Construção e Rotulamento de Constelações de Sinais Geometricamente Uniformes em $\mathbb{R}^n$

Edson Donizete de Carvalho, * Reginaldo Palazzo Jr.,† Marcelo Firer,‡

Abstract

O objetivo deste artigo é de estabelecer as condições de quando é possível construir constelações de sinais que sejam geometricamente uniformes e também casadas a grupos. Tais constelações fazem parte do espaço de sinais em $\mathbb{R}^n$ cuja identificação será através dos elementos dos correspondentes anéis de inteiros. O rotulamento casado decorrerá da ação transitiva dos correspondentes p-grupos aditivos G_{p^m} ou dos grupos aditivos do corpo de Galois $GF(p^m)$.

1 Introdução

Em [4], Egri e Horrigan propuseram a construção de um grupo multiplicativo finito de inteiros complexos para o uso em detecção diferencial de sinais de uma constelação de sinais 16-QAM.

Em [5], Rifà classificou, caracterizou e construiu os grupos multiplicativos G_m de cardinalidade 2^m e os grupos das unidades de G_m, denotado por $G_m^{'}$, que podem ser utilizados em detecção diferencialmente coerente de sinais do tipo QAM.

Em [11], Dong e Soh propuseram a construção de subgrupos a partir dos grupos multiplicativos das unidades dos quocientes $\mathbb{Z}[i]/(p^m)$ e $\mathbb{Z}[\omega]/(p^m)$, para p primo ímpar, de tal

*The author was with the Department of Telematics, DT-FEEC-UNICAMP, P.O.Box 6101, 13.083-970, Campinas, SP, Brazil. e-mail: edsondonizete@yahoo.com.br

†The author is with the Department of Telematics, State University of Campinas, DT-FEEC-UNICAMP. This work has been supported by Fundação de Amparo à Pesquisa do Estado de São Paulo, FAPESP, under grant 95/4720-08, and by Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq, under grant 301416/85-0. email:palazzo@dt.fee.unicamp.br

‡The author is with the Department of Mathematics, IMECC-UNICAMP, Campinas, SP. e-mail firer@ime.unicamp.br

forma que estes subgrupos estão casados a constelações de sinais QAM com $4p^{2m-2}$ e $6p^{2m-2}$ sinais, respectivamente.

Nos trabalhos [4], [5] e [11] foram propostos códigos corretores de erros não lineares tendo como alfabetos elementos dos grupos multiplicativos associados aos correspondentes anéis de inteiros. Sob a operação de multiplicação, tais grupos não dão origem a reticulados.

Em [3], Huber propos um método de construção de códigos de bloco lineares tendo como alfabeto elementos de um corpo de Galois $GF(p)$ obtido via classes de resíduos de um anel de inteiros de Gauss módulo ideais primos. Tais códigos apresentam capacidade de correção de um erro para codificação de sinais identificados em $\mathbb{R}^2$. Neste mesmo trabalho, foi introduzida uma distância modular denominada distância de Mannheim que é bastante eficaz no projeto de códigos de bloco lineares para as constelações do tipo QAM.

Favareto et.al [8] propuseram um procedimento algébrico de rotulamento casado dos sinais de uma constelação de sinais em $\mathbb{R}^2$ por elementos do grupo aditivo de $GF(p)$, para os casos em que um inteiro primo p seja fatorável como elementos irredutíveis em um anel de inteiros.

Em [12] Interlando e Elia estenderam o procedimento de rotulamento casado de sinais em $\mathbb{R}^n$, por elementos de $GF(p)$ e de $GF(p^m)$, através da aplicação do Lema de Kummer, [13], ao polinômio minimal $p(X)$ associado ao corpo de números $\mathbb{K}$ de grau n. Se $p(X)$ é fatorável em $\mathbb{Z}_p[X]$, para um inteiro primo p fixo, então existe um ideal primo de norma p^k no anel de inteiros proveniente do corpo de números $\mathbb{K}$, cujo grau do polinômio irredutível usado na obtenção do ideal primo é k.

O quociente do anel de inteiros por este ideal primo, resulta no corpo de Galois $GF(p^k)$. O grupo que irá rotular os p^k sinais de uma constelação de sinais em $\mathbb{R}^n$ será o grupo aditivo de $GF(p^k)$.

Neste trabalho iremos propor procedimentos de construção de constelações de sinais casadas a grupos aditivos associados a corpos de Galois. Para o caso em que p é um número primo, não fatorável nos anéis de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, mostramos que não é possível construir uma constelação com p sinais. Entretanto, é possível construir constelações com p^2 sinais casadas ao grupo aditivo de $GF(p^2)$. Iremos também propor um procedimento de construção de constelação com p^m sinais casada a um p-grupo aditivo G_{p^m}.

Do estudo da representatividade dos números p^m através das formas quadráticas $f(X,Y) = X^2+Y^2$ e $g(X,Y) = X^2+XY+Y^2$ associadas aos correspondentes reticulados (identificados

pelos anéis de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente) em $\mathbb{R}^2$, estabeleceremos as condições de quando é possível construir constelações com p^m sinais em $\mathbb{R}^2$. Uma vez que seja possível construir a constela ção de sinais, o próximo passo está relacionado com a estrutura algébrica do grupo que irá rotular os sinais destas constelações. A caracterização de tais grupos depende da congruência de um inteiro primo p módulo 4 para o anel de inteiros $\mathbb{Z}[i]$, ou módulo 6 para o anel de inteiros $\mathbb{Z}[\omega]$.

Em $\mathbb{R}^n$ mostramos que quando o polinômio minimal $p(X)$ associado a um corpo de números $\mathbb{K}$ de grau n, não é fatorável módulo p, para um inteiro primo p fixo, é possível construir constelações de sinais casadas a grupos aditivos de $GF(p^n)$, onde n é o grau de $p(X)$.

Propomos um método de construção de constelações com p^m sinais, com os sinais tendo como rótulos elementos de um p-grupo G_{p^k} , a partir de ideais de norma p^m no anel de inteiros proveniente do corpo de números $\mathbb{K}$, para tanto basta tomar estes ideais como potências de ideais primos de norma p^k, onde p^m é uma potência de p^k. O quociente do anel de inteiros por estes ideais resulta nos p-grupos aditivos G_{p^m} como grupos de rótulos para constelações de p^m sinais em $\mathbb{R}^n$.

Nos casos em que um inteiro primo p não é fatorável em um anel de inteiros, Favareto et.al [8] não fornece um procedimento de construção de constelações de sinais com os sinais tendo como rótulos elementos de um corpo de Galois, e também, não há uma proposta de construção de constelações com p^m sinais casada a um outro grupo aditivo G de cardinalidade p^m que não seja proveniente de um corpo de Galois.

Quando $p(X)$ não é fatorável em $\mathbb{Z}_p[X]$, para um inteiro p primo fixo, não foi considerada em [12] não fornecem procedimentos para a construção de constelações de p^m sinais, tendo como grupo de rótulos elementos de $GF(p^m)$, e também, não é fornecido nenhum procedimento de construção de constelação de sinais tendo como grupo de rótulos um outro grupo aditivo G de cardinalidade p^m, que não seja proveniente de um corpo de Galois.

