Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação
Departamento de Telemática

# Códigos Geometricamente Uniformes Derivados de Grafos sobre Anéis Quocientes de Inteiros e de Ordens dos Quatérnios

**Cátia Regina de Oliveira Quilles Queiroz**

Tese de Doutorado

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

Banca Examinadora:

**Prof. Dr. Reginaldo Palazzo Jr.** - FEEC/UNICAMP
**Prof. Dr. Antônio Aparecido de Andrade** - IBILCE/UNESP
**Prof. Dr. Henrique Lazari** - IGCE/UNESP
**Prof. Dr. Marcelo Firer** - IMECC/UNICAMP
**Prof. Dr. Sueli Irene Rodrigues Costa** - IMECC/UNICAMP

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas - FEEC - UNICAMP, como parte dos requisitos para a obtenção do Título de Doutor em Engenharia Elétrica.

**Campinas - SP**
**Fevereiro - 2011**

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

Q32c

Queiroz, Cátia Regina de Oliveira Quilles
Códigos geometricamente uniformes derivados de grafos sobre anéis quocientes de inteiros e de ordens dos quatérnios / Cátia Regina de Oliveira Quilles Queiroz. -- Campinas, SP: [s.n.], 2011.

Orientador: Reginaldo Palazzo Júnior.
Tese de Doutorado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Teoria da codificação. 2. Geometria hiperbólica. 3. Teoria dos reticulados. I. Palazzo Júnior, Reginaldo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Título em Inglês: Geometrically uniform codes derived from graphs over quotient rings of integers and quaternion orders
Palavras-chave em Inglês: Coding theory, Hyperbolic geometry, Lattice theory
Área de concentração: Telecomunicações e Telemática
Titulação: Doutor em Engenharia Elétrica
Banca examinadora: Antônio Aparecido de Andrade, Henrique Lazari, Marcelo Firer, Sueli Irene Rodrigues Costa
Data da defesa: 25/02/2011
Programa de Pós Graduação: Engenharia Elétrica

## COMISSÃO JULGADORA - TESE DE DOUTORADO

**Candidata:** Cátia Regina de Oliveira Quilles Queiroz

**Data da Defesa:** 25 de fevereiro de 2011

**Título da Tese:** "Códigos Geometricamente Uniformes Derivados de Grafos sobre Anéis Quocientes de Inteiros e de Ordens dos Quatérnios"

Prof. Dr. Reginaldo Palazzo Júnior (Presidente): _____

Prof. Dr. Antonio Aparecido de Andrade: _____

Prof. Dr. Henrique Lazari: _____

Prof. Dr. Marcelo Firer: _____

Profa. Dra. Sueli Irene Rodrigues Costa: _____

"É graça divina começar bem e persistir na caminhada certa. Graça maior é diante das dificuldades não desistir nunca, pois provavelmente aquele que nunca cometeu um erro nunca fez uma descoberta."

*D. Hélder Câmara e Samuel Smiles*

Ao meu marido Igor,
companheiro de erros e acertos
na caminhada da vida,
e razão do meu viver,
*dedico*

# Agradecimentos

Ao concluir este trabalho, agradeço:

A Deus, por ter me colocado neste caminho e me guiado em todos os momentos, colocando pessoas tão especiais na minha vida, me dando sempre forças para lutar e realizar todos os meus sonhos.

Ao meu orientador Prof. Dr. Reginaldo Palazzo Júnior, pela amizade tão sincera, pelo incentivo, pela paciência, dedicação e compreensão. Por ser um exemplo para todos os que o cercam, não só como profissional, pelo entusiasmo e amor que dedica ao trabalho, mas como pessoa humilde e de coração puro que se pode contar em todas as horas.

Ao meu marido Igor, por ser a razão da minha vida, meu amigo e companheiro, por seu amor, sua confiança, incentivo e compreensão na minha ausência, que foram fundamentais para a minha perseverança e a quem dedico toda a minha vida e minhas conquistas e com quem espero passar a vida toda.

Aos meus pais José e Maria, que com muito esforço possibilitaram o início deste sonho. Que mesmo sem perceber, ao mostrar o orgulho e confiança que depositavam em mim me davam forças pra continuar.

Aos meus avós José e Terezinha, que estiveram sempre com as mãos estendidas pra me ajudar nos momentos de dificuldade, pela confiança, amor e carinho depositados.

Aos meus irmãos Lucas e Angélica, que entenderam a minha ausência em momentos importantes.

Aos meus segundos pais, minha sogra Regina e meu sogro Romualdo, pelo carinho e confiaça e por me entregarem seu maior tesouro, seu filho Igor.

Ao Prof. Dr. Antonio Aparecido de Andrade, por ter me apresentado este novo caminho e confiado em mim quando eu ainda era uma menina de "olhos vermelhos"lutando contra o sono após ter trabalhado o dia todo para estudar e mudar de vida.

Às minhas grandes amigas Clarice e Luzinete, com quem sempre pude contar em todos os momentos de dificuldade e de alegria e com as quais passei momentos inesquecíveis e importantes desta caminhada.

A todos os amigos do LTIA, em especial a Andréa, Lucila, Wanessa, Eduardo, Mércio e Alessandro, pela amizade sincera, o agradável convívio, os momentos de descontração e as importantes discussões que contribuiram muito para a realização deste trabalho.

Aos professores da FEEC, IMECC e UNESP-São José do Rio Preto, pela excelente formação e amizade.

Ao pessoal técnico administrativo, em especial a Flávia, Noêmia, Soraia e Edson por sua ajuda e competência.

Aos membros da banca examinadora por aceitarem o convite, pela atenção dedicada a este trabalho, pelas sugestões e considerações que foram de grande valia.

À Capes por parte do auxílio financeiro.

A todos que direta ou indiretamente contribuíram para a realização deste trabalho.

# Resumo

Neste trabalho apresentamos a construção de códigos geometricamente uniformes derivados de grafos sobre anéis quocientes de inteiros e de ordens dos quatérnios. Inicialmente propomos um procedimento para a geração de códigos quase-perfeitos derivados de grafos sobre anéis quocientes de inteiros, que além de serem geometricamente uniformes, são capazes de corrigir mais padrões de erros que os códigos perfeitos, porém com uma menor cardinalidade. Além disso, observamos que os códigos perfeitos são um caso particular dos códigos quase-perfeitos. Os códigos geometricamente uniformes derivados de quocientes de ordens dos quatérnios foram obtidos de forma similar, porém a geometria relacionada é a hiperbólica e os códigos derivados estão no plano hiperbólico. A estrutura algébrica associada a essa classe de códigos não havia sido obtida até então para esta geometria. Apresentamos ainda um procedimento para o rotulamento de pontos gerados por tesselações do plano hiperbólico no disco de Poincaré, e obtemos a representação geométrica dos códigos obtidos.

**Palavras-chave:** códigos geometricamente uniformes, anéis quocientes, grafos, ordens dos quatérnios, tesselações, geometria hiperbólica.

# Abstract

In this work we present the construction of geometrically uniform codes derived from graphs over quotient rings of integers and quaternion orders. Initially we propose a procedure to generate quasi-perfect codes derived from graphs over quotient rings of integers, which in addition to preserving the property of being geometrically uniform codes they are able to correct more error patterns than the perfect codes, by decreasing its cardinality. Furthermore, we observe that the perfect codes are a particular case of the quasi-perfect codes. The geometrically uniform codes derived from quotient of the quaternion orders are obtained similarly as in the previous case, however the related geometry is the hyperbolic and the derived codes are on the hyperbolic plane. The algebraic structure associated with this class of codes had not been obtained so far for this geometry. We also present a procedure for labeling the points generated by tesselations of the Poincaré disk, and showing the geometric representation of the aforementioned codes.

**Keywords:** geometrically uniform codes, quotient rings, graphs, quaternion orders, tessellations, hyperbolic geometry.

# Índice de Símbolos

$\mathbb{N}$: conjunto dos números naturais

$\mathbb{Z}$: conjunto dos números inteiros

$\mathbb{Q}$: conjunto dos números racionais

$\mathbb{R}$: conjunto dos números reais

$\mathbb{C}$: conjunto dos números complexos

$R$: anel

$M$: módulo

$D$: domínio

$E$: espaço métrico

$\mathcal{G}$: grupo

$\{\alpha_1, \ldots, \alpha_n\}$: n-upla

$I_R(A)$: fêcho inteiro de $A$ em $R$

$\mathbb{K}, \mathbb{L}$: corpos

$I_R(\mathbb{K})$: fêcho algébrico de $\mathbb{K}$ em $R$

$[\mathbb{L} : \mathbb{K}]$: grau de $\mathbb{L}$ sobre $\mathbb{K}$

$\mathbb{K}(\alpha_1, \ldots, \alpha_n)$: corpo obtido pela adjunção de $\alpha_1, \ldots, \alpha_n$ a $\mathbb{K}$

$\mathbb{Q}(\theta)$: corpo de números

$\mathbb{Q}(\sqrt{d})$: corpo quadrático

$\sigma$: monomorfismo de $\mathbb{K}$ em $\mathbb{C}$

$\prod$: produtório

$\sum$: somatório

$(a_{ij})$: matriz

$det(a_{i,j})$: determinante de $(a_{i,j})$

$f_\alpha(x)$: polinômio característico de $\alpha$

$m_\alpha(x)$: polinômio minimal de $\alpha$

$N(\alpha)$: norma de $\alpha$

$T(\alpha)$: traço de $\alpha$

$I_{\mathbb{K}}$: anel dos inteiros de $\mathbb{K}$

$U(R)$: grupo das unidades de $R$

$\alpha|\beta$: $\alpha$ divide $\beta$

$\langle\alpha\rangle$: ideal gerado por $\alpha$

$< \alpha_1, \ldots, \alpha_n >$: ideal gerado por $\alpha_1, \ldots, \alpha_n$

$\mathcal{I}$: ideal

$N(\mathcal{I})$: norma do ideal $\mathcal{I}$

$card(X)$: cardinalidade do conjunto $X$

$|X|$: módulo do conjunto $X$

$\frac{A}{I}$: quociente de A por I

$mdc(m, n)$: máximo divisor comum de $m$ e $n$

$A \times B$: produto cartesiano de $A$ por $B$

$\overline{x}$: conjugado complexo do elemento $x$

$f(v)$: forma quadrática

$B_f$: aplicação bilinear

$\Lambda_\beta$: reticulado com base $\beta$

$\mathcal{P}_\beta$: região fundamental de $\Lambda_\beta$

$||a||$ norma de $a$

$vol(\Lambda_\beta)$ volume do reticulado

$\Delta(\Lambda_\beta)$ : densidade de empacotamento

$\mathcal{B}(\rho)$ esfera com centro na origem e raio $\rho$

$\delta(\Lambda_\beta)$ : densidade de centro do reticulado $\Lambda_\beta$

$\sigma_{\mathbb{K}}$: homomorfismo canônico ou de Minkowiski

$\overline{\sigma}$ : conjugação complexa ($\overline{\sigma}(x) = \overline{x}$)

$[z]$ : o inteiro mais próximo de $z$

$d_{min}$ : distância mínima

$\mathcal{S}$: constelação de sinais

$U(\mathcal{S})$: grupo de simetrias de $\mathcal{S}$

$\mathcal{V}_{\mathcal{S}}(s_0)$: região de Voronoi de $s_0$ em $\mathcal{S}$

$\mathbb{H}^{n+1}$: espaço hiperbólico de dimensão $n + 1$

$\mathbb{H}^2$: plano hiperbólico

$ds$: métrica hiperbólica

$\gamma$: curva continuamente diferenciável por partes

$\|\gamma\|$: comprimento de $\gamma$

$d(p, q)$: distância entre $p$ e $q$

$\partial_\infty \mathbb{H}^2$: bordo de $\mathbb{H}^2$

$\mu(A)$: área hiperbólica do conjunto $A$

$\mathbb{D}^2$: disco unitário

$\partial \mathbb{D}^2$: bordo de $\mathbb{D}^2$

$PSL(2,\mathbb{R})$: grupo projetivo linear

$SL(2,\mathbb{R})$: grupo unimodular

$Isom(\mathbb{H}^2)$: grupo de isometrias de $\mathbb{H}^2$

$\Gamma$: grupo Fuchsiano

$\mathcal{G}(x)$: $\mathcal{G}$-órbita do ponto $x$

$\mathcal{G}_x$: estabilizador do ponto $x$

$D_{z_0}(\Gamma)$: região de Dirichlet de $\Gamma$

$\{p,q\}$: tesselação hiperbólica

$(g; m_1, \ldots, m_r)$: assinatura de $\Gamma$

$\mathbb{S}$: superfície compacta

$A$: álgebra

$\mathcal{R}$: radical de $A$

$Z$: centro de $A$

$\mathcal{A} = (a,b)_{\mathbb{K}}$: álgebra dos quatérnios

$\{1,i,j,k\}$: base da álgebra dos quatérnios

$Nrd(\alpha)$: norma reduzida de $\alpha$

$Trd(\alpha)$: traço reduzido de $\alpha$

$\mathcal{O}$: ordem dos quatérnios

$\mathcal{H}$: quatérnios de Hamilton

$\mathbb{H}$: álgebra de divisão

$\mathcal{M}$: ordem maxinal

$d(\mathcal{A})$: discriminante de $\mathcal{A}$

$\mathcal{A}^{\varphi}$: lugar da álgebra dos quatérnios $\mathcal{A}$

$g$ : gênero da superfície

$\mathbb{Z}[i]$: anel dos inteiros de Gauss

$\mathbb{Z}[\omega]$: anel dos inteiros de Einsenstein-Jacobi

$\mathbb{Z}[\rho]_{\alpha}$: ideal de $\mathbb{Z}[\rho]$ gerado por $\alpha$

$G_{\alpha}$: grafo gerado por $\alpha$

$D_{\alpha}$: distância induzida por $G_{\alpha}$

$\mathcal{C}$: código

$t$: raio de cobertura do código

$B_t(\eta)$: bola de raio $t$

$P_{4g}$: polígono hiperbólico regular de $4g$ lados

# Sumário

**Dedicatória** **vii**

**Agradecimentos** **ix**

**Resumo** **xi**

**Abstract** **xiii**

**Índice de Símbolos** **xv**

**1 Introdução** **1**

1.1 Histórico . . . . . 1

1.2 Proposta do trabalho . . . . . 3

1.3 Descrição do trabalho . . . . . 4

**2 Elementos de Teoria Algébrica dos Números e Geometria Hiperbólica** **5**

2.1 Teoria Algébrica dos Números . . . . . 5

2.1.1 Módulos Noetherianos . . . . . 5

2.1.2 Elementos Inteiros . . . . . 7

2.1.3 Extensões de Corpos . . . . . 11

2.1.4 Corpos Quadráticos . . . . . 14

2.1.5 Norma e Traço de um Elemento . . . . . 16

2.1.6 Decomposição em Irredutíveis . . . . . 16

2.1.7 Norma de um Ideal . . . . . 21

2.1.8 Formas Quadráticas . . . . . 22

2.1.9 Reticulados . . . . . 23

2.1.10 Empacotamento Esférico . . . . . 26

2.1.11 Constelações de Sinais . . . . . 31

2.2 Geometria Hiperbólica . . . . . 32
2.2.1 Notas Históricas . . . . . 32
2.2.2 Espaço Hiperbólico . . . . . 34
2.2.3 Modelos Euclidianos do Plano Hiperbólico . . . . . 35
2.2.4 Grupos Fuchsianos . . . . . 37
2.2.5 Região Fundamental . . . . . 41
2.2.6 Tesselações Regulares no Plano Hiperbólico . . . . . 41
2.2.7 Grupos Fuchsianos Co-Compactos . . . . . 42
2.2.8 Assinatura de um Grupo Fuchsiano . . . . . 44

**3 Ordens dos Quatérnios e Grupos Fuchsianos Aritméticos 47**
3.1 Ordens dos Quatérnios . . . . . 47
3.2 Reticulados Hiperbólicos . . . . . 52
3.3 Grupos Fuchsianos Aritméticos . . . . . 56
3.3.1 Grupo Fuchsiano Aritmético $\Gamma_{4g}$ . . . . . 62
3.4 Identificação de Grupos Fuchsianos $\Gamma_{4g}$ por Ordens dos Quatérnios . . . . . 64

**4 Códigos Geometricamente Uniformes Derivados de Grafos sobre Anéis dos Inteiros 67**
4.1 Anéis Quocientes . . . . . 67
4.2 Códigos sobre Grafos . . . . . 69
4.3 Códigos Perfeitos Derivados de Grafos sobre Anéis dos Inteiros . . . . . 72
4.4 Códigos Quase-Perfeitos Derivados de Grafos sobre Anéis dos Inteiros Gaussianos 73
4.5 Códigos Quase-Perfeitos Derivados de Grafos sobre Anéis dos Inteiros de Einsenstein-Jacobi . . . . . 77

**5 Códigos Geometricamente Uniformes Derivados de Grafos sobre Ordens dos Quatérnios 81**
5.1 Anéis Quocientes de Ordens dos Quatérnios Associadas à $\Gamma_{4g}$ . . . . . 82
5.1.1 Caso $g = 2^n$ . . . . . 82
5.1.2 Caso $g = 3.2^n$ . . . . . 88
5.1.3 Caso $g = 5.2^n$ . . . . . 90
5.2 Rotulamento de Pontos Gerados por Tesselações do Plano Hiperbólico no Disco de Poincaré . . . . . 92
5.3 Códigos sobre Grafos . . . . . 97

5.4 Códigos Geometricamente Uniformes sobre Ordens dos Quatérnios . . . . . 98

**6 Conclusões** **101**

6.1 Perspectivas para Trabalhos Futuros . . . . . 102

**Referências Bibliográficas** **103**

# Capítulo 1

# Introdução

Neste capítulo apresentaremos um breve histórico do que foi feito até então no contexto de códigos geometricamente uniformes e geometria hiperbólica, falaremos sobre a nossa proposta e descre-
veremos os demais capítulos que compõem este trabalho.

## 1.1 Histórico

O estudo de códigos de grupo foi iniciado por Slepian [1] para canais Gaussianos. Forney [2] propôs uma classe mais geral de códigos de grupo que tem propriedades de simetria similares, chamados *códigos geometricamente uniformes*. Esta classe de códigos engloba a classe dos códigos de grupo de Slepian e os códigos reticulados permitindo que os elementos do grupo gerador sejam isometrias arbitrárias do espaço euclidiano $\mathbb{R}^n$ ao invés de transformações ortogonais ou translações consideradas de forma separada. Tais códigos apresentam propriedades de simetria altamente desejáveis, tais como: todas as regiões de Voronoi são congruentes; o perfil de distâncias é o mesmo para qualquer palavra-código; e as palavras código possuem a mesma probabilidade de erro.

O conceito de códigos geometricamente uniformes é ampliado em [3] para qualquer espaço métrico e em [4], [5], foram propostas novas métricas vindas da teoria de grafos sobre estruturas matemáticas dadas por anéis quocientes e uma subclasse dos códigos geometricamente uniformes, chamados *códigos perfeitos*, foi construída em dimensão 2, utilizando grafos sobre quocientes de anéis dos inteiros de Gauss e de Einsenstein-Jacobi.

Em [6], [7] construimos uma outra subclasse de códigos geometricamente uniformes, mais geral que os códigos perfeitos, chamados *códigos quase-perfeitos*, também utilizando grafos

sobre quocientes de anéis dos inteiros. Para o anel dos inteiros de Gauss observamos que a constelação de sinais possui região de Voronoi dada por quadrados e pode ser representada pelo reticulado $\mathbb{Z}^2$, enquanto que para o anel dos inteiros de Einsenstein-Jacobi a constelação de sinais possui região de Voronoi dada por hexágonos e pode ser representada pelo reticulado hexagonal $A_2$.

No estudo dos códigos reticulados de dimensão dois, sabe-se que para o reticulado $\mathbb{Z}^2$ a modulação do tipo $QAM$ tem um melhor desempenho que a modulação do tipo $PSK$. A pergunta que surge é, porque a constelação com modulação $QAM$ tem melhor desempenho? Observou-se que as constelações obtidas podem ser representadas geometricamente por um círculo para a modulação $PSK$, e por um quadrado para a modulação $QAM$. Fazendo o pareamento dos lados destas figuras, as superfícies obtidas são a esfera e o toro, respectivamente, que possuem gênero $g = 0$ e $g = 1$. Uma possível inferência aqui é a de que o invariante topológico associado ao desempenho de uma modulação é o gênero da superfície, que se obtém fazendo o pareamento dos lados da figura ou região fundamental da constelação. Nesta busca por constelações de sinais com melhor desempenho, constelações associadas à superfícies com gênero $g \geq 2$ tem sido estudadas. Tais superfícies podem ser obtidas de forma homogênea ( curvatura constante) como quocientes do plano hiperbólico e portanto a geometria utilizada deve ser a hiperbólica.

Em um trabalho pioneiro no contexto da teoria de comunicações e projeto de sistemas de comunicações no plano hiperbólico [8] considera as tesselações auto-duais $\{p, p\}$, que são um importante subconjunto das tesselações $\{p, q\}$, onde $\{p, q\}$ denota um polígono regular de $p$ lados onde em cada vértice $q$ desses polígonos regulares se encontram, tendo em comum somente as arestas. Em [9] foram construídas famílias de constelações de sinais provenientes de quocientes de espaços hiperbólicos por grupos discretos de isometrias. Em [10] foi proposta 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, região fundamental da tesselação $\{8, 8\}$, e do grupo de isometrias do $p$-ágono da tesselação $\{p, 3\}$. Em [11] as tesselações do tipo $\{4g, 4g\}$ para $g = 2$ e 3, e em [12] para $g = 2^n$, $3.2^n$ e $5.2^n$, foram consideradas de modo que os grupos Fuchsianos aritméticos formados por elementos que fazem o pareamento dos lados dos polígonos obtidos por estas tesselações, são identificados em ordens dos quatérnios e o rotulamento de algumas constelações de sinais geometricamente uniformes particulares para $g = 2, 3$ e 4 a partir dos grupos Fuchsianos aritméticos foi obtido. Já em [13], foram consideradas tesselações hiperbólicas da forma $\{12g - 6, 3\}$, cuja cardinalidade é maior do que as obtidas a partir das auto-duais $\{4g, 4g\}$. Ainda, sob o ponto de

vista geométrico e combinatorial, em [14] foram obtidas tabelas de possíveis códigos no plano hiperbólico.

Na prática, também verifica-se que dimensões maiores são mais úteis. Em [15] foram estudados códigos sobre espaços de sinais de dimensão quatro e as constelações modeladas por meio de grafos definidos sobre anéis quocientes dos inteiros de Lipschitz, ou seja, anéis quocientes da ordem dos quatérnios sobre o corpo dos números reais.

## 1.2 Proposta do trabalho

A construção de códigos perfeitos derivados de grafos sobre quocientes de anéis dos inteiros proposta por [4] e [5] abre espaço para a construção de uma classe de códigos mais geral chamados códigos quase-perfeitos, que possui uma capacidade de correção de erros maior que os códigos perfeitos, com o custo de se obter um menor número de pontos, sendo ambos uma subclasse dos códigos geometricamente uniformes. Tais códigos podem ser utilizados em canais apresentando assimetria. Essa é a primeira parte da nossa proposta de estudo.

Além disso, estendemos as idéias utilizadas para a construção dos códigos geometricamente uniformes derivados de grafos sobre quocientes de anéis dos inteiros para grafos sobre quociente de ordens dos quatérnios, assim como feito em [15] para a ordem dos quatérnios de Hamilton, também chamada inteiros de Lipschitz, a qual está relacionada ainda à geometria euclidiana. Nossa proposta de construção de códigos geometricamente uniformes sobre quociente de ordens dos quatérnios segue os mesmos passos usados na construção sobre quocientes de anéis dos inteiros, contudo levando em consideração a geometria relacionada às superfícies de gênero $g \geq 2$, a geometria hiperbólica.

Em [11] e [12] os grupos Fuchsianos $\Gamma_{4g}$ para $g \geq 2$, formados pelas isometrias que fazem o pareamento dos lados de um polígono hiperbólico $P_{4g}$ que tessela o plano hiperbólico $\mathbb{D}^2$, foram associados às ordens dos quatérnios. Assim, conhecidas as ordens dos quatérnios que fazem o pareamento dos lados dos polígonos, obtemos resultados para quocientes de ordens dos quatérnios análogos aos obtidos para quocientes de anéis dos inteiros e construimos então códigos geometricamente uniformes derivados de grafos sobre o quociente destas ordens. Desta forma, obtemos códigos geometricamente uniformes no plano hiperbólico.

Até onde é de nosso conhecimento estruturas de códigos não foram obtidas anteriormente em geometria hiperbólica, neste sentido tivemos um avanço na aplicação deste contexto.

## 1.3 Descrição do trabalho

A organização básica dos capítulos que compõem o escopo deste trabalho está dividida como se segue.

Inicialmente, no **Capítulo 2**, estabelecemos a terminologia e a notação adotadas neste trabalho, revisando os conceitos de teoria dos números e de geometria hiperbólica necessários para a compreensão e desenvolvimento dos demais capítulos.

O **Capítulo 3** apresenta as ordens dos quatérnios e os grupos Fuchsianos aritméticos. Em seguida fazemos a identificação destes grupos pela ordem dos quatérnios associada.

Apresentamos nossos primeiros resultados no **Capítulo 4** referentes à códigos geometricamente uniformes no plano euclidiano. Construiremos uma sub-classe dos códigos geometricamente uniformes, chamados códigos quase-perfeitos, sobre os anéis quocientes dos inteiros de Gauss e de Einsenstein-Jacobi. Veremos que esta construção pode ser facilmente estendida para um anel dos inteiros qualquer.

No **Capítulo 5**, apresentamos a construção de códigos geometricamente uniformes no plano hiperbólico. Inicialmente construimos anéis quocientes de ordens dos quatérnios e obtemos resultados para superfícies de gênero $g = 2^n$, $3.2^n$ e $5.2^n$. Fazemos ainda o rotulamento de pontos gerados por tesselações do plano hiperbólico no disco de Poincaré e vemos alguns conceitos sobre grafos e códigos sobre grafos a fim de construirmos códigos geometricamente uniformes derivados de grafos sobre anéis quocientes de ordens dos quatérnios.

Finalmente, concluímos o trabalho no **Capítulo 6** com uma avaliação dos resultados e os possíveis trabalhos decorrentes.

# Capítulo 2

# Elementos de Teoria Algébrica dos Números e Geometria Hiperbólica

Neste capítulo apresentamos os principais elementos da teoria algébrica dos números e da geometria hiperbólica necessários para o desenvolvimento dos demais capítulos.

## 2.1 Teoria Algébrica dos Números

Nesta seção apresentamos conceitos básicos da teoria algébrica dos números envolvendo módulos Noetherianos, elementos inteiros, norma e traço, decomposição de elementos, norma de um ideal, formas quadráticas, reticulados e constelações. Estes resultados são fundamentais e formam a base para o entendimento dos demais capítulos e o desenvolvimento do trabalho. Para tal, utilizamos as referências [16]-[25].

### 2.1.1 Módulos Noetherianos

Nesta subseção apresentamos a definição e algumas propriedades sobre módulos e módulos Noetherianos, necessárias para o entendimento das demais seções.

Seja $R$ um anel. Um *$R$-módulo* $M$ é um grupo abeliano $(M, +)$, junto com a função $\alpha : R \times M \to M$ definida por $\alpha(r, m) = rm$, com $r \in R$ e $m \in M$, satisfazendo para todo $r, s \in R$, $m, n \in M$:

1. $(r + s)m = rm + sm$;

2. $r(m + n) = rm + rn$;

3. $r(s \cdot m) = (r \cdot s)m$;

4. $1 \cdot m = m$.

A função $\alpha$ é chamada uma *R-ação* sobre $M$. Se $R$ é um corpo $\mathbb{K}$, então um $R$-módulo é o mesmo que um espaço vetorial sobre $\mathbb{K}$.

Um anel $R$ com as operações de soma e produto é chamado *domínio* se o produto de quaisquer dois elementos não nulos de $R$ é um elemento não nulo. Um ideal $\mathcal{I}$ de $R$ é dito *principal* se existe $\alpha \in R$ tal que $\mathcal{I}$ é gerado por $\alpha$, e é denotado por $\mathcal{I} = \langle \alpha \rangle$. Um domínio no qual todo ideal é principal é chamado *domínio de ideais principais*.

**Definição 2.1.1** *Um* $R$-submódulo *de* $M$ *é um subgrupo* $N$ *de* $M$ *tal que se* $n \in N$, $r \in R$, *então* $rn \in N$.

Um módulo $M$ é dito *finitamente gerado* se possuir um conjunto finito de geradores. O conjunto de elementos linearmente independentes que gera $M$ é chamado *base*. Um $R$-módulo $M$ que possui uma base (não necessariamente finita) é chamado de *módulo livre*, e o número de elementos da base é chamado *posto* de $M$. Nem todo módulo finitamente gerado possui uma base, e nem todo submódulo de um módulo livre é livre.

**Definição 2.1.2** *Seja* $R$ *um domínio. Dizemos que um* $R$*-módulo* $M$ *é livre de torção se não existe* $\alpha \in R$, $\alpha \neq 0$, *tal que* $\alpha m = 0$, *para todo* $m \in M$.

**Teorema 2.1.1** *[16, Theorem 1, p.92] Todo módulo finitamente gerado livre de torção sobre um domínio de ideais principais é um módulo livre.*

**Demonstração:** *Sejam* $R$ *um domínio de ideais principais,* $M$ *um* $R$*-módulo livre de torção e* $\{\alpha_1, \ldots, \alpha_n\}$ *um conjunto de geradores de* $M$. *Se* $\{\beta_1, \ldots, \beta_m\} \neq \{\alpha_1, \ldots, \alpha_n\}$ *é um conjunto de elementos de* $M$ *linearmente independentes, então* $\{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m\}$ *é linearmente dependente, para* $1 \leq i \leq n$ *e* $1 \leq j \leq m$. *Assim, existem* $a_i, b_{i,1}, \ldots, b_{i,m} \in R$, *não todos nulos, tais que*

$$a_i\alpha_i + b_{i,1}\beta_1 + \ldots + b_{i,m}\beta_m = 0. \tag{2.1}$$

*Temos que* $a_i$ *é não nulo, pois* $b_{i,1}, \ldots, b_{i,m}$ *são todos não nulos e* $\{\beta_1, \ldots, \beta_m\}$ *é linearmente independente. Seja então* $L$ *o submódulo de* $M$ *gerado por* $\{\beta_1, \ldots, \beta_m\}$. *Logo,* $L$ *é livre, pois o conjunto de geradores é uma base. Da Equação (2.1) temos que* $a_i\alpha_i = -(b_{i,1}\beta_1 + \ldots + b_{i,m}\beta_m)$, *e isto implica que* $a_i\alpha_i \in L$. *Tomando* $a = \prod_{i=1}^{n} a_i$ *temos que* $a\alpha_i \in L$ *para todo* $1 \leq i \leq n$ *e como* $\{\alpha_1, \ldots, \alpha_n\}$ *é um conjunto de geradores de* $M$, *segue que* $aM \subseteq L$, *então* $aM$ *é um submódulo*

*livre. Agora, considere a função* $f : M \to aM$ *definida por* $f(m) = am$ *para todo* $m \in M$. *Como* $M$ *é livre de torção, temos que* $f$ *é um isomorfismo. Portanto,* $M$ *é livre.* ■

Sejam $R$ um anel e $M$ um $R$-módulo. Dizemos que $M$ é um *$R$-módulo Noetheriano* se satisfaz uma das seguintes condições:

1. Toda família não vazia de $R$-submódulos de $M$ tem um elemento maximal.
2. Toda sequência crescente de $R$-submódulos de $M$ é estacionária.
3. Todo $R$-submódulo de $M$ é finitamente gerado.

Um anel $R$ é Noetheriano se $R$ considerado como um $R$-módulo for Noetheriano.

**Teorema 2.1.2** *[17, Theorem 1,p.21] Sejam* $R$ *um anel de ideais principais e* $M$ *um* $R$*-módulo livre de posto* $n$. *Se* $M'$ *é um* $R$*-submódulo de* $M$, *então:*

1. $M'$ *é livre de posto* $r$, *para* $0 \leq r \leq n$.
2. *Se* $M' \neq 0$, *então existe uma base* $\{v_1, \ldots, v_n\}$ *de* $M$ *e elementos não nulos* $a_1, \ldots, a_r \in R$ *tais que* $\{a_1v_1, \ldots, a_rv_r\}$ *é uma base de* $M'$ *e que* $a_i$ *divide* $a_{i+1}$, *para* $1 \leq i \leq r-1$.

### 2.1.2 Elementos Inteiros

Nesta subseção veremos o conceito de elementos inteiros sobre um anel enfocando suas principais propriedades.

Seja $A \subseteq R$ um anel. Um elemento $\alpha \in R$ é chamado *elemento inteiro* sobre $A$ se $\alpha$ é raiz de um polinômio mônico com coeficientes em $A$, isto é, se existem $a_0, a_1, \ldots, a_{n-1} \in A$, não todos nulos, tal que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

Em particular, todo elemento de $A$ é inteiro sobre $A$.

**Exemplo 2.1.1** *O elemento* $\alpha = \frac{1}{2}(1 + \sqrt{5}) \in \mathbb{R}$ *é inteiro sobre* $\mathbb{Z}$, *pois é raiz do polinômio mônico* $x^2 - x - 1$ *com coeficientes em* $\mathbb{Z}$.

Se $R$ é o corpo dos números complexos e os coeficientes do polinômio mônico são números racionais, o elemento $\alpha$ é chamado *número algébrico*. Se os coeficientes do polinômio mônico são números inteiros, o elemento $\alpha$ é chamado *inteiro algébrico*.

**Exemplo 2.1.2**

1. *O elemento* $\alpha = e^{\frac{2\pi i}{5}} \in \mathbb{C}$ *é um inteiro algébrico, pois é raiz do polinômio mônico* $x^5 - 1$ *com coeficientes em* $\mathbb{Z}$.

2. *O elemento* $\alpha = \frac{22}{7} \in \mathbb{C}$ *é um número algébrico, pois é raiz do polinômio mônico* $x - \frac{22}{7}$ *com coeficientes em* $\mathbb{Q}$.

**Teorema 2.1.3** *[18, Teorema 1.1] Sejam* $A \subseteq R$ *anéis e* $\alpha$ *um elemento de* $R$. *As seguintes afirmações são equivalentes:*

1. $\alpha$ *é inteiro sobre* $A$.

2. *O anel* $A[\alpha]$ *é um* $A$*-módulo finitamente gerado.*

3. *Existe um subanel* $B$ *de* $R$ *contendo* $A$ *e* $\alpha$ *que é um* $A$*-módulo finitamente gerado.*

**Demonstração:** (1) $\Rightarrow$ (2) *Como* $\alpha$ *é inteiro segue que*

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

*onde* $a_0, a_1, \ldots, a_{n-1} \in A$ *e não são todos nulos. Seja* $M$ *o submódulo de* $R$ *gerado por* $\{1, \alpha, \ldots, \alpha^{n-1}\}$. *Temos que* $M \subseteq A[\alpha]$. *Por outro lado, temos que* $\alpha^n = -(a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0) \in M$ *e por indução segue que* $\alpha^{n+j} \in M$ *para todo* $j \geq 0$. *Assim* $A[\alpha] \subseteq M$ *e deste modo* $A[\alpha] = M$. *Portanto,* $A[\alpha]$ *é um* $A$*-módulo finitamente gerado.*
(2) $\Rightarrow$ (3) *Neste caso, é suficiente tomar* $B = A[\alpha]$.
(3) $\Rightarrow$ (1) *Seja* $\{\beta_1, \ldots, \beta_n\}$ *um conjunto finito de geradores de* $B$ *como um módulo sobre* $A$, *ou seja,* $B = A\beta_1 + \ldots + A\beta_n$. *Como* $\alpha \in B$ *e* $B$ *é um subanel de* $R$ *segue que* $\alpha\beta_i \in B$ *para todo* $i = 1, \ldots, n$. *Assim,* $\alpha\beta_i = \sum_{j=1}^{n} a_{i,j}\beta_j$, *com* $a_{i,j} \in A$ *para* $1 \leq i, j \leq n$. *Daí*

$$\alpha\beta_i - \sum_{j=1}^{n} a_{i,j}\beta_j = 0, \ e \qquad \sum_{j=1}^{n} (\alpha\frac{\beta_i}{\beta_j} - a_{i,j})\beta_j = 0.$$

*Tomando* $\frac{\beta_i}{\beta_j} = \delta_{i,j} = \begin{cases} 0 & se \quad i \neq j \\ 1 & se \quad i = j \end{cases}$, *temos que*

$$\sum_{j=1}^{n} (\alpha\delta_{i,j} - a_{i,j})\beta_j = 0, \ \textit{para } i = 1, \ldots, n.$$

*Assim, temos um sistema de n equações lineares homogêneas em* $\{\beta_1, \ldots, \beta_n\}$*, ou seja,*

$$\begin{cases} \sum_{j=1}^{n}(\alpha\delta_{1,j} - a_{1,j})\beta_j = 0 \\ \qquad\qquad \vdots \\ \sum_{j=1}^{n}(\alpha\delta_{n,j} - a_{n,j})\beta_j = 0 \end{cases}$$

*Escrevendo na forma matricial obtemos que*

$$\begin{pmatrix} \alpha\delta_{1,1} - a_{1,1} & \alpha\delta_{1,2} - a_{1,2} & \ldots & \alpha\delta_{1,n} - a_{1,n} \\ \alpha\delta_{2,1} - a_{2,1} & \alpha\delta_{2,2} - a_{2,2} & \ldots & \alpha\delta_{2,n} - a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha\delta_{n,1} - a_{n,1} & \alpha\delta_{n,2} - a_{n,2} & \ldots & \alpha\delta_{n,n} - a_{n,n} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

*Seja d o determinante* $det(\delta_{i,j}\alpha - a_{i,j})$*. Pela regra de Cramer temos que* $d\beta_j = 0$ *para todo* $j = 1, 2, \ldots, n$*. Como B é gerado por* $\{\beta_1, \ldots, \beta_n\}$*, segue que* $dB = 0$*, e em particular* $d1 = d = 0$*. Deste modo, temos que d é um polinômio mônico em* $\alpha$*, onde o termo com ordem máxima aparece na expansão do produto*

$$\prod_{i=1}^{n}(\delta_{i,i}\alpha - a_{i,i}) = \prod_{i=1}^{n}(\frac{\beta_i}{\beta_i}\alpha - a_{i,i}) = \prod_{i=1}^{n}(\alpha - a_{i,i})$$

*das entradas da diagonal principal. Portanto,* $\alpha$ *é raiz de um polinômio mônico com coeficientes em A, ou seja,* $\alpha$ *é inteiro sobre A.* ∎

**Proposição 2.1.1** *[18, Corolário 1.2] Sejam* $A \subseteq R$ *anéis e* $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$*. Se* $\alpha_1$ *é inteiro sobre A e* $\alpha_i$ *é inteiro sobre* $A[\alpha_1, \ldots, \alpha_{i-1}]$*, para* $i = 2, \ldots, n$*, então* $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *é um A-módulo finitamente gerado.*

**Demonstração:** *A prova será feita por indução sobre n. O caso* $n = 1$ *segue do item 2 do Teorema 2.1.3. Agora suponhamos que o resultado é verdadeiro para* $n - 1$*, ou seja, que* $B = A[\alpha_1, \ldots, \alpha_{n-1}]$ *é um A-módulo finitamente gerado. Logo, existe um conjunto finito* $\{\beta_1, \beta_2, \ldots, \beta_p\}$ *de geradores de B sobre A. Assim,* $B = \sum_{j=1}^{p} A\beta_j$*. Pelo item 2 do Teorema 2.1.3 obtemos que* $A[\alpha_1, \alpha_2, \ldots, \alpha_n] = B[\alpha_n]$ *é um B-módulo finitamente gerado, e assim possui um conjunto finito de geradores* $\{\gamma_1, \gamma_2, \ldots, \gamma_q\}$*. Deste modo, podemos escrever* $B[\alpha_n] = \sum_{k=1}^{q} B\gamma_k$*. Assim,*

$$A[\alpha_1, \alpha_2, \ldots, \alpha_n] = \sum_{k=1}^{q} B\gamma_k = \sum_{k=1}^{q}(\sum_{j=1}^{p} A\beta_j)\gamma_k = \sum_{j,k} A\beta_j\gamma_k,$$

*e deste modo* $(\beta_j\gamma_k)_{1\leq j\leq p, 1\leq k\leq q}$ *é um conjunto finito de geradores de* $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *como um* $A$*- módulo. Portanto,* $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *é um* $A$*-módulo finitamente gerado.* ■

**Corolário 2.1.1** *Sejam* $A \subseteq R$ *anéis. Se* $\alpha_1, \ldots, \alpha_n$ *são elementos de* $R$ *que são inteiros sobre* $A$*, então* $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ *é um* $A$*-módulo finitamente gerado.*
**Demonstração:** *Uma vez que se* $\alpha_i$ *é inteiro sobre* $A$ *então* $\alpha_i$ *é inteiro sobre* $A[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}]$*, para* $i = 1, 2, \ldots, n$*, o resultado segue pela Proposição 2.1.1.* ■

**Corolário 2.1.2** *[17, Corollary 1, p.29] Sejam* $A \subseteq R$ *anéis. Se* $\alpha$ *e* $\beta$ *são elementos de* $R$ *que são inteiros sobre* $A$*, então* $\alpha + \beta$*,* $\alpha - \beta$ *e* $\alpha\beta$ *são inteiros sobre* $A$*.*
**Demonstração:** *Como* $A[\alpha, \beta]$ *é um subanel de* $R$ *e* $\alpha, \beta \in A[\alpha, \beta]$ *segue que* $\alpha + \beta$*,* $\alpha - \beta$ *e* $\alpha\beta \in A[\alpha, \beta]$*. Pela Proposição 2.1.1, como* $\alpha$ *e* $\beta$ *são inteiros sobre* $A$*, segue que* $A[\alpha, \beta]$ *é um* $A$*-módulo finitamente gerado. Logo existe um subanel* $B = A[\alpha, \beta]$ *de* $R$ *contendo* $A, \alpha + \beta$*,* $\alpha - \beta$ *e* $\alpha\beta \in A[\alpha, \beta]$*. Assim, pelo item* 3 *do Teorema 2.1.3, segue que* $\alpha + \beta$*,* $\alpha - \beta$ *e* $\alpha\beta$ *são inteiros sobre* $A$*.* ■

Seja $A \subseteq R$ um anel. O conjunto dos elementos de $R$ que são inteiros sobre $A$ é chamado *anel dos inteiros* de $A$ em $R$ ou *fecho inteiro* de $A$ em $R$, denotado por $I_R(A)$, ou quando não houver confusão simplesmente por $I_R$.

**Corolário 2.1.3** *[18, Corolario 1.3] Se* $A \subseteq R$ *é um anel, então:*

1. *O conjunto* $I_R(A)$ *é um subanel de* $R$ *que contém* $A$*.*

2. *Todo subanel de* $R$ *que é um* $A$*-módulo finitamente gerado está contido em* $I_R(A)$*.*

**Demonstração:**

1. *Pelo Corolário 2.1.2 temos que* $I_R(A)$ *é um subanel de* $R$*. Como todo elemento de* $A$ *é inteiro sobre* $A$ *segue que* $I_R(A)$ *contém* $A$*.*

2. *Sejam* $B$ *um subanel de* $R$ *que é um* $A$*-módulo finitamente gerado e* $\{\alpha_1, \ldots, \alpha_n\}$ *um conjunto finito de geradores de* $B$*. Se* $\alpha \in B$*, então* $A[\alpha]$ *é finitamente gerado como* $A$*-módulo, pois* $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n$*, com* $a_i \in A$*. Assim pelo Teorema 2.1.3 segue que* $\alpha$ *é inteiro sobre* $A$*, ou seja,* $\alpha \in I_R(A)$*. Portanto* $B$ *está contido em* $I_R(A)$*.* ■

Seja $A \subseteq R$ um anel. Quando $I_R(A) = R$ dizemos que $R$ é *inteiro* sobre $A$.

