Universidade Federal do ABC
Centro de Matemática, Computação e Cognição

Dissertação de Mestrado

Álgebras Munidas de Função Peso e Códigos de Goppa Bi-Pontuais

por

Joyce dos Santos Caetano[1]
Mestrado em Matemática Aplicada

Santo André
2010

[1]Este trabalho contou com o apoio financeiro da Fundação Universidade Federal do ABC

Álgebras munidas de função peso e códigos de Goppa bi-pontuais.

Este exemplar corresponde à redação final da dissertação por **Joyce dos Santos Caetano**.

Santo André, 26 de Abril de 2010.

Prof. Dr. Ercílio Carvalho da Silva
Orientador

Banca Examinadora:

1. Prof. Dr. Ercílio Carvalho da Silva.
2. Prof. Dr. Paulo Roberto Brumatti.
3. Prof. Dr. Edson Ryoji Okamoto Iwaki.

Dissertação a ser apresentada ao CMCC - Centro de Matemática, Computação e Cognição, UFABC, como requisito parcial para a obtenção do Título de MESTRE em Matemática Aplicada.

CAETANO, Joyce dos Santos

Álgebras munidas de função de peso e códigos de Goppa bi-pontuais / Joyce dos Santos Caetano - Santo André : Universidade Federal do ABC, 2010.

90 fls. il. 29 cm

Orientador: Ercílio Carvalho da Silva

Dissertação (Mestrado) - Universidade Federal do ABC, Centro de Matemática, Computação e Cognição, Matemática, 2010.

1. Álgebra 2. Goppa - Códigos 3. Teoria dos códigos I. SILVA, Ercílio Carvalho da. II. Centro de Matemática, Computação e Cognição, Matemática, 2010, III. Título.

CDD 512

Universidade Federal do ABC

Serviço Público Federal
UNIVERSIDADE FEDERAL DO ABC

Assinaturas dos membros da Banca Examinadora que avaliaram e aprovaram a defesa de Dissertação de Mestrado da candidata ***Joyce dos Santos Caetano****, realizada em 26 de abril de 2010:*

Dr. Ercílio Carvalho da Silva (UFABC)

Dr. Paulo Roberto Brumatti (UNICAMP)

Dr. Edson Ryoji Okamoto Iwaki (UFABC)

Dedicatória

Dedico este trabalho à minha mãe e a todos que estiveram presentes na minha vida durante o desenvolvimento deste trabalho

Agradecimento

Ao meu orientador professor Ercílio Carvalho da Silva, pela orientação, paciência e sua enorme dedicação em responder meus questionamentos.

Aos professores Paulo Roberto Brumatti e Edson Ryoji Okamoto Iwaki, pelas sugestões e observações feitas neste trabalho.

Ao Leandro, auxiliar administrativo da PPG-Matemática, no auxílio rotineiro.

Ao apoio financeiro da Fundação Universidade Federal do ABC.

Resumo

O objetivo principal desta dissertação é apresentar o resultado de F. Torres e C. Munuera sobre as álgebras munidas de duas funções peso fraco bem comportadas serem anéis de coordenadas afim de curvas algébricas com exatamente dois lugares de grau um no infinito. A partir disto, pode-se concluir que os códigos de avaliação construídos sobre estas álgebras são códigos geométricos de Goppa bi-pontuais.

Abstract

The main objective of this text is to present the central result of F. Torres and C. Munuera concerning those algebra with two weight function good behaved being affine coordinate ring of an affine algebraic curve with exactly two place at infinity. From this we can conclude that the evaluation codes constructed on this algebra are geometric Goppa codes support two point.

Lista de Símbolos

$\mathbb{F}_q$	corpo finito com q elementos;
ω(a)	peso da palavra a;
$\mathbb{N}_0$	conjunto dos inteiros não negativos;
R	$\mathbb{F}$-álgebra (anel comutativo com unidade contendo $\mathbb{F}$);
v_P	valorização no ponto P;
$C_\Omega(D;G)$	código geométrico de Goppa associado aos divisores D e G;
deg(G)	grau do divisor G;
$\ell(G)$	dimensão do divisor G;
$\mathcal{X}$	curva projetiva, não singular e absolutamente irredutível;
G(Q)	conjunto das lacunas Weierstrass no ponto Q;
H(P)	semigrupo de Weierstrass associado ao ponto P;
K	corpo de funções algébricos de uma variável.
$\mathcal{O}_P$	anel de valorização;
$d(l;m)$	cota ordem fraca.

Sumário

Introdução

A Teoria de Códigos Corretores de Erros surgiu no começo da década de 50 como parte complementar de um trabalho teórico do matemático americano Claude E. Shannon, que em 1948 publicou uma série de resultados que se tornaram conhecidos como A Teoria Matemática das Comunicações, hoje conhecida como A Teoria da Informação.

Algumas formas simples de codificação e decodificação de mensagens foram propostas pelo próprio Shannon, porém muito mais como instrumentos para auxiliar as provas matemáticas dos seus resultados gerais do que como maneiras eficientes de se obter tamanho grau de confiabilidade na comunicação. Em suma, Shannon demonstrou a existência de codificadores e decodificadores eficientes, porém não ensinou como obtê-los.

O trabalho inicial para a obtenção das primeiras classes de bons códigos corretores de erros foi árduo, pois exigia um profundo conhecimento de Álgebra Abstrata e Teoria de Probabilidade, sendo desenvolvido por um grupo restrito composto basicamente por matemáticos, embora a importância prática daquele tema já fosse reconhecida pelos engenheiros de comunicações da época.

Os primeiros estudos realizados após a publicação do trabalho de Shannon foram aplicados aos sistemas de comunicação espacial. No entanto códigos corretores de erros estão presentes em nosso cotidiano de inúmeras formas, por exemplo, quando fazemos uso de informações digitalizadas, tais como ouvir CD de música, assistir um filme de DVD, navegar pela Internet, etc.

Na década de 80 o matemático russo V.D. Goppa publicou alguns artigos, onde a principal ferramenta matemática para a construção dos códigos eram as curvas algébricas e por este motivo receberam o nome de Códigos Geométricos de Goppa. Desde então, os pesquisadores vem aprimorando esta teoria.

Contudo, a construção proposta por Goppa é muito trabalhosa para não conhecedores de geometria algébrica. Então em 1998, Høholdt, van Lint e Pellikaan propuseram em [14] uma construção alternativa de códigos lineares, onde deixaram de utilizar as curvas algébricas e passaram a utilizar resultados de álgebra linear e da teoria de semigrupos numéricos. Mas para que fosse possível esta nova construção, os autores introduziram os conceitos de função ordem e função peso e os códigos assim construídos ficaram conhecidos como códigos de avaliação. Eles acreditavam que havia surgido uma nova classe de códigos, mas Matsumoto[12] provou que na realidade os códigos de avaliação eram códigos de Goppa pontuais.

Em 2004, E.Silva [7] estendeu o conceito de função ordem e peso, deu-lhe o nome de função ordem fraca e função peso fraco e a partir deste conceito construiu códigos de avaliação envolvendo duas funções peso fraco e assim como fizeram Høholdt, van Lint e Pellikaan para códigos de avaliação envolvendo uma função peso, exibiu uma cota inferior para os códigos duais dos códigos de avaliação construídos. Em seguida C.Munuera e F.Torres [2] estudaram a estrutura do semigrupo gerado por duas funções peso fraco bem comportadas e caracterizaram as álgebras que as admitem.

Nesta dissertação, estamos interessados em apresentar o resultado central de C.Munuera e F.Torres. Os autores provaram que uma álgebra munida de duas funções peso fraco bem comportadas, é o anel de coordenadas afim de uma curva algébrica com dois lugares de grau um no infinito e consequentemente os códigos construídos sobre essas álgebras são códigos de geométricos de Goppa bi-pontuais. Para este fim, este trabalho foi estruturado da seguinte maneira:

No primeiro capítulo veremos os conceitos relacionados com a teoria de Goppa. Assim, apresentaremos as teorias dos códigos corretores de erros, dos corpos de funções algébricas sobre uma variável e dos códigos geométricos de Goppa.

No segundo capítulo, inicialmente veremos a construção dos códigos de avaliação proposto por Høholdt, van Lint e Pellikaan. Em seguida, apresentaremos os resultados relativos ao conceito de função ordem fraca e peso fraco, construiremos os códigos de avaliação envolvendo duas funções peso fraco e determinaremos uma cota inferior para a distância minima do seu código dual também apresentaremos uma ligação entre os códigos de ava-

liação construídos sobre determinadas álgebras e os códigos geométricos de Goppa.

No terceiro capítulo apresetaremos os resultados relativos as álgebras que admitem duas funções peso fraco bem comportadas e finalizaremos concluindo que os códigos de avaliação construídos sobre essas álgebras são códigos geométricos de Goppa bi-pontuais.

Para finalizar existem dois apêndices, no primeiro expomos os conceitos de álgebra comutativa utilizados ao longo deste trabalho e no segundo são fornecidos algumas definições e resultados sobre curvas algébricas.

Capítulo 1

Preliminares

Neste capítulo apresentaremos os conceitos básicos tais como as definições e teoremas mais relevantes da teoria de códigos corretores erros, mas para que seja possível o seu entendimento necessitamos realizar os estudos de conceitos de corpos de funções algébricos, divisores e espaço associado ao divisor, para a partir deste estudo realizarmos a construção dos códigos algébricos geométricos proposto por Goppa que também são conhecidos por Códigos Geométricos de Goppa. Todo o capítulo foi baseado no livro *Algebraic function fields and codes*, referência [9], isto que dizer que as definições e os resultados podem ser encontrados na referência.

1.1 Códigos

Nesta seção apresentaremos as noções básicas da teoria de códigos.
Seja $\mathbb{F}_q$ um corpo finito com q elementos e considere o espaço vetorial n-dimensional $\mathbb{F}_q^n$ chamado *alfabeto* cujo os elementos são as n-uplas $a = (a_1, ..., a_n)$, com $a_i \in \mathbb{F}_q$.
Para $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n) \in \mathbb{F}_q^n$ seja

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

A função d é chamada de *distância de Hamming* em $\mathbb{F}_q^n$. Definimos também o *peso* de

um elemento $a \in \mathbb{F}_q^n$ como sendo

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

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

Definição 1.1. *Um* **código linear** C *(sobre o alfabeto* $\mathbb{F}_q^n$*) é um subespaço linear de* $\mathbb{F}_q^n$*. Os elementos de* C *são chamados de* **palavras-códigos**. *Chamamos* n *o comprimento de* C *e dim* C *(como* $\mathbb{F}_q-$*espaço vetorial) a dimensão de* C*. Um* $[n, k]-$*código é um código de comprimento* n *e dimensão* k*. A* **distância mínima** $d(C)$ *de um código* $C \neq 0$ *é definido por*

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

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

$$d(C) = min\{\omega(c), c \in C, c \neq 0\}$$

Vamos nos referir a um $[n, k]$-código com distância mínima d por $[n, k, d]-$código.
Uma maneira simples de descrever um específico código C é descrever sua base (como $\mathbb{F}_q-$espaço vetorial). Assim, seja C um $[n, k]-$código sobre $\mathbb{F}_q$, uma *matriz geradora* de C é a matriz $k \times n$, cujas linhas formam uma base de C.

Definição 1.2. *Se* $C \subset \mathbb{F}_q^n$ *é um código, então*

$$C^{\perp} := \left\{u \in \mathbb{F}_q^n : \langle u, c\rangle = 0, \forall c = (c_1, ..., c_n) \in C\right\}$$

é chamado de o **código dual** *de* C*, onde* $\langle , \rangle$ *denota o produto interno canônico. Quando* $C = C^{\perp}$ *dizemos que* C *é auto-dual e se* $C \subset C^{\perp}$ *então definimos* C *como auto-ortogonal.*

Da álgebra linear temos que o dual de um $[n, k]-$código é um $[n, n - k]-$código e $(C^{\perp})^{\perp} = C$. Em particular a dimensão de um código auto-dual de comprimento n é $n/2$. Seja C um $[n, k]-$código em $\mathbb{F}_q^n$. Definimos como *matriz teste de paridade* do código C a matriz geradora $H_{(n-k)\times n}$ de $C^{\perp}$. Mais ainda,

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

onde u^t denota a transposta do vetor u. Observe que uma matriz teste de paridade identifica se um vetor $u \in \mathbb{F}_q^n$ é uma palavra código ou não.

Um dos problemas básicos na teoria de códigos algébricos é o de construir, sobre um alfabeto fixado $\mathbb{F}_q^n$, códigos cujas as dimensões e a distância mínima são grandes em relação ao comprimento. Entretanto, há algumas restrições: se a dimensão de um código é grande (com relação ao comprimento) então a distância mínima é pequena. Veremos a seguir, uma cota simples que relaciona os parâmetros de um código.

Proposição 1.3 (Cota de Singleton)**.** *Para um* $[n, k, d]-$*código temos que*

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

Códigos satisfazendo $k + d = n + 1$ tem seus parâmetros otimizados e são chamados códigos MDS (códigos separados pela máxima distância). Se $n \leq q + 1$, existem códigos MDS sobre $\mathbb{F}_q$ para todas as dimensões $k \leq n$.

1.2 Corpos de Funções Algébricas

Nesta seção veremos os elementos necessários para a construção do código geométrico de Goppa.

1.2.1 Lugares

Definição 1.4. *Um* **corpo de funções algébricas** *ou (simplesmente, corpo de funções)* $F|K$ *de uma variável sobre um corpo* K *é uma extensão de corpos* $K \subseteq F$ *tal que* F *é uma extensão algébrica finita de* $K(x)$ *e* $x \in F$ *é transcendente sobre* K*.*

O conjunto $\widetilde{K} = \{z \in F | z$ é algébrico sobre $K\}$ é um subcorpo de F chamado de *corpo de constantes* de $F|K$. Mais ainda, $F|\widetilde{K}$ é um corpo de funções sobre K .

Um corpo de funções $F|K$ é dito ser *racional* se $F = K(x)$ para algum $x \in F$ transcendente sobre K. Neste caso, $K(x)$ é o corpo de frações do anel de polinômios $K[x]$ em uma variável sobre K.

Definiremos agora o que vem a ser um anel de valorização.

Definição 1.5. *Um* **anel de valorização** *do corpo de funções $F|K$ é um anel $\mathcal{O} \subseteq F$ com as seguintes propriedades:*

1. $K \subsetneq \mathcal{O} \subsetneq F$;
2. *Qualquer $z \in F$ temos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$*

Tal anel é local cujo único ideal maximal é $P = \mathcal{O} \setminus \mathcal{O}^*$, com $\mathcal{O}^* = \{z \in \mathcal{O} |$ existe $w \in \mathcal{O}$ com $zw = 1\}$, isto é, $\mathcal{O}^*$ é o grupo das unidades de $\mathcal{O}$. Assim, para $x \in F$ tem-se que $x \in P$ se, e somente se, $x^{-1} \notin \mathcal{O}$ e para o corpo de constantes $\widetilde{K}$ de $F|K$ temos que $\widetilde{K} \subseteq \mathcal{O}$ e $P \cap \widetilde{K} = \{0\}$. A seguir enunciaremos o resultado principal que caminha nesta direção.

Teorema 1.6. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções $F|K$ e $P = \mathcal{O} \setminus \mathcal{O}^*$ seu único ideal maximal. Então:*

1. *P é um ideal principal.*
2. *Se $P = t\mathcal{O}$, então qualquer $z \in F$ e $z \neq 0$ tem uma única representação na forma $z = t^n u$ para algum $n \in \mathbb{Z}$ e $u \in \mathcal{O}^*$.*
3. *$\mathcal{O}$ é um domínio de ideal principal. Mais precisamente, se $P = t\mathcal{O}$ e $\{0\} \neq I \subseteq \mathcal{O}$ é um ideal, então $I = t^n\mathcal{O}$ para algum $n \in \mathbb{N}$.*

Isto nos leva a um outro conceito, a saber:

Definição 1.7.
1. *Um* **lugar** *P de um corpo de funções $F|K$ é o ideal maximal de algum anel de valorização $\mathcal{O}$ de $F|K$. Qualquer elemento $t \in P$ tal que $P = t\mathcal{O}$ é chamado* **elemento primo** *de P;*
2. *$\mathbb{P}_F := \{P : P$ é um lugar de $F|K\}$.*

Observe que dado um anel de valorização $\mathcal{O}$ cujo ideal maximal é P, então $\mathcal{O}$ pode ser unicamente determinado por P, a saber: $\mathcal{O} := \mathcal{O}_P = \{z \in F | z^{-1} \notin P\}$. Neste caso, chamamos $\mathcal{O}_P$ de *anel de valorização do lugar P*. Uma segunda descrição muito útil de lugares é dada em termos de valorizações.

Definição 1.8. *Um* **valorização discreta** *de $F|K$ é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades: Para quaisquer $x, y \in F$ temos*

1. *$v(x) = \infty$ se, e somente se $x = 0$;*
2. *$v(xy) = v(x) + v(y)$;*
3. *$v(x + y) \geq min\{v(x), v(y)\}$, com igualdade quando $v(x) \neq v(y)$;*
4. *Existe $z \in F$ tal que $v(z) = 1$;*
5. *$v(a) = 0$ para todo $0 \neq a \in K$.*

Neste contexto, o símbolo ∞ se refere a um elemento não pertencente a $\mathbb{Z}$ tal que $\infty + \infty = \infty + n = n + \infty = \infty$ e $\infty > m$ para todo $m, n \in \mathbb{Z}$.
Das propriedades (2) e (4) segue que v é sobrejetora e a propriedade (3), quando válido a igualdade, é chamada de *desigualdade triangular estrita.*

Agora, seja um lugar $P \in \mathbb{P}_F$. Podemos associar a P uma função $v_P : F \to \mathbb{Z} \cup \{\infty\}$ da seguinte maneira: escolha um elemento primo $t \in P$, então, do teorema 1.6, qualquer elemento não-nulo $z \in F$ possui uma única representação da forma $z = t^n u$ com $u \in \mathcal{O}_P^*$ e $n \in \mathbb{Z}$. Assim, definimos $v_P(z) := n$ e $v_P(0) := \infty$, segue:

Teorema 1.9. *Seja $F|K$ um corpo de funções.*

1. *Para qualquer lugar $P \in \mathbb{P}_F$, a função v_P definida acima é uma valorização discreta de $F|K$. Mais ainda:*

$$\mathcal{O}_P = \{z \in F | v_P \geq 0\},$$

$$\mathcal{O}_P^* = \{z \in F | v_P = 0\},$$

$$P = \{z \in F | \upsilon_P > 0\}.$$

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

2. *Reciprocamente, supondo que υ é uma valorização discreta de $F|K$, então o conjunto $P = \{z \in F | \upsilon(x) > 0\}$ é um lugar de $F|K$ e $\mathcal{O}_P = \{z \in F | \upsilon_P(z) \geq 0\}$ é o anel de valorização correspondente.*

3. *Qualquer anel de valorização $\mathcal{O}$ de $F|K$ é um subanel maximal de F.*

Seja P um lugar de $F|K$ e $\mathcal{O}_P$ o anel de valorização correspondente. Então o anel das classes residuais $\mathcal{O}_P/P := F_P$ é um corpo, chamado de *corpo das classes residuais* de P. A aplicação $x \mapsto x(P)$ de F em $F_P \cup \{\infty\}$, onde $x(P) := x + P$ se $x \in \mathcal{O}_P$ e $x(P) := \infty$ caso contrário, é chamada de *aplicação de classe residual* com respeito a P. Assim, podemos considerar que K é um subcorpo de F_P, pois $K \subseteq \mathcal{O}_P$, $K \cap P = \{0\}$ e logo a aplicação residual $\mathcal{O}_P \to F_P$ induz um mergulho canônico de K em F_P. Do mesmo modo, K é visto como um subcorpo de F_P.

Definição 1.10. *Seja $P \in \mathbb{P}_F$. Definimos o* **grau** *de um lugar P como sendo:*

$$grau\ P := [F_P : K]$$

O grau de um lugar é sempre finito, mais precisamente, dados um lugar $P \in \mathbb{P}_F$ e $0 \neq x \in P$ tem-se que $grau\ P \leq [F : K(x)] < \infty$. (ver na referência [9], proposição I.1.14)

Uma importante descrição dos elementos de $\mathbb{P}_F$ é dada a partir da valorização discreta correspondente a estes elementos sobre os elementos de F.

Definição 1.11. *Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um* **zero de ordem m** *se e somente se $\upsilon_P(z) = m > 0$; P é um* **pólo de ordem m** *se e somente se $\upsilon_P(z) = -m < 0$.*

A seguir, nos concetraremos em questões sobre a existência de lugares em $F|K$.

Teorema 1.12. *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 $R \subseteq \mathcal{O}_P$.*

Desta forma podemos afirmar que:

Corolário 1.13. *Sejam $F|K$ um corpo de funções e $z \in F$ tal que z é transcendente sobre K. Então z tem no mínimo um zero e um pólo. Em particular $\mathbb{P}_F \neq \emptyset$.*

Demonstração. Considere o anel $R = K[z]$ e o ideal $I = zK[z]$. O teorema anterior assegura que existe um lugar $P \in \mathbb{P}_F$ com $z \in P$, daí $\upsilon_P(z) > 0$ e logo P é um zero de z. Analogamente, existe um lugar Q que é zero de z^{-1}. Logo, Q é um pólo de z. □

Vimos que se $x \in F$ é transcendente sobre K então este possui zeros e pólos. O próximo resultado nos permite, de alguma forma, concluir algo a respeito da quantidade de zeros e pólos de x.

Proposição 1.14. *Em um corpo de funções $F|K$, qualquer elemento não nulo $x \in F$ possui uma quantidade finita de zeros e pólos.*

Demonstração. Seja $F|K$ um corpo de funções e $P_1, ..., P_r$ zeros de um elemento $z \in F$. Então

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

Assim, se x é algébrico sobre K e como $K \cap P = \{0\}$, temos que x não tem zeros nem pólos. E, se x é transcendente sobre K então o número de zeros de x é menor ou igual a $[F : K(x)]$. De maneira análoga, tem-se que a quantidade de pólos de x é finita. □

O seguinte resultado, conhecido como o Teorema da Aproximação Fraca, estabelece que se $\upsilon_1, ..., \upsilon_n$ são valorizações discretas de $F|K$ duas a duas distintas, $z \in F$ e se sabemos os valores $\upsilon_1(z), ..., \upsilon_{n-1}(z)$, então não podemos concluir nada a respeito de $\upsilon_n(z)$.

Teorema 1.15 (Teorema da Aproximação Fraca (T.A.F))**.** *Seja $F|K$ um corpo de funções, $P_1, ..., P_n \in \mathbb{P}_F$, lugares dois a dois distintos de $F|K$, $x_1, ..., x_n \in F$ e $r_1, ..., r_n \in \mathbb{Z}$. Então existe algum $x \in F$ tal que $\upsilon_{P_i}(x - x_i) = r_i$ para $i = 1, ..., n$.*

1.2.2 Corpos de Funções Racionais

Nesta seção veremos um exemplo de corpos de funções, seus respectivos anel de valorização e lugares. Dado um polinômio arbitrário $p(x) \in K[x]$, mônico e irredutível, considere o anel de valorização.

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

de $K(x)|K$ e que tem o ideal maximal

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

Neste caso, $p(x)$ é um elemento primo para P e a valorização discreta corresponde v_P pode ser descrita como: se $z \in K(x) \backslash \{0\}$ é escrito da forma $z = p(x)^n h(x)$ com $n \in \mathbb{Z}$ e $h(x) \in \mathcal{O}_{p(x)} \setminus P_{p(x)}$, então $v_P(z) = n$. O corpo das classes residuais $K(x)_P = \mathcal{O}_P / P_{p(x)}$ é isomorfo a $K[x]/(p(x))$ e consequentemente $grau\ P = grau\ p(x)$.

