Universidade Estadual de Campinas

Faculdade de Engenharia Elétrica e de Computação

Departamento de Telemática

Construção e Rotulamento de Constelações de Sinais Geometricamente Uniformes em Espaços Euclidianos e Hiperbólicos

Tese de Doutorado

Autor: **Edson Donizete de Carvalho**

Orientador: **Prof. Dr. Reginaldo Palazzo Jr.**

Co-orientador: **Prof. Dr. Marcelo Firer**

Banca Examinadora:

Prof. Dr. Reginaldo Palazzo Jr. - FEEC/UNICAMP

Prof. Dr. Henrique Lazari - IGCE/UNESP

Prof. Dr. José Carmelo Interlando-IBILCE/UNESP

Prof. Dr. Trajano Pires Nóbrega Neto - IBILCE/UNESP

Prof. Dr. Osvaldo Germano Rocio - CCE/UEM

Tese submetida à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, para preenchimento dos pré-requisitos parciais para obtenção do Título de Doutor em Engenharia Elétrica.

06 de Dezembro de 2001

Resumo

Neste trabalho fornecemos técnicas para a geração de alfabetos de códigos corretores de erros dotados de uma estrutura algébrica, a partir de constelações de sinais geometricamente uniformes, cujos sinais sejam rotulados por elementos de um p-grupo G_{p^m} e por elementos de um corpo de Galois $GF(p^m)$ em espaços de sinais euclidianos identificados por elementos de um anel de inteiros e em espaços de sinais no plano hiperbólico identificados por elementos de uma ordem dos quatérnios.

Abstract

In this work we propose procedures for the generation of alphabet of error correcting codes having the structure of a group from geometric uniform lattice constellations. The signals a constellations are labeled by elements of a p-group G_{p^m} or by elements of a Galois field $GF(p^m)$. In the Euclidean space the signals are identified by the elements of a ring of integers. In the hyperbolic plane the signals are identified by the elements of a quaternion order.

Orgão Financiador

Trabalho financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico-CNPq, Processo No. 95/4720-8.

Agradecimentos

Em primeiro lugar agradeço a Deus pela concretização de mais esta etapa em minha vida.

De maneira especial gostaria de agradecer aos professores Reginaldo Palazzo Jr e Marcelo Firer. Ao professor Reginaldo Palazzo Jr pela competente e segura orientação e pelo constante incentivo e amizade.

Ao professor Marcelo Firer pelas construtivas críticas e sugestões apresentadas, prestatividade e a amizade.

Aos meus pais e irmãos Isabel, Elias e Carlos pelo carinho e a confiança que sempre me transmitiram, nos momentos mais difíceis de minha vida acadêmica.

De maneira particular agradeço a Iara pela paciência que teve comigo durante o periodo de Doutorado.

Aos amigos de Doutorado pelo incentivo e companherismo, de maneira particular, ao João de Deus, Diogo, Rodrigo, Alessandro, Givaldo, Martinho, Mário, Aido, Osmar e o Marinaldo.

E aos amigos: Escobar, Júnior, Erico, Daniel, Eduardo, José Carlos, Fabiano, Maurício, Helmann.

Aos colegas do DT.

E ao CNPq pelo financiamento deste trabalho.

Dedico este trabalho aos meus pais João Luciano e Maria Aparecida.

Sumário

Lista de Figuras

Lista de Símbolos

(V, B):	espaço quadrático
Γ_{4g}:	grupo fuchsiano associado ao polígono hiperbólico F_{4g}
Γ_I:	subgrupo normal de um grupo fuchsiano
Λ:	reticulado
$\{4g, 4g\}$:	tesselação de $4g$ polígonos no plano hiperbólico
ω:	raiz sexta da unidade
σ:	automorfismo de corpos
θ:	elemento primitivo de uma extensão de corpos
$b(\Lambda)$:	invariante de Brant
D_f:	conjunto de valores da forma quadrática f
d_H:	métrica de Hamming
d_L:	métrica de Lee
$f(X_1, \ldots, X_n)$:	forma quadrática de dimensão n
F_{4g}:	polígono hiperbólico de $4g$ lados
G:	grupo
$G(\Lambda)$:	fecho de Gorenstein

G_{p^n}: grupo de cardinalidade p^n

$GF(p^n)$: corpo de Galois de cardinalidade p^n

I: ideal

i: raiz quarta da unidade

$I(T)$: círculo isométrico

$Nrd(x)$: norma reduzida em uma álgebra dos quatérnios

$p(x)$: polinômio minimal

R: anel

$Trd(x)$: traço reduzida em uma álgebra dos quatérnios

$\mathcal{O}^1$: ordem dos quatérnios de norma unitária

$\mathcal{P}$: ideal primo

Capítulo 1

Introdução

A demanda por sistemas de comunicações que operem com taxas de transmissão e capacidade de armazenamento altas requer que a confiabilidade também seja alta. Este paradigma poderá ser alcançado através da proposição de novos códigos corretores de erros com parâmetros (n, k, d), onde n denota o comprimento da palavra código, k o número de dígitos de informação e d a distância mínima, de tal forma que assintoticamente satisfaçam as características exigidas pelos usuários.

Como as palavras-código de um código são sequências finitas de símbolos pertencentes a um alfabeto, então o procedimento mais eficiente de composição na formação dessas seqüências é aquele em que os símbolos do alfabeto são identificados por elementos de um conjunto contendo uma estrutura algébrica.

Um procedimento natural de se realizar esta identificação é através de uma aplicação injetora de um subconjunto finito de pontos (**constelação de sinais**) de um espaço de sinais em uma estrutura algébrica, ou equivalentemente, a determinação da representação geométrica associada à estrutura algébrica resultando com isso na caracterização geométrica e algébrica do alfabeto do código.

Com o objetivo de redução da complexidade de demodulação/decodificação a representação geométrica mais adequada é aquela decorrente da ação transitiva de um grupo no conjunto de sinais. Quando tal situação ocorre dizemos que a constelação de sinais é **geometricamente uniforme**. Estes conjuntos de sinais, cujos elementos são representantes de classes laterais de

energia mínima no espaço de sinais, dão origem aos alfabetos dos **códigos geometricamente uniformes**, Forney [1].

Huber em [3], utilizou como alfabeto para um código de bloco elementos de um corpo de Galois obtidos através das classes laterais do anel de inteiros de Gauss módulo ideais primos.

Em [4], Egri e Horrigan utilizaram um grupo multiplicativo finito de inteiros de Gauss para uso em detecção diferencial, a partir de uma constelação de sinais 16-QAM proveniente de um espaço de sinais euclidiano bidimensional. Em [5], Rifà caracterizou algebricamente a proposta apresentada por Egri e Horrigan estendendo-a para os grupos das unidades, G'_{2^n}, do grupo multiplicativo G_{2^n} de cardinalidade 2^n em um anel de inteiros de Gauss. Dong e Soh [35] estenderam a proposta apresentada por Rifà para subgrupos obtidos a partir dos grupos multiplicativos provenientes dos anéis quocientes $\mathbb{Z}[i]/(p^n)$ e $\mathbb{Z}[\omega]/(p^n)$, para p primo ímpar de cardinalidade $4p^{2n-2}$ e $6p^{2n-2}$, respectivamente.

Em [19] e [24] Favareto et.al propuseram um procedimento geral de construção de constelações de sinais a partir da proposta apresentada por Huber em que os sinais são rotulados por elementos de um corpo de Galois $GF(p)$. Interlando e Elia [37] estenderam o procedimento de Favareto e et.al de rotulamento de constelações de sinais por elementos dos corpos de Galois $GF(p)$ para corpos de Galois $GF(p^m)$, em espaços de sinais euclidianos de dimensão finita. Mostraremos que a proposta de Interlando e Elia de rotulamento de sinais por elementos de uma estrutura algébrica para as constelações de sinais com p^m sinais nos espaços de sinais de dimensão finita se estende a p-grupos G_{p^m}.

Lazari [22] propos a construção de constelações de sinais geometricamente uniformes no plano hiperbólico através do processo de construção de cadeias de partições geometricamente uniformes a partir do grupo de isometrias do octógono F_8, **domínio fundamental** da tesselação $\{8,8\}$, e do grupo de isometrias do p-ágono da tesselação $\{p,3\}$.

Um dos objetivos deste trabalho está relacionado com a construção de constelações de sinais no plano hiperbólico como sendo formado pelos baricentros dos octógonos da tesselação $\{8,8\}$ e dos baricentros de dodecágonos da tesselação $\{12,12\}$ que tenham como identificação elementos das ordens dos quatérnios $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ e $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$, respectivamente.

Tais constelações contém p^m sinais e estão associadas aos ideais $\mathcal{O}_{\mathbb{Z}[I]}$ de cardinalidade p^m nas ordens dos quatérnios $\mathcal{O}_{\mathbb{Z}[\theta]}$ para os casos em que $\theta = \sqrt{2}, \sqrt{3}$. Como conseqüência desta associação, os sinais serão rotulados pelos elementos do grupo G resultante do anel quociente $\mathcal{O}_{\mathbb{Z}[\theta]}/\mathcal{O}_{\mathbb{Z}[I]}$.

Este trabalho estará dividido da seguinte forma.

No Capítulo 2, apresentaremos uma revisão dos conceitos de álgebra e geometria necessários para compreensão do texto. Em álgebra revisaremos os conceitos de corpos de números, ideais, grupos de Galois, anéis de inteiros. Em geometria abordaremos os conceitos de espaços métricos, espaços hiperbólicos, grupos fuchsianos, e as tesselações regulares no plano hiperbólico. Encerrando o capítulo abordaremos as constelações de sinais.

No Capítulo 3 iremos considerar algumas propriedades relativas ás formas quadráticas de interesse ao trabalho em consideração. Veremos que existe uma associação entre reticulados e formas quadráticas, possibilitando que o estudo de equivalência de reticulados seja realizado através da equivalência de formas quadráticas. Mostraremos que a **isotropia** de uma forma quadrática constituirá em um **invariante geométrico** nas formas quadráticas de dimensão 2 quanto a caracterização da geometria a que o reticulado associado estará inserido.

No Capítulo 4, proporemos a construção de constelações com p^m sinais, cujos sinais são rotulados por elementos de um p-grupo G_{p^m} ou por elementos de um corpo de Galois $GF(p^m)$ em espaços de sinais euclidianos identificados pelos elementos de um anel de inteiros $\mathcal{D}_{\mathbb{F}}$ proveniente de um corpo de números $\mathbb{F}$.

Para tal, consideraremos ideais I em $\mathcal{D}_{\mathbb{F}}$ de índice p^m. O grupo G resultante do anel quociente de $\mathcal{D}_{\mathbb{F}}$ módulo o ideal I, será o grupo que usaremos para rotular os sinais destas constelações. Caso I seja um ideal primo em $\mathcal{D}_{\mathbb{F}}$, teremos que G será um corpo de Galois $GF(p^m)$, caso contrário, G será um p-grupo aditivo G_{p^m}. As funções de rotulamento serão apresentadas através de exemplos de constelações de sinais geometricamente uniformes de p^m sinais em espaços de dimensão $2, 3$ e 4.

No Capítulo 5, forneceremos um procedimento para determinar as transformações geradoras de um grupo fuchsiano Γ_{4g} associado a um domínio fundamental F_{4g} de uma tesselação

$\{4g, 4g\}$, através de um particular emparelhamento de arestas em F_{4g}, como conseqüência a presentação de Γ_{4g} será apresentada.

Faremos um estudo das álgebras dos quatérnios e dos correspondentes reticulados os quais serão denominadas de **ordem dos quatérnios**. Apresentaremos a identificação de uma ordem dos quaténios em um grupo fuchsiano aritmético como proposto por Johansson [11].

Recipocramente, mostraremos que é possível identificar específicos grupos fuchsianos aritméticos com as ordens dos quatérnios, como é o caso de determinados grupos Γ_{4g}, na qual associaremos seus elementos por elementos de uma ordem dos quaténios $\mathcal{O}_{\mathbb{Z}[\theta]}$, onde $\mathbb{Z}[\theta]$ é o anel de inteiros de um corpo totalmente real $\mathbb{Q}(\sqrt{m})$, para $m \in \mathbb{Z}$.

Sob estas condições forneceremos um procedimento de determinação de subgrupos normais Γ_I no grupo fuchsiano aritmético Γ_{4g} através da procura de ideais $\mathcal{O}_{\mathbb{Z}[I]}$ de cardinalidade p^m na ordem dos quatérnios $\mathcal{O}_{\mathbb{Z}[\theta]}$, uma vez que estes ideais correspondem a subgrupos normais Γ_I.

Tais subgrupos normais Γ_I garantirão a existência das constelações de p^m sinais e mais do que isso, que as mesmas são geometricamente uniformes no plano hiperbólico. Tais constelações são formadas pelo espaço das órbitas do sinal dado pelo baricentro do domínio fundamental F_{4g}.

Mostraremos que esses conjuntos de sinais admitem uma decomposição em partições geometricamente uniformes, ou seja, existirá um grupo rótulos para os conjuntos de sinais em consideração.

Com isso, ficará estabelecida a existência de um alfabeto para a construção de códigos corretores de erros a partir dos procedimentos considerados neste capítulo.

Capítulo 2

Revisão de Conceitos

2.1 Introdução

Neste trabalho apresentaremos técnicas de geração de alfabetos para códigos corretores de erros em espaços euclidianos e hiperbólicos. O que se tem mostrado mais eficiente neste processo é quando este alfabeto apresenta uma estrutura algébrica. Por outro lado, um código possui uma capacidade de deteção e correção de erros que depende da distância mínima dentre as palavras-códigos, ou seja, inerente a um código existe associado um espaço métrico. Esta característica geométrica está relacionada com a forma combinada de codificação e modulação. Todavia, é através da constelação de sinais (um subconjunto finito de pontos de um espaço métrico) que os elementos do alfabeto do código são identificados por elementos de uma estrutura algébrica. Para estabelecer tais condições, estaremos neste capítulo fazendo uma revisão de conceitos de álgebra abstrata, geometria e constelações de sinais. Em álgebra revisaremos os conceitos de grupos, anéis, ideais, corpos de números, módulos, norma de ideais e grupo de Galois.

Em geometria, revisaremos os conceitos de espaços métricos, domínio fundamental, tesselações hiperbólicas e grupos de simetrias de polígonos hiperbólicos (grupos fuchsianos). No final do capítulo, apresentaremos as constelações de sinais, que é o elo de ligação entre as componentes algébricas e geométricas no processo.

2.2 Revisão de Álgebra

Nesta seção revisaremos os conceitos básicos de álgebra que consideramos necessário para compreensão do texto, cujos resultados podem ser encontrados em livros de álgebra abstrata, [15] e [20].

Dizemos que um conjunto G, não vazio, possui uma estrutura de **grupo**, se para uma operação $*$, definida no conjunto G, forem satisfeitas as sequintes propriedades :

i) Associativa, isto é, $a*(b*c) = (a*b)*c$, para todo a, b e $c \in G$.

ii) A existência de um elemento neutro para a operação em G, isto é, $a*e = a = e*a$, para todo $a \in G$.

iii) A existência de um elemento inverso para cada elemento em G, isto é, $\forall a \in G$, existe um elemento $a^{-*} \in G$, tal que $a*a^{-*} = e = a^{-*}*a$.

Ao longo deste trabalho utilizaremos as operações de grupo aditiva e multiplicativa, denotadas por $(G, +)$ e $(G, .)$.

Se G for um grupo aditivo, e se para uma segunda operação (denominada multiplicativa) forem verificadas as propriedades v) e vii).

iv) A propriedade distributiva da multiplicação com relação a adição a esquerda, isto é $a.(b+c) = ac + bc$, para todos a, b e $c \in G$.

v) A propriedade distributiva da multiplicação com relação a adição a direita, isto é $(b+c)a = ba + ca$, para todos a, b e $c \in G$.

vi) A propriedade associativa, isto é $a.(b.c) = (a.b).c$, para todos a, b e $c \in G$.

Diremos que o grupo G nestas condições é um **anel**. Denotamos o este anel por $(A, +, .)$.

vii) A propriedade comutativa da multiplicação, $ab = ba$, para todos $a, b \in A$. Caso a propriedade vii) seja satisfeita, diremos A, é um **anel comutativo**.

No caso de A ser um grupo aditivo e $A - \{0\}$ for um grupo multiplicativo, e além disso forem verificadas as propriedades iv) a vi) diremos que A é um **corpo**.

Os subanéis I de interesse são os que possuem uma estrutura de **ideal** em um anel comutativo A, isto é, para quaisquer $a \in A$ e $x \in I$ verifica-se que $ax \in I$.

Um ideal $\mathcal{P}$ em um anel comutativo A é chamado de ideal **primo**, se $\mathcal{P} \neq A$, e se para quaisquer $a, b \in A$ for verificada a condição de que $ab \in \mathcal{P}$ implicar em $a \in \mathcal{P}$ ou $b \in \mathcal{P}$.

Já um ideal $\mathcal{M}$ em um anel comutativo A, é dito ser **maximal**, se $\mathcal{M} \neq A$ e os únicos ideais em A, que contém $\mathcal{M}$, são A e $\mathcal{M}$.

Uma aplicação φ definida entre dois grupos $(G, *)$ e $(G', \circ)$,

$$\varphi : G \longrightarrow G'$$

tal que $\varphi(a * b) = \varphi(a) \circ \varphi(b), \forall a, b \in G$, é chamada de **homomorfismo** de G em G'. Caso esta aplicação seja bijetiva, diremos que φ é um **isomorfismo**. Se $(G, *) = (G', \circ)$, e φ é isomorfismo diremos que φ é um **automorfismo**. Definições análogas valem para anéis e corpos.

2.2.1 Teoria dos números algébricos

Sejam $\mathbb{E}$ e $\mathbb{F}$ subcorpos do corpo $\mathbb{C}$ dos complexos. Caso $\mathbb{E}$ seja um subcorpo de $\mathbb{F}$, dizemos que $\mathbb{F}$ é uma extensão do corpo $\mathbb{E}$, e escrevemos esta extensão por $\mathbb{F}/\mathbb{E}$. A dimensão de $\mathbb{F}$ vista como espaço vetorial sobre $\mathbb{E}$ é chamado de grau de $\mathbb{F}$ sobre $\mathbb{E}$ e é denotado por $[\mathbb{F} : \mathbb{E}]$.

Consideremos $p(X)$ 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 $p(X)$ e $\mathbb{E}$.

Chamamos de **número algébrico** qualquer elemento $\alpha \in \mathbb{C}$ que é raiz de algum polinômio $p(X) \neq 0$ sobre $\mathbb{Q}$. Podemos e iremos sempre considerar $p(X)$ mônico. Qualquer extensão finita de $\mathbb{Q}$ é chamado de **corpo de números**, em particular $\mathbb{F} = \mathbb{Q}(\alpha)$.

Sejam 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** $\mathbb{F}$ [20], que denotaremos por $\mathcal{D}_{\mathbb{F}}$. Exemplos conhecidos 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 é m 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

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

Exemplo 2.2.1 **i)** *Se extensão quadrática* $\mathbb{F} = \mathbb{Q}(\sqrt{-1})$.

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 por anel de inteiros de Gauss.*

ii) *Se extensão quadrática* $\mathbb{F} = \mathbb{Q}(\sqrt{-3})$.

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 por anel de inteiros de Eisenstein-Jacobi.*

O Teorema 2.2.1 relaciona polinômios $p(x)$ que contém como uma das raízes um elemento algébrico com extensões de corpos.

Teorema 2.2.1 *[26] Sejam* $\mathbb{F}/\mathbb{E}$ *uma extensão de corpos e* $\alpha \in \mathbb{F}$ *um elemento algébrico sobre* $\mathbb{E}$.

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

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

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

Lema 2.2.1 *[26] Dado $p(X) \in \mathbb{E}[X]$ um polinômio não constante e 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 $p(X)$.*

Definição 2.2.1 *Seja $\mathbb{F}/\mathbb{E}$ uma extensão de corpos. O grupo de Galois $\mathbb{F}/\mathbb{E}$ que denotamos por $G(\mathbb{F}/\mathbb{E})$ é o conjunto de todos os automorfismos de $\mathbb{F}$ de 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 $G(\mathbb{F}/\mathbb{E})$.*

Teorema 2.2.2 *[26] Se $p(x)$ é um polinômio com coeficientes sobre $\mathbb{E}$ e se for 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, consideremos 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, [20], 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.

Definição 2.2.2 *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**.

Definição 2.2.3 *Um domínio noetheriano R, integralmente fechado onde todo ideal primo não nulo é maximal é chamado* **domínio de Dedekind**.

Teorema 2.2.3 *[20] Se $\mathbb{F}$ for um corpo de números, então seu anel de inteiros algébricos é um domínio de Dedekind.*

Proposição 2.2.1 *[20] 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 $GF(p)$, corpo finito com p elementos, 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 verficadas:

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 foi estabelecido 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 chamamos 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.

Teorema 2.2.4 *[17] Se $\mathbb{F}$ é um corpo de números então $\mathbb{F} = \mathbb{Q}(\theta)$, para algum inteiro algébrico θ .*

Quando $\mathbb{F} = \mathbb{Q}(\theta)$ e o grau do polinônio minimal associado a θ é n então $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma $\mathbb{Q}$-base para $\mathbb{F}$.

Veremos que nem sempre esta base será um conjunto ordenado de geradores do grupo abeliano aditivo de $\mathcal{D}_{\mathbb{F}}$, para tal terá que satisfazer algumas condições que descreveremos a seguir. Uma $\mathbb{Z}$-base de $\mathcal{D}_{\mathbb{F}}$ é chamada **base integral** do corpo $\mathbb{F}$. Assim, $\{\alpha_1, \ldots, \alpha_n\}$ é uma base integral para um corpo de números $\mathbb{F}$ se, e somente se, todo elemento de $\mathcal{D}_{\mathbb{F}}$ for unicamente expresso como

$$a_1\alpha_1 + \cdots + a_n\alpha_n,$$

para $a_1, \ldots, a_n$ números inteiros.

Teorema 2.2.5 *[17] Todo corpo de número $\mathbb{F}$ possui uma base integral e o grupo aditivo $\mathcal{D}_{\mathbb{F}}$ é um $\mathbb{Z}$-módulo livre com posto igual a dimensão de $\mathbb{F}/\mathbb{Q}$.*

Dado $\mathbb{F} = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico, nem sempre é verificado a igualdade $\mathcal{D}_{\mathbb{F}} = \mathbb{Z}[\theta]$.

Como exemplo podemos citar o corpo de números $\mathbb{Q}(\sqrt{5})$, onde $\sqrt{5}$ é um inteiro algébrico. Por outro lado, $\frac{1+\sqrt{5}}{2}$ é raiz do polinômio $p(X) = X^2 - X - 1$, portanto um inteiro algébrico que não pertence a $\mathbb{Z}[\sqrt{5}]$.

Embora, o Teorema 2.2.5 estabeleça que todo corpo de números possui uma base integral, nem sempre é fácil apresentar quem é de fato esta base.

Dado $\{\alpha_1, \ldots, \alpha_n\}$ uma base do $\mathbb{Q}$-espaço vetorial $\mathbb{F}$, definimos o **discriminante** desta base por $\Delta[\alpha_1, \ldots, \alpha_n] = det(\sigma_j(\alpha_i))^2$, onde os $\sigma_{j'}s$, para $1 \leq j \leq n$, são os homomorfismos do grupo de Galois associado ao corpo de números $\mathbb{F}$.

Para duas bases integrais $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_n\}$ de um mesmo corpo de números $\mathbb{F}$ vale a relação $\Delta[\alpha_1, \ldots, \alpha_n] = (\pm 1)^2 \Delta[\beta_1, \ldots, \beta_n]$. Esta relação provém do fato de que a matriz mudança de base ser inversível.

No caso em que $\{\alpha_1, \ldots, \alpha_n\}$ é uma base integral de $\mathbb{F}$, $\Delta[\alpha_1, \ldots, \alpha_n]$ será chamado de **discriminante do corpo** $\mathbb{F}$, e denotado por $d(\mathbb{F})$.

Teorema 2.2.6 *[17] Se o conjunto ordenados $\{\alpha_1, \ldots, \alpha_n\}$ de elementos de $\mathcal{D}_{\mathbb{F}}$ formar uma $\mathbb{Q}$-base para o corpo $\mathbb{F}$, e $\Delta[\alpha_1, \ldots, \alpha_n]$ for um inteiro livre de quadrados, então $\{\alpha_1, \ldots, \alpha_n\}$ será uma base integral para $\mathbb{F}$.*

No caso $\mathbb{Q}(\sqrt{5})$, considerando $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ como uma $\mathbb{Q}$-base temos que $\Delta[1, \frac{1+\sqrt{5}}{2}]$ é dado por

$$\begin{vmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{vmatrix} = 5$$

Pelo Teorema 2.2.6, $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral de $\mathbb{Q}(\sqrt{5})$.

Proposição 2.2.2 *[17] Os números algébricos $\alpha_1, \ldots, \alpha_n$ formam uma base integral se, e somente se, forem inteiros algébricos e $\Delta[\alpha_1, \ldots, \alpha_n] = d(\mathbb{F})$, onde $d(\mathbb{F})$ é o discriminante do corpo $\mathbb{F}$.*

Proposição 2.2.3 *[17] Se $\{\alpha_1, \ldots, \alpha_n\}$ é um conjunto de inteiros algébricos, então $\Delta[\alpha_1, \ldots, \alpha_n] \equiv 0$ ou $1(mod 4)$.*

O grau n do polinômio $p(X) = a_n X^n + \cdots + a_1 X + a_0$, será denotado por $deg(p)$ e o coeficiente líder a_n por $l(p(X))$.

Sejam $\mathbb{F}$ um corpo de números, e $p(X), q(X) \in \mathcal{D}_{\mathbb{F}}[X]$ e $\overline{\mathbb{F}}$ o fecho algébrico de $\mathbb{F}$ (o corpo que contém todas as raízes dos polinômios não nulos com coeficientes em $\mathbb{F}$).

Definição 2.2.4 *Sejam $p(X) = a(X - \alpha_1).\cdots(X - \alpha_m)$ e $q(X) = b(X - \beta_1).\cdots(X - \beta_n)$, as decomposições de $p(X)$ e $q(X)$ em $\overline{\mathbb{F}}$. Então a **resultante** $R(p(X), q(X))$ de $p(X)$ e $q(X)$ é definida como sendo uma das fórmulas equivalentes:*

$$R(p(X), q(X)) = a^n q(\alpha_1) \cdots q(\alpha_n) = (-1)^{mn} b^m p(\beta_1). \cdots p(\beta_n)$$
$$= a^n b^m \prod_{1 \leq i \leq m, 1 \leq j \leq n} (\alpha_i - \beta_j).$$

Proposição 2.2.4 *Seja* $p(X) = a(X - \alpha_1). \cdots (X - \alpha_m) \in \mathcal{D}_{\mathbb{F}}[X]$, *com* $m = deg(p(X))$. *Então o discriminante de* $p(X)$ *é dado por*

$$(-1)^{m(m-1)/2} R(p(X), p^{'}(X))/l(p(X)),$$

onde $p'(X)$ *denota a derivada formal de* $p(X)$.

O corolário a seguir fornece a resposta quando um corpo de números $\mathbb{F}$ possui uma base integral do tipo $\{1, \theta, \ldots, \theta^{n-1}\}$.

Corolário 2.2.1 *Sejam* $p(X)$ *um polinômio mônico em* $\mathbb{Z}[X]$; θ *uma raiz de* $p(X)$; *e* $\mathbb{F} = \mathbb{Q}(\theta)$. *Assumindo que o discriminante de* $p(X)$ *é livre de quadrados ou é do tipo* $4d$, *onde* d *é livre de quadrados e não congruente a 1 módulo* 4, *então o discriminante de* $\mathbb{F}$ *é igual ao discriminante de* $p(X)$ *e* $\{1, \theta, \ldots, \theta^{n-1}\}$ *é a base integral de* $\mathbb{F}$.

Quando $\Delta[\alpha_1, \ldots, \alpha_n] \neq d(\mathbb{F}]$, portanto não valendo a Proposição 2.2.2, a Proposição 2.2.5 garante que podem existir inteiros algébricos na base integral do tipo descrito a seguir.

Proposição 2.2.5 *[17] Suponha que os elementos* $\alpha_1, \ldots, \alpha_n \in \mathcal{D}_{\mathbb{F}}$, *não forme uma base integral de* $\mathcal{D}_{\mathbb{F}}$. *Então existe um inteiro algébrico da forma* $\frac{1}{p}(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n)$, *onde* $0 \leq \lambda_i \leq p-1, \lambda_i \in \mathbb{Z}$, *e* p *é um número primo tal que* $p^2/\Delta[\alpha_1, \ldots, \alpha_n]$.

2.3 Revisão de Geometria

Nesta seção definiremos espaços métricos e apresentaremos alguns exemplos de espaços dotados das métricas de Hamming e de Lee, que são as distâncias mais usadas em códigos corretores de erros. Outra definição importante nesta seção é de isometrias, que são funções que preservam distâncias no espaço em que estão definidas. Embora a maior parte desta seção seja destinada à revisão de conceitos básicos de geometria hiperbólica, com destaque para o estudo

de grupos de simetrias de polígonos hiperbólicos (grupos fuchsianos), as referências [9] e [7] são excelentes para o aprofundamento dos conceitos.

2.3.1 Espaços Métricos

Proposição 2.3.1 *Um conjunto não vazio* $\mathbb{E}$ *é denominado* ***espaço métrico*** *se existe uma função* $d : \mathbb{E} \times \mathbb{E} \longrightarrow \mathbb{R}$, *chamada* ***métrica***, *que satisfaça as condições :*

i) $d(x, y) \geq 0$ *e* $d(x, y) = 0$ *se, e somente se,* $x = y, \forall x, y \in \mathbb{E}$;

ii) $d(x, y) = d(y, x), \forall x, y \in \mathbb{E}$;

iii) $d(x, z) \leq d(x, y) + d(y, z), \forall x, y, z \in \mathbb{E}$.

A notação usada para designar um espaço métrico com a métrica d é $(\mathbb{E}, d)$.

Exemplo 2.3.1 *Seja* $\mathbb{E}$, *um conjunto finito qualquer, é sempre possível definir uma métrica em* $\mathbb{E}$, *chamada métrica discreta do tipo;*

$$d(x, y) = \begin{cases} 0, & se\ x = y \\ \\ 1, & se\ x \neq y \end{cases}$$

Sejam $\mathbb{E}^n$, espaço n-dimensional e $d_H(x, y) = \sum_{i=1}^{n} d(x_i, y_i)$, com $d(x_i, y_i)$ definido como no Exemplo 2.3.1. Então, d_H é uma métrica em $\mathbb{E}^n$, chamada **métrica de Hamming**. No caso de $\mathbb{E} = \mathbb{Z}_q$ ser um corpo finito com q potência de um número primo , para um $x \in \mathbb{Z}_q^n$, definimos o peso de Lee do elemento $x = (x_1, \ldots, x_n)$, onde $x_i \in \mathbb{Z}_q, \forall i = 1, \ldots, n$, como $\omega_L(x) = \sum_{i=1}^{n} |x_i|$, onde

$$|x_i| = \begin{cases} x_i, & se\ 0 \leq x_i \leq q/2 \\ \\ q - x_i, & se\ q/2 < x_i \leq q - 1 \end{cases}$$

A **distância de Lee** entre $x, y \in \mathbb{Z}_q^n$ é dada por $d_L(x, y) = \omega_L(x - y)$.

Definição 2.3.1 *Dado um espaço métrico* $(\mathbb{E}, d)$*, uma* ***isometria*** *é uma transformação* $T : \mathbb{E} \longrightarrow \mathbb{E}$ *tal que* $d(\mathbf{x}, \mathbf{y}) = d(T(\mathbf{x}), T(\mathbf{y}))$ *para quaisquer* $x, y \in \mathbb{E}$.

Uma **figura geométrica** é um conjunto finito de pontos limitados numa região de um espaço métrico $\mathbb{E}$.

Uma isometria u que deixa uma figura geométrica K invariante, isto é, $u(K) = K$, é chamada **simetria** de K. O conjunto das simetrias de K forma um grupo $U(K)$ com relação à operação de composição.