**Proposição 2.1.2** *[17, Proposition 2, p.29] (Transitividade) Sejam $A \subseteq B \subseteq R$ anéis. Assim, $R$ é inteiro sobre $B$ e $B$ é inteiro sobre $A$, se, e somente se, $R$ é inteiro sobre $A$.*

**Demonstração:** *Suponhamos $R$ inteiro sobre $B$ e $B$ inteiro sobre $A$. Se $\alpha \in R$, então $\alpha$ é inteiro sobre $B$. Logo $\alpha$ é raiz de um polinômio mônico $f(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0$ com coeficientes em $B$. Tomando $B' = A[b_0, \ldots, b_{n-1}]$ temos que $\alpha$ é inteiro sobre $B'$. Como $B$ é inteiro sobre $A$, segue que os $b_i's$ são inteiros sobre $A$. Pela Proposição 2.1.1 segue que $B'[\alpha] = A[b_0, \ldots, b_{n-1}, \alpha]$ é um $A$-módulo finitamente gerado, e pelo Teorema 2.1.3 segue que $\alpha$ é inteiro sobre $A$. Portanto $R$ é inteiro sobre $A$. Reciprocamente, suponhamos que $R$ é inteiro sobre $A$. Se $\alpha \in R$, então $\alpha$ é raiz de um polinômio mônico com coeficientes em $A$, ou seja, $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ com $a_i \in A$ para todo $i = 1, \ldots, n-1$. Como $A \subseteq B$, segue que $a_i \in B$ para todo $i = 1, \ldots, n-1$, ou seja, $\alpha$ é inteiro sobre $B$. Assim $R$ é inteiro sobre $B$. Agora, se $\alpha \in B$ e como $B \subseteq R$ segue que $\alpha \in R$. Por hipótese, segue que $\alpha$ é inteiro sobre $A$. Portanto $B$ é inteiro sobre $A$.* ∎

### 2.1.3 Extensões de Corpos

Nesta subseção veremos o conceito de extensões de corpos e suas principais propriedades que serão utilizados no restante do trabalho.

Sejam $R$ um anel e $\mathbb{K}$ um corpo tal que $\mathbb{K} \subseteq R$. Um elemento $\alpha \in R$ é chamado *elemento algébrico* sobre $\mathbb{K}$ se for raiz de um polinômio com coeficientes em $\mathbb{K}$. Caso contrário, $\alpha$ é chamado *transcendente* sobre $\mathbb{K}$. Se $\alpha$ é algébrico sobre $\mathbb{K}$, então o polinômio mônico $m_\alpha(x)$ de grau mínimo tal que $m_\alpha(\alpha) = 0$ é chamado *polinômio minimal* de $\alpha$ sobre $\mathbb{K}$.

**Definição 2.1.3** *Um corpo $\mathbb{K}$ é chamado* algebricamente fechado *se qualquer polinômio em $\mathbb{K}[X]$ tem todas raízes em $\mathbb{K}$.*

Sejam $R$ um anel e $\mathbb{K}$ um corpo. O conjunto dos elementos de $R$ que são algébricos sobre $\mathbb{K}$ é chamado *fecho algébrico* de $\mathbb{K}$ em $R$ e denotado por $I_R(\mathbb{K})$.

**Exemplo 2.1.3** *O elemento $\alpha = \sqrt{7} - \sqrt{3}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio $x^4 - 20x^2 + 16$ com coeficientes em $\mathbb{Q}$.*

Sejam $R$ um anel e $\mathbb{K}$ um corpo tal que $\mathbb{K} \subseteq R$. Dizemos que $R$ é algébrico sobre $\mathbb{K}$ se todo elemento de $R$ é algébrico sobre $\mathbb{K}$. Se $R$ é um corpo, $R$ é chamado uma *extensão algébrica* de $\mathbb{K}$.

**Observação 2.1.1** *Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos.*

1. *O fecho algébrico de* $\mathbb{K}$ *em* $\mathbb{L}$ *é igual a* $\mathbb{L}$ *se, e somente se,* $\mathbb{L}$ *é uma extensão algébrica sobre* $\mathbb{K}$.

2. *Todo elemento algébrico sobre* $\mathbb{K}$ *é um elemento inteiro sobre* $\mathbb{K}$. *Em particular, sobre corpos, elementos algébricos e inteiros são equivalentes.*

Dada $\mathbb{L} : \mathbb{K}$ uma extensão de corpos, $\mathbb{L}$ tem uma estrutura natural como um espaço vetorial sobre $\mathbb{K}$, onde a adição vetorial é a adição em $\mathbb{L}$ e a multiplicação por escalar de $\lambda \in \mathbb{K}$ sobre $v \in \mathbb{L}$, é $\lambda v \in \mathbb{L}$.

**Definição 2.1.4** *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos tal que* $\mathbb{K} \subseteq \mathbb{L}$. *A dimensão de* $\mathbb{L}$ *sobre* $\mathbb{K}$ *é chamada grau da extensão, ou grau de* $\mathbb{L}$ *sobre* $\mathbb{K}$, *e denotada por* $[\mathbb{L} : \mathbb{K}]$.

Assim podemos reescrever as equivalências do Teorema 2.1.3 para corpos da seguinte forma:

**Teorema 2.1.4** *[17, p.30] Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos tal que* $\mathbb{K} \subseteq \mathbb{L}$ *e* $\alpha$ *um elemento de* $\mathbb{L}$. *As seguintes afirmações são equivalentes:*

1. $\alpha$ *é algébrico sobre* $\mathbb{K}$.

2. $[\mathbb{K}[\alpha] : \mathbb{K}]$ *é finito.*

**Demonstração:** (1) $\Rightarrow$ (2) *Suponhamos que* $\alpha$ *é algébrico sobre* $\mathbb{K}$ *com polinômio minimal* $m_\alpha(x)$ *de grau* $n$. *Temos que* $\mathbb{K}(\alpha)$ *é um espaço vetorial sobre* $\mathbb{K}$ *gerado por* $\{1, \alpha, \ldots, \alpha^{n-1}\}$. *Observamos que* $\mathbb{K}(\alpha)$ *é fechado sobre a adição, subtração e multiplicação por* $\alpha$. *Como* $\alpha^n = -m_\alpha(\alpha) + \alpha^n = g(\alpha)$, *onde* $\partial(g) < n$, *segue que* $\mathbb{K}(\alpha)$ *é fechado sobre a multiplicação e, assim,* $\mathbb{K}(\alpha)$ *é um anel. Finalmente, mostramos que se* $v \in \mathbb{K}(\alpha)$, $v \neq 0$, *então* $\frac{1}{v} \in \mathbb{K}(\alpha)$. *Temos que* $v = h(\alpha)$, *onde* $h(x) \in \mathbb{K}[x]$ *e* $\partial(h) < n$. *Como* $m_\alpha(x)$ *é irredutível segue que* $m_\alpha(x)$ *e* $h(x)$ *são coprimos. Assim, existem* $p(x), q(x) \in \mathbb{K}[x]$ *tal que* $m_\alpha p(x) + h(x)q(x) = 1$. *Logo,* $1 = m_\alpha(\alpha)p(\alpha) + h(\alpha)q(\alpha) = h(\alpha)q(\alpha)$. *Assim,* $q(\alpha) = \frac{1}{v} \in \mathbb{K}(\alpha)$ *e* $[\mathbb{K}(\alpha) : \mathbb{K}] = n$. *Portanto,* $[\mathbb{K}(\alpha) : \mathbb{K}]$ *é finita.*
(2) $\Rightarrow$ (1) *Se* $[\mathbb{K}(\alpha) : \mathbb{K}] = n$, *então* $\{1, \alpha, \ldots, \alpha^n\}$ *é linearmente dependente. Logo existem* $a_0, a_1, \ldots, a_n \in \mathbb{K}$, *não todos nulos, tais que* $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$ *e daí temos que* $\alpha$ *é algébrico sobre* $\mathbb{K}$. ∎

**Corolário 2.1.4** *[17, p.31] Toda extensão finita é algébrica.*
**Demonstração:** *Sejam* $\mathbb{L}$ *e* $\mathbb{K}$ *corpos tal que* $\mathbb{K} \subseteq \mathbb{L}$, $[\mathbb{L} : \mathbb{K}] = m < \infty$ *e* $\alpha \in \mathbb{L}$. *Como* $\mathbb{K}[\alpha]$ *é um subespaço de* $\mathbb{L}$ *segue que* $[\mathbb{K}(\alpha) : \mathbb{K}] = n \leq m < \infty$. *Pelo Teorema 2.1.4 segue que* $\alpha$ *é algébrico sobre* $\mathbb{K}$. *Assim,* $\mathbb{L}$ *é uma extensão algébrica.* ∎

**Teorema 2.1.5** *[17, Proposition 1, p.31] (Multiplicidade dos Graus) Sejam $\mathbb{K}$, $\mathbb{L}$ e $\mathbb{M}$ corpos. Se $\mathbb{M}$ é uma extensão algébrica finita de $\mathbb{L}$ e $\mathbb{L}$ é uma extensão algébrica finita de $\mathbb{K}$, então $\mathbb{M}$ é uma extensão algébrica finita de $\mathbb{K}$ e $[\mathbb{M}:\mathbb{K}] = [\mathbb{M}:\mathbb{L}][\mathbb{L}:\mathbb{K}]$.*

**Demonstração:** *Sejam $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ uma base de $\mathbb{M}$ sobre $\mathbb{L}$ e $\{\beta_1, \beta_2, \ldots, \beta_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Verifiquemos que $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_n\}$ é uma base de $\mathbb{M}$ sobre $\mathbb{K}$. Se $\alpha \in \mathbb{M}$, então $\alpha = a_1\beta_1 + a_2\beta_2 + \ldots + a_n\beta_n$, onde $a_j \in \mathbb{L}$, para $j = 1, 2, \ldots, n$. Agora, como cada $a_j \in \mathbb{L}$, segue que podemos escrevê-lo como $a_j = b_1\alpha_1 + b_2\alpha_2 + \ldots + b_m\alpha_m$, onde $b_i \in \mathbb{K}$, para $i = 1, 2, \ldots, m$. Assim, $\alpha = \sum_{j=1}^{n} a_j\beta_j = \sum_{i,j} b_{i,j}\alpha_i\beta_j$, onde $b_{i,j} \in \mathbb{K}$. Logo, $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_n\}$ gera $\mathbb{M}$ sobre $\mathbb{K}$. Da relação $\sum_{i,j} b_{i,j}\alpha_i\beta_j = 0$, temos que $\sum_{j=1}^{n}(\sum_{i=1}^{m} b_{i,j}\alpha_i)\beta_j = 0$. Como $\{\beta_1, \beta_2, \ldots, \beta_n\}$ é linearmente independente, segue que $\sum_{i=1}^{m} b_{i,j}\alpha_i = 0$ e, novamente, como $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ é linearmente independente segue que $b_{i,j} = 0$ para todo $i = 1, 2, \ldots, m$ e $j = 1, 2, \ldots, n$. Assim, $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_n\}$ é linearmente independente. Portanto é uma base de $\mathbb{M}$ sobre $\mathbb{K}$. Além disso, temos que $[\mathbb{M}:\mathbb{K}] = [\mathbb{M}:\mathbb{L}][\mathbb{L}:\mathbb{K}]$.* ■

Seja $\mathbb{K}$ um corpo. Dizemos que $\mathbb{K}$ tem *característica* $m$ se $m\alpha = 0$ para todo elemento $\alpha \in \mathbb{K}$, e $m$ é o menor inteiro positivo com esta propriedade. Se $m\alpha \neq 0$ para todo elemento não nulo $\alpha$ e inteiro positivo $m$, dizemos que $\mathbb{K}$ tem característica zero.

**Observação 2.1.2** *Todo corpo possui um único subcorpo minimal, chamado subcorpo primo, e este é isomorfo a $\mathbb{Q}$ ou a $\mathbb{Z}_p$, onde $p$ é primo. Se é isomorfo a $\mathbb{Q}$ o corpo tem característica zero e se é isomorfo a $\mathbb{Z}_p$ o corpo tem característica $p$.*

**Definição 2.1.5** *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{Q}$. Se o grau de $\mathbb{L}$ sobre $\mathbb{Q}$ é finito, dizemos que $\mathbb{L}$ é um corpo de números.*

Seja $\mathbb{K}$ um corpo de números, então existem vários monomorfismos distintos $\sigma_i$ de $\mathbb{K}$ em $\mathbb{C}$. Por exemplo, se $\mathbb{K} = \mathbb{Q}(i)$, onde $i = \sqrt{-1}$, então temos as possibilidades

$$\sigma_1(a + bi) = a + bi,$$

$$\sigma_2(a + bi) = a - bi,$$

para $a, b \in \mathbb{Q}$.

**Teorema 2.1.6** *[19, Theorem 2.3,p.41] Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau $n$ sobre $\mathbb{Q}$. Então existem exatamente $n$ distintos monomorfismos $\sigma_i$ de $\mathbb{K}$ em $\mathbb{C}$.*

**Demonstração:** *Sejam $\theta_1, \theta_2, \ldots, \theta_n$ raízes do polinômio minimal $m$ de $\theta$, então cada $\theta_i$ também tem o mesmo polinômio minimal $m$ e segue que existe um único isomorfismo $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ tal que $\sigma_i(\theta) = \theta_i$. De fato, se $\alpha \in \mathbb{Q}(\theta)$ então $\alpha = r(\theta)$ para um único $r \in \mathbb{Q}[x]$ com grau menor que $n$, e devemos ter $\sigma_i(\alpha) = r(\theta_i)$.*

*Reciprocamente, se $\sigma : \mathbb{K} \to \mathbb{C}$ é um monomorfismo então $\sigma$ é a identidade sobre $\mathbb{Q}$. Então temos*

$$0 = \sigma(m(\theta)) = m(\sigma(\theta))$$

*tal que $\sigma(\theta)$ é um dos $\theta_i$, daí $\sigma$ é um dos $\sigma_i$.* ■

### 2.1.4 Corpos Quadráticos

Nesta subseção apresentamos os corpos quadráticos e suas principais propriedades enfocando o anel dos inteiros desses corpos.

Um *corpo quadrático* é uma extensão de grau 2 sobre o corpo $\mathbb{Q}$ dos números racionais.

**Proposição 2.1.3** *[19, Proposition 3.1,p.67] Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde $d$ é um inteiro livre de quadrados.*

**Demonstração:** *Se $\mathbb{K}$ é um corpo quadrático, então todo elemento $\alpha \in \mathbb{K}$ tal que $\alpha \notin \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$. Pelo Teorema do Elemento Primitivo temos que $\mathbb{K} = \mathbb{Q}(\alpha)$. Tomando o polinômio minimal de $\alpha$ sobre $\mathbb{K}$, $m_\alpha(x) = x^2 + bx + c$, e resolvendo a equação quadrática $\alpha^2 + b\alpha + c = 0$, obtemos que $2\alpha = -b \pm \sqrt{b^2 - 4c}$. Portanto, $\mathbb{K} = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2 - 4c})$. Observando que $b^2 - 4c$ é um número racional da forma $\frac{u}{v} = \frac{uv}{v^2}$, com $u, v \in \mathbb{Z}$, temos que $\mathbb{Q}(\sqrt{b^2 - 4c}) = \mathbb{Q}(\sqrt{uv})$. Assim, como $uv \in \mathbb{Z}$, segue que $uv$ é fatorado em produtos de primos. Portanto, $\mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{d})$, onde $d$ é inteiro livre de quadrados.* ■

**Observação 2.1.3**

1. *Pela Proposição 2.1.3, temos que todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde $d$ é um inteiro livre de quadrados. Portanto, $\{1, \sqrt{d}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$.*

2. *O elemento $\sqrt{d} \in \mathbb{K}$ é uma raiz do polinômio irredutível $x^2 - d$, e seu conjugado é $-\sqrt{d}$. Assim, existe um automorfismo $\sigma$ tal que $\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$ é dado por $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$.*

**Lema 2.1.1** *[17, p.35] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde $d$ é um inteiro livre de quadrados. Se $\alpha = a + b\sqrt{d}$ é um inteiro algébrico, então $2a$ e $2b$ são números inteiros.*

**Demonstração:** *Pelo item* 2 *da Observação* 2.1.3*, temos que existe um automorfismo* $\sigma$ *tal que* $\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$ *é dado por* $\sigma(\alpha) = \sigma(a+b\sqrt{d}) = a - b\sqrt{d}$*. Como* $\sigma(\alpha)$ *também é raiz da mesma equação de* $\alpha$*, segue que* $\sigma(\alpha) \in I_{\mathbb{K}}(\mathbb{Z})$*. Como* $\alpha$ *e* $\sigma(\alpha) \in I_{\mathbb{K}}(\mathbb{Z})$*, pelo Corolário* 2.1.2*, segue que* $\alpha + \sigma(\alpha) \in I_{\mathbb{K}}(\mathbb{Z})$ *e* $\alpha\sigma(\alpha) \in I_{\mathbb{K}}(\mathbb{Z})$*. Além disso,* $\alpha + \sigma(\alpha) = (a+b\sqrt{d}) + (a-b\sqrt{d}) = 2a \in \mathbb{Q}$ *e* $\alpha\sigma(\alpha) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}$*. Como* $\mathbb{Z}$ *é um anel de ideais principais, segue que* $\mathbb{Z}$ *é algebricamente fechado e, portanto,* $2a \in \mathbb{Z}$ *e* $a^2 - db^2 \in \mathbb{Z}$*. Assim, temos que* $(2a)^2 - d(2b)^2 \in \mathbb{Z}$*, e como* $2a \in \mathbb{Z}$*, segue que* $(2a)^2 \in \mathbb{Z}$*. Por outro lado, se* $2b \notin \mathbb{Z}$*, o seu denominador teria um fator primo* $p$ *e este fator apareceria como* $p^2$ *no denominador de* $d(2b)^2$*. Sendo* $d$ *livre de quadrados, segue que* $d(2b)^2 \notin \mathbb{Z}$*, o que é um absurdo. Portanto,* $2b \in \mathbb{Z}$*.* ■

**Teorema 2.1.7** *[19, Theorem 3.2,p.67] Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *um corpo quadrático, onde* $d \in \mathbb{Z}$ *é livre de quadrados, ou seja,* $d \not\equiv 0(\text{modulo } 4)$*. Se* $d \not\equiv 1(\text{modulo } 4)$*, então o anel dos inteiros* $I_{\mathbb{K}}$ *é* $\mathbb{Z}[\sqrt{d}]$ *e* $\{1, \sqrt{d}\}$ *é uma base de* $\mathbb{Z}[\sqrt{d}]$ *como um* $\mathbb{Z}$*-módulo.*

**Demonstração:** *Seja* $\alpha = a + b\sqrt{d}$ *com* $a, b \in \mathbb{Q}$ *um inteiro algébrico sobre* $\mathbb{Z}$*. Pelo Lema 2.1.1 temos que* $a = \frac{u}{2}, b = \frac{v}{2}$*, com* $u, v \in \mathbb{Z}$*, e* $a^2 - db^2 \in \mathbb{Z}$*. Substituindo* $a$ *e* $b$ *por* $\frac{u}{2}$ *e* $\frac{v}{2}$*, respectivamente, temos que* $u^2 - dv^2 \in 4\mathbb{Z}$*. Se* $d \not\equiv 1(\text{modulo } 4)$*, então* $d \equiv 2(\text{modulo } 4)$ *ou* $d \equiv 3(\text{modulo } 4)$*. Assim,* $u$ *e* $v$ *são pares. Se por absurdo,* $v$ *fosse ímpar, então* $v^2 \equiv 1(\text{modulo } 4)$*. Como* $u^2 - dv^2 \in 4\mathbb{Z}$ *segue que* $u^2 - d(4k+1) \in 4\mathbb{Z}$ *o que implica que* $u^2 - d \in 4\mathbb{Z}$*. Assim,* $u^2 \equiv d(\text{modulo } 4)$*. Portanto,* $d \equiv 1(\text{modulo } 4)$ *ou* $d \equiv 0(\text{modulo } 4)$*, o que é um absurdo por hipótese. Assim, sendo* $v$ *par, temos que* $v^2 \equiv 0(\text{modulo } 4)$ *e deste modo* $u^2 \in 4\mathbb{Z}$*. Portanto,* $u$ *também é par. Assim,* $u$ *e* $v$ *são pares. Logo,* $a, b \in \mathbb{Z}$ *e* $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$*. Portanto,* $I_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}]$*. Por outro lado, tomando* $\alpha \in \mathbb{Z}[\sqrt{d}]$*, temos que* $\alpha$ *é raiz do polinômio* $x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$*. Assim,* $\mathbb{Z}[\sqrt{d}] \subset I_{\mathbb{K}}$*, e portanto,* $\mathbb{Z}[\sqrt{d}] = I_{\mathbb{K}}$*.* ■

**Teorema 2.1.8** *[19, Theorem 3.2,p.67] Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *um corpo quadrático, onde* $d \in \mathbb{Z}$ *é livre de quadrados, ou seja,* $d \not\equiv 0(\text{modulo } 4)$*. Se* $d \equiv 1(\text{modulo } 4)$*, então o anel dos inteiros* $I_{\mathbb{K}}$ *é* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *e* $\{1, \frac{1+\sqrt{d}}{2}\}$ *é uma base de* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *como um* $\mathbb{Z}$*-módulo.*

**Demonstração:** *Se* $d \equiv 1(\text{modulo } 4)$*, então* $u, v$ *tem a mesma paridade. Assim, se* $u$ *e* $v$ *são pares temos que* $a, b \in \mathbb{Z}$*, e que* $\alpha = a + b\sqrt{d} = \frac{u}{2} + \frac{v}{2}\sqrt{d} = \frac{u-v}{2} + \frac{v}{2}(1+\sqrt{d}) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$*. Se* $u$ *e* $v$ *são ímpares, então* $\alpha = \frac{u}{2} + \frac{v\sqrt{d}}{2} = \frac{u-v}{2} + \frac{v}{2}(1+\sqrt{d}) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$*. Portanto, temos que* $I_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$*. Por outro lado, se* $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *com* $a, b \in \mathbb{Z}$*, então temos que* $\alpha$ *é raiz do polinômio* $x^2 - (2a+b)x + \left(a^2 + ab - \frac{(1-d)b^2}{4}\right) \in \mathbb{Z}[x]$*,*

*pois* $d \equiv 1(\textit{modulo } 4)$. *Assim, segue que* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset I_{\mathbb{K}}$. *Portanto,* $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = I_{\mathbb{K}}$. ■

### 2.1.5 Norma e Traço de um Elemento

Nesta subseção veremos os conceitos de norma e traço de um elemento e suas principais propriedades que serão úteis para o desenvolvimento das propriedades do anel dos inteiros de um corpo.

Sejam $\mathbb{K}$ um corpo de números de grau $n$ e $\sigma_1, \sigma_2, ..., \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Para qualquer $\alpha \in \mathbb{K}$ definimos a *norma*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

e o *traço*

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Como os $\sigma_i's$ são monomorfismos segue que

$$N(\alpha\beta) = N(\alpha)N(\beta),$$

para quaisquer $\alpha, \beta \in \mathbb{K}$. Ainda, se $\alpha \neq 0$, $N(\alpha) \neq 0$ e se $a, b \in \mathbb{Q}$, então

$$T(a\alpha + b\beta) = aT(\alpha) + bT(\beta).$$

**Exemplo 2.1.4** *Dado* $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, *pelo Teorema 2.1.7 temos que o anel dos inteiros é* $\mathbb{Z}[\sqrt{2}]$. *Os monomorfismos* $\sigma_i's$ *são dados por* $\sigma_1(a+b\sqrt{2}) = a+b\sqrt{2}$ *e* $\sigma_2(a+b\sqrt{2}) = a-b\sqrt{2}$. *Assim, a norma e o traço são dados, respectivamente, por*

$$N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2,$$

*e*

$$T(a + b\sqrt{2}) = (a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a.$$

### 2.1.6 Decomposição em Irredutíveis

Nesta subseção veremos a teoria de decomposição prima em $\mathbb{Z}$ para um domínio integral $D$ e em particular para o anel dos inteiros de um corpo de números. Veremos que a norma de um elemento é uma ferramenta conveniente para detectarmos unidades e elementos irredutíveis, o que nos será muito útil nas próximas seções.

Um elemento $\alpha$ em um anel $R$ é chamado uma *unidade* se existe $\beta \in R$ tal que $\alpha\beta = 1$. Se $u$ é uma unidade em $R$, então qualquer elemento $\alpha \in R$ pode ser fatorado como

$$\alpha = u\beta,$$

onde $\beta = u^{-1}\alpha$. Um elemento $\beta$ é chamado um *associado* de $\alpha$ se $\alpha = u\beta$ para uma unidade $u$.

**Proposição 2.1.4** *[19, Proposition 4.1,p.82] As unidades $U(R)$ de um anel $R$ formam um grupo sobre a multiplicação.*

**Exemplo 2.1.5**

1. *Dado $R = \mathbb{Q}$. O grupo das unidades é dado por $U(\mathbb{Q}) = \mathbb{Q}^*$, que é um grupo infinito.*

2. *Dado $R = \mathbb{Z}$. O grupo das unidades é dado por $U(\mathbb{Z}) = \{1, -1\}$, que é um grupo cíclico de ordem 2.*

3. *Dado $R = \mathbb{Z}[i]$ o anel dos inteiros Gaussianos. Os elementos de $\mathbb{Z}[i]$ são da forma $a + bi$, onde $a, b \in \mathbb{Z}$. Assim, $a + bi$ é uma unidade se, e somente se, existe um elemento $c + di \in \mathbb{Z}[i]$ tal que*

   $$(a + bi)(c + di) = 1.$$

   *Multiplicando obtemos $(ac-bd)+(ad+bc)i = 1$, logo devemos ter $ac-bd = 1$ e $ad+bc = 0$. Isto tem solução inteira apenas quando $a^2 + b^2 = 1$, então $a = \pm 1$, $b = 0$ ou $a = 0$ e $b = \pm 1$. Portanto, o grupo das unidades é dado por $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$, que é um grupo cíclico de ordem 4.*

Usando normas podemos estender os resultados do Exemplo 2.1.5 para um caso mais geral de anéis dos inteiros de um corpo quadrático.

**Proposição 2.1.5** *[19, Proposition 4.2,p.82] O grupo das unidades $U$ dos inteiros em um corpo quadrático $\mathbb{Q}(\sqrt{d})$, onde $d < 0$ é um inteiro livre de quadrados, é dado por:*

1. *$U = \{\pm 1, \pm i\}$ para $d = -1$;*

2. *$U = \{\pm 1, \pm\omega, \pm\omega^2\}$ para $d = -3$;*

3. *$U = \{\pm 1\}$ para todos os outros $d < 0$.*

**Demonstração:** *Suponhamos que $\alpha$ é uma unidade no anel dos inteiros de $\mathbb{Q}(\sqrt{d})$ com inverso $\beta$. Logo, $\alpha\beta = 1$ e tomando normas $N(\alpha)N(\beta) = 1$. Como $N(\alpha)$, $N(\beta)$ são inteiros racionais, temos que $N(\alpha) = \pm 1$. Escrevendo $\alpha = a + b\sqrt{d}$, onde $a, b \in \mathbb{Q}$, temos que*

$$N(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 > 0$$

*pois estamos tomando $d < 0$. Assim, $N(\alpha) = a^2 - db^2 = +1$. Agora, se $a, b \in \mathbb{Z}$ e $d = -1$, temos $a^2 + b^2 = 1$, que tem soluções $a = \pm 1$, $b = 0$ ou $a = 0$ e $b = \pm 1$, como encontrado no Exemplo 2.1.5, assim obtemos o item 1. Para $d < -3$ imediatamente concluimos que $b = 0$, pois caso contrário $a^2 - db^2$ excederia 1, então as únicas soluções são $a = \pm 1$, $b = 0$. Se $d \not\equiv 1$(modulo 4), então $a, b \in \mathbb{Z}$, logo as únicas soluções são as apresentadas. Para $d \equiv 1$(modulo 4), entretanto, devemos também considerar a possibilidade adicional $a = A/2$, $b = B/2$ onde ambos $A$ e $B$ são inteiros racionais ímpares. Neste caso, $A^2 - dB^2 = 4$. Para $d < -3$, temos $B = 0$, logo $A = 2$ e obtemos $a = 1$, e não existe solução adicional. Isto completa o item 3. Para $d = -3$, encontramos as soluções adicionais $A = \pm 1, B = \pm 1$. Do caso $A = 1$, $B = 1$ temos que*

$$\alpha = \frac{1}{2}(-1 + \sqrt{-3}) = e^{2\pi i/3}$$

*que denotamos por $\omega$ e nos outros três casos obtemos $-\omega, \omega^2$ e $-\omega^2$. Isto somado as soluções encontradas nos fornece o item 2.* ■

Veremos a seguir algumas propriedades das unidades, tais como elementos associados e irredutíveis.

**Proposição 2.1.6** *[19, Proposition 4.3,p.84] Em um domínio $D$,*

1. *$\alpha$ é uma unidade se, e somente se, $\alpha|1$;*
2. *Quaisquer duas unidades são associados, e qualquer associado de uma unidade é uma unidade;*
3. *$\alpha, \beta$ são associados se, e somente se, $\alpha|\beta$ e $\beta|\alpha$;*
4. *$\alpha$ é irredutível se, e somente, se todo divisor de $\alpha$ é um associado de $\alpha$ ou uma unidade;*
5. *um associado de um irredutível é irredutível.*

**Demonstração:** *Os itens $1, 2, 4$ e $5$ seguem da definição. Provaremos apenas o item 3 que requer a lei do cancelamento. Suponhamos que $\alpha|\beta$ e $\beta|\alpha$, então existem $a, b \in D$ tais que $\beta = a\alpha$ e $\alpha = b\beta$. Logo,*

$$\alpha = ba\alpha.$$

*Assim, ou $\alpha = 0$ e segue $\beta = 0$ e, portanto, eles são associados, ou $\alpha \neq 0$, e cancelando $\alpha$ obtemos*

$$1 = ba,$$

*então $a$ e $b$ são unidades. Portanto, $\alpha$ e $\beta$ são associados. A recíproca é imediata.* ■

Podemos estender algumas destas idéias em termos de ideais.

**Proposição 2.1.7** *[19, Proposition 4.4,p.84] Seja $D$ um domínio e $\alpha, \beta$ elementos não nulos de $D$. Então,*

1. *$\alpha|\beta$ se, e somente se, $\langle\alpha\rangle \supseteq \langle\beta\rangle$;*
2. *$\alpha$ e $\beta$ são associados se, e somente se, $\langle\alpha\rangle = \langle\beta\rangle$;*
3. *$\alpha$ é uma unidade se, e somente se, $\langle\alpha\rangle = D$;*
4. *$\alpha$ é irredutível se, e somente se, $\langle\alpha\rangle$ é maximal dentre os ideais principais de $D$.*

**Demonstração:**

1. *Se $\alpha|\beta$, então $\beta = \gamma\alpha \in \langle\alpha\rangle$ para algum $\gamma \in D$, logo $\langle\beta\rangle \subseteq \langle\alpha\rangle$. Reciprocamente, se $\langle\beta\rangle \subseteq \langle\alpha\rangle$, então $\beta = \gamma\alpha$ para algum $\gamma \in D$.*
2. *imediato de* 1.
3. *Se $\alpha$ é uma unidade, então $\alpha\eta = 1$ para algum $\eta \in D$, logo para qualquer $\beta \in D$ temos $\beta = \alpha\eta\beta \in \langle\alpha\rangle$ e $D = \langle\alpha\rangle$. Se $D = \langle\alpha\rangle$ então como $1 \in D$, $1 = \gamma\beta$ para algum $\gamma \in D$ e $\alpha$ é uma unidade.*
4. *Suponhamos $\alpha$ é irredutível, com $\langle\alpha\rangle \subsetneqq \langle\beta\rangle \subsetneqq D$. Então $\beta|\alpha$ mas não é uma unidade nem um associado de $\alpha$, contradizendo o item* 4 *da Proposição* 2.1.6*. Reciprocamente, se nenhum tal $\beta$ existe, então todo divisor de $\alpha$ é uma unidade ou um associado, então $\alpha$ é irredutível.* ■

Em um domínio $D$, se uma não unidade $\alpha$ é *redutível*, podemos escrevê-la como $\alpha = \beta\gamma$. Se $\beta$ ou $\gamma$ é redutível podemos expressá-lo novamente como um produto de fatores. Seguindo este processo escrevemos

$$\alpha = p_1 p_2 \dots p_m,$$

onde cada $p_i$ é irredutível. Dizemos que a decomposição em irredutíveis em $D$ é possível se todo $\alpha \in D$, não unidade e não nulo, pode ser escrito como o produto de um número finito de irredutíveis.

**Teorema 2.1.9** *[19, Theorem 4.6,p.87] Se um domínio $D$ é Noetheriano, então a decomposição em irredutíveis em $D$ é possível.*

**Demonstração:** *Suponhamos que $D$ é Noetheriano, mas existe uma não unidade $\alpha \neq 0$ em $D$ que não pode ser escrita como um produto de um número finito de irredutíveis. Escolha $\alpha$ tal que $\langle\alpha\rangle$ é maximal com estas condições sobre $\alpha$, que é possível pela maximalidade. Por esta definição, este $\alpha$ não pode ser irredutível, então $\alpha = \beta\gamma$, onde $\beta$ e $\gamma$ não são unidades. Assim, pelo item* 1 *da Proposição* 2.1.7 *segue que $\langle\beta\rangle \supseteq \langle\gamma\rangle$. Agora, se $\langle\beta\rangle = \langle\gamma\rangle$, então pelo item* 2 *da Proposição* 2.1.7*, $\beta$ e $\gamma$ são associados e este não é o caso pois isto implica que $\gamma$ é uma unidade. Assim, $\langle\beta\rangle \supsetneqq \langle\gamma\rangle$, e analogamente $\langle\gamma\rangle \supsetneqq \langle\gamma\rangle$. Pela maximalidade de $\langle\alpha\rangle$ devemos ter*

$$\beta = p_1 \dots p_r,$$

$$\gamma = q_1 \dots q_s,$$

*onde cada $p_i$ e $q_i$ são irredutíveis. Multiplicando $\beta$ e $\gamma$ escrevemos $\alpha$ como um produto de irredutíveis, o que é uma contradição. Portanto, a afirmação que existe uma não unidade diferente de zero é falsa, e a decomposição em irredutíveis é sempre possível.* ∎

**Teorema 2.1.10** *[19, Theorem 4.7,p.87] O anel dos inteiros $I_{\mathbb{K}}$ em um corpo de números $\mathbb{K}$ é Noetheriano.*

**Demonstração:** *Vamos provar que todo ideal $\mathcal{I}$ de $I_{\mathbb{K}}$ é finitamente gerado. Agora, $(I_{\mathbb{K}}, +)$ é abeliano livre de posto $n$ igual ao grau de $\mathbb{K}$. Daí $(\mathcal{I}, +)$ é abeliano livre de posto $r \leq n$ pelo Teorema 2.1.2. Se $\alpha_1, \dots, \alpha_r$ é uma $\mathbb{Z}$-base para $(\mathcal{I}, +)$, então claramente $\langle\alpha_1, \dots, \alpha_r\rangle = I$. Logo $\mathcal{I}$ é finitamente gerado e $I_{\mathbb{K}}$ é Noetheriano.* ∎

**Corolário 2.1.5** *[19, Corollary 4.8,p.88] Decomposição em irredutíveis é possível em $I_{\mathbb{K}}$.*

Através da norma podemos identificar se um dado elemento é irredutível, como veremos a seguir.

**Proposição 2.1.8** *[19, Proposition 4.9,p.88] Seja $\mathbb{K}$ um corpo de números e $I_{\mathbb{K}}$ o anel dos inteiros. Dados $\alpha, \beta \in I_{\mathbb{K}}$ temos:*

1. *$\alpha$ é uma unidade se, e somente se, $N(\alpha) = \pm 1$;*
2. *Se $\alpha$ e $\beta$ são associados, então $N(\alpha) = \pm N(\beta)$;*
3. *Se $N(\alpha)$ é um primo racional, então $\alpha$ é irredutível em $I_{\mathbb{K}}$.*

**Demonstração:**

1. *Se* $\alpha u = 1$, *então* $N(\alpha)N(u) = 1$. *Como* $N(\alpha), N(u) \in \mathbb{Z}$, *temos* $N(\alpha) = \pm 1$. *Reciprocamente, se* $N(\alpha) = \pm 1$, *então*

$$\sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha) = \pm 1,$$

*onde os* $\sigma_i's$ *são os monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$. *Além disso, sem perda de generalidade,* $\sigma_1(\alpha)$ *é igual a* $\alpha$ *e todos os outros* $\sigma_i's$ *são inteiros. Tomando*

$$u = \pm\sigma_2(\alpha)\ldots\sigma_n(\alpha),$$

*então* $\alpha u = 1$, *logo* $u = \alpha^{-1} \in \mathbb{K}$. *Portanto,* $u \in I_{\mathbb{K}}$ *e* $\alpha$ *é uma unidade.*

2. *Se* $\alpha, \beta$ *são associados, então* $\alpha = u\beta$, *onde* $u$ *é uma unidade. Assim, pelo item* (1)

$$N(\alpha) = N(u\beta) = N(u)N(\beta) = \pm N(\beta).$$

3. *Se* $\alpha = \beta\gamma$, *então* $N(\alpha) = N(\beta)N(\gamma)$. *Como por hipótese* $N(\alpha) = p$ *primo racional, segue que* $N(\beta)N(\gamma) = p$, *e então* $N(\beta)$ *ou* $N(\gamma)$ *é* $\pm p$ *e a outra é* $\pm 1$. *Assim, pelo item* (1), $\beta$ *ou* $\gamma$ *é uma unidade, e segue que* $\alpha$ *é irredutível.*

### 2.1.7 Norma de um Ideal

Nesta subseção apresentamos o conceito de norma de um ideal do anel dos inteiros de um corpo de números e suas principais propriedades que serão úteis para o cálculo da cardinalidade dos anéis quocientes sob os quais os códigos serão construídos.

Sejam $\mathbb{K}$ um corpo de números, $I_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathcal{I}$ um ideal de $I_{\mathbb{K}}$. A *norma do ideal* $\mathcal{I}$ é definida como sendo a cardinalidade do anel quociente $\frac{I_{\mathbb{K}}}{\mathcal{I}}$, ou seja,

$$N(\mathcal{I}) = card\left(\frac{I_{\mathbb{K}}}{\mathcal{I}}\right).$$

**Exemplo 2.1.6** *Seja* $\mathcal{I}$ *um ideal principal de* $\mathbb{Z}[i]$, *onde* $i^2 = -1$, *gerado por* $2 - i$. *Assim,* $\frac{\mathbb{Z}[i]}{\mathcal{I}} = \{x + \mathcal{I};\, x \in \mathbb{Z}[i]\}$. *A norma de* $\mathcal{I}$ *é o número das classes laterais de* $\mathcal{I}$. *Uma vez que* $2 - i \equiv 0 (mod\, \mathcal{I})$, *segue que* $2 \equiv i (mod\, \mathcal{I})$. *Assim, para* $x = a + bi$, *com* $a, b \in \mathbb{Z}$, *temos que* $x = a + bi \equiv a + 2b (mod\, \mathcal{I})$. *Como* $(2 + i)(2 - i) = 5 \in \mathcal{I}$, *segue que as classes laterais de* $\mathcal{I}$ *em* $\mathbb{Z}[i]$ *são* $\{0, 1, 2, -1, -2\}$, *ou seja,* $N(\mathcal{I}) = 5$.

Agora, dado um corpo de números $\mathbb{K}$, e $I_{\mathbb{K}}\alpha = \langle\alpha\rangle$ o ideal de $I_{\mathbb{K}}$ gerado por $\alpha$, então temos o seguinte resultado.

**Proposição 2.1.9** *[17, Proposition 1, p.52] Seja* $0 \neq \alpha \in I_{\mathbb{K}}$. *Então*

$$|N(\alpha)| = card\left(\frac{I_{\mathbb{K}}}{I_{\mathbb{K}}\alpha}\right),$$

*ou seja, o anel quociente* $\frac{I_{\mathbb{K}}}{I_{\mathbb{K}}\alpha}$ *possui* $|N(\alpha)|$ *elementos.*

**Proposição 2.1.10** *[20, Proposição 1.7.2]* $N(\mathcal{I})$ *é finita.*

**Demonstração:** *Se* $\alpha \in \mathcal{I}$ *é um elemento não nulo, então* $I_{\mathbb{K}}\alpha \subset \mathcal{I}$. *Além disso, podemos escrever* $I_{\mathbb{K}}/\mathcal{I}$ *como um quociente de* $I_{\mathbb{K}}/I_{\mathbb{K}}\alpha$. *Assim,*

$$card\left(\frac{I_{\mathbb{K}}(\mathbb{Z})}{I_{\mathbb{K}}(\mathbb{Z})\alpha}\right) = card\left(\frac{I_{\mathbb{K}}(\mathbb{Z})}{\mathcal{I}}\right) card\left(\frac{\mathcal{I}}{I_{\mathbb{K}}(\mathbb{Z})\alpha}\right)$$

*Mas pela Proposição* 2.1.9 *temos que* $card\left(\frac{I_{\mathbb{K}}}{I_{\mathbb{K}}\alpha}\right)$ *é finita. Portanto,* $card\left(\frac{I_{\mathbb{K}}}{\mathcal{I}}\right)$ *é finita.* ∎

### 2.1.8 Formas Quadráticas

Nesta subseção consideraremos as formas quadráticas, que como exemplo temos a norma de um elemento, na qual estamos interessados e será utilizada nos próximos capítulos.

**Definição 2.1.6** *Uma forma quadrática* ($n$*-ária*) *sobre um corpo* $\mathbb{K}$ *é um polinômio* $f$ *homogêneo de grau* 2 *com* $n$ *variáveis sobre* $\mathbb{K}$, *tendo a seguinte forma geral*

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j \in \mathbb{K}[x_1, \ldots, x_n]. \tag{2.2}$$

Para obter os coeficientes simétricos é usual reescrevermos $f$ como

$$f(x) = \sum_{i,j=1}(a_{ij} + a_{ji})x_ix_j = \sum_{i,j=1} a_{ij}^{'}x_ix_j, \tag{2.3}$$

onde $a_{ij}^{'} = \frac{1}{2}(a_{ij} + a_{ji})$. Desta forma, $f$ determina unicamente uma matriz simétrica $(a_{ij}^{'})$, que podemos denotar por $M_f$. Em termos de notação matricial, temos

$$f(X) = (x_1, \ldots, x_n).M_f.\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = X^t.M_f.X,$$

onde $X$ é visto como um vetor coluna e $X^t$ denota a transposta de $X$.

Isto nos permite denotar $f(x_1, \ldots, x_n)$ por $f(v)$, para $v = (x_1, \ldots, x_n)$. Tomando $v = \sum_{i,j=1}^{n} x_ie_i$ e $w = \sum_{i,j=1}^{n} y_ie_i$, com $x_i$, $y_i \in \mathbb{K}$, para todo $i = 1, \ldots, n$ e a aplicação $B_f : V \times V \longrightarrow \mathbb{K}$ definida por

$$B_f(v, w) = \frac{1}{2}[f(v + w) - f(v) - f(w)]. \tag{2.4}$$

Desenvolvendo a equação (2.4) podemos observar que $B_f$ é uma aplicação bilinear. Portanto, associada a uma forma quadrática $f$ existe uma aplicação bilinear $B_f$ dada pela equação (2.4).

Por outro lado, considerando $\{e_1, \ldots, e_n\}$ uma base de $V$ e uma aplicação bilinear como a da equação (2.4), para um vetor não nulo $u = \sum_{i=1}^{n} a_i e_i$ temos que

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

Logo, da equação (2.3) segue que

$$f_B(a_1, \ldots, a_n) = f(u) = B(u,u).$$

Isto mostra que existe uma correspondência biunívoca entre formas quadráticas e aplicações bilineares.