Um outro anel de valorização de $K(x)|K$ é descrito como

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], grau\ f(x) \leq grau\ g(x) \right\}$$

cujo ideal maximal é

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

Este é chamado de *lugar no infinito* de $K(x)$. Observe que este rótulo depende especificamente da escolha do elemento $x \in K(x)|K$ por exemplo, $K(x) = K(\frac{1}{x})$ e o lugar P_∞ com respeito a $\frac{1}{x}$ é o lugar P_0 com respeito a x. Com efeito

$$\begin{aligned} P_\infty &= \left\{ \frac{f(\frac{1}{x})}{g(\frac{1}{x})}; f\left(\frac{1}{x}\right); g\left(\frac{1}{x}\right) \in K\left[\frac{1}{x}\right],\ grau\ f\left(\frac{1}{x}\right) < grau\ g\left(\frac{1}{x}\right) \right\} \\ &= \left\{ \frac{a_0 + a_1 \frac{1}{x} + \ldots + a_n \left(\frac{1}{x}\right)^n}{b_0 + b_1 \frac{1}{x} + \ldots + b_m \left(\frac{1}{x}\right)^m}; b_m \neq 0, m > n \right\} \\ &= \left\{ \frac{\left(\frac{1}{x}\right)^n (a_0 x^n + \ldots a_n)}{\left(\frac{1}{x}\right)^m (b_0 x^m + \ldots + b_m)}; b_m \neq 0, m > n \right\} \\ &= \left\{ x^{m-n} \frac{f'(x)}{g'(x)}; x \not| g'(x), m > n \right\} = P_0 \end{aligned}$$

Assim, $t = \frac{1}{x}$ é um elemento primo de P e $grau\ P_\infty = 1$. A valorização discreta correspondente a P_∞ é dada por

$$v_\infty \left(\frac{f(x)}{g(x)} \right) = grau\ g(x) - grau\ f(x),\ onde\ f(x), g(x) \in K[x].$$

Na realidade, estes são os únicos anéis de valorização de $K(x)$. Logo,

Teorema 1.16. *Os únicos lugares no corpo de funções racionais $K(x)|K$ são os lugares $P_{p(x)}$ e P_∞ definimos acima.*

1.2.3 Divisores

Nesta seção definiremos o que vem a ser um divisor os seus elementos além de seus respectivos espaços associados e por fim as suas propriedades. No que segue, $F|K$ denotará um corpo de funções algébricos de uma variável sobre K, com K algebricamente fechado em F.

Definição 1.17. *O grupo abeliano livre o qual é gerado pelos lugares de $F|K$ é denotado por $\mathcal{D}_F$ sendo chamado de* **grupo divisor** *de $F|K$. Os elementos de $\mathcal{D}_F$ são chamados de* **divisores** *de $F|K$ e são da forma*

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

com $n_P \in \mathbb{Z}$ quase todos não nulos.

O *suporte* de D é definido por

$$supp\ D := \{P \in \mathbb{P}_F; n_P \neq 0\}$$

Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ é chamado de *divisor primo.* Dois divisores $D = \sum n_P P$ e $D' = \sum n'_P P$ são somados da seguinte maneira

$$D + D' = \sum (n_P + n'_P) P.$$

O elemento zero do grupo divisor $\mathcal{D}_F$ é o divisor com todos os n_p nulos.
Dados $Q \in \mathbb{P}_F$ e $D \in \mathcal{D}_F$, definimos $\upsilon_Q(D) := n_Q$, logo

$$supp\ D = \{P \in \mathbb{P}_F; \upsilon_P(D) \neq 0\}\ e$$

$$D = \sum_{P \in supp\ D} \upsilon_P(D) P.$$

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

$$D_1 \leq D_2 \Leftrightarrow \upsilon_P(D_1) \leq \upsilon_P(D_2),$$

para qualquer $P \in \mathbb{P}_F$.

Assim, dizemos que um divisor é *positivo* se $D \geq 0$.

O *grau* de um divisor é definido por:

$$grau\ D := \sum_{P \in \mathbb{P}_F} \upsilon_P(D) grau\ P$$

Sabemos que um elemento não nulo $x \in F$ tem uma quantidade finita de zeros e pólos em $\mathbb{P}_F$. Deste modo, podemos definir:

Definição 1.18. *Seja $0 \neq x \in F$ e denotaremos por Z e por N o conjunto de zeros e pólos de x em $\mathbb{P}_F$. Então definimos:*

$$\begin{array}{ll} (x)_0 = \sum_{P \in Z} \upsilon_P(x)P, & o \textbf{ divisor zero } de\ x; \\ (x)_\infty = \sum_{P \in N} -\upsilon_P(x)P, & o \textbf{ divisor de pólo } de\ x; \\ (x) := (x)_0 - (x)_\infty, & o \textbf{ divisor principal } de\ x; \end{array}$$

Observe que se $(x)_0 \geq 0$, $(x)_\infty \geq 0$ e que $x \in K$ se, e somente se, $(x) = 0$.

Definimos como sendo o *grupo dos divisores principais* de $F|K$ o conjunto $\mathcal{P}_F := \{(x); x \in F \setminus \{0\}\} \subseteq \mathcal{D}_F$. O grupo quociente $\mathcal{C}_F = \mathcal{D}_F/\mathcal{P}_F$ é chamado de o *grupo de classe dos divisores.* A classe corresponde em $\mathcal{C}_F$ do divisor $D \in \mathcal{D}_F$ será denotada por $[D]$. Dois divisores D e D' são ditos *equivalentes*, denotaremos por $D \sim D'$, se $[D] = [D']$, isto é, $D = D' + (x)$ para algum $x \in F \setminus \{0\}$.

Definiremos agora um espaço vetorial que é fundamental importância à teoria de corpos de funções algébricas.

Definição 1.19. *Para um divisor $A \in \mathcal{D}_F$, definimos o K-espaço vetorial associado ao divisor A, como sendo o conjunto*

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

dito de outro modo,

$$\mathcal{L}(A) = \{x \in F | \upsilon_P(x) \geq -\upsilon_P(A), \forall P \in \mathbb{P}_F\} \cup \{0\}.$$

Lema 1.20. *1.* $\mathcal{L}(0) = K$;

2. $\mathcal{L}(A) \neq \{0\}$ *se e somente se, existe* $A' \sim A$ *com* $A' \geq 0$;

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

4. Se $A' \sim A$ *então* $\mathcal{L}(A)$ *é isomorfo (como* K*-espaço vetorial) a* $\mathcal{L}(A')$.

Dado um espaço vetorial V, denotaremos sua dimensão por *dim* V.

Lema 1.21. *Seja* A, B *divisores de* $F|K$ *com* $A \leq B$. *Então temos que* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *e*

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

O resultado abaixo nos fornece uma importante informação sobre a dimensão dos espaços $\mathcal{L}(A)$.

Definição 1.22. *Para* $A \in \mathcal{D}_F$, *o inteiro dim* $A :=$ *dim* $\mathcal{L}(A)$ *é chamado de* **dimensão** *do divisor* A.

O próximo resultado nos diz que há, essecialmente, uma relação entre o número de zeros e o números de pólos (contando com a respectiva ordem) de um elemento não-nulo de F.

Teorema 1.23. *Qualquer divisor principal tem grau zero. Mais precisamente, dado* $x \in F \setminus K$, *temos que*

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

Demonstração. Seja $n = [F : K(x)]$ e $B := (x)_\infty = \sum_{i=1}^{r} -\upsilon_{P_i}(x)P_i$ onde $P_1, ..., P_r$ são pólos de x. Então

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

É suficiente mostrar que $n \leq grau\ B$. Escolha uma base $u_1, ..., u_n$ de $F|K(x)$ e um divisor $C \geq 0$ tal que $(u_i) \geq -C$ para $i = 1, ..., n$. Então, temos que

$$dim\ (lB + C) \geq n(l + 1),\ para\ todo\ l \geq 0,$$

pois, $x^i u_j \in \mathcal{L}(lB + C)$ para $0 \leq i \leq l$ e $1 \leq j \leq n$. Observe também que estes elementos são linearmente independente sobre K, devido ao fato de $x^i \in K(x)$ para $i = 1, .., l$ serem

linearmente independentes sobre K e $u_1, ..., u_n$ serem linearmente independente sobre $K(x)$. Chamando $c := grau\ C$ temos que $n(l+1) \leq dim\ \mathcal{L}(lB+C) \leq l\ grau\ B + c + 1$ o que implica que

$$l(grau\ B - n) \geq n - c - 1,\ para\ todo\ l \in \mathbb{N}.$$

Logo, para l suficientemente grande, temos que $grau\ B \geq n$.
Portanto, $grau\ (x)_\infty = [F : K(x)]$. Como $(x)_0 = (x^{-1})_\infty$, concluimos que $grau\ (x)_0 = grau\ (x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$. □

Este teorema nos traz a seguintes consequência:

Corolário 1.24. *Sejam os divisores A, A' com $A \sim A'$. Então:*

a) *$dim\ A = dim\ A'$ e $grau\ A = grau\ A'$;*

b) *Se $grau\ A < 0$ então $dim\ A = 0$;*

c) *Se $grau\ A = 0$ então as seguintes afirmações são equivalentes:*

- **1)** *A é principal*
- **2)** *$dim\ A \geq 1$*
- **3)** *$dim\ A = 1$*

O próximo resultado é fundamental para definirmos o que vem a ser o gênero de um corpo de funções.

Proposição 1.25. *Existe uma constante $\gamma \in \mathbb{Z}$ tal que para todos divisores $A \in \mathcal{D}_F$ temos que*

$$grau\ A - dim\ A \leq \gamma$$

Definição 1.26. *O* **gênero** *g de $F|K$ é definido por*

$$g := max\{grau\ A - dim\ A + 1 | A \in \mathcal{D}_F\}$$

Observe que o gênero de $F|K$ é um inteiro não negativo, pois tomando $A = (0)$ temos que $grau\ A - dim\ A + 1 = 0$, concluímos que $g \geq 0$. Um primeiro resultado a respeito do gênero de um corpo de funções é o seguinte:

Teorema 1.27 (Teorema de Riemann)**.** *Seja $F|K$ um corpo de funções de gênero g.*

a) *Para qualquer divisor $A \in \mathcal{D}_F$, temos que $dim\ A \geq grau\ A + 1 - g$;*

b) *Existe um inteiro c, dependendo de $F|K$ tal que $dim\ A = grau\ A + 1 - g$ sempre que $grau\ A \geq c$.*

Disto, pode-se mostrar que o gênero de um corpo de funções racionais $K(x)|K$ é zero, mas no geral, é complicado de se determinar o gênero de um corpo de funções.

1.2.4 O Teorema de Riemann-Roch

Nesta subseção denotaremos $F|K$ como um corpo de funções algébricas de gênero g.

Definição 1.28. *Para $A \in \mathcal{D}_F$ definimos o* **índice de especialidade** *de A como sendo:*

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

O Teorema de Riemann diz que $i(A)$ é um inteiro não negativo e $i(A) = 0$ se $grau\ A$ é suficientemente grande.

Definição 1.29. *Um* **adele** *de $F|K$ é uma aplicação*

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

tal que $\alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$.

O adele pode ser visto como um elemento do produto direto $\prod_{P \in \mathbb{P}_F} F$, assim usaremos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou simplesmente $\alpha = (\alpha_P)$. Definiremos o conjunto

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

por *espaço dos adele* de $F|K$, sendo este um espaço vetorial sobre K. Definimos também o *adele principal* de um elemento $x \in F$ como sendo o adele onde todas as componentes são iguais a x. Observe que esta definição faz sentido devido ao fato de a quantidade de pólos de x ser finito.

Definição 1.30. *Para $A \in \mathcal{D}_F$ definimos*

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

É fácil ver que este conjunto é um $K-$subespaço vetorial de $\mathcal{A}_F$.
O próximo resultado nos diz que apesar de $\mathcal{A}_F$, $\mathcal{A}_F(A)$ e F terem dimensão infinita o quociente

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

tem dimenão finita sobre K.

Teorema 1.31. *Para qualquer divisor A, o índice de especialidade é*

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

Consequentemente, tem-se que $g = dim\ (\mathcal{A}_F/(\mathcal{A}_F(0) + F))$.
Agora introduziremos o conceito de diferencial de Weil o qual dará uma segunda interpretação para o índice de especialidades de um divisor.

Definição 1.32. *Um* **diferencial Weil** *de $F|K$ é uma aplicação $K-$linear $\omega : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(A) + F$ para algum divisor $A \in \mathcal{D}_F$. Chamamos*

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

o módulo de diferencial de Weil de $F|K$. Para $A \in \mathcal{D}_F$ seja

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

O espaço Ω_F é um $K-$espaço vetorial e $\Omega_F(A)$ um subespaço de Ω_F. Observe que para $x \in F$ e $\omega \in \Omega_F$ a aplicação $x\omega : \mathcal{A}_F \to F$ definida por $(x\omega)(\alpha) := \omega(x\alpha)$ ainda é um diferencial de Weil. Disto pode-se concluir (não naturalmente) que Ω_F é um espaço vetorial unidimensional sobre F. Mais ainda, para $A \in \mathcal{D}_F$, temos que $dim\ \Omega_F = i(A)$.

É possível fazer uma conexão entre divisores e qualquer diferencial de Weil não-nulo. Fixando $0 \neq \omega \in \Omega_F$ e considerando o conjunto de divisores

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

pode-se garantir a existência de um único divisor $W \in M(\omega)$ tal que $A \leq W$ para qualquer $A \in M(\omega)$. Isto, nos permite definir:

Definição 1.33. *1. O* **divisor** (ω) *de um diferencial de Weil* $\omega \neq 0$ *é o único divisor de* $F|K$ *satisfazendo:* ω *se anula em* $\mathcal{A}_F((\omega)) + F$*; e se* ω *se anula em* $\mathcal{A}_F(A) + F$ *então* $A \leq (\omega)$*.*

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

3. Um lugar P *é dito um zero (respectivamente pólo) de* ω *se* $\upsilon_P(\omega) > 0$ *(respectivamente* $\upsilon_P(\omega) < 0$*).* ω *é chamado* **regular** *em* P *se* $\upsilon_P(\omega) \geq 0$ *e* ω *é dito ser regular (ou holomorfico) se* P *é regular para qualquer lugar* $P \in \mathbb{P}_F$*.*

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

Das observações feitas após a definição 1.32 tem-se que para $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$ então $(x\omega) = (x) + (\omega)$ e quaisquer dois divisores canônicos de $F|K$ são equivalentes. Uma simples consequência disto é que os dois divisores de $F|K$ formam uma única classe $[W]$ no grupo quociente $\mathcal{C}_F$. A esta classe de divisores damos o nome de *classe canônica* de $F|K$.

Teorema 1.34. *Seja* A *um divisor arbitrário e* $W = (\omega)$ *um divisor canônico de* $F|K$*. Então aplicação*

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

é um isomorfismo de $K-$*espaço vetorial. Em particular,* $i(A) = dim\ (W - A)$*.*

Agora estamos em condições de enunciar e provar um dos principais resultados da teoria de Corpos de Funções Algébricos.

Teorema 1.35 (Teorema de Riemann-Roch)**.** *Seja* W *um divisor canônico de* $F|K$*. Então, para qualquer divisor* $A \in \mathcal{D}_F$ *temos*

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

Demonstração. Como $i(A) = dim\ A - grau\ A + g - 1$ e do teorema anterior temos $dim\ (W - A) = i(A)$ segue que

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

□

Corolário 1.36. *Para um divisor canônico W, nós temos grau $W = 2g-2$ e dim $W = g$.*

Sabemos do Teorema de Riemann que existe uma constante c tal que se *grau* $A \geq c$ então $i(A) = 0$. Agora, podemos dar, mais precisamente, uma descrição de como escolher esta constante.

Teorema 1.37. *Se A é um divisor de $F|K$ de grau $A \geq 2g-1$ então*

$$dim\ A = grau\ A + 1 - g.$$

Vejamos agora algumas das consequências do Teorema de Riemann-Roch. O primeiro resultado é um melhoramento do Teorema da Aproximação Fraca.

Teorema 1.38 (Teorema da Aproximação Forte)**.** *Seja $S \subsetneqq \mathbb{P}_F$, um subconjunto próprio de $\mathbb{P}_F$ e $P_1, ..., P_n \in S$. Suponha que sejam dados $x_1, ..., x_r \in F$ e $n_1, ..., n_r \in \mathbb{Z}$. Então existe um elemento $x \in F$ tal que*

$$\begin{aligned} &\upsilon_{P_i}(x - x_i) = n_i, \quad &&\text{para i=1,...,r e} \\ &\upsilon_P(x) \geq 0, &&\text{para P}\in S \setminus \{P_1, ..., P_r\}. \end{aligned}$$

Veremos agora alguns resultados sobre os elementos de F que possui apenas um pólo.

Proposição 1.39. *Seja $P \in \mathbb{P}_F$. Então para qualquer $n > 2g$ existe um elemento $x \in F$ com divisor de pólos $(x)_\infty = nP$.*

Definição 1.40. *Seja $P \in \mathbb{P}_F$. Um inteiro $n \geq 0$ é chamado de* **não lacuna** *de P se e somente se existe um elemento $x \in F$ com $(x)_\infty = nP$. Do contrário chamamos de n de* **lacuna** *de P.*

Claramente, n é uma não lacuna de P se e somente se *dim* $(nP) >$ *dim* $((n-1)P)$. Veremos posteriormente uma outra maneira de definir tais elementos.

Teorema 1.41 (Teorema das Lacunas de Weiestreiss)**.** *Suponha que $F|K$ tem gênero $g > 0$ e P é um lugar de grau um. Então existem exatamente g lacunas $i_1 < ... < i_g$ de P. Mais ainda, $i_1 = 1$ e $i_g \leq 2g - 1$.*

Vejamos agora o que vem a ser uma componente local de um diferencial de Weil.

Definição 1.42. *Seja* $P \in \mathbb{P}_F$

1. *Para* $x \in F$ *seja* $i_P(x) \in \mathcal{A}_F$ *o adele cuja a* $P-$*componenete é* x *e o restantes dos componentes é zero.*

2. *Para um diferencial de Weil* $\omega \in \Omega_F$ *definimos sua* **componente local** $\omega_P : F \to K$ *como sendo* $\omega_P(x) := \omega(i_P(x))$. *(Claramente,* ω_P *é* $K-$*linear)*

Sobre as componentes locais temos os seguintes resultados:

Proposição 1.43. *Seja* $\omega \in \Omega_F$ *e* $\alpha = (\alpha_P) \in \mathcal{A}_F$. *Então* $\omega_P(\alpha_P) \neq 0$ *para uma quantidade finita de lugares* P *e*

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

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

Proposição 1.44. 1. *Seja* $\omega \neq 0$ *um diferencial de Weil de* $F|K$ *e* $P \in \mathbb{P}_F$. *Então*

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

Em particular $\omega_P \neq 0$.

2. *Se* $\omega, \omega' \in \Omega_F$ *e* $\omega_P = \omega'_P$ *para algum lugar* $P \in \mathbb{P}_F$, *então* $\omega = \omega'$.
Disto, segue que, para $r \in \mathbb{Z}$, *que* $v_P(\omega) \geq r$ *se, e somente se,* $\omega(x) = 0$ *para todo* $x \in F$ *com* $v_P(x) \geq -r$.

1.3 Códigos Geométricos de Goppa

Nesta seção apresentaremos alguns resultados importantes e a construção dos Códigos Geométricos de Goppa. Sendo que de agora em diante, denotaremos $\mathbb{F}_q$ denota um corpo finito com q elementos.

Considere as seguintes notações:

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

$P_1, ..., P_n$ são lugares dois a dois distintos de $F|\mathbb{F}_q$ de grau 1.

$D = P_1 + ... + P_n$.

G é um divisor de $F|\mathbb{F}_q$ tal que *supp* $D \cap$ *supp* $G = \emptyset$

Definição 1.45. *O* **código geométrico de Goppa** $C_{\mathcal{L}}(D, G)$ *associados aos divisores* D *e* G *é definido por*

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

Observe que tal definição faz sentido: para $x \in \mathcal{L}(G)$ temos que $\upsilon_{P_i}(x) \geq 0$, para todo $i = 1, ..., n$, pois *supp* $D \cap$ *supp* $G = \emptyset$; para $x(P_i) \in F_{P_i}$, como *grau* $P_i = 1$ segue que $F_{P_i} = \mathbb{F}_q$, assim $x(P_i) \in \mathbb{F}_q$.

Diz-se que o código geométrico de Goppa é m-pontuais se existirem m pontos $\mathbb{F}_q$-racionais no suporte do divisor G. Consideremos a *aplicação avaliação*

$$\begin{array}{rccc} av_D: & \mathcal{L}(G) & \rightarrow & \mathbb{F}_q^n \\ & x & \mapsto & (x(P_1), ..., x(P_n)). \end{array}$$

Temos que av_D é $\mathbb{F}_q-$linear e a imagem de $\mathcal{L}(G)$ por esta aplicação é $C_{\mathcal{L}}(D, G)$.

Vejamos agora que, para um código $C_{\mathcal{L}}(D, G)$ cujos parâmetros são $[n, k, d]$, é possível, pelo teorema de Riemann-Roch, estimar seus parâmetros e obter um cota inferior para a distância mínima d_G.

Teorema 1.46. $C_{\mathcal{L}}(D, G)$ *é um* $[n, k, d]-$*código linear tal que*

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

Demonstração. Considerando a aplicação $av_D : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n$, definida acima, temos que $\mathcal{L}(G)/Ker(av_D)$ é isomorfo a $Im(av_D) = C_{\mathcal{L}}(D, G)$.

Como

$$\begin{aligned} Ker(av_D) &= \{x \in \mathcal{L}(G)\backslash\{0\} : (x(P_1), ..., x(P_n)) = (0, ..., 0)\} \\ &= \{x \in \mathcal{L}(G)\backslash\{0\}; \upsilon_{P_i}(x) > 0\ para\ i = 1, ..., n\} \cup \{0\} \\ &= \{x \in \mathcal{L}(G)\backslash\{0\} : \upsilon_{P_i}(x) \geq 1 = \upsilon_{P_i}(D) = \upsilon_{P_i}(D - G), i = 1, ..., n\} \\ &= \mathcal{L}(G - D) \end{aligned}$$

segue que $k = dim\ (\mathcal{L}(G)/Ker(av_D)) = dim\ G - dim\ (G - D)$.

Calculemos agora uma cota inferior para a distância mínima d. Lembre-se que o peso de um elemento x de um código é denotado por $\omega(x)$. Assuma que $C_{\mathcal{L}}(D,G) \neq \{0\}$. Escolha $x \in \mathcal{L}(G)$ tal que $\omega(av_D(x)) = d$. Então, existem $n-d$ lugares $P_{i_1}, ..., P_{i_{n-d}}$ no suporte de D tais que $v_{P_{i_j}}(x) > 0$, para $j = 1, ..., n-d$.
Logo $x \in \mathcal{L}(G - (P_{i_1} + ... + P_{i_{n-d}})) \setminus \{0\}$, ou seja, $dim\ (\mathcal{L}(G - (P_{i_1} + ... + P_{i_{n-d}}))) \geq 1$. Portanto, do corolário 1.24, segue que

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

ou seja, $d \geq n - grau\ G$. □

Uma consequência deste teorema é o seguinte resultado.

Corolário 1.47. *Suponha que grau de G é estritamente menor que n. Então a aplicação avaliação $av_D : \mathcal{L}(G) \to C_{\mathcal{L}}(D,G)$ é injetiva e ainda:*

1. *$C_{\mathcal{L}}(D,G)$ é um $[n,k,d]-$código com $d \geq n - grau\ G$ e $k = dim\ G \geq grau\ G + 1 - g$. Logo $k + d \geq n + 1 - g$.*

2. *Se $2g - 2 < grau\ G < n$ então $k = grau\ G + 1 - g$.*

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

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

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

Observe que a cota inferior para a distância mínima dada no item (1) deste corolário é muito parecida com a cota de Singleton. Assim toda vez que tivermos $grau\ G < n$ teremos

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

Note também que se F é um corpo de funções de gênero $g = 0$, então $d = n + 1 - k$. Assim, os códigos geométricos de Goppa construidos sobre um corpo de funções racionais $\mathbb{F}_q(z)$ serão códigos MDS (*Maximum Distance Separable*). Isto nos motiva a dar a seguinte definição:

Definição 1.48. *O inteiro $d_G := n - grau\ G$ é chamado de* **distância designada** *do código $C_{\mathcal{L}}(D, G)$.*

O teorema 1.46 estabelece que a distância mínima de um código geométrico de Goppa não pode ser menor que a distância designada. Agora, quando supomos que $dim\ G > 0$ e $d_G > 0$, temos que $d_G = d$ se e somente se existe um divisor D' com $0 \leq D' \leq D$, $grau\ D' = grau\ G$ e $dim\ (G - D') > 0$.
Por meio das componentes locais da diferencial de Weil, podemos associar um outro código aos divisores D e G, a saber:

Definição 1.49. *Seja G e $D = P_1 + ... + P_n$ divisores onde P_i são dois a dois distintos, $grau\ P_i = 1$ e $supp\ D \cap supp\ G = \emptyset$. Então definimos o código $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ por*

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

Um resultado análogo ao teorema 1.46 é o seguinte:

Teorema 1.50. *$C_\Omega(D, G)$ é um $[n, k', d']-$código tal que $k' = i(G - D) - i(G)$ e $d' \geq grau\ G - (2g - 2)$. Mais ainda, adicionando a hipótese de $grau\ G > 2g - 2$ temos que $k' = i(G - D) \geq n + g - 1 - grau\ G$. Se, contudo, tivermos $2g - 2 < grau\ G < n$, então $k' = n + g - 1 - grau\ G$.*

O próximo resultado nos mostra que existe uma relação entre os códigos $C_{\mathcal{L}}(D, G)$ e $C_\Omega(D, G)$.