2.3.2 Espaços Hiperbólicos

Consideremos o conjunto $\mathbb{H}^{n+1} = \{(x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} | x_{n+1} > 0\}$ dotado de uma estrutura riemanniana $ds^2 = \frac{dx_1^2 + \ldots + dx_{n+1}^2}{x_{n+1}^2}$. O semi-espaço $\mathbb{H}^{n+1}$ é chamado de **espaço hiperbólico** $(n+1)$-dimensional, a métrica definida acima é a **métrica hiperbólica**. A introdução desta métrica riemanniana permite definir comprimento de curvas, curvas geodésicas e distância entre pontos em $\mathbb{H}^{n+1}$. Se considerarmos $\gamma : [a, b] \to \mathbb{H}^{n+1}$, uma curva diferenciável por partes, onde $\gamma(t) = (x_1(t), \ldots, x_n(t))$, definimos o comprimento de γ por :

$$\|\gamma\| = \int_a^b \frac{\sqrt{(\frac{dx_1}{dt})^2 + \ldots + (\frac{dx_{n+1}}{dt})^2}}{x_{n+1}} dt.$$

Tomando a aplicação $\phi : [0, 1] \to [a, b]$, definida por $\phi(t) = a + (b - a)t$ e uma reparemetrização $\gamma' = \gamma(\phi(t)) = \gamma(a + bt)$, obtem-se pela regra da cadeia que

$$\|\gamma\| = \int_a^b \frac{\sqrt{(\frac{dx_1}{d\phi})^2 + \ldots + (\frac{dx_{n+1}}{d\phi})^2}}{x_{n+1}} d\phi = \int_0^1 \frac{\sqrt{(\frac{dx_1}{dt})^2 + \ldots + (\frac{dx_{n+1}}{dt})^2}}{x_{n+1}} dt = \|\gamma'\|.$$

Como é sempre possível obter uma reparametrização como acima, sem perda de generalidade, consideraremos uma curva γ definida no intervalo fechado $[0, 1]$.

A definição a seguir fornece uma maneira de calcularmos a distância entre pontos de $\mathbb{H}^{n+1}$.

Definição 2.3.2 *Dados dois pontos $p, q \in \mathbb{H}^{n+1}$, a distância entre p e q é definida como $d(p,q) = inf\|\gamma\|$, onde o ínfimo é considerado sobre o conjunto de todas as curvas continuamente diferenciáveis por partes $\gamma : [0,1] \to \mathbb{H}^{n+1}$, com $\gamma(0) = p$ e $\gamma(1) = q$.*

Tendo definido a distância entre dois pontos, já estamos aptos a definir as geodésicas em $\mathbb{H}^{n+1}$.

Definição 2.3.3 *Uma curva $\gamma : [a,b] \to \mathbb{H}^{n+1}$ é dita geodésica se para quaisquer pontos $s, t \in [a,b]$, tivermos*

$$d(\gamma(s), \gamma(t)) = \int_s^t \frac{\sqrt{(\frac{dx_1}{dt})^2 + \ldots + (\frac{dx_{n+1}}{dt})^2}}{x_{n+1}} dt,$$

ou seja, se γ minimizar a distância entre os pontos de seu traçado.

Neste trabalho proporemos constelações de sinais apenas para o caso bidimensional $\mathbb{H}^2$, isto é¸ o semi-plano superior do plano complexo $\mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) > 0\}$, conhecido como **semi-plano de Lobatchvsky** .

Em decorrência deste fato, daqui em diante estaremos restringindo nossos estudos apenas ao caso bidimensional.

Observação 2.3.1 *As geodésicas em $\mathbb{H}^2$ são semi-círculos e/ou segmentos de retas ortogonais ao bordo de $\mathbb{H}^2$, isto é, $\partial_\infty \mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) = 0\} \cup \{\infty\}$.*

Definimos o fecho de $\mathbb{H}^2$ (o menor conjunto fechado que contém $\mathbb{H}^2$) como sendo $\overline{\mathbb{H}^2} = \mathbb{H}^2 \cup \partial_\infty \mathbb{H}^2$.

Apresentaremos a seguir um outro modelo da geometria hiperbólica, para o caso bidimensional. Considere o disco unitário $\mathbb{D}^2 = \{z \in \mathbb{C} : |z| < 1\}$.

Considere a aplicação $f(z) = \frac{zi+1}{z+i}$. Observa-se facilmente que f é uma bijeção entre $\mathbb{H}^2$ e $\mathbb{D}^2$. Para tornar f uma isometria basta que definamos em $\mathbb{D}^2$ a métrica riemanniana $ds = \frac{2|dz|}{1-|z|^2}$.

Observação 2.3.2 *As retas neste modelo são os diâmetros do círculo unitário, e segmentos de círculos euclidianos ortogonais ao bordo de* $\mathbb{D}^2$*, o círculo* $\{z \in \mathbb{C} : |z| = 1\}$.

A área de um conjunto $A \subseteq \mathbb{H}^2$, é definida por

$$\mu(A) = \int_A \frac{dxdy}{y^2}$$

se esta integral existir. A formula de Gauss-Bonnet mostra que a área hiperbólica de um triângulo hiperbólico depende somente de seus ângulos.

Teorema 2.3.1 *(Gauss-Bonnet)[7] Seja* Δ *um triângulo hiperbólico com ângulos* α, β, γ*. Então*

$$\mu(\Delta) = \pi - \alpha - \beta - \gamma.$$

O conjunto formado pelas tranformações lineares fracionárias, também conhecidas por transformações de Möbius, definidas de $\mathbb{C}$ em $\mathbb{C}$ do tipo $T(z) = \frac{az+b}{cz+d}$, com $a, b, c, d \in \mathbb{R}$ onde $ad - bc = 1$, forma um grupo com relação à operação composição que denotaremos por $\mathbb{M}$.

Note, que associado a uma transformação de Möbius $T(z) = \frac{az+b}{cz+d}$, existe uma matriz do tipo

$$A_T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

com $a, b, c, d \in \mathbb{R}$ e $det(A_T) = ad - bc = 1$, ou seja com $A_T \in SL(2, \mathbb{R})$, o grupo especial linear constituído de todas as matrizes 2×2 com elementos em $\mathbb{R}$.

Observação 2.3.3 *No disco de Poincaré* $\mathbb{D}^2$*, as tranformações de Möbius são dadas por* $T(z) = \frac{az+c}{\overline{c}z+\overline{a}}$*, com* $a, c \in \mathbb{C}$ *e* $a^2 - c^2 = 1$*. Logo, existe uma isometria entre* $\mathbb{H}^2$ *e* $\mathbb{D}^2$.

O conjunto das matrizes A_T formam um grupo, com a operação multiplicação. Este grupo é chamado de **grupo unimodular**, e denotamos por $SL(2, \mathbb{R})$.

Note que $T(z) = \frac{az+b}{cz+d}$ e $T(z) = \frac{-az-b}{-cz-d}$ são caracterizadas matricialmente por $\pm A_T$. Dessa forma podemos estabelecer um grupo quociente chamado de **grupo projetivo linear**, denotado por $PSL(2, \mathbb{R}) \simeq SL(2, \mathbb{R})/\{\pm Id\}$, onde Id é a identidade. As transformações em $PSL(2, \mathbb{R})$ são isometrias do plano hiperbólico e, portanto levam geodésicas em geodésicas em $\mathbb{H}^2$.

Teorema 2.3.2 *[7] A área hiperbólica é invariante pelas imagens das tranformações em* $PSL(2,\mathbb{R})$. *Se* $\mu(A)$ *existir para algum subconjunto* $A \subseteq \mathbb{H}^2$, *então para* $T \in PSL(2,\mathbb{R})$ *é válida a igualdade* $\mu(T(A)) = \mu(A)$.

As transformações identificadas em $PSL(2,\mathbb{R})$ são classificadas em três tipos, quanto ao valor do módulo do traço da matriz associada .

Seja $T(z) = \frac{az+b}{cz+d}, a, b, c, d \in \mathbb{R}$, tal que $ad - bc = 1$. Então T é chamada:

i) Transformação elíptica, se $Tr(T) = |a + d| < 2$;

ii) Transformação parabólica, se $Tr(T) = |a + d| = 2$;

iii) Transformação hiperbólica, se $Tr(T) = |a + d| > 2$.

Teorema 2.3.3 *[9] Para toda transformação* $Id \neq T_A \in PSL(2,\mathbb{R})$, *existe uma matriz* $B \in SL(2,\mathbb{R})$, *tal que,* $T_B o T_A o T_B^{-1}$ *é uma das matrizes abaixo:*

$$\begin{bmatrix} cos\theta & sen\theta \\ -sen\theta & cos\theta \end{bmatrix}, \qquad \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{bmatrix}$$

onde $0 \leq \theta \leq 2\pi, t, \lambda \in \mathbb{R}$.

Note que cada transformação $T(z) = \frac{az+b}{cz+d}$ pode ser identificada de modo natural por pontos $(a, b, c, d) \in \mathbb{R}^4$. Mais precisamente, $SL(2,\mathbb{R})$ pode ser identificado como um subconjunto de $\mathbb{R}^4$, $X = \{(a, b, c, d) \in \mathbb{R}^4 : ad - bc = 1\}$ herdando assim a estrutura topológica ambiente.

A aplicação $\varphi(a, b, c, d) = (-a, -b, -c, -d)$ é um homomorfismo, e φ com a identidade forma um grupo cíclico de ordem 2 agindo em X. Definiremos a topologia em $PSL(2,\mathbb{R})$ como um espaço quociente $PSL(2,\mathbb{R}) \simeq SL(2,\mathbb{R})/\{ker\varphi\}$.

A norma em $PSL(2,\mathbb{R})$ induzida no $\mathbb{R}^4$, para $T(z) = \frac{az+b}{cz+d}$, com $ad - bc = 1$ é dada por $\| T \| = (a^2 + b^2 + c^2 + d^2)^{\frac{1}{2}}$. O grupo $PSL(2,\mathbb{R})$ é um grupo topológico com a topologia métrica $\| T - S \|$, para $T, S \in PSL(2,\mathbb{R})$.

O grupo de todas as isometrias de $\mathbb{H}^2 (Isom(\mathbb{H}^2))$ é também topológico.

Definição 2.3.4 *Um subgrupo* Γ *de* $Isom(\mathbb{H}^2)$ *é chamado discreto se a topologia induzida em* Γ *é uma topologia discreta, isto é, se* Γ *é um conjunto discreto no espaço topológico* $Isom(\mathbb{H}^2)$.

Observação 2.3.4 Γ *é discreto se, e somente se,* $T_n \to Id, T_n \in \Gamma$ *implica que* $T_n = Id$ *para* n *suficientemente grande.*

A seguir apresentaremos a definição de grupo fuchsiano, a ser usada na geração das constelações de sinais no plano hiperbólico.

Definição 2.3.5 *Um grupo é chamado de* ***grupo fuchsiano*** *se este for um subgrupo discreto de* $PSL(2, \mathbb{R})$.

No sentido de caracterizarmos os grupos fuchsianos, iremos apresentar algumas definições. Sejam X um espaço topológico e G um grupo de endomorfismos de X.

Definição 2.3.6 *Uma família* $\{M_\alpha | \alpha \in A\}$ *de subconjuntos de* X, *indexados por um conjunto* A *é chamado localmente finito se para um dado subconjunto compacto* $K \subseteq X, M_\alpha \cap K \neq \phi$ *para uma quantidade finita de* $\alpha \in A$.

Definição 2.3.7 *Para* $x \in X$, *a família* $G_x = \{g(x) : g \in G\}$ *é chamada de* G***-órbita do ponto*** x.

Definição 2.3.8 *Dizemos que um grupo* G *age de maneira* ***propriamente descontínua*** *em* X, *se uma* G*-órbita para um dado ponto* $x \in X$ *é localmente finita.*

Teorema 2.3.4 *[9] Seja* Γ *um subgrupo de* $PSL(2, \mathbb{R})$. *Então* Γ *é um grupo fuchsiano se, e somente se,* Γ *age de maneira propriamente descontínua em* $\mathbb{H}^2$.

Definição 2.3.9 *Um subgrupo* $\Gamma \subseteq PSL(2, \mathbb{R})$ *é dito* ***grupo elementar*** *se existe* $z \in \overline{\mathbb{H}}^2$, *tal que a órbita* $\Gamma(z)$ *é finita.*

Teorema 2.3.5 *[9]*

Seja Γ um grupo não elementar. Então Γ possui elemento hiperbólico.

Definição 2.3.10 *Seja Γ um grupo fuchsiano e $z \in \overline{\mathbb{H}}^2$.*

1) *Chamamos de conjunto limite de Γ, determinado por z, ao conjunto $\Lambda_z(\Gamma)$ formado por todos os pontos $\eta \in \overline{\mathbb{H}}^2$ tais que η é ponto de acumulação de $\Gamma(z)$.*

2) *Chamamos de conjunto limite de Γ ao conjunto $\Lambda_z(\Gamma)$ formado pela união dos conjuntos $\Lambda_z(\Gamma)$.*

Convém observar que, se Γ for grupo discreto, a órbita $\Gamma(z)$ não pode possuir pontos de acumulação em $\overline{\mathbb{H}}^2$, ou seja, $\Lambda_z(\Gamma) \subseteq \partial\mathbb{H}_\infty = \mathbb{R} \cup \{\infty\}$. O mesmo valendo para o conjunto limite $\Lambda(\Gamma)$.

Teorema 2.3.6 *[9] Seja Γ grupo fuchsiano e suponha que $\Lambda(\Gamma)$ possua mais de dois pontos. Então uma das possibilidades ocorre:*

1) $\Lambda(\Gamma) = \partial_\infty \mathbb{H}^2$.

2) *$\Lambda(\Gamma)$ é perfeito e magro (isto é, todo ponto de $\Lambda(\Gamma)$ é ponto de acumulação de $\Lambda(\Gamma)$, e o complementar de $\Lambda(\Gamma)$ é denso).*

Apresentaremos a seguir a Definição 2.3.11, a ser usada na geração de uma região no plano hiperbólico, esta contendo os pontos de uma órbita de um elemento x.

Seja G um grupo de homomorfismos agindo de maneira propriamente descontínua em X.

Definição 2.3.11 *Um conjunto fechado $F \subset X$ com interior $\dot{F}$ não vazio é definido por* ***região fundamental*** *de G caso satisfaça:*

i) $\cup_{T \in G} T(F) = X$;

ii) $\dot{F} \cap T(\dot{F}) = \phi$, *para todo* $T \in G - \{Id\}$. *A família* $\{T(F) : T \in G\}$ *é chamada de* ***tesselação*** *de* X.

Para apresentarmos uma proposta de tesselação no plano hiperbólico através da ação descontínua de certos grupos fuchsianos Γ, necessitaremos do conceito de região de Dirichlet. Sejam Γ um grupo fuchsiano qualquer e $p \in \mathbb{H}^2$ um elemento qualquer que não é fixado por elementos de Γ. Definimos **região de Dirichlet** de Γ, centrado em p, o conjunto

$$D_p(\Gamma) = \left\{ z \in \mathbb{H}^2 \,|\, d(z,p) \leq d(z, T(p)), \forall T \in \Gamma \right\}.$$

Teorema 2.3.7 *[9]*

Se p *não é elemento fixo de* $\Gamma - \{Id\}$, *então* $D_p(\Gamma)$ *é uma região fundamental de* Γ.

2.3.3 Círculos Isométricos

Nesta subseção, iremos apresentar um procedimento para a obtenção de uma região fundamental associada a um grupo fuchsiano. Para isto, necessitaremos do conceito de círculo isométrico.

Seja $T(z) = \frac{az+b}{cz+d} \in PSL(2,\mathbb{R})$ uma isometria hiperbólica. Então a sua derivada é

$$T'(z) = \frac{a(cz+d) - c(az+b)}{(cz+d)^2} = \frac{ad-bc}{(cz+d)^2} = \frac{1}{(cz+d)^2}.$$

Se $z \equiv z(t)$ for uma curva diferenciável tal que $|cz+d| \equiv 1$, então

$$\int_a^b |z'(t)|dt = \int_a^b |T'(t)||z'(t)|dt,$$

ou seja, o comprimento das curvas $z(t)$ e $Toz(t)$ coincidem. Logo, a distância hiperbólica ao longo da curva e a distância euclidiana são preservadas, ou seja, a restrição de T a esta curva é uma isometria euclidiana.

Mas, se assumirmos que $c \neq 0$, então

$$|cz+d| = 1 \Longleftrightarrow |z+\frac{d}{c}| = \frac{1}{|c|},$$

ou seja, o conjunto dos pontos nos quais T age como isometria tanto no sentido euclidiano quanto no hiperbólico é um círculo de centro no ponto $-\frac{d}{c}$ e raio $\frac{1}{|c|}$.

Definição 2.3.12 *Seja $T(z) = \frac{az+b}{cz+d} \in PSL(2,\mathbb{R})$ uma isometria de $\mathbb{H}^2$, com $c \neq 0$. Chamamos de* ***círculo isométrico*** *de T ao conjunto $I(T) = \{z \in \mathbb{C} : |cz+d| = 1\}$.*

Denotaremos por $\hat{I}(T) = \{z \in \mathbb{C} : |cz+d| < 1\}$ o conjunto dos pontos interiores ao círculo isométrico, e por $\breve{I}(T) = \{z \in \mathbb{C} : |cz+d| > 1\}$ o conjunto dos pontos exteriores ao círculo isométrico.

Teorema 2.3.8 *[9] Os círculos isométricos $I(T)$ e $I(T^{-1})$ possuem o mesmo raio, e $T(I(T)) = I(T^{-1})$.*

Seja Γ um grupo discreto de isometrias que preserva a orientação no disco unitário $\mathbb{D}^2$. Assumiremos que 0 não é um ponto elíptico fixo, tal que $c \neq 0$ para todo $T(z) = \frac{az+c}{\bar{c}z+\bar{a}}$ no grupo Γ.

Definiremos $R_0 = \cap_{T\in\Gamma}\overline{\breve{I}(T) \cap \mathbb{D}^2}$, como sendo o fecho do conjunto dos pontos de $\mathbb{D}^2$ que são pontos exteriores ao círculo isométrico de todas as transformações do grupo Γ.

Teorema 2.3.9 *[7] R_0 é uma região fundamental, conhecida por* ***região fundamental de Ford****.*

2.3.4 Grupos Co-compactos

Gostariamos de reforçar que o interesse deste trabalho reside na procura do espaço das órbitas em $\mathbb{H}^2/\Gamma$, com uma estrutura compacta, a partir de um domínio de Dirichlet.

Por outro lado, relembramos que a topologia quociente $\mathbb{H}^2/\Gamma$ em qualquer espaço topológico módulo uma relação de equivalência é a maior topologia que torna a projeção $P : \mathbb{H}^2 \longrightarrow \mathbb{H}^2/\Gamma$ contínua.

Definição 2.3.13 *Um grupo fuchsiano* Γ *é dito* ***co-compacto*** *se o quociente* $\mathbb{H}^2/\Gamma$ *for compacto.*

O Teorema 2.3.10 fornece uma maneira de se obter grupos fuchsianos co-compactos.

Teorema 2.3.10 *[9] Um grupo fuchsiano* Γ *é co-compacto se, e somente se, todo domínio de Dirichlet de* Γ *for compacto.*

Como um dos objetivos é propor tesselações (recobrimento por polígonos) no plano hiperbólico, consistindo de domínios de Dirichlet (polígonos de $4g$ lados) compactos cujos grupos fundamentais são isomofos aos g-toros, é que iremos considerar um procedimento de obtenção dos geradores dos grupos fuchsianos Γ associados a esses polígonos.

Teorema 2.3.11 *[9] Um grupo fuchsiano* Γ *é co-compacto se, e somente se,* Γ *não possui elementos parabólicos e* $\mu(\mathbb{H}^2/\Gamma) < \infty$.

Como consequência do Teorema 2.3.11, iremos considerar somente os grupos fuchsianos que não contenham elementos parabólicos.

2.3.5 Assinatura de um grupo fuchsiano

Nesta seção, iremos considerar quais grupos fuchsianos Γ poderão ser utilizados no processo de aplicação de recobrimento em $\mathbb{H}^2/\Gamma$. Para isso, necessitaremos do conceito de assinatura de um grupo fuchsiano.

Em um domínio de Dirichlet $D(\Gamma)$ de Γ, existe um número finito de r vértices que são pontos fixos por elementos elípticos de Γ.

Sejam $m_1, \ldots, m_r$ as correspondentes ordens dos elementos elípticos e g o gênero da superfície compacta $\mathbb{H}^2/\Gamma$. O conjunto ordenado de inteiros $(g; m_1, \ldots, m_r)$ é chamado de **assinatura** de Γ.

O Teorema 2.3.12 fornece a área associada ao grupo fuchsiano Γ de assinatura $(g; m_1, \ldots, m_r)$.

Teorema 2.3.12 *[9] Seja Γ um grupo fuchsiano co-compacto e $(g; m_1, \ldots, m_r)$ sua assinatura. Então, $\mu(\mathbb{H}^2/\Gamma) = 2\pi[(2g-2) + \sum_{k=1}^{r}(1 - \frac{1}{m_k})]$.*

O Teorema 2.3.13 mostra que a recíproca do Teorema 2.3.12 é válida.

Teorema 2.3.13 *[9] Dados os inteiros $g \geq 0, r \geq 0$ e $m_k \geq 2 (1 \leq k \leq r)$ tais que $(2g-2) + \sum_{k=1}^{r}(1 - \frac{1}{m_k}) > 0$, existe um grupo fuchsiano co-compacto com assinatura $(g; m_1, \ldots, m_r)$.*

Se Γ não possuir elementos elípticos, então a ação de Γ em $\mathbb{H}^2$ é livre, ou seja, a projeção $P : \mathbb{H}^2 \longrightarrow \mathbb{H}^2/\Gamma$ é uma **aplicação de recobrimento**.

Teorema 2.3.14 *[9] Toda superfície compacta com gênero $g \geq 2$, pode ser modelada no plano hiperbólico.*

Mais adiante estaremos modelando superfícies compactas de gênero $g \geq 2$, no plano hiperbólico. Estas superfícies serão obtidas a partir de polígonos regulares de $4g$ lados, onde g é o gênero da superfície. Como mencionado, para que $P : \mathbb{H}^2 \longrightarrow \mathbb{H}^2/\Gamma$ seja uma aplicação de recobrimento, o grupo fuchsiano Γ associado não pode possuir elementos elípticos. A assinatura de Γ é dada por $(g; m_1, m_2, \ldots, m_r) = (g; 0, \ldots, 0)$, que denotaremos por $(g; -)$. Como consequência, o grupo fuchsiano Γ é formado apenas por elementos hiperbólicos.

2.3.6 Tesselações regulares no plano hiperbólico

Nesta seção estaremos abordando o conceito de tesselação regular no plano hiperbólico, e apresentaremos a diferença existentes entre as tesselações regulares nos planos euclidiano e hiperbólico.

Definição 2.3.14 *Uma **tesselação regular** no plano hiperbólico é uma partição deste plano por polígonos regulares não sobrepostos, todos congruentes, sujeitos à restrição de somente se interceptarem em suas arestas ou vértices, e de modo a termos o mesmo número de polígonos partilhando um mesmo vértice, independente do vértice.*

Uma tesselação regular constituída de polígonos de p lados, onde cada vértice é recoberto por q polígonos será denotada por $\{p, q\}$.

No caso em que $p = q$, a tesselação hiperbólica $\{p, p\}$ é chamada **auto-dual**.

Como consequência do fato de que a soma dos ângulos internos de um triângulo hiperbólico ser sempre menor do que π, haverá uma tesselação hiperbólica $\{p, q\}$ se, e somente se, $(p-2)(q-2) > 4$, ao contrário, do plano euclidiano, que para haver uma tesselação regular basta que $(p-2)(q-2) = 4$. Como consequência no plano euclidiano existem apenas as tesselações regulares $\{4, 4\}, \{6, 3\}$ e suas duais $\{4, 4\}, \{3, 6\}$. Já no plano hiperbólico existem infinitas tesselações regulares, ver [30].

2.4 Constelações de Sinais Geometricamente Uniformes

Apresentaremos nesta seção os conceitos de **espaço de sinais** e de **constelação de sinais**, que serão os objetos centrais de estudo deste trabalho.

Um **espaço de sinais** é um conjunto discreto de pontos em um espaço métrico $(\mathbb{E}, d)$ em que seja possível realizar uma identificação dos pontos de $(\mathbb{E}, d)$ por sinais.

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

Definição 2.4.1 *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,*

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

Definição 2.4.2 *A região de Voronoi $R_V(k)$ associada a um dado ponto de sinal $k \in K$ é o conjunto $R_V(k) = \{\mathbf{x} \in \mathbb{E} : d(\mathbf{x}, k) \leq d(\mathbf{x}, T(k)), \forall T \in U\}$.*

Definição 2.4.3 *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.

Teorema 2.4.1 *[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.*

Em decorrência das condições 1) e 2) do Teorema 2.4.1 restringiremos nosso trabalho às constelações de sinais geometricamente uniformes.

Como nossa meta será propor a construção das constelações de sinais geometricamente uniformes. Consideraremos como espaço de sinais os conjuntos dos pontos que sejam baricentros das tesselações regulares tanto no plano euclidiano quanto no hiperbólico.

Identificaremos os espaços de sinais euclidianos e hiperbólicos pelos elementos de anéis de inteiros e ordens dos quatérnios, respectivamente nos Capítulos 4 e 5.

As constelações geometricamente uniformes de sinais que proporemos, serão obtidas a partir dos elementos que sejam representantes de classes laterais de energia média mínima obtidos a partir dos anéis quocientes de um anel de inteiros/ uma ordem dos quatérnios por ideais nos espaços de sinais euclidiano/hiperbólico.

Dentre todos os possíveis conjuntos de sinais com cardinalidade m finita, obtidos pelos particionamentos nestes espaços de sinais, aquele que apresenta a menor energia média mínima é denominado de *região fundamental* associada aos m pontos de sinais. A energia média mínima E_{min} de uma constelação com sinais, dada por $\{x_0, x_1, \ldots, x_m\}$ é a função $\sum_{i=1}^{m} d_i^2 \frac{1}{m}$, 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*. 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*.

Nos Capítulos 4 e 5 apresentaremos procedimentos para a geração de constelações S que sejam geometricamente uniformes com cardinalidade p^m em espaços de sinais euclidianos e hiperbólicos, respectivamente, com os sinais tendo como rótulos elementos de um corpo de Galois $GF(p^m)$ ou por elementos de um p-grupo G_{p^m}.

Capítulo 3

Formas Quadráticas

3.1 Introdução

Neste capítulo consideraremos as formas quadráticas, isto é, polinômios homogênios de grau 2 com n váriaveis do tipo

$$f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} b_{ij} X_i X_j \in \mathbb{F}[X_1, ..., X_n], \tag{3.1}$$

sobre um corpo $\mathbb{F}$ de $Car(\mathbb{F}) \neq 2$, onde $b_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$.

O objetivo deste capítulo é apresentar aspectos aritméticos/geométricos (representatividade de números/espaços quadráticos) que serão utilizados nos Capítulos 4 e 5.

Através destes aspectos estaremos propondo procedimentos de construção e rotulamento de constelações de sinais. Mostraremos que os reticulados, contendo tais constelações de sinais, estão associados a formas quadráticas. Com isso, a propriedade de equivalência entre constelações de sinais poderá ser apreciada através da equivalência das formas quadráticas associadas aos reticulados que as contém.

3.2 Espaços Quadráticos

Nesta seção veremos que existe um espaço associado a uma forma quadrática, que chamamos de **espaço quadrático**, que caracterizará a componente geométrica mencionada na introdução deste capítulo.

Seja f uma forma quadrática dada por

$$f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} b_{ij} X_i X_j \in \mathbb{F}[X_1, ..., X_n]. \tag{3.2}$$

A matriz simétrica constituída pelos coeficientes b_{ij} do polinômio f, será denotada por $M_f = (b_{ij})_{n\times n}$, e chamada de matriz associada a f.

O número de variáveis de f, caracterizando a **dimensão** de f, será denotada por $dim(f)$.

Sejam V um $\mathbb{F}$-espaço vetorial de dimensão n e $\{e_1, \ldots, e_n\}$ uma base de V. Tomemos $v = \sum_{i=1}^{n} x_i e_i \in V$ e uma forma quadrática f, como definida na equação (3.2) possuindo $M_f = (b_{ij})_{n\times n}$ como matriz associada.

Note, que podemos re-escrever f como

$$f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} b_{ij} X_i X_j = (X_1 \ldots X_n).M_f.\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}, \tag{3.3}$$

o que nos permite denotar $f(x_1, \ldots, x_n)$ por $f(v)$, para $v = (x_1, \ldots, x_n)$. Consideremos, $v = \sum_{i=1}^{n} x_i e_i$ e $w = \sum_{i=1}^{n} y_i e_i$ com $x_i, y_i \in \mathbb{F}, \forall i = 1, \ldots, n$ e a aplicação: $B_f : V \times V \longrightarrow \mathbb{F}$ definida por:

$$B_f(v, w) = \frac{1}{2}[f(v + w) - f(v) - f(w))]. \tag{3.4}$$

Desenvolvendo (3.4), nota-se que B_f é uma aplicação bilinear, ou seja, associada a uma forma quadrática f existe uma aplicação bilinear B_f como estabelecida na equação (3.4).

Por outro lado, considerando uma aplicação bilinear em V como em (3.4), e $\{e_1, \ldots, e_n\}$ como sendo a base do espaço vetorial V então para um vetor não nulo $u = \sum_{i=1}^{n} a_i e_i \in V$ com $a_i \in \mathbb{F}$, se avaliarmos B em $w, v = u$ obtemos

$$B(u,u) = B(a_1e_1 + \cdots + a_ne_n, a_1e_1 + \cdots + a_ne_n) = \sum_{i,j=1}^{n} B(e_i, e_j)a_ia_j.$$

Como conseqüência de (3.3) $f_B(a_1, \ldots, a_n) = f(u) = B(u,u)$. Isto mostra que existe uma correspondência biunívoca entre formas quadráticas e aplicações bilineares.

Ao par (V, B), constituído do espaço vetorial V e da aplicação bilinear B definida em V, chamamos de **espaço quadrático**.

3.3 Formas Quadráticas Equivalentes

Nesta seção veremos como a componente aritmética fará parte do estudo das formas quadráticas.

Sejam f e g duas formas quadráticas de mesma dimensão sobre $\mathbb{F}$ e M_f e M_g as respectivas matrizes associadas. Dizemos que f é **equivalente** a g, ou que f é **isométrica** a g, se existe uma matriz $C \in GL(n, \mathbb{F})$, (grupo das matrizes inversíveis de posto n sobre $\mathbb{F}$) tal que $M_f = C^t M_g C$, onde C^t denota a transposta de C. Denotaremos tal equivalência por $f \sim g$.

Observação 3.3.1 *Dizemos que um conjunto $\mathcal{C}$ é uma classe de equivalência, se para quaisquer formas quadráticas $f, g, h \in \mathcal{C}$, forem satifeitas as seguintes relações,*

i) *(Reflexiva) Para todo $f \in \mathcal{C}$, vale $f \sim f$;*

ii) *(Simétrica) Para quaisquer $f, g \in \mathcal{C}$, se $f \sim g$ então $g \sim f$;*

iii) *(Transitiva) Para quaisquer $f, g, h \in \mathcal{C}$, se $f \sim g$ e $g \sim h$ então $f \sim h$.*

Teorema 3.3.1 *[27] Toda forma quadrática simétrica $f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij}X_iX_j \in \mathbb{F}[X_1, \ldots, X_n]$ é equivalente a uma forma quadrática diagonal do tipo*
$g(X_1, \ldots, X_n) = \sum_{i=1}^{n} d_iX_i^2 \in \mathbb{F}[X_1, \ldots, X_n]$.

As propriedades algébricas que são satisfeitas numa classe de equivalência de uma forma quadrática são chamadas de **invariantes algébricos**. Como exemplo, mencionamos a dimensão de uma forma quadrática. A seguir estaremos apresentando outros invariantes para as classes de equivalência de uma forma quadrática.