Este trabalho esta dividido da seguinte maneira. Na Seção 2 faremos uma revisão de conceitos de teoria dos números tais como corpo de números, anéis de inteiros, norma de um ideal e grupo de Galois bem como os conceitos de constelações de sinais geometricamente uniformes e a definição de função de rotulamento casado entre os sinais de uma constelação de sinas e elementos de um grupo G. Na Seção 3 a definição de reticulado em $\mathbb{R}^n$ e os

procedimentos para a identificação dos pontos dos reticulados em $\mathbb{R}^2$ e $\mathbb{R}^n$, por elementos de anéis de inteiros são apresentados. Na Seção 4 fornecemos procedimentos para a construção de constelações de p^m sinais em $\mathbb{R}^2$ e $\mathbb{R}^n$, de maneiras distintas. Na Seção 5 apresentamos constelações de p^m sinais com os sinais tendo como rótulos elementos de corpos de Galois $GF(p^m)$ e p-grupos ativos G_{p^m} em $\mathbb{R}^2, \mathbb{R}^3$ e $\mathbb{R}^4$.

2 Preliminares

2.1 Teoria dos Números

Sejam $\mathbb{E}$ e $\mathbb{F}$ subcorpos de $\mathbb{C}$, o corpo dos números complexos. Se $\mathbb{E}$ é um subcorpo de $\mathbb{F}$, então $\mathbb{F}$ é uma extensão de $\mathbb{E}$, denotada por $\mathbb{F}/\mathbb{E}$. A dimensão de $\mathbb{F}$, vista como espaço vetorial sobre $\mathbb{E}$, é chamada de grau de $\mathbb{F}$ sobre $\mathbb{E}$ e será denotada por $[\mathbb{F} : \mathbb{E}]$.

Considere $p(X)$ um polinômio irredutível sobre $\mathbb{E}$. Pelo Teorema Fundamental da Álgebra é sempre possível obter um subcorpo $\mathbb{F}$ de $\mathbb{C}$, que seja uma extensão do corpo $\mathbb{E}$, chamado *corpo de fatoração* de $p(X)$, como sendo o menor corpo $\mathbb{F}$ contendo todas as raízes de $p(X)$.

Chamamos de *número algébrico* qualquer elemento $\alpha \in \mathbb{C}$ que é raiz de algum polinômio não nulo $p(X)$ sobre $\mathbb{Q}$. Podemos e iremos sempre considerar $p(X)$ mônico. Qualquer extensão finita de $\mathbb{Q}$ é chamada de *corpo de números*, em particular $\mathbb{F} = \mathbb{Q}(\alpha)$.

Sejam $\mathbb{F}$ um corpo de números e $\alpha \in \mathbb{F}$ raiz de um polinômio $p(X)$ mônico com coeficientes em $\mathbb{Z}$, diremos que α é um *inteiro algébrico* e o conjunto desses inteiros algébricos constitui um anel denominado *anel de inteiros de* $\mathbb{F}$ [6], denotado por $\mathcal{D}_{\mathbb{F}}$. Exemplos de corpos de números são as extensões quadráticas imaginárias, isto é, subcorpos $\mathbb{F}$ de $\mathbb{C}$ de grau 2 caracterizados por:

$$\mathbb{F} = \mathbb{Q}(\sqrt{-m}) = \left\{ a + ib\sqrt{m} : a, b \in \mathbb{Q} \right\},$$

onde m é um inteiro positivo livre de quadrados.

Já os anéis de inteiros $\mathcal{D}_{\mathbb{F}}$ são caracterizados por $\mathbb{Z}[\theta] = \{a + b\theta : a, b \in \mathbb{Z}\}$, onde θ é dado por

$$\theta = \begin{cases} \sqrt{-m}, & se \ -m \equiv 2, 3 \ mod \, 4 \\ \\ \frac{1+\sqrt{-m}}{2}, & se \ -m \equiv 1 \ mod \, 4 \end{cases}$$

Example 2.1 i) *Se a extensão quadrática é* $\mathbb{F} = \mathbb{Q}(\sqrt{-1})$*, então o anel de inteiros* $\mathbb{Z}[\theta]$ *de* $\mathbb{F}$ *é dado por* $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$*, onde* $i = \sqrt{-1}$*, também conhecido como o anel de inteiros de Gauss.*

ii) *Se a extensão quadrática é* $\mathbb{F} = \mathbb{Q}(\sqrt{-3})$*, então o anel de inteiros* $\mathbb{Z}[\theta]$ *de* $\mathbb{F}$ *é dado por* $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$*, onde* $\omega = \frac{1+\sqrt{-3}}{2}$*, também conhecido como o anel de inteiros de Eisenstein-Jacobi.*

O Teorema 2.1 relaciona polinômios $p(X)$, tendo uma das raízes um inteiro algébrico, com extensões de corpos.

Theorem 2.1 *[9] Sejam* $\mathbb{F}/\mathbb{E}$ *uma extensão de corpos e* $\alpha \in \mathbb{F}$ *um inteiro algébrico sobre* $\mathbb{E}$*.*

i) *Existe um polinômio mônico irredutível* $p(X) \in \mathbb{E}[X]$ *tendo* α *como raiz;*

ii) $p(X)$ *é o polinômio mônico de menor grau em* $\mathbb{E}[X]$ *tendo* α *como raiz e é único;*

iii) *A dimensão* $[\mathbb{F} : \mathbb{E}]$ *é igual ao grau de* $p(X)$*.*

Lemma 2.1 *[9] Seja* $p(X) \in \mathbb{E}[X]$ *um polinômio não constante. Seja* $\mathbb{F}$ *o corpo de fatoração de* $p(X)$*. Se* $\sigma : \mathbb{F} \to \mathbb{F}$ *é um automorfismo e se* α *é uma raiz de* $p(X)$*, então* $\sigma(\alpha)$ *também é uma raiz de* $p(X)$*.*

Definition 2.1 *Seja* $\mathbb{F}/\mathbb{E}$ *uma extensão de corpos. O grupo de Galois* $\mathbb{F}/\mathbb{E}$*, denotado por* $G(\mathbb{F}/\mathbb{E})$*, é o conjunto de todos os automorfismos de* $\mathbb{F}$ *que deixam fixos os elementos de* $\mathbb{E}$*. Se o polinômio* $p(X) \in \mathbb{E}[X]$ *tiver como corpo de fatoração* $\mathbb{F}$*, então o grupo de Galois de* $p(X)$ *é* $G(\mathbb{F}/\mathbb{E})$*,*

Theorem 2.2 *[9] Seja* $p(X)$ *um polinômio com coeficientes sobre* $\mathbb{E}$*. Se* $p(X)$ *é separável (isto é, possui todas raízes distintas na corpo de fatoração), então* $|G(\mathbb{F}/\mathbb{E})| = [\mathbb{F} : \mathbb{E}]$*.*

Seja $G(\mathbb{F}/\mathbb{E}) = \{\sigma_0, \ldots, \sigma_{n-1}\}$ o grupo de Galois $\mathbb{F}/\mathbb{E}$. Chamamos de *norma relativa* de um elemento $z \in \mathbb{F}$ a aplicação $N_{\mathbb{F}/\mathbb{E}}(z) = \prod_{i=0}^{n-1} \sigma_i(z)$ com valores em $\mathbb{E}$.

Como exemplo, considere uma extensão quadrática racional imaginária do tipo $\mathbb{Q}(\sqrt{-m})/\mathbb{Q}$, onde m é um inteiro positivo livre de quadrados. O grupo de Galois associado a esta extensão é $G(\mathbb{Q}(\sqrt{-m})/\mathbb{Q}) = \{\sigma_0, \sigma_1\}$, onde σ_0 é a identidade e $\sigma_1(a + b\sqrt{-m}) = a - b\sqrt{-m}$.