**Definição 2.1.7** *O par constituído pelo espaço vetorial $V$ e a aplicação bilinear $B$ é chamado espaço quadrático.*

### 2.1.9 Reticulados

Nesta subseção apresentamos o conceito de reticulados, enfocando suas principais propriedades.

Sejam $\mathbb{K}$ um corpo, $R \subseteq \mathbb{K}$ um anel, $V$ um espaço vetorial de dimensão finita $n$ sobre $\mathbb{K}$ e $\{v_1, \ldots, v_m\}$ vetores de $V$ linearmente independentes sobre $\mathbb{K}$, com $m \leq n$. O conjunto dos elementos de $V$ da forma

$$\left\{ x = \sum_{i=1}^{m} a_i v_i, \text{ com } a_i \in R \right\},$$

é chamado *reticulado* com base $\beta = \{v_1, \ldots, v_m\}$ e será denotado por $\Lambda_\beta$.

A seguir estaremos considerando em $\mathbb{R}^n$ apenas os $\mathbb{Z}$-reticulados.

**Definição 2.1.8** *Seja $\beta = \{v_1, \ldots, v_n\}$ uma $\mathbb{Z}$-base do reticulado $\Lambda_\beta \subset \mathbb{R}^n$. O conjunto*

$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n : x = \sum_{i=1}^{n} \lambda_i v_i,\ 0 \leq \lambda_i < 1 \right\},$$

*é chamado região fundamental de $\Lambda_\beta$.*

**Exemplo 2.1.7** *Temos que $\Lambda_\beta = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $v_1 = (1,0)$ e $v_2 = (0,1)$ com região fundamental descrita na Figura* 2.1.

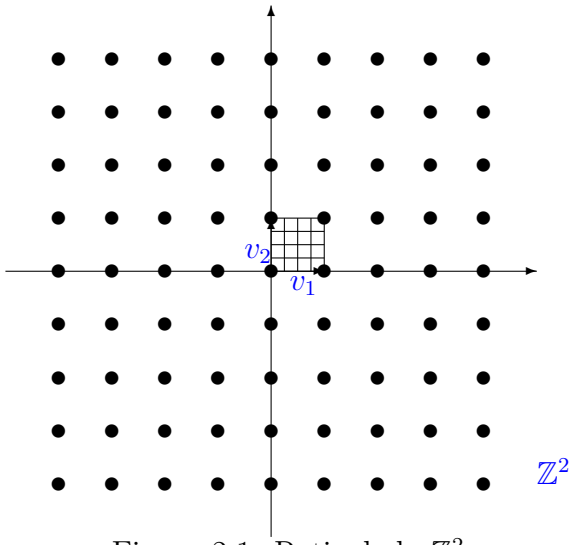


Figura 2.1: Reticulado $\mathbb{Z}^2$

**Exemplo 2.1.8** *Temos que* $\Lambda_\beta = \{(a,b) \in \mathbb{Z}^2;\, a+b \equiv 0 (mod\, 2)\}$ *é um reticulado gerado pelos vetores* $v_1 = (2,0)$ *e* $v_2 = (1,1)$ *com região fundamental descrita na Figura* 2.2.

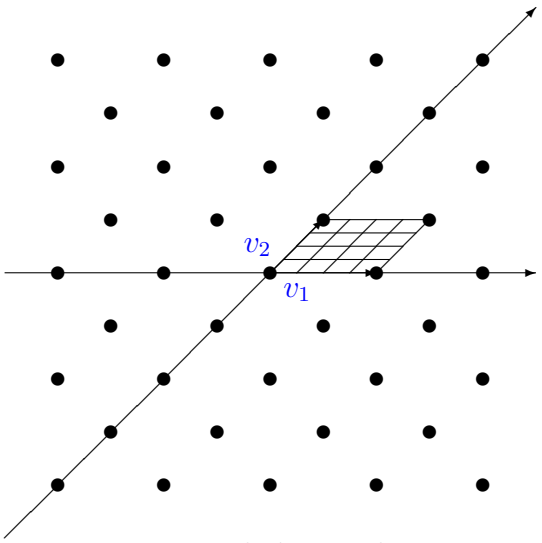


Figura 2.2: Reticulado gerado por $v_1$ e $v_2$

**Observação 2.1.4** *Seja* $\Lambda_\beta$ *um reticulado do* $\mathbb{R}^n$ *com base* $\beta = \{v_1, \ldots, v_n\}$. *Se* $c_1, \ldots, c_n$ *são elementos quaisquer de* $\Lambda_\beta$, *então* $c_i = \sum_{j=1}^{n} a_{ij} v_j$, *com* $a_{ij} \in \mathbb{Z}$. *Assim, temos que* $\{c_1, \ldots, c_n\}$ *é uma base de* $\Lambda_\beta$ *se, e somente se,* $\det(a_{ij})$ *é um elemento inversível de* $\mathbb{Z}$.

**Definição 2.1.9** *Um subconjunto do* $\mathbb{R}^n$ *é dito discreto se a intersecção com qualquer bola de centro zero e raio* $r$ *é um conjunto finito.*

**Exemplo 2.1.9** *Temos que* $\mathbb{Z}^n$ *é um subconjunto discreto do* $\mathbb{R}^n$.

**Lema 2.1.2** *[20, Lema 2.6.1] O conjunto dos pontos de um reticulado* $\Lambda$ *no* $\mathbb{R}^n$ *é discreto.*

**Demonstração:** *Seja* $\{v_1, \ldots, v_n\}$ *uma base do reticulado* $\Lambda$. *Temos que as condições* $\langle x, v_2 \rangle =$

$0, \ldots, \langle x, v_n \rangle = 0$ *fornecem um sistema linear com* $n-1$ *equações lineares homogêneas e* $n$ *incógnitas. Como este sistema tem uma solução não nula, segue que existe um vetor* $x$ *ortogonal aos vetores* $v_2, \ldots, v_n$. *Se* $\langle x, v_1 \rangle = 0$, *então o vetor* $x$ *seria ortogonal a todos os vetores do* $\mathbb{R}^n$, *o que é impossível. Assim,* $\langle x, v_1 \rangle \neq 0$. *O vetor* $s_1 = [1/\langle x, v_1 \rangle]/x$ *também é ortogonal a todos os vetores* $v_2, \ldots, v_n$, *e* $\langle s_1, v_1 \rangle = 1$. *Deste modo, para todo* $1 \leq i \leq n$, *podemos escolher um vetor* $s_i$ *tal que* $\langle s_i, v_i \rangle = 1$ *e* $\langle s_j, v_i \rangle \neq 1$, *para* $i \neq j$. *Agora, suponhamos, que o vetor* $z = a_1 z_1 + \ldots + a_n z_n$ *de* $\Lambda$, *com* $a_i \in \mathbb{Z}, i = 1, 2 \ldots, n$, *pertence a uma bola de raio* $r$. *Como* $a_k = \langle z, s_k \rangle$, *pela inequação de Cauchy-Schwartz, segue que*

$$||a_k|| = ||\langle z, s_k \rangle|| \leq ||z||||s_k|| < r||s_k||,$$

*onde* $r||s_k||$ *não depende de* $z$. *Portanto, existe um número finito de possibilidades para* $a_k$ *e o conjunto de todos os* $z \in \Lambda$ *tal que* $||z|| < r$ *é finito.* ■

O próximo teorema diz que um reticulado é gerado sobre $\mathbb{Z}$ por uma base do $\mathbb{R}^n$, ou seja, por uma $\mathbb{Z}$-base do reticulado dado.

**Teorema 2.1.11** *[17, Theorem 1, p.53] Se* $\Lambda$ *é um subgrupo discreto do* $\mathbb{R}^n$, *então* $\Lambda$ *é gerado como um* $\mathbb{Z}$*-módulo por* $r$ *vetores linearmente independentes sobre* $\mathbb{R}$, *com* $r \leq n$.

**Demonstração:** *Sejam* $\beta = \{v_1, \ldots, v_r\}$ *um conjunto de vetores de* $\Lambda$ *que são linearmente independentes sobre* $\mathbb{R}$, *onde* $r$ *é o maior possível com* $r \leq n$, *e*

$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n : \, x = \sum_{i=1}^{r} \alpha_i v_i, \, 0 \leq \alpha_i \leq 1 \right\},$$

*o paralelepípedo construído a partir destes vetores. Temos que* $\mathcal{P}_\beta$ *é fechado e limitado, logo* $\mathcal{P}_\beta$ *é compacto. Agora, como* $\Lambda$ *é discreto, segue que* $\mathcal{P}_\beta \cap \Lambda$ *é finito. Tomando* $x \in \Lambda$, *pela maximalidade de* $r$, *segue que* $\{x, v_1, \ldots, v_r\}$ *é linearmente dependente. Assim, existem* $\lambda_i \in \mathbb{R}$, $i = 1, \ldots, r$, *não todos nulos, tal que* $x = \sum_{i=1}^{r} \lambda_i v_i$. *Para cada* $j \in \mathbb{N}$, *seja*

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] v_i \, \in \, \Lambda, \tag{2.5}$$

*onde* $[k]$ *denota o maior inteiro menor ou igual a* $k$. *Assim,*

$$x_j = j \sum_{i=1}^{r} \lambda_i v_i - \sum_{i=1}^{r} [j\lambda_i] v_i = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) v_i \in \mathcal{P}_v \cap \Lambda.$$

*Deste modo, tomando* $j = 1$ *na Equação (2.5) obtemos que*

$$x_1 = x - \sum_{i=1}^{r} [\lambda_i] v_i, \;\; \textit{ou seja,} \;\; x = x_1 + \sum_{i=1}^{r} [\lambda_i] v_i.$$

*Assim, como $x_1 \in \mathcal{P}_v \cap \Lambda$ e este é finito, segue que $\Lambda$ é finitamente gerado como um $\mathbb{Z}$-módulo. Por outro lado, do fato de $\mathcal{P}_v \cap \Lambda$ ser finito e $\mathbb{N}$ ser infinito, existem inteiros $j$ e $k$, tais que $x_j = x_k$. Da Equação (2.5), segue que* $x_j = x_k \Longrightarrow jx - \sum_{i=1}^{r}[j\lambda_i]v_i = kx - \sum_{i=1}^{r}[k\lambda_i]v_i \Longrightarrow (j-k)x = \sum_{i=1}^{r}([j\lambda_i] - [k\lambda_i])v_i \Longrightarrow (j-k)\sum_{i=1}^{r}\lambda_i v_i = \sum_{i=1}^{r}([j\lambda_i] - [k\lambda_i])v_i \Longrightarrow (j-k)\lambda_i = [j\lambda_i] - [k\lambda_i] \Longrightarrow \lambda_i = \dfrac{[j\lambda_i] - [k\lambda_i]}{(j-k)}$, *ou seja, $\lambda_i \in \mathbb{Q}$. Assim, $\Lambda$ é gerado como um $\mathbb{Z}$-módulo por um número finito de elementos, que são combinações lineares com coeficientes racionais dos $v_i's$. Seja $d \neq 0$ um denominador comum destes coeficientes. Consideremos o conjunto $d\Lambda$. Temos que $d\Lambda \subset \sum_{i=1}^{r}\mathbb{Z}v_i$. Daí, pelo Teorema* 2.1.2, *segue que existe uma base $\{s_1, \ldots, s_r\}$ do $\mathbb{Z}$-módulo $\sum_{i=1}^{r}\mathbb{Z}v_i$ e inteiros $\alpha_i$, tal que $\{\alpha_1 s_1, \ldots, \alpha_r s_r\}$ gera $d\Lambda$ sobre $\mathbb{Z}$. Como o $\mathbb{Z}$-módulo $d\Lambda$ tem o mesmo posto de $\Lambda$ e como $\sum_{i=1}^{r}\mathbb{Z}v_i \subset \Lambda$, segue que o posto de $d\Lambda \geq r$. Pela maximalidade de $r$ decorre que o posto de $d\Lambda$ é $r$ e os $\alpha_i's$ são não nulos, pois caso contrário $d\Lambda$ não teria posto $r$. Assim os $s_i's$ são linearmente independentes sobre $\mathbb{R}$, uma vez que $\{v_1, \ldots, v_r\}$ é linearmente independente sobre $\mathbb{R}$. Portanto, $d\Lambda$ é gerado por $r$ vetores linearmente independentes sobre $\mathbb{R}$ e, consequentemente, $\Lambda$ também é gerado por $r$ vetores linearmente independentes sobre $\mathbb{R}$.* ■

**Observação 2.1.5** *[19, Theorem 6.1, p.142] Segue do Teorema* 2.1.11 *que um subgrupo aditivo discreto do $\mathbb{R}^n$ é um reticulado em $\mathbb{R}^n$.*

### 2.1.10 Empacotamento Esférico

Nesta subseção apresentamos os conceitos de empacotamento esférico, densidade de empacotamento e densidade de centro, relacionando-os e enfocando as principais propriedades.

**Definição 2.1.10** *Um empacotamento esférico, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

Um problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço euclidiano $n$-dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Isto pode ser visto como a versão euclidiana do 18º Problema de Hilbert, proposto em 1900.

A Teoria dos Códigos Corretores de Erros nasceu em 1948, com o famoso trabalho de Shannon, onde foi demonstrado o Teorema da Capacidade do Canal. Em linhas gerais, este resultado diz que para a transmissão de dados abaixo de uma certa taxa $C$ (símbolos por segundo), chamada de capacidade do canal, é possível obter a probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

A prova do Teorema da Capacidade do Canal implica que no caso de valores altos da relação sinal-ruído (SNR), um código de bloco ótimo para um canal com ruído gaussiano branco (AWGN), limitado em faixa consiste em um empacotamento denso de sinais dentro de uma esfera, no espaço euclidiano $n$-dimensional, para $n$ suficientemente grande. Assim, se estabeleceu o vínculo entre empacotamento esférico e Teoria da Informação.

Para cada $n$, Minkowski provou a existência de reticulados no espaço euclidiano $n$-dimensional com densidade de empacotamento esférico $\Delta$ satisfazendo

$$\Delta \geq \frac{\zeta(n)}{2^{n-1}},$$

onde $\zeta$ é a função zeta de Riemann. Como consequência, obtêm-se

$$\frac{1}{n} log_2 \Delta \geq -1. \tag{2.6}$$

Em [41] Leech e Sloane estabeleceram as primeiras relações entre empacotamento de esferas e os códigos corretores de erro, e desenvolveram a "construção código"de muitos reticulados conhecidos. A busca de empacotamentos densos como métodos de modulação codificada teve sucesso com o trabalho de Forney et al. [42] em 1984, no qual sistemas de modulação codificada em bloco foram construídos usando-se reticulados densos nas dimensões 4, 8, 16 e 24, com ganhos de codificação em torno de 1.5, 3.0, 4.5, e 6.0 dB, respectivamente; e em [43] Conway e Sloane provaram que reticulados satisfazendo a cota de Minkowski, dada pela Equação (2.6) são equivalentes a códigos atingindo a capacidade do canal.

Dentre os métodos de geração de reticulados, o homomorfismo de Minkowski apresenta características interessantes. Usando a Teoria Algébrica dos Números, Craig [44] reproduziu o reticulado de Leech $\Lambda_{24}$ através da representação geométrica de um ideal do anel dos inteiros de $\mathbb{Q}(\zeta_{39})$. Com o mesmo método, ainda obteve a família $A_n^m$ em dimensões $n = p - 1$, através de $\mathbb{Q}(\zeta_p)$, onde $p$ é um número primo.

Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis. Lembramos que os reticulados de maior interesse são aqueles com maior densidade de empacotamento.

Para que possamos prosseguir no estudo de reticulados, precisamos da noção de volume. O volume no $\mathbb{R}^n$ é bem conhecido e pode ser facilmente transferido para o $\mathbb{R}$-espaço $V$ através do isomorfismo natural entre $\mathbb{R}^n$ e $V$, e definido por meio de uma base $\{v_1, \ldots, v_n\}$. Além disso, é possível restringir a subconjuntos $C$ de $V$ que são reuniões finitas da região fundamental, usando apenas as seguintes propriedades de volume.

1. $vol(x + C) = vol(C)$, para todo $x \in V$.

2. $vol(\gamma C) = \gamma^n vol(C)$, para todo $\gamma \in \mathbb{R},\ \gamma > 0$.

3. Se $C \cap C' = \emptyset$, então $vol(C \cup C') = vol(C) + vol(C')$.

4. Sejam $\{v_1, \ldots, v_n\}$ uma base de um reticulado $\Lambda \subseteq \mathbb{R}^n$ e $\mathcal{P}_v$ a sua região fundamental. Se $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, para $i = 1, 2, \ldots, n$, então o volume da região fundamental $\mathcal{P}_v$, denotado por $vol(\mathcal{P}_v)$, é dado por

$$vol(\mathcal{P}_v) = |det(B)|,$$

onde

$$B = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}.$$

**Proposição 2.1.11** *[17, Lemma 1, p.55] O volume de uma região fundamental independe da base do reticulado.*

**Demonstração:** *Seja $v = \{v_1, \ldots, v_n\}$ uma base de um reticulado $\Lambda \subseteq \mathbb{R}^n$. Se $s = \{s_1, \ldots, s_n\}$ é uma outra base de $\Lambda$, então, $s_i = \sum_{j=1}^{n} \alpha_{ij} v_j$, com $\alpha_{ij} \in \mathbb{Z}$. Assim,*

$$vol(\mathcal{P}_s) = |\det(\alpha_{ij})| vol(\mathcal{P}_v).$$

*Como a matriz de mudança de base $(\alpha_{ij})$ é inversível com entradas inteiras, segue que $\det(\alpha_{ij}) = \pm 1$. Portanto, $vol(\mathcal{P}_s) = vol(\mathcal{P}_v)$.* ∎

**Observação 2.1.6** *Sendo $\beta'$ uma outra base para $\Lambda_\beta$, segue que $vol(\Lambda_\beta) = vol(\Lambda_{\beta'})$, pois $\beta$ e $\beta'$ diferem pelo produto de uma matriz inversível com entradas inteiras. Deste modo, podemos definir o volume de $\Lambda_\beta$ como o volume de uma região fundamental.*

Seja $\beta = \{v_1, v_2, \ldots, v_n\}$ uma base de um reticulado $\Lambda \subseteq \mathbb{R}^n$. O *volume do reticulado* $\Lambda_\beta$ é definido por $vol(\Lambda_\beta) = vol(\mathcal{P}_v)$.

Um *empacotamento reticulado* é um empacotamento em que o conjunto dos centros das esferas formam um reticulado $\Lambda_\beta$ de $\mathbb{R}^n$.

**Exemplo 2.1.10** *Empacotamento do reticulado* $\Lambda_\beta = \mathbb{Z}^2$.

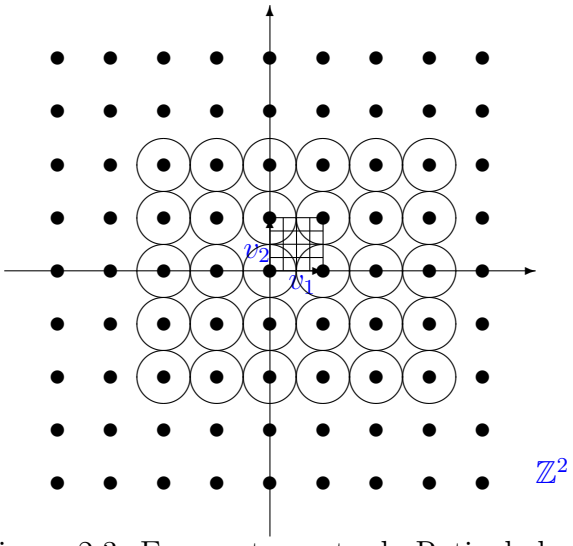


Figura 2.3: Empacotamento do Reticulado $\mathbb{Z}^2$

**Definição 2.1.11** *Dado um empacotamento no* $\mathbb{R}^n$, *associado a um reticulado* $\Lambda_\beta$, *com* $\beta = \{v_1, \ldots, v_n\}$ *uma* $\mathbb{Z}$*-base, definimos a sua densidade de empacotamento como a proporção do espaço* $\mathbb{R}^n$ *coberta pela união das esferas.*

Estamos interessados nos empacotamentos associados a um reticulado $\Lambda_\beta$ em que as esferas tenham raio máximo, onde consigamos cobrir a maior área possível. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado $\Lambda_\beta$ é um conjunto finito, de onde segue que o número $\Lambda_{\beta_m} = min\{|\lambda|; \lambda \in \Lambda_\beta, \lambda \neq 0\}$ está bem definido e $(\Lambda_{\beta_m})^2$ é chamado *norma mínima*. Observamos que $\rho = \Lambda_{\beta_m}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de $\Lambda_\beta$ e obter um empacotamento. Dessa forma, o estudo dos empacotamentos reticulados é equivalente ao estudo dos reticulados.

A densidade de empacotamento de um reticulado $\Lambda_\beta$ é definida por

$$\Delta(\Lambda_\beta) = \frac{\text{Volume de uma esfera de raio } \rho}{\text{Volume do reticulado}}.$$

Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio $\rho$, temos que o seu volume é dado por

$$vol(\mathcal{B}(\rho)) = vol(\mathcal{B}(1))\rho^n,$$

onde $vol(\mathcal{B}(1))$ é o volume de uma esfera de raio 1. Assim, a densidade de empacotamento é dada por

$$\Delta(\Lambda_\beta) = vol(\mathcal{B}(1))\frac{\rho^n}{vol(\Lambda_\beta)}.$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado *densidade de centro*, dado por

$$\delta(\Lambda_\beta) = \frac{\rho^n}{vol(\Lambda_\beta)}.$$

**Exemplo 2.1.11** *Seja $\Lambda_\beta = \mathbb{Z}^2$ um reticulado do $\mathbb{R}^2$ gerado pelos vetores $(1,0)$ e $(0,1)$. Temos que o raio de empacotamento é $\rho = 1/2$, e $vol(\mathcal{B}(1)) = \pi.1 = \pi$. Assim, o volume do reticulado é $vol(\Lambda_\beta) = 1$, a densidade de empacotamento é*

$$\Delta(\Lambda_\beta) = vol(\mathcal{B}(1)).\frac{\rho^2}{vol(\Lambda_\beta)} = \pi\frac{1}{4} = \frac{\pi}{4}$$

*e a densidade de centro é $\delta(\Lambda_\beta) = 1/4$.*

**Exemplo 2.1.12** *Seja $\Lambda_\beta = \mathbb{Z}^n$ um reticulado do $\mathbb{R}^n$, gerado pelos vetores $v_1 = (1,0,\ldots,0)$, $(0,1,\ldots,0),\ldots,v_n = (0,0,\ldots,1)$. A forma quadrática $|v|^2 = x_1^2 + \ldots + x_n^2$ assume o valor mínimo quando $x_i = 1$ para algum $i = 1,\ldots,n$, e os demais são nulos. Assim $|v|^2 = 1$ e $\rho = \frac{1}{2}$. Visto que $v(\Lambda_\beta) = |\det B|$, e $B$ neste caso é a matriz identidade, temos que o $vol(\Lambda_\beta) = 1$, e portanto, $\delta(\Lambda_\beta) = \frac{1}{2^n}$.*

Um dos problemas de empacotamento esférico de um reticulado $\Lambda_\beta$ do $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade. Em dimensão um, temos que os pontos de coordenadas inteiras da reta formam um reticulado cuja densidade de empacotamento é a melhor possível dada por $\Delta = 1$. Neste caso as "esferas" são intervalos como podemos ver na Figura 2.4.

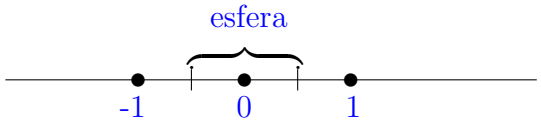

Figura 2.4: Empacotamento de esferas em dimensão 1

A resposta também é conhecida para dimensão dois, o reticulado hexagonal com base $\beta = \left\{(1,0),(-\frac{1}{2},\frac{\sqrt{3}}{2})\right\}$ e $\rho = \frac{1}{2}$ é o de maior densidade, dada por $\Delta = \frac{\pi}{\sqrt{12}} \approx 0,9069$. O empacotamento deste reticulado é ilustrado na Figura 2.5.

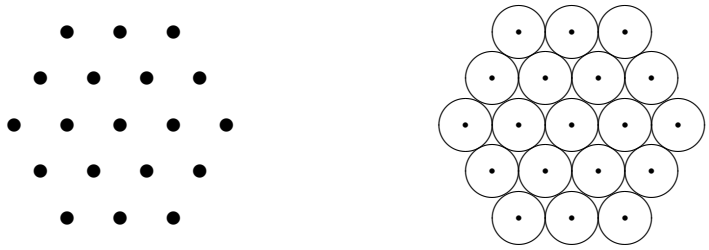

Figura 2.5: Empacotamento de esferas em dimensão 2

Em dimensão três *Gauss* sugeriu em 1831 que o reticulado denominado $face-centered-cubic$, denotado por $fcc$ (pilha de laranjas ou bala de canhões) é o empacotamento reticulado com maior densidade, sendo $\Delta = \frac{\pi}{\sqrt{18}} \approx 0,7405$.

O empacotamento reticulado mais denso no $R^4$ é o do reticulado denominado *checkerboard* $D_4$. Analogamente ao anterior, este reticulado consiste de todos os pontos $(x, y, z, w) \in \mathbb{R}^4$ tais que $x + y + z + w = 2k$, com $x, y, z, w, k \in \mathbb{Z}$. Os reticulados com maior densidade estão determinados até dimensão 8 [43]. Nas dimensões 2 e 3 já foi provado que os empacotamentos reticulados são os mais densos dentre todos os empacotamentos.

As definições e propriedades apresentadas até aqui para reticulados $\Lambda_\beta$ do $\mathbb{R}^n$, podem ser estendidas para $\Lambda_\beta$ em um espaço métrico $(\mathbb{E}, d)$. Nosso objetivo neste trabalho será construir códigos reticulados em dimensões 2 e 3 no $\mathbb{R}^n$ e em dimensões $n \geq 4$ no espaço hiperbólico.

### 2.1.11 Constelações de Sinais

Nesta subseção veremos alguns conceitos fundamentais para os objetivos do nosso trabalho, como constelações de sinais geometricamente uniformes e regiões de Voronoi.

**Definição 2.1.12** *Uma constelação de sinais $\mathcal{S}$ é um subconjunto finito de pontos em um espaço métrico $(\mathbb{E}, d)$. Os pontos da constelação são chamados de sinais.*

Seja $U(\mathcal{S})$ o grupo de simetrias de $\mathcal{S}$ em $\mathbb{E}$. Uma constelação de sinais é dita *geometricamente uniforme* se para quaisquer sinais $s_0, s_1 \in \mathcal{S}$, existe uma isometria $T \in U(\mathcal{S})$, tal que $T(s_0) = s_1$, ou seja, $U(\mathcal{S})$ age transitivamente em $\mathcal{S}$. Equivalentemente,

$$U(s_0) = \{T(s_0) : T \in U(\mathcal{S})\} = \mathcal{S}.$$

**Definição 2.1.13** *Sejam $\mathcal{S}$ uma constelação de sinais e $s_0 \in \mathcal{S}$. A região de Voronoi de $s_0$ em $\mathcal{S}$ consiste dos pontos que estão mais próximos de $s_0$ que de qualquer outro ponto de $\mathcal{S}$, ou seja,*

$$\mathcal{V}_\mathcal{S}(s_0) = \{s \in \mathbb{E} : d(s, s_0) \leq d(s, r), \forall r \in \mathcal{S}, s \neq s_0\}.$$

O *perfil de distância global* com relação a $s_0$, denotado por $PD(s_0)$, é dado pelo conjunto das distâncias dos pontos de $\mathcal{S}$ com relação a $s$, ou seja,

$$PD(s_0) = \{d(s_0, s) : s \in \mathcal{S}\}.$$

No próximo teorema veremos a relação entre uma constelação de sinais geometricamente uniforme e regiões de Voronoi.

**Teorema 2.1.12** *[2] Seja $\mathcal{S}$ uma constelação de sinais. Se $\mathcal{S}$ é uniforme, então:*

1. *Todas as regiões de Voronoi são congruentes;*

2. *O perfil de distância global é o mesmo para qualquer sinal $s \in \mathcal{S}$.*

Uma constelação de sinais $\mathcal{S}$ está casada a um grupo $\mathcal{G}$, se existe uma aplicação sobrejetora $\eta : \mathcal{G} \to \mathcal{S}$ tal que

$$d(\eta(h_1), \eta(h_2)) = d(\eta(e), \eta(h_1^{-1}h_2)), \forall h_1, h_2 \in \mathcal{G},$$

onde $e$ é o elemento neutro de $\mathcal{G}$ e $d$ é uma distância em $\mathcal{S}$. A aplicação $\eta$ é uma *aplicação casada*. Além disso, se $\eta$ é injetora, então dizemos que $\eta^{-1}$ é um *rotulamento casado*. Nesse caso, dizemos que $\eta$ é um rotulamento isométrico.

Tanto no aspecto da geração de constelações, como na implementação prática, a construção de sinais que possuam boas propriedades geométricas e boas estruturas algébricas é fundamental e relevante. Assim, nosso trabalho será dedicado as constelações de sinais geometricamente uniformes.

## 2.2 Geometria Hiperbólica

Esta seção tem por objetivo a apresentação das principais definições e resultados da geometria hiperbólica, principalmente aqueles relacionados aos próximos capítulos. As referências aqui utilizadas são [26]-[31].

### 2.2.1 Notas Históricas

Nesta subseção apresentamos algumas notas históricas sobre o desenvolvimento da geometria hiperbólica.

Por mais de dois mil anos "Os Elementos"do matemático Euclides ($325ac - 265ac$), foi o texto padrão na geometria. No primeiro dos seus trinta conjunto de volumes sistematicamente

descobriu a geometria euclidiana introduzindo definições de termos geométricos (tais como reta e ponto), cinco noções comuns concentrando magnitudes, e os seguintes cinco postulados:

(i) Uma reta pode ser traçada de qualquer ponto a outro.

(ii) Qualquer segmento finito de reta pode ser prolongado indefinidamente para construir uma reta.

(iii) Dados um ponto e uma distância quaisquer, pode-se traçar um círculo de centro naquele ponto e raio igual à distância dada.

(iv) Todos os ângulos retos são iguais entre si.

(v) Se uma reta cortar duas outras retas de modo que a soma dos dois ângulos interiores, de um mesmo lado, seja menor que dois ângulos retos, então as duas outras retas se cruzam, quando suficientemente prolongadas, do lado da primeira reta em que se acham os dois ângulos.

Ao longo dos séculos foram encontrados diversos enunciados equivalentes ao $5^o$ postulado, sendo o mais popular deles feito por John Fairplay $(1748 - 1819)$ que afirma que, "Por um ponto não contido em uma reta dada, pode ser traçada uma e apenas uma reta paralela a reta dada", que ficou conhecido como Postulado das Paralelas.

Durante o século $XVIII$ diversos matemáticos tais como Girolomo Sacheri e Johann Heinrich Lambert tentaram demonstrar o $5^o$ postulado mas não foram bem sucedidos, já que este é um postulado independente, fato conhecido hoje em dia. Apesar disso, conseguiram avanços importantes, como provar por exemplo, que sem o Postulado das Paralelas, obtém-se que a soma dos ângulos internos de um triângulo pode ser maior ou menor do que $\pi$.

Na primeira metade do século $XIX$ começou-se a suspeitar da independência do Postulado das Paralelas. Matemáticos como Karl Friedrich Gauss $(1777-1855)$, János Bolyai $(1802-1860)$ e Nicolai Lobatchevsky $(1793-1856)$ trataram da questão ao considerar três situações distintas: Por um ponto não contido em uma reta dada passa, mais de uma, apenas uma ou nenhuma reta paralela à reta dada. Por suspeitarem da independência do Postulado das Paralelas, ou seja, de que sua negação poderia gerar uma geometria consistente, sem contradições, desenvolveram de forma axiomática um estudo amplo e detalhado de uma geometria que assumia a existência de mais de uma reta paralela (a terceira hipótese, da inexistência de retas paralelas pode ser descartada se assumirmos que as retas são infinitas), criando o que veio a ser chamada com o tempo de *Geometria de Lobatchevsky* ou *Geometria Hiperbólica*. No entanto, as dúvidas referentes à consistência desta nova geometria só foram dirimidas no final do século, quando matemáticos como Eugenio Beltrami, Henri Poincaré e Felix Klein criaram modelos euclidianos para esta geometria. A criação de modelos euclidianos para a geometria hiperbólica resolve a questão da consistência desta geometria, pois qualquer eventual contradição a ser encontrada implicaria

em uma contradição existente na geometria euclidiana, ou seja, as geometrias hiperbólica e euclidiana tem o mesmo grau de consistência.

Neste texto exploraremos apenas dois modelos para a geometria hiperbólica, conhecidos como *disco de Poincaré* e o *semi-plano de Lobatchevsky*. Os modelos exercem para a geometria a mesma função que um bom atlas exerce para a geografia: apesar de os mapas apresentarem distorções, estas são quantificáveis e razoavelmente "bem comportadas", de modo que podemos nos situar de forma bastante satisfatória apenas através de nossos mapas. Além disto, de forma análoga ao que acontece com os distintos mapas de um atlas, modelos distintos distorcem ou preservam propriedades distintas. Assim, dependendo da propriedade que desejamos estudar, podemos escolher o mapa mais conveniente.

### 2.2.2 Espaço Hiperbólico

Nesta subseção definiremos o espaço hiperbólico e alguns conceitos importantes como comprimento hiperbólico e distância hiperbólica entre dois pontos.

Consideremos o conjunto

$$\mathbb{H}^{n+1} = \{x_1, \ldots, x_{n+1} \in \mathbb{R}^{n+1} : x_{n+1} > 0\}$$

dotado da estrutura Riemanniana

$$ds^2 = \frac{dx_1^2 + \ldots + dx_{n+1}^2}{x_{n+1}^2} \tag{2.7}$$

Com essa estrutura, o semi-espaço $\mathbb{H}^{n+1}$ é chamado *espaço hiperbólico (n+1)-dimensional*, e a métrica $ds$ é chamada *métrica hiperbólica*.

A introdução desta estrutura Riemanniana nos permite definir comprimentos de curvas, geodésicas e distância entre pontos, que faremos a seguir.

Sejam $[a, b]$ um intervalo fechado e $\gamma : [a, b] \to \mathbb{H}^{n+1}$ uma curva continuamente diferenciável por partes, onde $\gamma(t) = (x_1(t), \ldots, x_{n+1}(t))$. O *comprimento* da curva $\gamma([a, b])$ denotado por $\|\gamma\|$, é dado por

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

Sem perda de generalidade, podemos assumir que a curva $\gamma$ está definida no intervalo $[0, 1]$. De fato, considerando a aplicação $\phi : [0, 1] \to [a, b]$ definida por $\phi(t) = a + (b - a)t$ e $\tilde{\gamma}(t) = (\gamma \circ \phi)(t) = \gamma(a + bt - at)$, obtemos pela regra da cadeia que

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

A seguir definimos a distância entre dois pontos.

**Definição 2.2.1** *Dados dois pontos $p$, $q \in \mathbb{H}^{n+1}$, a distância entre $p$ e $q$ é dada por*

$$d(p,q) = inf\|\gamma\|$$

*onde o ínfimo é considerado sobre o conjunto das curvas continuamente diferenciáveis por partes $\gamma : [0,1] \to \mathbb{H}^{n+1}$, com $\gamma(0) = p$ e $\gamma(1) = q$.*

Uma prova detalhada de que $d(.,.)$ é de fato uma distância pode ser vista em [26].

A partir da definição de distância definimos as geodésicas, que são curvas de menor comprimento entre dois pontos.

**Definição 2.2.2** *Uma curva $\gamma : [a,b] \to \mathbb{H}^{n+1}$ é chamada geodésica se para quaisquer $s,t \in [a,b]$ tivermos*

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

*ou seja, se $\gamma$ minimizar a distância entre os pontos de seu traçado.*

### 2.2.3 Modelos Euclidianos do Plano Hiperbólico

Existem várias formas distintas de se construir o plano hiperbólico. Nesta subseção veremos dois modelos euclidianos do plano hiperbólico, simples e convenientes, e algumas propriedades.

Consideremos o semi-plano superior $\mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) > 0\}$ com a métrica Riemanniana

$$ds = \frac{\sqrt{dx^2 + dy^2}}{y}, \tag{2.8}$$

onde $z = x + yIm$. Com esta métrica $\mathbb{H}^2$ é um modelo do plano hiperbólico chamado *plano de Lobachevski*.

**Observação 2.2.1** *O limitante euclidiano ou bordo de $\mathbb{H}^2$ é dado por $\partial_\infty \mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) = 0\} \cup \{\infty\}$.*

Podemos ainda determinar as geodésicas do plano hiperbólico.

**Teorema 2.2.1** *[26, Teorema 3.7, p.23] As geodédicas de $\mathbb{H}^2$ são as semi-retas e semi-circunferências ortogonais a $\partial_\infty \mathbb{H}^2$.*

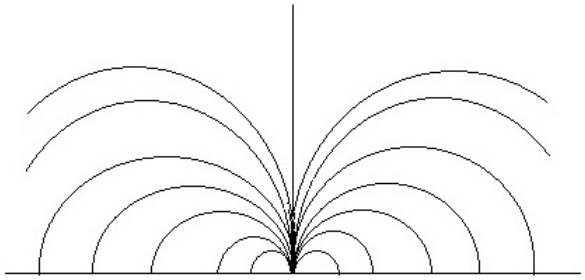

Figura 2.6: Geodésicas no plano de Lobatschevsky

Dado um conjunto $A \subset \mathbb{H}^2$, sua *área hiperbólica*, denotada por $\mu(A)$ é dada por

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

se a integral existir.

Um outro modelo euclidiano do plano hiperbólico é o disco unitário $\mathbb{D}^2 = \{z \in \mathbb{C} : |z| < 1\}$ com a métrica derivada da diferencial

$$ds = \frac{2|dz|}{1 - |z|^2} \tag{2.9}$$

e é chamado *modelo de Poincaré*.

**Observação 2.2.2** *O limitante euclidiano ou bordo de* $\mathbb{D}^2$ *é dado por* $\partial\mathbb{D}^2 = \{z \in \mathbb{C} : |z| = 1\}$.

Neste caso as geodésicas do plano hiperbólico são dadas pelo seguinte resultado.

**Teorema 2.2.2** *[26, Observação 3.12, p.27] As geodédicas de* $\mathbb{D}^2$ *são segmentos de retas ortogonais a* $\mathbb{D}^2$ *(pela origem) e de circunferências ortogonais a* $\partial\mathbb{D}^2$.

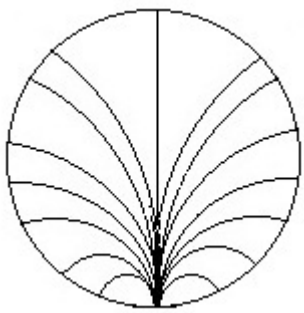

Figura 2.7: Geodésicas no plano de Poincaré

Dado um conjunto $A \subset \mathbb{D}^2$, sua área hiperbólica, denotada por $\mu(A)$ é dada por

$$\mu(A) = \int_A \frac{4dxdy}{(1-(x^2+y^2))^2},$$

se a integral existir.

Para determinarmos a área de um triângulo hiperbólico podemos usar o seguinte teorema que mostra que a área hiperbólica de um triângulo hiperbólico depende apenas de seus ângulos.

**Teorema 2.2.3** *Seja $\Delta$ um triângulo hiperbólico com ângulos $\alpha, \beta, \gamma$. Então a área de $\Delta$ é dada por*

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

A função $f : \mathbb{H}^2 \to \mathbb{D}^2$ dada por

$$f(z) = \frac{zIm + 1}{z + Im} \tag{2.10}$$

é uma bijeção e podemos verificar que é uma isometria. Isso nos permite trabalhar com o modelo mais adequado de acordo com a necessidade. Existem ainda outros dois modelos, à saber, de Klein e Minkowsky, que não serão considerados neste trabalho.

### 2.2.4 Grupos Fuchsianos

Nesta subseção vamos definir e caracterizar os grupos Fuchsianos, que são fundamentais para o desenvolvimento do nosso trabalho, visto que em [11] e [12] alguns destes grupos, que veremos no próximo capítulo, foram identificados em ordens dos quatérnios, as quais são a base para a construção dos códigos que iremos propor.

Seja $PSL(2,\mathbb{R})$ o conjunto de todas transformações de Möbius de $\mathbb{C}$ sobre ele mesmo da forma

$$\{z \to \frac{az+b}{cz+d} : a, b, c, d \in \mathbb{R},\ ad - bc = 1\}. \tag{2.11}$$

Consideremos um grupo de matrizes reais $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ com $det(g) = ad - bc = 1$, e $tr(g) = a + d$ o traço da matriz $g$. Este grupo é chamado *grupo unimodular* e é denotado por $SL(2,\mathbb{R})$.

O conjunto de transformações fracionárias lineares (transformações de Möbius) de $\mathbb{C}$ sobre ele mesmo da forma (2.11) forma um grupo tal que o produto de duas transformações corresponde ao produto das matrizes correspondentes e a inversa corresponde a matriz inversa.

Cada transformação $T$ é representada por um par de matrizes $\pm g \in SL(2,\mathbb{R})$. Assim, o grupo de todas transformações (2.11), chamado *grupo projetivo linear* $PSL(2,\mathbb{R})$, é isomorfo a $SL(2,\mathbb{R})/\{\pm I_2\}$, onde $I_2$ é a matriz identidade $2 \times 2$, ou seja

$$PSL(2,\mathbb{R}) \approx \frac{SL(2,\mathbb{R})}{\{\pm I_2\}}.$$

**Teorema 2.2.4** *[27, Theorem 1.1.1, p.3] $PSL(2,\mathbb{R})$ age sobre $\mathbb{H}^2$ por homeomorfismos.*

**Demonstração:** *Primeiro vamos mostrar que qualquer transformação do tipo* (2.11) *leva $\mathbb{H}^2$ sobre ele mesmo. Seja $T \in PSL(2,\mathbb{R})$, e $w = T(z) = \frac{az+b}{cz+d}$. Então*

$$w = \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} = \frac{ac|z|^2 + adz + bc\bar{z} + bd}{|cz+d|^2},$$

*é tal que*

$$Im(w) = \frac{w-\bar{w}}{2i} = \frac{z-\bar{z}}{2i|cz+d|^2} = \frac{Im(z)}{|cz+d|^2}. \tag{2.12}$$

*Assim, $Im(z) > 0$ implica que $Im(w) > 0$. O Teorema agora segue da continuidade de $T(z)$ e sua inversa.* ■

As transformações da forma da equação (2.11) em $PSL(2,\mathbb{R})$ podem ser classificadas quanto ao valor do módulo do traço da matriz associada em três tipos:

1. Elíptica, se $T(T) = |a+d| < 2$;
2. Parabólica, se $T(T) = |a+d| = 2$;
3. Hiperbólica, se $T(T) = |a+d| > 2$.

**Teorema 2.2.5** *[26, Teorema 5.3, p.50] Toda transformação $T_A \in PSL(2,\mathbb{R})$, $T_A \neq I_2$, possui uma matriz $B \in SL(2,\mathbb{R})$ associada, tal que $T_B \circ T_A \circ T_{B^{-1}}$ é associada a uma das matrizes*

$$\begin{pmatrix} cos(\theta) & sen(\theta) \\ -sen(\theta) & cos(\theta) \end{pmatrix}, \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} ou \begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix} \tag{2.13}$$

*onde $0 \leq \theta \leq 2\pi$, $t \in \mathbb{R}^*$ e $\lambda \in \mathbb{R}^* - \{1\}$.*

Portanto, a menos de conjugação, podemos assumir que a matriz $A$ associada a transformação $T_A$ seja uma das matrizes como na equação (2.13), conforme $A$ seja elíptica, parabólica ou hiperbólica, respectivamente.