Seja f uma forma quadrática de dimensão n. Denotamos por $D_f = \{d \in \dot{\mathbb{F}} : \exists a_1, \ldots, a_n \in \mathbb{F}$ tal que $f(a_1, \ldots, a_n) = d\}$, o **conjunto de valores** da forma quadrática f. Dizemos, neste caso, que f **representa** d, sendo portanto, uma componente aritmética no estudo das formas quadráticas. A Proposição 3.3.1 mostra que o conjunto de valores é um invariante para uma classe de equivalência da forma quadrática f.

Proposição 3.3.1 *[27] Se $f \sim g$ então $D_f = D_g$.*

Chamamos de **discriminante** de f ao elemento $d(f) = \det(f)\dot{\mathbb{F}}^2 \in \dot{\mathbb{F}}/\dot{\mathbb{F}}^2$, onde $det(f)$ denota o determinante da matriz M_f. A notação $d(f) = \det(f)\dot{\mathbb{F}}^2 \in \dot{\mathbb{F}}/\dot{\mathbb{F}}^2$, tem o seguinte significado: se f e g possuem o mesmo discriminante, então o discriminante de suas matrizes associadas diferem por um quadrado em $\dot{\mathbb{F}}$. Tal condição caracteriza o discriminante de uma forma quadrática como um invariante em uma classe de equivalência $\mathcal{C}$.

Na próxima seção veremos que através desse invariante é possível caracterizar todas as formas quadráticas de dimensão 2 em dois conjuntos distintos.

3.4 Classificação das Formas Quadráticas

Nesta seção será estabelecida, através do Teorema 3.4.1, em que geometria os reticulados associados às formas quadráticas de dimensão 2 estão inseridas. Se existirem $a_1, \ldots, a_n \in \mathbb{F}$, não todos nulos, tais que $f(a_1, \ldots, a_n) = 0$, dizemos que f é uma forma quadrática **isotrópica**, ou equivalentemente, se existir um $v \in V, v \neq 0$ tal que $B_f(v, v) = 0$, então v é dito **isotrópico**.

Quando o espaço quadrático (V, B) contém um vetor isotrópico, dizemos que (V, B) é um **espaço quadrático isotrópico**, caso contrário, **anisotrópico**.

Teorema 3.4.1 *[27] Seja $f(X_1, X_2)$ uma forma quadrática sobre $\mathbb{F}$. As seguintes afirmações são equivalentes:*

(a) f é isotrópica;

(b) $d(f) = -1\dot{\mathbb{F}}^2$;

(c) $f \sim X_1^2 - X_2^2$;

(d) $f \sim X_1 X_2$.

(e) Existe um $\mathbb{F}$-espaço vetorial de dimensão 2, com base $\{v_1, v_2\}$ tal que $B_f(v_1, v_1) = B_f(v_2, v_2) = 0$ e $B_f(v_1, v_2) = B_f(v_2, v_1) = \frac{1}{2}$.

Note que o Teorema 3.4.1 caracteriza as formas quadráticas com discriminante -1 como sendo isotrópricas e as que apresentam $+1$ como sendo anisotrópricas.

Um outro fato a ser destacado é que as formas quadráticas isotrópricas de dimensão 2 podem ser vistas como um espaço quadrático (V, B) de $dim(V) = 2$, isto é, $X^t T X$, onde $X^t = (x_1, x_2)$ e

$$T = \begin{bmatrix} a & c \\ \overline{c} & \overline{a} \end{bmatrix}$$

é uma transformação de Möbius do tipo $T(z) = \frac{az+c}{\overline{c}z+\overline{a}}$, com $a, c, \overline{a}, \overline{c} \in \mathbb{C}$, agindo no disco de Poincaré $\mathbb{D}^2$. Logo, concluímos que o espaço quadrático (V, B) de dimensão 2 associado às formas quadráticas isotrópricas, é o plano hiperbólico.

Por outro lado, as formas quadráticas anisotrópicas f de dimensão 2, que por consequência do Teorema 3.4.1, possuem discriminante positivo são do tipo $f = ax_1^2 + bx_2^2$, com $a, b > 0$ ou $a, b < 0$.

No Capítulo 2, vimos que a norma, $N_{\mathbb{Q}(\sqrt{-m})/\mathbb{Q}}(x) = x.\overline{x}$, onde $x \in \mathbb{Z}[\theta]$, o anel de inteiros de uma extensão quadrática imaginária $\mathbb{Q}(\sqrt{-m})$ para m inteiro positivo, é dada por uma forma quadrática anisotróprica, como mostrada a seguir

$$N_{\mathbb{Q}(\sqrt{-m})/\mathbb{Q}}(a+b\theta) = (a+b\theta)(\overline{a+b\theta}) = \begin{cases} a^2 - mb^2, & se\ \theta = \sqrt{m} \\ \\ a^2 + ab + \frac{(1-m)}{4}b^2, & se\ \theta = \frac{1+\sqrt{m}}{2} \end{cases} \tag{3.5}$$

O espaço quadrático (V, B) de dimensão 2 associado às formas quadráticas anisotrópricas, mostradas em (3.5) é o plano complexo $\mathbb{C}$. Veremos no Capítulo 4 que essas formas quadráticas estão associadas a reticulados no plano complexo tais que seus elementos pertencem aos anéis de inteiros das extensões quadráticas imaginárias $\mathbb{Q}(\sqrt{-m})$.

Com isso, concluímos que a isotropria de uma forma quadrática f de dimensão 2 é o **invariante geométrico** que caracteriza a geometria que o espaço quadrático (V, B) está inserido.

Capítulo 4

Construção e Rotulamento de Constelações de Sinais em Espaços Euclidianos

4.1 Introdução

Em [3], Huber propos um método de construção de códigos de bloco tendo como alfabeto elementos de corpos de Galois $GF(p)$ obtidos através das classes laterais do anel de inteiros de Gauss módulo ideais primos. Tais códigos apresentam capacidade de correção de um erro para a codificação de sinais identificados como pontos do plano complexo. 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.

Em [4], Egri e Horrigan utilizaram um grupo multiplicativo finito proveniente do anel de inteiros de Gauss para uso em detecção diferencial de uma constelação de sinais 16-QAM.

Em [5], Rifà caracterizou algébricamente a proposta [4] estendo para os grupos das unidades $G_n^{'}$ dos grupos multiplicativos G_n de cardinalidade 2^n a partir de $\mathbb{Z}[i]$, que podem ser utilizados em detecção diferencialmente coerente de sinais em constelações de sinais do tipo QAM. Esses grupos foram utilizados para projetar códigos de bloco através da matriz verificação de paridade para constelações do tipo QAM. Esses códigos de bloco não são nem lineares e nem códigos de grupo. A construção desses códigos está baseada na geração de sequências que pertencem ao grupo G_n ou ao grupo $G_n^{'}$.

Em [35], Dong e Soh mostraram uma maneira de se construir subgrupos a partir dos grupos multiplicativos das unidades dos quocientes $\mathbb{Z}[i]/(p^n)$ e $\mathbb{Z}[\omega]/(p^n)$, para p primo ímpar, e que estes subgrupos estão casados a espaços de sinais QAM respectivamente de $4p^{2n-2}$ e $6p^{2n-2}$ pontos de sinais, onde o alfabeto destes grupos multiplicativos podem ser usados para a construção de códigos de bloco corretores de erros.

Em [19] e [24] Favareto propos um procedimento geral de construção de constelações de sinais e de códigos sobre corpos de números quadráticos com rótulos em corpos de Galois $GF(p)$.

Em [37] Interlando e Elia estenderam o precedimento de rotular constelações de sinais pertencentes a corpos de números de dimensão finita n com rótulos em corpos de Galois $GF(p)$ e $GF(p^m)$.

Neste capítulo, iremos apresentar alguns resultados que estendem o processo de construção de constelações de sinais tais que os mesmos são rotulados pelos elementos de um corpo de Galois $GF(p^m)$ para p-grupos G_{p^m} (isto é grupos com cardinalidade potência de primos p) em espaços euclidianos.

4.2 Grupos de Simetrias

Nesta seção, determinaremos explicitamente, quem são as matrizes associadas aos geradores do grupo de simetrias de um quadrado de área 2, como consequência poderemos obter um subgrupo de ordem 2, que tessele o plano complexo, pela ação transitiva desse subgrupo no quadrado inicial.

Verificaremos que associado a estas matrizes geradoras existe uma forma quadrática $f(X,Y) = X^2 + Y^2$, que por sua vez, estará associada a um reticulado no plano complexo cujos pontos são identificados por elementos de um anel de inteiros $\mathbb{Z}[i]$, conforme veremos na Seção 4.4.2.

Considere o quadrado da Figura 4.1.

As matrizes associadas às simetrias do quadrado são dadas por

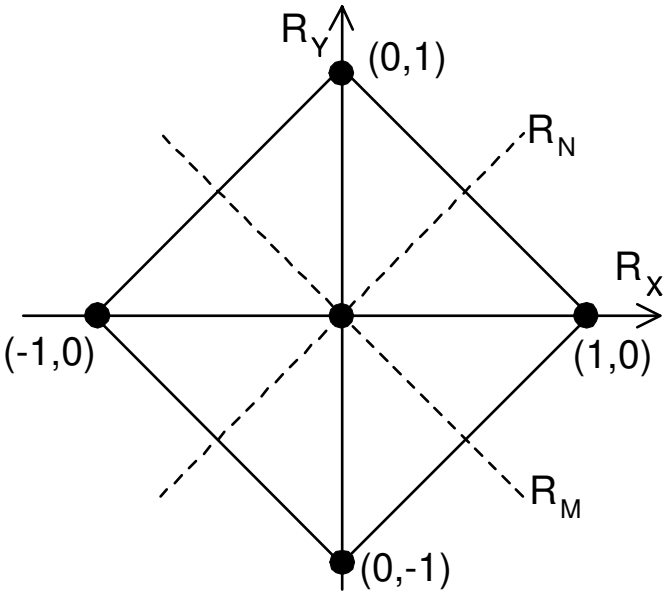

Figura 4.1: Simetrias do quadrado

$$Id = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad R_{\frac{\pi}{2}} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad R_{\frac{3\pi}{2}} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$R_{\pi} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad R_X = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad R_Y = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$R_M = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \qquad R_N = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

onde $R_{\frac{\pi}{2}}$ é a matriz de rotação da simetria que rotaciona uma das arestas do quadrado em $\frac{\pi}{2}$ radianos.

Sejam $\alpha = R_{\frac{\pi}{2}}$ e $\beta = R_N$. Tomando as composições dessas simetrias, notamos que $\alpha^2 = R_{\pi}, \alpha^3 = R_{\frac{3\pi}{2}}, \alpha\beta = R_X, \alpha^2\beta = R_M$ e $\alpha^3\beta = R_Y$. Essas relações fornecem a presentação do grupo diedral $D_4 = \langle \alpha, \beta \rangle$, onde $\alpha^4 = id, \beta^2 = id, \beta\alpha = \alpha^3\beta$. As matrizes asssociadas aos elementos do grupo diedral, são ortogonais, ou seja, a seguinte igualdade matricial é verificada:

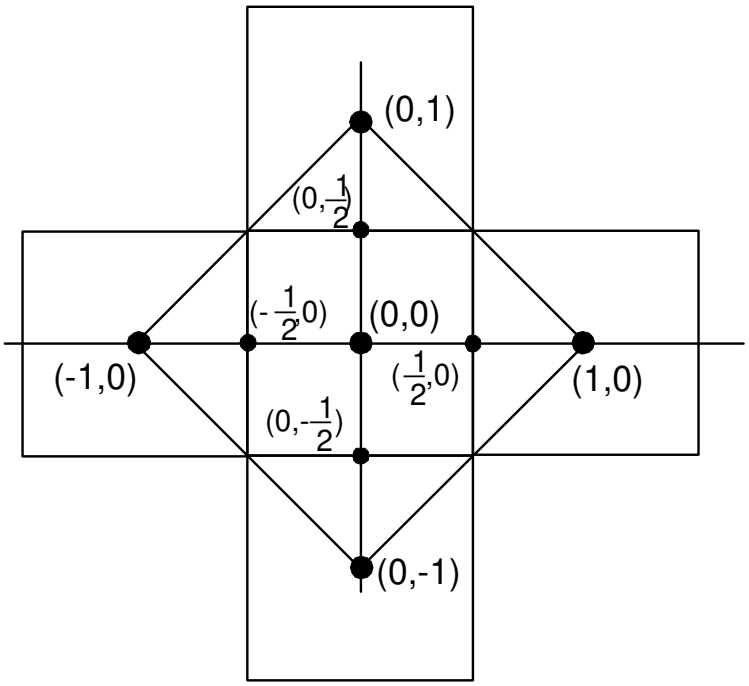

Figura 4.2: Quadrados de área unitária

$$A = M.M^t = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

para cada matriz M do grupo diedral, onde A é a matriz diagonal correspondente a forma quadrática $f(X,Y) = X^2 + Y^2$. Convém destacar neste processo que os vetores u, v da forma $\pm(1,0), \pm(0,1)$ (linhas ou colunas das matrizes M) são as soluções mínimas da forma quadrática $f(X,Y) = 1$. E mais, essas soluções $(x,y) \in \mathbb{R}^2$ são baricentros dos quadrados de área unitária que intercepta o quadrado original em uma aresta conforme ilustrado na Figura 4.2.

4.3 Reticulados em Espaços Euclidianos

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 $N(x) = N(x_1e_1 + \cdots + x_ne_n) =$

$\Sigma_{i=1}^{n}\Sigma_{j=1}^{n}x_ix_je_ie_j = x.M.M^tx^t = x.A.x^t = f(x)$, 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.

Dois reticulados (Λ, f) e (Λ', f') são equivalantes se existir um
$\mathbb{Z}$-isomorfismo entre Λ e Λ' que realiza a mudança de base da forma quadrática f para a forma quadrática f', ou seja, existe uma matriz $P \in GL(n, \mathbb{Z})$ (grupo das matrizes inversíveis), tal que $f(X) = (PX)^tA(PX) = X^tA'X$, onde $A' = P^tAP$.

Por esta relação concluímos que classes de equivalência de reticulados correspondem a classes de equivalência das matrizes positivas definidas associadas, onde a relação de equivalência, $A \simeq A'$ é verificada se, e somente se, existir $P \in GL(n, \mathbb{Z})$ tal que $A' = P'AP$ é positiva definida, $det(A) > 0$, então o **determinante do reticulado** Λ é dado por $d(\Lambda) = det(A)^{\frac{1}{2}}$.

Proposição 4.3.1 *[28]*

i) Seja A uma matriz de uma forma quadrática anisotrópica. Então A é a matriz Gram para alguma base de um reticulado, se existir uma matriz $M \in GL(n, \mathbb{R})$ tal que $A = M^tM$;

ii) Se β e β' são ambas bases de um mesmo reticulado, então a matriz Gram A' associada à base β' pode ser obtida da matriz Gram A associada à base β, através de uma composição por uma transformação ortogonal. Em notação matricial, $A' = PA$, onde P é uma matriz ortogonal.

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

Em [37] 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 aos pontos do reticulado Λ uma estrutura aditiva de grupo. 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 estivessemos operando os elementos do anel de inteiros.

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

Seja um corpo de números $\mathbb{F} = \mathbb{Q}(\theta_1)$ cujo polinômio minimal $p(X)$ associado ao elemento algébrico θ_1 seja sepáravel, com n raízes distintas $\theta_1, \theta_2, \ldots, \theta_n$.

Associado a esta extensão de corpos existem 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-megulhos tais que $\sigma_j(\mathbb{F}) \not\subseteq \mathbb{R}$. 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 (4.1), 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 megulhos associado ao corpo de números $\mathbb{F}$ aplicada num elemento de $\mathbb{F}$, isto é,

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

$$x \longrightarrow (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x) \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)). \tag{4.1}$$

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

Como visto no Capítulo 2, 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 (4.2).

$$u_i = (\sigma_1(\omega_i), \ldots, \sigma_{r_1}(\omega_i), \Re\sigma_{r_1}(\omega_i), \Im\sigma_{r_1}(\omega_i), \ldots, \Re\sigma_{r_1+r_2}(\omega_i), \Im\sigma_{r_1+r_2}(\omega_i)), \tag{4.2}$$

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 $\mathbb{F}$.

4.4 Construção de Constelações Geometricamente Uniformes com p^m Sinais n-Dimensionais

Através das identificações dos anéis de inteiros provenientes de corpos de números no espaço $\mathbb{R}^n$, Interlando e Elia propuseram em [37] 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.

Neste trabalho veremos que é possível obter constelações de sinais de cardinalidade p^m rotuladas 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], [19], [24] e [37] só consideraram a estrutura aditiva do corpo para a efetivação do rotulamento.

A importância da proposta feita em [37] e a que proporemos neste trabalho em relação às propostas [3], [19] e [24], é que elas são válidas para quaisquer dimensões finitas.

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 (4.2), 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 Kummer e uma definição que serão importantes para a realização do rotulamento.

Teorema 4.4.1 *(Lema de Kummer)[40] 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 $\overline{p(X)}$ em polinômios mônicos irredutíveis de grau $f_i (1 \leq i \leq s)$ sobre $\mathbb{Z}_p[X]$, 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 $1 \leq i \leq s$ com a condição de que p não divida o índice $[\mathcal{D}_{\mathbb{F}} : \mathbb{Z}[\theta]]$.*

Definição 4.4.1 *[37] 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 $\mathbb{Q}$ e seja o reticulado $\Lambda = \sigma(\mathcal{D}_{\mathbb{F}})$. 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 4.4.1 exibe de fato quem é o rotulamento.

Proposição 4.4.1 *[37] 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 determinado por $l(\sigma(\theta)) = \overline{\theta}$, onde $\overline{\theta}$ é a raiz do polinômio $p_i(X)$ sobre $GF(p)$.*

Demonstração Usando as propriedades das aplicações φ, pr e σ, temos que $l(\sigma(x_1\omega_1 + \cdots + x_n\omega_n)) = \varphi(pr(\sigma^{-1}(\sigma(x_1\omega_1 + \cdots + x_n\omega_n)))) = \varphi(pr(x_1\omega_1 + \cdots + x_n\omega_n)) = \varphi(pr(x_1\omega_1) + \cdots + pr(x_n\omega_n)) = \varphi(pr(x_1\omega_1)) + \cdots + \varphi(pr(x_n\omega_n)) = x_1\varphi(pr(\omega_1)) + \cdots + x_n\varphi(pr(\omega_n)) = l(\sigma(x_1\omega_1)) + \cdots + l(\sigma(x_n\omega_n))$. ∎

Como consequência da Proposição 4.4.1, fica claro o Corolário (4.4.1).

Corolário 4.4.1 *[37] Se α e γ são elementos de uma mesma classe lateral $\mathcal{P}_j$ em $\mathcal{D}_{\mathbb{F}}$, então $l(\sigma(\alpha)) = l(\sigma(\gamma))$.*

Com o objetivo de estender o rotulamento proposto por Interlando e Elia em [37] para outras estruturas algébricas é que consideraremos o próximo resultado.

Proposição 4.4.2 *Seja $\mathcal{D}_{\mathbb{F}}$ o anel de inteiros do corpo de números $\mathbb{F} = \mathbb{Q}(\theta)$. Com as mesmas condições do Teorema 4.4.1, 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^{f_i}, são dados por $\mathcal{P}_i = \left\langle p^{f_i}, p_i(\theta) \right\rangle$ e que $\mathcal{D}_{\mathbb{F}}/\mathcal{P}_i \simeq GF(p^{f_i})$. Então existem ideais I em $\mathcal{D}_{\mathbb{F}}$ dados por $I = \mathcal{P}_i^n$, tais que o quociente $\mathcal{D}_{\mathbb{F}}/I \simeq G_{p^{nf_i}}$, onde $m = p^{nf_i}$.*

Demonstração:

Seja p um número primo fatorável em $\mathcal{D}_{\mathbb{F}}$, então do Teorema 4.4.1 existe um ideal $\mathcal{P}_i$ de norma euclidiana p. Tomando-se as n-potências do ideal $\mathcal{P}_i$, encontraremos os ideiais $I = \mathcal{P}_i^n$ de normas euclidianas 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.

Definição 4.4.2 *Seja $\mathbb{F} = \mathbb{Q}(\theta)$ um corpo de números de grau n, onde $\theta \in \mathcal{D}_{\mathbb{F}}$. Seja o reticulado $\Lambda = \sigma_{\mathbb{F}}(\mathcal{D}_{\mathbb{F}})$. Dados um número primo p e um inteiro positivo m, uma aplicação $l : \Lambda \longrightarrow G_{p^m}$ 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 $1 \leq i \leq n$.*

4.4.1 Aspectos geométricos dos anéis $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$

Em [19] e [24], Favareto et-al. propuseram procedimentos para construção de reticulados (constelações de sinais) no plano complexo, cujos pontos de sinais são identificados por representantes das classes laterais de anéis de inteiros de energia mínima com rótulos em corpos de Galois $GF(p)$.

O procedimento de rotulamento proposto em [19] consiste primeiramente em determinar se um número primo p é fatorável em um anel de inteiros.

Para os primos que são fatoráveis o procedimento é tormar o quociente do anel pelo ideal gerado por um dos fatores irredutíveis da correspondente fatoração. Deste quociente obtem-se um corpo de cardinalidade prima.

Antes, apresentaremos uma maneira natural de identificar anéis de inteiros provenientes de extensões quadráticas imaginárias em $\mathbb{R}^2$.

Consideremos os anéis de inteiros $\mathbb{Z}[\theta]$, para $\theta = i$, se a extensão é a $\mathbb{Q}(\sqrt{-1})$, e $\theta = \omega$ se a extensão for $\mathbb{Q}(\sqrt{-3})$. Veremos que há uma identificação natural dos elementos destes anéis com os elementos de um reticulado em $\mathbb{R}^2$, e que o recobrimento de $\mathbb{R}^2$ por paralelogramos e/ou hexágonos é realizável através da identificação dos vértices e/ou centros desses polígonos com os elementos dos correspondentes anéis.

O Teorema 4.4.2 explicita de que maneira esta indentificação será realizada.

Teorema 4.4.2 *Seja $\alpha_{(a,b)} = a + b\theta$ um elemento de um anel de inteiros $\mathbb{Z}[\theta]$ de $\mathbb{Q}(\sqrt{-m})$, 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, equanto que $\alpha_{(a,b+1)}$ e $\alpha_{(a,b-1)}$ são identificados como sendo os outros dois 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 $\alpha_{(a,b)}$.

Demonstração:

1) Para $-m \equiv 2, 3 \ mod\, 4$, temos que $\theta = i\sqrt{m}$. Logo, $\alpha_{(a,b)} = a + b\theta = a + ib\sqrt{m}$. Por outro lado,

$\alpha_{(a+1,b)} = (a+1) + b\theta = (a+1) + ib\sqrt{m} = a + ib\sqrt{m} + 1 = \alpha_{(a,b)} + 1,$

$\alpha_{(a-1,b)} = (a-1) + b\theta = (a-1) + ib\sqrt{m} = a + ib\sqrt{m} - 1 = \alpha_{(a,b)} - 1,$

$\alpha_{(a,b+1)} = a + (b+1)\theta = a + i(b+1)\sqrt{m} = a + ib\sqrt{m} + i\sqrt{m} =$
$\alpha_{(a,b)} + i\sqrt{m},$

$\alpha_{(a,b-1)} = a + (b-1)\theta = a + i(b+1)\sqrt{m} = a + ib\sqrt{m} - i\sqrt{m} =$
$\alpha_{(a,b)} - i\sqrt{m}.$

Portanto, $\alpha_{(a+1,b)} = \alpha_{(a,b)} + 1, \alpha_{(a-1,b)} = \alpha_{(a,b)} - 1,$
$\alpha_{(a,b+1)} = \alpha_{(a,b)} + i\sqrt{m}, \alpha_{(a,b-1)} = \alpha_{(a,b)} - i\sqrt{m}.$

2) Para $-m \equiv 1 \ mod\, 4$, temos que $\theta = \frac{1+i\sqrt{m}}{2}$. Logo, $\alpha_{(a,b)} = a + b\theta = a + ib(\frac{1+i\sqrt{m}}{2}) = \frac{2a+b}{2} + i\frac{b\sqrt{m}}{2}$.

Por outro lado,

$\alpha_{(a+1,b)} = \frac{2(a+1)+b}{2} + i\frac{b\sqrt{m}}{2} = \frac{2a+b}{2} + i\frac{b\sqrt{m}}{2} + 1,$

$\alpha_{(a-1,b)} = \frac{2(a-1)+b}{2} + i\frac{b\sqrt{m}}{2} = \frac{2a+b}{2} + i\frac{b\sqrt{m}}{2} - 1,$

$\alpha_{(a-1,b+1)} = \frac{2(a-1)+(b+1)}{2} + i\frac{(b+1)\sqrt{m}}{2} = \frac{2a+b}{2} + i\frac{b\sqrt{m}}{2} + (\frac{-1+i\sqrt{m}}{2}),$

$\alpha_{(a+1,b-1)} = \frac{2(a+1)+(b-1)}{2} + i\frac{(b-1)\sqrt{m}}{2} = \frac{2a+b}{2} + i\frac{b\sqrt{m}}{2} - (\frac{-1+i\sqrt{m}}{2}),$

$\alpha_{(a,b+1)} = \frac{2a+(b+1)}{2} + i\frac{(b+1)\sqrt{m}}{2} = \frac{2a+b}{2} + i\frac{b\sqrt{m}}{2} + (\frac{1+i\sqrt{m}}{2})$

e $\alpha_{(a,b-1)} = \frac{2a+(b-1)}{2} + i\frac{(b-1)\sqrt{m}}{2} = \frac{2a+b}{2} + i\frac{b\sqrt{m}}{2} - (\frac{1+i\sqrt{m}}{2}).$

Logo,

$\alpha_{(a+1,b)} = \alpha_{(a,b)} + 1, \qquad \alpha_{(a-1,b)} = \alpha_{(a,b)} - 1,$

$\alpha_{(a-1,b+1)} = \alpha_{(a,b)} + (\frac{-1+i\sqrt{m}}{2}), \qquad \alpha_{(a+1,b-1)} = \alpha_{(a,b)} - (\frac{-1+i\sqrt{m}}{2}),$

$\alpha_{(a,b+1)} = \alpha_{(a,b)} + (\frac{1+i\sqrt{m}}{2}), \qquad \alpha_{(a,b-1)} = \alpha_{(a,b)} - (\frac{1+i\sqrt{m}}{2}).$

Por simples inspeção, vemos que $\alpha_{(a+1,b)}$ e $\alpha_{(a-1,b)}$ estão a uma distância euclidiana 1 de $\alpha_{(a,b)}$, e que $\alpha_{(a-1,b+1)}, \alpha_{(a+1,b-1)}, \alpha_{(a,b+1)}, \alpha_{(a,b-1)}$ estão a uma distância euclidiana $\frac{\sqrt{1+m}}{2}$ de $\alpha_{(a,b)}$.

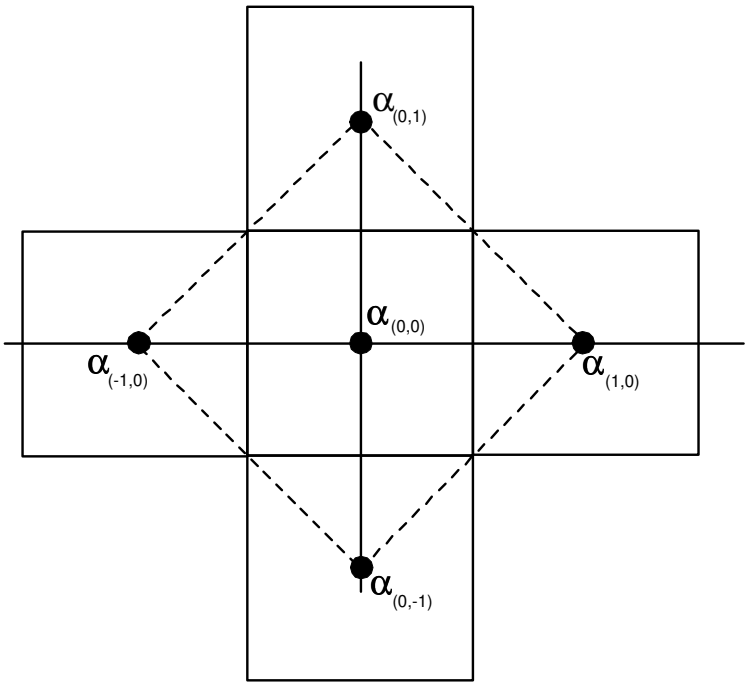

Figura 4.3: Tesselação por quadrados

■

O Corolário 4.4.2 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 $m > 0$.

Corolário 4.4.2 **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;*

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.*

Demonstração:

1) Para que a distância euclidiana seja 1 entre os vértices de um parelelogramo e seu centro implica que $\sqrt{m} = 1$, ou seja $m = 1$. Disto segue que $\theta = i$.

2) Para que a distância euclidiana seja 1 entre os vértices de um hexágono e seu centro implica que $\frac{\sqrt{1+m}}{2} = 1$, ou seja $m + 1 = 4$. Disto segue que $\theta = \frac{1+i\sqrt{3}}{2}$.

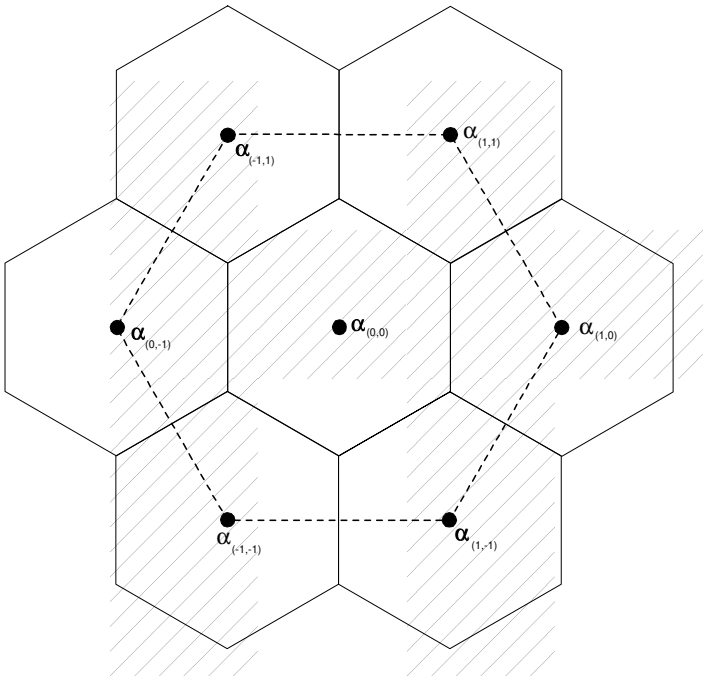

Figura 4.4: Tesselação por hexágonos

■

Corolário 4.4.3 **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 4.4.2 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 4.4.2 como baricentros de hexágonos de área mínima com os elementos do anel de inteiros de Eisenstein-Jacobi.*

Demonstração

i) A válidade do item 1) do Corolário 4.4.3 é uma consequência direta do fato de que uma tesselação $\{4,4\}$ ser formada por quadrados, o que garante que a partir do baricentro e dos vértices de um quadrado, seja possível obter quadrados de área unitária tendo tais

pontos como baricentro, conforme observa-se no quadrado de área 2 da Figura 4.2. Já o recobrimento é uma consequência direta do fato da tesselação $\{4,4\}$ satisfazer a equação $(p-2)(q-2)=4$, isto é, um polígono de p lados, onde cada vértice é recoberto por q polígonos, no caso $p=q=4$.

ii) A demonstração de item 2), segue de maneira análoga ao caso descrito no item 1).

■

Avaliando a forma quadrática $f(X,Y)=X^2+Y^2$ nos baricentros dos quadrados de área unitária, obtidos a partir dos vértices do quadrado de área unitária da Figura 4.2, verificamos que f assume valor 1 nesses pontos. Por outro lado, as soluções mínimas de f são identificadas pelos elementos inversíveis em $\mathbb{Z}[i]$.

