Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Tese de Doutorado

Funções Pesos Fracos sobre Variedades Algébricas

por

Rafael Peixoto[†]

Doutorado em Matemática - Campinas - SP

Orientador: Prof. Dr. Fernando Eduardo Torres Orihuela

Co-orientador: Prof. Dr. Cícero Fernandes de Carvalho

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

Funções Pesos Fracos sobre Variedades Algébricas

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

Campinas, 22 de Setembro de 2011.

Prof. Dr. Fernando Eduardo Torres Orihuela

Orientador

Prof. Dr. Cícero Fernandes de Carvalho

Coorientador

Banca examinadora:

1. Prof. Dr. Fernando Eduardo Torres Orihuela
2. Prof. Dr. Paulo Roberto Brumatti
3. Prof. Dr. Ercílio Carvalho da Silva
4. Prof. Dr. Reginaldo Palazzo Junior
5. Prof. Dr. Jose Gilvan Oliveira

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

FICHA CATALOGRÁFICA ELABORADA POR
MARIA FABIANA BEZERRA MÜLLER - CRB8/6162
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E
COMPUTAÇÃO CIENTÍFICA - UNICAMP

Peixoto, Rafael, 1983-
P359f Funções pesos fracos sobre variedades algébricas / Rafael Peixoto. - Campinas, SP : [s.n.], 2011.

Orientador: Fernando Eduardo Torres Orihuela.
Coorientador: Cícero Fernandes de Carvalho.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria da codificação. 2. Geometria algébrica. 3. Teoria da valorização. 4. Álgebra comutativa. I. Torres Orihuela, Fernando Eduardo, 1961-. II. Carvalho, Cícero Fernandes de. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

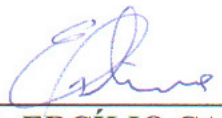
Informações para Biblioteca Digital

Título em inglês: Near weights on higher dimensional varieties
Palavras-chave em inglês:
Coding theory
Algebraic geometry
Valuation theory
Commutative algebra
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Fernando Eduardo Torres Orihuela [Orientador]
Ercílio Carvalho da Silva
Jose Gilvan Oliveira
Reginaldo Palazzo Junior
Paulo Roberto Brumatti
Data da defesa: 22-09-2011
Programa de Pós-Graduação: Matemática

Tese de Doutorado defendida em 22 de setembro de 2011 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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



Prof(a). Dr(a). ERCÍLIO CARVALHO DA SILVA

Prof(a). Dr(a). JOSE GILVAN OLIVEIRA

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

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

À minha "gordinha".

AGRADECIMENTOS

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

Ao meu orientador, Fernando Torres, e coorientador, Cícero Carvalho, pela credibilidade que depositaram em mim, pela paciência e por toda ajuda que me concederam com o seus extensos conhecimentos matemáticos.

Aos professores membros da Banca, pelos conselhos e sugestões.

À minha esposa Vanessa, pelo amor, carinho, companheirismo, pela paciência e por vários momentos felizes em minha vida. Além disso, à toda sua família sou muito grato.

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.

Aos meus avós, tios, primos e amigos, pelo apoio e carinho.

Aos professores do IMECC-UNICAMP, em especial ao professor Brumatti, o qual me orientou no mestrado, e aos professores do Departamento de Matemática da UFTM, pelo apoio e incentivo em prosseguir nesta jornada.

Ao CNPq, pelo apoio financeiro.

RESUMO

Definidas sobre uma $\mathbb{F}$-álgebra, os conceitos de função peso e função peso fraco foram introduzidos de forma a simplificar a teoria dos códigos corretores de erros que utilizam ferramentas da geometria algébrica. Porém, todos os códigos suportados por estes conceitos estão intimamente ligados à códigos provenientes de curvas algébricas, ou seja, os códigos geométricos de Goppa. Uma modificação da noção de função peso foi apresentada permitindo assim construir códigos lineares sobre variedades algébricas. Nesta tese, apresentamos uma generalização da teoria de funções pesos fracos que possibilitou a construção de códigos sobre variedades de dimensão arbitrária. Determinamos uma cota para a distância mínima destes códigos, e finalmente, apresentamos uma caracterização tanto para as álgebras munidas de funções pesos quanto para as álgebras munidas de um conjunto especial de funções pesos fracos.

Palavras-Chave: Função peso, função peso fraco, códigos corretores de erros, conjunto admissível.

ABSTRACT

Defined on a $\mathbb{F}$-algebra, the concepts of weight and near weight function were introduced to simplify the theory of error correcting codes using tools from algebraic geometry. However, all codes supported by these theories are geometric Goppa codes. The concept of weight function was generalized and used to construct linear codes on algebraic varieties. In this thesis, we present a generalization of near weights theory able to construct codes on higher dimensional varieties, and we define a formula for the minimum distance of such codes. Finally, we characterize the algebras with a weight function and the algebras admitting a special set of two near weight functions.

Key words: weight function, near weight function, error-correcting codes, admissible set.

SUMÁRIO

INTRODUÇÃO

A teoria de códigos corretores de erros foi introduzida em 1948, por C. E. Shannon, e desde então vem sendo amplamente desenvolvida. Uma importante revelação desta teoria se deu na década de 80. Baseado em uma curva algébrica projetiva $\mathcal{X}$ irredutível e não-singular definida sobre um corpo finito $\mathbb{F}$ e dois divisores $\mathbb{F}$-racionais de $\mathcal{X}$, a saber, $D = P_1 + ... + P_n$ e $G = \alpha_1 Q_1 + ... + \alpha_m Q_m$, onde $P_1, ..., P_n$ e $Q_1, ..., Q_m$ são pontos racionais distintos de $\mathcal{X}$ e $\alpha_1, ..., \alpha_m \in \mathbb{Z}$, V. D. Goppa, em 1981, construiu os conhecidos *Códigos Geométricos de Goppa*

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), ..., f(P_n)) \in \mathbb{F}^n : f \in \mathcal{L}(G)\}, \text{ e}$$
$$C_{\Omega}(D, G) = \{(res_{P_1}(\omega), ..., res_{P_n}(\omega)) \in \mathbb{F}^n : \omega \in \Omega(G - D)\} = C_{\mathcal{L}}(D, G)^{\perp}.$$

Porém, a compreensão destes códigos exigia do leitor um conhecimento aprofundado sobre geometria algébrica e teoria de corpos de funções. Devido a isto, vários pesquisadores passaram a buscar por métodos mais "simples"de se chegar a estes códigos. Então, em 1998, Høholdt, van Lint e Pellikaan apresentaram em [H-vL-P] uma construção alternativa à de Goppa. Baseados em uma $\mathbb{F}$-álgebra $\mathcal{R}$ (anel comutativo com unidade) e no semigrupo numérico $\mathbb{N}_0$, os autores introduziram o conceito de *Função Peso* ($\rho : \mathcal{R} \to \mathbb{N}_0 \cup \{-\infty\}$), e a partir desta definição construíram códigos lineares "sem"o uso de geometria algébrica, obtendo dentre eles os códigos geométricos de

Goppa pontuais.

Uma caracterização das álgebras munidas destas funções foi dada posteriormente em [Ma]. Neste artigo, Matsumoto provou que tais álgebras são anéis de coordenadas afins de curvas algébricas projetivas com exatamente um ponto racional no infinito, e que as funções pesos são restrições de valorizações discretas de posto um associadas a tais pontos. Disto, concluiu-se que todos os códigos construídos a partir de funções pesos são códigos de Goppa pontuais.

Em 2002, Geil e Pellikaan apresentaram em [Ge-Pe] uma generalização do conceito de função peso. Tal conceito, que antes era definido de uma $\mathbb{F}$-álgebra $\mathcal{R}$ sobre o semigrupo numérico, passou a ser definido sobre um semigrupo ordenado Γ qualquer, permitindo então obter códigos corretores de erros sobre variedades algébricas, aos quais serão apresentados no Capítulo 1. Alguns resultados sobre as estruturas das álgebras munidas destas funções são expostos no Capítulo2, tendo em destaque os resultados Teorema 2.5, Corolário 2.6 e Proposição 2.7, onde provamos que sob certas condições, as álgebras munidas de funções pesos são anéis de coordenadas afins de variedades algébricas projetivas cuja a normalização possui pelo menos um divisor irredutível (ver definição 1.13) no infinito. Ao final deste, ilustramos, na Observação 2.8, o resultado acima, mostrando que, para a superfície quádrica não-singular $XY - ZW = 0$ em $\mathbb{P}^3$, a qual possui dois divisores irredutíveis no infinto, é possível construir uma função peso sobre o seu anel de coordenadas afins.

Independente desta generalização, o conceito de função peso, quando definida sobre um semigrupo numérico, produzia apenas os códigos de Goppa pontuais. Assim, em 2004, uma modificação desta definição permitiu estender esta construção. Em [Si], Silva introduziu as *Funções Pesos Fracos*. Funções que também são definidas de uma $\mathbb{F}$-álgebra $\mathcal{R}$ sobre o semigrupo numérico e são utilizadas para construir códigos lineares, sendo agora dentre eles, os códigos geométricos de Goppa bi-pontuais. Tais resultados foram publicados em [NOC], e recentemente, em [Ca-Si], eles foram estendidos para os códigos de Goppa suportados em m pontos racionais. Para tal construção, é necessário que a $\mathbb{F}$-álgebra $\mathcal{R}$ admita m funções pesos fracos satisfazendo a propriedade de ser um

Conjunto Completo (ver [Ca-Si], definição 2.2 e [NOC], definição 4.4).

Resultados similares aos de Matsumoto sobre as estruturas das álgebras são dados em [Mu-To] e [Ca-Si]. Em [Mu-To], os autores provam que se uma $\mathbb{F}$-álgebra admite um conjunto completo de duas funções pesos fracos então esta álgebra é o anel de coordenadas afins de uma curva algébrica projetiva irredutível com exatamente dois pontos no infinito, enquanto que em [Ca-Si], tal resultado é generalizado utilizando m funções pesos fracos, concluindo assim que os códigos construídos por esta teoria são códigos de Goppa m-pontuais.

Neste trabalho, vamos apresentar uma generalização do conceito de função peso fraco, agora definindo-a sobre um semigrupo ordenado, permitindo assim construir estas funções sobre variedades algébricas de dimensões arbitrárias, diferentemente do caso anterior, que estava apenas ligado à curvas algébricas (ver [Mu-To] e [Ca-Si]). Este "novo"conceito de função peso fraco, será introduzido no Capítulo 3, (Definição 3.1), onde também destacamos dois métodos de obter estas funções; um utilizando de teoria de valorizações sobre corpos de funções de variedades algébricas (Seção 3.2, Proposição 3.10): Se $\mathcal{R}$ é o domínio afim de uma variedade projetiva $\mathcal{X}$ irredutível e definida sobre um corpo $\mathbb{F}$ com k divisores irredutíveis $C_1, ..., C_k$ no infinito, e se ν_i, para $i \in \{1, ..., k\}$, são valorizações no corpo de funções $\mathbb{F}(\mathcal{X})$ tais que:

a) $r.posto(\nu_i) = dim\mathcal{X} = d$, e

b) ν_i está centrada em um ponto $\mathbb{F}$-racional não-singular $Q_i \in C_i \subset \mathcal{X}$,

então as funções $\rho_i : \mathcal{R} \to \Gamma_i \cup \{-\infty\}$, definidas por

$$\rho_i(f) = \begin{cases} -\infty & , \ se \ f = 0; \\ \mathbf{0} & , \ se \ \nu_i(f) \succeq_i \mathbf{0}; \\ -\nu_i(f) & , \ se \ \nu_i(f) \prec_i \mathbf{0}. \end{cases}$$

onde $\Gamma_i := \{-\nu_i(f) : f \in \mathcal{R} \text{ e } \nu_i(f) \prec_i \mathbf{0}\} \cup \{\mathbf{0}\}$, são funções pesos fracos em R; e outro utilizando de teoria de bases de Gröbner sobre ideais tóricos (Seção 3.4): Sobre um subconjunto $\mathcal{A} = \{a_1, ..., a_n\} \subset \mathbb{Z}^d$, definimos o *anel tórico* $\mathbb{F}[X_1, ..., X_n]/I_{\mathcal{A}}$, onde

$$I_{\mathcal{A}} := (\mathbf{X}^{\alpha} - \mathbf{X}^{\beta} : \alpha, \beta \in \mathbb{N}_0^n, \ \omega(\mathbf{X}^{\alpha}) = \omega(\mathbf{X}^{\beta})),$$

e, construímos a função peso fraco $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ definida por

$$\rho(f) = \begin{cases} -\infty & , \text{ se } f = 0; \\ \mathbf{0} & , \text{ se } f \neq 0 \text{ e } \omega(f) \preceq \mathbf{0}; \\ \omega(f) & , \text{ se } \omega(f) \succ \mathbf{0}, \end{cases}$$

onde $\Gamma := \{\gamma \in \mathbb{N}_0\mathcal{A} : \mathbf{0} := (0, ..., 0) \preceq \gamma\} \subseteq \mathbb{N}_0\mathcal{A}$.

No capítulo 4, veremos como esta teoria pode ser usada para construir códigos lineares. Determinaremos uma cota para a distância mínima do código dual $C(\alpha)$ (ver Definição 4.1) e a ilustraremos em alguns exemplos. Finalizaremos este capítulo mostrando que esta cota, quando calculada sobre códigos baseados em curvas algébricas, é, em alguns casos, melhor que a cota de Goppa.

No último capítulo, assim como no capítulo 2, apresentaremos uma caracterização para as álgebras agora munidas de um conjunto admissível de duas funções pesos fracos (ver Definição 3.28). Mostraremos, na Proposição 5.14, uma relação entre a dimensão destas álgebras e os postos racionais dos semigrupos de valores destas duas funções, e, no Teorema 5.16, Corolário 5.17 e Proposição 5.18, provaremos que sob certas hipóteses, tais álgebras são anéis de coordenadas afins de variedades algébricas projetivas cuja normalização possui pelo menos dois divisores irredutíveis no infinito.

Por fim, no apêndice A, introduzimos os conceitos básicos e resultados da teoria de valorizações que serão utilizados ao longo de todo o texto.

CAPÍTULO 1

FUNÇÕES ORDENS

Uma generalização do conceito de função ordem é dada, possibilitando a construção destas funções sobre álgebras de dimensão de Krull maiores ou iguais a um, e consequentemente a construção de códigos lineares sobre tais álgebras. Porém, este novo conceito requer alguns conhecimentos sobre semigrupos ordenados. Assim, neste capítulo, introduzimos alguns conceitos básicos da teoria de semigrupos, que serão utilizados ao longo de todo o texto, a "nova"definição de uma função ordem, e a construção de códigos algébricos utilizando tais funções.

1.1 Semigrupos

Definição 1.1. Seja Γ um conjunto com uma operação binaria $+$, e seja 0 um elemento em Γ. Dizemos que $(\Gamma, +, 0)$ é um *monóide comutativo* se são satisfeitas as seguintes condições: para quaisquer $\alpha, \beta, \gamma \in \Gamma$,

1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$; (associativo)
2. $\alpha + \beta = \beta + \alpha$; (comutativo)
3. $\alpha + 0 = \alpha = 0 + \alpha$. (elemento neutro)

Um monóide comutativo $(\Gamma, +, 0)$ é chamado um *semigrupo* se este tem a propriedade do cancelamento, isto é, para quaisquer $\alpha, \beta, \gamma \in \Gamma$,

$$\text{se } \alpha + \beta = \gamma + \beta \text{ então } \alpha = \gamma.$$

Definição 1.2. Um semigrupo $(\Gamma, +, 0)$ é dito ser

1. *livre de inverso*, se para quaisquer $\alpha, \beta \in \Gamma$ tais que $\alpha + \beta = 0$ então $\alpha = \beta = 0$;

2. *livre de torção*, se para qualquer $\alpha \in \Gamma$ tal que $\underbrace{\alpha + \cdots + \alpha}_{n \text{ vezes}} = 0$, para algum $n \in \mathbb{N}$, então $\alpha = 0$; e

3. *finitamente gerado*, se Γ é gerado por um numero finito de seus elementos, a saber, se existem $\alpha_1, ..., \alpha_n \in \Gamma$ tais que, para qualquer elemento $\gamma \in \Gamma$, existem $\lambda_1, ..., \lambda_n \in \mathbb{N}_0$ tais que

$$\gamma = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n.$$

Neste caso, denotamos $\Gamma := \langle \alpha_1, ..., \alpha_n \rangle$.

Observe, da definição acima, que todo semigrupo livre de inverso é um semigrupo livre de torção.

Definição 1.3. Dado um semigrupo $(\Gamma, +, 0)$, definimos a relação $\sim$ em $\Gamma \times \Gamma$ por $(\alpha, \beta) \sim (\gamma, \delta)$ se, e somente se, $\alpha + \delta = \beta + \gamma$. Então $\sim$ é uma relação de equivalência. A classe de equivalência de (α, β) é denotada por $[\alpha, \beta]$ e o conjunto das classes de equivalência é denotado por $G(\Gamma)$. Defina $[\alpha, \beta] + [\gamma, \delta] = [\alpha + \gamma, \beta + \delta]$. Então esta operação $+$ está bem definida e dá a $G(\Gamma)$ uma estrutura de grupo comutativo que é chamado de *grupo de diferenças* de Γ.

Observação 1.4. Seja $(\Gamma, +, 0)$ um semigrupo finitamente gerado. Então $G(\Gamma)$ é um grupo abeliano finitamente gerado. Então, da estrutura dos grupos abelianos finitamente gerados (ver [La],cap.1,§10 e [Ga-Le], cap.IX,§1), segue que $G(\Gamma)$ é isomorfo a $T(G(\Gamma)) \oplus$

$\mathbb{Z}^r$, para algum $r \in \mathbb{N}_0$, onde $T(G(\Gamma))$ é o subgrupo de torção de $G(\Gamma)$. Assim, se Γ é um semigrupo livre de torção e finitamente gerado, então $G(\Gamma) \cong \mathbb{Z}^r$, para algum $r \in \mathbb{N}_0$ ([Shif], §1).

Definição 1.5. Seja $(\Gamma, +, 0)$ um monóide comutativo. Uma ordem parcial $\preceq$ em Γ é chamada *admissível (ou compatível)* se para quaisquer $\alpha, \beta, \gamma \in \Gamma$, temos

1. $0 \prec \alpha$, quando $\alpha \neq 0$, e
2. se $\alpha \prec \beta$ então $\alpha + \gamma \prec \beta + \gamma$.

Uma ordem total admissível em Γ pode ser extendida a uma ordem total admissível[1] em $G(\Gamma)$ através de:

$$[\alpha, \beta] \preceq [\gamma, \delta] \text{ se, e somente se, } \alpha + \delta \preceq \beta + \gamma.$$

Definição 1.6. Seja $(\Gamma, +, 0)$ um semigrupo. Dizemos que Γ é um semigrupo *bem ordenado* se este é um semigrupo totalmente ordenado por uma ordem admissível $\preceq$ e se toda sequência decrescente, com respeito a $\preceq$, de elementos de Γ admite elemento mínimo em Γ.

Observação 1.7 ([Shif],§1)**.** 1. Um semigrupo bem ordenado é livre de inverso, e portanto livre de torção.
2. Um semigrupo finitamente gerado livre de inverso com uma ordem total admissível é bem ordenado.

Definição 1.8. Seja $(\Gamma, +, 0)$ um semigrupo. Definimos o *posto racional* do semigrupo Γ por

$$r.posto(\Gamma) := r.posto(G(\Gamma)) = dim_{\mathbb{Q}}(G(\Gamma) \otimes_{\mathbb{Z}} \mathbb{Q}),$$

onde $G(\Gamma)$ é o grupo de diferenças de Γ.

Exemplo 1.9. Seja $(\Gamma, +, 0)$ um semigrupo livre de inverso finitamente gerado. Então da observação 1.4, existe $r \in \mathbb{N}_0$ tal que $G(\Gamma) \cong \mathbb{Z}^r$. Logo, da definição acima, temos que $r.posto(\Gamma) = r$.

[1] se $a \preceq b$ então $a + c \preceq b + c, \forall a, b, c \in G(\Gamma)$

Vejamos agora alguns exemplos de ordens sobre $\mathbb{Z}^r$.

Sejam $\alpha = (\alpha_1, ..., \alpha_r)$ e $\beta = (\beta_1, ..., \beta_r)$ elementos quaisquer de $\mathbb{Z}^r$.

- **Ordem Lexicográfica** ($\prec_{lex}$)

$$\alpha \prec_{lex} \beta \Leftrightarrow \begin{cases} \alpha_i = \beta_i, & \text{para todo } i < j \\ \alpha_j < \beta_j, & \text{para algum } j \in \{1, ..., r\}. \end{cases}$$

- **Ordem Lexicográfica Graduada** ($\prec_{grlex}$)

$$\alpha \prec_{grlex} \beta \Leftrightarrow \begin{cases} \sum_{i=1}^r \alpha_i < \sum_{i=1}^r \beta_i, & \text{ou} \\ \sum_{i=1}^r \alpha_i = \sum_{i=1}^r \beta_i \text{ e } \alpha \prec_{lex} \beta. \end{cases}$$

- **Ordem Lexicográfica Graduada com pesos** ($\prec_{\mathbb{R}}$)

Sejam $w_1, ..., w_r \in \mathbb{R}_+$, onde $\mathbb{R}_+$ é o conjunto dos números reais positivos. Se estes elementos são racionalmente independentes (ver A.2), então dizemos que

$$\alpha \prec_{\mathbb{R}} \beta \Leftrightarrow \begin{cases} \sum_{i=1}^r \alpha_i w_i < \sum_{i=1}^r \beta_i w_i. \end{cases}$$

Se $w_1, ..., w_r$ são elementos racionalmente dependentes, então dizemos que

$$\alpha \prec_{\mathbb{R}} \beta \Leftrightarrow \begin{cases} \sum_{i=1}^r \alpha_i w_i < \sum_{i=1}^r \beta_i w_i, & \text{ou} \\ \sum_{i=1}^r \alpha_i w_i = \sum_{i=1}^r \beta_i w_i \text{ e } \alpha \prec_{lex} \beta. \end{cases}$$

1.2 Funções Ordens

Sejam $\mathcal{R}$ uma $\mathbb{F}$-álgebra, isto é, $\mathcal{R}$ é um anel comutativo com unidade contendo um corpo $\mathbb{F}$, e $(\Gamma, \preceq)$ um semigrupo bem ordenado. Adicionamos a Γ um elemento $-\infty$ e estendemos a ordem $\preceq$ a $\Gamma \cup \{-\infty\}$ por $-\infty \prec \alpha$ para todo $\alpha \in \Gamma$, e estendemos a adição a $\Gamma \cup \{-\infty\}$ por $-\infty + \alpha = (-\infty) + (-\infty) = -\infty$.

Definição 1.10. Seja $\mathcal{R}$ uma $\mathbb{F}$-álgebra. Uma função $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ é chamada uma *função ordem* sobre $\mathcal{R}$ se esta é sobrejetiva e são satisfeitas as seguintes condições: para $f, g, h \in \mathcal{R}$,

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

(O.2) $\rho(\lambda f) = \rho(f)$, para todo $\lambda \in \mathbb{F}^*$;

(O.3) $\rho(f + g) \preceq max\{\rho(f), \rho(g)\}$;

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

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

Se, além dos axiomas anteriores, também é satisfeita a condição:

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

então dizemos que ρ é uma *função peso* em $\mathcal{R}$.

Denotamos a tripla $(\mathcal{R}, \rho, \Gamma)$ por uma *estrutura ordem (peso)* sobre o corpo $\mathbb{F}$, se $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ é uma função ordem (peso) sobre $\mathbb{F}$, e chamamos Γ o *semigrupo de valores* de ρ.

Exemplo 1.11. Considere o anel de polinômios $\mathcal{R} = \mathbb{F}[X_1, ..., X_n]$ e o semigrupo ordenado $(\mathbb{N}_0^n, <_L)$, onde $<_L$ é a ordem lexicográfica em $\mathbb{N}_0^n$. Para $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}_0^n$ denote $X^\alpha = X_1^{\alpha_1} \cdot ... \cdot X_n^{\alpha_n}$. Para $f = \sum_\alpha \lambda_\alpha X^\alpha \in \mathcal{R}$, com $\lambda_\alpha \in \mathbb{F}$, temos que a função $\rho : \mathcal{R} \to \mathbb{N}_0^n \cup \{-\infty\}$ definida por:

$$\rho(f) = \begin{cases} -\infty & \text{, se } f = 0; \\ \max\{\alpha : \lambda_\alpha \neq 0\} & \text{, se } f \neq 0. \end{cases}$$

é uma função peso em $\mathcal{R}$.

Exemplo 1.12 ([H-vL-P],§3, ex.3.8)**.** Considere $\mathcal{X}$ uma curva algébrica projetiva 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 têm pólos, possivelmente, no ponto P, ou seja,

$$\mathcal{R} = \bigcap_{Q \in \mathcal{X} \setminus \{P\}} \mathcal{O}_Q(\mathcal{X}),$$

onde $\mathcal{O}_Q(\mathcal{X})$ é o anel local associado a Q. Seja ν_P a valorização em P. Então, definindo $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$, com $(\Gamma, \leq) \subset (\mathbb{N}_0, \leq)$, por $\rho(f) = -\nu_P(f)$ para $f \in \mathcal{R}$, temos, das propriedades de valorização discreta, que ρ é uma função peso.

Para $\mathcal{X} = V(X^5 - Y^4 - Y)$ (curva hermitiana) sobre o corpo $\mathbb{F}_{16}$ e $\mathcal{R} = \mathbb{F}_{16}[X,Y]/(X^5 - Y^4 - Y)$, temos que $\rho(x^\alpha y^\beta) = 4\alpha + 5\beta$ é uma função peso sobre $\mathcal{R}$ com semigrupo de valores $\Gamma = \langle 4, 5\rangle \subset \mathbb{N}_0$.

Um exemplo mais geral envolvendo valorizações e variedades algébricas de dimensão arbitrária é dado a seguir.

Seja $\mathcal{X}$ uma variedade algébrica irredutível definida sobre um corpo $\mathbb{F}$, de dimensão d, e seja $\mathbb{F}(\mathcal{X})|\mathbb{F}$ o seu corpo de funções.

Definição 1.13. Um *divisor irredutível* em $\mathcal{X}$ é uma subvariedade C de $\mathcal{X}$ irredutível e definida sobre $\mathbb{F}$ de codimensão 1 (isto é, $dim(C) = d - 1$) tal que o anel local $\mathcal{O}_C(\mathcal{X})$ é integralmente fechado em $\mathbb{F}(\mathcal{X})$.

Teorema 1.14 ([Li],§3,teorema 2)**.** *Seja $\mathcal{R}$ um domínio afim sobre $\mathbb{F}$, isto é, $\mathcal{R} \cong \mathbb{F}[X_1, ..., X_n]/I$, onde I é um ideal primo. Seja $\mathcal{X}$ o fecho projetivo de $V(I)$ em $\mathbb{P}^n$ e seja C a interseção de $\mathcal{X}$ com o hiperplano no infinito. Assuma que C é um divisor irredutível em $\mathcal{X}$. Seja ν qualquer valorização do corpo de funções $\mathbb{F}(\mathcal{X})$ tal que*

i) o posto racional de ν é $d = dim\mathcal{X}$;

ii) ν está centrada em um ponto racional não-singular $Q \in C \subset \mathcal{X}$, e

iii) $\nu(f) \preceq 0$ para todo $f \in \mathcal{R}$.

Então $\rho = -\nu|_R$ é uma função peso em $\mathcal{R}$.

Aqui $\mathcal{R}$ pode ser visto como um subanel de $\mathbb{F}(\mathcal{X})$ consistindo de funções com pólos em C, ou seja,

$$\mathcal{R} = \bigcap_{D \in \mathcal{X} \setminus \{C\}} \mathcal{O}_D(\mathcal{X}),$$

onde D percorre todos os divisores irredutíveis de $\mathcal{X}$, exceto C, e $\mathcal{O}_D(\mathcal{X})$ é o anel local associado a D.

Exemplo 1.15 ([Su],§3,ex.3.1)**.** Seja $\mathbb{P}^2$ o plano projetivo parametrizado por $\mathbb{F}[X,Y,Z]$. Seja C a linha $Z = 0$ e P o ponto $(0:1:0)$. Seja $\mathcal{R} = \mathbb{F}[x,y]$, onde $x = X/Z$ e $y = Y/Z$.