Avaliando a norma dos elementos nos anéis de inteiros $\mathbb{Z}[\theta]$ provenientes dessas extensões quadráticas imaginárias, concluímos que

$$N_{\mathbb{Q}(\sqrt{-m})/\mathbb{Q}}(a+b\theta) = (a+b\theta)(\overline{a+b\theta}) = \begin{cases} a^2 - mb^2, & se \ -m \equiv 2,3 \ mod\, 4 \\ \\ a^2 + ab + \frac{(1-m)}{4}b^2, & se \ -m \equiv 1 \ mod\, 4 \end{cases}$$

É conhecido que o algoritmo da divisão de Euclides é válido nos anéis $\mathbb{Z}[\theta]$ para $\theta = \sqrt{-m}$, se $m = 1, 2$ e para $\theta = \frac{1+\sqrt{-m}}{2}$, se $m = 3, 7, 11$ através do uso da aplicação norma, [6], isto é, dados $a, b \in \mathbb{Z}[\theta]$, sempre existem $q, r \in \mathbb{Z}[\theta]$ satifazendo a condição de que $a = bq + r$, com $r = 0$ ou $N_{\mathbb{Q}(\sqrt{-m})/\mathbb{Q}}(r) < N_{\mathbb{Q}(\sqrt{-m})/\mathbb{Q}}(b)$.

Os anéis onde o algoritmo da divisão de Euclides é aplicável são denominados **anéis euclidianos**.

No sentido de fundamentar os conceitos envolvidos neste trabalho, iremos necessitar dos conceitos de anel noetheriano e de anel de Dedekind.

Definition 2.2 *Um anel R em que todos os ideais são finitamente gerados (isto é, cada elemento do ideal é escrito como combinação linear de um número finito de geradores) é chamado* **anel noetheriano**.

Definition 2.3 *Um domínio noetheriano R, integralmente fechado onde todo ideal primo não nulo é maximal é chamado* **domínio de Dedekind**.

Theorem 2.3 *[6] Se $\mathbb{F}$ for um corpo de números, então seu anel de inteiros algébricos é um domínio de Dedekind.*

Proposition 2.1 *[6] Sejam $\mathbb{F}$ um corpo de números, $\mathcal{D}_{\mathbb{F}}$ seu anel de inteiros algébricos e $\mathcal{P}$ um ideal não nulo de $\mathcal{D}_{\mathbb{F}}$, então são válidas as seguintes afirmações:*

(i) *$\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, onde p é o único número primo em $\mathcal{P}$;*

(ii) *O quociente $\mathcal{D}_{\mathbb{F}}/\mathcal{P}$ é uma extensão finita do corpo $GF(p)$ cujo grau $[\mathcal{D}_{\mathbb{F}}/\mathcal{P} : GF(p)] \leq n$*

.

Sejam R um anel comutativo e I um ideal de R. Em R/I a operação $(a+I)+(b+I) = (a+b)+I$ para $a, b \in R$, está bem definida e as seguintes condições são verificadas:

i) A classe $0 + I$ é o elemento neutro para esta operação.

ii) $a + I = b + I$ se, e somente se, $a - b \in I$, neste caso denotamos por $a \equiv b(mod\ I)$.

Assim fica estabelecida uma estrutura de grupo aditivo em R. A notação $a \equiv b(mod\ I)$ significa que os elementos a e b de R estão na mesma classe lateral (isto é, representam o mesmo elemento em R/I). Chamamos R/I de **grupo quociente aditivo** de R sobre I.

O número de elementos de R/I é chamado de **norma do ideal** I.

Outro fato conhecido é que anéis euclidianos são **anéis principais**, isto é, todo ideal é gerado por um elemento que é único a menos de associados.

2.2 Constelações de sinais geometricamente uniformes

Um conjunto discreto de pontos em $\mathbb{R}^n$ em que seja possível realizar uma identificação destes pontos por sinais é chamado de *espaço de sinais*.

Uma *constelação de sinais* é um subconjunto finito de sinais em um espaço de sinais.

Definition 2.4 *Um conjunto de sinais K é uma constelação de sinais geometricamente uniforme se para quaisquer sinais $k_0, k_1 \in K$, existir uma isometria $T \in U(K)$ tal que $T(k_0) = k_1$, ou seja, $U(K)$ age transitivamente em K, equivalentemente,*

$$U(k_0) = \{T(k_0) : \forall T \in U(K)\} = K.$$

Definition 2.5 *A região de Voronoi $R_V(k)$ associada a um dado ponto de sinal $k \in K$ é o conjunto $R_V(k) = \{\mathbf{x} \in \mathbb{R}^n : d(\mathbf{x}, k) \leq d(\mathbf{x}, T(k)), \forall T \in U\}$.*

Definition 2.6 *O perfil de distância global com relação a $k \in K$, denotado por $PD(k)$, é definido como sendo o conjunto das distâncias dos pontos de K com relação a k.*

O teorema a seguir relaciona constelações de sinais geometricamente uniformes com regiões de Voronoi.

Theorem 2.4 *[1] Se K for uma constelação de sinais geometricamente uniforme, então:*

1) *Todas as regiões de Voronoi são do mesmo tipo, isto é, são congruentes;*

2) *O perfil de distância global $PD(k)$ é o mesmo para qualquer ponto de sinal em K.*

Dentre todos os possíveis conjuntos de sinais com cardinalidade m finita, obtidos a partir de convenientes particionamentos em espaços de sinais, aquele que apresenta a menor energia média é denominado de *região fundamental* associada aos m pontos de sinais. A energia média mínima E_{min} de uma constelação de sinais $\{x_0, x_1, \ldots, x_{m-1}\}$ é a função $\sum_{i=1}^{m-1} d_i^2 \frac{1}{m}$, onde $d(x_0, x_i)$ denota a distância do ponto de sinal x_i a x_0, onde x_0 o centro de massa de constelação.

Diremos que uma constelação de sinais S está *casada* a um grupo G, se existe uma aplicação μ de G sobre S tal que $d(\mu(g), \mu(h)) = d(\mu(e), \mu(g^{-1}h))$, para todo $g, h \in G$, onde e é o elemento neutro de G e $d(.,.)$ é uma distância em S. A aplicação μ é chamada *aplicação casada* [2]. Além disso, se μ é injetiva, dizemos que μ^{-1} é um *rotulamento casado*, isto é, se G é isomorfo a $G(S)$ então μ é um *rotulamento isométrico*.

3 Reticulados em $\mathbb{R}^n$

Dizemos que um subconjunto discreto Λ de pontos de $\mathbb{R}^n$ é um *reticulado de dimensão n* se este for um $\mathbb{Z}$-módulo, gerado através de uma base $\{e_1, \ldots, e_n\}$. Note que $e_1, \ldots, e_n$ podem ser vistos como linhas de uma matriz geradora M. Um vetor $x = (x_1, \ldots, x_n) \in \Lambda$, é escrito como $x = x_1e_1 + \cdots + x_ne_n = x.M$, onde x_i são inteiros. A norma de x é $N(x) = N(x_1e_1 + \cdots + x_ne_n) = \Sigma_{i=1}^n \Sigma_{j=1}^n x_i x_j e_i e_j = x.M.M^t x^t = x.A.x^t = f(x)$, onde a matriz $A = M.M^t$ é chamada *matriz Gram de* Λ.

A função $f(x)$ de n variáveis inteiras $x_1, \ldots, x_n$ é uma forma quadrática associada ao reticulado Λ.

3.1 Reticulados em $\mathbb{R}^n$ identificados por anéis de inteiros

Em [12] Interlando e Elia propuseram uma maneira sistemática de identificação de pontos de um reticulado Λ no espaço $\mathbb{R}^n$ por elementos de um anel de inteiros proveniente de corpos de números de grau n.