Mais do que isso, se considerarmos as transformações associadas às matrizes de determinante 1, matrizes essas geradoras do grupo diedral D_4 descritas na Seção 4.2, temos que esses pontos são vetores linhas ou colunas dessas matrizes, ou seja, os baricentros estão associados às transformações geradoras do grupo diedral.

Vimos nesta seção que o reticulado obtido a partir da tesselação de quadrados de área unitária é identificado pelo anel $\mathbb{Z}[i]$, onde seus elementos são identificados pelos baricentros desses polígonos.

Na Seção 4.2 vimos 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 outro lado, é a norma dos elementos de $\mathbb{Z}[i]$. Mostramos indiretamente que para cada ponto do reticulado $\mathbb{Z}[i]$, existe uma transformação resultante de composições das transformações geradoras de D_4 que desloca a origem a esse ponto, e que o determinante desta transformação é dado pela forma quadrática f.

No caso da tesselação do plano $\mathbb{R}^2$ ser por hexágonos regulares, de maneira análoga ao caso da tesselação do plano $\mathbb{R}^2$ por quadrados, temos que a forma quadrática $f'(X,Y)=X^2+XY+Y^2$, que é a norma dos elementos de $\mathbb{Z}[\omega]$, é também a forma quadrática associada ao reticulado $\mathbb{Z}[\omega]$, com as mesmas identificações de pontos de $\mathbb{Z}[\omega]$ por transformações compostas

pelas transformações geradoras de D_6 o grupo de simetrias de um hexágono regular.

4.4.2 Construção de constelações geometricamente uniformes com p^m sinais bidimensionais

As constelações com p^m sinais que realizaremos geometricamente em $\mathbb{R}^2$, são constituídas por representantes de classes laterais de energia mínima nos anéis $\mathbb{Z}[\theta]$ por meio de ideais I de norma algébrica p^m para $\theta = i$ ou $\theta = \omega$, 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 que se um elemento de $\mathbb{Z}[\theta]$ possui norma algébrica 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 $\mathcal{P}$ um ideal primo de $\mathbb{Z}[\theta]$. 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 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 $\mathbb{Z}[\theta]$ que sejam pontências de um ideal primos $\mathcal{P}$ em $\mathbb{Z}[\theta]$, o que permite a construção das constelações com p^m sinais a partir das extensões finitas de $\mathbb{Z}[\theta]/\mathcal{P}$, isto é, as extensões $\mathbb{Z}[\theta]/I \supset \mathbb{Z}[\theta]/\mathcal{P}$.

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 [19] é possível construir constelações com p sinais, em $\mathbb{Z}[i]$

somente nos casos em que $p = 2$ ou $p = 4k + 1$. 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 $p = 6k + 1$.

Proposição 4.4.3 **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 $N(\alpha) = x^2 + y^2 = p$. Logo, tomando $\alpha^2 = (x+iy)^2 = (x^2+y^2) + i(2xy)$, tem-se que $N(\alpha^2) = N(\alpha)N(\alpha) = p.p = p^2$. 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 $N(\alpha) = N(p) = p.p = p^2$. 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 $N(\alpha) = N(p)N(1-\omega) = p^2.1 = p^2$. O ideal I em $\mathbb{Z}[\omega]$, neste caso, é $I = \langle p(1-\omega) \rangle$.

■

Proposição 4.4.4 *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 $m = 2k$, 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 $N(\alpha) = x^2+y^2 = p$. Tomando $\gamma = \alpha^m$, temos que $N(\gamma) = N(\alpha^m) = p^m$. Neste caso o ideal I em $\mathbb{Z}[i]$, será dado por $I = \langle \alpha^m \rangle$.

2) Caso em que $p = 4k+3$, com $k \in \mathbb{Z}$. Da Proposição 4.4.3, com $p = 4k+3$, seja $\alpha = p$, então $N(\alpha) = N(p) = p.p = p^2$. Tomando $\gamma = \alpha^k$, sua norma será $N(\gamma) = N(\alpha^k) = (p^2)^k$. Neste caso o ideal I em $\mathbb{Z}[i]$, é dado por $I = \left\langle \alpha^k \right\rangle$.

■

Proposição 4.4.5 *É possível construir constelações com p^m sinais em $\mathbb{Z}[\omega]$ para quaisquer números primos que sejam fatoráveis em $\mathbb{Z}[\omega]$. Já para os primos p que não são fatoráveis em $\mathbb{Z}[\omega]$ é possível construir constelações de p^m sinais somente para os 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, $N(\alpha) = p$. Logo, tomando-se $\gamma = \alpha^m$, sua norma será $N(\gamma) = N(\alpha^m) = p^m$. 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 $N(\gamma) = N(p^k)N(1-\omega) = p^{2k}.1 = p^m$ Basta tomar o ideal I em $\mathbb{Z}[\omega]$, dado por $I = \langle \gamma \rangle$.

■

Pelas Proposições acima, concluimos que:

1 - Os sinais de uma constelação com p sinais são rotulados apenas por elementos do grupo aditivo de um corpo de Galois $GF(p)$, nos espaços de sinais identificados por $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente.

2.1- Os sinais de uma constelação com p^2 sinais são rotulados por elementos de um corpo de Galois $GF(p^2)/p$-grupo G_{p^2} para valores de p da forma $p = 4k+3/4k+1$, com $k \in \mathbb{Z}$ é um inteiro no espaço de sinais $\mathbb{Z}[i]$.

2.2- Os sinais de uma constelação com p^2 sinais são rotulados por elementos de um corpo de Galois $GF(p^2)/p$-grupo G_{p^2} quando $p(1-\omega)$ é irredutível/redutível no espaço de sinais $\mathbb{Z}[\omega]$.

3 - Os sinais de uma constelação com p^m sinais são rotulados apenas por elementos de um p-grupo G_{p^m}, para $n > 2$, tanto no espaço de sinais $\mathbb{Z}[i]$, quanto no espaços de sinais $\mathbb{Z}[\omega]$.

4.5 Rotulamento Casado de Constelações de Sinais Bidimensionais

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 $\mathbb{Z}[i]$. 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 4.4.1.

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

Passo 1 Se $\gamma = a + b\theta \in \mathbb{Z}[\theta]$ tiver $N(\gamma) = p^m$, para p: primo em $\mathbb{Z}$ vá ao Passo 2, caso contrário, avalie outro $\gamma' \in \mathbb{Z}[\theta]$;

Passo 2 Se $r \in \mathbb{Z}$ a única solução (em s) da equação $a + bs \equiv 0 \, mod \, p^m$, onde $0 \leq r \leq p^m - 1$, vá ao Passo 3, caso contrário vá ao Passo 1;

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

Exemplo 4.5.1 *Considere* $81 = 9(1-w)9(1+w)$. *Seja* I *o ideal primo gerado por* $I = \langle 9 - 9w \rangle$. *Então,* $r = -8$ *é a solução inteira de* $9 - s9 = 81$. *Com isso, o rótulo do elemento* $x + yw$ *em* $\mathbb{Z}[w]$ *é obtido de* $x - 8y \equiv l \, mod \, 81$ *como sendo o elemento do grupo* G_{81}, *onde* $G_{81} = \mathbb{Z}[\omega]/I$.

Exemplo 4.5.2 *Considere* $25 = 5(1-w)5(1+w)$. *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* $GF(25)$ *onde* $GF(25) = \mathbb{Z}[\omega]/I$.

Exemplo 4.5.3 *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}, *onde* $G_{25} = \mathbb{Z}[i]/I$.

Exemplo 4.5.4 *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* $GF(49)$, *onde* $GF(25) = \mathbb{Z}[i]/I$.

Exemplo 4.5.5 *Considere* $125 = (10+5i)(10-5i)$. *Seja* I *o ideal primo gerado por* $I = \langle 10+5i \rangle$. *Então,* $r = 23$ *é solução inteira de* $10 + s5 = 125$. *Com isso, o rótulo do elemento* $x + yi$ *em* $\mathbb{Z}[i]$ *é obtido de* $x + 23y \equiv l \ mod\, 125$ *como sendo o elemento do grupo aditivo* G_{125} *onde* $G_{125} = \mathbb{Z}[i]/I$

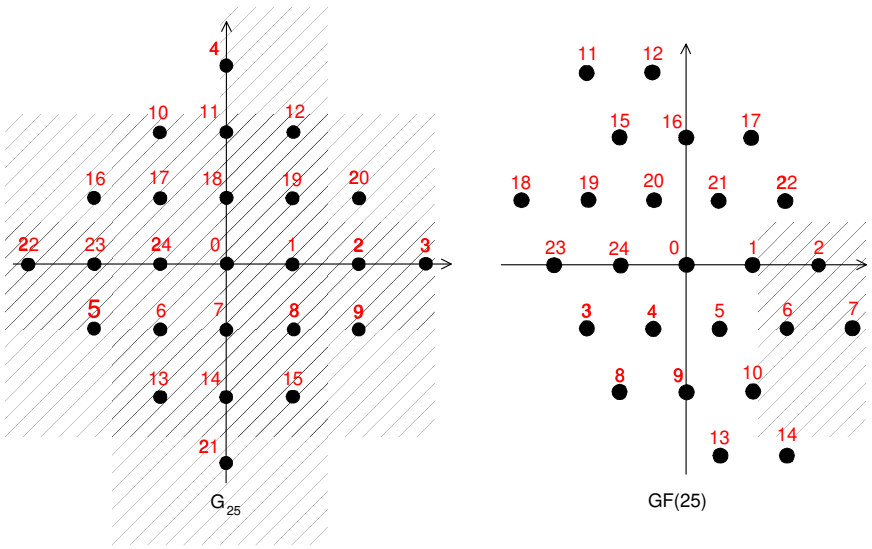

Figura 4.5: Constelações de sinais

A Figura 4.5 fornece as regiões de energia mínima das constelações de sinais $A_{25}[i]$ e $A_{25}[\omega]$ cujos sinais são rotulados pelos elementos do grupo aditivo G_{25} e pelos elementos do grupo aditivo do corpo $GF(25)$, respectivamente.

4.6 Rotulamento de Constelações de Sinais n-Dimensionais

Forneceremos alguns exemplos de constelações com sinais rotulados por elementos dos corpos de Galois $GF(p^m)$ e p-grupos G_{p^m} em espaços de dimensão maior do que 2.

Exemplo 4.6.1 *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 de 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 $l(\sigma(x_0 + x_1\alpha + x_2(-1+\alpha^2)(mod 121\mathbb{Z}[X]) =$
$x_0 + 5x_1 + 24x_2, \forall x_i \in \mathbb{Z}$, *com* $0 \leq i \leq 2$.

Exemplo 4.6.2 *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* $\beta = \{1, \alpha, \alpha^2, \alpha^3\}$. *Tomando* $p(X)$ *módulo* 11, *obtemos* $p(X) = (X-3)(X-4)(X-5)(X-9)(mod 11\mathbb{Z}[X])$. *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 $l(\sigma(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3(mod 11\mathbb{Z}[X]) = x_0 + 3x_1 + 9x_2 + 5x_3, \forall x_i \in \mathbb{Z}$, *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* $\alpha \equiv 3(mod I)$.

A função de rotulamento é $l(\sigma(x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3(mod 121\mathbb{Z}[X]) = x_0 + 3x_1 + 9x_2 + 27x_3, \forall x_i \in \mathbb{Z}$, *com* $0 \leq i \leq 2$.

Capítulo 5

Construção e Rotulamento de Constelações de Sinais no Plano Hiperbólico

5.1 Introdução

Uma constelação de sinais, sob o ponto de vista geométrico, por um bom tempo foi abordada como sendo um subconjunto discreto de pontos em um espaço vetorial euclidiano. Huber [3] e Favareto et.al. [19] consideraram a construção de constelações de sinais no plano complexo onde os sinais foram identificados por elementos de um anel de inteiros. Interlando e Elia em [37] estenderam estes resultados para espaços vetoriais de dimensão finita. Lazari [22], considerou constelações de sinais como sendo um subconjunto discreto de pontos em espaços que podem ser tanto euclidiano quanto hiperbólico. Em todos os trabalhos mencionados, as constelações de sinais apresentam a propriedade de serem geometricamente uniformes, (Forney [1]), ou seja o grupo de isometrias do espaço ambiente que deixa o conjunto de sinais Ω invariante, age de maneira transitiva em Ω. Como consequência, as constelações de sinais apresentam o mesmo perfil de distância independente do sinal escolhido. Com isso, é mais do que suficiente levarmos em consideração no processo de análise, apenas uma região fundamental denominada **região de Voronoi**.

A introdução da teoria de códigos geometricamente uniformes no plano hiperbólico advém do trabalho de Lazari [22] com o estabelecimento do processo de construção de cadeias de par-

tições geometricamente uniformes a partir do grupo de isometrias de um polígono hiperbólico (**domínio fundamental**) para certas tesselações do plano hiperbólico.

Uma maneira de construir e realizar um rotulamento para uma constelação de sinais é considerar o espaço das órbitas no plano hiperbólico, pela ação de um subgrupo normal de um grupo fuchsiano agindo no baricentro de um domínio fundamental de uma tesselação. Por outro lado, existe a dificuldade natural na determinação de tais grupos decorrente do algoritmo de Reidemeister- Schreirer ser um algoritmo computacionalmente complexo, pois o mesmo está inserido no "Problema da Palavra"(do inglês "Word Problem").

Por outro lado, Takeuchi [8] mostrou existir uma identificação de maneira natural entre um grupo fuchsiano aritmético e uma ordem $\mathcal{O}$ de uma álgebra dos quatérnios.

Johansson [11] mostrou que ordens $\mathcal{O}_{\mathbb{Z}[\theta]}$, onde $\mathbb{Z}[\theta]$ é o anel de inteiros de $\mathbb{Q}(\sqrt{m})$ para m um inteiro positivo livre de quadrados, correspondem a específicos grupos fuchsianos aritméticos.

Através do Teorema 5.4.4 mostramos sob que condições existe uma correspondência entre os grupos fuchsianos aritméticos Γ_{4g} derivados de uma álgebra dos quatérnios e ordens $\mathcal{O}_{\mathbb{Z}[\theta]}$.

Nas Seções 5.5 e 5.6 mostraremos que Γ_8 e Γ_{12} são grupos fuchsianos aritméticos derivados de uma álgebra dos quatérnios, e os mesmos correspondem de maneira biunívoca às ordens dos quatérnios $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ e $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$, respectivamente.

Por outro lado, mostraremos através da Proposição 5.7.2 que os ideais $\mathcal{O}_{\mathbb{Z}[I]}$ em $\mathcal{O}_{\mathbb{Z}[\theta]}$ correspondem a subgrupos normais Γ_I do grupo fuchsiano aritmético Γ_{4g}.

Pela identificação a ser realizada entre $\mathcal{O}$ e Γ_{4g}, será indiferente rotularmos os sinais via os elementos do subgrupo normal em Γ_{4g}, ou via os elementos do ideal $\mathcal{O}_{\mathbb{Z}[I]}$ da ordem na álgebra dos quatérnios $\mathcal{O}_{\mathbb{Z}[\theta]}$. Entretanto, a proposta de rotulamento a ser apresentada considerará os ideais da ordem dos quatérnios.

Como consequência, na Seção 5.7 apresentaremos um algoritmo para a realização deste rotulamento.

Inicialmente iremos propor uma maneira de realizar o rotulamento dos elementos da base de uma ordem dos quatérnios pelos elementos de um p-grupo G_{p^m}. Consequentemente,

obteremos o rotulamento da referida ordem na álgebra dos quatérnios.

5.2 Determinação de Γ_{4g}

Consideraremos uma tesselação regular auto-dual $\{4g, 4g\}$ no plano hiperbólico (Definição 2.3.14). Denotaremos o polígono regular de $4g$ lados por F_{4g} e suas arestas, em uma ordem cíclica fixa, por

$$u_1, v_1, u_1^{'}, v_1^{'}, \ldots, u_g, v_g, u_g^{'}, v_g^{'}.$$

O modelo da geometria hiperbólica que usaremos para estudar tais tesselações será o disco de Poincaré, $\mathbb{D}^2$. Sem perda de generalidade, consideraremos o polígono F_{4g} centrado na origem de $\mathbb{D}^2$. A partir deste polígono apresentaremos um procedimento aritmético (Teorema 5.2.1) com o objetivo de determinar as transformações de Möbius que realizam os emparelhamentos das correspondentes arestas.

Os emparelhamentos são realizados por isometrias hiperbólicas do tipo $T_1, S_1, \ldots, T_{2g}, S_{2g}$ tais que $T_i(u_i) = u_i^{'}$ e $S_i(v_i) = v_i^{'}$, $i = 1, \ldots, g$. Para explicitarmos tal tesselação basta determinar a transformação T_1 associada ao emparelhamento da aresta u_1 com a aresta $u_1^{'}$, isto é, $T_1(u_1) = u_1^{'}$. As demais transformações T_i são obtidas através das conjugações $T_i = T_{C^{r_i}} T_1 T_{C^{-r_i}}$ e $S_i = T_{C^{r_i}} T_1 T_{C^{-r_i}}$, onde T_C é uma transformação elíptca de ordem $4g$ que leva a aresta u_1 na aresta adjacente do polígono F_{4g} no sentido anti-horário; o indíce r_i é a potência da tranformação elíptica que leva a aresta u_1 em cada uma das arestas $u_i, u_i^{'}, v_i, v_i^{'}$, para $i = 1, 2, \ldots, g$.

Seja Γ_{4g} o grupo fuchsiano associado ao polígono regular de $4g$ lados, F_{4g}. A assinatura deste grupo fuchsiano é $(g, -)$. Pelo Teorema 2.3.12, a área hiperbólica de F_{4g} é dada por $\mu(F_{4g}) = 2\pi.(2g-2) = 4\pi.(g-1)$.

Se considerarmos o baricentro do polígono F_{4g} e ligá-lo aos seus vértices por segmentos de retas, obteremos $4g$ triângulos hiperbólicos em F_{4g} cada um com área $\frac{\pi(g-1)}{g}$ e com ângulo $\frac{\pi}{2g}$ para o vértice que é o baricentro de F_{4g}.

Da definição de tesselação regular $\{4g, 4g\}$, decorre que cada vértice em F_{4g} tem que ser recoberto por $4g$ polígonos regulares do tipo F_{4g}, ou seja, cada vértice deve possuir ângulo $\frac{\pi}{2g}$.

Desse modo, os triângulos hiperbólicos obtidos são isósceles com ângulos $\frac{\pi}{2g}$ para o vértice no baricentro de F_{4g} e com ângulos $\frac{\pi}{4g}$ nos outros dois vértices de F_{4g}.

A Figura 5.1 mostra uma região fundamental F_{4g} um polígono regular de $4g$ lados de uma tesselação $\{4g, 4g\}$ com o baricentro determinado pelo ponto 0 no disco de Poincaré, com as arestas $v_g^{'}, u_1, v_1$ dadas respectivamente pelos arcos $EH^{'}, H^{'}H, HF$. Consideraremos o ponto D como o centro do círculo isométrico $I(T_1)$ da transformação T_1, o ponto N em $I(T_1), G$ o ponto médio do arco euclidiano $H^{'}H, R$ o raio de $I(T_1)$ e r a reta tangente ao círculo isométrico $I(T_1)$ no ponto H e $\hat{\gamma}, \hat{\alpha}, \hat{\beta}, \hat{d}, \hat{e}, \hat{k}$ são os ângulos determinados pelas relações trigonométricas dos triângulos euclidianos $OD^{'}H$ e ODN e $\hat{t}$ o ângulo determinado pela interseção da reta r e o segmento de reta $\overline{ON}$ (hipotenusa do triângulo ODN).

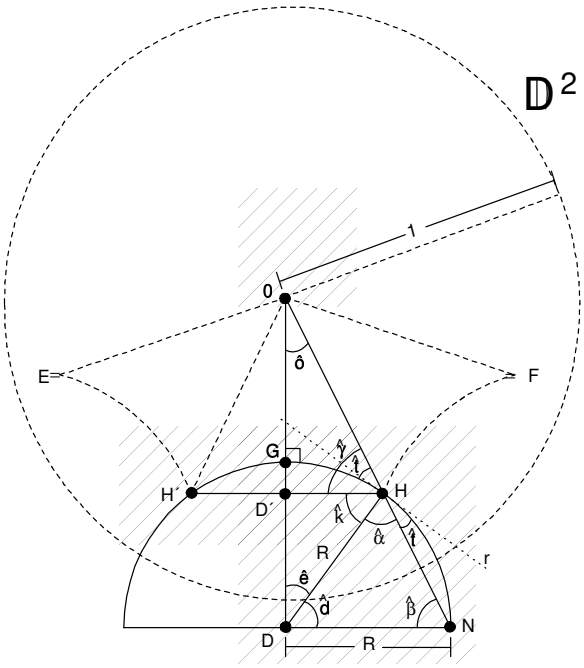

Figura 5.1: Triângulo $\{4g, 4g\}$

Com o objetivo de determinar uma das transformações do grupo fuchsiano Γ_{4g}, é que desenvolveremos a seguir, uma sequência de cálculos culminando na Proposição 5.2.1 e no Teorema 5.2.1.

Nesta direção, seja C a matriz de rotação associada ao elemento elíptico T_C, de ordem $4g$, isto é,

$$C = \begin{bmatrix} e^{\frac{i\pi}{4g}} & 0 \\ 0 & e^{-\frac{i\pi}{4g}} \end{bmatrix}. \tag{5.1}$$

Seja

$$A_1 = \begin{bmatrix} a & c \\ \overline{c} & \overline{a} \end{bmatrix}, \tag{5.2}$$

a matriz associada à transformação hiperbólica $T_1(z) = \frac{az+c}{\overline{c}z+\overline{a}}$. Seja $T_1^{-1}(z)$ a transformação inversa de $T_1(z)$. Então, $T_1^{-1}(z) = \frac{-\overline{a}z+c}{\overline{c}z-a}$. A matriz associada a $T_1^{-1}(z)$ é dada por

$$A_1^{-1} = \begin{bmatrix} -\overline{a} & c \\ \overline{c} & -a \end{bmatrix}. \tag{5.3}$$

Os centros isométricos de T_1 e T_1^{-1} são $I(T_1) = \frac{-\overline{a}}{\overline{c}}$ e $I(T_1^{-1}) = \frac{a}{\overline{c}}$, respectivamente.

Como $T_1(u_1) = u_1'$, a transformação $T_{C^{-2}}$ leva o círculo isométrico $I(T_1)$ em $I(T_1^{-1})$. Vamos usar o fato de $T_{C^{-2}}(\frac{-\overline{a}}{\overline{c}}) = \frac{a}{\overline{c}}$ para determinar os elementos da matriz A_1. Como,

$$T_{C^{-2}}(-\frac{\overline{a}}{\overline{c}}) = \frac{e^{-\frac{i2\pi}{4g}}}{e^{\frac{i2\pi}{4g}}}.(\frac{-\overline{a}}{\overline{c}}) = e^{-\frac{i\pi}{g}}.(\frac{-\overline{a}}{\overline{c}}),$$

temos que $\frac{-\overline{a}}{\overline{c}}e^{-\frac{i\pi}{g}} = \frac{a}{\overline{c}}$, resultando em $a = \pm|a|\sqrt{-e^{-\frac{i\pi}{g}}}$.

Se $x = ln(\sqrt{-e^{-\frac{i\pi}{g}}})$, então $e^{2x} = -e^{-\frac{i\pi}{g}} = -cos(\frac{\pi}{g}) + isen(\frac{\pi}{g})$. Como $g \geq 2$ temos que $0 \leq \frac{\pi}{g} \leq \frac{\pi}{2}$. Consequentemente, teremos

$$-cos(\frac{\pi}{g}) = -cos(\pi - \frac{\pi}{g}) = cos(\frac{(g-1)\pi}{g}),$$

e

$$sen(\frac{\pi}{g}) = sen(\pi - \frac{\pi}{g}) = sen(\frac{(g-1)\pi}{g}).$$

Como, $e^{2x} = e^{i\frac{(g-1)\pi}{g}}$, então, $x = i\frac{(g-1)\pi}{2g}$ e segue que $arg(a) = \frac{(g-1)\pi}{2g}$.

Sem perda de generalidade, suponhamos que u_1 seja a aresta (obtida da região de Ford) entre $arg(\frac{(g-1)\pi}{2g})$ e $arg(-\frac{\pi}{2})$, proveniente do círculo isométrico $I(T_1)$. Este círculo é obtido da

transformação hiperbólica $T_1(z) = \frac{az+c}{\overline{c}z+\overline{a}}$ pela equação $|\overline{c}z + \overline{a}| \equiv 1$ satisfeita precisamente nos pontos em que $T_1(z)$ é simultaneamente uma isometria hiperbólica e euclidiana.

A Figura 5.1, mostra a relação que podemos obter com os triângulos euclidianos mencionados.

Por semelhança de triângulos, obtemos:

$$\hat{\gamma} = \frac{(2g+1)\pi}{4g}, \hat{\alpha} = \hat{\beta} = \frac{(2g-1)\pi}{4g},$$

$$\hat{d} = \frac{\pi}{2g}, \hat{e} = \frac{(g-1)\pi}{2g}, \hat{t} = \frac{\pi}{4g}.$$

Como já vimos o ângulo $\hat{t} = \frac{\pi}{4g}$, e observando a Figura 5.1, temos que $\hat{\alpha} + \frac{\pi}{4g} = \frac{\pi}{2}$, ou seja $\hat{\alpha} = \frac{\pi}{2} - \frac{\pi}{4g} = \frac{(2g-1)\pi}{4g}$.

Por outro lado, sendo ODN um triângulo retângulo euclidiano, no ponto D obtemos que $\hat{\beta} = \frac{(2g-1)\pi}{4g}$, ou seja $\hat{\alpha} = \hat{\beta}$, e daí concluímos que o triângulo DHN é isósceles com $\overline{DH} = \overline{DN}$. Consequentemente, $\overline{DN} = R$, onde R é o raio do círculo isométrico $I(T_1)$. Por esta relação, concluímos que $tan[\frac{(2g-1)\pi}{4g}] = \frac{\overline{OD}}{R}$, ou seja $\overline{OD} = R.tan(\frac{(2g-1)\pi}{4g})$.

De posse desta consideração podemos apresentar a Proposição 5.2.1, que fornecerá as coordenadas polares dos vértices do polígono F_{4g}.

Proposição 5.2.1 *Seja F_{4g} o polígono regular de $4g$ lados, cujo grupo fuchsiano associado é Γ_{4g} com assinatura $(g,-)$. Os vértices do polígono F_{4g}, em coordeanadas polares, são da forma $w^k = \rho.e^{i\frac{2\pi.k}{4g}}$ para $k = 0, \ldots, 4g-1$, onde $\rho = \overline{OH}$.*

Demonstração:

Da Figura 5.1 notamos que o lado $\overline{D'H}$ é paralelo a $\overline{DN}$ o que implica em $\hat{\gamma} \equiv \hat{\beta}$. Logo, $\hat{k} = \hat{\gamma} - \hat{\beta}$. Por outro lado, $cos(\hat{k}) = \frac{\overline{DN}}{R}$, ou seja, $\overline{DN} = R.cos(\hat{k})$. Do triângulo ODN notamos que $cos(\hat{\beta}) = \frac{\overline{D'H}}{\overline{OH}}$, ou seja, $\overline{OH} = \frac{\overline{D'H}}{cos(\hat{\beta})}$. ∎

Sabemos que $|c| = \frac{1}{R}$ e que $\overline{OD} = \frac{|a|}{|c|}$, uma vez que, $I(T_1) = \frac{-\overline{a}}{c}$, implicando em $|a| = tan[\frac{(2g-1)\pi}{4g}]$. Logo, $a = |a|e^{iarg(a)} = tan[\frac{(2g-1)\pi}{4g}](cos\frac{(g-1)\pi}{2g} + isen\frac{(g-1)\pi}{2g})$. Pela igualdade $|a|^2 - |c|^2 = 1$, temos que $|c| = ((tan[\frac{(2g-1)\pi}{4g}])^2 - 1)^{\frac{1}{2}}$. Do triângulo euclidiano ODN observamos que $arg(-\frac{a}{c}) = \frac{\pi}{4g}$. Com isso, temos que

$$\overline{c} = -\frac{|\overline{c}|}{|\overline{a}|}|\overline{a}|e^{-i\frac{(g-1)\pi}{2g}}e^{-i\frac{\pi}{4g}} = -|\overline{c}|e^{-i\frac{(2g-1)\pi}{4g}},$$

resultando na seguinte relação,

$$\overline{c} = -|\overline{c}|(cos\frac{(2g-1)\pi}{4g} - isen\frac{(2g-1)\pi}{4g}) = |\overline{c}|(-cos\frac{(2g-1)\pi}{4g} + isen\frac{(2g-1)\pi}{4g}).$$

Mas, $2g - 1 \geq 1$ implicando que $0 \leq \frac{\pi(2g-1)}{g} \leq \frac{\pi}{2}$. Com isso,

$$-cos(\frac{(2g-1)\pi}{4g}) = -cos(\pi - \frac{(2g-1)\pi}{4g}) = cos(\frac{(2g+1)\pi}{4g}),$$

$$sen(\frac{(2g-1)\pi}{4g}) = sen(\pi - \frac{(2g-1)\pi}{4g}) = sen(\frac{(2g+1)\pi}{4g}),$$

$$\overline{c} = |\overline{c}|(cos(\frac{(2g+1)\pi}{4g}) + isen(\frac{(2g+1)\pi}{4g}).$$

Disto segue que $c = |c|e^{-(\frac{2g+1}{4g})\pi}$. Portanto, $arg(c) = -(\frac{2g+1}{4g})\pi$. Assim,

$$c = ((tan[\frac{(2g-1)\pi}{4g}])^2 - 1)^2 e^{i\frac{(g-1)\pi}{2g}})^2)^{\frac{1}{2}})e^{-(\frac{2g+1}{4g})\pi}.$$

Notamos pelo triângulo euclidiano ODN que $|a| = tan\hat{\beta}$. Consequentemente, $|c|$ pode ser determinado indiretamente. Assim, $arg(a) = \hat{e}$, $|a| = tan\hat{\beta}$, $|c| = ([tan\hat{\beta}]^2 - 1)^{\frac{1}{2}}$ e $arg(c) = -\hat{\gamma}$, o que é suficiente, para a obtenção dos elementos $a, \overline{a}, c, \overline{c} \in \mathbb{C}$ da transformação hiperbólica T_1.

Com isso acabamos de provar o seguinte teorema.

Teorema 5.2.1 *Seja F_{4g} o polígono regular de $4g$ lados, cujo grupo fuchsiano associado é Γ_{4g} com assinatura $(g, -)$. Consideremos u_1 como sendo a aresta entre os argumentos $-\frac{\pi}{2}$ e $-\frac{(g-1)\pi}{2g}$ e T_1 a transformação hiperbólica de emparelhamento das arestas u_1 e u_1' do polígono F_{4g}. Então $T_1(z) = \frac{az+c}{\overline{c}z+\overline{a}}$, onde a e c são dados por*

$$arg(a) = \frac{(g-1)\pi}{2g}, \qquad |a| = tan\frac{(2g-1)\pi}{4g},$$
$$|c| = ([tan\frac{(2g-1)\pi}{4g}]^2 - 1)^{\frac{1}{2}}, \qquad arg(c) = -\frac{(2g+1)\pi}{4g}.$$

As demais transformações hiperbólicas $T_i(u_i) = u_i^{'}$ *e* $S_j(v_j) = v_j^{'}$ *geradoras do grupo fuchsiano* Γ_{4g} *que realizam os emparelhamentos são obtidas pelas conjugações* $T_i = C^{r_i}T_1C^{-r_i}$ *e* $S_j = C^{r_j}T_1C^{-r_j}$

Através deste procedimento de determinação dos geradores de um grupo fuchsiano Γ_{4g} associado ao polígono regular F_{4g} pelas tranformações de emparelhamento de arestas, obtemos que Γ_{4g} é isomorfo a um grupo G cuja presentação é dada por

$$G = \langle a_1, b_1, \ldots, a_g, b_g : a_1b_1a_1^{-1}b_1^{-1}...a_gb_ga_g^{-1}b_g^{-1} = e\rangle.$$

5.3 Reticulados em Álgebras dos Quatérnios

Neste trabalho estamos interessados em realizar particionamento de conjuntos de pontos do plano hiperbólico, constituídos pelos baricentros dos polígonos de uma tesselação regular $\{4g, 4g\}$. Para concretizarmos esta proposta restringiremos este estudo às tesselações em que o grupo fuchsiano Γ_{4g} associado à região fundamental F_{4g} possa ser construído de maneira aritmética.

