Cintya Wink de Oliveira Benedito

Construção de Grupos Fuchsianos Aritméticos provenientes de Álgebras dos Quatérnios e Ordens Maximais dos Quatérnios Associados a Reticulados Hiperbólicos

Campinas
2014

Universidade Estadual de Campinas

Faculdade de Engenharia Elétrica e de Computação

Cintya Wink de Oliveira Benedito

Construção de Grupos Fuchsianos Aritméticos provenientes de Álgebras dos Quatérnios e Ordens Maximais dos Quatérnios Associados a Reticulados Hiperbólicos

Tese de doutorado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos exigidos para a obtenção do título de Doutora em Engenharia Elétrica. Área de concentração: Telecomunicações e Telemática.

Orientador: Reginaldo Palazzo Jr.
Co-orientadora: Cátia Regina de Oliveira Quilles Queiroz

Este exemplar corresponde à versão final da tese defendida pela aluna Cintya Wink de Oliveira Benedito, orientada pelo Prof. Dr. Reginaldo Palazzo Jr e co-orientada pela Profa. Dra. Cátia Regina de Oliveira Quilles Queiroz.

Campinas
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Área de Engenharia e Arquitetura
Rose Meire da Silva - CRB 8/5974

B434c

Benedito, Cintya Wink de Oliveira, 1985-
Construção de grupos fuchsianos aritméticos provenientes de álgebras dos quatérnios e ordens maximais dos quatérnios associados a reticulados hiperbólicos / Cintya Wink de Oliveira Benedito. – Campinas, SP : [s.n.], 2014.

Orientador: Reginaldo Palazzo Júnior.
Coorientador: Cátia Regina de Oliveira Quilles Queiroz.
Tese (doutorado) – Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Teoria de reticulados. 2. Teoria dos números algébricos. 3. Geometria hiperbólica. 4. Quatérnios. 5. Grupos discretos (Matemática). I. Palazzo Júnior, Reginaldo,1951-. II. Queiroz, Cátia Regina de Oliveira Quilles. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Construction of arithmetic fuchsian groups derived from quaternion algebras and maximal quaternion orders associated with hyperbolic lattices
Palavras-chave em inglês:
Lattice theory
Algebraic number theory
Hyperbolic geometry
Quaternion
Discrete groups
Área de concentração: Telecomunicações e Telemática
Titulação: Doutora em Engenharia Elétrica
Banca examinadora:
Reginaldo Palazzo Júnior [Orientador]
José Carmelo Interlando
Antonio Aparecido de Andrade
Sueli Irene Rodrigues Costa
Carina Alves
Data de defesa: 18-06-2014
Programa de Pós-Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE DOUTORADO

Candidato: Cintya Wink de Oliveira Benedito

Data da Defesa: 18 de junho de 2014

Título da Tese: "Construção de Grupos Fuchsianos Aritméticos Provenientes de Álgebras dos Quatérnios e Ordens Maximais dos Quatérnios Associados e Reticulados Hiperbólicos"

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

Prof. Dr. José Carmelo Interlando: José Carmelo Interlando

Prof. Dr. Antonio Aparecido de Andrade: [illegible]

Profa. Dra. Sueli Irene Rodrigues Costa: [illegible]

Profa. Dra. Carina Alves: Carina Alves

Resumo

Na busca por novos sistemas de comunicações muitos trabalhos têm sido realizados com o objetivo de obter constelações de sinais e códigos geometricamente uniformes no plano hiperbólico. Neste contexto, nossa proposta é identificar uma estrutura algébrica e geométrica para que códigos e reticulados possam ser construídos neste espaço. O problema central deste trabalho consiste em construir grupos fuchsianos provenientes de tesselações hiperbólicas regulares $\{p, q\}$ utilizando diversos tipos de emparelhamentos e identificá-los com álgebras e ordens dos quatérnios, definindo-os assim como aritmético. Desta forma, propomos um algoritmo para construir grupos fuchsianos aritméticos provenientes de tesselações hiperbólicas regulares $\{p, q\}$ cujo polígono hiperbólico regular gera uma superfície orientada de gênero maior ou igual a dois. Para isso, fornecemos uma condição necessária para que estes grupos possam ser obtidos, esta condição será denominada condição de Fermat devido a sua identificação com os números de Fermat. Através da construção destes grupos, mostramos que existe um isomorfismo entre dois grupos fuchsianos aritméticos provenientes de uma tesselação $\{p, q\}$ a partir de emparelhamentos diferentes. Além disso, descrevemos alguns dos corpos de números que utilizamos para construir grupos fuchsianos aritméticos, como subcorpos maximais reais de corpos ciclotômicos, a fim de propor uma relação entre os reticulados hiperbólicos e os reticulados euclidianos. Reticulados hiperbólicos completos obtidos através da identificação de grupos fuchsianos com ordens maximais dos quatérnios também são apresentados. Desta forma, obtemos um rotulamento completo dos pontos da constelação de sinal associada.

Palavras-chave: reticulado, geometria hiperbólica, álgebra dos quatérnios, ordem maximal dos quatérnios, grupo fuchsiano aritmético.

Abstract

In the search for new communications systems many studies have been conducted with the goal of obtaining signal constellations and geometrically uniform codes in the hyperbolic plane. In this context, our proposal is to identify an algebraic and geometric structures for constructing codes and lattices in this space. The central problem of this work is to construct fuchsian groups derived from hyperbolic tessellations $\{p, q\}$ using different edge-pairings sets and identify them with quaternion algebras and quaternion orders, by setting it as arithmetic. We also propose an algorithm to construct arithmetic fuchsian groups from a tessellation $\{p, q\}$ whose regular hyperbolic polygon generates an oriented and compact surface with genus greater or equal than 2. For that we provide a necessary condition for these groups to be obtained, this necessary condition is called Fermat condition due to its identification with the Fermat numbers. By the construction of these groups, it is also shown an isomorphism between two arithmetic fuchsian groups derived from a tessellation $\{p, q\}$ via different edge-pairings sets. Furthermore, we will describe some of the number fields that we use to construct arithmetic fuchsian groups as maximal real subfields of cyclotomic fields in order to propose a relationship between hyperbolic lattices and euclidean lattices. Complete hyperbolic lattices obtained by identifying fuchsian groups with maximal quaternion orders will also be presented. In this way we have a complete labeling of the points of the corresponding signal constellation.

