = Im(\sigma_1)$, de fato : Seja $\alpha \in \mathcal{A}_F(B)$ tal que $\sigma_2(\alpha + \mathcal{A}_F(A)) = \bar{0}$. Então $\alpha \in \mathcal{A}_F(A) + F$, logo existe $x \in F$ *e* $\alpha' \in \mathcal{A}_F(A)$ t.q. $\alpha = \alpha' + x$, ou seja $\alpha - x \in \mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$, com isso temos que $x \in \mathcal{A}_F(B)$ e portanto $x \in F \cap \mathcal{A}_F(B) = \mathcal{L}(B)$. Além do mais $\alpha + \mathcal{A}_F(A) = x + \mathcal{A}_F(A) = \sigma_1(x + \mathcal{L}(A)) \in Im(\sigma_1)$. Agora tomemos $x \in \mathcal{L}(B) \subset F$ logo $\sigma_1(x + \mathcal{L}(A)) = x + \mathcal{A}_F(A)$, mas $\sigma_2(x + \mathcal{A}_F(A)) = x + \mathcal{A}_F(A) + F = \mathcal{A}_F(A) + F$, portanto $x + \mathcal{A}_F(A) \in Ker(\sigma_2)$.

Portanto a sequência é exata curta, logo temos:

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

mas da proposição (1.4.8) temos $dim(\ \mathcal{A}_F(B)/\mathcal{A}_F(A)\ ) = (deg\ B - deg\ A)$, ou seja

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

□

Proposição 1.4.10 *Se $B \in \mathcal{D}_F$, com $dim(B) = deg\ B + 1 - g$, então :*

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

Dem. :
Observamos que, dado $C \in \mathcal{D}_F$ com $C \geq B$, pelo lema (1.3.11) temos

$$dim(C) - dim(B) = dim(\mathcal{L}(C)/\mathcal{L}(B)) \quad \leq \quad deg\ C - deg\ B$$

mas $dim(B) = deg\ B + 1 - g$, logo $dim(C) \leq deg\ C + 1 - g$. Pelo teorema (1.3.22) temos que $dim\ C \geq deg\ C + 1 - g$. Portanto,

$$dim(C) = deg\ C + 1 - g, \text{ para todo } C \geq B. \tag{1.25}$$

Tomemos $\alpha \in \mathcal{A}_F$. Podemos encontrar $C \in \mathcal{D}_F$, com $C \geq B$ tal que $\alpha \in \mathcal{A}_F(C)$.[31] Pela proposição (1.4.9) e pela equação (1.25) temos

$$dim(\mathcal{A}_F(C) + F/\mathcal{A}_F(B) + F) = (deg\ C - dim(C)) - (deg\ B - dim(B)) = (g-1) - (g-1) = 0\ .$$

[31] Como $\alpha \in \mathcal{A}_F$ temos que $v_P(\alpha_P) \geq 0$ para quase todo $P \in \mathbb{P}_F$. Portanto dado $B \in \mathcal{D}_F$ é so tomar $C \in \mathcal{D}_F$, com $C \geq B$, $C \geq 0$ *e* $v_Q(C) \geq -v_Q(\alpha)$ para todo $Q \in \mathbb{P}_F$ tal que $v_Q(\alpha) < 0$. Logo teremos $\alpha \in \mathcal{A}_F(C)$.

Isto implica que $dim(\mathcal{A}_F(C) + F) = dim(\mathcal{A}_F(B) + F)$ ou seja $\mathcal{A}_F(C) + F = \mathcal{A}_F(B) + F$, então $\alpha \in \mathcal{A}_F(B) + F$ e portanto $\mathcal{A}_F \subsetneq \mathcal{A}_F(B) + F$, mas $\mathcal{A}_F(B) + F \subset \mathcal{A}_F$ para todo $B \in \mathcal{D}_F$. Logo temos o resultado.

□

Com estes resultados podemos provar o seguinte teorema.

Teorema 1.4.11 *Para qualquer divisor $A \in \mathcal{D}_F$, o índice de especialidade é*

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

Dem. :

Seja $A \in D_F$ um divisor arbitrário. Pelo Teorema de Riemann (1.3.22,(b)), existe um divisor $B \geq A$ tal que $dim(B) = deg\ B + 1 - g$. Pela proposição (1.4.10) temos

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

Da proposição (1.4.9) temos

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

mas por definição $i(A) = dim(A) - deg\ A - 1 + g$, portanto vale o teorema.

□

Notemos que embora os espaços $\mathcal{A}_F$, $\mathcal{A}_F(A)$ e F possuam dimensão infinita como K-espaços vetoriais o teorema afirma que o espaço quociente $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ tem dimensão finita sobre K.

Corolário 1.4.12 *O gênero de um corpo de funções pode ser dado por :*

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

Dem. :
No teorema (1.4.11), tomemos $A = \mathbf{0}$ como $dim(\mathbf{0}) = 1$ e $deg\ \mathbf{0} = 0$, temos $dim(\mathbf{0}) = deg\ \mathbf{0} + 1 - g + dim(\mathcal{A}_F/\mathcal{A}_F(\mathbf{0}) + F)$, ou seja

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

□

A seguir introduziremos o conceito de diferenciais de Weil, que fornecerá uma segunda interpretação para o indíce de especialidade de um divisor.

Definição 1.4.13 *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 $A \in \mathcal{D}_F$. Para um diferencial de Weil ω definimos sua* **componenete local** *$\omega_P : F \longrightarrow K$ por $\omega_P(x) := \omega(i_P(x))$.*

Notação : Denotamos por

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

o conjunto das diferenciais de Weil de F/K. Para $A \in \mathcal{D}_F$, o conjunto das diferenciais de Weil que se anulam em $\mathcal{A}_F(A) + F$ é denotado por

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

Observação 1.4.14 (i) O conjunto Ω_F é um K-espaço vetorial.

(ii) $\Omega_F(A)$ é um subespaço de Ω_F para todo $A \in \mathcal{D}_F$.

Dem. :

(i) Podemos ver o espaço Ω_F como um subespaço do espaço das transformações lineares, logo dado $\omega_1,\ \omega_2 \in \Omega_F$ *e* $a \in K$, a adição e multiplicação por escalar são definidas de maneira natural. Notamos que como $\omega_1,\ \omega_2 \in \Omega_F$ temos

$$\omega_1 \text{ se anula em } \mathcal{A}_F(A_1) + F \text{ } e \text{ } \omega_2 \text{ se anula em } \mathcal{A}_F(A_2) + F \text{ , para } A_1,\ A_2 \in \mathcal{D}_F \text{ .}$$

tomando $A_3 \in \mathcal{D}_F$, tal que $A_3 \leq A_1$ *e* $A_3 \leq A_2$ temos que $\omega_1 + \omega_2$ se anula em $\mathcal{A}_F(A_3) + F$. Agora como $\omega_1(a\alpha) = a\omega_1(\alpha)$ para qualquer $\alpha \in \mathcal{A}_F$ temos que $a\omega_1$ se anula em $\mathcal{A}_F(A_1) + F$.

O ítem **(ii)** é claro e não desmonstraremos aqui .

□

Lema 1.4.15 *Para qualquer* $A \in \mathcal{D}_F$ *tem-se* $dim(\ \Omega_F(A)\ ) = i(A)$.

Dem. :

O espaço $\Omega_F(A)$ é naturalmente o espaço vetorial dual[32] de $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$, mas pelo teorema (1.4.11) $dim(\ \mathcal{A}_F/(\mathcal{A}_F(A)+F)\ ) = i(A)$ que é finito, logo pela álgebra linear temos que $dim(\ \Omega_F(A)\ ) = i(A)$.

□

Como resultado imediato deste lema temos :

Corolário 1.4.16 $\Omega_F \neq 0$.

Dem. :
Escolha um divisor $A \in \mathcal{D}_F$ com $deg\ A \leq -2$. Então:

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

pois, $g \geq 0$ e pelo corolário (1.3.16.b) $dim(A) = 0$, logo $dim(\ \Omega_F(A)\ ) \geq 1$ e então $\Omega_F \supseteq \Omega_F(A) \neq 0$.

□

Definição 1.4.17 *Para* $x \in F$ *e* $\omega \in \Omega_F$ *definimos*

$$\begin{array}{rccl} x\omega : & \mathcal{A}_F & \longrightarrow & K \\ & \alpha & \longmapsto & (x\omega)(\alpha) := \omega(x\alpha) \end{array}$$

Façamos agora a seguinte observação sobre adeles e diferenciais.

Observação 1.4.18 Seja $x \in F$ e (x) seu divisor principal, temos

(i) $\alpha \in \mathcal{A}_F(A)$ se e somente se $x\alpha \in \mathcal{A}_F(A - (x))$.

[32] Isto é um exercício simples de ágebra linear.

(ii) Se $\omega \in \Omega_F$ então $x\omega \in \Omega_F$.

(iii) Ω_F é um espaço vetorial sobre F.

Dem. :

(i) Seja $\alpha \in \mathcal{A}_F(A)$ logo $v_P(\alpha_P) + v_P(A) \geq 0$, para qualquer $P \in \mathbb{P}_F$. Logo

$$v_P(x\alpha) + v_P(A - (x)) = v_P(x) + v_P(\alpha) + v_P(A) - v_P((x)) = v_P(\alpha_P) + v_P(A)$$

pois, para cada $P \in \mathbb{P}_F$ temos $v_P((x)) = v_P(x)$ e $v_P(\alpha) = v_P(\alpha_P)$. Portanto

$$v_P(x\alpha) + v_P(A - (x)) \geq 0\,,$$

para todo $P \in \mathbb{P}_F$.
De maneira análoga, aplicando x^{-1} em $x\alpha \in \mathcal{A}_F(A - (x))$ teremos $\alpha \in \mathcal{A}_F(A)$.

(ii) Tomemos $\omega \in \Omega_F$, logo ω se anula em $\mathcal{A}_F(A) + F$ para algum $A \in \mathcal{D}_F$, pela definição (1.4.17) e por ω ser K-linear observa-se que $x\omega$ é uma aplicaçãoK-linear. Agora afirmamos que $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$; de fato, seja $\alpha + t \in \mathcal{A}_F(A + (x)) + F$, com $\alpha \in \mathcal{A}_F(A + (x))$ e $t \in F$, logo pela definição (1.4.17) temos

$$(x\omega)(\alpha + t) = \omega(x\alpha + xt) = 0$$

pois, $xt \in F$ e pelo ítem (i) $x\alpha \in \mathcal{A}_F(A)$. Portanto $x\omega \in \Omega_F(A) \subseteq \Omega_F$.

(iii) Sejam ω_1, $\omega_2 \in \Omega_F$ e $k \in F$, temos pelo (ii) que ω_1, $k\omega_2$ são K-lineares logo $(\omega_1 + k\omega_2)$ é K-linear e mais como $k\omega_2 \in \Omega_F$ temos $(\omega_1 + k\omega_2) \in \Omega_F$.

□

De fato temos que o espaço vetorial Ω_F é unidimensional sobre F, isto é a nossa próxima proposição.

Proposição 1.4.19 *Ω_F é um F-espaço vetorial de dimensão 1.*

Dem. :
Queremos mostrar que existe $0 \neq \omega_1 \in \Omega_F$ tal que, qualquer outro elemento de Ω_F é múltiplo, por escalar, de ω_1. Pelo corolário (1.4.16) temos que existe $0 \neq \omega_1 \in \Omega_F$. Agora tomemos $\omega_2 \in \Omega_F$ se $\omega_2 = 0$ é só tomar $z = 0$ e temos o resultado.

Vamos assumir que $\omega_2 \neq 0$. Escolhemos A_1, $A_2 \in \mathcal{D}_F$ tais que $\omega_1 \in \Omega_F(A_1)$ e $\omega_2 \in \Omega_F(A_2)$.

Observe que, se $x \in \mathcal{L}(A_i + B)$ então $(x) + A_i + B \geq 0$, ou seja $-B - (x) \leq A_i$ então

$$\mathcal{A}_F(-B - (x)) \subseteq \mathcal{A}_F(A_i)\,,$$

pela observação (1.4.18.(i)) se $\alpha \in \mathcal{A}_F(-B)$ então $x\alpha \in \mathcal{A}_F(-B - (x)) \subseteq \mathcal{A}_F(A_i)$, logo

$$(x\omega_i)(\alpha) = \omega_i(x\alpha) = 0\,,$$

portanto $x\omega_i \in \Omega_F(-B)$. Com isso faz sentido definir, para um divisor B (a ser determinado mais adiante) as seguintes aplicações

$$\varphi_i : \begin{array}{ccc} \mathcal{L}(A_i + B) & \longrightarrow & \Omega_F(-B) \\ x & \longmapsto & x\omega_i \end{array} \quad \text{para } i = 1, 2.$$

Pela observação (1.4.18.(ii)) temos que φ_i para $i = 1, 2$, é K-linear. Além do mais as φ_i são injetoras, pois se $x \in ker(\varphi_i)$ então $\varphi_i(x) = x\omega_i \equiv 0$, mas $\omega_i \neq 0$ logo $x = 0$.

Afirmação : Existe um divisor $B \in \mathcal{D}_F$, tal que :

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

Com esta afirmação, podemos tomar

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

então existem $x_i \in \mathcal{L}(A_i + B)$, para $i = 1, 2$ tais que $\varphi_1(x_1) = \varphi_2(x_2) = \eta$ ou seja $x_1\omega_1 = x_2\omega_2$ então $\omega_2 = (x_2^{-1}x_1)\omega_1$, com $x_2^{-1}x_1 \in F$, e temos o resultado. Basta então provarmos a afirmação.

Prova da afirmação

Temos da álgebra linear que, se U_1, U_2 são subespaços de dimensão finita de um espaço vetorial V então

$$dim(\ U_1 \cap U_2\ ) \geq dim(U_1) + dim(U_2) - dim(V) \tag{1.26}$$

Pelo teorema (1.3.22) podemos tomar $B \in \mathcal{D}_F$ com $B > \mathbf{0}$ *e deg* B suficientemente grande, tal que

$$dim(A_i + B) = deg\ (A_i + B) + 1 - g, \text{ para } i = 1, 2. \tag{1.27}$$

Chamemos $U_i = \varphi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B) = V$, para $i = 1, 2$.

Pelo lema (1.4.15) temos

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

mas como $B > \mathbf{0}$ temos $deg\ (-B) < 0$, logo pelo corolário (1.3.16) obtemos que $dim(-B) = 0$. Portanto

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

Obtemos então

$$dim(U_1) + dim(U_2) - dim(V) = dim(\ \varphi_1(\mathcal{L}(A_1 + B))) + dim(\ \varphi_2(\mathcal{L}(A_2 + B))) - (deg\ B + g - 1)$$

como φ_i são K-lineares e injetoras temos

$$dim(\ \varphi_i(\mathcal{L}(A_i + B))) = dim(\ \mathcal{L}(A_i + B)\ ) = dim(A_i + B)$$

logo por (1.27) obtemos

$$dim(U_1) + dim(U_2) - dim(V) = deg\ B + \underbrace{(deg\ A_1 + deg\ A_2 + 3(1 - g))}_{independe\ de\ B}\ .$$

Como *deg* B é suficientemente grande obtemos

$$dim(U_1(+dim(U_2) - dim(V) > 0\ .$$

De (1.26) segue que $dim(U_1 \cap U_2) > 0$ o que prova a afirmação.

□

Devido a definição de diferenciais de Weil, necessitamos vincular a todo diferencial $\omega \in \Omega_F$, não nula, um divisor. Para isto, dado $0 \neq \omega \in \Omega_F$ considere o seguinte conjunto de divisores :

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

Lema 1.4.20 *Seja* $\omega \in \Omega_F$, $\omega \neq 0$. *Então existe um único divisor* $W \in \mathcal{D}_F$ *tal que* $W \in M(\omega)$ *e* $A \leq W$ *para todo* $A \in M(\omega)$.

Dem. :
Pelo Teorema (1.3.22), existe $c \in \mathcal{Z}$ dependendo somente de F/K tal que

$$i(A) = 0 \text{ para todo } A \in \mathcal{D}_F \text{ com } deg\ A \geq c\ .$$

Notamos ainda que $deg\ A < c$ para todo $A \in M(\omega)$, pois suponhamos $A \in M(\omega)$, com $deg\ A \geq c$, logo $i(A) = 0$ e pelo teorema (1.4.11) temos $\mathcal{A}_F(A) + F = \mathcal{A}_F$, como ω se anula em $\mathcal{A}_F(A) + F$ teriamos $\omega \equiv 0$, o que é um absurdo.

Então o grau dos divisores de $M(\omega)$ é limitado superiormente . Assim, podemos escolher um divisor $W \in M(\omega)$ de grau maximal.

Agora, suponhamos que existe $B \in M(\omega)$ tal que $B \not\leq W$, isto é, $v_Q(B) > v_Q(W)$ para algum $Q \in \mathbb{P}_F$.

Afirmação : $W + Q \in M(\omega)$

Isto é um absurdo pois, $deg(W + Q) = degW + 1$, o que contradiz a maximalidade de W. Logo fica provado o lema.[33]

Passamos então a demonstrar a afirmação .

Prova da afirmação : Dado um adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$. Podemos escrever α da seguinte maneira $\alpha = \alpha' + \alpha''$, onde

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

Com isso temos que

- Para $P \in \mathbb{P}_F$, com $P \neq Q$ vale

$$v_P(\alpha') + v_P(W) = v_P(\alpha) + v_P(W) + v_P(Q) \geq 0$$

pois, $v_P(Q) = 0$ e $\alpha \in \mathcal{A}_F(W + Q)$;

Para $P \neq Q$ temos

$$v_Q(\alpha') + v_Q(W) = v_Q(0) + v_Q(W) \geq 0$$

pois $v_Q(0) = +\infty$. Portanto $\alpha' \in \mathcal{A}_F(W)$.

- De maneira análoga obtemos que $\alpha'' \in \mathcal{A}_F(B)$

Seja $\alpha \in \mathcal{A}_F(W + Q)$, logo

$$\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$$

pois W, $B \in M(\omega)$ Portanto $W + Q \in M(\omega)$.

□

A nossa próxima definição é motivada pelo lema (1.4.20) acima.

Definição 1.4.21 (a) *O* **divisor** (ω) *de um diferencial de Weil* $\omega \neq 0$ *é o divisor unicamente determinado de* F/K *satisfazendo :*

[33] A unicidade de W é devida a sua construção pois se existe W' com as mesmas propriedades de W teriamos que $W \geq W'$ e $W' \geq W$, ou seja $W = W'$.

1. $\omega(\mathcal{A}_F((\omega)) + F) \equiv 0$.