Temos ainda o seguinte resultado.

**Teorema 2.2.6** *[27, Theorem 1.2.4, p.5] Qualquer transformação em $PSL(2,\mathbb{R})$ leva geodésicas em geodésicas em $\mathbb{H}^2$.*

Agora, cada transformação $T \in PSL(2,\mathbb{R})$ dada por $T(z) = \frac{az+b}{cz+d}$ pode ser identificada de modo natural com o elemento $(a,b,c,d) \in \mathbb{R}^4$. Logo, $SL(2,\mathbb{R})$ pode ser identificado como espaço topológico, associado a um subconjunto de $\mathbb{R}^4$,

$$E = \{(a,b,c,d) \in \mathbb{R}^4 : ad - bc = 1\}$$

herdando assim a estrutura topológica de $\mathbb{R}^4$.

A aplicação $\varphi : E \to E$ dada por $\varphi(a,b,c,d) = (-a,-b,-c,-d)$ é um homeomorfismo, e $\varphi$ com a identidade forma um grupo cíclico de ordem 2 agindo em $E$. Definimos a topologia em $PSL(2,\mathbb{R})$ como o espaço quociente

$$PSL(2,\mathbb{R}) \simeq \frac{SL(2,\mathbb{R})}{\{\pm\varphi\}}.$$

A norma em $PSL(2,\mathbb{R})$ é induzida do $\mathbb{R}^4$ da seguinte forma: para cada $T \in PSL(2,\mathbb{R})$ dada por $T(z) = \frac{az+b}{cz+d}$, $ad - bc = 1$, seja

$$\|T\| = \sqrt{a^2 + b^2 + c^2 + d^2},$$

que está bem definida. Assim, $PSL(2,\mathbb{R})$ é um grupo topológico com relação à métrica

$$d(T,S) = \|T - S\|$$

onde $T, S \in PSL(2,\mathbb{R})$. Temos ainda que o grupo das isometrias de $\mathbb{H}^2$ também é topológico.

**Definição 2.2.3** *Uma transformação de $\mathbb{H}^2$ sobre ele mesmo é chamada uma isometria se ela preserva a distância hiperbólica sobre $\mathbb{H}^2$.*

É claro que o conjunto de todas as isometrias de $\mathbb{H}^2$ forma um grupo, denotado por $Isom(\mathbb{H}^2)$.

**Teorema 2.2.7** *[27, Theorem 1.1.2, p.4]* $PSL(2,\mathbb{R}) \subset Isom(\mathbb{H}^2)$.

**Demonstração:** *Pelo Teorema* 2.2.4 *todas transformações em $PSL(2,\mathbb{R})$ levam $\mathbb{H}^2$ nele mesmo. Vamos mostrar que, se $\gamma : [a,b] \to \mathbb{H}^2$ é uma curva continuamente diferenciável por partes em $\mathbb{H}^2$, então para qualquer $T \in PSL(2,\mathbb{R})$ temos que $\|T(\gamma)\| = \|\gamma\|$. Suponhamos $\gamma : [a,b] \to \mathbb{H}^2$ é dado por $z(t) = (x(t), y(t))$, e $w(t) = T(z(t)) = u(t) + iv(t)$. Temos*

$$\frac{dw}{dz} = \frac{a(cz + d - c(az + b))}{(cz + d)^2} = \frac{1}{(cz + d)^2} \tag{2.14}$$

*Agora, pela equação* (2.12) *temos que* $v = \frac{y}{|cz+d|^2}$, *e daí* $\left|\frac{dw}{dz} = \frac{v}{y}\right|$. *Assim,*

$$\|T(\gamma)\| = \int_0^1 \frac{|\frac{dw}{dt}|dt}{v(t)} = \int_0^1 \frac{|\frac{dw}{dz}\frac{dz}{dt}|dt}{v(t)} = \int_0^1 \frac{|\frac{dz}{dt}|dt}{y(t)} = \|\gamma\|.$$

■

**Definição 2.2.4** *Um subgrupo* $\Gamma$ *de* $Isom(\mathbb{H}^2)$ *é chamado discreto se a topologia induzida sobre* $\Gamma$ *é uma topologia discreta, isto é, se* $\Gamma$ *é um conjunto discreto no espaço topológico* $Isom(\mathbb{H}^2)$.

**Definição 2.2.5** *Um subgrupo de* $Isom(\mathbb{H}^2)$ *é chamado um grupo Fuchsiano se ele for discreto e consistir de transformações que preservam orientação, em outras palavras, um grupo Fuchsiano é um subgrupo discreto de* $PSL(2,\mathbb{R})$.

Analogamente, o grupo discreto $\Gamma_p$ de isometrias que preservam orientação $T_p : \mathbb{D}^2 \to \mathbb{D}^2$ também é um grupo Fuchsiano, dado por transformações $T_p \in \Gamma_p < PSL(2,\mathbb{C})$ tais que

$$T_p(z) = \frac{az+c}{\bar{c}z+\bar{a}},\ a,b \in \mathbb{C},\ |a|^2 - |c|^2 = 1.$$

Além disso, podemos escrever $T_p = f \circ T \circ f^{-1}$, onde $T \in PSL(2,\mathbb{R})$ e $f : \mathbb{H}^2 \to \mathbb{D}^2$ é uma isometria dada pela equação (2.10).

A seguir veremos algumas definições no sentido de caracterizarmos os grupos Fuchsianos. Sejam $E$ um espaço métrico e $G$ um grupo de homeomorfismos de $E$.

Uma família $\{M_\alpha : \alpha \in A\}$ de subconjuntos de $E$ indexados pelos elementos de um conjunto $A$ é chamada *localmente finita* se para qualquer subconjunto compacto $K \subset E$, $M_\alpha \cap K \neq \emptyset$ apenas para uma quantidade finita de $\alpha \in A$.

**Definição 2.2.6** *Seja* $x \in E$. *A família* $\mathcal{G}(x) = \{g(x) : g \in \mathcal{G}\}$ *é chamada a* $\mathcal{G}$*- órbita do ponto* $x$.

**Definição 2.2.7** *Seja* $x \in E$. *O subgrupo* $\mathcal{G}_x = \{g \in \mathcal{G} : g(x) = x\}$ *é chamado estabilizador do ponto* $x$.

Dizemos que um grupo $\mathcal{G}$ *age de maneira propriamente descontínua* sobre $E$ se a $\mathcal{G}$-órbita de qualquer ponto $x \in E$ é localmente finita.

**Teorema 2.2.8** *[26, Teorema 5.16, p.62]* $\Gamma$ *é um grupo Fuchsiano se, e somente se,* $\Gamma$ *age de maneira propriamente descontínua sobre* $\mathbb{H}^2$.

**Observação 2.2.3** *Como veremos a seguir, o grupo* $\Gamma$ *tem uma região fundamental em* $\mathbb{H}^2$ *e estaremos interessados principalmente em grupos que tem uma região fundamental de área hiperbólica finita.*

### 2.2.5 Região Fundamental

Nesta subseção veremos o conceito de região fundamental de um grupo Fuchsiano. Este conceito está intimamente ligado no processo de construção das constelações de sinais geometricamente uniformes no plano hiperbólico.

Sejam $E$ um espaço métrico e $\Gamma$ um grupo de homeomorfismos agindo sobre $E$ de maneira propriamente descontínua. Um subconjunto fechado $D \subset E$ com conjunto interior denotado por $\dot{D}$ não vazio é chamado *região fundamental* de $\Gamma$ se

1. $\bigcup_{g\Gamma} g(D) = E$
2. $\dot{D} \cap g(\dot{D}) = \emptyset$, para todo $g \in \Gamma - \{Id\}$.

**Definição 2.2.8** *A família $\{g(D) : g \in \Gamma\}$ é chamada tesselação ou ladrilhamento de $E$.*

**Definição 2.2.9** *Sejam $\Gamma$ um grupo Fuchsiano e $z_0 \in \mathbb{H}^2$ tal que $T(z_0) \neq z_0$, para todo $T \in \Gamma$. Chamamos de domínio (ou região) de Dirichlet de $\Gamma$ centrado em $z_0$ ao conjunto*

$$D_{z_0}(\Gamma) = \{z \in \mathbb{H}^2 : d(z, z_0) \leq d(z, T(z_0)), \forall T \in \Gamma\}.$$

**Observação 2.2.4** *Em outras palavras, $D_{z_0}(\Gamma)$ consiste de pontos de $\mathbb{H}^2$ que estão mais próximos de $z_0$ do que de qualquer outro ponto da órbita $\Gamma(z_0)$.*

### 2.2.6 Tesselações Regulares no Plano Hiperbólico

Com o objetivo de determinar os reticulados hiperbólicos usados no processo de construção de constelações de sinais, apresentaremos nesta subseção a definição de tesselação regular no plano hiperbólico.

**Definição 2.2.10** *Uma tesselação regular no plano hiperbólico é uma partição deste plano por polígonos regulares não sobrepostos, todos congruentes, sujeitos à restrição de se interceptarem somente em suas arestas ou vértices, de modo a termos o mesmo número de polígonos partilhando um mesmo vértice, independente do vértice.*

Se os polígonos de uma tesselação de $\mathbb{H}^2$ contém $p$ lados, onde cada vértice é o encontro de $q$ desses polígonos, então a tesselação será denotada por $\{p, q\}$. Em particular, se $p = q$, então a tesselação é chamada auto-dual.

Como a soma dos ângulos internos de um triângulo hiperbólico é menor do que $\pi$, pelo Teorema 2.2.3, segue que $\{p, q\}$ é uma tesselação regular de $\mathbb{H}^2$ se, e somente se,

$$\frac{2\pi}{p} + \frac{2\pi}{q} < \pi,$$

ou seja, se, e somente se

$$(p-2)(q-2) > 4.$$

Portanto, existem infinitas tesselações regulares em $\mathbb{H}^2$. Por outro lado, como a soma dos ângulos internos do triângulo euclidiano é igual a $\pi$, segue que $\{4, 4\}$, $\{6, 3\}$ e $\{3, 6\}$ são as únicas tesselações regulares no plano euclidiano. Nesses casos, temos partições de $\mathbb{R}^2$ por quadrados, hexágonos regulares e triângulos regulares, respectivamente.

### 2.2.7 Grupos Fuchsianos Co-Compactos

Nesta subseção definiremos grupos Fuchsianos co-compactos, importantes para a caracterização dos grupos Fuchsianos que serão utilizados.

Consideremos a ação

$$\begin{aligned} P : \Gamma \times E &\to E \\ (T, x) &\mapsto T(x) \end{aligned}$$

de um grupo $\Gamma$ como homeomorfismos de um espaço topológico $E$, ou seja, para todo $S, T \in \Gamma$, a transformação $x \mapsto T(x)$ é um homeomorfismo de $E$, $Id(x) = x$ e $S(T(x)) = ST(x)$. Dizemos que a ação de $\Gamma$ é:

1. *Livre* se $T(x) = x$ para algum $x \in E$ se, e somente se, $T = Id$;

2. *Propriamente Descontínua* se para todo compacto $K$ de $E$, $T(K) \cap K \neq \emptyset$ apenas para um número finito de elementos $T$ de $\Gamma$.

A primeira situação que nos ocorre de uma ação livre e propriamente descontínua é no caso de recobrimento: Dizemos que uma aplicação contínua $P : \tilde{E} \to E$ entre espaços topológicos conexos por caminhos é uma *aplicação de recobrimento* se todo ponto $x \in E$ possui uma vizinhança aberta $U$ tal que $P^{-1}(U)$ é uma união disjunta de abertos e conexos, cada um deles homeomorfos a $U$.

Podemos obter uma superfície de Riemann considerando, por exemplo, os espaços quociente $\mathbb{H}^2/\Gamma_p$ e $\mathbb{D}^2/\Gamma_p$, onde $\Gamma_p$ é um grupo discreto agindo de maneira propriamente descontínua sobre $\mathbb{H}^2$ ou $\mathbb{D}^2$ [28]. O espaço $\mathbb{H}^2/\Gamma_p$ é construído por meio da seguinte relação de equivalência sobre $\mathbb{H}^2$:

$$z_1 \sim z_2 \Leftrightarrow \exists\, T \in \Gamma_p : T(z_1) = z_2. \tag{2.15}$$

Além disso, a classe de equivalência de um elemento $z \in \mathbb{H}^2$, denotada por $[z]$ é tal que $[z] = \Gamma_p$-órbita de $z$. Assim, os elementos do espaço $\mathbb{H}^2/\Gamma_p$ são as $\Gamma_p$-órbitas, isto é,

$$\mathbb{H}^2/\Gamma_p = \{[z] : z \in \mathbb{H}^2\}.$$

Analogamente, construimos o espaço $\mathbb{D}^2/\Gamma_p$.

Topologicamente, qualquer $g$-toro $\mathcal{T}_g$ localmente isométrico a $\mathbb{H}^2$ pode ser obtido pelo quociente de $\mathbb{H}^2$ por um grupo Fuchsiano $\Gamma_p$, isto é, $\mathcal{T}_g = \mathbb{H}^2/\Gamma_p$. De um modo geral, para cada gênero $g$ a ação do grupo $\Gamma_p$ em $\mathbb{H}^2$ pode se processar pela identificação das arestas de um polígono regular $P_p$ de $p$ arestas em $\mathbb{H}^2$ por isometrias que geram $\Gamma_p$.

Considerando o grupo Fuchsiano $\Gamma_p$ para o qual o espaço quociente $\mathbb{H}^2/\Gamma_p$ é uma superfície compacta, esse grupo será chamado *grupo Fuchsiano co-compacto*, e temos os seguintes resultados que o caracterizam.

Se $\Gamma$ possuir domínio fundamental compacto $D$, então $\Gamma$ é co-compacto, pois a restrição de $P$ à $D$ é sobrejetora. A recíproca também é válida:

**Teorema 2.2.9** *[26, Teorema 7.27, p.125] Seja $\Gamma$ um grupo Fuchsiano que possui domínio fundamental convexo não compacto. Então $\mathbb{H}^2/\Gamma$ não é compacto.*

**Demonstração:** *Seja $D$ um domínio fundamental convexo não compacto. Como $D$ é fechado e não compacto, existe sequência ilimitada $(z_n)_{n=1}^{\infty}$ de pontos de $D$. Sem perda de generalidade podemos assumir que $z_n$ converge para um ponto $q \in \partial_\infty \mathbb{H}^2$. Dado $p$ um ponto interior de $D$, a sequência dos segmentos geodésicos ligando $p$ à $z_n$ converge para um raio $\gamma$ geodésico ligando $p$ à $q$. Mas como $D$ é convexo e $p$ ponto interior, temos que $\gamma$ está contido no interior de $D$. Logo, se tomarmos uma cobertura de $\gamma$ que não possua subcobertura finita por abertos suficientemente pequenos, estes se projetarão homeomorfamente sobre sua imagem, e obteremos que $\mathbb{H}^2/\Gamma$ não é compacto.* ∎

**Corolário 2.2.1** *[26, Corolário 7.28, p.125] Um grupo Fuchsiano $\Gamma$ é co-compacto se, e somente se, toda região de Dirichlet for compacta.*

**Demonstração:** *Segue do Teorema* 2.2.9 *e da consideração que o antecede.* ∎

**Teorema 2.2.10** *[26, Teorema 7.29, p.125] Um grupo Fuchsiano $\Gamma$ é co-compacto se, e somente se, ele não possui elementos parabólicos e $\mu(\mathbb{H}^2/\Gamma) < \infty$.*

A área sobre o quociente $\mathbb{H}^2/\Gamma$ está bem definida, pois ela é induzida pela área hiperbólica sobre $\mathbb{H}^2$, e é dada por $\mu(D)$, sendo $D$ a região fundamental obtida através da ação de $\Gamma$ sobre $\mathbb{H}^2$.

Como consequência do Teorema 2.2.10 iremos considerar apenas os grupos Fuchsianos que não contenham elementos parabólicos, que foram utilizados em [11] e [12].

### 2.2.8 Assinatura de um Grupo Fuchsiano

Nesta subseção iremos considerar os grupos Fuchsianos $\Gamma$ que foram utilizados no processo de aplicação de recobrimento em $\mathbb{H}^2/\Gamma$. Para isso, necessitamos do conceito de assinatura de um grupo Fuchsiano.

Seja $\Gamma$ um grupo Fuchsiano co-compacto e $D(\Gamma)$ um domínio de Dirichlet de $\Gamma$. Em $D(\Gamma)$ existe um número finito de vértices, $r$, que são pontos fixos por elementos elípticos de $\Gamma$. Consideremos $m_1, \ldots, m_r$ as 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 *assinatura* de $\Gamma$.

O teorema a seguir relaciona a área de $\mathbb{H}^2/\Gamma$ com a assinatura de $\Gamma$.

**Teorema 2.2.11** *[26, Teorema 7.34, p.129] Sejam $\Gamma$ um grupo Fuchsiano co-compacto e $(g; m_1, \ldots, m_r)$ sua assinatura. Então a área de $\mathbb{H}^2/\Gamma$ é dada por*

$$\mu(\mathbb{H}^2/\Gamma) = 2\pi \left[ (2g-2) + \sum_{k=1}^{r} \left( 1 - \frac{1}{m_k} \right) \right].$$

Reciprocamente,

**Teorema 2.2.12** *[26, Teorema 7.35, p.131] Dados os inteiros $g \geq 0$, $r \geq 0$ e $m_k \geq 2$ para $1 \leq k \leq r$, tais que*

$$(2g-2) + \sum_{k=1}^{r} \left( 1 - \frac{1}{m_k} \right) > 0$$

*então existe um grupo Fuchsiano co-compacto com assinatura $(g; m_1, \ldots, m_r)$.*

Se o grupo Fuchsiano não possui elementos elípticos, então sua assinatura é dada por $(g; 0, \ldots, 0)$, ou simplesmente $(g; -)$. Pelo Teorema 2.2.11 a área de $\mathbb{H}^2/\Gamma$ é dada por $\mu(\mathbb{H}^2/\Gamma) = 2\pi(2g-2)$ e a ação de $\Gamma$ em $\mathbb{H}^2$ é livre, ou seja, a projeção $P : \mathbb{H}^2 \to \mathbb{H}^2/\Gamma$ é uma aplicação de recobrimento.

O último teorema afirma que dada uma superfície compacta $\mathbb{S}$ com gênero $g \geq 2$, existe um grupo Fuchsiano $\Gamma$ tal que $\mathbb{S} \equiv \mathbb{H}^2/\Gamma$.

Encerramos o capítulo com o seguinte resultado, que é uma consequência do Teorema 2.2.12.

**Corolário 2.2.2** *[26, Corolário 7.37, p.135] Toda superfície compacta com gênero $g \geq 2$ pode ser modelada no plano hiperbólico.*

**Demonstração:** *De fato, temos que* $2g - 2 > 0$*, logo, existe um grupo Fuchsiano* $\Gamma$ *com assinatura* $(g; -)$*. Como* $\Gamma$ *não possui ciclos elípticos, temos que a ação de* $\Gamma$ *em* $\mathbb{H}^2$ *é livre e a aplicação* $P : \mathbb{H}^2 \to \mathbb{H}^2/\Gamma$ *é aplicação de recobrimento. Temos então que* $\mathbb{H}^2/\Gamma$ *é uma superfície de gênero* $g$*.* ■

Em [11] e [12] superfícies compactas orientáveis foram modeladas no plano hiperbólico a partir de tesselações hiperbólicas, de modo a obter os geradores dos grupos Fuchsianos, que por sua vez estão associados a uma ordem dos quatérnios, a qual utilizaremos para a construção dos códigos.

# Capítulo 3

# Ordens dos Quatérnios e Grupos Fuchsianos Aritméticos

Neste capítulo definiremos grupos Fuchsianos aritméticos e faremos a identificação de alguns destes grupos com ordens dos quatérnios, as quais serão utilizadas para construção de constelações de sinais e códigos no Capítulo 5. Utilizaremos as referências [11], [12], [27]-[29], [32]-[35].

## 3.1 Ordens dos Quatérnios

Nesta seção apresentaremos as álgebras dos quatérnios e seus subanéis chamados ordens dos quatérnios, além de algumas propriedades que serão importantes para o desenvolvimento das demais seções.

Seja $A$ um espaço vetorial sobre um corpo $\mathbb{K}$. Dizemos que $A$ é uma $\mathbb{K}$-*álgebra* se existe uma multiplicação de $A \times A$ em $A$ dada por $(a, b) \mapsto ab$ satisfazendo para todo $a, b, c \in A$ e $\alpha \in \mathbb{K}$:

1. $a(b + c) = ab + ac$;
2. $a(\alpha b) = (\alpha a)b = \alpha(ab)$;
3. $a(bc) = (ab)c$;
4. Existe $1_A \in A$ tal que $a.1_A = 1_A.a$.

**Definição 3.1.1** *Uma álgebra $A$ é chamada simples se o radical $\mathcal{R}$, isto é, um ideal $\mathcal{R} \subseteq A$ tal que $\mathcal{R}^n = \{0\}$ para algum $n \in \mathbb{N}$, é o trivial, ou seja, $\mathcal{R} = \{0\}$.*

**Definição 3.1.2** *Uma álgebra $A$ é chamada central se o centro $Z = \{x \in A : xy = yx, \forall y \in A\} = \mathbb{K}$.*

**Teorema 3.1.1** *Se $A$ é uma álgebra central simples de dimensão 4 sobre $\mathbb{K}$, então $A$ tem uma base da forma $\{1, i, j, k\}$, onde 1 é uma identidade multiplicativa, $i^2 = a.1$, $j^2 = b.1$, onde $a, b \in \mathbb{K}^*$ e $ij = -ji$.*

**Definição 3.1.3** *Uma álgebra dos quatérnios $\mathcal{A}$ sobre $\mathbb{K}$ é definida como uma álgebra central simples de dimensão 4.*

**Observação 3.1.1** *Para quaisquer $a, b \in \mathbb{K}^*$, podemos definir uma álgebra dos quatérnios sobre $\mathbb{K}$, como no teorema anterior.*

**Observação 3.1.2** *Denotaremos a álgebra dos quatérnios $\mathcal{A}$ sobre $\mathbb{K}$ pelo símbolo de Hilbert $\left(\frac{a,b}{\mathbb{K}}\right)$, ou simplesmente por $(a, b)_{\mathbb{K}}$.*

**Exemplo 3.1.1**

1. *$M_2(\mathbb{Q}) = (1, 1)_{\mathbb{Q}}$ é uma álgebra dos quatérnios, onde*

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} e \; ij = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

2. *$(-7, e^{2\pi i/5})_{\mathbb{Q}(e^{2\pi i/5})} = \{a_0 + a_1 i + a_2 j + a_3 ij : a_i \in \mathbb{Q}(e^{2\pi i/5})\}$ é uma álgebra dos quatérnios, onde a multiplicação é definida por $i^2 = -7$, $j^2 = e^{2\pi i/5}$, $ij = -ji$.*

Sobre qualquer álgebra dos quatérnios, existe uma função conjugada definida para $\alpha = a_0 + a_1 i + a_2 j + a_3 ij$, onde $a_0, a_1, a_2, a_3 \in \mathbb{K}$, por $\bar{\alpha} = a_0 - a_1 i - a_2 j - a_3 ij$. Daí obtemos a norma reduzida,

$$Nrd(\alpha) = \alpha.\bar{\alpha} = a_0^2 - aa_1^2 - ba_2^2 + aba_3^2 \tag{3.1}$$

e o traço reduzido,

$$Trd(\alpha) = \alpha + \bar{\alpha} = 2a_0. \tag{3.2}$$

Além disso, podemos verificar que

$$Nrd(\alpha.\beta) = Nrd(\alpha).Nrd(\beta), \tag{3.3}$$

para quaisquer $\alpha, \beta \in \mathcal{A}$.

**Observação 3.1.3**

1. *Sobre uma álgebra matricial, a norma é simplesmente o determinante.*

2. *A função conjugada não depende da escolha da base.*

3. *O símbolo de Hilbert não é unicamente determinado, isto é,* $\left(\frac{a,b}{\mathbb{K}}\right) \cong \left(\frac{ax^2,by^2}{\mathbb{K}}\right)$*, para qualquer* $x, y \in \mathbb{K}$*.*

Existe entretanto um poderoso teorema de existência e classificação para a álgebra dos quatérnios sobre corpos de números, que veremos mais adiante.

**Observação 3.1.4** *Se considerarmos a álgebra dos quatérnios sobre* $\mathbb{R}$*, então existem apenas duas possibilidades*

$$\left(\frac{1,1}{\mathbb{R}}\right) \cong \left(\frac{1,-1}{\mathbb{R}}\right) \cong M_2(\mathbb{R}) \text{ } ou \text{ } \left(\frac{-1,-1}{\mathbb{R}}\right) \cong \mathcal{H} \text{ } (quatérnio \text{ } de \text{ } Hamilton). \tag{3.4}$$

**Observação 3.1.5** *Como* $ij = -ji$*, segue que não vale a comutatividade numa álgebra dos quatérnios* $\mathcal{A}$*.*

Sejam $\mathcal{A} = (a,b)_{\mathbb{K}}$ e $M_0, M_1, M_2$ e $M_3$ matrizes linearmente independentes de $M_2(\mathbb{K}(\sqrt{a}))$, dadas por

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, M_2 = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} e \ M_3 = \begin{pmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{pmatrix}.$$

Consideremos agora o mergulho $\varphi$ da álgebra $\mathcal{A} = (a,b)_{\mathbb{K}}$ sobre $M_2(\mathbb{K}(\sqrt{a}))$ definido por

$$\varphi(a_0 + a_1 i + a_2 j + a_3 k) = a_0 M_0 + a_1 M_1 + a_2 M_2 + a_3 M_3.$$

Como $\varphi(M_1^2) = a.I_2$, $\varphi(M_2^2) = b.I_2$ e $\varphi(M_1)\varphi(M_2) = -\varphi(M_2)\varphi(M_1)$, onde $I_2$ é a matriz identidade de ordem 2, verifica-se que $\varphi$ é um isomorfismo de $\mathcal{A} = (a,b)_{\mathbb{K}}$ em uma subálgebra de $M_2(\mathbb{K}(\sqrt{a}))$. Assim, cada elemento de $\mathcal{A}$ é identificado com

$$\alpha \mapsto \varphi(\alpha) = a_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} + a_2 \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{pmatrix}$$

$$= \begin{pmatrix} a_0 + a_1\sqrt{a} & a_2 + a_3\sqrt{a} \\ b(a_2 - a_3\sqrt{a}) & a_0 - a_1\sqrt{a} \end{pmatrix}$$

Dessa forma, se $a = t^2$ com $t \in \mathbb{K} - \{0\}$, então

$$\varphi(\alpha) = \begin{pmatrix} a_0 + a_1 t & a_2 + a_3 t \\ b(a_2 - a_3 t) & a_0 - a_1 t \end{pmatrix}$$

e segue que $\mathcal{A} \cong M_2(\mathbb{K})$. Também observe que $\mathbb{K}(\sqrt{a}) \cong \mathbb{K}(\sqrt{\lambda^2 a})$, para qualquer $\lambda \in \mathbb{K}^*$. Assim, temos o seguinte resultado:

**Teorema 3.1.2** *[27, Theorem 5.2.1, p.114]*

1. *Se $a \in (\mathbb{K}^*)^2$, então $\mathcal{A} \cong M_2(\mathbb{K})$.*

2. *Para qualquer $\lambda \in \mathbb{K}^*$, temos $(a, b)_{\mathbb{K}} \cong (\lambda^2 a, b)_{\mathbb{K}}$*

**Corolário 3.1.1** *[27, Corollary 5.2.2, p.115] Se $\mathbb{K}$ é um corpo algebricamente fechado, então para qualquer $a$ e $b$, temos $\mathcal{A} = (a, b)_{\mathbb{K}} \cong M_2(\mathbb{K})$.*

**Definição 3.1.4** *Seja $\mathcal{A}$ uma álgebra dos quatérnios. Se cada elemento de $\mathcal{A}$ tem um inverso, então $\mathcal{A}$ é chamada álgebra de divisão.*

**Teorema 3.1.3** *[27, Theorem 5.2.3, p.115] $\mathcal{A}$ é uma álgebra de divisão se, e somente se, $Nrd(\alpha) = 0$ apenas para $\alpha = 0$.*

**Demonstração:** *Suponhamos $\alpha \neq 0$. Então $Nrd(\alpha) \neq 0$, pois temos que $Nrd(\alpha) = \alpha\bar{\alpha}$, logo $\frac{\bar{\alpha}}{Nrd(\alpha)}\alpha = 1$, o que significa que $\frac{\bar{\alpha}}{Nrd(\alpha)}$ é o elemento inverso de $\alpha$, logo $\mathcal{A}$ é uma álgebra de divisão. Reciprocamente, se $\mathcal{A}$ é uma álgebra de divisão e $\alpha \neq 0$, então $\alpha^{-1} \neq 0$, e daí $Nrd(\alpha)Nrd(\alpha^{-1}) = 1$, isto é, $Nrd(\alpha) \neq 0$.* ∎

**Teorema 3.1.4** *[27, Theorem 5.2.4, p.115] Se $\mathcal{A} = (a, b)_{\mathbb{K}}$ não é isomorfa a $M_2(\mathbb{K})$, então $\mathcal{A}$ é uma álgebra de divisão.*

**Demonstração:** *Primeiro observamos que $a \notin (\mathbb{K}^*)^2$, caso contrário teríamos $\mathcal{A} \cong M_2(\mathbb{K})$ pelo Teorema 3.1.2. Então $\mathbb{L} = \mathbb{K}(i)$ é uma extensão quadrática de $\mathbb{K}$ e $\mathcal{A} = \mathbb{L} + \mathbb{L}j$. Suponhamos que $\mathcal{A}$ não é uma álgebra de divisão. Então pelo Teorema 3.1.3, existe $\alpha \in \mathcal{A}$, $\alpha \neq 0$ com $Nrd(\alpha) = 0$. Seja $\alpha = a_0 + a_1 i + a_2 j + a_3 k$, então temos que*

$$0 = Nrd(\alpha) = a_0^2 - a_1^2 a - a_2^2 b + a_3^2 ab = (a_0^2 - a_1^2 a) - b(a_2^2 - a_3^2 a) = N(a_0 + ia_1) - bN(a_2 + ia_3), \quad (3.5)$$

*onde $N$ é a norma no corpo $\mathbb{L}$. Mostraremos primeiro que $a_2 + ia_3 \neq 0$. De fato, se $a_2 + ia_3 = 0$, temos $N(a_0 + ia_1) = 0$, e como não existem divisores de zero em $\mathbb{L}$, $a_0 + ia_1 = 0$, e então $\alpha = 0$, uma contradição. Assim deduzimos de (3.5) que*

$$b = \frac{N(a_0 + ia_1)}{N(a_2 + ia_3)} = N(q_0 + iq_1),$$

*onde $q_0, q_1 \in \mathbb{K}$, isto é, $b = q_0^2 - aq_1^2$. Agora, construimos uma função de $\mathcal{A}$ em $M_2(\mathbb{F})$ levando os elementos da base de $\mathcal{A}$ nas seguintes matrizes:*

$$1 \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i \longrightarrow \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \quad e \quad j \longrightarrow \begin{pmatrix} q_0 & -q_1 \\ q_1 a & -q_0 \end{pmatrix}$$

*É fácil verificar que $i^2 \to \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $j^2 \to \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$ e $ij = -ji$, e que as matrizes são linearmente independentes. Daí $\mathcal{A} \cong M_2(\mathbb{K})$, uma contradição. Portanto, $\mathcal{A}$ é uma álgebra de divisão.* ∎

Consideremos agora $\mathcal{A} = (a, b)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre o corpo $\mathbb{K}$ e $\varphi : \mathbb{K} \longrightarrow \mathbb{F}$ um homomorfismo de corpos. Definimos

$$\mathcal{A}^{\varphi} = (\varphi(a), \varphi(b))_{\varphi(\mathbb{K})} \quad e \quad \mathcal{A}^{\varphi} \otimes \mathbb{F} = (\varphi(a), \varphi(b))_{\mathbb{F}}, \tag{3.6}$$

onde $\mathcal{A}^{\varphi} \otimes \mathbb{F}$ denota o produto tensorial da álgebra $\mathcal{A}^{\varphi}$ com o corpo $\mathbb{F}$, que continua sendo uma álgebra central simples [21].

**Definição 3.1.5** *Para cada homomorfismo $\varphi$, a álgebra $\mathcal{A}^{\varphi} = (\varphi(a), \varphi(b))_{\varphi(\mathbb{K})}$ é chamada de lugar da álgebra dos quatérnios $\mathcal{A}$.*

Seja $\mathbb{K}$ um corpo de números algébricos totalmente real de grau $n$. Isso significa que os $n$ monomorfismos $\varphi_i$, $i = 1, \ldots, n$ são todos reais, ou seja, $\varphi_i(\mathbb{K}) \subset \mathbb{R}$. Portanto, os $n$ distintos lugares são definidos pelos $\mathbb{R}$-isomorfismos

$$\rho_1 : \mathcal{A}^{\varphi_1} \otimes \mathbb{R} \longrightarrow M_2(\mathbb{R}) \quad e \quad \rho_i : \mathcal{A}^{\varphi_i} \otimes \mathbb{R} \longrightarrow \mathbb{H} \tag{3.7}$$

onde $\varphi_1$ é a identidade, $\varphi_i$ um mergulho de $\mathbb{K}$ em $\mathbb{R}$, para $i = 1, \ldots, n$, e $\mathbb{H}$ uma subálgebra de divisão de $M_2(\mathbb{K}(\sqrt{a}))$. Desse modo, dizemos que $\mathcal{A}$ é não ramificada no lugar $\varphi_1$ e ramificada nos lugares $\varphi_i$, para $2 \leq i \leq n$.

Sejam $Nrd_{\mathbb{H}}$ e $Trd_{\mathbb{H}}$ a norma e o traço reduzidos em $\mathbb{H}$, respectivamente. Dado $\alpha \in \mathcal{A}$, verificamos através de simples cálculos que

$$Nrd_{\mathbb{H}}(\alpha) = det(\rho_1(\alpha)) \quad e \quad Trd_{\mathbb{H}}(\alpha) = tr(\rho_1(\alpha)). \tag{3.8}$$

E, desde que identifiquemos $\alpha_i$ com $\varphi_i(\alpha_i)$, para $i = 0, 1, 2, 3$, obtemos para todo $2 \leq i \leq n$,

$$\varphi_i(Nrd_{\mathbb{H}}(\alpha)) = Nrd_{\mathbb{H}}(\rho_i(\alpha)) \;\; e \;\; \varphi_i(Trd_{\mathbb{H}}(\alpha)) = Trd_{\mathbb{H}}(\rho_i(\alpha)). \tag{3.9}$$

**Exemplo 3.1.2** *Sejam* $\mathbb{H} = \mathcal{H} = (-1,-1)_{\mathbb{R}}$ *a álgebra dos quatérnios de Hamilton e* $\mathbb{H}^1 = \{\alpha \in \mathbb{H} : Nrd_{\mathbb{H}}(\alpha) = 1\}$. *Então, dado* $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}^1$, *obtemos de* (3.1) *que*

$$Nrd_{\mathbb{H}}(\alpha) = a_0^2 - aa_1^2 - ba_2^2 + aba_3^2 = a_0^2 + a_1^2 + a_2^2 + a_3^2 = 1,$$

*o que implica que* $a_0^2 = 1 - a_1^2 - a_2^2 - a_3^2$ *e daí* $|a_0| \leq 1$. *Agora de* (3.2) *segue que* $Trd_{\mathbb{H}}(\alpha) = 2a_0$, *e assim* $Trd_{\mathbb{H}}(\alpha) = 2a_0 \in [-2,2]$. *Portanto,* $Trd_{\mathbb{H}}(\mathbb{H}^1) = [-2,2]$.

Agora, dados $\mathcal{A}$ uma álgebra dos quatérnios sobre $\mathbb{K}$ e $R$ um anel de $\mathbb{K}$, uma *$R$-ordem* $\mathcal{O}$ em $\mathcal{A}$ é um subanel com unidade de $\mathcal{A}$ que é um $R$-módulo finitamente gerado tal que $\mathcal{A} = \mathbb{K}\mathcal{O}$. Assim, sendo $\mathcal{A} = (a,b)_{\mathbb{K}}$ e $I_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$, onde $a, b \in I_{\mathbb{K}} - \{0\}$, então

$$\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 ij : a_0, a_1, a_2, a_3 \in I_{\mathbb{K}}\},$$

é uma ordem em $\mathcal{A}$ denotada por $\mathcal{O} = (a,b)_{I_{\mathbb{K}}}$.

**Exemplo 3.1.3** *Dada* $\mathcal{H} = (-1,-1)_{\mathbb{R}}$ *a álgebra dos quatérnios de Hamilton, temos que o anel de inteiros de* $\mathbb{R}$ *é* $\mathbb{Z}$ *e a ordem dos quatérnios*

$$\mathcal{H}[\mathbb{Z}] = \{a_0 + a_1 i + a_2 j + a_3 ij : a_0, a_1, a_2, a_3 \in \mathbb{Z}\},$$

*é chamada anel dos inteiros dos quatérnios de Hamilton, ou inteiros de Lipschitz.*

## 3.2 Reticulados Hiperbólicos

Nesta seção definiremos reticulados hiperbólicos, que são usados no processo de rotulagem de sinais de uma constelação de sinais geometricamente uniforme no plano hiperbólico, como proposto em [11].

Sejam $\mathcal{A}$ uma álgebra dos quatérnios sobre $\mathbb{K}$ e $R$ um anel de $\mathbb{K}$. Uma $R$-ordem $\mathcal{O}$ em $\mathcal{A}$ é um subanel com unidade de $\mathcal{A}$ que é um $R$-módulo finitamente gerado tal que $\mathcal{A} = \mathbb{K}\mathcal{O}$, como vimos na seção anterior.

**Observação 3.2.1** *Também chamaremos uma $R$-ordem $\mathcal{O}$ de* reticulado hiperbólico*, devido a sua identificação com grupos Fuchsianos aritméticos.*

Sendo $\mathcal{O}$ uma ordem em $\mathcal{A}$, então existe uma base $\{e_1, e_2, e_3, e_4\}$ de $\mathcal{A}$ em $R$ e um $R$-ideal $\mathcal{I}$ tal que

$$\mathcal{O} = \mathcal{I}e_1 \oplus Re_2 \oplus Re_3 \oplus Re_4,$$

onde $\oplus$ denota a soma direta.

**Observação 3.2.2** *Por definição, dados $\alpha, \beta \in \mathcal{O}$, temos $\alpha\beta \in \mathcal{O}$. Além disso, como todo elemento $\alpha \in \mathcal{O}$ é integral sobre $R$, então $Nrd(\alpha), Trd(\alpha) \in R$.*

Na próxima seção definiremos grupos Fuchsianos aritméticos, e então podemos identificar grupos Fuchsianos aritméticos em uma ordem dos quatérnios $\mathcal{O}$, de modo a realizar o rotulamento dos sinais das constelações (quociente em uma ordem por um ideal próprio). Entretanto, para que a rotulamento algébrico seja completo, é necessário que as respectivas ordens sejam maximais.

**Definição 3.2.1** *Uma ordem $\mathcal{M}$ em uma álgebra $\mathcal{A}$ é chamada maximal se $\mathcal{M}$ não está propriamente contida em nenhuma outra ordem em $\mathcal{A}$.*

A existência de uma ordem maximal $\mathcal{M}$ é garantida pelo seguinte resultado.

**Proposição 3.2.1** *[32] Existe pelo menos uma $R$-ordem maximal em $\mathcal{A}$. Além disso, toda $R$-ordem em $\mathcal{A}$ está contida em uma $R$-ordem maximal de $\mathcal{A}$.*

Podemos ainda, verificar se uma ordem é maximal através do seu discriminante. O *discriminante* de uma álgebra dos quatérnios $\mathcal{A}$, é definido como o produto dos ideais primos nos quais $\mathcal{A}$ é ramificado, e será denotado por $d(\mathcal{A})$.

**Exemplo 3.2.1** *Consideremos a álgebra $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$. Então, por [33]*

$$d(\mathcal{A}) = \sqrt{2}.$$

Seja $\{a_0, a_1, a_2, a_3\}$ um conjunto de geradores de $\mathcal{O}$ sobre $R$. O *discriminante* de $\mathcal{O}$ denotado por $d(\mathcal{O})$, é definido pela raiz quadrada do $R$-ideal gerado pelo conjunto de elementos

$$\{det(Trd(a_i\bar{a_j})) : 0 \leq i, j \leq 3\}. \tag{3.10}$$

**Exemplo 3.2.2** *Sejam $\mathcal{A} = (a, b)_{\mathbb{K}}$ e $I_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$, onde $a, b \in I_{\mathbb{K}} - \{0\}$. Então*

$$\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in I_{\mathbb{K}}\},$$

*é uma ordem em $\mathcal{A}$ denotada por $\mathcal{O} = (a, b)_{I_{\mathbb{K}}}$. Vamos determinar $d(\mathcal{O})$. Temos que o discriminante de $\mathcal{O}$ definido anteriormente é o seguinte ideal principal,*

$$I_{\mathbb{K}}.det(Trd(a_i\bar{a_j})),$$

*onde* $\{a_0, a_1, a_2, a_3\} = \{1, i, j, k\}$. *Assim, por definição*

$$d(\mathcal{O}) = (det(Trd(a_i\bar{a_j})))^{1/2}.$$

*Por outro lado, verifica-se que* $Trd(a_i\bar{a_j})$ *é a seguinte matriz diagonal*

$$Trd(a_i\bar{a_j}) = \begin{pmatrix} Trd(1) & & & 0 \\ & Trd(i) & & \\ & & Trd(j) & \\ 0 & & & Trd(k) \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2a & 0 & 0 \\ 0 & 0 & -2b & 0 \\ 0 & 0 & 0 & 2ab \end{pmatrix}$$

*Portanto,* $d(\mathcal{O}) = (16a^2b^2)^{1/2} = 4ab$.

Se $\mathcal{M}$ é uma ordem maximal em $\mathcal{A}$ contendo uma outra ordem $\mathcal{O}$, então o discriminante satisfaz

$$d(\mathcal{O}) = d(\mathcal{M}).[\mathcal{M} : \mathcal{O}], \quad d(\mathcal{M}) = d(\mathcal{A}). \tag{3.11}$$

Reciprocamente, se $d(\mathcal{O}) = d(\mathcal{A})$, então $\mathcal{O}$ é uma ordem maximal em $\mathcal{A}$ [33].

**Exemplo 3.2.3** *Consideremos a álgebra* $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$ *com uma base* $\{1, i, j, k\}$, *satisfazendo* $i = \sqrt[4]{2}$, $j = Im$, $k = \sqrt[4]{2}$ *e* $\mathcal{O} = (\sqrt{2}, -1)_R$, *onde* $R = \{\frac{x}{2n} : x \in \mathbb{Z}(\sqrt{2}), n \in \mathbb{N}\}$. *Pelo Exemplo 3.2.1 temos que* $d(\mathcal{A}) = \sqrt{2}$, *e pelo Exemplo 3.2.2 segue que* $d(\mathcal{O}) = -\sqrt{2}$. *Portanto,* $\mathcal{O}$ *é uma ordem maximal em* $\mathcal{A}$.