Key-words: lattice, hyperbolic geometry, quaternion algebra, maximal quaternion order, arithmetic fuchsian group.

Sumário

Aos meus avós Isolina da Conceição e Domingos Benedito, *in memorian*.
DEDICO

Agradecimentos

Agradeço,

primeiramente a Deus, pela força, saúde e determinação que me deu para cumprir mais esta etapa em minha vida.

Ao meu orientador Prof. Dr. Reginaldo Palazzo Jr pela exímia orientação e convivência. Me sinto honrada por ter trabalhado e convivido com este ser humano tão espetacular. À minha co-orientadora Profa. Dra. Cátia Regina de Oliveira Quilles Queiroz pela colaboração, sugestões e leitura instrutiva.

Aos membros da banca examinadora pelos valiosos comentários e sugestões. Em especial ao Toninho, por quem tenho o maior respeito e admiração como pessoa e profissional e que fez parte da minha trajetória acadêmica como orientador de iniciação científica e mestrado. E ao Prof. Carmelo pela agradável convivência, dedicação e orientação durante o período em que estive na SDSU sob sua supervisão.

Aos professores da FEEC-UNICAMP pelos ensimanentos transmitidos durante as disciplinas e aos funcionários pela prestatividade.

Aos meus avós Domingos Benedito (in memorian) e Isolina da Conceição (in memorian) a quem dedico este trabalho, pois através de sua educação e amor me fizeram o que sou.

Aos meus pais, Gaudeley de Oliveira Benedito (in memorian) e Denise Wink, e aos demais membros da minha família, por todo amor e que, mesmo sem perceber, ao mostrar o orgulho e confiança que depositavam em mim me davam forças para continuar. Em especial, aos meus irmãos Erika, Fabio e Lilian, às minhas tias Marlene, Vera e Deise, e à minha cachorra Winnie.

Aos meus colegas do laboratório LTIA: Lucila, Clarice, Andrea, Daniel, Fernando, Nelson, Mario, Luiz, Diogo, Gustavo, Leandro, Cibele, Lucas e Akemi. Em especial, aos meus amigos queridos Anderson e Maicon que estiveram comigo em todos os momentos desde o início desta caminhada. E à Luzinete e Cátia pela convivência e ensinamentos vividos durante o período que passamos na SDSU.

Às minhas amigas queridas Grasi, Rosy, Nati, Mari, Fer e Carina pela amizade que se iniciou ou se fortaleceu durante este período e que, tenho certeza, levarei por toda a minha vida. Obrigada amigas pelos momentos que vivemos neste período. Amo vocês!

Aos meus amigos de Rio Preto, em especial aos meus grandes amigos Jucilene e Gustavo, que mesmo distante se fazem presentes em todos os momentos de minha vida.

Aos meus amigos de Bom Jardim de Minas, pelas amizades e momentos que guardo com carinho. Em especial, às minhas amigas de infância do TC: Andreza, Bruna, Deisiane, Elisângela, Flavia, Kelly, Livia, Rafaela e Vitória.

My California girls Juliana, Andressa, Daiana e Ana por terem vivido comigo uma das melhores fases da minha vida, lembranças e momentos que jamais serão esquecidos. Love you my girls!

Às minhas lindas da república Atacama: Dani, Mari, Debs, Lu, Le, Ana, Nathi e Di, pela alegria, juventude e agradável convivência.

Ao Alexandre, que mesmo aparecendo em minha vida no final desta jornada, fez toda a diferença.

Aos alunos que tive neste período que me ajudaram a crescer como profissional e amar ainda mais a minha profissão.

Ao CNPq pelo auxílio financeiro.

À todos que direta ou indiretamente contribuiram para a realização deste trabalho.

Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes.

Martin Luther King

Lista de Figuras

Lista de Tabelas

Lista de Acrônimos e Notação

$\mathbb{C}$	conjunto dos números complexos
$\mathbb{R}$	conjunto dos números reais
$\mathbb{Q}$	conjunto dos números racionais
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{N}$	conjunto dos números naturais (incluindo o zero)
$\mathbb{K}, \mathbb{L}, \mathbb{F}$	corpos
$\mathcal{I}_{\mathbb{K}}$	anel dos inteiros do corpo $\mathbb{K}$
$\mathbb{K}/\mathbb{L}$	extensão de corpos
$[\mathbb{K} : \mathbb{L}]$	grau da extensão $\mathbb{K}/\mathbb{L}$
$Gal(\mathbb{K}/\mathbb{L})$	grupo de Galois de $\mathbb{K}$ sobre $\mathbb{L}$
$A[x]$	anel de polinômios com coeficientes em A
$\mathfrak{I}, \mathfrak{p}, \mathfrak{m}, \mathfrak{a}$	ideais
$A/\mathfrak{I}$	anel quaciente
$M(2, \mathbb{K})$	espaço das matrizes 2×2 com coeficientes no corpo $\mathbb{K}$
$\mathbb{H}^2$	semi-plano superior
$\mathbb{D}^2$	disco de Poincaré
T	transformação de Möbius
$\mathcal{P}_p$	polígono hiperbólico de p lados
$\mathcal{A}$	álgebra dos quatérnios
$\mathcal{O}$	ordem dos quatérnios
$\mathcal{M}$	ordem maximal dos quatérnios
$\mathrm{PSL}(2, \mathbb{R})$	grupo projetivo linear
$\mathrm{SL}(2, \mathbb{R})$	grupo das matrizes reais de ordem 2 com determinante 1
Γ	grupo fuchsiano
$\Gamma(\mathcal{A}, \mathcal{O})$	grupo derivado de uma álgebra dos quatérnios $\mathcal{A}$ cuja ordem dos quatérnios é $\mathcal{O}$
$\{p, q\}$	tesselação hiperbólica
Γ_p	grupo fuchsiano associado a tesselaçãp $\{p, q\}$
$\mathbb{H}^2/\Gamma$	espaço quociente $\mathbb{H}^2$ por Γ localmente isométrico a $\mathbb{H}^2$

