Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Dissertação de Mestrado

Álgebras munidas de Função Peso e Códigos de Goppa Pontuais.

por

Rafael Peixoto[†]

Mestrado em Matemática - Campinas - SP

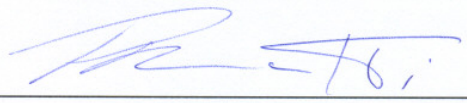
Orientador: Prof. Dr. Paulo Roberto Brumatti

[†]Este trabalho contou com apoio financeiro do CNPq.

Álgebras munidas de Função Peso e Códigos de Goppa Pontuais.

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Rafael Peixoto** e aprovada pela comissão julgadora.

Campinas, 07 de Março de 2007.



Prof. Dr. Paulo Roberto Brumatti

Banca examinadora:

Prof. Dr. Paulo Roberto Brumatti.

Prof. Dr. Fernando Eduardo Torres Orihuela.

Prof. Dr. Cícero Fernandes de Carvalho.

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

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues – CRB8a / 2116

Peixoto, Rafael

P350a Álgebras munidas de função peso e códigos de Goppa pontuais / Rafael Peixoto -- Campinas, [S.P. :s.n.], 2007.

Orientador : Paulo Roberto Brumatti

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria da codificação. 2. Riemann-Roch, Teoremas de. 3. Curvas algébricas. I. Brumatti, Paulo Roberto. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Algebras with a weight function and one-point AG codes.

Palavras-chave em inglês (Keywords): 1. Codification theory. 2. Riemann-Roch theorem. 3. Algebraic curves.

Área de concentração: Álgebra Comutativa, Geometria Algébrica

Titulação: Mestre em Matemática

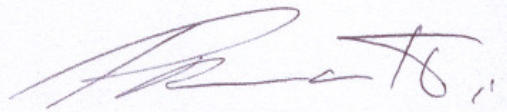
Banca examinadora: Prof. Dr. Paulo Roberto Brumatti (IMECC-UNICAMP)
Prof. Dr. Fernando Eduardo Torres Orihuela (IMECC-UNICAMP)
Prof. Dr. Cícero Fernandes de Carvalho (UFU)

Data da defesa: 07/03/2007

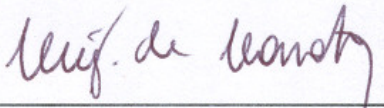
Programa de Pós-Graduação: Mestrado em Matemática

Dissertação de Mestrado defendida em 07 de março de 2007 e aprovada

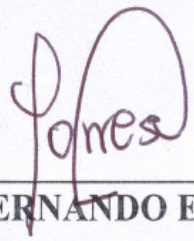
Pela Banca Examinadora composta pelos Profs. Drs.



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



Prof. (a). Dr (a). CÍCERO FERNANDES DE CARVALHO



Prof. (a). Dr (a). FERNANDO EDUARDO TORRES ORIHUELA

Aos meus pais e à minha amada Vanessa

AGRADECIMENTOS

Agradeço primeiramente à Deus, por estar sempre presente na minha vida, permitindo conquistar mais este objetivo.

Ao meu orientador, Paulo Brumatti, pela credibilidade que depositou em mim, pela paciência e por toda ajuda que me concedeu com o seu extenso conhecimento matemático.

Aos meus pais Eurico e Vera, pessoas que sempre foram exemplos de coragem, amor, determinação, retidão e perseverança.

Às minha irmãs, Michele e Gabriele e ao meu sobrinho Pedro, pelo carinho que sempre me dão.

À minha amada Vanessa, pelo amor, carinho, companheirismo, pela paciência (que não foi pouca) e por vários momentos felizes em minha vida. Além disso, à toda sua familia sou muito grato.

Aos meus avós, tios e primos, em especial minha tia Ormezinda, pelo apoio e carinho.

Aos meus companheiros de "guerra", Vander, Marcão, Marquinho, Pedro e Elvis, dentre tantos outros que permanecerão em minha memória.

À minha família que fiz em Campinas, Marcelo, Ariosvaldo, Weber, Vinícius, Allan, Carlos Jr. e Neiton; à galera do futebol e aos amigos do predinho.

Aos professores do IMECC-UNICAMP, aos professores da FAMAT-UFU, em especial ao professor Cícero Carvalho, e aos integrantes do PETMAT-UFU, pelo apoio e incentivo em prosseguir nesta jornada.

RESUMO

O objetivo principal desta dissertação é apresentar o resultado central de R. Matsumoto sobre as álgebras munidas de função peso serem anéis de coordenadas afim de curvas algébricas com exatamente um lugar de grau um no infinito. A partir disto, pode-se concluir que os códigos de avaliação, introduzidos por Høholdt, van Lint e Pellikaan, construídos sobre estas álgebras são um caso particular dos códigos geométricos de Goppa, isto é, códigos de Goppa pontuais. Para isto, utilizamos resultados sobre teoria de corpos de funções algébricas, de códigos geométricos de Goppa e de álgebra comutativa. Com a introdução dos conceitos de funções ordem e peso, nos é permitido descrever os códigos de avaliação e assim determinar cotas inferiores para a distância mínima do seus códigos duais, que em alguns casos são melhores que as cotas de Goppa.

ABSTRACT

The main objective of this text is to present the central result of R. Matsumoto concerning those algebra with a weight function being affine coordinate ring of an affine algebraic curve with exactly one place at infinity. From that statement one can conclude that the evaluation codes, introduced by Høholdt, van Lint e Pellikaan, constructed on this algebra are particular cases of geometric Goppa codes, that is, one point AG codes. For this, we use results of the algebraic function fields theory, geometric Goppa codes and commutative algebra. The introduction of the concepts of order and weight functions enable us to describe the evaluation codes and thus to determine lower bounds for the minimum distance of its duals codes, in same cases, are better than the Goppa's bounds.

SUMÁRIO

INTRODUÇÃO

A teoria dos Códigos Corretores de Erros foi iniciada pelo matemático C.E. Shanon, do laboratório Bell, num trabalho publicado em 1948. No começo os maiores interessados nesta teoria foram os matemáticos, que a desenvolveram consideravelmente, mas, na década de 70, com o avanço das pesquisas espaciais e a grande popularização dos computadores, essa teoria passou também a interessar aos engenheiros. Hoje em dia, os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo sua confiabilidade, e estão presentes no nosso cotidiano, por exemplo, quando fazemos uso de informações digitalizadas, tais como assistir um programa de tv, falar ao telefone, ouvir um CD/DVD de música, navegar na internet, etc..

A mais importante revolução na teoria dos códigos corretores de erros se deu na década de 80, quando foram introduzidos ferramentas de curvas algébricas para a construção de códigos lineares (códigos estes que são subespaços vetoriais do espaço vetorial $\mathbb{F}_q^n$, onde $\mathbb{F}_q$ denota um corpo finito com q elementos). Tais códigos foram apresentados por V.D. Goppa em um artigo publicado em 1983 e são conhecidos por Códigos Geométricos de Goppa. Desde sua construção, tal classe de códigos vem sendo amplamente desenvolvida.

Contudo, os estudos dos códigos geométricos de Goppa eram trabalhosos para não especialistas em geometria algébrica. Assim, em 1998, Høholdt, van Lint e Pellikaan propuseram, em [7], um método alternativo ao de Goppa para a construção de tais códigos. Em vez de usarem conhecimentos sobre curvas algébricas, os autores utilizaram noções elementares de álgebra linear e teoria de semigrupos. Foram introduzidos os conceitos de Função Ordem e Função Peso, e os códigos construídos sobre $\mathbb{F}$-álgebras, a partir destas

funções, os autores deram o nome de Códigos de Avaliação.

Nesta altura se imaginava que esta teoria poderia gerar novos códigos. Porém, em [11], Matsumoto provou que tais códigos são um caso particular dos códigos geométricos de Goppa, isto é, os códigos de Goppa pontuais.

Nesta dissertação, estamos interessados em apresentar o resultado central de Matsumoto sobre as $\mathbb{F}$-álgebras munidas de função peso. Na verdade, vamos ver como Matsumoto provou que estas $\mathbb{F}$-álgebras são nada mais que os anéis de coordenadas afim de curvas algébricas (neste texto, curva algébrica significa curva algébrica afim absolutamente irredutível e não singular) com um ponto no infinito e que os códigos de avaliação construídos sobre elas são códigos geométricos de Goppa pontuais. Para tanto, este texto está dividido em três capítulos e dois apêndices, estruturados da seguinte forma:

O primeiro capítulo é dedicado à apresentação dos conceitos básicos da teoria de códigos de Goppa. Nele, definimos o que são os códigos corretores de erros, os corpos de funções algébricas sobre uma variável e os códigos geométricos de Goppa, tendo como um dos principais resultados o toerema de Riemann-Roch. Este capítulo auxilia o leitor como referência quanto aos resultados e a terminologia empregada nos capítulos seguintes.

No segundo capítulo introduziremos os conceitos de funções ordem e peso afim de construir os códigos de avaliação e de determinar uma cota inferior para a distância mínima do seu código dual, e apresentaremos uma conexão entre estes códigos, construídos sobre determinadas álgebras, e os códigos geométricos de Goppa pontuais.

No capítulo 3, veremos algumas importantes características das $\mathbb{F}$-álgebras munidas de função peso. Características que nos permitirão concluir que os códigos de avaliação construídos sobre elas são códigos geométricos de Goppa pontuais. Ao final deste, vamos apresentar alguns exemplos a fim de ilustrar os resultados obtidos neste e nos capítulos anteriores.

Para finalizar esta dissertação, apresentamos dois apêndices. O primeiro consiste em expor os resultados clássicos de álgebra comutativa utilizados ao longo do texto. No segundo, fornecemos as definições e os resultados básicos sobre curvas algébricas necessários à compreensão deste trabalho.

É importante comentar que os resultados desta dissertação foram generalizados por Carvalho, Munuera, Silva e Torres, em [2]. Nele é introduzido uma versão mais "abrangente" da definição de função ordem (peso) com o objetivo de obter construções alternativas dos códigos geométricos de Goppa, utilizando-se de métodos elementares.

CAPÍTULO 1

Preliminares

Neste capítulo iremos introduzir as definições e os conceitos básicos da teoria de corpos de funções algébricas e descreveremos, a partir desta, a construção de códigos algébricos geométricos propostos por Goppa, códigos também conhecidos como Códigos Geométricos de Goppa. Todo este capítulo foi escrito baseado no livro "*Algebraic function fields and codes*", referência [12], isto é, todos os resultados e definições citados aqui podem ser encontrados em tal referência. Contúdo, nos propusemos à apresentar algumas das demosntrações dos resultados mais reelevantes para esta dissertação.

1.1 Códigos

Nesta seção apresentaremos algumas 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 de *alfabeto* cujos elementos são as n-uplas $a = (a_1, ..., a_n)$, com $a_i \in \mathbb{F}_q$.

Para $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ 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

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

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-código**. *Chamamos* n *o comprimento de* C *e* $dimC$ *(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 $d(a,b) = d(a-b,0) = w(a-b)$ e C é um espaço linear, a distância mínima é equivalente a

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

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*

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

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,

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

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 dos códigos algébricos é o de construir, sobre um alfabeto fixado $\mathbb{F}_q^n$, códigos cujas dimensão 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 parametros 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, estudaremos as ferramentas necessárias para a construção dos códigos geométricos 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 $\tilde{K} = \{z \in F | z \text{ é algébrico sobre } K\}$ é um subcorpo de F chamado de *corpo de constantes* de $F|K$. Mais ainda, $F|\tilde{K}$ é um corpo de funções sobre $\tilde{K}$.

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 $P = \mathcal{O} \backslash \mathcal{O}^*$, 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 $\tilde{K}$ de $F|K$ temos que $\tilde{K} \subseteq \mathcal{O}$ e $P \cap \tilde{K} = \{0\}$. A seguir enunciamos o principal resultado 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:*
a) P é um ideal principal.
b) 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 $u \in \mathcal{O}^*$.
c) $\mathcal{O}$ 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. *a) 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;*
b) $\mathbb{P}_F := \{P : P$ 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. *Uma* **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 sobrejetiva 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, definindo $v_P(z) := n$ e $v_P(0) := \infty$, segue:

Teorema 1.9. *Seja $F|K$ um corpo de funções.*
a) Para qualquer lugar $P \in \mathbb{P}_F$, a função v_P definida acima é uma valorização discreta de $F|K$. Mais ainda:

$$\mathcal{O}_P = \{z \in F | v_P(z) \geq 0\},$$
$$\mathcal{O}_P^* = \{z \in F | v_P(z) = 0\},$$
$$P = \{z \in F | v_P(z) > 0\}.$$

Um elemento $x \in F$ é um elemento primo de P se e só se $v_P(x) = 1$
b) Reciprocamente, supondo que v é uma valorização discreta de $F|K$, então o conjunto $P = \{z \in F | v(z) > 0\}$ é um lugar de $F|K$ e $\mathcal{O}_P = \{z \in F | v_P(z) \geq 0\}$ é o anel de valorização correspondente.
c) 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 de 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, $\tilde{K}$ 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 [12], proposição I.1.14)

Uma importante descrição dos elementos de $\mathbb{P}_F$ é dada a partir da aplicação 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 z se e somente se $v_P(z) > 0$; P é um* **polo** *de z se e somente se $v_P(P) < 0$. Se $v_P(z) = m > 0$, P é um zero de z de ordem m; se $v_P(z) = -m < 0$, P é um polo de z de ordem m.*

A seguir, nos concentraremos 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 $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Isto nos permite afirmar:

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 polo. Em particular $\mathbb{P}_F \neq \emptyset$.*

Dem. 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 $v_P(z) > 0$ e logo P é um zero de z. Analogamente, existe um lugar Q que é um zero de z^{-1}. Logo, Q é um polo de z. ∎

O seguinte resultado, conhecido como Teorema da Aproximação Fraca, estabelece que se $v_1, \ldots, v_n$ são valorizações discretas de $F|K$ duas a duas distintas, $z \in F$ e se sabemos os valores $v_1(z), \ldots, v_{n-1}(z)$, então não podemos concluir nada a respeito de $v_n(z)$.

Teorema 1.14. Teorema da Aproximação Fraca (T.A.F.)
Seja $F|K$ um corpo de funções, $P_1, \ldots, P_n \in \mathbb{P}_F$, lugares dois a dois distintos de $F|K$, $x_1, \ldots, x_n \in F$ e $r_1, \ldots, r_n \in \mathbb{Z}$. Então existe algum $x \in F$ tal que $v_{P_i}(x - x_i) = r_i$ para $i = 1, \ldots, n$.

Vimos que se $x \in F$ é transcendente sobre K então este possui zeros e polos. O próximo resultado, que é uma consequência (não trivial) do T.A.F., nos permite, de alguma forma, concluir algo a respeito da quantidade de zeros e polos de x.

Proposição 1.15. *Em um corpo de funções $F|K$, qualquer elemento não nulo $x \in F$ possui uma quantidade finita de zeros e polos.*

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

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

Assim, se x é algébrico sobre K então, como $\tilde{K} \cap P = \{0\}$, 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. ∎

1.2.2 Corpos de funções racionais

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

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

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

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

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

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

cujo ideal maximal é

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

Este é chamado de *lugar 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). 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

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

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_∞ definidos acima.*

1.2.3 Divisores

Nesta subseção apresentaremos a definição de divisores de um corpo de funções e veremos alguns resultados importantes a teoria de corpos de funções.

No que segue, $F|K$ denotará um corpo de funções algébricas 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 $\mathcal{D}_F$ e é 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 nulos.

O *suporte* de D é definido por

$$suppD := \{P \in \mathbb{P}_F; n_P \neq 0\}.$$

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 n_P nulos.

Dados $Q \in \mathbb{P}_F$ e $D \in \mathcal{D}_F$, definimos $v_Q(D) := n_Q$, logo

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

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

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

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

O *grau* de um divisor é definido por:

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

e isto fornece um homomorfismo de $\mathcal{D}_F$ em $\mathbb{Z}$.

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 denotemos por Z e N o conjunto dos zeros e pólos de x em $\mathbb{P}_F$. Então definimos:*

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

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

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

Definiremos agora um espaço vetorial que é de 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 a A, como sendo o conjunto*

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

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

Observação 1.20. *$\mathcal{L}(0) = K$; $\mathcal{L}(A) \neq \{0\}$ se, e somente se, existe $A' \sim A$ com $A' \geq 0$; se $A < 0$ então $\mathcal{L}(A) = \{0\}$; e se $A' \sim A$ então $\mathcal{L}(A)$ é isomorfo (como K-espaço vetorial) a $\mathcal{L}(A')$.*

Dado um espaço vetorial V, denotemos 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 $\mathcal{L}(A)$.

Proposição 1.22. *Para qualquer divisor $A \in \mathcal{D}_F$, o espaço $\mathcal{L}(A)$ é um K-espaço vetorial de dimensão finita. Mais precisamente se $A = A_+ - A_-$ com os divisores positivos A_+ e A_- então*

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

Definição 1.23. *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, essencialmente, uma relação entre o número de zeros e o número pólos (contando com a respectiva ordem) de um elemento não-nulo de F.

Teorema 1.24. *Qualquer divisor principal tem grau zero. Mais precisamente, dado $x \in F\backslash K$, temos que*

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

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

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

É suficiente mostrar que $n \leq grau\ B$. Escolha uma base $u_1, \ldots, u_n$ de $F|K(x)$ e um divisor $C \geq 0$ tal que $(u_i) \geq -C$ para $i = 1, \ldots, n$. 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 L.I. sobre K, devido ao fato de $x^i \in K(x)$ para $i = 1, \ldots, l$ serem L.I. sobre K e $u_1, \ldots, u_n$ serem L.I. 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 consequências:

Corolário 1.25. *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 1.26. *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 1.27. *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 $grau\ A - dim\ A + 1 = 0$, concluindo que $g \geq 0$. Um primeiro resultado a respeito do gênero de um corpo de funções é o seguinte:

Teorema 1.28. (Teorema de Riemann) *Seja $F|K$ um corpo de funções de gênero g.*
a) Para qualquer divisor $A \in \mathcal{D}_F$, temos $dim\ A \geq grau\ A + 1 - g$;

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 genero g.