2. *Se* $\omega(\mathcal{A}_F(A) + F) \equiv 0$, *então* $A \leq (\omega)$.

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

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

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

As observações a seguir seguem imediatamente das definições acima, e não as demonstraremos aqui.

Observação 1.4.22 **(i)** $\Omega_F(A) = \{ \omega \in \Omega_F | \ \omega \equiv 0 \text{ ou } (\omega) \geq A \}$.

(ii) $\Omega_F(\mathbf{0}) = \{ \omega \in \Omega_F | \ \omega \text{ é regular} \}$.

(iii) $dim(\ \Omega_F(\mathbf{0})\ ) = g$.[34]

Antes de prosseguirmos para uma outra interpretação de indice de especialidade de um divisor, mostraremos agora que uma diferencial de Weil é unicamente determinada por qualquer de suas componentes locais.

Proposição 1.4.23 *Se* $\omega \in \Omega_F$ *e* $\alpha = (\alpha_P) \in \mathcal{A}_F$. *Então,* $\omega_P(\alpha_P) \neq 0$ *para no máximo um número finito de lugares* $P \in \mathbb{P}_F$, *e*

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

Em particular,

$$\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0 \ . \tag{1.28}$$

Dem. :
Sejam $\alpha = (\alpha_P) \in \mathcal{A}_F$ e $0 \neq \omega \in \Omega_F$, consideremos o divisor canônico $W = (\omega)$. Tomemos o conjunto $S \subset \mathbb{P}_F$ tal que

$$S = Supp(W) \cup \{ P \in \mathbb{P}_F | \ P \text{ é Polo de } \alpha \}$$

logo S é finito, pois $\alpha \in \mathcal{A}_F$ e para todo $P \notin S$ vale $v_P(W) = 0$ e $v_P(\alpha_P) \geq 0$. Agora definimos o adele $\beta = (\beta_P) \in \mathcal{A}_F$ onde

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

Para $P \notin S$ temos

$$v_P(\beta) = v_P(\alpha_P) \geq 0 = -v_P(W)$$

para $P \in S$ vale

$$v_P(\beta) = v_P(0) = \infty \geq -v_P(W)$$

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

Observa-se que podemos escrever $\alpha \in \mathcal{A}_F$ da seguinte maneira

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

[34] Isto é consequência do lema (1.4.15) e da definição (1.4.1).

observamos ainda, como $\beta \in \mathcal{A}_F(W)$ e ω se anula em $(\mathcal{A}_F(W) + F)$ temos que $\omega(\beta) = 0$.

Com isso

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

Dado $P \notin S$ seja o adele $i_P(\alpha_P) \in \mathcal{A}_F$, onde $i_P(\alpha_P) = \begin{cases} \alpha_P & \text{no lugar } P \\ 0 & \text{nos outros lugares} \end{cases}$

Claramente temos que $i_P(\alpha_P) \in \mathcal{A}_F(W)$, para todo $P \in S$. Ou seja,

$$\omega_P(i_P(\alpha_P)) = \omega_P(\alpha_P) = 0 \text{ para todo } P \notin S\ .$$

Com isso

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

E ainda, como $\omega \in \Omega_F$ se anula em F, dado qualquer $x \in F$ consideremos $\alpha = (\alpha_P)$ o adele principal[35] de x temos

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(x) = 0\ .$$

□

Proposição 1.4.24 **(a)** *Seja $\omega \neq 0$ um diferencial de Weil de F/K e $P \in \mathbb{P}_F$. Então*

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

Em particular , $\omega_P \neq 0$.

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

Dem. :

(a) Dado $0 \neq \omega \in \Omega_F$, seja $W = (\omega)$ o divisor canônico de ω, por definição $v_P(\omega) = v_P(W)$, consideremos $s = v_P(\omega)$ para $P \in \mathbb{P}_F$ fixado. Agora para $x \in F$ tal que $v_P(x) \geq -s$, consideremos o adele $i_P(x) \in A_F$ definido em (1.4.6), logo temos que $i_P(x) \in \mathcal{A}_F(W)$. Então $\omega_P(x) = \omega(i_P(x)) = 0$, ou seja, $\omega_P(x) = 0$, para todo $x \in F$ com $v_P(x) \geq -s$.

Suponhamos que,

$$\omega_P(x) = 0 \text{ para qualquer } x \in F \text{ com } v_P(x) \geq -(s+1) = -v_P(W) - v_P(P)\ . \tag{1.29}$$

Com isso $i_P(x) \in \mathcal{A}_F(W + P)$. Tomemos $\alpha = (\alpha_Q) \in \mathcal{A}_F(W + P)$, podemos escrever α como

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

onde o adele $i_P(\alpha_P) = \begin{cases} \alpha_P & \text{para } P \\ 0 & \text{para qualquer lugar diferente de } P \end{cases}$

Agora observamos que $\beta = \alpha - i_P(\alpha_P) \in \mathcal{A}_F(W)$, de fato :
Para $Q \in \mathbb{P}_F$, com $Q \neq P$ temos

$$v_Q(\beta) = v_Q(\alpha_Q - 0) \geq -v_Q(W) - v_Q(P) = -v_Q(W)$$

[35] Ou seja, $\alpha_P = x$, $\forall P \in \mathbb{P}_F$.

pois $\alpha = (\alpha_Q) \in \mathcal{A}_F(W+P)$, para P temos

$$v_P(\beta) = v_P(\alpha_P - \alpha_P) = +\infty \geq -v_P(W) .$$

Logo $\omega(\beta) = 0$, mais temos também que

$$v_Q(i_P(\alpha_P)) = \begin{cases} v_Q(\alpha_Q) & \geq -v_Q(W-P) \quad = -(s+1) \quad se \quad Q = P \\ v_Q(0) & = +\infty \qquad\quad \geq -(s+1) \quad se \quad Q \neq P \end{cases}$$

então por (1.29) $\omega(i_P(\alpha_P)) = \omega_P(\alpha_P) = 0$.

Portanto para todo $\alpha = (\alpha_Q) \in \mathcal{A}_F(W+P)$ temos

$$\omega(\alpha) = \omega(\beta) + \omega(i_P(\alpha_P)) = 0 .$$

Ou seja, ω se anula em $\mathcal{A}_F(W+P)$, o que é um absurdo pela definição (1.4.21).

Logo, existe $x \in F$, com $v_P(x) = -(s+1)$ tal que $\omega_P(x) \neq 0$. Com isto demonstramos o ítem (a).

(b) Sejam $\omega, \omega' \in \Omega_F$, para qualquer $x \in F$, e $P \in \mathbb{P}_F$ temos

$$(\omega_P - \omega'_P)(x) = \omega(i_P(x)) - \omega'(i_P(x)) = (\omega - \omega')(i_P(x)) = (\omega - \omega')_P(x)$$

Logo se $\omega_P = \omega'_P$ para algum $P \in \mathbb{P}_F$, então

$$(\omega - \omega')_P(x) = 0 \text{ para todo } x \in F .$$

então pelo ítem (a) temos que $\omega - \omega' \equiv 0$, ou seja $\omega = \omega'$.

□

Estas duas proposições acima serão usadas, em particular, no capítulo seguinte quando definiremos os Códigos Geométricos de Goppa.

Proposição 1.4.25 (a) *Para* $0 \neq x \in F$ *e* $0 \neq \omega \in \Omega_F$, *temos* $(x\omega) = (x) + (\omega)$.

(b) *Quaisquer dois divisores canônicos de* F/K *são equivalentes.*

Dem. :

(a) Seja $0 \neq \omega \in \Omega_F$, podemos tomar $A = (\omega)$ e por (1.4.18) temos

$$(\omega) + (x) \leq (x\omega) \tag{1.30}$$

De maneira análoga, tomando $(x\omega)$ no lugar de (ω) e (x^{-1}) no lugar de (x) obtemos

$$(x\omega) \leq (\omega) - (x^{-1}) = (\omega) + (x) \tag{1.31}$$

De (1.30) e (1.31) temos :

$$(x\omega) = (\omega) + (x)$$

(b) Sejam W e W' divisores canônicos de F/K pela definição (1.4.21.(d)) $W = (\omega_1)$ e $W' = (\omega_2)$ para ω_1, $\omega_2 \in \Omega_F$. Como pela proposição (1.4.19) $dim(\Omega_F) = 1$, existe $z \in F$ tal que

$$\omega_2 = y\omega_1$$

e assim $W' = (z) + W$.

□

Uma consequência desta proposição é que os divisores canônicos de F/K formam uma única classe $[W]$ do grupo quociente $\mathcal{C}_F$. Esta classe de divisores é chamada **classe canônica** de F/K.

Teorema 1.4.26 *Seja $A \in \mathcal{D}_F$ um divisor arbitrário e $W = (\omega)$ um divisor canônico de F/K. Então a aplicação*

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

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

Dem. :
Observamos que se $x \in \mathcal{L}(W - A)$ então

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

logo pela observação (1.4.22.(i)) temos $x\omega \in \Omega_F(A)$ com isso μ está bem definida.

Verifica-se naturalmente que μ é K-linear, agora se $x \in \mathcal{L}(W - A)$ tal que $\mu(x) = 0$, ou seja $x\omega \equiv 0$, então $x = 0$, pois $\omega \neq 0$. Logo μ é injetiva .

Para mostrar que μ é sobrejetiva, tomemos $\gamma \in \Omega_F(A)$; como $dim(\Omega_F) = 1$ existe $x \in F\backslash\{0\}$ t.q. $x\omega = \gamma$, mas $\gamma = x\omega \in \Omega_F(A)$ então $(x\omega) = (x) + (\omega) \geq (A)$ com isso $(x) \geq -((\omega) - A)$, em outras palavras existe $x \in \mathcal{L}((\omega) - A)$ tal que $\mu(x) = \gamma$. Portanto μ é um isomorfismo. Com isso $dim(\ \Omega_F(A)\ ) = dim(W - A)$ então pelo lema (1.4.15) $i(A) = dim(W - A)$.

□

A partir dos resultados desta seção obtemos o Teorema de Riemann-Roch que será uma ferramenta fundamental para todos os nossos próximos resultados.

Teorema 1.4.27 (Riemann-Roch) *Seja W um divisor canônico de F/K. Então para qualquer $A \in \mathcal{D}_F$,*

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

Dem. :

Pela definição (1.4.1) de indíce de especialidade e pelo teorema (1.4.26) temos o resultado. □

Corolário 1.4.28 *Para um divisor canônico W, nós temos*

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

Dem. :
Tomemos o divisor $A = \mathbf{0}$, pelo teorema (1.4.27) temos

$$1 = dim(\mathbf{0}) = deg\ \mathbf{0} + 1 - g + dim(W - \mathbf{0})$$

logo $dim(W) = g$. Para $A = W$, vale

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

com isso $deg\ W = 2g - 2$. □

Pelo teorema de Riemann (1.3.22) temos que $i(A) = 0$ para um divisor A com $deg\ A \geq c$, para um certa constante c. Agora nos podemos dar uma descrição mais exata desta constante.

Teorema 1.4.29 *Se A é um divisor de F/K com grau maior ou igual que $2g - 1$, então*

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

Dem. :
Pelo teorema (1.4.27) se W é um divisor canônico temos

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

como $deg\ A \geq 2g - 1$ por hipótese e $deg\ W = 2g - 2$ pelo corolário (1.4.28), obtemos

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

logo $deg\ (W - A) < 0$ então pelo corolário (1.3.16) $dim(W - A) = 0$, ou seja $dim(A) = deg\ A + 1 - g$. □

Observamos que o limitante $2g - 1$ deste corolário é o melhor possível.

1.5 Lacunas de Weierstrass e Outras Consequências 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 a classe canônica de F/K.

Proposição 1.5.1 *Um divisor $B \in \mathcal{D}_F$ é canônico se e somente se*

$$deg\ B = 2g - 2\ \ e\ \ dim(B) \geq g\ .$$

Dem. :
Suponhamos que $deg\ B = 2g - 2$ e $dim(B) \geq g$. Tomemos um divisor canônico W; então pelo teorema (1.4.27) :

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

ou seja, $1 \leq dim(W - B)$, mas

$$deg\ (W - B) = deg\ W - deg\ B = 0$$

logo pelo corolário (1.3.16) $W - B$ é principal. Portanto B é um divisor canônico.

Agora, se B é um divisor canônico temos pelo corolário (1.4.28) que

$$dim(B) = g\ \ e\ \ deg\ B = 2g - 2\ ,$$

e temos o resultado.

□

A caracterização de alguns espaços é outra consequência do teorema de Riemann-Roch e isto é a nossa próxima proposição .

Proposição 1.5.2 *Sejam* $P \in \mathbb{P}_F$ *com deg* $P = 1$ *e* $B \in \mathcal{D}_F$, *assim* $\mathcal{L}(nP + B) = \mathcal{L}((n-1)P + B)$ *se e somente se*

$$\mathcal{L}(W - nP - B) \subsetneq \mathcal{L}(W - (n-1)P - B), \text{ onde } W \text{ é um divisor canônico .}$$

Dem. :

Suponhamos que $\mathcal{L}(nP + B) = \mathcal{L}((n-1)P + B)$
Tomemos $x \in \mathcal{L}(W - nP - B)$ então

$$(x) \geq -W + nP + B > -W + nP + B - P = -W + (n-1)P + B$$

ou seja, $x \in \mathcal{L}(W - (n-1)P - B)$, logo $\mathcal{L}(W - nP - B) \subseteq \mathcal{L}(W - (n-1)P - B)$.
Agora se $\mathcal{L}(W - nP - B) = \mathcal{L}(W - (n-1)P - B)$ temos

$$dim(\ W - nP - B\ ) = dim(\ W - (n-1)P - B\ ),$$

como W é um divisor canônico, segue pelo teorema de Riemann-Roch (1.4.27) que

$$dim(nP + B) - 1 + g - deg\ (nP + B) = dim((n-1)P + B) - 1 + g - deg\ ((n-1)P + B)\ ,$$

com isto obtemos $dim(nP + B) = dim((n-1)P + B) + 1$, então $\mathcal{L}((n-1)P + B) \subsetneq \mathcal{L}(nP + B)$ mas isto contradiz a hipótese, logo

$$\mathcal{L}(W - nP - B) \subsetneq \mathcal{L}(W - (n-1)P - B)$$

para W divisor canônico.
Tomemos por hipótese que $\mathcal{L}(W - nP - B) \subsetneq \mathcal{L}(W - (n-1)P - B)$ para W um divisor canônico.
Suponhamos que $\mathcal{L}((n-1)P + B) \subsetneq \mathcal{L}(nP + B)$, logo $dim(nP + B) > dim((n-1)P + B)$, então pelo teorema de Riemann-Roch temos

$$deg\ (nP + B) + 1 - g + dim(\ W - nP - B\ ) > deg\ ((n-1)P + B) + 1 - g + dim(\ W - (n-1)P - B\ )$$

ou seja, $dim(\ W - nP - B\ ) > 1 + dim(\ W - (n-1)P - B\ )$, mas

$$\mathcal{L}(W - (n-1)P - B) \supseteq \mathcal{L}(W - nP - B)\ ,^{36}$$

Portanto, $\mathcal{L}(W - nP - B) = \mathcal{L}(W - (n-1)P - B)$ o que é um absurdo. Logo temos o resultado.

□

Agora, vamos definir o que será a nossa principal ferramenta, para o cálculo da distância mínima dos códigos de Goppa.

Definição 1.5.3 *Sejam* $P \in \mathbb{P}_F$, *com deg* $P = 1$, *e o divisor* $B \in \mathcal{D}_F$; *dizemos que o número natural* γ *é uma* B**-lacuna em** P *se não existe* $x \in F$ *tal que*

$$((x) + B)_\infty = \gamma P\ .$$

Definição 1.5.4 *Na definição acima quando* $B = 0$, *ou seja o divisor nulo, as* B*-lacunas são chamadas de Lacunas de Weierstrass em* P.

[36] Pois $W - (n-1)P - B \leq W - nP - B$.

Definição 1.5.5 *Dados P e B como em (1.5.3), dizemos que n* **é uma ordem em P para B,** *se existe $\omega \in \Omega_F(B)$ tal que $v_P((\omega) - B) = n$.*

Proposição 1.5.6 *Dados $P \in \mathbb{P}_F$, com deg $P = 1$, e o divisor $B \in \mathcal{D}_F$ as seguintes afirmações são equivalentes :*

(a) *n é uma ordem em P para B.*

(b) *$(\omega) - B \sim nP + E$, com $\omega \in \Omega_F$, $E \geq 0$ e $P \notin Supp(E)$.*

Dem. :
Seja n é uma ordem em P para B, por definição temos que existe $\omega' \in \Omega_F(B)$ tal que $v_P((\omega') - B) = n$ então

$$(\omega') \geq B \ \ e \ \ v_P((\omega') - B) = n \ ,$$

logo existe $E \geq 0$ *e* $P \notin Supp(E)$ tal que

$$(\omega') - B \ = \ nP + E \tag{1.32}$$

mas como quaisquer dois divisores conônicos são equivalentes, existe $x \in F\backslash\{0\}$ t.q. $(\omega') = (\omega) - (x)$ então

$$(\omega) - B \ = \ nP + E + (x) \ ,$$

ou seja, $(\omega) - B \sim nP + E$, com $E \geq 0$ e $P \notin Supp(E)$.

Suponhamos que $(\omega) - B \sim nP + E$, para o divisor canônico W, $E \geq 0$ e $P \notin Supp(E)$, então existe $0 \neq x \in F$ tal que

$$(\omega) - B = nP + E + (x) \ ,$$

ou seja,

$$-(x) + (\omega) = (x^{-1}\omega) = nP + E + B \geq B \ ,$$

pois $nP \geq 0$ e $E \geq 0$, portanto por (1.4.17) $(x^{-1}\omega) \in \Omega_F(B)$.

Mais ainda

$$v_P(x^{-1}\omega) = v_P(nP) + v_P(E) + v_P(B) = n + v_P(B) \ ,$$

ou seja,

$$v_P(x^{-1}\omega) - v_P(B) = v_P((x^{-1}\omega) - B) = n \ .$$

Portanto n é uma ordem em P para B.

□

Verificaremos a seguir, algumas situações em que ocorrem B-lacunas.

Lema 1.5.7 *Dados P e B como em (1.5.3) temos que n é uma B-lacuna em P se e somente se*

$$\mathcal{L}((n-1)P + B) = \mathcal{L}(nP + B) \ .$$

Dem. :
Seja n uma B-lacuna em P, como $-nP - B < -nP - B + P$ temos

$$\mathcal{L}((n-1)P + B) \subseteq \mathcal{L}(nP + B) \ .$$

Suponhamos que exista $x \in \mathcal{L}(nP + B)$ com $x \notin \mathcal{L}((n-1)P + B)$, isto é

$$(x) \geq -nP - B \ \ e \ \ (x) < -(n-1)P - B \ ,$$

então $(x) + B = -nP$ Com isso $v_P((x) + B) = -n$ e $v_Q((x) + B) = 0$ para todo $Q \in \mathbb{P}_F$ com $Q \neq P$, portanto

$$((x) + B)_\infty = nP$$

absurdo, pois n é uma B-lacuna em P.