Considere o corpo de funções $\mathbb{F}(x,y)$ de $\mathbb{P}^2$. Então $1/y$ é um parâmetro local de C em $\mathbb{P}^2$ e x/y é um parâmetro local de P em C. Assim, é possível construir uma valorização ν de $\mathbb{F}(x,y)$ em $\mathbb{Z}^2 \cup \{+\infty\}$, ordenado pela ordem lexicográfica, da seguinte forma:

$$\nu(0) = +\infty,\ \nu(1/y) = (1,0) \text{ e } \nu(x/y) = (0,1).$$

Logo, $\nu(y) = (-1,0)$ e $\nu(x) = (-1,1)$. Então $\rho : \mathcal{R} \to \langle (1,-1),(1,0)\rangle \cup \{-\infty\}$ dada por $\rho(f) = -\nu_{|\mathcal{R}}(f)$ é uma função peso em $\mathcal{R}$.

Vejamos agora algumas propriedades de funções ordens.

Proposição 1.16 ([Ge-Pe], prop.2.5, [H-vL-P], lema 3.9)**.** *Seja $(\mathcal{R},\rho,\Gamma)$ uma estrutura ordem em $\mathcal{R}$. Temos as seguintes propriedades para a função ordem:*

(1) Se $\rho(f) = \rho(g)$, então $\rho(fh) = \rho(gh)$ para todo $h \in \mathcal{R}$.

(2) Se $\rho(f) \neq \rho(g)$ então $\rho(f+g) = max_{\prec}\{\rho(f),\rho(g)\}$.

(3) Se $f \in \mathcal{R}\backslash\{0\}$, então $\rho(1) \preceq \rho(f)$.

(4) $\mathbb{F} = \{f \in \mathcal{R} : \rho(f) \preceq \rho(1)\}$.

(5) O elemento $\lambda \in \mathbb{F}^*$ no axioma (O.5) de função ordem é único.

Observe que, destas propriedades, $\mathcal{R}$ pode ser visto como uma união de dois conjuntos, isto é, $\mathcal{R} = \mathcal{M} \cup \mathcal{U}$ onde

$$\mathcal{M} = \{f \in \mathcal{R} : \rho(1) \prec \rho(f)\}, \text{ e } \mathcal{U} = \{f \in \mathcal{R} : \rho(f) \preceq \rho(1)\}.$$

Neste caso, $\mathcal{U}^* := \mathcal{U}\backslash\{0\} = \{f \in \mathcal{R} : \rho(f) = \rho(1)\} = \mathbb{F}^*$.

Uma consequência imediata da definição de função ordem é dada a seguir.

Lema 1.17 ([Ge-Pe],§2,prop.2.4)**.** *Seja $(\mathcal{R},\rho,\Gamma)$ uma estrutura ordem em $\mathcal{R}$. Seja S uma $\mathbb{F}$-subálgebra de $\mathcal{R}$. Então para $\Lambda = \{\rho(f) : f \in S, f \neq 0\} \subseteq \Gamma$, temos que a restrição de ρ sobre S, isto é, $\rho_{|S} : S \to \Lambda_{-\infty}$, é uma função ordem em S.*

Proposição 1.18 ([Ge-Pe], prop.2.6, [H-vL-P], prop. 3.10)**.** *Se existe uma função ordem em $\mathcal{R}$, então $\mathcal{R}$ é um domínio de integridade.*

Uma $\mathbb{F}$-álgebra munida de uma função ordem é dita ser um *domínio ordem*.

Porém, a recíproca da proposição anterior é falsa. Por exemplo, para o anel $\mathcal{R} = \mathbb{F}[X,Y]/(XY-1)$, temos que $\mathcal{R}$ é uma $\mathbb{F}$-álgebra que é um domínio, mas não existe função ordem sobre $\mathcal{R}$, pois caso contrário, tomando x e y as classes de X e Y, respectivamente, e ρ uma função ordem em $\mathcal{R}$, então temos, das propriedades de função ordem, que $\rho(1) \prec \rho(x) \prec \rho(xy) = \rho(1)$, contradição.

1.3 Bases de um Domínio Ordem

Agora, estamos interessados em encontrar bases de um domínio ordem como um $\mathbb{F}$-espaço vetorial. Sejam $\mathcal{R}$ uma $\mathbb{F}$-algebra e $(\Gamma, \preceq)$ um semigrupo bem ordenado. Seja $\{f_\alpha |\ \alpha \in \Gamma\}$ uma base de $\mathcal{R}$ sobre $\mathbb{F}$. Para cada $\gamma \in \Gamma$, considere o subconjunto $L(\gamma)$ de $\mathcal{R}$ gerado por $\{f_\alpha \in \mathcal{R} |\ \alpha \preceq \gamma\}$. Então, vendo $\mathcal{R}$ como um $\mathbb{F}$-espaço vetorial, temos que $L(\gamma)$ é um subespaço vetorial de $\mathcal{R}$. Assim, defina a seguinte função $l : \Gamma \times \Gamma \to \Gamma$ por

$$l(\alpha, \beta) := \min_{\preceq}\{\gamma \in \Gamma : f_\alpha f_\beta \in L(\gamma)\}, \text{ para } \alpha, \beta \in \Gamma.$$

Uma base de $\mathcal{R}$ é chamada de uma *base ordenada* se $l(\alpha,\gamma) \prec l(\beta,\gamma)$ para todos $\alpha, \beta, \gamma \in \Gamma$ tais que $\alpha \prec \beta$.

Teorema 1.19 ([Ge-Pe],§3, prop. 3.2)**.** *Se $(\mathcal{R}, \rho, \Gamma)$ é uma estrutura ordem sobre $\mathbb{F}$ e $\{f_\alpha : \alpha \in \Gamma\}$ é uma sequência de elementos em $\mathcal{R}$ tal que $\rho(f_\alpha) = \alpha$ para todo $\alpha \in \Gamma$, então esta sequência é uma base ordenada em $\mathcal{R}$.*

Teorema 1.20 ([Ge-Pe],§3, prop. 3.3)**.** *Sejam $(\Gamma, \prec)$ um semigrupo bem ordenado e $\{f_\alpha : \alpha \in \Gamma\}$ uma base ordenada de $\mathcal{R}$. Defina $\rho(f) = -\infty$ se $f = 0$, e para $0 \neq f \in \mathcal{R}$, $\rho(f) = \gamma$, onde γ é o menor elemento de Γ, com respeito a ordem $\preceq$, tal que $f \in L(\gamma)$. Então $(\mathcal{R}, \rho, \Gamma)$ é uma estrutura ordem sobre $\mathbb{F}$.*

Dado um semigrupo bem ordenado, então é possível construir sobre este uma estrutura ordem.

Seja $(\Gamma, \preceq)$ um semigrupo bem ordenado. Por definição a *álgebra de semigrupo* $\mathbb{F}[\Gamma] := \mathbb{F}[\{X^\alpha : \alpha \in \Gamma\}]$ tem uma base $(X^\alpha : \alpha \in \Gamma)$ sobre $\mathbb{F}$, cuja multiplicação sobre os elementos da base é definida por $X^\alpha X^\beta = X^{\alpha+\beta}$ e é extendida linearmente.

Corolário 1.21. *Se $(\Gamma, \preceq)$ é um semigrupo bem ordenado então $\mathbb{F}[\Gamma]$ é um domínio ordem sobre $\mathbb{F}$ com semigrupo de valores Γ.*

1.4 Códigos para Domínios Ordens

Nesta seção apresentamos a construção de códigos algébricos sobre domínios ordens. Esta seção é fundamentada nas referências [[Ge1],cap. I.11] e [[Ge2], §3].

Seja $\mathbb{F}$ um corpo finito. Denote por $*$ a multiplicação em $\mathbb{F}^n$ dada por $(a_1, ..., a_n) * (b_1, ..., b_n) = (a_1b_1, ..., a_nb_n)$, com $a_i, b_i \in \mathbb{F}$, $i = 1, ..., n$. Então, o espaço vetorial $\mathbb{F}^n$ com esta multiplicação torna-se um anel comutativo com unidade $(1, ..., 1)$. Assim, identificando $\{(a, ..., a) : a \in \mathbb{F}\}$ com $\mathbb{F}$, temos que $\mathbb{F}^n$ é uma $\mathbb{F}$-álgebra.

Definição 1.22. Seja $\mathcal{R}$ uma $\mathbb{F}$-álgebra. A aplicação sobrejetiva $\varphi : \mathcal{R} \to \mathbb{F}^n$ é chamada um *morfismo* de $\mathbb{F}$-álgebras, se φ é $\mathbb{F}$-linear e $\varphi(fg) = \varphi(f) * \varphi(g)$, para todos $f, g \in \mathcal{R}$.

Exemplo 1.23. Dado um anel quociente $\mathcal{R} = \mathbb{F}[X_1, ..., X_m]/I$, seja $\mathcal{V}_\mathbb{F}(I) = \{P_1, ..., P_n\} \subset \mathbb{F}^m$ o conjunto dos zeros de I sobre $\mathbb{F}$. Então a seguinte aplicação de avaliação

$$\begin{array}{rccc} av: & \mathcal{R} & \longrightarrow & \mathbb{F}^n \\ & F + I & \longmapsto & (F(P_1), ..., F(P_n)) \end{array}$$

é um morfismo sobrejetor de $\mathbb{F}$-álgebras.

Agora, seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura ordem sobre $\mathbb{F}$. Seja $\{f_\alpha : \rho(f_\alpha) = \alpha \in \Gamma\}$ uma base ordenada de $\mathcal{R}$ e considere o subespaço vetorial $\mathcal{L}(\alpha) = \{f \in \mathcal{R} : \rho(f) \preceq \alpha\} = \langle f_{\alpha'} : \alpha' \preceq \alpha \rangle_\mathbb{F}$, onde $\langle \cdot \rangle_\mathbb{F}$ denota o subespaço gerado por $\cdot$ sobre $\mathbb{F}$.

Definição 1.24. Seja φ um morfismo sobrejetor em $\mathcal{R}$. Para um dado $\alpha \in \Gamma$, definimos o *código de avaliação* $E(\alpha)$ e seu código dual $C(\alpha)$, respectivamente, por

$$E(\alpha) = \varphi(\mathcal{L}(\alpha)) = \langle \varphi(f_{\alpha'}) : \alpha' \preceq \alpha \rangle_{\mathbb{F}}, \text{ e}$$
$$C(\alpha) = \{c \in \mathbb{F}^n : c \cdot \varphi(f_{\alpha'}) = 0, \text{para todo } \alpha' \preceq \alpha\}.$$

Observe que para $\alpha, \alpha' \in \Gamma$ tais que $\alpha' \preceq \alpha$ temos que $E(\alpha') \subseteq E(\alpha)$ e $C(\alpha') \supseteq C(\alpha)$.

Exemplo 1.25. Considere o domínio ordem $\mathcal{R} = \mathbb{F}_2[x, y]$ com a função peso $\rho : \mathcal{R} \to \mathbb{N}_0^2 \cup \{-\infty\}$ dada por $\rho(x) = (1, 0)$ e $\rho(y) = (0, 1)$ e $\mathbb{N}_0^2$ é ordenado pela ordem lexicográfica graduada. Então

$$B = \{f_{(0,0)} = 1, f_{(0,1)} = y, f_{(1,0)} = x, f_{(0,2)} = y^2, f_{(1,1)} = xy, f_{(2,0)} = x^2, f_{(0,3)} = y^3, ...\}$$

é uma base ordenada de $\mathcal{R}$. Considere a aplicação de avaliação

$$\begin{array}{rccl} av: & \mathcal{R} & \longrightarrow & \mathbb{F}_2^4 \\ & F & \longmapsto & (F((0,0)), F((0,1)), F((1,0)), F((1,1))) \end{array}$$

Os códigos de avaliação são:

$$\begin{aligned} E((0,0)) &= \langle (1,1,1,1) \rangle_{\mathbb{F}} \\ E((0,1)) &= \langle (1,1,1,1), (0,1,0,1) \rangle_{\mathbb{F}} \\ E((1,0)) &= \langle (1,1,1,1), (0,1,0,1), (0,0,1,1) \rangle_{\mathbb{F}} \\ &= E((0,2)) \\ E((1,1)) &= \langle (1,1,1,1), (0,1,0,1), (0,0,1,1), (0,0,0,1) \rangle_{\mathbb{F}} \\ &= \mathbb{F}_2^4 = E((2,0)) = E((0,3)) = ... \end{aligned}$$

E os códigos duais são:

$$\begin{aligned} C((0,0)) &= \{c \in \mathbb{F}_2^4 : c \cdot (1,1,1,1) = 0\} \\ C((0,1)) &= \{c \in \mathbb{F}_2^4 : c \cdot (1,1,1,1) = c \cdot (0,1,0,1) = 0\} \\ C((1,0)) &= \{c \in \mathbb{F}_2^4 : c \cdot (1,1,1,1) = c \cdot (0,1,0,1) = c \cdot (0,0,1,1) = 0\} \\ &= C((0,2)) \\ C((1,1)) &= \{c \in \mathbb{F}_2^4 : c \cdot (1,1,1,1) = c \cdot (0,1,0,1) = c \cdot (0,0,1,1) = c \cdot (0,0,0,1) = 0\} \\ &= \{(0,0,0,0)\} = C((2,0)) = C((0,3)) = ... \end{aligned}$$

Exemplo 1.26. Continuando o exemplo 1.12, sejam $P_1, ..., P_n$ pontos $\mathbb{F}$-racionais de $\mathcal{X}$, dois a dois distintos, diferentes de P. Considere a aplicação de avaliação

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

Tomando $D = P_1 + ... + P_n$ e o subespaço vetorial de $\mathcal{R}$,

$$\mathcal{L}(m) = \{f \in \mathcal{R} : \rho(f) \leq m\} = \mathcal{L}(mP) = \{f \in \mathbb{F}(\mathcal{X}) : div(f) + mP \geq 0\},$$

obtemos, aplicando av, os códigos geométricos de Goppa pontuais

$$E(m) = av(\mathcal{L}(m)) = av(\mathcal{L}(mP)) = C_{\mathcal{L}}(D, mP), \text{ e}$$
$$C(m) = (E(m))^{\perp} = C_{\Omega}(D, mP).$$

Vamos agora encontrar uma cota inferior $d(\alpha)$ para a distância mínima $d(C(\alpha))$ do código $C(\alpha)$.

Definição 1.27. Para $\gamma \in \Gamma$, defina

$$N_\gamma := \{(\alpha, \beta) \in \Gamma^2 : l(\alpha, \beta) = \gamma\} \text{ e}$$
$$\mu(\gamma) := \#N_\gamma.$$

Lema 1.28. *Seja $r \preceq \mu(\gamma)$. Dados r elementos $(\alpha_1, \beta_1), ..., (\alpha_r, \beta_r) \in N_\gamma$, então podemos enumera-los de forma que $\alpha_1 \prec ... \prec \alpha_r$ e $\beta_1 \succ ... \succ \beta_r$.*

Assim, seja $\gamma \in \Gamma$. Sejam $\alpha_1, ..., \alpha_r \in \Gamma$ tais que $(\alpha_1, \alpha_r), ..., (\alpha_r, \alpha_1) \in N_\gamma$ e $\alpha_1 \prec ... \prec \alpha_r$. Considere a matriz M cujas primeiras linhas são $\varphi(f_{\alpha_1}), ..., \varphi(f_{\alpha_r})$ e completemos M de forma que o posto de M seja igual a n.

Para $y = (y_1, ..., y_n) \in \mathbb{F}^n$, considere a matriz diagonal $D(y) := (a_{ij})_{n \times n}$, onde $a_{ij} = 0$ se $i \neq j$ e $a_{ii} = y_i$, para $i, j = 1, ..., n$. Seja $S(y) := MD(y)M^T$, então , para $i, j \in \{1, ..., r\}$, temos que $(S(y))_{i,j} = y \cdot (\varphi(f_{\alpha_i}) * \varphi(f_{\alpha_j}))$, onde $\cdot$ é o produto interno usual em $\mathbb{F}^n$. Assim, como $posto(M) = n$, temos que

$$posto(S(y)) = wt(y),$$

onde $wt(y)$ é o peso de y.

Lema 1.29. *1) Se $y \in C(\gamma')$ para todo $\gamma' \prec \gamma$ e $l(\alpha_i, \alpha_j) \prec \gamma$ então $(S(y))_{i,j} = 0$.*

2) Se $y \in C(\gamma')$ para todo $\gamma' \prec \gamma$, mas $y \notin C(\gamma)$ e $l(\alpha_i, \alpha_j) = \gamma$ então $(S(y))_{i,j} \neq 0$.

Proposição 1.30. *Se $y \in C(\gamma')\backslash C(\gamma)$ para todo $\gamma' \prec \gamma$ então $wt(y) \geq \mu(\gamma)$.*

Defina a *cota ordem*

$$d(\gamma) := min\{\mu(\lambda) : \gamma \prec \lambda\}.$$

Teorema 1.31. *A distância mínima $d(C(\gamma))$ de $C(\gamma)$ é limitada inferiormente por $d(\gamma)$, isto é,*

$$d(C(\gamma)) \geq d(\gamma).$$

Exemplo 1.32. Considere a função peso $\rho : \mathbb{F}_3[x,y] \to \mathbb{N}_0^2 \cup \{-\infty\}$ definida por $\rho(x) = (1,0)$ e $\rho(y) = (0,1)$, onde a ordem $\preceq$ em $\mathbb{N}_0^2$ é a ordem lexicográfica graduada. Então $\{f_{(\alpha,\beta)} = x^\alpha y^\beta : \alpha, \beta \in \mathbb{N}_0\}$ é uma base ordenada de $\mathbb{F}_3[x,y]$. Tome o morfismo $\varphi : \mathbb{F}_3[x,y] \to \mathbb{F}_3^9$ dado por $\varphi(f) = (f(0,0), f(0,1), ..., f(2,1), f(2,2))$. Então, temos os códigos $E((\alpha,\beta)) = \varphi(\{f \in \mathbb{F}_3[x,y] : \rho(f) \preceq (\alpha,\beta)\})$ e $C((\alpha,\beta)) = E((\alpha,\beta))^\perp$.

Assim, temos as seguintes cotas para a distância mínima de $C((\alpha,\beta))$:

(α,β)	$(0,0)$	$(0,1)$	$(1,0)$	$(0,2)$	$(1,1)$	$(2,0)$	$(1,2)$	$(2,1)$	$(2,2)$
μ	1	2	2	3	4	3	6	6	7
$d(\alpha,\beta)$	1	2	2	3	3	3	4	4	5

Exemplo 1.33. Para $\mathcal{X} = \mathcal{V}(X^5 - Y^4 - Y)$ (curva hermitiana) sobre o corpo $\mathbb{F}_{16}$ e $\mathcal{R} = \mathbb{F}_{16}[X,Y]/(X^5 - Y^4 - Y)$, tomando x e y as classes correspondentes a X e Y, respectivamente, temos que $\{x^\alpha y^\beta : \alpha < 5\}$ é uma base ordenada de $\mathcal{R}$ e $\rho(x^\alpha y^\beta) = 4\alpha + 5\beta$ é uma função peso sobre $\mathcal{R}$. Então, continuando o exemplo 1.26, para tal curva, temos as seguintes cotas:

f_γ :	1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	...
$\rho(f_\gamma) = \gamma$:	0	4	5	8	9	10	12	13	14	15	16	...
$d(\gamma)$:	2	2	3	3	3	4	4	4	4	5	8	...
$d_{Goppa}(\gamma)$:	-10	-6	-5	-2	-1	0	2	3	4	5	6	...

CAPÍTULO 2

ESTRUTURAS PESOS FINITAMENTE GERADAS

Matsumoto prova, em [Ma] Teorema 1, que quando Γ é um subsemigrupo de $\mathbb{N}_0$, ou seja, $r.posto(\Gamma) = 1$, se $\mathcal{R}$ admite uma função peso ρ com semigrupo de valores Γ então existe uma curva algébrica projetiva irredutível $\mathcal{X}$ e um ponto racional $P \in \mathcal{X}$ tal que o fecho integral de $\mathcal{R}$ em seu corpo de frações é o anel das funções regulares da curva afim $\mathcal{X}\backslash\{P\}$ e $\rho = -\nu_P$, onde ν_P é a valorização associada a P.

Neste capítulo, veremos um resultado similar ao de Matsumoto para uma classe especial de semigrupos de posto racional maior ou igual a 1.

2.1 Estrutura das Álgebras

Definição 2.1. Uma estrutura peso $(\mathcal{R}, \rho, \Gamma)$ sobre um corpo $\mathbb{F}$ é chamado *finitamente gerado* ou *Noetheriano* se $(\Gamma, +)$ é um semigrupo finitamente gerado.

Proposição 2.2 ([Ge-Pe],§5, prop.5.2)**.** *Seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura peso finitamente gerada sobre $\mathbb{F}$. Então $\mathcal{R}$ é uma álgebra finitamente gerada sobre $\mathbb{F}$.*

Disto, segue que $\mathcal{R} \cong \mathbb{F}[X_1, ..., X_n]/I$, onde I é um ideal primo de $\mathbb{F}[X_1, ..., X_n]$.

Assim, seja K o corpo de frações do domínio ordem $\mathcal{R}$. Então, a aplicação $\nu : K \to G(\Gamma) \cup \{+\infty\}$ definida por $\nu(0) = +\infty$ e

$$\nu(f/g) = \rho(g) - \rho(f),$$

para $f, g \in \mathcal{R}\backslash\{0\}$ é uma valorização em K, com anel de valorização $\mathcal{R}_\nu = \{h \in K : \nu(h) \succeq 0\}$, ideal de maximal $\mathcal{M}_\nu = \{h \in K : v(h) \succ 0\}$ e com corpo de resíduos $\mathbb{F}$ (ver [[Ge-Pe],§6, obs.6.2]). Observe que, para $f \in \mathcal{R}\backslash\{0\}$, $\rho(f) = -\nu(f)$.

Teorema 2.3 ([Ge-Pe],§11, teo.11.9)**.** *Seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura ordem finitamente gerada sobre um corpo $\mathbb{F}$. Então a dimensão de Krull de $\mathcal{R}$ é igual ao posto racional de Γ.*

Corolário 2.4. *Se $(\mathcal{R}, \rho, \Gamma)$ é uma estrutura ordem finitamente gerada sobre $\mathbb{F}$, então o corpo de frações K de $\mathcal{R}$ é um corpo de funções em r.posto(Γ) variáveis sobre $\mathbb{F}$.*

Dem. Das proposições 1.18 e proposição 2.2, segue que $\mathcal{R}$ é um domínio finitamente gerado. Assim, do teorema A de [[Ei],cap.13, §1, pag. 290], e da proposição anterior, temos que $trgrau(K|\mathbb{F}) = dim(R) = r.posto(\Gamma)$, e portanto segue o resultado. ∎

Os próximos resultados generalizam a ideia de Matsumoto para álgebras munidas de uma função peso de posto racional arbitrário.

Teorema 2.5. *Seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura peso finitamente gerada sobre um corpo $\mathbb{F}$ tal que o grupo $G(\Gamma)$ gerado por Γ tenha um subgrupo isolado de posto racional r.posto$(\Gamma) - 1$. Então o fecho integral de R em K é um subanel de K consistindo de funções com pólos em pelo menos um divisor primo de K.*

Dem. Seja K o corpo de frações de $\mathcal{R}$. Suponha que $r.posto(\Gamma) = n$. Então, como $(\mathcal{R}, \rho, \gamma)$ é uma estrutura peso finitamente gerada, temos que $\mathcal{R}$ é um domínio finitamente gerado e que $dim\mathcal{R} = n = r.posto(\Gamma)$. Logo, temos que K é um corpo de funções algébricas em n variáveis sobre $\mathbb{F}$. Da função peso ρ, seja ν a valorização em K associada a ρ, definida como antes. Seja R_ν o anel de valorização de ν e M_ν seu ideal

maximal. Então, do axioma (O.5) de função peso, temos que $\kappa_\nu = R_\nu/M_\nu \cong \mathbb{F}$, ou seja, $dim(\nu) = trgrau(\kappa_\nu|\mathbb{F}) = 0$ (ver definição A.13). Agora, seja Δ o subgrupo isolado de $G(\Gamma)$ tal que $r.posto(\Delta) = n-1$. Então, das propriedades de valorizações, temos que $\nu = \mu \circ \overline{\nu}$, onde $\mu : K \to (G(\Gamma)/\Delta) \cup \{+\infty\}$ é uma valorização discreta de posto 1 em K, pois $posto(\mu) \leq r.posto(\mu) = 1$, e $\overline{\nu} : \kappa_\mu \to \Delta \cup \{+\infty\}$ é uma valorização do corpo de resíduos κ_μ de μ. Assim, falta mostrar que μ é um divisor primo em K. De fato, da desigualdade de Abhyankar (proposição A.14), $r.posto(\mu)+dim(\mu) \leq trgrau(K|\mathbb{F}) = n$, ou seja, $dim(\mu) \leq n-1$. Como $r.posto(\overline{\nu}) = r.posto(\Delta) = n-1$ e o corpo de resíduos $\kappa_{\overline{\nu}}$ de $\overline{\nu}$ é igual ao corpo de resíduos de ν, ou seja, $\kappa_{\overline{\nu}} = \mathbb{F}$, (ver prop. A.22), segue que

$$n-1 = r.posto(\overline{\nu}) + dim(\overline{\nu}) \leq trgrau(\kappa_\mu|\mathbb{F}) = dim(\mu) \leq n-1.$$

Logo, $dim(\mu) = n-1$, e portanto, μ é um divisor primo de $K|\mathbb{F}$.

Agora, seja $\overline{\mathcal{R}}$ o fecho integral de $\mathcal{R}$ em K. Seja $S(\mathcal{R})$ o conjunto dos divisores primos de $K|\mathbb{F}$ cujo anel de valorização associado contem $\mathcal{R}$, ou seja,

$$S(\mathcal{R}) := \{\omega \text{ divisor primo em } K|\mathbb{F} : \mathcal{R} \subset R_\omega\}.$$

Sabemos que [ver [Za-Sa II], cap. VI, §14,pag.97]

$$\overline{\mathcal{R}} = \bigcap_{\omega \in S(\mathcal{R})} R_\omega.$$

Mostremos que $\mu \notin S(R)$. Suponha que $\mu \in S(\mathcal{R})$, ou seja, $\mathcal{R} \subset R_\mu$. Então, para todo $f \in \mathcal{R}\backslash\mathbb{F}$, temos que $\rho(f) \succ 0$, ou seja, $\nu(f) \prec 0$. Logo $\mu(f) \leq 0$. Como $\mathcal{R} \subset R_\mu$, segue que $\mu(f) = 0$ para todo $f \in \mathcal{R}\backslash\{0\}$. Mas μ é um divisor primo de $K|\mathbb{F}$, então existe $a/b \in K$, com $a, b \in \mathcal{R}\backslash\{0\}$, tal que $\mu(a/b) = 1$, ou seja, $1 = \mu(a/b) = \mu(a) - \mu(b) = 0$, contradição. Logo, $\mu \notin S(R)$ e portanto, segue o resultado. ∎

Corolário 2.6. *Se, para qualquer $f \in \mathcal{R}\backslash\mathbb{F}$, $\mu(f) < 0$, então o fecho integral de R em K é um subanel de K consistindo de funções com pólos apenas no divisor primo μ de K.*

Dem. Vimos acima que

$$\overline{\mathcal{R}} = \bigcap_{\omega \in\, S(\mathcal{R})} R_\omega,$$

onde $\mu \notin S(\mathcal{R})$. Assim, seja S o conjunto de todos os divisores primos de $K|\mathbb{F}$. Mostremos que $S(\mathcal{R}) = S\backslash\{\mu\}$. Suponha que $S(\mathcal{R}) \cup \{\mu\} \neq S$. Seja

$$R' = \bigcap_{\omega \in S(\mathcal{R})\cup\{\mu\}} R_\omega \subset \overline{\mathcal{R}}.$$

Do teorema de aproximação [ver [Bo], cap VII, §1.5, prop.9, pag. 484], existe $0 \neq x \in K$ tal que $\mu(x) > 0$ e $\omega(x) \geq 0$, para todo $\omega \in S(\mathcal{R})$. Disto, segue que $x \in R'$. Seja $I = \{f \in \mathcal{R} : f\overline{\mathcal{R}} \subset \mathcal{R}\} \neq (0)$ o condutor de $\mathcal{R}$ em $\overline{\mathcal{R}}$. Como $x \in \overline{\mathcal{R}}$, para qualquer $0 \neq y \in I$, temos que $yx \in \mathcal{R}$. Então, para algum $y \in I$, $\mu(xy) < 0$, ou seja, $\mu(x) < \mu(y^{-1})$. Como μ é uma valorização discreta de posto 1, segue que μ é arquimediano (ver observação A.8), e portanto existe um inteiro positivo n tal que $n\mu(x) > \mu(y^{-1})$, ou seja, $\mu(yx^n) > 0$. Mas $yx^n \in \mathcal{R}$, pois $y \in I$ e $x^n \in \overline{\mathcal{R}}$. Logo $\mu(yx^n) \leq 0$, contradição.