O objetivo desta identificação é prover uma estrutura aditiva de grupo aos pontos do reticulado Λ. Neste caso, em particular, a estrutura aditiva do grupo provém da parte aditiva do anel de inteiros.

Uma vez que se tenha esta identificação poderemos operar estes pontos como se estivesse-

mos operando os elementos do anel de inteiros.

Neste sentido é que apresentamos alguns resultados da teoria dos números necessários para que ocorra esta identificação.

Seja $\mathbb{F} = \mathbb{Q}(\theta_1)$ uma extensão separável de $\mathbb{Q}$, com $\theta_1 \in \mathbb{C}$ raiz de um polinômio mônico $p(X) \in \mathbb{Z}[X]$ de grau n. As raízes $\theta_2, \ldots, \theta_n$ são as conjugadas de θ_1.

Associados a esta extensão de corpos temos os n mergulhos $\sigma_i : \mathbb{F} \longrightarrow \mathbb{C}$. Seja r_1 o número dos j-mergulhos tais que $\sigma_j(\mathbb{F}) \subseteq \mathbb{R}$ e $2r_2$ o número dos j-mergulhos tais que $\sigma_j(\mathbb{F}) \nsubseteq \mathbb{R}$. Com isso, $n = r_1 + 2r_2$. Se $n = r_1, \mathbb{F}$ é dito um *corpo totalmente real*, se $n = 2r_2$, então $\mathbb{F}$ é dito um *corpo totalmente complexo*, caso contrário $\mathbb{F}$ é dito ser *propriamente complexo*.

Ao par (r_1, r_2) de um corpo $\mathbb{F}$ chamamos de *assinatura* de $\mathbb{F}$. Seja (r_1, r_2) a assinatura de um corpo de números $\mathbb{F}$. Suponha que σ_j, para $j = 1, \ldots, r_1$, sejam mergulhos reais de $\mathbb{F}$ em $\mathbb{C}$, e σ_j, para $j = r_1 + 1, \ldots, r_1 + r_2$ os mergulhos complexos de $\mathbb{F}$ em $\mathbb{C}$ com $\overline{\sigma_{j+r_1}} = \sigma_{j+r_1+r_2}$.

Para estabelecer esta identificação consideraremos a aplicação estabelecida em (1), que realiza o mergulho dos elementos de um corpo de números $\mathbb{F}$ em $\mathbb{R}^n$, onde cada coordenada desta identificação em $\mathbb{R}^n$ é a imagem dos n distintos mergulhos associados ao corpo de números $\mathbb{F}$ aplicados num elemento de $\mathbb{F}$, isto é,

$$\sigma_{\mathbb{F}} : \mathbb{F} \longrightarrow \mathbb{R}^n$$

$$x \longrightarrow (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x) \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)). \tag{1}$$

Não é dificil mostrar que $\sigma_{\mathbb{F}}$ é um monomorfismo, que chamamos de *mergulho canônico* de $\mathbb{F}$ em $\mathbb{R}^n$.

Por outro lado, o anel de inteiros $\mathcal{D}_{\mathbb{F}}$ de um corpo de números $\mathbb{F}$ é um $\mathbb{Z}$-módulo livre com uma base integral do tipo $\beta = \{\omega_1, \ldots, \omega_n\}$.

Para cada $\omega_i \in \beta$, consideraremos os pontos $u_i = \sigma_{\mathbb{F}}(\omega_i)$, como mostrado em (2).

$$u_i = (\sigma_1(\omega_i), \ldots, \sigma_{r_1}(\omega_i), \Re\sigma_{r_1}(\omega_i), \Im\sigma_{r_1}(\omega_i), \ldots, \Re\sigma_{r_1+r_2}(\omega_i), \Im\sigma_{r_1+r_2}(\omega_i)), \tag{2}$$

Assim, $\sigma_{\mathbb{F}}(\beta) = \{u_1, \ldots, u_n\}$ será uma base para um reticulado Λ em $\mathbb{R}^n$. Avaliando $\sigma_{\mathbb{F}}$ em $y \in \mathcal{D}_{\mathbb{F}}$, onde $y = a_1\omega_1 + \cdots + a_n\omega_n$, e $a_1, \ldots, a_n \in \mathbb{Z}$, temos que

$$\sigma_{\mathbb{F}}(y) = a_1\sigma_{\mathbb{F}}(\omega_1) + \cdots + a_n\sigma_{\mathbb{F}}(\omega_n) = a_1u_1 + \cdots + a_nu_n.$$

O que torna a identificação completa.

Através do homomorfismo $\sigma_{\mathbb{F}}$ estamos exportando a estrutura aditiva de $\mathcal{D}_{\mathbb{F}}$ para o reticulado Λ, onde $\mathcal{D}_{\mathbb{F}}$ é o anel de inteiros de $\mathbb{F}$.

3.2 Reticulados em $\mathbb{R}^2$ identificados pelos anéis $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$

Nesta seção apresentaremos uma outra maneira natural de se fazer uma identificação dos anéis de inteiros em $\mathbb{R}^2$.

Considere os anéis de inteiros $\mathbb{Z}[\theta]$, provenientes das extensões quadráticas imaginárias $\mathbb{Q}(\sqrt{-m})$, para m inteiro positivo livre de quadrados. Neste sentido considere os recobrimentos de $\mathbb{R}^2$ por paralelogramos e/ou hexágonos. Através do Teorema 3.1 explicitamos uma maneira de indentificar vértices e centros destes polígonos por elementos dos anéis de inteiros.

Theorem 3.1 *Seja $\alpha_{(a,b)} = a + b\theta$ um elemento de um anel de inteiros $\mathbb{Z}[\theta]$ proveniente de uma extensão quadrática $\mathbb{Q}(\sqrt{-m})$, onde m é um inteiro positivo livre de quadrados. Temos dois casos a considerar:*

1) *Caso em que $-m \equiv 2, 3 \ mod\, 4$.*

Seja $\alpha_{(a,b)}$ o baricentro de um paralelogramo. Então, $\alpha_{(a+1,b)}$ e $\alpha_{(a-1,b)}$ são identificados como sendo os vértices opostos do paralelogramo cuja distância euclidiana de $\alpha_{(a,b)}$ vale 1, enquanto que $\alpha_{(a,b+1)}$ e $\alpha_{(a,b-1)}$ são identificados como sendo o par de vértices opostos do paralelogramo cuja distância euclidiana de $\alpha_{(a,b)}$ vale $\sqrt{m}$;

2) *Caso em que $-m \equiv 1 \ mod\, 4$.*

Seja $\alpha_{(a,b)}$ o baricentro de um hexágono. Então, $\alpha_{(a+1,b)}$ e $\alpha_{(a-1,b)}$ são identificados como sendo os vértices opostos de um hexágono cuja distância euclidiana de $\alpha_{(a,b)}$ vale 1, equanto que $\alpha_{(a-1,b+1)}$ e $\alpha_{(a+1,b-1)}$; e $\alpha_{(a,b-1)}$ e $\alpha_{(a,b+1)}$ são identificados como sendo os demais pares de vértices opostos do hexágono com distância euclidiana $\frac{\sqrt{m+1}}{2}$ de $\alpha_{(a,b)}$.

O Corolário 3.1 explicita como obter recobrimentos de $\mathbb{R}^2$ por polígonos cujos vértices e baricentros são identificados por elementos dos anéis de inteiros $\mathbb{Z}[\theta]$ provenientes das extensões quadráticas $\mathbb{Q}(\sqrt{-m})$, para $m > 0$.