Agora, se $\mathcal{L}((n-1)P + B) = \mathcal{L}(nP + B)$, suponhamos que n não seja uma B-lacuna em P, logo existe $x \in F$ tal que

$$((x) + B)_\infty = nP$$

isto é

$$v_P((x) + B) = -n \ \ e \ \ v_Q((x) + B) \geq 0 \text{ para todo } Q \neq P \ .$$

Logo $x \in \mathcal{L}(nP + B)$ pois,

$$\begin{array}{rcccl} v_P(x) & \geq & -n - v_P(B) & = & -v_P(nP + B) \\ e & & & & \\ v_Q(x) & \geq & -v_Q(B) & = & -v_Q(nP + B) \ , \text{ para } Q \neq P \ , \end{array}$$

mas $x \notin \mathcal{L}((n-1)P + B)$ pois,

$$v_P(x) = -n - v_P(B) < -n + 1 - v_P(B) = -v_P((n-1)P + B) \ .$$

Portanto $\mathcal{L}((n-1)P + B) \neq \mathcal{L}(nP + B)$ o que é um absurdo. Logo, n é uma B-lacuna em P.

□

Proposição 1.5.8 *Sejam $P \in \mathbb{P}_F$, com deg $P = 1$ e $B \in \mathcal{D}_F$ então n é uma B-lacuna em P se e somente se $(n-1)$ é uma ordem em P para B.*

Dem. :
Se n é uma B-lacuna em P, então pelo lema (1.5.7)

$$\mathcal{L}((n-1)P + B) = \mathcal{L}(nP + B) \ ,$$

o que, pela proposicao (1.5.2), nos dá que

$$\mathcal{L}(W - nP - B) \subsetneq \mathcal{L}(W - (n-1)P - B) \ .$$

Onde W é um divisor canônico, logo existe $x \in \mathcal{L}(W - (n-1)P - B) \backslash \mathcal{L}(W - nP - B)$, isto é

$$(x) + W \geq (n-1)P + B \ \ e \ \ (x) + W < nP + B \ ,$$

mas pela definição de divisor canônico e pela proposição (1.4.25) temos

$$(x\omega) - B \geq (n-1)P \ \ e \ \ (x\omega) - B < nP \ ,$$

logo $v_P((x\omega) - B) = n - 1$ e $(x\omega) \in \Omega_F(B)$. Portanto existe

$$x\omega \in \Omega_F(B) \text{ tal que } v_P((x\omega) - B) = n - 1 \ ,$$

ou seja, $n - 1$ é uma ordem em P para B.

Agora, se $n - 1$ é uma ordem em P para B, temos que existe

$$\gamma \in \Omega_F(B) \text{ tal que } v_P((\gamma) - B) = n - 1 \ ,$$

logo

$$v_Q(\gamma)\begin{cases} \geq & v_Q(B) & \text{para } Q \neq P \\ = & n-1+v_P(B) & \text{para } Q = P \end{cases}$$

como quaisquer dois divisores canônicos são equivalentes temos que existe $0 \neq x \in F$ tal que

$$(\gamma) = (\omega) + (x)\ ,$$

onde $W = (\omega)$ é um divisor canônico, com isso temos

$$v_P((x)) = -v_P(W) + (n-1) + v_P(B) = -v_P(W - (n-1)P - B)$$

$$v_Q((x)) \geq -v_Q(W) + v_Q(B) = -v_Q(W) + v_Q((n-1)P) + v_Q(B) = -v_Q(W - (n-1)P - B)\ ,$$

para $Q \neq P$.

Com isso temos que $x \in \mathcal{L}(W - (n-1)P - B)$, mas $x \notin \mathcal{L}((W - nP - B)$, pois

$$v_P(x) = -v_P(W) + (n-1) + v_P(B) < -v_P(\omega) + n + v_P(B) = -v_P(W - nP - B)\ ,$$

logo $\mathcal{L}(W - nP - B) \subsetneq \mathcal{L}(W - (n-1)P - B)$, pela proposição(1.5.2) e pelo lema (1.5.7) n é uma B-lacuna em P.

□

Proposição 1.5.9 *Dado $B \in \mathcal{D}_F$ e $P \in \mathbb{P}_F$, como acima. Então para qualquer $n \geq 2g - deg\ B$, existe $x \in F$ tal que*

$$(\ (x) + B\ )_\infty\ =\ nP\ .$$

Dem. :
Considerando o divisor $(n-1)P + B$, notamos que como $n + deg\ B \geq 2g$ temos

$$deg\ ((n-1)P + B) = (n-1)deg\ P + deg\ B \geq 2g - 1\ ,$$

pelo teorema (1.4.29)

$$dim(\ (n-1)P + B\ ) = deg\ ((n-1)P + B) + 1 - g = n - g + deg\ B\ .$$

Notemos também que o divisor $nP + B$ satisfaz o teorema (1.4.29) logo

$$dim(\ nP + B\ ) = deg\ (nP + B) + 1 - g = n - g + 1 + deg\ B\ .$$

Logo $dim(\ (n-1)P + B\ ) < dim(\ nP + B\ )$, ou seja

$$\mathcal{L}((n-1)P + B) \subsetneq \mathcal{L}(nP + B)\ ,$$

pelo lema (1.5.7) existe $x \in F$ tal que $((x) + B)_\infty = nP$.

□

Em outras palavras, o que a proposição (1.5.9) acima afirma é que, se n é uma B-lacuna então $n \leq 2g - deg\ B - 1$. Observa-se também que, definimos uma B-lacuna como um número natural, então faz sentido afirmar que se $deg\ B \geq 2g$, então não temos B-lacunas. Por esta razão quando nos referirmos a B-lacunas de um corpo de funções de genêro g, estaremos assumindo que B é um divisor com $deg\ B \leq 2g - 1$.

No caso particular de B ser o divisor nulo,[37] temos o seguinte teorema.

[37] $B = 0$, isto é $v_P(B) = 0$, para todo $P \in \mathbb{P}_F$.

Teorema 1.5.10 *[Lacunas de Weierstrass] Suponha que F/K tem gênero $g > 0$ e P é um lugar de grau um. Então existem exatamente g lacunas $i_1 < \cdots < i_g$ em P. E temos que*

$$i_1 = 1 \ \ e \ \ i_g \leq 2g - 1 \, .$$

Dem. :
Pela proposição (1.5.9) temos, se n é uma lacuna em P então

$$0 \leq n \leq 2g - 1 \, .$$

Note que $n = 0$ não é uma lacuna em P pois, para todo $x \in K \subset F$ temos

$$(x)_\infty = 0P \, .$$

Afirmamos que $n = 1$ é uma lacuna em P.
Suponhamos que $n = 1$ não seja uma lacuna em P, logo existe

$$x \in F \text{ tal que } (x)_\infty = 1P \, .$$

Pelo teorema (1.3.15) temos

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

então $F = K(x)$, ou seja F/K é um corpo de funções racionais e pelo exemplo (1.3.23) temos que $g = 0$, mas por hipótese $g > 0$ então $n = 1$ é uma lacuna em P.
Agora, consideremos a seguinte sequência de espaços vetorias

$$\mathcal{L}(\mathbf{0}) \subseteq \mathcal{L}(1P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq \mathcal{L}((2g-1)P) \tag{1.33}$$

Por (1.3.10) sabemos que

$$dim \ \mathcal{L}(\mathbf{0}) = 1 \, ,$$

como $deg \ ((2g-1)P) = 2g - 1$ temos por (1.4.29) que

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

Observamos ainda que, pelo lema (1.3.11)

$$dim \ \mathcal{L}(iP) \leq dim \ \mathcal{L}((i-1)P) + 1 \, ,$$

ou seja, $\mathcal{L}(iP) = \mathcal{L}((i-1)P)$ ou $dim \ \mathcal{L}(iP) = dim \ \mathcal{L}((i-1)P) + 1$.

Em (1.33) há $2g - 1$ inclusões consecutivas, mas como a dimensão dos espaços variam de 1 até g temos que existem $g - 1$ inclusões próprias, o que nos dá

$$(2g - 1) - (g - 1) = g$$

igualdades, ou seja, temos exatamente g números $i \in \{1, \ldots, 2g - 1\}$ tal que

$$\mathcal{L}((i-1)P) = \mathcal{L}(iP) \, .$$

Portanto pelo lema (1.5.7) temos exatamente g lacunas $i_1 < \cdots < i_g$ em P. Com

$$i_1 = 1 \ \ e \ \ i_g \leq 2g - 1 \, .$$

□

Ainda considerando o divisor nulo ($B = \mathbf{0}$) temos a seguinte observação.

Observação 1.5.11 Dado $P \in \mathbb{P}_F$ com $deg\ P = 1$ o conjunto

$$H_P = \{\, n \in \mathbb{N} |\ n \text{ é uma não} - \text{lacuna em } P \,\}$$

é um subsemigrupo de $\mathbb{N}$.[38]

Dem. :

Pela proposição (1.5.9) para todo $n \geq 2g$ temos que $n \in H_P$, logo $H_P \neq \emptyset$.
Agora se n_1, $n_2 \in H_P$ então existem x_1, $x_2 \in F$, não nulos, tal que

$$(x_1)\infty = n_1 P \ \ e \ \ (x_2)\infty = n_2 P\ ,$$

é claro que $x_1 x_2 \in F$ e como

$$(x_1 x_2)\infty = (x_1)\infty + (x_2)\infty = n_1 P + n_2 P = (n_1 + n_2)P\ ,$$

e assim temos que $(n_1 + n_2) \in H_P$.

□

Esta observação juntamente com o teorema (1.5.10) são fundamentais para o cálculo das lacunas de Weierstrass.

Abaixo calcularemos as sequências de lacunas de Weierstrass em alguns lugares particulares. Como sabemos, não temos lacunas em um corpo de funções racionais, portanto buscaremos alguns exemplos em corpos de funções que são extensões de corpos de funções racionais, que definimos e damos as principais propriedades no apêndice B. Vale já comentar aqui que os lugares de grau 1, de tais corpos de funções são extensões dos lugares de grau 1, do corpo de função racionais de que eles se extendem.

Exemplo 1.5.12 *Vamos tomar q como uma potência de 2, por exemplo $q = 2^6$ e consideremos o corpo de funções $F = \mathbb{F}_q(x,y)$ definidos pela equação*

$$y^2 + y = x^9\ ,$$

o genêro deste corpo de funções já é conhecido e vale

$$g = \frac{(9-1)(2-1)}{2} = 4\ .$$

Portanto por (1.5.10), existem exatamente $g = 4$ lacunas

$$1 = i_1 < i_2 < i_3 < i_4 \leq 2g - 1 = 7$$

para todo lugar $P \in \mathbb{P}_F$ de grau 1.

(a) *Vamos calcular as lacunas para Q_∞ , o divisor de polos de x em F. Para isso, como veremos no Apêndice B , consideramos o corpo de funções racionais $F' = \mathbb{F}_q(x)$ e o divisor P_∞ de polos de x em F'.*

Tomemos o polinômio

$$\psi(T) = T^2 + T - x^9 \in \mathbb{F}_q(x)[T]\ ,$$

[38] Quando K é algebricamente fechado, todo $P \in \mathbb{P}_F$ tem grau 1. Logo para qualquer $P \in \mathbb{P}_F$ temos o semigrupo H_P, podemos então considerar o conjunto $\mathcal{G}_P = \mathbb{N} \backslash H_P$. O conjunto $\mathcal{G}_P$ quase independente de P. Para o corpo de funções F/K $\mathcal{G} = \mathcal{G}_F$ é o conjunto das lacunas de F/K. Se caracteristica de K é zero então $\mathcal{G} = \{1, 2, 3, \ldots, g\}$. Apesar de não demonstrarmos aqui, gostariamos de citar que $\mathcal{G} = \mathcal{G}_P$ para quase todo $P \in \mathbb{P}_F$. Um lugar $P \in \mathbb{P}_F$ é dito ser um lugar de Weierstrass de F/K se $\mathcal{G}_P \neq \mathcal{G}$.

por (A.1.1) temos

$$v_{P_\infty}(1) = 0 \ \ e \ \ v_{P_\infty}(x^9) = -9 < 0$$

então pela condição 2 de (B.1.11) $\psi(T)$ *é irredutível.*

Notemos que $\psi(y) = 0$ *, logo* y *é uma raiz de* $\psi(T)$ *, então ainda por (B.1.11)* P_∞ *tem uma única extensão* $Q_\infty \in \mathbb{P}_F$ *e*

$$v_{Q_\infty}(x) = deg\ (\psi(T))v_{P_\infty}(x) = 2v_{P_\infty}(x)\ ,$$

como P_∞ *é o único polo de* x*, temos que*

$$(x)_\infty = 2Q_\infty\ ,$$

logo 2 é uma não-lacuna em Q_∞ *, então por (1.5.11) 2, 4, 6 são não-lacunas em* Q_∞*.*
Portanto a sequência de lacunas em Q_∞ *são*

$$1,\ 3,\ 5,\ 7\ .$$

Continuaremos a considerar o mesmo corpo de funções $F = \mathbb{F}_q(x,y)$ *acima definido.*

(b) *Vamos calcular a sequência de lacunas de um outro lugar* $Q \in \mathbb{P}_F$ *diferente de* Q_∞*.*
Para isto vamos considerar P_0 *o divisor de zeros de* x *em* $\mathbb{F}_q(x)$*, logo*

$$v_{P_0}(x) = 1 > 0\ .$$

Como $[F : \mathbb{F}_q(x)] = 2$ *, pois* $\psi(T) = T^2 + T - x^9 \in \mathbb{F}_q(x)[T]$ *é irredutível, como vimos acima. Pelo teorema (B.1.9) temos que* P_0 *possui apenas 2 extensões* $Q_1,\ Q_2 \in \mathbb{P}_F$ *tais que*

$$v_{Q_i}(\alpha) = v_{P_0}(\alpha) \tag{1.34}$$

para todo $\alpha \in \mathbb{F}_q(x)$*, e* $i = 1, 2$*.*
Observamos que, para $i = 1, 2$*, temos*

$$v_{Q_i}(y^2 + y) = v_{Q_i}(x^9) = v_{P_0}(x^9) = 9 > 0$$

ou seja,

$$v_{Q_i}(y^2 + y) = v_{Q_i}(y) + v_{Q_i}(y + 1) = 9 \tag{1.35}$$

mais ainda

$$v_{Q_i}(y + 1) = min\{\ v_{Q_i}(y), v_{Q_i}(1) = 0\ \}$$

para $i = 1, 2$*. Agora se* $v_{Q_i}(y) < 0$*, então* $v_{Q_i}(y + 1) < 0$ *o que é um absurdo por (1.35). Portanto*

$$\begin{array}{c} v_{Q_i}(y) > 0 \implies v_{Q_i}(y + 1) = 0 \\ \quad rmou \\ v_{Q_i}(y) = 0 \implies v_{Q_i}(y + 1) > 0 \end{array}$$

Podemos supor então que

$$v_{Q_1}(y) = 9 \ \ e \ \ v_{Q_1}(y + 1) = 0 \tag{1.36}$$

Vamos calcular a sequência das lacunas em $Q_1 \in \mathbb{P}_F$*, para isto consideremos*

$$\alpha_1 = \frac{x^2}{y} \in \mathbb{F}_q(x,y)\ ,$$

temos por (1.34) e (1.36) que

$$v_{Q_1}(\alpha_1) = v_{Q_1}(x^2) - v_{Q_1}(y) = 2v_{P_0}(x) - 9 = -7 \tag{1.37}$$

Agora, observamos que, por (1.3.3) para todo $\alpha \in F$

$$(\alpha)_\infty \geq -v_P(\alpha)P \ ,$$

onde P *é um polo de* α*, pela definição do grau de um divisor, vale*

$$deg\ ((\alpha)_\infty) \geq -v_P(\alpha) \ ,$$

logo de (1.37)

$$7 \leq deg\ ((\alpha)_\infty) \tag{1.38}$$

Tomemos o polinômio

$$\psi_1(T) = T^7 - \left(\frac{y}{x^2}\right)^2 T^2 - \frac{y}{x^2} \ \in \ I\!F_q\left(\frac{y}{x^2}\right) = I\!F_q\left(\frac{x^2}{y}\right)$$

observamos que x *é raiz de* $\psi_1(T)$*, pois*

$$\psi_1(x) = x^7 - x^2\frac{y^2}{x^4} - \frac{y}{x^2} = \frac{x^9}{x^2} - \frac{y^2}{x^2} - \frac{y}{x^2} = 0 \ .$$

Portanto

$$\left[F : I\!F_q\left(\frac{x^2}{y}\right)\right] \leq 7 \ ,$$

então pelo teorema (1.3.15) e por (1.38) vale

$$7 \leq deg\ (\alpha_1) = [F : I\!F_q(\alpha_1)] \leq 7$$

e com isso obtemos que

$$(\alpha_1)\infty = 7Q_1 \ ,$$

ou seja, 7 é uma não-lacuna em Q_1*.*

Da mesma forma, tomando

$$\alpha_2 = \frac{x^3}{y} \ \ e \ \ \alpha_3 = \frac{x^4}{y} \text{ em } I\!F_q(x,y)$$

e considerando os polinômios

$$\psi_2(T) = T^6 - \left(\frac{y}{x^3}\right)^2 T^3 - \frac{y}{x^3}$$

$$\psi_3(T) = T^5 - \left(\frac{y}{x^4}\right)^2 T^4 - \frac{y}{x^4}$$

respectivamente em $I\!F_q\left(\frac{y}{x^3}\right) = I\!F_q\left(\frac{x^3}{y}\right)$ *e* $I\!F_q\left(\frac{y}{x^4}\right) = I\!F_q\left(\frac{x^4}{y}\right)$*. Obtemos que*

$$(\alpha_2)\infty = 6Q_1 \ \ e \ \ (\alpha_3)\infty = 5Q_1 \ .$$

Portanto a sequência de lacunas em $Q_1 \in I\!P_F$ *é*

$$1,\ 2,\ 3,\ 4 \ .$$

O cálculo das sequências de lacunas de um lugar num corpo de funções arbitrário, nem sempre é simples, mas como veremos, as sequência de lacunas serão fundamentais no Capítulo 3.