Definição 1.29. *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 1.30. *Um* **adele** *de $F|K$ é uma aplicação*

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

tal que $\alpha_P \in \mathcal{O}_P$ 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 1.31. *Para $A \in \mathcal{D}_F$ definimos*

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

É fácil ver que este conjunto é um K-subespaço vetorial de $\mathcal{A}_F$.

O próximo resultado nos diz que apezar de $\mathcal{A}_F, \mathcal{A}_F(A)$ e F terem dimensão infinita o quociente $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ tem dimensão finita sobre K.

Teorema 1.32. *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 1.33. *Um* **diferencial de Weil** *de $F|K$ é uma aplicação K-linear $\omega : \mathcal{A}_F \longrightarrow K$ que se anula em $\mathcal{A}_F(A) + F$ para algum divisor $A \in \mathcal{D}_F$. Chamamos*

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

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

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

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 vetrorial unidimensional sobre F. Mais ainda, para $A \in \mathcal{D}_F$, temos que $dim\Omega_F = i(A)$.

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

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

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 1.34. *a) 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* $A \leq (\omega)$*.*
b) Para $0 \neq \omega \in \Omega_F$ *e* $P \in \mathbb{P}_F$ *definimos* $v_P(\omega) := v_P((\omega))$*.*
c) Um lugar P *é dito um zero (respectivamente pólo) de* ω *se* $v_P(\omega) > 0$ *(respectivamente* $v_P(\omega) < 0$*).* ω *é chamado* **regular** *em* P *se* $v_P(\omega) \geq 0$ *e* ω *é dito ser regular (ou holomorfico) se* P *é regular para qualquer lugar* $P \in \mathbb{P}_F$*.*
d) 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 1.33 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 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 1.35. *Seja* A *um divisor arbitrário e* $W = (\omega)$ *um divisor canônico de* $F|K$*. Então a aplicação*

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

é um isomorfismo de K*-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 Algébricas.

Teorema 1.36. (Teorema de Riemann-Roch)
Seja W *um divisor canônico de* $F|K$*. Então, para qualquer divisor* $A \in \mathcal{D}_F$ *temos*

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

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

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

■

Corolário 1.37. *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 1.38. *Se A é um divisor de $F|K$ de grau $A \geq 2g - 1$ então*

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

Vejamos agora algumas consequências do Teorema de Riemann-Roch.

O primeiro resultado é um melhoramento do Teorema da Aproximação Fraca.

Teorema 1.39. (Teorema da Aproximação Forte) *Seja $S \subsetneqq \mathbb{P}_F$, um subconjunto próprio de $\mathbb{P}_F$ e $P_1, \ldots, P_n \in S$. 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*

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

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

Proposição 1.40. *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 1.41. *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 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 1.42. (Teorema das Lacunas de Weierstrass) *Suponha que $F|K$ tem gênero $g > 0$ e P é um lugar de grau um. Então existem exatamente g lacunas $i_1 < ... < i_g$ 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 1.43. *Seja $P \in \mathbb{P}_F$*
a) Para $x \in F$ seja $i_P(x) \in \mathcal{A}_F$ o adele cuja a P-componente é x e o restantes dos componentes é 0.
b) Para um diferencial de Weil $\omega \in \Omega_F$ definimos sua **componente local** *$\omega_P : F \longrightarrow K$ como sendo $\omega_P(x) := \omega(i_P(x))$.(Claramente, ω_P é K-linear)*

Sobre as componentes locais temos os seguintes resultados:

Proposição 1.44. *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 1.45. *a) Seja $\omega \neq 0$ um diferencial de Weil de $F|K$ e $P \in \mathbb{P}_F$. Então*

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

Em particular $\omega_P \neq 0$.
b) Se $\omega, \omega' \in \Omega_F$ e $\omega_P = \omega'_P$ para algum $P \in \mathbb{P}_F$, então $\omega = \omega'$.

Disto, segue, 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

Esta seção é dedicada à construção dos códigos geométricos de Goppa. Neste, $\mathbb{F}_q$ denota um corpo 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 $supp\ G \cap supp\ D = \emptyset$.

Definição 1.46. *O* **código geométrico de Goppa** *$C_{\mathcal{L}}(D, G)$ associados aos divisores D e G é definido por*

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

Obeserve que tal definição faz sentido: para $x \in \mathcal{L}(G)$ temos que $v_{P_i}(x) \geq 0$, para todo $i = 1, \ldots, n$, 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 $x(P_i) \in \mathbb{F}_q$.

Consideremos a *aplicação avaliação*

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

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 uma cota inferior para a distância mínima d.

Teorema 1.47. *$C_{\mathcal{L}}(D, G)$ é um $[n, k, d]$-código tal que*

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

Dem. Considerando a aplicação $av_D : \mathcal{L}(G) \longrightarrow \mathbb{F}_q^n$, definida acima, temos que $\mathcal{L}(G)/Ker(av_D)$ é isormorfo a $Im(av_D) = C_{\mathcal{L}}(D, G)$. Como $Ker(av_D) = \{x \in \mathcal{L}(G); v_{P_i}(x) > 0 \text{ para } i = 1, \ldots, n\} = \mathcal{L}(G - D)$ 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 $w(x)$. Assuma que $C_{\mathcal{L}}(D, G) \neq \{0\}$. Escolha $x \in \mathcal{L}(G)$ tal que $w(av_D(x)) = d$. 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 $x \in \mathcal{L}(G - (P_{i_1} + ... + P_{i_{n-d}}))\backslash\{0\}$, ou seja, $dim(\mathcal{L}(G - (P_{i_1} + ... + P_{i_{n-d}}))) \geq 1$. Portanto, do corolário 1.25, segue que

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

ou seja, $d \geq n - grau\ G$. ∎

Uma consequência deste teorema é o seguinte resultado.

Corolário 1.48. *Suponha que grau de G é estritamente menor que n. Então a aplicação avaliação $av_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D, G)$ é injetiva e ainda:*
a) $C_{\mathcal{L}}(D, G)$ é um $[n, k, d]$-código com $d \geq n - grauG$ e $k = dimG \geq grauG + 1 - g$. Logo $k + d \geq n + 1 - g$.

b) Se $2g-2 < grau\, G < n$ *então* $k = grau\, G + 1 - g$.
c) Se $\{x_1, \ldots, x_k\}$ *é uma base de* $\mathcal{L}(G)$ *então a matriz*

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

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

Observe que a cota inferior para a distância mínima dada no item (a) deste corolário é muito parecida com o 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. Isto nos motiva a dar a seguinte definição:

Definição 1.49. *O inteiro* $d^* := n - grau\ G$ *é chamado de* **distância designada** *do código* $C_{\mathcal{L}}(D, G)$.

O Teorema 1.47 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 $d^* > 0$, temos que $d^* = d$ 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 1.50. *Seja* G *e* $D = P_1 + ... + P_n$ *divisores onde* P_i *são dois a dois distintos,* $grau\ P_i = 1$ *e* $suppD \cap suppG = \emptyset$. *Então definimos o código* $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ *por*

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

Um resultado análogo ao Teorema 1.47 é o seguinte:

Teorema 1.51. $C_\Omega(D, G)$ *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 1.52. *Os códigos $C_{\mathcal{L}}(D,G)$ e $C_{\Omega}(D,G)$ são duais um do outro, isto é*

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

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

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

De fato, como *grau* $P = 1$, podemos escrever $x = a + y$ onde $a = x(P) \in \mathbb{F}_q$ e $v_P(y) \geq 1$. 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 $v_P(\omega) \geq -1$, $v_P(y) \geq 1$ e proposição 1.45).

Mostremos 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 1.44 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 $P \in \mathbb{F} \setminus \{P_1, \ldots, P_n\}$ temos que $v_P(x) \geq -v_P(\omega)$. Logo, da proposição 1.45, segue que $\omega_P(x) = 0$. Assim,

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

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

Agora mostremos que a dimensão dos códigos $C_{\Omega}(D,G)$ e $C_{\mathcal{L}}(D,G)^{\perp}$ são iguais. Pelos teoremas 1.47 e 1.51 e o Teorema de Riemann-Roch, temos

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

■

Observação 1.53. *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 $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$ para $i = 1, ..., n$. Então*

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

1.4 Subanéis de um corpo de funções

O objetivo desta seção é de apresentar conceitos e resultados que serão fundamentais no último capítlulo desta dissertação. No que segue, $F|K$ denota um corpo de funções com corpo de constantes K.

Definição 1.54. *Um* **subanel** *de $F|K$ é um anel 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 1.55. *Para $\emptyset \neq S \subsetneqq \mathbb{P}_F$ seja*

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

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 holomorfico; 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 1.56. *Seja R um subanel de $F|K$ e $S(R) := \{P \in \mathbb{P}_F \mid R \subseteq \mathcal{O}_P\}$. 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.

Dem. i) Como R não é um corpo, existe um ideal próprio I de R. Do teorema 1.12, existe $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$. Logo, $S(R) \neq \emptyset$. Por outro lado, considere $x \in R$ transcendente sobre K. Então, do colorário 1.13, segue que $S(R) \neq \mathbb{P}_F$.

ii) Como $R \subseteq \mathcal{O}_{S(R)}$ e $\mathcal{O}_{S(R)}$ é integralmente fechado, segue que $\overline{R} \subseteq \mathcal{O}_{S(R)}$. Agora, considere $z \in \mathcal{O}_{S(R)}$. Afirmamos que $z^{-1}R[z^{-1}] = R[z^{-1}]$. De fato, suponha que isto é falso, isto é, $z^{-1}R[z^{-1}]$ é um ideal próprio em $R[z^{-1}]$. Pelo teorema 1.12, podemos encontrar

$Q \in \mathbb{P}_F$ tal que $R[z^{-1}] \subseteq \mathcal{O}_Q$ e $z^{-1} \in Q$. Assim, temos que $Q \in S(R)$ e $z \notin \mathcal{O}_Q$, o que uma contradiçao com o fato de $z \in \mathcal{O}_{S(R)}$. Logo, existem $a_0, ..., a_s \in R$ tais que

$$1 = z^{-1} \sum_{i=0}^{s} a_i (z^{-1})^i.$$

Multiplicando esta equação por z^{s+1}, obtemos

$$z^{s+1} - z^s \sum_{i=0}^{s} a_i z^{s+1-i} = 0.$$

Logo, z é inteiro sobre R. Portanto, $\mathcal{O}_{S(R)} \subseteq \overline{R}$. ∎

Uma consequência direta deste teorema é o seguinte resultado.

Corolário 1.57. *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 1.58. *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 teroema 1.6.*

CAPÍTULO 2

Códigos de Avaliação

Neste capítulo apresentaremos uma conexão entre códigos de avaliação sobre uma determinada álgebra e códigos geométricos de Goppa pontuais e determinaremos cotas inferiores para as distâncias mínimas dos códigos avaliados e seus códigos duais. Para isso, introduziremos os conceitos de função ordem, função peso e semigrupos.

No que segue, $\mathcal{R}$ denotará uma $\mathbb{F}$-álgebra, isto é, $\mathcal{R}$ é um anel comutativo com unidade contendo um corpo $\mathbb{F}$. Denotaremos também $\mathbb{N}_0$ como sendo o conjunto dos números inteiros não-negativos e o símbolo $-\infty$ é menor que n, para todo $n \in \mathbb{N}_0$.

2.1 Funções ordem (peso)

Definição 2.1. *Seja $\mathcal{R}$ uma $\mathbb{F}$-álgebra. Uma aplicação $\rho : \mathcal{R} \to \mathbb{N}_0 \cup \{-\infty\}$ é chamada uma* ***função ordem*** *sobre $\mathcal{R}$ se são satisfeitas as seguintes condições:*

(1) $\rho(f) = -\infty$ se, e somente se, $f = 0$;
(2) $\rho(\lambda f) = \rho(f)$ para todo $\lambda \in \mathbb{F}\backslash\{0\}$;
(3) $\rho(f+g) \leq max\{\rho(f), \rho(g)\}$ com igualdade quando $\rho(f) \neq \rho(g)$;
(4) Se $\rho(f) < \rho(g)$ e $h \neq 0$, então $\rho(fh) < \rho(gh)$;
(5) Se $\rho(f) = \rho(g)$, então existe $\lambda \in \mathbb{F}$ tal que $\rho(f - \lambda g) < \rho(g)$.

A função ρ é chamada ***função peso*** *se além de satisfazer as condições anteriores também satisfazer:*

(6) $\rho(fg) = \rho(f) + \rho(g)$*, para todo* $f, g \in \mathcal{R}$.

Observação 2.2. *Uma consequência imediata da definição de função ordem é que se ρ é uma função ordem de uma $\mathbb{F}$-álgebra $\mathcal{R}$ e $\mathcal{R}'$ é um $\mathbb{F}$-subálgebra de $\mathcal{R}$ então $\rho_{|_{\mathcal{R}'}}$ também é uma função ordem de $\mathcal{R}'$.*

Exemplo 2.3. *A função $\rho(f) = grau(f)$ para $f \in \mathcal{R} = \mathbb{F}[x]$ é uma função peso.*

O resultado abaixo nos traz algumas propriedades para a função ordem.

Lema 2.4. *Seja ρ uma função ordem em $\mathcal{R}$. Então,*
(1) Se $\rho(f) = \rho(g)$, então $\rho(fh) = \rho(gh)$ para todo $h \in \mathcal{R}$.
(2) Se $f \in \mathcal{R}\backslash\{0\}$, então $\rho(1) \leq \rho(f)$.
(3) $\mathbb{F} = \{f \in \mathcal{R} | \rho(f) \leq \rho(1)\}$.
(4) Se $\rho(f) = \rho(g)$, então existe um único $\lambda \in \mathbb{F}$ tal que $\rho(f - \lambda g) < \rho(g)$.

Dem. No transcorrer da demonstração, sempre que colocarmos $(i)^*$, com $1 \leq i \leq 5$, estamos nos referindo aos respectivos itens da definição 2.1

(1) Seja $\rho(f) = \rho(g)$. Então, de $(5)^*$, existe um $\lambda \in \mathbb{F}$ tal que $\rho(f - \lambda g) < \rho(g)$. Logo, de $(4)^*$, para $h \in \mathcal{R}$, temos que $\rho(fh - \lambda gh) < \rho(gh)$. Como $fh = (fh - \lambda gh) + \lambda gh$, temos que $\rho(fh) = \rho(\lambda gh) = \rho(gh)$ por $(3)^*$ e $(2)^*$, respectivamente.

(2) Suponha, por absurdo, que f é um elemento não-nulo de $\mathcal{R}$ tal que $\rho(f) < \rho(1)$. Então, de $(4)^*$, a seqüência $\rho(1) > \rho(f) > \rho(f^2) > ...$ é estritamente decrescente, contradizendo o fato de $\mathbb{N}_0 \cup \{\infty\}$ ser bem-ordenado. Logo, $\rho(1) \leq \rho(f)$.

(3) Pelas condições $(1)^*$ e $(2)^*$ temos que $\mathbb{F} \subset \{f \in \mathcal{R} | \rho(f) \leq \rho(1)\}$. Agora, seja $f \neq 0$ tal que $\rho(f) \leq \rho(1)$, então, do item anterior, temos $\rho(f) = \rho(1)$. Logo, de $(5)^*$, existe um $\lambda \in \mathbb{F}$ tal que $\rho(f - \lambda 1) < \rho(1)$. Portanto, $f - \lambda = 0$, ou seja, $f \in \mathbb{F}$.

(4) A existência de λ é garantida pela definição de função ordem, assim, provemos a unicidade. Suponha que exista $\lambda, \alpha \in \mathbb{F}$ tal que $\rho(f - \lambda g) < \rho(g)$ e $\rho(f - \alpha g) < \rho(g)$. Temos, de $(3)^*$, que $\rho(f - \lambda g - (f - \alpha g)) < \rho(g)$, ou seja, $\rho((\lambda - \alpha)g) < \rho(g)$. Logo, de $(2)^*$, temos que $\lambda = \alpha$. ■

O próximo resultado nos mostra que uma $\mathbb{F}$-álgebra munida de uma função peso é um domínio.

Proposição 2.5. *Se existe uma função ordem ρ em $\mathcal{R}$, então $\mathcal{R}$ é um domínio de integridade.*

Dem. Suponha que $\mathcal{R}$ não seja um domínio, então existem $f, g \in \mathcal{R}\backslash\{0\}$ tal que $fg = 0$. Sem perda de generalidade, suponha $\rho(f) \leq \rho(g)$. Então, $\rho(f^2) \leq \rho(fg) = \rho(0) = -\infty$. Logo $\rho(f^2) = -\infty$ e portanto $f^2 = 0$. Agora, como $f \neq 0$ então, por (2) do lema anterior, temos $\rho(1) \leq \rho(f)$. Assim, $\rho(f) \leq \rho(f^2) = -\infty$ e logo $f = 0$, absurdo. ∎

Vejamos em um exemplo que a recíproca da proposição anterior é falsa.

Exemplo 2.6. *A $\mathbb{F}$-álgebra $\mathcal{R} = \mathbb{F}[X, Y]/(XY - 1)$ é um domínio, mas não existe função ordem sobre $\mathcal{R}$. De fato, denote por x a classe $X + (XY - 1)$ e y para $Y + (XY - 1)$. Logo, $\mathcal{R} = \mathbb{F}[x] + \mathbb{F}[y]$ e é claro que $x \neq 0$ e $y \neq 0$. Assim, se ρ é uma função ordem em $\mathcal{R}$, então, do lema 2.4 (2), $\rho(1) \leq \rho(x)$ e logo $\rho(y) \leq \rho(xy) = \rho(1)$. Portanto, $\rho(y) = \rho(1)$. Analogamente, $\rho(x) = \rho(1)$. Então, para todo $f \in \mathcal{R}$, temos que $\rho(f) \leq \rho(1)$, ou seja, $\mathcal{R} = \mathbb{F}$, pelo lema 2.4 (3). Isto é uma contradição, pois $x \notin \mathbb{F}$.*

Veremos a seguir que se uma $\mathbb{F}$-álgebra $\mathcal{R}$ é munida de uma função ordem, então existe uma $\mathbb{F}$-base de $\mathcal{R}$, $\mathcal{R}$ visto com um espaço vetorial, com certas propriedades.