Veremos que tais grupos fuchsianos herdam propriedades de uma **anel de divisão** (qualquer elemento não divisor de zero no anel possui um inverso multiplicativo). A existência dos grupos fuchsianos dotados desta aritmeticidade é garantida pela associação destes grupos com as álgebras dos quatérnios, como proposto por Takeuchi [8] veja também Katok [7].

Uma **álgebra dos quatérnios** $A = (a, b)_{\mathbb{F}}$ sobre um corpo $\mathbb{F}$ é um espaço vetorial de dimensão 4 sobre $\mathbb{F}$, com uma base $\{1, i, j, ij\}$, satisfazendo a condição de que $i^2 = a, j^2 = b, ij = -ji$ e que $(ij)^2 = -ab$, onde $a, b \in \dot{\mathbb{F}} = \mathbb{F} - \{0\}$. Note que uma álgebra dos quatérnios não é comutativa.

O elemento $\overline{x} = x_0 - x_1 i - x_2 j - x_3 ij \in A$ é dito **conjugado** do elemento $x = x_0 + x_1 i + x_2 j + x_3 ij \in A$. Da estrutura de espaço vetorial de A, para quaisquer $x, y \in A$, onde $x = x_0 + x_1 i + x_2 j + x_3 ij$ e $y = y_0 + y_1 i + y_2 j + y_3 ij$, decorre que

$$\overline{\overline{x}} = x, \qquad \overline{x+y} = \overline{x} + \overline{y}, \qquad \overline{x.y} = \overline{x}.\overline{y}.$$

O traço reduzido e a norma reduzida de um elemento $x \in A$ são denotados por $Trd(x) = x + \overline{x}$ e $Nrd(x) = x.\overline{x}$, respectivamente. Note que $Nrd(x)$ é uma forma quadrática sobre $\mathbb{F}$, cuja correspondente forma bilinear é dada por $B(x, y) = Nrd(x.\overline{y})$. Por um cálculo direto temos que $B(x, x) = Nrd(x.\overline{x}) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$.

Sejam $A = (a, b)_{\mathbb{F}}$ uma álgebra dos quatérnios e M_0, M_1, M_2, M_3, elementos da álgebra de matrizes $M(2, \mathbb{F}(\sqrt{a}))$, dados por

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad M_1 = \begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}, \qquad M_3 = \begin{bmatrix} 0 & -\sqrt{a} \\ b\sqrt{a} & 0 \end{bmatrix}$$

Dado $x = x_0 + x_1 i + x_2 j + x_3 ij \in A$. A aplicação

$$\varphi(x) = g_x = x_0.M_0 + x_1.M_1 + x_2.M_2 + x_3.M_3 = \begin{bmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{bmatrix} \tag{5.4}$$

é um mergulho de A em $M(2, \mathbb{F}(\sqrt{a}))$. Satisfazendo a condição de que $\varphi(i^2) = (\varphi(i))^2, \varphi(j^2) = (\varphi(j))^2$ e $\varphi(ij) = \varphi(i)\varphi(j)$, segue-se que φ é um homomorfismo de álgebra. É imediato constatar que φ é sobrejetor em $M(2, \mathbb{F})$ se, e somente se, $a = t^2$, para algum $t \in \dot{\mathbb{F}}$.

Isto mostra haver duas possibilidades para uma álgebra dos quatérnios A sobre um corpo $\mathbb{F}$: ser isomorfa a álgebra de matrizes $M(2, \mathbb{F})$ (neste caso dizemos que A é **não ramificada**), ou a uma subálgebra de $M(2, \mathbb{F}(\sqrt{a}))$ (neste caso dizemos que A é **ramificada** para algum $a \in \mathbb{F}$) com $\sqrt{a} \notin \mathbb{F}$ possuindo uma estrutura de anel de divisão que denotaremos por $\mathbb{H}$.

Estamos interessados nas álgebras dos quatérnios $A \simeq (a,b)_{\mathbb{F}}$ sobre corpos de números reais. Com o objetivo de estabelecer e/ou identificar quando uma álgebra dos quatérnios A é ou não ramificada sobre um corpo real $\mathbb{F}$ de grau n, é que definiremos os n diferentes **lugares** para verificar se A é ramificada. Para isso, consideraremos os n homomorfismos $\sigma_i^{'}$s do grupo de Galois associado à extensão de corpos $\mathbb{F}$ sobre $\mathbb{Q}$.

Dados uma álgebra dos quatérnios $A \simeq (a,b)_{\mathbb{F}}$ e um homomorfismo $\sigma : \mathbb{F} \to \mathbb{K}$ de corpos, definimos por **lugar de uma álgebra dos quatérnios** A a estrutura algébrica resultante $A^{\sigma} = (\sigma(a), \sigma(b))_{\sigma(\mathbb{F})}$, onde e $A^{\sigma} \otimes \mathbb{K} = (\sigma(a), \sigma(b))_{\mathbb{K}} \simeq M(2,\mathbb{R})$ ou $\mathbb{H}$. Logo, os n diferentes lugares de uma álgebra dos quatérnios $A \simeq (a,b)_{\mathbb{F}}$ são dados pelos $\mathbb{R}$-isomorfismos $\rho_i, i = 1, \ldots, n$, como definidos na equação (5.5), e $\sigma_i : \mathbb{F} \to \mathbb{C}$.

$$\rho_1 : A^{\sigma_1} \otimes \mathbb{R} \to M(2,\mathbb{R}), \qquad \rho_i : A^{\sigma_i} \otimes \mathbb{R} \to \mathbb{H}, \qquad 2 \leq i \leq n. \tag{5.5}$$

onde, A é **não ramificado** em ρ_1 e **ramificado** nos demais ρ_i's. Denotaremos por $Nrd_{\mathbb{H}}$ e $Trd_{\mathbb{H}}$, a norma reduzida e o traço reduzido de $\mathbb{H}$, respectivamente.

Dado $x \in A$, temos

$$Nrd(x) = det(\rho_1(x)), \qquad Trd(x) = tr(\rho_1(x)). \tag{5.6}$$

$$\varphi_i(Nrd(x)) = Nrd_{\mathbb{H}}(\rho_i(x)), \qquad \varphi_i(Trd(x)) = Trd_{\mathbb{H}}(\rho_i(x)). \tag{5.7}$$

Exemplo 5.3.1 *Seja* $\mathbb{H} \simeq (-1,-1)_{\mathbb{R}}$ *a álgebra dos quatérnios de Hamilton e* $\mathbb{H}^1 = \{x \in \mathbb{H} : Nrd_{\mathbb{H}}(x) = 1\}$ *o conjunto dos quatérnios de norma* 1. *Um elemento* x *em* $\mathbb{H}$ *é escrito como* $x = x_0 + x_1 i + x_2 j + x_3 ij$, *onde* $i^2 = j^2 = (ij)^2 = -1$. *A norma reduzida de* x *é* $Nrd_{\mathbb{H}}(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1$, $x \in \mathbb{H}$. *Disso segue que* $|x_0| \leq 1$, *e que* $Trd_{\mathbb{H}}(x) = 2x_0 \in [-2,2]$. *Logo,* $Trd_{\mathbb{H}}(\mathbb{H}^1) = [-2,2]$.

As álgebras dos quatérnios de interesse são aquelas ramificadas nos corpos em que estão definidas. Para isto estudaremos certos invariantes relevantes neste processo.

Um invariante importante nas classes das álgebra dos quatérnios A é seu **discriminante** $d(A)$, definido como sendo o produto dos geradores dos ideais primos nos quais A é ramificada. No caso em que $\mathbb{F} = \mathbb{Q}$, o discriminante é suficiente para determinar as classes de isomorfismos. Todavia para $\mathbb{F} \neq \mathbb{Q}$ mais informações são necessárias.

Sejam $A = (a, b)_{\mathbb{F}}$ uma álgebra dos quatérnios sobre $\mathbb{F}$ e R um anel de $\mathbb{F}$. Diremos que $\Lambda \subseteq A$ é um R-**reticulado** se Λ for um R-módulo finitamente gerado tal que $\mathbb{F}\Lambda = A$. É sempre possível encontrar uma base $\{e_1, e_2, e_3, e_4\}$ de A e um R-ideal t, tal que $\Lambda = te_1 \otimes Re_2 \otimes Re_3 \otimes Re_4$, [10].

Definição 5.3.1 *Um R-reticulado em uma álgebra de quatérnios A sobre um corpo real $\mathbb{F}$ é chamado de R-**ordem** $\mathcal{O}$.*

Proposição 5.3.1 *Uma R-ordem $\mathcal{O}$ possui uma estrutura de um subanel multiplicativo em A.*

Demonstração:

Seja $\mathcal{O} = \{x = x_0 + x_1 i + x_2 j + x_3 ij : x \in A, x_0, x_1, x_2, x_3 \in R\}$, onde $A \simeq (a, b)_{\mathbb{F}}$, e R é um anel de $\mathbb{F}$, com a condição de que $i^2 = a, j^2 = b, (ij)^2 = -ab$ com $a, b \in R$. Sejam $x = x_0 + x_1 i + x_2 j + x_3 ij$ e $y = y_0 + y_1 i + y_2 j + y_3 ij \in \mathcal{O}$ tais que $x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3 \in R$. Assim,

$x.y = (x_0 + x_1 i + x_2 j + x_3 ij)(y_0 + y_1 i + y_2 j + y_3 ij) =$
$(x_0 y_0 + (ab)^2 x_3 y_3 + x_1 y_1 a + x_2 y_2 b) + (x_0 y_1 + x_1 y_0 + x_2 y_3 b + x_3 y_2 b)i + (x_0 y_2 + x_2 y_0 + x_1 y_3 a - x_3 y_1 a)j + (x_0 y_3 + x_3 y_0 + x_1 y_1 - x_2 y_1)ij.$

Pela estrutura de fechamento do anel R, obtemos o fechamento de $\mathcal{O}$.

■

O interesse de se estudar reticulados em álgebras dos quatérnios tem como motivação o fato de que na próxima seção estaremos identificando grupos fuchsianos aritméticos Γ_{4g} associados

aos polígonos F_{4g} provenientes das tesselações $\{4g, 4g\}$ por um reticulado em $\mathcal{O}$ (uma ordem dos quatérnios).

Na Seção 5.2 apresentamos um procedimento para determinar os geradores do grupo fuchsiano Γ_{4g}, que não é necessariamente único. Caso seja adotado um outro procedimento, resultará em um conjunto de geradores distintos para o mesmo grupo. Isto decorre do fato de que um grupo têm diferentes presentações, isto é, diferentes geradores e relações, porém isomorfos.

Analogamente, as correspondentes ordens $\mathcal{O}$ e $\mathcal{O}'$ em A são isomorfas. Tendo como motivação este fato iremos apresentar uma sequência de resultados, culminando no Corolário 5.3.1 demonstrado por Brzezinski em [41], que estabelecerá em que condições duas ordens são isomorfas.

Se Λ e Λ' são dois reticulados em A, com Λ' um subreticulado em Λ, então o índice $[\Lambda : \Lambda']$ de Λ' em Λ é definido por um R-ideal gerado por $det(\varphi)$, ou equivalentemente, a transformação linear $\varphi : A \longrightarrow A$, tal que $\varphi(\Lambda) \subseteq \Lambda'$. Em particular, se Λ e Λ' são reticulados sobre o mesmo anel R, então $[\Lambda : \Lambda']$ é o determinante da matriz que leva a base Λ na base Λ'.

Para um dado R-reticulado Λ em A, definimos seu dual Λ^* por

$$\Lambda^* = \{x \in A : Trd(x\Lambda) \subseteq R\},$$

que também é um reticulado em A.

Se Λ é um reticulado em A, definimos **ordem a direita (esquerda)** $\mathcal{O}_d(\Lambda)(\mathcal{O}_e(\Lambda))$ em Λ da seguinte maneira: $\mathcal{O}_d(\Lambda) = \{x \in A : \Lambda x \subseteq \Lambda\}$ e $\mathcal{O}_e(\Lambda) = \{x \in A : x\Lambda \subseteq \Lambda\}$. Facilmente verifica-se que $\mathcal{O}_d(\Lambda)$ e $\mathcal{O}_e(\Lambda)$ são ambas ordens em A.

Um ideal a direita (esquerda) de uma ordem $\mathcal{O}$ é um reticulado Λ em A tal que $\mathcal{O}\Lambda \subseteq \Lambda(\Lambda\mathcal{O} \subseteq \Lambda)$. Chamamos um ideal de **regular** em $\mathcal{O}$ se este for simultaneamente ideal a direita e a esquerda em $\mathcal{O}$. Se Λ é um reticulado, então Λ é um $\mathcal{O}_d(\Lambda)$-ideal a direita e um $\mathcal{O}_e(\Lambda)$-ideal a esquerda. Por outro lado, um ideal Λ é um **$\mathcal{O}$-ideal principal**, caso exista $x \in A$ tal que $\Lambda = \mathcal{O}x$. O discriminante $d(\mathcal{O})$ de $\mathcal{O}$ é definido pela raiz quadrada de um R-ideal gerado por todos os $det(Trd(x_i.\overline{x_j}))$, onde $\{x_0, x_1, x_2, x_3\} \subseteq \mathcal{O}$, é um conjunto de geradores sobre R.

Exemplo 5.3.2 *Seja $A \simeq (a,b)_{\mathbb{F}}$ uma álgebra dos quatérnios. Então,*

$$\mathcal{O} = R + Ri + Rj + Rij,$$

é uma ordem denotada por $(a,b)_R$. O discriminante de $(a,b)_R$ é $(det(Tr(x_i,\overline{x_j})))^{\frac{1}{2}}$, onde $\{x_0,x_1,x_2,x_3\} = \{1,i,j,ij\}$. Por um cálculo simples, podemos mostrar que $d(\mathcal{O}) = 4ab$.

Dizemos que uma ordem M é **maximal**, se M não está contida em nenhuma outra ordem em A. Se M for uma ordem maximal em A contendo uma outra ordem $\mathcal{O}$ em A, então o discriminante satisfaz

$$d(\mathcal{O}) = d(M).[M:\mathcal{O}], \qquad d(M) = d(A).$$

A diferença de reticulados na álgebra dos quatérnios em relação aos reticulados no espaço euclidiano é que as formas quadráticas associadas aos reticulados neste contexto estão definidas sobre extensões racionais totalmente reais, ao contrário dos reticulados no caso euclidiano, apresentados no Capítulo 4, que estão definidos sobre os racionais. Logo, a discussão de reticulados equivalentes em uma álgebra dos quatérnios é mais geral, uma vez que apenas o discriminante de uma forma quadrática, considerado como invariante, não é suficiente para caracterizar reticulados equivalentes.

O discriminante e a norma associados a um reticulado Λ serão denotados, respectivamente por $d(\Lambda)$ e $N(\Lambda)$. A norma de um reticulado $N(\Lambda)$ é definida pelos $\mathbb{F}$-ideais gerados pela norma de cada $x \in \Lambda$. Denotaremos por $l(\Lambda)$ o ideal $N(\Lambda^*)^{-1}$.

Chamamos uma R-ordem Λ em A de **ordem de Gorenstein** se Λ^* é Λ-projetivo a esquerda (ou a direita) como Λ-módulo, ou equivalentemente, se cada reticulado Λ-regular em A é Λ-projetivo (isto é, a dimensão de Λ^* é reduzida em uma dimensão em relação à Λ). Agora, se cada R-ordem em A contém uma ordem de Gorenstein, então Λ é uma **ordem de Bass**. Chamaremos Λ de **hereditária** se cada Λ-reticulado é Λ-projetivo.

Proposição 5.3.2 *[41] Uma $\mathbb{F}$-ordem Λ em A é hereditária se, e somente se, $d(\Lambda)$ é livre de quadrados.*

Para um dado R-reticulado Λ em A, chamamos de **invariante de Brant** ao produto $b(\Lambda) = d(\Lambda)l(\Lambda)^{-1}$ e Λ é chamado de **semi-ordem** se $1 \in \Lambda$ e $N(\Lambda) = R$. O invariante de Brant é importante por causa do resultado a seguir:

Proposição 5.3.3 *[41] Se Λ é uma semi-ordem em A, então:*

i) Λ é uma ordem se $b(\Lambda) \subset R$;

ii) Λ é uma ordem de Gorenstein se, e somente se, $b(\Lambda) = R$.

Proposição 5.3.4 *[41] Se Λ é uma R-ordem em A, então $G(\Lambda) = l(\Lambda)\Lambda^*\Lambda^*$ é uma ordem de Gorenstein contida em Λ, e mais $\Lambda = \langle 1, b(\Lambda)G(\Lambda)\rangle$; e $[G(\Lambda) : \Lambda] = b(\Lambda)^3$, e $G(\Lambda)$ é chamado de* ***fecho de Gorenstein*** *em Λ. Note que se Λ for uma ordem de Gorenstein, então $G(\Lambda) = \Lambda$. Neste caso $l(\Lambda)\Lambda^*$ é o inverso de Λ^*.*

Uma consequência direta da Proposição 5.3.4 é que através dela podemos obter um resultado que garante em que condições duas ordens dos quatérnios estão na mesma classe de isomorfismo.

Corolário 5.3.1 *[41] Duas R-ordens em A são isomorfas se os correspondentes fechos de Gorenstein são R-isomorfos e os invariantes de Brant são iguais.*

Corolário 5.3.2 *[41] Uma R-ordem Λ em A cujo discriminante $d(\Lambda)$ é livre de cubo é uma ordem de Bass.*

As classes de ordens satisfazem a seguinte inclusão:

$$\{Gorenstein\} \supset \{Bass\} \supset \{Hereditaria\} \supset \{Maximal\}\,.$$

A Proposição 5.3.4 e os Corolários 5.3.1 e 5.3.2 reduzem alguns problemas de descrição e classificação de ordens em álgebras dos quatérnios a problemas de ordens de Gorenstein. As propriedades destas ordens dependem de alguns invariantes cuja definição é motivada pelo seguinte resultado.

Proposição 5.3.5 *[41] Seja R um anel sobre um corpo $\mathbb{F}$ e M seu ideal maximal em R. Se Λ é uma R-ordem em A, então a dimensão de $\Lambda/J(\Lambda)$ sobre $\mathbb{F} = R/M$ divide $dim_{\mathbb{F}}A = 4$, onde $J(\Lambda)$ denota o* ***radical de Jacobson*** *de Λ, que é o ideal em Λ formado pela interseção dos ideais maximais em Λ.*

Definição 5.3.2 *Quando $\mathcal{O}$ é um anel de divisão definiremos os* ***invariantes de Eichler*** *por*

i) $e(\mathcal{O}) = 1$, *se* $\mathcal{O}/J(\mathcal{O}) \simeq \mathbb{F} \oplus \mathbb{F}$;

ii) $e(\mathcal{O}) = 0$, *se* $\mathcal{O}/J(\mathcal{O}) \simeq \mathbb{F}$;

iii) $e(\mathcal{O}) = -1$, *se* $\mathcal{O}/J(\mathcal{O})$ *é uma extensão quadrática de* $\mathbb{F}$.

Note que o invariante de Eichler $e(\mathcal{O})$ é definido pela determinação de qual tipo de particionamento o radical de Jacobson $J(\mathcal{O})$ realiza na ordem $\mathcal{O}$, e de qual estrutura algébrica é rotulada em $\mathcal{O}$ pelas classes laterais módulo o ideal $J(\mathcal{O})$.

Embora seja garantido o particionamento por meio do radical de Jacobson, este procedimento não é de nosso interesse uma vez que ao fixarmos um valor de g para a tesseleção $\{4g, 4g\}$ estamos concomitantemente fixando a estrutura algébrica de rotulamento para a constelação. Por outro lado, se desejarmos uma outra estrutura algébrica teremos que alterar o valor de g e, consequentemente a tesselação $\{4g, 4g\}$. O problema decorrente da busca por outras tesselações variando g, é o aumento do cálculo computacionalmente. Como um indicativo deste aumento, basta observar os cálculos realizados para as tesselações $\{8, 8\}$ e $\{12, 12\}$ nas Seções 5.5 e 5.6. Como conseqüência deste fato procuraremos novos métodos, de modo a realizar particionamentos casados a estruturas algébricas em uma ordem $\mathcal{O}$ para uma mesma tesselação $\{4g, 4g\}$ com complexidade reduzida.

5.4 Identificação de Grupos Fuchsianos Aritméticos com Álgebras dos Quatérnios

Em [8] Takeuchi mostrou que é possível obter grupos fuchsianos a partir das álgebras dos quatérnios de maneira aritmética. Tais grupos são denominados **grupos fuchsianos aritméticos**.

Como consequência, estes grupos herdam propriedades de uma subálgebra na álgebra dos quatérnios.

Com o intuito de explicitar tais propriedades iremos nos deter nos elementos de norma mínima de uma ordem $\mathcal{O}$ na álgebra dos quatérnios A, isto é, no conjunto
$\mathcal{O}^1 = \{x \in \mathcal{O} : Nrd(x) = 1\}$.

Proposição 5.4.1 *O conjunto* $\mathcal{O}^1 = \{x \in \mathcal{O} : Nrd(x) = 1\}$ *é um subanel multiplicativo de* $\mathcal{O}$.

Demonstração: Dados $x = x_0 + x_1 i + x_2 j + x_3 ij$ e $y = y_0 + y_1 i + y_2 j + y_3 ij$ em $\mathcal{O}^1$, com $x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3 \in R$ (anel de inteiros de $\mathbb{F}$), pela Proposição 5.3.1, vimos que os coeficientes do produto xy estão em R. Aplicando a norma reduzida em xy, temos que $Nrd(xy) = Nrd(x).Nrd(y) = 1.1 = 1$. Portanto, $xy \in \mathcal{O}^1$.

■

Se tomarmos a restrinção do homomorfismo ρ_1 em $\mathcal{O}^1$, equação (5.5), então a imagem de $\mathcal{O}^1$ é um subgrupo de $SL(2, \mathbb{R})$. Isto garante que $\rho_1(\mathcal{O}^1)$ é um anel de divisão, uma vez que todos os elementos de $SL(2, \mathbb{R})$ são inversíveis com determinante 1. Mais do que isso, o quociente $\Gamma(A, \mathcal{O}) = \rho_1(\mathcal{O}^1)/\{+1_2, -1_2\}$ é um subgrupo de $PSL(2, \mathbb{R})$, ou seja, o homomorfismo ρ_1 leva a estrutura multiplicativa da aplicação norma reduzida em $\mathcal{O}^1$ na estrutura multiplicativa da aplicação determinante em $SL(2, \mathbb{R})$.

O Teorema a seguir mostra que $\Gamma(A, \mathcal{O})$ é um grupo fuchsiano.

Teorema 5.4.1 *[8]* $\Gamma(A, \mathcal{O})$ *é um grupo fuchsiano.*

Demonstração: Mostraremos para o caso em que A é um anel de divisão sobre um corpo racional quadrático $\mathbb{Q}(\sqrt{m})$, onde m é um inteiro positivo livre quadrados, ou seja, $A \simeq (a, b)_{\mathbb{Q}(\sqrt{m})}$, com $a > 0$, e

$$\mathcal{O}^1 = \{x = x_0 + x_1 i + x_2 j + x_3 ij : x_0, x_1, x_2, x_3 \in R\},$$

onde R é o anel de inteiros de $\mathbb{Q}(\sqrt{m})$. Vimos anteriormente que a imagem de $\mathcal{O}^1$ através de $\rho_1(\mathcal{O}^1)$ está contida em $PSL(2, \mathbb{R})$. O nosso objetivo será mostrar que $\rho_1(\mathcal{O}^1)$ é um subgrupo

discreto de $PSL(2,\mathbb{R})$. Para isso, é suficiente determinar uma vizinhança de $SL(2,\mathbb{R})$, que não contenha outros elementos de $\rho_1(\mathcal{O}^1)$, a menos da identidade em $SL(2,\mathbb{R})$, denotada por id.

Consideremos uma vizinhança V da id em $SL(2,\mathbb{R})$, dada por:

$$V = \left\{ (g_{ij})_{i,j=1,2} \in SL(2,\mathbb{R}) : |g_{11}-1| < \frac{1}{2}; |g_{12}|, |g_{21}| < \frac{1}{2}; |g_{22}-1| < \frac{1}{2} \right\}$$

Suponha que exista $g_x \in \rho_1(\mathcal{O}^1) \cap V$, onde $g_{11} = x_0 + x_1\sqrt{a}, g_{12} = x_2 + x_3\sqrt{a}, g_{21} = b(x_2 - x_3)\sqrt{a}, g_{22} = x_0 - x_1\sqrt{a}$, com $x_0, x_1, x_2, x_3 \in R$, onde R é o anel de inteiros de $\mathbb{Q}(\sqrt{m})$.

Note que $|(g_{11}-1)+(g_{22}-1)| \leq |g_{11}-1|+|g_{22}-1| < \frac{1}{2}+\frac{1}{2} = 1$, ou melhor, $|g_{11}+g_{22}-2| \leq 1$, isto é, $|2x_0-2| < 1$, o que implica que $x_0 = 1$, pois x_0 é inteiro. Como $b > 1$, temos $|x_2 - x_3\sqrt{a}| < \frac{1}{2b} < \frac{1}{2}$.

Assim, $|(x_2 - x_3\sqrt{a}) + (x_2 + x_3\sqrt{a})| \leq |x_2 - x_3\sqrt{a}| + |x_2 + x_3\sqrt{a}| < \frac{1}{2} + \frac{1}{2} = 1$, ou seja, $|2x_2| < 1$, acarretando em $x_2 = 0$.

Por outro lado, $|g_{12}| < \frac{1}{2}$, ou melhor $|x_1\sqrt{a}| < \frac{1}{2}$ e $|x_3\sqrt{a}| < \frac{1}{2}$, implicando em $x_1 = x_3 = 0$. Assim, $g_x = id$.

Conclusão, se $g_x \in \rho_1(\mathcal{O}^1) \cap V$, então $g_x = id$, ou seja, $\Gamma(A,\mathcal{O})$ é um subgrupo discreto de $PSL(2,\mathbb{R})$, garantindo que $\Gamma(A,\mathcal{O})$ é um grupo fuchsiano.

■

Quando Γ for um subgrupo de índice finito para algum $\Gamma(A,\mathcal{O})$, diremos que Γ é um **grupo fuchsiano derivado da álgebra dos quatérnios** A.

Dois grupos são chamados **comensuráveis** se a interseção destes grupos têm índice finito em cada um dos grupos. Se Γ é comensurável para algum $\Gamma(A,\mathcal{O})$, então Γ é chamado **grupo fuchsiano aritmético**. São esses os grupos que estamos interessados, cujo objetivo é aliar a aritmicidade à estrutura geométrica proveniente destes grupos na construção das constelações de sinais geometricamente uniformes no plano hiperbólico.

Uma das maneiras de caracterizar os grupos fuchsianos aritméticos Γ é através do conjunto formado pelos traços dos elementos em Γ.

Para um corpo $\mathbb{F}$, seja

$$SL(2,\mathbb{F}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{F}, ad-bc=1 \right\}$$

e $PSL(2,\mathbb{F}) = SL(2,\mathbb{F})/\{+1_2, -1_2\}$.

A seguir enunciaremos uma sequência de resultados (do Lema 5.4.1 ao Teorema 5.4.3) demonstrados em [7] que caracterizarão os grupos fuchsianos $\Gamma(A,\mathcal{O})$ que são aritméticos.

Lema 5.4.1 *Seja Γ um grupo fuchsiano cuja área da região fundamental $\mu(\mathbb{H}^2/\Gamma)$ é finita. Seja $tr(\Gamma)$ o conjunto formado pelos traços dos elementos de Γ tal que estes estejam contidos num corpo de números algébricos $\mathbb{F}$, com dimensão $[\mathbb{F}:\mathbb{Q}]$ finita. Então existe um corpo de números $\mathbb{F}_1, [\mathbb{F}_1:\mathbb{Q}] < \infty$ e $g \in SL(2,\mathbb{R})$, tal que $g^{-1}\Gamma g \subseteq PSL(2,\mathbb{F}_1)$.*

Demonstração: No Capítulo 2 vimos que se Γ é um grupo fuchsiano do primeiro tipo, e portanto não elementar, então Γ conterá ao menos uma transformação hiperbólica T. Sejam e_1, e_2 autovetores da matriz que representa T e λ, λ^{-1} os autovalores correspondentes . Como $Tr(T) > 2$, temos que λ é um número real. Escolheremos e_1, e_2 de tal maneira que $det((e_1,e_2)) > 0$. Seja $g_1 = \frac{1}{\sqrt{det((e_1,e_2))}}(e_1,e_2)$ e $\mathbb{F}_1 = \mathbb{F}(\lambda)$. Então,

$$g_1^{-1} T g_1 = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}.$$

Considere um elemento $T_1 \in \Gamma$, tal que

$$g_1^{-1} T_1 g_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

com $c \neq 0, b > 0$. Seja

$$g_2 = \begin{bmatrix} \sqrt{b} & 0 \\ 0 & \frac{1}{\sqrt{b}} \end{bmatrix},$$

Então $(g_1 g_2)^{-1}\Gamma(g_1 g_2)$ contém os elementos

$$T_0 = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} e \qquad T_1 = \begin{bmatrix} a_1 & 1 \\ c_1 & d_1 \end{bmatrix}, \tag{5.8}$$

para $\lambda \neq 1, c_1 \neq 0$.

Considere um elemento

$$T = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

de $(g_1 g_2)^{-1}\Gamma(g_1 g_2)$.

Então,

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \lambda a & \lambda b \\ \lambda^{-1} c & \lambda^{-1} d \end{bmatrix}, \tag{5.9}$$

está em $(g_1 g_2)^{-1}\Gamma(g_1 g_2)$. O traço desta transformação vale $\lambda a + \lambda^{-1} d$. Assim, se $\lambda a + \lambda^{-1} d \in \mathbb{F}_1$ como $a, b \in \mathbb{F}_1$ então $a + d \in \mathbb{F}_1$. Em particular, $a_1, d_1 \in \mathbb{F}_1$, e como $det(T_1) = 1$ então $c_1 \in \mathbb{F}_1$, obtemos a relação

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a_1 & 1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} aa_1 + bc_1 & a + bd_1 \\ ca_1 + dc_1 & c + dd_1 \end{bmatrix}, \tag{5.10}$$

implicando que $aa_1 + bc_1 \in \mathbb{F}_1$ e $c + dd_1 \in \mathbb{F}_1$. Como $a, a_1, d, d_1, c_1 \in \mathbb{F}_1$, concluímos que $b, c \in \mathbb{F}_1$.

■

Teorema 5.4.2 *Assumindo o enunciado do Lema anterior. Sejam* $\mathbb{F} = \{\mathbb{Q}(tr(T) : T \in \Gamma)\}$ *e* $A = \mathbb{F}[\Gamma] = \left\{\sum_{i=1}^{d} a_i T_i : a_i \in \mathbb{F}, T_i \in \Gamma\right\}$. *Então, A é uma álgebra dos quatérnios sobre* $\mathbb{F}$.

Lema 5.4.2 *Sejam* Γ *um grupo fuchsiano com* $\mu(\mathbb{H}^2/\Gamma) < \infty$;

$$\mathbb{F} = \{\mathbb{Q}(tr(T) : T \in \Gamma)\}; \qquad [\mathbb{F} : \mathbb{Q}] < \infty$$

e $tr(\Gamma) \subset R$, *onde R é o anel de inteiros* $\mathbb{F}$. *Considere* $A = \mathbb{F}[\Gamma] = \left\{\sum_{i=1}^{d} a_i T_i : a_i \in \mathbb{F}, T_i \in \Gamma\right\}$, *e* $\mathcal{O} = R[\Gamma] = \left\{\sum_{i=1}^{d} a_i T_i : a_i \in R, T_i \in \Gamma\right\}$. *Então,* $\mathcal{O}$ *é uma ordem na álgebra dos quatérnios A.*

Lema 5.4.3 *Seja Γ um grupo fuchsiano com $\mu(\mathbb{H}^2/\Gamma) < \infty$ satisfazendo as condições:*

i) *Seja $\mathbb{F} = \{\mathbb{Q}(tr(T) : T \in \Gamma)\}$. Então, $\mathbb{F}$ é um corpo de números de grau finito e $tr(\Gamma)$ está contido em R, o anel de inteiros de $\mathbb{F}$;*

ii) *Seja φ o mergulho de $\mathbb{F}$ em $\mathbb{C}$ diferente da identidade. Então, $\varphi(tr(\Gamma))$ é limitada em $\mathbb{C}$.*

Então, $\mathbb{F} = \{\mathbb{Q}(tr(T) : T \in \Gamma)\}$ é um corpo de números totalmente real. Se φ é o único mergulho de $\mathbb{F}$ em $\mathbb{R}$ tal que φ é diferente da identidade, então $\varphi(tr(\Gamma))$ está contido no intervalo $[-2, 2]$.