Portanto,

$$\overline{\mathcal{R}} = \bigcap_{\omega \in\, S\backslash\{\mu\}} R_\omega.$$

■

Proposição 2.7. *Seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura peso finitamente gerada sobre um corpo $\mathbb{F}$ tal que o grupo $G(\Gamma)$ gerado por Γ tenha um subgrupo isolado de posto racional r.posto$(\Gamma) - 1$. Então $\mathcal{R}$ é o anel de funções regulares de uma variedade afim, cujo normalização de seu fecho projetivo $\mathcal{X}$ possui um divisor irredutível Z no infinito. Se, além disso, para qualquer $f \in \mathcal{R}\backslash\mathbb{F}$, $\mu(f) < 0$, então a normalização do fecho projetivo $\mathcal{X}$ possui apenas um divisor irredutível Z no infinito.*

Dem.

Seja $\mathcal{X}$ a variedade projetiva definida pelo domínio afim $\mathcal{R}$ e $\overline{\mathcal{X}}$ sua normalização. Então, pela proposição A.21, teorema A.22 e do teorema 2.5, segue que a valorização μ, está centrada em um divisor irredutível Z de $\overline{\mathcal{X}}$. Agora, se, para qualquer $f \in \mathcal{R}\backslash\mathbb{F}$, $\mu(f) < 0$, temos, do corolário anterior, que Z é o único divisor irredutível de $\overline{\mathcal{X}}$ no infinito.

■

Observação 2.8. Da proposição A.21, segue que o divisor primo μ da decomposição $\nu = \mu \circ \overline{\nu}$ está centrado em uma subvariedade D de $\mathcal{X}$ e $dim(D) \leq dim(\mu)$. E, da proposição A.23, a valorização ν está centrada em um ponto racional $Q \in D \subset \mathcal{X}$.

Mais ainda, se $\mu(f) = 0$ para algum $f \in \mathcal{R}\backslash\mathbb{F}$, então o fecho projetivo $\mathcal{X}$ da variedade afim definida por $\mathcal{R}$ tem mais de uma subvariedade W de $codim(W) \geq 1$ no infinito.

De fato, sabemos que $\overline{\mathcal{R}} = \bigcap_{\omega \in S(\mathcal{R})} R_\omega$ e $\mu \notin S(\mathcal{R})$. Se $\mu(f) = 0$, para algum $f \in \mathcal{R}\backslash\mathbb{F}$, então $f \in \overline{\mathcal{R}} \cap R_\mu$. Mas, como f possui um número finito de zeros e pólos [ver [Za-Sa II], cap. VI, §14,pag.97], então existe pelo menos um divisor primo η em $K|\mathbb{F}$ tal que $\eta(f) < 0$. Disto, segue que $\eta \notin S(\mathcal{R})$, e portanto, da observação A.20, existe uma subvariedade W de $\mathcal{X}$ tal que η está centrado em W, e portanto, $codim(W) \geq 1$.

Por exemplo, considere $\mathcal{X}$ a superfície quádrica não-singular $XY - ZW = 0$ em $\mathbb{P}^3$. Seja $H_\infty = V(W)$ o hiperplano no infinito. Então $\mathcal{X} \cap H_\infty$ é o divisor consistindo de duas linhas $C_1 : X = W = 0$ e $C_2 : Y = W = 0$, ou seja,

$$C_1 := \{(0 : Y : Z : 0)/(Y : Z) \in \mathbb{P}^1\} \text{ e } C_2 := \{(X : 0 : Z : 0)/(X : Z) \in \mathbb{P}^1\}.$$

Como $\mathcal{X}$ é não-singular, segue que C_1 e C_2 são divisores irredutíveis em $\mathcal{X}$ (ver [Sh1], cap. 2, §5). Deshomogenizando $\mathcal{X}$ com respeito a W, temos que o anel de coordenadas afim de $\mathcal{X}\backslash V(W)$ é $\mathcal{R} = \mathbb{F}[x, y, z]/(xy - z) \cong \mathbb{F}[x, y]$. Assim, para o ponto $P = (0 : 0 : 1 : 0) \in C_1 \cap C_2$, é possível construir uma função peso ρ de $\mathcal{R}$ em $\Gamma = \mathbb{N}_0^2$, ordenado pela ordem lexicográfica, com $\rho(x) = (0, 1)$ e $\rho(y) = (1, 0)$ (a construção desta função peso segue do exemplo 3.12 (capítulo 3), onde $1/y$ é o parâmetro local de C_1 em $\mathcal{X}$, e $1/x$ é o parâmetro local de P em C_1).

Observação 2.9. Quando $\Gamma \subseteq \mathbb{N}_0$, temos que $\nu = \mu$, pois $\overline{\nu}$ é uma valorização trivial. Como, neste caso, $\nu(f) < 0$ para todo $f \in \mathcal{R}\backslash\mathbb{F}$, temos, pela proposição anterior, que o divisor irredutível Z é um ponto racional, e tal resultado coincide com [Ma], Teorema 1. Disto, e do exemplo 1.26, segue que os códigos de avaliação são códigos geométricos de Goppa pontuais.

CAPÍTULO 3

FUNÇÕES ORDENS FRACAS

Assim como funções ordens, o conceito de função ordem fraca, introduzido por Silva em [Si], é generalizado, permitindo sua construção sobre álgebras de dimensão arbitrária. Neste capítulo, apresentamos esta generalização, suas propriedades, e veremos dois métodos diferentes de construir tais funções. Um dos métodos consiste em usar valorizações sobre corpos de funções de variedades algébricas, e o outro utiliza teorias sobre bases de Gröbner para anéis tóricos.

3.1 Funções Ordens Fracas

Seja $(\Gamma, +, 0, \prec)$ um semigrupo aditivo ordenado com relação a ordem total $\prec$, com elemento mínimo 0. Adicionamos a Γ um elemento $-\infty$ tal que $-\infty \prec \alpha$ para todo $\alpha \in \Gamma$, e estendemos a lei em $\Gamma \cup \{-\infty\}$ por $(-\infty) + \alpha = (-\infty) + (-\infty) = -\infty$.

Seja $\mathcal{R}$ uma $\mathbb{F}$-álgebra e $(\Gamma, \prec)$ um semigrupo ordenado. Seja $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ uma função e considere os seguintes conjuntos associados a ρ:

$$\mathcal{U}_\rho := \{f \in \mathcal{R} : \rho(f) \preceq \rho(1)\},$$
$$\mathcal{M}_\rho := \{f \in \mathcal{R} : \rho(1) \prec \rho(f)\}.$$

Definição 3.1. Dizemos que ρ é uma *função ordem fraca* (ou *quase-ordem*, ou apenas *q-ordem*) em $\mathcal{R}$ se são satisfeitas as seguintes condições: para $f, g, h \in \mathcal{R}$,

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

(Q.2) $\rho(\lambda f) = \rho(f)$, para todo $\lambda \in \mathbb{F}^*$;

(Q.3) $\rho(f + g) \preceq max_{\preceq}\{\rho(f), \rho(g)\}$;

(Q.4) Se $\rho(f) \prec \rho(g)$ e $h \neq 0$, então $\rho(fh) \preceq \rho(gh)$. Se $h \in \mathcal{M}_\rho$ então $\rho(fh) \prec \rho(gh)$;

(Q.5) Se $\rho(f) = \rho(g) \neq -\infty$ com $f, g \in \mathcal{M}_\rho$, então existe $\lambda \in \mathbb{F}^*$ tal que $\rho(f - \lambda g) \prec \rho(g)$.

Se, além dos axiomas anteriores, também é satisfeita a condição

(Q.6) $\rho(fg) \preceq \rho(f) + \rho(g)$, com igualdade se $f, g \in \mathcal{M}_\rho$,

então dizemos que ρ é uma *função peso fraco* (ou *quase-peso*, ou apenas *q-peso*) em $\mathcal{R}$.

Para simplificar, chamaremos de *estrutura q-ordem* (resp. *estrutura q-peso*), denotada por $(\mathcal{R}, \rho, \Gamma)$, uma $\mathbb{F}$-álgebra $\mathcal{R}$ com função q-ordem (resp. q-peso) $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$.

Observação 3.2. 1. Se $(\mathcal{R}, \rho, \Gamma)$ for uma estrutura q-ordem em $\mathcal{R}$, onde $\mathcal{U}_\rho = \{f \in \mathcal{R} \mid \rho(f) \preceq \rho(1)\} = \mathbb{F}$, Γ é um semigrupo bem ordenado e ρ é sobrejetiva, então ρ é uma função ordem em $\mathcal{R}$.

2. Toda função ordem é uma função q-ordem com $\mathcal{U}_\rho = \mathbb{F}$.

Exemplo 3.3. Seja $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ definida por $\rho(0) = -\infty$ e para todo $f \in \mathcal{R}^*$, $\rho(f) = \alpha$, para algum $\alpha \in \Gamma$. Logo $\mathcal{M}_\rho = \emptyset$ e $\mathcal{U}_\rho = \mathcal{R}\backslash\{0\}$ e portanto ρ é uma função q-ordem, mas não é uma função ordem, pois $\mathcal{U}_\rho \neq \mathbb{F}$.

Exemplo 3.4. Considere o anel de polinômios $\mathcal{R} = \mathbb{F}[X_1, ..., X_n]$. Seja $(\mathbb{N}_0^n, \prec)$ um semigrupo ordenado, onde $\prec$ é a ordem lexicográfica em $\mathbb{N}_0^n$. Denote por $\alpha = (\alpha_1, ..., \alpha_n)$, com $\alpha_i \in \mathbb{N}_0$ e $\mathbf{X}^\alpha = X_1^{\alpha_1} \cdot ... \cdot X_n^{\alpha_n}$. Para $f \in \mathcal{R}$, temos que $f = \sum_{finita} \lambda_\alpha \mathbf{X}^\alpha$ com $\lambda_\alpha \in \mathbb{F}$. Então, dado $\delta \in \mathbb{N}_0^n\backslash\{(0, ..., 0)\}$, defina $\rho_\delta : \mathcal{R} \to \mathbb{N}_0^n \cup \{-\infty\}$ como

$$\rho_\delta(f) := \begin{cases} -\infty, & \text{se } f = 0, \\ (0,...,0), & \text{se } f \neq 0 \text{ e } \alpha \preceq \delta, \\ max_\prec\{\alpha : \lambda_\alpha \neq 0\}, & \text{se } f \neq 0 \text{ e } \alpha \succ \delta. \end{cases}$$

Logo $\mathcal{U}_{\rho_\delta} = \{\langle 1, ..., \mathbf{X}^\alpha\rangle_\mathbb{F} : \alpha \preceq \delta\}$ e $\mathcal{M}_{\rho_\delta} = \{\langle \mathbf{X}^\alpha\rangle_\mathbb{F} : \alpha \succ \delta\}$. Então ρ_δ é uma q-ordem sobre $\mathcal{R}$ que não é função ordem, pois $\mathcal{U}_{\rho_\delta} \neq \mathbb{F}$.

De fato, observe que (Q.1), (Q.2) e (Q.3) são claramente satisfeitos.

Axioma (Q.4): Sejam $f = \sum_{\alpha\preceq\gamma} \lambda_\alpha \mathbf{X}^\alpha$, $\lambda_\gamma \neq 0$ e $g = \sum_{\alpha\preceq\beta} \mu_\alpha \mathbf{X}^\alpha$, $\mu_\beta \neq 0$ tal que $\rho_\delta(f) \prec \rho_\delta(g)$ (note que $\rho_\delta(f) = (0,...,0)$ ou $\rho_\delta(f) = \gamma$, e $\rho_\delta(g) = \beta$). Seja $h = \sum_{\alpha\preceq\delta} a_\alpha \mathbf{X}^\alpha \in R$, com $a_\delta \neq 0$. Então temos que $\rho_\delta(fh) = (0,...,0)$ ou $\rho_\delta(fh) = \gamma + \delta$ e como $\rho_\delta(gh) = \beta + \delta$, segue, por hipótese, que $\rho_\delta(fh) \prec \rho_\delta(gh)$.

Axioma (Q.5): se $\gamma = \rho_\delta(f) = \rho_\delta(g) = \beta$, para $f, g \in \mathcal{M}_{\rho_\delta}$ como o axioma (Q.4). Logo, tomando $\lambda = \frac{\lambda_\gamma}{\mu_\beta} \in \mathbb{F}^*$, temos que $\rho_\delta(f - \lambda g) \prec_L \rho_\delta(g)$.

Portanto, ρ_δ é uma q-ordem sobre $\mathcal{R}$. Mas ρ_δ não é uma função q-peso, pois para $f = \mathbf{X}^\delta$ e $g = X_1$, temos que $fg = X_1^{1+\delta_1} \cdot X_2^{\delta_2} \cdot ... \cdot X_n^{\delta_n}$ e $\rho_\delta(fg) = (1+\delta_1, \delta_2, ..., \delta_n) \succ (0,...,0) = \rho_\delta(f) + \rho_\delta(g)$.

Exemplo 3.5. Seja $\mathcal{R} = \mathbb{F}[X_1, ..., X_n]$. Seja $(\mathbb{N}_0^n, \prec)$ um semigrupo ordenado, onde $\prec$ é a ordem lexicográfica em $\mathbb{N}_0^n$. Denote por $\alpha = (\alpha_1, ..., \alpha_n)$, com $\alpha_i \in \mathbb{N}_0$ e $\mathbf{X}^\alpha = X_1^{\alpha_1} \cdot ... \cdot X_n^{\alpha_n}$. Seja $\mathcal{M} = \{\mathbf{X}^\alpha : \alpha \in \mathbb{N}_0^n\}$ o conjunto dos monômios de $\mathcal{R}$. Defina, sobre $\mathcal{M}$, a função $\omega : \mathcal{M} \to \mathbb{N}_0^n$ dada por:

$$\omega(\mathbf{X}^\alpha) = \begin{cases} (0,...,0) & \text{, se } \alpha_1 = 0 \\ (\alpha_1, ..., \alpha_n) & \text{, se } \alpha_1 \neq 0. \end{cases}$$

Para $f \in \mathcal{R}$, temos que $f = \sum_{finita} \lambda_\alpha \mathbf{X}^\alpha$ com $\lambda_\alpha \in \mathbb{F}$. Então, definindo $\rho : \mathcal{R} \to \mathbb{N}_0^n \cup \{-\infty\}$ como

$$\rho(f) = \begin{cases} -\infty & \text{, se } f = 0; \\ \max\{\omega(\mathbf{X}^\alpha) : \lambda_\alpha \neq 0\} & \text{, se } f \neq 0; \end{cases}$$

temos, de forma análoga ao exemplo anterior, que ρ é uma função q-ordem em $\mathcal{R}$. Note que $\mathcal{U}_\rho = \mathbb{F}[X_2, ..., X_n]$. Logo ρ não é uma função ordem. Temos também que ρ não é

uma função q-peso em R, pois para $f = X_1$ e $g = X_2$ temos que $\rho(fg) = \rho(X_1X_2) = (1, 1, 0, ..., 0) \succ (1, 0, 0, ..., 0) = \rho(f) + \rho(g)$.

Vimos no capítulo 1 que se $\mathcal{R}$ possui uma função ordem, então $\mathcal{R}$ é um domínio de integridade. Porém, o mesmo não se pode dizer das álgebras munidas de funções q-ordens.

Exemplo 3.6. Considere a $\mathbb{F}$-álgebra $\mathcal{R} = \mathbb{F}[X, Y, Z]/(X^2) = \mathbb{F}[x, y, z]$, onde x, y, z são as classes de X, Y, Z módulo (X^2). Então $\mathcal{R}$ não é um domínio. Assim, seja $f \in \mathcal{R}\backslash\{0\}$, então f pode ser escrito da seguinte maneira: $f(x, y, z) = g(x, y, z) + h(0, y, z)$, com $g, h \in \mathcal{R}$,$x|g$, e $h(0, y, z) = \sum_{finita} \lambda_{\alpha,\beta} y^\alpha z^\beta$, $\lambda_{\alpha,\beta} \in \mathbb{F}$. Seja $(\mathbb{N}_0^2, \preceq)$ um semigrupo ordenado, onde $\preceq$ é a ordem lexicográfica graduada. Então a função $\rho : \mathcal{R} \to \mathbb{N}_0^2 \cup \{-\infty\}$, definida por

$$\rho(f) \begin{cases} -\infty, & \text{se } f = 0; \\ (0, 0), & \text{se } f \neq 0 \text{ e } h \in \mathbb{F}; \\ max_{\preceq}\{(\alpha, \beta) : \lambda_{\alpha,\beta} \neq 0\}, & \text{se } h \notin \mathbb{F}. \end{cases}$$

é uma função q-ordem em $\mathcal{R}$, com $\mathcal{U}_\rho = x\mathcal{R} \cup \mathbb{F}$.

Vejamos agora algumas propriedades para funções q-ordens.

Lema 3.7. *Dado $(\mathcal{R}, \rho, \Gamma)$ uma estrutura q-ordem, temos:*

1) $\mathcal{M}_\rho$ não contém divisores de zero.

2) Se $\rho(f) \neq \rho(g)$ então $\rho(f + g) = max_{\preceq}\{\rho(f), \rho(g)\}$.

3) Se $f, g, h \in \mathcal{M}_\rho$ e $\rho(f) = \rho(g)$ então $\rho(fh) = \rho(gh)$.

4) O elemento $\lambda \in \mathbb{F}^*$ no axioma (Q.5) é único.

5) Se $\mathcal{R}'$ é uma subálgebra de $\mathcal{R}$ e então $\sigma := \rho_{|_{\mathcal{R}'}}$ também é uma função q-ordem sobre $\mathcal{R}'$. Caso ρ seja uma função q-peso então σ também é uma função q-peso.

Dem. 1) Sejam $f, g \in \mathcal{M}_\rho$ tais que $fg = 0$. Como $\rho(1) \prec \rho(f)$ e $\rho(1) \prec \rho(g)$, temos, pelo axioma (Q.4), que $\rho(1) \prec \rho(f) \prec \rho(fg) = -\infty$, contradição.

2) Se $\rho(f) \neq \rho(g)$, suponha que $\rho(f) \prec \rho(g)$. Então suponha que $\rho(f+g) \prec max_{\preceq}\{\rho(f), \rho(g)\} = \rho(g)$. Como $g = g - f + f$ e $\rho(f) = \rho(-f)$ segue que $\rho(g) = \rho(-f+f+g) \preceq max_{\preceq}\{\rho(-f), \rho(f+g)\} \prec \rho(g)$, contradição.

3) Se $f, g, h \in \mathcal{M}_\rho$ e $\rho(f) = \rho(g)$, pelo axioma (Q.5), temos que existe $\lambda \in \mathbb{F}^*$ tal que $\rho(f - \lambda g) \prec \rho(g)$. Do axioma (Q.4), $\rho((f-\lambda g)h) \prec \rho(gh)$. Como $fh = fh - \lambda gh + \lambda gh$ temos, da propriedade 2, que $\rho(fh) = \rho(fh - \lambda gh + \lambda gh) = max_{\preceq}\{\rho((f - \lambda g)h), \rho(\lambda gh)\} = \rho(gh)$.

4) Suponha que existem $\lambda, \mu \in \mathbb{F}$ tais que $\rho(f - \lambda g) \prec \rho(g)$ e $\rho(f - \mu g) \prec \rho(g)$. Então, de (Q.3), $\rho(f - \lambda g - (f - \mu g)) \prec \rho(g)$, ou seja, $\rho((\mu - \lambda)g) \prec \rho(g)$. Logo, do axioma (Q.2) e (Q.1), temos que ter $\mu - \lambda = 0$.

5) De fato, basta observar que $U_\sigma = \{f \in \mathcal{R}' \mid \sigma(f) \preceq \sigma(1)\}$ e $\mathcal{M}_\sigma = \{f \in \mathcal{R}' \mid \sigma(1) \prec \sigma(f)\}$ e aplicar os axiomas de função q-ordem (respectivamente, q-peso) para σ em $\mathcal{R}'$.

■

Veremos a seguir um exemplo de um domínio que admite funções q-ordens mas não admite função ordem.

Exemplo 3.8 ([NOC], ex.3.2,[Si], ex.2.10)**.** Seja $\mathcal{R} = \mathbb{F}[X,Y]/(XY-1) = \mathbb{F}[x,y]$ com x e y as classes de X e Y módulo $(XY-1)$, respectivamente. Assim, para todo $f \in \mathcal{R}$, temos que $f = f_1(x) + f_2(y)$, onde $f_1, f_2 \in \mathbb{F}[T]$ com $f_2(0) = 0$. Vimos no capítulo 1 que não existe uma função ordem em $\mathcal{R}$. Mas, porém, $\mathcal{R}$ admite uma função q-ordem $\rho : \mathcal{R} \to \mathbb{N}_0 \cup \{-\infty\}$ dada por:

$$\rho(f) := \begin{cases} -\infty & , \text{ se } f = 0; \\ 0 & , \text{ se } f_1 \neq 0 \text{ e } f_2 = 0; \\ grau(f_2) & , \text{ se } f_2 \neq 0. \end{cases}$$

Aqui, $\mathcal{U}_\rho = \{f_1(x) : f_1 \in \mathbb{F}[T]\}$ e $\mathcal{M}_\rho = \{f_1(x) + f_2(y) : f_2 \in \mathbb{F}[T], f_2 \neq 0 \text{ e } f_2(0) = 0\}$.

3.2 Construindo Funções Q-Ordens a partir de Valorizações

Uma introdução à teoria de valorizações será dada no apêndice A.

Exemplo 3.9 ([NOC], ex.3.5, [Si], ex. 2.4)**.** Seja $\mathcal{X}$ uma curva algébrica projetiva não-singular absolutamente irredutível sobre o corpo $\mathbb{F}$. Sejam $Q_1, ..., Q_n$ pontos $\mathbb{F}$-racionais distintos de $\mathcal{X}$. Seja $\mathcal{X}' := \mathcal{X}\backslash\{Q_1, ..., Q_n\}$ e seja $\mathcal{R}$ a $\mathbb{F}$-subálgebra de $\mathbb{F}(\mathcal{X})$ consistindo de funções regulares em $\mathcal{X}'$, ou seja,

$$\mathcal{R} = \mathcal{R}(Q_1, ..., Q_n) = \bigcap_{P \in \mathcal{X}'} \mathcal{O}_P(\mathcal{X}),$$

onde $\mathcal{O}_P$ é o anel local associado a $P \in \mathcal{X}$. Para cada Q_i, defina a função $\rho_i : \mathcal{R} \to \mathbb{N}_0 \cup \{-\infty\}$ por

$$\rho_i(f) = \begin{cases} -\infty & , \ se \ f = 0; \\ 0 & , \ se \ v_i(f) \geq 0; \\ -v_i(f) & , \ se \ v_i(f) < 0. \end{cases}$$

Note que $\mathcal{U}_{\rho_i} = \mathcal{R} \cap \mathcal{O}_{Q_i}(\mathcal{X})$ e $\mathcal{M}_{\rho_i} = \mathcal{R}\backslash\mathcal{O}_{Q_i}(\mathcal{X})$. Das propriedades de valorização, segue que cada ρ_i é uma função q-peso em $\mathcal{R}$.

O exemplo acima motiva as seguintes considerações.

Seja $\mathcal{R}$ o domínio afim de uma variedade projetiva $\mathcal{X}$ irredutível e definida sobre um corpo $\mathbb{F}$ com k divisores irredutíveis $C_1, ..., C_k$ no infinito (veja definição 1.13 para divisores irredutíveis). Para $i \in \{1, ..., k\}$, seja ν_i uma valorização no corpo de funções $\mathbb{F}(\mathcal{X})$ tal que:

a) $r.posto(\nu_i) = dim\mathcal{X} = d$, e

b) ν_i está centrada em um ponto $\mathbb{F}$-racional não-singular $Q_i \in C_i \subset \mathcal{X}$.

Considere o conjunto ordenado $\Gamma_i := \{-\nu_i(f) : f \in \mathcal{R} \text{ e } \nu_i(f) \prec_i \mathbf{0}\} \cup \{\mathbf{0}\}$ com a ordem $\prec_i$ induzida do grupo de valores de ν_i. Aqui $\mathbf{0}$ é o elemento neutro do grupo de valores de ν_i. Então, pela definição da valorização ν_i, segue que cada $(\Gamma_i, \preceq_i)$ é um semigrupo ordenado.

Proposição 3.10. *Sejam $\mathcal{R}$, ν_i e Γ_i como descrito acima. Então as funções $\rho_i : \mathcal{R} \to \Gamma_i \cup \{-\infty\}$ definidas por*

$$\rho_i(f) = \begin{cases} -\infty & , \text{ se } f = 0; \\ \boldsymbol{0} & , \text{ se } \nu_i(f) \succeq_i \boldsymbol{0}; \\ -\nu_i(f) & , \text{ se } \nu_i(f) \prec_i \boldsymbol{0}. \end{cases}$$

são funções q-pesos em R.

Note que $\mathcal{R}$ pode ser visto como o subanel de K consistindo das funções racionais com pólos em $C_1, ..., C_k$, ou seja,

$$\mathcal{R} = \bigcap_{C \neq C_1,...,C_k} \mathcal{O}_C(\mathcal{X}),$$

onde C percorre todos os divisores irredutíveis de $\mathcal{X}$, exceto $C_1, ..., C_k$, e $\mathcal{O}_C(\mathcal{X})$ é o anel local associado a C.

Dem. Segue, de (a) e da desigualdade de Abhyankar, $rat.posto(\nu_i) + dim(\nu_i) \leq dim(\mathcal{X})$, que $dim(\nu_i) = 0$, e portanto, da hipótese (b), temos que o corpo de resíduos κ_i da valorização ν_i coincide com o corpo $\mathbb{F}$.

Logo, os axiomas Q.1, Q.2, Q.3, Q.4 e Q.6 de funções q-pesos seguem imediatamente da definição de valorização. Provemos o axioma Q.5.

Sejam $f, g \in \mathcal{M}_{\rho_i}$ tais que $\rho_i(f) = \rho_i(g)$. Então $-\nu_i(f) = -\nu_i(g)$, ou seja, $\nu_i(f/g) = \mathbf{0}$. Assim, como $\kappa_i \cong \mathbb{F}$, existe $\lambda_i \in \mathbb{F}$ tal que $\nu_i(f/g - \lambda_i) \succ_i \mathbf{0}$. Logo, $\rho_i(f - \lambda_i g) \prec_i \rho_i(g)$.

Portanto, segue que ρ_i é uma função q-peso em $\mathcal{R}$. ∎

Observação 3.11. Como ν_i é uma valorização de posto racional d, segue que o grupo de valores Λ_i de ν_i é isomorfo (como grupo) a $\mathbb{Z}^d$ (logo $\mathbf{0} = (0, ..., 0) \in \mathbb{Z}^d$). Agora o posto de ν_i pode ser qualquer inteiro r tal que $1 \leq r \leq d$. Assim, no grupo de valores Λ_i podemos ter r ordens diferentes. Por exemplo, se $r = d$ então Λ_i é discreto, e portanto, a ordem em Λ é a ordem lexicográfica. Se $r = 1$ temos que Λ_i é um subgrupo de $\mathbb{R}$ gerado por d números reais $\mathbb{Q}$-linearmente independentes e a ordem em Λ_i é a ordem induzida de $\mathbb{R}$ (ver cap.1, §1.1, ordem lexicográfica graduada com pesos).

Exemplo 3.12. Seja $\mathcal{X}$ uma variedade projetiva irredutível e definida sobre um corpo $\mathbb{F}$, e sejam $C_1, ..., C_k$ divisores irredutíveis de $\mathcal{X}$. Considere, para cada $i = 1, ..., k$, a seguinte cadeia de subvariedades

$$\mathcal{F}_i : \mathcal{X} = V_{i_0} \supset V_{i_1} \supset V_{i_2} \supset ... \supset V_{i_{d-1}} \supset V_{i_d},$$

onde d é a dimensão de $\mathcal{X}$, V_{i_j} é um divisor irredutível em $V_{i_{j-1}}$, $j = 1, ..., d$ e $V_{i_1} = C_i$.

Como cada V_{i_j} é um divisor irredutível em $V_{i_{j-1}}$, cada função racional g em $V_{i_{j-1}}$ tem uma ordem (de zero ou de pólo) bem definida ao longo de V_{i_j}, denotada por $\nu_{i_j}(g)$. Note que, das hipóteses, segue que V_{i_d} é um ponto $\mathbb{F}$-racional não singular na curva irredutível $V_{i_{d-1}}$.