Capítulo 2

Introdução aos Códigos de Goppa

Como o próprio título do capítulo sugere apresentaremos uma introdução aos Códigos Geométricos de Goppa, ou códigos de Goppa como são mais conhecidos, descrevendo a construção de Goppa para códigos corretores de erros, usando corpos de funções algébricas.

2.1 Códigos

Iniciaremos com um estudo dos principais conceitos da Teoria dos Códigos. Seja $\mathbb{F}_q$ um corpo finito com q elementos.[1] Consideramos ${\mathbb{F}_q}^n$ o espaço vetorial n-dimensional, cujos elementos são n-uplas $a \in {\mathbb{F}_q}^n$ onde $a = (a_1, \ldots, a_n)$ com $a_i \in \mathbb{F}_q$.

Definição 2.1.1 *Para todo* $a = (a_1, \ldots, a_n)$ *e* $b = (b_1, \ldots, b_n)$ *pertencentes a* ${\mathbb{F}_q}^n$, *definimos*

$$d(a,b) = \#\{i |\ a_i \neq b_i,\ 1 \leq i \leq n\ \}$$

como a **distância de Hamming sobre** ${\mathbb{F}_q}^n$. *E definimos*

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

como o **peso** *de um elemento* $a \in {\mathbb{F}_q}^n$.

Observação 2.1.2 A distância de Hamming é uma métrica em ${\mathbb{F}_q}^n$.

A demonstração desta observação é trivial e não a faremos aqui.[2]

Definição 2.1.3 *Um* **código** C, *sobre* $\mathbb{F}_q$ *é um subespaço linear de* ${\mathbb{F}_q}^n$. *Os elementos de* C *são chamados* **palavras código**, n *é o* **comprimento de** C *e* $dim\ C$ *é a* **dimensão de** C *visto como* $\mathbb{F}_q$*-espaço vetorial.*

Em geral um código é definido sobre um alfabeto A, onde A é um conjunto finito qualquer, mas aqui consideraremos o alfabeto $A = \mathbb{F}_q$, e como consequência disto os códigos aqui considerados serão *códigos lineares.*

Definição 2.1.4 *A* **distância mínima** $d(C)$ *de um código* $C \neq 0$ *é definida por*

$$d(C) = min\{\ d(a,b) |\ a,b \in C,\ a \neq b\ \} = min\{\ \omega(c) |\ 0 \neq c \in C\ \}.^3$$

[1] Onde $q = p_i$ com p um número primo e i um inteiro positivo.

[2] Em particular temos a *Desigualdade Triangular* $d(a,c) \leq d(a,b) + d(b,c)$ para todo $a,b,c \in {\mathbb{F}_q}^n$.

[3] Pois $d(a,b) = d(a-b,0) = \omega(a-b)$ e C é um espaço linear.

Notação : Um $[n,k,d]$-código é um código de comprimento n, dimensão k e distância mínima d.

Definição 2.1.5 *A* **ditribuição dos pesos** *de um $[n,k,d]$-código é a $(n+1)$-upla*

$$(A_0,\ldots,A_n) \in \mathbb{N}^{n+1}, \text{ onde } A_i = \#\{\, c \in C \mid \omega(c) = i \,\}\,.$$

Como C é um espaço vetorial, seu elemento neutro é único logo,

$$A_0 = 1 \text{ e } A_i = 0 \text{ para } 1 \leq i \leq d(C) - 1\,.$$

Definição 2.1.6 *O polinômio*

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

é chamado o **enumerador de peso de C**.

Para um $[n,k,d]$-código C, definimos o inteiro $t = [(d-1)/2]$, onde $[x]$ denota a parte inteira do número real x, como o número máximo de erros que C pode corrigir. Em outras palavras temos :

Proposição 2.1.7 *Seja C um $[n,k,d]$-código. Então C pode corrigir até t erros e detectar até $d-1$ erros.*

Dem. :
Se $u \in \mathbb{F}_q{}^n$ e $d(u,c) \leq t$ para algum $c \in C$, então c é a única palavra do código com $d(u,c) \leq t$. De fato, suponhamos que exista $c' \in C$, $c' \neq c$, tal que $d(u,c') \leq t$, logo

$$d(c,c') \leq d(u,c) + d(u,c') \leq t + t = 2\left[\frac{d-1}{2}\right] = d - 1 < d\,,$$

então $d(c,c') < d$ absurdo, pois d é a distância mínima de C.
Claramente se $c \in \mathbb{F}_q{}^n$ tal que $d(u,c) \leq d-1$ para algum $u \in C$ então sabemos que $c \notin C$

□

Neste caso C é dito ser um código corretor de t erros.

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

Definição 2.1.8 *Seja C um $[n,k,d]$-código sobre $\mathbb{F}_q{}^n$. Uma* **matriz geradora de C** *é uma matriz $k \times n$, cujas linhas formam uma base de C.*

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

$$< a,b >= \sum_{i=1}^{n} a_i\, b_i$$

para $a = (a_1,\ldots,a_n)$ e $b = (b_1,\ldots,b_n)$ em $\mathbb{F}_q{}^n$. Pela álgebra linear temos que esta é uma forma bilinear simétrica não degenerada sobre $\mathbb{F}_q{}^n$.

Definição 2.1.9 *Se $C \subseteq \mathbb{F}_q{}^n$ é um código, então*

$$C^{\perp} = \{\, u \in \mathbb{F}_q{}^n \mid < u,c >= 0, \text{ para todo } c \in C \,\}$$

é chamado o **código dual de C**.
C é chamado **auto-dual** *(respect.* **auto-ortogonal** *) se $C = C^{\perp}$ (respec. $C \subseteq C^{\perp}$).*

Pela álgebra linear temos que o dual de um $[n,k]$-código é um $[n,n-k]$-código e ainda $(C^{\perp})^{\perp} = C$. Em particular, a dimensão de um código auto-dual de comprimento n é $n/2$.

Definição 2.1.10 *Uma matriz geradora H do código $C^{\perp}$ é dita* **matriz teste de paridade** *de C.*

Observação 2.1.11 Seja H uma matriz teste de paridade de um $[n,k]$-código C, temos :

(i) H é uma matriz, $(n-k) \times n$ com posto $n-k$.

(ii) Podemos descrever C como

$$C = \{ u \in \mathbb{F}_q{}^n | \; H.u^t = 0 \} ,$$

onde u^t denota o transposto de u.

Dem. :

(i) Por definição H é a matriz geradora de um $[n,n-k]$-código, ou seja é uma matriz $n-k \times n$, onde suas linhas formam uma base para o espaço vetorial $C^{\perp}$, pela álgebra linear o posto de H é $n-k$.

(ii) H é a matriz geradora de $C^{\perp}$, logo para todo $c \in C$ temos $< u_i, c >= 0$ para $i = 1, \ldots, n-k$, onde $u_i's$ são vetores da base de $C^{\perp}$ então $H.c^t = 0$ para todo $c \in C$.

□

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

Observamos que códigos interessantes são aqueles que possuem dimensão e distância mínima grandes em comparação com o seu comprimento. Um dos problemas fundamentais na teoria de códigos é estudar a interdependência entre estes três valores.

Uma das relações mais simples é a seguinte .

Proposição 2.1.12 (Cota de Singleton) *Para um $[n,k,d]$-código C vale*

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

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

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

logo para qualquer $a \in W \subseteq \mathbb{F}_q{}^n$ a definição do peso de um elemento nos garante

$$\omega(a) \leq d - 1 ,$$

mas $d \leq \omega(c)$, para todo $c \in C$, ou seja $W \cap C = 0$. Como $dim(W) = d-1$, obtemos

$$k + (d-1) \;=\; dim(C) + dim(W) \;=\; dim(C+W) + dim(C \cap W) \;=\; dim(C+W) \;\leq\; n$$

pois $C + W \subseteq \mathbb{F}_q{}^n$. Portanto, vale o resultado.

□

Códigos com $k + d = n + 1$ são , de certa forma, considerados ótimos. Tais códigos são chamados *códigos MDS (maximum distance separable)*. Mostraremos mais adiante que se $n \leq q + 1$, então existem códigos MDS sobre $\mathbb{F}_q$ para toda dimensão $k \leq n$.

A cota de Singleton não considera o tamanho q do alfabeto. No entanto existem outras cotas para k e d, envolvendo n e q, elas são melhores que a cota de Singleton se n é suficientemente grande em relação a q.

Aquí, estaremos interessados em obter cotas para a distância mínima de certos códigos, que definiremos a seguir.

2.2 Códigos Geométricos de Goppa

Introduziremos agora a noção de Código Geometricos de Goppa . Para isto, fixemos algumas notações que usaremos no decorrer da seção .

$F/\mathbb{F}_q$ é um corpo de funções algébricas de gênero g.
$P_1, \ldots, P_n \in \mathbb{P}_F$, dois a dois distintos, com $deg\ P_i = 1$ para $i = 1, \ldots, n$.
$D = P_1 + \ldots + P_n$.
$G \in \mathcal{D}_F$ um divisor tal que $SuppG \cap SuppD = \emptyset$.

Definição 2.2.1 *O* **Código Geométrico de Goppa** $C_{\mathcal{L}}(G, D)$ *associado aos divisores* D *e* G *é definido por*

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

Notação : Na literatura os código geometrico de Goppa são conhecidos ainda como códigos de Goppa , e é assim que vamos nos referir a eles.

Observe que esta definição faz sentido pois, para todo

$$x \in \mathcal{L}(G) \text{ temos } v_{P_i}(x) \geq -v_{P_i}(G) = 0 \text{ para qualquer } i = 1, \ldots, n\ ,$$

pois $SuppD \cap SuppG = \emptyset$. Logo, a classe residual $x(P_i) = x + P_i \in F_{P_i}$ mas pela definição (1.1.18) como o $deg\ P_i = 1$ temos

$$x(P_i) \in F_{P_i} = \mathbb{F}_q \text{ para } i = 1, \ldots, n\ .$$

Com isto podemos definir a seguinte aplicação .

Definição 2.2.2 *Definimos a aplicação*

$$\begin{array}{rccc} ev_D : & \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q{}^n \\ & x & \longmapsto & (x(P_1), \ldots, x(P_n)) \end{array} \tag{2.1}$$

como a **aplicação de avaliação** .

A aplicação de avaliação ev_D é $\mathbb{F}_q$-linear[4] e $C_{\mathcal{L}}(G, D)$ é naturalmente a imagem de $\mathcal{L}(G)$ por ev_D, ou seja

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

Para o caso particular em que $n = q - 1$ e $1 \leq deg\ G \leq n$ temos o código de *Reed-Solomon* , um código sobre um corpo de funções racionais que veremos na próxima seção .

[4]Para cada $i = 1, \ldots, n$ a classe residual em F_{P_i} satisfaz

$$(tx + y)P_i = (tx + P_i) + (y + P_i) = tx(P_i) + y(P_i)\ .$$

Teorema 2.2.3 *$C_{\mathcal{L}}(G,D)$ é um $[n,k,d]$-código com parâmetros*

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

Dem. :

Considerando $ev_D : \mathcal{L}(G) \longrightarrow \mathbb{F}_q{}^n$ definida em (2.1) sabemos da álgebra linear que,

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

Logo,

$$dim(G) - dim(\ Ker(ev_D)\ ) = dim(C_{\mathcal{L}}(G,D)) = k\ ,$$

onde

$$Ker(ev_D) = \{\ f \in \mathcal{L}(G) |\ f(P_i) = 0,\ i = 1,\ldots,n\ \}\ ,$$

logo, se $f \in Ker(ev_D)$ então

$$v_Q(f) \geq -v_Q(G) \ \ e\ \ v_{P_i}(f) > 0 \text{ para } i = 1,\ldots,n$$

mas como $SuppD \cap SuppG = \emptyset$, temos que, para todo $Q \in \mathbb{P}_F$ vale

$$\begin{array}{rcl} v_Q(f) & \geq & -v_Q(G) = -v_Q(G) + v_Q(D) \quad \text{se} \quad Q \notin \{P_1,\ldots,P_n\} \\ v_Q(f) & \geq & 1 \ = \ -v_Q(G) + v_Q(D) \quad \text{se} \quad Q \in \{P_1,\ldots,P_n\} \end{array}$$

então $Ker(ev_D) \subseteq \mathcal{L}(G-D)$.

Agora, se $x \in \mathcal{L}(G-D) \subseteq \mathcal{L}(G)$ temos

$$v_{P_i}(x) \ \geq \ -v_{P_i}(G) + v_{P_i}(D) = 1 > 0 \text{ para } i = 1,\ldots,n\ ,$$

logo, $x \in \mathcal{L}(G)$ e $v_{P_i}(x) > 0$ para $i = 1,\ldots,n$. Portanto,

$$Ker(ev_D) = \mathcal{L}(G-D)\ .$$

Segue que $k = dim(G) - dim(G-D)$.

Vamos assumir agora que $C_{\mathcal{L}}(G,D) \neq 0$, pois do contrário não tem sentido falar em distância mínima. Então ,seja $x \in C_{\mathcal{L}}(G,D)$ tal que $\omega(x) = d$, como $C_{\mathcal{L}}(G,D) = Im(ev_D)$ existe $0 \neq f \in \mathcal{L}(G)$ tal que

$$\omega(ev_D(f)) = n - \#\{i |\ f(P_i) = 0\} = d\ ,$$

depois de uma reordenação dos $P_i's$, se necessário, podemos supor que $f(P_1) = \cdots = f(P_{n-d}) = 0$, logo

$$0 \neq f \in \mathcal{L}(\ G - \sum_{i=1}^{n-d} P_i\ )\ ,$$

pelo corolário (1.3.16.b)

$$0 \leq deg\ (\ G - \sum_{i=1}^{n-d} P_i\ ) = deg\ G - (n-d)\ ,$$

ou seja $d \geq n - deg\ G$.

□

Corolário 2.2.4 *Suponha que $deg\ G < n$. Então a aplicação de avaliação $ev_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(G,D)$ é injetiva e temos :*

(a) *$C_{\mathcal{L}}(G,D)$ 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,

$$k + d \ \geq \ n + 1 - g \tag{2.2}$$

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

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

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

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

Dem. :
Temos por hipótese que $deg\ (G - D) = deg\ G - n < 0$, logo por (1.3.16.b) vale

$$0 \ = \ \mathcal{L}(g - D) \ = \ Ker(ev_D)\ ,$$

ou seja, ev_D é injetiva.

(a) Pelo teorema (2.2.3) $C_{\mathcal{L}}(G,D)$ é um $[n,k,d]$-código com

$$k = dim(G) - dim(G - D) \ \ e \ \ d \geq n - deg\ G\ .$$

Como ev_D é injetiva $dim(G - D) = 0$, logo pelo teorema (1.3.22) temos

$$k = dim(G) \geq deg\ G + 1 - g \geq n - d + 1 - g\ .$$

(b) Se $2g - 2 < deg\ G$, então pelo teorema (1.4.29)

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

(c) $\{x_1, \ldots, x_n\}$ é base de $\mathcal{L}(G)$ então $(x_i(P_1), \ldots, x_i(P_n)) \in C_{\mathcal{L}}(G,D)$, $i = 1, \ldots, n$ e como ev_D é injetiva, $\mathbb{F}_q$-linear e $dim(G) = dim(\ C_{\mathcal{L}}(G,D)\ )$, então, ev_D preserva bases; logo, se $\{\ (x_i(P_1), \ldots, x_i(P_n)) |\ i = 1, \ldots, k\ \}$ é uma base de $C_{\mathcal{L}}(G,D)$, então M é a matriz geradora de $C_{\mathcal{L}}(G,D)$.

□

Observamos que a cota inferior (2.2) para a distância mínima é muito parecida com a cota superior de Singleton. Logo para $deg\ G < n$, temos da proposição (2.1.12) e do corolário (2.2.4) que

$$n + 1 - g \ \leq \ k + d \ \leq \ n + 1 \tag{2.3}$$

Observe 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 de Goppa construídos por meio de um corpo de funções racionais são sempre MDS.

De fato, para se obter uma cota significativa para a distância mínima de $C_{\mathcal{L}}(G,D)$, pelo teorema (2.2.3) basta assumir que $deg\ G < n$.

Ainda pelo teorema (2.2.3) temos que a distância mínima d de um código de Goppa não pode ser menor do que $n - deg\ G$.

Vamos analizar na observação seguinte quando $d = n - deg\ G$ ou $d > n - deg\ G$.

Observação 2.2.5 *Suponha que* $dim(G) > 0$ *e* $d \geq n - deg\ G > 0$. *Então,* $d = n - deg\ G$ *se e somente se existe um divisor* $D' \in \mathcal{D}_F$ *com*

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

Dem. :
Primeiro, suponhamos $d = n - deg\ G$.[5] Seja $0 \neq x \in \mathcal{L}(G)$ tal que $\omega(ev_D(x)) = d$. Então, $ev_D(x) = (x(P_1), \ldots, x(P_n))$, onde depois de reenumerar os $P_i's$, se necessário, temos $x(P_1) = \cdots = x(P_{deg\ G}) = 0$.
Tomemos

$$D' = \sum_{i=1}^{deg\ G} P_i\ '$$

então

$$deg\ D' = \sum_{i=1}^{deg\ G} v_{P_i}(D')deg\ (P_i) = \underbrace{1 + 1 + \cdots + 1}_{deg\ G\ \text{parcelas}} = deg\ G\ '$$

claramente $0 \leq D' \leq D$ e como na demonstração do teorema (2.2.3) temos $x \in \mathcal{L}(G - D')$ logo, $dim(G - D') > 0$.
Agora seja $D' \in \mathcal{D}_F$ tal que

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

logo, existe $y \in \mathcal{L}(G - D')$ com isso o peso da palavra-código $(y(P_1), \ldots, y(P_n))$ é $n - deg\ G \geq d$, pela definição do peso, com isso e pelo teorema (2.2.3) temos $d = n - deg\ G$.

□

Dados os divisores G e D, podemos associar a eles um outro código, por meio das componentes locais das diferenciais de Weil definidas no Capítulo I, estes códigos são conhecidos como códigos originais de Goppa. Para isto, relembramos algumas notacões :

Para $A \in \mathcal{D}_F$ o conjunto $\Omega_F(A)$ é um $\mathbb{F}_q$-espaço vetorial de dimensão $i(A)$ (índice de especialidade).

Para uma diferencial ω e um lugar $P \in \mathbb{P}_F$, $\omega_P : F \longrightarrow \mathbb{F}_q$ denota a componente local de ω em P.

Definição 2.2.6 *Sejam* G *e* $D = P_1 + \ldots + P_n$ *divisores como definido anteriormente. Então, definimos o código* $C_\Omega(G,D) \subseteq \mathbb{F}_q{}^n$ *por*

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

[5] Novamente observamos que não tem sentido falar em distância mínima se $\mathcal{L}(G) = 0$.