Teorema 2.7. *Seja $\mathcal{R}$ uma $\mathbb{F}$-álgebra com função ordem ρ. Assuma que $\mathcal{R} \neq \mathbb{F}$. Então:*
(1) Existe uma $\mathbb{F}$-base $\{f_i : i \in \mathbb{N}\}$ de $\mathcal{R}$ tal que $\rho(f_i) < \rho(f_{i+1})$ para todo $i \in \mathbb{N}$;
(2) Se $f \in \mathcal{R}$ e $f = \lambda_1 f_1 + \cdots + \lambda_i f_i$, com $\lambda_j \in \mathbb{F}$ para $j = 1, ..., i$ e $\lambda_i \neq 0$, então $\rho(f) = \rho(f_i)$;
(3) Seja $l(i, j) := l$ tal que $\rho(f_i f_j) = \rho(f_l)$. Então $l(i, j) < l(i + 1, j)$ para todo i e j;
(4) Seja $\rho_i := \rho(f_i)$. Se ρ é uma função peso então $\rho_{l(i,j)} = \rho_i + \rho_j$.

Dem. (1) Como $\mathcal{R} \neq \mathbb{F}$, existe $f \in \mathcal{R}\backslash\mathbb{F}$. Assim, pelo lema 2.4, $\rho(1) < \rho(f)$. Logo, $\rho(f^n) < \rho(f^{n+1})$ para todo $n \in \mathbb{N}_0$ e portanto, o conjunto de valores de ρ é infinito. Seja $(\rho_i : i \in \mathbb{N})$ uma seqüência crescente de inteiros não-negativos tais que os ρ_i's são todos os valores da função ordem, isto é, $\rho(\mathcal{R}\backslash\{0\}) = \{\rho_i : i \in \mathbb{N}\}$. Assim, para todo $i \in \mathbb{N}$ existe um $f_i \in \mathcal{R}$ tal que $\rho(f_i) = \rho_i$. Logo, pela construção acima, $\rho(f_i) < \rho(f_{i+1})$ para todo i e para todo $f \in \mathcal{R}$ não-nulo existe um índice i com $\rho(f) = \rho(f_i)$. Temos também que $\rho(1) = \rho_1$. Mostremos que o conjunto $\{f_i : i \in \mathbb{N}\} := B$ é uma $\mathbb{F}$-base para $\mathcal{R}$. Segue facilmente da definição 2.1 que B é linearmente independente. Mostremos, então, que B gera $\mathcal{R}$.

Seja $f \in \mathcal{R}$, então existe um $f_k \in B$ tal que $\rho(f_k) = \rho(f)$. Logo, pelo lema 2.4 (4), existe um único $\lambda_k \in \mathbb{F}$ tal que $\rho(f - \lambda_k f_k) < \rho(f_k)$. Novamente, existe um $f_h \in B$, com $h < k$ tal que $\rho(f-\lambda_k f_k) = \rho(f_h)$ e consequentemente existe $\lambda_h \in \mathbb{F}$ tal que $\rho(f-\lambda_k f_k-\lambda_h f_h) < \rho(f_h)$. Continuando esse processo, temos que $\rho(f - \lambda_k f_k - ... - \lambda_1 f_1) < \rho(f_1) = \rho(1)$. Portanto, $\rho(f - \lambda_k f_k - ... - \lambda_1 f_1) = -\infty$, ou seja, $f = \lambda_1 f_1 + ... + \lambda_k f_k$. Portanto B gera $\mathcal{R}$.
(2) Segue de (1) e de (3) da definição 2.1.
(3) Como $\rho(f_i) < \rho(f_{i+1})$ então, $\rho(f_i f_j) < \rho(f_{i+1} f_j)$. Logo, $l(i,j) < l(i+1,j)$.
(4) Como ρ é uma função peso, $\rho_{l(i,j)} = \rho(f_i f_j) = \rho(f_i) + \rho(f_j) = \rho_i + \rho_j$. ■

O próximo resultado nos fornece um procedimento a ser seguido quando buscamos exemplos de funções ordens sobre uma dada $\mathbb{F}$-álgebra.

Teorema 2.8. *Sejam $\mathcal{R}$ uma $\mathbb{F}$-álgebra, $\{f_i : i \in \mathbb{N}\}$ uma $\mathbb{F}$-base do $\mathbb{F}$-espaço vetorial $\mathcal{R}$ com $f_1 = 1$ e $\{\rho_i : i \in \mathbb{N}\}$ uma sequência estritamente crescente de inteiros não negativos. Para cada $i \in \mathbb{N}$ considere L_i o $\mathbb{F}$-subespaço vetorial gerado por $f_1, ..., f_i$ e para cada par (i,j) chame $l(i,j)$ o menor inteiro positvo l tal que $f_i f_j \in L_l$. Seja ρ uma função de $\mathcal{R}$ em $\mathbb{N}_0 \cup \{-\infty\}$ definida por $\rho(0) = -\infty$ e $\rho(f) = \rho_i$ se i é o menor inteiro positivo tal que $f \in L_i$. Se para todo par $(i,j) \in \mathbb{N}^2$ tem-se $l(i,j) < l(i+1,j)$ então ρ é uma função ordem sobre $\mathcal{R}$. Mais ainda, se $\rho_{l(i,j)} = \rho_i + \rho_j$, então ρ é uma função peso.*

Dem. Observe que as condições (1), (2), (3) e (5) seguem diretamente da definição de ρ e do fato que $L_1 \subseteq L_2 \subseteq L_3 \subseteq ...$ são subespaços vetoriais de $\mathcal{R}$. Mostremos, assim, as condições (4) e (6).

Para cada $f \in \mathcal{R}\backslash\{0\}$ associamos um índice $\iota(f)$ que é o menor inteiro positivo tal que $f \in L_{\iota(f)}$. Sejam $f, g \in \mathcal{R}$. Então, existem $\lambda_i, \alpha_i, \beta_i \in \mathbb{F}$ com $\lambda_{\iota(f)} \neq 0$, $\alpha_{\iota(g)} \neq 0$ e $\beta_{\iota(fg)} \neq 0$ tal que

$$f = \sum_{i \leq \iota(f)} \lambda_i f_i;\ g = \sum_{j \leq \iota(g)} \alpha_j f_j \text{ e } fg = \sum_{l \leq \iota(fg)} \beta_l f_l.$$

Existem também $\mu_{ijl} \in \mathbb{F}$ tal que

$$f_i f_j = \sum_{l \leq l(i,j)} \mu_{ijl} f_l$$

e $\mu_{ijl(i,j)} \neq 0$. Logo,

$$fg = (\sum_{i\leq\iota(f)} \lambda_i f_i)(\sum_{j\leq\iota(g)} \alpha_j f_j) = \sum_{i\leq\iota(f)} \sum_{j\leq\iota(g)} \lambda_i\alpha_j f_i f_j = \sum_{i\leq\iota(f)} \sum_{j\leq\iota(g)} \lambda_i\alpha_j \sum_{l\leq l(i,j)} \mu_{ijl} f_l = \sum_{i\leq\iota(f)} \sum_{j\leq\iota(g)} \sum_{l\leq l(i,j)} \lambda_i\alpha_j\mu_{ijl} f_l.$$

Então,

$$\beta_l = \sum_{l(i,j)=l} \lambda_i\alpha_j\mu ijl.$$

Como $l(i,j) < l(i+1,j)$, então $l(i,j) < l(\iota(f),\iota(g))$ se $i < \iota(f)$ ou $j < \iota(g)$. Contudo, se $i = \iota(f)$ e $j = \iota(g)$, temos que $\lambda_i\alpha_j\mu_{ijl(i,j)} = \beta_{\iota(fg)} \neq 0$, e portanto temos que $\iota(fg) = l(\iota(f),\iota(g))$. Logo, dado $f, g, h \in \mathcal{R}$ com $\rho(f) < \rho(g)$ e $h \neq 0$ temos que $\rho(fh) = \rho_{\iota(fh)} = \rho_{l(\iota(f),\iota(h))} < \rho_{l(\iota(g),\iota(h))} = \rho(gh)$, o que prova a condição (4) da definição 2.1.

Agora, se $\rho_{l(i,j)} = \rho_i + \rho_j$, então $\rho(fg) = \rho_{\iota(fg)} = \rho_{l(\iota(f),\iota(g))} = \rho_{\iota(f)} + \rho_{\iota(g)} = \rho(f) + \rho(g)$, verificando a condição (6) da definição 2.1 e portanto provando que ρ é uma função peso. ■

O exemplo abaixo ilustra o teorema anterior.

Exemplo 2.9. *Considere a ordem lexicográfica graduada $\prec$ no conjunto dos monômios $\{X^aY^b \mid a, b \in \mathbb{N}_0\}$, ou seja,*

$$X^aY^b \prec X^cY^d \iff a+b < c+d \text{ ou } a+b = c+d \text{ e } (a,b) \prec_L (c,d),$$

onde $\prec_L$ é a ordem lexicográfica[1]*. Sejam $f_1, f_2, \ldots$ a enumeração do conjunto de monômios tal que $f_i \prec f_{i+1}$ para todo $i \in \mathbb{N}$. Abaixo apresentamos duas matrizes onde uma corresponde ao conjunto dos monômios e a outra corresponde aos respectivos índices, segundo a enumeração acima.*

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
Y^5	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdots$
Y^4	XY^4	$\cdot$	$\cdot$	$\cdot$	$\cdots$
Y^3	XY^3	X^2Y^3	$\cdot$	$\cdot$	$\cdots$
Y^2	XY^2	X^2Y^2	X^3Y^2	$\cdot$	$\cdots$
Y	XY	X^2Y	X^3Y	X^4Y	$\cdots$
1	X	X^2	X^3	X^4	$\cdots$

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
16	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdots$
11	17	$\cdot$	$\cdot$	$\cdot$	$\cdots$
7	12	18	$\cdot$	$\cdot$	$\cdots$
4	8	13	19	$\cdot$	$\cdots$
2	5	9	14	20	$\cdots$
1	3	6	10	15	$\cdots$

[1]Dados $(a,b),(c,d) \in \mathbb{N}^2$ temos que $(a,b) \prec_L (c,d)$ se, e somente se, $a < c$ ou $a = c$ e $b < d$.

Seja $\mathcal{R} := \mathbb{F}[X,Y]$ *e* $f = \lambda_1 f_1 + ... + \lambda_n f_n$ *em* $\mathcal{R}$. *Defina* $\rho(0) = -\infty$ *e* $\rho(f) = n-1$ *se* $\lambda_n \neq 0$. *É fácil ver que* ρ *é uma função ordem sobre* $\mathcal{R}$. *Observe que,* $f_9 = X^2Y$, $f_5 = XY$ *e* $f_5 f_9 = X^3Y^2 = f_{19}$. *Logo* $l(5,9) = 19$.

Na seguinte proposição veremos que para uma classe específica de $\mathbb{F}$-álgebras existem funções pesos.

Proposição 2.10. *Seja* I *o ideal em* $\mathbb{F}[X,Y]$ *gerado por um polinômio da forma* $X^aY^c + uY^{b+c} + G$ *onde* $0 \neq u \in \mathbb{F}$, $G \in \mathbb{F}[X,Y]$, $grau_X(G) = d < a$, $grau(G) < b+c$, $b < a$ *e* $mdc(a,b) = 1$. *Seja* $S = \mathbb{F}[X,Y]/I$. *Denote as classes resíduais de* X, Y *e* G *por* x, y *e* g, *respectivamente. Seja* $\mathcal{R}$ *o espaço vetorial gerado por* $\{x^\alpha y^\beta | \alpha, \beta \in \mathbb{N}_0, \alpha < a \text{ e } c\alpha \leq (a-d)\beta\}$. *Então* $\mathcal{R}$ *é uma* $\mathbb{F}$*-álgebra com uma função peso* ρ *tal que* $\rho(x) = b$ *e* $\rho(y) = a$.

Dem. Observe que $x^a y^c = -uy^{b+c} - g$, então temos que $x^a y^c$ é uma combinação linear de $x^\alpha y^\beta$ com $\alpha < a$, pois $grau_X(G) < a$. Logo, por indução, temos que o conjunto $\{x^\alpha y^\beta | \alpha, \beta \in \mathbb{N}_0, \alpha < a \text{ ou } \beta < c\}$ forma uma base de S sobre $\mathbb{F}$ e portanto, o conjunto $\{x^\alpha y^\beta | \alpha, \beta \in \mathbb{N}_0, \alpha < a \text{ e } c\alpha \leq (a-d)\beta\}$ é uma base de $\mathcal{R}$. Assim, seja $(f_i : i \in \mathbb{N})$ uma enumeração dos elementos da base de $\mathcal{R}$. Se $f_i = x^\alpha y^\beta$, com $\alpha < a$ e $c\alpha \leq (a-d)\beta$, então defina $\rho_i = \alpha b + \beta a$. Então, como $mdc(a,b) = 1$, a aplicação $(\alpha, \beta) \mapsto \alpha b + \beta a$ é injetiva no domínio $\{(\alpha, \beta) \in \mathbb{N}_0 | \alpha < a\}$. Logo, se $i \neq j$ então temos que $\rho_i \neq \rho_j$. Portanto, podemos assumir uma enumeração tal que a sequência $(\rho_i : i \in \mathbb{N})$ é estritamente crescente.

Seja $L_l = \langle f_1, ..., f_l \rangle$. Provemos que para todo i, j existe um inteiro não-negativo l tal que $f_i f_j \in L_l$. Daí, segue que $\mathcal{R}$ é uma $\mathbb{F}$-álgebra. Além disso, mostremos que se $l(i,j)$ é o menor inteiro não-negativo l tal que $f_i f_j \in L_l$ então $\rho_{l(i,j)} = \rho_i + \rho_j$. Logo, teremos, do teorema 2.8, que existe uma função peso ρ em $\mathcal{R}$ tal que $\rho(x^\alpha y^\beta) = \alpha b + \beta a$.

Sejam $f_i = x^\alpha y^\beta$ e $\rho_i = \alpha b + \beta a$ com $\alpha < a$ e $c\alpha \leq (a-d)\beta$, e $f_j = x^\gamma y^\delta$ e $\rho_j = \gamma b + \delta a$ com $\gamma < a$ e $c\gamma \leq (a-d)\delta$. Então $f_i f_j = x^{\alpha+\gamma} y^{\beta+\delta}$ e $\rho_i + \rho_j = (\alpha+\gamma)b + (\beta+\delta)a$ com $c(\alpha+\gamma) \leq (a-d)(\beta+\delta)$.

(1) Se $\alpha + \gamma < a$ então $f_i f_j$ é um elemento da base de $\mathcal{R}$ e portanto $f_{l(i,j)} = f_i f_j$ e $\rho_{l(i,j)} = \rho_i + \rho_j$.

(2) Se $\alpha + \gamma \geq a$, então existe $\epsilon \in \mathbb{N}_0$, $\epsilon < a$, tal que $\alpha + \gamma = a + \epsilon$. Assim,

$$ca \leq c(\alpha+\gamma) \leq (a-d)(\beta+\delta) \leq a(\beta+\delta).$$

Logo, $\beta+\delta = c+\eta$ para algum $\eta \in \mathbb{N}_0$ e $c(a+\epsilon) \leq (a-d)(c+\eta)$. Portanto $c(d+\epsilon) \leq (a-d)\eta$. Como $\epsilon < a$ segue que $c\epsilon \leq (a-d)(b+c+\eta)$. Além disso,

$$f_i f_j = x^a y^c x^\epsilon y^\eta = -ux^\epsilon y^{b+c+\eta} - x^\epsilon y^\eta g.$$

Então, segue que o termo $x^\epsilon y^{b+c+\eta}$ é um elemento f_l da base de $\mathcal{R}$ e

$$\rho_i + \rho_j = (\alpha+\gamma)b + (\beta+\delta)a = \epsilon b + (b+c+\eta)a = \rho_l.$$

Mostremos agora que $x^\epsilon y^\eta g \in L_{l-1}$, pois assim teremos que $f_i f_j \in L_l$ e $f_i f_j \notin L_{l-1}$ e portanto $l(i,j) = l$.

Sabemos que um monômio de G, com coeficientes não-nulos, é da forma $X^\kappa Y^\lambda$ com $\kappa \leq d$ e $\kappa + \lambda < b + c$, pois $grau_X(G) = d$ e $grau(G) < b + c$. Assim, provemos por indução sobre ϵ que:

$$\begin{gathered}\text{Se } (\epsilon,\eta),(\kappa,\lambda) \in \mathbb{N}_0^2,\ \epsilon < a,\ c(\epsilon+d) \leq (a-d)\eta,\ \kappa \leq d,\\ \kappa+\lambda < b+c \text{ e } \rho_l = \epsilon b + (b+c+\eta)a \text{ então } x^{\epsilon+\kappa}y^{\eta+\lambda} \in L_{l-1}.\end{gathered}$$

Disto, resulta que $x^\epsilon y^\eta g \in L_{l-1}$.

(2.i) Se $\epsilon+\kappa < a$, então $x^{\epsilon+\kappa}y^{\eta+\lambda}$ é um elemento da base de $\mathcal{R}$, pois $c(\epsilon+\kappa) \leq (a-d)(\eta+\lambda)$. Além disso, como $b < a$, por hipótese, e $\kappa+\lambda < b+c$, temos que

$$(\epsilon+\kappa)b + (\eta+\lambda)a = \epsilon b + (\kappa b + \lambda a) + \eta a < \epsilon b + (b+c+\eta)a = \rho_l.$$

Portanto, $x^{\epsilon+\kappa}y^{\eta+\lambda} \in L_{l-1}$.