Corollary 3.1 1) *O recobrimento de $\mathbb{R}^2$ por quadrados é obtido através da identificação dos vértices dos quadrados com os elementos do anel de inteiros de Gauss;*

Figure 1: Tessellation by squares

2) *O recobrimento de $\mathbb{R}^2$ por hexágonos regulares é obtido através da identificação dos vértices dos hexágonos com os elementos do anel de inteiros de Eisenstein-Jacobi.*

Figure 2: Tessellation by hexagons

Corollary 3.2 1) *O recobrimento de $\mathbb{R}^2$ por quadrados de área unitária é obtido através da identificação dos baricentros e vértices dos polígonos da tesselação descritos no Corolário 3.1 como baricentros dos quadrados unitários com os elementos do anel de inteiros de Gauss;*

2) *O recobrimento de $\mathbb{R}^2$ por hexágonos regulares de área mínima é obtido através da identificação dos baricentros e vértices dos hexágonos da tesselação do Corolário 3.1 como baricentros de hexágonos de área mínima com os elementos do anel de inteiros de Eisenstein-Jacobi.*

Vimos nesta seção que o reticulado obtido a partir da tesselação de quadrados de área unitária é identificado pelo anel $\mathbb{Z}[i]$.

Por outro lado, sabemos que associado a um reticulado existe uma forma quadrática. Como nesse caso o reticulado é o próprio $\mathbb{Z}[i]$ segue que a forma quadrática é $f(X,Y) = X^2 + Y^2$, que por sua vez é a norma relativa dos elementos de $\mathbb{Z}[i]$.

De maneira analoga mostra-se que a partir de uma tesselação de $\mathbb{R}^2$ obtida por hexágonos regulares, obtem-se um reticulado identificado com o anel de inteiros $\mathbb{Z}[\omega]$ e associado a este reticulado está a forma quadrática $g(X,Y) = X^2 + XY + Y^2$, que é a norma relativa dos elementos de $\mathbb{Z}[\omega]$.

4 Construção de Constelações Geometricamente Uniformes

Nesta seção apresentaremos procedimentos de construção de constelações de sinais geometricamente uniformes em $\mathbb{R}^2$ e $\mathbb{R}^n$. Em $\mathbb{R}^n$ faremos uso do Lemma de Kummer [13] e da proposta

de Interlando e Elia [12] de parametrização dos elementos de um anel de inteiros por pontos de $\mathbb{R}^n$. Em $\mathbb{R}^2$ usaremos a representatividade das potências de primos com relação às formas quadráticas provenientes das normas relativas dos anéis de inteiros.

4.1 Constelações geometricamente uniformes com p^m sinais em $\mathbb{R}^n$

Através das identificações dos anéis de inteiros provenientes de corpos de números no espaço $\mathbb{R}^n$, Interlando e Elia propuseram em [12] uma maneira de construir constelações de sinais de cardinalidade prima ou potência de primo com rótulos em corpos de Galois $GF(p^m)$ a partir dos quocientes dos anéis de inteiros $\mathcal{D}_{\mathbb{F}}$ por ideais primos.

Nesta seção veremos que é possível obter constelações de sinais de cardinalidade p^m rotulada não apenas para corpos de Galois $GF(p^m)$, mas também para p-grupos G_{p^m}, uma vez que as propostas anteriores de rotulamento de constelações de sinais [3], [8] e [12] só consideraram a estrutura aditiva do corpo para a efetivação do rotulamento.

A importância da proposta feita em [12] e a que proporemos neste trabalho em relação às propostas [3] e [8], é que elas são válidas para qualquer dimensão finita.

Considere um ideal I de um anel de inteiros $\mathcal{D}_{\mathbb{F}}$ do corpo de números $\mathbb{F}$. Considerando o mergulho do ideal como em (2), obtemos que $\sigma_{\mathcal{D}_{\mathbb{F}}}(I) \subseteq \mathbb{R}^n$ é um subreticulado de Λ.

Do fato de $\sigma_{\mathbb{F}} : \mathcal{D}_{\mathbb{F}} \longrightarrow \Lambda$ ser uma aplicação bijetiva, é possível definir a aplicação inversa, $\sigma_{\mathbb{F}}^{-1} : \Lambda \longrightarrow \mathcal{D}_{\mathbb{F}}$.

Apresentaremos o Lema de Kumer e uma definição que serão importantes para a realização do rotulamento.

Theorem 4.1 *[13] Seja $\mathcal{D}_{\mathbb{F}}$ o anel de inteiros do corpo de números $\mathbb{F} = \mathbb{Q}(\theta)$ e $p(X) \in \mathbb{Z}[X]$ o polinômio minimal de θ de grau n. Um ideal primo $\langle p \rangle$ de $\mathbb{Z}$ se decompõem em produto de ideais primos de $\mathcal{D}_{\mathbb{F}}$ da seguinte maneira: seja $\overline{p}(X) = \overline{p_1}(X)^{e_1} \ldots \overline{p_n}(X)^{e_s}$ a fatoração de $p(X)$ em polinômios mônicos irredutíveis de grau $f_i (1 \leq i \leq s)$ sobre $\mathbb{Z}_p[X]$ com $e_1 + \cdots + e_s = n$, onde a barra denota a classe de resíduos módulo p. Então $p\mathcal{D}_{\mathbb{F}}$ tem uma única fatoração $p\mathcal{D}_{\mathbb{F}} = \mathcal{P}_1^{e_1} \ldots \mathcal{P}_s^{e_s}$ como produto de potências de ideais primos em $\mathcal{D}_{\mathbb{F}}$, onde $\mathcal{P}_i = \langle p, p_i(\theta) \rangle$ e $\mathcal{D}_{\mathbb{F}}/\mathcal{P}_i \simeq GF(p^{f_i})$, para $1 \leq i \leq s$.*

Definition 4.1 *[12] Sejam $\mathbb{F} = \mathbb{Q}(\theta)$ um corpo de números de grau n com $\theta \in \mathcal{D}_{\mathbb{F}}$ e $\{\omega_1, \ldots, \omega_n\}$ uma base de $\mathbb{F}$ sobre $\mathbb{Q}$. Seja Λ um reticulado obtido a partir de $\mathcal{D}_{\mathbb{F}}$. Dado*

um número primo p e um inteiro positivo t, a aplicação $l : \Lambda \longrightarrow GF(p^t)$ é chamada de rotulamento linear se $l(\sigma(x_1\omega_1 + \ldots + x_n\omega_n)) = x_1 l(\sigma(\omega_1)) + \ldots + x_n l(\sigma(\omega_n))$, para quaisquer $x_i \in \mathbb{Z}$, com $1 \leq i \leq n$.

A Proposição 4.1 exibe de fato quem é o rotulamento.

Proposition 4.1 *[12] Seja φ um isomorfismo de $\mathcal{D}_\mathbb{F}/\mathcal{P}_i$ em $GF(p^{f_i})$. Seja pr a projeção de $\mathcal{D}_\mathbb{F}$ em $\mathcal{D}_\mathbb{F}/\mathcal{P}_i$. Então $l = \varphi(pr)\sigma^{-1}$ é o rotulamento linear de Λ em $GF(p^{f_i})$. Além disso, se $\mathcal{D}_\mathbb{F} = \mathbb{Z}[\theta]$, então l pode ser completamente especificado por $l(\sigma(\theta)) = \overline{\theta}$, onde $\overline{\theta}$ é a raiz do polinômio $p_i(x)$ sobre $GF(p)$.*

Como consequência da Proposição 4.1, fica claro o Corolário 4.1.