O próximo teorema é análogo ao teorema (2.2.3), mas antes de enunciá -lo vamos demonstrar o seguinte lema.

Lema 2.2.7 *Consideremos um corpo de funções F/K qualquer. Sejam $P \in \mathbb{P}_F$, com deg $P = 1$ e $\omega \in \Omega_F$ um diferencial de Weill tal que $v_P(\omega) \geq -1$. Então*

$$\omega_P(1) = 0 \text{ se e somente se } v_P(\omega) \geq 0 .$$

Dem. :
Suponhamos primeiramente que $v_P(\omega) \geq 0$, logo pela proposição (1.4.24) temos

$$\omega_P(x) = 0 \text{ para todo } x \in F \text{ com } v_P(x) \geq 0 ,$$

mas $1 \in K \subset F$ e $v_P(1) = 0$, portanto $\omega_P(1) = 0$.

Agora, suponhamos que $\omega_P(1) = 0$, com isso temos que

$$\omega_P(a) = a\omega_P(1) = 0 \text{ para todo } a \in K .$$

Pelo teorema (1.2.1) existe $x \in F$ tal que $v_P(x) \geq 0$, ou seja $x \in O_P$, como *deg* $P = 1$ temos que $O_P/P = K$. Logo podemos escrever $x - y = a$, com $y \in P$ e $a \in K$, isto é

$$v_P(y) \geq 1 \ \ e \ \ v_P(a) = 0 .$$

Observamos ainda que $v_P(\omega) \geq -1$, por hipótese, e $v_P(y) \geq 1$ então pela proposição (1.4.24) $\omega_P(y) = 0$. Com isso,

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

Novamente pela proposição (1.4.24) temos $v_P(\omega) \geq 0$ e o lema está provado.

□

Teorema 2.2.8 *$C_\Omega(G, D)$ é um $[n, k', d']$-código com parâmetros*

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

E ainda temos :
Se deg $G > 2g - 2$, então $k' = i(G - D) \geq n + g - 1 - deg\ G$.
Se $2g - 2 < deg\ G < n$, então $k' = n + g - 1 - deg\ G$.

Dem. :

Consideremos a seguinte aplicação

$$\begin{array}{rccl} \varphi : & \Omega_F(D - G) & \longrightarrow & \mathbb{F}_q{}^n \\ & \omega & \longmapsto & \varphi(\omega) = (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \end{array}$$

como cada componente local ω_{P_i} é uma aplicação $\mathbb{F}_q$-linear, temos que φ é $\mathbb{F}_q$-linear e claramente $Im(\varphi) = C_\Omega(G, D)$.

Agora, seja $\omega \in Ker(\varphi)$, ou seja,

$$\omega \in \Omega_F(G - D) \text{ tal que } \omega_{P_i}(1) = 0 \text{ para } i = 1, \ldots, n ,$$

logo $(\omega) \geq G - D$ e pelo lema (2.2.7) $v_{P_i}(\omega) \geq 0$ para $i = 1, \ldots, n$, então para qualquer $Q \in \mathbb{P}_F$ vale

$$\begin{array}{lll} v_Q(\omega) \geq v_Q(G) - v_Q(D) = v_Q(G) & \text{se} & Q \notin \{P_1, \ldots, P_n\} \\ v_Q(\omega) \geq 0 = v_Q(G) & \text{se} & Q \in \{P_1, \ldots, P_n\} \end{array}$$

então $\omega \in \Omega_F(G)$.

Se $\omega \in \Omega_F(G) \subseteq \Omega_F(G - D)$, então

$$v_{P_i}(\omega) \geq v_{P_i}(G) = 0 \text{ para } i = 1, \ldots, n \ ,$$

pelo lema (2.2.7) $\omega_{P_i}(1) = 0$ para $i = 1, \ldots, n$. Portanto, $Ker(\varphi) = \Omega_F(G)$.

Com isto, temos pela álgebra linear que

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

Mas pelo lema (1.4.15) temos

$$dim(\Omega_F(G - D)) = i(G - D) \ \ e \ \ dim(\Omega_F(G)) = i(G) \ ,$$

então

$$k' = i(G - D) - i(G) \ . \tag{2.4}$$

Consideremos $\varphi(\omega) \in C_\Omega(G, D)$, com $\omega \neq 0$ uma palavra-código com peso $m > 0$, então depois de reenumerar os $P_i's$, se necessário, podemos afirmar que

$$\omega_{P_i}(1) = 0 \text{ para } i = 1, \ldots, n - m \ .$$

De maneira análoga a demonstração de que $Ker(\varphi) = \Omega_F(G)$ temos

$$0 \neq \omega \in \Omega_F(G - (D - \sum_{i=1}^{n-m} P_i)) \ .$$

Logo, $\Omega_F(G - (D - \sum_{i=1}^{n-m} P_i)) \neq 0$ então $i(G - (D - \sum_{i=1}^{n-m} P_i)) > 0$.
Portanto pelo teorema (1.4.29)

$$deg \ (G - (D - \sum_{i=1}^{n-m} P_i)) \leq 2g - 2 \ ,$$

ou seja,

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

Logo

$$m \geq deg \ G - (2g - 2) \tag{2.5}$$

Como (2.5) vale para qualquer $m > 0$ temos que vale também para a distância mínima d, ou seja,

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

Supondo que $deg\ G > 2g - 2$, pelo teorema (1.4.29) temos que

$$0 = dim(G) - deg\ G + 1 - g = i(G)\ .$$

Logo a equação(2.4) e a definição (1.4.1) nos afirma que

$$k' = i(G - D) = dim(G - D) - deg\ (G - D) + g - 1\ .$$

Com $dim(G - D) \geq 0$ temos

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

Se ainda $deg\ G < n$, temos $deg\ (G - D) < 0$ e então por (1.3.16.b) $dim(G - D) = 0$ e com isto ,

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

e o teorema esta demonstrado.

□

Na próxima seção estudaremos os códigos de Goppa, para o caso particular, em que o corpo de funções é um corpo de funções racionais $\mathbb{F}_q(x)/\mathbb{F}_q$.

Apesar de não demonstrarmos neste trabalho, existe uma relação que é muito importante na teoria de códigos, e enunciaremos abaixo.

Teorema 2.2.9 *Os códigos $C_\Omega(G, D)$ e $C_\Omega(G, D)$ são duais entre si, isto é,*

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

2.3 Construção dos Códigos de Goppa sobre Corpos de Funções Racionais

Nesta seção mostraremos explicitamente a descrição dos códigos de Goppa no caso particular em que o corpo de funções é um corpo de funções racionais. Na teoria de códigos esta classe de códigos é conhecida como *códigos Reed-Solomon Generalizados* .

As notações utilizadas serão as mesmas da seção anterior, só que agora trabalharemos com o corpo de funções racionais $\mathbb{F}_q(z)/\mathbb{F}_q$.[6]

Definição 2.3.1 *Um código de Goppa $C_\mathcal{L}(G, D)$ associado aos divisores D e G de um corpo de funções racionais $\mathbb{F}_q(x)/\mathbb{F}_q$ é dito ser um* **código geometrico racional de Goppa**.

Notação : Denotaremos um código geometrico racional de Goppa por código de Goppa racional.

Observação 2.3.2 Se n é o comprimento de $C_\mathcal{L}(G, D)$, então $n \leq q + 1$.

Dem. :
De fato, pela proposição (A.1.1) do apêndice A, os lugares de grau 1 de $\mathbb{F}_q(z)$ são P_∞ o polo de z e para cada $\alpha \in \mathbb{F}_q$ o zero P_α de $z - \alpha$, mas $\#(\mathbb{F}_q) = q$, logo $\mathbb{F}_q(z)$ possui somente $q + 1$ lugares de grau 1, ou seja, $n \leq q + 1$.

O resultado a seguir faz uma sinopse da seção anterior.

[6] Lembrando que o gênero de $\mathbb{F}_q(z)/\mathbb{F}_q$ é $g = 0$.

Proposição 2.3.3 *Seja* $C = C_{\mathcal{L}}(G, D)$ *um código de Goppa racional sobre* $\mathbb{F}_q$, *e sejam* n, k, d *os parâmetros de* C. *Então,*

(a) $n \leq q + 1$.

(b) $k = 0$ *se e so se* $deg\ G < 0$, *e* $k = n$ *se e so 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 MDS-código.

Dem. :

(a) É a observação (2.3.2).

(b) **(i)** Suponhamos $k = 0$. Pelo corolário (2.2.4) e pelo teorema (1.3.22) temos

$$k = dim(G) \geq deg\ G + 1 - g\ ,$$

logo como $g = 0$, então $0 \geq deg\ G + 1$, ou seja $deg\ G < 0$.
Agora, se $deg\ G < 0 < n$, pelo corolário (2.2.4)

$$k = dim(G)\ ,$$

mas do corolário (1.3.16) $0 = dim(G) = k$.

(ii) Seja $k = n$. Pela cota de Singleton, temos

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

então $d \leq 1$. Pelo teorema (2.2.3)

$$deg\ G \ \geq \ n - d \ \geq n - 1 \ > \ n - 2\ .$$

Se $deg\ G > n - 2$, como $n > 0$ temos

$$deg\ G \ > \ -1 = 2g - 1 \ \ e \ \ deg\ (G - D) \ = \ deg\ G - n \ > \ -2 = 2g - 2\ ,$$

então do teorema (1.4.29) obtemos

$$dim(G) \ = \ deg\ G + 1 \ \ e \ \ dim(G - D) \ = \ deg\ (G - D) + 1 \ = \ deg\ G - n + 1\ ,$$

mas de (2.2.3)

$$k \ = \ dim(G) - dim(G - D) \ = \ deg\ G + 1 - (deg\ G - n + 1) \ = \ n\ .$$

(c) Suponhamos $0 \leq deg\ G \leq n - 2$, ou seja,

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

Pelo corolário (2.2.4)

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

Agora, pelo teorema (2.2.3) $d \geq n - deg\ G$, mas por (2.1.12)

$$d \ \leq \ n - k + 1 \ = \ n - deg\ G\ .$$

Portanto, $d = n - deg\ G$.
Em particular, $n - d = k - 1$, ou seja C é um MDS-código.

□

Temos ainda que $C^{\perp}$ é também um código de Goppa racional. Todavia, não iremos considerá - lo neste trabalho.

Determinaremos, a seguir, a matriz geradora para código de Goppa racional.

Proposição 2.3.4 *Seja $C = C_{\mathcal{L}}(G, D)$ um Goppa Código Racional sobre $\mathbb{F}_q$ com parâmetros n, k e d.*

(a) *Se $n \leq q$ existem elementos dois a dois distintos $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ e $u_1, \ldots, u_n \in \mathbb{F}_q \setminus \{0\}$, não necessariamente distintos, tais que*

$$C = \{ (u_1 f(\alpha_1), \ldots, u_n f(\alpha_n)) \mid f \in \mathbb{F}_q[z] \text{ e } deg\ f \leq k-1 \} .$$

A matriz

$$M = \begin{pmatrix} u_1 & u_2 & \ldots & u_n \\ \alpha_1 u_1 & \alpha_2 u_2 & \ldots & \alpha_n u_n \\ \alpha_1^2 u_1 & \alpha_2^2 u_2 & \ldots & \alpha_n^2 u_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} u_1 & \alpha_2^{k-1} u_2 & \ldots & \alpha_n^{k-1} u_n \end{pmatrix} \tag{2.6}$$

é uma matriz geradora de C.

(b) *Se $n = q+1$, C possui uma matriz geradora*

$$M = \begin{pmatrix} u_1 & u_2 & \ldots & u_{n-1} & 0 \\ \alpha_1 u_1 & \alpha_2 u_2 & \ldots & \alpha_{n-1} u_{n-1} & 0 \\ \alpha_1^2 u_1 & \alpha_2^2 u_2 & \ldots & \alpha_{n-1}^2 u_{n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{k-1} u_1 & \alpha_2^{k-1} u_2 & \ldots & \alpha_{n-1}^{k-1} u_{n-1} & 1 \end{pmatrix}$$

onde $\mathbb{F}_q = \{ \alpha_1, \ldots, \alpha_{n-1} \}$ e $u_1, \ldots, u_{n-1} \in \mathbb{F}_q \setminus \{0\}$.

Dem. :

(a) Seja $D = P_1 + P_2 + \cdots + P_n$, com $n \leq q$ e $deg\ P_i = 1$ para $i = 1, \ldots, n$. Como há $q+1$ lugares de grau 1 em $F/\mathbb{F}_q$, existe um lugar $P \in \mathbb{P}_F$ tal que $deg\ P = 1$ e $P \notin Supp D$.

Tomemos $Q \in \mathbb{P}_F$, com $deg\ Q = 1$ e $Q \neq P$.[7] Com isso

$$deg\ (Q - P) = deg\ Q - deg\ P = 0 > -1 = 2g - 1 ,$$

então por (1.4.29)

$$dim(Q - P) = deg\ (Q - P) + 1 - g = 1 .$$

Pelo corolário (1.3.16.c), $(Q - P)$ é principal, então existe

$$x \in \mathbb{F}_q(z) \text{ tal que } (x) = Q - P .$$

[7] Por exemplo $Q = P_1$.

Notamos então que P é o divisor de polos de x e Q é divisor de zeros de x, por (1.3.15) vale

$$1 = deg\ Q = deg\ P = [\mathbb{F}_q(z) : \mathbb{F}_q(x)] ,$$

portanto, x é o elemento gerador do corpo de funções racional sobre $\mathbb{F}_q$.

Denotaremos $P = P_\infty$.

Vamos supor que $k > 0$ e $k < n$, pela proposição (2.3.3.b) temos

$$0 \leq deg\ G \leq n - 2 .$$

Por (2.3.3.c) obtemos

$$deg\ G = k - 1 \geq 0 .$$

Consideremos agora, o divisor $(k-1)P_\infty - G$, é claro que $deg\ ((k-1)P_\infty - G) = 0$. Pelo teorema (1.3.22)

$$dim((k-1)P_\infty - G) \geq deg\ ((k-1)P_\infty - G) + 1 - g = 1 ,$$

e pelo corolário (1.3.16.c) temos que $(k-1)P_\infty - G$ é principal. Logo, existe

$$h \in \mathbb{F}_q(z) \setminus \{0\} \text{ tal que } (h) = (k-1)P_\infty - G .$$

Os k elementos $h, hx, \ldots, hx^{k-1}$ são l.i. sobre $\mathbb{F}_q$. Pois, suponha que exista $a_i \in \mathbb{F}_q$ tal que

$$0 = \sum_{i=0}^{k-1} a_i(hx^i) = \sum_{i=0}^{k-1}(a_i h)x^i ,$$

logo $a_i h = 0$, mas $h \neq 0$ portanto $a_i = 0$ para $i = 1, \ldots, k-1$.

Notemos ainda que

$$(h) = (k-1)P_\infty - G \geq -G$$

e para $i = 1, \ldots, k-1$

$$(hx^i) = (h) + i(x) = (k-1)P_\infty - G + i(Q - P_\infty) = iQ + (k-1-i)P_\infty - G \geq -G ,$$

logo $h, hx, \ldots, hx^{k-1} \in \mathcal{L}(G)$ e são l.i., como

$$k = dim(C_{\mathcal{L}}(G, D)) = dim(\mathcal{L}(G))$$

temos que $\{ h, hx, \ldots, hx^{k-1} \}$ forma uma base para $\mathcal{L}(G)$, ou seja,

$$\mathcal{L}(G) = \{ hf(x) |\ f(x) \in \mathbb{F}_q[x] \ e\ deg\ f(x) \leq k-1 \} .$$

Como $deg\ P_i = 1$ temos $\mathbb{F}_q = O_{P_i}/P_i$ então podemos considerar $\alpha_i := x(P_i)$ e $u_i := h(P_i)$ para $i = 1, \ldots, k-1$. Como os $P_i's$ são distintos, temos que $\alpha_i's$ são distintos, os $u_i's \neq 0$ pois, $P_i \notin Supp(h)$ então $h \notin P_i$ logo $h(P_i) \neq 0$.

Com isso, obtemos que

$$\begin{array}{rccl} \varphi : & \mathcal{L}(G) & \longrightarrow & C_{\mathcal{L}}(G, D) \\ & hf(x) & \longmapsto & (hf(x)(P_1), \ldots, hf(x)(P_n)) . \end{array}$$

Mas

$$(hf(x))(P_i) = h(P_i)f(x)(P_i)) = u_i f(\alpha_i),\ i = 1, \ldots, n .$$

Portanto,

$$C_{\mathcal{L}}(G,D) = \{\ (u_1 f(\alpha_1),\ldots,u_n f(\alpha_n))|\ deg\ f(x) \leq k-1,\ f(x) \in I\!F_q[x]\ \}\ .$$

Pelo corolário (2.2.4.c) $\{\ h, hx, \ldots, hx^{k-1}\ \}$ é uma base para $\mathcal{L}(G)$ então

$$M = \begin{pmatrix} h(P_1) & h(P_2) & \ldots & h(P_n) \\ hx(P_1) & hx(P_2) & \ldots & hx(P_n) \\ \vdots & \vdots & & \vdots \\ hx^{k-1}(P_1) & hx^{k-1}(P_2) & \ldots & hx^{k-1}(P_n) \end{pmatrix}$$

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

(b) Suponhamos que $n = q+1$, de maneira análoga ao ítem (a) demonstra-se o ítem (b), só que agora consideraremos o nosso divisor $P = P_n$ e teremos que $P_n = P_\infty$ o divisor de polo de x.

Teremos então $(k-1)P_\infty - G = (h)$, com $h \in I\!F_q(x)\backslash\{0\}$ e $\{\ h, hx, \ldots, hx^{k-1}\ \}$ uma base para $\mathcal{L}(G)$.

Para $i \in \{1,\ldots,n-1=q\}$ os $\alpha_i := x(P_i)$ são distintos, logo $I\!F_q = \{\alpha_1,\ldots,\alpha_{n-1}\}$, e $u_i := h(P_i) \in I\!F_q\backslash\{0\}$. Como

$$v_{P_n}(hx^i) = v_{P_n}(h) + i v_{P_n}(x) = (k-1) + i(-1) = k-1-i > 0 \ \text{ para} i = 0,\ldots,k-2$$

portanto $hx^i \in P_n$, ou seja $(hx^i)(P_n) = 0$ para $i = 0,\ldots,k-2$. Agora

$$v_{P_n}(hx^i) = k-1-i = 0 \ \text{ para}\, i = k-1\ ,$$

ou seja, $0 \neq (hx^{k-1})P_n = \gamma \in I\!F_q$.