(2.ii) Se $\epsilon + \kappa \geq a$ então existe $\epsilon' \in \mathbb{N}_0$ tal que $\epsilon + \kappa = a + \epsilon'$. Observe que $\epsilon' < \epsilon$, pois $\kappa \leq d < a$. Agora, como

$$ca \leq c(\epsilon+\kappa) \leq (a-d)(\eta+\lambda) \leq a(\eta+\lambda)$$

temos que existe $\eta' \in \mathbb{N}_0$ tal que $\eta + \lambda = c + \eta'$ e $c\epsilon' \leq (a-d)\eta'$. Temos também que

$$x^{\epsilon+\kappa}y^{\eta+\lambda} = x^a y^c x^{\epsilon'} y^{\eta'} = -ux^{\epsilon'}y^{b+c+\eta'} - x^{\epsilon'}y^{\eta'}g.$$

Então, segue que o termo $x^{\epsilon'}y^{b+c+\eta'}$ é um elemento $f_{l'}$ da base de $\mathcal{R}$ e

$$\rho_{l'} = \epsilon' b + (b+c+\eta')a = (a+\epsilon')b + (c+\eta')a = (\epsilon+\kappa)b + (\eta+\lambda)a < \rho_l$$

como feito em (2,i). Assim, temos que $l' < l$ e, por indução, $x^{\epsilon'}y^{\eta'}g \in L_{l'-1}$. Portanto, $x^{\epsilon+\kappa}y^{\eta+\lambda} \in L_{l-1}$. Logo existe uma fução peso ρ em $\mathcal{R}$ tal que $\rho(x^\alpha y^\beta) = \alpha b + \beta a$.

■

Vejamos um exemplo que ilustra a proposição anterior.

Exemplo 2.11. *Considere a curva plana $\mathcal{X}$ definida por $X^5 - Y^4 - Y = 0$ sobre o corpo $\mathbb{F}_{16}$. Note que esta equação é da forma $X^aY^c + uY^{b+c} + G(X,Y) = 0$, como na proposição anterior, onde $a = 5$, $b = 4$, $c = d = 0$, $G(X,Y) = -Y$ e $u = -1$. Seja $\mathcal{R}$ a $\mathbb{F}_{16}$-álgebra dada por $\mathcal{R} = \mathbb{F}_{16}[X,Y]/(X^5 + Y^4 + Y)$, isto é, $\mathcal{R}$ é o anel de coordenadas de $\mathcal{X}$. Denotemos as classes residuais correspondentes a X e Y por x e y, respectivamente. Então, da proposição anterior, $\{x^\alpha y^\beta : \alpha < 5\}$ é uma base de $\mathcal{R}$ e $\rho(x^\alpha y^\beta) = 4\alpha + 5\beta$ gera uma função peso sobre $\mathcal{R}$. Seja a sequência $(f_l : l \in \mathbb{N})$ uma enumeração crescente dos elementos da base, com relação seus pesos. Então os primeiros termos da base com seus respectivos pesos são:*

f_l :	1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	x^3y	x^2y^2	xy^3	y^4	x^4y	...
ρ_l :	0	4	5	8	9	10	12	13	14	15	16	17	18	19	20	21	...

Logo, $f_4 = x^2$, $f_7 = x^3$ e $f_4 f_7 = x^5 = y^4 + y = f_{15} + f_3$. Portanto $l(4,7) = 15$. Note também que $\rho_l = \rho(f_l) = l + 5$, para todo $l \geq 7$.

2.2 Códigos de avaliação e distância mínima dual.

Nesta seção estudaremos os códigos de avaliação e daremos uma conexão entre os códigos avaliados sobre uma determinada álgebra e os códigos geométricos de Goppa pontuais. Também, neste, determinaremos uma cota inferior para as distâncias mínimas dos códigos duais aos códigos avaliados.

Sejam $\mathbb{F}_q$ um corpo finito com q elementos e $\mathcal{R}$ uma $\mathbb{F}_q$-álgebra com uma função ordem ρ. Sejam $(f_i : i \in \mathbb{N})$ uma base de $\mathcal{R}$ sobre $\mathbb{F}_q$ tal que, para cada $i \in \mathbb{N}$, $\rho(f_i) < \rho(f_{i+1})$ (e logo para todo $f \in \mathcal{R}$, não nulo, existe um índice j com $\rho(f) = \rho(f_j)$). Seja L_l o espaço vetorial gerado por $f_1, ..., f_l$. Então para todo $f \in \mathcal{R}$ temos que $\rho(f) = \rho(f_l)$ se, e somente se, l é o menor inteiro positivo tal que $f \in L_l$.

Com o propósito de transfomar o espaço vetorial $\mathbb{F}_q^n$ em uma $\mathbb{F}_q$-álgebra, introduziremos uma multiplicação em $\mathbb{F}_q^n$. Sejam $a, b \in \mathbb{F}_q^n$. Definimos a multiplicação $*$ em $\mathbb{F}_q^n$ como $a * b = (a_1b_1, ..., a_nb_n)$ onde $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n)$. O espaço vetorial $\mathbb{F}_q^n$ com esta multiplicação torna-se um anel comutativo com unidade $(1, ..., 1)$. Assim, identificando $\{(\alpha, ..., \alpha) : \alpha \in \mathbb{F}_q\}$ com $\mathbb{F}_q$, temos que $\mathbb{F}_q^n$ é uma $\mathbb{F}_q$-álgebra.

Definição 2.12. *A aplicação $\varphi : \mathcal{R} \to \mathbb{F}_q^n$ é chamada de um* **morfismo** *de $\mathbb{F}_q$-álgebras, se φ é $\mathbb{F}_q$-linear e $\varphi(fg) = \varphi(f) * \varphi(g)$.*

Definição 2.13. *Na situação descrita acima considere L_l o espaço gerado por $f_1, ..., f_l$ e seja φ um morfismo 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

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

A seqüência 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 $\mathcal{R}$.

Neste trabalho estamos somente interessados nos morfismos sobrejetores.

Exemplo 2.14. *Sejam $\mathcal{P}$ um conjunto consistindo de n pontos distintos $P_1, ..., P_n$ de $\mathbb{F}_q^m$ e $\mathcal{R} = \mathbb{F}_q[X_1, ..., X_m]$ o anel de polonômios em m variáveis sobre $\mathbb{F}_q$. Considere a aplicação de avaliação*

$$\begin{array}{rccc} av_{\mathcal{P}} : & \mathcal{R} & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & (f(P_1), ..., f(P_n)). \end{array}$$

Isto é um morfismo de $\mathbb{F}_q$-álgebras, pois $(FG)(P) = F(P)G(P)$ para quaisquer dois polinômios F e G e qualquer ponto P em $\mathbb{F}_q^m$.

Observação 2.15. *A aplicação de avaliação $av_{\mathcal{P}}$, definida acima, é sobrejetiva. De fato, para todo $1 \leq j \leq n$ definimos $P_j := (x_{j1}, ..., x_{jm})$ e também para cada par (i, l), com $1 \leq i \leq n$ e $1 \leq l \leq m$, denotaremos $A_{il} = \{x_{jl} : 1 \leq j \leq n\} \backslash \{x_{il}\}$. Observe que se definimos o polinômio*

$$G_i = \prod_{i=1}^{m} \prod_{x \in A_{il}} (X_l - x)$$

então se tem que $G_i(P_j) = 0$ e $G_i(P_i) \neq 0$, pois $P_1, ..., P_n$ são distintos. Assim, a imagem dos polinômios $G_i/G_i(P_i)$, pela aplicação, $av_{\mathcal{P}}$ nos dá a base canônica de $\mathbb{F}_q^n$ e portanto, $av_{\mathcal{P}}$ é sobrejetiva.

A partir deste exemplo geral podemos exibir um morfismo sobre $\mathbb{F}_q^n$associado a uma curva. De fato, suponha que I é um ideal no anel $\mathbb{F}_q[X_1, ..., X_n]$ e $\mathcal{P} = \{P_1, .., P_n\}$ o conjunto de zeros de I em $\mathbb{F}_q^n$, ou seja, $f(P_j) = 0$ para todo $P_j \in \mathcal{P}$ e todo $f \in I$. Então, a aplicação avaliação definida no exemplo anterior induz uma aplicação linear (bem definida)

$$\begin{array}{rccc} av_{\mathcal{P}}: & \mathbb{F}_q[X_1,...,X_n]/I & \longrightarrow & \mathbb{F}_q^n \\ & f+I & \longmapsto & (f(P_1),...,f(P_n)) \end{array}$$

que também é um morfismo de $\mathbb{F}_q$-álgebras.

Agora, considere $\mathcal{X}$ uma curva algébrica afim não-singular absolutamente irredutível sobre o corpo $\mathbb{F}$. Sejam P um ponto $\mathbb{F}$-racional e $\mathcal{R}$ o anel das funções racionais que tem pólos, possivelmente, apenas em P. Seja v_P a valorização em P. Então $v_P(f) \leq 0$ para todo $f \in \mathcal{R}\backslash\{0\}$, pois caso $v_P(f) > 0$, P seria zero de f e logo existiria um pólo de f diferente de P, o que é uma contradição. Assim, definindo $\rho(f) = -v_P(f)$ para $f \in \mathcal{R}$, temos, das propriedades de valorização discreta, que ρ é uma função peso.

Assim, mostremos uma conexão entre códigos de avaliação construídos sobre $\mathcal{R}$ e códigos geométricos de Goppa (pontuais) no ponto P. Sejam $P_1, ..., P_n$ pontos dois a dois distintos, $\mathbb{F}_q$-racionais de $\mathcal{X}$ diferentes de P e considere o divisor $D = P_1 + ... + P_n$. Sejam $(f_i : i \in \mathbb{N})$ uma base de $\mathcal{R}$ sobre $\mathbb{F}_q$ tal que $\rho_i := \rho(f_i) < \rho(f_{i+1}) =: \rho_{i+1}$. Então $\rho(\mathcal{R}\backslash\{0\}) = \{\rho_i : i \in \mathbb{N}\}$. Como $\mathcal{L}(\rho_l P) = \{f \in \mathcal{R} : \rho(f) \leq \rho_l \; e \; v_Q(f) \geq 0, \forall Q \neq P\}$, então os elementos da base de $\mathcal{R}$, que estão em $\mathcal{L}(\rho_l P)$ formam uma $\mathbb{F}_q$-base de $\mathcal{L}(\rho_l P)$. Portanto $\mathcal{L}(\rho_l P) = \langle f_1, ..., f_l \rangle = L_l$. Logo, pela aplicação de avaliação, onde $\mathcal{P} = \{P_1, ..., P_n\}$ em $\mathbb{F}_q^n$, podemos concluir que

$$E_l = av_{\mathcal{P}}(L_l) = av_{\mathcal{P}}(\mathcal{L}(\rho_l P)) = C(D, \rho_l P),$$

onde $C(D, \rho_l P)$ denota o Código Geométrico de Goppa associado aos divisores D e $\rho_l P$. Logo,

$$C_l = E_l^{\perp} = C(D, \rho_l P)^{\perp} = C_{\Omega}(D, \rho_l P).$$

Agora vamos determinar uma cota inferior para a distância mínima d_l do código C_l. Veremos, em um exemplo, que esta cota é melhor, para alguns l, do que a cota $d_G(l) = \rho_l - (2g-2)$ dada no teorema 1.51, onde g denota o gênero da curva $\mathcal{X}$.

Para isto, seja $h_i = \varphi(f_i)$, onde φ é o morfismo de $\mathcal{R}$ em $\mathbb{F}_q^n$. Sabemos, da seção anterior, que existe um inteiro positivo N tal que $E_l = E_N = \mathbb{F}_q^n$ para todo $l \geq N$. Seja H a matriz $N \times n$ cuja a i-ésima linha é dada pelo vetor h_i.

Definição 2.16. *Seja $y \in \mathbb{F}_q^n$. Considere as síndromes $s_i(y) = y \cdot h_i$ e $s_{ij}(y) = y \cdot (h_i * hj)$. Então $S(y) = (s_{ij}(y) : 1 \leq i, j \leq N)$ é a matriz síndrome de y.*

O seguinte resultado estabelece uma relação entre o peso de um elemento de $\mathbb{F}_q^n$ com o posto da matriz síndrome deste elemento.

Lema 2.17. *Seja $y \in \mathbb{F}_q^n$ Seja $D(y)$ a matriz diagonal com as coordenadas de y na diagonal. Então*

$$S(y) = HD(y)H^t,$$

e

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

onde $\omega(y)$ denota o peso de y.

Dem. Temos que $s_{ij}(y) = y \cdot (h_i * h_j) = \sum_l y_l h_{il} h_{jl}$, onde h_{il} é a l-ésima entrada de h_i. Logo, $S(y)_{ij} = \sum_{k=1}^{n} H_{ik} y_k H_{kj}^t$, e portanto segue a igualdade. Agora, como o posto da matriz diagonal $D(y)$ é igual ao número de entradas não-nulas de y, temos que $\omega(y) = postoD(y)$. Assim, como a matriz H tem posto máximo igual a n, pois φ é sobrejetiva, temos que o posto de $S(y)$ é igual ao posto de $D(y)$, como queríamos. ■

Lema 2.18. *(1) Se $y \in C_l$ e $l(i,j) \leq l$ então $s_{ij}(y) = 0$.*
(2) Se $y \in C_l \backslash C_{l+1}$ e $l(i,j) = l+1$ então $s_{ij}(y) \neq 0$.

Dem. (1) Seja $y \in C_l$. Se $l(i,j) \leq l$ então $f_i f_j \in L_l$. Então $h_i * h_j = \varphi(f_i f_j)$ é um elemento de $\varphi(L_l)$ que é dual de C_l. Portanto, $s_{ij}(y) = y \cdot (h_i * h_j) = 0$.

(2) Seja $y \in C_l \backslash C_{l+1}$. Se $l(i,j) = l+1$ então $f_i f_j \in L_{l+1} \backslash L_l$. Assim $f_i f_j \equiv \mu f_{l+1}$ módulo L_l, para algum $\mu \in \mathbb{F}_q \backslash \{0\}$. Logo, $h_i * h_j \equiv \mu h_{l+1}$ módulo $\varphi(L_l)$. Como $y \notin C_{l+1}$, então $s_{l+1}(y) = y \cdot h_{l+1} \neq 0$. Portanto $s_{ij}(y) \neq 0$. ■

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

$$N_l = \{(i,j) \in \mathbb{N}^2 : l(i,j) = l+1\}.$$

Seja ν_l o número de elementos de N_l.

Lema 2.19. *Se $t = \nu_l$ e $(i_1, j_1), ..., (i_t, j_t)$ é uma enumeração dos elementos de N_l em ordem crescente com respeito a ordem lexicográfica em $\mathbb{N}^2$, então $i_1 < ... < i_t$ e $j_t < ... < j_1$. Mais ainda, se $y \in C_l \backslash C_{l+1}$, então $s_{i_u j_v} = 0$ se $u < v$ e $s_{i_u j_v} \neq 0$ se $u = v$.*

Dem. Pela ordem da seqüência $(i_1, j_1), ..., (i_t, j_t)$ temos que $i_1 \leq ... \leq i_t$. Suponha que $i_u = i_{u+1}$. Então $j_t < j_{u+1}$ e logo

$$l+1 = l(i_u, j_u) < l(i_u, j_{u+1}) = l(i_{u+1}, j_{u+1}) = l+1$$

o que é um absurdo. Logo a seqüência $i_1, ..., i_t$ é estritamente crescente.

Agora, suponha que $j_{u+1} \geq j_u$. Novamente, temos que

$$l+1 = l(i_{u+1}, j_{u+1}) \geq l(i_{u+1}, j_u) > l(i_u, j_u) = l+1$$

um outro absurdo. Logo, $j_{u+1} < j_u$, para todo $u < t$.

Seja $y \in C_l$. Se $u < v$, então $l(i_u, j_v) < l(i_v, j_v) = l+1$. Logo, do lema2.18, segue que $s_{i_u j_v}(y) = 0$.

Do mesmo modo, seja $y \notin C_{l+1}$. Se $u = v$ então $l(i_u, j_v) = l+1$, e do lema 2.18, segue que $s_{i_u j_v}(y) \neq 0$ ∎

Observe que para $y \in C_l \backslash C_{l+1}$, temos, do lema acima, que a matriz $(s_{i_u j_v}(y))$ com $1 \leq u, v \leq \nu_l$ é uma sub-matriz de $S(y)$ com posto igual a ν_l. Logo, do lema 2.17, temos que $\omega(y) = posto(S(y)) \geq posto(s_{i_u j_v}(y)) = \nu_l$, provando, assim, o seguinte resultado.

Proposição 2.20. *Se $y \in C_l \backslash C_{l+1}$ então $\omega(y) \geq \nu_l$.*

Devido a esta proposição, podemos determinar uma cota inferior para o código dual C_l. Mas antes, considere o número

$$d(l) = min\{\nu_m : m \geq l\}.$$

chamado de *cota ordem*.

Teorema 2.21. *O numero $d(l)$ é uma cota inferior para a distância mínima de C_l, ou seja,*

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

Dem. Segue diretamente da proposição anterior. ∎

Vejamos um exemplo.

Exemplo 2.22. *Da geometria algébrica temos que o gênero da curva $\mathcal{X}$, considerada no exemplo 2.11, é dado por $g = (n-1)(n-2)/2$ onde n é o grau desta curva; neste caso, $g = 6$. Então, dando continuidade ao exemplo citado acima, a tabela abaixo nos fornece uma lista dos valores de ρ_l, ν_l, $d(l)$ e $d_G(l)$.*

l :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
f_l :	1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	x^3y	x^2y^2	xy^3	y^4	x^4y	...
ρ_l :	0	4	5	8	9	10	12	13	14	15	16	17	18	19	20	21	...
ν_l :	2	2	3	4	3	4	6	6	4	5	8	9	8	9	10	12	...
$d(l)$:	2	2	3	3	3	4	4	4	4	5	8	8	8	9	10	12	...
$d_G(l)$:	-10	-6	-5	-2	-1	0	2	3	4	5	6	7	8	9	10	11	...

Observe também que $d(l) = \nu_l = l - 5$ *para todo* $l > 16$.

2.3 Semigrupos

Nesta seção veremos algumas propriedades sobre semigrupos e determinaremos uma cota inferior para as distâncias mínimas dos códigos avaliados.

Definição 2.23. *Um subconjunto* Λ *de* $\mathbb{N}_0$ *é chamado* ***semigrupo numérico*** *se* $0 \in \Lambda$ *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.

Observação 2.24. *Suponha que* ρ *é uma função peso sobre uma* $\mathbb{F}$*-algebra* $\mathcal{R}$*. A condição (6) da definição 2.1 implica que o subconjunto* $\Lambda = \{\rho(f) : f \in \mathcal{R}, f \neq 0\}$ *é um semigrupo numérico chamado de semigrupo de* ρ*.*

Em particular, se $\rho = -\upsilon_P$*, como visto na descrição após a observação 2.15, então* Λ *é chamado de* **semigrupo de Weierstrass de** P*.*

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, $c = g + 1$.