Para cada ordem $\mathcal{O}$ em $\mathcal{A}$, consideremos $\mathcal{O}^1$ o conjunto

$$\mathcal{O}^1 = \{\alpha \in \mathcal{O} : Nrd(\alpha) = 1\}.$$

**Proposição 3.2.2** *[12, Proposição 3.2.5, p.34]* $\mathcal{O}^1$ *é um grupo multiplicativo.*
**Demonstração:** *Sejam* $\alpha, \beta \in \mathcal{O}^1$. *Logo* $\alpha, \beta \in \mathcal{O}$. *Mas por* (3.3), *segue que* $Nrd(\alpha, \beta) = Nrd(\alpha).Nrd(\beta) = 1$. *Assim,* $\alpha\beta \in \mathcal{O}^1$. *Por outro lado, o inverso de* $\alpha$ *é* $\bar{\alpha}$ *e* $Nrd(\bar{\alpha}) = 1$. ■

**Teorema 3.2.1** (*Borel-Harishchandra*) *Sejam* $\mathbb{K}$ *um corpo de números real,* $(a, b)_{\mathbb{K}}$ *uma álgebra dos quatérnios sobre* $\mathbb{K}$ *tal que* $(a, b)_{\mathbb{K}} \cong M_2(\mathbb{R})$ *e* $\mathcal{O}$ *uma ordem em* $(a, b)_{\mathbb{K}}$. *Então* $\mathcal{O}^1$ *é um reticulado em* $(a, b)_{\mathbb{K}} \cong SL(2, \mathbb{R})$ *se, e somente se:*

1. $\mathbb{K}$ *é totalmente real,*

2. *Para todo* $\sigma$ *monomorfismo de Galois,* $\sigma : \mathbb{K} \longrightarrow \mathbb{R}$, $\sigma \neq Id$, *temos* $(\sigma(a), \sigma(b))_{\mathbb{R}} \cong \mathcal{H}$ (*quatérnio de Hamilton*).

**Exemplo 3.2.4** *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. *Temos que* $\mathbb{K}$ *é totalmente real, pois* $x^2-2$ *é o seu polinômio minimal e suas raízes* $\pm\sqrt{2}$ *são reais. Seja* $\mathcal{A} = (-1,\sqrt{2})_{\mathbb{Q}(\sqrt{2})}$ *uma álgebra dos quatérnios sobre* $\mathbb{Q}(\sqrt{2})$. *Observe que* $(-1,\sqrt{2})_{\mathbb{R}} \cong M_2(\mathbb{R})$. *Seja* $\mathcal{O} = \mathbb{Z}(\sqrt{2})[1,i,j,ij]$ *uma ordem em* $\mathcal{A}$. *Temos ainda que os monomorfismos de Galois são* $\sigma_1$, $\sigma_2$ *tais que* $\sigma_1(a+b\sqrt{2}) = a+b\sqrt{2}$ *e* $\sigma_2(a+b\sqrt{2}) = a-b\sqrt{2}$. *Assim*

$$(\sigma(-1),\sigma(\sqrt{2}))_{\mathbb{R}} = (-1,-\sqrt{2})_{\mathbb{R}} \cong \mathcal{H}.$$

*Portanto, as condições do teorema são satisfeitas. Agora, queremos mostrar que* $\mathcal{O}^1$ *é discreto em* $(-1,\sqrt{2})_{\mathbb{R}}$. *Faremos um esboço da prova. Suponhamos que não. Então existe uma sequência* $\alpha_n \in \mathcal{O}^1$ *tal que* $\alpha_n \longrightarrow 1$. *Seja* $\alpha_n = a_0^{(n)} + a_1^{(n)}i + a_2^{(n)}j + a_3^{(n)}ij$, *onde* $a_i^{(n)} \in \mathbb{Z}[\sqrt{2}]$. *Agora, considere a sequência*

$$\sigma(\alpha_n) = \sigma(a_0^{(n)}) + \sigma(a_1^{(n)}))i' + \sigma(a_2^{(n)})j' + \sigma(a_3^{(n)})i'j',$$

*onde* $\{1,i',j',i'j'\}$ *é a base de* $(-1,-\sqrt{2})_{\mathbb{R}}$. *Mas* $\sigma(\alpha_n) \in (-1,-\sqrt{2})_{\mathbb{R}} \cong \mathcal{H} \cong S^3$, *que é compacto. Então, para todo* $n$, $\sigma(a_0^{(n)})$, $\sigma(a_1^{(n)})$, $\sigma(a_2^{(n)})$ *e* $\sigma(a_3^{(n)})$ *são limitados.*

*Por hipótese, os elementos* $a_0^{(n)}$, $a_1^{(n)}$, $a_2^{(n)}$ *e* $a_3^{(n)}$ *também são limitados para todo* $n$ *grande. Suponhamos sem perda de generalidade* $a_0^{(n)} = x_n + y_n\sqrt{2}$, $x_n$, $y_n \in \mathbb{Z}$. *Assim, para muitos valores de* $n$, $x_n + y_n\sqrt{2}$ *e* $x_n - y_n\sqrt{2}$ *são limitados. Então* $x_n$ *e* $y_n$ *são limitados para muitos valores de* $n$, *o que é uma contradição. Portanto,* $\mathcal{O}^1$ *é discreto em* $(-1,\sqrt{2})_{\mathbb{R}}$.

**Observação 3.2.3** *O ponto crítico desta demonstração é que existe uma sequência infinita* $x_n$ *de todos os inteiros algébricos cujos conjugados são limitados, isto vem da condição de compacidade como descrito nesta demonstração, que é uma consequência da segunda condição do Teorema de Borel-Harishchandra.*

Agora, observamos que os grupos Fuchsianos podem ser obtidos do isomorfismo $\rho_1$ em (3.7). De fato, pela equação (3.8) temos que $Nrd(\alpha) = det(\rho_1(\alpha))$. Além disso, pela Proposição 3.2.2 temos que $\mathcal{O}^1$ é um grupo multiplicativo. Logo, $\rho_1(\mathcal{O}^1)$ é um subgrupo de $SL(2,\mathbb{R})$, ou seja, $\rho_1(\mathcal{O}^1) < SL(2,\mathbb{R})$. Portanto, o grupo derivado de uma álgebra dos quatérnios $\mathcal{A} = (a,b)_{\mathbb{K}}$ cuja ordem é $\mathcal{O}$, denotado por $\Gamma(\mathcal{A},\mathcal{O})$ é dado por

$$\Gamma(\mathcal{A},\mathcal{O}) = \frac{\rho_1(\mathcal{O}^1)}{\{\pm I_2\}} < \frac{SL(2,\mathbb{R})}{\{\pm I_2\}} \cong PSL(2,\mathbb{R}). \tag{3.12}$$

Mais ainda,

**Teorema 3.2.2** *[27, Theorem 5.2.7, p.119]* $\Gamma(\mathcal{A},\mathcal{O})$ *é um grupo Fuchsiano.*

**Demonstração:** *Provaremos para o caso em que a álgebra de divisão é* $\mathcal{A}=(a,b)_{\mathbb{K}}$, $a>0$ *e* $\mathcal{O}=\{\alpha=a_0+a_1i+a_2j+a_3k : a_0,a_1,a_2,a_3\in\mathbb{Z}\}$. *Para o caso de um corpo de números* $\mathbb{K}=\mathbb{Q}(\theta)$, *a demonstração segue o mesmo raciocínio com algumas adaptações. Precisamos mostrar que* $\Gamma(\mathcal{A},\mathcal{O})$ *é um subgrupo discreto de* $PSL(2,\mathbb{R})$. *Para isso, é necessário encontrarmos uma vizinhança* $V_{I_2}$ *de* $I_2\in SL(2,\mathbb{R})$ *que não contenha nenhum elemento de* $\rho_1(\mathcal{O}^1)$ *diferente de* $I_2$. *Consideremos*

$$V_{I_2}=\{(g_{ij})_{i,j=1,2}\in SL(2,\mathbb{R}) : |g_{11}-1|<1/2, |g_{12}|<1/2, |g_{21}|<1/2, |g_{22}-1|<1/2\}.$$

*Seja* $g_\alpha\in\rho_1(\mathcal{O}^1)\cap V_{I_2}$, *digamos*

$$g_\alpha=\begin{pmatrix} a_0+a_1\sqrt{a} & a_2+a_3\sqrt{a} \\ b(a_2-a_3\sqrt{a}) & a_0-a_1\sqrt{a}\end{pmatrix}.$$

*Deste modo,* $2|a_0-1|$, *ou seja,* $a_0=1$. *Como* $b>1$ *temos também que* $|a_2-a_3\sqrt{a}|<1/2b<1/2$, *e assim* $|2a_2|<1$, *o que implica que* $a_2=0$. *Por outro lado,* $|a_1\sqrt{a}|<1/2$, $|a_3\sqrt{a}|<1/2$, *implicando que* $a_1=a_3=0$, *e consequentemente* $g_\alpha=I_2$. *Portanto,* $\Gamma(\mathcal{A},\mathcal{O})$ *é um subgrupo discreto de* $PSL(2,\mathbb{R})$. ∎

Tudo isto finalmente conduz à definição de grupo Fuchsiano aritmético.

## 3.3 Grupos Fuchsianos Aritméticos

Os grupos Fuchsianos aritméticos foram considerados no processo de construção de constelações de sinais geometricamente uniformes no plano hiperbólico, no trabalho de Carvalho [11], onde as partes aritmética e geométrica inerentes a esses grupos são unidas nesse processo. Nesta seção consideraremos um critério para caracterização de grupos Fuchsianos aritméticos e destacaremos os principais resultados que usaremos no processo de identificação desses grupos em ordens dos quatérnios.

Se $\Gamma$ é um grupo Fuchsiano de índice finito de algum $\Gamma(\mathcal{A},\mathcal{O})$, então dizemos que $\Gamma$ é um *grupo Fuchsiano derivado da álgebra dos quatérnios* $\mathcal{A}$. Dois grupos $\Gamma_1$ e $\Gamma_2$ são *comensuráveis* se a intersecção $\Gamma_1\cap\Gamma_2$ tem índice finito em $\Gamma_1$ e $\Gamma_2$.

**Definição 3.3.1** *Se* $\Gamma$ *é comensurável para algum* $\Gamma(\mathcal{A},\mathcal{O})$, *então* $\Gamma$ *é chamado grupo Fuchsiano aritmético.*

**Observação 3.3.1** *Por definição um grupo Fuchsiano derivado de uma álgebra dos quatérnios $\mathcal{A}$ é um grupo Fuchsiano aritmético.*

Mostraremos a seguir que podemos caracterizar os grupos Fuchsianos aritméticos através do conjunto do traço de seus elementos

$$tr(\Gamma) = \{\pm tr(T) : T \in \Gamma\},$$

conforme o Teorema 3.3.2, que é o principal resultado desta seção.

Para cada corpo de números $\mathbb{K}$, vamos considerar

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

e

$$PSL(2,\mathbb{K}) = \frac{SL(2,\mathbb{K})}{\{\pm I_2\}}.$$

**Lema 3.3.1** *[27, Lemma 5.3.1, p.120] Seja $\Gamma$ um grupo Fuchsiano tal que $\mu(\mathbb{H}^2/\Gamma) < \infty$. Consideremos o conjunto formado pelos traços dos elementos de $\Gamma$ denotado por $tr(\Gamma)$ e suponhamos que $tr(\Gamma) \subset \mathbb{K}_1$, onde $\mathbb{K}_1$ é um corpo de números algébricos $[\mathbb{K}_1 : \mathbb{Q}] < \infty$. Então existem um corpo de números $\mathbb{K}$ e $h \in SL(2,\mathbb{K})$ tais que $h^{-1}\Gamma h \subseteq PSL(2,\mathbb{K})$.*

**Teorema 3.3.1** *[27, Theorem 5.3.2, p.122] Assumindo as hipóteses do Lema* 3.3.1*, consideremos $\mathbb{K}_1 = \mathbb{Q}(tr(T) : T \in \Gamma)$. Então,*

$$\mathcal{A}[\Gamma] = \mathbb{K}_1[\Gamma] = \left\{ \sum_{i=1}^{d} a_i T_i : a_i \in \mathbb{K}_1, T_i \in \Gamma \right\} \tag{3.13}$$

*é uma álgebra dos quatérnios sobre $\mathbb{K}_1$.*

**Demonstração:** *Como $\mu(\mathbb{H}^2/\Gamma) < \infty$, segue que $\Gamma$ é um grupo Fuchsiano do primeiro tipo e, portanto não elementar. Assim, pelo Lema* 3.3.1*, podemos assumir que $\Gamma$ contém os elementos*

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad T_1 = \begin{pmatrix} a_1 & 1 \\ c_1 & d_1 \end{pmatrix}, \quad (c_1 \neq 0 \ \ e\ \lambda \neq 1), \tag{3.14}$$

*e $\Gamma \subseteq PSL(2,\mathbb{K})$, onde $\mathbb{K} = \mathbb{K}_1(\lambda)$ é uma extensão quadrática de $\mathbb{K}_1$, ou seja, $[\mathbb{K} : \mathbb{K}_1] = 2$. Para simplificar a notação vamos indicar a álgebra $\mathcal{A}[\Gamma]$ por $\mathcal{A}$. Dessa forma, $\mathcal{A} \subset M_2(\mathbb{K})$ e $1 < dim_{\mathbb{K}_1}(\mathcal{A}) \leq 8$. Vamos mostrar agora que:*

1. $\mathcal{R} = \{0\}$,

2. $Z = \mathbb{K}_1$,

3. $dim_{\mathbb{K}_1}(\mathcal{A}) = 4$,

*onde $\mathcal{R}$ e $Z$ denotam o radical e o centro de $\mathcal{A}$, respectivamente. De fato:*

1. *Sejam $n \in \mathbb{N}$ e $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{R}$ tais que $T^n = 0$. Logo $det(T) = 0$, ou seja, $ad - bc = 0$, e daí $ab = bc$ e segue que $tr(T^n) = tr(T)^n$, ou ainda*

$$(a+d)^n = 0 \Leftrightarrow tr(T) = a + d = 0. \tag{3.15}$$

*Agora, como $\mathcal{R}$ é um ideal, temos que*

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda^{-1}c & \lambda^{-1}d \end{pmatrix} \in \mathcal{R} \Leftrightarrow \lambda a + \lambda^{-1}d = 0. \tag{3.16}$$

*Portanto, de (3.15) e (3.16), temos que $a = d = 0$. Analogamente,*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} aa_1 + bc_1 & a + bd_1 \\ ca_1 + dc_1 & c + dd_1 \end{pmatrix} \in \mathcal{R},$$

*logo $bc_1 + c = 0$ e $bc(c_1 - a_1d_1) = 0$. Daí $bc = 0 \Rightarrow b = c = 0$. Portanto, $\mathcal{R} = \{0\}$.*

2. *Consideremos agora $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z$. Como $TT_0 = T_0T$, obtemos*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} = \begin{pmatrix} a\lambda & b\lambda^{-1} \\ c\lambda & d\lambda^{-1} \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda^{-1}c & \lambda^{-1}d \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{3.17}$$

*e daí $b\lambda^{-1} = \lambda b$, $c\lambda = \lambda^{-1}c$, o que implica*

$$b\lambda^2 = b \Rightarrow b\lambda^2 - b = 0 \Rightarrow b(\lambda^2 - 1) = 0,$$

$$c\lambda^2 = c \Rightarrow c(\lambda^2 - 1) = 0.$$

*Disso segue que $b = c = 0$. Mas, $T$ também comuta com $T_1$, assim $a = d$. Por outro lado, para qualquer $T' \in \mathcal{A}$, $tr(T') \in \mathbb{K}_1$. Daí, $tr(T) = a + d = 2a$, implicando que $a \in \mathbb{K}_1$. Portanto,*

$$Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in \mathbb{K}_1 \right\} \cong \mathbb{K}_1.$$

*3. Finalmente, a dimensão de $\mathcal{A}$ sobre $\mathbb{K}$ é o quadrado de um inteiro. Logo $dim_{\mathbb{K}_1}(\mathcal{A}) = 4$.*■

**Lema 3.3.2** *[27, Lemma 5.3.3, p.122] Sejam $\Gamma$ um grupo Fuchsiano com $\mu(\mathbb{H}^2/\Gamma) < \infty$, $\mathbb{K}_1 = \mathbb{Q}(tr(T) : T \in \Gamma)$, $[\mathbb{K}_1 : \mathbb{Q}] < \infty$ e $tr(\Gamma) \subset I_{\mathbb{K}_1}$, onde $I_{\mathbb{K}_1}$ é o anel dos inteiros de $\mathbb{K}_1$. Então*

$$\mathcal{O}[\Gamma] = I_{\mathbb{K}_1}(\Gamma) = \left\{ \sum_{i=1}^{d} a_i T_i : a_i \in I_{\mathbb{K}_1}, T_i \in \Gamma \right\} \tag{3.18}$$

*é uma ordem da álgebra dos quatérnios $\mathcal{A}[\Gamma]$.*

Consideremos $T_0$ e $T_1$ como em (3.14). Verificamos que o conjunto $\{I_2, T_0, T_1, T_0T_1\}$ é uma base para a álgebra $\mathcal{A}(\Gamma)$ sobre $\mathbb{K}_1$. Consequentemente,

$$\mathcal{A}[\Gamma] = \left\{ \begin{pmatrix} a & b \\ b'c_1 & a' \end{pmatrix} : a, b \in \mathbb{K}, c_1 \in \mathbb{K}_1 \right\}, \tag{3.19}$$

onde $a', b'$ são os conjugados de $a$ e $b$ em $\mathbb{K} = \mathbb{K}_1(\lambda)$, respectivamente. A álgebra $\mathcal{A}[\Gamma]$ desempenhará um papel fundamental no estudo dos grupos aritméticos $\Gamma < \Gamma(\mathcal{A}, \mathcal{O})$.

**Lema 3.3.3** *[12, Lema 3.3.4, p.38] Seja $\Gamma$ um grupo Fuchsiano com $\mu(\mathbb{H}^2/\Gamma) < \infty$ satisfazendo as condições:*

1. *Seja $\mathbb{K}_1$ o corpo $\mathbb{Q}(tr(T) : T \in \Gamma)$. Então $\mathbb{K}_1$ é um corpo de números algébricos de grau finito, e $tr(\Gamma)$ está contido no anel dos inteiros de $\mathbb{K}_1$, $I_{\mathbb{K}_1}$;*

2. *Seja $\varphi$ um mergulho de $\mathbb{K}_1$ em $\mathbb{C}$ tal que $\varphi \neq Id$. Então $\varphi(tr(\Gamma))$ é limitado em $\mathbb{C}$.*

*Então $\mathbb{K}_1$ é um corpo de números totalmente real. Além disso, $\varphi(tr(\Gamma))$ está contido no intervalo $[-2, 2]$.*

**Proposição 3.3.1** *[12, Proposição 3.3.5, p.39] Seja $\varphi$ um mergulho de $\mathbb{K} = \mathbb{K}_1(\lambda)$ em $\mathbb{C}$ tal que $\varphi|_{\mathbb{K}_1} \neq Id$. Então, para qualquer elemento*

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

*temos que $|\varphi(a)| \leq 1$. Em particular, para*

$$T_1 = \begin{pmatrix} a_1 & 1 \\ c_1 & a_1' \end{pmatrix} \in \Gamma,$$

*obtemos* $\varphi(c_1) < 0$.

**Demonstração:** *Consideremos*

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in \Gamma.$$

*Como* $TT_0^n \in \Gamma$, *então pelo Lema* 3.3.3 *segue que*

$$|\varphi(tr(TT_0^n))| \leq 2. \tag{3.20}$$

*Usando o Lema* 3.3.3, *podemos mostrar que* $|\varphi(\lambda)| = 1$ *e* $\frac{1}{\lambda} = \lambda'$. *Desse modo, para* $a = a_0\lambda + a_1\lambda' \in \mathbb{K} = \mathbb{K}_1(\lambda)$,

$$\varphi(a') = \overline{\varphi(a)}, \tag{3.21}$$

*basta notar que* $\mathbb{K}_1$ *é um corpo de números totalmente real e* $\varphi(\lambda') = \overline{\varphi(\lambda)}$. *Por outro lado,*

$$\varphi(tr(TT_0^n)) = a\lambda^n + a'(\lambda')^n.$$

*Daí, usando* (3.21) *obtemos*

$$\varphi(tr(TT_0^n)) = \varphi(a\lambda^n) + \varphi(a'(\lambda')^n) = \varphi(a\lambda^n) + \overline{\varphi(a'(\lambda')^n)},$$

*isto é*

$$\varphi(tr(TT_0^n)) = 2Re(\varphi(a)\varphi(\lambda^n)).$$

*Logo, de* (3.20)

$$|Re(\varphi(a)\varphi(\lambda^n))| \leq 1. \tag{3.22}$$

*Como* $\varphi(\lambda^n) \neq 1$ *para todo* $n \in \mathbb{N}$, *o conjunto* $\{\varphi(\lambda)^m : m \in \mathbb{Z}\}$ *é um subgrupo denso de* $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. *Disso segue que* $|Re(\varphi(a)z))| \leq 1, \forall z \in S^1$. *Assim, de* (3.22) *obtemos que* $|\varphi(a)| \leq 1$. *Agora, aplicando o mesmo raciocínio ao elemento* $T_1$, *obtemos que* $|\varphi(a_1)| \leq 1$. *Por outro lado, temos que*

$$det(T_1) = a_1a_1' - c_1 = 1 \Leftrightarrow \varphi(c_1) = |\varphi(a_1)|^2 - 1 \leq 0.$$

*Mas sendo* $c_1 \neq 0$, *temos* $\varphi(c_1) < 0$. ∎

Seja $\mathbb{K}_1$ um corpo de números tal que $[\mathbb{K}_1 : \mathbb{Q}] = n$, e sejam

$$\varphi_i : \mathbb{K}_1 \longrightarrow \mathbb{R}$$

os monomorfismos de $\mathbb{K}_1$ em $\mathbb{R}$, $i = 1, \ldots, n$ e $\varphi_1$ a identidade. A partir de cada $\varphi_i$, consideremos o isomorfismo

$$\psi_i : \mathbb{K} \longrightarrow \mathbb{C},$$

onde $\mathbb{K} = \mathbb{K}_1(\lambda)$, $[\mathbb{K} : \mathbb{K}_1] = 2$. Logo,

$$\Psi_i : \mathcal{A}[\Gamma] \longrightarrow M_2(\mathbb{C})$$

definido por

$$\Psi_i(\alpha) = \begin{pmatrix} \psi_i(a) & \psi_i(b) \\ \psi_i(b'c) & \psi_i(a') \end{pmatrix},$$

onde $\alpha = \begin{pmatrix} a & b \\ b'c & a' \end{pmatrix}$ é um mergulho. Portanto,

$$\mathcal{A}^{\varphi_i} = \mathcal{A}^{\psi_i}\Psi_i\mathcal{A}[\Gamma] = \left\{ \begin{pmatrix} \psi_i(a) & \psi_i(b) \\ \psi_i(b'c) & \psi_i(a') \end{pmatrix} : a, b \in \mathbb{K} \right\},$$

onde $\mathcal{A}^{\varphi_i}$ é uma álgebra dos quatérnios sobre $\varphi_i(\mathbb{K}_1)$. Disso segue que

$$\mathcal{A}^{\varphi_1} \otimes \mathbb{R} \cong M_2(\mathbb{R}). \tag{3.23}$$

Por outro lado, usando a Proposição 3.3.1 e considerando que $\psi_i(a') = \overline{\psi_i(a)}$ para $i \neq 1$ temos

$$\mathcal{A}^{\varphi_i} \otimes \mathbb{R} \cong \mathbb{H},\ 2 \leq i \leq n. \tag{3.24}$$

Portanto, de (3.23) e (3.24) concluímos que $\mathcal{A}[\Gamma]$ satisfaz (3.7). Disso segue que $\mathcal{A}[\Gamma]$ é uma álgebra de divisão sobre $\mathbb{K}_1$. Encerramos este capítulo apresentando o resultado principal, pois a partir dele caracterizamos os grupos derivados de uma álgebra dos quatérnios.

**Teorema 3.3.2** *[27, Theorem 5.3.4, p.123] Seja $\Gamma$ um grupo Fuchsiano com $\mu(\mathbb{H}^2/\Gamma) < \infty$. Então $\Gamma$ é derivado de uma álgebra dos quatérnios $\mathcal{A}$ sobre um corpo de números $\mathbb{K}$ totalmente real se, e somente se, satisfaz as seguintes condições:*

1. *Seja $\mathbb{K}_1$ o corpo $\mathbb{Q}(tr(T) : T \in \Gamma)$. Então $\mathbb{K}_1$ é um corpo de números algébricos de grau finito, e $tr(\Gamma)$ está contido no anel de inteiros de $\mathbb{K}_1$, $I_{\mathbb{K}_1}$;*

2. *Seja $\varphi$ um mergulho de $\mathbb{K}_1$ em $\mathbb{C}$ tal que $\varphi \neq Id$. Então $\varphi(tr(\Gamma))$ é limitado em $\mathbb{C}$.*

**Demonstração:** *Suponhamos primeiro que $\Gamma$ seja um subgrupo de índice finito em $\Gamma(\mathcal{A}, \mathcal{O})$, ou seja, $\Gamma$ é derivado de uma álgebra dos quatérnios $\mathcal{A}$ sobre um corpo de números $\mathbb{K}$ totalmente real. Para qualquer $T \in \Gamma$, $tr(\Gamma) \in \mathbb{K}$. Mas, sendo $\mathbb{K}_1$ o corpo $\mathbb{Q}(tr(T) : T \in \Gamma)$, temos que $\mathbb{K}_1 \subset \mathbb{K}$. Portanto, $\mathbb{K}_1$ também é totalmente real. Agora, como $Trd(\mathcal{O}) \subset R_{\mathbb{K}}$, obtemos $tr(\Gamma) \subset I_{\mathbb{K}}$. Com isso segue a primeira condição. Consideremos agora um mergulho $\varphi_i$ de*

$\mathbb{K}_1$ *em* $\mathbb{C}$ *tal que* $\varphi \neq Id$. *Por* (3.9) *temos que* $\varphi_i(tr(\Gamma)) \subset Trd_{\mathbb{H}}(\rho_i\mathcal{O}^1)$, *para* $2 \leq i \leq n$, $[\mathbb{K}_1 : \mathbb{Q}] = n$. *Por outro lado, para qualquer* $\alpha \in \mathcal{O}^1$, *temos* $\varphi_i(Nrd(\alpha)) = Nrd_{\mathbb{H}}(\rho_i(\alpha))$. *Portanto,* $\rho_i(\mathcal{O}^1) \subset \mathbb{H}^1 = \{\alpha \in \mathbb{H} : Nrd_{\mathbb{H}}(\alpha) = 1\}$. *Mas pelo Exemplo* 3.1.2, *sabemos que* $Trd_{\mathbb{H}}(\mathbb{H}^1) = [-2, 2]$. *Desse modo,*

$$\varphi_i(tr(\Gamma)) \subset Trd_{\mathbb{H}}(\rho_i(\mathcal{O}^1)) \subset Trd_{\mathbb{H}}(\mathbb{H}^1) = [-2, 2],$$

*isto é,* $\varphi_i(tr(\Gamma)) \subset [-2, 2]$. *Logo,* $\varphi_i(tr(\Gamma))$ *é limitado em* $\mathbb{R}$. *Vamos mostrar que* $\mathbb{K} = \mathbb{K}_1$. *Suponhamos que* $\mathbb{K}$ *é uma extensão própria de* $\mathbb{K}_1$. *Dessa forma, existe um mergulho* $\varphi : \mathbb{K} \longrightarrow \mathbb{R}$, $\varphi \neq Id$ *tal que* $\varphi(\mathbb{K}_1) = \mathbb{K}_1$. *Portanto, pela definição de* $\mathbb{K}_1$, *obtemos* $\varphi(tr(\Gamma)) = tr(\Gamma) \subset [-2, 2]$. *Isso significa que* $\Gamma$ *não contém elementos hiperbólicos, o que contraria o fato de* $\Gamma$ *ser não elementar (por hipótese* $\mu(\mathbb{H}^2/\Gamma)$*). Portanto,* $\mathbb{K} = \mathbb{K}_1$, *e a segunda condição é satisfeita. Consideremos agora a recíproca. Em decorrência da Proposição* 3.3.1, *mostramos que a álgebra* $\mathcal{A}[\Gamma]$ *em* (3.17) *satisfaz as condições de* (3.7). *Por outro lado, temos que* $\Gamma$ *é um subgrupo de* $\Gamma(\mathcal{A}[\Gamma], \mathcal{O}[\Gamma])$. *Mas como* $\mathbb{H}^2/\Gamma$ *e* $\mathbb{H}^2/\Gamma(\mathcal{A}[\Gamma], \mathcal{O}[\Gamma])$ *tem covolume finito, segue que* $\Gamma$ *é um subgrupo de índice finito em* $\Gamma(\mathcal{A}[\Gamma], \mathcal{O}[\Gamma])$. *Portanto,* $\Gamma$ *é um grupo Fuchsiano derivado de uma álgebra dos quatérnios.* ∎

**Observação 3.3.2** *Na primeira condição do Teorema* 3.3.2, *o anel de inteiros algébricos de* $\mathbb{K}_1$, $I_{\mathbb{K}_1}$ *pode ser substituído por um anel* $R$ *tal que* $I_{\mathbb{K}_1} \subset R \subset \mathbb{K}_1$, *mas desde que* $\mathcal{O} = (a, b)_R$ *e* $\mathcal{A} = (a, b)_{\mathbb{K}_1}$.

### 3.3.1 Grupo Fuchsiano Aritmético $\Gamma_{4g}$

Nesta subseção o grupo Fuchsiano aritmético $\Gamma_{4g}$ é apresentado. No que segue o modelo do plano hiperbólico que será utilizado é o disco de Poincaré, por sua conveniência na visualização.

Vamos considerar a tesselação auto-dual $\{4g, 4g\}$, $g \geq 2$, e o polígono hiperbólico regular $P_{4g}$ com $4g$ arestas associado, que tessela o plano hiperbólico $\mathbb{D}^2$, tal que em cada vértice existem $4g$ polígonos $P_{4g}$, temos que $P_{4g}$ é uma região fundamental de $\Gamma_{4g}$.

Sem perda de generalidade assumimos que $P_{4g}$ está centrado na origem de $\mathbb{D}^2$ e consideramos as arestas ordenadas de forma cíclica como segue:

$$u_1, v_1, u_1', v_1', \ldots, u_g, v_g, u_g', v_g'. \tag{3.25}$$

As isometrias hiperbólicas $T_1, S_1, \ldots, T_g, S_g$ geradoras do grupo Fuchsiano $\Gamma_{4g}$ são tais que,

$$T_k(u_k) = u_k' \quad e \quad S_l(v_l) = v_l', \tag{3.26}$$

onde $k, l = 1, 2, \ldots g$.

Destes pareamentos resulta a superfície compacta orientável $\mathbb{D}^2/\Gamma_{4g}$ com gênero $g$. Assim, está associado com uma tesselação auto-dual $\{4g, 4g\}$ um polígono hiperbólico regular $P_{4g}$ que por sua vez está associado com um grupo Fuchsiano $\Gamma_{4g}$. Disto segue que a área hiperbólica é dada por

$$\mu(P_{4g}) = \mu(\mathbb{D}^2/\Gamma_{4g}) = 4\pi(g-1). \tag{3.27}$$

Se considerarmos agora uma transformação elíptica $T_C$ com ordem $4g$ cuja matriz associada é

$$\begin{pmatrix} e^{\frac{\pi Im}{4g}} & 0 \\ 0 & e^{\frac{-\pi Im}{4g}} \end{pmatrix}, \tag{3.28}$$

tal que $T_C(u_1) = v_1$ e $r_k$ é a potência de $T_C$ onde

$$T_{C^{r_k}}(u_1) \in \{u_k, v_k, u'_k, v'_k, k = 1, \ldots, g\}, \tag{3.29}$$

podemos escrever os geradores de $\Gamma_{4g}$ como conjugações de $T_1$ por meio de potências de $C$. Por exemplo, suponha que queremos determinar $T_2$ tal que $T_2(u_2) = u'_2$. Sabemos que $T_1(u_1) = u'_1$ e $T_{C^4}(u_1) = u_2$ pois $u_2$ está 4 arestas após $u_1$ como adotamos em (3.25). Logo, $T_{C^{-4}}(u_2) = u_1$. Portanto,

$$T_{C^4}(T_1(T_{C^{-4}}(u_2))) = T_{C^4}(u'_1) = u'_2, \tag{3.30}$$

isto é, $T_{C^4} \circ T_1 \circ T_{C^{-4}}(u_2) = u'_2$. Logo, obtemos $T_2 = T_{C^4} \circ T_1 \circ T_{C^{-4}}$. Portanto, de (3.26) e (3.29) segue que:

$$A_k = C^{4\lambda} A_1 C^{-4\lambda} \text{ e } B_l = C^{\nu} A_1 C^{-\nu}, \tag{3.31}$$

onde $A_k$ e $B_l$ são matrizes correspondentes às transformações $T_k$ e $S_l$, respectivamente, com $k, l = 1, \ldots g$, $\lambda = k - 1$ e $\nu = 4l - 3$.

Assim, uma vez obtido o gerador $T_1$ os outros geradores são obtidos por conjugação. Agora, por [11] temos o seguinte resultado:

**Proposição 3.3.2** *[11, Teorema 5.2.1, p.63] Os elementos $a, c$ da transformação $T_1$ associada à matriz $A_1 = \begin{pmatrix} a & c \\ \bar{c} & \bar{a} \end{pmatrix}$ são dados por*

$$|a| = tan\left(\frac{(2g-1)\pi}{4g}\right),\ arg(a) = -\frac{(g-1)\pi}{2g},$$

*e*

$$|c| = \sqrt{tan^2\left(\frac{(2g-1)\pi}{4g}\right) - 1},\ arg(c) = -\frac{(g-1)\pi}{4g}.$$

*As outras transformações hiperbólicas $T_k(u_k) = u'_k$ e $S_l(v_l) = v'_l$ que geram o grupo Fuchsiano hiperbólico $\Gamma_{4g}$ e também realizam os pareamentos de arestas restantes são obtidos pelas conjugações*

$$T_k = T_{C^{r_k}} \circ T_1 \circ T_{C^{-r_k}} \qquad e \qquad S_l = S_{C^{r_l}} \circ S_1 \circ S_{C^{-r_l}}.$$

## 3.4 Identificação de Grupos Fuchsianos $\Gamma_{4g}$ por Ordens dos Quatérnios

Nesta seção identificaremos os grupos Fuchsianos aritméticos $\Gamma_{4g}$ derivados de uma álgebra dos quatérnios $\mathcal{A}$ sobre um corpo de números $\mathbb{K}$, para $[\mathbb{K} : \mathbb{Q}] = 2^n$, $3.2^n$ e $5.2^n$, onde $[\mathbb{K} : \mathbb{Q}]$ é o gênero da superfície $\mathbb{D}^2/\Gamma_{4g}$ em uma ordem dos quatérnios.

**Teorema 3.4.1** *[12, Teorema 4.2.5, p.50] Para cada gênero $g = 2^n$, onde $n$ é um número natural qualquer, os elementos do grupo Fuchsiano $\Gamma_{4g}$ são identificados via isomorfismo com elementos da ordem $\mathcal{O} = (\theta, -1)_R$, onde*

$$R = \left\{ \frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta] \quad e \quad m \in \mathbb{N} \right\} \tag{3.32}$$

*e $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \sqrt{2}}}}$ contém $n$ radicais.*

**Teorema 3.4.2** *[12, Teorema 4.2.6, p.51] Para cada gênero $g = 2^n$, onde $n$ é um número natural qualquer, o grupo Fuchsiano $\Gamma_{4g}$ associado ao polígono regular $P_{4g}$, é derivado de uma álgebra de divisão dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, sobre $\mathbb{K} = \mathbb{Q}(\theta)$, onde $[\mathbb{K} : \mathbb{Q}] = 2^{n+1}$ e $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \sqrt{2}}}}$ contém $n$ radicais.*

Em particular, para $g = 2$ temos.

**Corolário 3.4.1** *[11, Seção 5.5, p.83] Dado $g = 2$ os elementos do grupo Fuchsiano $\Gamma_8$ são identificados via isomorfismo com elementos da ordem $\mathcal{O} = (\theta, -1)_{I_{\mathbb{K}}}$, onde $I_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$ denota o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ e $\theta = \sqrt{2}$.*

**Teorema 3.4.3** *[12, Teorema 4.3.2, p.56] Para cada gênero $g = 3.2^n$, onde $n$ é um número natural qualquer, os elementos do grupo Fuchsiano $\Gamma_{4g}$ são identificados via isomorfismo com elementos da ordem $\mathcal{O} = (\theta, -1)_R$, onde*

$$R = \left\{ \frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta] \quad e \quad m \in \mathbb{N} \right\} \tag{3.33}$$

*e $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \sqrt{3}}}}$ contém $n$ radicais.*

**Teorema 3.4.4** *[12, Teorema 4.3.3, p.56] Para cada gênero $g = 3.2^n$, onde $n$ é um número natural qualquer, o grupo Fuchsiano $\Gamma_{4g}$ associado ao polígono regular $P_{4g}$, é derivado de uma álgebra de divisão dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, sobre $\mathbb{K} = \mathbb{Q}(\theta)$, onde $[\mathbb{K} : \mathbb{Q}] = 2^{n+1}$ e $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \sqrt{3}}}}$ contém $n$ radicais.*

Em particular, para $g = 3$ temos.

**Corolário 3.4.2** *[11, Seção 5.6, p.93] Dado $g = 3$ os elementos do grupo Fuchsiano $\Gamma_{12}$ são identificados via isomorfismo com elementos da ordem $\mathcal{O} = (\theta, -1)_{I_{\mathbb{K}}}$, onde $I_{\mathbb{K}} = \mathbb{Z}[\sqrt{3}]$ denota o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ e $\theta = 3 + 2\sqrt{3}$.*

**Teorema 3.4.5** *[12, Teorema 4.4.2, p.61] Para cada gênero $g = 5.2^n$, onde $n$ é um número natural qualquer, os elementos do grupo Fuchsiano $\Gamma_{4g}$ são identificados via isomorfismo com elementos da ordem $\mathcal{O} = (\theta, -1)_R$, onde*

$$R = \left\{ \frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta] \quad e \quad m \in \mathbb{N} \right\} \tag{3.34}$$

*e $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \sqrt{5}}}}$ contém $n$ radicais.*

**Teorema 3.4.6** *[12, Teorema 4.4.3, p.61] Para cada gênero $g = 5.2^n$, onde $n$ é um número natural qualquer, o grupo Fuchsiano $\Gamma_{4g}$ associado ao polígono hiperbólico regular $P_{4g}$, é derivado de uma álgebra de divisão dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, sobre o corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$, $[\mathbb{K} : \mathbb{Q}] = 2^{n+1}$ e $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \sqrt{5}}}}$ contém $n$ radicais.*

Consequentemente, para qualquer um destes casos, $\{1, \sqrt{\theta}, Im, \sqrt{\theta}Im\}$ é uma $R$-base para o reticulado $\mathcal{O}$, onde $Im$ é a unidade imaginária.

A seguir, vamos verificar que os grupos Fuchsianos associados às ordens encontradas nos Teoremas 3.4.1, 3.4.3 e 3.4.5 são de fato aritméticos. Para isso, basta mostrar que a álgebra dos quatérnios é não ramificada em $\varphi_1$ e ramificada nos demais lugares.

Tomando o grupo Fuchsiano $\Gamma_{4g}$, dada uma álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, temos que os elementos $T \in \Gamma$ são dados na forma:

$$T = \frac{1}{2^s} \begin{pmatrix} x_l + y_l\sqrt{\theta} & z_l + w_l\sqrt{\theta} \\ -z_l + w_l\sqrt{\theta} & x_l - y_l\sqrt{\theta} \end{pmatrix}$$

onde $s \in \mathbb{N}$, $x_l, y_l, z_l, w_l \in \mathbb{Z}[\theta]$ e $\theta$ é dado por:

$$\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2}}}, \quad para \quad g = 2^n;$$

$$\theta = \sqrt{2 + \sqrt{2 + ... + \sqrt{3}}}, \quad para \quad g = 3.2^n;$$

e

$$\theta = \sqrt{2 + \sqrt{2 + ... + \sqrt{5}}}, \quad para \quad g = 5.2^n.$$

Como $\varphi_1$ é a identidade, segue que $\mathcal{A} \simeq M_2(\mathbb{K})$ é não ramificada em $\varphi_1$. Agora observe que $\theta$ não é um quadrado para $\mathbb{K} = \mathbb{Q}(\theta)$, ou seja, não existe $t \in \mathbb{K} - \{0\}$ tal que $t^2 = \theta$. Portanto, $\mathcal{A}$ é ramificada em todos os lugares $\varphi_i$, exceto em $\varphi_1$.

# Capítulo 4

# Códigos Geometricamente Uniformes Derivados de Grafos sobre Anéis dos Inteiros

Em [36] Golomb e Welch definem códigos perfeitos (close-packed) usando poliominos, dados por esferas de Lee de raio $t$, consideradas como regiões de Voronoi. Essas regiões tesselam o toro por translações e formam, portanto, códigos geometricamente uniformes. Em [3] toros planos foram usados com um objetivo similar, bem como conjuntos de sinais do tipo QAM considerados como códigos de classe lateral perfeitos com a distância de grafos induzida pela métrica euclidiana.

Em [4], [5] e [15] foi introduzida uma nova métrica, que se confunde com a métrica de Lee, proveniente da teoria de grafos sobre constelações do tipo QAM modeladas por inteiros Gaussianos, e em [5] sobre constelações hexagonais nas quais todo baricentro possui seis outros vizinhos (baricentros) com distância um modeladas por inteiros de Eisenstein-Jacobi [37]. Por outro lado, códigos de grupo perfeitos de comprimento um foram construídos resolvendo um problema teórico sobre grafos circulantes, qual seja o problema do conjunto perfeito de vértices dominantes. Neste capítulo propomos a construção de códigos quase-perfeitos, que além de preservarem a estrutura de um código geometricamente uniforme, corrigem alguns padrões de erros além da capacidade de correção dos códigos perfeitos, porém com uma menor cardinalidade.

## 4.1 Anéis Quocientes

Nesta seção definiremos anéis quocientes do anel dos inteiros de Gauss e de Eisenstein-Jacobi.