Substituindo h por $\gamma^{-1}h$ teremos $\{\ \gamma^{-1}h, \gamma^{-1}hx, \ldots, \gamma^{-1}hx^{k-1}\ \}$ uma base para $\mathcal{L}(G)$, pelo corolário (2.2.4) temos

$$M = \begin{pmatrix} \gamma^{-1}h(P_1) & \gamma^{-1}h(P_2) & \ldots & \gamma^{-1}h(P_n) \\ \gamma^{-1}hx(P_1) & \gamma^{-1}hx(P_2) & \ldots & \gamma^{-1}hx(P_n) \\ \vdots & \vdots & & \vdots \\ \gamma^{-1}hx^{k-1}(P_1) & \gamma^{-1}hx^{k-1}(P_2) & \ldots & \gamma^{-1}hx^{k-1}(P_n) \end{pmatrix}$$

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

□

Definição 2.3.5 *Sejam $\alpha = (\alpha_1,\ldots,\alpha_n)$ onde $\alpha_i's$ são elementos distintos em $I\!F_q$ e $h = (h_1,\ldots,h_n)$ onde $h_i \in I\!F_q\backslash\{0\}$, não necessariamente distintos. Então o código Reed-Solomon generalizado, denotado por $GRS_k(\alpha,h)$, consiste de todos os vetores*

$$(\ h_1 f(\alpha_1),\ldots,h_n f(\alpha_n)\ ) \text{ com } f(z) \in I\!F_q[z] \text{ e } deg\ f(z) \leq k-1\ ,$$

para $k \leq n$ fixado.[8]

Claramente vemos que $GRS_k(\alpha,h)$ é um $[n,k]$-código. Observamos também que a proposição (2.3.4.a) afirma que todo código de Goppa racional sobre $I\!F_q$ e de comprimento $n \geq q$, são $GRS_k(\alpha,h)$. A recíproca é verdadeira.

[8]Equivalentemente $GRS_k(\alpha,h)$ é gerado pela matriz do ítem (a) da proposição (2.3.4).

Proposição 2.3.6 *Todo código Reed-Solomon generalizado ($GRS_k(\alpha, h)$) pode ser representado como um código de Goppa racional.*

Dem. :

Seja $GRS_k(\alpha, h)$ um código Reed-Solomon generalizado, pela defnição temos

$$\alpha = (\alpha_1, \ldots, \alpha_n)\ \alpha_i \in \mathbb{F}_q \text{ distintos } \ e\ \ h = (h_1, \ldots, h_n)\ h_i \in \mathbb{F}_q \backslash \{0\}\ .$$

Considerando o corpo de funções racionais $\mathbb{F}_q(z)$, denotemos
P_i o divisor de zeros de $z - \alpha_i$ para $i = 1, \ldots, n$.
P_∞ o polo de z.
Como os $\alpha_i's$ são distintos temos que os $P_i's$ são distintos, e como $h_i \in \mathbb{F}_q$ pelo teorema (1.2.1) existe

$$u \in \mathbb{F}_q(z) \text{ tal que } v_{P_i}(u - h_i) > 0\ ,$$

então $u - h_i \in P_i$, ou seja $u(P_i) = h_i$ para $i = 1, \ldots, n$.

Agora, seja $D = P_1 + P_2 + \cdots + P_n$ e $G = (k-1)P_\infty - (u)$ logo pela prova da proposição (2.3.4) temos que $GRS_k(\alpha, h) = C_{\mathcal{L}}(G, D)$.

□

Para finalizar a seção e também este capítulo apresentamos dois exemplos de códigos de Goppa sobre um corpo de funções racionais.

Seguimos aqui, os passos da proposição (2.3.4), tomando para isto $q = 7$ e $\mathbb{F}_7(z)/\mathbb{F}_7$ o corpo de funções racionais.[9] Pelo corolário (A.1.3), $\mathbb{F}_7$ tem $7 + 1 = 8$ lugares de grau 1, que idetificaremos por P_∞ e P_i para $i = 0, 1, \ldots, 6$ como em (A.4) e respectivamente (A.2) do apêndice, lembrando também que o gênero de $\mathbb{F}_7(z)/\mathbb{F}_7$ é $g = 0$.

Exemplo 2.3.7 Vamos considerar $n = 6 < q = 7$ e com isso tomar o divisor

$$D = P_1 + P_2 + \cdots + P_6\ ,$$

é de se esperar que escolheremos o divisor G tal que o código $C_{\mathcal{L}}(G, D)$ obtido seja MDS. Logo, pela proposição (2.3.3) temos que tomar G tal que

$$0 \leq deg\ G \leq n - 2 = 4\ .$$

Vamos considerar $deg\ G = 4$, ainda por (2.3.3) temos

$$k = 1 + deg\ G = 5\ \ e\ \ d = n - deg\ G = 2\ .$$

Podemos tomar $G = 4P_0$, logo :
$D = P_1 + P_2 + \cdots + P_6$, com $P_i's$ 2 a 2 distintos e $deg\ P_i = 1$ para $i = 0, 1, \ldots, 6$.
$G = 4P_0$, claramente $SuppG \cap SuppD = \emptyset$.

Agora, seja o divisor $(P_1 - P_\infty)$, logo

$$deg\ (P_1 - P_\infty) = 0 > -1 = 2g - 1\ ,$$

e pelo teorema (1.4.29)

$$dim(P_1 - P_\infty) = deg\ (P_1 - P_\infty) + 1 - g = 1\ ,$$

[9] Identificaremos $\mathbb{F}_q = \{0, 1, 2, \ldots, q-2, q-1\}$.

No próximo exemplo, continuaremos considerando $q = 7$ e $I\!F_7(z)/I\!F_7$ o corpo de funções racionais.

Exemplo 2.3.8 Seja $n = q + 1 = 8$ e tomemos

$$D = P_0 + P_1 + P_2 + P_3 + P_4 + P_5 + P_6 + P_\infty ,$$

com os $P_i's$ e P_∞ definidos como no exemplo anterior.

Novamente escolheremos o divisor G de modo que $C_{\mathcal{L}}(G, D)$ seja MDS, pela proposição (2.3.3) temos que considerar G tal que

$$0 \leq deg\ G \leq n - 2 = 6 ,$$

por uma escolha aleatória tomemos $deg\ G = 4$. Logo temos

$$k = 1 + deg\ G = 5 \ \ e \ \ d = n - deg\ G = 4 .$$

Vamos construir G da seguinte forma :

Consideremos o polinômio

$$p(z) = z^2 + z + 3 \in I\!F_7[z] ,$$

que é irredutível.[10] Pela proposição (A.1.1) $Q_{p(z)}$ é um lugar de grau 2 em $I\!F_7(z)/I\!F_7$.

Consiremos

$$G = 2Q_{p(z)} ,$$

claramente $SuppG \cap SuppD = \emptyset$.

Como no exemplo anterior, tomemos o divisor $(P_0 - P_\infty)$, logo

$$deg\ (P_0 - P_\infty) = 0 \ \ e \ \ dim(P_0 - P_\infty) = 1 ,$$

ou seja, $(P_0 - P_\infty)$ é principal, então existe

$$z' \in I\!F_7(z)/I\!F_7 \text{ tal que } (z') = P_0 - P_\infty .$$

Tomemos também o divisor $(4P_\infty - G)$, onde

$$deg\ (4P_\infty - G) = 4deg\ P_\infty - 2deg\ Q_{p(z)} = 0 ,$$

logo por (1.4.29) temos

$$dim(4P_\infty - G) = deg\ (4P_\infty - G) + 1 - g = 1 ,$$

então existe

$$u \in I\!F_7(z)/I\!F_7 \text{ tal que } (u) = 4P_\infty - G .$$

Notemos que

$$v_{P_0}(z') = 1,\ v_{P_\infty}(z') = -1,\ v_{p(z)}(u) = -2\ e\ v_{P_\infty} = 4 ,$$

portanto, pela proposição (A.1.1) temos

$$u = \frac{a}{p(z)^2} \ \ e \ \ z' = bz ,$$

com $a, b \in I\!F_7 \backslash \{0\}$, e novamente consideraremos $a = b = 1$.

[10] Note que $p(z)$ não possui raizes em $I\!F_7$.

Tomemos agora

$$\alpha_i = z(P_i) \ \ e \ \ h_i = u(P_i) \ ,$$

para $i = 0, 1, \ldots, 6$ e α_{P_∞} e h_{P_∞} tal que

$$h_{P_\infty} \alpha_{P_\infty}^j = (uz^j)(P_\infty) \ ,$$

para $j = 0, 1, \ldots, 4$. Pela proposição (A.1.1) temos

$$\alpha_i = i \ \ e \ \ h_i = \frac{1}{p(i)^2} \ ,$$

para $i = 0, 1, \ldots, 6$, e

$$h_{P_\infty} \alpha_{P_\infty}^j = (\frac{z^j}{p(z)^2})(P_\infty) = \begin{cases} 0 & se \quad j < 4 \\ 1 & se \quad j = 4 \end{cases}$$

para $j = 0, 1, \ldots, 4$.

Portanto, pela proposição (2.3.4)

$$C_{\mathcal{L}}(G, D) = \{ \ (4f(0), 2f(1), 2f(2), 1f(3), 2f(4), 2f(5), 4f(6), \gamma) | \ f(z) \in \mathbb{F}_7[z] \text{ com } deg \ f(z) \leq 4 \ \} \ ,$$

com

$$\gamma = \begin{cases} o & se \quad deg \ f(z) < 4 \\ a_4 & se \quad f(z) = a_4 z^4 + \cdots + a_1 z^1 + a_0, \ com \ a_4 \neq 0 \end{cases}$$

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

$$M = \begin{pmatrix} 4 & 2 & 2 & 1 & 2 & 2 & 4 & 0 \\ 0 & 2 & 4 & 3 & 1 & 3 & 3 & 0 \\ 0 & 2 & 1 & 2 & 4 & 1 & 4 & 0 \\ 0 & 2 & 2 & 6 & 2 & 5 & 3 & 0 \\ 0 & 2 & 4 & 4 & 2 & 4 & 4 & 1 \end{pmatrix}$$

Capítulo 3

B-Lacunas e Códigos de Goppa

Neste capítulo estaremos interessados em encontrar melhores cotas para a distância mínima dos códigos de Goppa. Como vimos no Capítulo 2, estes códigos são construídos a partir dos divisores D e G pertencentes a $\mathcal{D}_F$ tomados de uma maneira "particular". Nossa proposta é , utilizando o conhecimento dos conceitos de B-lacunas, melhorarmos as cotas para a distância mínima dos códigos de Goppa pela inclusão de mais hipóteses sobre o divisor G.

3.1 Requisitos e Notação

Esta seção servirá para fixarmos a notação e as informações necessárias para o desenvolvimento do cápitulo.

Consideraremos o corpo de funções $F/\mathbb{F}_q$ de gênero g, onde q é potência de um número primo.

Dados um divisor $B \in \mathcal{D}_F$ e um lugar $P \in \mathbb{P}_F$ de grau 1, consideraremos as B-lacunas em P, conforme a definição (1.5.3).

Sejam $P_1, P_2, \ldots, P_n \in \mathbb{P}_F$, lugares de grau 1 distintos entre si. Consideraremos os divisores D, $G \in \mathcal{D}_F$ tal que

$$D = P_1 + P_2 + \cdots + P_n \ \ e \ \ Supp G \cap Supp D = \emptyset \ .$$

Apartir deste divisores definiremos, conforme (2.2.1) e (2.2.6), os respectivos códigos de Goppa :

$$C_{\mathcal{L}}(G,D) := \{ \ (x(P_1), \ldots, x(P_n)) | \ x \in \mathcal{L}(G) \ \} \ ,$$

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

Notação :[1]

n : comprimento do código .
k : dimensão do código .
d : distância mínima do código .

[1] Conforme as definições do Capítulo 2.

com $E' \geq 0$ e $P \notin Supp(E)$. Então existe $x \in F$ tal que

$$(\omega) - B = (\gamma_k - 1)P + E' - (x) .$$

Logo por (3.1) vale

$$(\gamma_j + \gamma_k - 1)P + 2B - (P_1 + \cdots P_d) - B = (\gamma_k - 1)P + E' - (x) ,$$

ou seja,

$$(x) + B = -\gamma_j P + (P_1 + \cdots + P_d) + E'$$

como $P_i's \geq 0$, $P \geq 0$ e $E' \geq 0$ então

$$((x) + B)_\infty = \gamma_j P ,$$

o que é um absurdo, pois γ_j é uma B-lacuna em P.

Portanto, $d > deg\ G - (2g-2)$, ou seja

$$d \geq deg\ G - (2g-2) + 1 = deg\ G - 2g + 3 .$$

□

Seguindo a mesma idéia do teorema anterior, o próximo teorema melhora a cota da distância mínima para o código $C_{\mathcal{L}}(G, D)$.

Teorema 3.2.2 *Suponhamos que γ é uma B-lacuna em P. Tomemos $G = \gamma P + B$. Se o código $C_{\mathcal{L}}(G, D)$ tem dimensão positiva então*

$$d \geq n - deg\ G + 1 .$$

Dem. :

Pelo teorema (2.2.3) temos que o código $C_{\mathcal{L}}(G, D)$ tem distância mínima d tal que

$$d \geq n - deg\ G .$$

Suponhamos que $d = n - deg\ G$, como

$$dim(C_{\mathcal{L}}(G, D)) > 0 ,$$

existe $f \in \mathcal{L}(G)$, $f \neq 0$, tal que

$$\varphi(f) = (\ f(P_1), f(P_2), \ldots, f(P_d), 0, \ldots, 0\ ) \in C_{\mathcal{L}}(G, D) ,$$

com $f(P_i) \neq 0$, para $i = 1, \ldots, d$.[4]

Como $f \in \mathcal{L}(G)$ temos

$$(f) \geq -G ,$$

mas $f(P_j) = 0$, para $j = d+1, \ldots, n$, então

$$f \in P_j \text{ para } j = d+1, \ldots, n ,$$

ou seja $v_{P_j}(f) > 0$, então

$$v_{P_j}(f) \geq 1 = v_{P_j}(P_j) .$$

[4] Reenumerando os $P_i's$ se necessário.

notemos que $(n-w) - deg\ G + t \geq 0$ então $deg\ E \leq t$. Com isso podemos escrever

$$E = \lambda P + E' ,$$

com $E' \geq 0$, $P \notin Supp E'$ e $0 \leq \lambda \leq t$; então

$$(f) = P_1 + \cdots + P_{n-w} - G + \lambda P + E' ,$$

mas $G = \gamma P + B$

$$(f) + B = P_1 + \cdots + P_{n-w} + E' - (\gamma - \lambda)P ,$$

com $0 \leq \lambda \leq t$. Portanto

$$((f) + B)_\infty = (\gamma - \lambda)P; \text{ para } 0 \leq \lambda \leq t .$$

Isto contradiz a hipótese de $(\gamma - \lambda)$, ser uma B-lacuna em P para $\lambda = 0, \ldots, t$.

Então $w(f) > n - deg\ G + t$, para todo $f \in \mathcal{L}(G)$, ou seja,

$$d \geq n - deg\ G + t + 1 .$$

□

O próximo teorema é uma generalização do teorema (3.2.1), mas para demonstrá-lo necessitámos do seguinte lema .

Lema 3.2.4 *Suponhamos que cada número inteiro*

$$\alpha,\ \alpha + 1, \ldots,\ \alpha + t;\ \beta - (t-1), \ldots,\ \beta - 1,\ \beta$$

sejam B-lacunas em P, com $\alpha + t \leq \beta$ e $t \geq 1$. Tomemos $G = (\alpha + \beta - 1)P + 2B$, e suponhamos que existe um divisor canônico K da forma

$$K = G + E - (P_1 + P_2 + \cdots + P_w) ,$$

onde $E \geq 0$, $deg\ E = t$ e $w = deg\ G - (2g-2) + t \leq n$, então :

(1) $\mathcal{L}((\alpha + i)P + E + B) \neq \mathcal{L}((\alpha + i - 1)P + E + B)$, *para* $i = 0, 1, \ldots, t-1$.
Também $\mathcal{L}((\beta - j)P + E + B) \neq \mathcal{L}((\beta - j - 1)P + E + B)$, *para* $j = 0, \ldots, t$.

(2) *Se $P \notin Supp(E)$, então a função*

$$h(s) = dim(sP + E + B) - dim(sP + B) ,$$

é uma função não decrecente em s.