Exemplo 2.25. *Seja* $\Lambda = \{0, 4, 5, 8, 9, 10\} \cup \{n \in \mathbb{N}_0 : n \geq 12\}$*. Então* Λ *é o semigrupo da função peso definida no exemplo 2.11. As lacunas de* Λ *são 1,2,3,6,7 e 11. Logo, o número de lacunas é* $g = 6$*,* $c = 12$ *é o condutor e 11 é a maior lacuna de* Λ*.*

Seja $(\rho_l : l \in \mathbb{N})$ uma enumeração dos semigrupo de ρ, Λ, tal que $\rho_l < \rho_{l+1}$ para todo l. Denote por $g(l)$ o número de lacunas menores que ρ_l. Então, temos a seguintes propriedades:

Lema 2.26. *Sejam Λ um semigrupo com finitas lacunas e $l \in \mathbb{N}$. Então,*
(1) $g(l) = \rho_l - l + 1$;
(2) $\rho_l \leq l + g - 1$, valendo a igualdade se, e somente se, $\rho_l \geq c$;
(3) Se $l > c - g$ então $\rho_l = l + g - 1$;
(4) Se $l \leq c - g$ então $\rho_l < c - 1$.

Dem. (1) A não-lacuna $\rho_l \in \Lambda$ é o $(\rho_l + 1)$-ésimo elemento de $\mathbb{N}_0$. Logo, ρ_l é o $(\rho_l + 1 - g(l))$-ésimo elemento de Λ e portanto, segue que $l = \rho_l + 1 - g(l)$.
(2) Como $g(l) \leq g$, temos que $\rho_l + 1 - l \leq g$, ou seja, $\rho_l \leq g - 1 + l$. Agora, se $\rho_l \geq c$ temos que todas as lacunas são menores que ρ_l e portanto $g(l) = g$, valendo a igualdade.
(3) O condutor c é o $(c+1)$-ésimo elemento de $\mathbb{N}_0$ e mais, é o $(c + 1 - g)$-ésimo elemento de Λ. Logo, $c = \rho_{c+1-g}$. Assim, se $l > c - g$ então $\rho_l \geq \rho_{c+1-g} = c$. Portanto, de (2), temos que $\rho_l = l + g - 1$.
(4) Seja $l \leq c - g$. Então $\rho_l \leq l + g - 1 \leq c - 1$. Como $c - 1$ é a maior lacuna de Λ, temos que $\rho_l < c - 1$. ∎

O próximo resultado nos mostra uma importante relação entre o condutor e o número de não-lacunas de um semigrupo.

Proposição 2.27. *Seja Λ um semigrupo com um número finito de lacunas. Se g é o gênero de Λ e c seu condutor, então $c \leq 2g$, valendo a igualdade se, e somente se, para qualquer $s \in \mathbb{N}_0$, se s é uma lacuna, então $c - 1 - s$ é uma não-lacuna.*

Dem. Consideremos os pares $(s, t) \in \mathbb{N}_0^2$ tais que $s + t = c - 1$. Pelo fato de $c - 1$ ser uma lacuna e de Λ ser fechado pra a adição, temos que pelo menos um dos dois termos de cada par deve ser uma lacuna. Assim, como temos c pares desses, levando-se em consideração a ordem, temos que existem pelo menos $[\frac{c+1}{2}]$ lacunas. Logo, $c \leq 2g$.

Agora, se a igualdade é válida, temos que $g = c/2$. Então, se dados $s, t \in \mathbb{N}_0$ tais que $s + t = c - 1$ temos que apenas um destes dois elementos é uma lacuna. Assim, tomando s com lacuna, temos que $c - 1 - s$ é uma não-lacuna. Reciprocamente, se s é uma lacuna então $c - 1 - s$ é uma não-lacuna. Logo, somente um dos temos dos pares (s, t) satisfazendo $s + t = c - 1$ é uma lacuna, portanto temos $c/2$ lacunas, ou seja, $c = 2g$. ∎

Definição 2.28. *Um semigrupo é chamado de* **simétrico** *se* $c = 2g$.

Exemplo 2.29. *O semigrupo* Λ *do exemplo 2.25 é um semigrupo simétrico.*

Definição 2.30. *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 denotamos* $\Lambda = \langle A \rangle$.

Veremos a seguir uma caracterização dos semigrupos gerados por dois elementos, cujo máximo divisor comum é 1, e algumas propriedades sobre esses semigrupos.

Proposição 2.31. *Seja* $a, b \in \mathbb{N}$ *tais que* $mdc(a, b) = 1$. *Então o semigrupo gerado por* a *e* b *é simétrico, tem* $ab - a - b$ *como maior lacuna,* $(a-1)(b-1)$ *como condutor e o número de lacunas* g *é igual a* $(a-1)(b-1)/2$.

Dem. Como $mdc(a, b) = 1$ temos que todo inteiro m pode ser escrito de maneira única como $m = xb + ya$ onde x e y são inteiros e $0 \leq y < b$. Assim, segue que toda lacuna (resp. não-lacuna) m tem uma única representação $m = xb + ya$ tal que $0 \leq y < b$ e $x < 0$ (resp. $x \geq 0$), pois $\Lambda = \langle a, b \rangle = \{ya + xb : y, x \in \mathbb{N}_0\}$.

Seja c o condutor de $\Lambda = \langle a, b \rangle$. Sabemos que a maior lacuna de Λ é $c - 1$. Os números $ya \in \Lambda$, com $y = 0, 1, ..., b - 1$ formam um conjunto completo de representantes da forma $ya + b\mathbb{Z}$ e observe que $ya - b$ é o maior elemento no conjunto $ya + b\mathbb{Z}$ sem uma representação com coeficientes inteiros não-negativos. Logo $(b-1)a - b$ é a maior lacuna de Λ, que é igual a $c-1$. Assim, $c = (b-1)a-b+1 = (a-1)(b-1)$. Agora, mostremos que Λ é um semigrupo simétrico. Suponha, por absurdo, que existe $s, t \in \mathbb{N}$, ambos lacunas, tais que $s + t = c - 1$. Então

$$s = x_1 b + y_1 a,\ t = x_2 b + y_2 a, \text{ onde } 0 \leq y_1, y_2 < b \text{ e } x_1, x_2 < 0.$$

Logo, $ab - a - b = c - 1 = (x_1 + x_2)b + (y_1 + y_2)a$ e portanto

$$0 < b \leq \beta = (-x_1 - x_2 - 1)b = (y_1 + y_2 - b + 1)a \leq (b-1)a < ba,$$

pois $0 \leq y_1 + y_2 \leq 2b - 2$ e $x_1 + x_2 \leq -2$. Como o $mdc(a, b) = 1$ temos que $a|(-x_1 - x_2 - 1)$ e que $b|(y_1 + y_2 - b + 1)$. Logo $0 < \frac{\beta}{ab} < 1$, absurdo. Portanto Λ é um semigrupo simétrico e $c = 2g$. Assim, $g = (a-1)(b-1)/2$. ∎

Agora, para obtermos, a partir da proposição anterior, uma caracterização de um semigrupo de gênero finito, vamos provar o seguinte lema:

Lema 2.32. *Se Λ é um semigrupo tal que o máximo divisor comum dos seus elementos é 1 então existem $a, b \in \Lambda$ tais que $mdc(a, b) = 1$.*

Dem. De fato, pois se o máximo divisor comum dos elementos de Λ é 1, então existem $a_1, ..., a_m \in \Lambda$, com $a_m \neq 0$, e $x_1, ..., x_m \in \mathbb{Z}$ tais que $1 = a_1x_1 + ... + a_mx_m$. Assim, para $i \leq m-1$, temos que existem $q_i, r_i \in \mathbb{Z}$ tais que $x_i = q_ia_m + r_i$, com $0 \leq r_i < a_m$. Então

$$1 = r_1a_1 + ... + r_{m-1}a_{m-1} + (a_1q_1 + ... + a_{m-1}q_{m-1} + x_m)a_m.$$

Logo, como Λ é fechado para a soma, basta tomar $a = a_m$ e $b = r_1a_1 + ... + r_{m-1}a_{m-1}$. ■

Isto, juntamente com a proposição 2.31, prova o seguinte resultado:

Corolário 2.33. *Um semigrupo tem um número finito de lacunas se, e somente se, o máximo divisor comum dos seus elementos é 1.*

Exemplo 2.34. *O semigrupo do exemplo 2.25 é gerado por 4 e 5, e $g = 6 = (4-1)(5-1)/2$.*

Lema 2.35. *Seja Λ um semigrupo com finitas lacunas. Seja $s \in \Lambda$. Então $\#(\Lambda \backslash (s+\Lambda)) = s$.*

Dem. Seja c o condutor de Λ. Seja $T = \{t \in \mathbb{N}_0 : t \geq s + c\}$. Temos que $T \subset \Lambda$, e mais, $T \subset s + \Lambda = \{s + \lambda : \lambda \in \Lambda\}$. Seja $U = \{u \in \Lambda : u < s + c\}$. Então $\#U = s + c - g$ e Λ é a união disjunta de T e U, ou seja, $\Lambda = U \cup T$. Seja $V = \{v \in s + \Lambda : s \leq v \leq s + c\} \subset U$. Então temos que $\#V = s + c - g - s = c - g$ e $s + \Lambda = V \cup T$. Assim, segue que

$$\#(\Lambda \backslash (s + \Lambda)) = \#U - \#V = (s + c - g) - (c - g) = s.$$

■

A seguinte proposição é uma consequência do lema anterior:

Proposição 2.36. *Seja f um elemento não-nulo de uma $\mathbb{F}_q$-álgebra $\mathcal{R}$ com uma função peso ρ. Então $dim_{\mathbb{F}_q}(\mathcal{R}/\langle f \rangle) = \rho(f)$.*

Dem. Sejam Λ o semigrupo da função peso ρ, ou seja, $\Lambda = \{\rho(g) : g \in \mathcal{R}, g \neq 0\}$ e $s = \rho(f)$. Seja $(\rho_i : i \in \mathbb{N})$ a sequência, em ordem crescente, dos elementos de Λ. Da definição de função peso, temos que a imagem dos elementos não nulos do ideal $\langle f \rangle$, segundo a função ρ, é igual a $s+\Lambda$. Sabemos que para todo $\rho_i \in \Lambda$, existe um $f_i \in \mathcal{R}$ tal que $\rho(f_i) = \rho_i$, assim, caso $\rho_i \in s + \Lambda$, podemos tomar $f_i \in \langle f \rangle$. Observe que os conjuntos $\{f_i : i \in \mathbb{N}\}$

e $\{f_i : i \in \mathbb{N}, \rho_i \in s + \Lambda\}$, via demonstração do teorema 2.7, formam uma base para a álgebra $\mathcal{R}$ e o ideal $\langle f \rangle$, respectivamente. Logo, as classes de equivalência f_i módulo $\langle f \rangle$ com $i \in \mathbb{N}$ e $\rho_i \in \Lambda \backslash (s + \Lambda)$ formam uma base para o quociente $\mathcal{R}/\langle f \rangle$. Portanto temos que a dimensão de $\mathcal{R}/\langle f \rangle$ é igual ao número de elementos de $\Lambda \backslash (s+\Lambda) = \rho(f)$, pelo lema anterior. ■

O resultado abaixo nos mostra que existe uma relação entre o número de zeros de um elemento não-nulo de uma álgebra afim e seu peso.

Lema 2.37. *Seja $\mathcal{R}$ uma álgebra afim com função peso ρ e aplicação de avaliação $av_{\mathcal{P}}$. Seja f um elemento não-nulo de $\mathcal{R}$. Então o número de zeros de f é no máximo $\rho(f)$.*

Dem. Seja $\mathcal{P}$ o conjunto de zeros de f, isto é, $f(P) = 0$ para todo $P \in \mathcal{P}$, e seja $t = \#\mathcal{P}$. Temos, da observação 2.15, que a aplicação de avaliação $av_{\mathcal{P}} : \mathcal{R} \to \mathbb{F}_q^t$ é linear e sobrejetiva. Assim, do teorema do isomorfismo, temos que $\mathcal{R}/Ker(av_{\mathcal{P}}) \cong \mathbb{F}_q^t$. Como $\langle f \rangle \subset Ker(av_{\mathcal{P}})$ e olhando ambos como subespaço vetorial de $\mathcal{R}$, temos que $dim_{\mathbb{F}_q}(\langle f \rangle) \leq dim_{\mathbb{F}_q}(Ker(av_{\mathcal{P}}))$. Então, segue que

$$t = dim_{\mathbb{F}_q}(\mathcal{R}/Ker(av_{\mathcal{P}})) = dim_{\mathbb{F}_q}(\mathcal{R}) - dim_{\mathbb{F}_q}(Ker(av_{\mathcal{P}})) \leq dim_{\mathbb{F}_q}(\mathcal{R}) - dim_{\mathbb{F}_q}(\langle f \rangle) = dim_{\mathbb{F}_q}(\mathcal{R}/\langle f \rangle) = \rho(f),$$

pela proposição 2.36. ■

A partir de agora estamos interessados em calcular uma cota inferior para os códigos de avaliação E_l.

Seja $\mathcal{R} = \mathbb{F}_q[X_1, ..., X_n]/I$, onde I é um ideal de $\mathbb{F}_q[X_1, ..., X_n]$, e suponha que ρ é uma função peso em $\mathcal{R}$. Seja $(\rho_i : i \in \mathbb{N})$ uma enumeração, em ordem crescente, dos elementos do semigrupo de ρ. Tomemos $\mathcal{P}$ um conjunto com n pontos do conjunto dos zeros de I $(Z(I) = \{P \in \mathbb{F}_q^n \mid f(P) = 0, \forall\ f \in I\})$ e considere a aplicação de avaliação $av_{\mathcal{P}} : \mathcal{R} \to \mathbb{F}_q^n$. Então, definimos os códigos de avaliação E_l como

$$E_l = \{av_{\mathcal{P}}(f) : f \in \mathcal{R}, \rho(f) \leq \rho_l\}.$$

Teorema 2.38. *A distância mínima do código E_l é maior ou igual a $n - \rho_l$. Se $\rho_l < n$ então $dim_{\mathbb{F}_q}(E_l) = l$.*

Dem. Seja c um elemento não-nulo do código E_l, logo existe $f \in \mathcal{R}\backslash\{0\}$ tal que $\rho(f) \leq \rho_l$ e $c = av_{\mathcal{P}}(f)$. Seja c_i as coordenadas da palavra c, então temos que $c_i = f(P_i)$ para todo i. Do lema 2.37, temos que o número de zeros de f é no máximo $\rho(f) \leq \rho_l$ e portanto $\omega(c) \geq n - \rho(f) \geq n - \rho_l$.

Agora, suponha que $\rho_l < n$. Sabemos que E_l é a imagem do espaço vetorial L_l, de dimensão l, via a aplicação de avaliação $av_{\mathcal{P}}$. Assim, se $f \in L_l$ e $av_{\mathcal{P}}(f) = 0$ então f tem no mínimo n zeros. Como, do lema 2.37, se f é não-nulo então f admite no máximo $\rho(f) \leq \rho_l < n$, temos que $f = 0$. Portanto, $Ker(av_{\mathcal{P}}|_{L_l}) = \{0\}$, ou seja, $dim_{\mathbb{F}_q}(E_l) = dim_{\mathbb{F}_q}(L_l) = l$. ■

O próximo resultado é consequência imediata do teorema anterior e do lema 2.26.

Corolário 2.39. *Seja ρ uma função peso com g lacunas. Se $\rho_l < n$ então E_l é um $[n, k, d]$-código tal que $k + d \geq n + 1 - g$.*

CAPÍTULO 3

Álgebras munidas de Função Peso e Códigos de Goppa Pontuais

Neste capítulo, mostraremos que se uma álgebra é munida de uma função peso então esta álgebra é um anel de coordenadas de uma curva algébrica afim com exatamente um lugar de grau um no infinito. Disto, poderemos concluir que os códigos de avaliação constuídos sobre álgebras com função peso são códigos geométricos de Goppa pontuais. Em alguns resultados deste capítulo utilizaremos de conceitos importantes da álgebra comutativa que serão enfatizados no apêndice A desta dissertação.

Ao longo deste, $\mathcal{R}$ denotará uma $\mathbb{F}_q$-álgebra diferente de $\mathbb{F}_q$.

Para obtermos uma importante caracterização sobre álgebras com funções pesos, necessitaremos provar o seguinte resultado:

Lema 3.1. *Seja M um subsemigrupo dos números inteiros não-negativos $\mathbb{N}_0$. Então, existe um subconjunto finito $\{a_1, ..., a_t\}$ em $\mathbb{N}_0$ que gera M, ou seja, para qualquer $m \in M$, existem $n_i \in \mathbb{N}_0$, para $i = 1, ..., t$, tal que*

$$m = n_1 a_1 + ... + n_t a_t.$$

Dem. Seja $0 \neq t \in M$. Para $i = 1, ..., t$ defina $a_i = min(M \cap \{i + tn : n \in \mathbb{N}_0\})$. Se $M \cap \{i + tn : n \in \mathbb{N}_0\} = \emptyset$, tome $a_i = 0$. Mostremos que $\{a_1, ..., a_t\}$ gera M. Seja $m \in M$. Se $m \leq t$ temos que $m = a_m$. Agora, se $m > t$, então existem $q_1, i_1 \in \mathbb{N}_0$ tal que $m = q_1 t + i_1$,

com $0 < i_1 \leq t$. Observe que $t = a_t$ e que $m \in M \cap \{i_1 + tn : n \in \mathbb{N}_0\}$. Logo, $m \geq a_{i_1}$. Suponha que $a_{i_1} = i_1 + tn_1$ para algum $n_1 \in \mathbb{N}_0$. Então, como $m \geq a_{i_1}$, temos que $q_1 \geq n_1$ e portanto

$$m = (q_1 - n_1 + n_1)t + i_1 = (q_1 - n_1)t + n_1 t + i_1 = (q_1 - n_1)a_t + a_{i_1}.$$

Como $q_1 - n_1 \in \mathbb{N}_0$, segue o resultado. ∎

Agora, podemos provar uma primeira característica de uma álgebra munida de uma função peso.