Corollary 4.1 *[12] Se α e γ são elementos de uma mesma classe lateral $\mathcal{P}_j$, então $l(\sigma(\alpha)) = l(\sigma(\gamma))$.*

Com o objetivo de estender o rotulamento proposto por Interlando e Elia em [12] para p-grupos com cardinalidade p^m é que consideraremos o próximo resultado.

Proposition 4.2 *[7] Seja $\mathcal{D}_\mathbb{F}$ o anel de inteiros do corpo de números $\mathbb{F} = \mathbb{Q}(\theta)$. Sob as mesmas condições do Teorema 4.1, para os casos em que um número primo p é fatorado em $\mathcal{D}_\mathbb{F}$, temos que os ideais primos de $\mathcal{D}_\mathbb{F}$, de norma p, são dados por $\mathcal{P}_i = \langle p, p_i(\theta)\rangle$ e que $\mathcal{D}_\mathbb{F}/\mathcal{P}_i \simeq GF(p^{f_i})$. Então existem ideais I em $\mathcal{D}_\mathbb{F}$, tais que $I \supset \mathcal{P}_i$ e $I = \mathcal{P}_i^n$, cuja norma do ideal vale p^m, e $\mathcal{D}_\mathbb{F}/I \simeq G_{p^m}$.*

O próximo passo é considerar uma definição mais geral de rotulamento que seja válida não apenas para corpos de Galois, mas também para p-grupos de cardinalidade p^m.

Definition 4.2 *[7] Seja $\mathbb{F} = \mathbb{Q}(\theta)$ um corpo de números de grau n, onde $\theta \in \mathcal{D}_\mathbb{F}$. Seja Λ um reticulado obtido de $\mathcal{D}_\mathbb{F}$. Dados um número primo p e um inteiro positivo t, uma aplicação $l : \Lambda \longrightarrow G_{p^t}$ é chamada de rotulamento linear se $l(\sigma(x_1\omega_1 + \ldots + x_n\omega_n)) = x_1 l(\sigma(\omega_1)) + \ldots + x_n l(\sigma(\omega_n))$, para quaisquer $x_i \in \mathbb{Z}$, com $1 \leq i \leq n$.*

4.2 Constelações geometricamente uniformes com p^m sinais em $\mathbb{R}^2$

As constelações geometricamente uniformes com p^m sinais que realizaremos em $\mathbb{R}^2$ são constituídas por representantes de classes laterais de energia mínima nos anéis $\mathbb{Z}[\theta]$ por meio de ideais I cuja norma é p^m para $\theta = i$ e $\theta = \omega$, respectivamente.

Para tal, consideraremos os casos em que os ideais I em $\mathbb{Z}[\theta]$ são primos.

Uma maneira de se obter ideais primos em $\mathbb{Z}[\theta]$ é analisar quem são os elementos irredutíveis nestes anéis. Com isso, é suficiente considerar I como sendo gerado por um destes elementos.

Por outro lado, é fato conhecido [10] que se um elemento de $\mathbb{Z}[\theta]$ possui norma relativa prima, então este elemento é irredutível no anel $\mathbb{Z}[\theta]$. Mas isto equivale a encontrar as soluções inteiras das formas quadráticas $h(X,Y) = p$ em $\mathbb{Z}[\theta]$. No caso $\mathbb{Z}[i], h(X,Y) = f(X,Y) = X^2 + Y^2$, e no caso $\mathbb{Z}[\omega], h(X,Y) = g(X,Y) = X^2 + XY + Y^2$. Se um par de inteiros a, b é uma solução de $h(a,b) = p$, então $\gamma = a + b\theta$ é irredutível em $\mathbb{Z}[\theta]$ e p é fatorado em $\mathbb{Z}[\theta]$, caso contrário, p não é fatorado em $\mathbb{Z}[\theta]$, e consequentemente irredutível no anel $\mathbb{Z}[\theta]$.

Denotaremos por $\mathcal{P}$ os ideais primos desses anéis. O quociente $\mathbb{Z}[\theta]/\mathcal{P}$ é um corpo, para $\theta = i, \omega$, quando $\mathcal{P} = \langle\gamma\rangle$ tiver norma igual a p e p é fatorável em $\mathbb{Z}[\theta]$, ou $\mathcal{P} = \langle p\rangle$ tiver norma igual a p^2 no caso em que p não é fatorado em $\mathbb{Z}[\theta]$.

Com o objetivo de caracterizarmos todas as constelações de sinais cujos representantes das classes laterais tenham cardinalidade potência de um primo, tomaremos os ideais I em $\mathbb{Z}[\theta]$ como potências dos ideais primos $\mathcal{P}$ em $\mathbb{Z}[\theta]$, o que permite a construção das constelações com p^n sinais a partir dos anéis quocientes $\mathbb{Z}[\theta]/\mathcal{P}$.

A partir deste procedimento estabeleceremos para quais números primos será possível obter constelações com p^m sinais em $\mathbb{Z}[i]$ e em $\mathbb{Z}[\omega]$ com estrutura de corpo ou apenas de grupo.

Como mostrado em [3] e [8] é possível construir constelações com p sinais, em $\mathbb{Z}[i]$ somente nos casos em que $p = 2$ ou $p = 4k + 1$, onde k é um inteiro positivo. No caso $\mathbb{Z}[\omega]$ também é possível construir constelações com p sinais, já no caso $\mathbb{Z}[\omega]$ ocorrerá para $p = 3$ ou para $p = 6k + 1$, para k inteiro positivo.

Proposition 4.3 1) *É possível construir constelações com p^2 sinais para qualquer número primo p, no caso $\mathbb{Z}[i]$.*

2) *É possível construir constelações com p^2 sinais para qualquer número primo em $\mathbb{Z}[\omega]$.*

Demonstração:

Caso 1

1-1) Para $p = 4k+1$, com $k \in \mathbb{Z}$, existe $\alpha = x+iy \in \mathbb{Z}[i]$, tal que $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = x^2+y^2 = p$. Logo, tomando $\alpha^2 = (x+iy)^2 = (x^2+y^2)+i(2xy)$, tem-se que $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha^2) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha)N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = p.p = p^2$.

O ideal I tomado em $\mathbb{Z}[i]$ neste caso é $I = \langle \alpha^2 \rangle$.

1-2) Para $p = 4k+3$, com $k \in \mathbb{Z}$, basta escolher $\alpha = p$, pois $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(p) = p.p = p^2$. O ideal I em $\mathbb{Z}[i]$, considerado neste caso, é $I = \langle p \rangle$.

Caso 2 Considere $\alpha = p(1-\omega)$ para cada número primo p, uma vez que é imediata a verificação $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(p)N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(1-\omega) = p^2.1 = p^2$. O ideal I em $\mathbb{Z}[\omega]$, neste caso, é $I = \langle p(1-\omega) \rangle$.

Quanto ao grupo de rótulos do quociente a ser tomado, temos dois casos a considerar:

2-1) Para $p = 6k+1$, com $k \in \mathbb{Z}$, existe $\alpha = x+\omega y \in \mathbb{Z}[\omega]$, tal que $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha) = x^2+3y^2 = p$. Neste caso o ideal I tomado em $\mathbb{Z}[\omega]$ é $I = \langle \alpha^2 \rangle$.

2-2) Para $p \neq 6k+1$, com $k \in \mathbb{Z}$, basta escolher $\alpha = p$, pois $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(p) = p.p = p^2$. O ideal I em $\mathbb{Z}[\omega]$, considerado neste caso, é $I = \langle p \rangle$.