Tomando o corpo de números $\mathbb{K} = \mathbb{Q}[\sqrt{-1}] = \{a + b\sqrt{-1} | a, b \in \mathbb{Q}\}$, pelo Teorema 2.1.7 o anel dos inteiros de $\mathbb{K}$ é $\mathbb{Z}[\sqrt{-1}]$, chamado *anel dos inteiros de Gauss* e denotado por $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, onde $i = \sqrt{-1}$. Se $\alpha = a + bi \in \mathbb{Z}[i]$ sua norma é dada por

$$N(\alpha) = \alpha.\bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2,$$

ou seja, a norma é dada por uma forma quadrática $N$ tal que

$$\begin{aligned} N : \ \mathbb{Z}[i] &\longrightarrow \mathbb{Z}^+ \\ a + bi &\longmapsto a^2 + b^2. \end{aligned}$$

Agora, tomando o corpo de números $\mathbb{K} = \mathbb{Q}[\sqrt{-3}] = \{a + b\sqrt{-3} | a, b \in \mathbb{Q}\}$, pelo Teorema 2.1.8 o anel dos inteiros de $\mathbb{K}$ é $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, chamado *anel dos inteiros de Eisenstein-Jacobi* e denotado por $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$, onde $\omega = \left(\frac{-1+\sqrt{-3}}{2}\right)$. Podemos observar que $\omega$ é tal que $\omega^2 + \omega + 1 = 0$. Assim, se $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ sua norma é dada por

$$\begin{aligned} N(\alpha) = \alpha.\bar{\alpha} &= (a + b\omega)(a + b\omega^2) \\ &= (a + b\omega)((a - b) - b\omega) = a^2 + b^2 - ab, \end{aligned}$$

ou seja, a norma é dada por uma forma quadrática $N$ tal que

$$\begin{aligned} N : \ \mathbb{Z}[\omega] &\longrightarrow \mathbb{Z}^+ \\ a + b\omega &\longmapsto a^2 + b^2 - ab. \end{aligned}$$

Se $\langle\alpha\rangle$ denota o ideal de $\mathbb{Z}[\rho]$ gerado por $\alpha$, onde $\rho = i$ ou $\rho = \omega$, então o anel quociente $\frac{\mathbb{Z}[\rho]}{\langle\alpha\rangle}$, onde $\alpha \in \mathbb{Z}[\rho]$, será denotado por $\mathbb{Z}[\rho]_\alpha$. Da Proposição 2.1.9 segue que:

**Teorema 4.1.1** *Seja $0 \neq \alpha \in \mathbb{Z}[\rho]$, onde $\rho = i$ ou $\rho = \omega$. Então $\mathbb{Z}[\rho]_\alpha$ tem $N(\alpha)$ elementos.*

**Corolário 4.1.1** *Seja $0 \neq \alpha \in \mathbb{Z}[\rho]$, onde $\rho = i$ ou $\rho = \omega$.*

1. *Se $\beta \in \mathbb{Z}[\rho]$ é tal que $\beta | \alpha$, então o ideal $\langle\beta\rangle \subset \mathbb{Z}[\rho]_\alpha$ tem ordem $N(\alpha)/N(\beta)$;*

2. *Se $\beta \in \mathbb{Z}[\rho]$ é tal que $\beta \not| \alpha$ e $\gamma = mdc(\alpha, \beta)$, então o ideal $\langle\beta\rangle \subset \mathbb{Z}[\rho]_\alpha$ é gerado por $\gamma$ e tem ordem $N(\alpha)/N(\gamma)$.*

**Exemplo 4.1.1** *Dado $\alpha = 3 + 4i$, temos $N(\alpha) = 25$. Logo, pelo Teorema 4.1.1, $\mathbb{Z}[i]_{3+4i}$ tem 25 ele-*

*mentos, que são obtidos pelo quociente do anel $\mathbb{Z}[i]$ e o ideal $\langle 3 + 4i\rangle$, ou seja, tomamos os elementos de $\mathbb{Z}[i]$ e fazemos módulo $(3 + 4i)$, obtendo $\mathbb{Z}[i]_{3+4i} = \{0, 1, 2, 3, -1, -2, -3, i, 2i, 3i, -i,$ $-2i, -3i, 1 + i, 1 + 2i, 1 - i, 1 - 2i, -1 - i, -1 - 2i, -1 + i, -1 + 2i, 2 + i, -2 + i, 2 - i, -2 - i\}$.*

**Exemplo 4.1.2** *Dado $\alpha = 3+4\omega$, temos $N(\alpha) = 13$. Logo, pelo Teorema 4.1.1, $\mathbb{Z}[\omega]_{3+4\omega}$ tem 13 elementos, que são obtidos pelo quociente do anel $\mathbb{Z}[\omega]$ e o ideal $\langle 3+4\omega \rangle$, ou seja, tomamos os elementos de $\mathbb{Z}[\omega]$ e fazemos módulo $(3+4\omega)$, obtendo $\mathbb{Z}[\omega]_{3+4\omega} = \{0, 1, -1, \omega, -\omega, 1+\omega, -1-\omega, 2, -2, 2\omega, -2\omega, 2+2\omega, -2-2\omega\}$.*

## 4.2 Códigos sobre Grafos

A seguir veremos alguns conceitos sobre grafos e códigos sobre grafos, os quais serão usados na próxima seção.

**Definição 4.2.1** *Seja $0 \neq \alpha \in \mathbb{Z}[\rho]$. A distância sobre $\mathbb{Z}[\rho]_\alpha$ é a distância induzida pelo grafo $G_\alpha$. Assim, se $\eta,\ \tau \in Z[\rho]_\alpha$, a distância $D_\alpha$ é dada por:*

1. *$D_\alpha(\eta, \tau) = min\{|x| + |y|\}$, tal que $\tau - \eta \equiv x + yi\ (mod\ \alpha)$, onde $\rho = i$.*

2. *$D_\alpha(\eta, \tau) = min\{|x| + |y| + |z|\}$, tal que $\tau - \eta \equiv x + y\omega + z\omega^2\ (mod\ \alpha)$, onde $\rho = \omega$.*

**Exemplo 4.2.1** *Novamente no Exemplo 4.1.1, para $V = \mathbb{Z}[i]_{3+4i}$. Se $\tau = 1+2i$ e $\eta = -1$, temos $\tau - \eta = 2+2i$, logo $D_\alpha(\eta, \tau) = 2+2 = 4$. Se $\tau = 1+2i$ e $\eta = -3i$, temos $\tau - \eta = 1+5i \equiv -2-i(mod\ \alpha)$, logo $D_\alpha(\eta, \tau) = 2+1 = 3$.*

**Exemplo 4.2.2** *Novamente no Exemplo 4.1.2, para $V = \mathbb{Z}[\omega]_{3+4\omega}$. Se $\tau = \omega$ e $\eta = -\omega$, temos $\tau - \eta = 2\omega$, logo $D_\alpha(\eta, \tau) = 2$. Se $\tau = 1+\omega$ e $\eta = -1$, temos $\tau - \eta = 2+\omega \equiv -2(mod\ \alpha)$, logo $D_\alpha(\eta, \tau) = 2$.*

Dada a distância $D_\alpha$, definimos um grafo gerado por $\alpha$, para $\alpha \in \mathbb{Z}[\rho]$.

**Definição 4.2.2** *Seja $0 \neq \alpha \in \mathbb{Z}[\rho]$, onde $\rho = i$ ou $\rho = \omega$. O grafo gerado por $\alpha$, denotado por $G_\alpha = (V, E)$, é definido por:*

1. *$V = \mathbb{Z}[\rho]_\alpha$ é o conjunto de vértices;*

2. *$E = \{(\eta, \tau) \in V \times V : D_\alpha(\eta, \tau) = 1\}$ é o conjunto de arestas.*

**Exemplo 4.2.3** *No Exemplo 4.1.1, temos que o conjunto de vértices é $V = \mathbb{Z}[i]_{3+4i}$ e o conjunto de arestas satisfaz E.*

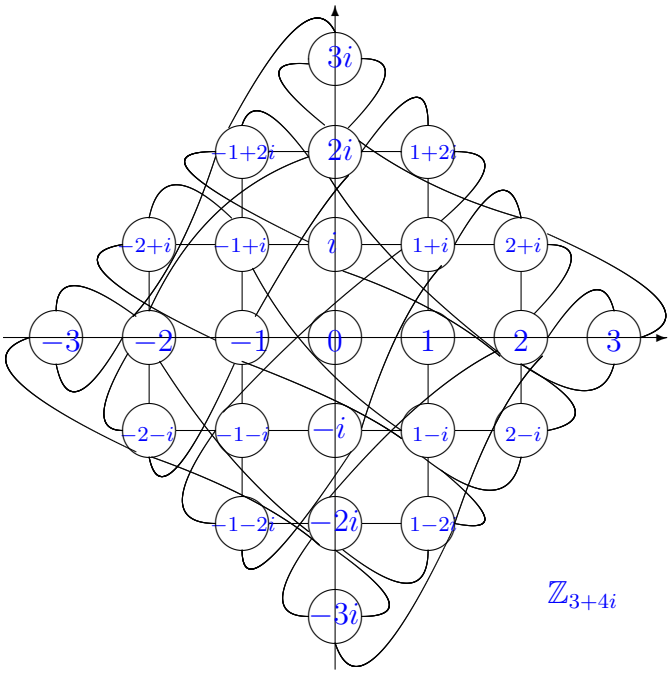


Figura 4.1: Grafo gerado por $3 + 4i$

**Exemplo 4.2.4** *No Exemplo 4.1.2, temos que o conjunto de vértices é* $V = \mathbb{Z}[\omega]_{3+4\omega}$ *e o conjunto de arestas satisfaz E.*

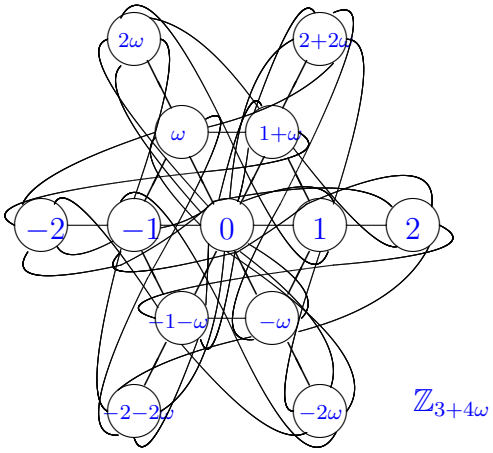


Figura 4.2: Grafo gerado por $3 + 4\omega$

**Observação 4.2.1** *Note que a distância entre dois pontos* $\eta$ *e* $\tau$ *no grafo, nada mais é do que o menor número de arestas necessárias para ligar o ponto* $\eta$ *ao ponto* $\tau$*.*

Dado um grafo $G_\alpha$ com conjunto de vértices $V$ e distância $D_\alpha$, um *código* em $G_\alpha$ é um subconjunto não vazio $\mathcal{C}$ de $G_\alpha$. A região de Voronoi $V_\eta$ associada com $\eta \in \mathcal{C}$ é o subconjunto formado pelos elementos de $V$ para os quais $\eta$ é o ponto mais próximo em $\mathcal{C}$, ou seja, $V_\eta = \{\tau \in V; D(\eta, \tau) = D(\eta, \mathcal{C})\}$. O número $t = max\{D(\eta, \mathcal{C}); \eta \in V\}$ é chamado *raio de cobertura* do código. O raio de cobertura é o menor número $t$ tal que as bolas de raio $t$ centradas nos pontos de $\mathcal{C}$, dadas por $B_t(\eta) = \{\tau \in V : D(\eta, \tau) \leq t\}$ cobrem $V$. O número $\delta = min\{D(\eta, \tau) : \eta, \tau \in \mathcal{C}, \eta \neq \tau\}$ é a distância mínima de $\mathcal{C}$, e $\delta \leq 2t + 1$, a igualdade vale quando as bolas de

raio $t$ centradas nos pontos de $\mathcal{C}$ formam uma partição de $V$. Um código com esta propriedade é chamado *perfeito* e é dito corrigir $t$ erros. Na busca por esses códigos voltamos à teoria de grafos para descrever tais bolas e, assim, as partições do conjunto $V$.

**Definição 4.2.3** *Um vértice $\eta$ de um grafo $G$ é dito $t$-dominar outro vértice $\tau$ se $D(\eta, \tau) \leq t$, onde $D$ denota a distância do grafo. Então, um subconjunto $S$ de vértices é chamado um conjunto $t$-dominante se todo vértice de $G$ é $t$- dominado por um único vértice em $S$.*

O próximo teorema fornece um procedimento para a obtenção destes conjuntos no caso do anel dos inteiros de Gauss:

**Teorema 4.2.1** *[3][5][15] Seja $0 \neq \alpha \in \mathbb{Z}[i]$ e $t$ um inteiro positivo. Temos que:*

1. *Se $\beta = t + (t+1)i$ divide $\alpha$, então o ideal $S = \langle \beta \rangle \subseteq \mathbb{Z}[i]_\alpha$ é um conjunto perfeito $t$-dominante em $G_\alpha$;*

2. *Se $\bar{\beta} = t - (t+1)i$ divide $\alpha$, então o ideal $S = \langle \bar{\beta} \rangle \subseteq \mathbb{Z}[i]_\alpha$ é um conjunto perfeito $t$-dominante em $G_\alpha$.*

Observe que dado $\beta$ tal que $\beta = t \pm (t+1)i$, sua norma $N(\beta) = 2t^2 + 2t + 1$ resulta no número de pontos da região de Voronoi, que pode então ser vista como uma esfera de Lee de raio $t$, onde cada ponto do grafo é uma célula da esfera.

Analogamente, obtemos um procedimento para o caso do anel dos inteiros de Eisenstein-Jacobi:

**Teorema 4.2.2** *[3][15] Seja $0 \neq \alpha \in \mathbb{Z}[\omega]$ e $t$ um inteiro positivo. Temos que:*

1. *Se $\beta = t + (2t+1)\omega$ divide $\alpha$, então o ideal $S = \langle \beta \rangle \subseteq \mathbb{Z}[\omega]_\alpha$ é um conjunto perfeito $t$-dominante em $G_\alpha$;*

2. *Se $-\bar{\beta} = (t+1) + (2t+1)\omega$ divide $\alpha$, então o ideal $S = \langle -\bar{\beta} \rangle = \langle \bar{\beta} \rangle \subseteq \mathbb{Z}[\omega]_\alpha$ é um conjunto perfeito $t$-dominante em $G_\alpha$.*

Novamente, dado $\beta$ tal que $\beta$ é da forma $t + (2t+1)\omega$ ou $(t+1) + (2t+1)\omega$, sua norma $N(\beta) = 3t^2 + 3t + 1$ resulta no número de pontos da região de Voronoi, que agora é dada por hexágonos de raio $t$.

Podemos observar que os procedimentos para obtenção de códigos perfeitos sobre os anéis dos inteiros apresentados são análogos e podem ser facilmente estendidos para outros anéis de inteiros, obtendo outras constelações.

## 4.3 Códigos Perfeitos Derivados de Grafos sobre Anéis dos Inteiros

Nesta seção vamos definir códigos perfeitos e ver exemplos sobre os anéis dos inteiros de Gauss e de Einsenstein-Jacobi.

Um código $\mathcal{C}$ é chamado *perfeito* se as bolas de raio $t$ centradas nos pontos de $\mathcal{C}$ particionam o conjunto de pontos $V$, ou seja, é um código que corrige todos os padrões com até $t$ erros e nenhum padrão com $t+1$ erros ou mais. Dado um conjunto perfeito $t$-dominante $S$ como nos Teoremas 4.2.1 e 4.2.2, podemos observar que ele forma um código perfeito.

**Exemplo 4.3.1** *Dado $\alpha = 6+7i$, temos $N(\alpha) = 6^2+7^2 = 85$. Logo, pelo Teorema 4.1.1, $\mathbb{Z}[i]_{6+7i}$ tem 85 elementos. Agora, $\alpha = 6+7i$ pode ser escrito como $6+7i = (-i)(1+2i)(1+4i)$, e se tomarmos $\beta$ como no Teorema 4.2.1 temos o gerador do conjunto perfeito $t$-dominante. Assim, $\beta = 1+2i$ satisfaz estas condições, e disso segue que o ideal $\langle\beta\rangle = \langle 1+2i\rangle$ é um conjunto perfeito 1-dominante em $G_{6+7i}$. Portanto, o código perfeito que corrige todos os padrões com 1 erro e nenhum padrão com 2 ou mais erros, pelo Corolário 4.1.1 possui $\frac{N(\alpha)}{N(\beta)} = \frac{85}{5} = 17$ elementos, é dado por $S = \{0, 1+2i, 2+4i, -3-i, -2+i, -1+3i, 5i, -5, -4+2i, -1-2i, -2-4i, 3+i, 2-i, 1-3i, -5i, 5, 4-2i\}$ e é identificado no grafo pelos pontos duplamente circulados, formando os baricentros dos 17 polígonos fundamentais (contendo 5 elementos) que recobrem a constelação de sinais, esta contendo os 85 elementos de $\mathbb{Z}_{6+7i}$, como ilustrado na Figura 4.3.*

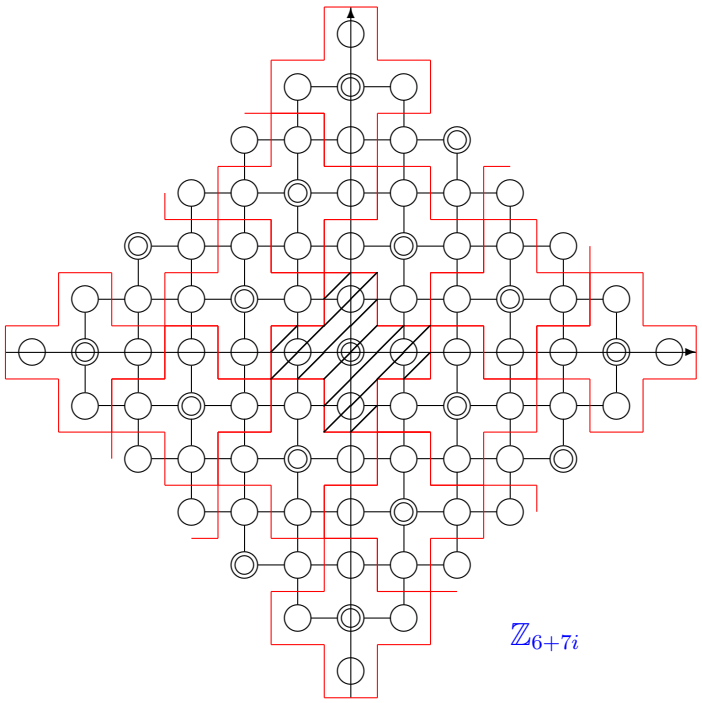


Figura 4.3: Código Perfeito 1-dominante em $G_{6+7i}$

**Exemplo 4.3.2** *Dado* $\alpha = -8 - 3\omega$, *temos* $N(\alpha) = (-8)^2 + (-3)^2 - 24 = 49$. *Logo, pelo Teorema 4.1.1,* $\mathbb{Z}[\omega]_{-8-3\omega}$ *tem* 49 *elementos. Agora,* $\alpha = -8 - 3\omega$ *pode ser escrito como* $-8 - 3\omega = (1 + 3\omega)^2$, *e se tomarmos* $\beta$ *como no Teorema 4.2.2 temos o gerador do conjunto perfeito t-dominante. Assim,* $\beta = 1 + 3\omega$ *satisfaz estas condições, e disso segue que o ideal* $\langle\beta\rangle = \langle 1+3\omega\rangle$ *é um conjunto perfeito* 1*-dominante em* $G_{-8-3\omega}$. *Portanto, o código perfeito que corrige todos os padrões com 1 erro e nenhum padrão com 2 ou mais erros, pelo Corolário 4.1.1 possui* $\frac{N(\alpha)}{N(\beta)} = \frac{49}{7} = 7$ *elementos, é dado por* $S = \{0, 1+3\omega, -3-2\omega, -2+\omega, 2-\omega, 3+2\omega, -1-3\omega\}$ *e é identificado no grafo pelos pontos duplamente circulados, formando os baricentros dos 7 polígonos fundamentais (contendo 7 elementos) que recobrem a constelação de sinais, esta contendo os* 49 *elementos de* $\mathbb{Z}_{-8-3\omega}$, *como ilustrado na Figura* 4.4.

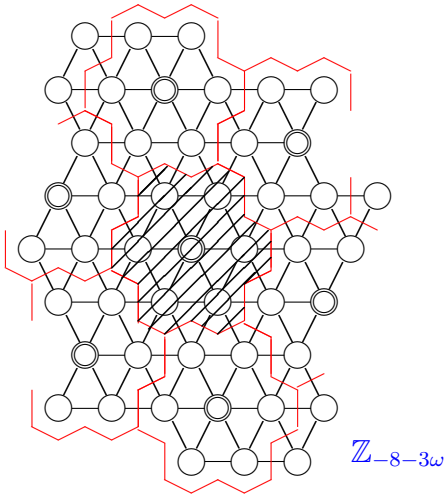


Figura 4.4: Código Perfeito 1-dominante em $G_{-8-3\omega}$

## 4.4 Códigos Quase-Perfeitos Derivados de Grafos sobre Anéis dos Inteiros Gaussianos

Nesta seção definiremos códigos quase-perfeitos, veremos um resultado construtivo para obtermos tais códigos derivados de grafos sobre o anel dos inteiros de Gauss e mostraremos que com certas propriedades estes códigos são únicos.

Um código é dito *quase-perfeito* se o mesmo é capaz de corrigir todos os padrões com até $t$ erros e alguns padrões com $t + 1$ erros.

Até aqui observamos que escolhendo $\beta$ divisor de $\alpha$ tal que $\beta$ é da forma $t + (t + 1)i$ ou $t - (t + 1)i$, obtemos um código perfeito, e a constelação de pontos é coberta por regiões fundamentais cujo raio de cobertura tem valor no máximo $t$, ou seja, as regiões fundamentais são constituídas por esferas de Lee de raio $t$. Assim, códigos perfeitos são obtidos através de

translações de esferas de Lee de raio $t$, onde $t \leq r$. Como observado em [36], uma esfera de Lee de raio $r$ em $\mathbb{Z}^2$ possui $2r^2 + 2r + 1$ pontos. Agora, se tomarmos um $\beta$ divisor de $\alpha$, que não contenha nenhuma das formas $t + (t+1)i$ ou $t - (t+1)i$, podemos obter um novo código, não mais perfeito, mas que cobre a constelação de pontos por regiões fundamentais idênticas, e mantendo as propriedades de um código geometricamente uniforme. Nesta busca, chegamos ao seguinte procedimento.

**Teorema 4.4.1** *Seja $0 \neq \alpha \in \mathbb{Z}[i]$ e $t$ um inteiro positivo. Temos que:*

1. *Se $\beta = (t-c) + (t + (c+1))i$ divide $\alpha$, então o ideal $S = \langle \beta \rangle \subseteq \mathbb{Z}[i]_\alpha$ forma um código quase-perfeito que corrige todos os padrões com até $t$ erros e $2c^2 + 2c$ padrões com $t+1$ erros em $G_\alpha$;*

2. *Se $\bar{\beta} = (t-c) - (t + (c+1))i$ divide $\alpha$, então o ideal $S = \langle \bar{\beta} \rangle \subseteq \mathbb{Z}[i]_\alpha$ forma um código quase-perfeito capaz de corrigir todos os padrões com até $t$ erros e $2c^2 + 2c$ padrões com $t+1$ erros em $G_\alpha$.*

**Demonstração:**

*Pelo Corolário 4.1.1 temos que se $\beta$ é um divisor de $\alpha$, então $S = \langle \beta \rangle$ tem ordem $N(\alpha)/N(\beta)$, ou seja, $S$ tem $N(\alpha)/N(\beta)$ elementos. Ainda, tomando $\alpha = a + bi \in \mathbb{Z}[i]$, temos que $N(\alpha) = a^2 + b^2$.*

1. *Dado $\beta$ divisor de $\alpha$ tal que $\beta = (t-c)+(t+(c+1))i$, temos que $N(\beta) = (t-c)^2+(t+(c+1))^2 = 2t^2+2t+1+(2c^2+2c)$. Vamos provar que, se $\beta_1, \beta_2 \in S$, então $D_\alpha(\beta_1, \beta_2) \geq 2t+1$. Sejam $\beta_1, \beta_2 \in \langle \beta \rangle$, então $\beta_1 = \alpha_1\beta$ e $\beta_2 = \alpha_2\beta$, com $\alpha_1, \alpha_2 \in \mathbb{Z}[i]$. Temos que mostrar que $D_\alpha(\beta_1, \beta_2) = D_\alpha(\alpha_1\beta, \alpha_2\beta) = D_\alpha((\alpha_1 - \alpha_2)\beta, 0) \geq 2t+1$. Observe que é suficiente provar que para qualquer $\eta \in \mathbb{Z}[i]$ tal que $\eta\beta \not\equiv 0 (mod\ \alpha)$ implica $D_\alpha(\eta\beta, 0) \geq 2t+1$. É claro que para $\eta = \{1, i, -1, -i\}$, $D_\alpha(\eta\beta, 0) = 2t+1$. Suponhamos por absurdo que $D_\alpha(\eta\beta, 0) < 2t+1$. Então $\eta\beta \equiv x + yi (mod\ \alpha)$, com $|x| + |y| < 2t+1$ mínimo. Assim, $\eta\beta = (x+yi)+\gamma_1\alpha = (x+yi)+\gamma_2\alpha$, onde $\gamma_1, \gamma_2 \in \mathbb{Z}[i]$ e como $\beta|\alpha$, então $x+yi = \beta(\eta-\gamma_2)$. Agora, $N(x+yi) \leq 4t^2$ pois $|x| + |y| < 2t+1$. Como $N(\beta) = 2t^2 + 2t + 1 + (2c^2 + 2c) > 2t^2$ para $t > 0$, $c \in \mathbb{Z}$, então $N(\eta - \gamma_2) = 1$. Consequentemente, $x + yi = \beta u$, com $u \in \{1, i, -1, -i\}$. Então, em qualquer caso, $|x| + |y| = 2t+1$, que é uma contradição. Portanto, $D_\alpha(\beta_1, \beta_2) \geq 2t+1$.*

   *Agora, $2t^2 + 2t + 1$ é o número de pontos de uma esfera de Lee de raio $t$, logo cada uma das $N(\alpha)/N(\beta)$ regiões de Voronoi com centro nos pontos dados por $S$ tem exatamente*

$2t^2 + 2t + 1$ *pontos de distância até* $t$ *e* $2c^2 + 2c$ *pontos com distância* $t + 1$*, formando assim um código quase perfeito que corrige* $2t^2 + 2t + 1$ *padrões com até* $t$ *erros e* $2c^2 + 2c$ *padrões com* $t + 1$ *erros.*

2. *Dado* $\beta$ *divisor de* $\alpha$ *tal que* $\beta = (t - c) - (t + (c + 1))i$*, temos que* $N(\beta) = (t - c)^2 + (t + (c + 1))^2 = 2t^2 + 2t + 1 + (2c^2 + 2c)$*, portanto a demonstração é análoga.*

■

**Observação 4.4.1** *Códigos perfeitos podem ser vistos como um caso particular de códigos quase-perfeitos, note que tomando* $c = 0$ *no Teorema 4.4.1 obtemos o Teorema 4.2.1.*

**Exemplo 4.4.1** *Voltando ao Exemplo 4.3.1, vimos que* $\alpha = 6+7i$ *pode ser escrito como* $6+7i = (-i)(1 + 2i)(1 + 4i)$ *e* $N(\alpha) = 85$*. Se tomarmos* $\beta = 1 + 4i$ *como gerador do ideal, ele tem a forma* $\beta = (t-1)+(t+2)i$*, e obtemos um código quase-perfeito que corrige todos os padrões com* $t = 2$ *erros e* $4$ *padrões com* $3$ *erros, pois temos que* $N(\beta) = 17$ *e a maior esfera de Lee contida em* $17$ *pontos possui* $13$ *pontos com raio de cobertura* $2$*, logo restam* $4$ *pontos para completarmos os* $17$*. Assim, obtemos uma região fundamental que cobre* $17$ *pontos. Logo,* $S = \langle\beta\rangle$ *tem ordem* $N(\alpha)/N(\beta) = \frac{85}{17} = 5$ *e o código quase-perfeito, que corrige todos os padrões com* $2$ *erros e* $4$ *padrões com* $3$ *erros, dado por* $S = \{0, 1+4i, -4+i, 4-i, -1-4i\}$ *é identificado no grafo pelos pontos duplamente circulados, formando os baricentros dos 5 polígonos fundamentais contendo 17 elementos que recobrem a constelação de sinais contendo os 85 elementos de* $\mathbb{Z}_{6+7i}$*, como ilustrado na Figura* 4.5.

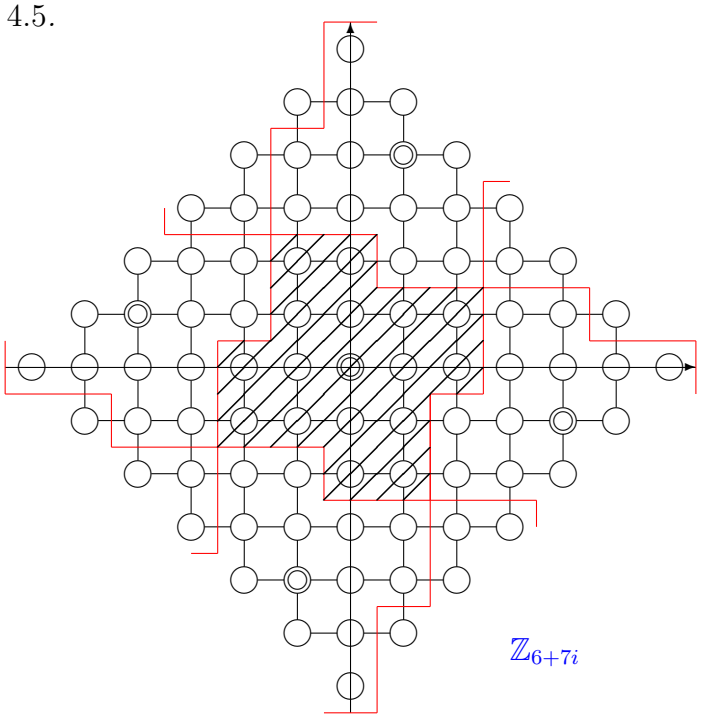


Figura 4.5: Código quase-perfeito sobre $\mathbb{Z}_{6+7i}$

**Exemplo 4.4.2** *Dado* $\alpha = 8 + 9i$*, temos que* $N(\alpha) = 145$*. Logo pelo Teorema 4.1.1,* $\mathbb{Z}[i]_{8+9i}$ *possui 145 elementos. Como* $8 + 9i = (-1)(1 - 2i)(2 - 5i)$*, se tomarmos* $\beta = 2 - 5i$ *como gerador do ideal, ele tem a forma* $\beta = (t-1)+(t+2)i$*, logo forma um código quase-perfeito que corrige todos os padrões com* $t = 3$ *erros e* 4 *padrões com* 4 *erros. Como* $N(\beta) = 29$ *e a maior esfera de Lee possui* 25 *elementos com raio de cobertura* 3*, restam* 4 *elementos para completar os* 29*. Assim, obtemos uma região fundamental contendo* 29 *elementos. Logo,* $S = \langle\beta\rangle$ *tem ordem* $N(\alpha)/N(\beta) = \frac{145}{29} = 5$ *e o código quase-perfeito, que corrige todos os padrões com* 3 *erros e* 4 *padrões com* 4 *erros é dado por* $S = \{0, 2-5i, -5-2i, 5-2i, -2+5i\}$ *e é identificado no grafo pelos pontos escuros, formando os baricentros dos polígonos fundamentais contendo 29 elementos que recobrem a constelação de sinais contendo os 145 elementos de* $\mathbb{Z}_{8+9i}$*, como ilustrado na Figura* 4.6.

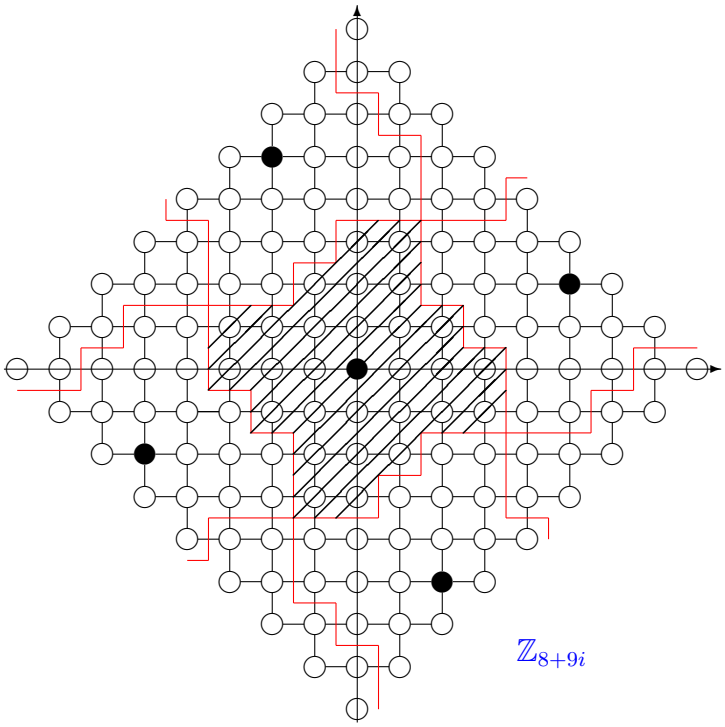


Figura 4.6: Código quase-perfeito sobre $\mathbb{Z}_{8+9i}$

Nesta seção apresentamos um resultado para a obtenção de códigos geometricamente uniformes quase-perfeitos derivados de grafos sobre anéis de inteiros de Gauss, cujas palavras códigos são elementos do ideal $S = \langle\beta\rangle \subseteq \mathbb{Z}[i]_\alpha$. Além disso, se garantirmos a propriedade de ser um ideal do anel, podemos mostrar que estes códigos são únicos. Para tal, necessitamos introduzir o seguinte resultado:

**Lema 4.4.1** *[5] Seja* $0 \neq \alpha \in \mathbb{Z}[i]$ *e* $t$ *um inteiro positivo. Para todo* $\eta \in \mathbb{Z}[i]_\alpha$ *temos que:*

$$B_t(\eta) \cap B_t(0) = \emptyset \Leftrightarrow D_\alpha(\eta, 0) \geq 2t + 1.$$

Pelo Corolário 4.1.1 e o Lema 4.4.1 podemos provar a unicidade dos códigos quase-perfeitos dados, como veremos a seguir:

**Teorema 4.4.2** *Seja $0 \neq \alpha \in \mathbb{Z}[i]$ e $t$ um inteiro positivo. Se existe um código ideal quase-perfeito que corrige todos os padrões com até $t$ erros e $2c^2+2c$ padrões com $t+1$ erros sobre $\mathbb{Z}[i]_\alpha$, então ele deve ser o grupo gerado por $(t-c)+(t+(c+1))i$ ou $(t-c)-(t+(c+1))i$.*
**Demonstração:** *Dado um código quase-perfeito que corrige todos os padrões com até $t$ erros e $2c^2+2c$ padrões com $t+1$ erros sobre $\mathbb{Z}[i]_\alpha$, ele possui $\frac{N(\alpha)}{2t^2+2t+(2c^2+2c+1)}$ elementos. Como estamos em um domínio de ideais principais, este código deve ser gerado por um elemento $\beta \in \mathbb{Z}[i]$ divisor de $\alpha$, tal que $N(\beta) = 2t^2+2t+(2c^2+2c+1)$, pelo Corolário 4.1.1. Assim, se $\beta$ é da forma $a+bi$, devemos ter $a^2+b^2 = 2t^2+2t+(2c^2+2c+1)$. Vamos mostrar que $|a|+|b| = 2t+1$. Suponhamos por absurdo que $|a|+|b| < 2t+1$, logo $D_\alpha(\beta,0) \leq |a|+|b| < 2t+1$, e pelo Lema 4.4.1 segue que $B_t(\eta) \cap B_t(0) \neq \emptyset$, que é um absurdo pois $\beta$ e $0$ são elementos do código. Agora, suponhamos que $|a|+|b| > 2t+1$, então temos que $|a|+|b| > 2t+1$ e $a^2+b^2 = 2t^2+2t+(2c^2+2c+1)$, assim $|a| > 2t+1-|b|$, logo $|a|^2 > (2t+1)^2-2(2t+1)|b|+|b|^2$ e pela segunda equação segue que $2t^2+2t+(2c^2+2c+1) = a^2+b^2 > (2t+1)^2-2(2t+1)|b|+|b|^2+|b|^2$, de onde obtemos $t^2+t-(2t+1+|b|)|b| < 0$, que é um absurdo pois $t, c$ e $b$ são inteiros. Portanto, $|a|+|b| = 2t+1$. Assim, temos que $\beta = a+bi$, com $|a|+|b| = 2t+1$ e $a^2+b^2 = 2t^2+2t+(2c^2+2c+1)$, de onde segue que $|a| = (t-c)$ e $|b| = (t+(c+1))$ ou $|a| = (t+(c+1))$ e $|b| = (t-c)$, ou seja, $\beta$ é da forma $(t-c)+(t+(c+1))i$ ou $(t-c)-(t+(c+1))i$, a menos de associados.*

■

## 4.5 Códigos Quase-Perfeitos Derivados de Grafos sobre Anéis dos Inteiros de Einsenstein-Jacobi

Nesta seção veremos como construir códigos quase-perfeitos derivados de grafos sobre o anel dos inteiros de Einsenstein-Jacobi.

Analogamente ao caso do anel dos inteiros de Gauss, podemos observar que escolhendo $\beta$ divisor de $\alpha$ tal que $\beta$ é da forma $t+(2t+1)\omega$ ou $(t+1)+(2t+1)\omega$, obtemos um código perfeito, e a constelação de pontos é coberta por regiões fundamentais cujo raio de cobertura tem valor no máximo $t$, ou seja, as regiões fundamentais são agora constituídas por hexágonos de raio $t$. Assim, códigos perfeitos são obtidos através de translações de hexágonos de raio $t$, onde $t \leq r$.

Neste caso, um hexágono de raio $r$ possui $3r^2+3r+1$ pontos. Agora, se tomarmos um $\beta$ divisor de $\alpha$, que não contenha nenhuma das formas $t+(2t+1)\omega$ ou $(t+1)+(2t+1)\omega$, podemos obter um novo código, não mais perfeito, mas que cobre a constelação de pontos por regiões fundamentais idênticas, e mantendo as propriedades de um código geometricamente uniforme. Nesta busca, chegamos ao seguinte procedimento.

**Teorema 4.5.1** *Seja $0 \neq \alpha \in \mathbb{Z}[\omega]$ e $t$ um inteiro positivo. Temos que:*

1. *Se $\beta = (t+2c+1)+(2t+1)\omega$ ou $\beta = (t-2c)+(2t+1)\omega$ divide $\alpha$, então o ideal $S = \langle\beta\rangle \subseteq \mathbb{Z}[\omega]_\alpha$ forma um código quase-perfeito que corrige todos os padrões com até $t$ erros e $4c^2+2c$ padrões com $t+1$ erros em $G_\alpha$;*

2. *Se $\beta = (t+2c)+(2t+1)\omega$ ou $\beta = (t-2c+1)+(2t+1)\omega$ divide $\alpha$, então o ideal $S = \langle\bar{\beta}\rangle \subseteq \mathbb{Z}[\omega]_\alpha$ forma um código quase-perfeito capaz de corrigir todos os padrões com até $t$ erros e $4c^2-2c$ padrões com $t+1$ erros em $G_\alpha$.*

**Demonstração:** *Pelo Corolário 4.1.1 temos que se $\beta$ é um divisor de $\alpha$, então $S = \langle\beta\rangle$ tem ordem $N(\alpha)/N(\beta)$, ou seja, $S$ tem $N(\alpha)/N(\beta)$ elementos. Ainda, tomando $\alpha = a+b\omega \in \mathbb{Z}[\omega]$, temos que $N(\alpha) = a^2+b^2-ab$.*

1. *Dado $\beta$ divisor de $\alpha$ tal que $\beta = (t+2c+1)+(2t+1)\omega$ ou $\beta = (t-2c)+(2t+1)\omega$, temos que $N(\beta) = 3t^2+3t+1+(4c^2+2c)$. Primeiro, vamos provar que $\beta$ é tal que $D_\alpha(\beta,0) = 2t+1$. Como $\beta = (t+2c+1)+(2t+1)\omega \equiv (t-2c)\omega+(t+2c+1)(1+\omega) = (t-2c)\omega-(t+2c+1)\omega^2 (mod\ \alpha)$ com $|t-2c|+|t+2c+1| = 2t+1$, e $\beta = (t-2c)+(2t+1) \equiv (t+2c+1)\omega+(t-2c)(1+\omega) = (t+2c+1)\omega-(t-2c)\omega^2 (mod\ \alpha)$, com $|t+2c+1|+|t-2c| = 2t+1$, temos que $D_\alpha(\beta,0) = 2t+1$. Agora, vamos provar que, se $\beta_1, \beta_2 \in S$, então $D_\alpha(\beta_1,\beta_2) \geq 2t+1$. Sejam $\beta_1, \beta_2 \in \langle\beta\rangle$, então $\beta_1 = \alpha_1\beta$ e $\beta_2 = \alpha_2\beta$, com $\alpha_1, \alpha_2 \in \mathbb{Z}[\omega]$. Temos que mostrar que $D_\alpha(\beta_1,\beta_2) = D_\alpha(\alpha_1\beta, \alpha_2\beta) = D_\alpha((\alpha_1-\alpha_2)\beta, 0) \geq 2t+1$. Observe que é suficiente provar que para qualquer $\eta \in \mathbb{Z}[\omega]$ tal que $\eta\beta \not\equiv 0 (mod\ \alpha)$ implica $D_\alpha(\eta\beta,0) \geq 2t+1$. É claro que para $\eta = \{1, \omega, -1, -\omega\}$, $D_\alpha(\eta\beta,0) = 2t+1$. Suponhamos por absurdo que $D_\alpha(\eta\beta,0) < 2t+1$. Então $\eta\beta \equiv x+y\omega+z\omega^2 (mod\ \alpha)$, com $|x|+|y|+|z| < 2t+1$ mínimo. Assim, $\eta\beta = (x+y\omega+z\omega^2)+\gamma_1\alpha = (x+y\omega+z\omega^2)+\gamma_2\alpha$, onde $\gamma_1, \gamma_2 \in \mathbb{Z}[\omega]$ e como $\beta|\alpha$, então $x+y\omega+z\omega^2 = \beta(\eta-\gamma_2)$. Agora, $N(x+y\omega+z\omega^2) \leq 4t^2$ pois $|x|+|y|+|z| < 2t+1$. Como $N(\beta) = 3t^2+3t+1+(4c^2+2c) > 3t^2$ para $t > 0$, $c \in \mathbb{Z}$, então $N(\eta-\gamma_2) = 1$. Consequentemente, $x+y\omega+z\omega^2 = \beta u$, com $u \in \{1, \omega, -1, -\omega\}$. Então, em qualquer caso, $|x|+|y|+|z| = 2t+1$, que é uma contradição. Portanto, $D_\alpha(\beta_1,\beta_2) \geq 2t+1$.*

*Finalmente,* $3t^2+3t+1$ *é o número de pontos de um hexágono de raio* $t$*, logo cada uma das* $N(\alpha)/N(\beta)$ *regiões de Voronoi com centro nos pontos dados por* $S$ *tem exatamente* $3t^2+3t+1$ *pontos de distância até* $t$ *e* $4c^2+2c$ *pontos com distância* $t+1$*, formando assim um código quase perfeito que corrige* $3t^2+3t+1$ *padrões com até* $t$ *erros e* $4c^2+2c$ *padrões com* $t+1$ *erros.*

2. *Dado* $\beta$ *divisor de* $\alpha$ *tal que* $\beta=(t+2c)+(2t+1)\omega$ *ou* $\beta=(t-2c+1)+(2t+1)\omega$*, temos que* $N(\beta)=3t^2+3t+1+(4c^2-2c)$*, e a demonstração segue analogamente.*

■

**Observação 4.5.1** *Note que tomando* $c=0$ *no Teorema 4.5.1 obtemos o Teorema 4.2.2.*

**Exemplo 4.5.1** *Dado* $\alpha=-5+2\omega$*, ele pode ser escrito como* $-5+2\omega=(1+2\omega)(3+4\omega)$ *e* $N(\alpha)=39$*. Se tomarmos* $\beta=3+4\omega$ *como gerador do ideal, ele tem a forma associada a* $\beta=(t+2c+1)+(2t+1)\omega$ *com* $c=1$*, e obtemos um código quase-perfeito que corrige todos os padrões com* $t=1$ *erro e* $4c^2+2c=6$ *padrões com* $2$ *erros, pois temos que* $N(\beta)=13$ *e o maior hexágono contido em* $13$ *pontos possui* $7$ *pontos com raio de cobertura* $1$*, logo restam* $6$ *pontos para completarmos os* $13$*. Assim, obtemos uma região fundamental que cobre* $13$ *pontos. Logo,* $S=\langle\beta\rangle$ *tem ordem* $N(\alpha)/N(\beta)=\frac{39}{13}=3$ *e o código quase-perfeito, que corrige todos os padrões com* $1$ *erro e* $6$ *padrões com* $2$ *erros, dado por* $S=\{0,3+4\omega,-3-4\omega\}$ *é identificado no grafo pelos pontos duplamente circulados, formando os baricentros dos 3 polígonos fundamentais contendo 13 elementos que recobrem a constelação de sinais contendo os 39 elementos de* $\mathbb{Z}_{-5+2\omega}$*, como ilustra a figura* 4.7.