Teorema 1.51. *Os códigos $C_{\mathcal{L}}(D, G)$ e $C_\Omega(D, G)$ são duais um do outro, isto é,*

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

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

$$\omega_P(x) = x(P)\omega_P(1) \tag{1.1}$$

De fato, com *grau* $P = 1$, podemos escrever $x = a+y$ onde $a = x(P) \in \mathbb{F}_q$ e $\upsilon_P(y) \geq 1$. Então

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

Note que $\omega_P(y) = 0$, pois $\upsilon_P(\omega) \geq -1,\ \upsilon_P(y) \geq 1$ e proposição 1.44.

Mostraremos que $C_\Omega(D,G) \subset C_\mathcal{L}(D,G)^\perp$. Seja $\omega \in \Omega_F(G-D)$ e $x \in \mathcal{L}(G)$, então, da proposição 1.50 e do fato de $x \in F$ e ω se anular em F, temos que $0 = \omega(x) = \sum_{P\in\mathbb{P}_F} \omega_P(x)$. Para $P \in \mathbb{P}_F \setminus \{P_1,..,P_n\}$ temos que $\upsilon_P(x) \geq -\upsilon_P(\omega)$.

Logo, da proposição 1.44, segue que $\omega_P(x) = 0$ e assim

$$0 = \sum_{P\in\mathbb{P}_F} \omega_P(x) = \sum_{i=1}^{n} \omega_{P_i} =^{1.1} \sum_{i=1}^{n} x(P_i)\omega_{P_i}(1) = \langle(\omega_{P_i}(1),...,\omega_{P_n}(1)),(x(P_1),...,x(P_n))\rangle$$

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

Agora mostraremos que a dimensão dos códigos $C_\Omega(D,G)$ e $C_\mathcal{L}(D,G)^\perp$ são iguais. Pelos teoremas 1.46 e 1.50 e o Teorema de Riemann-Roch, temos

$$\begin{aligned} dim\ C_\Omega(D,G) &= i(G-D) - i(G) \\ &= dim\ (G-D) - grau\ (G-D) - 1 + g - (dim\ G - grau\ G - 1 + g) \\ &= grau\ D + dim\ (G-D) - dim\ G \\ &= n - (dim\ G - dim\ (G-D)) \\ &= n - dim\ C_\mathcal{L}(D,G) = C_\mathcal{L}(D,G)^\perp \end{aligned}$$

□

Observação 1.52. *Um código $C_\Omega(D,G)$ pode ser representado como $C_\mathcal{L}(D,H)$, para um apropriado divisor H. A saber: seja η uma diferencial de Weil tal que $\upsilon_{P_i}(\eta) = -1$ e $\upsilon_{P_i}(1) = 1$ para $i = 1,...,n$. Então*

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

1.4 Subanéis de um Corpo de Funções

Nesta seção veremos os conceitos e resultados que serão fundamentais no último capítulo desta dissertação. No que segue, $F|K$ denota um corpo de funções com corpo de constantes K.

Definição 1.53. *Um* **subanel** *de $F|K$ é um anel de R tal que $K \subseteq R \subseteq F$ e R não é um corpo.*

Em particular, se R é um subanel de $F|K$ então $K \subsetneqq R \subsetneqq F$. Dois exemplos disso são:

a) $R = \mathcal{O}_P$ para algum $P \in \mathbb{P}_F$;

b) $R = K[x_1, ..., x_n]$ onde $x_1, ..., x_n \in F|K$.

Um exemplo mais geral de (a) é dado na seguinte definição:

Definição 1.54. *Para $\emptyset \neq S \subsetneqq \mathbb{P}_F$ seja*

$$\mathcal{O}_S := \{z \in F | v_P(z) \geq 0, \text{ para todo } P \in S\}$$

a interseção de todos os anéis de valorização $\mathcal{O}_P$ com $P \in S$. Qualquer anel $R \subseteq F$ que é dessa forma é chamado de **anel de holomorfia** *de $F|K$.*

Disto, temos que qualquer anel de holomorfia $\mathcal{O}_S$ é um subanel de $F|K$ que é integralmente fechado; o corpo de frações de $\mathcal{O}_S$ é F; qualquer anel de valorização $\mathcal{O}_P$ é um anel holomórfico; e para $P \in \mathbb{P}_F$ e $\emptyset \neq S \subsetneqq \mathbb{P}_F$ temos que $\mathcal{O}_S \subseteq \mathcal{O}_P$ se, e somente se, $P \in S$.

Teorema 1.55. *Seja R um subanel de $F|K$ e $\mathcal{S}(R) := \{P \in \mathbb{P}_F | R \subseteq \mathcal{O}_P\}$. Então:*

i) $\emptyset \neq S(R) \subsetneqq \mathbb{P}_F$;

ii) $\mathcal{O}_{S(R)}$ é o fecho integral $\overline{R}$ de R em F. Em particular, $\overline{R}$ é um subanel integralmente fechado de $F|K$ com corpo de frações F.

Uma consequência direta deste teorema é o seguinte resultado.

Corolário 1.56. *Um subanel R de $F|K$ com corpo de frações F é integralmente fechado se, e somente se, R é um anel de holomorfia.*

Observação 1.57. *Para $\emptyset \neq S \subseteq \mathbb{P}_F$ temos que $\mathcal{O}_S$ é um domínio de ideais principais. Tal resultado é uma generalização do teorema 1.6.*

Capítulo 2

Códigos de Avaliação

Este capítulo é parte fundamental dessa dissertação, pois veremos conceitos de função ordem e sua generalização conhecida como função ordem fraca bem como seus principais resultados e logo após passaremos a construção dos códigos via a estrutura de álgebra além de estudarmos uma parte da estrutura do semigrupo de Weiestrass para o caso onde $n = 2$.

2.1 Funções Ordens

Nesta seção descreveremos a construção de códigos de avaliação por meio de funções ordens. Sendo que no que segue, R denotará uma $\mathbb{F}$-álgebra, isto é, R é um anel comutativo com unidade contendo $\mathbb{F}$ como subanel.

Definição 2.1. *Uma função $\rho : R \to \mathbb{N}_0 \cup \{-\infty\}$ é chamada uma* **função ordem** *sobre R se as seguintes propriedades são satisfeitas. Sejam $f, g, h \in R$.*

(1) $\rho(f) = -\infty$ se, e somente se, $f = 0$;

(2) Para $\lambda \in \mathbb{F}^*$, $\rho(\lambda f) = \rho(f)$;

(3) $\rho(f + g) \leq max\{\rho(f), \rho(g)\}$, e a igualdade vale sempre que $\rho(f) \neq \rho(g)$;

(4) Se $\rho(f) < \rho(g)$ e $h \neq 0$, então $\rho(fh) < \rho(gh)$;

(5) Se $\rho(f) = \rho(g) \neq 0$, então existe $\lambda \in \mathbb{F}^*$ tal que $\rho(f - \lambda g) < \rho(f)$.

A função ρ é chamada uma **função peso** *sobre R, se além de (1)-(5) também satisfaz:*

(6) $\rho(fg) = \rho(f) + \rho(g)$.

Aqui, $\infty + n = -\infty$ para todo $n \in \mathbb{N}_0 \cup \{-\infty\}$.

Exemplo 2.2. *Uma $\mathbb{F}$-álgebra $R = \mathbb{F}[X]$ com a função ρ definida por $\rho(f) = grau\ f$ para toda $f \in R$, definida desta maneira ρ é uma função peso.*

Exemplo 2.3. *Seja $\mathbb{F}(\mathcal{X})$ o corpo de funções de uma curva $\mathcal{X}$ sobre $\mathbb{F}$. Seja P um ponto $\mathbb{F}$-racional. Seja $R := R(P)$ a $\mathbb{F}$-álgebra dada pela interseção dos anéis locais $\mathcal{O}_Q$ de $\mathbb{F}(\mathcal{X})$, nos pontos Q, como $Q \neq P$. Seja v_P a valorização em P. Portanto, $v_P(f) \geq 0$ para todo f não nulo em R. Defina $\rho(f) := -v_P(f)$ para $f \in R$. É consequência imediata das propriedades da valorização discreta que ρ é uma função peso.*

Lema 2.4. *Seja ρ uma função ordem sobre R. Então,*

(1) Se $\rho(f) = \rho(g)$ então $\rho(fg) = \rho(gh)$ para todo $h \in R$;

(2) Se $f \in R$ e $f \neq 0$ então $\rho(1) \leq \rho(f)$;

(3) $\mathbb{F} = \{f \in R : \rho(f) \leq \rho(1)\}$;

(4) Se $\rho(f) = \rho(g)$ então existe um único $\lambda \in \mathbb{F}^*$ tal que $\rho(f - \lambda g) < \rho(g)$.

Agora veremos que a existência de funções ordens sobre R está ligada á existência de certas $\mathbb{F}$-bases de R. O próximo teorema nos mostra que se existe uma função ordem sobre uma $\mathbb{F}$-álgebra R então existe uma $\mathbb{F}$-base de R, sendo que R visto como $\mathbb{F}$-espaço vetorial, com certas propriedades. Tal base nos permite construir os chamados Códigos de Avaliação.

Teorema 2.5. *Seja R uma $\mathbb{F}$-álgebra com função ordem ρ. Assuma que $R \neq \mathbb{F}$.*

(1) Então existe uma base $\{f_i : i \in \mathbb{N}\}$ de R sobre $\mathbb{F}$ tal que $\rho(f_i) < \rho(f_{i+1})$ para todo i.

(2) Se $f \in R$ e $f = \lambda_1 f_1 + ... + \lambda_i f_i$ onde $\lambda_1, ..., \lambda_i \in \mathbb{F}$ e $\lambda_i \neq 0$ então $\rho(f) = \rho(f_i)$.

(3) Seja $l(i,j) := l$ tal que $\rho(f_i f_j) = \rho(f_l)$. Assim, $l(i,j) < l(i+1,j)$ para todo i e j.

(4) Seja $\rho_i := \rho(f_i)$. *Se* ρ *é uma função peso então* $\rho_{l(i,j)} = \rho_i + \rho_j$.

Teorema 2.6. *Sejam* R *uma* $\mathbb{F}$*-álgebra. Seja* $\{f_i : i \in \mathbb{N}\}$ *uma* $\mathbb{F}$*-base do* $\mathbb{F}$*-espaço vetorial* R *com* $f_1 = 1$. *Seja* L_i *o espaço vetorial gerado por* $f_1, ...f_i$. *Seja* $l(i,j)$ *o menor inteiro* l *tal que* $f_i f_j \in L_l$. *Suponha que* $l(i,j) < l(i+1,j)$ *para todo* $i, j \in \mathbb{N}$. *Seja* $(\rho_i : i \in \mathbb{N})$ *uma sequência estritamente crescente de inteiros não negativos. Defina* $\rho(0) = -\infty$ *e* $\rho(f) = \rho_i$ *se* i *é o menor inteiro tal que* $f \in L_i$. *Então* ρ *é uma função ordem sobre* R.

Definição 2.7. *A aplicação*

$$\varphi : R \to \mathbb{F}_q^n,$$

é chamada um **morfismo** *de* $\mathbb{F}_q^n$*-álgebras se* φ *é* $\mathbb{F}_q$*-linear e*

$$\varphi(fg) = \varphi(f)\varphi(g)$$

Definição 2.8. *Na situação descrita acima considere* L_l *o espaço gerado por* $f_1, ..., f_l$ *e seja* φ *é um morfismo sobrejetor entre* $\mathbb{F}_q$*-álgebras. Definimos um código de avaliação* E_l *e seu código dual* C_l, *respectivamente, por*

$$E_l = \varphi(L_l) = \langle \varphi(f_1), ..., \varphi(f_l) \rangle$$

e

$$C_l = \{c \in \mathbb{F}_q^n : c.\varphi(f_i) = 0, \ \textit{para todo } i \leq l\}.$$

A sequência de códigos $(E_l : l \in \mathbb{N})$ é crescente com respeito a inclusão e todos eles são subespaços de $\mathbb{F}_q^n$. Logo, existe um natural N tal que $E_l = E_N$ para todo $l \geq N$. Observe que o código E_N é a imagem de R.

2.2 Funções ordem fraca

Nesta seção iremos abordar alguns dos resultados da função ordem fraca que trata-se de uma generalização da função ordem vista na seção 2.1, para modificarmos tais conceitos, vamos introduzir a seguintes notações.

Seja a aplicação

$$\rho : R \to \mathbb{N}_0 \cup \{-\infty\}.$$

Considere os seguintes conjuntos

$$\mathcal{M} = \mathcal{M}_\rho := \{f \in R : \rho(f) > \rho(1)\}$$

e

$$\mathcal{U} = \mathcal{U}_\rho := \{f \in R : f \neq 0 \text{ e } \rho(f) \leq \rho(1)\}.$$

Que chamamos de **não unidades** e **unidades** de R com respeito a ρ, respectivamente.

Definição 2.9. *A função ρ é chamada uma* **função ordem fraca** *sobre R se as seguintes propriedades são satisfeitas. Sejam f,g,h $\in R$.*

(I) $\rho(f) = -\infty$ *se, e somente se,* $f = 0$;

(II) Para $\lambda \in \mathbb{F}^*$, $\rho(\lambda f) = \rho(f)$;

(III) $\rho(f+g) \leq max\{\rho(f), \rho(g)\}$, *e a igualdade vale sempre que* $\rho(f) \neq \rho(g)$;

(IV) Se $\rho(f) < \rho(g)$ *então* $\rho(fh) \leq \rho(gh)$. *Entretanto, se* $h \in \mathcal{M}$, *então* $\rho(fh) < \rho(gh)$;

(V) Se $\rho(f) = \rho(g)$ *e* $f, g \in \mathcal{M}$, *então existe* $\lambda \in \mathbb{F}^*$ *tal que* $\rho(f - \lambda g) < \rho(f)$.

A função ρ é chamada de **função peso fraco** *sobre R, se além de $(I) - (V)$ também satisfaz:*

(VI) $\rho(fg) \leq \rho(f) + \rho(g)$ *e vale a igualdade sempre que* $f, g \in \mathcal{M}$.

Exemplo 2.10. *Naturalmente, uma função ordem é uma função ordem fraca com* $\mathcal{U} = \mathbb{F}^*$, *ver lema (2.4(3)).*

Exemplo 2.11 (Função Constante)**.** *Seja* $c \in \mathbb{N}_0$. *Para* $f \in R$ *definimos* $\rho(f) = -\infty$ *se* $f = 0$ *e* $\rho(f) = c$ *se* $f \neq 0$. *Assim,* $\mathcal{U} = R^*$ *e* $\mathcal{M} = \emptyset$. *Note que, por vacuidade, as propriedades (IV) e (V) são satisfeitos. É imediato que ρ é função ordem fraca sobre R mas não é função ordem sobre R. De fato, lembre que* $R \neq \mathbb{F}$. *Seja* $f \in R \backslash \mathbb{F} \subseteq R^*$. *Assim,* $\rho(f) \leq \rho(1)$, *mas* $\rho(f) = c \in \mathbb{N}_0$ *então* $\rho(f) \geq \rho(1)$, *o que implica* $\rho(f) = \rho(1)$. *Se ρ é uma função ordem, segue da propriedade (5) que existe* $\lambda \in \mathbb{F}^*$ *tal que* $\rho(f - \lambda 1) < \rho(1) = c$, *implica que* $\rho(f - \lambda 1) = -\infty$ *e assim* $f - \lambda = 0$ *o que implica* $f = \lambda \in \mathbb{F}$, *absurdo pois* $f \notin \mathbb{F}$.

Agora, veremos resultados da função ordem fraca e da estrutura da $\mathbb{F}$-álgebra R.

Lema 2.12. *Seja ρ uma função ordem fraca. Se $f, g, h \in \mathcal{M}$ e $\rho(f) = \rho(g)$ então $\rho(fh) = \rho(gh)$.*

Demonstração. Como $\rho(f) = \rho(g)$ então pela propriedade (V), existe $\lambda \in \mathbb{F}^*$ tal que $\rho(f - \lambda g) < \rho(g)$. Assim, aplicando as propriedades (IV) e (II), nessa ordem, temos que $\rho(fh - \lambda gh) < \rho(gh) = \rho(\lambda gh)$. Portanto, aplicando a propriedade (III) para as funções $(fh - \lambda gh)$ e λgh, concluímos que

$$\rho(fh) = \rho((fh - \lambda gh) + \lambda gh) = \rho(\lambda gh) = \rho(gh).$$

□

Proposição 2.13. *Seja $\widetilde{\mathcal{U}} := \mathcal{U} \cup \{0\}$. Uma $\mathbb{F}$-álgebra R é um domínio de integridade se, e somente se, existe uma função ordem fraca ρ sobre R tal que $\widetilde{\mathcal{U}}$ é um subanel de R que é um domínio.*

Demonstração. Suponha que R é um domínio de integridade. Tome ρ a função ordem fraca constante (ver Exemplo 2.11). Assim, $\widetilde{\mathcal{U}} = R$.
Agora, seja ρ função ordem fraca sobre R tal que $\widetilde{\mathcal{U}}$ é domínio de integridade. Tome $f, g \in R^*$. Devemos mostrar que $fg \neq 0$. Se $f, g \in \widetilde{\mathcal{U}}$, por hipótese, não há nada a provar. Assim, suponha que $f \in \mathcal{M}$ ou $g \in \mathcal{M}$. Sem perda de generalidade, admita que $f \in \mathcal{M}$, isto é, $\rho(1) < \rho(f)$. Como $g \neq 0$, então $\rho(0) < \rho(g)$. Logo, aplicando a propriedade (IV), temos que $\rho(0f) = \rho(0) < \rho(fg)$. Portanto, $fg \neq 0$. □

Exemplo 2.14. *Seja R uma $\mathbb{F}$-álgebra diferente de $\mathbb{F}$ e $g \in R \backslash \mathbb{F}$. A função $\rho := \rho_g$ definida por*

$$\rho_g(f) := \begin{cases} -\infty, & \text{se } f = 0 \\ 0, & \text{se } f \in \langle g \rangle \backslash \{0\} \\ 1, & \text{se } f \notin \langle g \rangle \end{cases}$$

onde $\langle g \rangle$ é o espaço gerado por g e ρ_gé uma função ordem fraca com $\mathcal{U}_\rho = R^*$. Que passaremos a demonstrar. Da definição, é imediato que as propriedades (I) e (II) são satisfeitas. Por vacuidade, as propriedades (IV) e (V) são satisfeitas. Resta-nos provar

a propriedade (III). Primeiramente vamos mostrar que $\rho_g(f+h) \leq max\{\rho_g(f), \rho_g(h)\}$. *Sejam* $f, h \in R$. *Se* $f+h=0$, *segue o que queremos. Se* $0 \neq f+h = \lambda g$ *então* $f \neq 0$ *ou* $h \neq 0$ *e, portanto,* $\rho_g(f+h) = 0 \leq \rho_g(f)$ *ou* $\rho_g(f+h) \leq \rho_g(h)$. *Se* $0 \neq f+h \notin \langle g \rangle$ *então* $f \notin \langle g \rangle$ *ou* $h \notin \langle g \rangle$ *e, portanto,* $\rho_g(f+h) = 1 = \rho_g(f)$ *ou* $\rho_g(f+h) = 1 = \rho_g(h)$. *Agora vamos mostrar que vale a igualdade se* $\rho_g(f) < \rho_g(h)$. *Se* $f = 0$, *é imediato o que queremos. Se* $0 \neq f \in \langle g \rangle$ *então* $h \notin \langle g \rangle$, $f+h \notin \langle g \rangle$ *e portanto* $\rho_g(f+h) = \rho_g(h)$.

O resultado abaixo caracteriza a função ordem em termos da função ordem fraca.

Lema 2.15. *Seja* $\rho : R \to \mathbb{N}_0 \cup \{-\infty\}$ *uma função. Então* ρ *é uma função ordem se, e somente se,* ρ *é uma função ordem fraca tal que* $\mathcal{U} = \mathbb{F}^*$.

Demonstração. Admita que ρ é uma função ordem. Da definição segue que ρ é função ordem fraca e do lema 2.4(3) segue que $\mathcal{U} = \mathbb{F}^*$.
Suponha que ρ é uma função ordem fraca com $\mathcal{U} = \mathbb{F}^*$. Temos que provar que ρ satisfaz as propriedades da definição de função ordem (ver 2.11). Da definição de função ordem fraca é imediato que ρ satisfaz as propriedades (1), (2) e (3). Sejam $f, g, h \in R$ tal que $h \neq 0$. Note que $R = \mathcal{M} \cup \mathcal{U} = \mathcal{M} \cup \mathbb{F}^*$. Primeiro, vamos provar que ρ satisfaz a propriedade (4). Com efeito, admita que $\rho(f) < \rho(g)$. Se $h \in \mathcal{M}$ então pela propriedade (IV) temos que $\rho(fh) < \rho(gh)$. Portanto, ρ satisfaz a propriedade (4). Para finalizar, provaremos que ρ satisfaz a propriedade (5). Suponha que $-\infty < \rho(f) = \rho(g)$. Se $f, g \in \mathcal{M}$ então pela propriedade (V) existe $\lambda \in \mathbb{F}^*$ tal que $\rho(f - \lambda g) < \rho(f)$. Se $f, g \in \mathcal{U} = \mathbb{F}^*$ tome $\lambda := \frac{f}{g}$. Assim, $\rho(f - \lambda g) < \rho(f)$. Logo, ρ satisfaz a propriedade (5). □

Agora trataremos da unicidade de $\lambda \in \mathbb{F}^*$ satisfazendo a propriedade (V). No caso de ρ ser função ordem esta questão foi tratada no Lema 2.4(4).

Lema 2.16. *Se* $\rho(1) < \rho(f) = \rho(g)$ *então existe único* $\lambda \in \mathbb{F}^*$ *tal que* $\rho(f - \lambda g) < \rho(f)$.

Demonstração. A existência é garantida pela propriedade (V). Vamos mostrar a unicidade. É imediato que $g \neq 0$. Admita que existem $\lambda, \mu \in \mathbb{F}^*$ tais que $\rho(f - \lambda g) < \rho(g)$ e $\rho(f - \mu g) < \rho(g)$. Assim, das propriedades (II) e (III) segue que

$$\rho((\mu - \lambda)g) = \rho((f - \lambda g) - (f - \mu g)) \leq Max\{\rho(f - \lambda g), (f - \mu g)\}.$$

Logo,

$$\rho((\mu - \lambda)g) < \rho(g).$$

Isto acontece apenas se $\mu - \lambda = 0$, pois $g \neq 0$. Daí temos que $\lambda = \mu$. □

Lema 2.17. *Seja ρ função ordem fraca tal que $\mathcal{U} \neq R^*$. Então $\mathcal{M} \neq \emptyset$ e o conjunto $\rho(\mathcal{M})$ possui infinitos elementos.*

Demonstração. É imediato que $\mathcal{M} \neq \emptyset$, pois caso contrário $\mathcal{U} = R^*$. Seja $f \in \mathcal{M}$. Aplicando a propriedade (IV) sucessivas vezes temos que

$$\rho(1) < \rho(f) < \rho(f^2) < \rho(f^3) < \dots .$$

Isto nos mostra que $\rho(\mathcal{M})$ possui infinitos elementos. □

Observação 2.18. *Para ρ como no lema anterior, admita que*

$$\rho(\mathcal{M}) = \{\rho_1 < \rho_2 < \rho_3 < \dots\}$$

Seja $F := \{f_i \in \mathcal{M} : i \in \mathbb{N}\}$ tal que $\rho(f_i) = \rho_i$, para todo $i \in N$. Assim, $\rho(F) = \rho(\mathcal{M})$.