$Tr(\alpha)$	traço do elemento α
$\mathcal{N}(\alpha)$	norma do elemento α
$Trd(\alpha)$	traço reduzido do elemento α
$Nrd(\alpha)$	norma reduzida do elemento α
$\mathcal{D}$	discriminante
$tr(M)$	traço da matriz M
$det(M)$	determinante da matriz M
I_d	matriz identidade de dimensão d
∂A	fronteira de um conjunto A
$\mu(A)$	área hiperbólica de um conjunto A
$\|A\|$	cardinalidade do conjunto A
id	função identidade
f'	derivada da função f
$p(x)$	polinômio minimal
ζ_n	raiz n-ésima da unidade
$Re(z)$	parte real do número complexo z
$Im(z)$	parte imaginária do número complexo z
$\overline{a}$	conjugado do elemento a
$arg(a)$	argumento do elemento a
$\|a\|$	valor absoluto do elemento a
$mdc(a,b)$	máximo divisor comum entre os elementos a e b
$\circ$	operação composição de funções
$\otimes$	produto tensorial
$\sum$	somatório
$\prod$	produtório

Introdução Geral

A teoria de códigos corretores de erros surgiu com o artigo seminal do matemático Claude A. Shannon, [46]. Neste artigo foi mostrado que dado um canal de comunicação digital é possível, com uma codificação adequada, transmitir informações com probabilidade de erro arbitrariamente pequena, desde que a uma taxa menor que uma constante que depende do sistema e chamada *capacidade do canal*. Quando transmitimos uma informação existe a possibilidade da mensagem recebida ser diferente da mensagem enviada. Assim, esta teoria surgiu da necessidade de detectar e recuperar a mensagem enviada ao receptor, e com isso poder construir códigos com probabilidade de erro tão pequena quanto desejado. Diferentes técnicas e abordagens, as quais objetivam otimizar a eficiência da transmissão dentro de características específicas do canal de transmissão de sinais têm sido desenvolvidas desde então.

Um dos parâmetros para se encontrar bons códigos corretores de erros está ligado ao problema do empacotamento de esferas, que surgiu a partir do 18º Problema de Hilbert, que é uma forma de dispor esferas no espaço euclidiano de modo a cobrir a maior parte do espaço. Este problema é denominado empacotamento esférico e, quando o conjunto dos centros das esferas formam um subgrupo discreto do $\mathbb{R}^n$ então estes empacotamentos passam a se chamar empacotamentos reticulados, [16]. O interesse pela teoria de reticulados, no contexto dos sistemas de comunicações digitais, foi estimulado pela sua conexão com a teoria dos números, teoria de grupos e teoria da codificação. Neste caso, devemos ressaltar que a teoria dos reticulados demonstrou ser uma ferramenta de grande importância para o problema de empacotamento de esferas, auxiliando na construção de códigos ótimos dentro do contexto dos trabalhos de Nyquist e Shannon, [16]. Além disso, constelações de sinais tendo estrutura de reticulados apresentam alta eficiência espectral na transmissão, [9].

Quando consideramos a informação transmitida através de um sistema de comunicação, esta informação sempre estará sujeita a um conjunto de interferências provenientes do canal de transmissão, o qual chamamos *ruído*. O processamento de sinal a ser utilizado na transmissão com o objetivo de reduzir a ação do ruído pode ser realizada de diversas maneiras, como por exemplo, via modulação ou codificação. Dependendo do tipo de canal, os dígitos que constituem a palavra-código devem ser associados à formas de ondas apropriadas para transmissão. O responsável por essa transformação é o modulador. A forma de atuação do modulador é através de mudanças na amplitude e/ou frequência e/ou fase em um sinal padrão. Algumas destas técnicas são conhecidas como:

- PSK (phase shift-keying): modulação por chaveamento de fase.
- QAM (quadrature amplitude modulation): modulação em amplitude por quadratura.

Como estamos interessados em sistemas discretos, o modulador deve gerar um sinal contínuo (analógico) de duração T segundos para cada dígito, ou grupo de dígitos, da palavra-código. Desta forma, a transmissão da sequência de sinaism, correspondente às palavras-código, é chamada transmissão digital.

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 (Figura 1.*a)*), e por um quadrado para a modulação QAM (Figura 1.*b)*). 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 seja 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 às 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, [42].