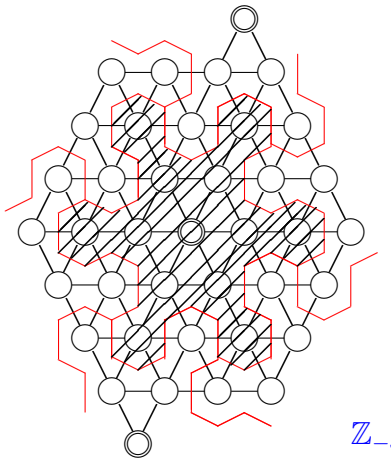


Figura 4.7: Código quase-perfeito sobre $\mathbb{Z}_{-5+2\omega}$

Observe que os procedimentos adotados podem ser facilmente estendidos para outros tipos de anéis, obtendo assim formas para a construção de novos códigos quase-perfeitos sobre constelações de sinais diferentes.

# Capítulo 5

# Códigos Geometricamente Uniformes Derivados de Grafos sobre Ordens dos Quatérnios

Códigos geometricamente uniformes foram propostos por Forney [2] e apresentam propriedades de simetria altamente desejáveis, tais como: todas as regiões de Voronoi são congruentes; o perfil de distâncias é o mesmo para qualquer palavra-código; as palavras código possuem a mesma probabilidade de erro; e o grupo gerador é isomorfo a um grupo de permutações transitivo sobre as palavras-código.

Uma subclasse dos códigos geometricamente uniformes, chamados códigos perfeitos foram estudados em [15] sobre espaços de sinais de dimensão quatro e as constelações modeladas por meio de grafos definidos sobre anéis quocientes da ordem dos quatérnios sobre o corpo dos números reais, chamados inteiros de Lipschitz.

Neste capítulo construiremos códigos geometricamente uniformes sobre ordens dos quatérnios, as quais em [12] foram associadas aos grupos Fuchsianos $\Gamma_{4g}$, para $g = 2^n$, $3.2^n$ e $5.2^n$ formados pelas isometrias que fazem o pareamento dos lados de um polígono hiperbólico $P_{4g}$ que tessela o plano hiperbólico $\mathbb{D}^2$, de modo que cada vértice é compartilhado por $4g$ polígonos de mesma forma, obtendo assim uma tesselação auto-dual do tipo $\{4g, 4g\}$, onde $g \geq 2$ é o gênero da superfície.

## 5.1 Anéis Quocientes de Ordens dos Quatérnios Associadas à $\Gamma_{4g}$

Nesta seção definiremos anéis quocientes de ordens dos quatérnios associadas à grupos Fuchsianos aritméticos $\Gamma_{4g}$ para os casos $g = 2^n$, $3.2^n$ e $5.2^n$ e veremos algumas propriedades.

Dado um grupo Fuchsiano aritmético $\Gamma_{4g}$ derivado de uma álgebra dos quatérnios $\mathcal{A}$ sobre um corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$, com $[\mathbb{K} : \mathbb{Q}] = g$, onde $g$ é o gênero da superfície $\mathbb{D}^2/\Gamma_{4g}$. Tomando tesselações do tipo $\{4g, 4g\}$, pelos Teoremas 3.4.1, 3.4.3 e 3.4.5 vimos que os elementos do grupo Fuchsiano $\Gamma_{4g}$ são identificados via isomorfismo com elementos da ordem $\mathcal{O} = (\theta, -1)_R$, onde

$$R = \left\{ \frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta] \quad e \quad m \in \mathbb{N} \right\}, \tag{5.1}$$

e pelos Teoremas 3.4.2, 3.4.4 e 3.4.6 o grupo Fuchsiano $\Gamma_{4g}$ é derivado de uma álgebra de divisão dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ sobre o corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$.

Assim, seja $\mathbb{K} = \mathbb{Q}(\theta)$ e $\{1, i, j, k\} = \{1, \sqrt{\theta}, Im, \sqrt{\theta}Im\}$ a base da álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, onde $i^2 = \theta, j^2 = -1, k = ij = \sqrt{\theta}Im$ e $Im$ denota a unidade imaginária $Im^2 = -1$. Em [12] foi provado que o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\theta)$ é dado por $I_{\mathbb{K}} = \mathbb{Z}[\theta]$, logo $\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in I_{\mathbb{K}}\}$ é de fato uma ordem em $\mathcal{A}$. Inicialmente trabalharemos com esta ordem por facilidade dos cálculos, e então estenderemos para a ordem $\mathcal{O} = (\theta, -1)_R$, onde $R = \left\{ \frac{\alpha}{2^m} : \alpha \in I_{\mathbb{K}} \quad e \quad m \in \mathbb{N} \right\}$ que faz o rotulamento completo e que também foi mostrado em [12] que é uma ordem.

Observe ainda que $\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in I_{\mathbb{K}}\}$ é uma extensão de $I_{\mathbb{K}}$ de dimensão 4, pois tem $\{1, i, j, k\}$ como base, e temos que $\mathcal{O}$ é um subanel de $\mathcal{A}$ contendo 1 que é um $I_{\mathbb{K}}$-módulo finitamente gerado. Agora, se olharmos a ordem $\mathcal{O}$ como extensão de $\mathbb{Z}$, a dimensão aumenta para $2^{n+2}$. Neste caso, a ordem será denotada por $\mathcal{O}_{\mathbb{Z}}$. Podemos verificar ainda que de acordo com a definição de ordem, $\mathcal{O}_{\mathbb{Z}}$ é um $\mathbb{Z}$-módulo livre de posto $4r = 2^{n+2}$, onde $r = [\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}] = 2^n$, e desta forma, não estaremos mais trabalhando com quatérnios, mas com extensões maiores onde perdemos várias propriedades.

### 5.1.1 Caso $g = 2^n$

Nesta subseção veremos anéis quocientes de ordens dos quatérnios associadas a grupos Fuchsianos aritméticos $\Gamma_{4g}$ para o caso $g = 2^n$.

Pelos Teoremas 3.4.1 e 3.4.2 dado o gênero $g = 2^n$, temos que os elementos do grupo

Fuchsiano $\Gamma_{4g}$ são identificados via isomorfismo com elementos da ordem $\mathcal{O} = (\theta, -1)_R$, onde

$$R = \left\{ \frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta] \;\; e \;\; m \in \mathbb{N} \right\},$$

e o grupo Fuchsiano aritmético $\Gamma_{4g}$ é derivado de uma álgebra de divisão dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, sobre $\mathbb{K} = \mathbb{Q}(\theta)$, onde $[\mathbb{K} : \mathbb{Q}] = 2^n$ e

$$\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{2}}}}},$$

contém $n$ radicais. Assim, dados $K = \mathbb{Q}(\theta)$ e $\mathcal{O} = (\theta, -1)_{\mathbb{Z}[\theta]}$ tal que

$$\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{Z}[\theta], i^2 = \theta, j^2 = -1, k^2 = -\theta\},$$

a norma reduzida de um elemento $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}$ é dada por

$$Nrd_{\mathbb{Z}[\theta]}(\alpha) = \alpha\bar{\alpha} = a_0^2 - \theta a_1^2 + a_2^2 - \theta a_3^2 \in \mathbb{Z}[\theta] \tag{5.2}$$

e satisfaz $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in I_{\mathbb{K}} = \mathbb{Z}[\theta]$. Vamos verificar em quais casos essa norma é um elemento $\in \mathbb{Z}$.

**Observação 5.1.1** *Dado* $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{2}}}}}$ *com n radicais, temos que* $\theta \in \mathbb{Z}$ *apenas para* $n = 0$*, mas neste caso temos* $g = 1$ *o qual não estamos interessados, logo consideraremos apenas* $n > 0$ *e* $\theta \notin \mathbb{Z}$*. Podemos observar ainda que,* $\theta^2 \in \mathbb{Z}$ *apenas para* $n = 1$ *e* $\theta^3 \notin \mathbb{Z}$*,* $\forall n > 0$*.*

**Proposição 5.1.1** *Seja* $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}$*, onde* $a_i = x_i + y_i\theta$ *e* $\theta$ *com n radicais dado por* $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{2}}}}}$*. Então,* $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in \mathbb{Z}$ *se, e somente se,*

1. *Para* $n = 1$*,*

$$2x_0y_0 - x_1^2 - 2y_1^2 + 2x_2y_2 - x_3^2 - 2y_3^2 = 0.$$

*Neste caso, a norma é dada por* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = x_0^2 + 2y_0^2 - 4x_1y_1 + x_2^2 + 2y_2^2 - 4x_3y_3$*.*

2. *Para* $n > 1$*,*

$$2x_0y_0 - x_1^2 + 2x_2y_2 - x_3^2 = y_0^2 - 2x_1y_1 + y_2^2 - 2x_3y_3 = y_1^2 + y_3^2 = 0.$$

*Neste caso, a norma é dada por* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = x_0^2 + x_2^2$*.*

**Demonstração:** *Da equação* (5.2) *temos* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = \alpha\bar{\alpha} = a_0^2 - \theta a_1^2 + a_2^2 - \theta a_3^2$. *Como* $a_i \in \mathbb{Z}[\theta]$ *ele pode ser escrito por* $a_i = x_i + y_i\theta$, *onde* $x_i, y_i \in \mathbb{Z}$. *Assim,* $a_i^2 = x_i^2 + \theta^2 y_i^2 + 2\theta x_i y_i$ *e disso segue que*

$Nrd_{\mathbb{Z}[\theta]}(\alpha) = a_0^2 - \theta a_1^2 + a_2^2 - \theta a_3^2 = x_0^2 + \theta^2 y_0^2 + 2\theta x_0 y_0 - \theta(x_1^2 + \theta^2 y_1^2 + 2\theta x_1 y_1) + x_2^2 + \theta^2 y_2^2 + 2\theta x_2 y_2 - \theta(x_3^2 + \theta^2 y_3^2 + 2\theta x_3 y_3) = x_0^2 + x_2^2 + \theta(2x_0 y_0 - x_1^2 + 2x_2 y_2 - x_3^2) + \theta^2(y_0^2 - 2x_1 y_1 + y_2^2 - 2x_3 y_3) + \theta^3(-y_1^2 - y_3^2)$.

*Para o caso* $n = 1$ *temos* $g = 2$ *e* $\theta = \sqrt{2}$, *logo* $\theta^2 = 2$ *e* $\theta^3 = 2\sqrt{2}$, *e daí* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = x_0^2 + 2y_0^2 - 4x_1 y_1 + x_2^2 + 2y_2^2 - 4x_3 y_3 + \sqrt{2}(2x_0 y_0 - x_1^2 - 2y_1^2 + 2x_2 y_2 - x_3^2 - 2y_3^2)$. *Portanto,* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) \in \mathbb{Z}$ *se, e somente se,* $2x_0 y_0 - x_1^2 - 2y_1^2 + 2x_2 y_2 - x_3^2 - 2y_3^2 = 0$, *e disso segue que* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = x_0^2 + 2y_0^2 - 4x_1 y_1 + x_2^2 + 2y_2^2 - 4x_3 y_3 \in \mathbb{Z}$.

*Agora, para o caso* $n > 1$, *pela Observação* 5.1.1 *temos que* $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in \mathbb{Z}$ *se, e somente, se* $2x_0 y_0 - x_1^2 + 2x_2 y_2 - x_3^2 = y_0^2 - 2x_1 y_1 + y_2^2 - 2x_3 y_3 = y_1^2 + y_3^2 = 0$, *e disso segue que* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = x_0^2 + x_2^2 \in \mathbb{Z}$. ■

Agora, tomando a ordem $\mathcal{O}$ como extensão de $\mathbb{Z}$, que denotaremos por $\mathcal{O}_{\mathbb{Z}}$, a norma reduzida de um elemento $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}_{\mathbb{Z}}$ será dada por

$$Nrd_{\mathbb{Z}}(\alpha) = \alpha\bar{\alpha} = a_0\bar{a_0} - \theta a_1\bar{a_1} + a_2\bar{a_2} - \theta a_3\bar{a_3} \in \mathbb{Z}[\theta] \tag{5.3}$$

onde $\bar{a_i}$ denota o conjugado de $a_i$.

**Proposição 5.1.2** *Seja* $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}_{\mathbb{Z}}$, *onde* $a_i = x_i + y_i\theta$ *e* $\theta$ *com* $n$ *radicais dado por* $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{2}}}}}$. *Então,* $Nrd_{\mathbb{Z}}(\alpha) \in \mathbb{Z}$ *se, e somente se,*

1. *Para* $n = 1$,

$$x_1^2 + x_3^2 - 2(y_1^2 + y_3^2) = 0.$$

*Neste caso, a norma é dada por* $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 - 2y_0^2 + x_2^2 - 2y_2^2 \in \mathbb{Z}$.

2. *Para* $n > 1$,

$$x_1^2 + x_3^2 = y_0^2 + y_3^2 = y_1^2 + y_3^2 = 0.$$

*Neste caso, a norma é dada por* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = x_0^2 + x_2^2$.

**Demonstração:** *Da equação* (5.3) *temos que* $Nrd_{\mathbb{Z}}(\alpha) = \alpha\bar{\alpha} = a_0\bar{a_0} - \theta a_1\bar{a_1} + a_2\bar{a_2} - \theta a_3\bar{a_3}$. *Como* $a_i \in \mathbb{Z}[\theta]$ *ele pode ser escrito por* $a_i = x_i + y_i\theta$, *onde* $x_i, y_i \in \mathbb{Z}$. *Assim,* $a_i\bar{a_i} = x_i^2 - \theta^2 y_i^2$ *e disso segue que*

$Nrd_{\mathbb{Z}}(\alpha) = x_0^2 - \theta^2 y_0^2 - \theta(x_1^2 - \theta^2 y_1^2) + x_2^2 - \theta^2 y_2^2 - \theta(x_3^2 - \theta^2 y_3^2) = x_0^2 + x_2^2 - \theta(x_1^2 + x_3^2) - \theta^2(y_0^2 + y_2^2) + \theta^3(y_1^2 + y_3^2)$.

*Para o caso* $n = 1$ *temos* $g = 2$ *e* $\theta = \sqrt{2}$, *logo* $\theta^2 = 2$ *e* $\theta^3 = 2\sqrt{2}$, *e daí* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = x_0^2 - 2y_0^2 + x_2^2 - 2y_2^2 - \sqrt{2}(x_1^2 + x_3^2 - 2(y_1^2 + y_3^2))$. *Assim,* $Nrd_{\mathbb{Z}}(\alpha) \in \mathbb{Z}$ *se, e somente se,* $x_1^2 - 2y_1^2 + x_3^2 - 2y_3^2 = 0$, *e neste caso segue que* $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 - 2y_0^2 + x_2^2 - 2y_2^2 \in \mathbb{Z}$.

*Agora, para o caso* $n > 1$, *pela Observação* 5.1.1 *temos que* $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in \mathbb{Z}$ *se, e somente se,* $x_1^2 + x_3^2 = y_0^2 + y_3^2 = y_1^2 + y_3^2 = 0$ *e disso segue que* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = x_0^2 + x_2^2 \in \mathbb{Z}$. ■

**Observação 5.1.2** *Quando não houver confusão de notação denotaremos por simplicidade a norma reduzida de* $\alpha$ *apenas por* $Nrd(\alpha)$.

**Teorema 5.1.1** *Seja* $0 \neq \alpha \in \mathcal{O}$. *Se* $Nrd(\alpha) \in \mathbb{Z}$, *então* $\frac{\mathcal{O}}{<\alpha>}$ *tem* $Nrd(\alpha)^4$ *elementos.*

**Demonstração:** *Seja* $0 \neq \alpha \in \mathcal{O}$ *e* $Nrd(\alpha) = N \in \mathbb{Z}$. *Primeiro vamos mostrar que o* $\mathcal{O}$*-módulo à esquerda* $\frac{\mathcal{O}}{<N>}$ *tem* $N^8$ *elementos. Como* $N \in \mathbb{Z}$, *vamos tomar* $\mathcal{O}$ *sobre* $\mathbb{Z}$. *Mas* $[\mathcal{O} : \mathbb{Z}] = 8$ *e a base de* $\mathcal{O}$ *sobre* $\mathbb{Z}$ *é* $\{1, \theta, i, i\theta, j, j\theta, k, k\theta\}$. *Assim,* $\alpha \in \mathcal{O}$ *é da forma* $\alpha = a_0 + a_1\theta + a_2 i + a_3 i\theta + a_4 j + a_5\theta j + a_6 k + a_7 k\theta$. *Agora, dados dois elementos* $\beta, \beta' \in \mathcal{O}$, $\beta = b_0 + b_1\theta + b_2 i + b_3 i\theta + b_4 j + b_5\theta j + b_6 k + b_7 k\theta, b_i \in \mathbb{Z}$ *e* $\beta' = b'_0 + b'_1\theta + b'_2 i + b'_3 i\theta + b'_4 j + b'_5\theta j + b'_6 k + b'_7 k\theta, b'_i \in \mathbb{Z}$ *dizemos que* $\beta$ *e* $\beta'$ *são congruentes módulo* $N$ *se existe* $\beta'' = b''_0 + b''_1\theta + b''_2 i + b''_3 i\theta + b''_4 j + b''_5\theta j + b''_6 k + b''_7 k\theta, b''_i \in \mathbb{Z}$ *tal que* $\beta - \beta' = \beta'' N$. *Assim,* $b_i - b'_i = b''_i N$, *para* $i = 0, 1, ..., 7$, *isto é,* $b_i \equiv b'_i (mod\ N)$ *o que implica que existem* $N$ *possibilidades para cada* $b_i$ *e, assim,* $N^8$ *classes de equivalência diferentes módulo* $N$.

*Agora, como* $Nrd(\alpha) = \alpha\bar{\alpha}$ *temos a seguinte cadeia de ideais:* $\langle Nrd(\alpha)\rangle = \langle \bar{\alpha}\alpha\rangle \subseteq \langle \alpha\rangle$. *Pelo Terceiro Teorema do Isomorfismo para A-módulos [22], temos a seguinte sequência de A-módulos à esquerda:*

$$0 \to \frac{\langle \alpha\rangle}{\langle \alpha\bar{\alpha}\rangle} \to \frac{A}{\langle \alpha\bar{\alpha}\rangle} \to \frac{A}{\langle \alpha\rangle} \to 0.$$

*Denotamos o número de elementos de* $\frac{A}{\langle \alpha\rangle}$ *por* $n$ *e o número de elementos de* $\frac{\langle \alpha\rangle}{\langle \alpha\bar{\alpha}\rangle}$ *por* $m$. *Então, como consequência do Teorema de Lagrange [22], podemos considerar a sequência exata anterior como uma sequência de grupos abelianos, assim obtendo que* $Nrd(\alpha)^8 = nm$. *Se provarmos que* $n = m$ *podemos finalmente concluir que* $n = Nrd(\alpha)^4$. *Agora, observe que a função*

$$f : \frac{A}{\langle \bar{\alpha}\rangle} \to \frac{\langle \alpha\rangle}{\langle \alpha\bar{\alpha}\rangle},$$

*definida por* $f(\beta + \langle \bar{\alpha}\rangle) = \beta\alpha + \langle \alpha\bar{\alpha}\rangle$ *está bem definida e é um isomorfismo de A-módulos à esquerda. Portanto,* $m$ *é exatamente o número de elementos de* $\frac{A}{\langle \bar{\alpha}\rangle}$.

*Finalmente, a conjugação de quatérnios é um anti-automorfismo, o que implica que* $\frac{A}{\langle \bar{\alpha}\rangle}$ *e* $\frac{A}{\langle \alpha\rangle}$ *tem a mesma cardinalidade, isto é,* $n = m$, *como queríamos provar.* ■

**Exemplo 5.1.1** *Seja* $\alpha = 1 + j \in \mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, *logo* $Nrd(\alpha) = 2$. *Pelo Teorema 5.1.1, temos que* $\frac{\mathcal{O}}{<\alpha>}$ *tem 16 elementos, que são obtidos pelo quociente da ordem* $\mathcal{O}$ *e o ideal* $\langle 1 + j \rangle$, *ou seja, tomamos os elementos de* $\mathcal{O}$ *e fazemos módulo* $(1 + j)$, *obtendo* $\frac{\mathcal{O}}{\langle 1+j \rangle} = \{0, 1, \sqrt{2}, 1 + \sqrt{2}, i, 1 + i, \sqrt{2} + i, \sqrt{2}i, (1 + \sqrt{2} + i), 1 + \sqrt{2}i, \sqrt{2} + \sqrt{2}i, (1 + \sqrt{2}) + \sqrt{2}i, (1 + \sqrt{2})i, 1 + (1 + \sqrt{2})i, \sqrt{2} + (1 + \sqrt{2})i, (1 + \sqrt{2}) + (1 + \sqrt{2})i\}$.

**Exemplo 5.1.2** *Dado* $\alpha = \sqrt{2} \in \mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, *temos* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 2$ *e* $Nrd_{\mathbb{Z}}(\alpha) = -2$. *Logo,* $\frac{\mathcal{O}}{<\alpha>}$ *tem 16 elementos, agora dados por* $\frac{\mathcal{O}}{\langle \sqrt{2} \rangle} = \{0, 1, i, j, k, 1 + i, 1 + j, 1 + k, i + j, i + k, j + k, 1 + i + j, 1 + i + k, 1 + j + k, i + j + k, 1 + i + j + k\}$.

**Exemplo 5.1.3** *Dado* $\alpha = 2 + \sqrt{2} \in \mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, *temos* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 6 + 4\sqrt{2} \notin \mathbb{Z}$. *Mas, tomando a ordem como extensão de* $\mathbb{Z}$, *ou seja,* $\mathcal{O}_{\mathbb{Z}} = (\sqrt{2}, -1)_{\mathbb{Z}}$ *temos* $Nrd_{\mathbb{Z}}(\alpha) = 2$ *e* $\frac{\mathcal{O}}{<\alpha>}$ *tem 16 elementos, novamente dados por* $\frac{\mathcal{O}}{\langle \sqrt{2} \rangle} = \{0, 1, i, j, k, 1+i, 1+j, 1+k, i+j, i+k, j+k, 1 + i + j, 1 + i + k, 1 + j + k, i + j + k, 1 + i + j + k\}$.

**Exemplo 5.1.4** *Dado* $\alpha = \sqrt{2} + j \in \mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, *temos* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 3$. *Logo,* $\frac{\mathcal{O}}{<\alpha>}$ *tem 81 elementos, dados por* $\frac{\mathcal{O}}{\langle \sqrt{2}+j \rangle} = \{0, 1, -1, \sqrt{2}, -\sqrt{2}, 1 + \sqrt{2}, 1 - \sqrt{2}, -1 + \sqrt{2}, -1 - \sqrt{2}, i, -i, \sqrt{2}i, -\sqrt{2}i, (1 + \sqrt{2})i, (1 - \sqrt{2})i, (-1 + \sqrt{2})i, (-1 - \sqrt{2})i, 1 + i, -1 + i, \sqrt{2} + i, -\sqrt{2} + i, (1+\sqrt{2})+i, (1-\sqrt{2})+i, (-1+\sqrt{2})+i, (-1-\sqrt{2})+i, 1-i, -1-i, \sqrt{2}-i, -\sqrt{2}-i, (1+\sqrt{2})-i, (1-\sqrt{2})-i, (-1+\sqrt{2})-i, (-1-\sqrt{2})-i, 1+\sqrt{2}i, -1+\sqrt{2}i, \sqrt{2}+\sqrt{2}i, -\sqrt{2}+\sqrt{2}i, (1+\sqrt{2})+\sqrt{2}i, (-1+\sqrt{2})+\sqrt{2}i, (-1-\sqrt{2})+\sqrt{2}i, 1-\sqrt{2}i, -1-\sqrt{2}i, \sqrt{2}-\sqrt{2}i, -\sqrt{2}-\sqrt{2}i, (1+\sqrt{2})-\sqrt{2}i, (1-\sqrt{2})-\sqrt{2}i, (-1+\sqrt{2})-\sqrt{2}i, (-1-\sqrt{2})-\sqrt{2}i, 1+(1+\sqrt{2})i, -1+(1+\sqrt{2})i, \sqrt{2}+(1+\sqrt{2})i, -\sqrt{2}+(1+\sqrt{2})i, (1+\sqrt{2})+(1+\sqrt{2})i, (1-\sqrt{2})+(1+\sqrt{2})i, (-1+\sqrt{2})+(1+\sqrt{2})i, (-1-\sqrt{2})+(1+\sqrt{2})i, 1+(1-\sqrt{2})i, -1+(1-\sqrt{2})i, \sqrt{2}+(1-\sqrt{2})i, -\sqrt{2}+(1-\sqrt{2})i, (1+\sqrt{2})+(1-\sqrt{2})i, (1-\sqrt{2})+(1-\sqrt{2})i, (-1+\sqrt{2})+(1-\sqrt{2})i, (-1-\sqrt{2})+(1-\sqrt{2})i, 1+(-1+\sqrt{2})i, -1+(-1+\sqrt{2})i, \sqrt{2}+(-1+\sqrt{2})i, -\sqrt{2}+(-1+\sqrt{2})i, (1+\sqrt{2})+(-1+\sqrt{2})i, (1-\sqrt{2})+(-1+\sqrt{2})i, (-1+\sqrt{2})+(-1+\sqrt{2})i, (-1-\sqrt{2})+(-1+\sqrt{2})i, 1+(-1-\sqrt{2})i, -1+(-1-\sqrt{2})i, \sqrt{2}+(-1-\sqrt{2})i, -\sqrt{2}+(-1-\sqrt{2})i, (1+\sqrt{2})+(-1-\sqrt{2})i, (1-\sqrt{2})+(-1-\sqrt{2})i, (-1+\sqrt{2})+(-1-\sqrt{2})i, (-1-\sqrt{2})+(-1-\sqrt{2})i\}$.

**Observação 5.1.3** *Neste trabalho não estamos interessados em ordens* $\mathcal{O}_{\mathbb{Z}}$, *pois como mencionado anteriormente, quando estendemos da ordem* $\mathcal{O}$ *para a ordem* $\mathcal{O}_{\mathbb{Z}}$ *passamos a trabalhar com extensões maiores e com isso perdemos propriedades importantes. Por isso, só tomamos esta extensão quando ela é realmente necessária, ou seja, quando a norma sobre* $I_{\mathbb{K}}$ *não é um elemento em* $\mathbb{Z}$.

**Corolário 5.1.1** *Se $\beta \in \mathcal{O} = (\theta, -1)_{\mathbb{Z}[\theta]}$ é um divisor à direita de $\alpha$ e $Nrd(\beta) \in \mathbb{Z}$, então o ideal à esquerda gerado por $\beta$, $< \beta > \subseteq \mathcal{O}$ tem $\left(\frac{Nrd(\alpha)}{Nrd(\beta)}\right)^4$ elementos.*

**Exemplo 5.1.5** *Dado $\alpha = 1 + 2\sqrt{2}j$, temos $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = (1)^2 + (2\sqrt{2})^2 = 9$. Agora, $\alpha = 1 + 2\sqrt{2}j$ pode ser escrito como $1 + 2\sqrt{2}j = (\sqrt{2} + j)^2$, logo $\beta$ é um divisor à direita de $\alpha$ e $Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta) = 3 \in \mathbb{Z}$, então o ideal à esquerda gerado por $\beta$, $< \beta > \subseteq \mathcal{O}$ tem $\left(\frac{Nrd(\alpha)}{Nrd(\beta)}\right)^4 = \left(\frac{9}{3}\right)^4 = 81$ elementos.*

Como verificado em [11] para $\theta = \sqrt{2}$ e [12] nos demais casos, a ordem $\mathcal{O} = (\theta, -1)_{\mathbb{Z}[\theta]}$ não é uma ordem maximal. Portanto, devemos tomar a ordem sobre o anel $R = \{\frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta],\ m \in \mathbb{N}\}$, que torna a ordem maximal. Assim, dados $\mathbb{K} = \mathbb{Q}(\theta)$ e $\mathcal{O} = (\theta, -1)_R$, onde $R = \{\frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta],\ m \in \mathbb{N}\}$ tal que

$$\mathcal{O} = \{a_0 + \frac{a_1}{2}i + \frac{a_2}{2}j + \frac{a_3}{2}k : a_i \in \mathbb{Z}[\theta], i^2 = \theta, j^2 = -1, k^2 = -\theta\},$$

temos que a norma reduzida de um elemento $\alpha \in \mathcal{O}$ é dada por

$$Nrd_R(\alpha) = a_0^2 - \frac{1}{2}\theta a_1^2 + \frac{1}{2}a_2^2 - \frac{1}{4}\theta a_3^2 \in \mathbb{Z}[\theta]. \tag{5.4}$$

Agora, para a ordem maximal, a cardinalidade do anel quociente segue os dois seguintes resultados:

**Teorema 5.1.2** *Seja $\alpha \in \mathcal{O} = (\theta, -1)_R$, onde $R = \{\frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta],\ m \in \mathbb{N}\}$. Se $Nrd_R(\alpha) = 2^s$, $s \in \mathbb{N}$, então $\frac{\mathcal{O}}{<\alpha>}$ possui apenas 1 elemento.*

**Demonstração:** *Seja $\gamma \in \frac{\mathcal{O}}{<\alpha>}$. Vamos mostrar que $\gamma \equiv 0(mod\ \alpha)$. Mostrar que $\gamma \equiv 0(mod\ \alpha)$ é equivalente a provar que $\gamma = x\alpha$, onde $x \in \mathcal{O}$. Como $Nrd_R(\alpha) = 2^s$, $s \in \mathbb{N}$, temos que $\bar{\alpha}\alpha = 2^s$, logo $\gamma$ pode ser escrito como*

$$\gamma = \frac{\gamma}{2^s}\bar{\alpha}\alpha,$$

*ou seja, $\gamma \equiv 0(mod\ \alpha)$. Em particular, verifica-se que $1 \equiv 0(mod\ \alpha)$, pois $1 = \frac{1}{2^s}\bar{\alpha}\alpha$.* ∎

**Teorema 5.1.3** *Seja $\alpha \in \mathcal{O} = (\theta, -1)_R$, onde $R = \{\frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta],\ m \in \mathbb{N}\}$. Se $Nrd_R(\alpha) \neq 2^s$, $s \in \mathbb{N}$, então $\frac{\mathcal{O}}{<\alpha>}$ possui $Nrd_R(\alpha)^4$ elementos.*

**Demonstração:** *Seja $0 \neq \alpha \in \mathcal{O}$ e $Nrd_R(\alpha) \neq 2^s$, $s \in \mathbb{N}$, $Nrd_R(\alpha) = N \in \mathbb{Z}$. Temos que mostrar que o $\mathcal{O}$-módulo à esquerda $\frac{\mathcal{O}}{<N>}$ tem $N^8$ elementos. Como $N \in \mathbb{Z}$, vamos tomar $\mathcal{O}$ sobre $\mathbb{Z}$. Mas $[\mathcal{O} : \mathbb{Z}] = 8$ e a base de $\mathcal{O}$ sobre $\mathbb{Z}$ é $\{\frac{1}{2^s}, \frac{\theta}{2^s}, \frac{i}{2^s}, \frac{i\theta}{2^s}, \frac{j}{2^s}, \frac{j\theta}{2^s}, \frac{k}{2^s}, \frac{k\theta}{2^s}\}$. Assim, a demonstração segue análoga à demonstração do Teorema 5.1.1.* ∎

**Exemplo 5.1.6** *Seja* $\alpha = 2 \in \mathcal{O}_R$, *logo pela equação* (5.4) *temos que* $Nrd_R(\alpha) = 4$, *e pelo Teorema 5.1.2 segue que* $\frac{\mathcal{O}}{<\alpha>}$ *possui apenas 1 elemento* $\{0\}$.

**Exemplo 5.1.7** *Seja* $\alpha = \sqrt{2} + \frac{\sqrt{2}}{2}j \in \mathcal{O}_R$, *logo pela equação* (5.4) *temos que* $Nrd_R(\alpha) = 3$ *e pelo Teorema 5.1.3 segue que* $\frac{\mathcal{O}}{<\alpha>}$ *possui* 81 *elementos.*

### 5.1.2 Caso $g = 3.2^n$

Nesta subseção veremos anéis quocientes de ordens dos quatérnios associadas a grupos Fuchsianos aritméticos $\Gamma_{4g}$ para o caso $g = 3.2^n$.

Analogamente ao caso anterior, dado o gênero $g = 3.2^n$, pelos Teoremas 5.1.1 e 5.1.2, os elementos do grupo Fuchsiano $\Gamma_{4g}$ são identificados via isomorfismo com elementos da ordem $\mathcal{O} = (\theta, -1)_R$, onde

$$R = \left\{ \frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta] \quad e \quad m \in \mathbb{N} \right\},$$

e o grupo Fuchsiano aritmético $\Gamma_{4g}$ é derivado de uma álgebra de divisão dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, sobre $\mathbb{K} = \mathbb{Q}(\theta)$, onde $[\mathbb{K} : \mathbb{Q}] = 2^{n+1}$ e

$$\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{3}}}}},$$

contém $n + 1$ radicais. Assim, dados $K = \mathbb{Q}(\theta)$ e $\mathcal{O} = (\theta, -1)_{\mathbb{Z}[\theta]}$ tal que

$$\mathcal{O} = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{Z}[\theta], i^2 = \theta, j^2 = -1, k^2 = -\theta\},$$

a norma reduzida de um elemento $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}$ é dada por

$$Nrd_{\mathbb{Z}[\theta]}(\alpha) = \alpha\bar{\alpha} = a_0^2 - \theta a_1^2 + a_2^2 - \theta a_3^2 \in \mathbb{Z}[\theta], \tag{5.5}$$

e satisfaz $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in I_{\mathbb{K}} = \mathbb{Z}[\theta]$. Vamos novamente verificar em quais casos essa norma é um elemento $\in \mathbb{Z}$.

**Observação 5.1.4** *Dado* $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{3}}}}}$ *com* $n + 1$ *radicais, temos para* $n = 0$ *que* $\theta \notin \mathbb{Z}$, *mas* $\theta^2 \in \mathbb{Z}$ *e* $\theta^3 \notin \mathbb{Z}$. *Podemos observar ainda que,* $\theta$, $\theta^2$, $\theta^3 \notin \mathbb{Z}$ *para todo* $n > 0$.

**Proposição 5.1.3** *Seja* $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}$, *onde* $a_i = x_i + y_i\theta$ *e* $\theta$ *com* $n+1$ *radicais dado por* $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{3}}}}}$. *Então,* $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in \mathbb{Z}$ *se, e somente se,*

1. *Para* $n = 0$,

$$2x_0y_0 - x_1^2 - 3y_1^2 + 2x_2y_2 - x_3^2 - 3y_3^2 = 0.$$

*Neste caso, a norma é dada por* $Nrd_{\mathbb{Z}[\sqrt{3}]}(\alpha) = x_0^2 + 3y_0^2 - 6x_1y_1 + x_2^2 + 3y_2^2 - 6x_3y_3$.

2. *Para* $n > 0$,

$$2x_0y_0 - x_1^2 + 2x_2y_2 - x_3^2 = y_0^2 - 2x_1y_1 + y_2^2 - 2x_3y_3 = y_1^2 + y_3^2 = 0.$$

*Neste caso, a norma é dada por* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = x_0^2 + x_2^2$.

**Demonstração:** *Da equação* (5.5) *temos* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = \alpha\bar{\alpha} = a_0^2 - \theta a_1^2 + a_2^2 - \theta a_3^2$. *Como* $a_i \in \mathbb{Z}[\theta]$ *ele pode ser escrito por* $a_i = x_i + y_i\theta$, *onde* $x_i, y_i \in \mathbb{Z}$. *Assim,* $a_i^2 = x_i^2 + \theta^2 y_i^2 + 2\theta x_i y_i$ *e disso segue que*
$Nrd_{\mathbb{Z}[\theta]}(\alpha) = a_0^2 - \theta a_1^2 + a_2^2 - \theta a_3^2 = x_0^2 + \theta^2 y_0^2 + 2\theta x_0y_0 - \theta(x_1^2 + \theta^2 y_1^2 + 2\theta x_1y_1) + x_2^2 + \theta^2 y_2^2 + 2\theta x_2y_2 - \theta(x_3^2 + \theta^2 y_3^2 + 2\theta x_3y_3) = x_0^2 + x_2^2 + \theta(2x_0y_0 - x_1^2 + 2x_2y_2 - x_3^2) + \theta^2(y_0^2 - 2x_1y_1 + y_2^2 - 2x_3y_3) + \theta^3(-y_1^2 - y_3^2)$.
*Para o caso* $n = 0$ *temos* $g = 3$ *e* $\theta = \sqrt{3}$, *logo* $\theta^2 = 3$ *e* $\theta^3 = 3\sqrt{3}$, *e daí* $Nrd_{\mathbb{Z}[\sqrt{3}]}(\alpha) = x_0^2 + 3y_0^2 - 6x_1y_1 + x_2^2 + 3y_2^2 - 6x_3y_3 + \sqrt{3}(2x_0y_0 - x_1^2 - 3y_1^2 + 2x_2y_2 - x_3^2 - 3y_3^2)$. *Portanto,* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) \in \mathbb{Z}$ *se, e somente se,* $2x_0y_0 - x_1^2 - 3y_1^2 + 2x_2y_2 - x_3^2 - 3y_3^2 = 0$, *e disso segue que* $Nrd_{\mathbb{Z}[\sqrt{3}]}(\alpha) = x_0^2 + 3y_0^2 - 6x_1y_1 + x_2^2 + 3y_2^2 - 6x_3y_3 \in \mathbb{Z}$.
*Agora, para o caso* $n > 1$, *pela Observação* 5.1.4 *temos que* $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in \mathbb{Z}$ *se, e somente se* $2x_0y_0 - x_1^2 + 2x_2y_2 - x_3^2 = y_0^2 - 2x_1y_1 + y_2^2 - 2x_3y_3 = y_1^2 + y_3^2 = 0$, *e disso segue que* $Nrd_{\mathbb{Z}[\theta]}(\alpha) = x_0^2 + x_2^2 \in \mathbb{Z}$. ■

Novamente, tomando a ordem $\mathcal{O}$ como extensão de $\mathbb{Z}$ a norma reduzida de um elemento $\alpha = a_0 + a_1i + a_2j + a_3k \in \mathcal{O}$ será dada por

$$Nrd_{\mathbb{Z}}(\alpha) = \alpha\bar{\alpha} = a_0\bar{a_0} - \theta a_1\bar{a_1} + a_2\bar{a_2} - \theta a_3\bar{a_3} \in \mathbb{Z}[\theta], \tag{5.6}$$

onde $\bar{a_i}$ denota o conjugado de $a_i$.

**Proposição 5.1.4** *Seja* $\alpha = a_0 + a_1i + a_2j + a_3k \in \mathcal{O}_{\mathbb{Z}}$, *onde* $a_i = x_i + y_i\theta$ *e* $\theta$ *com* $n+1$ *radicais dado por* $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{3}}}}}$. *Então,* $Nrd_{\mathbb{Z}}(\alpha) \in \mathbb{Z}$ *se, e somente se,*

1. *Para* $n = 0$,

$$x_1^2 + x_3^2 - 2(y_1^2 + y_3^2) = 0.$$

*Neste caso, a norma é dada por* $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 - 3y_0^2 + x_2^2 - 3y_2^2 \in \mathbb{Z}$.

*2. Para $n > 0$,*

$$x_1^2 + x_3^2 = y_0^2 + y_3^2 = y_1^2 + y_3^2 = 0.$$

*Neste caso, a norma é dada por $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 + x_2^2$.*

**Demonstração:** *Da equação (5.3) temos que $Nrd_{\mathbb{Z}}(\alpha) = \alpha\bar{\alpha} = a_0\bar{a_0} - \theta a_1\bar{a_1} + a_2\bar{a_2} - \theta a_3\bar{a_3}$. Como $a_i \in \mathbb{Z}[\theta]$ ele pode ser escrito por $a_i = x_i + y_i\theta$, onde $x_i, y_i \in \mathbb{Z}$. Assim, $a_i\bar{a_i} = x_i^2 - \theta^2 y_i^2$ e disso segue que*
$Nrd_{\mathbb{Z}}(\alpha) = x_0^2 - \theta^2 y_0^2 - \theta(x_1^2 - \theta^2 y_1^2) + x_2^2 - \theta^2 y_2^2 - \theta(x_3^2 - \theta^2 y_3^2) = x_0^2 + x_2^2 - \theta(x_1^2 + x_3^2) - \theta^2(y_0^2 + y_2^2) + \theta^3(y_1^2 + y_3^2)$.
*Para o caso $n = 0$ temos $g = 3$ e $\theta = \sqrt{3}$, logo $\theta^2 = 3$ e $\theta^3 = 3\sqrt{3}$, e daí $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 - 3y_0^2 + x_2^2 - 3y_2^2 - \sqrt{3}(x_1^2 + x_3^2 - 3(y_1^2 + y_3^2))$. Assim, $Nrd_{\mathbb{Z}}(\alpha) \in \mathbb{Z}$ se, e somente se, $x_1^2 - 3y_1^2 + x_3^2 - 3y_3^2 = 0$, e neste caso segue que $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 - 3y_0^2 + x_2^2 - 3y_2^2 \in \mathbb{Z}$.*
*Agora, para o caso $n > 1$, pela Observação 5.1.1 temos que $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in \mathbb{Z}$ se, e somente se, $x_1^2 + x_3^2 = y_0^2 + y_3^2 = y_1^2 + y_3^2 = 0$ e disso segue que $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 + x_2^2 \in \mathbb{Z}$.* ■

Observe que o Teorema 5.1.1 foi demonstrado para qualquer $\theta$, portanto continua válido para o caso $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{3}}}}}$ com $n + 1$ radicais.

**Exemplo 5.1.8** *Seja $\alpha = 1 + j \in \mathcal{O} = (\sqrt{3}, -1)_{\mathbb{Z}[\sqrt{3}]}$, logo $Nrd(\alpha) = 2$. Pelo Teorema 5.1.1, temos que $\frac{\mathcal{O}}{<\alpha>}$ tem 16 elementos, que são obtidos pelo quociente da ordem $\mathcal{O}$ e o ideal $\langle 1 + j\rangle$, ou seja, tomamos os elementos de $\mathcal{O}$ e fazemos módulo $(1 + j)$, obtendo $\frac{\mathcal{O}}{\langle 1+j\rangle} = \{0, 1, \sqrt{3}, 1 + \sqrt{3}, i, 1 + i, \sqrt{3} + i, \sqrt{3}i, 1 + \sqrt{3} + i, 1 + \sqrt{3}i, \sqrt{3} + \sqrt{3}i, (1 + \sqrt{3}) + \sqrt{3}i, (1 + \sqrt{3})i, 1 + (1 + \sqrt{3})i, \sqrt{3} + (1 + \sqrt{3})i, (1 + \sqrt{3}) + (1 + \sqrt{3})i\}$.*

**Corolário 5.1.2** *Se $\beta \in \mathcal{O} = (\theta, -1)_{\mathbb{Z}[\theta]}$, onde $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{3}}}}}$ cotém $n + 1$ radicais é um divisor à direita de $\alpha$ e $Nrd(\beta) \in \mathbb{Z}$, então o ideal à esquerda gerado por $\beta$, $< \beta > \subseteq \mathcal{O}$ tem $\left(\frac{Nrd(\alpha)}{Nrd(\beta)}\right)^4$ elementos.*

Analogamente à seção anterior, tomaremos a ordem maximal e obteremos da mesma forma os Teoremas 5.1.2 e 5.1.3.

### 5.1.3 Caso $g = 5.2^n$

Nesta subseção veremos anéis quocientes de ordens dos quatérnios associadas a grupos Fuchsianos aritméticos $\Gamma_{4g}$ para o caso $g = 5.2^n$.

Como nos casos anteriores, pelos Teoremas 3.4.5 e 3.4.6, dado o gênero $g = 5.2^n$ os elementos do grupo Fuchsiano $\Gamma_{4g}$ são identificados via isomorfismo com os elementos da ordem $\mathcal{O} = (\theta, -1)_R$, onde

$$R = \left\{ \frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta] \;\; e \;\; m \in \mathbb{N} \right\},$$

e o grupo Fuchsiano aritmético $\Gamma_{4g}$ é derivado de uma álgebra de divisão dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, sobre $\mathbb{K} = \mathbb{Q}(\theta)$, onde $[\mathbb{K} : \mathbb{Q}] = 2^{n+1}$ e

$$\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{5}}}}},$$

contém $n+1$ radicais. Este caso é idêntico ao da seção anterior, portanto apenas enunciaremos os resultados com as alterações devidas.