Demonstração: Seja $T \in \Gamma$ uma transformação hiperbólica. Sabemos que existe ao menos uma pelo fato de Γ ser não elementar, logo a transformação T é do tipo

$$\begin{bmatrix} u & 0 \\ 0 & 1/u \end{bmatrix}.$$

Seja φ um mergulho de $\mathbb{F}$ em $\mathbb{C}$, com φ diferente da identidade. Estendendo φ a um isomorfismo Ψ de $\mathbb{F}(u)$ em $\mathbb{C}$, mostraremos que $|\Psi(u)| = 1$. Suponha que $|\Psi(u)| \neq 1$. Pela desigualdade $|\varphi(tr(T^m)| = |(\Psi(u))^m + 1/(\Psi(u))^m| \geq |(\Psi(u))^m - 1|/|(\Psi(u))^m|$, o conjunto $\{\varphi(tr(T^m)|m \in \mathbb{Z}\}$ é não limitado, o que contradiz *ii*). Neste caso $|\Psi(u)| = 1$, então

$$\varphi(tr(\Gamma)) = \Psi(u) + 1/\Psi(u) = \Psi(u) + \overline{\Psi(u)}.$$

Logo, $\varphi(tr(\Gamma))$ é um número real contido no intervalo $[-2, 2]$.

■

Lema 5.4.4 *Seja Ψ um mergulho de $\mathbb{F} = \mathbb{F}_1(\lambda)$ em $\mathbb{C}$ tal que $\Psi(\mathbb{F}_1) \neq$ identidade. Então*

i) *Para um elemento T de Γ da forma*

$$T = \begin{bmatrix} a & b \\ b'c_1 & a' \end{bmatrix},$$

temos que $|\Psi(a)| \leq 1$.

ii) *Para um elemento* T_1 *de* Γ *da forma*

$$T_1 = \begin{bmatrix} a_1 & 1 \\ c_1 & a_1^{'} \end{bmatrix},$$

temos que $|\Psi(c_1)| < 0$.

Demonstração: Pelo Lema 5.4.1 e para um dado

$$T = \begin{bmatrix} a & b \\ b^{'}c_1 & a^{'} \end{bmatrix} \in \Gamma,$$

vale a desigualdade $|\Psi(tr(TT_1^m)| \leq 2$. Note que para um dado $a = \alpha_0\lambda + \alpha_1\lambda^{'} \in \mathbb{F}, \Psi(a^{'}) = \Psi(\alpha_0)\Psi(\lambda^{'}) + \Psi(\alpha_1)\Psi(\lambda) = \overline{\Psi(\alpha_0)\Psi(\lambda) + \Psi(\alpha_1)\Psi(\lambda^{'})} = \overline{\Psi(a)}$, desde que $|\Psi(\lambda)| = 1$. Da demonstração do Lema 5.4.3 e do fato de que $\mathbb{F}_1$ é totalmente real, temos que $\Psi(TT_1^m) = \Psi(a\lambda^m) + \Psi(a^{'}(\lambda^{'})^m) = \Psi(a\lambda^m) + \overline{\Psi(a\lambda^m)} = 2Re(\Psi(a).\Psi(\lambda^m) \leq 2$.

Como $\Psi(\lambda)$ não é raiz da unidade, o conjunto $\{\Psi(\lambda)^m | m \in \mathbb{Z}\}$ é um subgrupo denso da unidade de um círculo unitário S^1. Portanto, $|Re(\Psi(a).z)| \leq 1$, para um dado $z \in S^1$, implicando que $|\Psi(a)| \leq 1$, o que prova i).

Provaremos ii), aplicando i) em T_1, temos $|\Psi(a_1)| \leq 1$. Pela equação $det(T_1) = a_1a_1^{'} - c_1 = 1$, temos $\Psi(c_1) = \Psi(a_1a_1^{'}) - 1 = |\Psi(a_1)|^2 - 1 \leq 0$. Pelo fato de que $c_1 \neq 0$, concluímos que $\Psi(c_1) \leq 0$.

■

Proposição 5.4.2 *Seja* Γ *é um grupo fuchsiano com* $\mu(\mathbb{H}^2/\Gamma) < \infty$*, satisfazendo as condições i) e ii) do Lema 5.4.4. Então,* $A(\Gamma)$ *satisfaz a equação (5.5)*

Demonstração: Como vimos no Lema 5.4.1, Γ contém dois elementos:

$$T_0 = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} e \qquad T_1 = \begin{bmatrix} a_1 & 1 \\ c_1 & d_1 \end{bmatrix},$$

para $\lambda \neq 1$ e $c_1 \neq 0$. Mostraremos que $\mathbb{F} = \mathbb{F}_1(\lambda)$ é uma extensão própria de $\mathbb{F}_1$. Se $\mathbb{F}$ é uma extensão própria de $\mathbb{Q}$, então existe um mergulho $\Psi : \mathbb{F} \to \mathbb{C}$ tal que $\Psi(\mathbb{F}_1) \neq id$, onde

id é a identidade. Por outro lado, $\Psi(\lambda)$ e $1/\Psi(\lambda)$ são raízes da equação $x^2 - \Psi(t_0)x + 1 = 0$, onde $t_0 = tr(T_0)$. Pelo Lema 5.4.1, temos que $|\varphi(t_0)| \leq 2$. Portanto, $\Psi(\mathbb{F}) = \Psi(\mathbb{F}_1(\lambda))$, é um corpo imaginário decorrente do fato que se tomarmos a equação $x^2 - \lambda x + 1 = 0$, esta apresenta o discriminante $\Delta = \lambda^2 - 4$ negativo, pois sabemos que $|\lambda| \leq 2$. Por outro lado, como $\mathbb{F}_1$ é totalmente real, $\Psi(\mathbb{F}_1)$ é um corpo real, logo $\mathbb{F}$ não coincide com $\mathbb{F}_1$. Se $\mathbb{F}_1 = \mathbb{Q}$, então t_0 é um inteiro racional tal que $|t_0| \geq 2$. Portanto, o polinômio $x^2 - t_0 x + 1$ é irredutível sobre $\mathbb{Q}$ e $\mathbb{F}$ é uma extensão própria de $\mathbb{F}_1$. Para $a \in \mathbb{F}$, seja $a^{'}$ seu $\mathbb{F}_1$-conjugado, então $1/\lambda = \lambda^{'}$. Sabemos que

$$tr(T_1) = a_1 + d_1 \in \mathbb{F}_1, \tag{5.11}$$

$$tr(T_0 T_1) = a_1\lambda + d_1\lambda^{'} \in \mathbb{F}_1. \tag{5.12}$$

Como λ e $\lambda^{'}$ são linearmente independentes sobre $\mathbb{F}_1$, podemos escrever de maneira única que $a_1 = \alpha_0\lambda + \alpha_1\lambda^{'}$ e $d_1 = \delta_0\lambda + \delta_0\lambda^{'}$. De (5.11), temos que

$$(\alpha_0\lambda + \alpha_1\lambda^{'})\lambda + (\delta_0\lambda + \delta_0\lambda^{'})\lambda^{'} = (\alpha_0\lambda^{'} + \alpha_1\lambda)\lambda^{'} + (\delta_0\lambda^{'} + \delta_0\lambda)\lambda.$$

Assim, $(\alpha_0 - \delta_1)\lambda^2 + (\delta_1 - \alpha_0)(\lambda^{'})^2 = 0$, implicando que $\alpha_0 = \delta_1$. De (5.10) temos que $\alpha_0\lambda + \alpha_1\lambda^{'} + \delta_0\lambda + \delta_1\lambda^{'} = \alpha_0\lambda^{'} + \alpha_1\lambda + \delta_0\lambda^{'} + \delta_1\lambda$. Assim, $\alpha_0 + \delta_0 - \alpha_1 - \delta_1 = 0$, implica em $\alpha_1 = \delta_0$. Disso segue que $d_1 = a_1^{'}$, e como $det(T_1) = 1$, implica que $c_1 \in \mathbb{F}_1$. Consequentemente,

$$T_0 = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{'} \end{bmatrix} e \qquad T_1 = \begin{bmatrix} a_1 & 1 \\ c_1 & a_1^{'} \end{bmatrix},$$

para $\lambda \neq 1$ $c_1 \neq 0, c_1 \in \mathbb{F}_1$.

Note que $\{Id, T_0, T_1, T_0T_1\}$ forma uma base para o espaço vetorial de $A(\Gamma)$ sobre $\mathbb{F}_1$, isto é,

$$A(\Gamma) = \left\{ \begin{bmatrix} a & b \\ b^{'}c_1 & a^{'} \end{bmatrix} : a, b \in \mathbb{F}, c_1 \in \mathbb{F}_1 \right\}.$$

Seja $\{\varphi_i\}, 1 \leq i \leq n$, mergulhos distintos de $\mathbb{F}_1$ em $\mathbb{R}$. Assuma que $\varphi_1 = id$, onde id é a identidade. Estendendo φ a um isomorfismo de $\mathbb{F}_1$ em $\mathbb{C}$ e definindo o mergulho Ψ de $A(\Gamma)$ em $M(2,\mathbb{R})$ por

$$\Psi : \alpha = \begin{bmatrix} a & b \\ b'c_1 & a' \end{bmatrix} \rightarrow \Psi(\alpha) = \begin{bmatrix} \Psi_i(a) & \Psi_i(b) \\ \Psi_i(b'c_1) & \Psi_i(a'_1) \end{bmatrix},$$

então $A^{\varphi_i} = A^{\Psi_i} = \Psi_i(A(\Gamma))$ é uma álgebra dos quatérnios sobre $\Psi_i(\mathbb{F}_1) = \varphi_i(\mathbb{F}_1)$. Assim, $A^{\varphi_1} \otimes \mathbb{R} \simeq M(2,\mathbb{R})$. Da demonstração do Lema 5.4.2 com $\Psi(a') = \overline{\Psi(a)}$, para $2 \leq i \leq n$, concluímos que

$$A^{\varphi_i} = \left\{ \begin{bmatrix} a & b \\ \overline{b}\Psi(c_1) & \overline{a} \end{bmatrix} | a, b \in \Psi(\mathbb{F}), c_1 \in \mathbb{F}_1 \right\}.$$

Através do Lema 5.4.2 e da equação (5.6) concluímos que $A^{\varphi_i} \otimes \mathbb{R} \simeq \mathbb{H}$.

■

Iremos a seguir estabelecer as condições necessárias e suficientes para a determinação de grupos fuchsianos aritméticos.

Teorema 5.4.3 *Seja Γ um grupo fuchsiano com $\mu(\mathbb{H}^2/\Gamma) < \infty$. Então, Γ é derivado de uma álgebra dos quatérnios A sobre um corpo totalmente real $\mathbb{F}$ se, e somente se, Γ satisfaz as condições i) e ii) do Lema 5.4.3.*

Demonstração: Provaremos primeiro a necessidade das condições i) e ii). Seja Γ um subgrupo de índice finito em $\Gamma(A,\mathcal{O})$, onde $\mathcal{O}$ é uma ordem em A. Dado $T \in \Gamma, tr(T) \in \mathbb{F}_1$ e portanto, $\mathbb{F}$ está contido em $\mathbb{F}_1$, de modo que $\mathbb{F}$ é um corpo totalmente real. Como $Trd(\mathcal{O})$ está contido em $R_{\mathbb{F}_1}$(anel de inteiros de $\mathbb{F}_1$), temos que $tr(\Gamma) \subseteq R_{\mathbb{F}}$ (anel de inteiros de $\mathbb{F}$). Com isto, a condição i) é satisfeita. Suponha que $n \geq 2$. Das equações (5.5) e (5.7) segue que $\varphi_i(tr(\Gamma) \subseteq Tr_{\mathbb{H}}(\rho_i(\mathcal{O}^1))$, para $2 \leq i \leq n$. Por outro lado, para $x \in \mathcal{O}^1$, temos que $Nrd_{\mathbb{H}}(\rho_i(x)) = \varphi_i(Nrd(x))$. Como $\rho_i(\mathcal{O})$ está contido em $\mathbb{H}^1 = \{x \in \mathbb{H} | Nrd_{\mathbb{H}}(x) = 1\}$, pelo Exemplo 5.3.1, o $Trd(\mathbb{H})$ coincide com o intervalo $[-2,2]$, e $\varphi_i(tr(\Gamma))$ é limitado em $\mathbb{R}$ para $2 \leq i \leq n$.

Mostraremos que $\mathbb{F} = \mathbb{F}_1$. Suponha que $\mathbb{F}_1$ é uma extensão própria de $\mathbb{F}$. Então para algum $i, \varphi_i(\mathbb{F}) = id, 2 \leq i \leq n$. Usando φ_i e a maneira que definimos $\mathbb{F}$, temos que $tr(\Gamma) = \varphi_i(tr(\Gamma))$ está contido no intervalo $[-2, 2]$. Logo, Γ não contém elementos hiperbólicos, o que é uma contradição com o fato de Γ ser não elementar.

Provaremos agora a suficiência das condições. Note que pelos Lemas 5.4.1 e 5.4.3 e a Proposição 5.4.2, $A(\Gamma)$, e $\mathcal{O}(\Gamma)$ satisfazem as condições de uma álgebra dos quatérnios. É claro que Γ é um subgrupo de $\Gamma(A(\Gamma), \mathcal{O}(\Gamma))$. Como $\mathbb{H}^2/\Gamma$ e $\mathbb{H}^2/\Gamma(A(\Gamma), \mathcal{O}(\Gamma))$ têm volume finito, Γ é um subgrupo finito de índice finito em $\Gamma(A(\Gamma), \mathcal{O}(\Gamma))$. Disto segue que Γ é um grupo fuchsiano derivado de uma álgebra dos quatérnios.

■

Em [11] Johansson mostrou que o processo pode ser aplicado ao caso particular em que $A \simeq (t, s)_{\mathbb{F}}$, onde $\mathbb{F} = \mathbb{Q}(\sqrt{m})$, com m um inteiro positivo. Para tal, basta supor $t > 0$ e $\sqrt{t} \notin \mathbb{F}$, e considerar o mergulho estabelecido pelo homomorfismo φ de $\mathcal{O}$ em $M(2, \mathbb{F}(\sqrt{t}))$, equação (5.4), para um elemento $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{O}$, obtem-se que $\varphi(x) = x_0 M_0 + x_1 M_1 + x_2 M_2 + x_3 M_3$, com a seguinte condição:

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$M_1 = \begin{bmatrix} \sqrt{t} & 0 \\ 0 & -\sqrt{t} \end{bmatrix}, \qquad M_2 = \begin{bmatrix} 0 & r_1 \\ r_2 & 0 \end{bmatrix}.$$

onde $r_1, r_2 \in \mathbb{R}$ são tais que $s = r_1 r_2$.

Através deste homomorfismo, obtemos como elementos geradores do grupo fuchsiano $\Gamma(A, \mathcal{O})$, matrizes do tipo

$$g = \frac{1}{r} \begin{bmatrix} a + b\sqrt{t} & r_1(c + d\sqrt{t}) \\ r_2(c - d\sqrt{t}) & a - b\sqrt{t} \end{bmatrix},$$

onde $a = a_1 + a_2\theta, b = b_1 + b_2\theta, c = c_1 + c_2\theta, d = d_1 + d_2\theta \in \mathbb{Z}[\theta]$, e $\mathbb{Z}[\theta]$ é o anel de inteiros de $\mathbb{Q}(\sqrt{m})$. O determinante de g neste caso pode ser visto pela forma quadrática $det(g) = \frac{1}{r^2}(a^2 - tb^2 - sc^2 + std^2)$.

Katok em [7], e Johansson em [11] mostraram maneiras de se obter grupos fuchsianos aritméticos a partir de uma álgebra dos quatérnios por meio do homomorfismo estabelecido na equação (5.4).

Mostraremos que a recípocra também é verdadeira, ou seja, a partir de um grupo fuchsiano Γ, associaremos uma ordem $\mathcal{O}^1$ de uma álgebra dos quatérnios A.

Teorema 5.4.4 *Se Γ for um grupo fuchsiano cujos elementos geradores são dados por matrizes em $PSL(2,\mathbb{R})$ do tipo;*

$$g = \frac{1}{r}\begin{bmatrix} a+b\sqrt{t} & r_1(c+d\sqrt{t}) \\ r_2(c-d\sqrt{t}) & a-b\sqrt{t} \end{bmatrix},$$

para $a = a_1 + a_2\theta, b = b_1 + b_2\theta, c = c_1 + c_2\theta, d = d_1 + d_2\theta \in \mathbb{Z}[\theta]$, com $r_1 = -r_2 \in \mathbb{Z}$ e $\sqrt{t} \notin \mathbb{Z}[\theta]$, mas com $t \in \mathbb{Z}[\theta]$ onde $\mathbb{Z}[\theta]$ é o anel de inteiros de $\mathbb{Q}(\sqrt{m})$, com m um inteiro positivo livre de quadrados. Então, Γ é identificado numa ordem $\mathcal{O} \simeq (t,s)_{\mathbb{Z}[\theta]}$ de uma álgebra dos quatérnios A sobre $\mathbb{Q}(\sqrt{m})$.

Demonstração: Note que os elementos geradores g de Γ são matrizes em $M(2,\mathbb{Z}[\theta])$. Caso $M(2,\mathbb{Z}[\theta])$ seja visto como um espaço vetorial, este apresentará como geradores as matrizes:

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad M_1 = \begin{bmatrix} \sqrt{t} & 0 \\ 0 & -\sqrt{t} \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 0 & 1 \\ s & 0 \end{bmatrix}, \qquad M_3 = \begin{bmatrix} 0 & \sqrt{t} \\ -s\sqrt{t} & 0 \end{bmatrix}.$$

Tomando a aplicação φ^{-1}, a inversa do homomorfismo injetivo φ de A em $M(2,\mathbb{F}(\sqrt{t}))$, temos que esta aplicação é dada por $\varphi^{-1}(g_x) = x_0 + x_1 i + x_2 j + x_3 ij$, para $g_x = x_0M_0 + x_1M_1 + x_2M_2 + x_3M_3$, caracterizando a ordem $\mathcal{O} \simeq (t,s)_{\mathbb{Z}[\theta]}$.

■

Teorema 5.4.5 *Sejam $T_1, T_2, \ldots, T_k$ os geradores de um grupo fuchsiano Γ_{4g}, identificados por elementos de uma ordem dos quatérnios $\mathcal{O} \simeq (t,s)_{\mathbb{Z}[\theta]}$, onde $\mathbb{Z}[\theta]$ é um anel de inteiros. Então, $tr(T) \in \mathbb{Z}[\theta]$, para quaisquer T obtido pelo produto de elementos de Γ_{4g}.*

Demonstração: Vimos no Teorema 5.2.1 que uma transformação geradora $T_i \in \Gamma_{4g}$, para algum $i \in \{1, \ldots, k\}$ pode ser obtida por uma composição do tipo $T_i = C^{r_i} T_1^{-1} C^{-r_i}$, onde C^{r_i} denota a matriz de rotação. Como sabemos, estas transformações são hiperbólicas. Logo, a transformação T_i apresenta como matriz associada

$$T_i = \begin{bmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{bmatrix},$$

e o $tr(T_i) = \lambda + \frac{1}{\lambda} \in \mathbb{Z}[\theta]$. Por outro lado, como as demais transformações de T_j, para $j = 1, \ldots, k$, com $j \neq i$ são todas conjugadas, concluímos que elas apresentam o mesmo traço de T_i.

Logo, para provarmos os produtos das transformações geradores equivale provarmos os traços das potências de T_i, ou seja $tr(T_i^k) \in \mathbb{Z}[\theta]$.

Provaremos este teorema por indução sobre k.

Mostraremos

i) Para o caso $k = 2$.

ii) Suponha válida a afirmação para $k-1$, mostraremos ser válida para k.

Vejamos o caso i) Temos que

$$(T_i)^2 = \begin{bmatrix} \lambda^2 & 0 \\ 0 & \frac{1}{\lambda^2} \end{bmatrix},$$

com isto, $tr(T_i^2) = \lambda^2 + \frac{1}{\lambda^2}$.

Por outro lado, $(\lambda + \frac{1}{\lambda})^2 = \lambda^2 + \frac{1}{\lambda^2} + 2$. Logo, $\lambda^2 + \frac{1}{\lambda^2} = (\lambda + \frac{1}{\lambda})^2 - 2 \in \mathbb{Z}[\theta]$.

O que prova o caso i).

Vejamos o caso ii) Temos que,

$$(T_i)^k = \begin{bmatrix} \lambda^k & 0 \\ 0 & \frac{1}{\lambda^k} \end{bmatrix},$$

com isto, $tr(T_i^k) = \lambda^k + \frac{1}{\lambda^k}$.

Considerando

$$(\lambda + \frac{1}{\lambda})^k = \begin{pmatrix} k \\ 0 \end{pmatrix} \lambda^k + \begin{pmatrix} k \\ 1 \end{pmatrix} \frac{\lambda^{k-1}}{\lambda} + \begin{pmatrix} k \\ 2 \end{pmatrix} \frac{\lambda^{k-2}}{\lambda^2}$$

$$\cdots + \begin{pmatrix} k \\ k-2 \end{pmatrix} \frac{\lambda^2}{\lambda^{k-2}} + \begin{pmatrix} k \\ k-1 \end{pmatrix} \frac{\lambda}{\lambda^{k-1}} + \begin{pmatrix} k \\ k \end{pmatrix} \frac{1}{\lambda^k}$$

Assim,

$$(\lambda + \frac{1}{\lambda})^k = (\lambda^k + \frac{1}{\lambda^k}) + k(\lambda^{k-2} + \frac{1}{\lambda^{k-2}}) + (k-1)(\lambda^{k-4} + \frac{1}{\lambda^{k-4}}) + \cdots$$

Pela hipótese por indução sobre $k-1$, temos que

$$k(\lambda^{k-2} + \frac{1}{\lambda^{k-2}}) + (k-1)(\lambda^{k-4} + \frac{1}{\lambda^{k-4}}) + \cdots \in \mathbb{Z}[\theta].$$

Logo,

$$\lambda^k + \frac{1}{\lambda^k} = (\lambda + \frac{1}{\lambda})^k - k(\lambda^{k-2} + \frac{1}{\lambda^{k-2}}) + (k-1)(\lambda^{k-4} + \frac{1}{\lambda^{k-4}}) + \cdots \in \mathbb{Z}[\theta].$$

O que prova o teorema. ■

Nas Seções 5.5 e 5.6, mostraremos que os grupos fuchsianos Γ_8 e Γ_{12} associados, respectivamente, aos domínios fundamentais F_8 e F_{12} são aritméticos e derivados das álgebra dos quatérnios sobre os corpos $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$, respectivamente.

5.5 Tesselação $\{8,8\}$ no Plano Hiperbólico

Nesta seção, apresentaremos aspectos aritméticos relacionados a uma tesselação $\{8,8\}$, inicialmente proporemos uma maneira de se gerar um grupo fuchsiano Γ_8 associado ao domínio

fundamental F_8 (octógono) de área hiperbólica $\mu(F_8) = 4\pi(2.2 - 2) = 4\pi$. O cálculo da área de F_8 é uma consequência direta da aplicação do Teorema 2.3.12, observando o fato de que a assinatura do grupo fuchsiano Γ_8 é $(g, -)$, para $g = 2$.

Do procedimento de geração dos geradores do grupo fuchsiano Γ_8, obtemos os vértices do octógono F_8, via a Proposição 5.2.1.

Mostraremos que o grupo fuchsiano Γ_8 é aritmético, e derivado de uma álgebra dos quatérnios sobre $\mathbb{Q}(\sqrt{2})$, e exibiremos a identificação dos geradores de Γ_8 pelos geradores da ordem $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ em uma álgebra dos quatérnios A sobre $\mathbb{Q}(\sqrt{2})$.

Verificaremos que a ordem $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ não é maximal na álgebra dos quatérnios A. Para isto usaremos os resultados do Exemplo 5.3.2.

Como o nosso interesse é obter um rotulamento algébrico via classes laterais do grupo quociente em uma ordem dos quatérnios em A, por ideais em A, precisaremos que essa ordem seja maximal para que o rotulamento seja completo. Como tal condição não será verificada para a ordem $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ indentificada pelo grupo fuchsiano Γ_8, faremos uma mudança de base que levará em uma outra base de uma ordem $\mathcal{O}'_{\mathbb{Z}[\sqrt{2}]}$ que contenha a ordem $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ e seja maximal, para que possamos realizar de maneira completa o rotulamento algébrico nesta nova ordem.

Da análise da Figura 5.1, vimos que os ângulos trigonométricos são dados por

$$\hat{\gamma} = \frac{(2g+1)\pi}{4g}, \hat{\alpha} = \hat{\beta} = \frac{(2g-1)\pi}{4g}, \hat{d} = \frac{\pi}{2g}, \hat{e} = \frac{(g-1)\pi}{2g}, \hat{t} = \frac{\pi}{4g}.$$

Como estamos trabalhando em uma tesselação $\{8, 8\}$, para $g = 2$, obtemos como ângulos trigonométricos, Figura 5.2, os seguintes valores:

$$\hat{o} = \frac{\pi}{8}, \hat{e} = \frac{\pi}{4}, \hat{\gamma} = \frac{5\pi}{8}, \hat{\beta} = \frac{3\pi}{8}, \hat{t} = \frac{\pi}{4}.$$

Pela Proposição 5.2.1, vimos que os vértices do domínio fundamental F_{4g}, são dados por $\omega^k = \rho.e^{\frac{i2\pi.k}{4g}}$, para $k = 1, \ldots, 2g-1$, onde $\rho = \frac{\overline{D'H}}{cos\beta}$. Logo, no caso $\{8, 8\}$ teremos,

$$\rho = \frac{\overline{D'H}}{cos\beta} = \frac{\sqrt{2\sqrt{2}}}{2}(2 - \sqrt{2}).$$

Das relações acima concluímos que os vértices do octógono são dados por:

$w^0 = \rho.e^{\frac{i.2\pi.0}{8}} = \frac{\sqrt{2}\sqrt[4]{2}}{2}(2-\sqrt{2});$

$w^1 = \rho.e^{\frac{i.2\pi.1}{8}} = \frac{\sqrt{2}\sqrt[4]{2}(2-\sqrt{2})(\sqrt{2}+i\sqrt{2})}{2};$

$w^2 = \rho.e^{\frac{i.2\pi.2}{8}} = \frac{\sqrt[4]{2}}{2}(-2+\sqrt{2}i);$

$w^3 = \rho.e^{\frac{i.2\pi.3}{8}} = \frac{\sqrt[4]{2}}{2}(-2-\sqrt{2})+i(2-\sqrt{2});$

$w^4 = \rho.e^{\frac{i.2\pi.4}{8}} = \frac{\sqrt[4]{2}}{2}(2-\sqrt{2});$

$w^5 = \rho.e^{\frac{i.2\pi.5}{8}} = \frac{\sqrt[4]{2}}{2}(-2+\sqrt{2})+i(-2+\sqrt{2});$

$w^6 = \rho.e^{\frac{i.2\pi.6}{8}} = \frac{\sqrt[4]{2}}{2}(i(2-\sqrt{2}));$

$w^7 = \rho.e^{\frac{i.2\pi.7}{8}} = \frac{\sqrt{2}\sqrt[4]{2}(2+\sqrt{2})(-\sqrt{2}+i\sqrt{2})}{2}.$

Seja,

$$C = \begin{bmatrix} e^{\frac{i\pi}{4g}} & 0 \\ 0 & e^{-\frac{i\pi}{4g}} \end{bmatrix}, \tag{5.13}$$

a matriz de rotação que leva uma aresta em outra aresta adjacente no sentido anti-horário em um domínio F_{4g}.

No caso $\{8,8\}$ os emparelhamentos de arestas em F_8 são realizados por transformações hiperbólicas T_i, S_i, para $i = 1, 2$, com

$$T_i(u_i) = u_i', \qquad S_i(v_i) = v_i'.$$

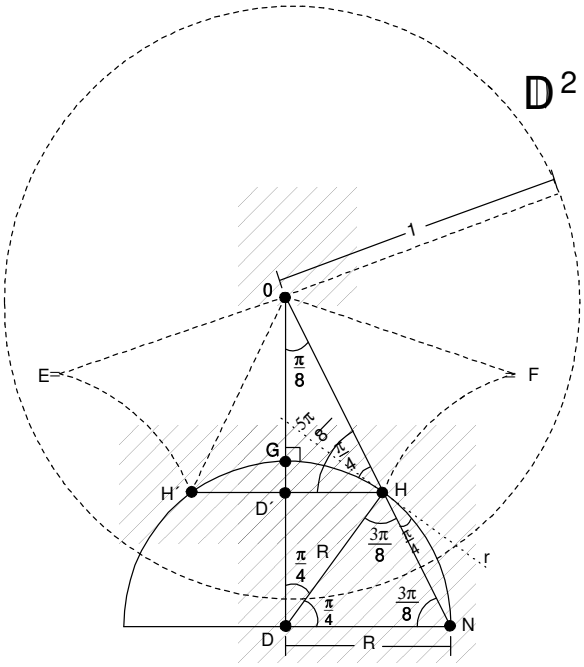

Figura 5.2: Triângulo $\{8, 8\}$

No caso em consideração, a matriz é dada por

$$C = \begin{bmatrix} e^{\frac{i\pi}{8}} & 0 \\ 0 & e^{-\frac{i\pi}{8}} \end{bmatrix}. \tag{5.14}$$

Pelo Teorema 5.2.1, temos que T_1 é definida por

$$A_1 = \begin{bmatrix} a & c \\ \overline{c} & \overline{a} \end{bmatrix}, \tag{5.15}$$

com

$$arg(a) = \hat{e} = \frac{\pi}{8}, \qquad |a| = tan(\hat{\beta}) = tg(\frac{3\pi}{8}) = (1 + \sqrt{2}),$$

$$arg(c) = \frac{-5\pi}{8}, \qquad |c| = \sqrt{2 + 2\sqrt{2}}.$$

Logo, temos que

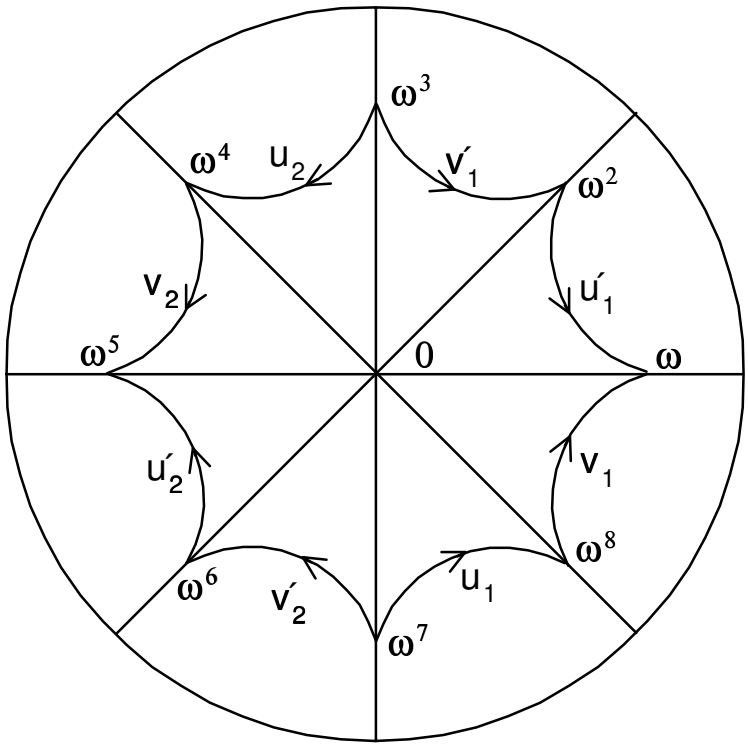

Figura 5.3: Octógono

$$a = |a|e^{iarg(a)} = tan(\frac{3\pi}{8})e^{\frac{i\pi}{8}} = (1+\sqrt{2})\frac{1+i}{2} = \frac{2+\sqrt{2}(1+i)}{2}.$$

e $c = |c|e^{-i\frac{5\pi}{8}} = \sqrt{2+2\sqrt{2}}(-\frac{\sqrt{2-\sqrt{2}}}{2} - i\frac{\sqrt{2+\sqrt{2}}}{2}) = -\frac{\sqrt[4]{2}}{2}(\sqrt{2}+i(2+\sqrt{2}))$.