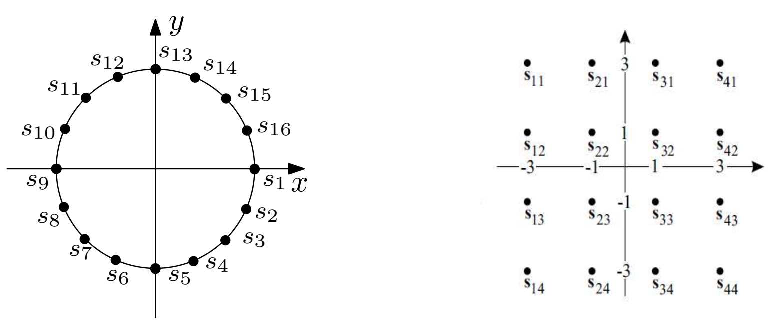

Figura 1: *a)* 16-*PSK* *b)* 16-*QAM*

O conceito de códigos geometricamente uniformes, introduzido por Forney [23], está fortemente ligado com a existência de tesselações regulares em espaços homogêneos. Esta classe de códigos proposta por Forney engloba a classe de códigos de grupo de Slepian [47], e os códigos reticulados, e permite 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 esperada. Desde então, procurou-se ampliar este novo conceito de códigos bem como estabelecer condições para generalizações e possíveis extensões para esta classe importante de códigos, como pode ser visto em [17] e [14], por exemplo. A probabilidade de erro associada a um sistema de comunicação, quando se considera constelações de sinais geometricamente uniformes no plano hiperbólico, depende do gênero da superfície, superfície esta que pode ser vista como um polígono regular hiperbólico, e conforme o que foi exposto anteriormente, estaremos interessados em superfícies de gênero $g \geq 2$. Algebricamente, estas constelações de sinais são geradas por grupos, mais precisamente, por grupos de isometrias do espaço em que a constelação está inserida. Para constelações no plano hiperbólico, um de nossos objetivos é encontrar o grupo que age transitivamente no polígono regular hiperbólico, os grupos fuchsianos, no intuito de gerar tais constelações. Neste sentido, consideramos reticulados no plano hiperbólico, o qual é definido como uma ordem de uma álgebra dos quatérnios devido a associação destas ordens com um grupo fuchsiano. Esta é a estrutura algébrica a partir da qual a construção de constelações de sinais pode ser realizada.

Alguns trabalhos já existentes na literatura apresentam estudos sobre constelações de sinais geometricamente uniformes provenientes de tesselações hiperbólicas regulares $\{p, q\}$, onde q polígonos regulares de p arestas se encontram em cada vértice. Em trabalhos pioneiros nesta área Brandani em [10], considera tesselações auto-duais $\{p, p\}$. Lazari em [33], propõe a construção de constelações de sinais geometricamente uniformes no plano hiperbólico através do processo de construção de cadeias de partições geometricamente uniformes. Para esta construção, Lazari utiliza o grupo de isometrias do octógono, região fundamental da tesselação $\{8, 8\}$, e o grupo de isometrias do p-ágono da tesselação $\{p, 3\}$. Já Agustini em [1], constrói famílias de constelações de sinais provenientes de quocientes de espaços hiperbólicos por grupos discretos de isometrias.

Ainda neste contexto, Carvalho em [13], considera as tesselações do tipo $\{4g, 4g\}$, para $g = 2$ e 3, e Vandemberg em [53], considera a mesma tesselação porém para $g = 2^n$, 3.2^n e 5.2^n, de modo que os grupos fuchsianos aritméticos formados por elementos que fazem o pareamento dos lados dos polígonos obtidos por estas tesselações, são identificados com as ordens dos quatérnios, e o rotulamento de algumas constelações de sinais geometricamente uniformes particulares para $g = 2$, 3 e 4 foi obtido. Os grupos fuchsianos que estamos interessados são aqueles derivados de uma álgebra e uma ordem dos quatérnios. Assim, conhecidas as ordens dos quatérnios que fazem o pareamento dos lados dos polígonos, Queiroz em [42], apresenta resultados para quocientes de ordens dos quatérnios análogos aos obtidos para quocientes de anéis dos inteiros, com o intuito de construir códigos geometricamente uniformes derivados de grafos sobre o quociente destas ordens. Sob o ponto de vista geométrico e combinatorial, Albuquerque em [2], apresenta tabelas de possíveis códigos no plano hiperbólico, com aplicações na codificação quântica, chamados códigos quânticos topológicos.

Um grupo fuchsiano Γ é um grupo discreto de isometrias no plano hiperbólico. A teoria de grupos fuchsianos é muito acessível devido a existência de modelos euclidianos para o espaço hiperbólico. Quando um grupo fuchsiano é derivado de uma álgebra dos quatérnios $\mathcal{A} = (a, b)_{\mathbb{K}}$ cuja ordem dos quatérnios associada é $\mathcal{O} = (a, b)_R$, com $a, b \in R$ e R é um anel de um corpo de números $\mathbb{K}$, então dizemos que Γ é um grupo fuchsiano aritmético, [30]. É de grande dificuldade obter estes grupos para qualquer tesselação $\{p, q\}$. Em [13] e [53], foram obtidos alguns casos de tesselações $\{p, q\}$ em que é possível obter o grupo fuchsiano aritmético associado. O caso $\{4g, 4g\}$, para $g = 2^n, 3 \cdot 2^n, 5 \cdot 2^n$, mencionado acima são exemplos destes casos. Mas, permanece a necessidade de saber quando é possível obter o grupo fuchsiano aritmético associado a qualquer tesselação $\{p, q\}$, pois fazendo uso destes grupos é que códigos geometricamente uniformes para gênero $g \geq 2$ podem ser obtidos. Devido a essa necessidade, um dos objetivos deste trabalho é obter uma condição necessária para conseguir obter grupos fuchsianos aritméticos a partir de uma tesselação $\{p, q\}$ qualquer. Chamamos esta condição de condição de Fermat devido a sua identificação com os números de Fermat. Ainda com o objetivo de construir constelações de sinais no espaço hiperbólico, destacamos neste trabalho a importância de que a ordem dos quatérnios a ser associada ao grupo fuchsiano seja a maximal, pois quando isto ocorre temos um rotulamento completo dos pontos da constelação de sinais obtida.

A grosso modo, um reticulado é um conjunto discreto de pontos. Usualmente, reticulados são definidos em espaços euclidianos e desta forma, um reticulado é um conjunto discreto de pontos no $\mathbb{R}^n$. Porém, no plano euclidiano os únicos reticulados totalmente regulares são aqueles formados somente por triângulos equiláteros, quadrados e hexágonos regulares. Já se considerarmos reticulados em espaços hiperbólicos, podemos defini-los como conjuntos discretos de pontos em modelos hiperbólicos como $\mathbb{H}^2$, conhecido como semi-plano superior, ou $\mathbb{D}^2$ conhecido como disco de Poincaré. Para o caso do plano hiperbólico existem infinitas possibilidades de reticulados regulares os quais estão associados a tesselações regulares $\{p, q\}$.