Lema 2.19. *Seja ρ uma função ordem fraca com $\mathcal{U} \neq R^*$ e F nas condições da observação acima. Se $f \in \mathcal{M}$ e $\rho(f) = \rho(f_n)$ então existem únicos $\lambda_1, \dots, \lambda_n \in \mathbb{F}$, $\lambda_n \neq 0$ tais que*

$$f - (\lambda_1 f_1 + \dots + \lambda_n f_n) \in \widetilde{\mathcal{U}}.$$

Demonstração. Vamos provar a existência. Usaremos indução sobre n. Suponha que $\rho(f) = \rho(f_1)$. Pela propriedade (V), existe $\lambda_1 \in \mathbb{F}^*$ tal que

$$\rho(f - \lambda_1 f_1) < \rho(f_1).$$

Isto mostra que $(f - \lambda_1 f_1) \in \widetilde{\mathcal{U}}$, pois $\rho(h) \leq \rho(f_1)$ para todo $h \in \mathcal{M}$ por construção. Suponha que vale a propriedade para $m < n$. Se $\rho(f) = \rho(f_n)$, pela propriedade (V) existe $\lambda_n \in \mathbb{F}^*$ tal que

$$\rho(f - \lambda_n f_n) < \rho(f_n).$$

Caso $f - \lambda_n f_n = 0$, tome $\lambda_1 = \dots = \lambda_{n-1} = 0$. Assim,

$$f - (\lambda_1 f_1 + \dots + \lambda_n f_n) \in \widetilde{\mathcal{U}}.$$

Caso contrário, existe $a < n$ tal que $\rho(f - \lambda_n f_n) = \rho(f_a)$. Pela hipótese de indução, existem $\lambda_1, ..., \lambda_a \in F$, $\lambda_a \neq 0$, tal que

$$(f - \lambda_n f_n) - (\lambda_1 f_1 + ... + \lambda_a f_a) \in \widetilde{\mathcal{U}}.$$

Fazendo $\lambda_{a+1} = ... = \lambda_{n-1} = 0$, se necessário for, teremos que

$$f - (\lambda_1 f_1 + ... + \lambda_n f_n) \in \widetilde{\mathcal{U}}.$$

Vamos mostrar a unicidade. Suponha que existam $\lambda_1, ..., \lambda_n \in \mathbb{F}$ e $\mu_1, ..., \mu_n \in \mathbb{F}$ tais que $\lambda_n \neq 0,\ \mu_n \neq 0$ e

$$h_1 := f - (\lambda_1 f_1 + ... + \lambda_n f_n) \in \widetilde{\mathcal{U}} \ e$$

$$h_2 := f - (\mu_1 f_1 + ... + \mu_n f_n) \in \widetilde{\mathcal{U}}.$$

Assim,

$$\rho(f - \lambda_n f_n) = \rho(h_1 + \lambda_1 f_1 + ... + \lambda_{n-1} f_{n-1}) < \rho(f_n) \ e$$

$$\rho(f - \mu_n f_n) = \rho(h_2 + \mu_1 f_1 + ... + \mu_{n-1} f_{n-1}) < \rho(f_n).$$

Do Lema 2.16 segue que $\lambda_n = \mu_n$. Argumento análogo nos mostra que $\lambda_i = \mu_i$ para todo i tal que $1 \leq i \leq n - 1$. □

Teorema 2.20. *Seja ρ uma função ordem fraca sobre R tal que $\mathcal{U} \neq R^*$.*

(1) Existe um conjunto linearmente independente $F = \{f_i : i \in \mathbb{N}\} \cup \mathcal{M}$ tal que $\rho(f_i) < \rho(f_{i+1})$ e $\rho(F) = \rho(\mathcal{M})$.

(2) Seja $f \in R$. Então f pode ser escrito, de maneira única, da forma

$$f = f_0 + \sum_{i=1}^{n} \lambda_i f_i$$

onde $f_0 \in \widetilde{\mathcal{U}}$ e $\lambda_1, ..., \lambda_n \in \mathbb{F}$. Em outras palvras,

$$R = \widetilde{\mathcal{U}} \oplus \langle F \rangle .$$

Se $f \neq 0$ e n é o menor inteiro tal que f pode ser escrito da forma acima, então $\rho(f) = \rho(f_n)$.

(3) Seja l(i,j) o menor inteiro l tal que $\rho(f_i f_j) = \rho(f_l)$. *Então* $l(i,j) < l(i+1,j)$ *para todo* $i \in \mathbb{N}_0$ *e* $j \in \mathbb{N}$. *Se* ρ *é função peso fraco e* $i, j \in \mathbb{N}$, *então*

$$\rho_{l(i,j)} = \rho_i + \rho_j$$

onde $\rho(f_i) = \rho_i$.

Demonstração. (1) Da observação 2.18 segue que existe $F = \{f_i : i \in \mathbb{N}\} \subseteq \mathcal{M}$ tal que $\rho(f_i) < \rho(f_{i+1})$ e $\rho(F) = \rho(\mathcal{M})$. Vamos mostrar que F é linearmente independente. Suponha que

$$\lambda_1 f_1 + ... + \lambda_n f_n = 0$$

Sem perda de generalidade, admita que $\lambda_n \neq 0$. Assim,

$$0 < \rho(f_n) = \rho(\lambda_1 f_1 + ... + \lambda_n f_n) = \rho(0) = -\infty$$

contradição. Logo, $\lambda_1 = ... = \lambda_n = 0$.

(2) Se $f = 0$ o resultado é imediato. Suponha que $f \in R^*$. Se $f \in \mathcal{U}$, não há nada a provar. Assim, $f \in \mathcal{M}$ e existe $n \in \mathbb{N}$ tal que $\rho(f) = \rho(f_n)$. Do lema 2.19, existem únicos $\lambda_1, ..., \lambda_n \in \mathbb{F},\ \lambda_n \neq 0$, tal que

$$f_0 := f - (\lambda_1 f_1 + ... + \lambda_n f_n) \in \widetilde{\mathcal{U}}.$$

Isto nos mostra que f_0 é único. Portanto, f pode ser escrito de maneira única. Agora admita que n é o menor inteiro tal que

$$0 \neq f = f_0 + \lambda_1 f_1 + ... + \lambda_n f_n.$$

Se $f \in \widetilde{\mathcal{U}}$ então $f = f_0$ e $\rho(f) = \rho(f_0)$. Se $f \in \mathcal{M}$ então $\lambda_n \neq 0$. Das propriedades (III) e (II), temos

$$\rho(f) = \rho(f_0 + \lambda_1 f_1 + ... + \lambda_n f_n) = max\{\lambda_1 f_1, ..., \lambda_n f_n\} = \rho(\lambda_n f_n) = \rho(f_n)$$

(3) Já sabemos que $\rho(f_i) < \rho(f_{i+1})$ para todo $i \in \mathbb{N}_0$. Aqui, f_0 representa qualquer elemento de $\widetilde{\mathcal{U}}$. Seja $j \in \mathbb{N}$. Assim, $f_j \in \mathcal{M}$ e pela propriedade (IV) temos que $\rho(f_i f_j) < \rho(f_{i+1} f_j)$, como queríamos demonstrar. Da definição de função peso fraca segue que $\rho_{l(i,j)} = \rho_i + \rho_j$, sempre que $i, j \in \mathbb{N}$.

□

Teorema 2.21. *Seja* $\{f_i : i \in \mathbb{N}\} \cup R\backslash\mathbb{F}$ *um conjunto linearmente independente e* R_0 *o seu complemento que determina uma* $\mathbb{F}$*-base de R. Assim,*

$$R = \langle R_0 \rangle \oplus \langle f_1, f_2, ... \rangle .$$

Sejam $L_0 = \langle R_0 \rangle$, $L_l = R_0 \oplus \langle f_1, ..., f_l \rangle$ *para todo* $l \in \mathbb{N}$ *e l(i,j)=Min*$\{l : f_i f_j \in L_l\}$.
Para todo $i \in \mathbb{N}_0$, *suponha que*

$$l(i, j) < l(i + 1, j)$$

para todo $j \in \mathbb{N}$ *e que*

$$l(i, 0) \leq l(i + 1, 0).$$

Seja $(\rho_i : i \in \mathbb{N}_0)$ *uma sequência estritamente crescente de inteiros não negativos. Defina* $\rho(0) = -\infty$ *e* $\rho(f) = \rho_l$ *se l é o menor inteiro tal que* $f \in L_l$. *Então* ρ *é uma função ordem fraca sobre R. Se além disso,* $\rho_{l(i,j)} = \rho_i + \rho_j$ *para todo* $i, j \in \mathbb{N}$, *então* ρ *é uma função peso.*

Demonstração. Devemos provar que existe uma função peso fraco que satisfaz as condições do teorema. Com efeito, as propriedades (I), (II), (III) e (V) são consequências imediatas das definições. Vamos provar que a propriedade (IV) é satisfeita. Sejam $f, g, h \in R$ tais que

$$f = f_0 + \lambda_1 f_1 + ... + \lambda_r f_r,$$

$$g = g_0 + \beta_1 f_1 + ... + \beta_s f_s,$$

$$h = h_0 + \gamma_1 f_1 + ... + \gamma_t f_t,$$

$r < s$ e $1 \leq t$. Assim, $\rho(f) = \rho_r < \rho_s = \rho(g)$. Se $f = 0$ a propriedade (IV) é satisfeita. Suponha que $f \neq 0$. Logo, $s \geq 1$. Para $1 \leq i \leq s$ temos que $f_i h \in L_{l(t,i)}$ e $g_0 h \in L_{l(t,0)}$, pois $L_{l(0,i)} \subseteq L_{l(1,i)} \subseteq L_{l(t,i)}$. Portanto, $gh \in L_{l(t,s)}$. Pelo mesmo raciocínio, temos que $fh \in L_{l(t,r)}$. Por hipótese, $l(i, j) < l(i + 1, j)$ para todo $j \in N$. Assim, como $t \geq 1$ segue que $t \in \mathbb{N}$ e, portanto,

$$l(t, r) < l(t, r + 1) < l(t, r + 2) < ...$$

Consequentemente,

$$l(t, r) < ... < l(t, s - 1) < l(t, s)$$

pois $r \leq s-1 < s$. Isto mostra que,

$$\rho(fh) \leq \rho_{l(t,r)} < \rho_{l(t,s)} = \rho(gh)$$

onde a última igualdade vale pois $gh \in L_{l(t,s)} \backslash L_{l(t,s-1)}$. Do contrário, $f_s f_t \in L_{l(t,s-1)}$ o que é uma absurdo. Logo, podemos concluir que ρ é função ordem fraca. Agora veremos que ρ é função peso sobre R. Já sabemos que $1 \leq s, t$. Se $\rho_{l(i,j)} = \rho_i + \rho_j$ para todo $i, j \in N$ então

$$\rho(gh) = \rho_{l(t,s)} = \rho_t + \rho_s = \rho(h) + \rho(g) = \rho(g) + \rho(h).$$

Isto mostra que ρ é função peso. □

Agora, vamos fazer algumas considerações com o objetivo de se determinar uma $\mathbb{F}$-base para R por meio de funções ordens fracas. Recordemos que, se ρ é uma função ordem fraca sobre R então existe um subconjunto $F = \{f_i : i \in \mathbb{N}\} \subseteq \mathcal{M}$, linearmente independente sobre $\mathbb{F}$, tal que

$$R = \widetilde{\mathcal{U}}_\rho \oplus \langle F \rangle .$$

Portanto, ρ gerou um conjunto linearmente independente sobre $\mathbb{F}$, que por sua vez pode ser completado gerando um $\mathbb{F}$-base de R. Agora imagine que σ é uma outra função ordem fraca sobre R tal que $\mathcal{U}_\rho \not\subset \mathcal{U}_\sigma$, isto é, $\mathcal{U}_\rho \cap \mathcal{M}_\sigma \neq \emptyset$. Admita que $\widetilde{\mathcal{U}}_\rho$ é um anel. Logo, $\sigma_1 := \sigma|_{\widetilde{\mathcal{U}}_\rho}$ é função ordem fraca sobre $\widetilde{\mathcal{U}}_\rho$ com $\mathcal{U}_{\sigma_1} = \mathcal{U}_\rho \cap \mathcal{U}_\sigma$.
Assim, existe $G = \{g_i : i \in \mathbb{N}\} \subseteq \mathcal{M}_{\sigma_1} = \mathcal{M}_\sigma \cap \mathcal{U}_\sigma = \mathbb{F}^*$, linearmente independente sobre $\mathbb{F}$, tal que $\widetilde{\mathcal{U}}_\rho = \widetilde{\mathcal{U}}_{\sigma_1} \oplus \langle G \rangle$. Portanto,

$$R = \widetilde{\mathcal{U}}_{\sigma_1} \oplus \langle G \rangle \oplus \langle F \rangle = \widetilde{\mathcal{U}_\rho \cap \mathcal{U}_\sigma} \oplus \langle G \rangle \oplus \langle F \rangle .$$

Se $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}^*$ então

$$R = \mathbb{F} \oplus \langle G \rangle \oplus \langle F \rangle ,$$

e portanto ρ e σ fornecem uma $\mathbb{F}$-base de R. Esta análise motiva a próxima definição e também nos faz entender as condições suficientes que aparecem no teorema abaixo.

Definição 2.22. *Dizemos que uma função ordem fraca ρ sobre R, tem a* **propriedade de anel** *quando $\widetilde{\mathcal{U}}_\rho$ é um subanel de R.*

Teorema 2.23. *Sejam $\rho_1, ..., \rho_n$ funções ordens fracas sobre R com a propriedade de anel, $\mathcal{U}_i = \mathcal{U}_{\rho_i}$ e $\mathcal{M}_i = \mathcal{M}_{\rho_i}$ para $1 \leq i \leq n$. Suponha que*

$$R^* \supsetneq \mathcal{U}_1 \supsetneq \mathcal{U}_1 \cap \mathcal{U}_2 \supsetneq ... \supsetneq \mathcal{U}_1 \cap ... \cap \mathcal{U}_n = \mathbb{F}^*.$$

Então, existem $F_1 := \{f_{1j} : j \in \mathbb{N}\} \subseteq \mathcal{M}_1$ e $F_i := \{f_{ij} : j \in \mathbb{N}\} \subseteq (\mathcal{U}_1 \cap ... \cap \mathcal{U}_{i-1}) \cap \mathcal{M}_i$ para $2 \leq i \leq n$ tais que:

(1) $\rho_i(f_{ij}) < \rho_i(f_{i(j+1)})$ para $1 \leq i \leq n$ e $j \in \mathbb{N}$;

(2) $\rho_1(F_1) = \rho_1(\mathcal{M}_1)$ e $\rho_i(F_i) = \rho_i(\mathcal{U}_1 \cap ... \cap \mathcal{U}_{i-1} \cap \mathcal{M}_i)$;

(3) O conjunto $F_1 \cup ... \cup F_n \cup \{1\}$ forma uma $\mathbb{F}$-base de R. Ou seja,

$$R = \langle F_1 \rangle \oplus .... \oplus \langle F_n \rangle \oplus \langle 1 \rangle .$$

Demonstração. Provaremos usando indução sobre n. Se $n = 1$, então $\mathcal{U} = \mathbb{F}^*$ e portanto ρ_1 é uma função ordem sobre R (ver lema 2.15). Pelo teorema 2.8(1) segue o resultado. Admita, por hipótese de indução que o resultado é verdadeiro para $m < n$. Aplicando o Teorema 2.20 para ρ_1, temos que existe $F_1 = \{f_{1j} : j \in \mathbb{N}\} \subseteq \mathcal{M}_1$, linearmente independente sobre $\mathbb{F}$, tal que

$$\rho_1(f_{1j}) < \rho_1(f_{1(j+1)})$$

e

$$R = \langle F_1 \rangle \oplus \widetilde{\mathcal{U}_1}. \tag{2.1}$$

Agora, para $2 \leq i \leq n$ considere $\rho_i^{'} := \rho_i|_{\widetilde{\mathcal{U}_1}}$. Assim, $\rho_2^{'}, ..., \rho_n^{'}$ são funções ordens fracas sobre $\widetilde{\mathcal{U}_1}$, com a propriedade de anel, tais que

$$\mathcal{U}_i^{'} := \mathcal{U}_{\rho_i^{'}} = \mathcal{U}_1 \cap \mathcal{U}_i \quad e \quad \mathcal{M}_i^{'} := \mathcal{M}_{\rho_i^{'}} = \mathcal{U}_1 \cap \mathcal{M}_i.$$

Logo,

$$\mathcal{U}_2^{'} \cap ... \cap \mathcal{U}_i^{'} = \mathcal{U}_1 \cap \mathcal{U}_2 \cap ... \cap \mathcal{U}_i$$

e portanto

$$\widetilde{\mathcal{U}_1}^* \supsetneq \mathcal{U}_2^{'} \supsetneq ... \supsetneq \mathcal{U}_2^{'} \cap ... \cap \mathcal{U}_n^{'} = \mathbb{F}^*$$

pois

$$\widetilde{\mathcal{U}}_1^* = \mathcal{U}_1 \supsetneqq \mathcal{U}_1 \cap \mathcal{U}_2 \supsetneqq ... \supsetneqq \mathcal{U}_1 \cap .... \cap \mathcal{U}_n = \mathbb{F}^*.$$

Pela hipótese de indução, existem

$$F_2 = \{f_{2j} : j \in \mathbb{N}\} \subseteq \mathcal{M}_2^{'} = \mathcal{U}_1 \cap \mathcal{M}_2 \;\; e$$

$$F_i = \{f_{ij} : j \in \mathbb{N}\} \subseteq \mathcal{U}_2^{'} \cap ... \cap \mathcal{U}_{i-1}^{'} \cap \mathcal{M}_i^{'} = \mathcal{U}_1 \cap ... \cap \mathcal{U}_{i-1} \cap \mathcal{M}_i$$

para $3 \leq i \leq n$ tais que

$$\rho_i(f_{ij}) = \rho_i^{'}(f_{ij}) < \rho_i^{'}(f_{i(j+1)}) = \rho_i(f + i(j+1)) \;\; e$$

$$\rho_i(F_i) = \rho_i^{'}(F_i) = \rho_i^{'}(\mathcal{U}_1 \cap ... \cap \mathcal{U}_{i-1} \cap \mathcal{M}_i) = \rho_i(\mathcal{U}_i \cap ... \cap \mathcal{U}_{i-1} \cap \mathcal{M}_i)$$

para todo $2 \leq i \leq n$. Mais ainda,

$$F_2 \cup ... \cup F_n \cup \{1\}$$

é uma $\mathbb{F}$-base de $\widetilde{\mathcal{U}}_1$. Portanto, da equação 2.1 segue que

$$F_1 \cup F_2 \cup ... \cup F_n \cup \{1\}$$

gera R. Para finalizar, vamos mostrar que o conjunto acima é linearmente independente. Sejam $f = \sum_{j=1}^{r_1} \alpha_{1j} f_{1j} \in \langle F_1 \rangle$ e $g = \sum_{i=2}^{n} \sum_{j=1}^{r_i} \alpha_{ij} f_{ij} \in \langle F_2 \cup ... \cup F_n \cup \{1\} \rangle = \widetilde{\mathcal{U}}_1$ tais que

$$\sum_{j=1}^{r_1} \alpha_{1j} f_{1j} + \sum_{i=2}^{n} \sum_{j=1}^{r_i} \alpha_{ij} f_{ij} = 0$$

Sem perda de generalidade, suponha que $\alpha_{1r_1} \neq 0$. Então, pelas propriedades (II) e (III), temos que

$$0 \leq \rho_1(1) < \rho_1(f_{1r_1}) = \rho_1(\alpha_{1r_1} f_{1r_1}) = \rho_1(f) = \rho(f + g) = \rho_1(0) = -\infty.$$

Contradição. Assim, $\alpha_{1r_1} = 0$. Pelo mesmo raciocínio, segue que $\alpha_{11} = ... = \alpha_{1(r_1-1)} = 0$. Como $F_2 \cup ... \cup F_n \cup \{1\}$ é um conjunto linearmente sobre $\mathbb{F}$, segue que $\alpha_{ij} = 0$ para todo $2 \leq i \leq n$ e $1 \leq j \leq r_i$. Portanto, $F_1 \cup F_2 \cup ... \cup F_n \cup \{1\}$ é uma $\mathbb{F}$-base de R. $\square$

2.3 Códigos de Avaliação e Distância Mínima Dual.

Seja $\mathbb{F}(\mathcal{X})$ o corpo de funções de uma curva $\mathcal{X}$ sobre $\mathbb{F}$ de gênero g. Sejam P e Q pontos $\mathbb{F}$-racionais. Seja $R := R(P,Q)$ a $\mathbb{F}$-álgebra dada pela interseção dos anéis locais $\mathcal{O}_{Q_1}$ de $\mathbb{F}(\mathcal{X})$, nos pontos Q_1, com $Q_1 \neq P$ e $Q_1 \neq Q$. Sejam v_P a valorização em P e ρ a função ordem fraca definida por

$$\rho(f) := \begin{cases} -\infty, & se\ f = 0 \\ 0, & se\ v_P(f) \geq 0\ e\ f \neq 0 \\ -v_P(f), & se\ v_P(f) < 0 \end{cases} \tag{2.2}$$

para $f \in R$. Sejam v_Q a valorização em Q e σ a função ordem fraca definida por

$$\sigma(f) := \begin{cases} -\infty, & se\ f = 0 \\ 0, & se\ v_Q(f) \geq 0\ e\ f \neq 0 \\ -v_Q(f), & se\ v_Q(f) < 0 \end{cases} \tag{2.3}$$

para $f \in R$. Na verdade, ρ e σ são funções peso fraco sobre R. Assim, $\mathcal{U}_\rho = R(Q)^*$, $\mathcal{U}_\sigma = R(P)^*$ e

$$\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}^*.$$

Logo,

$$R \supsetneq \mathcal{U}_\rho \supsetneq \mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}^*.$$

Aplicando o teorema 2.23, existe $F \cup G_1 \cup \{1\} \subseteq R$ uma $\mathbb{F}$-base de R tal que:

$$\begin{cases} \begin{cases} F = \{f_i : i \in \mathbb{N}\} \subseteq \mathcal{M}_\rho \\ \rho(f_i) < \rho(f_{i+1}) \\ \rho(F) = \rho(\mathcal{M}_\rho) \end{cases} \\ \begin{cases} G_1 = \{g_i : i \in \mathbb{N}\} \subseteq \mathcal{U}_\rho \cap \mathcal{M}_\sigma = R(Q)^* \cap \mathcal{M}_\sigma = R(Q)\backslash\mathbb{F} \\ \sigma(g_i) < \sigma(g_{i+1}) \\ \sigma(G_1) = \sigma(\mathcal{U}_\rho \cap \mathcal{M}_\sigma) = \sigma(R(Q)\backslash\mathbb{F}) \end{cases} \\ \begin{cases} R &= \langle F \rangle \oplus \langle G_1 \rangle \oplus \langle 1 \rangle \\ &= \langle f_0, f_1, f_2, ... \rangle \oplus \langle g_1, g_2, ... \rangle\ \ onde\ f_0 = 1. \end{cases} \end{cases} \tag{2.4}$$

Se ρ é uma função peso fraco, então $d\rho$ para todo $d \in \mathbb{N}$ também será. Então definimos a normalização de ρ como sendo a função ordem fraca $\widehat{\rho}$ dada por

$$\begin{cases} \widehat{\rho}(f) & = 0 \qquad se\ f \in \mathcal{U}^* \\ \widehat{\rho}(f) & = \frac{\rho(f)}{d} \quad se\ f \in \mathcal{M} \end{cases}$$

onde $d = mdc\{\rho(f) : f \in \mathcal{M}\}$. No que segue, todas as funções peso fraco serão normais, isto é, $\rho = \widehat{\rho}$. O próximo lema relaciona os elementos da base com elementos do semigrupo de Weierstrss em P, Q e (P,Q).