**Proposição 5.1.5** *Seja $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}$, onde $a_i = x_i + y_i\theta$ e $\theta$ com $n+1$ radicais dado por $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{5}}}}}$. Então, $Nrd_{\mathbb{Z}[\theta]}(\alpha) \in \mathbb{Z}$ se, e somente se,*

1. *Para $n = 0$,*

$$2x_0y_0 - x_1^2 - 5y_1^2 + 2x_2y_2 - x_3^2 - 5y_3^2 = 0.$$

*Neste caso, a norma é dada por $Nrd_{\mathbb{Z}[\sqrt{3}]}(\alpha) = x_0^2 + 5y_0^2 - 10x_1y_1 + x_2^2 + 5y_2^2 - 10x_3y_3$.*

2. *Para $n > 0$,*

$$2x_0y_0 - x_1^2 + 2x_2y_2 - x_3^2 = y_0^2 - 2x_1y_1 + y_2^2 - 2x_3y_3 = y_1^2 + y_3^2 = 0.$$

*Neste caso, a norma é dada por $Nrd_{\mathbb{Z}[\theta]}(\alpha) = x_0^2 + x_2^2$.*

**Proposição 5.1.6** *Seja $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{O}_{\mathbb{Z}}$, onde $a_i = x_i + y_i\theta$ e $\theta$ com $n+1$ radicais dado por $\theta = \sqrt{2 + \sqrt{2 + \sqrt{\ldots + \sqrt{2 + \sqrt{5}}}}}$. Então, $Nrd_{\mathbb{Z}}(\alpha) \in \mathbb{Z}$ se, e somente se,*

1. *Para $n = 0$,*

$$x_1^2 + x_3^2 - 2(y_1^2 + y_3^2) = 0.$$

*Neste caso, a norma é dada por $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 - 3y_0^2 + x_2^2 - 3y_2^2 \in \mathbb{Z}$.*

2. *Para $n > 0$,*

$$x_1^2 + x_3^2 = y_0^2 + y_3^2 = y_1^2 + y_3^2 = 0.$$

*Neste caso, a norma é dada por $Nrd_{\mathbb{Z}}(\alpha) = x_0^2 + x_2^2$.*

Como dito anteriormente o Teorema 5.1.1 continua válido para o caso onde $\theta$ com $n+1$ radicais é dado por $\theta = \sqrt{2+\sqrt{2+\sqrt{\ldots+\sqrt{2+\sqrt{5}}}}}$.

**Exemplo 5.1.9** *Seja* $\alpha = 1+j \in \mathcal{O} = (\sqrt{5},-1)_{\mathbb{Z}[\sqrt{5}]}$, *logo* $Nrd(\alpha) = 2$. *Pelo Teorema* 5.1.1, *temos que* $\frac{\mathcal{O}}{<\alpha>}$ *tem* 16 *elementos, que são obtidos pelo quociente da ordem* $\mathcal{O}$ *e o ideal* $\langle 1+j\rangle$, *ou seja, tomamos os elementos de* $\mathcal{O}$ *e fazemos módulo* $(1+j)$, *obtendo* $\frac{\mathcal{O}}{\langle 1+j\rangle} = \{0, 1, \sqrt{5}, 1+\sqrt{5}, i, 1+i, \sqrt{5}+i, \sqrt{5}i, 1+\sqrt{5}+i, 1+\sqrt{5}i, \sqrt{5}+\sqrt{5}i, (1+\sqrt{5})+\sqrt{5}i, (1+\sqrt{5})i, 1+(1+\sqrt{3})i, \sqrt{3}+(1+\sqrt{5})i, (1+\sqrt{5})+(1+\sqrt{5})i\}$.

**Corolário 5.1.3** *Se* $\beta \in \mathcal{O} = (\theta,-1)_{\mathbb{Z}[\theta]}$, *onde* $\theta = \sqrt{2+\sqrt{2+\sqrt{\ldots+\sqrt{2+\sqrt{5}}}}}$ *contém* $n+1$ *radicais é um divisor à direita de* $\alpha$ *e* $Nrd(\beta) \in \mathbb{Z}$, *então o ideal à esquerda gerado por* $\beta$, $<\beta> \subseteq \mathcal{O}$ *tem* $\left(\frac{Nrd(\alpha)}{Nrd(\beta)}\right)^4$ *elementos.*

Analogamente às seções anteriores, tomaremos a ordem maximal e obteremos da mesma forma os Teoremas 5.1.2 e 5.1.3.

## 5.2 Rotulamento de Pontos Gerados por Tesselações do Plano Hiperbólico no Disco de Poincaré

Nesta seção veremos como rotular os pontos de uma tesselação obtida pelo anel quociente de ordens dos quatérnios através das transformações que realizam os pareamentos dos lados do polígono hiperbólico regular $P_{4g}$ que tessela o plano hiperbólico para regiões fundamentais do tipo $\{4g, 4g\}$.

Na subseção 3.3.1 consideramos o polígono hiperbólico regular $P_{4g}$, ordenamos suas arestas e obtemos as isometrias hiperbólicas que geram o grupo Fuchsiano $\Gamma_{4g}$ e realizam o pareamento destas arestas. Por [11] dado o gênero $g$ da superfície obtemos estas transformações. Assim, conhecidas as transformações e a região fundamental somos capazes de tesselar o plano hiperbólico e rotular os seus pontos, é o que faremos a seguir.

Dado um polígono hiperbólico regular $P_{4g}$ vamos colocá-lo no "centro"do disco de Poincaré e identificá-lo com o ponto zero. Pela Proposição 3.3.2 obtemos as $2g$ transformações que fazem o pareamento dos lados deste polígono. Aplicando estas transformações no ponto 0 geramos $4g$ pontos. Aplicamos novamente as transformações nestes novos pontos, e desta forma vamos tesselando o disco de Poincaré e rotulando os pontos obtidos.

**Exemplo 5.2.1** *Para o caso $g = 2$, tomando a região fundamental $P_8$, dada por um octógono, que gerará a tesselação, vamos colocá-la no centro do disco de Poincaré, e identificá-la como o ponto zero. Pela Proposição* 3.3.2 *temos 4 transformações que realizam o pareamento dos lados deste polígono, $T_1$, $T_2$, $S_1$ e $S_2$ dadas por $T_1(z) = \frac{az+c}{\bar{c}z+\bar{a}}$, $T_2(z) = \frac{az-c}{-\bar{c}z+\bar{a}}$, $S_1(z) = \frac{\bar{a}z+\bar{c}}{cz+a}$ e $S_2(z) = \frac{\bar{a}z-\bar{c}}{-cz+a}$, onde $a = \frac{(2+\sqrt{2})(1+i)}{2}$ e $c = \frac{-\sqrt[4]{2}(\sqrt{2}+(2+\sqrt{2})i)}{2}$ são obtidos pela Proposição 3.3.2. Assim, pelas transformações a partir do ponto* 0 *geramos os 8 pontos:*

$$T_1(0) = \frac{-\sqrt[4]{2}(-1+(\sqrt{2}+1)i)}{2+\sqrt{2}} \approx 0.3483 - 0.84i,$$

$$T_2(0) = \frac{\sqrt[4]{2}(-1+(\sqrt{2}+1)i)}{2+\sqrt{2}} \approx -0.3483 + 0.84i,$$

$$S_1(0) = \frac{\sqrt[4]{2}(1+(\sqrt{2}+1)i)}{2+\sqrt{2}} \approx 0.3483 + 0.84i,$$

$$S_2(0) = \frac{-\sqrt[4]{2}(1+(\sqrt{2}+1)i)}{2+\sqrt{2}} \approx -0.3483 - 0.84i,$$

$$T_1^{-1}(0) = \frac{\sqrt[4]{2}((\sqrt{2}+1)+i)}{2+\sqrt{2}} \approx 0.84 + 0.3483i,$$

$$T_2^{-1}(0) = \frac{-\sqrt[4]{2}((\sqrt{2}+1)+i)}{2+\sqrt{2}} \approx -0.84 - 0.3483i,$$

$$S_1^{-1}(0) = \frac{-\sqrt[4]{2}((-\sqrt{2}-1)+i)}{2+\sqrt{2}} \approx 0.84 - 0.3483i,$$

$$S_2^{-1}(0) = \frac{\sqrt[4]{2}((-\sqrt{2}-1)+i)}{2+\sqrt{2}} \approx -0.84 + 0.3483i.$$

*que são representados graficamente, como mostra a Figura* 5.1.

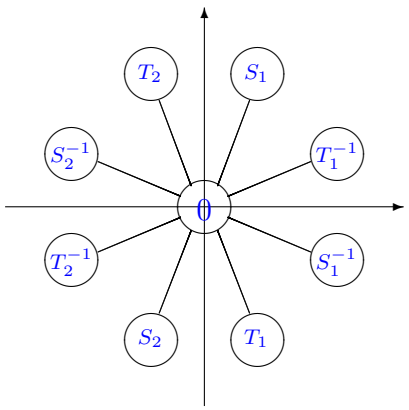


Figura 5.1: Aplicação das transformações

*Fazendo uma rotação de* $\frac{\pi}{8}$ *radianos e normalizando os pontos obtidos, temos os novos pontos:*

$$\begin{array}{ll} T_1'(0) = \frac{\sqrt{2}}{2}(1-i) & T_2'(0) = \frac{\sqrt{2}}{2}(-1+i) \\ S_1'(0) = i & S_2'(0) = -i \\ T_1'^{-1}(0) = \frac{\sqrt{2}}{2}(1+i) & T_2'^{-1}(0) = \frac{\sqrt{2}}{2}(-1-i) \\ S_1'^{-1}(0) = 1 & S_2'^{-1}(0) = -1 \end{array}$$

*com a nova representação gráfica rotacionada, como ilustra a Figura* 5.2.

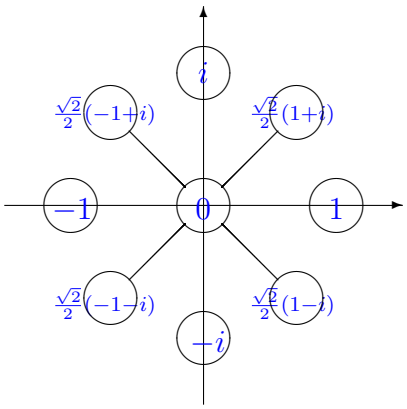


Figura 5.2: Representação rotacionada

*A partir dos pontos obtidos aplicamos novamente as transformações* $T_1, T_2, S_1, S_2, T_1^{-1}, T_2^{-1}, S_1^{-1}$ *e* $S_2^{-1}$*, obtendo assim outros* 56 *pontos:*

$$\begin{array}{ll} T_1(T_1(0)) \approx 0.463 - 0.84i, & T_2(T_1(0)) \approx -0.292 + 0.9472, \\ S_1(T_1(0)) \approx 0.16419 - 0.9569i, & S_2(T_1(0)) \approx -0.4161 - 0.9036i, \\ T_1^{-1}(T_1(0)) = 0, & T_2^{-1}(T_1(0)) \approx -0.9198 - 0.38099i, \\ S_1^{-1}(T_1(0)) \approx 0.933 - 0.3447i, & S_2^{-1}(T_1(0)) \approx -0.7928 + 0.5605i, \\ T_1(T_2(0)) \approx 0.292 - 0.9472i, & T_2(T_2(0)) \approx -0.4632 + 0.8863i, \\ S_1(T_2(0)) \approx 0.4161 + 0.9036i, & S_2(T_2(0)) \approx -0.1641 - 0.9569i, \\ T_1^{-1}(T_2(0)) \approx 0.9198 + 0.3809i, & T_2^{-1}(T_2(0)) = 0, \\ S_1^{-1}(T_2(0)) \approx 0.7928 - 0.5605i, & S_2^{-1}(T_2(0)) \approx -0.933 + 0.3447i, \\ T_1(S_1(0)) \approx 0.1641 - 0.9569i, & T_2(S_1(0)) \approx -0.4611 + 0.9036i, \\ S_1(S_1(0)) \approx 0.4632 + 0.8763i, & S_2(S_1(0)) \approx -0.292 - 0.947i, \\ T_1^{-1}(S_1(0)) \approx 0.933 + 0.344i, & T_2^{-1}(S_1(0)) \approx -0.7928 - 0.5605i, \\ S_1^{-1}(S_1(0)) = 0, & S_2^{-1}(S_1(0)) \approx -0.9198 + 0.4161i, \\ T_1(S_2(0)) \approx 0.4161 - 0.9036i, & T_2(S_2(0)) \approx -0.1641 + 0.9569i, \\ S_1(S_2(0)) \approx 0.292 + 0.947i, & S_2(S_2(0)) \approx -0.4632 - 0.9332i, \end{array}$$

$$
\begin{array}{ll}
T_1^{-1}(S_2(0)) \approx 0.7928 + 0.5605i, & T_2^{-1}(S_2(0)) \approx -0.933 - 0.344i, \\
S_1^{-1}(S_2(0)) \approx 0.9198 - 0.38099i, & S_2^{-1}(S_2(0)) = 0, \\
T_1(T_1^{-1}(0)) = 0, & T_2(T_1^{-1}(0)) \approx -0.3809 + 0.9198i, \\
S_1(T_1^{-1}(0)) \approx 0.5605 + 0.7928i, & S_2(T_1^{-1}(0)) \approx -0.3447 - 0.9332i, \\
T_1^{-1}(T_1^{-1}(0)) \approx 0.947 + 0.292i, & T_2^{-1}(T_1^{-1}(0)) \approx -0.8763 - 0.4632i, \\
S_1^{-1}(T_1^{-1}(0)) \approx 0.9569 - 0.1641i, & S_2^{-1}(T_1^{-1}(0)) \approx -0.9036 + 0.4161i, \\
T_1(T_2^{-1}(0)) \approx 0.3809 - 0.9198i, & T_2(T_2^{-1}(0)) = 0, \\
S_1(T_2^{-1}(0)) \approx 0.3447 + 0.933i, & S_2(T_2^{-1}(0)) \approx -0.5605 - 0.7928i, \\
T_1^{-1}(T_2^{-1}(0)) \approx 0.8763 + 0.463i, & T_2^{-1}(T_2^{-1}(0)) \approx -0.9472 - 0.292i, \\
S_1^{-1}(T_2^{-1}(0)) \approx 0.9036 - 0.4161i, & S_2^{-1}(T_2^{-1}(0)) \approx -0.9569 + 0.1641i, \\
T_1(S_1^{-1}(0)) \approx 0.5605 - 0.7928i, & T_2(S_1^{-1}(0)) \approx -0.3447 + 0.933i, \\
S_1(S_1^{-1}(0)) = 0, & S_2(S_1^{-1}(0)) \approx -0.3809 - 0.9198i, \\
T_1^{-1}(S_1^{-1}(0)) \approx 0.9569 + 0.1641i, & T_2^{-1}(S_1^{-1}(0)) \approx -0.9036 - 0.4161i, \\
S_1^{-1}(S_1^{-1}(0)) \approx 0.9472 - 0.292i, & S_2^{-1}(S_1^{-1}(0)) \approx -0.8763 + 0.4632i, \\
T_1(S_2^{-1}(0)) \approx 0.3447 - 0.933i, & T_2(S_2^{-1}(0)) \approx -0.5605 + 0.7928i, \\
S_1(S_2^{-1}(0)) \approx 0.3809 + 0.9198i, & S_2(S_2^{-1}(0)) = 0, \\
T_1^{-1}(S_2^{-1}(0)) \approx 0.9036 + 0.4161i, & T_2^{-1}(S_2^{-1}(0)) \approx -0.9569 - 0.1641i, \\
S_1^{-1}(S_2^{-1}(0)) \approx 0.8763 - 0.463i, & S_2^{-1}(S_2^{-1}(0)) \approx -0.947 + 0.292i,
\end{array}
$$

*que novamente normalizados formam a figura com* 65 *pontos, como mostra a Figura* 5.3.

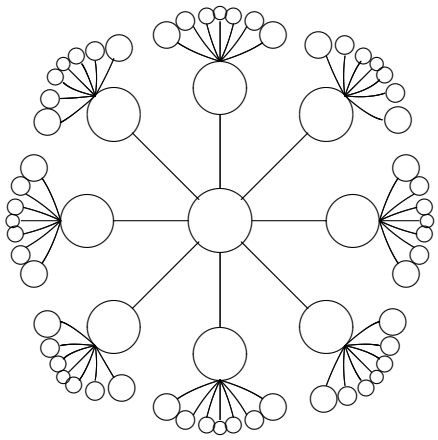

Figura 5.3: Nova Aplicação das transformações

*À medida que vamos aplicando as transformações estamos tesselando o disco de Poincaré, pois cada ponto representa um octógono, com o rótulo que acabamos de ver. Isso pode ser visto na Figura* 5.4*, onde o baricentro de cada octógono é um ponto da Figura* 5.3*.*

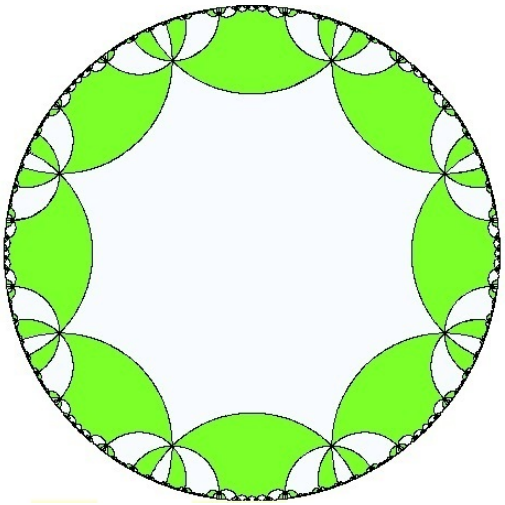

Figura 5.4: Tesselação gerada por octógonos

**Exemplo 5.2.2** *Para o caso* $g = 3$*, tomando a região fundamental* $P_{12}$*, dada por um dodecágono, que gerará a tesselação, novamente vamos colocá-la no centro do disco de Poincaré, e identificá-la como o ponto zero. Por [11] temos* 6 *transformações que realizam o pareamento dos lados deste polígono,* $T_1$*,* $T_2$*,* $T_3$*,* $S_1$*,* $S_2$ *e* $S_3$ *dadas por* $T_1(z) = \frac{az+c}{\bar{c}z+\bar{a}}$*,* $T_2(z) = \frac{-\bar{a}z-\bar{c}i}{ciz+a}$*,* $T_3(z) = \frac{-\bar{a}z+ci}{-\bar{c}iz+a}$*,* $S_1(z) = \frac{-\bar{a}z-\bar{c}}{-cz+a}$*,* $S_2(z) = \frac{-\bar{a}z+c}{\bar{c}z+a}$ *e* $S_3(z) = \frac{-\bar{a}z+\bar{c}}{-\bar{c}z+a}$ *onde* $a = \frac{(2+\sqrt{3})+i(3+2\sqrt{3})}{2}$ *e* $c = \frac{\sqrt{3+2\sqrt{3}}((-1+\sqrt{3})+i(1+\sqrt{3}))}{2}$ *são obtidos pela Proposição 3.3.2.*

*Analogamente ao caso* $g = 2$*, obtemos os rótulos dos pontos e tesselamos o plano hiperbólico, agora por dodecágonos como ilustra a Figura* 5.5*.*

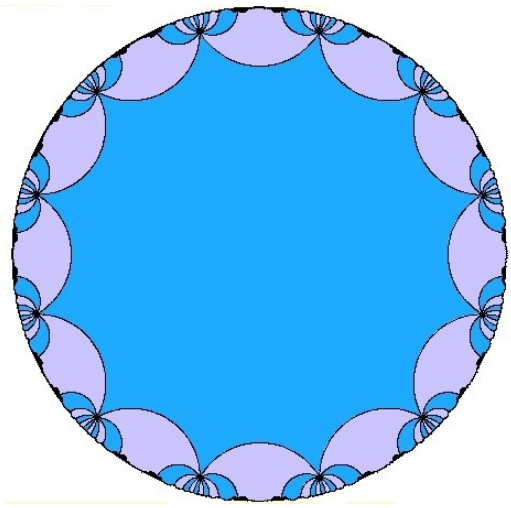

Figura 5.5: Tesselação gerada por dodecágonos

## 5.3 Códigos sobre Grafos

A seguir veremos alguns conceitos sobre grafos e códigos sobre grafos que serão úteis na próxima seção.

**Definição 5.3.1** *Seja* $0 \neq \alpha \in \mathcal{O} = (\theta, -1)_R$. *A distância sobre* $\mathcal{O}$ *é a distância induzida pelo grafo* $G_\alpha$. *Assim, se* $\eta,\ \tau \in \mathcal{O}$, *a distância é dada por:*

$$D_\alpha(\eta, \tau) = min\{|x_1| + |x_2| + 2|x_3| + 2|x_4| - 2|x_2x_3|\},$$

*tal que* $\tau - \eta \equiv x_1 + x_2i + x_2j + x_3k \ (mod\ \alpha)$, $x_i \in \mathbb{Z}$.

**Exemplo 5.3.1** *Novamente no Exemplo 5.1.4, para* $V = \frac{\mathcal{O}}{\langle\sqrt{2}+j\rangle}$. *Se* $\tau = 1$ *e* $\eta = i$, *temos* $\tau - \eta = 1 - i$, *logo* $D_\alpha(\eta, \tau) = 2$. *Se* $\tau = \frac{\sqrt{2}}{2}(1+i)$ *e* $\eta = \frac{\sqrt{2}}{2}(1-i)$, *temos* $\tau - \eta = \sqrt{2}i \equiv k(mod\ \alpha)$, *logo* $D_\alpha(\eta, \tau) = 2$.

Dada a distância $D_\alpha$, definimos um grafo gerado por $\alpha$, para $\alpha \in \mathcal{O}$.

**Definição 5.3.2** *Seja* $0 \neq \alpha \in \mathcal{O} = (\theta, -1)_{I_\mathbb{K}}$. *O grafo gerado por* $\alpha$ *é definido por* $G_\alpha = (V, E)$, *onde:*

1. $V = \frac{\mathcal{O}}{\langle\alpha\rangle}$ *é o conjunto de vértices;*
2. $E = \{(\eta, \tau) \in V \times V : D_\alpha(\eta, \tau) = 1\}$ *é o conjunto de arestas.*

**Exemplo 5.3.2** *No Exemplo 5.1.4 temos que* $\mathcal{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$, *o conjunto de vértices, é* $V = \frac{\mathcal{O}}{\langle\sqrt{2}+j\rangle}$ *e o conjunto de arestas satisfaz E.*

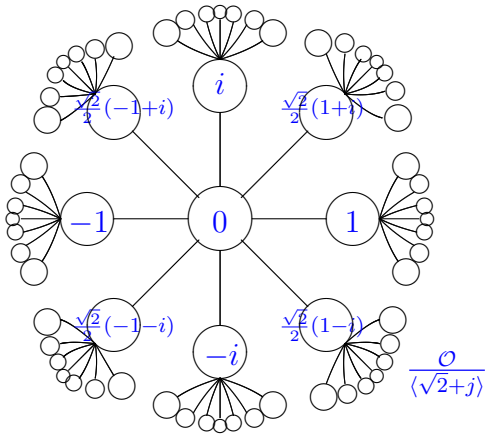


Figura 5.6: Rotulo dos baricentros dos octógonos

**Observação 5.3.1** *Note que a distância entre dois pontos $\eta$ e $\tau$ no grafo, nada mais é do que o menor número de arestas necessárias para ligar o ponto $\eta$ ao ponto $\tau$.*

Dado um grafo $G_\alpha$ com conjunto de vértices $V$ e distância $D_\alpha$, um código em $G_\alpha$ é um subconjunto não vazio $\mathcal{C}$ de $G_\alpha$. A região de Voronoi $V_\eta$ associada com $\eta \in \mathcal{C}$ é o subconjunto formado pelos elementos de $V$ para os quais $\eta$ é o ponto mais próximo em $\mathcal{C}$, ou seja, $V_\eta = \{\tau \in V; D(\eta,\tau) = D(\eta,\mathcal{C})\}$. O número $t = max\{D(\eta,\mathcal{C}); \eta \in V\}$ é chamado raio de cobertura do código. O raio de cobertura é o menor número $t$ tal que as bolas de raio $t$ centradas nos pontos de $\mathcal{C}$, dadas por $B_t(\eta) = \{\tau \in V : D(\eta,\tau) \leq t\}$ cobrem $V$. O número $\delta = min\{D(\eta,\tau) : \eta,\tau \in \mathcal{C}, \eta \neq \tau\}$ é a distância mínima de $\mathcal{C}$, e $\delta \leq 2t+1$, a igualdade vale quando as bolas de raio $t$ centradas nos pontos de $\mathcal{C}$ formam uma partição de $V$. Um código com esta propriedade é chamado *perfeito* e é dito corrigir $t$ erros. Um código é dito quase-perfeito se o mesmo é capaz de corrigir todos os padrões com até $t$ erros e alguns padrões com $t+1$ erros. Códigos perfeitos e quase-perfeitos fazem parte de uma classe mais geral de códigos chamados geometricamente uniformes, nos quais estamos interessados, e trataremos na próxima seção.

## 5.4 Códigos Geometricamente Uniformes sobre Ordens dos Quatérnios

Nesta seção utilizamos os conceitos obtidos nas seções anteriores e apresentamos códigos geometricamente uniformes derivados de grafos sobre anéis quocientes de ordens dos quatérnios.

Um código do espaço de sinais é definido como geometricamente uniforme se, para quaisquer duas sequências do código, existir uma isometria que leva uma sequência na outra enquanto deixa o código invariante. Assim, códigos geometricamente uniformes particionam um conjunto de pontos por regiões de Voronoi.

Dado um elemento $\alpha \in \mathcal{O}_R$, geramos uma constelação de sinais através do anel quociente $\frac{\mathcal{O}_R}{\langle\alpha\rangle}$. Assim, escolhendo $\beta$ divisor de $\alpha$ obtemos um código geometricamente uniforme, e a constelação de pontos é coberta por regiões fundamentais através de isometrias, como foi construído na Seção 5.1.

**Exemplo 5.4.1** *Para $g = 2$, dado $\alpha = 1 + 2\sqrt{2}j$, vimos no Exemplo 5.1.5 que $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 9$. Logo, pelo Teorema 5.1.1 a constelação possui $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha)^4 = 9^4 = 6561$ pontos. Como $\alpha = 1 + 2\sqrt{2}j$ pode ser escrito como $1 + 2\sqrt{2}j = (\sqrt{2}+j)^2$, segue que $\beta$ é um divisor à*

*direita de* $\alpha$ *e* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta) = 3 \in \mathbb{Z}$. *Portanto, o código gerado por* $\beta$, $< \beta > \subseteq \mathcal{O}$ *tem* $\left(\frac{Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha)}{Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta)}\right)^4 = \left(\frac{9}{3}\right)^4 = 81$ *palavras-código.*

**Exemplo 5.4.2** *Para* $g = 2$, *dado* $\alpha = 3j$, *temos que* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 9$. *Logo, pelo Teorema 5.1.1 a constelação possui* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha)^4 = 9^4 = 6561$ *pontos. Como* $\alpha = 3j$ *pode ser escrito como* $(1+\sqrt{2}j)(\sqrt{2}+j)$, *segue que* $\beta = \sqrt{2}+j$ *é um divisor à direita de* $\alpha$ *e* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta) = 3 \in \mathbb{Z}$. *Portanto, o código gerado por* $\beta$, $< \beta > \subseteq \mathcal{O}$ *tem* $\left(\frac{Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha)}{Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta)}\right)^4 = \left(\frac{9}{3}\right)^4 = 81$ *palavras-código.*

**Exemplo 5.4.3** *Para* $g = 2$, *dado* $\alpha = (3 + 4\sqrt{2}) + (2 + 2\sqrt{2})i + (2 + 2\sqrt{2})k$, *temos que* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 9$. *Logo, pelo Teorema 5.1.1 a constelação possui* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha)^4 = 9^4 = 6561$ *pontos. Como* $\alpha = (3 + 4\sqrt{2}) + (2 + 2\sqrt{2})i + (2 + 2\sqrt{2})k = ((1 + \sqrt{2}) + i + k)^2$, *segue que* $\beta = (1 + \sqrt{2}) + i + k$ *é um divisor à direita de* $\alpha$ *e* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta) = 3 \in \mathbb{Z}$. *Portanto, o código gerado por* $\beta$, $< \beta > \subseteq \mathcal{O}$ *tem* $\left(\frac{Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha)}{Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta)}\right)^4 = \left(\frac{9}{3}\right)^4 = 81$ *palavras-código.*

**Exemplo 5.4.4** *Para* $g = 2$, *dado* $\alpha = (1 + 4\sqrt{2}) + (2 + 2\sqrt{2})i + (4 + 2\sqrt{2})j + (2 + 2\sqrt{2})k$, *temos que* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha) = 25$. *Logo, pelo Teorema 5.1.1 a constelação possui* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha)^4 = 25^4 = 390625$ *pontos. Agora,* $\alpha = ((1+2\sqrt{2})+i+\sqrt{2}j+k)^2$, *logo* $\beta = (1+2\sqrt{2})+i+\sqrt{2}j+k$ *é um divisor à direita de* $\alpha$ *e* $Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta) = 5 \in \mathbb{Z}$. *Portanto, o código gerado por* $\beta$, $< \beta > \subseteq \mathcal{O}$ *tem* $\left(\frac{Nrd_{\mathbb{Z}[\sqrt{2}]}(\alpha)}{Nrd_{\mathbb{Z}[\sqrt{2}]}(\beta)}\right)^4 = \left(\frac{25}{5}\right)^4 = 625$ *palavras-código.*

**Exemplo 5.4.5** *Para* $g = 3$, *dado* $\alpha = 3j$, *temos novamente que* $Nrd_{\mathbb{Z}[\sqrt{3}]}(\alpha) = 9$. *Logo, pelo Teorema 5.1.1 a constelação possui* $Nrd_{\mathbb{Z}[\sqrt{3}]}(\alpha)^4 = 9^4 = 6561$ *pontos. Agora* $\alpha = 3j$ *pode ser escrito como* $(\sqrt{3})(\sqrt{3}j)$, *segue que* $\beta = \sqrt{3}j$ *é um divisor à direita de* $\alpha$ *e* $Nrd_{\mathbb{Z}[\sqrt{3}]}(\beta) = 3 \in \mathbb{Z}$. *Portanto, o código gerado por* $\beta$, $< \beta > \subseteq \mathcal{O}$ *tem* $\left(\frac{Nrd_{\mathbb{Z}[\sqrt{3}]}(\alpha)}{Nrd_{\mathbb{Z}[\sqrt{3}]}(\beta)}\right)^4 = \left(\frac{9}{3}\right)^4 = 81$ *palavras-código.*

Note que, pelos Teoremas 5.1.2 e 5.1.3, a menor norma possível é 3, logo os menores conjuntos de códigos possuem $3^4 = 81$ elementos e as menores constelações $9^4 = 6561$ pontos.

Os procedimentos adotados podem ser estendidos para superfícies de outros gêneros conhecendo a ordem dos quatérnios que está associada a ela, obtendo assim formas para a construção de novos códigos geometricamente uniformes sobre constelações de sinais diferentes.

# Capítulo 6

# Conclusões

Este trabalho pode ser dividido em dois resultados principais: a construção de códigos geometricamente uniformes derivados de grafos sobre quocientes de inteiros e a construção de códigos geometricamente uniformes derivados de grafos sobre quocientes de ordens dos quatérnios.

Em relação aos códigos geometricamente uniformes derivados de grafos sobre quocientes de inteiros, obtivemos um resultado para a geração de códigos quase-perfeitos, que além de serem geometricamente uniformes, são capazes de corrigir mais erros que os códigos perfeitos, observando que o custo de se obter códigos com maior capacidade de correção de erros é reduzir o número de vértices ou pontos sobre o mesmo anel quando comparado aos códigos perfeitos. Além disso, verificamos que os códigos perfeitos são obtidos de um caso particular dos códigos quase-perfeitos.

A segunda parte do trabalho apresenta códigos geometricamente uniformes sobre quocientes de ordens dos quatérnios, onde obtemos códigos no plano hiperbólico. A principal motivação para o estudo de códigos no plano hiperbólico vem da observação que o invariante topológico que melhora o desempenho de uma modulação é o gênero da superfície, e a geometria relativa à superfícies de gênero $g \geq 2$ é a geometria hiperbólica.

Em [11] e [12] foram estabelecidas as condições algébricas necessárias para o rotulamento de sinais de uma constelação geometricamente uniforme no plano hiperbólico. A proposta consistiu na busca de subgrupos normais com $p^m$ elementos, em grupos Fuchsianos aritméticos através da identificação destes grupos em ordens dos quatérnios $\mathcal{O}$ sobre um corpo $\mathbb{K}$.

Em nosso trabalho utilizamos as ordens associadas aos grupos Fuchsianos provenientes das tesselações do tipo $\{4g, 4g\}$. Inicialmente fizemos um estudo e obtemos resultados para a cardinalidade do quociente destas ordens dos quatérnios nos casos em que $g = 2^n$, $3.2^n$ e $5.2^n$,

similares aos obtidos para quocientes de anéis de inteiros. Apresentamos ainda um procedimento para o rotulamento de pontos gerados por tesselações do plano hiperbólico no disco de Poincaré, onde podemos notar que a geração de pontos cresce de forma muita rápida, assim como a cardinalidade do quociente de ordens dos quatérnios, e dessa forma os elementos do anel quociente podem ser representados geometricamente. Construímos então códigos geometricamente uniformes derivados de grafos sobre quocientes de ordens dos quatérnios, analogamente a construção feita sobre grafos derivados de quocientes de anéis dos inteiros.

## 6.1 Perspectivas para Trabalhos Futuros

Para finalizar gostaríamos de apresentar de modo sucinto alguns tópicos para dar prosseguimento a este trabalho:

- A identificação e o processo construtivo das subclasses de códigos perfeitos e quase-perfeitos dos códigos geometricamente uniformes sobre quocientes de ordens dos quatérnios apresentados.
- A construção de códigos geometricamente uniformes sobre o quocientes de ordens dos quatérnios provenientes de outras tesselações que foram identificadas em [12].
- A identificação da ordem dos quatérnios associada a família de tesselações do tipo $\{12g-6, 3\}$ que são as tesselações mais densas, como mostrado em [45], e a construção de códigos geometricamente uniformes sobre o quociente destas ordens.
- O estudo da cardinalidade de quocientes de ordens dos quatérnios que possuem a norma de seu elemento gerador não pertencente ao conjunto dos inteiros.
- O desenvolvimento de programas capazes de mostrar geometricamente as constelações e os códigos encontrados, visto que o número de pontos obtidos na geração cresce muito rapidamente.

# Referências Bibliográficas


[1] Slepian, D.; "Group codes for the Gaussian channel," *Bell Syst. Tech. J*, Vol. 47, pp. 575-602, April 1968.

[2] Forney, G. D.; "Geometrically uniform codes," *IEEE Trans. on Inform. Theory*, Vol. 37 No. 5, pp. 1241-1260, September 1991.

[3] Costa, S. I., Muniz, M., Agustini, E., Palazzo, R.; "Graphs, tessellations, and perfect codes on flat tori," *IEEE Trans. on Inform. Theory*, Vol. 50 No. 10, pp. 2363-2377, October 2004.

[4] Martínez, C., Beivide, R., Gabidulin, E.; "On the perfect t-dominating set problem in circulant graphs and codes over gaussian integers," *Proc. IEEE Intl. Symp. Information Theory*, Adelaide, Australia, September 2005, pp. 254-258.

[5] Martínez, C., Beivide, R., Gabidulin, E.; "Perfect codes from metrics induced by circulant graphs," *IEEE Trans. on Inform. Theory*, Vol. 53 No. 9, pp. 3042-3052, September 2007.

[6] Quilles, C., Palazzo, R.; "Quasi-perfect geometrically uniform codes derived from graphs over Gaussian integer rings," *Proc. IEEE Intl. Symp. Information Theory*, Austin, Texas, U.S.A. June 2010, pp. 1158-1162.

[7] Quilles, C., Palazzo, R.; "Quasi-perfect geometrically uniform codes Derived from graphs over integer rings,"submetido à *IEEE Transactions on Information Theory*.

[8] Brandani, E.; *Constelações de Sinais e Análise de desempenho no Plano Hiperbólico*. Tese de Doutorado, FEEC-UNICAMP, 2000.

[9] Agustini, E.; *Constelações de Sinais em Espaços Hiperbólicos*. Tese de Doutorado, IMECC-UNICAMP, 2002.

[10] Lazari, H.; *Uma contribuição à Teoria dos Códigos Geometricamente Uniformes Hiperbólicos*. Tese de Doutorado, FEEC-UNICAMP, 2000.

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

[12] Vieira, V.L.; *Grupos Fuchsianos Aritméticos Identificados em Ordens dos Quatérnios para Construção de Constelações de Sinais*. Tese de Doutorado, FEEC-UNICAMP, 2007.

[13] Faria, M.; *Coordenadas Fricke e Empacotamento Hiperbólico de Discos*. Tese de Doutorado, IMECC-UNICAMP, 2005.

[14] Albuquerque, C.D.; *Análise e Construção de Códigos Quânticos Topológicos sobre Variedades Bidimensionais*. Tese de Doutorado, FEEC-UNICAMP, 2009.

[15] Martínez, C., Beivide, R., Gabidulin, E.; "Perfect codes from Cayley graphs over Lipschitz integers,"*IEEE Trans. on Inform. Theory*, Vol. 55 No. 8, pp. 3552-3562, August 2009.

[16] Ribenboim, P.; *Algebraic Numbers*. Wiley-Interscience, 1972.

[17] Samuel, P.; *Algebraic Theory of Numbers*. Herman, Paris, 1967.

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

[19] Stewart, I., and Tall, D., *Algebraic Number Theory*. New York: Chapman-Hall, 1987.

[20] Oliveira, C. M.; *Discriminante, Ramificação e Diferente*. Dissertação de Mestrado, IBILCE-UNESP, 2005.

[21] O'Meara, O. T.; *Introduction to Quadratic Forms*. Springer-Verlag, Berlim-New York, 1973.

[22] Hungerford, T.W.; *Álgebra*. New York: Springer Verlag, 1974.

[23] Lang, S.; *Álgebra*. New York: Addison-Wesley, 1965.

[24] Marcus, D. A.; *Number Fields*. New York: Springer-Verlag, 1977.

[25] Washington, L. C.; *Introduction to Cyclotomic Fields*. New York: Board, 1982.

[26] Firer, M.; *Grupos Fuchsianos*. Notas de Aula, IMECC-UNICAMP, 2001.

[27] Katok, S.; *Fuchsian Groups*. The University of Chicago Press, 1992.

[28] Beardon, A.; *The Geometry of Discret Groups*. Springer-Verlag, New York, 1983.

[29] Takeuchi, K.; "A Characterization of Arithmetic Fuchsian Groups," *Journal Math. Soc. Japan*, Vol.27, No. 4, pp. $600 - 612$, 1975.

[30] Stillwell, J.; *Geometry of Surfaces*. Springer-Verlag, 2000.

[31] Firby, P.A. and Gardiner, C.F.; *Surface Topology*. Ellis Horwood Series in Mathematics and its Applications, England, 1991.

[32] Reiner, I.; *Maximal Orders*. Academic Press, London, 1975.

[33] Johansson, S.; *On Fundamental Domains of Arithmetic Fuchsian Groups*. www.math.chalmers.se/~ sj/forskning.html.

[34] Johansson, S.; *Genera of Arithmetic Fuchsian Groups*. www.math.chalmers.se/~ sj/forskning.html.

[35] Johansson, S.; *A Description of Quaternion Algebra*. www.math.chalmers.se/~ sj/forskning.html.

[36] Golomb, S.W., Welch, L.R.; "Perfect codes in the lee Metric and the packing of the polyominoes," *SIAM J. Applied Mathematics*, Vol. 18 No. 2, pp. 302-317, 1970.

[37] Huber, K. "Codes over Eisenstein-Jacobi integers," *Finite fields: theory, applications, and algorithms*, Las Vegas, NV, 1993, pp. 165-179.

[38] Faria, M.; *Empacotamento de Esferas em Espaços Hiperbólicos*. Dissertação de Mestrado, IMECC-UNICAMP, 2001.

[39] Nóbrega, T.P., Interlando, J.C., Lopes, J.O.D.; "The Discriminant of Abelian Number Fields," *Journal of Algebra and its Applications*, Vol.5, No. 1, pp. $1 - 7$, 2006.

[40] Nóbrega, T.P.; *Cúbicas Reais, Algumas Aplicações*. Anais do $VI$ Encontro de Álgebra USP-UNICAMP, 1997.

[41] Leech, J., Sloane, N.J.A. *Sphere Packing and Error- Correcting Code*. Canad. J. Math, v. 23, pp. 718-745, 1971.

[42] Forney, G.D., Gallager, G.R., Lang, G., Longstaff, F.M., Qureshi, S.U. *Eficient Modulation for Band-Limited Channels*. IEEE Transactions on Information Theory, v. 2, pp. 632-647, 1984.

[43] Sloane, N.J.A., Conway, J.H.; *Sphere Packing, Lattices and Groups*. Springer-Verlag, 1999.

[44] Craig, M. *A Cyclotomic Construction for Leech's Lattice*. Math. 25, pp.236-241, 1978.

[45] Bavard, C.; *Disques extrémaux et surfaces modulaires*. Annales de la Faculté des Sciences de Toulose, Vol. V, No. 2, pp. 191 – 202, 1996.

# Índice Remissivo


álgebra, 47
    central, 48
    de divisão, 50
    dos quatérnios, 48
    simples, 47

anel dos inteiros, 10
    de Einsenstein-Jacobi, 68
    de Gauss, 68
aplicação
    casada, 32
    de recobrimento, 42
area hiperbólica, 36

base, 6

código
    perfeito, 72
    quase-perfeito, 73
    sobre grafo, 70
característica, 13
comprimento de uma curva, 34
conjunto discreto, 24
constelação de sinais, 31
corpo
    algebricamente fechado, 11
    de números, 13
    quadrático, 14

densidade
    de centro, 30
    de empacotamento, 29
dimensão, 12
discriminante
    de uma álgebra dos quatérnios, 53
    de uma ordem dos quatérnios, 53
distância
    hiperbólica, 35
    induzida pelo grafo, 69
domínio, 6
    de Dirichlet, 41
    de ideais principais, 6

elemento
    algébrico, 11
    associado, 17
    inteiro, 7
    inteiro algébrico, 7
    redutível, 19
    transcendente, 11
empacotamento, 26, 29
espaço
    hiperbólico, 34
    quadrático, 23
estabilizador, 40
extensão algébrica, 11

família localmente finita, 40
fecho

algébrico, 11
inteiro, 10
forma quadrática, 22

geodésica, 35
grafo, 69
grupo
age de maneira propriamente descontínua, 40
projetivo linear, 38
unimodular, 37
grupo Fuchsiano, 40
aritmético, 56
assinatura de, 44
co-compacto, 43
derivado da álgebra dos quatérnios, 56
grupos comensuráveis, 56

ideal principal, 6
isometria, 39

lugar da álgebra dos quatérnios, 51

métrica hiperbólica, 34
módulo, 5
finitamente gerado, 6
livre, 6
livre de torção, 6
Noetheriano, 7
modelo
de Lobachevski, 35
de Poincaré, 36
monomorfismos, 13

número algébrico, 7
norma
de um elemento, 16
de um ideal, 21
mínima, 29

orbita, 40
ordem, 52

perfil de distância global, 32
polinômio minimal, 11

raio de cobertura, 70
região
de Voronoi, 31
fundamental, 23, 41
reticulado, 23
hiperbólico, 52
rotulamento casado, 32

submódulo, 6
subrupo discreto, 40

tesselação, 41
traço, 16

unidade, 17

vértice dominante, 71
volume
da região fundamental, 28
do reticulado, 29