Logo, a matriz dada por:

$$A_1 = \begin{bmatrix} \frac{2+\sqrt{2}}{2}(1+i) & -\frac{\sqrt[4]{2}}{2}(\sqrt{2}+i(2+\sqrt{2})) \\ -\frac{\sqrt[4]{2}}{2}(\sqrt{2}-i(2+\sqrt{2})) & \frac{2+\sqrt{2}}{2}(1-i) \end{bmatrix}, \tag{5.16}$$

é a matriz associada à transformação $T_1(z) = \frac{az+c}{\bar{c}z+\bar{a}}$ que realiza o emparelhamento da aresta u_1 (com argumento entre $-\frac{\pi}{2}$ e $-\frac{\pi}{4}$) com a aresta $u_1^{'}$ em F_8.

De maneira imediata verifica-se que

$$A_2 = C^4A_1^{-1}C^{-4}, \qquad B_1 = CA_1^{-1}C^{-1}, \qquad B_2 = C^5A_1^{-1}C^{-5}. \tag{5.17}$$

onde A_1, A_2 são as matrizes associadas às transformações T_1 e T_2 e B_1, B_2 são as matrizes associadas às transformações S_1 e S_2, uma vez que as seguintes relações são verificadas,

$$T_{C^{-4}}(u_2) = u_1, \qquad T_{C^{-1}}(v_1) = u_1, \qquad T_{C^{-5}}(v_2) = u_1. \tag{5.18}$$

Como consequência da equação (5.17), temos

$$A_2 = \begin{bmatrix} a & -c \\ -\overline{c} & \overline{a} \end{bmatrix}, \tag{5.19}$$

$$B_1 = \begin{bmatrix} \overline{a} & \overline{c} \\ c & a \end{bmatrix}, \tag{5.20}$$

$$B_2 = \begin{bmatrix} \overline{a} & -\overline{c} \\ -c & a \end{bmatrix}. \tag{5.21}$$

Fazendo as substituições nas equações (5.19), (5.20), (5.21) obtemos

$$A_2 = \begin{bmatrix} \frac{2+\sqrt{2}}{2}(1+i) & \frac{\sqrt[4]{2}}{2}(\sqrt{2}+i(2+\sqrt{2})) \\ \frac{\sqrt[4]{2}}{2}(\sqrt{2}-i(2+\sqrt{2})) & \frac{2+\sqrt{2}}{2}(1-i) \end{bmatrix}, \tag{5.22}$$

$$B_1 = \begin{bmatrix} \frac{2+\sqrt{2}}{2}(1-i) & \frac{\sqrt[4]{2}}{2}(\sqrt{2}-i(2+\sqrt{2})) \\ \frac{\sqrt[4]{2}}{2}(\sqrt{2}+i(2+\sqrt{2})) & \frac{2+\sqrt{2}}{2}(1+i) \end{bmatrix}, \tag{5.23}$$

$$B_2 = \begin{bmatrix} \frac{2+\sqrt{2}}{2}(1-i) & -\frac{\sqrt[4]{2}}{2}(\sqrt{2}-i(2+\sqrt{2})) \\ -\frac{\sqrt[4]{2}}{2}(\sqrt{2}+i(2+\sqrt{2})) & \frac{2+\sqrt{2}}{2}(1+i) \end{bmatrix}. \tag{5.24}$$

Tomando as correspondentes matrizes reais de $PSL(2,\mathbb{R})$ via a isometria $\phi : \mathbb{H}^2 \longrightarrow \mathbb{D}^2$ dada por $\phi(z) = \frac{zi+1}{z+i}$, então, $\Gamma_8 = \phi^{-1}\Gamma_8\phi$ é um subgrupo de $PSL(2,\mathbb{R})$ cujos geradores são dados por

$$G_1 = \begin{bmatrix} \frac{(2+\sqrt{2})+(-2-\sqrt{2})\sqrt[4]{2}}{2} & \frac{(2+\sqrt{2})-(\sqrt{2})(\sqrt[4]{2})}{2} \\ \frac{(-2-\sqrt{2})+(\sqrt{2})(\sqrt[4]{2})}{2} & \frac{(2+\sqrt{2})+(2+\sqrt{2})\sqrt[4]{2}}{2} \end{bmatrix},$$

$$G_2 = \begin{bmatrix} \frac{(2+\sqrt{2})+(2+\sqrt{2})\sqrt[4]{2}}{2} & \frac{(2+\sqrt{2})+(\sqrt{2})(\sqrt[4]{2})}{2} \\ \frac{-(2+\sqrt{2})+(\sqrt{2})(\sqrt[4]{2})}{2} & \frac{(2+\sqrt{2})+(-2-\sqrt{2})\sqrt[4]{2}}{2} \end{bmatrix},$$

$$G_3 = \begin{bmatrix} \frac{(2+\sqrt{2})+(-2-\sqrt{2})\sqrt[4]{2}}{2} & \frac{-(2+\sqrt{2})+\sqrt{2}(\sqrt[4]{2})}{2} \\ \frac{(2+\sqrt{2})+(\sqrt{2})\sqrt[4]{2}}{2} & \frac{(2+\sqrt{2})+(2+\sqrt{2})\sqrt[4]{2}}{2} \end{bmatrix},$$

$$G_4 = \begin{bmatrix} \frac{(2+\sqrt{2})+(2+\sqrt{2})\sqrt[4]{2}}{2} & \frac{-(2+\sqrt{2})-\sqrt{2}\sqrt[4]{2}}{2} \\ \frac{(2+\sqrt{2})+(-\sqrt{2})\sqrt[4]{2}}{2} & \frac{(2+\sqrt{2})+(-2-\sqrt{2})\sqrt[4]{2}}{2} \end{bmatrix}.$$

Calculando os traços dos geradores G_1, G_2, G_3, G_4, constatamos que os mesmos estão em $\mathbb{Z}[\sqrt{2}]$, o anel de inteiros de $\mathbb{Q}(\sqrt{2})$. Por consequência do Teorema 5.4.5, $tr(\Gamma_8)$ também está em $\mathbb{Z}[\sqrt{2}]$, ou seja, a condição i) do Teorema 5.4.3 é satisfeita.

Por outro lado, $A^{\varphi_2} \otimes \mathbb{R} \approx \mathbb{H}$ e como consequência disto e do Exemplo 5.3.1, temos que $\varphi_2(\Gamma_8)$ é limitado em $\mathbb{C}$. Com isso, a condição ii) do Teorema 5.4.3 é verificada. Logo, Γ_8 é um grupo fuchsiano derivado de uma álgebra dos quatérnios sobre $\mathbb{Q}(\sqrt{2})$, uma vez que Γ_8 satisfaz as condições i) e ii) do Teorema 5.4.3.

Caso um grupo fuchsiano apresente como geradores elementos do tipo

$$G_i = \frac{1}{r}\begin{bmatrix} a+b\sqrt{t} & r_1(c+d\sqrt{t}) \\ r_2(c-d\sqrt{t}) & a-b\sqrt{t} \end{bmatrix} \tag{5.25}$$

com as condições de que $r, r_1, r_2 \in \mathbb{R}$ e $r_1 = -r_2$, com $a, b, c, d \in \mathbb{Z}[\theta]$, para $m > 0$, então determinante $det(G_i)$ é igual a norma de $N(G_i)$, isto é,

$$det(G_i) = N(G_i) = \frac{1}{r^2}(a^2 - tb^2 - sc^2 + std^2). \tag{5.26}$$

Para estas condições o Teorema 5.4.4 afirma que podemos associar a este grupo fuchsiano uma ordem dos quatérnios $\mathcal{O} \simeq (t, s)_{\mathbb{Z}[\theta]}$.

Considerando G_1, G_2, G_3 e G_4 os geradores de Γ_8, obtemos pelo Teorema 5.4.4 que a ordem dos quatérnios associada é $\mathcal{O} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, com $r_1 = 1, r_2 = -1, s = -1, r = 2$ e $\sqrt{t} = \sqrt[4]{2}$. Por outro lado, pelo cálculo dos elementos de norma mínima encontramos elementos em $\mathcal{O} \simeq (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$ correspondentes aos geradores do grupo fuchsiano Γ_8.

Considerando $G_i, i = 1, \ldots, 4$ como em (5.25), com valores $r_1 = 1, r_2 = -1, s = -1, r = 2$ e $\sqrt{t} = \sqrt[4]{2}$, então

$$a = 2 + \sqrt{2}, \qquad c = 2 + \sqrt{2},$$

$$b = -(2 + \sqrt{2}), \qquad d = \sqrt{2}.$$

$$Logo, N(G_1) = \frac{1}{4}((2 + \sqrt{2})^2 - \sqrt{2}(2 + \sqrt{2})^2 + (-2 - \sqrt{2})^2 - \sqrt{2}(\sqrt{2})^2)$$

$$= \frac{1}{4}(6 + 4\sqrt{2} - 6\sqrt{2} - 8 + 6 + 4\sqrt{2} - 2\sqrt{2}) = \frac{4}{4} = 1.$$

Considerando G_2 com valores $r_1 = 1, r_2 = -1, s = -1, r = 2$ e $t = \sqrt[4]{2}$, temos

$$a = 2 + \sqrt{2}, \qquad c = 2 + \sqrt{2},$$

$$b = 2 + \sqrt{2}, \qquad d = \sqrt{2}.$$

$$Logo, N(G_2) = \frac{1}{4}((2 + \sqrt{2})^2 - \sqrt{2}(2 + \sqrt{2})^2 + (2 + \sqrt{2})^2 - \sqrt{2}(\sqrt{2})^2)$$

$$= \frac{1}{4}(6 + 4\sqrt{2} - 6\sqrt{2} - 8 + 6 + 4\sqrt{2} - 2\sqrt{2}) = \frac{4}{4} = 1$$

Considerando G_3 com valores $r_1 = 1, r_2 = -1, s = -1, r = 2$ e $t = \sqrt[4]{2}$, então

$$a = 2 + \sqrt{2}, \qquad c = -2 - \sqrt{2},$$

$$b = -(2 + \sqrt{2}), \qquad d = \sqrt{2}.$$

$$Logo, N(G_3) = \frac{1}{4}((2 + \sqrt{2})^2 - \sqrt{2}(2 + \sqrt{2})^2 + (-2 - \sqrt{2})^2 - \sqrt{2}(\sqrt{2})^2)$$

$$= \frac{1}{4}(6 + 4\sqrt{2} - 6\sqrt{2} - 8 + 6 + 4\sqrt{2} - 2\sqrt{2}) = \frac{4}{4} = 1.$$

Considerando G_4 com valores $r_1 = 1, r_2 = -1, s = -1, r = 2$ e $t = \sqrt[4]{2}$, então

$$a = 2 + \sqrt{2}, \qquad c = -2 - \sqrt{2},$$

$$b = 2 + \sqrt{2}, \qquad d = -\sqrt{2}.$$

$$Logo, N(G_4) = \frac{1}{4}((2 + \sqrt{2})^2 - \sqrt{2}(2 + \sqrt{2})^2 + (-2 - \sqrt{2})^2 - \sqrt{2}(\sqrt{2})^2)$$
$$= \frac{1}{4}(6 + 4\sqrt{2} - 6\sqrt{2} - 8 + 6 + 4\sqrt{2} - 2\sqrt{2}) = \frac{4}{4} = 1.$$

Da equação (5.26), a álgebra dos quatérnios é $A \simeq (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$, e $\mathcal{O} \simeq (\sqrt{2}, -1)_{\mathbb{Z}(\sqrt{2})}$ como sendo a ordem de norma mínima associada a Γ_8. A norma de um elemento $g = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{O}$, é dada por $N(g) = \frac{1}{4} f(x_0, x_2, x_3, x_4)$, onde

$$f(x_0, x_1, x_2, x_3) = x_0^2 - \sqrt{2}x_1^2 + x_2^2 + \sqrt{2}x_3^2. \tag{5.27}$$

Logo, os elementos associados aos geradores de Γ_8 em $\mathcal{O} \simeq (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$ são dados por:

$$g_1 = (2 + \sqrt{2}) + (2 + \sqrt{2})i + (2 + \sqrt{2})j + \sqrt{2}ij; \tag{5.28}$$

$$g_2 = (2 + \sqrt{2}) + (-2 - \sqrt{2})i + (2 + \sqrt{2})j + \sqrt{2}ij; \tag{5.29}$$

$$g_3 = (2 + \sqrt{2}) + (-2 - \sqrt{2})i + (-2 - \sqrt{2})j + \sqrt{2}ij; \tag{5.30}$$

$$g_4 = (2 + \sqrt{2}) + (2 + \sqrt{2})i - (2 + \sqrt{2})j - \sqrt{2}ij. \tag{5.31}$$

Os elementos da base de $A_{\mathbb{Q}(\sqrt{2})}$ são dados por $i = \sqrt[4]{2}, j = Im, ij = \sqrt[4]{2}Im$, onde Im é a unidade imaginária.

Do Exemplo 5.3.2 temos que $d(\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}) = -4\sqrt{2}$, logo $[\mathcal{O} : A] = 4$, uma vez que $d(A) = \sqrt{2}$, ou seja, $\mathcal{O}$ não é uma ordem maximal em A. Como o objetivo da proposta é a realização de um rotulamento algébrico completo, temos que procurar uma ordem que contenha a ordem $\mathcal{O}$ em A e que seja maximal.

Considere uma base do tipo

$$\left\{1, i', j', i'j'\right\} = \left\{1, \frac{1}{2}\sqrt{2}\sqrt[4]{2}, \frac{1}{2}\sqrt{2}Im, \frac{1}{2}\sqrt[4]{2}Im\right\} \tag{5.32}$$

para uma ordem $\mathcal{O}'$ de $A_{\mathbb{Q}(\sqrt{2})}(\sqrt{2}, -1)$. Do Exemplo 5.3.2 temos que $d(\mathcal{O}') = \sqrt{2}$. Portanto, $\mathcal{O}'$ é uma ordem maximal em A, uma vez que $d(\mathcal{O}') = d(A)$. Logo, os elementos indentificados pelos geradores de Γ_8 na base de $\mathcal{O}'$, os quais são expressos por $\{g_1, g_2, g_3, g_4\}$ são dados por

$$g_1 = (2 + \sqrt{2}) + (2 + 2\sqrt{2})i' + (2 + 2\sqrt{2})j' + 2\sqrt{2}i'j'; \tag{5.33}$$

$$g_2 = (2 + \sqrt{2}) + (-2 - 2\sqrt{2})i' + (2 + 2\sqrt{2})j' + 2\sqrt{2}i'j'; \tag{5.34}$$

$$g_3 = (2 + \sqrt{2}) + (-2 - 2\sqrt{2})i' + (-2 - 2\sqrt{2})j' + 2\sqrt{2}i'j'; \tag{5.35}$$

$$g_4 = (2 + \sqrt{2}) + (2 + 2\sqrt{2})i' - (2 + 2\sqrt{2})j' - 2\sqrt{2}i'j'. \tag{5.36}$$

A norma associada à ordem $\mathcal{O}'_{\mathbb{Z}[\sqrt{2}]}(\sqrt{2}, -1)$, é dada por $N(g) = \frac{1}{4}f(x_0, x_1, x_2, x_3)$ com

$$f(x_0, x_1, x_2, x_3) = x_0^2 - \frac{1}{2}\sqrt{2}x_1^2 + \frac{1}{2}x_2^2 + \frac{1}{4}\sqrt{2}x_3^2. \tag{5.37}$$

Como consequência, $[\mathcal{O}^1; \mathcal{O}] = 4$.

5.6 Tesseleção $\{12, 12\}$ no Plano Hiperbólico

Análoga ao caso $\{8, 8\}$, apresentaremos nesta seção os aspectos aritméticos relacionados a uma tesselação $\{12, 12\}$. Explicitaremos os geradores de um grupo fuchsiano Γ_{12} associado ao domínio fundamental F_{12} e mostraremos que o grupo fuchsiano Γ_{12} é aritmético e derivado de uma álgebra dos quatérnios sobre $\mathbb{Q}(\sqrt{3})$.

Exibiremos a identificação dos geradores de Γ_{12} pelos geradores da ordem $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$ em uma álgebra dos quatérnios A sobre $\mathbb{Q}(\sqrt{3})$.

Verificaremos que a ordem $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$ não é maximal na álgebra dos quatérnios A, através dos resultados do Exemplo 5.3.2.

Da análise da Figura 5.4, temos como ângulos trigonométricos para o triângulo $\{12, 12\}$, são os seguintes valores

$$\hat{o} = \frac{\pi}{12}, \hat{e} = \frac{\pi}{3}, \hat{\gamma} = \frac{7\pi}{12}, \hat{\beta} = \frac{5\pi}{12}.$$

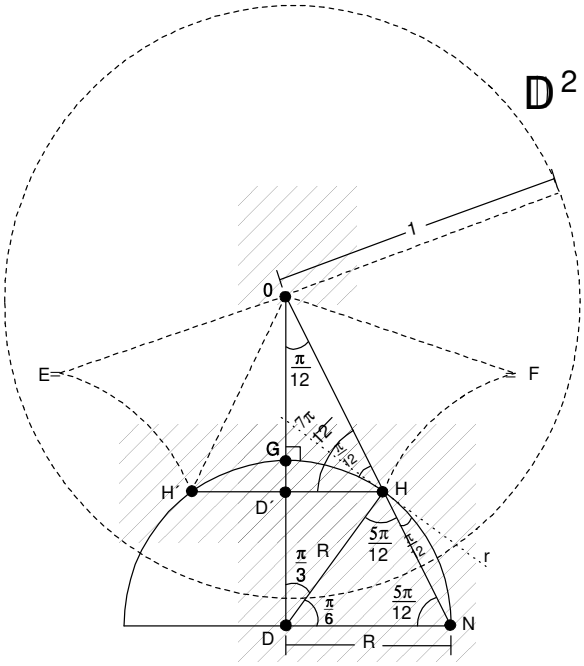

Figura 5.4: Triângulo $\{12, 12\}$

Logo, os 12 triângulos hiperbólicos obtidos a partir de F_{12} possuem área $\frac{4\pi}{3}$ e com ângulo $\frac{\pi}{6}$ na origem do domínio fundamental F_{12}, e os demais vértices destes triângulos possuem ângulos $\frac{\pi}{12}$.

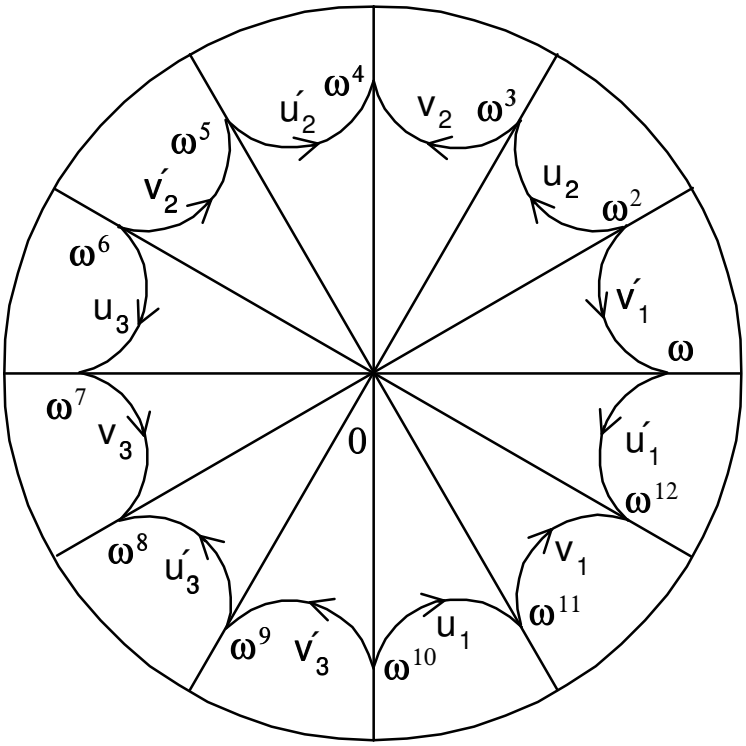

Figura 5.5: Dodecágono

Para o caso da tesselação $\{12, 12\}$ temos que os emparelhamentos de arestas em F_{12} são realizados por transformações hiperbólicas T_i, S_i, para $i = 1, 2, 3$, da seguinte maneira:

$$T_i(u_i) = u_i^{'}, \qquad S_i(v_i) = v_i^{'}, i = 1, 2, 3$$

como mostrado na Figura 5.5.

A matriz

$$C = \begin{bmatrix} e^{\frac{i\pi}{12}} & 0 \\ 0 & e^{-\frac{i\pi}{12}} \end{bmatrix}, \tag{5.38}$$

leva uma aresta a outra aresta adjacente no sentido anti-horário em F_{12}.

Pelo Teorema 5.2.1, a transformação T_1 que emparelha u_1 e u_1' é dada por

$$A_1 = \begin{bmatrix} a & c \\ \overline{c} & \overline{a} \end{bmatrix}, \tag{5.39}$$

onde a e c são definidos por

$$arg(a) = e = \frac{\pi}{3}, \qquad |a| = tg(\beta) = tg(\frac{5\pi}{12}) = (2+\sqrt{3});$$
$$arg(c) = \frac{-7\pi}{12}, \qquad |c| = \sqrt{6+4\sqrt{3}},$$

ou seja, $a = |a|e^{iarg(a)} = (2+\sqrt{3}).(\frac{1+i\sqrt{3}}{2})$,

e $c = |c|e^{i\frac{-7\pi}{12}} = \sqrt{6+4\sqrt{3}}(cos(\frac{7\pi}{12}) + isen(\frac{7\pi}{12})) = \frac{\sqrt{3+2\sqrt{3}}}{2}((-1+\sqrt{3}) + i(1+\sqrt{3}))$.

Desta maneira encontramos a matriz

$$A_1 = \begin{bmatrix} a & c \\ \overline{c} & \overline{a} \end{bmatrix} = \begin{bmatrix} \frac{(2+\sqrt{3})+i(3+2\sqrt{3})}{2} & \frac{(\sqrt{3+2\sqrt{3}})[(-1+\sqrt{3})+i(1+\sqrt{3})}{2} \\ \frac{(\sqrt{3+2\sqrt{3}})[(-1+\sqrt{3})-i(1+\sqrt{3})}{2} & \frac{(2+\sqrt{3})-i(3+2\sqrt{3})}{2} \end{bmatrix}$$

associada à transformação T_1.

De maneira imediata verifica-se que

$$A_2 = C^4 A_1^{-1} C^{-4} \qquad A_3 = C^8 A_1^{-1} C^{-8}$$
$$B_1 = C A_1^{-1} C^{-1}, \qquad B_2 = C^5 A_1 C^{-5}, \qquad B_3 = C^{10} A_1 C^{-10}.$$

onde A_1, A_2, A_3 são as matrizes associadas às transformações T_1, T_2, T_3 e B_1, B_2, B_3 são as matrizes associadas às transformações S_1, S_2 e S_3.

Explicitando as matrizes, obtemos

$$A_2 = \begin{bmatrix} \frac{-(2+\sqrt{3})+i(3+2\sqrt{3})}{2} & \frac{(\sqrt{3+2\sqrt{3}})[(-1-\sqrt{3})+i(1-\sqrt{3})}{2} \\ \frac{(\sqrt{3+2\sqrt{3}})[(-1-\sqrt{3})-i(1-\sqrt{3})]}{2} & \frac{(2+\sqrt{3})+i(3+2\sqrt{3})}{2} \end{bmatrix}$$

$$A_3 = \begin{bmatrix} \frac{-(2+\sqrt{3})+i(3+2\sqrt{3})}{2} & \frac{(\sqrt{3+2\sqrt{3}})[(-1-\sqrt{3})-i(1-\sqrt{3})}{2} \\ \frac{(\sqrt{3+2\sqrt{3}})[(-1-\sqrt{3})+i(1+\sqrt{3})}{2} & \frac{(2+\sqrt{3})+i(3+2\sqrt{3})}{2} \end{bmatrix}$$

$$B_1 = \begin{bmatrix} \frac{-(2+\sqrt{3})+i(3+2\sqrt{3})}{2} & \frac{(\sqrt{3+2\sqrt{3}})[(1-\sqrt{3})+i(1+\sqrt{3})}{2} \\ \frac{(\sqrt{3+2\sqrt{3}})[(1-\sqrt{3})-i(1+\sqrt{3})}{2} & \frac{(2+\sqrt{3})+i(3+2\sqrt{3})}{2} \end{bmatrix}$$

$$B_2 = \begin{bmatrix} \frac{-(2+\sqrt{3})+i(3+2\sqrt{3})}{2} & \frac{(\sqrt{3+2\sqrt{3}})[(-1+\sqrt{3})+i(1+\sqrt{3})}{2} \\ \frac{(\sqrt{3+2\sqrt{3}})[(-1+\sqrt{3})-i(1+\sqrt{3})}{2} & \frac{(2+\sqrt{3})+i(3+2\sqrt{3})}{2} \end{bmatrix}$$

$$B_3 = \begin{bmatrix} \frac{-(2+\sqrt{3})+i(3+2\sqrt{3})}{2} & \frac{(\sqrt{3+2\sqrt{3}})[(-1+\sqrt{3})-i(1+\sqrt{3})}{2} \\ -\frac{(\sqrt{3+2\sqrt{3}})[(1-\sqrt{3})+i(1+\sqrt{3})}{2} & \frac{(2+\sqrt{3})+i(3+2\sqrt{3})}{2} \end{bmatrix}$$

Tomando as correspondentes matrizes reais de $PSL(2,\mathbb{R})$ via isometrias $\phi : \mathbb{H}^2 \longrightarrow \mathbb{D}^2$ dada por $\phi(z) = \frac{zi+1}{z+i}$, então, $\Gamma = \phi^{-1}\Gamma_{12}\phi$ é um subgrupo de $PSL(2,\mathbb{R})$, cujos geradores são dados por

$$G_1 = \frac{1}{2}\begin{bmatrix} (2+\sqrt{3})+\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & (3+2\sqrt{3})+\sqrt{3+2\sqrt{3}}(-1+\sqrt{3}) \\ -(3+2\sqrt{3})+\sqrt{3+2\sqrt{3}}(-1+\sqrt{3}) & (2+\sqrt{3})-(\sqrt{3+2\sqrt{3}})(1+\sqrt{3}) \end{bmatrix}$$

$$G_2 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3})+\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & (3+2\sqrt{3})-\sqrt{3+2\sqrt{3}}(-1-\sqrt{3}) \\ -(3+2\sqrt{3})+\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & -(2+\sqrt{3})-(\sqrt{3+2\sqrt{3}})(1-\sqrt{3}) \end{bmatrix}$$

$$G_3 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3})-\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & (3+2\sqrt{3})+\sqrt{3+2\sqrt{3}}(-1-\sqrt{3}) \\ -(3+2\sqrt{3})+\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & -(2+\sqrt{3})+(\sqrt{3+2\sqrt{3}})(1-\sqrt{3}) \end{bmatrix}$$

$$G_4 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3})+\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & (3+2\sqrt{3})-\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) \\ -(3+2\sqrt{3})-\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & -(2+\sqrt{3})-(\sqrt{3+2\sqrt{3}})(1+\sqrt{3}) \end{bmatrix}$$

$$G_5 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3}) + \sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & (3+2\sqrt{3}) + \sqrt{3+2\sqrt{3}}(1+\sqrt{3}) \\ -(3+2\sqrt{3}) - \sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & -(2+\sqrt{3}) - (\sqrt{3+2\sqrt{3}})(1+\sqrt{3}) \end{bmatrix}$$

$$G_6 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3}) - \sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & (3+2\sqrt{3}) - \sqrt{3+2\sqrt{3}}(1+\sqrt{3}) \\ -(3+2\sqrt{3}) - \sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & -(2+\sqrt{3}) + (\sqrt{3+2\sqrt{3}})(1+\sqrt{3}) \end{bmatrix}$$

Calculando os traços dos geradores $G_1, G_2, G_3, G_4, G_5, G_6$, temos que estes estão em $\mathbb{Z}[\sqrt{3}]$ o anel de inteiros de $\mathbb{Q}(\sqrt{3})$. Do Teorema 5.4.5, o $tr(\Gamma_{12})$ também está em $\mathbb{Z}[\sqrt{3}]$, uma vez que são satisfeito para os geradores de Γ_{12}, ou seja a condição (i) do Teorema 5.4.3 é satisfeita.

Por outro lado, se tomarmos $\varphi : \mathbb{Q}(\sqrt{3}) \longrightarrow \mathbb{R}$ um dos homomorfismos do grupo de Galois $G(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$ que não é a identidade, temos que este é dado por $\varphi_1(3+2\sqrt{3}) = -(3+2\sqrt{3})$, e se estendermos φ_2 a isomorfismo $\Psi_2 : \mathbb{K} \longrightarrow \mathbb{C}$ tal que $\Psi(\sqrt{-(3+2\sqrt{3})} = i\sqrt{3+2\sqrt{3}}$, onde $\mathbb{Q}(\sqrt{3})(\sqrt{3+2\sqrt{3}})$.

Por este mergulho os geradores são mapeados nas seguintes matrizes em $M(2,\mathbb{C})$:

$$G_1 = \frac{1}{2}\begin{bmatrix} (2+\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & (3+2\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(-1+\sqrt{3}) \\ -(3+2\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(-1+\sqrt{3}) & (2+\sqrt{3}) - i(\sqrt{3+2\sqrt{3}})(1+\sqrt{3}) \end{bmatrix}$$

$$G_2 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & (3+2\sqrt{3}) - i\sqrt{3+2\sqrt{3}}(-1-\sqrt{3}) \\ -(3+2\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & -(2+\sqrt{3}) - i(\sqrt{3+2\sqrt{3}})(1-\sqrt{3}) \end{bmatrix}$$

$$G_3 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3}) - i\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & (3+2\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(-1-\sqrt{3}) \\ -(3+2\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & -(2+\sqrt{3}) + i(\sqrt{3+2\sqrt{3}})(1-\sqrt{3}) \end{bmatrix}$$

$$G_4 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & (3+2\sqrt{3}) - i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) \\ -(3+2\sqrt{3}) - i\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & -(2+\sqrt{3}) - i(\sqrt{3+2\sqrt{3}})(1+\sqrt{3}) \end{bmatrix}$$

$$G_5 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & (3+2\sqrt{3}) + i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) \\ -(3+2\sqrt{3}) - i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & -(2+\sqrt{3}) - i(\sqrt{3+2\sqrt{3}})(1+\sqrt{3}) \end{bmatrix}$$

$$G_6 = \frac{1}{2}\begin{bmatrix} -(2+\sqrt{3}) - i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) & (3+2\sqrt{3}) - i\sqrt{3+2\sqrt{3}}(1+\sqrt{3}) \\ -(3+2\sqrt{3}) - i\sqrt{3+2\sqrt{3}}(1-\sqrt{3}) & -(2+\sqrt{3}) + i(\sqrt{3+2\sqrt{3}})(1+\sqrt{3}) \end{bmatrix}$$

É fácil verificar que $A^{\varphi_2} \otimes \mathbb{R} \approx \mathbb{H}$. Disto e do Exemplo 5.3.1 , temos que $\varphi_2(\Gamma)$ é limitado em $\mathbb{C}$. Com isso, a condição (ii) do Teorema 5.4.3 é verificada. Logo, Γ_{12} é um grupo fuchsiano derivado de uma álgebra dos quatérnios sobre $\mathbb{Q}(\sqrt{3})$, uma vez que Γ_{12} satisfaz as condições (i) e (ii) do Teorema 5.4.3.