Lema 2.24. *(1)* $\rho(\mathcal{M}_\rho) = \mathbb{N}$;

(2) $\sigma(\mathcal{U}_\rho \cap \mathcal{M}_\sigma) = \sigma(R(Q)\backslash\mathbb{F}) = H(Q)^*$.

Demonstração. (1) Da definição, é imediato que $\rho(\mathcal{M}_\rho) \subseteq \mathbb{N}$. Agora, seja $n \in \mathbb{N}$. Se $n \in H(P)$, então existe $f \in \mathbb{F}(\mathcal{X})$ tal que $div_\infty(f) = nP$. Assim, $f \in R(P) \subseteq R(P,Q) = R$ e $\rho(f) = n$. Caso $n \in G(P)$, então existe $m \in G(Q)$ tal que $(n,m) \in H(P,Q)$ onde $m = min\{s \in \mathbb{N} : (n,s) \in H(P,Q)\}$. Em outras palavras, existe $f \in \mathbb{F}(\mathcal{X})$ tal que $div_\infty(f) = nP + mQ$. Logo, $f \in R$ e $\rho(f) = n$. Portanto, $\rho(\mathcal{M}_\rho) = \mathbb{N}$.
(2) Imediato. □

Ainda estabelecendo as condições sobre os elememtos de F e G_1, suponha que $H(Q) = \{0 < m_1 < m_2 < ...\}$. De acordo com a demonstração do lema anterior, para todo $i \in \mathbb{N}$ temos:

$$\begin{cases} \rho(f_i) & = i \\ \sigma(f_i) & = \begin{cases} 0 & se\ i \in H(P) \\ min\{a : (i,a) \in H(P,Q)\} \in G(Q) & se\ i \in G(P) \end{cases} \\ \sigma(g_i) & = m_i. \end{cases} \tag{2.5}$$

De agora em diante, consideremos as funções $f_i, g_i \in R = R(P,Q)$ satisfazendo as condições dadas em 2.4 e 2.5. Também, considere o conjunto da lacunas associados ao ponto Q,

$$G(Q) = \{l_1' < ... < l_g'\}.$$

Seja G um divisor sobre a curva $\mathcal{X}$.

Proposição 2.25. *Se $G = lP + mQ$ e $l_g^{'} \leq m$ então*

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

Demonstração. Sabemos que $\mathcal{L}(G) \subseteq R$ e que $F \cup G_1 \cup \{1\}$ é uma $\mathbb{F}$-base de R. Vamos mostrar que $A := \{f_0, ..., f_l\} \cup \{g_j : m_j \leq m\}$ é uma $\mathbb{F}$-base de $\mathcal{L}(G)$. Já sabemos que o conjunto é linearmente independente. Da construção de f_i e g_j, é imediato que $A \subset \mathcal{L}(G)$. Resta-nos mostrar que o conjunto A gera $\mathcal{L}(G)$. Seja $f \in \mathcal{L}(G)$. Logo, $f \in R$. Do fato que $F \cup G_1 \cup \{1\}$, existem $i \in \mathbb{N}_0$, $j \in \mathbb{N}$, $\lambda_1, ..., \lambda_i \in \mathbb{F}$ e $\gamma_1, ..., \gamma_j \in \mathbb{F}$ tais que

$$f = \lambda_0 f_0 + ... + \lambda_i f_i + \gamma_1 g_1 + ... + \gamma_j g_j.$$

Sem perda de generalidade, suponha que $\lambda_i \neq 0$. Assim,

$$i = \rho(f_i) = \rho(f) = \begin{cases} 0, & se\ i = 0. \\ -\upsilon_P(f), & se\ i \geq 1. \end{cases}$$

Como $-\upsilon_P(f) \leq l$, pois $f \in \mathcal{L}(G)$, segue que

$$i \leq l. \tag{2.6}$$

Também, sem perda de generalidade, suponha que $\gamma_j \neq 0$. Assim,

$$m_j = \sigma(g_j) = \sigma(\gamma_1 g_1 + ... + \gamma_j g_j) = \sigma(f - (\lambda_0 f_0 + ... + \lambda_i f_i)).$$

Agora,

$$\sigma(f) = \begin{cases} 0, & se\ \upsilon_Q(f) \geq 0 \\ -\upsilon_Q(f), & se\ \upsilon_Q(f) < 0. \end{cases}$$

Disto e do fato de f estar em $\mathcal{L}(G)$, segue que $\sigma(f) \leq m$. Lembre que, por construção, $\sigma(f_i) \leq l_g^{'}$ para todo $i \in \mathbb{N}_0$. Consequentemente, $\sigma(\lambda_0 f_0 + ... + \lambda_i f_i) \leq l_g^{'}$. Portanto,

$$\begin{aligned} m_j &= \sigma(f - (\lambda_0 f_0 + ... + \lambda_i f_i)) \\ &\leq max\{\sigma(f), \sigma(\lambda_0 f_0 + ... + \lambda_i f_i)\} \\ &\leq max\{m, l_g^{'}\} = m. \end{aligned} \tag{2.7}$$

Das equações 2.6 e 2.7 nos mostram que A gera $\mathcal{L}(G)$. Assim sendo,

$$\begin{aligned}\ell(G) &= \#A \\ &= (l+1) + \#\{g_j : m_j \leq m\}\end{aligned}$$

Agora, $l_g^{'} \leq m$ nos diz que existem exatamente $(m-g)$ elementos no conjunto $\{g_j : m_j \leq m\}$. De fato, existem exatamente $(m-g)$ elementos m_j, maiores que 1 e menores ou iguais a m (tiramos as g lacunas). Portanto,

$$\ell(G) = (l+1) + (m-g) = deg\ G + 1 - g.$$

□

Corolário 2.26. *Se $G = lP + mQ$ e $l_g^{'} \leq m$ então*

$$\ell(W - G) = 0$$

onde W é um divisor canônico.

Demonstração. Segue da proposição 2.25 e do teorema de Riemann-Roch. □

Observação 2.27. *O resultado do corolário anterior já era conhecido sempre que $2g-1 \leq l+m$. O corolário anterior nos diz que podemos ter $l+m < 2g-1$, mas ainda $\ell(W-G) = 0$ se $l_g^{'} \leq m$.*

Agora vamos fazer uma **aplicação aos Códigos Geométricos de Goppa**, para códigos bi-pontuais.

De agora em diante, vamos trabalhar com $\mathbb{F} = \mathbb{F}_q$.

Sejam $P_1, ..., P_n$ pontos $\mathbb{F}_q$-racionais de $\mathcal{X}$, diferentes dois a dois e diferentes de P e Q.

Consideremos $m \in \mathbb{N}$. Seja $a \in \mathbb{N}$ tal que $m_a \leq m < m_{a+1}$.

Considere, o morfismo de $\mathbb{F}_q$-álgebras

$$\begin{array}{rccc}\varphi : & \langle f_0, f_1, ...\rangle \oplus \langle g_1, g_2, ...\rangle & \rightarrow & \mathbb{F}_q^n \\ & f & \mapsto & (f(P_1), f(P_2), ..., f(P_n)).\end{array}$$

Para $l \in \mathbb{N}$, sejam

$$L_l := \langle f_0, ...f_l \rangle \oplus \langle g_1, ..., g_a \rangle ,$$
$$E_l := \varphi(L_l),$$
$$C_l := E_l^{\perp}.$$

Logo, existe $N \in \mathbb{N}$ tal que $E_N = E_l$ e $C_N = C_l$ para todo $N \leq l$. Assim,

$$E_0 \subseteq E_1 \subseteq ... \subseteq E_N \subseteq \mathbb{F}_q^n$$

$$C_0 \supseteq C_1 \supseteq ... \supseteq C_N \supseteq \{0\}.$$

Para $l, s \in \mathbb{N}$, sejam

$$\begin{aligned} c(s) &:= max\{\sigma(f_0), ..., \sigma(f_s)\} \\ N(l,m) &:= \{(i,j) \in \mathbb{N}_0^2 : i + j = l + 1 \ e \ \sigma(f_i) + c(j) < m + 1\}, \\ \nu(l,m) &:= \#N(l,m). \end{aligned}$$

Mais adiante exploraremos as propriedades das funções numéricas $c(s)$ e $\nu(l,m)$. Admita que

$$N(l,m) = \{(i_1, j_1), ..., (i_t, j_t)\}$$

com $i_1 < ... < i_t$ e $j_1 > ... > j_t$.
Por outro lado, para $y \in \mathbb{F}_q^n$ recordemos que

$$\omega(y) \geq posto\ (S(y)),$$

onde $S(y) = (s_{ij}(y) = y.(h_i * h_j) : 1 \leq i, j \leq N)$ e $h_i = \varphi(f_i)$ (ver referência [14] Lema 4.7)
Fixemos $l \in \mathbb{N}$ tal que

$$l + 1 < N.$$

Agora estamos prontos para provar um resultado de fundamental importância na determinação de uma cota para a distância mínima do código C_l.

Proposição 2.28. *Se $y \in C_l \backslash C_{l+1}$ então*

$$\omega(y) \geq \nu(l,m).$$

Demonstração. Seja $(i_u, j_u) \in N(l, m)$.

Primeiramente, vamos mostrar que $s_{i_u j_v}(y) = 0$ se $t \geq v > u \geq 1$. De fato, como $(i_u, j_u) \in N(l, m)$ então

$$i_u + j_u = l + 1 \text{ e } \sigma(f_{i_u}) + \sigma(f_{j_v}) \geq m$$

se $v > u$. Em outras palavras,

$$i_u + j_v \geq l \text{ e } \sigma(f_{i_u} f_{j_v}) \geq \sigma(f_{i_u}) + \sigma(f_{j_n}) \geq m$$

se $v > u$. Logo, $f_{i_u} f_{j_v} \in L_l$ se $v > u$. Isto nos mostra que $\varphi(f_{i_u} f_{j_v}) \in E_l$ se $v > u$ e portanto,

$$s_{i_u j_v}(y) = y.\varphi(f_{i_u} f_{j_v}) = 0,$$

pois $y \in C_l$.
Agora, vamos mostrar que $s_{i_u j_u}(y) \neq 0$. Neste caso, recordaremos que

$$i_u + j_u = l + 1 \text{ e } \sigma(f_{i_u} f_{j_u}) \leq \sigma(f_{i_u}) + \sigma(f_{j_u}) \leq m.$$

Isto nos mostra que $f_{i_u} f_{j_u} \in L_{l+1} \backslash L_l$. Assim, existem $\lambda_{l+1} \in \mathbb{F}_q^*$ e $f \in L_l$ tais que

$$f_{i_u} j_{j_u} = \lambda_{l+1} f_{l+1} + f.$$

Logo,

$$\begin{aligned} s_{i_u j_u}(y) &= y.\varphi(f_{i_u} f_{j_u}) \\ &= \lambda_{l+1} y.\varphi(f_{l+1}) + y.\varphi(f) \\ &= \lambda_{l+1} y.\varphi(f_{l+1}) \neq 0 \end{aligned}$$

pois $y \notin C_{l+1}$ e $\lambda_{l+1} \neq 0$.
Para finalizar, vamos mostrar que

$$posto(S(y)) \geq t.$$

Aplicando operações elementares sobre a matriz $S(y)$, primeiro coloque as linhas $i_1, ...i_t$ como as t primeiras linhas e em seguida coloque as colunas $j_t, ...j_1$ como as t primeiras colunas. Assim, temos que

$$S(y) = (s_{ij}(y)) \sim \begin{pmatrix} s_{i_1j_t}(y) & s_{i_1j_{t-1}}(y) & \cdots & s_{i_1j_2}(y) & s_{i_1j_1}(y) & \cdots \\ s_{i_2j_t}(y) & s_{i_2j_{t-1}}(y) & \cdots & s_{i_2j_2}(y) & & \\ \vdots & \vdots & . & & & \\ s_{i_{t-1}j_t}(y) & s_{i_{t-1}j_{t-1}}(y) & & & & \\ s_{i_tj_t}(y) & & & & & \\ \vdots & & & & & \end{pmatrix}$$

Se $y \in C_l \backslash C_{l+1}$, dos dois parágrafos anteriores segue que

$$S(y) \sim \begin{pmatrix} 0 & 0 & \cdots & 0 & \underbrace{s_{i_1j_1}(y)}_{\neq 0} & \cdots \\ 0 & 0 & \cdots & \underbrace{s_{i_2j_2}(y)}_{\neq 0} & & \\ \vdots & \vdots & . & & & \\ 0 & \underbrace{s_{i_{t-1}j_{t-1}}(y)}_{\neq 0} & & & & \\ \underbrace{s_{i_tj_t}(y)}_{\neq 0} & & & & & \\ \vdots & & & & & \end{pmatrix}$$

Portanto,

$$\omega(y) \geq posto(S(y)) \geq t = \nu(l, m).$$

□

Note que o morfismo $\varphi : R(P, Q) \to \mathbb{F}_q^n$ é sobrejetor pois $\varphi|_{R(P)}$ é sobrejetor. Assim, $E_N = \mathbb{F}_q^n$ e $C_N = \{0\}$. Logo, podemos fazer a seguinte definição.

Definição 2.29. *Sejam $l, m \in \mathbb{N}$ tal que $l+1 < N$. O número $d(l, m)$ é chamado de* **cota ordem fraca** *onde*

$$d(l, m) := Min\{\nu(r, m) : r \geq l\}.$$

Vamos examinar o conjunto $N(l, m)$. Primeiro, vamos fixar o conjunto das lacunas de P por

$$G(P) = \{l_1 < ... < l_g\}.$$

Recorde que já definimos o conjunto das lacunas de Q por

$$G(Q) = \{l_1^{'} < ... < l_g^{'}\}.$$

Observe que

$$\nu(l, m) \leq l + 2.$$

De agora em diante, considere

$$l_g^{'} \leq m.$$

Assim, $(i, j) \in N(l, m)$ sempre que $i + j = l + 1$ e $i \in H(P)$. De fato, neste caso

$$\sigma(f_i) + c(j) = 0 + c(j) \leq l_g^{'} \leq m.$$

Portanto, para determinar $N(l, m)$ basta verificar se o par $(l_i, l + 1 - l_i) \in N(l, m)$ para todo $l_i \leq l$. Disto, concluímos que

$$\nu(l, m) = l + 2 - \#\{l_i \leq l : (l_i, l + 1 - l_i) \notin N(l, m)\}. \tag{2.8}$$

Para podermos formalizar o que dissemos acima, lembre que Kim [13] mostrou a existência de uma permutação τ de $\{1, ..., g\}$ tal que $(l_i, l_{\tau(g)}^{'}) \in H(P, Q)$ onde $l_{\tau(i)}^{'} = min\{s : (l_i, s) \in H(P, Q)\}$. Então

$$\Gamma(P, Q) := \{(l_1, l_{\tau(1)}^{'}), ..., (l_g, l_{\tau(g)}^{'})\}.$$

O estudo de $N(l, m)$ passa, primeiro, pelo estudo de $c(s)$. Lembre que

$$c(s) = max\{\sigma(f_0), ..., \sigma(f_s)\}.$$

Esta função tem as seguintes propriedades:

(1) $c(s) = max\{l_{\tau(i)}^{'} : l_i \leq s\}$;

(2) $c(s) = l_g^{'}$ se $s \geq l_g$;

(3) $c(1) = l_{\tau(1)}^{'}$;

(4) $c(s)$ é não decrescente: $c(s) \leq c(s^{'})$ se $s \leq s^{'}$.

Agora, para $l \in \mathbb{N}$ e $m \in \mathbb{N}_0$ definimos:

$$B(l,m) := \{l_i \in G(P) : l_i \leq l \text{ e } l'_{\tau(i)} + c(l+1-l_i) \geq m+1\};$$

$$b(l,m) := \#B(l,m).$$

A função $b(l,m)$ tem as seguintes propriedades:

(i) $0 \leq b(l,m) \leq g$;

(ii) $b(l,0) = g$ se $l \geq l_g$;

(iii) $b(1,m) = \begin{cases} 0 & se \quad 2l'_{\tau(1)} < m+1; \\ 1 & se \quad 2l'_{\tau(1)} \geq m+1; \end{cases}$

(iv) $b(l,m+1) \leq b(l,m) \leq b(l+1,m)$.

É imediato da definição de $b(l,m)$ e da equação 2.8 que

$$\nu(l,m) = l + 2 - b(l,m).$$

Portanto,

$$\begin{aligned} d(l,m) &= min\{\nu(j,m) : j \geq l\} \\ &= min\{j + 2 - b(j,m); j \geq l\}. \end{aligned}$$

Como $b(j,m) \leq g$ para todo $j \geq 1$, temos que

$$j + 2 - b(j,m) \geq j + 2 - g \geq l + 2 - b(l,m)$$

sempre que $j \geq l + g - b(l,m)$. Isto nos mostra que

$$d(l,m) = min\{j + 2 - b(j,m) : l \leq j \leq l + g - b(l,m)\}.$$

Com o objetivo de ver o código C_l como um código de Goppa, note que a prova da Proposição 2.25 nos mostra que

$$L_l = \mathcal{L}(lP + mQ),$$

e portanto,

$$C_l = C_\Omega(D, lP + mQ). \tag{2.9}$$

Desta forma, assim como fizeram Høholdt, Van Lint e Pellikaan, podemos comparar $d(l,m)$ com $d_G(l,m) = l + m - (2g-2)$.
Agora, vamos enunciar o teorema principal deste capítulo.

Teorema 2.30. *O número $d(l,m)$ é uma cota inferior para a distância mínima de C_l, isto é,*

$$d(C_l) \geq d(l,m).$$

Demonstração. O teorema é consequência direta da definição 2.29 e da proposição 2.28. □

Teorema 2.31. *Seja $G = lP + mQ$ tal que $l_g^{'} \geq m$ e $l + m < n$. Então $C := C_\Omega(D,G) \neq \{0\}$ e*

$$d(C) \geq d(l,m).$$

Além disso, se $d(l,m) = j + 2 - b(j,m)$, para algum j onde $l \leq j \leq l + g - b(l,m)$ e $m \leq 2g + (j-l) - b(j,m)$ então

$$d(C) \geq d(l,m) \geq d_G(l,m).$$

Demonstração. A condição $l + m < n$ nos mostra que o morfismo $\varphi|_{L_l}$ não é sobrejetor. Assim, $E_l \subsetneqq \mathbb{F}_q^n$ e portanto, $C_l \neq \{0\}$. A condição $l_g^{'} \leq m$ implica que $C = C_l$ (ver equação 2.9) e $d(C) \geq d(l,m)$ pelo teorema 2.30.
Agora, das condições $d(l,m) := j + 2 - b(j,m)$ e $m \leq 2g + (j-l) - b(j,m)$ é imediato que $d(l,m) \geq d_G(l,m)$. □

Corolário 2.32. *Considere o código C do Teorema 2.31. Se $k = dim\ C$, então*

$$k = n - \ell(G).$$

Demonstração. Como C é o dual de $C_{\mathcal{L}}(D,G)$, então

$$k = n - dim\ C_{\mathcal{L}}(D,G).$$

Por outro lado, Goppa mostrou que

$$dim\ C_{\mathcal{L}}(D,G) = \ell(G) - \ell(G-D) = \ell(G)$$

pois $deg\ G = l + m < n = deg\ D$. Logo,

$$k = n - \ell(G).$$

□

Corolário 2.33. *Considere o código C do Teorema 2.31. Se d denota a distância mínima de C, então*

$$d(l,m) \leq d \leq n - k + 1 = l + 2 + (m - g).$$

Em particular, quando $d(l,m) = l + 2$ temos

$$l + 2 \leq d \leq l + 2 + (m - g).$$

Se além disso, $m = g$ então o código C é MDS.

Demonstração. A desigualdade $d(l,m) \leq d$ segue do teorema 2.31. Agora, a desigualdade $d \leq n - k + 1$ é conhecida (Cota de Singleton). Já a igualdade $n - k + 1 = l + 2 + (m - g)$ segue do Corolário 2.32 e da Proposição 2.25. □

Observação 2.34. *O Corolário 2.33 nos fornece um caminho a ser seguido na busca por códigos MDS.*

2.4 Semigrupo

Definição 2.35. *Um subconjunto Λ de $\mathbb{N}_0^2$ é chamado* **semigrupo numérico** *se $(0,0) \in \Lambda$ e se Λ é fechado para a adição.*

Os elementos de $\mathbb{N}_0 \backslash \Lambda$ são chamados de **lacunas** e os elementos de Λ de **não lacunas**. O número de lacunas é denotado por $g = g(\Lambda)$ e é chamado de *gênero* de Λ.
Observe que se $g < \infty$, então existe $n \in \Lambda$ tal que $x \in \Lambda$ se $x \in \mathbb{N}_0$ e $x \geq n$. Nesse caso, o menor $n \in \Lambda$ tal que $\{x \in \mathbb{N}_0; x \geq n\}$ está contido em Λ é chamado de *condutor de* Λ e é

denotado por $c = c(\Lambda)$. Assim, se $g > 0$, observe que $c - 1$ é a maior lacuna de Λ. Observe também que se Λ é um semigrupo com g lacunas e condutor c então, $g = 0$ se, e somente se, $c = 0$ e quando $g > 0$ temos que $c \geq g + 1$ e $\Lambda = \{x \in \mathbb{N}_0 : x \geq g + 1\} \cup \{0\}$ se, e somente se, $c = g + 1$.

Definição 2.36. *Dizemos que um semigrupo numérico Λ é finitamente gerado se existe um subconjunto $A = \{a_1, ..., a_t\}$ de Λ tal que para todo $x \in \Lambda$, existem $\lambda_1, ..., \lambda_t \in \mathbb{N}_0$ tais que $x = \sum_{i=1}^{t} \lambda_i a_i$. Assim, dizemos que Λ é gerado por A e denotaremos $\Lambda = \langle A \rangle$.*

2.4.1 Semigrupo de Weierstrass

Seja $\mathcal{X}$ uma curva sobre $\mathbb{F}$ de gênero finito g, $\mathbb{F}$ finito, e sejam $Q_1, ..., Q_m$ pontos $\mathbb{F}$-racionais de $\mathcal{X}$, distintos dois a dois. O conjunto

$$\begin{aligned} H &= H(Q_1, ..., Q_m) \\ &:= \{\mathbf{a} = (a_1, ..., a_m) \in \mathbb{N}_0^m : \exists f \in \mathbb{F}(\mathcal{X}) \text{ com } (f)_\infty = \textstyle\sum_{i=1}^{m} a_i Q_i\}, \end{aligned}$$

é um subsemigrupo de $(\mathbb{N}_0^m, +)$ e é chamado de **semigrupo de Weierstrass** de $\mathcal{X}$ em $Q_1, ..., Q_m$. Os elementos do complemento $G = G(Q_1, ..., Q_m)$ de H em $\mathbb{N}_0^m$ são chamados de **lacunas de Weierstrass** de $\mathcal{X}$ em $Q_1, ..., Q_m$. Tais conjuntos tem as seguintes caracterizações(ver referência [4]):

- $\mathbf{a} \in H \Leftrightarrow \ell(\mathbf{a}) = \ell(\mathbf{a} - \mathbf{e_i}) + 1$ para todo $i = 1, ...m$;
- $\mathbf{a} \in G \Leftrightarrow$ existe $i \in \{1, ..., m\}$ tal que $\ell(\mathbf{a}) = \ell(\mathbf{a} - \mathbf{e_i})$;

onde $\#\mathbb{F} \geq m$, $\mathbf{e_i}$ denota o vetor em $\mathbb{N}_0^m$ com 1 na i-ésima posição e 0 nas demais, $\ell(\mathbf{a}) = dim_{\mathbb{F}}\mathcal{L}(\mathbf{a}) = \mathcal{L}(a_1Q_1 + ... + a_mQ_m) = \{f \in \mathbb{F}(\mathcal{X})^* : (a_1Q_1 + ... + a_mQ_m) + (f) \succeq 0\} \cup \{0\}$.

A partir de agora estamos interessados em estudar o semigrupo de Weierstrass sobre dois pontos $\mathbb{F}$-racionais.

Sejam ρ e σ são funções peso fraco sobre uma $\mathbb{F}$-álgebra R.