(3) *Suponha $h(s) = m$. Se $\alpha - 1 \leq s \leq \alpha + t - 2$ ou $\beta - t \leq s \leq \beta$, então $h(s+1) = m + 1$.*

Dem. :
(1) Suponha que $\mathcal{L}((\alpha + i)P + E + B) = \mathcal{L}((\alpha + i - 1)P + E + B)$ para $i = 0, , \ldots, t-1$, como $P > 0$ temos

$$(\alpha + i)P + E + B \geq (\alpha + i)P - P + E + B, \text{ com } i = o, \ldots, t-1$$

então temos que

$$(\alpha + i)P + E + B - (P_1 + P_2 + \cdots + P_w) \geq (\alpha + i)P - P + E + B - (P_1 + P_2 + \cdots + P_w) ,$$

Portanto

$$\mathcal{L}((\alpha+i)P+E+B) \neq \mathcal{L}((\alpha+i-1)P+E+B); \text{ para } i=0,1,\ldots,t-1\,.$$

De maneira análoga, prova-se que $\mathcal{L}((\beta-j)P+E+B) \neq \mathcal{L}((\beta-j-1)P+E+B)$, para $j=0,\ldots,t$. □

Dem. :

(2) Para todo $s \in \mathcal{Z}$ temos que

$$sP+B \geq (s-1)P+B\,,$$

então pelo lema (1.3.11)

$$\mathcal{L}(sP+B) \supseteq \mathcal{L}((s-1)P+B) \tag{3.8}$$

Agora para qualquer $f \in \mathcal{L}(sP+B)\backslash\mathcal{L}((s-1)P+B)$ temos

$$(f) \geq -sP-B \tag{3.9}$$
$$(f) < -(s-1)P-B \tag{3.10}$$

como $E \geq 0$ temos de (3.9) que

$$(f) \geq -sP-B \geq -sP-B-E\,,$$

então

$$f \in \mathcal{L}(sP+E+B)$$

como $P \notin Supp(E)$ de (3.10) temos

$$v_P((f)) < -v_P((s-1)P) - v_P(B) = v_P((s-1)P) - v_P(E) - v_P(B)$$

logo

$$f \notin \mathcal{L}((s-1)P+E+B)\,.$$

Com isto temos que, para qualquer

$$f \in \mathcal{L}(sP+B)\backslash\mathcal{L}((s-1)P+B)$$

então

$$f \in \mathcal{L}(sP+E+B)\backslash\mathcal{L}((s-1)P+E+B)\,.$$

Portanto,

$$dim(\mathcal{L}(sP+B)/\mathcal{L}((s-1)P+B)) \leq dim(\mathcal{L}(sP+E+B)/\mathcal{L}((s-1)P+E+B))\,,$$

ou seja,

$$dim((s-1)P+E+B) - dim((s-1)P+B) \leq dim(sP+E+B) - dim(sP+B)\,,$$

logo $h(s-1) \leq h(s)$ para qualquer $s \in \mathcal{Z}$. Portanto h é não decrescente. □

Dem. :

(3) Suponhamos $h(s)=m$. Se $\alpha-1 \leq s \leq \alpha+t-2$, ou $\beta-t \leq s < \beta$, temos que

$$\alpha \leq s+1 \leq \alpha+(t-1), \text{ ou } \beta-(t-1) \leq s+1 \leq \beta\,.$$

Por hipótese $(s+1)$ é uma B-lacuna em P, pela parte **(1)** deste lema temos

$$\mathcal{L}((s+1)P+E+B) \neq \mathcal{L}(sP+E+B) \tag{3.11}$$

mas pelo lema (1.3.11)

$$dim((s+1)P+E+B) - dim(sP+E+B) \leq deg\ ((s+1)P+E+B) - deg\ (sP+E+B) = 1\ .$$

Portanto por (3.11) temos

$$dim(\ (s+1)P+E+B\ ) = dim(sP+E+B)+1\ ,$$

como $(s+1)$ é uma B-lacuna por (1.5.7), temos

$$\mathcal{L}((s+1)P+B) = \mathcal{L}(sP+B)\ .$$

Portanto

$$h(s+1) = dim((s+1)P+E+B) - dim(sP+E+B) = dim(sP+E+B)+1-dim(sP+B) = h(s)+1\ ,$$

ou seja, $h(s+1) = m+1$. □

Teorema 3.2.5 *Suponhamos que os inteiros*

$$\alpha,\ \alpha+1,\ldots,\ \alpha+t;\ \beta-(t-1),\ \beta-(t-2),\ldots,\ \beta-1,\ \beta$$

sejam B-lacunas em P, com $\alpha+t \leq \beta$ e $t \geq 1$. Tomemos $G = (\alpha+\beta-1)P+2B$. Se o código $C_\Omega(G,D)$ tem dimensão positiva então

$$d \geq deg\ G - (2g-2) + (t+1)\ .$$

Dem. :
A prova é feita por indução sobre t.

Tomemos $t=1$. logo α, $\alpha+1$ e β são B-lacunas em P e por (3.2.1) temos que

$$d \geq deg\ G - 2g + 3\ .$$

Suponhamos que $d = deg\ G - 2g + 3$, como $C_\Omega(G,D)$ tem dimensão positiva, existe

$$\omega \in \Omega(G-D),\ \text{tal que}\ ^6(\omega_{P_i}(1),\ldots,\omega_{P_d}(1),0,\ldots,0)\ ,$$

com $\omega_{P_i}(1) \neq 0$, para $i = 1,\ldots,d$. como $\omega \in \Omega(G-D)$ temos que

$$(\omega) \geq G - D\ ,$$

mas pela demonstração do teorema (2.2.8) como $\omega_{P_i}(1) \neq 0$, para $i = 1,\ldots,d$ obtemos

$$(\omega) = G - P_1 - P_2 - \cdots - P_d + Q\ ,$$

onde $Q \in I\!P_F$, com $deg\ Q = 1$, pela parte **(1)** do lema (3.2.4) temos

$$\mathcal{L}(\alpha P+Q+B) \neq \mathcal{L}((\alpha-1)P+Q+B)\ .$$

[6] Reenumerando os $P_i's$ se necessário .

e

$\alpha' = \alpha+1,\ \alpha'+1 = \alpha+2, \ldots,\ \alpha'+(t-1) = \alpha+t$ e $\beta' = \alpha'+(t-1),\ \beta'-1 = \alpha'+(t-2), \ldots,\ \beta'-(t-1) = \alpha'$,

notemos que $\alpha' + (t-1) = \beta$ e $t \geq 1$, tendo as hipóteses do teorema e pela hipótese de indução o teorema é válido para $t-1$, temos que a distância mínima do código $C_\Omega(G', D)$ vale

$$d' \geq deg\ G' - (2g-2) + t = deg\ G + deg\ P - (2g-2) + t = d+1 .$$

Mas $(\eta) = G - (P_1 + \cdots + P_d) + E$ e como $P \in Supp E$, temos

$$E = P + E' ,$$

onde $E' \geq 0$, logo

$$(\eta) = G + (P + E') - (P_1 + \cdots + P_d) = G' - (P_1 + \cdots + P_d) + E' ,$$

então $(\eta) \geq G' - D$, ou seja,

$$\eta \in \Omega(G' - D) ,$$

um absurdo, pois η tem peso d e $C_\Omega(G' - D)$ tem distância mínima $d' \geq d+1$. Portanto

$$P \notin Supp E .$$

Com isto temos as hipóteses do lema (3.2.4), considerando então a parte **(2)** de (3.2.4), isto é ,

$$h(s) = dim(sP + E + B) - dim(sP + B) ,$$

e considerando $s = \alpha - 1$, por (3.2.4) parte **(3)** obtemos

$$h(\alpha) = h(\alpha - 1) + 1 ,$$

ou seja,

$$h(\alpha) \geq 1 \tag{3.14}$$

Continuando com a função h, pelo lema (1.3.11) temos,

$$h(\beta) = dim(\beta P + E + B) - dim(\beta P + B) \leq deg\ (\beta P + E + B) - deg\ (\beta P + B) = deg\ E = t ,$$

então

$$h(\beta) \leq t \tag{3.15}$$

agora, por (3.2.4) parte **(3)**, $h(\alpha + (t-1)) = h(\alpha) + t - 1$, então por (3.14)

$$h(\alpha + (t-1)) \geq t \tag{3.16}$$

por hipótese, $\alpha + t \leq \beta$ ou seja, $\alpha + (t-1) \leq \beta - 1$, como h é não decrescente

$$h(\alpha + (t-1)) \leq h(\beta - 1) .$$

Por (3.16) e por (3.2.4.**(3)**) temos $t \leq h(\beta) - 1$, assim,

$$h(\beta) \geq t + 1 ,$$

o que é um absurdo, por (3.15). Portanto $d > deg\ G - (2g-2) + t$, ou seja

$$d \geq deg\ G - (2g-2) + t + 1$$

e o teorema está provado. □

Como consequência direta deste teorema obtemos os seguintes corolários.

Corolário 3.2.6 *Suponhamos que* $\alpha,\ \alpha+1,\ldots,\ \alpha+t$, *sejam* $(t+1)$*-consecutivas B-lacunas em* P. *Seja*

$$G = (2\alpha + t - 1)P + 2B\ .$$

Se o código $C_\Omega(G,D)$, *tem dimensão positiva, então*

$$d \geq deg\ G - (2g-2) + (t+1)\ .$$

Dem. :

Tomemos

$$\beta = \alpha + t,\ \beta - 1 = \alpha + (t-1), \ldots,\ \beta - (t-1) = \alpha + 1\ ,$$

logo

$$G = (\alpha + (\alpha + t) - 1)P + 2B = (\alpha + \beta - 1)P + 2B\ ,$$

portanto pelo teorema (3.2.5) temos que

$$d \geq deg\ G - (2g-2) + (t+1)\ .$$

□

Corolário 3.2.7 *Suponhamos que* $\alpha,\ \beta\ e\ \beta+1$ *sejam B-lacunas em* P, *com* $\alpha < \beta$. *Tomemos* $G = (\alpha+\beta)P + 2B$. *Se o código* $C_\Omega(G,D)$ *tem dimensão positiva, então*

$$d \geq deg\ G - 2g + 4\ .$$

Dem. :
Considerando

$$\alpha' = \alpha,\ \alpha' + 1 = \beta\ e\ \beta' = \beta + 1$$

logo, temos $\alpha' + 1 < \alpha' + 1 + 1 = \beta'$ e $t = 1$. Com isso

$$G = (\alpha' + \beta' - 1)P + 2B\ .$$

Então pelo teorema (3.2.5) temos

$$d \geq deg\ G - 2g + 4\ .$$

□

3.3 Ilustração

Nesta seção apresentamos um exemplo, como aplicação dos teoremas da seção anterior. A ilustração concentra a atenção no cálculo da distância mínima de certos códigos particulares, já que o cálculo das sequências de lacunas não é trivial.

As demonstrações dos resultados podem ser encontradas em [4], [2] e [1] .

Vamos considerar, o corpo de funções Hermitiano, sobre $\mathbb{F}_{q^2}$,[8] definido por :

$$H = \mathbb{F}_{q^2}(x,y)\ \text{ com } y^q + y = x^m\ \ e\ \ m|q+1\ .$$

De [3], temos que :

[8] q é potência de um primo p.

(i) O gênero de H é

$$g = \frac{(q-1)(m-1)}{2} ,$$

(ii) H tem $1 + q(1 + m(q-1))$ lugares de grau 1.

Exemplo 3.3.1 Se $m = q+1$ temos

$$H = I\!F_{q^2}(x,y) \text{ com } y^q + y = x^{q+1}$$

(i) o genero de H é

$$g = \frac{q(q-1)}{2} ,$$

(ii) H tem $1 + q^3$ lugares de grau 1.

Se tomarmos o divisor $B \in \mathcal{D}_F$ igual ao divisor nulo ($B = \mathbf{0}$), temos, por [2], que as lacunas de Weierstrass para todo $P \in I\!P_F$ com $deg\ P = 1$ são

$$\begin{aligned}
&1, 2, 3, \ldots, q-1, && = (\ 0(q+1)+1, 0(q+1)+2, \ldots, 0(q+1)+q-1\ )\\
&q+2, q+3, \ldots, 2q-1, && = (\ 1(q+1)+1, 1(q+1)+2, \ldots, 1(q+1)+q-2\ )\\
&2q+3, 2q+4, \ldots, 3q-1, && = (\ 2(q+1)+1, 2(q+1)+2, \ldots, 2(q+1)+q-3)\\
&\vdots\\
&(q-4)(q+1)+1, (q-4)(q+1)+2, (q-3)q-1 = (q-4)(q+1)+3,\\
&(q-3)(q+1)+1, (q-2)q-1 = (q-3)(q+1)+2,\\
&(q-2)(q+1)+1\ .
\end{aligned}$$

Note que $(q-2)(q+1)+1 = q(q-1)-1 = 2g-1$ e pela proposição (1.5.9) esta é a maior lacuna possível.

Agora, denotamos $P = P\infty$, o divisor de polos de x e fixamos um inteiro r, com $1 \leq r \leq q-2$.

Tomemos $\gamma = (r+1)q - 1$, e seja

$$G = \gamma P$$

e

$$D = P_1 + P_2 + \cdots + P_{q^3} ,$$

onde $P_i's$ denotam outros lugares de grau 1 diferentes de P.

Pelo teorema (2.2.3) temos que $C_{\mathcal{L}}(G,D)$ é um código de Goppa com distância mínima

$$d \geq n - deg\ G = q^3 - (r+1)q + 1 .$$

Mas, observamos que

$$r(q+1)+1,\ r(q+1)+2, \ldots,\ r(q+1)+q-1-r = \gamma ,$$

são $q-r-1$ lacunas consecutivas em P. Logo, pelo teorema (3.2.3) a distância mínima d de $C_{\mathcal{L}}(G,D)$ vale

$$d \geq n - deg\ G + (q-r-1) = q^3 - r(q+1) .$$

Para ilustrar o teorema (3.2.5), façamos o seguinte : Fixemos um inteiro s, com $0 \leq s \leq q-3$, e tomemos

$$\alpha = s(q+1)+1 .$$

Agora, para $t = q-2-s$ temos que

$$\alpha,\ \alpha+1,\ \alpha+2, \ldots,\ \alpha+(t-1),\ \alpha+t ,$$

são $t+1$ lacunas consecutivas em P, observe que $t \geq 1$.

Tomemos também $\beta = \alpha + t$ e consideremos

$$G = (\alpha + \beta - 1)P .$$

Pelo teorema (2.2.8) temos que $C_\Omega(G, D)$ é um código com distância mínima d tal que

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

Todavia, observamos que

$$\beta,\ \beta - 1,\ \ldots,\ \beta - (t-2),\ \beta - (t-1)$$

são t lacunas consecutivas. Logo pelo teorema (3.2.5) temos que

$$d \geq deg\ G - (2g-2) + (t+1) = deg\ G - (2g-2) + (q - 1 - s) .$$

Que é uma melhora considerável.

Na verdade [2] mostra que vale a igualdade nas inequações da distância mínima, acima.

Apêndice A

O Corpo das Funções Racionais

A.1 Anéis de Valorização e Lugares

Vamos investigar os conceitos de valorização e lugares no caso de um corpo de funções racionais $F = K(x)$, onde x transcendente sobre K. Dado um polinômio arbitrário mônico e irredutível $p(x) \in K[x]$, considere o anel de valorização $O_{p(x)}$,[1] de $K(x)$, dado por:

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

Tomemos $P_{p(x)}$, seu ideal maximal,[2] dado por

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

No caso particular quando $p(x)$ é linear, i.e., $p(x) = x - \alpha$ com $\alpha \in K$, nós escrevemos $P_\alpha = P_{x-\alpha} \in \mathbb{P}_F$. Existe um outro anel de valorizações de $K(x)/K$, a saber

$$O_\infty = \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x],\ deg\ f(x) \leq deg\ g(x) \right\} \tag{A.3}$$

cujo ideal maximal é

$$P_\infty = \left\{ \frac{f(x)}{g(x)} | deg\ f(x) < deg\ g(x) \right\}. \tag{A.4}$$

Este ideal é chamado o lugar **infinito** de $K(x)$. Observe que esta classificação de anéis e lugares dependem da escolha específica do elemento gerador x de $K(x)$ (*por exemplo, $K(x) = K(1/x)$, o lugar infinito com relação a $1/x$ é o lugar P_0 com relação a x*).

A partir destas definições tem-se o seguinte resultado.

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

[1] Como vimos na observação (1.1.7).

[2] Suponhamos $P_{p(x)} \subsetneq S \subseteq O_{p(x)}$, um ideal, logo existe $\frac{h(x)}{q(x)} \in S$; $h(x)$, $q(x) \in K[x]$, com $p(x) \not| h(x)$ e $p(x) \not| q(x)$; temos que $\frac{q(x)}{h(x)} \in O_{p(x)}$, pois $p(x) \not| h(x)$, então $1 = \frac{q(x)}{h(x)} \cdot \frac{h(x)}{q(x)} \in S$; portanto $P_{p(x)}$ é maximal.

(a) *Se $p(x) \in K[x]$ é irredutível. Então $p(x)$ é um elemento primo para $P = P_{p(x)} \in \mathbb{P}_F$ dado por (A.2). Mais ainda considerando v_P a valorização discreta definida em (1.1.15), tem-se $O_P/P = K(x)_P$ é isomorfo a $K[x]/(p(x))$, i.é., deg P = deg $p(x)$. Tal isomorfismo é dado por :*

$$\begin{array}{rccl} \phi : & K[x]/(p(x)) & \longrightarrow & O_P/P \\ & f(x)+(p(x)) & \longmapsto & f(P) := f(x)+P. \end{array}$$

(b) *Se $p(x) = x - \alpha$; $\alpha \in K$, Tem-se que a aplicação de classes residuais é dada por: $z(P) = z(\alpha)$, para $z \in K(x)$, onde $z(\alpha)$ é definido como segue: escreva $z = \frac{f(x)}{g(x)}$ com $f(x)$, $g(x) \in K[x]$, primos entre si. Tome*

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

(c) *Se $P = P_\infty$ é o lugar infinito de $K(x)/K$ definido por (A.4). Então $t = 1/z$ é um elemento primo de P_∞. A valorização discreta associada a P_∞ é dada por $v_\infty(f(x)/g(x)) = deg\ g(x) - deg\ f(x)$, onde $f(x), g(x) \in K[x]$. E $deg P_\infty = 1$. A aplicação residual correspondente a P_∞ é determinada por $z(P_\infty) = z(\infty)$, para $z \in K(x)$, onde $z(\infty)$ é definido da seguinte forma; se $z = \frac{a_n.x^n+\ldots+a_0}{b_m.x^m+\ldots+b_0}$, com $a_n, b_m \neq 0$, então*

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

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

Dem. :

(a) As provas de que $p(x)$ é um elemento primo de $P = P_{p(x)}$ e que $v_P(z) = \begin{cases} n & , \text{se } z = p(x)^n.\frac{f(x)}{g(x)} \\ \infty & , \text{se } z = 0 \end{cases}$ é a valorização associada a P são bastante simples e deixaremos de mostrá-las aqui. Considere agora o homomorfismo de anéis:

$$\begin{array}{rccl} \varphi : & K[x] & \longrightarrow & O_{p(x)}/P_{p(x)} := K(x)_P \\ & f(x) & \longmapsto & f(P) := f(x) + P_{p(x)} \end{array}$$

Observe que

$$Ker(\varphi) = \{f(x) \in K[x] |\ f(x) \in P\} = \{f(x) \in K[x] \mid p(x)/f(x)\}\,,$$

isto é, $Ker(\varphi) = (p(x))$.

Agora seja $\forall\ z(P) \in K(x)_P = O_P/P$; $z(P) = z(x) + P$, onde $z(x) \in O_P$, logo $z(x) = \frac{u(x)}{v(x)}$; $u(x), v(x) \in K[x]$ e $p(x) \nmid v(x)$. Como $p(x)$ é irredutível e $p(x) \nmid v(x)$, tem-se que $p(x)$ e $v(x)$ são relativamente primos, i.e., existem $a(x), b(x) \in K[x]$ tal que $a(x)p(x) + b(x)v(x) = 1$. Logo,

$$z(x) = z(x).1 = \underbrace{\frac{a(x)u(x)}{v(x)}.p(x)}_{\in P_{p(x)}} + \underbrace{b(x)u(x)}_{\in K[x]}, \text{ então } z(P) = \varphi(b(x)u(x)) \text{ e } \varphi \text{ é sobrejetora.}$$

Assim, φ induz um isomorfismo ϕ de $K[x]/(p(x))$ sobre $O_{p(x)}/P_{p(x)} = K(x)_P$.

(b) Análogo a **(a)** tomando-se $p(x) = (x - \alpha)$, $\alpha \in K$.