Dessa forma, considerando o espaço hiperbólico, o projetista de um sistema de comunicações terá a seu dispor uma infinidade de tesselações hiperbólicas de onde poderá selecionar a constelação de sinais mais apropriada para a aplicação que está sendo considerada. Como citado anteriormente, estamos interessados em grupos fuchsianos obtidos a partir do pareamento dos lados de um polígono hiperbólico que tessela o plano hiperbólico. É conhecido que existem vários tipos de emparelhamentos de arestas que nos fornecem as isometrias do grupo fuchsiano, [40], desta forma, é também de grande interesse verificar se existe uma relação entre os grupos fuchsianos obtidos através de diferentes emparelhamentos. Por exemplo, em codificação quântica topológica o emparelhamento diametralmente oposto é o mais desejado, pois este é o caminho homologicamente não trivial com a maior distância mínima possível, [2]. Como consequência, o código resultante apresenta uma capacidade de correção de erros maior dentre todos os códigos oriundos dos demais emparelhamentos. Já o emparelhamento normal das arestas, apresenta uma menor complexidade computacional dentre diversos emparelhamentos. Assim, provado que existe uma relação entre grupos fuchsianos oriundos de emparelhamentos diferentes, podemos utilizar, neste caso por exemplo, o emparelhamento normal das arestas, para estudar grupos fuchsianos aritméticos (quando estes existem) obtidos através do emparelhamento diametralmente oposto.

Dentre os diversos tipos de tesselações regulares hiperbólicas $\{p, q\}$ existentes, para o desenvolvimento das propostas deste trabalho iremos focar em algumas delas: $\{4g, 4g\}$, $\{4g+2, 2g+1\}$ e $\{12g-6, 3\}$. Veremos que para a tesselação auto-dual $\{4g, 4g\}$ será possível construir grupos fuchsianos aritméticos para diversos valores de $g \geq 2$ e, esta tesselação apresenta uma baixa complexidade computacional devido a sua autodualidade, [8]. Além disso, em [13, 42, 53], os autores propuseram construções de códigos geometricamente uniformes no plano hiperbólico utilizando a tesselação $\{4g, 4g\}$, e em [42], foi feito um rotulamento de pontos gerados por esta tesselação para alguns valores de g. Já a tesselação $\{4g+2, 2g+1\}$ é uma tesselação mais densa que a tesselação auto-dual $\{4g, 4g\}$ e, para esta tesselação assim como para $\{4g, 4g\}$, é possível obter o grupo fuchsiano utilizando o emparelhamento diametralmente oposto das arestas, que como já citamos, é o emparelhamento mais desejado em codificação quântica topológica, [2]. A tesselação $\{12g-6, 3\}$ é a tesselação mais densa dentre todas as tesselações hiperbólicas, ou seja, esta tesselação apresenta densidade de empacotamento ótima, [6]. Além disso, as tesselações $\{4g + 2, 2g + 1\}$ e $\{12g - 6, 3\}$ foram utilizadas em [20] para projetar os pontos do espaço de Teichm$\ddot{u}$ller no espaço dos polígonos com $4g + 2$ e $12g - 6$ arestas através de coordenadas Fricke, onde ainda o autor relacionou o estudo de empacotamento de esferas com a teoria de Teichm$\ddot{u}$ller.

Uma outra proposta que apresentamos neste trabalho, é sobre a possibilidade de associar reticulados euclidianos com reticulados hiperbólicos. Utilizando grupos Kleinianos, Alves e Belfiore em [3], apresentam uma construção do reticulado E_8 através de ordens maximais dos quatérnios. Além disso, existem diversos trabalhos na literatura, como por exemplo [4, 5, 7, 29], que apresentam maneiras de construir versões rotacionadas de reticulados conhecidos utilizando a teoria algébrica dos números, mais precisamente corpos ciclotômicos. Dessa forma, motivados pelo Teorema de Kronecker-Weber, que diz que toda extensão abeliana finita dos racionais está contida em um corpo ciclotômico, durante o nosso trabalho observamos que os corpos de números associados a álgebras dos quatérnios podem ser descritos como subcorpos maximais reais de certos corpos ciclotômicos. Para estes corpos de números, foram obtidas versões rotacionadas do reticulado D_n em [29] e, conjecturado por Giraud et al., em [25], que poderiam ser utilizados para construir um reticulado $\mathbb{Z}^n$-rotacionado. Sendo assim, acreditamos que com a associação de grupos fuchsianos aritméticos e subcorpos maximais reais de corpos ciclotômicos, será possível mostrar relações entre os reticulados hiperbólicos, caracterizados por ordens maximais dos quatérnios, com versões rotacionadas do reticulado $\mathbb{Z}^n$ ou do reticulado D_n.

Em síntese, o problema central deste trabalho consiste em construir grupos fuchsianos provenientes de tesselações hiperbólicas regulares $\{p, q\}$ utilizando diversos tipos de emparelhamentos e identificá-los com álgebras e ordens dos quatérnios, definindo-os desta forma como aritméticos. O objetivo central com a construção destes grupos, é fornecer uma ferramenta algébrica para que constelações de sinais e códigos geometricamente uniformes no plano hiperbólico possam ser obtidos. Para tal proposta, este trabalho foi estruturado da seguinte forma.

No Capítulo 1, apresentamos os pré-requisitos que são utilizados no decorrer deste trabalho na área de álgebra, topologia e geometria hiperbólica. As definições e resultados apresentados neste capítulo servem de base para os capítulos posteriores. Iniciamos apresentando alguns conceitos algébricos, geométricos e sobre a teoria algébrica dos números. Em seguida, apresentamos um estudo mais aprofundado sobre geometria hiperbólica que será o ambiente onde este trabalho é desenvolvido, para isso definimos os modelos hiperbólicos que são utilizados assim como as tesselações regulares no plano hiperbólico.

No Capítulo 2, temos o objetivo de apresentar a ferramenta algébrica fundamental deste trabalho: os grupos fuchsianos aritméticos. Com este propósito, iniciamos apresentando os conceitos de grupos fuchsianos, álgebra e ordem dos quatérnios, além dos principais resultados envolvendo tais conceitos. Após esta primeira abordagem, apresentamos os resultados de Takeuchi, [51], e Katok, [30], que mostram como é feita a identificação de forma natural entre os grupos fuchsianos e uma álgebra dos quatérnios. A partir desta identificação, podemos associar, via isomorfismo, os elementos dos grupos fuchsianos com os elementos de uma ordem dos quatérnios, sendo possível então definir estas ordens dos quatérnios como reticulados hiperbólicos. Neste sentido, finalizamos o capítulo apresentando definições e propriedades de tais reticulados.