Observação 2.37. *A condição (6) da definição 2.2 implica que o subconjunto* $\Lambda = \{(\rho(f), \sigma(f)) : f \in R^*\}$ *é um semigrupo numérico chamado de semigrupo de* ρ *e* σ*.*
Em particular, se tomarmos $\rho = -\upsilon_{Q_1}$ *e* $\sigma = -\upsilon_{Q_2}$*, como visto na descrição 2.2 e 2.3, então* Λ *é chamado de semigrupo de Weierstrass de* Q_1, Q_2*.*

Definição 2.38. *Dizemos que* ρ *e* σ *são bem comportadas se* $\#(\mathbb{N}_0^2 \backslash H)$ *é finito, neste caso dizemos que o conjunto possui genêro finito, e* $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$*.*

Desta forma podemos realizar uma identificação dos conjuntos H e Λ da seguinte forma. Seja ρ e σ são duas funções peso fraco normais bem comportadas definidas sobre uma $\mathbb{F}$-álgebra R. Então

$$\begin{aligned} H &= H(P, Q) \\ &:= \{(\rho(f), \sigma(f)) \in \mathbb{N}_0^2 \ f \in R, \\ &= H(\rho, \sigma) \end{aligned}$$

Generalizando a definição do conjunto $H = H(S)$, para algum $S \subseteq R$ como sendo

$$H(S) := \{(\rho(f), \sigma(f)) : f \in S^*\} \subseteq \mathbb{N}_0^2$$

onde $S^* := S \backslash \{0\}$.

Exemplo 2.39. *Seja* K *o corpo de funções algébricas de uma variavél sobre* $\mathbb{F}$*, tal que* $\mathbb{F}$ *é o corpo cheio de constantes de* K*. Para um lugar* $S \in K$*, seja* $\mathcal{O}_S$ *o seu anel local em* S *e* υ_S *que corresponde a valorização. Seja* P, Q *dois lugares distintos de* K*. Considere uma* $\mathbb{F}-$*álgebra* $R \subseteq K$ *e defina*

$$\varsigma'(f) := \begin{cases} -\infty & se\ f = 0, \\ 0 & se\ \upsilon_P(f) \geq 0, \\ -\upsilon_P(f) & se\ \upsilon_P(f) < 0 \end{cases}$$

e

$$\xi'(f) := \begin{cases} -\infty & se\ f = 0, \\ 0 & se\ \upsilon_Q(f) \geq 0, \\ -\upsilon_Q(f) & se\ \upsilon_Q(f) < 0. \end{cases}$$

Seja ς *e* ξ *são as normalizações de* ς' *e* ξ' *respectivamente. Se* $R = R(P, Q) := \cap_{S \neq P,Q} \mathcal{O}_S$*, então* ς *e* ξ *são funções ordem fraca bem comportadas sobre* R*.*

Dado $\mathbf{a} = (a_1, a_2)$ e $\mathbf{b} = (b_1, b_2) \in \mathbb{N}_0^2$, a *menor das cotas superiores* de $\mathbf{a}$ e $\mathbf{b}$ é definido com

$$lub(\mathbf{a}, \mathbf{b}) := (max\{a_1, b_1\}, max\{a_2, b_2\})$$

Lema 2.40. *Seja $f \in R^*$ e $g \in \mathcal{U}_\rho \backslash \mathbb{F}$. Então existe $\lambda \in \mathbb{F}$ tal que $\rho(f(g - \lambda)) < \rho(f)$.*

Demonstração. Da propriedade que caracteriza peso fraco, temos que $\rho(fg) \leq \rho(f) + \rho(g)$, mas $g \in \mathcal{U}_\rho \backslash \mathbb{F}$ o que implica $\rho(g) = 0$, daí $\rho(fg) \leq \rho(f)$. Se $\rho(fg) = \rho(f)$, pela propriedade (IV), temos que existe $\lambda \in \mathbb{F}$ tal que $\rho(f(g - \lambda)) = \rho(fg - f\lambda) < \rho(f)$. □

Lema 2.41. *Seja $f, g \in R^*$. Seja $a := (\rho(f), \sigma(f))$ e $b := (\rho(g), \sigma(g))$. Então existem $\lambda, \mu \in \{0, 1\}$ tal que*

$$lub(a, b) = (\rho(\lambda f + \mu g), \sigma(\lambda f + \mu g)).$$

Em particular, se $f, g \in S \subseteq R$ e S é fechado sobre adição, então $lub(a, b) \in H(S)$.

Demonstração. Vamos dividir a prova em duas partes.
(i) Se $a = b$ implica que $\rho(f) = \rho(g)$ e $\sigma(f) = \sigma(g)$

$$\begin{aligned} lub(a, b) &= (max\{\rho(f), \rho(g)\}, max\{\sigma(f), \sigma(g)\}) \\ &= (\rho(f), \sigma(f)) \\ &= (\rho(1.f + 0.g), \sigma(1.f + 0.g)) = a \end{aligned}$$

e análogo para $\sigma(g)$. Por outro lado, podemos assumir que $\rho(f) < \rho(g)$. Se $\sigma(f) \leq \sigma(g)$, então

$$lub(a, b) = (max\{\rho(f), \rho(g)\}, max\{\sigma(f), \sigma(g)\}),$$

como $\rho(f) \neq \rho(g)$ e $\sigma(f) \neq \sigma(g)$ temos pela propriedade (III) que

$$max\{\rho(f), \rho(g)\} = \rho(f + g) \text{ e } max\{\sigma(f), \sigma(g)\} = \sigma(f + g),$$

logo $lub(a, b) = (\rho(f + g), \sigma(f + g))$

(ii) Seja $f, g \in S \subseteq R$, por hipótese temos $f + g \in S$, então pela parte (i) e a definição de $H(S)$, temos que $lub(a, b) = (\rho(f + g), \sigma(f + g)) \in H(S)$ □

Proposição 2.42. *Se $S \subseteq R$ é fechado sobre adição e multiplicação então H(S) é fechado sobre adição.*

Demonstração. Seja $a = (\rho(f), \sigma(f))$ e $b = (\rho(g), \sigma(g))$ com $f, g \in S^*$. Se $a = 0$, então $a + b = b \in H(S)$. Os inteiros $\rho(f)$, $\sigma(f)$, $\rho(g)$ e $\sigma(g)$ são todos positivos, isto é, $f, g \in \mathcal{M}_\rho \cap \mathcal{M}_\sigma$, então pela propriedade (VI), temos $\rho(fg) = \rho(f) + \rho(g)$ e $\sigma(fg) = \sigma(f) + \sigma(g)$, assim

$$a + b = (\rho(f) + \rho(g), \sigma(f) + \sigma(g)) = (\rho(fg), \sigma(fg)) \in H(S),$$

pois S é fechado sobre a multiplicação.
Assuimindo que $\rho(f) > 0$ e $\sigma(f) = 0$, temos três possibilidade.

(a) Se $\rho(g) = 0$ e $\sigma(g) > 0$, então

$$\begin{aligned} a + b &= (\rho(f) + \rho(g), \sigma(f) + \sigma(g)) \\ &= (max\{\rho(f), \rho(g)\}, max\{\sigma(f), \sigma(g)\}) \qquad aplicando(III) \\ &= (\rho(f + g), \sigma(f + g)) \\ &= lub(a, b) \end{aligned}$$

Assim pelo lema 2.41, teremos que $lub(a, b) \in H(S)$.

(b) Se $\rho(g) > 0$ e $\sigma(g) = 0$, então

$a + b = (\rho(f) + \rho(g), \sigma(f) + \sigma(g))$, como $\rho(g) > 0$ e $\rho(f) > 0$ implica que $f, g \in \mathcal{M}_\rho$, e por (VI) segue que $\rho(f) + \rho(g) = \rho(fg)$, onde $fg \in S$.
Por outro lado, $\sigma(fg) \leq \sigma(f) + \sigma(g)$ o que implica $\sigma(fg) \leq 0$ e assim $\sigma(fg) = 0$, logo $\sigma(fg) = \sigma(f) + \sigma(g)$ e portanto $a + b = (\rho(f) + \rho(g), \sigma(f) + \sigma(g)) = (\rho(fg), \sigma(fg)) \in H(S)$.

(c) Se $\rho(g) > 0$ e $\sigma(g) > 0$ então
$a + b = (\rho(f) + \rho(g), \sigma(f) + \sigma(g))$, como $\rho(g) > 0$ e $\rho(f) > 0$ implica que $f, g \in \mathcal{M}_\rho$, por (VI) segue que $\rho(f) + \rho(g) = \rho(fg)$, onde $fg \in S$ e $\sigma(fg) \leq \sigma(f) + \sigma(g) = \sigma(g)$ mais ainda $\sigma(fg) = \sigma(g)$. Com efeito, vamos supor que $\sigma(fg) = 0$, sabemos que $f \in \mathcal{U}_\sigma$ e $g \in \mathcal{M}_\sigma$, ou seja, $\sigma(f) = 0$ e $\sigma(g) > 0$, como σ é função peso fraco, temos por (VI) que $0 = \sigma(fg) \leq \sigma(f) + \sigma(g) = \sigma(g)$, isto é, $0 \leq \sigma(g)$ contradição. Assim $a + b = (\rho(f) + \rho(g), \sigma(f) + \sigma(g)) = (\rho(fg), \sigma(fg)) \in H(S)$.

□

Corolário 2.43. *Seja R' é uma $\mathbb{F}$-subálgebra de R. Então $H(R')$ é um semigrupo.*

Demonstração. Consequência direta da proposição 2.42. □

No que segue iremos associar os conjuntos com o semigrupo $H = H(R)$:

$$H_x := \{(m, 0) \in H\}, \quad H_y := \{(0, n) \in H\},$$

e suas projeções

$$\overline{H}_x := \{m : (m, 0) \in H\}, \quad \overline{H}_y := \{n : (0, n) \in H\}.$$

Para $n \in \mathbb{N}_0$, o conjunto

$$x_H(n) := min\{m \in N_0 : (m, n) \in H\} \quad \text{e} \quad y_H(n) := min\{m \in N_0 : (n, m) \in H\}.$$

Lema 2.44. *Se $y_H(n) > 0$, então $x_H(y_H(n)) = n > 0$. Se $x_H(n) > 0$, então $y_H(x_H(n)) = n > 0$.*

Demonstração. Seja $f \in R^*$ tal que $\rho(f) = n$ e $\sigma(f) = y_H(n)$. Pela definição $x_H(y_H(n)) = min\{m \in N_0 : (m, y_H(n)) \in H\} \leq n = \rho(f)$.
Vamos supor por absurdo que $x_H(y_H(n)) < n$. Assim se $\rho(g) < n$ e $\sigma(g) = y_H(n)$, para algum $g \in R$, pela propriedade (V), temos que existe $\lambda \in \mathbb{F}$ tal que $\sigma(f - \lambda g) < \sigma(g) = y_H(n)$, assim $\rho(f - \lambda g) = \rho(f) = n$, absurdo, pela minimalidade de $x_H(y_H(n))$, logo $n = x_H(y_H(n))$. □

Lema 2.45. *Se (x, y) e $(x', y) \in H(P, Q)$ com $x > x'$ e $y \geq 1$, então existe um elemento $(x, \delta) \in H(P, Q)$ com $\delta < y$.*

Demonstração. Seja f e g são funções meromorficas satisfazendo $(f)_\infty = xP + yQ$ e $(g)_\infty = x'P + yQ$. Então podemos escolher sutilmente número complexos a e b tal que $(af + bg)_\infty = xP + \delta Q$, com $\delta < y$. Assim $(x, \delta) \in H(P, Q)$ com $\delta < y$. □

Lema 2.46. *Sejam $x \in G(P)$ e $y_H(x) = min\{y; (x,y) \in H(P,Q)\}$, então $(\gamma, y_H(x)) \notin H(P,Q)$ para todo $\gamma < x$, sendo este $x = min\{\gamma; (\gamma, y_H(x)) \in H(P,Q)\}$.*

Demonstração. Note que $y_H(x) \geq 1$ desde que $x \notin H(P)$. Suponha que $(x', y_H(x)) \in H(P,Q)$ para algum $x' < x$. Então, pelo lema 2.45, existe um inteiro $\delta < y_H(x)$ tal que $(x, \delta) \in H(P,Q)$, o qual contradiz a minimalidade de $y_H(x)$. □

Corolário 2.47. *Seja $n \in G(\overline{H}_x)$ se e somente se $y_H \in G(\overline{H}_y)$. Em particular, o semigrupo $\overline{H}_x$ e $\overline{H}_y$ possuem o mesmo gênero.*

Demonstração. Pelo lema 2.46 implica que $y_H(x) \notin H(Q)$ e que $y_H(x) \neq y_H(\gamma)$, para $x \neq \gamma$. Assim o conjunto $\{y_H(x); x \in G(P)\}$ está contido em $G(Q)$ que possui cardinalidade g entretanto é a mesma de $G(Q)$. □

Consideremos agora os seguintes subconjuntos de H :

$$\widetilde{\Gamma} = \widetilde{\Gamma}(H) := \{(m, y_H(m)) : m \in G(\overline{H}_x)\} = \{(x_H(n), n) : n \in G(\overline{H}_y)\},$$

$$\Gamma = \Gamma(H) := \{(m, y_H(m)), (x_H(m), m) : m \in N_0\} = \widetilde{\Gamma} \cup H_x \cup H_y$$

Note que $\widetilde{\Gamma}$ está bem definido, isto decorre do lema 2.44. O próximo resultado nos fornece uma boa descrição do semigrupo H.

Proposição 2.48. $H = \{lub(a,b); a, b \in \Gamma\}$

Demonstração. Dividiremos a prova em duas partes.

(i) Sejam $a, b \in H(R)$, $f, g \in R^*$ tais que $a = (\rho(f), \sigma(f))$ e $b = (\rho(g), \sigma(g))$, pelo lema 2.41 existem $\lambda, \mu \in \{0,1\}$ tal que $lub(a,b) = (\rho(\lambda f + \mu g), \sigma(\lambda f + \mu g))$, temos $lub(a,b) \in H(R)$.

(ii) Para $a \in H$, $a = (a_1, a_2)$, podemos escrever a como sendo $a = lub((a_1, y_H(a_1)), (x_H(a_2), a_2))$. De fato, temos que $a_1 \in \overline{H}_x$ ou $a_1 \notin \overline{H}_x$ e $a_2 \in \overline{H}_y$ ou $a_2 \notin \overline{H}_y$. Disto, temos quatro possibilidade.

(a) $a_1 \in \overline{H}_x$ e $a_2 \in \overline{H}_y$, então $max\{a_1, x_H(a_2)\} = a_1$ e $max\{y_H(a_1), a_2\} = a_2$, segue da minimalidade de $x_H(a_2)$ e $y_H(a_1)$.

(b) $a_1 \notin \overline{H}_x$ e $a_2 \in \overline{H}_y$, então $max\{a_1, x_H(a_2)\} = a_1$, pois $a \in H$ implica que $x_H(a_2) \leq a_1$ e $max\{y_H(a_1, a_2)\} = a_2$, pois $a \in H$ o que implica $y_H(a_1) \leq a_2$.

(c) $a_1 \notin \overline{H}_x$ e $a_2 \notin \overline{H}_y$, análogo ao caso (a).

(d) $a_1 \in \overline{H}_x$ e $a_2 \notin \overline{H_y}$, análogo ao caso (b).

Logo, $lub((a_1, y_H(a_2)), (x_H(a_1), a_2)) = (a_1, a_2) = a$ □

Para todo $a \in H$ tome um elemento $\phi_a \in R^*$ tal que $(\rho(\phi_a), \sigma(\phi_a)) = a$, e o conjunto

$$\mathcal{B} := \{\phi_a : a \in \Gamma\}.$$

Proposição 2.49. *O conjunto $\mathcal{B}$ é uma base de R como um $\mathbb{F}$-espaço vetorial.*

Demonstração. Primeiramente vamos provar que o conjunto $\mathcal{B}$ é linearmente independente.
Seja $a \neq b \in \Gamma$ e $\phi_a, \phi_b \in R^*$ tal que $a = (\rho(\phi_a), \sigma(\phi_a))$ e $b = (\rho(\phi_b), \sigma(\phi_b))$. Então a e b não pertencem a mesma linha ou coluna, ou seja, $\rho(\phi_a) \neq \rho(\phi_b)$ ou $\sigma(\phi_a) \neq \sigma(\phi_b)$. Vamos supor que exista $\alpha, \beta \in \mathbb{F}^*$ tal que $\alpha\phi_a = \beta\phi_b$. Assim,

$$\rho(\alpha\phi_a) = \rho(\beta\phi_b)$$

e pela propriedade (II)

$$\rho(\phi_a) = \rho(\phi_b).$$

Análogamente, concluimos que $\sigma(\phi_a) = \sigma(\phi_b)$ desta forma teremos um contradição.
Iremos agora provar que um subconjunto finito $\mathcal{B}' = \{\phi_{a_1}, ..., \phi_{a_n}\}$ de $\mathcal{B}$ é linearmente independente. Com efeito, considere $a_i \neq a_j$, se $i \neq j$, como $a_i \in \Gamma$, $\forall\ 1 \leq i \leq n$, isto implica que existe $\phi_{a_i} \in R^*$ tal que $a_i = (\rho(\phi_{a_i}), \sigma(\phi_{a_i}))$, para todo $1 \leq i \leq n$. Tome $\rho(\phi_{a_i}) \neq \rho(\phi_{a_j})$ e $\sigma(\phi_{a_i}) \neq \sigma(\phi_{a_j})$, se $i \neq j$. Existem $\lambda_i \in \mathbb{F}$, com $1 \leq i \leq n$, tais que

$$\lambda_1\phi_{a_1} + ... + \lambda_n\phi_{a_n} = 0.$$

Suponha, sem perda de generalidade, que $\lambda_n \neq 0$. Assim,

$$\lambda_1\phi_{a_1} + ... + \lambda_{n-1}\phi_{a_{n-1}} = \lambda_n\phi_{a_n},$$

Isto quer dizer que existe $k \in \{1, ..., n-1\}$ tal que $\lambda_k \neq 0$ e aplicando ρ teremos

$$\rho(\lambda_1\phi_{a_1} + ... + \lambda_{n-1}\phi_{a_{n-1}}) = \rho(\lambda_n\phi_{a_n}) \Rightarrow \rho(\lambda_k\phi_k) = \rho(\lambda_n\phi_n)$$

pela propriedade (II) de ordem fraca, temos

$$\rho(\phi_k) = \rho(\phi_n),$$

contradição.

Passaremos a provar que o conjunto $\mathcal{B}$ gera R, tome $f \in R^*$. Vamos primeiramente assumir que $\sigma(f) = 0$ e utilizar indução sobre $\rho(f)$. Se $\rho(f) = 0$, então segue o resultado, pois $a = (\rho(f), \sigma(f)) = (0, 0)$ o que implica $a \in \mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$.

Se $\rho(f) = k > 0$, tome $\phi_a \in \Gamma$ com $a = (\rho(\phi_a), \sigma(\phi_a)) = (k, 0)$, como $\rho(f) = \rho(\phi_a)$ existe $\lambda \in \mathbb{F}$ tal que ou

$$\lambda\phi_a - f = 0 \text{ e daí } \lambda\phi_a = f$$

ou pela propriedade (V) de ordem fraca temos

$$\rho(f - \lambda\phi_a) < \rho(f) = k \text{ e } \sigma(f - \lambda\phi_a) = 0,$$

pois $\sigma(f) = 0 = \sigma(\phi_a) = \sigma(\lambda\phi_a)$. Assim, $\sigma(f + (-\lambda\phi_a)) \leq max\{\sigma(f), \sigma(\lambda\phi_a)\}$ e daí temos $\sigma(f - \lambda\phi_a) = 0$. Pela hipótese de indução, todos os elementos g com $\sigma(g) = 0$ e $\rho(g) < k$ são geradores de $\mathcal{B}$, logo f pertence ao conjunto de geradores de $\mathcal{B}$.

O caso geral, segue quando $\sigma(f) > 0$, então aplicando indução sobre $\sigma(f)$. Vamos assumir que $\rho(f) = k > 0$. Se $\sigma(f) = 0$ então $a = (\rho(f), \sigma(f)) = (k, 0)$ e retornamos ao caso anterior. Se $\sigma(f) = c > 0$, tome $\phi_b \in R$ com $b = (\rho(\phi_b), \sigma(\phi_b)) = (k, c) \in H$. Pela proposição 2.48, existem $\phi_k, \phi_c \in R^*$ tais que $(\rho(\phi_k), \sigma(\phi_c)) = (k, y_H(k))$ e $(\rho(\phi_k), \sigma(\phi_c)) = (x_H(c), c)$. Pelo lema 2.41, existem $\lambda, \mu \in \{0, 1\}$ tal que

$$\begin{aligned}(k, c) &= lub((k, y_H(k)), (x_H(c), c) \\ &= (\rho(\lambda\phi_k + \mu\phi_c), \sigma(\lambda\phi_k + \mu\phi_c))\end{aligned}$$

Como $\sigma(f) = c = \sigma(\lambda\phi_k + \mu\phi_c)$, pela propriedade (V), existe $\lambda_1 \in \mathbb{F}$ tal que $\sigma(f - \lambda_1(\lambda\phi_k + \mu\phi_c)) < \sigma(f) = c$. Pela hipótese de indução, todos os elementos g com $\rho(g) = k$ e $\sigma(g) < c$ são geradores de $\mathcal{B}$ e assim segue que f pertence ao conjunto de geradores de $\mathcal{B}$. □

Para $(m, n) \in \mathbb{N}_0^2$ escrevemos $\Delta(m, n) := \{(m, \ell) : \ell < n\} \cup \{(\ell, n) : \ell < m\}$ e seja $G(H)$ o conjuntos das lacunas de H.

Corolário 2.50. *Temos*

$$G(H) = \bigcup_{a \in \widetilde{\Gamma}} \Delta(a)$$

Demonstração. Se $(m, n) \in \Delta(a)$, para algum $a \in \widetilde{\Gamma}$ onde $a = (m, y_H(m))$ ou $a = (x_H(n), n)$ e $n \in G(\overline{H}_y)$, $m \in G(\overline{H}_x)$, admita sem perda de generalidade que $a = (m, y_H(m))$. Como $(m, n) \in \Delta(a) := \{(m, l); l < y_H(m)\} \cup \{(l, y_H(m)); l < m\}$, então temos que $n < y_H(m)$. De modo análogo, concluimos que $m < x_H(n)$. Pelo corolário 2.47 e da definição de y_H e x_H temos que $(m, n) \notin H$ o que implica que $(m, n) \in G(H)$.
Se $(m, n) \notin \Delta(a)$ para todo $a \in \widetilde{\Gamma}$, então $n \geq y_H(m)$ e $m \geq x_H(n)$. Pela definição de x_H e y_H, temos que $(m, y_H(n)), (x_H(n), n) \in H$ e das desigualdades acima segue que $(m, n) = lub((m, y_H(m)), (x_H(n), n)) \in H$. □

Capítulo 3

Álgebras munidas de Funções Peso Fraco e Códigos de Goppa Bi-Pontuais

Neste capítulo, mostraremos que uma álgebra munida de duas funções peso fraco bem comportadas, é o anel de coordenadas de uma curva algébrica afim. Disto, poderemos concluir que os códigos de avaliação constuídos sobre estas álgebras são códigos geométricos de Goppa Bi-Pontuais. Em alguns resultados deste capítulo utilizaremos de conceitos importantes da álgebra comutativa que poderão ser encontradas no apêndice A desta dissertação.

3.1 A Estrutura da Álgebra R

Manteremos a seguinte notação nesta seção, seja R é uma $\mathbb{F}-$álgebra e ρ e σ duas bem comportadas funções peso fraco de R. O semigrupo $\overline{H}_x$ e $\overline{H}_y$ são finitamente gerados desde que tenham gênero finito e escrevemos

$$\overline{H}_x = \langle m_1, ...m_r \rangle$$

e

$$\overline{H}_y = \langle n_1, .., n_s \rangle$$

e definimos

$$\Gamma^+ = \Gamma^+(H) := \widetilde{\Gamma} \cup \{(m_1, 0), ..., (m_r, 0), (0, n_1), ..., (0, n_s) \subseteq H.$$

No próximo resultado veremos que dada uma sub-álgebra $R^{'}$, o semigrupo que ela gera é igual ao da álgebra R.