Assim, qualquer família $\mathcal{F}_i$ define uma valorização $\nu_{\mathcal{F}_i}$ no corpo de funções $\mathbb{F}(\mathcal{X})$ como segue. Para cada $i \in \{1, ..., k\}$ e $j \in \{1, ..., d\}$, fixe uma função g_{i_j} em $V_{i_{j-1}}$ com um zero de ordem 1 ao longo de V_{i_j}, ou seja, g_{i_j} é um parâmetro local de V_{i_j} [ver [Sh1], cap.2,§3, teorema 1]. Dado $f \in \mathbb{F}(V_{i_{j-1}})$, denote por $\overline{f}^{i_j} \in \mathbb{F}(V_{i_j})$ o V_{i_j}-resíduo da função f.

Então, dado $f \in \mathbb{F}(\mathcal{X})$, temos que $f = g_{i_1}^{n_{i_1}} u_{i_1}$, com $n_{i_1} = \nu_{i_1}(f) \in \mathbb{Z}$ e $\nu_{i_1}(u_{i_1}) = 0$. Assim, $\overline{u_{i_1}}^{i_1} \in \mathbb{F}(V_{i_1})$. Logo, $\overline{u_{i_1}}^{i_1} = g_{i_2}^{n_{i_2}} u_{i_2}$, com $n_{i_2} = \nu_{i_2}(\overline{u_{i_1}}^{i_1}) \in \mathbb{Z}$ e $\nu_{i_2}(u_{i_2}) = 0$. Então $\overline{u_{i_2}}^{i_2} \in \mathbb{F}(V_{i_2})$. Continuando, temos que $\overline{u_{i_{j-1}}}^{i_{j-1}} = g_{i_j}^{n_{i_j}} u_{i_j}$, com $n_{i_j} = \nu_{i_j}(\overline{u_{i_{j-1}}}^{i_{j-1}}) \in \mathbb{Z}$ e $\nu_{i_j}(u_{i_j}) = 0$.

Tome

$$\nu_{\mathcal{F}_i}(f) = (n_{i_1}, ..., n_{i_d}) \in \mathbb{Z}^d.$$

Então $\nu_{\mathcal{F}_i}$ é uma valorização discreta de $\mathbb{F}(\mathcal{X})$ de posto racional d, posto d e grupo de valores $\mathbb{Z}^d$, ordenado pela ordem lexicográfica ($\preceq_{lex}$). Os valores de $\nu_{\mathcal{F}_i}(f)$ dependem da escolha dos parâmetros locais g_{i_j}, mas todas as escolhas de g_{i_j} terão ordens equivalentes (ver [Sh1],cap.3,§1 e [Gri-Ha], cap.1,§1).

Agora, seja $\mathcal{R} = \cap_{V \neq V_{i_1}} \mathcal{O}_V(\mathcal{X})$ o subanel de $\mathbb{F}(\mathcal{X})$ consistindo das funções com pólos somente ao longo de V_{i_1}, $i = 1, ..., k$. Então, para cada i, segue que

$$\Gamma_i := \{-\nu_{\mathcal{F}_i}(f) : f \in \mathcal{R} \text{ e } \nu_{\mathcal{F}_i}(f) \prec_{lex} \mathbf{0}\} \cup \{\mathbf{0}\}$$

é um subsemigrupo ordenado de $\mathbb{Z}^d$, e, pela proposiçao anterior, a função $\rho_i : \mathcal{R} \to \Gamma_i \cup \{-\infty\}$,

$$\rho_i(f) = \begin{cases} -\infty & , \ se\ f = 0; \\ \mathbf{0} & , \ se\ \nu_{\mathcal{F}_i}(f) \succeq_{lex} \mathbf{0}; \\ -\nu_{\mathcal{F}_i}(f) & , \ se\ \nu_{\mathcal{F}_i}(f) \prec_{lex} \mathbf{0}. \end{cases}$$

é uma função q-peso em R.

3.3 Normalização

Definição 3.13. Seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura q-ordem. Definimos a *normalização* de ρ como sendo a função $\tilde{\rho} : \mathcal{R} \to \Gamma \cup \{-\infty\}$ dada por $\tilde{\rho}(0) = -\infty$ e para $f \neq 0$

$$\tilde{\rho}(f) := \begin{cases} 0 & , \text{ se } f \in \mathcal{U}_\rho, \\ \rho(f) & , \text{ se } f \in \mathcal{M}_\rho. \end{cases}$$

Então, se ρ é uma função q-ordem em $\mathcal{R}$ segue que $\tilde{\rho}$ também é uma função q-ordem em $\mathcal{R}$. Diremos que uma função q-ordem ρ é *normal* se $\rho = \tilde{\rho}$ e se ρ for sobrejetiva.

A partir de agora, todas as funções q-ordem serão tomadas normais.

Lema 3.14. *Se $(\mathcal{R}, \rho, \Gamma)$ é uma estrutura q-peso sobre $\mathbb{F}$, então os conjuntos $\mathcal{U}_\rho$ e $\mathcal{M}_\rho$ são fechados para o produto em $\mathcal{R}$ e $\mathcal{U}_\rho$ também é fechado para a soma em $\mathcal{R}$. Neste caso, $\mathcal{U}_\rho$ é uma subálgebra de $\mathcal{R}$.*

Dem. Se $f, g \in \mathcal{U}_\rho$ então $\rho(g) \preceq \rho(1) = 0$ e $\rho(f) \preceq \rho(1) = 0$. Logo $\rho(f+g) \preceq max\{\rho(f), \rho(g)\} \preceq 0$ e portanto $f + g \in \mathcal{U}_\rho$, e $\rho(fg) \preceq \rho(f) + \rho(g) \preceq 0$ e portanto $fg \in \mathcal{U}_\rho$.

Agora, se $f, g \in \mathcal{M}_\rho$ então $\rho(f) \succ 0$ e $\rho(g) \succ 0$. Logo $\rho(fg) = \rho(f) + \rho(g) \succ 0$ e portanto $fg \in \mathcal{M}_\rho$. ∎

Uma maneira de construir funções q-ordens sobre uma $\mathbb{F}$-álgebra é dada a seguir. Aqui, denotamos por $\langle \cdot \rangle_{\mathbb{F}}$ o subespaço vetorial gerado por $\cdot$ sobre $\mathbb{F}$.

Teorema 3.15. *Sejam $(\Gamma, \preceq)$ um semigrupo ordenado e $\mathcal{R}$ uma $\mathbb{F}$-álgebra. Seja $\{f_\alpha : \alpha \in \Gamma^*\} \subset \mathcal{R}\backslash\mathbb{F}$ um conjunto linearmente independente e $\mathcal{U}$ seu completamento que determina uma base de $\mathcal{R}$ sobre $\mathbb{F}$. Seja $L_0 = \langle \mathcal{U} \rangle_{\mathbb{F}}$ e $L_\gamma = \langle \mathcal{U} \cup \{f_\alpha : \alpha \in \Gamma \text{ e } \alpha \preceq \gamma\}\rangle_{\mathbb{F}}$, para cada $\gamma \in \Gamma^*$. Para $\alpha, \beta \in \Gamma$ defina $l(\alpha, \beta) = min_{\preceq}\{\gamma \in \Gamma : f_\alpha f_\beta \in L_\gamma\}$ e suponha, para $\alpha, \delta \in \Gamma$ com $\alpha \prec \delta$, que $l(\alpha, \beta) \prec l(\delta, \beta)$ para todo $\beta \in \Gamma^*$, e que $l(\alpha, 0) \preceq l(\delta, 0)$. Seja $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ uma função definida por $\rho(0) = -\infty$ e se $f \in \mathcal{R}\backslash\{0\}$, $\rho(f) = min_{\preceq}\{\gamma \in \Gamma : f \in L_\gamma\}$. Então $(\mathcal{R}, \rho, \Gamma)$ é uma estrutura q-ordem sobre $\mathbb{F}$. Se, além disso, $l(\alpha, \beta) \preceq \alpha + \beta$, com igualdade se $\alpha, \beta \succ 0$, então ρ é uma função q-peso em $\mathcal{R}$.*

Dem. Observe que $\langle \mathcal{U} \rangle_{\mathbb{F}} \subseteq \mathcal{U}_\rho$, $\{f_\alpha | \alpha \in \Gamma^*\} \subset \mathcal{M}_\rho$ e que $\rho(f_\alpha) = \alpha$ para todo $\alpha \in \Gamma$. Logo, ρ é sobrejetiva. Os axiomas (Q.1), (Q.2) e (Q.3) de função q-ordem são imediatos da definição de ρ. Provemos (Q.4) e (Q.5).

Axioma (Q.4): Sejam $f, g, h \in \mathcal{R}$ tais que

$$f = \sum_{\substack{finita \\ \alpha \preceq \alpha_0}} \lambda_\alpha f_\alpha,\ g = \sum_{\substack{finita \\ \alpha \preceq \alpha_1}} a_\alpha f_\alpha \text{ e } h = \sum_{\substack{finita \\ \alpha \preceq \alpha_2}} b_\alpha f_\alpha.$$

Suponha que $\rho(f) \prec \rho(g)$ e $h \neq 0$. Se $f = 0$, então $-\infty = \rho(f) \prec 0 \preceq \rho(g)$ e $\rho(fh) = -\infty \preceq \rho(gh)$. Suponha agora, s.p.g., que $\lambda_{\alpha_0}, a_{\alpha_1}, b_{\alpha_2} \neq 0$. Se $f \neq 0$ então $0 \preceq \alpha_0 = \rho(f) \prec \rho(g) = \alpha_1$. Para $0 \preceq \alpha \prec \alpha_1$, como $h \in L_{\alpha_2}$, temos que $f_\alpha h \in L_{l(\alpha,\alpha_2)}$. Como $L_{l(0,\alpha_2)} \subseteq L_{l(\alpha,\alpha_2)} \subseteq L_{l(\alpha_1,\alpha_2)}$, temos que $gh \in L_{l(\alpha_1,\alpha_2)}$. De forma análoga, $fh \in L_{l(\alpha_0,\alpha_2)}$. Mais ainda, $\rho(fh) = l(\alpha_0, \alpha_2)$ e $\rho(gh) = l(\alpha_1, \alpha_2)$. Assim, se $h \in \mathcal{U}_\rho$ então $\alpha_2 = 0$ e logo, por hipótese, $\rho(fh) = l(\alpha_0, 0) \preceq l(\alpha_1, 0) = \rho(gh)$. Agora, se $h \in \mathcal{M}_\rho$, então $\alpha_0 \succ 0$ e $l(\alpha_0, \alpha_2) \prec l(\alpha_1, \alpha_2)$. Logo $\rho(fh) \prec \rho(gh)$.

Axioma (Q.5): Se $\rho(f) = \rho(g) \neq 0$, basta tomar $\lambda = \lambda_{\alpha_0}/a_{\alpha_1} \in \mathbb{F}\backslash\{0\}$.

Portanto ρ é uma função q-ordem em $\mathcal{R}$.

Agora se $l(\alpha, \beta) \preceq \alpha + \beta$, com igualdade se $\alpha, \beta \succ 0$, para todo $\alpha, \beta \in \Gamma$, então $\rho(fg) = l(\alpha_0, \alpha_1) \preceq \alpha_0 + \alpha_1 = \rho(f) + \rho(g)$, e se $\alpha_0, \alpha_1 \succ 0$, então $\rho(fg) = l(\alpha_0, \alpha_1) = \alpha_0 + \alpha_1 = \rho(f) + \rho(g)$, ou seja, ρ é uma função q-peso em $\mathcal{R}$. ∎

3.4 Funções Q-Ordens sobre Anéis Tóricos

Nesta seção, veremos um método de como construir exemplos de funções q-ordens sobre anéis tóricos. Para maiores detalhes sobre anéis tóricos veja [Stu], cap. 4, e [IVA], cap.3, §3.

Fixe um subconjunto $\mathcal{A} = \{a_1, ..., a_n\} \subset \mathbb{Z}^d$. Seja M_n o conjunto de todos os monômios em $\mathbb{F}[X_1, ..., X_n]$. Defina uma função monomial $\omega : M_n \to \mathbb{Z}^d$ por

$$\omega(\mathbf{X}^\alpha) = \sum_{i=1}^{n} \alpha_i a_i,$$

onde $\alpha = (\alpha_1, ..., \alpha_n), \alpha_i \in \mathbb{N}_0$ e $\mathbf{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$.

Note que a imagem de ω é o semigrupo

$$\mathbb{N}_0\mathcal{A} = \langle \alpha_1 a_1 + ... + \alpha_n a_n : \alpha_i \in \mathbb{N}_0 \rangle \subseteq \mathbb{Z}^d.$$

Definição 3.16. Definimos um *ideal tórico* em $\mathbb{F}[X_1, ..., X_n]$ como sendo o ideal

$$I_\mathcal{A} := (\mathbf{X}^\alpha - \mathbf{X}^\beta : \alpha, \beta \in \mathbb{N}_0^n,\ \omega(\mathbf{X}^\alpha) = \omega(\mathbf{X}^\beta)).$$

A variedade afim $\mathcal{V}(I_\mathcal{A})$ em $\mathbb{F}^n$ é chamada *variedade tórica afim*, e definimos o *anel tórico* de $\mathcal{V}(I_\mathcal{A})$ como sendo o anel quociente $\mathbb{F}[X_1, ..., X_n]/I_\mathcal{A}$.

Observação 3.17. O anel tórico $\mathbb{F}[X_1, ..., X_n]/I_\mathcal{A}$ é isomorfo a um subanel do anel de polinômios de Laurent

$$\mathbb{F}[\mathbf{T}^{\pm 1}] = \mathbb{F}[T_1^{\pm 1}, ..., T_d^{\pm 1}] \cong \mathbb{F}[T_0, T_1 ..., T_d]/(T_0 \cdot T_1 \cdot ... \cdot T_d - 1).$$

Neste caso, o ideal tórico $I_\mathcal{A}$ é o núcleo do homomorfismo de álgebras

$$\pi : \mathbb{F}[X_1, ..., X_n] \to \mathbb{F}[\mathbf{T}^{\pm 1}]$$
$$f(X_1, ..., X_n) \longmapsto f(\mathbf{T}^{a_1}, ..., \mathbf{T}^{a_n}),$$

onde $a_i = (a_{i1}, ..., a_{id}) \in \mathbb{Z}^d$ e $\mathbf{T}^{a_i} = T_1^{a_{i1}} \cdots T_d^{a_{id}}$.

Um procedimento para encontrar os geradores do ideal tórico $I_{\mathcal{A}}$ é dado a seguir.

Algoritmo:

1) Seja o anel $\mathbb{F}[T_0, T_1, ..., T_d, X_1, ..., X_n] =: \mathbb{F}[\mathbf{T}, \mathbf{X}]$. Considere a ordem lexicográfica $\prec_{lex}$ em $\mathbb{F}[\mathbf{T}, \mathbf{X}]$ dada por

$$X_n \prec_{lex} ... \prec_{lex} X_1 \prec_{lex} T_d \prec_{lex} ... \prec_{lex} T_0.$$

2) Compute a base de Gröbner $\mathcal{G}$ para o ideal

$$(T_0 \cdot T_1 \cdot ... \cdot T_d - 1, X_1\mathbf{T}^{a_1^-} - \mathbf{T}^{a_1^+}, ..., X_n\mathbf{T}^{a_n^-} - \mathbf{T}^{a_n^+}),$$

onde $a_i = a_i^+ - a_i^-$, com $a_i^+, a_i^- \in \mathbb{N}_0^d$, $i = 1, ..., n$.

3) Saída: O conjunto $\tilde{\mathcal{G}} = \mathcal{G} \cap \mathbb{F}[\mathbf{X}]$ é a base de Gröbner reduzida para o ideal $I_{\mathcal{A}}$ com respeito a ordem lexicográfica.

Observação 3.18. O conjunto $\tilde{\mathcal{G}}$ é um conjunto finito de elementos da forma $\mathbf{X}^\alpha - \mathbf{X}^\beta$ tais que $\alpha, \beta \in \mathbb{N}_0^n$ e $\omega(\mathbf{X}^\alpha) = \omega(\mathbf{X}^\beta)$.

Vejamos agora como podemos construir as funções q-ordens sobre anéis tóricos.

Seja F um elemento não-nulo do anel $\mathbb{F}[X_1, ..., X_n]$. Então F pode ser escrito da seguinte maneira: $F = \sum_{finita} \lambda_\alpha \mathbf{X}^\alpha$, $\lambda_\alpha \in \mathbb{F}$. Assim, defina o *suporte* de F como $supp(F) = \{\mathbf{X}^\alpha : \lambda_\alpha \neq 0\}$. Considere em $\mathbb{Z}^d$ uma ordem total $\preceq$. Então podemos estender a função monomial $\omega : M_n \to \mathbb{Z}^d$, definida acima, para $\mathbb{F}^*[X_1, ..., X_n]$ por

$$\begin{array}{rccl} \omega: & \mathbb{F}^*[X_1, ..., X_n] & \to & \mathbb{Z}^d \\ & F & \mapsto & \omega(F) = max_{\preceq}\{\omega(\mathbf{X}^\alpha) : \mathbf{X}^\alpha \in supp(F)\}. \end{array}$$

Seja $I_{\mathcal{A}} = (\tilde{\mathcal{G}})$ o ideal tórico de $\mathbb{F}[X_1, ..., X_n]$ associado ao conjunto $\mathcal{A}$.

Considere o anel tórico $\mathcal{R} = \mathbb{F}[X_1, ..., X_n]/I_{\mathcal{A}}$ e seja $\mathbf{x}^\alpha$ a classe de $\mathbf{X}^\alpha$ módulo $I_{\mathcal{A}}$. Defina, para cada $\mathbf{x}^\alpha \in \mathcal{R}$ a função $\omega(\mathbf{x}^\alpha) := \omega(\mathbf{X}^\alpha)$. Temos que esta função está bem definida, pois se $\mathbf{x}^\alpha = \mathbf{x}^\beta$ então $\mathbf{X}^\alpha - \mathbf{X}^\beta \in I_{\mathcal{A}}$ e logo $\omega(\mathbf{X}^\alpha) = \omega(\mathbf{X}^\beta)$ (ver [Stu], cap. 4, Lema 4.1) , ou seja, $\omega(\mathbf{x}^\alpha) = \omega(\mathbf{x}^\beta)$.

Seja $\Delta(I_{\mathcal{A}})$ a pegada de $I_{\mathcal{A}}$, ou seja, $\Delta(I_{\mathcal{A}}) = \{\alpha \in \mathbb{N}_0^n : \mathbf{X}^\alpha \notin LT(I_{\mathcal{A}})\}$, onde $LT(I_{\mathcal{A}})$ é o conjunto dos termos lideres de $I_{\mathcal{A}}$, com respeito a ordem lexicográfica. Tome o conjunto $B = \{\mathbf{x}^\alpha : \alpha \in \Delta(I_{\mathcal{A}})\} \subset \mathcal{R}$. Temos que B é uma base de $\mathcal{R}$ como $\mathbb{F}$-espaço vetorial (ver [IVA], cap.5, §3, prop.1). Assim, dado $f \in \mathcal{R}$, $f \neq 0$, este elemento pode ser escrito de maneira única como $f = \sum_{finita} \lambda_\alpha \mathbf{x}^\alpha$, com $\lambda_\alpha \in \mathbb{F}$. Então, defina

$$\omega(f) = max_{\preceq}\{\omega(\mathbf{x}^\alpha) : \mathbf{x}^\alpha \in supp(f)\}.$$

Seja $\Gamma := \{\gamma \in \mathbb{N}_0\mathcal{A} : \mathbf{0} := (0, ..., 0) \preceq \gamma\} \subseteq \mathbb{N}_0\mathcal{A}$. Suponha que $\preceq$ seja uma ordem total admissível em Γ. Então $(\Gamma, \preceq)$ é um semigrupo ordenado.

Proposição 3.19. *A função $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ definida por*

$$\rho(f) = \begin{cases} -\infty & , \text{ se } f = 0; \\ \mathbf{0} & , \text{ se } f \neq 0 \text{ e } \omega(f) \preceq \mathbf{0}; \\ \omega(f) & , \text{ se } \omega(f) \succ \mathbf{0}. \end{cases}$$

é uma função q-peso em $\mathcal{R}$.

Dem. Seja $B' = \{\mathbf{x}^\alpha \in B : \omega(\mathbf{x}^\alpha) \in \Gamma^*\} \subset B$. Temos que B' é um conjunto linearmente independente de $\mathcal{R}$. Seja $\mathcal{U} = B \backslash B'$. Seja $L_0 := \langle \mathcal{U} \rangle_{\mathbb{F}}$ e $L_\gamma := \langle \mathcal{U} \cup \{\mathbf{x}^\alpha \in B' : \omega(\mathbf{x}^\alpha) \preceq \gamma\}\rangle_{\mathbb{F}}$ subconjuntos de $\mathcal{R}$. Como ω é sobrejetivo, segue que, para cada $\gamma \in \Gamma$, existe $\mathbf{x}^\alpha \in L_\gamma$ tal que $\omega(\mathbf{x}^\alpha) = \gamma$. Logo ρ é uma função sobrejetiva. Assim, defina

$$l(\omega(\mathbf{x}^\alpha), \omega(\mathbf{x}^\beta)) := min_{\preceq}\{\gamma \in \Gamma : \mathbf{x}^\alpha \mathbf{x}^\beta \in L_\gamma\}.$$

Observe que, $\mathbf{x}^\alpha \cdot \mathbf{x}^\beta = \mathbf{x}^{\alpha+\beta}$ e, da definição de ω, $\omega(\mathbf{x}^\alpha \mathbf{x}^\beta) = \omega(\mathbf{x}^\alpha) + \omega(\mathbf{x}^\beta)$.

Assim, se $\omega(\mathbf{x}^\alpha) \prec \omega(\mathbf{x}^\beta)$ e $\omega(\mathbf{x}^\gamma) \succ 0$, temos que $\omega(\mathbf{x}^\alpha \mathbf{x}^\gamma) \prec \omega(\mathbf{x}^\beta \mathbf{x}^\gamma)$, e portanto $l(\omega(\mathbf{x}^\alpha), \omega(\mathbf{x}^\gamma)) \preceq l(\omega(\mathbf{x}^\beta), \omega(\mathbf{x}^\gamma))$. Agora, se $\omega(\mathbf{x}^\beta) \succ 0$ então $l(\omega(\mathbf{x}^\alpha), \omega(\mathbf{x}^\gamma)) \prec l(\omega(\mathbf{x}^\beta), \omega(\mathbf{x}^\gamma))$. Mais ainda, $l(\omega(\mathbf{x}^\alpha), \omega(\mathbf{x}^\beta)) \preceq \omega(\mathbf{x}^\alpha) + \omega(\mathbf{x}^\beta)$ se $\omega(\mathbf{x}^\alpha), \omega(\mathbf{x}^\beta) \in \Gamma$, com igualdade se $\omega(\mathbf{x}^\alpha) \succ \mathbf{0}$ e $\omega(\mathbf{x}^\beta) \succ \mathbf{0}$.

Então, da definição de ω, de ρ e de L_γ, segue, para $f \in \mathcal{R}\backslash\{0\}$, que $\rho(f) = min_{\preceq}\{\gamma \in \Gamma | f \in L_\gamma\}$, e portanto, do teorema 3.15, segue que ρ é uma função q-peso em $\mathcal{R}$. ∎

Observação 3.20. Note que, se $\mathcal{U}_\rho = \mathbb{F}$, então $\Gamma = \mathbb{N}_0\mathcal{A}$ é bem ordenado, pois este é um semigrupo finitamente gerado livre de inverso. Logo, da observação 3.2, segue que ρ é uma função peso.

Exemplo 3.21. Seja $\mathcal{A} = \{(-1,1),(0,1),(1,1)\} \subset \mathbb{Z}^2$. Considere M o conjunto dos monômios de $\mathbb{F}[X,Y,Z]$ e defina a função monomial $\omega : M \to \mathbb{Z}^2$ por

$$\omega(X) = (-1,1);\ \omega(Y) = (1,1);\ \omega(Z) = (0,1).$$

Vamos encontrar o ideal tórico associado a $\mathcal{A}$ em $\mathbb{F}[X,Y,Z]$. Pelo algoritmo dado acima, uma base de Gröbner para o ideal $(T_0T_1T_2 - 1, XT_1 - T_2, Y - T_1T_2, Z - T_2)$ de $\mathbb{F}[T_0,T_1,T_2,X,Y,Z]$ é dada por

$$\mathcal{G} = \{XY - Z^2, T_2 - Z, ZT_1 - Y, XT_1 - Z, Z^2T_0 - X, YT_0 - 1\}.$$

Portanto, o ideal tórico associado a $\mathcal{A}$ em $\mathbb{F}[X,Y,Z]$ é dado por

$$I_\mathcal{A} = (XY - Z^2).$$

Seja $\mathbb{N}_0\mathcal{A} = \langle(-1,1),(0,1),(1,1)\rangle$ o semigrupo gerado por $\mathcal{A}$ e considere $\preceq$ a ordem lexicográfica em $\mathbb{Z}^2$. Seja $\Gamma := \{\gamma \in \mathbb{N}_0\mathcal{A} : (0,0) \preceq \gamma\} = \langle(0,1),(1,1)\rangle$. Então, para o anel tórico $\mathcal{R} = \mathbb{F}[X,Y,Z]/I_\mathcal{A}$, temos, da proposição 3.19, uma função q-peso $\rho_1 : \mathcal{R} \to \Gamma \cup \{-\infty\}$ com $\rho_1(x) = (0,0)$, $\rho_1(y) = (1,1)$ e $\rho_1(z) = (0,1)$, onde x, y, z são as classes de X, Y, Z modulo $I_\mathcal{A}$. Neste caso $\mathcal{U}_{\rho_1} = \{\sum_{finita} \lambda_{ab}x^az^b : \lambda_{ab} \in \mathbb{F},\ a \neq 0 \text{ ou } a = b = 0\}$.

Por outro lado, se tomarmos $\omega(X) = (1,1),\ \omega(Y) = (-1,1),\ \omega(Z) = (0,1)$, teremos o mesmo ideal tórico $I_\mathcal{A} = (XY - Z^2)$ em $\mathbb{F}[X,Y,Z]$, e portanto, da proposição 3.19, podemos construir uma outra função q-peso $\rho_2 : \mathcal{R} \to \Gamma \cup \{-\infty\}$ com $\rho_2(x) = (1,1)$, $\rho_2(y) = (0,0)$ e $\rho_2(z) = (0,1)$. Aqui, temos que $\mathcal{U}_{\rho_2} = \{\sum_{finita} \lambda_{bc}y^cz^b : \lambda_{bc} \in \mathbb{F},\ c \neq 0 \text{ e } c = b = 0\}$.

Exemplo 3.22. Considere agora $\mathcal{A} = \{-1,2,3\} \subset \mathbb{Z}$. Definindo ω sobre os monômios de $\mathbb{F}[X,Y,Z]$ com

$$\omega(X) = -1,\ \omega(Y) = 2 \text{ e } \omega(Z) = 3,$$

podemos encontrar, pelo algoritmo acima, a seguinte base de Gröbner para o ideal $(T_0T_1 - 1, XT_1 - 1, Y - T_1^2, Z - T_1^3)$ de $\mathbb{F}[T_0, T_1, X, Y, Z]$:

$$\mathcal{G} = \{Y^3 - Z^2, XZ - Y, XY^2 - Z, X^2Y - 1, T_1 - XY, T_0 - X\}.$$

Logo, temos que o ideal tórico associado a $\mathcal{A}$ é dado por

$$I_{\mathcal{A}} = (Y^3 - Z^2, XZ - Y, XY^2 - Z, X^2Y - 1).$$

Seja $\mathbb{N}_0\mathcal{A} = \langle -1, 2, 3\rangle = \mathbb{Z}$ o semigrupo gerado por $\mathcal{A}$ e considere $<$ a ordem usual de $\mathbb{Z}$. Então $\Gamma := \{\gamma \in \mathbb{N}_0\mathcal{A} : 0 \leq \gamma\} = \mathbb{N}_0$. Então, para o anel tórico $\mathcal{R} = \mathbb{F}[X, Y, Z]/I_{\mathcal{A}}$, temos, da proposição 3.19, uma função q-peso $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ com $\rho(x) = 0$, $\rho(y) = 2$ e $\rho(z) = 3$, onde x, y, z são as classes de X, Y, Z modulo $I_{\mathcal{A}}$. Aqui $\mathcal{U}_\rho = \{\sum_{finita} \lambda_{abc}x^a y^b z^c : \lambda_{abc} \in \mathbb{F} \text{ e } 2b + 3c \leq a\}$.