No Capítulo 3, começamos a apresentar as nossas contribuições. Neste capítulo, apresentamos uma condição necessária para a construção de grupos fuchsianos aritméticos, condição estabelecida no Teorema 3.1.3, o qual chamamos de condição de Fermat. Propomos um algoritmo para obter os geradores de um grupo fuchsiano aritmético, pois através dos geradores do grupo é que identificamos qual é a álgebra e a ordem dos quatérnios associada. Este algoritmo pode ser implementado em *softwares* como Maple e Mathematica. Utilizando a condição de Fermat e o algoritmo proposto, construímos grupos fuchsianos aritméticos considerando as tesselações regulares hiperbólicas $\{4g, 4g\}$, $\{4g+2, 2g+1\}$ e $\{12g-6, 3\}$.

No Capítulo 4, apresentamos as demais contribuições de nosso trabalho. A partir das construções propostas no Capítulo 3, mostramos que existe um isomorfismo entre grupos fuchsianos aritméticos obtidos a partir de diferentes emparelhamentos, descrevemos alguns dos corpos de números que utilizados na construção dos grupos fuchsianos aritméticos, como subcorpos maximais reais de corpos ciclotômicos. E, por fim, apresentamos as ordens maximais dos quatérnios, ou equivalentemente os reticulados hiperbólicos completos, associados à alguns grupos fuchsianos aritméticos obtidos no Capítulo 3.

Para finalizar, no Capítulo 5, apresentamos as conclusões, perspectivas e as publicações decorrentes deste trabalho, além de sugestões para trabalhos futuros.

Observamos que no decorrer de todo o texto apresentamos algumas demonstrações de resultados já provados nas referências citadas com o objetivo de facilitar a leitura e compreender as conexões entre tais resultados e os resultados apresentados neste trabalho.

Capítulo 1

Conceitos Preliminares

Na busca por novos sistemas de comunicações, em [1,10,13,33,42,53], os autores propuseram, de forma independente, construções de constelações de sinais geometricamente uniformes no plano hiperbólico associadas à tesselações hiperbólicas. Nesta direção, o objetivo central deste trabalho é fornecer condições para que estas constelações possam ser obtidas considerando tanto o ponto de vista algébrico quanto o geométrico.

Para tal desenvolvimento, faz-se necessária uma revisão de conceitos e propriedades associadas de álgebra, topologia e teoria algébrica dos números. Além disso, os principais conceitos e resultados sobre a geometria hiperbólica, geometria na qual este trabalho está inserido, também são fundamentais para o desenvolvimento deste trabalho.

Neste contexto, este capítulo é dedicado a apresentar um breve estudo dos conceitos básicos de álgebra, na Seção 1.1, e dos conceitos básicos de topologia, na Seção 1.2. Na Seção 1.3, apresentamos os elementos da teoria algébrica dos números que são utilizados neste trabalho. E para finalizar, na Seção 1.4, apresentamos um estudo sobre a geometria hiperbólica tendo como enfoque os modelos hiperbólicos e as tesselações hiperbólicas.

1.1 Conceitos Básicos de Álgebra

Nesta seção, apresentamos alguns conceitos básicos de álgebra que utilizamos frequentemente no decorrer do trabalho. Apesar desta teoria ser muito rica em resultados importantes, focamos apenas em alguns conceitos principais. Para um estudo mais detalhado sugerimos as referências [24, 26, 32, 38].

1.1.1 Anéis, Corpos e Módulos

Apresentamos, a seguir, as definições de grupos, anéis, corpos, ideais, módulos e, algumas de suas principais propriedades.

Definição 1.1.1 *Um conjunto não vazio G com uma operação $*$ sobre G é chamado* **grupo** *se essa operação satisfaz as seguintes propriedades:*

(i) $(a * b) * c = a * (b * c)$*, para todo* $a, b, c \in G$ *(associativa);*

(ii) *existe* $e \in G$ *tal que* $a * e = e * a = a$, *para todo* $a \in G$ *(existência de elemento neutro);*

(iii) *para todo* $a \in G$ *existe um elemento* $a' \in G$ *tal que* $a * a' = a' * a = e$ *(existência do elemento simétrico).*

Se além disso a operação $*$ for comutativa, isto é, $a * b = b * a$, para todo $a, b \in G$, o grupo é chamado **abeliano** ou **comutativo**.

Definição 1.1.2 *Um conjunto não vazio* A *e um par de operações* $+$ *(adição) e* $\cdot$ *(multiplicação) sobre* A *é chamado* **anel** *se* A *é um grupo abeliano em relação à operação* $+$ *e se a multiplicação satisfaz:*

(i) $a(bc) = (ab)c$, *para todo* $a, b, c \in A$ *(associativa);*

(ii) $a(b + c) = ab + ac$ *e* $(a + b)c = ac + bc$, *para todo* $a, b, c \in A$ *(distributiva).*

Definição 1.1.3 *Nas condições da Definição 1.1.2 ainda tem-se que:*

(i) *Quando a operação de multiplicação no anel* A *satisfaz* $ab = ba$, *para todo* $a, b \in A$, *dizemos que* A *é um* **anel comutativo**.

(ii) *A multiplicação pode admitir um elemento neutro, isto é, existe* $1 \in A$ *tal que* $a1 = 1a = a$, *para todo* $a \in A$. *Neste caso, dizemos que* A *é um* **anel com unidade**.

(iii) *Um anel cuja multiplicação é comutativa e que possui unidade é chamado* **anel comutativo com unidade**.

Definição 1.1.4 *Um subconjunto não vazio* B *de um anel* A *é um* **subanel** *de* A *se* B *é um anel com as mesmas operações de* A *porém restritas aos elementos de* B.