Proposition 4.4 *Em $\mathbb{Z}[i]$, é possível construir constelações com p^m sinais para qualquer número primo p da forma $p = 4k+1$. Para os números primos da forma $p = 4k+3$ é possível construir constelações com p^m sinais nos casos em que $n = 2k$, para k inteiro.*

Demonstração:

1) No caso em que $p = 4k+1$, com $k \in \mathbb{Z}$, existe $\alpha = x+iy \in \mathbb{Z}[i]$, tal que $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = x^2+y^2 = p$. Tomando $\gamma = \alpha^n$, temos que $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\gamma) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha^n) = p^n$. Neste caso o ideal I em $\mathbb{Z}[i]$, será dado por $I = \langle \alpha^n \rangle$.

2) Caso em que $p = 4k+3$, com $k \in \mathbb{Z}$. Da Proposição 4.3, com $p = 4k+3$, seja $\alpha = p$, então $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(p) = p.p = p^2$. Tomando $\gamma = \alpha^k$, sua norma será

$N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\gamma) = N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\alpha^k) = (p^2)^k$. Neste caso o ideal I em $\mathbb{Z}[i]$, é dado por $I = \langle \alpha^k \rangle$.

Proposition 4.5 *É possível construir constelações com p^m sinais em $\mathbb{Z}[\omega]$ para qualquer número primo da forma $p = 6k+1$. Para os números primos $p \neq 6k+1$ é possível construir constelações de p^m sinais somente para nos casos em que $m = 2k$.*

Demonstração:

1) Caso em que p é fatorável em $\mathbb{Z}[\omega]$ existe $\alpha \in \mathbb{Z}[\omega]$ tal que $p = \alpha.\overline{\alpha}$. Neste caso, $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha) = p$. Logo, tomando-se $\gamma = \alpha^m$, sua norma será $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\gamma) = N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\alpha^n) = p^m$. Neste caso, o ideal I em $\mathbb{Z}[\omega]$ é dado por $I = \langle \gamma \rangle$.

2) Caso em que p não é fatorável em $\mathbb{Z}[\omega]$. Neste caso para os valores de $m = 2k$, com k inteiro, basta que tomemos $\gamma = p^k(1-\omega)$, que teremos $N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\gamma) = N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(p^k) N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(1-\omega) = p^{2k}.1 = p^m$ Basta tomar o ideal I em $\mathbb{Z}[\omega]$, dado por $I = \langle \gamma \rangle$.

5 Rotulamento Casado de Constelações em $\mathbb{R}^n$ e em $\mathbb{R}^2$

Nesta seção iremos apresentar algumas constelações de sinais, cujos sinais são rotulados pelos elementos do grupo aditivo de $GF(p^m)$ e por p-grupos elementos de G_{p^m} em espaços de dimensão maior do que 2.

Example 5.1 *Considere $\mathbb{F} = \mathbb{Q}(\alpha)$, onde α é a raiz complexa do polinômio minimal $p(X) = X^3 - X + 1$. O anel de inteiros é $\mathcal{D}_{\mathbb{F}} = \mathbb{Z}[\alpha]$ com uma base integral $\beta = \{1, \alpha, -1 + \alpha^2\}$. Tomando $p(X)$ módulo 11, obtemos $p(X) = (X-5)(X^2+5X+2)(mod 11\mathbb{Z}[X])$, onde o polinômio do segundo grau é irredutível sobre $\mathbb{Z}_{11}$. Assim,*

i)

$$11\mathbb{Z}[\alpha] = \mathcal{P}_1\mathcal{P}_2,$$

onde $\mathcal{P}_1 = \langle 11, \alpha - 5 \rangle$ e $\mathcal{P}_2 = \langle 11, \alpha^2 - 6\alpha - 9 \rangle$. Temos que $\mathbb{Z}[\alpha]/\mathcal{P}_1 \simeq GF(11)$, e portanto, $\alpha \equiv 5(mod \mathcal{P}_1)$.

A função de rotulamento é $l(\sigma(X_0 + X_1\alpha + X_2(-1+\alpha^2)(mod 11\mathbb{Z}[X]) = X_0 + 5X_1 + 3X_2, \forall X_i \in \mathbb{Z}$, com $0 \leq i \leq 2$.

ii) *Considere o ideal* $I = \mathcal{P}_1^2$ *de norma* 121. *Então* $\mathbb{Z}[\alpha]/I \simeq G_{121}$, *e portanto,* $\alpha \equiv 5(modI)$.

A função de rotulamento é $l(\sigma(x_0 + x_1\alpha + x_2(-1+\alpha^2)(mod121\mathbb{Z}[X]) = x_0 + 5x_1 + 24x_2, \forall x_i \in \mathbb{Z}$, *com* $0 \leq i \leq 2$.

Example 5.2 *Consideraremos o mesmo corpo de números e anel de anteiros do Exemplo 5.1. Tomando* $p(X)$ *módulo* 3, *temos que* $p(X)$ *não é fatorável sobre* $\mathbb{Z}_3[X]$, *ou seja,* $p(X)$ *é irredutível no anel de polinômios* $\mathbb{Z}_3[X]$. *Logo, tomando o quociente* $\mathbb{Z}_3[X]/\mathcal{P} \simeq GF(27)$, *equivalentemente, temos que o ideal* $\mathcal{P}$ *faz parte da fatoração de* $27\mathbb{Z}[\alpha]$ *e temos que,* $\mathbb{Z}[\alpha]/\mathcal{P} \simeq GF(27)$. *Logo, existe um elemento* $\beta \in GF(27)$ *que é raiz de* $p(X) = X^3 - X + 1 \in \mathbb{Z}_3[X]$. *Assim, a função de rotulamento é* $l(\sigma(X_0 + X_1\alpha + X_2(-1+\alpha^2)(mod27\mathbb{Z}[X]) = X_0 + \beta X_1 + (-1+\beta)X_2, \forall X_i \in \mathbb{Z}$, *com* $0 \leq i \leq 2$.

Example 5.3 *Considere* $\mathbb{F} = \mathbb{Q}(\alpha)$, *onde* α *é a raiz complexa do polinômio minimal* $p(X) = X^4+X^3+X^2+X+1$. *O anel de inteiros é* $\mathcal{D}_{\mathbb{F}} = \mathbb{Z}[\alpha]$ *com uma base integral* $\beta = \left\{1, \alpha, \alpha^2, \alpha^3\right\}$. *Tomando* $p(X)$ *módulo* 11, *obtemos* $p(X) = (X-3)(X-4)(X-5)(X-9)(mod11\mathbb{Z}[X])$. *Assim,*

i)

$$11\mathbb{Z}[\alpha] = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4,$$

onde $\mathcal{P}_1 = \langle 11, \alpha - 3\rangle, \mathcal{P}_2 = \langle 11, \alpha - 4\rangle, \mathcal{P}_3 = \langle 11, \alpha - 5\rangle, \mathcal{P}_4 = \langle 11, \alpha - 9\rangle$. *Logo,* $\mathbb{Z}[\alpha]/\mathcal{P}_1 \simeq GF(11)$, *e portanto,* $\alpha \equiv 3(mod\mathcal{P}_1)$.

A função de rotulamento é $l(\sigma(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3(mod11\mathbb{Z}[X]) = x_0 + 3x_1 + 9x_2 + 5x_3, \forall x_i \in \mathbb{Z}$, *com* $0 \leq i \leq 3$.

ii) *Considere o ideal* $I = \mathcal{P}_1^2$ *de norma* 121. *Temos que* $\mathbb{Z}[\alpha]/I \simeq G_{121}$, *e* $\alpha \equiv 3(modI)$.