Exemplo 3.23. Seja $\mathcal{A} = \{(1, 0, 0), (0, 1, 0), (0, 0, -1)\} \subset \mathbb{Z}^3$. Definindo ω sobre os monômios de $\mathbb{F}[X, Y, Z]$ por

$$\omega(X) = (1, 0, 0),\ \omega(Y) = (0, 1, 0) \text{ e } \omega(Z) = (0, 0, -1)$$

podemos encontrar, pelo algoritmo acima, a seguinte base de Gröbner para o ideal $(T_0T_1T_2T_3 - 1, X - T_1, Y - T_2, ZT_3 - 1)$ de $\mathbb{F}[T_0, T_1, T_2, T_3, X, Y, Z]$:

$$\mathcal{G} = \{ZT_3 - 1, T_2 - Y, T_1 - X, YXT_0 - Z\}.$$

Assim, o ideal tórico associado a $\mathcal{A}$ é $I_{\mathcal{A}} = (0)$.

Seja $\mathbb{N}_0\mathcal{A}$ o semigrupo gerado por $\mathcal{A}$ e considere $\preceq$ a ordem lexicográfica graduada em $\mathbb{Z}^3$. Seja $\Gamma := \{\gamma \in \mathbb{N}_0\mathcal{A} : (0, 0, 0) \preceq \gamma\} = \langle (1, 0, 0), (0, 1, 0), (1, 0, -1), (0, 1, -1)\rangle$. Então, para o anel tórico $\mathcal{R} = \mathbb{F}[X, Y, Z]/I_{\mathcal{A}} = \mathbb{F}[X, Y, Z]$, temos, da proposição 3.19, uma função q-peso $\rho : \mathcal{R} \to \Gamma \cup \{-\infty\}$ com $\rho(X) = (1, 0, 0)$, $\rho(Y) = (0, 1, 0)$, $\rho(Z) = (0, 0, 0)$, $\rho(XZ) = (1, 0, -1)$ e $\rho(YZ) = (0, 1, -1)$. Neste caso $\mathcal{U}_\rho = \{\sum_{finita} \lambda_{abc}X^a Y^b Z^c : \lambda_{bc} \in \mathbb{F} \text{ e } a + b < c \text{ ou } a = b = c = 0\}$.

3.5 Bases

Agora, faremos algumas considerações com o objetivo de se determinar uma $\mathbb{F}$-base para a $\mathbb{F}$-álgebra $\mathcal{R}$ por meio de funções q-pesos. Aqui, vamos supor que o semigrupo de valores Γ de uma função q-peso é um semigrupo bem ordenado. Os resultados aqui obtidos são análogos aos apresentados em [Si], capítulo 2.

Seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura q-ordem sobre $\mathbb{F}$ com $\mathcal{U}_\rho \neq \mathcal{R}\backslash\{0\}$. Como ρ é sobrejetiva, então, para cada $\alpha \in \Gamma$, existe $f_\alpha \in \mathcal{R}$ tal que $\rho(f_\alpha) = \alpha$.

Lema 3.24. *Seja $f \in \mathcal{M}_\rho$. Então existem únicos $\lambda_\alpha \in \mathbb{F}^*$ com $\alpha \in I \subset \Gamma$, I finito, tais que*

$$f - \sum_{\alpha \in I} \lambda_\alpha f_\alpha \in \mathcal{U}_\rho.$$

Dem. Como $\mathcal{U}_\rho \neq \mathcal{R}\backslash\{0\}$ então $\mathcal{M}_\rho \neq \emptyset$. Logo $\rho(\mathcal{M}_\rho)$ possui infinitos elementos, pois se $f \in \mathcal{M}_\rho$ então $0 \prec \rho(f)$ e de (Q.4), $0 \prec \rho(f) \prec \rho(f^2) \prec \rho(f^3) \prec \ldots$. Assim, para $f \in \mathcal{M}_\rho$, suponha $\rho(f) = \alpha = \rho(f_\alpha)$. Então, pelo axioma (Q.5), existe $\lambda_\alpha \in \mathbb{F}^*$ tal que $\rho(f - \lambda_\alpha f_\alpha) \prec \alpha$. Logo, $f - \lambda_\alpha f_\alpha \in \mathcal{U}_\rho$, ou existe $\beta \in \Gamma$, $\beta \prec \alpha$, tal que $\rho(f - \lambda_\alpha f_\alpha) = \beta = \rho(f_\beta)$. Então, novamente pelo axioma (Q.5), existe $\lambda_\beta \in \mathbb{F}^*$ tal que $\rho(f - \lambda_\alpha f_\alpha - \lambda_\beta f_\beta) \prec \beta$. Continuando o processo, temos que existem $\lambda_\alpha \in \mathbb{F}^*$, com $\alpha \in I \subset \Gamma$, I finito (pois Γ é bem ordenado), tais que $\rho(f - \sum_{\alpha \in I} \lambda_\alpha f_\alpha) \preceq 0 = \rho(1)$, ou seja, $f - \sum_{\alpha \in I} \lambda_\alpha f_\alpha \in \mathcal{U}_\rho$.

A unicidade dos $\lambda_\alpha \in \mathbb{F}^*$ segue da propriedade (4) do lema 3.7 de funções q-ordens.

■

Teorema 3.25. *Para $\alpha, \beta \in \Gamma$, seja $L_\alpha := \{f \in \mathcal{R} | \rho(f) \preceq \alpha\}$ e defina $l(\alpha, \beta) = min_{\preceq}\{\gamma \in \Gamma | f_\alpha f_\beta \in L_\gamma\}$. Então,*

1) $(L_\alpha)_{\alpha \in \Gamma}$ forma uma sequência crescente de subespaços vetoriais de $\mathcal{R}$ com $\mathbb{F} \subseteq L_0$, e existe, para todo $\gamma \in \Gamma$, um subconjunto linearmente independente $\{f_\alpha \in \mathcal{R} | \alpha \in \Gamma \text{ e } \alpha \preceq \gamma\}$ em L_γ tal que, para $f \in L_\gamma$, f pode ser escrito de maneira única como $f = f_0 + \sum_{\beta \preceq \alpha} \lambda_\beta f_\beta$.

2) Para todos $\alpha, \beta \in \Gamma$, $l(\alpha, \beta) = l(\beta, \alpha)$ e se $\delta \in \Gamma$ é tal que $\alpha \prec \delta$ então $l(\alpha, \beta) \preceq l(\delta, \beta)$, com desigualdade estrita se $\beta \neq 0$.

3) Se ρ é uma função q-peso, então $l(\alpha, \beta) \preceq \alpha + \beta$, para todos $\alpha, \beta \in \Gamma$, com igualdade se $\alpha, \beta \neq 0$.

Dem. 1) Temos, de fato, que se $\alpha \preceq \beta$ então $L_\alpha \subseteq L_\beta$, para $\alpha, \beta \in \Gamma$. Assim, o conjunto $\{f_\alpha \in \mathcal{M}_\rho | \rho(f_\alpha) = \alpha \in \Gamma\} \subseteq L_\alpha$ é um conjunto linearmente independente em L_α, pois seja $\sum_{\beta \preceq \alpha} \lambda_\beta f_\beta = 0$, onde $\beta \in \Gamma$, $\beta \preceq \alpha$ e $\lambda_\beta \in \mathbb{F}$. Então, se $\lambda_\alpha \neq 0$, temos

$$0 \prec \alpha = \rho(\lambda_\alpha f_\alpha) = \rho(\textstyle\sum_{\beta \prec \alpha} \lambda_\beta f_\beta) = \rho(0) = -\infty, \text{ contradição.}$$

Logo, $\lambda_\alpha = 0$. Continuando o processo, temos que $\lambda_\beta = 0, \forall \beta \prec \alpha$. Assim, dos axiomas (Q.2) e (Q.3) de funções q-ordens, segue que L_α é um subespaço vetorial.

Mais ainda, se $f \in L_\alpha$ então, pelo lema anterior, existem únicos $\lambda_\beta \in \mathbb{F}$ tais que $f - \sum_{\beta \preceq \alpha} \lambda_\beta f_\beta \in \mathcal{U}_\rho$, ou seja, $f - \sum_{\beta \preceq \alpha} \lambda_\beta f_\beta = f_0 \in \mathcal{U}_\rho = L_0$ e portanto $f = f_0 + \sum_{\beta \preceq \alpha} \lambda_\beta f_\beta$.

2) Pela parte 1 e da definição de $l(\alpha, \beta)$, temos que $l(\alpha, \beta) = \rho(f_\alpha f_\beta)$. Assim, para $\delta \in \Gamma$ tal que $\alpha \prec \delta$, temos que $\rho(f_\alpha) \prec \rho(f_\delta)$ e do axioma (Q.4), segue que $l(\alpha, \beta) = \rho(f_\alpha f_\beta) \preceq \rho(f_\delta f_\beta) = l(\delta, \beta)$. Se $\beta \neq 0$, então $f_\beta \in \mathcal{M}_\rho$ e do axioma (Q.4), segue o resultado.

3) Se ρ é uma função q-peso, então $l(\alpha, \beta) = \rho(f_\alpha f_\beta) \preceq \rho(f_\alpha) + \rho(f_\beta) = \alpha + \beta$, valendo a igualdade se $\alpha \neq 0$ e $\beta \neq 0$, pois neste caso $f_\alpha, f_\beta \in \mathcal{M}_\rho$. ∎

Corolário 3.26. *Seja $\mathbb{F}$ um subcorpo do corpo $\mathbb{G}$. Seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura q-ordem sobre $\mathbb{F}$. Então $(\mathcal{R} \otimes_\mathbb{F} \mathbb{G}, \rho, \Gamma)$ é uma estrutura q-ordem sobre $\mathbb{G}$.*

Dem. Do teorema 3.25, temos que $\{f_\alpha : \alpha \in \Gamma \backslash \{0\}\} \subseteq \mathcal{M}_\rho$ é um conjunto linearmente independente sobre $\mathbb{F}$. Assim, o conjunto $\{f_\alpha \otimes_\mathbb{F} 1_\mathbb{G} : \alpha \in \Gamma \backslash \{0\}\} \subset \mathcal{R} \otimes_\mathbb{F} \mathbb{G}$ é um conjunto linearmente independente sobre $\mathbb{G}$. Então, do teorema 3.15, podemos construir uma estrutura q-ordem $(\mathcal{R} \otimes_\mathbb{F} \mathbb{G}, \rho, \Gamma)$ sobre $\mathbb{G}$. ∎

Para $i = 1, ..., m$, sejam $(\mathcal{R}, \rho_i, \Gamma_i)$ estruturas q-peso em $\mathcal{R}$, onde cada Γ_i é um

semigrupo bem ordenado e $\cap_{i=1}^{m}\mathcal{U}_{\rho_i} \neq \emptyset$. Do Teorema 3.25, $\{f_\alpha : \alpha \in \Gamma_i^*\} \subseteq \mathcal{M}_{\rho_i}$ são conjuntos linearmente independentes em $\mathcal{R}$.

Teorema 3.27. *Seja* $f_0 = 1$. *Seja* $B = \{f_\alpha : \alpha \in \Gamma_1\} \cup \{g_\beta \in \mathcal{U}_{\rho_1} \cap \mathcal{M}_{\rho_2} : \beta \in \Gamma_2^*\} \cup ... \cup \{h_\delta \in (\cap_{i=i}^{m-1}\mathcal{U}_{\rho_i}) \cap \mathcal{M}_{\rho_m} : \delta \in \Gamma_m^*\} \subset \mathcal{R}$. *Se* $\cap_{i=1}^{m}\mathcal{U}_{\rho_i} = \mathbb{F}$, *então o conjunto* B *é uma* $\mathbb{F}$*-base de* $\mathcal{R}$ *como* $\mathbb{F}$*-espaço vetorial.*

Dem. Primeiro, mostremos que o conjunto B é linearmente independente sobre $\mathbb{F}$. Sejam $\lambda_\alpha, \mu_\beta, ..., \xi_\delta \in \mathbb{F}$ tais que

$$\sum_{\alpha \preceq \alpha_0} \lambda_\alpha f_\alpha + \sum_{\beta \preceq \beta_0} \mu_\beta g_\beta + ... + \sum_{\delta \preceq \delta_0} \xi_\delta h_\delta = 0.$$

Então,

$$\rho_1(\sum_{\alpha \preceq \alpha_0} \lambda_\alpha f_\alpha) = \rho_1(-\sum_{\beta \preceq \beta_0} \mu_\beta g_\beta - ... - \sum_{\delta \preceq \delta_0} \xi_\delta h_\delta) = 0,$$

pois $g_\beta, ..., h_\delta \in \mathcal{U}_{\rho_1}$ e $\mathcal{U}_{\rho_1}$ é uma subálgebra de $\mathcal{R}$. Então, pelo axioma (Q.3), $\lambda_\alpha = 0$ para todo $\alpha \succ 0$. Assim, temos que $\lambda_0 + \sum_{\beta \preceq \beta_0} \mu_\beta g_\beta + ... + \sum_{\delta \preceq \delta_0} \xi_\delta h_\delta = 0$. Continuando o porcesso, aplicando ρ_i para $i = 2, ..., m$, temos pelo axioma (Q.3), $\mu_\beta = ... = \xi_\delta = 0$, para todo $\beta, \delta \succ 0$. Logo, $\lambda_0 = 0$ e portanto B é linearmente independente.

Agora, provemos que B gera R. Seja $f \in \mathcal{R}$ tal que $\rho_1(f) = \alpha$, para algum $\alpha \in \Gamma_1$. Pelo lema 3.24, existem $\lambda_a \in \mathbb{F}$, com $a \in \Gamma_1$, $a \preceq \alpha$ e $\lambda_\alpha \neq 0$ tal que $g := f - (\sum_{a \preceq \alpha} \lambda_a f_a) \in \mathcal{U}_{\rho_1}$. Suponha $\rho_2(g) = \beta$ para algum $\beta \in \Gamma_2$. Novamente, do lema 3.24, existem $\mu_b \in \mathbb{F}$, com $b \in \Gamma_2$, $b \preceq \beta$ e $\mu_\beta \neq 0$ tal que $g - (\sum_{b \preceq \beta} \mu_b g_b) \in \mathcal{U}_{(\rho_2|_{\mathcal{U}_{\rho_1}})} = \mathcal{U}_{\rho_1} \cap \mathcal{U}_{\rho_2}$. Continuando este processo, para $i = 3, ..., m$, temos que

$$f - (\sum_{\alpha \preceq \alpha_0} \lambda_\alpha f_\alpha) - (\sum_{\beta \preceq \beta_0} \mu_\beta g_\beta) - ... - (\sum_{\delta \preceq \delta_0} \xi_\delta h_\delta) \in \mathcal{U}_{\rho_m|_{\cap_{i=1}^{m-1}\mathcal{U}_{\rho_i}}} = \cap_{i=1}^{m}\mathcal{U}_{\rho_i} = \mathbb{F}.$$

Logo B gera $\mathcal{R}$ e portanto B é uma $\mathbb{F}$-base de $\mathcal{R}$. ∎

3.6 Conjunto Admissível de Estruturas Q-Pesos

Definição 3.28. Sejam $(\mathcal{R}, \rho_i, \Gamma_i), i = 1, ..., m$, m estruturas q-pesos em $\mathcal{R}$. Dizemos que o conjunto $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, ..., m\}$ é *admissível*, se $\cap_{i=1}^{m}\mathcal{U}_{\rho_i} = \mathbb{F}$.

Exemplo 3.29. No exemplo 3.12, temos que cada $\mathcal{U}_{\rho_k}$ está contido em $\mathcal{O}_{V_{k_1}}(\mathcal{X}) \cap \mathcal{R}$, onde $\mathcal{O}_{V_{k_1}}(\mathcal{X}) = \{f \in \mathbb{F}(\mathcal{X}) : \nu_{k_1}(f) \geq 0\}$. Logo, $\cap_{k=1}^{t} \mathcal{U}_{\rho_k} \subseteq \cap_{k=1}^{t} \mathcal{O}_{V_{k_1}} \cap \mathcal{R} = \mathbb{F}$, e portanto, $\{(\mathcal{R}, \rho_k, \Gamma_k), k = 1, ..., t\}$ é um conjunto admissível de estruturas q-pesos.

Já no exemplo 3.21, como $\mathcal{U}_{\rho_1} = \{\sum_{finita} \lambda_{ab} x^a z^b : \lambda_{bc} \in \mathbb{F},\ a \neq 0 \text{ ou } a = b = 0\}$ e $\mathcal{U}_{\rho_2} = \{\sum_{finita} \lambda_{bc} y^c z^b : \lambda_{bc} \in \mathbb{F},\ c \neq 0 \text{ e } c = b = 0\}$, temos que $\mathcal{U}_{\rho_1} \cap \mathcal{U}_{\rho_2} = \mathbb{F}$, e logo, da definição 3.28, segue que $\{(\mathcal{R}, \rho_1, \rho_2, \Gamma)\}$ é um conjunto admissível de estruturas q-pesos.

Uma consequência imediata da definição acima, é o seguinte resultado.

Proposição 3.30. *Se $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, ..., m\}$ é um conjunto admissível de estruturas q-pesos em $\mathcal{R}$, então $\mathcal{R}$ é um domínio de integridade.*

Dem. Como cada M_{ρ_i} não contém divisores de zero, ver lema 3.7 (1), então o conjunto dos divisores de zero de $\mathcal{R}$ está contido em $\cap_{i=1}^{m} \mathcal{U}_{\rho_i} = \mathbb{F}$ que é corpo. Logo, $\mathcal{R}$ não possui divisores de zero, ou seja, $\mathcal{R}$ é um domínio de integridade. ∎

CAPÍTULO 4

CÓDIGOS SOBRE UM CONJUNTO ADMISSÍVEL DE ESTRUTURAS Q-PESOS

Sabemos que os conceitos de função peso e função q-peso foram inicialmente introduzidos com o objetivo de se construir códigos, em particular, os códigos geométricos de Goppa. Diante disto, apresentaremos, neste capítulo, uma generalização desta construção sobre $\mathbb{F}$-álgebras munidas de um conjunto admissível de estruturas q-pesos, e determinaremos uma cota para a distância mínima dos códigos duais. Veremos, em um exemplo, que tal cota é, em alguns casos, melhor que a cota de Goppa.

4.1 Códigos

Seja $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, ..., m\}$ um conjunto admissível de estruturas q-pesos, onde cada Γ_i é um semigrupo bem ordenado. Para $\alpha = (\alpha_1, ..., \alpha_m) \in \oplus_{i=1}^{m} \Gamma_i$, defina

$$\mathcal{L}(\alpha) = \{f \in \mathcal{R} : \rho_i(f) \preceq_i \alpha_i, i = 1, ..., m\}$$

Pelos axiomas (Q.1), (Q.2) e (Q.3) de função q-ordem segue que $\mathcal{L}(\alpha)$ é um $\mathbb{F}$-subespaço vetorial de $\mathcal{R}$. Note também que $\mathcal{L}(0) = \mathbb{F}$.

Agora, considere a seguinte ordem parcial $\preceq$ em $\oplus_{i=1}^{m}\Gamma_i$: para $\alpha, \beta \in \oplus_{i=1}^{m}\Gamma_i$,

$$\alpha \preceq \beta \text{ se, e somente se, } \alpha_i \preceq_i \beta_i, \text{ para todo } i = 1, ..., m.$$

Então, para todo $\alpha, \beta \in \oplus_{i=1}^{m}\Gamma_i$ tal que $\alpha \preceq \beta$, temos que $\mathcal{L}(\alpha) \subseteq \mathcal{L}(\beta)$.

A partir de agora, assuma que $\mathbb{F}$ seja um corpo finito.

Definição 4.1. Seja $\varphi : \mathcal{R} \to \mathbb{F}^n$ um morfismo sobrejetivo de $\mathbb{F}$-álgebras. Então, para cada $\alpha \in \oplus_{i=1}^{m}\Gamma_i$, definimos os códigos

$$E(\alpha) := \varphi(\mathcal{L}(\alpha)) \text{ e}$$
$$C(\alpha) := (E(\alpha))^{\perp} = \{c \in \mathbb{F}^n : c \cdot \varphi(f) = 0, \forall f \in \mathcal{L}(\alpha)\},$$

onde $\cdot$ é o produto interno usual em $\mathbb{F}^n$.

Note que, para $\alpha \preceq \beta$, temos que $E(\alpha) \subseteq E(\beta)$ e $C(\alpha) \supseteq C(\beta)$.

Agora, considere o seguinte subconjunto de $\oplus_{i=1}^{m}\Gamma_i$.

$$\mathcal{H} = \mathcal{H}(\rho_1, ..., \rho_m) = \{(\rho_1(f), ..., \rho_m(f)) | f \in \mathcal{R}\backslash\{0\}\} \subseteq \oplus_{i=1}^{m}\Gamma_i.$$

Observe que, procedendo como na proposição 5.2, pode-se mostrar que $\mathcal{H}$ é um semigrupo.

Seja $\alpha_1 = \mathbf{0}$ e escolha uma sequência estritamente crescente $\alpha_1, \alpha_2, ..., \alpha_j, ...$ de elementos de $\mathcal{H}$, com respeito a ordem parcial $\preceq$ de $\oplus_{i=1}^{m}\Gamma_i$, tal que $dim_{\mathbb{F}}(\varphi(\mathcal{L}(\alpha_{j+1}))/\varphi(\mathcal{L}(\alpha_j))) = 1$. Observe que cada $\alpha_j \in \oplus_{i=1}^{m}\Gamma_i$ é da forma $\alpha_j = (\alpha_{j1}, ..., \alpha_{jm})$, onde cada $\alpha_{ji} \in \Gamma_i$, $i = 1, ..., m$.

Definição 4.2. Defina o conjunto de pares de funções $N(\alpha_j) := \{(f_{j,k}, g_{j,k}) : k = 1, ..., l_j\}$ tais que

a) $f_{j,k}, g_{j,k} \in \mathcal{L}(\alpha_{j+1})$;

b) $f_{j,k}g_{j,k} \in \mathcal{L}(\alpha_{j+1})\backslash\mathcal{L}(\alpha_j)$ (logo $\rho_i(f_{j,k}) + \rho_i(g_{j,k}) = \alpha_{(j+1)i}$, para algum $i = 1, ..., m$);

c) para tais i, $\rho_i(f_{j,1}) \prec_i ... \prec_i \rho_i(f_{j,l_j})$ (e, portanto, $\rho_i(g_{j,1}) \succ_i ... \succ_i \rho_i(g_{j,l_j})$);

d) para $s \in \{1, ..., l_j - 1\}$, $f_{j,s}g_{j,r} \in \mathcal{L}(\alpha_j)$ para todo $r = s+1, ..., l_j$.

Defina $\mu(\alpha_j) := \#N(\alpha_j)$.

Considere as matrizes M e N, onde as primeiras l_j linhas de M são $\varphi(f_{j,1}), ..., \varphi(f_{j,l_j})$, as primeiras l_j colunas de N são $\varphi(g_{j,1}), ..., \varphi(g_{j,l_j})$ e completamos as linhas e colunas restantes de M e N, respectivamente, de forma que os postos das matrizes M e N sejam iguais a n.

Para $y = (y_1, ..., y_n) \in \mathbb{F}^n$, considere a matriz diagonal $D(y) := (a_{sr})_{n\times n}$, onde $a_{sr} = 0$ se $r \neq s$ e $a_{rr} = y_r$, para $r, s = 1, ..., n$. Seja $S(y) := MD(y)N$, então , para $r, s \in \{1, ..., l_j\}$, temos que $(S(y))_{s,r} = y \cdot (\varphi(f_{j,s}) * \varphi(g_{j,r}))$, onde $\cdot$ é o produto interno usual em $\mathbb{F}^n$. Assim, como $posto(M) = posto(N) = n$, temos que

$$posto(S(y)) = wt(y),$$

onde $wt(y)$ é o peso de y.

Proposição 4.3. *Se $y \in C(\alpha_j) \setminus C(\alpha_{j+1})$ então $wt(y) \geq \mu(\alpha_j)$.*

Dem. Vimos acima que $(S(y))_{s,r} = y \cdot (\varphi(f_{j,s}) * \varphi(g_{j,r})) = y \cdot \varphi(f_{j,s}g_{j,r})$, para todo $r, s \in \{1, ..., l_j\}$. Da definição anterior, temos que $f_{j,s}g_{j,r} \in \mathcal{L}(\alpha_j)$ se $s < r$ e que $f_{j,r}g_{j,r} \in \mathcal{L}(\alpha_{j+1})\setminus\mathcal{L}(\alpha_j)$. Portanto, para $y \in C(\alpha_j) \setminus C(\alpha_{j+1})$, temos, para $s < r$, que $(S(y))_{s,r} = y \cdot \varphi(f_{j,s}g_{j,r}) = 0$, e da hipótese $dim_{\mathbb{F}}(\varphi(\mathcal{L}(\alpha_{j+1}))/\varphi(\mathcal{L}(\alpha_j)) = 1$, segue que $(S(y))_{r,r} = y \cdot \varphi(f_{j,r}g_{j,r}) \neq 0$.

Logo,

$$S(y) = \begin{pmatrix} \underbrace{y \cdot \varphi(f_{j,1}g_{j,1})}_{\neq 0} & \underbrace{y \cdot \varphi(f_{j,1}g_{j,2})}_{0} & \cdots & \underbrace{y \cdot \varphi(f_{j,1}g_{j,l_j})}_{0} & \cdots \\ y \cdot \varphi(f_{j,2}g_{j,1}) & \underbrace{y \cdot \varphi(f_{j,2}g_{j,2})}_{\neq 0} & \cdots & \underbrace{y \cdot \varphi(f_{j,2}g_{j,l_j})}_{0} & \cdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ y \cdot \varphi(f_{j,l_j}g_{j,1}) & \cdots & & \underbrace{y \cdot \varphi(f_{j,l_j}g_{j,l_j})}_{\neq 0} & \cdots \\ \vdots & & \vdots & & \vdots \end{pmatrix},$$

e, portanto,

$$posto(S(y)) \geq l_j = \mu(\alpha_j).$$

■

Como $\varphi(\mathcal{L}(\alpha_j)) \subsetneq \varphi(\mathcal{L}(\alpha_{j+1})) \subset \mathbb{F}^n$, então existe um inteiro positivo N tal que $\varphi(\mathcal{L}(\alpha_N)) = \mathbb{F}^n$. Assim, temos a seguinte cota para a distância mínima do código $C(\alpha)$.

Corolário 4.4. *Para $j = 1, ..., N$, temos*

$$d(C(\alpha_j)) \geq d(\alpha_j) := min\{\mu(\alpha_k) : j \leq k,\ k = 1, ..., N\}.$$

Dem. Isto é uma consequência direta dos resultados anteriores. ■

Para ilustrar os resultados acima, consideremos os seguintes exemplos.

Exemplo 4.5. Esta é uma continuação do exemplo 3.21. Considerando o anel tórico $\mathcal{R} = \mathbb{F}_3[X, Y, Z]/(XY - Z^2)$ sobre o corpo finito $\mathbb{F}_3$, temos o conjunto admissível $\{(\mathcal{R}, \rho_i, \Gamma_i) : i = 1, 2\}$, onde $\Gamma_i = \langle (0, 1), (1, 1) \rangle$ e $\rho_i : \mathcal{R} \to \Gamma_i \cup \{-\infty\}$ é definido por

$$\rho_1(x) = (0, 0),\ \rho_1(y) = (1, 1),\ \rho_1(z) = (0, 1) \text{ e}$$
$$\rho_2(x) = (1, 1),\ \rho_2(y) = (0, 0),\ \rho_2(z) = (0, 1).$$

Temos também que o conjunto dos pontos racionais da variedade tórica correspondente ao ideal $I = (XY - Z^2)$ é

$$\mathcal{V}_{\mathbb{F}_3}(I) = \{P_1 = (0, 0, 0), P_2 = (0, 1, 0), P_3 = (1, 0, 0), P_4 = (1, 1, 1), P_5 = (0, 2, 0), P_6 = (2, 0, 0), P_7 = (1, 1, 2), P_8 = (2, 2, 1), P_9 = (2, 2, 2)\}.$$

Assim, tomando o morfismo $\varphi : \mathcal{R} \to \mathbb{F}_3^9$ definido por $\varphi(f) = (f(P_1), ..., f(P_9))$, podemos construir os códigos $E(\alpha) := \varphi(\mathcal{L}(\alpha))$ e $C(\alpha) := (E(\alpha))^{\perp}$, para $\alpha \in \mathcal{H}$. A tabela 4.1 ilustra as cotas da distância mínima dos códigos $C(\alpha)$.

j	$\alpha_j = (\alpha_{j1}, \alpha_{j2})$	$\mu(\alpha_j)$	$d(\alpha_j)$
1	(0,0,0,0)	2	2
2	(0,1,0,1)	3	2
3	(0,2,0,2)	2	2
4	(1,1,0,2)	2	2
5	(1,1,1,1)	4	3
6	(1,2,1,2)	6	3
7	(1,2,1,3)	3	3
8	(2,2,1,3)	3	3
9	(2,2,2,2)	6	6

Tabela 4.1: Cota $d(\alpha_j)$ do código $C(\alpha_j)$ usando a ordem $\prec_{lex}$.