Definição 1.1.5 *Sejam* A *e* B *dois anéis com elementos identidades* 1_A *e* 1_B, *respectivamente. Uma aplicação* $\phi : A \to B$ *é um* **homomorfismo de anéis** *de* A *em* B *se satisfaz as seguintes condições:*

(i) $\phi(x + y) = \phi(x) + \phi(y)$, *para todo* $x, y \in A$;

(ii) $\phi(xy) = \phi(x)\phi(y)$, *para todo* $x, y \in A$;

(iii) $\phi(1_A) = 1_B$.

Definição 1.1.6 *Chamamos* **monomorfismo** *um homomorfismo injetor e* **isomorfismo** *um homomorfismo bijetor. O isomorfismo de um anel* A *sobre si mesmo é chamado* **automorfismo**.

Definição 1.1.7 *Seja* A *um anel comutativo. Um subconjunto* $\mathfrak{I} \subset A$, $\mathfrak{I} \neq \emptyset$, *é chamado* **ideal** *em* A *se, para quaisquer* $x, y \in \mathfrak{I}$ *e para qualquer* $a \in A$, *as seguintes condições são satisfeitas:*

(i) $x - y \in \mathfrak{I}$;

(ii) $ax \in \mathfrak{I}$.

Definição 1.1.8 *Seja A um anel comutativo com unidade.*

(i) Dizemos que um elemento $a \in A$ é um **divisor de zero** *se existe um elemento não nulo $b \in A$ tal que $ab = ba = 0$. Se, além disso, $a \neq 0$, então dizemos que a é um* **divisor próprio de zero***.*

(ii) Quando A não possui divisores próprios de zero dizemos que A é um **domínio de integridade***.*

Definição 1.1.9 *Seja A um anel. Um ideal $\mathfrak{I}$ gerado por um elemento $a \in A$, isto é, $\mathfrak{I} = \langle a \rangle = \{ax|\ x \in A\}$, é chamado* **ideal principal** *gerado por a. Se todo ideal do anel A é principal, então dizemos que A é um* **anel principal***. Em particular, se A é um domínio de integridade onde todo ideal é principal dizemos que A é um* **domínio principal***.*

Definição 1.1.10 *Seja A um anel.*

(i) Dizemos que um ideal $\mathfrak{p}$ de A é um **ideal primo** *se $\mathfrak{p} \neq A$ e se para todo $a, b \in A$ tal que $ab \in \mathfrak{p}$ então $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.*

(ii) Diz-se que um ideal $\mathfrak{m}$ é um **ideal maximal** *se $\mathfrak{m} \neq A$ e se os únicos ideais em A que contém $\mathfrak{m}$ são A e o próprio $\mathfrak{m}$.*

Definição 1.1.11 *Sejam A um anel e $\mathfrak{I}$ um ideal de A.*

(i) Chamamos de **classe de equivalência** *do elemento $a \in A$ em relação ao ideal $\mathfrak{I}$ o subconjunto $\bar{a} = a + \mathfrak{I} = \{a + x : x \in \mathfrak{I}\}$.*

(ii) Dados $a, b \in A$, dizemos que a **é côngruo a** *b* **módulo** *$\mathfrak{I}$ se $a - b \in \mathfrak{I}$, e denotamos por $a \equiv b(mod\ \mathfrak{I})$.*

Sejam A um anel e $\mathfrak{I}$ um ideal. Considerando $A/\mathfrak{I}$ o conjunto das classes de equivalência dos elementos de A, definimos as seguintes operações de soma e produto entre os seus elementos:

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \text{isto é,} \quad (a + \mathfrak{I}) + (b + \mathfrak{I}) = (a + b) + \mathfrak{I};$$

$$\bar{a}\bar{b} = \overline{ab}, \quad \text{isto é,} \quad (a + \mathfrak{I})(b + \mathfrak{I}) = (ab) + \mathfrak{I}.$$

Definição 1.1.12 *Sejam A um anel e $\mathfrak{I}$ um ideal. O conjunto $A/\mathfrak{I}$, munido das operações de soma e produto, é um anel chamado* **anel quociente** *de A pelo ideal $\mathfrak{I}$. Os ideais de $A/\mathfrak{I}$ são da forma $\mathfrak{I}'/\mathfrak{I}$ onde $\mathfrak{I}'$ pertence ao conjunto dos ideais de A que contém $\mathfrak{I}$.*

Definição 1.1.13 *Um anel comutativo com unidade $\mathbb{K}$ é chamado* **corpo***, se todo elemento não nulo de $\mathbb{K}$ possui inverso em relação à multiplicação, isto é, para todo $a \in \mathbb{K}/\{0\}$, existe $b \in \mathbb{K}$ tal que $ab = 1$.*

Definição 1.1.14 *Um subconjunto não vazio $\mathbb{L} \subset \mathbb{K}$ é chamado* **subcorpo** *de $\mathbb{K}$ se $\mathbb{L}$ é um corpo com as operações de $\mathbb{K}$ restritas a $\mathbb{L}$.*

Definição 1.1.15 *Seja A um domínio. Dizemos que um corpo $\mathbb{K}$ é o* **corpo de frações** *do anel A se $\mathbb{K}$ for o menor corpo contendo A.*

Definição 1.1.16 *Seja A um anel. Um conjunto não vazio M é dito um A-***módulo** *se M é um grupo abeliano com relação à operação $+$ e munido de uma aplicação $\phi : A \times M \to M$, definida por $\phi(a, m) = am$, que satisfaz:*

(i) $a(m + n) = am + an$;

(ii) $(a + b)m = am + bm$;

(iii) $(ab)m = a(bm)$;

(iv) $1m = m$,

para todo $a, b \in A$ e $m, n \in M$.

Definição 1.1.17 *Um subgrupo aditivo N do A-módulo M é chamado A-***submódulo** *de M se para todo $a \in A$ e $n \in N$, então $an \in N$.*

Dado um A-módulo M e um A-submódulo N podemos construir o **módulo quociente** M/N da mesma forma como construímos o anel quociente, onde

$$a(m + N) = am + N,$$

para todo $a \in A$ e $m \in M$.