(c) Por definição $deg\ P_\infty = [F_{P_\infty} : K]$, onde $F_{P_\infty} = O_{P_\infty}/P_\infty$. Sabemos que $K(x) = K(1/x)$. Agora, se $z \in P_\infty$ tem-se por (A.4) que $z = \frac{f(x)}{g(x)}$,com $deg\ f(x) < deg\ g(x)$, portanto podemos escrever

$$z = \frac{1}{x}.\frac{xf(x)}{g(x)} = \frac{1}{x}.\frac{\bar{f}(x)}{g(x)} \text{ onde } deg\ \bar{f}(x) \leq deg\ g(x),$$

por (A.3) temos $\frac{\bar{f}(x)}{g(x)} \in O_\infty$. Logo, $\frac{1}{x}$ é um elemento primo de P_∞, e mais ainda $O_\infty = O_{\frac{1}{x}}$, já que $K(x) = K(1/x)$, portanto $deg\ P_\infty = 1$.

(d) Tome P lugar de $K(x)/K$ de grau 1, por exemplo $P = P_\alpha$ com $\alpha \in K$. $\tilde{K}$ está imerso em $O_P/P = K(x)_P$. Temos $K \subseteq \tilde{K} \subseteq K(x)_P = K$, pois $1 = degP = [K(x)_P : K]$.

□

Na verdade , o que acabamos de descrever representa todos os lugares do corpo de funcoes racionais. Tal resultado, devido a Ostrowski, é o nosso proxímo teorema.

Teorema A.1.2 (Ostrowski) *Os únicos lugares no corpo de funções racionais $K(x)/K$ são os lugares $P_{p(x)}$ e P_∞ definidos em (A.2) e (A.4).*

Dem. :
Basta mostrar que dado um lugar $P \in \mathbb{P}_F$, com $P \neq P_\infty$, então existe $p(x) \in K[x]$, irredutível t.q. $O_{p(x)} = O_P$. Logo tome $P \in \mathbb{P}_F$, com $P \neq P_\infty$,

Caso 1: Se $x \in O_P$ então $O_{p(x)} \subseteq O_P$.
De fato, seja $I = K[x] \cap P$ um ideal primo de $K[x]$, a aplicação residual induz uma submersão $K[x]/I \hookrightarrow O_P/P = K_P$, logo pela proposição (1.1.19) temos $I \neq 0$. Então existe $p(x) \in K[x]$ mônico irredutível t.q. $I = p(x).K[x]$. Se tomo $g(x) \in K[x], p(x) \not| g(x) \Longrightarrow g(x) \notin I \supseteq P$, pela proposição (1.1.8) $g(x)^{-1} \in O_P$, então $O_{p(x)} = \left\{ \frac{f(x)}{g(x)} | \ f(x), g(x) \in K[x];\ p(x) \not| g(x) \right\} \subseteq O_P$, portanto pelo teorema (1.1.16) temos $O_P = O_{p(x)}$.

Caso 2: Se $x \notin O_P$ então $O_\infty \subseteq O_P$.
De fato, $x \notin O_P \Longrightarrow x^{-1} \in O_P$ trabalhando como no caso 1 teremos $O_{\frac{1}{x}} = O_\infty \subseteq O_P$, logo por (1.1.16) $O_{\frac{1}{x}} = O_\infty = O_P$.

□

Atravez da Proposição (A.1.1) e do Teorema (A.1.2) acima demonstra-se o seguinte corolário.

Corolário A.1.3 *Os lugares de $K(x)/K$ de grau 1 tem correspondência 1-1 com $K \cup \infty$.*[3]

A.2 Gênero e Corpos de Funções

Como vimos no exemplo (1.3.11) o gênero de um corpo de funções racionais é igual a zero. Agora se o gênero de um corpo de funções é zero, será que podemos dizer que este é um corpo de funções racionais? A resposta para isso é a nossa próxima proposição .

[3]Em termos de Geometria Algébrica, $K \cup \infty$ é usualmente interpretados como o espaço projetivo $P^1(K)$ sobre K.

Apêndice B

Extensões de Corpos de Funções Algébricas

B.1 Alguns Resultados Básicos

Como vimos, em um corpo de funções racionais podemos descrever todos os seus lugares. Agora como um corpo de funções algébricas é uma extensão finita de um corpo de funções racionais, neste apêndice apresentamos alguns resultados a respeito do estudo dos lugares de um corpo de funções algébricas em termos dos lugares do corpo de funções racionais.

Usualmente , um corpo de funções é representado da seguinte forma

$$F = \mathbb{F}_q(x,y) \text{ com } \psi(x,y) = 0$$

onde, $\psi(x,y) \in \mathbb{F}_q[X,Y]$ é um polinómio irredutível em duas variáveis, então F pode ser observado como uma extensão algébrica finita do corpo de funções racional $\mathbb{F}_q(x)$ (ou $\mathbb{F}_q(y)$).

Apesar desta ser parte fundamental na continuação dos estudos de corpos de funções só daremos aqui as definições e resultados principais.

Fixamos a notações a seguir:

- F/K - corpo de funções algébricas em uma variável com corpo de constantes K;
- K será perfeito; i.e., toda extensão algébrica de K é separável.[1]
- F'/K' - corpo de funções (K' corpo das constantes de F') tal que $F' \supseteq F$ é uma extensão algébrica e $K' \supseteq K$.

Por conveniência fixemos $\Phi \supseteq F$ algebricamente fechado e consideremos somente extensões F'/F com $F' \subseteq \Phi$.

Definição B.1.1 **(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 $[F' : F] = n < \infty$.*

[1] K com característica zero, finito ou algebricamente fechado.

Lema B.1.2 *Seja F'/K' uma extensão algébrica de F/K . Então, vale o seguinte:*

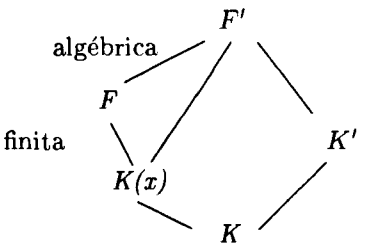
(a) *K'/K é algébrica e $F \cap K' = K$;*

(b) *F'/K' é extensão finita de F/K se e so 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).*

Dem. :

(a) Tomemos $x \in F$ tal que $[F : K(x)] = n < \infty$, isto é, $x \in F$ é transcendente sobre K e consideremos 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.

Agora $K' \cap F = K$ vem do fato de que estamos supondo K algebricamente fechado em F.

(b) Tomando o mesmo x da parte (a) e olhando o diagrama temos:

Suponhamos que $[F' : F] < \infty$, então $[F' : K(x)] < \infty$ e assim F'/K é corpo de funções . Mas então pelo corolário 1.1.20, considerando $\tilde{K}$ o corpo das constantes de F'/K, tem-se: $[\tilde{K} : K] < \infty$ e por (a) $K' \subseteq \tilde{K}$, i.e., $[K' : K] < \infty$.

Suponhamos $[K' : K] < \infty$, entãopelo diagrama tem-se $[K'(x) : K(x)] < \infty$. 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) Observamos que ao tomarmos $F_1 = F.K'$ 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 relações entre os lugares de F' e F.

Definição B.1.3 *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.*

(**3** $\Longrightarrow$ **1**) De $v_{P'}(x) = ev_P(x)$, para todo $x \in F$, temos:

$$x \in P \Longrightarrow v_P(x) \geq 1 \Longrightarrow v_{P'}(x) = ev_P(x) \geq 1 \Longrightarrow x \in P' \Longrightarrow P'/P$$

□

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

$$x(P) \longmapsto x(P') \text{ , para } x \in O_P \text{ .}$$

Assim, podemos considerar F_P um subcorpo de $F'_{P'}$.

Definição B.1.5 *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 $v_{P'}(x) = ev_P(x)$, para todo $x \in F$ 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 ramificações é sempre finito.

Proposição B.1.6 *Seja F'/K' uma extensão de F/K e P' um lugar de F'/K' sobre P lugar de F/K. Então*

(a) *$f(P'/P) < \infty$ se e so se $[F' : F] < \infty$.*

(b) *Se F''/K'' é uma extensão algébrica de F'/K' e $P'' \in \mathbb{P}''_F$ é uma extensão de P', então*

$$e(P''/P) = e(P''/P').e(P'/P) \quad \text{e} \quad f(P''/P) = f(P''/P').f(P'/P) \text{ .}$$

Dem. :

(a) Lembre que *deg* $P = [F_P : K] < \infty$ e *deg* $P' = [F'_{P'} : K'] < \infty$. Como

$$[F'_{P'} : K] = [F'_{P'} : K'].[K' : K] = [F'_{P'} : F_P].[F_P : K]$$

então: $[F'_{P'} : K] < \infty$ se e só se $[F'_{P'} : F_P] < \infty$ se e só se $[K' : K] < \infty$, por (??.b); isto é,

$$[K'/K] < \infty \iff [F' : F] < \infty \text{ .}$$

Logo, como $f(P'/P) = [F'_{P'} : F_P]$, tem-se

$$f(P'/P) < \infty \iff [F' : F] < \infty \text{ .}$$

(b) $x \in F \Longrightarrow v_{P'}(x) = e(P'/P).v_P(x)$

$$\begin{aligned} x \in F \subseteq F' \quad \Longrightarrow \quad v_{P''}(x) &= e(P''/P').v_{P'}(x) = \\ &= e(P''/P').e(P'/P)v_P(x) \end{aligned}$$

Considere $F_P \subseteq F'_{P'} \subseteq F''_{P''}$. Logo,

$$[F''_{P''} : F_P] = [F''_{P''} : F'_{P'}].[F'_{P'} : F_P] \text{ .}$$

□

Proposição B.1.7 *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.*

Dem. :

(a) Primeiro provemos que existe algum $z \in \mathbb{F}$ tal que $v_{P'}(z) \neq 0$. Isso será feito por contradição : Suponhamos que para todo $z \in \mathbb{F}$, $v_{P'}(z) = 0$; tome $t \in F'$ e suponhamos que $v_{P'}(t) > 0$; t é algébrico sobre F; logo, existem $c_i \in F$, $i = 0, \ldots, n$, com $c_0, c_n \in \mathbb{F}$ tais que

$$c_n t^n + \ldots + c_1 t + c_0 = 0 .$$

Por hipótese, $v_{P'}(c_i) = 0$; assim,

$$v_{P'}(c_0) = min\{iv_{P'}(t)/i = 1, \ldots, n\} > 0 .$$

Contradição. Logo, $P' \cap F \neq \emptyset$.

Por (B.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 1.5.9). Afirmamos que para $P' \in \mathbb{P}'_F$ vale:

$$P'/P \Longleftrightarrow v_{P'}(x) > 0 \tag{B.2}$$

$(\Rightarrow)$ $v_{P'}(x) = ev_P(x) = e > 0$.

$(\Leftarrow)$ $v_{P'}(x) > 0$.

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 (B.2), P'/P. Agora como o conjunto dos zeros de x em F' é finito, (B.2) garante que temos apenas um número finito P' tais que P'/P.

□

Lema B.1.8 *Seja K'/K extensão finita e x transcendente sobre K. Então*

$$[K'(x) : K(x)] = [K' : K] .$$

Dem. :
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 provarmos que $[K' : K] \leq [K'(x) : K(x)]$ precisamos 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 existe $g(T), h(T) \in K(x)[T]$ polinômios mônicos com grau menor que *deg* ϕ tais que $\phi(T) = g(T)h(T)$. Como $\phi(\alpha) = 0$, então $g(\alpha) = 0$ ou $h(\alpha) = 0$; suponhamos que $g(\alpha) = 0$ e *deg* $(g) = r$, então:

$$g(T) = T^r + c_{r-1}(x)T^{r-1} + \ldots + c_1(x)T + c_0(x)$$

com $c_i(x) \in K(x)$ e $r <$ *deg* ϕ; então

$$\alpha^r + c_{r-1}(x)\alpha^{r-1} + \ldots + c_1(x)\alpha + c_0(x) = 0\,.$$

Multiplicando por um denominador comum, obtemos:

$$g_r(x)\alpha^r + g_{r-1}(x)\alpha^{r-1} + \ldots + g_1(x)\alpha + g_0(x) = 0 \tag{B.3}$$

onde $g_i(x) \in K[x]$, e podemos assumir que $x \not| g_i(x)$para algum $i \in \{1, \ldots, r\}$. Tomando $x = 0$ em (B.3) obtem-se um polinômio em K, que se anula em α e tem grau menor que *deg* ϕ.

□

Teorema B.1.9 *Seja F'/K' extensão finita de F/K, P um lugar de F/K e $P_1, \ldots, P_n$ os lugares de F'/K que estão sobre P. Sejam $e_i = e(P_i/P)$ e $f_i = f(P_i/P)$. Então*

$$\sum_{i=1}^{n} e_i.f_i \;=\; [F' : F]\,.$$

Dem. :
Escolhemos $x \in F$;tal que 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 $P_i/P, i = 1, \ldots, n$ são exatamente os zeros de x em F'/K'. Agora vamos avaliar $[F' : K(x)]$.

$$\begin{aligned}
[F' : K(x)] &= [F' : K'(x)].[K'(x) : K(x)] \\
&= (\sum_{i=1}^{n} v_{P_i}(x)\,deg\ P_i)[K' : K] \\
&= (\sum_{i=1}^{n} e_i v_P(x)[F'_{P_i} : K'])[K' : K] \\
&= v_P(x)(\sum_{i=1}^{n} e_i[F'_{P_i} : K'])[K' : K] \\
&= s(\sum_{i=1}^{n} e_i[F'_{P_i} : K]) \\
&= s(\sum_{i=1}^{n} e_i[F'_{P_i} : F_P][F_P : K]) \\
&= s(\sum_{i=1}^{n} e_i.f_i)\,deg\ P \\
&= v_P(x)\,deg\ P(\sum_{i=1}^{n} e_i.f_i) = [F' : K(x)]
\end{aligned} \tag{B.4}$$

Temos também que $[F' : K(x)] = [F' : F].[F : K(x)]$. Mas, sendo P o único zero de x em F, temos que

$$[F : K(x)] = v_P(x) deg\ P \tag{B.5}$$

De (B.4) e (B.5) obtem-se que $[F' : F] = \sum_{i-1}^{n} e_i.f_i$.

□

Corolário B.1.10 *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 $f(P'/P) \leq [F' : F]$.*

Dem. :

(a) Seja $m = \#\{P' \in \mathbb{P}'_F | P'/P\}$ como $e_i, f_i \geq 1$, então $m \leq \sum_{i=1}^{m} e_i.f_i = [F' : F]$.

(b) $e_i, f_i \geq 1, \sum e_i.f_i = [F' : F] \Longrightarrow e_i, f_i \leq [F' : F]$.

□

O próximo resultado nos fornece um critério de irredutibilidade 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.

Proposição B.1.11 *Considere o corpo de funções F/K e o polinômio*

$$\phi(T) = a_n T^n + a_{n-1} T^{n-1} + \ldots + a_1 T + a_0$$

com coeficientes $a_i \in F$. Assuma que existe um lugar $P \in \mathbb{P}_F$ tal que uma das condição a seguir vale:

1. $v_P(a_n) = 0, v_P(a_i) \geq v_P(a_0) > 0$, *para* $i = 1, \ldots, n-1$ *e* $mdc\ (n, v_P(a_0)) = 1$.
2. $v_P(a_n) = 0, v_P(a_i) \geq 0$, *para* $i = 1, \ldots, n-1, v_P(a_0) < 0$ *e* $mdc(n, v_P(a_0)) = 1$.

Então $\phi(T)$ é irredutível em $F[T]$. Se $F' = F(y)$ onde y é uma raíz de $\phi(T)$, então P possui uma única extensão $P' \in \mathbb{P}'_F$, e tem-se $e(P'/P) = n$ e $f(P'/P) = 1$.

Dem. :
Consideremos 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 irredutível em $F(T)$. Seja $P' \in \mathbb{P}'_F$ extensão de P. Como $\phi(y) = 0$, temos:

$$-a_n y^n = a_0 + a_1 y + \ldots + a_{n-1} y^{n-1} \tag{B.6}$$

- se vale (1), temos:

$$\begin{aligned} v_{P'}(-a_n y^n) &= v_{P'}(a_n) + n v_{P'}(y) \\ &= e(P'/P) v_P(a_n) + n v_{P'}(y) \\ &\geq min\{v_{P'}(a_0), \{v_{P'}(a_i) + i v_{P'}(y)/i = 1, \ldots, n-1\}\} \\ &\geq min\{e(P'/P) v_P(a_0), \{e(P'/P) v_P(a_i) + i v_{P'}(y) | \ i = 1, \ldots, n-1\}\ \} \end{aligned}$$

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 $mdc(n, v_P(a_0)) = 1$, então $n|e$; logo, $n \leq e$. Mas, como $n = [F' : F] \geq e$, temos que $n = e$, e portanto, $f = f(P'/P) = 1$ e $\phi(T)$ é irredutível.

- se vale (2), temos:

$$v_{P'}(-a_0) \geq min\{v_{P'}(a_n y^n), \{v_{P'}(a_i) + i.v_{P'}(y)| \, i = 1, \ldots, n-1\}\}$$

Mas, como $v_P(a_0) < 0$, temos que $v_{P'}(y) < 0$, pois para $i = 1, \ldots, n-1$, $v_P(a_i) \geq 0$, 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.

□

Bibliografia

[1] A.Garcia e P.Viana : Weierstrass points on certain non-classical curves. Arch. Math. 46 (315-322), 1986.

[2] A.Garcia, S.J.Kim e R.F.lax : Consecutive Weierstrass gaps and minimum distance of Goppa codes. Journal of Pure and Applied Algebra 84 (199-207). North-Holland, 1993.

[3] H.Janwa : On the Parameters of Algebraic Geometric Codes. lecture Notes in Computer Science, 539 (19-28), Springer. Berlin, 1991.

[4] H.Stichtenoth : Algebraic Function Fields and Codes. Universitext, Springer-Verlag, Berlin heifelberg, 1993.

[5] H.Stichtenoth : A Note on Hermetian Codes over GF(q^2). IEEE Trns.Inform.Theory, 34 (1345-1348), 1988.

[6] K.Yang e P.V.Kumar : On the True Minimum Distance of Hermitian Codes. Lecture Notes in Mathematics, 1518 (99-107), Springer. Berlin, 1992.

[7] M.A.Tsfasman e S.G.Vladut : Algebraic-Geometric Codes. Kluwer A.Publishers. Dordrecht-Boston-London, 1991.

[8] V.D.Goppa : Algebraico-Geometric Codes. Math.USSR-Izv.21 (75-91), 1983.

[9] V.D.Goppa : Geometry and Codes. Kluwer A.Publishers, Dordrecht, 1988.