Lema 3.2. *Se $\mathcal{R}$ é uma $\mathbb{F}_q$-álgebra com função peso ρ, então $\mathcal{R}$ é uma álgebra finitamente gerada sobre $\mathbb{F}_q$.*

Dem. Considere o conjunto $\rho(\mathcal{R}\backslash\{0\}) \subset \mathbb{N}_0$. Então, do lema anterior, existem $a_1, ..., a_t \in \mathbb{N}_0$ tal que $\rho(\mathcal{R}\backslash\{0\}) = \langle a_1, ..., a_t \rangle$. Logo, existem $f_1, ..., f_t \in \mathcal{R}$, não-nulos, tal que $\rho(f_i) = a_i$. Assim, mostremos que $\mathcal{R} = \mathbb{F}_q[f_1, ..., f_t]$.

Seja $0 \neq g \in \mathcal{R}$. Então $\rho(g) \in \rho(\mathcal{R}\backslash\{0\})$, ou seja, existem $n_{11}, ..., n_{1t} \in \mathbb{N}_0$ tais que

$$\begin{aligned} \rho(g) &= n_{11}a_1 + ... + n_{1t}a_t = n_{11}\rho(f_1) + ... + n_{1t}\rho(f_t) \\ &= \rho(f_1^{n_{11}}) + ... + \rho(f_t^{n_{1t}}) = \rho(f_1^{n_{11}} \cdot ... \cdot f_t^{n_{1t}}) \end{aligned}.$$

Então, do lema 2.4 (4), existe um único $\lambda_1 \in \mathbb{F}_q$, não-nulo, tal que

$$\rho(g - \lambda_1 f_1^{n_{11}} \cdot ... \cdot f_t^{n_{1t}}) < \rho(g).$$

Novamente, existem $n_{21}, ..., n_{2t} \in \mathbb{N}_0$ tais que

$$\rho(g - \lambda_1 f_1^{n_{11}} \cdot ... \cdot f_t^{n_{1t}}) = n_{21}a_1 + ... + n_{2t}a_t = \rho(f_1^{n_{21}} \cdot ... \cdot f_t^{n_{2t}})$$

e portanto, existe um único $\lambda_2 \in \mathbb{F}_q$ tal que

$$\rho(g - \lambda_1 f_1^{n_{11}} \cdot ... \cdot f_t^{n_{1t}} - \lambda_2 f_1^{n_{21}} \cdot ... \cdot f_t^{n_{2t}}) < \rho(g - \lambda_1 f_1^{n_{11}} \cdot ... \cdot f_t^{n_{1t}}).$$

Como $\mathbb{N}_0$ é bem ordenado, continuando o processo, existem únicos $\lambda_{i's} \in \mathbb{F}_q$ tais que

$$\rho(g - \textstyle\sum_i \lambda_i f_1^{n_{i1}} \cdot ... \cdot f_t^{n_{it}}) < \rho(1).$$

Logo, segue que $g - \sum_i \lambda_i f_1^{n_{i1}} \cdot ... \cdot f_t^{n_{it}} = 0$, ou seja, $g = \sum_i \lambda_i f_1^{n_{i1}} \cdot ... \cdot f_t^{n_{it}}$. Portanto, $\mathcal{R} = \mathbb{F}_q[f_1, ..., f_t]$. ∎

Vejamos agora um exemplo de que é possível construir álgebras com funções ordens que não são finitamente geradas sobre $\mathbb{F}_q$.

Exemplo 3.3. *Seja $\mathcal{R}$ o $\mathbb{F}_q$-subespaço linear de $\mathbb{F}_q[X,Y]$ gerado pelo conjunto $\{X^iY^j \mid j = 0 \text{ ou } (j>0 \text{ e } i>0)\}$. Então $\mathcal{R}$ é um subanel de $\mathbb{F}_q[X,Y]$ e não é finitamente gerado sobre $\mathbb{F}_q$. De fato, suponha que $\mathcal{R}$ é finitamente gerado pelos monômios $f_1 = X$, $f_2 = X^{i_2}Y^{j_2}$, $f_3 = X^{i_3}Y^{j_3}$,..., $f_s = X^{i_s}Y^{j_s}$, onde $i_t, j_t \geq 1$ para $2 \leq t \leq s$. Como $f_t = X^{i_t}Y^{j_t} = X^{(i_t-1)}(XY^{j_t}) = f_1^{i_t-1}(XY^{j_t})$, podemos supor, sem perda de generalidade, que $f_t = XY^{j_t}$ para $2 \leq t \leq s$ e $1 \leq j_2 < j_3 < ... < j_s$.*

Assim, considere o monômio $XY^{j_s+1} \in \mathcal{R}$. Então, existem $a_{\lambda_k} \in \mathbb{F}_q$ com $\lambda_k = (\lambda_{k1}, ..., \lambda_{ks}) \in I \subseteq \mathbb{N}^s$ tais que

$$XY^{j_s+1} = \sum_{\lambda_k \in I} a_{\lambda_k} f_1^{\lambda_{k1}} ... f_s^{\lambda_{ks}}.$$

Logo,

$$\begin{aligned} XY^{j_s+1} &= \sum_{\lambda_k \in I} a_{\lambda_k} X^{\lambda_{k1}} (X^{\lambda_{k2}} Y^{j_2\lambda_{k2}}) ... (X^{\lambda_{ks}} Y^{j_s\lambda_{ks}}) \\ &= \sum_{\lambda_k \in I} a_{\lambda_k} X^{\lambda_{k1}+\lambda_{k2}+...+\lambda_{ks}} Y^{j_2\lambda_{k2}+...+j_s\lambda_{ks}}. \end{aligned}$$

Como os monômios são $\mathbb{F}_q$-linearmente independentes em $\mathbb{F}_q[X,Y]$, em particular, em $\mathcal{R}$, temos que existe $t \in \mathbb{N}$ tal que $a_{\lambda_k} = 1$ quando $k = t$ e $a_{\lambda_k} = 0$ quando $k \neq t$. Logo,

$$XY^{j_s+1} = X^{\lambda_{t1}+\lambda_{t2}+...+\lambda_{ts}} Y^{j_2\lambda_{t2}+...+j_s\lambda_{ts}}.$$

Logo $\lambda_{t1} + \lambda_{t2} + ... + \lambda_{ts} = 1$ e portanto, existe $\alpha \in \{1, ..., s\}$ tal que $\lambda_{t\alpha} = 1$ e $\lambda_{t\beta} = 0$ para $\beta \in \{1, ..., s\}$ e $\beta \neq \alpha$. Assim, $XY^{j_s+1} = XY^{j_\alpha}$, ou seja, $j_s + 1 = j_\alpha \leq j_s < j_s + 1$, absurdo.

Portanto, $\mathcal{R}$ não é finitamente gerado. Mas, como do exemplo 2.9, $\mathbb{F}_q[X,Y]$ tem função ordem, segue, da observação 2.2, que $\mathcal{R}$ tem função ordem.

Vimos na proposição 2.5 que $\mathbb{F}_q$-álgebras com funções pesos são domínios. Na seguinte proposição veremos que o corpo de frações destas álgebras são corpos de funções algébricas de uma variável sobre $\mathbb{F}_q$.

Proposição 3.4. *Seja $\mathcal{R}$ uma $\mathbb{F}_q$-álgebra com função peso ρ. Seja F o corpo de frações de $\mathcal{R}$. Então, F é um corpo de funções algébricas de uma variável sobre $\mathbb{F}_q$.*

Dem. Do lema 3.2, temos que $\mathcal{R}$ é uma $\mathbb{F}_q$-álgebra finitamente gerada. Assim, é suficiente provarmos que o grau de transcendência de F sobre $\mathbb{F}_q$, denotado por $grtr_{\mathbb{F}_q}(F)$, é igual a um, isto é, $grtr_{\mathbb{F}_q}(F) = 1$.

Seja $f \in \mathcal{R} \backslash \mathbb{F}_q$. Então a proposição 2.36 nos garante que $\mathcal{R}/\langle f \rangle$ é um $\mathbb{F}_q$-espaço vetorial de dimensão finita. Logo $\mathcal{R}/\langle f \rangle$ é artiniano e portanto a dimensão de *Krull* de $\mathcal{R}/\langle f \rangle$,

denotado por $dim_{Krull}(\mathcal{R}/\langle f\rangle)$, é igual a zero, isto é, $dim_{Krull}(\mathcal{R}/\langle f\rangle) = 0$. Então, do corolário A.46, temos que $dim_{Krull}\mathcal{R} = 1$.

Mas, como $\mathcal{R}$ é um domínio, do teorema A.44, segue que $grtr_{\mathbb{F}_q}(F) = dim_{Krull}(\mathcal{R}) = 1$.

■

Proposição 3.5. *Sejam $\mathcal{R}$ uma $\mathbb{F}_q$-álgebra finitamente gerada que é um domínio e F o corpo de frações de $\mathcal{R}$. Suponha que a dimensão de Krull de $\mathcal{R}$ é 1. Seja $\overline{\mathcal{R}}$ o fecho integral de $\mathcal{R}$ em F. Então $\frac{\overline{\mathcal{R}}}{\mathcal{R}}$ é um $\mathbb{F}_q$-espaço vetorial de dimensão finita.*

Dem. Como $\overline{\mathcal{R}}$ é o fecho integral de $\mathcal{R}$ em F, temos, pelo corolário A.47, que $\overline{\mathcal{R}}$ é um $\mathcal{R}$-módulo finitamente gerado. Logo, $\overline{\mathcal{R}} = \mathbb{F}_q[X_1, ..., X_n]/I$, onde I é um ideal primo de $\mathbb{F}_q[X_1, ..., X_n]$. Seja Γ o anulador do $\mathcal{R}$-módulo $\frac{\overline{\mathcal{R}}}{\mathcal{R}}$, ou seja, $\Gamma = \{x \in \mathcal{R} : x\overline{\mathcal{R}} \subset \mathcal{R}\}$. Então Γ é um ideal, não nulo, de $\mathcal{R}$ e de $\overline{\mathcal{R}}$. De fato, é fácil ver que Γ é um ideal de $\mathcal{R}$ e de $\overline{\mathcal{R}}$, assim mostremos que $\Gamma \neq \{0\}$. Como $\overline{\mathcal{R}}$ é um $\mathcal{R}$-módulo finitamente gerado, existem $y_1, ..., y_n \in \overline{\mathcal{R}}$ tais que $\overline{\mathcal{R}} = \mathcal{R}y_1 + ... + \mathcal{R}y_n$. Sabemos também que cada $y_i \in \overline{\mathcal{R}}$ é da forma $y_i = z_i/t_i$, com $z_i, t_i \in \mathcal{R}\backslash\{0\}$, para $i = 1, ..., n$. Assim, tomando $x = t_1 \cdot ... \cdot t_n \in \mathcal{R}$, temos que $x\overline{\mathcal{R}} \subset \mathcal{R}$, ou seja, $x \in \Gamma$.

Agora, seja J um ideal de $\mathbb{F}_q[X_1, ..., X_n]$ contendo I tal que $\frac{J}{I} = \Gamma$. Como $\mathcal{R} \subseteq \overline{\mathcal{R}}$ é uma extensão integral, pelo corolário A.33, segue que $dim_{krull}\overline{\mathcal{R}} = dim_{krull}\mathcal{R} = 1$. Logo, como $\overline{\mathcal{R}}$ é noetheriano e $\Gamma \neq \{0\}$ segue, do corolário A.45, que $dim_{krull}\frac{\overline{\mathcal{R}}}{\Gamma} = 0$. Portanto, $\overline{\mathcal{R}}/\Gamma$ é artiniano. Mais ainda, como $\frac{\overline{\mathcal{R}}}{\Gamma} \cong \mathbb{F}_q[X_1, ..., X_n]/J$, então $\frac{\overline{\mathcal{R}}}{\Gamma}$ é artiniano como $\mathbb{F}_q$-módulo. Portanto $\frac{\overline{\mathcal{R}}}{\Gamma}$ é um $\mathbb{F}_q$-espaço vetorial e pelo corolário A.7 tem dimensão finita. Como $\frac{\mathcal{R}}{\Gamma} \subseteq \frac{\overline{\mathcal{R}}}{\Gamma}$, então $\frac{\overline{\mathcal{R}}}{\mathcal{R}}$ tem dimensão finita. ■

Definição 3.6. *Sejam $\mathcal{R}$ o anel de coordenadas de uma curva $\mathcal{X}$ e F o corpo de frações de $\mathcal{R}$. Seja P um lugar de $F|\mathbb{F}_q$, onde $F|\mathbb{F}_q$ é o corpo de funções algébricas em uma variável sobre $\mathbb{F}_q$. Dizemos que a curva $\mathcal{X}$ tem exatamente um lugar P no infinito se todo elemento não nulo de $\mathcal{R}$ não tem pólos fora de P.*

Visto os resultados anteriores, estamos em condições de enunciar e provar o principal teorema deste capítulo.

Teorema 3.7. *Seja $\mathcal{R}$ uma $\mathbb{F}_q$-álgebra com função peso ρ. Suponha que existe $x \in \mathcal{R}$ tal que $\rho(x) > 0$. Então o corpo de frações F de $\mathcal{R}$ é um corpo de funções algébricas de uma variável sobre $\mathbb{F}_q$, existe uma única valorização discreta υ de $F|\mathbb{F}_q$ e um único inteiro positivo d tal que $\rho(x) = -d\upsilon(x)$, para todo $x \in \mathcal{R}$. Mais ainda, se P é o lugar correspondente a*

valorização υ, então o grau de P é 1, e $\mathcal{R}$ é o anel de coordenadas afim de uma curva algébrica definida sobre $\mathbb{F}_q$ com exatamente um lugar, P, no infinito.

Dem. Temos, do lema 3.4, que F é um corpo de funções algébricas de uma variável sobre $\mathbb{F}_q$. Assim, seja d o máximo divisor comum dos elementos de $\rho(\mathcal{R})\backslash\{0, -\infty\}$. Defina a função $\upsilon : F \to \mathbb{Z} \cup \{\infty\}$ por $\upsilon(f/g) = \frac{\rho(g)-\rho(f)}{d}$, para todo $f, g \in \mathcal{R}$, com $g \neq 0$ e $\upsilon(0) = \infty$. Então, da definição de função peso, segue que υ é uma valorização discreta de $F|\mathbb{F}_q$. Seja O_P o anel de valorização correspondente a υ e P o lugar de O_P. Denotemos por υ_P a valorização υ. Então, $\mathbb{F}_q$ é isomorfo a O_P/P, pois como $\mathbb{F}_q \subset O_P$ e $\mathbb{F}_q \cap P = \{0\}$ temos que $\mathbb{F}_q$ está mergulhado em O_P/P. Assim, seja $\phi : \mathbb{F}_q \to O_P/P$ esse mergulho. Mostremos que ϕ é sobrejetora. Seja $f/g \in O_P$ tal que $\overline{0} \neq f/g + P \in O_P/P$. Então $\upsilon_P(f/g) = 0$, ou seja, $\rho(g) = \rho(f)$. Logo, de (5) da definição de função peso, existe $\lambda \in \mathbb{F}_q$ tal que $\rho(f - \lambda g) < \rho(g)$ e portanto $\upsilon_P(\frac{f-\lambda g}{g}) = \upsilon_P(\frac{f}{g} - \lambda) > 0$. Então $\frac{f}{g} - \lambda \in P$ e logo $\phi(\lambda) = f/g + P$. Assim, temos que $\mathbb{F}_q$ é isomorfo a O_P/P e, portanto, $grau(P) = 1$.

Seja $\mathbb{P}_F$ o conjunto de lugares em $F|\mathbb{F}_q$, $\overline{\mathcal{R}}$ o fecho inteiro de $\mathcal{R}$ em F e $S(\mathcal{R}) := \{Q \in \mathbb{P}_F : \mathcal{R} \subset O_Q\}$. Então, do teorema 1.56, temos que $\overline{\mathcal{R}} = \bigcap_{Q \in S(\mathcal{R})} O_Q$. Mostremos que $S(\mathcal{R}) = \mathbb{P}_F\backslash\{P\}$. (Observe que $P \notin S(\mathcal{R})$, pois existe $x \in \mathcal{R}$ tal que $\rho(x) > 0$ e logo $\upsilon_P(x) < 0$, ou seja, $\mathcal{R} \not\subset \mathcal{O}_P$.)

Tome $W := \{x \in \overline{\mathcal{R}} : \upsilon_P(x) > 0\}$. Então W é um $\mathbb{F}_q$-espaço vetorial. Observe que $W \cap \mathcal{R} = \{0\}$, pois se $x \in W \cap \mathcal{R}$, então $\upsilon_P(x) > 0$. Logo, $\rho(x) < \rho(1)$, ou seja, $x = 0$. Então $W \subset \frac{\overline{\mathcal{R}}}{\mathcal{R}}$ e, da proposição 3.5, segue que $dim W < \infty$. Agora, suponha que exista $T \in \mathbb{P}_F\backslash(S(\mathcal{R}) \cup \{P\})$. Pelo teorema da aproximação forte, podemos encontrar $x_i \in F$ para $i = 1, 2, ...$ tais que $\upsilon_P(x_i) = i$ e $\upsilon_Q(x_i) \geq 0$ para todo $Q \in \mathbb{P}_F\backslash\{T\}$, em particular, $x_i \in \bigcap_{Q \in S(\mathcal{R})} O_Q = \overline{\mathcal{R}}$. Logo $x_i \in W$, para todo i. Como, da definição de valorização discreta, $x_1, x_2, x_3, ...$ são linearmente independentes sobre $\mathbb{F}_q$, temos que $dim W = \infty$, absurdo. Portanto $S(\mathcal{R}) = \mathbb{P}_F\backslash\{P\}$, o que implica pela definição 3.6 que $\mathcal{R}$ é um anel de coordenadas afim de uma curva algébrica afim com exatamente um lugar P de grau 1 no infinito.