Agora, se em cada Γ_i, considerarmos a ordem lexicográfica graduada reversa $\prec_{lgr}$, ou seja,

$$(a,b) \prec_{lgr} (c,d) \Leftrightarrow \begin{cases} a+b < c+d, \text{ ou} \\ a+b = c+d \text{ e } b < d, \text{ou} \\ a+b = c+d,\ b = d \text{ e } a < c, \end{cases}$$

temos que $\{(\mathcal{R}, \rho_i, \Gamma_i) : i = 1, 2\}$ é ainda um conjunto admissível de estruturas q-pesos em $\mathcal{R}$. Logo, temos as seguintes cotas para distância mínima dos códigos $C(\alpha)$, como mostra a tabela 4.2.

j	$\alpha_j = (\alpha_{j1}, \alpha_{j2})$	$\mu(\alpha_j)$	$d(\alpha_j)$
1	(0,0,0,0)	2	2
2	(0,1,0,1)	2	2
3	(1,1,0,1)	2	2
4	(1,1,1,1)	3	3
5	(0,2,0,2)	4	3
6	(0,2,1,2)	3	3
7	(2,2,1,2)	3	3
8	(2,2,2,2)	4	4
9	(1,3,2,2)	4	4

Tabela 4.2: Cota $d(\alpha_j)$ do código $C(\alpha_j)$ usando a ordem $\prec_{lgr}$.

Exemplo 4.6. Sejam $\mathcal{A} = \{(-1,3),(1,0),(1,2)\}, \mathcal{B} = \{(-1,1),(-1,3),(1,2)\} \subset \mathbb{Z}^2$. Definindo ω_1 e ω_2 sobre os monômios de $\mathbb{F}_5[X,Y,Z]$ por

$$\omega_1(X) = (1,0),\ \omega_1(Y) = (1,2),\ \omega_1(Z) = (-1,3) \text{ e}$$
$$\omega_2(X) = (-1,1),\ \omega_2(Y) = (-1,3),\ \omega_2(Z) = (1,2),$$

encontramos, procedendo como na seção 3.4, o ideal tórico associado a $\mathcal{A}$ e $\mathcal{B}$ em $\mathbb{F}_5[X,Y,Z]$:

$$I_{\mathcal{A}} = I_{\mathcal{B}} = (X^5Z^2 - Y^3) =: I.$$

Sejam $\mathbb{N}_0\mathcal{A}$ e $\mathbb{N}_0\mathcal{B}$ os semigrupos gerados por $\mathcal{A}$ e $\mathcal{B}$, respectivamente. Considere $\preceq$ a ordem lexicográfica em $\mathbb{Z}^2$. Sejam $\Gamma_1 := \{\gamma \in \mathbb{N}_0\mathcal{A} : (0,0) \preceq \gamma\}$ e $\Gamma_2 := \{\gamma \in \mathbb{N}_0\mathcal{B} : (0,0) \preceq \gamma\}$. Então,

$$\Gamma_1 = \langle (1,0),(1,2),(0,3),(0,5)\rangle \text{ e}$$
$$\Gamma_2 = \langle (1,2),(0,3),(0,5)\rangle.$$

Então, para o anel tórico $\mathcal{R} = \mathbb{F}_5[X,Y,Z]/I$, temos, da proposição 3.19, as funções q-pesos $\rho_i : \mathcal{R} \to \Gamma_i \cup \{-\infty\}$, $i = 1,2$,

$$\rho_i(f) = \begin{cases} -\infty & , \text{ se } f = 0; \\ \mathbf{0} & , \text{ se } f \neq 0 \text{ e } \omega_i(f) \preceq \mathbf{0}; \\ \omega_i(f) & , \text{ se } \omega_i(f) \succ \mathbf{0}. \end{cases}$$

Aqui, temos que $\mathcal{U}_{\rho_1} = \{\sum_{finita} \lambda_{abc} x^a y^b z^c : \lambda_{abc} \in \mathbb{F}_5,\ a+b<c \text{ ou } a=b=c=0\}$ e $\mathcal{U}_{\rho_2} = \{\sum_{finita} \lambda_{abc} x^a y^b z^c : \lambda_{abc} \in \mathbb{F}_5,\ a+b>a \text{ ou } a=b=c=0\}$. Logo, temos que $\mathcal{U}_{\rho_1} \cap \mathcal{U}_{\rho_2} = \mathbb{F}_5$, e, portando, $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, 2\}$ é um conjunto admissível de estruturas q-pesos em $\mathcal{R}$.

Assim, tomando $\mathcal{V}_{\mathbb{F}_5}(I)$ o conjunto ds pontos racionais da variedade tórica correspondente ao ideal $I = (X^5Z^2 - Y^3)$, onde $\#\mathcal{V}_{\mathbb{F}_5}(I) = 25$, e o morfismo $\varphi : \mathcal{R} \to \mathbb{F}_5^{25}$ definido por $\varphi(f) = (f(P_1), ..., f(P_{25}))$, podemos construir os códigos $E(\alpha) := \varphi(\mathcal{L}(\alpha))$ e $C(\alpha) := (E(\alpha))^{\perp}$, para $\alpha \in \mathcal{H}$. A seguir, listamos, verticalmente da esquerda pra direita, os termos $\alpha_i \in \mathcal{H}$, $j = 1, ..., 25$:

$(0,0,0,0)$	$(1,0,0,8)$	$(1,5,1,5)$	$(2,0,1,10)$	$(2,4,2,7)$
$(0,3,0,3)$	$(1,2,0,8)$	$(1,5,1,7)$	$(2,0,2,4)$	$(3,0,2,7)$
$(0,5,0,5)$	$(1,2,1,2)$	$(1,5,1,8)$	$(2,2,2,4)$	$(3,0,3,6)$
$(0,6,0,6)$	$(1,3,1,2)$	$(1,8,1,8)$	$(2,3,2,4)$	$(4,0,3,6)$
$(0,8,0,8)$	$(1,3,1,5)$	$(1,8,1,10)$	$(2,4,2,4)$	$(4,0,4,8)$

com os respectivos $\mu(\alpha_j)$-valores

2	2	4	3	4
2	2	6	4	4
3	4	6	6	5
4	4	8	3	5
2	6	3	6	6

Observe que, de $\alpha_1 = (0,0,0,0)$ à $\alpha_7 = (1,2,0,8)$ temos que $d(C(\alpha_j)) \geq 2$, de $\alpha_8 = (1,2,1,2)$ à $\alpha_{19} = (2,3,2,4)$ temos que $d(C(\alpha_j)) \geq 3$, de $\alpha_{20} = (2,4,2,4)$ à $\alpha_{22} = (3,0,2,7)$ temos que $d(C(\alpha_j)) \geq 4$, para $\alpha_{23} = (3,0,3,6)$ e $\alpha_{24} = (4,0,3,6)$ temos que $d(C(\alpha_j)) \geq 5$ e $d(C(4,0,4,8)) \geq 6$.

O próximo resultado mostra que os códigos geométricos de Goppa m-pontuais podem ser vistos como os códigos construídos nesta seção.

Teorema 4.7 ([Ca-Si],§ 2, Teorema 2.10)**.** *Seja $\mathcal{X}$ uma curva algébrica projetiva não-singular absolutamente irredutível definida sobre o corpo $\mathbb{F}$, e seja $G := a_1Q_1 + ... + a_mQ_m$ e $D := P_1 + ... + P_n$ divisores de $\mathcal{X}$ tais que $supp(D) \cap supp(G) = \emptyset$ e P_i são pontos racionais, para todo $i = 1, ..., n$ (logo temos o código de Goppa $C_{\mathcal{L}}(D, G) = \{(h(P_1), ..., h(P_n)) \in \mathbb{F}^n / \ h \in \mathcal{L}(G)\}$). Então, tomando*

$$\mathcal{R} = \bigcap_{P \in \mathcal{X} \setminus \{Q_1, ..., Q_m\}} \mathcal{O}_P(\mathcal{X}),$$

onde $\mathcal{O}_P$ é o anel local associado a $P \in \mathcal{X}$, e definindo $\varphi(f) := (f(P_1), ..., f(P_n))$, existe um conjunto admissível de m funções q-pesos em $\mathcal{R}$ tais que $C_{\mathcal{L}}(D, G) = \varphi(\mathcal{L}(a)) = E(a)$, e $C_\Omega(D, G) = C(a)$, onde $a := (a_1, ..., a_m)$.

Observação 4.8. Em [Ca-Si], tal resultado é provado mostrando a existência de um conjunto "completo"de m funções q-pesos em $\mathcal{R}$, a qual os autores definem como sendo um conjunto admissível de m funções q-pesos com a hipótese adicional de que cada $\Gamma_i \setminus \rho_i(\cap_{1 \leq k \leq m, k \neq i} \mathcal{U}_{\rho_k})$ seja um conjunto finito (neste caso, $\Gamma_i = \mathbb{N}_0$, para todo $i = 1, ..., m$). Porém, tal hipótese não interfere na validade do resultado acima, uma vez que esta não é utilizada em [Ca-Si], Teorema 2.10. Mas, esta hipótese, é de suma importância para o cálculo de cotas e para resultados ligados a estruturas das álgebras munidas de conjunto completo descritos em tal artigo.

Vejamos agora um exemplo onde a cota $d(\alpha)$ construída acima é, em alguns casos, melhor que a cota de Goppa.

Exemplo 4.9. Esta é uma continuação do exemplo 3.9. Seja $\mathcal{X}$ a curva hermitiana dada por $X^5 - ZY^4 - Z^4Y = 0$ sobre o corpo $\mathbb{F}_{16}$. Sejam $Q_1, Q_2 \in \mathcal{X}$ dois $\mathbb{F}$-pontos racionais distintos de $\mathcal{X}$, $\alpha = (\alpha_1, \alpha_2) \in \mathbb{N}_0^2$ e denote por $C_{\mathcal{L}}(D, G)$ o código de Goppa associado aos divisores $G := \alpha_1 Q_1 + \alpha_2 Q_2$ e $D := P_1 + ... + P_n$, onde $P_1, ..., P_n$, são $\mathbb{F}$-pontos racionais distintos, diferentes de Q_1 e Q_2. Como o gênero de $\mathcal{X}$ é $g = 6$, então a cota de Goppa para

o código $C_{\mathcal{L}}(D,G)^{\perp} = C_{\Omega}(D,G)$ é dada por $d_G(\alpha) = \alpha_1 + \alpha_2 - (2g-2) = \alpha_1 + \alpha_2 - 10$.

As tabelas a seguir, ilustram as cotas da distância mínima dos códigos $C(\alpha)$.

j	$\alpha_j = (\alpha_{j1}, \alpha_{j2})$	$\mu(\alpha_j)$	$d(\alpha_j)$	$d_G(\alpha_j)$
1	(0,0)	2	2	-10
2	(3,3)	2	2	-4
3	(4,3)	2	2	-3
4	(4,4)	2	2	-2
5	(4,5)	2	2	-1
6	(5,5)	3	3	0
7	(6,6)	4	4	2
8	(7,6)	5	5	3
9	(8,6)	6	5	4
10	(9,6)	5	5	5

Tabela 4.3: A cota $d(\alpha_j)$ é maior ou igual $d_G(\alpha_j)$ para o código $C(\alpha_j)$.

j	$\alpha_j = (\alpha_{j1}, \alpha_{j2})$	$\mu(\alpha_j)$	$d(\alpha_j)$	$d_G(\alpha_j)$
1	(0,0)	2	2	-10
2	(3,3)	2	2	-4
3	(4,3)	2	2	-3
4	(4,4)	2	2	-2
5	(4,5)	2	2	-1
6	(5,5)	3	3	0
7	(6,6)	4	4	2
8	(7,6)	4	4	3
9	(7,7)	5	4	4
10	(7,8)	5	4	5

Tabela 4.4: A cota $d(\alpha_j)$ é maior que $d_G(\alpha_j)$, para $j = i, ..., 8$, e $d(\alpha_j)$ é menor ou igual a $d_G(\alpha_j)$, para $j > 8$.

CAPÍTULO 5

SOBRE AS ÁLGEBRAS MUNIDAS DE UM CONJUNTO ADMISSÍVEL

Em [Ca-Si] e [Mu-To], os autores mostram que se uma $\mathbb{F}$-álgebra é munida de um conjunto "peculiar"de estruturas q-pesos com semigrupos de valores iguais a $\mathbb{N}_0$, então esta $\mathbb{F}$-álgebra é o anel de coordenadas afim de uma curva algébrica projetiva irredutível com mais de um ponto no infinito. Neste capítulo, faremos um estudo similar sobre as álgebras munidas de um certo conjunto admissível de estruturas q-pesos. Mais ainda, sob certas condições, mostraremos que tais álgebras são anéis de coordenadas afim de variedades algébricas projetivas irredutíveis com pelo menos dois divisores irredutíveis no infinito.

5.1 A Estrutura dos Semigrupos

Seja $\{(R, \rho_i, \Gamma_i), i = 1, 2\}$ um conjunto admissível de estruturas q-pesos em $\mathcal{R}$. Considere o conjunto $\Gamma_1 \oplus \Gamma_2$. Para $a = (a_1, a_2)$, $b = (b_1, b_2) \in \Gamma_1 \oplus \Gamma_2$, defina a adição em $\Gamma_1 \oplus \Gamma_2$ como segue,

$$a + b := (a_1 +_1 b_1, a_2 +_2 b_2),$$

onde $+_i$ é a adição em Γ_i, $i = 1, 2$. Por abuso de notação e se não houver dúvidas, denotaremos somente por $+$ a adição, e 0 os elementos neutros em Γ_1, Γ_2 e $\Gamma_1 \oplus \Gamma_2$, respectivamente. Então, segue que $(\Gamma_1 \oplus \Gamma_2, +, 0)$ é um semigrupo, pois cada $(\Gamma_i, +_i, 0)$ é um semigrupo.

Agora, tome o seguinte subconjunto de $\Gamma_1 \oplus \Gamma_2$,

$$\mathcal{H} = \mathcal{H}(\rho_1, \rho_2) = \{(\rho_1(f), \rho_2(f)) | f \in \mathcal{R}\backslash\{0\}\} \subseteq \Gamma_1 \oplus \Gamma_2.$$

Mostraremos que $\mathcal{H} = \mathcal{H}(\rho_1, \rho_2)$ é um subsemigrupo de $\Gamma_1 \oplus \Gamma_2$.

Primeiramente, dados $(\alpha_1, \alpha_2), (\beta_1, \beta_2) \in \Gamma_1 \oplus \Gamma_2$, defina

$$Lub((\alpha_1, \alpha_2), (\beta_1, \beta_2)) := (max_{\prec_1}\{\alpha_1, \beta_1\}, max_{\prec_2}\{\alpha_2, \beta_2\}).$$

Lema 5.1. *Sejam $a, b \in \mathcal{H}$. Então $Lub(a, b) \in \mathcal{H}$. Mais ainda, se $f, g \in \mathcal{R}$ são tais que $a = (\rho_1(f), \rho_2(f))$ e $b = (\rho_1(g), \rho_2(g))$ então existem $\lambda, \mu \in \mathbb{F}$ tais que $Lub(a, b) = (\rho_1(\lambda f + \mu g), \rho_2(\lambda f + \mu g))$.*

Dem. Sejam $f, g \in \mathcal{R}$ tais que $a = (\rho_1(f), \rho_2(f))$ e $b = (\rho_1(g), \rho_2(g))$. Se $a = b$ o resultado segue. Assim, suponha que $\rho_1(f) \prec_1 \rho_1(g)$. Se $\rho_2(f) \preceq_2 \rho_2(g)$ então $Lub(a, b) = b \in \mathcal{H}$. Se $\rho_2(f) \succ_2 \rho_2(g)$ então, do axioma (Q.3) da definição de função q-ordem, segue que $\rho_2(f + g) = \rho_2(f)$, mas como, por (Q.3), $\rho_1(f + g) = \rho_1(g)$, segue que $Lub(a, b) = (\rho_1(g), \rho_2(f)) = (\rho_1(f + g), \rho_2(f + g)) \in \mathcal{H}$. Agora, se $\rho_1(f) = \rho_1(g)$, então, como feito antes, se $\rho_2(f) \preceq_2 \rho_2(g)$ então $Lub(a, b) = b \in \mathcal{H}$ e se $\rho_2(f) \succ_2 \rho_2(g)$ então $Lub(a, b) = a \in \mathcal{H}$. Mais ainda, $Lub(a, b) = (\rho_1(\lambda f + \mu g), \rho_2(\lambda f + \mu g))$ onde $\lambda, \mu \in \{0, 1\}$. ∎

Proposição 5.2. *O conjunto $\mathcal{H}$ é um subsemigrupo de $\Gamma_1 \oplus \Gamma_2$.*

Dem. Sejam $f, g \in \mathcal{R}$ tais que $a = (\rho_1(f), \rho_2(f))$, $b = (\rho_1(g), \rho_2(g)) \in \mathcal{H}$. Seja $c = (\rho_1(fg), \rho_2(fg)) \in \mathcal{H}$. Então do axioma (Q.6) de função q-peso, para $i = 1, 2$, segue que $\rho_i(fg) \preceq_i \rho_i(f) + \rho_i(g)$, com igualdade quando $\rho_i(f) \succ_i 0$ e $\rho_i(g) \succ_i 0$. Logo $a + b = Lub(Lub(a, b), c) \in \mathcal{H}$. De fato, pois suponha que $f \in \mathcal{U}_{\rho_1}$. Então,

- se $f \in \mathcal{U}_{\rho_2}$ então $f \in \mathbb{F}$ e logo $a + b = b = Lub(Lub(a, b), c)$.
- Agora, se $f \in \mathcal{M}_{\rho_2}$, temos mais duas hipóteses:
  - se $g \in \mathcal{U}_{\rho_1}$, então $a + b = a = Lub(Lub(a, b), c)$ se $g \in \mathcal{U}_{\rho_2}$, ou, $a + b = c = Lub(Lub(a, b), c)$ se $g \in \mathcal{M}_{\rho_2}$.
  - se $g \in \mathcal{M}_{\rho_1}$, então $a + b = (\rho_1(g), \rho_2(f)) = Lub(a, b) = Lub(Lub(a, b), c)$ se $g \in \mathcal{U}_{\rho_2}$, ou, $a + b = (\rho_1(g), \rho_2(fg)) = Lub(b, c) = Lub(Lub(a, b), c)$ se $g \in \mathcal{M}_{\rho_2}$.

Agora, vamos supor que $f \in \mathcal{M}_{\rho_1}$. Então,

- se $f \in \mathcal{U}_{\rho_2}$, o resultado segue análogo ao anterior.
- Se $f \in \mathcal{M}_{\rho_2}$, então, novamente, temos mais duas hipóteses:
  - se $g \in \mathcal{U}_{\rho_1}$, temos que $a + b = a = Lub(Lub(a, b), c)$ se $g \in \mathcal{U}_{\rho_2}$, ou que, $a + b = (\rho_1(f), \rho_2(fg)) = Lub(a, c) = Lub(Lub(a, b), c)$ se $g \in \mathcal{M}_{\rho_2}$.
  - se $g \in \mathcal{M}_{\rho_1}$, temos que $a+b = (\rho_1(fg), \rho_2(f)) = Lub(a, c) = Lub(Lub(a, b), c)$ se $g \in \mathcal{U}_{\rho_2}$, ou, $a + b = c = Lub(Lub(a, b), c)$ se $g \in \mathcal{M}_{\rho_2}$.

Portanto, $a + b = Lub(Lub(a, b), c)$. ∎

A partir de agora, e até o final desta seção, admitiremos que cada Γ_i é um semigrupo bem ordenado.

Para $\alpha_i \in \Gamma_i$, $i = 1, 2$, sejam

$$x_1(\alpha_2) := min_{\prec_1}\{\alpha \in \Gamma_1 : (\alpha, \alpha_2) \in \mathcal{H}\} \subset \Gamma_1 \text{ e}$$
$$x_2(\alpha_1) := min_{\prec_2}\{\alpha \in \Gamma_2 : (\alpha_1, \alpha) \in \mathcal{H}\} \subset \Gamma_2.$$

Lema 5.3. *Se $\alpha \in \Gamma_i$ e $x_j(\alpha) \succ_j 0$ então $x_i(x_j(\alpha)) = \alpha \succ_i 0$, para $i, j = 1, 2, i \neq j$.*

Dem. Para $i = 1$ e $j = 2$, seja $f \in \mathcal{R}$ tal que $\rho_1(f) = \alpha$ e $\rho_2(f) = x_2(\alpha) \succ_2 0$. Pela definição anterior, temos que $x_1(x_2(\alpha)) \preceq_1 \alpha$. Se, para algum $g \in \mathcal{R}$, temos que $\rho_1(g) \prec_1 \alpha$ e $\rho_2(g) = x_2(\alpha)$, então do axioma (Q.5) da definição de função q-peso, existe $\lambda \in \mathbb{F}^*$ tal que $\rho_2(f - \lambda g) \prec_2 x_2(\alpha)$, mas pelo axioma (Q.3) da definição de função q-peso $\rho_1(f - \lambda g) = \rho_1(f) = \alpha$, e então $(\rho_1(f - \lambda g), \rho_2(f - \lambda g)) \in \mathcal{H}$, contradizendo a minimalidade de $x_2(\alpha)$. De forma análoga, temos o caso $i = 2$ e $j = 1$. ∎

Considere agora os seguintes subconjuntos de $\mathcal{H}$,

$$\mathcal{H}_{\rho_1} := \rho_1(\mathcal{U}_{\rho_2}) = \{\alpha \in \Gamma_1 | (\alpha, 0) \in \mathcal{H}\} \subset \Gamma_1, \text{ e}$$
$$\mathcal{H}_{\rho_2} := \rho_2(\mathcal{U}_{\rho_1}) = \{\alpha \in \Gamma_2 | (0, \alpha) \in \mathcal{H}\} \subset \Gamma_2.$$

Observe que ambos $\mathcal{H}_{\rho_1}$ e $\mathcal{H}_{\rho_2}$ são subsemigrupos de Γ_1 e Γ_2, respectivamente.

Proposição 5.4. *Temos que $\alpha \in Lacunas(\mathcal{H}_{\rho_i}) = \{\gamma \in \Gamma_i \backslash \mathcal{H}_{\rho_i}\}$ se, e somente se, $x_j(\alpha) \in Lacunas(\mathcal{H}_{\rho_j})$, para $i, j = 1, 2$, $i \neq j$.*

Dem. Seja $\alpha \in \Gamma_1 \backslash \mathcal{H}_{\rho_1}$, então $\alpha \neq 0$ e $(\alpha, 0) \notin \mathcal{H}_{\rho_1}$, logo $x_2(\alpha) \succ_2 0$. Se $x_2(\alpha) \in \mathcal{H}_{\rho_2}$ então $(0, x_2(\alpha)) \in \mathcal{H}$ e logo, do lema anterior, $0 = x_1(x_2(\alpha)) = \alpha \succ_1 0$, contradição. Então $x_2(\alpha) \in \Gamma_2 \backslash \mathcal{H}_{\rho_2}$. Da mesma forma, se $\alpha \in \Gamma_1$ e $x_2(\alpha) \in \Gamma_2 \backslash \mathcal{H}_{\rho_2}$ então $x_2(\alpha) \succ_2 0$. Do lema anterior, temos que $\alpha = x_1(x_2(\alpha)) \succ_1 0$. Assim, se $\alpha \in \mathcal{H}_{\rho_1}$ então $(\alpha, 0) \in \mathcal{H}$ e logo $x_2(\alpha) = 0$, contradição. Portanto $\alpha \in \Gamma_1 \backslash \mathcal{H}_{\rho_1}$. De forma análoga, $\alpha \in \Gamma_2 \backslash \mathcal{H}_{\rho_2}$ se, e somente se, $x_1(\alpha) \in \Gamma_1 \backslash \mathcal{H}_{\rho_1}$. ∎

Assim, seja Ω o subconjunto de $\mathcal{H}$ dado por

$$\Omega := \{(\alpha_1, x_2(\alpha_1)) : \alpha_1 \in \Gamma_1 \backslash \mathcal{H}_{\rho_1}\} \cup \{(\alpha_1, 0) : \alpha_1 \in \mathcal{H}_{\rho_1}\} \cup \{(0, \alpha_2) : \alpha_2 \in \mathcal{H}_{\rho_2}\}.$$

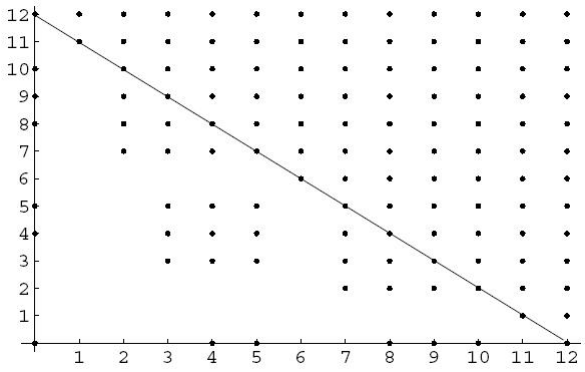
Observe que,

$$\{(\alpha_1, x_2(\alpha_1)) : \alpha_1 \in \Gamma_1 \backslash \mathcal{H}_{\rho_1}\} = \{(x_1(\alpha_2), \alpha_2) : \alpha_2 \in \Gamma_2 \backslash \mathcal{H}_{\rho_2}\}.$$

Proposição 5.5. *Temos que* $\mathcal{H} = \{Lub(a, b) : a, b \in \Omega\}$.

Dem. Pelo lema 5.1, temos que $Lub(a, b) \in \mathcal{H}$, para todo $a, b \in \Omega$. Assim, seja $a = (\rho_1(f), \rho_2(f)) \in \mathcal{H}$. Então, pelo lema 5.3, $a = Lub((\rho_1(f), x_2(\rho_1(f))), (x_1(\rho_2(f)), \rho_2(f)))$, e $(\rho_1(f), x_2(\rho_1(f)))$, $(x_1(\rho_2(f)), \rho_2(f)) \in \Omega$, concluindo o resultado. ■

Exemplo 5.6 ([Mat], ex. 6.2)**.** (Veja exemplo 3.9) Seja $\mathcal{X}$ a curva hermitiana dada por $X^5 - ZY^4 - Z^4Y = 0$ sobre o corpo $\mathbb{F}_{16}$, e seja $\mathcal{R} = \mathcal{R}(Q_1, Q_2)$, onde $Q_1, Q_2 \in \mathcal{X}$ são $\mathbb{F}$-pontos racionais distintos de $\mathcal{X}$. Então, temos que $H_{\rho_i} = \langle 4, 5\rangle \subset \mathbb{N}_0$ e $H(\rho_1, \rho_2)$ é representado pelo gráfico abaixo.



Para todo $a \in \mathcal{H}$, escolha $f_a \in \mathcal{R}\backslash\{0\}$ tal que $a = (\rho_1(f_a), \rho_2(f_a))$, sendo que para $(0, 0)$, temos $f_{(0,0)} = 1$.

Proposição 5.7. *O conjunto* $\mathcal{B} = \{f_a \in \mathcal{R}\backslash\{0\} : a \in \Omega\}$ *é uma base de* $\mathcal{R}$ *como* $\mathbb{F}$*-espaço vetorial.*

Dem. Mostremos que $\mathcal{B}$ é linearmente independente. Sejam $\lambda_a \in \mathbb{F}$ tais que $\sum_{finita} \lambda_a f_a = 0$. Como $a \in \Omega$ então

$$0 = \sum_{finita} \lambda_a f_a = \sum_{finita} \lambda_{(\alpha_1,0)} f_{(\alpha_1,0)} + \sum_{finita} \lambda_{(0,\alpha_2)} f_{(0,\alpha_2)} + \sum_{finita} \lambda_{(\alpha,x_2(\alpha))} f_\alpha.$$

Logo

$$\rho_1(\sum_{finita} \lambda_{(\alpha_1,0)} f_{(\alpha_1,0)} + \sum_{finita} \lambda_{(\alpha,x_2(\alpha))} f_\alpha) = \rho_1(\sum_{finita} \lambda_{(0,\alpha_2)} f_{(0,\alpha_2)}) = 0.$$

Então, dos axiomas (Q.2) e (Q.3) de função q-peso, temos que $\lambda_{(\alpha_1,0)} = \lambda_{(\alpha,x_2(\alpha))} = 0$ para $\alpha_1, \alpha \succ_1 0$. Como $f_{(0,0)} = 1$, temos,

$$\lambda_{(0,0)} + \sum_{finita} \lambda_{(0,\alpha_2)} f_{(0,\alpha_2)} = 0.$$

Assim, se algum $\lambda_{(0,\alpha_2)} \neq 0$, então $0 \prec_2 \rho_2(\sum_{finita} \lambda_{(0,\alpha_2)} f_{(0,\alpha_2)}) = \rho_2(\lambda_{(0,0)}) \preceq_2 0$, contradição; logo segue que $\lambda_{(0,\alpha_2)} = 0$, e portanto $\lambda_{(0,0)} = 0$.