A função de rotulamento é $l(\sigma(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3(mod121\mathbb{Z}[X]) = x_0 + 3x_1 + 9x_2 + 27x_3, \forall x_i \in \mathbb{Z}$, *com* $0 \leq i \leq 2$.

Denotaremos por $\mathcal{A}_{p^m}[\omega]$ as constelações com p^m sinais em $\mathbb{Z}[\omega]$ e por $\mathcal{A}_{p^m}[i]$ as constelações com p^m sinais em $\mathbb{Z}[i]$ em $\mathbb{R}^2$. O algoritmo que estabelecerá o rotulamento casado destas constelações de sinais à estrutura algébrica proveniente do quociente $\mathbb{Z}[\theta]/I$ é um caso particular daquele proposto na Definição 4.1.

Os passos do algoritmo que irá realizar o rotulamento casado do conjunto de sinais ao correspondente grupo são descritos a seguir.

Algoritmo de Rotulamento Casado a uma Estrutura Algébrica em $\mathbb{R}^2$

Passo 1 Considere $\gamma \in \mathbb{Z}[\theta]$ da forma $\gamma = a + b\theta$, cuja norma é $N(\gamma) = p^m$;

Passo 2 Seja $r \in \mathbb{Z}$ a única solução (em s) da equação $a+bs \equiv 0 \; mod\, p^m$, onde $0 \leq s \leq p^m - 1$;

Passo 3 Um elemento $l \in G$ (G um grupo com p^n elementos), é um rótulo do ponto $x + y\theta \in \mathbb{Z}[\theta]$ se $x + yr \equiv l \; mod\, p^m$.

Example 5.4 *Considere* $25 = (5-5w)(5+5w)$. *Seja* I *o ideal primo gerado por* $I = \langle 5 - 5w \rangle$. *Então,* $r = -4$ *é solução inteira de* $5 - s5 = 25$. *Com isso, o rótulo do elemento* $x + yw$ *em* $\mathbb{Z}[w]$ *é obtido de* $x - 4y \equiv l \; mod\, 25$ *como sendo o elemento do corpo* $GF(25)$.

Example 5.5 *Considere* $25 = (4 + 3i)(4 - 3i)$. *Seja* I *o ideal primo gerado por* $I = \langle 4 - 3i \rangle$. *Então,* $r = -7$ *é solução inteira de* $4 - s3 = 25$. *Com isso, o rotulo do elemento* $x + yi$ *em* $\mathbb{Z}[i]$ *é obtido de* $x - 7y \equiv l \; mod\, 25$ *como sendo o elemento do grupo* G_{25}.

Example 5.6 *Considere* $49 = 7.7 = (-7i)(7i)$. *Seja* $I = \langle -7i \rangle$. *Então,* $r = -7$ *é solução inteira de* $-s7 = 49$. *Com isso, o rótulo do elemento* $x + yi$ *em* $\mathbb{Z}[i]$ *é obtido de* $x - 7y \equiv l \; mod\, 49$ *como sendo o elemento do grupo aditivo do corpo* $GF(49)$.

A Figura 3 ilustra as constelações de sinais $A_{25}[i]$ e $A_{25}[\omega]$ de energia mínima, cujos sinais são rotulados pelos elementos do grupo aditivo G_{25} e pelos elementos do grupo aditivo do corpo $GF(25)$, respectivamente.

Figure 3: Signal constellations

6 Conclusões

Neste trabalho estendemos as propostas de Huber [3], Favareto et.al [8] e Interlando e Elia [12] de construção de constelações de sinais geometricamente uniformes cujos sinais podem ser rotulados por elementos do corpo de Galois $GF(p)$; ou por elementos do corpo de Galois

$GF(p^m)$, a partir de espaços de sinais identificados pelos elementos dos anéis de inteiros em $\mathbb{R}^2$ e $\mathbb{R}^n$, respectivamente.

Em $\mathbb{R}^2$, vimos que em função da representatividade de números da forma p^m, pelas formas quadráticas $f(X,Y) = X^2 + Y^2 = p^m$ e $g(X,Y) = X^2 + XY + Y^2 = p^m$ fornecemos resposta quando é possível obter constelações de p^m sinais nos espaços de sinais identificados pelos anéis de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente.

Mostramos que os grupos de rótulos casados às constelações com p^m sinais, são dados por corpos de Galois $GF(p^m)$ somente, para casos em que $m = 1$ e $m = 2$,e podendo ser dados por p-grupos G_{p^2} dependendo da congruência de um inteiro primo p módulo 4 ou módulo 6 no anel de inteiro dos $\mathbb{Z}[i]$ ou $\mathbb{Z}[\omega]$, respectivamente, e nos casos em que $m > 2$, os grupos de rótulos são dados somente por p-grupos G_{p^m}.

Em $\mathbb{R}^n$, a exemplo que mostramos no caso $\mathbb{R}^2$, o grupo de rótulos das constelações de p^m sinais que podem ser construídas são dados por corpos de Galois $GF(p^m)$ somente, para casos em que $m \leq n$, onde n é a dimensão de $\mathbb{R}^n$ vista como um espaço vetorial sobre $\mathbb{R}$, e podendo ser dados por p-grupos G_{p^m}; nos casos em que $m \leq n$, dependerá se o ideal considerado no anel de inteiros para o anel quociente tenha cardinalidade p^m seja primo ou não, para os casos em que $m > n$, os grupos de rótulos são dados somente por p-grupos G_{p^m}.

References

[1] G.D. Forney, "Geometrically uniform codes" *IEEE Trans. Inform. Theory*, vol.37,No.6 pp. 1241-1259, Set. 1991.

[2] H.A. Loeliger, "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol.37,No.6, pp. 1675-1682, Nov. 1991.

[3] K. Huber, "Codes over gaussian integers," *IEEE Trans. Inform. Theory*, vol.IT-40, pp. 207-216, Jan. 1994.

[4] R.G. Egri, e F.A. Horrigan, "A finite group of complex integers and its application to differentially coherent detection of QAM signals," *IEEE Trans. Inform. Theory*, vol.IT-40, pp. 216-219, Jan. 1994.

[5] J. Rifa, "Groups of complex integers used as QAM signals," *IEEE Trans. Inform. Theory*, vol.IT-41, pp. 1512-1517, Sept. 1995.

[6] O. Endler, *Teoria dos Números Algébricos*, Projeto Euclides, 1986.

[7] E.D.Carvalho, *Construção e Rotulamento de Constelações de Sinais Geometricamente Uniformes em Espaços Euclidianos e Hiperbólicos*, Tese de Doutorado, FECC-UNICAMP, 2001.

[8] T.P.Nobrega Neto, J.C.Interlando, O.M. Favareto, M.Elia e R.Palazzo Jr "Lattice constellations and codes from quadratic number fields', *IEEE Trans. Inform. Theory*, vol.47, pp. 1514-1527, May 2001.

[9] J. Rotman, *Galois Theory*, New York: Springer-Verlag, 1990.

[10] T.Y. Lam, *The Algebraic Theory of Quadratic Forms*, New York: Benjamim, 1963.

[11] X.D. Dong, and C.B. Soh "Group of algebric interger used for coding QAM signal" *IEEE Trans. Inform. Theory*, vol.44,No.5 pp. 1848-1860, Set. 1998.

[12] J.C.Interlando , e Michele Elia, "On the linear labeling of lattice constellations from algebraic numbers fields", *Combinatorics '2000 Gaeta, Italy, pp 181*

[13] M.Phost, e H.Zassenhaus *Algorithmic Algebraic Numbers Theory*, Cambridge University, 1989.