Lema 3.1. *Seja* $R^{'} = \mathbb{F}[\{\phi_a : a \in \Gamma^+\}] \subseteq R$. *Então* $H(R^{'}) = H(R)$.

Demonstração. É evidente que $H(R^{'}) \subseteq H(R)$, pois $R^{'} \subseteq R$. Para termos a igualdade, devemos recordar a proposição 2.48 e o lema 2.41, que nos diz que $H = \{lub(a, b); a, b \in \Gamma\}$ e que $lub(a, b) = (\rho(\lambda f + \mu g), \sigma(\lambda f + \mu g))$. Diante disto, é suficiente mostrar que $\Gamma \subseteq H(R^{'})$, onde $\Gamma = \widetilde{\Gamma} \cup H_x \cup H_y$. É fácil ver que $\widetilde{\Gamma} \subseteq H(R^{'})$, pois segue da definição de $R^{'}$. Vamos provar que $H_x \subset H(R^{'})$. Se $(m, 0) \in H_x$ então $m \in \overline{H}_x$ e portanto existem $\alpha_1, ..., \alpha_r \in N_0$ tal que $m = \sum_{i=1}^{r} \alpha_i m_i$. Assim o elemento

$$\phi = \prod_{i=1}^{r} \phi_{(m,0)}^{\alpha_i} \in R^{'}$$

Como $m_i > 0$, segue que $\phi_{(m_i,0)} \in \mathcal{M}_\rho$. Assim, se $\rho(\phi_{(m_i,0)}) = m_i$ teremos que

$$\begin{aligned} \rho(\phi) &= \rho(\textstyle\prod_{i=1}^{r} \phi_{(m_i,0)}^{\alpha_i}) \qquad aplicando(VI) \\ &= \textstyle\sum_{i=1}^{r} \rho(\phi_{(m_i,0)}^{\alpha_i}) \\ &= \textstyle\sum_{i=1}^{r} \alpha_i \rho(\phi_{(m_i,0)}) \\ &= \textstyle\sum_{i=1}^{r} \alpha_i m_i \end{aligned}$$

e

$$\begin{aligned} \sigma(\phi) &= \sigma(\textstyle\prod_{i=1}^{r} \phi_{(m_i,0)}^{\alpha_i}) \qquad aplicando(VI) \\ &\leq \textstyle\sum_{i=1}^{r} \sigma(\phi_{(m_i,0)}^{\alpha_i}) \\ &= 0 \end{aligned}$$

Como $\phi \neq 0$, segue que $\sigma(\phi) = 0$ e então $(m, 0) \in H(R^{'})$. Analogamente, $H_y \subseteq H(R^{'})$. Como $\widetilde{\Gamma} \cup H_x \cup H_y \subseteq H(R^{'})$, Logo $H(R) = H(R^{'})$. □

No resultado que segue, veremos que não há uma subálgebra própria $R^{'}$ de R, que tenha o mesmo semigrupo de Weiestrass de R.

Lema 3.2. *Seja* R' *é uma* $\mathbb{F}$*-subálgebra de* R. *Se* $H(R) = H(R')$, *então* $R' = R$.

Demonstração. Vamos provar que $R \subseteq R'$. Tome $f \in R$. Primeiramente consideremos o caso onde $\sigma(f) = 0$. Vamos escrever $\overline{H}_x = \{0 = h_0 < h_1 < h_2 < ...\}$ e provaremos por indução em $\rho(f)$. Se $\rho(f) = 0$ então $f \in \mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$ e assim $f \in \mathbb{F} \subseteq R^{'}$. Por hipótese de indução assumimos que $f \in R^{'}$ quando $\rho(f) < h_k$, $k > 0$. Seja $f \in R$ tal que $\rho(f) = h_k$ e $\sigma(f) = 0$. Tome $f' \in R^{'}$ tal que $\rho(f') = h_k$ e $\sigma(f') = 0$. Pela propriedade (V), existe $\lambda \in \mathbb{F}$ tal que ou $f = \lambda f'$ ou $\rho(f - \lambda f') < \rho(f) = h_k$ e $\sigma(f - \lambda f') \leq max\{\sigma(f), \sigma(-\lambda f')\} = 0$. Pela hipótese de indução temos que $f - \lambda f' \in R'$ e assim $f \in R'$.
Vamos agora provar o caso geral por indução em $\sigma(f)$, assumindo o resultado como verdadeiro quando $\sigma(f) < k$. Se $\sigma(f) = k$ tome $f'' \in R'$ tal que $\sigma(f'') = k$. Pela propriedade (V), existe $\lambda \in \mathbb{F}$ tal que ou $f = \lambda f''$ ou $\sigma(f - \lambda f'') < \sigma(f) = k$. Assim pela hipótese de indução, segue que $f - \lambda f'' \in R'$ e portanto $f \in R'$. □

Abaixo apresentaremos um resultado importante para o nosso estudo, que trata da estrutura da álgebra e a partir daí conseguimos obter outros resultados relevantes na identificação com a teoria de curvas.

Teorema 3.3. *A $\mathbb{F}$-algebra R é finitamente gerada sobre $\mathbb{F}$, isto é,*

$$R = \mathbb{F}[\{\phi_a : a \in \Gamma^+\}]$$

Demonstração. A prova segue como consequência direta dos lemas 3.1 e 3.2.

□

Lema 3.4. *Seja R uma $\mathbb{F}-$álgebra e ρ uma função ordem fraca em R. Então o conjunto $\mathcal{M}_\rho$ não contém divisores de zero.*

Proposição 3.5. *A $\mathbb{F}$-algebra R é um domínio de integridade.*

Demonstração. Como ρ e σ são bem comportadas, aplicando o lema 3.4 teremos que o conjunto de divisores de zero de R está contido em $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$. Seja $f, g \in R \backslash \mathbb{F}$ e suponha que $\rho(fg) = 0$. Fixando $f \in \mathcal{M}_\rho$, se $g \in \mathcal{M}_\rho$ então $0 = \rho(fg) = \rho(f) + \rho(g)$ e se $g \in \mathcal{U}_\rho$ então $0 = \rho(fg) \leq \rho(f) + \rho(g)$. Se agora fixamos $f \in \mathcal{U}_\rho$, se $g \in \mathcal{M}_\rho$ teremos $0 = \rho(fg) \leq \rho(f) + \rho(g)$. Em todos os casos teremos uma contradição e desta forma R é um domínio de integridade. □

Lema 3.6. *Seja $f \in R^*$ e $I = \langle f \rangle$ é o ideal gerado por f. Os conjuntos $H_x \cup (\mathbb{N}_0^2 \backslash H(I))$ e $H_y \cup (\mathbb{N}_0^2 \backslash H(I))$ são finitos.*

Demonstração. Mostraremos que $H_y \cup (\mathbb{N}_0^2 \backslash H(I))$ é finito. Se $f \in \mathbb{F}$ não há nada para provar, pois $H(R) = H(I)$. Suponha que $f \notin \mathbb{F}$. Escolha $g \in \mathcal{U}_\rho \backslash \mathbb{F}$. Do lema 2.47, existe $\lambda_1 \in \mathbb{F}$ tal que $0 \leq \rho(fg_1) < \rho(f)$, onde $g_1 = g - \lambda_1$. Se $\rho(fg_1) > 0$, podemos ainda usar o lema 2.47 e encontrar $g_2 \in R^*$ tal que $0 \leq \rho(fg_2) < \rho(fg_1)$ e continuando deste modo podemos encontrar $g \in R^*$ tal que $\rho(fg) = 0$ com $\sigma(fg) = 0$ ou $\sigma(fg) > 0$. Se $\sigma(fg) = 0$, recaíremos no caso já estudado. Seja l_σ é a maior lacuna de $\overline{H}_y$. Então para todo $m > \sigma(fg) + l_\sigma$ é seguro que $a = (0, m) \in H(I)$. De fato, se uma $\phi \in R$ é uma função tal que $(\rho(\phi), \sigma(\phi)) = (0, m - \sigma(fg))$, então $fg\phi \in I = \langle f \rangle$ e

$$\begin{aligned}(\rho(fg\phi), \sigma(fg\phi)) &= (\rho(fg) + \rho(\phi), \sigma(fg) + \sigma(\phi)) \\ &= (0, \sigma(fg) + m - \sigma(fg)) \\ &= (0, m) = a \in H(I)\end{aligned}$$

Daí $H(I)$ é identificado com H_y que é infinito. Como ρ e σ são bem comportadas, temos $\#(\mathbb{N}_0^2 \backslash H(I)) < \infty$ e assim $\#(H_y \cap (\mathbb{N}_0^2 \backslash H(I))) < \infty$. A prova é análoga para H_x. □

Proposição 3.7. *Seja $I \subseteq R$, é um ideal próprio de R. Então, como um espaço vetorial sobre $\mathbb{F}$, $dim_{\mathbb{F}}\ (R/I) \leq \#\{a \in \Gamma : a \notin H(I)\}$. Em particular, esta dimensão é finita.*

Demonstração. Seja $f \in I$, $f \neq 0$ e $J = \langle f \rangle$. Para cada $a \in \Gamma$ tome um elemento $\phi_a \in \mathcal{B}$, isto é, $(\rho(\phi_a), \sigma(\phi_a)) = a$. Note que $J \subset I$ e assim $H(J) \subset H(I)$. Se $a \in H(J)$ (respectivamente $a \in H(I)$), tome $\phi_a \in J$ (respectivamente $\phi_a \in I$). Como podemos ver na proposição 2.49, o conjunto $\mathcal{B}$ é uma base de R. Note que podemos reescrever Γ como sendo $\Gamma = H(I) \cup (\Gamma \backslash H(I))$. Então

$$dim(R/I) \leq \#\{\phi_a + I; a \in \Gamma\}.$$

Se $a \in \Gamma$ e $a \in H(I)$, então $\phi_a \in I$ e teremos que $\{\phi_a + I = I$. Assim

$$\begin{aligned}dim(R/I) &\leq \#\{\phi_a + I; a \in \Gamma\} \\ &\leq \#\{\phi_a + I; a \in \Gamma \backslash H(I)\} \\ &\leq \#\{\phi_a + I; a \in \Gamma \backslash H(J)\}\end{aligned}$$

sendo que $\#(\Gamma \backslash H(J))$ é finito pelo lema 3.6. □

Uma vez que, R é um domínio então admite um corpo quociente, o qual denotamos por K.

Teorema 3.8. *O grau de transcedência de K sobre* $\mathbb{F}$ *é um.*

Demonstração. No Teorema 3.6 provamos que $\mathbb{F}$-álgebra R é finitamente gerada sobre $\mathbb{F}$. Assim pelo teorema A.20, segue que o grau de transcedência de K sobre $\mathbb{F}$ é igual a dimensão de Krull de R.
Tome $f \in R^*$ tal que f não é invertível. Tal elemento existe, basta tomarmos $f \in R \backslash \mathbb{F}$. Seja $\mathfrak{p}$ o ideal primo minimal contendo f. Pelo Teorema A.10 então $ht\ \mathfrak{p} \leq 1$, mas pelo corolário A.11, teremos que $ht\ \mathfrak{p} = 1$. Assim, pelo corolário A.21, temos

$$dim\ R = ht\ (\mathfrak{p}) + dim\ (R/\mathfrak{p})$$

onde *dim* destina-se a dimensão de Krull. Afirmamos que $dim\ (R/\mathfrak{p}) = 0$. Com efeito, a proposição 3.7 nos garante que $R/\mathfrak{p}$ é um $\mathbb{F}$-espaço vetorial de dimensão finita. Logo $R/\mathfrak{p}$ é artiniano e portanto a dimensão de Krull de $R/\mathfrak{p}$, denotado por $dim\ (R/\mathfrak{p})$, será igual a zero. Assim, obtemos que $dim\ R = 1$. □

Lema 3.9. *Seja* $f \in R^*$ *e* $I = \langle f \rangle$ *é um ideal gerado por* f. *Então* $H(I) \cup \{0\}$ *é um semigrupo de gênero finito.*

Demonstração. Sejam $a \neq b \in \Gamma$ e ϕ_a, $\phi_b \in \mathcal{B}$ com $a = (\rho(\phi_a), \sigma(\phi_a))$ e $b = (\rho(\phi_b), \sigma(\phi_b))$ onde $\rho(\phi_a) \neq \rho(\phi_b)$ ou $\sigma(\phi_a) \neq \sigma(\phi_b)$. Note que, se $\phi_a - \phi_b \in I$ então lub(a,b)$\in$ H(I). Com efeito, pelo lema 2.41 temos

$$lub(a, b) = (\rho(\phi_a - \phi_b), \sigma(\phi_a - \phi_b))$$

e como I é fechado com relação a adição segue que $lub(a, b) \in H(I)$. Por outro lado, como visto na proposição 2.48, onde $H = \{lub(a, b); a, b \in \Gamma\}$, se tomarmos $\phi_a \in I$ exceto para um número finito de elementos $a \in \Gamma$, teremos pela justificativa acima que a maioria dos elementos de H também pertence a $H(I)$. □

Lema 3.10. *Seja* $f \in R^*$. *Então existe* $g \in \mathcal{M}_\rho$ *tal que* $fg \in \mathcal{M}_\rho$

Demonstração. Se $f \in \mathbb{F}^*$ então $\rho(fg) = \rho(g) > \rho(1)$ para todo $g \in \mathcal{M}_\rho$. Assuma que $f \notin \mathbb{F}^*$ e suponha que o resultado é falso, ou seja, $\rho(fg) = 0$ para todo $g \in \mathcal{M}_\rho$. Isto implica que $f \in \mathcal{U}_\rho$. Caso do contrário, isto é, $f \in \mathcal{M}_\rho$ e portanto

$$\rho(f^2) = \rho(f.f) > \rho(f.1) > \rho(1) = 0$$

o que é um absurdo. Assim, $\rho(fg) = 0$ para todo $g \in \mathcal{U}_\rho$ pois

$$0 \leq \rho(fg) \leq \rho(f) + \rho(g) = 0 + 0 = 0$$

Portanto, $\rho(fg) = 0 \ \forall g \in R^*$. Logo, $I = \langle f \rangle \subseteq \mathcal{U}_\rho$ e consequentemente o gênero de $H(I) \cup \{(0,0)\}$ é infinito pois

$$H(I) \cup \{(0,0)\} \subseteq H(\mathcal{U}_\rho)$$

e

$$H(\mathcal{U}_\rho) = \{(0, \sigma(h)); h \in \mathcal{U}_\rho\}$$

tem gênero infinito. Isto é um absurdo, pois contraria o lema 3.12 □

Defina a aplicação $\widetilde{\rho} : R \to \mathbb{Z} \cup \{-\infty\}$ como seguinte:

$$\widetilde{\rho}(f) := \begin{cases} -\infty & se\ f = 0 \\ min\{\rho(fg) - \rho(g) :\ g \in \mathcal{M}_\rho\} & se\ f \neq 0 \end{cases}$$

No próximo lema provaremos algumas propriedades relevantes de $\widetilde{\rho}$.

Lema 3.11. *(1) $\widetilde{\rho}$ é bem definida e $\widetilde{\rho}(f) = \rho(fg) - \rho(g)$ para todo $g \in \mathcal{M}_\rho$ tal que $fg \in \mathcal{M}_\rho$;*

(2) Se $f \in \mathcal{M}_\rho$, então $\widetilde{\rho}(f) = \rho(f) > 0$; se $f \in \mathcal{U}_\rho$, então $\widetilde{\rho}(f) \leq 0$;

(3) $\widetilde{\rho}(f) = 0$ para todo $f \in \mathbb{F}^*$;

(4) $\widetilde{\rho}(fg) = \widetilde{\rho}(f) + \widetilde{\rho}(g)$;

(5) $\widetilde{\rho}(f + g) \leq max\{\widetilde{\rho}(f), \widetilde{\rho}(g)\}$;

Demonstração. (1) Sejam $g_1, g_2 \in \mathcal{M}_\rho$ tal que $fg_1 \in \mathcal{M}_\rho$. Então, pela propriedade (VI) temos $\rho(fg_1) + \rho(g_2) = \rho(fg_1g_2) \leq \rho(fg_2) + \rho(g_1)$ e assim $\rho(fg_1) - \rho(g_1) \leq \rho(fg_2) - \rho(g_2)$. A igualdade é obtida quando procedemos de maneira análoga para $fg_2 \in \mathcal{M}_\rho$.

(2) Se $f \in \mathcal{M}_\rho$ implica que $\widetilde{\rho}(f) = min\{\rho(fg) - \rho(g);\ g \in \mathcal{M}_\rho\} = min\{\rho(f) + \rho(g) - \rho(g) :\ g \in \mathcal{M}_\rho\} = min\{\rho(f); g \in \mathcal{M}_\rho\} = \rho(f) > 0$
Se $f \in \mathcal{U}_\rho$, então $\widetilde{\rho}(f) = min\{\rho(fg) - \rho(g);\ g \in \mathcal{M}_\rho\}$. Sabemos que $\rho(fg) \leq \rho(f) + \rho(g) = \rho(g)$ e assim $\rho(fg) - \rho(g) \leq 0$ e portanto $\widetilde{\rho}(f) \leq 0$

(3) Se $f \in \mathbb{F}^*$ então $\widetilde{\rho}(f) = min\{\rho(fg) - \rho(g);\ g \in \mathcal{M}_\rho\} = min\{\rho(g) - \rho(g) = 0; g \in \mathcal{M}_\rho\} = 0$.

(4) Sejam $g, f \in R^*$. Pelo lema 3.10, existem $h_1, h_2 \in \mathcal{M}_\rho$ tais que $h_1g, h_2fg \in \mathcal{M}_\rho$. Fazendo $h = h_1h_2$ temos que $hg, hfg \in \mathcal{M}_\rho$. Então

$$\begin{aligned}\widetilde{\rho}(f) &= \rho(fgh) - \rho(h)\\ &= \rho(fgh) + \rho(gh) - \rho(gh) - \rho(h)\\ &= \rho(fgh) - \rho(gh) + \rho(gh) - \rho(h)\\ &= \widetilde{\rho}(f) + \widetilde{\rho}(g)\end{aligned}$$

(5) Sejam $f, g \in R^*$. Pelo lema 3.10 existe $h \in \mathcal{M}_\rho$ tal que $fh, gh \in \mathcal{M}_\rho$. Então

$$\begin{aligned}\widetilde{\rho}(f+g) &= min\{\rho((f+g)h_1) - \rho(h_1);\ h_1 \in \mathcal{M}_\rho\}\\ &\leq \rho((f+g)h) - \rho(h)\\ &= \rho(fh + gh) - \rho(h)\\ &\leq max\{\rho(fh), \rho(gh)\} - \rho(h)\\ &= max\{\rho(fh) - \rho(h), \rho(gh) - \rho(h)\}\\ &\leq max\{\widetilde{\rho}(f), \widetilde{\rho}(g)\}\end{aligned}$$

□

Defina agora as aplicações $v_\rho : K \to \mathbb{Z} \cup \{\infty\}$ por:

$$v_\rho\left(\frac{f}{g}\right) := \begin{cases} \infty & se\ f = 0 \\ \widetilde{\rho}(g) - \widetilde{\rho}(f) & se\ f \neq 0 \end{cases}$$

e $\upsilon_\sigma : K \to \mathbb{Z} \cup \{\infty\}$ por:

$$\upsilon_\sigma\left(\frac{f}{g}\right) := \begin{cases} \infty & se\ f = 0 \\ \widetilde{\sigma}(g) - \widetilde{\sigma}(f) & se\ f \neq 0 \end{cases}$$

Proposição 3.12. *A aplicação υ_ρ está bem definida e é uma valorização discreta de K sobre $\mathbb{F}$.*

Demonstração. 1. A aplicação υ_ρ está bem definida, pois $\widetilde{\rho}(f)$ é bem definida (ver lema 3.11(1)).

2. $\upsilon_\rho\left(\frac{f}{g}\right) = \infty \Leftrightarrow f = 0$, segue da definição de υ_ρ.

3. Sejam $\frac{f}{g}, \frac{h}{k} \in K^*$, então

$$\begin{aligned} \upsilon_\rho\left(\tfrac{fh}{gk}\right) &= \widetilde{\rho}(gk) - \widetilde{\rho}(fh) \\ &= \widetilde{\rho}(g) + \widetilde{\rho}(k) - (\widetilde{\rho}(f) + \widetilde{\rho}(h)) \\ &= \widetilde{\rho}(g) - \widetilde{\rho}(f) + \widetilde{\rho}(k) - \widetilde{\rho}(h) \\ &= \upsilon_\rho\left(\tfrac{f}{g}\right) + \upsilon_\rho\left(\tfrac{h}{k}\right) \end{aligned}$$

4. Sejam $f, g \in \mathbb{F}^*$. Assim,
$\upsilon_\rho\left(\frac{f}{g}\right) = \widetilde{\rho}(g) - \widetilde{\rho}(f)$ e pelo lema 3.11(3) temos que $\widetilde{\rho}(f) = 0$ e $\widetilde{\rho}(g) = 0$. Daí segue que $\upsilon_\rho(\frac{f}{g}) = 0$.

5. Sejam $f, g \in R \backslash \mathcal{U}_\rho = \mathcal{M}_\rho$, tais que $\frac{f}{g} \in K^*$. Pelo lema 3.11(2), $\widetilde{\rho}(g) = \rho(g) > 0$ e $\widetilde{\rho}(f) = \rho(f) > 0$. Como $\rho(\mathcal{M}_\rho) = \mathbb{N}$ tome f, g tais que $\widetilde{\rho}(g) = 2$ e $\widetilde{\rho}(f) = 1$. Daí $\upsilon_\rho\left(\frac{f}{g}\right) = 1$.

6. Sejam $\frac{f}{g}, \frac{h}{k} \in K$. Assim,

$$\begin{aligned} \upsilon_\rho\left(\tfrac{f}{g} + \tfrac{h}{k}\right) &= \upsilon_\rho\left(\tfrac{fk+hg}{gk}\right) \\ &= \widetilde{\rho}(gk) - \widetilde{\rho}(fk + hg) \\ &\geq \widetilde{\rho}(gk) - max\{\widetilde{\rho}(fk), \widetilde{\rho}(hg)\} \\ &= min\{\widetilde{\rho}(gk) - \widetilde{\rho}(fk), \widetilde{\rho}(gk) - \widetilde{\rho}(hg)\} \end{aligned}$$

Disto segue que $v_\rho\left(\frac{f}{g}+\frac{h}{k}\right) \geq min\{v_\rho\left(\frac{f}{g}\right), v_\rho\left(\frac{h}{k}\right)\}$.