Mostremos agora que $\mathcal{B}$ gera $\mathcal{R}$. Seja $f \in \mathcal{R}\backslash\{0\}$. Suponha que $\rho_2(f) = 0$ e faremos indução sobre $\rho_1(f) = \alpha_1$. Se $\rho_1(f) = 0$ então $f \in \cap_{i=1,2}\mathcal{U}_{\rho_i} = \mathbb{F}$ e o resultado segue. Assim, suponha que para todo elemento $g \in \mathcal{R}$ tal que $\rho_1(g) \prec_1 \alpha_1$ e $\rho_2(g) = 0$ temos que g é gerado por $\mathcal{B}$. Então, como $(\alpha_1, 0) \in \Omega$, tome $f_{(\alpha_1,0)} \in \mathcal{B}$. Temos que $\rho_1(f) = \alpha_1 = \rho_1(f_{(\alpha_1,0)})$ e pelo axioma (Q.5) de função q-peso, existe $\lambda_1 \in \mathbb{F}$ tal que $\rho_1(f - \lambda_1 f_{(\alpha_1,0)}) \prec_1 \alpha_1$ e $\rho_2(f - \lambda_1 f_{(\alpha_1,0)}) = 0$. Logo, pela hipótese de indução, segue $f - \lambda_1 f_{(\alpha_1,0)}$ é gerado por $\mathcal{B}$, e portanto f é gerado por $\mathcal{B}$.

Agora, faremos indução sobre $\rho_2(f) = \alpha_2$. Se $\rho_2(f) = 0$, temos o caso anterior. Então, suponha que para todo elemento $g \in \mathcal{R}$ tal que $\rho_2(g) \prec_2 \alpha_2$ e $\rho_1(g) \preceq_1 \rho_1(f)$, temos que g é gerado por $\mathcal{B}$. Tome $f_{(x_1(\alpha_2),\alpha_2)} \in \mathcal{B}$. Então, como $\rho_2(f) = \alpha_2 = \rho_2(f_{(x_1(\alpha_2),\alpha_2)})$, pelo axioma (Q.5), existe $\lambda_2 \in \mathbb{F}$ tal que $\rho_2(f - \lambda_2 f_{(x_1(\alpha_2),\alpha_2)}) \prec_2 \alpha_2$ e $\rho_1(f - \lambda_2 f_{(x_1(\alpha_2),\alpha_2)}) \preceq_1 \rho_1(f)$. Então, pela hipótese de indução, segue que $f - \lambda_2 f_{(x_1(\alpha_2),\alpha_2)}$ é gerado por $\mathcal{B}$, e logo, f é gerado por $\mathcal{B}$.

Portanto, $\mathcal{B}$ é uma $\mathbb{F}$-base de $\mathcal{R}$. ∎

5.2 A Estrutura das Álgebras

Agora estamos interessados em estudar uma classe especial de estruturas q-pesos.

Seja $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, 2\}$ um conjunto admissível de estruturas q-pesos. Suponha que cada Γ_i seja um semigrupo finitamente gerado

$$\Gamma_i = \langle \alpha_{i1}, ..., \alpha_{it_i}, \alpha_{it_i+1}, ..., \alpha_{im_i} \rangle, \tag{5.1}$$

e tal que $\alpha_{i1}, ..., \alpha_{it_i} \in \mathcal{H}_{\rho_i}$, $t_i \in \{1, ..., m_i\}$.

Então, para cada $\gamma \in \Gamma_i$, existem $\lambda_j \in \mathbb{N}_0$ tais que $\gamma = \sum_{j=1}^{m_i} \lambda_j \alpha_{ij}$. Note que cada semigrupo Γ_i é bem ordenado, via observação 1.7.

Assim, considere o seguinte subconjunto de $\mathcal{H}$,

$$\Lambda := \{(\alpha_{1t}, x_2(\alpha_{1t})) : 1 \leq t \leq m_1\} \cup \{(x_1(\alpha_{2k}), \alpha_{2k}) : 1 \leq k \leq m_2\}.$$

Para $i = 1, 2$ e $j = 1, ..., m_i$, escolha $f_{\alpha_{ij}} \in \mathcal{R}$ tal que $\rho_i(f_{\alpha_{ij}}) = \alpha_{ij}$ e $\rho_l(f_{\alpha_{ij}}) = x_l(\alpha_{ij})$, $l \in \{1, 2\}$ e $l \neq i$.

Então, para $\gamma \in \Gamma_i$, temos que

$$\gamma = \sum_{j=1}^{m_i} \lambda_j \alpha_{ij} = \sum_{j=1}^{m_i} \lambda_j \rho_i(f_{\alpha_{ij}}) = \sum_{j=1}^{m_i} \rho_i(f_{\alpha_{ij}}^{\lambda_j}) = \rho_i \left(\prod_{j=1}^{m_i} f_{\alpha_{ij}}^{\lambda_j} \right). \tag{5.2}$$

Suponha que os elementos $f_{\alpha'_{ij}s}$ possam ser escolhidos de forma que

$$\rho_l \left(\prod_{j=1}^{m_i} f_{\alpha_{ij}}^{\lambda_j} \right) = x_l(\gamma). \tag{5.3}$$

Por simplicidade, diremos que um conjunto admissível $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, 2\}$ de estruturas q-pesos é de *tipo finito*, se as condições (1.1), (1.2) e (1.3) são satisfeitas.

Proposição 5.8. *Seja $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, 2\}$ um conjunto admissível de tipo finito de estruturas q-pesos em $\mathcal{R}$. Então $\mathcal{R}$ é uma $\mathbb{F}$-álgebra finitamente gerada.*

Dem. Mostremos que $\mathcal{R} = \mathbb{F}[\{f_a : a \in \Lambda\}]$. Seja $f \in \mathcal{R} \backslash \{0\}$. Suponha que $\rho_2(f) = 0$. Faremos primeiro uma indução sobre $\rho_1(f) = \gamma$. Então, se $\gamma = 0$, temos que $f \in \mathcal{U}_{\rho_1} \cap \mathcal{U}_{\rho_2} = \mathbb{F}$, e portanto $f \in \mathbb{F}[\{f_a : a \in \Lambda\}] =: A$. Se $\gamma \succ_1 0$, então suponha, para todo $g \in \mathcal{R}$ tal que $\rho_1(g) \prec_1 \gamma$ e $\rho_2(g) = 0$, que $g \in A$. Como $\rho_1(f) = \gamma$, temos

$$\rho_1(f) = \gamma = \textstyle\sum_{j=1}^{m_1} \lambda_j \alpha_{1j} = \rho_1 \left(\prod_{j=1}^{m_1} f_{\alpha_{1j}}^{\lambda_j} \right).$$

Logo, do axioma (Q.5) de função q-peso, existe $\lambda \in \mathbb{F}^*$ tal que $\rho_1 \left(f - \lambda \prod_{j=1}^{m_1} f_{\alpha_{1j}}^{\lambda_j} \right) \prec_1 \gamma$. Mas, como $\rho_2 \left(\prod_{j=1}^{m_1} f_{\alpha_{1j}}^{\lambda_j} \right) = x_2(\gamma) = 0$, pois $\gamma \in \mathcal{H}_{\rho_1}$, segue que $\rho_2 \left(f - \lambda \prod_{j=1}^{m_1} f_{\alpha_{1j}}^{\lambda_j} \right) \preceq_2 0$, e portanto, por hipótese de indução, $f - \lambda \prod_{j=1}^{m_1} f_{\alpha_{1j}}^{\lambda_j} \in A$, ou seja $f \in A$.

Agora, se $\rho_2(f) = \beta \neq 0$, existem $\mu_{j1} \in \mathbb{N}_0$ tais que

$$\rho_2(f) = \beta = \sum_{j=1}^{m_2} \mu_{j1}\alpha_{2j} = \rho_2\left(\prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{j1}}\right).$$

Pelo axioma (Q.5) de função q-peso, existe $\lambda_1 \in \mathbb{F}^*$ tal que $\rho_2\left(f - \lambda_1 \prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{j1}}\right) \prec_2 \beta$. Novamente, existem $\mu_{j2} \in \mathbb{N}_0$ tais que

$$\rho_2\left(f - \lambda_1 \prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{j1}}\right) = \sum_{j=1}^{m_2} \mu_{j2}\alpha_{2j} = \rho_2\left(\prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{j2}}\right),$$

e pelo axioma (Q.5), existe $\lambda_2 \in \mathbb{F}^*$ tal que

$$\rho_2\left(f - \lambda_1 \prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{j1}} - \lambda_2 \prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{j2}}\right) \prec_2 \rho_2\left(\prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{j2}}\right).$$

Continuando o processo, como Γ_2 é bem ordenado, existem $\lambda_{i's} \in \mathbb{F}$ e $\mu_{ji's} \in \mathbb{N}_0$ tais que

$$\rho_2\left(f - \sum_i \lambda_i \prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{ji}}\right) = 0.$$

Logo, do parágrafo acima, segue que $f - \sum_i \lambda_i(\prod_{j=1}^{m_2} f_{\alpha_{2j}}^{\mu_{ji}}) \in A$, e portanto, $f \in A$.

Portanto, $\mathcal{R} = \mathbb{F}[\{f_a : a \in \Lambda\}]$, ou seja, $\mathcal{R}$ é uma álgebra finitamente gerada sobre $\mathbb{F}$. ∎

Da proposição 3.30, segue que $\mathcal{R}$ é um domínio finitamente gerado sobre $\mathbb{F}$, e portanto $\mathcal{R}$ é isomorfo a uma $\mathbb{F}$-álgebra afim, a saber,

$$\mathcal{R} \cong \mathbb{F}[X_1, ..., X_n]/I,$$

onde I é um ideal primo de $\mathbb{F}[X_1, ..., X_n]$.

Assim, seja $K = K(\mathcal{R})$ o corpo de frações de $\mathcal{R}$. Veremos agora que uma função q-peso está associada a uma valorização sobre K.

Lema 5.9. *Sejam $i \in \{1, 2\}$ e $f \in \mathcal{M}_{\rho_i}$. Se $g \in \mathcal{U}_{\rho_i} \backslash \mathbb{F}$, então existe $\lambda \in \mathbb{F}$ tal que $\rho_i(f(g - \lambda)) \prec_i \rho_i(f)$.*

Dem. Do axioma (Q.6) de função q-peso, temos que $\rho_i(fg) \preceq_i \rho_i(f)$. Assim, se $\rho_i(fg) = \rho_i(f)$, pelo axioma (Q.5), existe $\lambda \in \mathbb{F}^*$ tal que $\rho_i(f(g - \lambda)) = \rho_i(fg - \lambda f) \prec_i \rho_i(f)$. Se $\rho_i(fg) \prec_i \rho_i(f)$, basta tomar $\lambda = 0$. ∎

Lema 5.10. *Sejam $f \in \mathcal{R}\backslash\{0\}$ e $i \in \{1,2\}$. Então existe $g \in \mathcal{M}_{\rho_i}$ tal que $fg \in \mathcal{M}_{\rho_i}$.*

Dem. Seja $f \in \mathcal{R}\backslash\{0\}$. Se $f \in \mathbb{F}$ então para qualquer $g \in \mathcal{M}_{\rho_i}$ temos que $fg \in \mathcal{M}_{\rho_i}$. Assim, suponha que $f \in \mathcal{R}\backslash\mathbb{F}$. Se $\rho_i(f) \succ_i 0$, então para qualquer $g \in \mathcal{M}_{\rho_i}$ temos que $\rho_i(fg) = \rho_i(f) + \rho_i(g) \succ_i 0$, e portanto, $fg \in \mathcal{M}_{\rho_i}$. Agora, suponha que $f \in \mathcal{U}_{\rho_i}\backslash\mathbb{F}$. Então $\rho_j(f) \succ_j 0$, com $j = 1,2$ e $j \neq i$. Mostremos que existe $g \in \mathcal{U}_{\rho_j}\backslash\mathbb{F}$ tal que $\rho_j(fg) = 0$. Seja $h \in \mathcal{U}_{\rho_j}\backslash\mathbb{F}$. Então, $\rho_j(fh) \preceq_j \rho_j(f)$ e pelo lema 5.9, existe $\lambda_1 \in \mathbb{F}$ tal que $\rho_j(f(h-\lambda_1)) \prec_j \rho_j(f)$. Se $\rho_j(f(h-\lambda_1)) = 0$, tome $g = h - \lambda_1$, caso contrário, se $\rho_j(f(h-\lambda_1)) \succ_j 0$ então $\rho_j(f(h-\lambda_1)h) \preceq_j \rho_j(f(h-\lambda_1))$. Logo, pelo lema 5.9, existe $\lambda_2 \in \mathbb{F}$ tal que $\rho_j(f(h-\lambda_1)(h-\lambda_2)) \prec_j \rho_j(f(h-\lambda_1))$. Continuando o processo, e do fato de Γ_j ser bem ordenado, podemos encontrar $g = f \cdot \prod_{finito}(h-\lambda_k) \in \mathcal{U}_{\rho_j}\backslash\mathbb{F}$ tal que $\rho_j(fg) = 0$. Logo, $\rho_i(fg) \succ_i 0$ ou $\rho_i(fg) = 0$. Se $\rho_i(fg) \succ_i 0$, segue o resultado. Se $\rho_i(fg) = 0$, então $fg \in \mathcal{U}_{\rho_1} \cap \mathcal{U}_{\rho_2} = \mathbb{F}$ e como $g \in \mathcal{M}_{\rho_i}$, pois $g \in \mathcal{U}_{\rho_j}\backslash\mathbb{F}$, segue que $\rho_i(fg^2) \succ_i 0$. ∎

Logo, do lema acima, se $f, g \in \mathcal{R}\backslash\{0\}$, existem $h, z \in \mathcal{M}_{\rho_i}$ tais que $fh, gz \in \mathcal{M}_{\rho_i}$, com $i = 1,2$, e portanto $f(hz), g(hz) \in \mathcal{M}_{\rho_i}$.

Assim, podemos definir uma aplicação $\nu_i : K \to G(\Gamma_i) \cup \{+\infty\}$ por $\nu_i(0) := +\infty$ e

$$\nu_i(f/g) := \rho_i(hg) - \rho_i(hf),$$

onde $f, g \in \mathcal{R}\backslash\{0\}$ e $h \in \mathcal{M}_{\rho_i}$ é tal que $fh, gh \in \mathcal{M}_{\rho_i}$, $i = 1,2$.

Lema 5.11. *Para $i = 1,2$, segue que a aplicação ν_i está bem definida e é uma valorização no corpo de frações K que é trivial sobre $\mathbb{F}$.*

Dem. Mostremos primeiro que ν_i está bem definida. Seja $f/g \in K$, com $f, g \in \mathcal{R}\backslash\{0\}$ e $h \in \mathcal{M}_{\rho_i}$ tal que $fh, gh \in \mathcal{M}_{\rho_i}$. Se $z \in \mathcal{M}_{\rho_i}$ é tal que $fz, gz \in \mathcal{M}_{\rho_i}$ então

$$\begin{aligned}\rho_i(gh) - \rho_i(fh) - (\rho_i(zg) - \rho_i(zf)) &= \rho_i(gh) + \rho_i(zf) - (\rho_i(fh) + \rho_i(zg)) \\ &= \rho_i(ghzf) - \rho_i(fhzg) = 0,\end{aligned}$$

ou seja, $\nu_i(f/g)$ independe da escolha de $h \in \mathcal{M}_{\rho_i}$ tal que $fh, gh \in \mathcal{M}_{\rho_i}$. Agora, se $f/g = f'/g'$, com $f, f', g, g' \in \mathcal{R}\backslash\{0\}$, então $\nu_i(f/g) = \nu_i(f'/g')$, pois, seja $h \in \mathcal{M}_{\rho_i}$ tal

que $fh, f'h, gh, g'h \in \mathcal{M}_{\rho_i}$, então, como $fg' = f'g$ temos que $fhg'h = f'hgh$. Como ρ_i é bem definido, $\rho_i(fhg'h) = \rho_i(f'hgh)$, então $\rho_i(fh) + \rho_i(g'h) = \rho_i(f'h) + \rho_i(gh)$, ou seja, $\rho_i(g'h) - \rho_i(f'h) = \rho_i(gh) - \rho_i(fh)$, ou seja, $\nu_i(f'/g') = \nu_i(f/g)$. Portanto ν_i está bem definido.

Dos axiomas de função q-peso, segue $\nu_i(f) = 0$ para todo $f \in \mathbb{F}^*$, ou seja, ν_i é trivial sobre $\mathbb{F}$, e que $\nu_i(\lambda f) = \nu_i(f)$, para todo $\lambda \in \mathbb{F}^*$.

Sejam $f/g, f'/g' \in K\backslash\{0\}$, com $f, g, f', g' \in \mathcal{R}\backslash\{0\}$. Então, para $h, t \in \mathcal{M}_{\rho_i}$ tal que $fh, gh, f't, g't \in \mathcal{M}_{\rho_i}$, temos

$$\begin{aligned}
\nu_i(f/g) + \nu_i(f'/g') &= \rho_i(gh) - \rho_i(fh) + \rho_i(g't) - \rho_i(f't) \\
&= \rho_i(ghg't) - \rho_i(fhf't) \\
&= \rho_i(gg'ht) - \rho_i(ff'ht) \quad (\text{com } ht \in \mathcal{M}_{\rho_i} \text{ e } gg'ht, ff'ht \in \mathcal{M}_{\rho_i}) \\
&= \nu_i(ff'/gg') = \nu_i(f/g \cdot f'/g')
\end{aligned}$$

Agora, sejam $f/g, f'/g' \in K$, com $f, f' \in \mathcal{R}$ e $g, g' \in \mathcal{R}\backslash\{0\}$. Sejam $h, t \in \mathcal{M}_{\rho_i}$ tal que $fh, gh, f't, g't \in \mathcal{M}_{\rho_i}$. Então

$$\begin{aligned}
\nu_i(f/g + f'/g') = \nu_i\left(\tfrac{fg'+f'g}{gg'}\right) &= \rho_i(gg'ht) - \rho_i((fg' + f'g)ht) \\
&= \rho_i(ghg't) - \rho_i(fhg't + f'tgh) \ \ (\text{axioma (Q.3)}) \\
&\succeq_i min_{\succeq_i}\{\rho_i(ghg't) - \rho_i(fhg't), \rho_i(ghg't) - \rho_i(f'tgh)\} \\
&= min_{\succeq_i}\{\rho_i(gh) - \rho_i(fh), \rho_i(g't) - \rho_i(f't)\} \\
&= min_{\succeq_i}\{\nu_i(f/g), \nu_i(f'/g')\}.
\end{aligned}$$

Portanto, para $i = 1, 2$, segue que ν_i é uma valorização em K. ∎

Observação 5.12. Observe que cada função q-peso $\rho_i : \mathcal{R} \to \Gamma_i \cup \{-\infty\}$ pode ser vista da seguinte forma:

$$\rho_i(f) = \begin{cases} -\infty & , se\ f = 0; \\ 0 & , se\ \nu_i(f) \succeq_i 0; \\ -\nu_i(f) & , se\ \nu_i(f) \prec_i 0. \end{cases}$$

De fato, para $f \in \mathcal{R}\backslash\{0\}$, do lema 5.10, existe $g \in \mathcal{M}_{\rho_i}$ tal que $fg \in \mathcal{M}_{\rho_i}$. Logo, do axioma (Q.6) de função q-peso, temos que $\rho_i(fg) \preceq_i \rho_i(f) + \rho_i(g)$, com igualdade se

$f \in \mathcal{M}_{\rho_i}$. Então, se $f \in \mathcal{U}_{\rho_i}$, temos que $\nu_i(f/1) = \rho_i(g) - \rho_i(fg) \succeq -\rho_i(f) = 0$, ou seja, $\nu_i(f) \succeq_i 0$. Agora, se $f \in \mathcal{M}_{\rho_i}$, então $\nu_i(f/1) = \rho_i(g) - \rho_i(fg) = -\rho_i(f) \prec_i 0$, pois $\rho_i(f) \succ_i 0$.

Lema 5.13. *Dado ν_i como antes, seja R_{ν_i} o anel de valorização de ν_i e M_{ν_i} o seu respectivo ideal maximal, $i = 1, 2$. Então temos que o corpo de resíduos de cada ν_i é isomorfo ao corpo $\mathbb{F}$.*

Dem. De fato, pois seja $x = f/g \in R_{\nu_i}$, onde $f, g \in \mathcal{R}$, seja $h \in \mathcal{M}_{\rho_i}$ tal que $hf, hg \in \mathcal{M}_{\rho_i}$. Suponha que $\nu_i(x) = 0$. Então $\rho_i(hf) = \rho_i(gh)$, e pelo axioma (Q.5) de função q-peso, existe $\lambda \in \mathbb{F}^*$ tal que $\rho_i(fh - \lambda gh) \prec_i \rho_i(gh)$. Seja agora $z \in \mathcal{M}_{\rho_i}$ tal que $z(fh - \lambda gh), zh \in \mathcal{M}_{\rho_i}$. Então $\nu_i(f/g - \lambda) = \rho_i(gz) - \rho_i((f - \lambda g)z) = \rho_i(zhg) - \rho_i(zh(f - \lambda g))$. Mas como $0 \prec_i \rho_i(gh) - \rho_i(fh - \lambda gh)$, segue do axioma (Q.4), $0 \prec_i \rho_i(zhg) - \rho_i(zh(f - \lambda g))$, ou seja, $\nu_i(f/g - \lambda) \succ_i 0$. Logo $x - \lambda \in M_{\nu_i}$ e portanto $\overline{x} = \lambda$. ∎

A seguir, veremos uma relação entre a dimensão das álgebras munidas de uma função q-peso e o posto racional do semigrupo de valores de tais funções.

Proposição 5.14. *Seja $(\mathcal{R}, \rho, \Gamma)$ uma estrutura q-peso sobre $\mathbb{F}$. Então a dimensão de Krull de $\mathcal{R}$ é no mínimo o posto racional de Γ.*

Dem. Suponha que $r.posto(\Gamma) = r$ (ver definição 1.8). Então podemos encontrar r elementos $\gamma_1, ..., \gamma_r \in \Gamma$ que são racionalmente independentes (ver definição A.2). Assim, escolha $f_{\gamma_i} \in \mathcal{R}$ tal que $\rho(f_{\gamma_i}) = \gamma_i$, $i = 1, ..., r,$. Então, segue que $f_{\gamma_1}, ..., f_{\gamma_r}$ são algebricamente independentes sobre $\mathbb{F}$. De fato, pois caso contrário, existe $g \in \mathbb{F}[X_1, ..., X_r]$, $g \neq 0$, tal que $g(f_{\gamma_1}, ..., f_{\gamma_r}) = 0$. Mas, como consequência do lema 3.7, existe um par de termos distintos de $g(X_1, ..., X_r)$, a saber, $\lambda X_1^{\alpha_1} \cdots X_r^{\alpha_r}$ e $\mu X_1^{\beta_1} \cdots X_r^{\beta_r}$, com $\alpha_i, \beta_i \in \mathbb{N}_0$ e $\lambda, \mu \in \mathbb{F}$, tal que

$$\rho(\lambda f_{\gamma_1}^{\alpha_1} \cdots f_{\gamma_r}^{\alpha_r}) = \rho(\mu f_{\gamma_1}^{\beta_1} \cdots f_{\gamma_r}^{\beta_r}).$$

Dos axiomas de função q-peso, temos que $\sum_{i=1}^{r}(\alpha_i - \beta_i)\rho(f_{\gamma_i}) = 0$, ou seja, $\sum_{i=1}^{r}(\alpha_i - \beta_i)\gamma_i = 0$. Como $(\alpha_i - \beta_i)$ são não todos nulos para $i = 1, ..., r$, segue que $\gamma_1, ..., \gamma_r$ são racionalmente dependentes, contradição.

Assim, temos que $S := \mathbb{F}[f_{\gamma_1}, ..., f_{\gamma_r}]$ é um subanel de $\mathcal{R}$ e é isomorfo ao anel de polinômios $\mathbb{F}[X_1, ..., X_r]$. Portanto,

$$r = dim_{Krull}S \leq trgrau_{\mathbb{F}}K = dim_{Krull}\mathcal{R}.$$

■

De agora em diante, trataremos apenas o caso em que o posto racional dos semigrupos de valores de um conjunto admissível de duas funções q-pesos é igual a dimensão da álgebra; observe que tal caso apareceu em exemplos nas seções 3.2 e 3.4.

Proposição 5.15. *Seja* $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, 2\}$ *um conjunto admissível de tipo finito de estruturas q-pesos em* $\mathcal{R}$*. Então corpo de frações* K *de* $\mathcal{R}$ *é um corpo de funções algébricas em r.posto*(Γ_i) *variáveis independentes sobre* $\mathbb{F}$*.*

Dem. Segue da proposição 5.8 e de [[Ei], cap.8, teo.A]. ■

Teorema 5.16. *Seja* $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, 2\}$ *um conjunto admissível de tipo finito de estruturas q-pesos em* $\mathcal{R}$ *tal que cada grupo* $G(\Gamma_i)$ *tenha um subgrupo isolado de posto racional r.posto*$(\Gamma_i) - 1$*. Então o fecho integral de* $\mathcal{R}$ *em seu corpo de frações* K *é um subanel de* K *consistindo de funções com pólos em pelo menos dois divisores primos de* K*.*

Dem.

Dos resultados acima, vimos que $\mathcal{R}$ é um domínio finitamente gerado e que o corpo de frações K de $\mathcal{R}$ é um corpo de funções algébricas em $r.posto(\Gamma_i) =: r$ variáveis sobre $\mathbb{F}$.

Assim, sejam ν_i as valorizações em K associadas a cada ρ_i, definidas como antes. Seja R_{ν_i} o anel de valorização de cada ν_i e M_{ν_i} seu respectivo ideal maximal. Então, do lema 5.13, temos que $\kappa_{\nu_i} = R_{\nu_i}/M_{\nu_i} \cong \mathbb{F}$, ou seja, $dim(\nu_i) = trgrau(\kappa_{\nu_i}|\mathbb{F}) = 0$. Por hipótese,

seja Δ_i o subgrupo isolado de $G(\Gamma_i)$ tal que $r.posto(\Delta_i) = r-1$. Então, das propriedades de valorizações, temos que $\nu_i = \mu_i \circ \overline{\nu_i}$, onde cada $\mu_i : K \to (G(\Gamma_i)/\Delta_i) \cup \{+\infty\}$ é uma valorização discreta de posto 1 em K, pois $posto(\mu_i) \leq r.posto(\mu_i) = 1$, e $\overline{\nu_i} : \kappa_{\mu_i} \to \Delta_i \cup \{+\infty\}$ é uma valorização do corpo de resíduos κ_{μ_i} de μ_i. Da desigualdade de Abhyankar, temos $r.posto(\mu_i) + dim(\mu_i) \leq trgrau(K|\mathbb{F}) = r$, ou seja, $dim(\mu_i) \leq r-1$. Mas, como $r.posto(\overline{\nu_i}) = r.posto(\Delta_i) = r-1$ e o corpo de resíduos $\kappa_{\overline{\nu_i}}$ de $\overline{\nu_i}$ é igual ao corpo de resíduos de ν_i (ver proposição A.22), ou seja, $\kappa_{\overline{\nu_i}} = \mathbb{F}$, segue que

$$r-1 = r.posto(\overline{\nu_i}) + dim(\overline{\nu_i}) \leq trgrau(\kappa_{\mu_i}|\mathbb{F}) = dim(\mu_i) \leq r-1.$$

Logo, $dim(\mu_i) = r-1$ e, portanto, cada μ_i é um divisor primo de $K|\mathbb{F}$.