Dos geradores $G_i, i = 1, \ldots, 6$, do grupo fuchsiano Γ_{12}, podemos verificar que os mesmos podem se vistos como matrizes da forma

$$G_i = \frac{1}{r}\begin{bmatrix} a + b\sqrt{t} & r_1(c + d\sqrt{t}) \\ r_2(c - d\sqrt{t}) & a - b\sqrt{t} \end{bmatrix}, \tag{5.40}$$

onde $r = 2, \sqrt{t} = \sqrt{3+2\sqrt{3}}, r_1 = 1, r_2 = -1$ e $s = -1$.

Outro fato a ser observado é que

$$det(G_i) = N(G_i) = \frac{1}{r^2}(a^2 - tb^2 - sc^2 + std^2). \tag{5.41}$$

Logo, pelo Teorema 5.4.4, temos que o grupo fuchsiano Γ_{12} é identificado pela ordem $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]} \simeq (3+2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$ em uma álgebra dos quatérnios A sobre $\mathbb{Q}(\sqrt{3})$. Assim, $A = (3+2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$ é uma álgebra dos quatérnios associada a Γ_{12}, cuja norma de um elemento $g = x_0 + x_1 i + x_2 j + x_3 ij \in A$, é dada por $N(g) = \frac{1}{4} f(x_0, x_1, x_2, x_3)$, onde

$$f(x_0, x_1, x_2, x_3) = x_0^2 - (3+2\sqrt{3})x_1^2 + x_2^2 - (3+2\sqrt{3})x_3^2. \tag{5.42}$$

Vimos que os geradores do grupo fuchsiano Γ_{12} apresentam como matrizes 5.40. Caso tomemos os elementos $(x_0, x_1, x_2, x_3) = (a, b, c, d)$, temos que para estes valores $N(g) = 1$.

E mais os elementos de $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$ identificados pelos elementos do grupo fuchsiano Γ_{12} serão dados por $g_i = a + bi + cj + dij \in \mathcal{O} \simeq (3 + 2\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$.

Por esta identificação teremos que

$$g_1 = (2 + \sqrt{3}) + (1 + \sqrt{3})i + (3 + 2\sqrt{3})j + (-1 + \sqrt{3})ij; \tag{5.43}$$

$$g_2 = -(2 + \sqrt{3}) + (1 - \sqrt{3})i + (3 + 2\sqrt{3})j + (-1 + \sqrt{3})ij; \tag{5.44}$$

$$g_3 = -(2 + \sqrt{3}) + (1 + \sqrt{3})i + (3 + 2\sqrt{3})j - (-1 + \sqrt{3})ij; \tag{5.45}$$

$$g_4 = -(2 + \sqrt{3}) + (1 + \sqrt{3})i + (3 + 2\sqrt{3})j - (-1 + \sqrt{3})ij; \tag{5.46}$$

$$g_5 = (2 + \sqrt{3}) - (1 + \sqrt{3})i + (3 + 2\sqrt{3})j - (-1 + \sqrt{3})ij; \tag{5.47}$$

$$g_6 = (2 + \sqrt{3}) - (1 + \sqrt{3})i + (3 + 2\sqrt{3})j - (-1 + \sqrt{3})ij. \tag{5.48}$$

Os elementos da base de $A_{\mathbb{Q}(\sqrt{3})}(3+2\sqrt{3}, -1)$ são dados por $i = \sqrt[4]{3 + 2\sqrt{3}}, j = Im, ij = \sqrt[4]{3 + 2\sqrt{3}}Im$.

Do Exemplo 5.3.2, vemos que $d(\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}) = -4\sqrt{3}$, logo $[\mathcal{O} : A] = 4$, ou seja, $\mathcal{O}$ não é uma ordem maximal em A. Através de um procedimento semelhante ao caso da tesselação $\{8, 8\}$ encontramos uma ordem maximal $\mathcal{O}'$ contendo $\mathcal{O}$ em A.

5.7 Rotulamento de Constelações de Sinais no Plano Hiperbólico

Iremos propor nesta seção uma forma de rotular os sinais de uma constelação de sinais geometricamente uniforme no plano hiperbólico por elementos de uma estrutura algébrica provenientes dos baricentros dos polígonos de uma tesselação $\{4g, 4g\}$, e tenham como identificação elementos de uma ordem dos quatérnios $\mathcal{O}_{\mathbb{Z}[\theta]}$.

Em particular, tal proposta será aplicável às constelações de sinais geometricamente uniformes provenientes das tesselações $\{8, 8\}$ e $\{12, 12\}$, conforme vimos nas Seções 5.5 e 5.6. Os baricentros dos polígonos destas tesselações são identificados por elementos das ordens dos quatérnios $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ e $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$, respectivamente.

Para tal, mostraremos a existência de ideais $\mathcal{O}^1_{\mathbb{Z}[I]}$ em $\mathcal{O}^1_{\mathbb{Z}[\theta]}$ que correspondem a subgrupos normais Γ_I no grupo fuchsiano Γ_{4g}.

Consideremos inicialmente uma álgebra dos quatérnios $A \simeq (a, b)_{\mathbb{F}}$, e uma ordem $\mathcal{O}^1$ em A de norma unitária, isto é,

$$\mathcal{O}^1 = \{x = x_0 + x_1 i + x_2 j + x_3 ij : x_0, x_1, x_2, x_3 \in R\},$$

onde R é um anel no corpo $\mathbb{F}$.

Do conjunto $\mathcal{O}^1$, consideremos os subconjuntos do tipo

$$\mathcal{O}^1_{\mathbb{Z}[I]} = \{z = z_0 + z_1 i + z_2 j + z_3 ij : z_0, z_1, z_2, z_3 \in I\},$$

onde I é um ideal de R.

Proposição 5.7.1 *Um subconjunto $\mathcal{O}^1_{\mathbb{Z}[I]}$ tem uma estrutura de ideal na subordem $\mathcal{O}^1$.*

Demonstração: Sejam $x = x_0 + x_1 i + x_2 j + x_3 ij$ tais que $x_0, x_1, x_2, x_3 \in R$ e $y = y_0 + y_1 i + y_2 j + y_3 ij$ com $y_i \in I$, onde I é um ideal de R. Então, $x.y = (x_0 + x_1 i + x_2 j + x_3 ij)(y_0 + y_1 i + y_2 j + y_3 ij) = (x_0 y_0 + (ab)^2 x_3 y_3 + x_1 y_1 a + x_2 y_2 b) + (x_0 y_1 + x_1 y_0 + x_2 y_3 b + x_3 y_2 b)i + (x_0 y_2 + x_2 y_0 + x_1 y_3 a - x_3 y_1 a)j + (x_0 y_3 + x_3 y_0 + x_1 y_1 - x_2 y_1)ij$.

O fechamento da multiplicação em $\mathcal{O}^1_{\mathbb{Z}[I]}$ é garantido do fato de que os coeficientes são soma de produtos dos elementos de um ideal I pelo elementos do anel R.

■

Proposição 5.7.2 *Os ideais $\mathcal{O}^1_{\mathbb{Z}[I]}$ de $\mathcal{O}^1$ correspondem a subgrupos normais Γ_I no grupo fuchsiano $\Gamma(A,\mathcal{O})$.*

Demonstração: Já vimos que a aplicação φ é um homomorfismo multiplicativo entre uma álgebra dos quatérnios A e um subgrupo multiplicativo $\Gamma \subset PSL(2,\mathbb{R})$, isto é, $\varphi : A \to \Gamma$.

Seja $\Gamma = \Gamma(A,\mathcal{O})$ um subgrupo fuchsiano aritmético de $PSL(2,\mathbb{R})$ obtido pela imagem da restrição de φ em $\mathcal{O}^1$. Considere a restrição de φ em $\mathcal{O}^1_{\mathbb{Z}[I]}$. Da propriedade de homomorfismo, $\varphi(\mathcal{O}^1_{\mathbb{Z}[I]})$ corresponde a um subgrupo de $\Gamma(A,\mathcal{O})$, que denotaremos por Γ_I.

Sejam $x \in \mathcal{O}^1$ e $y \in \mathcal{O}^1_{\mathbb{Z}[I]}$ tais que $\varphi(x) = g$ e $\varphi(y) = h$ temos então que $\varphi(xyx^{-1}) = \varphi(x)\varphi(y)\varphi(x^{-1}) = ghg^{-1}$. Como $\mathcal{O}^1_{\mathbb{Z}[I]}$ é um ideal, $xyx^{-1} \in \mathcal{O}^1_I$ e $ghg^{-1} \in \varphi(\mathcal{O}^1_{\mathbb{Z}[I]})$.

Por outro lado, $\varphi(\varphi^{-1}(ghg^{-1})) = \varphi(xyx^{-1}) = \varphi(x)\varphi(y)\varphi(x^{-1}) = ghg^{-1} \in \Gamma_I$.

A Figura 5.6, mostra que se trabalharmos em Γ_{4g} ou em sua ordem associada é equivalente.

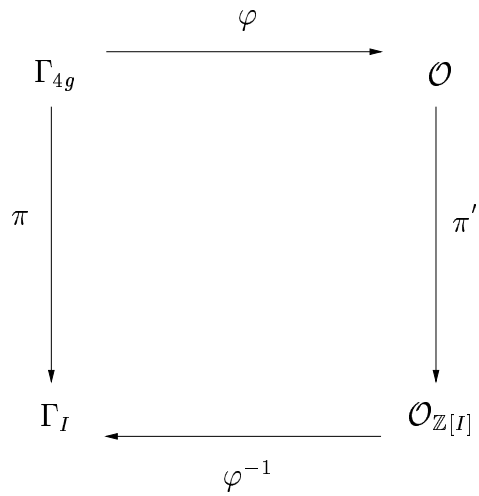

Figura 5.6: Diagrama de equivalência

■

A existência de subgrupos normais Γ_I em Γ, implica que Γ pode ser decomposto em

classes laterais $g_i\Gamma_I$, ou equivalentemente,

$$\Gamma = g_1\Gamma_I \cup g_2\Gamma_I \cup ... \cup g_n\Gamma_I, \qquad g_i \in \Gamma/\Gamma_I = \Gamma - \Gamma_I.$$

Disto decorre que a região fundamental associada a Γ_I é dada por

$$F_I = g_1F_{4g} \cup g_2F_{4g} \cup ... \cup g_nF_{4g}.$$

Seja 0 o baricentro de F_{4g}. Então a ação de $G_I \simeq \Gamma/\Gamma_I$ em 0 resulta em $G_I(0) = \{g_i(0) : g_i \in G_I\}$, ou seja, a G_I-órbita de 0 é uma constelação de sinais finita no espaço quociente $\mathbb{D}^2/G_I$.

Portanto, o grupo quociente Γ/Γ_I consiste dos representantes das classes laterais com a operação herdada de Γ. Para realizarmos o rotulamento dos sinais desta constelação utilizaremos o ideal $\mathcal{O}_{\mathbb{Z}[I]}$ em $\mathcal{O}_{\mathbb{Z}[\theta]}$ correspondente do subgrupo normal Γ_I em Γ, através dos elementos do anel quociente de $\mathcal{O}_{\mathbb{Z}[\theta]}/\mathcal{O}_{\mathbb{Z}[I]}$, estaremos rotulando estes sinais. Note que as operações a serem realizadas com os elementos do anel quociente são aquelas herdadas de $\mathcal{O}^1_{\mathbb{Z}[\theta]}$.

Como a operação definida em $\mathcal{O}^1_{\mathbb{Z}[\theta]}$ é a multiplicativa, então a operação a ser utilizada com os elementos de $\mathcal{O}^1_{\mathbb{Z}[\theta]}/\mathcal{O}^1_{\mathbb{Z}[I]}$ também será multiplicativa. Lembramos que o objetivo é rotular os sinais de uma constelação de sinais. Para isso, como efetuado no Capítulo 4, iremos considerar como constelações de sinais o arranjo de elementos provenientes do quociente de $\mathcal{O}^1_{\mathbb{Z}[\theta]}/\mathcal{O}^1_{\mathbb{Z}[I]}$ tal que a energia média seja mínima.

Vimos anteriormente uma maneira de obter os ideais $\mathcal{O}^1_{\mathbb{Z}[I]}$. Agora proporemos um algoritmo que realizará de maneira efetiva o rotulamento de uma ordem $\mathcal{O}^1_{\mathbb{Z}[\theta]}$ por um p-grupo G_{p^m} (grupo com p^m elementos).

Algoritmo de Rotulamento Algébrico de Constelações de Sinais em Tesselações $\{4g, 4g\}$ no Plano Hiperbólico

Passo 1) Determine a presentação do grupo fuchsiano Γ_{4g} associado ao domínio fundamental F_{4g} da tesselação $\{4g, 4g\}$.

Passo 2) Verifique se Γ_{4g} é um grupo fuchsiano aritmético derivado de uma álgebra dos quatérnios sobre um corpo $\mathbb{Q}(\sqrt{m})$, onde m é um inteiro livre de quadrados. Caso verdadeiro vá para o Passo 3, caso contrário retorne ao Passo 1.

Passo 3) Determine a ordem de norma reduzida $\mathcal{O}^1$ associada ao grupo fuchsiano Γ_{4g}.

Passo 4) Calcule o discriminante de $\mathcal{O}^1 \simeq (a,b)_{\mathbb{Z}[\theta]}$ de A, a álgebra dos quatérnios que contém $\mathcal{O}^1$, onde $a = a_1 + a_2\theta, b = b_1 + b_2\theta \in \mathbb{Z}[\theta]$. Se $d(A) = d(\mathcal{O}^1)$, então $\mathcal{O}^1$ é uma ordem maximal em A. Se $d(A) \neq d(\mathcal{O}^1)$, então $\mathcal{O}^1$ não é uma ordem maximal. Neste caso faça uma mudança de base de modo que a nova ordem tenha discriminante igual ao discriminante de A.

Passo 5) Determine o polinômio minimal $p(x)$ de ij sobre $\mathbb{Q}$.

Passo 6) Fixe p um número primo, e considere $\overline{p(x)} = p(x) mod p$.

Passo 7) Caso o polinômio $\overline{p(x)}$ do Passo 6 tenha solução em $\mathbb{Z}_p$, considere os ideais $\mathcal{O}^1_{\mathbb{Z}[I]}$ em $\mathcal{O}^1$ (para os ideais I em $\mathbb{Z}[\theta]$) que sejam gerados pelos elementos $\langle a + b\theta \rangle$ e que tenham como norma algébrica potências de p.

Passo 8) Caso o polinômio $\overline{p(x)}$ satisfaça o Passo 7, considere a raiz s de $p(x)$ como rótulo do elemento ij.

Passo 9) Se s não for primo, determine a fatoração de s como sendo dois números inteiros módulo p. Sejam u e v tais inteiros. Então u será o rótulo do elemento i e v será o rótulo do elemento j, ou vice-versa, caso contrário retorne ao Passo 1.

Passo 10) Caso o Passo 9 seja satisfeito, determine as soluções das equações diofantinas $a_1 + a_2 r_1 = u^2 (mod p)$ e $b_1 + b_2 r_2 = v^2 (mod p)$, onde $a_1, a_2, b_1,$
$b_2 \in \mathbb{Z}$ provenientes de $a = a_1 + a_2\theta, b = b_1 + b_2\theta$. Atribuiremos como sendo r o rótulo do elemento θ, onde r é dado por $r = r_1$ ou $r = r_2$, mas desde que $r_1, \neq s, u$ e $r_2 \neq s, v$.

Passo 11) Caso os Passos de 1 a 10 sejam satisfeitos o rótulo de um elemento $x = (x_0 + x_0'\theta) + (x_1 + x_1'\theta)i + (x_2 + x_2'\theta)j + (x_0 + x_0'\theta)ij \in \mathcal{O}^1 \simeq (a,b)_{\mathbb{Z}[\theta]}$, é dado pela função de rotulamento multiplicativo $l' : \mathcal{O}^1 \longrightarrow G_p$, onde $l'((x_0 + x_0'\theta) + (x_1 + x_1'\theta)i + (x_2 + x_2'\theta)j + (x_0 + x_0'\theta)ij) = (x_0 + x_0' r) + (x_1 + x_1' r)u + (x_2 + x_2' r)v + (x_3 + x_3' r)s (mod p)$.

Note que o Passo 11 é na verdade uma consequência indireta da Definição 4.4.1 e da Proposição 4.4.1 proposta por Interlando em [37]. A diferença é que nesse contexto não exigimos

que o elemento algébrico ij da extensão quadrática $\mathbb{Q}(ij)$, reproduza uma base integral para este corpo através das combinações das potências deste elemento, uma vez que a nossa itenção é apenas propor um procedimento que atribua rótulos aos elementos da base $\{1, i, j, ij\}$ e do elemento θ em uma ordem dos quatérnios $\mathcal{O}_{\mathbb{Z}[\theta]}$.

Todavia em [37] havia tal necessidade garantir que o um anel resultante fosse um anel maximal (anel de inteiros) no corpo de números em questão. Com isso, o rotulamento seria completo.

5.8 Partições Geometricamente Uniformes no Plano Hiperbólico

Lazari [22] mostrou que dado o grupo completo de simetrias $[4g, 4g]$ da tesselação auto-dual $\{4g, 4g\}$ é sempre possível determinar uma cadeia de decomposição de subgrupos normais através do algoritmo de Reidemeister-Schreier das presentações destes grupos. Isto possibilitou a introdução do conceito de partição geometricamente uniforme no plano hiperbólico. Além disso, mostrou que conjuntos de sinais casados a grupos podem ser decompostos em partições geometricamente uniformes.

As constelações de sinais no plano hiperbólico propostas neste capítulo provenientes dos baricentros dos polígonos $\{4g, 4g\}$ são justamente aquelas em que os pontos de sinais são identificados por elementos de uma ordem dos quatérnios $\mathcal{O}_{\mathbb{Z}[\theta]}$. Por outro lado, vimos pela Proposição 5.7.1 que existem ideais $\mathcal{O}_{\mathbb{Z}[I]}$ em $\mathcal{O}_{\mathbb{Z}[\theta]}$. Mais do que isto; a partir destes ideais propusemos um procedimento de rotulamento dos sinais das constelações através dos elementos resultantes do anel quociente $\mathcal{O}^1_{\mathbb{Z}[\theta]}/\mathcal{O}^1_{\mathbb{Z}[I]}$, ou seja, mostramos que estas constelações de sinais estão casadas a estruturas de grupo.

Como veremos a seguir os conceitos propostos por Lazari [22], se aplicam também neste trabalho.

Com o objetivo de complementação dos conceitos e clareza do paralelismo utilizado até agora, se faz necessário apresentar os resultados estabelecidos por Lazari [22].

Definição 5.8.1 *Chamamos de* ***partição geometricamente uniforme*** *de um conjunto de sinais S geometricamente uniforme com grupo gerador $U(S)$ a qualquer partição S/S^1 induzida por um subgrupo normal U^1 de $U(S)$.*

Os conjuntos de sinais S considerados neste contexto são os conjuntos formados pelos baricentros das tesselações $\{4g, 4g\}$ que possuem grupos fuchsianos aritméticos Γ_{4g} identificados nas ordens dos quatérnios $\mathcal{O}_{\mathbb{Z}[\theta]}$.

Logo, pela Definição 5.8.1, $U(S)$ é uma ordem dos quatérnios $\mathcal{O}_{\mathbb{Z}[\theta]}$, e $U^1(S)$ é um ideal $\mathcal{O}_{\mathbb{Z}[I]}$ em $\mathcal{O}_{\mathbb{Z}[\theta]}$.

Teorema 5.8.1 *[1] Se S/S^1 é uma partição geometricamente uniforme, então os elementos de S/S^1 são geometricamente uniformes, mutuamente congruentes e tem U^1 como grupo gerador comum.*

A importância do Teorema 5.8.1 é que através dele, podemos generalizar de modo natural o conceito de particionamento de conjuntos proposto por Ungerboeck, ou seja, a aplicação repetida em sequência

$$...U(S^2) \triangleleft U(S^1) \triangleleft U(S).$$

o que conduz a uma sequência de partições geometricamente uniformes

$$S/S^1/S^2...$$

e para cada nível os conjuntos das partições são congruentes com um grupo gerador comum.

Definição 5.8.2 *[22] Seja S/S^1 uma partição geometricamente uniforme. Dizemos que $\mathcal{A}$ é um* ***grupo de rótulos*** *para S/S^1, se existe um isomorfismo $m : \mathcal{A} \to \frac{U(S)}{U(S^1)}$ chamado de* ***isomorfismo de rotulamento****. A aplicação (bijetora) $m : \mathcal{A} \to \frac{S}{S^1}$ definida pela composição do isomorfismo de rotulamento com a bijeção $\frac{U(S)}{U(S^1)} \to \frac{S}{S^1}$ é chamado* ***rotulamento isométrico*** *dos subconjuntos de S pertencente à partição.*

Observação 5.8.1 *Uma partição admite um rotulamento isométrico por um grupo $\mathcal{A}$ se:*

i) *S é geometricamente uniforme;*

ii) *Os subconjuntos da partição geometricamente uniformes são mutuamente congruentes;*

iii) *Existem grupos de isometrias de $U(S)$ e $U(S^1)$ tais que $U(S)$ gera S, $U(S^1)$ gera S^1, $U(S^1) \triangleleft U(S)$ e $\mathcal{A} \simeq \frac{U(S)}{U(S^1)}$*

Teorema 5.8.2 *[22] Uma aplicação rotulamento $m : \mathcal{A} \to S/S^1$ é um rotulamento isométrico se, e somente se, para todo $a \in \mathcal{A}$ existe uma isometria u_a tal que para todo $b \in \mathcal{A}$.*

$$m(ab) = u_a(m(b)) \tag{5.49}$$

Com isso, concluímos que é possível estabelecer um alfabeto para um código a partir dos procedimentos adotados no decorrer deste trabalho, uma vez que existe um grupo de rótulos para uma partição geometricamente uniforme no plano hiperbólico.

Podemos citar como importância deste trabalho na geração de um alfabeto para um código corretor de erros a partir de uma constelação de sinais no plano hiperbólico, o fato de que nessa proposta é realizada uma identificação dos sinais da constelação por elementos de uma álgebra dos quatérnios.

Deve estar claro a relevância de termos considerados as álgebras dos quatérnios no contexto aritmético uma vez que a realizabilidade da proposta de construção de constelações de sinais geometricamente uniformes e os correspondentes rotulamentos é alcançada através da conjunção das estruturas algébricas e geométricas.

Capítulo 6

Conclusões

Neste trabalho foram estabelecidas as condições algébricas e geométricas necessárias para a geração de alfabetos de códigos corretores de erros contendo uma estrutura algébrica, a partir das **constelações de sinais geometricamente uniformes** em espaços de sinais euclidianos e hiperbólicos.

Identificamos os sinais dos espaços de sinais euclidianos e hiperbólicos por elementos de um reticulado. Tal identificação possibilitou que o estudo de equivalência dos espaços de sinais, fosse realizado pela equivalência de reticulados.

No Capítulo 3, caracterizamos a equivalência de reticulados através da equivalência das formas quadráticas. Mostramos que a **isotropria** de uma forma quadrática de dimensão 2, constitui um **invariante geométrico** caracterizando em que modelo geométrico os reticulados associados às formas quadráticas de dimensão 2 estão inseridos, ou seja, no plano hiperbólico caso a forma quadrática seja **isotróprica** ou no plano euclidiano caso a forma quadrática seja **anisotróprica**.

No Capítulo 4 estendemos as propostas de Huber [3] e Favareto [19] 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 $GF(p^2)$; ou por elementos de um p-grupo G_{p^n}, a partir de espaços sinais euclidianos bidimensinais identificados pelos elementos dos anéis de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente.

Tal procedimento foi estabelecido através da procura das soluções inteiras x e y das formas quadráticas $f(X,Y) = X^2 + Y^2 = p^n$ $g(X,Y) = X^2 + XY + Y^2 = p^n$ que são provenientes das normas algébricas associadas aos elementos dos anéis de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente.

A proposta de Interlando e Elia [37] de construção de constelações de p^n sinais rotuladas por elementos de corpos de Galois $GF(p^n)$, também foi estendida para p-grupos G_{p^n}, a partir de espaços de sinais euclidianos de dimensão qualquer, identificados por anéis de inteiros algébricos.

No Capítulo 5, fornecemos um procedimento para a determinação dos geradores de um grupo fuchsiano aritmético Γ_{4g}. Mostramos que os grupos Γ_8 e Γ_{12}, associados aos domínios fundamentais F_8 e F_{12} das tesselações $\{8,8\}$ e $\{12,12\}$, respectivamente, são grupos fuchsianos aritméticos.

Identificamos os elementos de um grupo fuchsiano aritmético Γ_{4g} com os elementos de uma ordem dos quatérnios nos casos em que $g = 2$ e 3. Tal identificação possibilitou propor a construção de constelações de sinais no plano hiperbólico, formadas pelos baricentros dos polígonos das tesselações $\{8,8\}$ e $\{12,12\}$. Estes sinais foram identificados com os elementos das ordens dos quatérnios $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ e $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$, respectivamente.

Foi proposta uma maneira de obtenção de subgrupos normais Γ_I, de cardinalidade p^m, em grupos fuchsianos aritméticos Γ_{4g} através da procura de ideais $\mathcal{O}_I$ em $\mathcal{O}$ de cardinalidade p^m, como conseqüência do fato de que os ideais $\mathcal{O}_I$ serem identificados com os subgrupos normais Γ_I no grupo fuchsiano Γ_{4g}.

Foi através da existência dos subgrupos normais Γ_I que garantimos a construção de constelações de p^m sinais no plano hiperbólico, como resultado da ação transitiva de $G_I \simeq \Gamma/\Gamma_I$ no baricentro 0 de F_{4g}.

Finalmente, mostramos que a proposta de **partição geometricamente uniforme** no plano hiperbólico de Lazari [22] se aplica nesse contexto. Dessa forma, ficou evidenciado o rotulamento casado do conjunto de sinais ao grupo G_I, ou seja, mostramos a existência de alfabetos dotados de uma estrutura algébrica para a construção de códigos corretores que venham a ser implementados no plano hiperbólico.

6.1 Propostas de Pesquisas Futuras

Durante o desenvolvimento do processo de construção e rotulamento de constelações de sinais em espaços de sinais euclidianos e hiperbólico, nos deparamos com tópicos que despertaram nossa atenção e que podem ser objetos de pesquisas futuras. Dentre estes podemos citar:

- Verificar se o invariante geométrico isotropria de uma forma quadrática caracteriza os reticulados em dimensões maiores que dois em espaços euclidianos e hiperbólicos, como mostramos no caso bidimensional.
- Construir constelações de sinais no plano hiperbólico que sejam identificadas por ordens dos quatérnios $\mathcal{O}$ diferente das ordens dos quatérnios $\mathcal{O}_{\mathbb{Z}[\sqrt{2}]}$ e $\mathcal{O}_{\mathbb{Z}[\sqrt{3}]}$.
- Propor critérios em função da congruência de um número primo p módulo 4, para a construção de constelações de p^m sinais no plano hiperbólico, e fornecer a estrutura algébrica proveniente deste rotulamento, se será um p-grupo multiplicativo G_{p^m} ou um grupo multiplicativo de um corpo de Galois $GF(p^m)$ em espaços de sinais hiperbólicos.
- Propor construção de constelações de sinais em espaços hiperbólicos de dimensão maior que 2 que sejam identificados por elementos de uma estrutura algébrica.
- Identificar uma métrica discreta d nas constelações de sinais S do plano hiperbólico que satisfaça o casamento entre os sinais de S e os elementos do grupo de rótulos G.

Referências Bibliográficas

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

[6] Z.I. Borevich, e I.R. Shafarevich, *Number Theory*, New York: Academic Press, 1966.

[7] Svetlana Katok, *Fuchsian Groups*, The University of Chicago Press, 1992.

[8] K. Takeuchi, *A characterization of aritmetic Fuchsian Groups*, J.Math.Soc. Japan, vol 27 No.4, 1975.

[9] Marcelo Firer, *Grupos Fuchsianos*, Notas de Aula, IMECC-UNICAMP .

[10] O.T.O'Meara, *Introduction to Quadratic Forms*, Spring-Verlag, Berlim-Heidelberg-New York, 1973.

[11] S.Johansson,"On fundamental domains of arithmetic fuchsian groups", www.math.chalmers.se/ sj/forskning.html.

[12] S.Johansson,"Genera of arithmetic fuchsian groups", www.math.chalmers.se/ sj/forskning.html.

[13] S.Johansson,"Description of quaternion algebras", www.math.chalmers.se/ sj/forskning.html.

[14] P. Samuel, *Théorie Algébrique des Nombres*, Paris: Hermann, 1967.

[15] S. Lang, *Algebra*, New York: Addison-Wesley, 1970.

[16] P. Ribenboim, *Algebraic Numbers*, New York, Wiley-Interscience, 1972.

[17] I.N.Stewart e D.O.Tall, *Algebraic Number Theory*, Chapman and Hall, 1986.

[18] D.A. Marcus, *Number Fields*, New York: Springer-Verlag, 1977.

[19] O.M. Favareto, *Códigos de Bloco Linares sobre Anéis de Inteiros Algébricos com Alfabeto Casado a $GF(p)$*, Tese de Doutorado, FEEC-UNICAMP, 1996.

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

[21] A.J. Engler, e P. Brumatti, *Anéis de Inteiros*, XII Escola de Álgebra, Diamantina, M.G, 1992.

[22] H.Lazari, *Uma Contribuição á Teoria de Códigos Geometricamente Uniformes Hiperbólicos*, Tese de Doutorado, FEEC-UNICAMP, 2000.

[23] E.D.Carvalho, *Estudo Local e Global de Propriedades Aritméticas*, Dissertação de Mestrado, IMECC-UNICAMP, 1997.

[24] 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.

[25] M.A. Armstrong, *Groups and Symmetry*, New York: Springer-Verlag, 1988.

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

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

[28] J.H. Conway, e N.J.A. Slone *Sphere Packing, Lattices and Groups*, New York: Springer, 1998.

[29] A.F. Beardon, *The Geometry of Discrete Groups* , New York: Springer, 1982.

[30] P.A. Firby, e C.F.Gardiner *Surface Topology*, New York, Ellis Horwood, 1991.

[31] J. Rotman, *The Theory of Groups, An Introduction*, Boston, Ally and Bacon, 1973.

[32] J.B. Conway, *A Course in Function Analysis*, Berlin: Springer, 1985.

[33] M.H. Coxeter, *Extrem Forms*, *Canadian Journal Of Mathematics*, vol.3, pp.391-441, 1951.

[34] O. Endler, *Valuation Theory*, New York: Springer-Verlag, 1972.

[35] 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.

[36] J.C.Interlando,R.Palazzo Jr,J.R.Geronimo,A.A.Andrade,O.M.Favareto e T.P.Nobrega Neto, *Códigos Corretores de Erro sobre Estruturas de Corpos, Anéis e Grupos* , Notas de Aula, FEEC-UNICAMP.

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

[38] E.D.Carvalho e R.Palazzo Jr. "Construção de Constelações com p^n Sinais Provenientes de um Corpo de Números", *XXIII Congresso Nacional de Matemática Aplicada-CNMAC*, Santos SP, Setembro de 2000.

[39] E.D.Carvalho, R.Palazzo Jr. e M.Firer "Constelações de Sinais Geometricamente Uniformes Provenientes de Grupos Fuchsianos Aritméticos", *IX Encontro em Álgebra USP/UNICAMP/UNESP - ENAL*, São Pedro S.P, Setembro de 2001.

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

[41] J.Brzezinsk "On Orders in quaternion algebras" *Communication in Algebras*, vol.11,No.5 pp. 501-522, 1983.

[42] A.Garcia , e I.Lequain *Álgebra: Um Curso de Introdução*, Projeto Euclides, 1988.

[43] H.Cohen *A Course in Computational Algebraic Numbers Theory*, Springer, 1993.