Com isso provamos que v_ρ corresponde a uma valorização discreta em K. □

Para um lugar $S \in K$, sejam v_S e $\mathcal{O}_S$ as correspondentes valorização e anel de valorização em K. Seja

$$\mathcal{S}(R) := \{S \in \mathbb{P}_K : R \subseteq \mathcal{O}_S\}.$$

Proposição 3.13. *Sejam v_ρ e v_σ valorizações associados aos lugares P e Q de K respectivamente. Então*

$$\mathcal{S}(R) = \mathbb{P}_K \backslash \{P, Q\}$$

Demonstração. Vamos supor que $\mathcal{S}(R) \supset \mathbb{P}_K$. Logo, $P, Q \in \mathcal{S}(R)$ e assim temos que $R \subseteq \mathcal{O}_P$. Então $\mathcal{U}_\rho = R$. Com efeito, se $f \in R \subseteq \mathcal{O}_P$, isto quer dizer que $\rho(f) = -v_P(f) \leq 0$, o que implica que $f \in \mathcal{U}_\rho$. Assim, $R = \mathcal{U}_\rho$ e portanto $\mathcal{M}_\rho = \emptyset$ e o semigrupo $H(R)$ pode não ter o gênero finito. Analogamente para Q, concluímos que $P, Q \notin \mathcal{S}(R)$. Agora, vamos supor que $\mathcal{S}(R) \cup \{P, Q\} \neq \mathbb{P}_K$. Podemos aplicar para $\mathcal{S}(R) \cup \{P, Q\}$ o teorema da aproximação forte 1.38 para concluir que existe uma sequência infinita $(h_1, h_2, ...)$ de funções em K tais que

$$v_\rho(h_i) = v_\sigma(h_i) = i \quad e$$

$$v_S(h_i) \geq 0, \ \textit{para cada } S \in \mathcal{S}(R).$$

Em particular, $h_i \in \cap_{S \in \mathcal{S}(R)} \mathcal{O}_S$ e este anel é precisamente $\overline{R}$, o fecho integral de R sobre K (ver teorema 1.55), ou seja, $\overline{R} = \cap_{S \in \mathcal{S}(R)} \mathcal{O}_S$.
A sequência $(h_1, h_2, ...)$ é $\mathbb{F}-$linearmente independente, pois $v_\rho(h_i) \neq v_\rho(h_j)$ e $v_\sigma(h_i) \neq v_\sigma(h_j)$ se $i \neq j$ e está contida no $\mathbb{F}-$espaço vetorial W, onde

$$W := \{x \in \overline{R}; v_\rho(x) > 0 \ e \ v_\sigma(x) > 0\}$$

Como as funções ordem fraca ρ e σ são bem comportadas, temos que $W \cap R \subseteq \mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$. De fato, se $x \in W \cap R$, então $v_\rho(x) > 0$. Logo, $\widetilde{\rho}(1) > \widetilde{\rho}(x)$ e portanto $x \in \mathcal{U}_\rho$ e análogamente, $x \in \mathcal{U}_\sigma$. Logo, $W \cap R = \{0\}$, pois zero é o único elemento de $\mathbb{F}$ em W. Agora, note que

$$W \subseteq W + R \subseteq \overline{R}$$

e consequentemente, como $R \cap W = \{0\}$, segue que

$$W \cong \frac{W}{R} \subseteq \frac{W+R}{R} \subseteq \frac{\overline{R}}{R}.$$

Portanto,

$$dim\ W \leq dim \frac{\overline{R}}{R}$$

Mas, pelo Teorema do Fecho Integral A.22, esta última dimensão é finita o que nos dá uma contradição. Portanto $\mathcal{S}(R) = \mathbb{P}_K/\{P, Q\}$, o que implica que R é um anel de coordenadas de uma curva algébrica afim com exatamente dois lugares de grau um no infinito. □

Em suma o que vimos anteriormente será agora enunciado em forma de teorema.

Teorema 3.14. *Seja R é uma $\mathbb{F}$-álgebra admitindo dois bem comportados pesos fraco ρ e σ. Então*

(1) R é um domínio de integridade e corpo quociente K é um corpo de funções algébricos de uma variável sobre $\mathbb{F}$;

(2) Então existe dois lugares $P, Q \in \mathbb{P}_K$ tal que ρ e σ são derivadas das valorizações associadas a P e Q através do procedimento indicado na exemplo 2.39;

(3) $\overline{R} = \cap_{S \in \mathbb{P}_K \setminus \{P,Q\}} \mathcal{O}_S$.

Seja R uma $\mathbb{F}_q$-álgebra com duas funções peso fraco. Do teorema 3.13, temos que R é um anel de coordenadas afim de uma curva algébrica $\mathcal{X}$, definida sobre $\mathbb{F}_q$, com dois lugares P, Q de grau um no infinito. Vimos também que $R \subset \overline{R} = \bigcap_{S \in \mathcal{S}(R)} \mathcal{O}_S$. Assim sejam $P_1, P_2, ..., P_n$ pontos $\mathbb{F}_q$-racionais dois a dois distintos sobre $\mathcal{X}$, diferentes de P e Q. Considere a aplicação de avaliação:

$$\begin{array}{rccc} av: & R & \to & \mathbb{F}_q^n \\ & f & \mapsto & (f(P_1), ..., f(P_n)) \end{array}$$

Sejam $D = P_1 + P_2 + ... + P_n$ e G um divisor de K tal que $supp\ G \cap supp\ D = \emptyset$. Sabemos que $\mathcal{L}(G) = \{x \in R; v_S(x) \geq -v_S(G); \forall\ S \in \mathbb{P}_F\}$. Agora observe que dado $x \in \mathcal{L}(G)$, como $R \subset \bigcap_{S \in \mathcal{S}(R)} \mathcal{O}_S$, temos que $v_S(x) \geq 0$, para todo $S \neq \{P, Q\}$. Logo $v_P(x) < 0$ e $v_Q(x) < 0$ e como $v_P(x) \geq -v_P(G)$ e $v_Q(x) \geq -v_Q(G)$, temos que $l := v_P(G) > 0$ e

$m := v_Q(G) > 0$. Assim, $P, Q \in supp\ (G)$. Mas $\mathcal{L}(lP + mQ) = \{x \in R : \rho(x) \leq l,\ \sigma(x) \leq m\ e\ v_S(x) \geq 0,\ \forall S \neq \{P, Q\}\}$, então, segue que $\mathcal{L}(G) = \mathcal{L}(lP + mQ)$. Como R possui uma $\mathbb{F}$-base e $\mathcal{L}(G) \subset R$, temos que os elementos da base de R formam uma base para $\mathcal{L}(G)$. Assim $\mathcal{L}(G) = \langle f_0, ...f_l \rangle \oplus \langle g_1, ..., g_a \rangle$ e portanto

$$E_l = av(\mathcal{L}(G)) = av(\mathcal{L}(lP + mQ)) = C(D, lP + mQ)$$

Portanto, podemos concluir que os códigos de avaliação construidos sobre álgebras com função peso fraco são códigos de Goppa bi-pontuais.

Apêndice A

Noções de Álgebra Comutativa

Neste apêndice estaremos apresentando as noções de álgebra comutativa que foram utilizadas ao longo desta dissertação, para maiores esclarecimento consultar, as seguintes referência [5] e [10].

A.1 Anéis Noetherianos e Artinianos

Definição A.1. *Sejam A um anel e M um A-módulo. Dizemos que um A-módulo M é* **noetheriano** *(resp.* **artiniano***) se toda cadeia ascendente (resp. descendente) de submódulos de M é estacionária, isto é,*

$$M_1 \subseteq M_2 \subseteq ... \subseteq M_n \subseteq ... \text{ então existe } n_0 \in \mathbb{N} \text{ tal que } M_n = M_{n_0}, \text{ para todo } n \geq n_0$$

$$(resp.\ M_1 \supseteq M_2 \supseteq ... \supseteq M_n \supseteq ... \text{ então existe } n_0 \in \mathbb{N} \text{ tal que } M_n = M_{n_0}, \text{ para todo } n \leq n_0).$$

Se $M = A$ é **noetheriano** *(resp.* **artiniano***) então dizemos que A é um* **anel noetheriano** *(resp.***anel artiniano***).*

Corolário A.2. *Se A é um anel noetheriano (resp. artiniano) e I é um ideal de A então A/I é um anel noetheriano (resp. artiniano).*

Sejam A um anel, I um ideal de A e P um ideal primo de A. Dizemos que P é um ideal primo minimal de I se P é um menor ideal primo de A que contém I. No caso em que $I = (0)$, dizemos que P é um ideal primo minimal de A.

Proposição A.3. *Se A é um anel noetheriano então A possui um número finito de ideais primos minimais.*

Proposição A.4. *Se A é um anel artiniano então todo ideal primo de A é maximal. Mais ainda, o número de ideais maximais de A é finito.*

Teorema A.5. *A é um anel artiniano se, e somente se, A é um anel noetheriano e cada ideal primo de A é maximal.*

Teorema A.6 (Teorema da Base de Hilbert)**.** *Se A é um anel noetheriano então o anel de polinômios $A[X]$ é um anel noetheriano.*

Corolário A.7. *Sejam A um anel e I um ideal de A. Se A é noetheriano então $A[X_1, ..., X_n]/I$ também é noetheriano.*

A.2 Teoria da Dimensão

Definição A.8. *Sejam A um anel e I um ideal de A.*

1. *A* **dimensão de Krull** *de A (ou simplesmente dimensão de A), denotada por $dim\ A$, é definida como o sendo o supremo do comprimento das cadeias de ideais primos de A, isto é,*

$$dim\ A = sup\{n \in \mathbb{N} | \exists P_0 \subset P_1 \subset ... \subset P_n,\ P_i \in Spec(A)\}.$$

2. *Se I é um ideal primo de A, definimos a altura de I, denotado por $ht(I)$, como sendo o supremo do comprimento das cadeias de ideias primos de A que terminam em I, isto é,*

$$ht(I) = sup\{n \in \mathbb{N} | \exists P_0 \subset P_1 \subset ... \subset P_n = I,\ P_i \in Spec(A)\}.$$

Em geral, a altura de um ideal I de A é dada por:

$$ht(I) = inf\{ht(P) | P \text{ é ideal primo minimal de } I\}.$$

Exemplo A.9. *1. A é anel artiniano então $dim\ A = 0$;*

2. *Se $A = \mathbb{Z}$ então dim $A = 1$;*

3. *Se A é finito então dim $A = 0$;*

4. *Se $A = K[X_1, X_2, ...]$, com K corpo, então dim $A = \infty$.*

Teorema A.10 (Teorema do Ideal Principal)**.** *Se $x_1, x_2, ..., x_c \in R$ e $P \subset R$ é ideal primo minimal, contendo $x_1, x_2, ..., x_c$, então ht(p)$\leq c$.*

Corolário A.11. *Seja R um anel de noetheriano e seja x um elemento de R o qual não é um divisor de zeros ou uma unidade. Então todo ideal primo minimal P de (x) possui altura igual a 1.*

A.3 Dependência de Integral

Ao longo desta seção, $B|A$ denotará uma extensão de anéis, isto é, $A \subseteq B$ e A é um subanel de B.

Definição A.12. *Seja $B|A$ uma extensão de anéis. Dizemos que um elemento $x \in B$ é* **inteiro** *(ou* **integral***) sobre A se x é raíz de um polinômio mônico com coeficientes em A, isto é, se existem $a_1, ..., a_n \in A$ tal que $x^n + a_1x^{n-1} + ... + a_n = 0$.*

Um primeiro resultado que caracteriza um elemento inteiro sobre um anel é dado pela seguinte proposição.

Proposição A.13. *Dados uma extensão de anéis $B|A$ e $x \in B$, são equivalentes:*

1. *x é inteiro sobre A;*

2. *$A[x] = \{g(x)|g(X) \in A[X]\}$ é um A-módulo finitamente gerado;*

3. *Existe um subanel C de B tal que $A \subseteq C$, C é finitamemte gerado como A-módulo e $x \in C$.*

Segue, como consequência da proposição anterior, os resultados abaixo.

Corolário A.14. *Sejam $B|A$ uma extensão de anéis e $x_1, ..., x_n \in B$ inteiros sobre A. Então o anel $A[x_1, ..., x_n]$ é um A-módulo finitamente gerado.*

Corolário A.15. *Sejam $B|A$ uma extensão de anéis. Então*

1. *Se $x, y \in B$ são inteiros sobre A então $x \pm y$ e $x.y$ também são.*

2. *$A = \{x \in B | x$ é inteiro sobre $A\}$ é subanel de B que contém A. Tal anel é conhecido como o* **fecho integral** *de A em B.*

Definição A.16. *Sejam $B|A$ uma extensão de anéis. Dizemos que $B|A$ é uma extensão* **integral de anéis** *(ou B é inteira sobre A) se para todo $x \in B$ temos que x é inteiro sobre A. Se $A = \overline{A}$ então dizemos que A é* **integralmente fechado** *em B.*

Corolário A.17. *Seja $B|A$ uma extensão integral de anéis. Então*

$$dim\ B = dim\ A.$$

Definição A.18. *Sejam $K \subseteq R$ uma extensão de anéis, $\Omega = \{y_1, ..., y_n\} \subset R$ e $B = K[X_1, ..., X_n]$ o anel de polinômios em n variáveis sobre K. Dizemos que:*

1. *O conjunto é* **algebricamente independente** *(ou* **transcendente***) sobre K se satisfaz:*
   Dado $G = G(X_1, ..., X_n) \in B$ tem-se que $G(y_1, ..., y_n) = 0$ se, e somente se, $G = 0$.
   Caso contrário, dizemos que é **algebricamente dependente.**

2. *Um conjunto não-vazio $S \subset R$ é algebricamente independente sobre K se todo subconjunto finito e não-vazio de S é algebricamente independente sobre K.*

Teorema A.19. *Seja $R = K[x_1, ..., x_n]$ uma K-álgebra finitamente gerada que é um domínio. Então apenas uma das seguintes afirmações é verdadeira:*

1. *A álgebra R é uma extensão algébrica finita de K e portanto R é um corpo (isto é, R é um domínio que tem dimensão de Krull igual a zero);*

2. *Existe $d \in \mathbb{N}$ com $1 \leq d \leq n$ e existe $\Lambda = \{z_1, ..., z_d\} \subset R$ tal que Λ é algebricamente independente sobre K e $K[z_1, ..., z_d] \subseteq R$ é uma extensão integral. Mais ainda, neste caso a dimensão de Krull de R é d.*

Uma relação entre o grau de transcedência e a dimensão de Krull de uma $\mathbb{F}$-álgebra finitamente gerada que é um domínio é dada no resultado abaixo.

Teorema A.20. *Se R é uma $\mathbb{F}$-álgebra finitamente gerada e além disso um domínio sobre um corpo $\mathbb{F}$, então*

$$dim\ R = grau\ de\ transcedência\ R$$

Sendo que este é o comprimento de todas as cadeias maximais de ideais primos de R.

Se P é um ideal primo de um anel R então definimos a dimensão de P, com notação $dim\ P$ como sendo $dim\ R/P$ e a codimensão de P, de notação codim P que é também conhecida por $ht\ P$. Vejamos algumas consequências (não todas naturais) deste resultado. Aqui, uma $\mathbb{F}$-álgebra finitamente gerada que é um domínio é dito ser um *domínio afim.*

Corolário A.21. *Se R é um domínio afim e $P \subset R$ é um ideal, então*

$$dim\ R = dim\ P + codim\ P$$

Teorema A.22. *Seja R um domínio afim sobre um corpo $\mathbb{F}$. Seja $K = K(R)$ e seja L a extensão finita do corpo K. Se T é o fecho integral de R em L, então T é finitamente gerado $R-$modulo, em particular, T é ainda um domínio afim.*

Apêndice A

Curvas Algébricas

Neste apêndice estaremos apresentando as noções de curvas algébricas, para maiores esclarecimento consultar, as seguintes referência [15].

Seja $\mathbb{F}$ um corpo, denota-se por $A^n(\mathbb{F})$, ou simplesmente A^n o produto cartesiano de $\mathbb{F}$, n vezes. A^n é conhecido como n - espaço afim sobre $\mathbb{F}$, os elementos de $A^n(\mathbb{F})$ são chamados pontos.

Seja $F \in \mathbb{F}[x_1, ..., x_n]$, um ponto $P = (a_1, ..., a_n) \in A^n$ é um zero de F se $F(P) = F(a_1, ..., a_n) = 0$. Se F não é constante, o conjunto de zeros de F é chamado *hiper-superficie* definida por F, que será denotado por $V(F)$. Uma hiper-superficie de A^2 é denominado curva plana afim.

Podemos generalizar este conceito, consideremos S um conjunto de polinômios de $\mathbb{F}[x_1, ..., x_n]$, definimos

$$V(S) = \{P \in A^n | F(P) = 0, \forall F \in S\}$$

Dado $V(S)$, podemos reescrever da seguinte forma $V(S) = \cap_{F \in S} V(F)$ e mais ainda se $S = \{F_1, ..., F_r\}$ podemos escrever $V(F_1, ..., F_r)$. Um subconjunto $X \subset A^n(\mathbb{F})$ é um *conjunto algébrico afim*, ou simplesmente um *conjunto algébrico* se $X = V(S)$ para algum S. Que safistaz as seguintes propriedades.

1. Se I é um ideal de $\mathbb{F}[x_1, ..., x_n]$ gerado por S, então $V(S) = V(I)$ e todo conjunto algébrico é igual a $V(I)$ para algum ideal I.

2. Se $\{I_\alpha\}$ é uma coleção de ideais, então $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$; somente a interseção de uma coleção de conjuntos algébricos é um conjunto algébrico.

3. Se $I \subset J$, então $V(I) \supset V(J)$.

4. $V(FG) = V(F) \cup V(G)$ para algum polinômio F e G; $V(I) \cup V(J) = V(\{FG|F \in I, G \in J\})$, somente para um número finito a união de conjuntos algébricos será também um conjunto algébrico.

5. $V(0) = A^n(\mathbb{F})$, $V(1) = \emptyset$ e $V(x_1 - a_1, ..., x_n - a_n) = \{a_1, ..., a_n\}$ para $a_i \in \mathbb{F}$. Assim alguns subconjuntos finito de $A^n(\mathbb{F})$ é um conjunto algébrico.

Para algum subconjunto X de A^n, consideremos polinômios que se anulam em todos os pontos de X, este conjunto forma um ideal de $\mathbb{F}[x_1, .., x_n]$ que denominamos de ideal de X, e escrevemos $I(X)$

$$I(X) = \{F \in \mathbb{F}[x_1, ..., x_n]|F(a_1, ..., a_n) = 0, \forall (a_1, ..., a_n) \in X\}$$

Que são validas as seguintes propriedades.

1. Se $X \subset Y$, então $I(X) \supset I(Y)$.

2. $I(\emptyset) = \mathbb{F}[x_1, ..., x_n]$, $I(A^n) = (0)$ se $\mathbb{F}$ é um corpo infinito, $I(a_1, ..., a_n) = (x_1 - a_1, ..., x_n - a_n)$ $\forall a_i \in \mathbb{F}$.

3. $I(V(S)) \supset S$ para algum conjunto S de polinômio e $V(I(X)) \supset X$ para algum conjunto X de pontos.

4. $V(I(V(S))) = V(S)$ para algum conjunto S de polinômios e $I(V(I(X))) = I(X)$ para algum conjunto X de pontos, assim se V é um conjunto algébrico $V = V(I(V))$ e se I é o ideal de um conjunto algébrico, então $I = I(V(I))$

Definição A.1. *Se I é um ideal de um anel R, definimos o radical de I, denotado por $Rad(I)$, como*

$$\{a \in R|a^n \in I, n \in \mathbb{Z}, n > 0\}$$

Note que $Rad(I)$ é um ideal e que $Rad(I) \supset I$, quando $Rad(I) = I$ o ideal I é chamado de *ideal radical*.

Embora tenhamos que um conjunto algébrico definido para algum conjunto de polinômio, o fato é que um número finito é suficiente, veremos este fato no próximo teorema.

Teorema A.2. *Todo conjunto algébrico é a interseção de um número finito de hipersuperficie.*

Um conjunto algébrico $V \subset A^n$ é *redutível* se $V = V_1 \cup V_2$, onde V_1, V_2 são conjuntos algébricos em A^n e $V_i \neq V$, $i = 1, 2$, caso contrário V é dito *irredutível*.

Proposição A.3. *Um conjunto algébrico V é irredutível se e somente se I(V) é primo.*

O objetivo é mostrar que um conjunto algébrico é união de um número finito de conjuntos algébricos irredutíveis. Se V é redutível, podemos escrever como $V = V_1 \cup V_2$, supondo que V_2 é redutível escrevemos $V_2 = V_3 \cup V_4$ e assim sucessivamente, o que precisamos então saber se este processo para.

Teorema A.4. *Seja V um conjunto algébrico em $A^n(\mathbb{F})$. Então existe alguns conjuntos algébricos irredutíveis, $V_1, ..., V_m$ tal que $V = V_1 \cup ... \cup V_m$ e $V_i \not\subset V_j$ $\forall i \neq j$*

Definição A.5. *i) Seja A um conjunto algébrico irredutível, então chamaremos de* **variedade algébrica afim***(ou simplesmente variedade afim).*

ii) Dado um variedade afim A, definimos o seu **anel de coordenadas afim** *como sendo*

$$\mathbb{F}[A] = \mathbb{F}[x_1, ...x_n]/I.$$

iii) Dada uma variedade algébrica afim A definimos o corpo de frações racional de $\mathbb{F}[A]$, denotado por $\mathbb{F}(A)$, como sendo o **corpo de frações racionais** *de A. Os elementos de $F(A)$ são chamados de* **funções racioanis.**

Se A é uma variedade e $\mathbb{F}(A)$ é uma extensão finita de $\mathbb{F}$, definimos a dimensão de A, como sendo o grau de transcedência $[\mathbb{F}(A) : \mathbb{F}] = n$. Uma variedade de dim $A = 1$ é chamada de curva algébrica afim(ou simplesmente curva afim).

Agora, considere uma variedade afim A e P um ponto de A. Observe que se $H(x_1,..,x_n)+I = \widetilde{H}(x_1,...,x_n)+I$ então $H-\widetilde{H} \in I$ e portanto $H(P)=\widetilde{H}(P)$. Assim, dado $h = H(x_1,...,x_n)+I \in \mathbb{F}[A]$ podemos definir: $h(P)=H(P)$. Logo o conjunto,

$$\mathcal{O}_P(A)=\left\{\frac{f}{g}\in\mathbb{F}(A)\Big| f,g\in\mathbb{F}[A]\ e\ g(P)\neq 0\right\}$$

é um anel local que tem como corpo de frações o próprio $\mathbb{F}(A)$ e ideal maximal

$$M_P(A)=\left\{\frac{f}{g}\in\mathbb{F}(A)\Big| f,g\in\mathbb{F}[A], f(P)=0\ e\ g(P)\neq 0\right\}$$

Definição A.6. *Seja $\mathcal{X}$ uma curva algébrica definida pelo polinômio $F\in\mathbb{F}[x,y]$. Seja P um ponto desta curva. Dizemos que o ponto P é um ponto não singular se pelo menos uma das derivadas parciais de F aplicadas neste ponto é não-nula, ou seja, $F_x(P)\neq 0$ ou $F_y(P)\neq 0$. Se todos os pontos da curva forem não singulares dizemos que a curva é não singular (ou regular).*

Definição A.7. *Dizemos que uma curva algébrica plana $\mathcal{X}$ é absolutamente irredutível se $\mathcal{X}=Z(f)$ onde $f\in\mathbb{F}[x,y]$ é absolutamente irredutível.*

Referências Bibliográficas

[1] A. Hefez e M.L.T.Villela, *Códigos corretores de erros,* IMPA, 2002.

[2] C.Munuera e F.Torres, *The structure of algebras admitting well agreeing near weights,* J. Pure Appl. Algebra. 212 (2007), 910-918.

[3] C.Carvalho, C.Munuera, E.Silva e F.Torres, *Nears orders and codes,* IEEE Trans. Inform. Theory 53(5), 1919-1924, 2007.

[4] C.Carvalho e F.Torres, *On Goppa codes and Weiertrass gaps at several points,* Des. Codes Cryptography 35(2), 211-225, 2005

[5] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry,* Springer-Verlag, New York, 1995.

[6] E.Ballico e S.J.Kim, *Weierstrass multiple loci of n-point algebraic curves,* J. Algebra 199, 455-471, 1998.

[7] E. Silva, *Funções ordens fracas e a distância mínima de códigos geométricos de Goppa,* Ph. D. Tese, Unicamp, 2004.

[8] G.L.Matthews, *Weiertrass pairs and minimum distance of Goppa codes,* Des. Codes Cryptog.,22, 107-121, 2001.

[9] H. Stichtenoth, *Algebraic function fields and codes,* Springer, New York-Berlin, 1993.

[10] M.F.Atiyah e I.G.MacDonald, *Introduction to commutative algebra,* Addison-Wesley, 1969.

[11] M.Homma e S.J.Kim, *Goppa codes with Weiertrass pairs,* J.Pure Appl. Algebra 162, 273-290, 2001.

[12] R. Matsumoto, *Miuras generalization of one-point ag codes is equivalent to Hoholdt,van Lint and Pellikaans generalization*, IEICE Trans. Fundamentals, vol.E82-A, no.10, pp.2007-2010, Outubro, 1999.

[13] S.J.Kim, *On the index of the Weierstrass semigroup of a pair of point on a curve,* Arch. Math. 62, 73-82, 1994.

[14] T.Høholdt, J.H. van Lint e R.Pellikaan, *Algebraic geometry codes,* in Handbook of Coding Theory, V.Pless e W.C.Huffman Eds., 871-961, Elsevier, 1998.

[15] W. Fulton, *Algebraic curves: an introduction to algebraic geometry,* Benjamin, 1969.