Seja $\overline{\mathcal{R}}$ o fecho integral de $\mathcal{R}$ em K. Seja $S(\mathcal{R})$ o conjunto dos divisores primos de $K|\mathbb{F}$ cujo anel de valorização associado contem $\mathcal{R}$, ou seja,

$$S(\mathcal{R}) := \{\omega \text{ divisor primo em } K|\mathbb{F} : \mathcal{R} \subset R_\omega\}.$$

Então sabemos que (ver [Za-Sa II], cap.VI,§14)

$$\overline{\mathcal{R}} = \bigcap_{\omega \in S(\mathcal{R})} R_\omega.$$

Observe que $\mu_i \notin S(\mathcal{R})$, pois suponha $\mathcal{R} \subset R_{\mu_i}$. Então, para qualquer $f \in \mathcal{M}_{\rho_i}$ temos que $\rho_i(f) \succ_i 0$, ou seja, $\nu_i(f) \prec_i 0$ e, portanto, $\mu_i(f) \leq 0$. Como $\mathcal{R} \subset R_{\mu_i}$ temos que $\mu_i(f) = 0$ para todo $f \in \mathcal{M}_{\rho_i}$. Assim, seja $a/b \in K$ com $a, b \in \mathcal{R}\backslash\{0\}$ tal que $\mu_i(a/b) > 0$. Como $a, b \in \mathcal{R}\backslash\{0\}$, do lema 5.10, existe $g \in \mathcal{M}_{\rho_i}$ tal que $ga, gb \in \mathcal{M}_{\rho_i}$. Logo, $0 < \mu_i(a/b) = \mu_i(ga/gb) = \mu_i(ga) - \mu_i(gb) = 0$, contradição. ∎

Corolário 5.17. *Se, para qualquer $f \in \mathcal{R}\backslash\mathbb{F}$, existe $i \in \{1,2\}$ tal que $\mu_i(f) < 0$, então o fecho integral de $\mathcal{R}$ em K é um subanel de K consistindo de funções com pólos em apenas dois divisores primos de K.*

Dem. Vimos acima que

$$\overline{\mathcal{R}} = \bigcap_{\omega \in S(\mathcal{R})} R_\omega,$$

e que $\mu_1, \mu_2 \notin S(\mathcal{R})$. Assim, seja S o conjunto de todos os divisores primos de $K|\mathbb{F}$. Mostremos que $S(\mathcal{R}) = S\backslash\{\mu_1, \mu_2\}$. Suponha que $S(\mathcal{R}) \cup \{\mu_1, \mu_2\} \neq S$. Seja

$$\mathcal{R}' = \bigcap_{\omega \in S(\mathcal{R}) \cup \{\mu_1, \mu_2\}} R_\omega \subset \overline{\mathcal{R}}.$$

Seja $x \in \mathcal{R}'$ tal que $\mu_i(x) > 0$, para $i = 1, 2$ (a existência de tal elemento é garantida pelo teorema da aproximação [ver [Bo], cap VII, §1.5, prop.9]). Seja $I = \{y \in \mathcal{R} : y\overline{\mathcal{R}} \subset \mathcal{R}\} \neq (0)$ o condutor de $\mathcal{R}$ em $\overline{\mathcal{R}}$. Então para qualquer $y \in I$, temos que $yx \in \mathcal{R}$. Logo, $\mu_i(xy) < 0$ para algum i, ou seja, $\mu_i(x) < \mu_i(y^{-1})$. Mas, como μ_i é arquimediano, existe um inteiro positivo n_i tal que $n_i\mu_i(x) > \mu_i(y^{-1})$, ou seja, $\mu_i(x^{n_i}y) > 0$. Para $j \in \{1, 2\}$,$j \neq i$, temos que $\mu_j(xy) < 0$ ou $\mu_j(xy) \geq 0$. Se $\mu_j(xy) < 0$, então existe um inteiro positivo n_j tal que $\mu_j(x^{n_j}y) > 0$, pois μ_j é arquimediano. Se $\mu_j(xy) \geq 0$, para qualquer inteiro positivo $n > 1$, temos que $\mu_j(x^n y) > 0$, pois $\mu_j(x) > 0$. Assim, seja $k = max\{n_i : i = 1, 2\} \geq 1$, então $\mu_i(x^m y) > 0$ para todo i e para todo $m \geq k$, ou seja, da observação 5.12, $x^m y \in \mathcal{U}_{\rho_i}$ para todo i e para todo $m \geq k$, pois $\nu_i(x^m y) \succeq 0$. Logo $x^m y \in \mathcal{U}_{\rho_1} \cap \mathcal{U}_{\rho_2} = \mathbb{F}$ para todo $m \geq k$, contradição.

Portanto,

$$\overline{\mathcal{R}} = \bigcap_{\omega \in\, S\backslash\{\mu_1, \mu_2\}} R_\omega.$$

■

Proposição 5.18. *Seja $\{(\mathcal{R}, \rho_i, \Gamma_i), i = 1, 2\}$ um conjunto admissível de tipo finito de estruturas q-pesos em $\mathcal{R}$ tal que cada grupo $G(\Gamma_i)$ tenha um subgrupo isolado de posto racional r.posto$(\Gamma_i) - 1$. Então $\mathcal{R}$ é o anel de funções regulares de uma variedade afim, cujo normalização do seu fecho projetivo $\mathcal{X}$ possui dois divisores irredutíveis Z_1 e Z_2 no infinito. Se, além disso, para qualquer $f \in \mathcal{R}\backslash\mathbb{F}$, existe $i \in \{1, 2\}$ tal que $\mu_i(f) < 0$, onde μ_i é o divisor primo de $K|\mathbb{F}$ na decomposição de ν_i, então a normalização do fecho projetivo $\mathcal{X}$ possui apenas dois divisores irredutíveis Z_1 e Z_2 no infinito.*

Dem. Seja $\mathcal{X}$ a variedade projetiva definida pelo domínio afim $\mathcal{R}$ e $\overline{\mathcal{X}}$ sua normalização. Então, pela proposição A.21, teorema A.22 e do teorema 5.16, segue que cada valorização

μ_i, $i = 1, 2$, está centrado em um divisor irredutível Z_i de $\overline{\mathcal{X}}$. Agora, se, para qualquer $f \in \mathcal{R}\backslash\mathbb{F}$, $\mu_i(f) < 0$ para algum i, temos, do corolário 5.17, que Z_1 e Z_2 são os únicos divisores irredutíveis de $\overline{\mathcal{X}}$ no infinito. ■

Observação 5.19. Da proposição A.21, segue que cada divisor primo μ_i da decomposição $\nu_i = \mu_i \circ \overline{\nu_i}$ está centrado em uma subvariedade D_i de $\mathcal{X}$ e $dim(D) \leq dim(\mu_i)$. Segue também, da proposição A.23 e do lema 5.13, que cada uma das valorizações ν_i está centrada em um ponto racional $Q_i \in D_i \subset \mathcal{X}$.

Quando $\Gamma_i = \mathbb{N}_0$, $i = 1, 2$, temos que os divisores irredutíveis Z_1 e Z_2 são pontos racionais de $\overline{\mathcal{X}}$. Então, supondo $\mathbb{F}$ um corpo finito, temos o seguinte resultado.

Teorema 5.20 ([Ca-Si],§ 3, Teorema 3.21)**.** *Sejam* $\{(\mathcal{R}, \rho_i, \mathbb{N}_0), i = 1, 2\}$ *um conjunto admissível de tipo finito de estruturas q-pesos em* $\mathcal{R}$*,* $\varphi : \mathcal{R} \to \mathbb{F}^n$ *um morfismo sobrejetivo de* $\mathbb{F}$*-álgebras e* $\alpha = (\alpha_1, \alpha_2) \in \mathbb{N}_0^2$*. Então o código* $E(\alpha)$ *é um código geométrico de Goppa* $C_{\mathcal{L}}(D, G)$ *com* $G = \alpha_1 Z_1 + \alpha_2 Z_2$*.*

APÊNDICE A

VALORIZAÇÕES

Neste capítulo introduziremos os conceitos e resultados básicos da teoria de valorizações. Todo este capítulo foi escrito baseado nas referências [Bo], [La], [Va] e [Za-Sa II], ou seja, todos os resultados e definições citados aqui podem ser encontrados em tais referências.

A.1 Conceitos Básicos

Seja Λ é um grupo abeliano aditivo totalmente ordenado. Adicionamos a Λ um elemento $+\infty$ tal que $\alpha \prec +\infty$ para todo $\alpha \in \Lambda$ e estendemos a adição em $\Lambda \cup \{+\infty\}$ por $(+\infty) + \alpha = (+\infty) + (+\infty) = +\infty$.

Definição A.1. Seja K um corpo. Uma *valorização* ν de K é uma aplicação de K em $\Lambda \cup \{+\infty\}$ satisfazendo

1- $\nu(f) = +\infty$ se e somente se $f = 0$;

2- $\nu(fg) = \nu(f) + \nu(g)$, para todos $f, g \in K$;

3- $\nu(f + g) \succeq min\{\nu(f), \nu(g)\}$, para todos $f, g \in K$.

Dizemos que Λ é o *grupo de valores* da valorização ν. A valorização ν também e conhecida como *valorização de Krull*.

O conjunto $R_\nu = \{f \in K : \nu(f) \succeq 0\}$ é um anel local, chamado *anel de valorização* de ν, cujo ideal maximal é dado por $M_\nu = \{f \in K : \nu \succ 0\}$, e o corpo $\kappa_\nu = R_\nu/M_\nu$ é chamado de *corpo de resíduos* de ν.

Seja K um corpo e seja $\mathbb{F}$ um subcorpo de K. Diremos que uma valorização ν é *trivial* sobre $\mathbb{F}$, se para qualquer $x \in \mathbb{F}, x \neq 0$, temos que $\nu(x) = 0$. Quando uma valorização ν de K é trivial sobre um subcorpo $\mathbb{F}$ de K, diremos que ν é uma valorização de $K|\mathbb{F}$.

Definição A.2. Seja Λ um grupo abeliano. Dizemos que $\alpha_1, ..., \alpha_n \in \Lambda$ são *racionalmente independentes* se existem $\lambda_1, ..., \lambda_n \in \mathbb{Z}$ tais que $\lambda_1\alpha_1 + ... + \lambda_n\alpha_n = 0$ então $\lambda_i = 0$ para todo $i = 1, ..., n$. Caso contrário, estes elementos são ditos *racionalmente dependentes*. Chamamos o número máximo de elementos racionalmente independentes em Λ de *posto racional* do grupo Λ, e o denotamos por $rat.posto(\Lambda)$.

Definição A.3. Seja ν uma valorização de K com grupo valor Λ. Definimos o *posto racional* de ν como sendo

$$r.posto(\nu) := r.posto(\Lambda) = dim_{\mathbb{Q}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}).$$

Definição A.4. Seja Δ um subgrupo de um grupo totalmente ordenado Λ. Dizemos que Δ é um *subgrupo isolado* de Λ se para todo elemento $\gamma \in \Lambda$ tal que $\alpha \preceq \gamma \preceq \beta$ onde $\alpha, \beta \in \Delta$, temos que $\gamma \in \Delta$.

Como o conjunto de todos os subgrupos isolados Δ de Λ é totalmente ordenado pela relação de inclusão, podemos dar a seguinte definição.

Definição A.5. Definimos o *posto* de um grupo totalmente ordenado Λ como sendo

$$posto(\Lambda) = max\{t|\{0\} \subsetneq \Delta_1 \subsetneq ... \subsetneq \Delta_{t-1} \subsetneq \Lambda\},$$

onde Δ_i são subgrupos isolados de Λ. Assim definimos o *posto* de uma valorização ν como sendo o posto do seu grupo de valores.

Proposição A.6. *O posto de uma valorização ν é menor ou igual a seu posto racional:*

$$posto(\nu) \leq r.posto(\nu).$$

Exemplo A.7. Considere o grupo $\mathbb{Z}^2$ com as seguintes ordens:

- Lexicográfica: $(a,b) \prec_L (c,d) \Leftrightarrow a < c \text{ ou } a = c \text{ e } b < d$;
- induzida de $\mathbb{R}$: $(a,b) <_{\mathbb{R}} (c,d) \Leftrightarrow a + bq < c + dq$, onde $q \in \mathbb{R}\backslash\mathbb{Q}$.

Então $(\mathbb{Z}^2, \prec_L)$ tem posto racional 2 e posto 2, pois $\{(0,0)\}, \{0\} \times \mathbb{Z}$ são subgrupos isolados de $(\mathbb{Z}^2, \prec_L)$. Mas $(\mathbb{Z}^2, <_{\mathbb{R}})$ tem posto racional 2 e posto 1, pois $\{(0,0)\}$ é seu único subgrupo isolado.

Observação A.8. Uma valorização ν de K é de posto 1 se, e somente se, o grupo de valores Λ de ν é isomorfo a um subgrupo de $(\mathbb{R}, +)$. Isto é equivalente a dizer que o grupo Λ é *arquimideano*, isto é, Λ satisfaz a seguinte condição: se α e β são quaisquer dois elementos de Λ, com $\alpha > 0$, então existe um inteiro n tal que $n\alpha > \beta$.

Seja ν uma valorização de um corpo K, com grupo de valores Λ e anel de valorização R_ν. Existe uma bijeção entre os ideais primos de R_ν e os subgrupos isolados de Λ. Neste caso, o ideal maximal M_ν está associado ao subgrupo isolado $\Delta = \{0\}$, e o ideal primo (0) está associado ao subgrupo isolado $\Delta = \Lambda$. Disto, segue que o posto de ν é igual a dimensão de Krull de R_ν. Assim, se o posto de ν é maior que 1, existe um subgrupo isolado $\Delta \neq \{0\}$ de Λ, e seja M' o ideal primo de R_ν associado a Δ. Então o anel local $R' = (R_\nu)_{M'}$ é um anel de valorização com ideal maximal M', e $R_\nu \subset R'$. Denotemos por ν' a valorização de K associada ao anel R' e seja Λ' seu grupo de valores.

Proposição A.9. *a) O grupo de valores Λ' é isomorfo ao grupo quociente Λ/Δ, e a valorização $\nu' : K^* \to \Lambda'$ é a composição de $\nu : K^* \to \Lambda$ e $\phi : \Lambda \to \Lambda/\Delta$.*
b) O anel quociente $\overline{R_\nu} = R_\nu/M'$ é um anel de valorização no corpo de resíduos $\kappa_{\nu'} = R'/M'$ da valorização ν' e o grupo valor da valorização $\overline{\nu}$ associado ao anel $\overline{R_\nu}$ é isomorfo a Δ.

Definição A.10. A valorização ν acima é chamada a *valorização composição com as valorizações ν e $\overline{\nu}$* e escrevemos $\nu = \nu' \circ \overline{\nu}$.

Proposição A.11. *Se ν é uma valorização composição $\nu' \circ \overline{\nu}$ então*

$$posto(\nu) = posto(\nu') + posto(\overline{\nu}),\ e$$
$$r.posto(\nu) = r.posto(\nu') + r.posto(\overline{\nu}).$$

Reciprocamente, se temos uma valorização ν' de um corpo K e uma valorização $\overline{\nu}$ do corpo de resíduos $\kappa_{\nu'}$, podemos definir a valorização composição $\nu = \nu' \circ \overline{\nu}$.

Proposição A.12. *Seja ν' uma valorização de K com anel de valorização $R_{\nu'}$ e corpo de resíduos $\kappa_{\nu'}$, e seja $\overline{\nu}$ uma valorização de $\kappa_{\nu'}$, então a valorização composição $\nu = \nu' \circ \overline{\nu}$ é uma valorização do corpo K associada ao anel de valorização R_ν definido por $R_\nu = \{x \in R_{\nu'} | \overline{\nu}(\overline{x}) \geq 0\}$.*

Disto, segue que o corpo de resíduos da valorização composição ν é igual ao corpo de resíduos $\kappa_{\overline{\nu}}$ da valorização $\overline{\nu}$.

Seja ν uma valorização de $K|\mathbb{F}$.

Definição A.13. A *dimensão* de uma valorização ν é o grau de transcendência do corpo de resíduos κ_ν de ν sobre o corpo $\mathbb{F}$:

$$dim(\nu) = tr.grau(\kappa_\nu|\mathbb{F}).$$

Proposição A.14. *Desigualdade de Abhyankar*

$$posto(\nu) + dim(\nu) \leq r.posto(\nu) + dim(\nu) \leq trgrau(K|\mathbb{F}).$$

Se assumimos que K é um *corpo de funções* sobre $\mathbb{F}$, isto é, que K é uma extensão finitamente gerada de $\mathbb{F}$, e se temos a igualdade $r.posto(\nu) + dim(\nu) = trgrau(K|\mathbb{F})$, então o grupo valor Λ é um $\mathbb{Z}$-módulo finitamente gerado e o corpo de resíduos κ_ν de ν é uma extensão finitamente gerada de $\mathbb{F}$. Contúdo, se temos a igualdade $posto(\nu) + dim(\nu) = trgrau(K|\mathbb{F})$, então a valorização ν é *discreta*, ou seja, o grupo de valores Λ de ν é isomorfo a $\mathbb{Z}^{posto(\nu)}$, ordenado com a ordem lexicográfica.

A.2 Divisores Primos

Seja K um corpo de funções sobre um corpo $\mathbb{F}$, de grau de transcendência d.

Definição A.15. Um *divisor primo* de $K|\mathbb{F}$ é uma valorização ν de $K|\mathbb{F}$ que tem dimensão $d-1$, isto é, tal que $trgrau(\kappa_\nu|\mathbb{F}) = d-1$, onde κ_ν é o corpo de resíduos de ν.

Assim, se ν é um divisor primo de $K|\mathbb{F}$, como ν é não trivial, temos, da desigualdade de Abhyankar, que $posto(\nu) = 1$, ou seja, ν é uma valorização discreta de posto 1, isto é, o grupo valor é isomorfo a $\mathbb{Z}$, e seu corpo de resíduos κ_ν é uma extensão finitamente gerada de $\mathbb{F}$.

Exemplo A.16. Seja $\mathcal{R}$ domínio integral normal finitamente gerado sobre $\mathbb{F}$, com corpo de frações K, e seja P um ideal primo de altura 1 de $\mathcal{R}$. Então o anel local $\mathcal{R}_P$ é um anel de valorização, cuja valorização ν_P associada é um divisor primo de K (ν_P é a valorização P-ádica, isto é, a valorização definida por $\nu_P(g) = max\{n \in \mathbb{N}|g \in P^n\}$, para qualquer $g \in R$). Se consideramos a variedade afim $\mathcal{X}$ associada a $\mathcal{R}$, ou seja, $\mathcal{X} = spec\mathcal{R}$, o ideal primo P define um *divisor irredutível* (ou *divisor primo de Weil*) D em $\mathcal{X}$, e a valorização ν_p é a valorização definida pela ordem de anulamento ao longo do divisor D. Neste caso, o anel local $\mathcal{R}_P$ coincide com o anel das funções regulares $\mathcal{O}_D(\mathcal{X})$ de $\mathcal{X}$ em D.

A.3 Centro de uma valorização

Seja K um corpo, ν uma valorização de K, e R_ν o anel de valorização associado a ν com ideal maximal M_ν.

Definição A.17. Seja A um subanel de K com $A \subset R_\nu$. Então o *centro* da valorização ν em A é o ideal P de A definido por $P = A \cap M_\nu$.

Na definição acima, se A é um anel local cujo ideal maximal é P, então dizemos que o anel R_ν *domina* o anel A, ou também que A é *dominado* por R_ν.

Seja $\mathcal{X}$ uma variedade algébrica definida sobre um corpo $\mathbb{F}$ e seja $K = \mathbb{F}(\mathcal{X})$ o corpo de funções de $\mathcal{X}$. Queremos definir o centro de uma valorização ν de $K|\mathbb{F}$, ou mais geralmente, de uma valorização ν de $L|\mathbb{F}$ onde L é uma extensão de K, sobre a variedade $\mathcal{X}$.

Proposição A.18. *Seja $\mathcal{X}$ uma variedade algébrica sobre $\mathbb{F}$ e seja ν uma valorização de um corpo L, extensão do corpo de funções $K = \mathbb{F}(\mathcal{X})$ de $\mathcal{X}$. Então existe no máximo um ponto $\xi \in \mathcal{X}$ tal que o anel local $\mathcal{O}_\xi(\mathcal{X})$ é dominado pelo anel de valorização R_ν associado a ν. Mais ainda, a subvariedade fechada irredutível Z de $\mathcal{X}$ definida por $Z = \overline{\{\xi\}}$ é o subconjunto de pontos $x \in \mathcal{X}$ cujo anel local $\mathcal{O}_x(\mathcal{X})$ está contido no anel de valorização R_ν associado a ν, ou seja, $Z = \{x \in \mathcal{X} | \mathcal{O}_x(\mathcal{X}) \subset R_\nu\}$.*

Definição A.19. Definimos o *centro* de uma valorização ν em uma variedade $\mathcal{X}$ ser o ponto ξ, quando este existe, dado na proposição acima. Dizemos também que o centro de uma valorização ν na variedade $\mathcal{X}$ é a subvariedade $Z = \overline{\{\xi\}} = \{x \in \mathcal{X} | \mathcal{O}_x(\mathcal{X}) \subset R_\nu\}$. Se não existe ξ, dizemos que a valorização ν não tem centro em $\mathcal{X}$, ou que o centro Z é vazio.

Observação A.20. A valorização ν pode não ter centro em uma variedade $\mathcal{X}$, basta tomar a variedade afim $\mathcal{X} = spec(A)$, onde A não está contido em R_ν. Agora, se $\mathcal{X}$ é uma variedade projetiva, qualquer valorização ν em $\mathcal{X}$ tem um centro em $\mathcal{X}$.

Veremos agora uma relação entre a dimensão de uma valorização e a dimensão de seu centro em uma variedade projetiva.

Proposição A.21. *Seja $\mathcal{X}$ uma variedade algébrica projetiva definida sobre um corpo $\mathbb{F}$ com corpo de funções $K = \mathbb{F}(\mathcal{X})$, e seja ν uma valorização de $K|\mathbb{F}$ com corpo de resíduos κ. Então o centro Z de ν em $\mathcal{X}$ é não vazio e temos que $dim(Z) \leq dim(\nu)$. Se, contudo, temos uma desigualdade estrita, existe um morfismo birracional próprio $Y \to \mathcal{X}$ tal que a dimensão do centro de ν em Y é igual a $dim(\nu)$.*

Teorema A.22. *Se Z é uma subvariedade irredutível de $\mathcal{X}$ de codimensão* 1 *então o conjunto dos divisores primos do corpo de funções K de $\mathcal{X}$ que tem centro Z em $\mathcal{X}$ é finito e não vazio. Se ν é qualquer divisor primo em K tendo centro em Z então o corpo de resíduos de ν é uma extensão algébrica do corpo de funções $\mathbb{F}(Z)$ de Z. Contudo, se a variedade $\mathcal{X}$ é normal, existe somente um divisor primo ν com centro em Z. Neste caso, o anel de valorização associado a ν coincide com o anel local $\mathcal{O}_Z(\mathcal{X})$, que é um anel de valorização noetheriano, e seu corpo de resíduos coincide com o corpo de funções $\mathbb{F}(Z)$ de Z.*

Seja $\mathcal{X}$ uma variedade algébrica sobre um corpo $\mathbb{F}$ com corpo de funções $K = \mathbb{F}(\mathcal{X})$ e seja ν uma valorização de $K|\mathbb{F}$ com corpo de resíduos κ. Assumimos que o grau de transcendência de κ sobre $\mathbb{F}$ é positivo, então existe uma valorização não trivial $\overline{\nu}$ de $\kappa|\mathbb{F}$ e podemos definir a valorização composição $\nu' = \nu \circ \overline{\nu}$ que é também uma valorização de $K|\mathbb{F}$. Se o centro Z de ν em $\mathcal{X}$ é não vazio, então o corpo de funções $\mathbb{F}(Z)$ de Z está contido no corpo de resíduos κ e assim podemos considerar o centro em Z da valorização $\overline{\nu}$ de $\kappa|\mathbb{F}$.

Proposição A.23. *O centro em Z da valorização $\overline{\nu}$ é igual ao centro em $\mathcal{X}$ da valorização composição $\nu' = \nu \circ \overline{\nu}$.*

Se ν' é a valorização composição $\nu' = \nu \circ \overline{\nu}$ de $K|\mathbb{F}$, o centro Z' de ν' está contido no centro Z de ν.

REFERÊNCIAS BIBLIOGRÁFICAS

[Abh] S.S. Abhyankar, *On the Valuations Centered in a Local Domain*, vol. 78, American Mathematical Society, pp. 321-348, 1956.

[Ad-Lo] W.W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994.

[An-Ge] H. E. Andersen, O. Geil, *Evaluation Codes from Order Domain Theory*, by Henning E. Andersen and Olav Geil. Published in Finite Fields and Their Applications Vol. 14 (1), pp. 92-123, Jan. 2008

[At-Ma] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[Bo] N. Bourbaki, *Elements of Mathematics, Commutative Algebra*, Addison-Wesley Publishing Company, 1972.

[Bras] M. Bras-Amorós, *Algebraic-Geometry Codes, One-Point Codes and Evaluation Codes*, Designs, Codes and Cryptography, Springer, vol. 43, n. 2-3, pp. 137-145, 2007.

[Ca] C. Carvalho, *Grobner bases and algebras admitting a complete set of near weights*, preprint 2010.

[NOC] C. Carvalho, C. Munuera, E. Silva, F. Torres, *Nears orders and codes*, IEEE Trans. Inform. Theory, vol. 53, issue 5, pp.1919-1924, 2007.

[Ca-Si] C. Carvalho, E. Silva, *On algebras admitting a complete set of near weights, evaluation codes, and Goppa codes*, Designs, Codes and Cryptography, pp. 0925-1022, 2009.

[IVA] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, ans Algorithms: An Introduction to Computational Algebraic Geometry*, 2nd ed., Springer-Verlag, 1996.

[UAG] D. Cox, J. Little, D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics, 2nd ed., Springer-Verlag, 2004.

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

[En] O. Endler, *Valuation Theory*, Universitext, Springer-Verlag, Berlin, 1972.

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

[Ge1] O. Geil, *Codes Based on an $\mathbb{F}_q$-Algebra*, Ph.D. Thesis, Aalborg University, Denmark, 1999.

[Ge2] O. Geil, *Algebraic geometry codes from order domains*, Gröbner Bases, Coding, and Cryptography, Springer, pp. 121-141, 2009.

[Ge-Pe] O. Geil, R. Pellikaan, *On the structure of order domains*, Finite Fields and their Applications, vol. 8, pp. 369-396, 2002.

[Gri-Ha] P. Griffiths, J. Harris, *Principles of Algebraic Geometry*, Wiley, New York, 1978.

[Ga-Le] A. Garcia, Y. Lequain, *Elementos de Álgebra*, Projeto Euclides, IMPA, 2003.

[Ha] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

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

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

[Li] J. Little, *The Ubiquity of Order Domains for the Construction of Error Control Codes*, Advances in Mathematics of Communications, vol. 1, n° 1, pp. 151-171, 2007.

[Ma] 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, 1999.

[Mat] G. L. Matthews, *Weierstrass Pairs and Minimum Distance of Goppa Codes*, Designs, Codes and Cryptography, vol.22, no.2, pp.107-121, 2001.

[Mo-Sw] E. Mosteig, M. Sweedler, *Valuations and Filtrations*, Journal of Symbolic Computation, vol. 34, no.5, pp. 399-435, 2002.

[Mu-To] C. Munuera, F. Torres, *The structure of algebras admitting well agreeing near weights*, Journal of Pure and Applied Algebra, vol. 212, Issue 4, pp. 910-918, 2008.

[Su] M. O'Sullivan, *New Codes for the Berlekamp-Massey-Sakata Algorithm*, Finite Fields and their Applications, vol. 7, pp. 293-317, 2001.

[Ro] L. Robbiano, *On the Theory of Graded Structures*, J. Symbolic Computation, vol. 2, pp. 139-170, 1986.

[Sh1] I. Shafarevich, *Basic Algebraic Geometry 1*, Springer-Verlag, 1994.

[Sh2] I. Shafarevich, *Basic Algebraic Geometry 2*, Springer-Verlag, 1996.

[Shif] G. Shiffels, *Orderings and Algorithms in Commutative Algebra*, Africa Mathematika, series 3, vol. 2, pp. 79-101, 1983.

[Si] E. Silva, *Funções Ordens Fracas e a Distância Mínima dos Códigos Geométricos de Goppa*, Tese de Doutorado, Unicamp, Campinas, 2004.

[Sp] M. Spivakovsky, *Valuations in Function Fields of Surfaces*, American Journal of Mathematics, Vol. 112, No. 1, pp. 107-156, 1990.

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

[Stu] , B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series, vol. 8, American Mathematical Society, 1995.

[Va] M. Vaquié, *Valuations and Local Uniformization*, Advanced Studies in Pure Mathematics, 2008, to appear.

[Za] O. Zariski, *An Introduction of the Theory of Algebraic Surfaces*, Springer-Verlag, Berlin, Heidelberg, 1969.

[Za-Sa I] O. Zariski, P. Samuel, *Commutative algebra*, vol. I, Reprint of the 1958 edition, Graduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1975.

[Za-Sa II] O. Zariski, P. Samuel, *Commutative algebra*, vol. II, Reprint of the 1960 edition, Graduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1975.