Mostremos agora a unicidade de d e $\upsilon(= \upsilon_P)$. Suponha que existam um inteiro positivo d_1 e uma valorização discreta υ_1 de $F|\mathbb{F}_q$ tal que $\rho(x) = -d_1\upsilon_1(x)$, para todo $x \in \mathcal{R}$. Então, da definição de valorização discreta, existe $f, g \in \mathcal{R}\backslash\{0\}$ tais que

$$1 = \upsilon_1(f/g) = \upsilon_1(f) - \upsilon_1(g) = \tfrac{-\rho(f)+\rho(g)}{d_1}.$$

Logo, $d_1 = \rho(g) - \rho(f) = -d\upsilon(f/g)$, ou seja, d divide d_1. De maneira análoga, tem-se que

d_1 divide d. Portanto, $d = d_1$. Agora, tomando P_1 o lugar correspondente a v_1, temos que $P_1 \in \mathbb{P}_F \backslash S(\mathcal{R}) = \{P\}$, ou seja, $P_1 = P$. Portanto $v_1 = v$.

■

Uma consequência natural deste teorema é o seguine resultado.

Corolário 3.8. *Seja $\mathcal{R}$ uma $\mathbb{F}_q$-álgebra. Se ρ_1, ρ_2 são funções pesos não-nulas de $\mathcal{R}$ então existe $d \in \mathbb{Q}$, positivo, tal que $\rho_1 = d\rho_2$.*

Agora estamos aptos a concluir o principal objetivo desta dissertação.

Seja $\mathcal{R}$ uma $\mathbb{F}_q$-álgebra com função peso ρ. Do teorema anterior, temos que $\mathcal{R}$ é um anel de coordenadas afim de uma curva algébrica $\mathcal{X}$ definida sobre $\mathbb{F}_q$ com exatamente um lugar P de grau 1 no infinito. Vimos também que $\mathcal{R} \subset \overline{\mathcal{R}} = \bigcap_{Q \in \mathbb{P}_F \backslash \{P\}} O_Q$.

Assim, sejam $P_1, ..., P_n$ pontos dois a dois distintos, $\mathbb{F}_q$-racionais de $\mathcal{X}$ diferentes de P. Considere a aplicação de avaliação

$$\begin{array}{rccc} av_{\mathcal{P}}: & \mathcal{R} & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & (f(P_1), ..., f(P_n)) \end{array}.$$

Sejam $D = P_1 + ... + P_n$ e G um divisor de F tal que $supp(D) \cap supp(G) = \emptyset$. Sabemos que $\mathcal{L}(G) = \{x \in \mathcal{R} | v_Q(x) \geq -v_Q(G), \forall Q \in \mathbb{P}_F\}$. Agora, observe que dado $x \in \mathcal{L}(G)$, como $\mathcal{R} \subset \bigcap_{Q \in \mathbb{P}_F \backslash \{P\}} O_Q$, temos que $v_Q(x) \geq 0$, para todo $Q \neq P$. Logo $v_P(x) < 0$ e como $v_P(x) \geq -v_P(G)$, temos que $m := v_P(G) > 0$. Assim, $P \in supp(G)$. Mas $\mathcal{L}(mP) = \{x \in \mathcal{R} : \rho(x) \leq m \; e \; v_Q(f) \geq 0, \forall Q \neq P\}$, então, segue que $\mathcal{L}(G) = \mathcal{L}(mP)$. Como $\mathcal{R}$ possui uma $\mathbb{F}_q$-base e $\mathcal{L}(G) \subset \mathcal{R}$, temos que os elementos da base de $\mathcal{R}$ formam uma base para $\mathcal{L}(G)$. Assim $\mathcal{L}(G) = \langle f_1, ..., f_l \rangle$ e portanto

$$E_l = av_{\mathcal{P}}(\mathcal{L}(G)) = av_{\mathcal{P}}(\mathcal{L}(mP)) = C(D, mP).$$

Portanto, podemos concluir que os códigos de avaliação construidos sobre álgebras com função peso são códigos de Goppa pontuais.

Vejamos alguns exemplos que ilustram o teorema 1.24, proposição 2.10 e os resultados acima.

Exemplo 3.9. *Considere a curva plana $\mathcal{X}$ definida pela equação $X^6 + Y^5 + Y = 0$ sobre o corpo $\mathbb{F}_4$. Seja $\mathcal{R}$ a $\mathbb{F}_4$-álgebra dada por $\mathcal{R} = \mathbb{F}_4[X, Y]/(X^6 + Y^5 + Y)$. Denotemos por x e*

y as classes residuais de X e Y, respectivamente. Então $\{x^\alpha y^\beta | \alpha < 6\}$ é uma base de $\mathcal{R}$. Suponha que $\mathcal{R}$ é munida de uma função peso ρ. Então, do teorema 3.7, segue que $\mathcal{R}$ é o anel de coordenadas afim da curva $\mathcal{X}$ com exatamente um lugar Q de grau 1 no infinito e que $\rho = -\upsilon_Q$. Determinemos os valores de ρ.

Seja $y \in \mathcal{R}$. Como $F = \mathbb{F}_4(x,y)|\mathbb{F}_4$ é o corpo de funções algébricas de uma variável sobre $\mathbb{F}_4$ e o polinômio $f(T) = T^6 + y(y^4+1)$ é o polinômio minimal de x sobre $\mathbb{F}_4(y)$, segue, do teorema 1.24, que

$$grau(y)_0 = grau(y)_\infty = [F : \mathbb{F}_4(y)] = 6.$$

Agora, como Q é o único pólo de y e grau $Q = 1$, temos que $\upsilon_Q(y) = -6$, ou seja, $\rho(y) = 6$. Mas, como $x^6 = -y^5 - y$, então

$$6\upsilon_Q(x) = \upsilon_Q(x^6) = \upsilon_Q(-y^5 - y) = min\{\upsilon_Q(y^5), \upsilon_Q(y)\} = 5\upsilon_Q(y)$$

e logo $\upsilon_Q(x) = -5$, ou seja, $\rho(x) = 5$.

Assim, tomando n pontos $\mathbb{F}_4$-racionas $P_1, ..., P_n$, dois a dois distintos, de $\mathcal{X}$ diferentes de Q e tomando D e G divisores de $F|\mathbb{F}_4$, como na descrição acima, segue, pela aplicação de avaliação, que o código de avaliação E_l é o código pontual $C(D, mQ)$, para algum $m \in \mathbb{N}$. Logo, $C_l = C_\Omega(D, mQ)$. Neste caso, o semigrupo de Weierstrass de Q é $\{0, 5, 6, 10, 11, 12, ...\}$ e tem gênero 10. Como feito no exemplo 2.22, a tabela abaixo nos fornece uma lista de valores de ρ_l, ν_l, $d(l)$ e $d_G(l)$.

l :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
f_l :	1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	x^3y	x^2y^2	xy^3	y^4	...
ρ_l :	0	5	6	10	11	12	15	16	17	18	20	21	22	23	24	...
ν_l :	2	2	3	4	3	4	6	6	4	5	8	9	8	9	10	...
$d(l)$:	2	2	3	3	3	4	4	4	4	5	8	8	8	9	10	...
$d_G(l)$:	−18	−13	−12	−8	−7	−6	−3	−2	−1	0	2	3	4	5	6	...

Exemplo 3.10. *A quártica de Klein sobre $\mathbb{F}_8$ com equação afim*

$$X^3Y + Y^3 + X = 0$$

é da forma $X^aY^c + uY^{b+c} + G(X,Y) = 0$, como na proposição 2.10, onde $a = 3$, $b = 2$, $c = d = 1$, $G(X,Y) = X$ e $u = 1$. Seja S a álgebra dada por $S = \mathbb{F}_8[X,Y]/(X^3Y + Y^3 + X)$ e denotemos as classes resíduais correspondentes a X e Y por x e y, respectivamente. Seja $\mathcal{R}$ a $\mathbb{F}_8$-subálgebra de S gerada pelos elementos $x^\alpha y^\beta$ tais que $\alpha < 3$ e $\alpha \leq 2\beta$. Então, da

proposição 2.10, temos que $\{1\} \cup \{x^\alpha y^\beta | \alpha < 3 \text{ e } 1 \leq \beta\}$ *é um base de* $\mathcal{R}$ *com* $\rho(1) = 0$ *e* $\rho(x^\alpha y^\beta) = 2\alpha + 3\beta$ *gerando uma função peso sobre* $\mathcal{R}$*. Então, do teorema 3.7, segue que* $\mathcal{R}$ *é um anel de coordenadas afim de uma curva algébrica afim* $\mathcal{X}$ *definida sobre* $\mathbb{F}_8$ *com exatamente um lugar* P *de grau 1 no infinito e* $\rho = -\upsilon_P$*, onde* υ_P *é a valorização correspondente a* P*.*

Agora, tomando $P_1, ..., P_n$*,* D *e* G *como na descrição acima, segue ,pela aplicação de avaliação, que o código de avaliação* E_l *é um código pontual* $C(D, mP)$*, para algum* $m \in \mathbb{N}$*. Logo,* $C_l = C_\Omega(D, mP)$ *e o semigrupo de Weierstrass de* P *é* $\{0, 3, 5, 6, 7, ...\}$ *com gênero* $g = 3$*. A seguinte tabela nos fornece uma lista de valores de* ρ_l*,* ν_l*,* $d(l)$ *e* $d_G(l)$*.*

l :	1	2	3	4	5	6	7	8	9	10	...
f_l :	1	y	xy	y^2	x^2y	xy^2	y^3	x^2y^2	xy^3	y^4	...
ρ_l :	0	3	5	6	7	8	9	10	11	12	...
ν_l :	2	2	3	2	4	4	5	6	7	8	...
$d(l)$:	2	2	2	2	4	4	5	6	7	8	...
$d_G(l)$:	-4	-1	1	2	3	4	5	6	7	8	...

Observe que $d(l) = d_G(l) = l - 2$*, para todo* $l \geq 6$*.*

APÊNDICE A

Noções de Álgebra Comutativa

Neste apêndice destacaremos os conceitos básicos, definições e resultados da álgebra comutativa que foram abordados ao longo do texto. Para maiores detalhes, recomendamos ao leitor às seguintes referências [1], [3], [8] e [9].

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,*

$M_1 \subseteq M_2 \subseteq ... \subseteq M_n \subseteq ...$ *então existe* $n_0 \in \mathbb{N}$ *tal que* $M_n = M_{n_0}$*, para todo* $n \geq n_0$
(resp. $M_1 \supseteq M_2 \supseteq ... \supseteq M_n \supseteq ...$ *então existe* $n_0 \in \mathbb{N}$ *tal que* $M_n = M_{n_0}$*, para todo* $n \geq n_0$*).*

Se $M = A$ é noetheriano (resp. artiniano) então dizemos que A é um **anel noetheriano** *(resp.* **anel artiniano***).*

Exemplo A.2. *1)Qualquer corpo K é noetheriano e artiniano.*
2) $\mathbb{Z}$ é um anel noetheriano (como $\mathbb{Z}$-módulo) mas não é anel artiniano.
3) Seja K um corpo. Se V é um K-espaço vetorial de dimensão finita então V é um K-módulo noetheriano e artiniano.
4) Todo domínio principal é noetheriano.

Abaixo, mencionamos alguns resultados sobre estas definições.

Proposição A.3. *Sejam M um A-módulo e N um A-submódulo de M. Então M é noetheriano (resp. artiniano) se, e somente se, N e M/N são noetherianos (resp. artinianos).*

Corolário A.4. *Se A é um anel noetheriano (resp. artiniano) e I é um ideal de A então A/I é um anel noetheriano (resp. artiniano).*

Definição A.5. *Seja A um anel e M um A-módulo. Dizemos que uma cadeia finita estrita de submódulos de M, i.é., $M = M_0 \supsetneqq M_1 \supsetneqq ... \supsetneqq M_n = (0)$, é uma* **série de composição** *se para todo $i = 0, ..., n-1$ não existe um submódulo N de M tal que $M_i \supsetneqq N \supsetneqq M_{i+1}$.*

Proposição A.6. *Seja M um A-módulo. Então M tem série de composição se, e somente se, M é noetheriano e artiniano.*

Observe que se M é noetheriano mas não é artiniano então M pode não admitir uma série de composição, por exemplo:

$$M = \mathbb{Z} \supsetneqq 2\mathbb{Z} \supsetneqq 4\mathbb{Z} \supsetneqq ... \supsetneqq 2^n\mathbb{Z} \supsetneqq ...$$

A partir dos resultados citados anteriormente tem-se como consequência os próximos dois resultados.

Corolário A.7. *Sejam K corpo e V um K-espaço vetorial. São equivalentes:*
i) $dim_K V = n < \infty$;
ii) V tem série de composição;
iii) V é noetheriano como K-módulo;
iv) V é artiniano como K-módulo.

Corolário A.8. *Sejam A um anel e $M_1, ..., M_n$ ideais maximais de A (não necessariamente distintos) tal que $M_1 \cdot ... \cdot M_n = (0)$. Então*

A é noetheriano se, e somente se, A é artiniano.

Vejamos a seguir algumas propriedades essenciais para caracterizar anéis artinianos em termos de anéis noetheriano.

Primeiro, sejam A um anel, I 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.9. *Se A é um anel noetheriano então A possui um número finito de ideais primos minimais.*

Proposição A.10. *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.*

Proposição A.11. *O nilradical de um anel artiniano (ou noetheriano) A, denotado por $\eta(A)$, é nilpotente.*

Assim, estamos em condições de enunciar e provar um dos principais resultados envolvendo anéis noetherianos e artinianos.

Teorema A.12. *A é um anel artiniano se, e somente se, A é um anel noetheriano e cada ideal primo de A é maximal.*

Dem. Suponha que A é artiniano. Então, segue, da proposição A.10, que cada ideal primo de A é maximal. Mais ainda, existe um número finito $P_1, ...P_n$ de ideais maximais de A. Como $\cap_{i=1}^n P_i = \eta(A)$ e da proposição A.11 existe $k \in \mathbb{N}$ tal que $\eta(A)^k = \{0\}$, segue que

$$\{0\} = \eta(A)^k = (\cap_{i=1}^n P_i)^k \supseteq \prod_{i=1}^n P_i^k, \text{ ou seja, } \prod_{i=1}^n P_i^k = \{0\}.$$

Logo, do corolário A.8, temos que A é noetheriano.

Suponha agora que A é um anel noetheriano e que cada cada ideal primo de A é maximal. Então, do fato de que cada ideal primo de A ser maximal, segue que os ideais primos de A são ideais primos minimais. Logo, da proposição A.9, existe um número finito $P_1, ...P_n$ de ideais primos de A. Novamente, como $\eta(A)$ é nilpotente, existe um $k \in \mathbb{N}$ tal que $\prod_{i=1}^n P_i^k = \{0\}$. Portanto, do corolário A.8, segue que A é artiniano. ■

Os próximos dois resultados são citados pois nos diz que todas as K-álgebras finitamente geradas são noetherianos.

Teorema A.13. (**Teorema da Base de Hilbert**) *Se A é um anel noetheriano então o anel de polinômios $A[X]$ é um anel noetheriano.*

Corolário A.14. *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.15. *Sejam A um anel e I um ideal de A.*
i) A **dimensão de Krull** *de A (ou simplismente dimensão de A), denotada por $dim_{Krull}A$, é definida como o sendo o supremo do comprimento das cadeias de ideais primos de A, isto é,*

$$dim_{Krull}A = sup\{n \in \mathbb{N} \mid \exists P_0 \subsetneqq P_1 \subsetneqq ... \subsetneqq P_n,\ P_i \in Spec(A)\}.$$

ii) 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,*

$$ht(I) = sup\{n \in \mathbb{N} | \exists P_0 \subsetneqq P_1 \subsetneqq ... \subsetneqq P_n = I,\ P_i \in Spec(A)\}.$$

Em geral, a altura de um ideal I de A é dada por:

$$ht(I) = inf\{ht(P) \mid P \text{ é ideal primo minimal de } I\}.$$

Exemplo A.16. *1) A é anel artiniano então $dim_{Krull}A = 0$*
2) Se $A = \mathbb{Z}$ então $dim_{Krull}A = 1$.
3) Se A é finito então $dim_{Krull}A = 0$.
4) Se $A = K[X_1, X_2, ...]$, com K corpo, então $dim_{Krull}A = \infty$.

Dadas estas definições, estamos em condições de enunciar dois dos principais resultados da teoria de dimensão de um anel comutativo, sendo que o segundo resultado usa-se de maneira fundamental o primeiro resultado..

Teorema A.17. (**Teorema de Krull para ideais principais**) *Sejam A um anel noetheriano e $I = (a) \neq A$ um ideal principal de A. Se $P \in Spec(A)$ é um primo minimal em cima de I então $ht(P) \leq 1$. Mais ainda, se $a \neq 0$ não for divisor de zero em A então $ht(P) = 1$.*

Teorema A.18. *Seja A um anel noetheriano de dimensão de Krull finita. Então a dimensão de Krull do anel de polinômios $A[X]$ é igual a $dim_{Krull}A + 1$.*

Uma consequência imediata do teorema anterior é o seguinte resultado:

Corolário A.19. *Se K é um corpo então a dimensão de Krull do anel $K[X_1, ..., X_n]$ é n.*

A.3 Dependência 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.20. *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 $x^n + a_1 x^{n-1} + ... + a_n = 0$.*

Exemplo A.21. *1) Seja $A = \mathbb{Z}$ e $B = \mathbb{C}$. Então $i \in \mathbb{C}$ é inteiro sobre $\mathbb{Z}$, pois $i^2 + 1 = 0$.*
2) Seja $A = \mathbb{Z}$ e $B = \mathbb{R}$ então $\sqrt{2} \in \mathbb{R}$ é inteiro sobre $\mathbb{Z}$, pois $(\sqrt{2})^2 - 2 = 0$.

Um primeiro resultado que caracteriza um elemento inteiro sobre um anel é dado pela seguinte proposição.

Proposição A.22. *Dados uma extensão de anéis $B|A$ e $x \in B$, são equivalentes:*
i) x é inteiro sobre A;
ii) $A[x] = \{g(x)|g(X) \in A[X]\}$ é um A-módulo finitamente gerado;
iii) 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.23. *Sejam $B|A$ uma extensão de anéis e $x_1, ..., x_n \in B$ inteiros dobre A. Então o anel $A[x_1, ..., x_n]$ é um A-módulo finitamente gerado.*

Corolário A.24. *Sejam $B|A$ uma extensão de anéis. Então*
i) Se $x, y \in B$ são inteiros sobre A então $x \pm y$ e $x \cdot y$ também são.
ii) $\overline{A} = \{x \in B|x$ é inteiro sobre $A\}$ é subanel de B que contém A. Tal anel é conhecido como o **fecho integral** *de A em B.*

Disto, temos as seguintes definições.

Definição A.25. *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.*

Exemplo A.26. *Sejam D um domínio e K seu corpo de frações. Se D é um domínio fatorial então D é integralmente fechado em K.*

Vejamos, a seguir, algumas propriedades fundamentais a respeito das extensões integrais.

Corolário A.27. *Se $B|A$ e $C|B$ são entensões integrais então $C|A$ é uma extensão integral.*

Proposição A.28. *Seja $B|A$ uma extensão integral de anéis. Se J é um ideal próprio de B e $I = J \cap A$ então B/J é integral sobre A/I.*

Proposição A.29. (**Lema de Noether**) *Seja $B|A$ uma extensão integral de anéis onde B é um domínio. Então B é corpo se, e somente se, A é um corpo. Neste caso, $B|A$ é uma extensão algébrica de corpos.*

Exemplo A.30. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ *é corpo, pois* $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$ *é uma extensão integral.*

Os próximos dois resultados são conhecidos como o Teorema de "Going-up".

Teorema A.31. *Sejam $B|A$ uma extensão integral e P um ideal primo de A. Então, existe um ideal primo Q em B tal que $Q \cap A = P$. Mais ainda, se $Q' \subseteq Q \in spec(B)$ então $Q' \cap A = P = Q \cap A$ se, e somente se, $Q' = Q$.*

Teorema A.32. *Seja $B|A$ uma extensão integral de anéis. Sejam $P_1 \subseteq P_2 \subseteq ... \subseteq P_n$ uma cadeia de ideais primos de A e $Q_1 \subseteq Q_2 \subseteq ... \subseteq Q_m$ $(m < n)$ uma cadeia de ideais primos de B tais que $Q_i \cap A = P_i$, para $1 \leq i \leq m$. Então a cadeia $Q_1 \subseteq Q_2 \subseteq ... \subseteq Q_m$ pode ser extendida a cadeia $Q_1 \subseteq ... \subseteq Q_m \subseteq ... \subseteq Q_n$ onde os $Q_{i's}$ são ideais primos de B e $Q_i \cap A = P_i$, para todo $1 \leq i \leq n$.*

Como o resultado abaixo é usado de maneira fundamental nesta dissertação, faremos sua demonstração aqui.

Corolário A.33. *Seja $B|A$ uma extensão integral de anéis. Então*

$$dim_{Krull} B = \dim_{Krull} A.$$

Dem. Afirmação 1: $dim_{Krull} B \leq \dim_{Krull} A$.
De fato, seja $Q_0 \subsetneqq Q_1 \subsetneqq ... \subsetneqq Q_n$ uma cadeia de ideais primos de B. Defina $P_i := Q_i \cap A \in spec(A)$. Então, da parte final do teorema A.31, $P_0 \subsetneqq P_1 \subsetneqq ... \subsetneqq P_n$ é uma cadeia de ideais primos de A. Portanto, da definiçao de dimensão, $dim_{Krull} B \leq \dim_{Krull} A$.

Afirmação 2: $dim_{Krull}B \geq \dim_{Krull} A$.
De fato, seja $P_0 \subsetneqq P_1 \subsetneqq ... \subsetneqq P_n$ uma cadeia de ideais primos de A. Do teorema A.31, existe $Q_0 \in spec(B)$ tal que $P_0 = Q_0 \cap A$. Logo, dos teoremas A.32 e A.31, existem $Q_1 \subsetneqq Q_2 \subsetneqq ... \subsetneqq Q_n \in spec(B)$ com $P_i = Q_i \cap A$ para $1 \leq i \leq n$ tais que $Q_0 \subsetneqq Q_1 \subsetneqq ... \subsetneqq Q_n$ é uma cadeia extendida de ideais primos de B. Portanto, $dim_{Krull}B \geq \dim_{Krull} A$.

■

A.4 Normalização de Noether

A idéia central nessa seção é de apresentar a parte da teoria da dimensão envolvendo a normalização de Noether de uma K-álgebra finitamente gerada.

Definição A.34. *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:*
i) O conjunto Ω é **algebricamente independente** *(ou transcendente) sobre K se satisfaz:*

$$\text{Dado } G = G(X_1, ..., X_n) \in B \text{ tem-se que } G(y_1, ..., y_n) = 0 \text{ se, e somente se, } G = 0.$$

Caso contrário, dizemos que Ω é algebricamente dependente.
ii) 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.

Observe que dados a extensão de anéis $K \subseteq R$ e $\Omega = \{y_1, ..., y_n\} \subset R$ então Ω é algebricamente independente sobre K se, e somente se, a K-subalgebra gerada por K e Ω, $A = K[y_1, ..., y_n]$, é isomorfa ao anel de polinômios $B = K[X_1, ..., X_n]$.

Dadas estas definições, estamos aptos a apresentar uma das versões do teorema de normalização de Noether para K-álgebras finitamente geradas sobre um corpo K. A partir de agora, K denotará um corpo e $B = K[X_1, ..., X_n]$ denotará o anel de polinômios em n variáveis sobre K.

Teorema A.35. *Seja $R = K[x_1, ..., x_n]$ uma K-álgebra finitamente gerada que é um domínio. Então apenas uma das seguintes afirmações é verdadeira:*
i) 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);

ii) 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.

Definição A.36. *Seja $R = K[x_1, ..., x_n]$ uma K-álgebra finitamente gerada que é um domínio. A extensão integral $K[z_1, ..., z_d] \subseteq R$, com $\Lambda = \{z_1, ..., z_d\}$ algebricamente independente sobre K é chamada de uma* **normalização de Noether** *de R.*

Definição A.37. *Dada uma extensão de corpos $K \subseteq L$ (isto é, K é subcorpo de L), dizemos que $\{x_1, ..., x_n\}$ gera L sobre K (ou que L é finitamente gerado, por $\{x_1, ..., x_n\}$, sobre K) se L é o corpo de frações do domínio $D = K[x_1, ..., x_n]$. Neste caso denotamos $L = K(x_1, ..., x_n)$.*

Um corpo do tipo $L = K(x_1, ..., x_n)$ tem um invariante numérico, $m \in \mathbb{N}$, chamado de grau de transcendência de $K \subseteq L$ e que é usualmente denotado por $grtr_K(L)$. Tal invariante será definido através dos conceitos e resultados que descreveremos abaixo.

Definição A.38. *Sejam $K \subseteq L$ uma extensão de corpos, com $L = K(x_1, ..., x_n)$, $d \in \mathbb{N}$ e $\alpha = \{y_1, ..., y_d\} \subset L$ (se $d = 0$ então $\alpha = \emptyset$). Dizemos que α é* **base de transcendência** *de $K \subseteq L$ se $\{y_1, ..., y_d\}$ é algebricamente independente sobre K e se $K(y_1, ..., y_d) \subseteq L$ é extensão algébrica.*

Lema A.39. *Sejam $K \subseteq L$ uma extensão de corpos, $\{y_1, ..., y_m\} \subset L$ um conjunto algebricamente independente sobre K e $w \in L$. Então, w é algébrico sobre $K(y_1, ..., y_m)$ se, e somente se, $\{y_1, ..., y_m, w\}$ é algebricamente dependente sobre K.*

Proposição A.40. *Seja $L = K(x_1, ..., x_n)$ um corpo finitamente gerado sobre o corpo K. Então,*
i) Existe $\alpha \subset \{x_1, ..., x_n\}$ tal que α é base de transcendência de $K \subseteq L$.
ii) Existe $\alpha = \{y_1, ..., y_d\}$, com $0 \leq d \leq n$, tal que $R = K[x_1, ..., x_n]$ é extensão integral de $A = K[y_1, ..., y_n]$ e α é base de transcendência de $K \subseteq L$.

Lema A.41. *Sejam $L = K(x_1, ..., x_n)$ um corpo finitamente gerado sobre o corpo K e $\alpha = \{y_1, ..., y_d\}$, $d \geq 1$, uma base de transcendência de $K \subseteq L$. Se $\beta = \{w_1, ..., w_k\} \subset L$, $k \geq 1$, é algebricamente independente sobre K então $k \leq d$.*

Como consequência natural do lema anterior estamos em condições de apresentar o resultado que define o grau de transcendência.

Proposição A.42. *Se L um corpo finitamente gerado sobre o corpo K então toda base de transcendência de $K \subseteq L$ tem o mesmo número, m, de elementos. Tal número m é chamado de* **grau de transcendência** *de $K \subseteq L$ e é denotado por $m = grtr_K(L)$.*

Definição A.43. *Se $R = K[x_1, ..., x_n]$ é uma K-álgebra finitamente gerada que é um domínio definimos o grau de transcendência de $K \subset R$ por $grtr_K(L)$, onde L é o corpo de frações de R. Vamos denotá-lo por: $grtr_K(R)$*

Uma relação entre o grau de transcedência e a dimensão de Krull de uma K-álgebra finitamente gerada que é um domínio é dada no resultado abaixo

Teorema A.44. *Se $R = K[x_1, ..., x_n]$ é uma K-álgebra finitamente gerada que é um domínio então*

$$dim_{Krull}R = grtr_K(R).$$

Dem. Seja L o corpo de frações de R. Pelos resultados citados acima, sabe-se que R é uma extensão integral de $A = K[y_1, ..., y_d]$, onde $d = grtr_K(L)$. Logo, do corolário A.33, tem-se que $dim_{krull}R = dim_{krull}A$. Mas, $\{y_1, ..., y_d\}$ são algebricamente independentes sobre K. Então, do corolário A.19, temos que $d = dim_{krull}A$. Portanto, $dim_{Krull}R = grtr_K(R)$. ■

Vejamos algumas consequências (não todas naturais) deste resultado. Aqui, uma K-álgebra finitamente gerada que é um domínio é dito ser um *domínio afim*.

Corolário A.45. *Se R é um domínio afim e I um ideal de R então,*

$$dim_{Krull}R = ht(I) + dim_{Krull}(R/I).$$

Corolário A.46. *Se R é um domínio afim e $f \in R$ não é uma unidade então,*

$$dim_{Krull}(R/\langle f\rangle)) = dim_{Krull}R - 1.$$

Corolário A.47. (**Teorema de Noether**) *Seja R um domínio afim sobre um corpo K. Sejam L o corpo de frações de R e F uma extensão de corpos finita de L. Se $\overline{R}$ é o fecho integral de R em F então $\overline{R}$ é finitamente gerado como R-módulo. Em particular, $\overline{R}$ é um domínio afim.*

APÊNDICE B

Curvas Algébricas

Este apêndice contém alguns conceitos básicos sobre curvas algébricas. Para maiores detalhes veja [4].

Ao longo deste, $\mathbb{F}$ denotará um corpo algebricamente fechado, $\mathbb{F}_q$ um corpo com q elementos cujo fecho algébrico é o próprio $\mathbb{F}$.

Seja n um inteiro não-negativo. O *espaço afim de dimensão* n, denotado por $\mathbb{A}^n(\mathbb{F})$ ou simplesmente por $\mathbb{A}^n$ (ou $\mathbb{F}^n$), é o conjunto de todas a n-uplas de elementos de $\mathbb{F}$. Um elemento $P = (a_1, ..., a_n) \in \mathbb{A}^n$ é dito ser um ponto de $\mathbb{A}^n$ e $a_1, ..., a_n$ são as coordenadas do ponto P.

Seja $\mathbb{F}[x_1, ..., x_n]$ o anel de polinômios em n variáveis sobre $\mathbb{F}$. Se $f \in \mathbb{F}[x_1, ..., x_n]$, dizemos que um ponto $P = (a_1, ..., a_n) \in \mathbb{A}^n$ é um *zero de* f se $f(P) = f(a_1, ..., a_n) = 0$.

No que segue, dado um ideal I de $\mathbb{F}[x_1, ..., x_n]$, definimos como um *conjunto algébrico afim* de $\mathbb{A}^n$ obtido a partir de I como sendo o conjunto

$$Z(I) = \{P = (a_1, ..., a_n) \in \mathbb{A}^n | f(P) = 0, \text{ para todo } f \in I\}.$$

Tal conjunto também é conhecido como o *conjunto dos zeros de* I.

Um conjunto algébrico afim $Z(I) \subset \mathbb{A}^n$ é dito ser *irredutível* se este não pode ser decomposto como como união de dois outros conjuntos algébricos próprios de $Z(I)$. De forma equivalente, temos que $Z(I)$ é irredutível se, e somente se, o radical de I for um ideal primo de $\mathbb{F}[x_1, ..., x_n]$.

Disto, temos as seguintes definições:

Definição B.1. *i) Se I é um ideal primo de $\mathbb{F}[x_1, ..., x_n]$, então o conjunto $\mathcal{X} = Z(I)$ dos zeros de I é dito ser uma* **variedade algébrica afim** (ou variedade afim).

ii) Dado uma variedade algébrica afim $\mathcal{X}$, definimos o seu **anel de coordenadas afim** *como sendo*

$$\mathbb{F}[\mathcal{X}] = \mathbb{F}[x_1, ..., x_n]/I.$$

Definição B.2. *Dada uma variedade algébrica afim $\mathcal{X}$ definimos o corpo de frações de $\mathbb{F}[\mathcal{X}]$, denotado por $\mathbb{F}(\mathcal{X})$, como sendo o* **corpo de funções racionais** *de $\mathcal{X}$. Os elementos de $\mathbb{F}(\mathcal{X})$ são chamados de* **funções racionais**.

A dimensão da variedade $\mathcal{X}$ é o grau de transcendência[1] de $\mathbb{F}(\mathcal{X})$ sobre $\mathbb{F}$. Caso $dim\mathcal{X} = 1$, então dizemos que $\mathcal{X}$ é uma *curva algébrica afim* (ou simplesmente *curva afim*). No caso em que $n = 2$, dizemos que $\mathcal{X}$ é uma *curva algébrica plana* e mais, uma curva plana irredutível é um conjunto algébrico afim da forma $\mathcal{X} = Z(f)$, onde f é um polinômio irredutível em $\mathbb{F}[x_1, x_2]$, ou seja,

$$\mathcal{X} = Z(f) = \{(a_1, a_2) \in \mathbb{A}^2 | f(a_1, a_2) = 0\}.$$

Os pontos da curva $\mathcal{X}$, cujas coordenadas estão sobre $\mathbb{F}_q$, são chamados de *pontos racionais*.

Neste caso, $\mathbb{F}(\mathcal{X})|\ \mathbb{F}$ é um corpo de funções algébricas de uma variável sobre $\mathbb{F}$, como introduzido no capítulo 1.

Agora, considere uma variedade afim $\mathcal{X}$ e P um ponto de $\mathcal{X}$. Observe que se $H(x_1, ..., x_n) + I = \tilde{H}(x_1, ..., x_n) + I$ então $H - \tilde{H} \in I$ e portanto $H(P) = \tilde{H}(P)$. Assim, dado $h = H(x_1, ..., x_n) + I \in \mathbb{F}[\mathcal{X}]$ podemos definir: $h(P) = H(P)$. Logo, o conjunto

$$O_P(\mathcal{X}) = \{f/g \in \mathbb{F}(\mathcal{X}) | f, g \in \mathbb{F}[\mathcal{X}] \text{ e } g(P) \neq 0\}$$

é um anel local que tem como corpo de frações o próprio $\mathbb{F}(\mathcal{X})$ e cujo ideal maximal é

$$M_P(\mathcal{X}) = \{f/g \in \mathbb{F}(\mathcal{X}) | f, g \in \mathbb{F}[\mathcal{X}], f(P) = 0 \text{ e } g(P) \neq 0\}.$$

Para finalizar, daremos duas outras importantes definições para melhor compreensão de alguns "dados"citados ao longo desta dissertação.

[1] ver apêndice A

Definição B.3. *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).

Neste caso, a derivada parcial de um polinômio é a sua derivada formal.

Agora, definiremos o que vem a ser uma curva algébrica plana absolutamente irredutível. Seja $f(x_1, ..., x_n)$ um polinômio em $\mathbb{F}_q[x_1, ..., x_n]$. Se f é irredutível em $\mathbb{F}[x_1, ..., x_n]$, onde $\mathbb{F}$ é o fecho algébrico de $\mathbb{F}_q$, dizemos que $f(x_1, ..., x_n)$ é *absolutamente irredutível em* $\mathbb{F}_q[x_1, ..., x_n]$.

Definição B.4. *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] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[2] C. Carvalho, C. Munuera, E. Silva e F. Torres, *Nears orders and codes*, c.s.IT/0603014.

[3] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol.150, Springer-Verlag, 1995.

[4] W. Fulton, *Algebraic Curves: an introduction to algebraic geometry*, Benjamin, 1969.

[5] A. Garcia, *Elementos de álgebra*, 2ed., IMPA, 2002.

[6] A. Hefez e M. L. T. Villela, *Códigos corretores de erros*, IMPA, 2002.

[7] T. Høholdt, J.H. van Lint, and R. Pellikaan, *Algebraic geometry codes*, in Handbook of Coding Theory, eds. V. Pless and W.C.Huffman, pp.871-961, Elsevier, 1998.

[8] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, 1985.

[9] S. Lang, *Algebra*, 3rd ed., Addison-Wesley, 1993.

[10] R. Matsumoto, *Linear codes on nonsingular curves are better than those on singular curves*, IEICE Trans. Fundamentals, vol.E82-A, no.4, pp. 665-670, Abril, 1999.

[11] R. Matsumoto, *Miura's generalization of one-point ag codes is equivalent to Hoholdt, van Lint and Pellikaan's generalization*, IEICE Trans. Fundamentals, vol.E82-A, no.10, pp.2007-2010, Outubro, 1999.

[12] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, 1993.

[13] I. Vainsencher, *Introdução às curvas algébricas planas*, Coleção Matemática Universitária, 1996.

ÍNDICE REMISSIVO