Definição 1.1.18 *Um A-módulo M é chamado* **finitamente gerado** *se existem elementos $x_1, \dots, x_n \in M$ tal que todo $m \in M$ é da forma $m = a_1x_1 + a_2x_2 + \dots a_nx_n$, com $a_i \in A$, onde $i = 1, \dots, n$. Neste caso, dizemos que $x_1, \dots, x_n$ formam um sistema de geradores de M.*

Definição 1.1.19 *Um A-módulo que possui uma base é chamado de A-***módulo livre**.

1.2 Conceitos Básicos de Topologia

Da mesma forma como para os conceitos algébricos, a teoria que engloba os conceitos topológicos é muito rica em resultados, porém neste trabalho focamos em alguns resultados básicos, mais precisamente sobre espaços métricos. Para um estudo mais aprofundado sugerimos as referências [34, 35, 39].

1.2.1 Espaços Métricos

Inicialmente, lembramos que um espaço métrico é um espaço em que é possível definir uma distância entre quaisquer dois pontos.

Definição 1.2.1 *Seja E um conjunto. Dizemos que uma função $d : E \times E \to \mathbb{R}$ é uma* **métrica** *se:*

(i) $d(x,y) \geq 0$ *e* $d(x,x) = 0$*, para todo* $x, y \in E$*;*

(ii) $d(x,y) = d(y,x)$*, para todo* $x, y \in E$*;*

(iii) $d(x,y) \leq d(x,z) + d(z,y)$*, para todo* $x, y, z \in E$ *(desigualdade triângular).*

Definição 1.2.2 *Dados* E *um conjunto e* d *uma métrica, o par* (E,d) *é chamado* **espaço métrico**.

Observação 1.2.1 *Com frequência iremos utilizar somente* E *para simbolizar o espaço métrico* (E,d).

Exemplo 1.2.1 *O conjunto* $E = \mathbb{R}^2$ *com a métrica*

$$d((x_1,y_1),(x_2,y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2},$$

com $(x_1,y_1),(x_2,y_2) \in E$*, é um espaço métrico.*

Definição 1.2.3 *Sejam* (E_1,d_1) *e* (E_2,d_2) *espaços métricos. Dizemos que uma função* $f : E_1 \to E_2$ *é uma função contínua no ponto* $x \in E_1$ *se, para todo* $\varepsilon > 0$*, existe* $\delta > 0$ *tal que, para todo* $y \in E_1$*,* $d_1(x,y) < \delta$ *implica que* $d_2(f(x),f(y)) < \varepsilon$*. Se* f *é contínua em todos os pontos, dizemos simplesmente que* f *é uma* **função contínua**.

Definição 1.2.4 *Nas condições da Definição 1.2.3, se* f *é bijetora e sua inversa também é contínua, dizemos que* f *é um* **homeomorfismo**.

Definição 1.2.5 *Seja* (E,d) *um espaço métrico. Dados* $a \in E$ *e* $\varepsilon > 0$*, o conjunto*

$$B(a,\varepsilon) = \{x \in E : d(x,a) < \varepsilon\},$$

é chamado **bola aberta** *de centro em* a *e raio* ε*.*

Definição 1.2.6 *Seja* (E,d) *um espaço métrico. Um conjunto* $U \subset E$ *é dito* **aberto** *em* E *se para cada* $a \in U$*, existir* $\varepsilon > 0$ *tal que* $B(a,\varepsilon) \subset U$*. Um conjunto* $F \subset E$ *é dito* **fechado** *em* E *se o seu complementar for aberto.*

Definição 1.2.7 *Seja* (E,d) *um espaço métrico. Dizemos que uma família* A *de conjuntos abertos de* (E,d) *é um* **recobrimento** *de* E *se* $\cup A = E$*.*

Proposição 1.2.1 *[35] Sejam* (E,d) *um espaço métrico e* $F \subset E$ *um subconjunto. Então são equivalentes:*

(i) F *é fechado;*

(ii) Para toda sequência $(x_n) \subset F$ *tal que* $x_n \to x$*, então* $x \in F$*.*

Definição 1.2.8 *Sejam* (E,d) *um espaço métrico e* $F \subset E$ *um subconjunto. O* **fêcho** $\overline{F}$ *de* F *é o menor conjunto fechado de* E *que contém* F*.*

Definição 1.2.9 *Seja* (E, d) *um espaço métrico. Dizemos que um conjunto* $K \subset E$ *é* **compacto** *se toda sequência de pontos de* K *admite uma subsequência convergente para um ponto de* K.

Definição 1.2.10 *Sejam* G *um grupo de homeomorfismos de um espaço métrico* E *e* $x \in E$. *O conjunto*

$$G(x) = \{T(x) : T \in G\}$$

é chamado G**-órbita** *de* x. *E, o subgrupo de* G

$$G_x = \{T \in G : T(x) = x\}$$

é chamado **estabilizador** *de* x.

Definição 1.2.11 *Uma família* $\{E_\alpha : \alpha \in A\}$ *de subconjuntos de um espaço métrico* E *é dita* **localmente finita** *se para todo conjunto compacto* $K \subseteq E$, *o conjunto* $\{\alpha \in A : E_\alpha \cap K \neq \emptyset\}$ *for finito.*

Definição 1.2.12 *Dizemos que um grupo* G **age de maneira propriamente descontínua** *em um espaço métrico* E, *se a* G*-órbita de qualquer ponto* $x \in E$ *é localmente finita.*

Definição 1.2.13 *Sejam* (E, d) *um espaço métrico e* $Y \subset E$ *um subconjunto não vazio. Dizemos que um ponto* $a \in Y$ *é* **isolado** *se existe* $\varepsilon > 0$ *tal que se* $B(a, \varepsilon) \cap Y = \{a\}$.

Definição 1.2.14 *Sejam* (E, d) *um espaço métrico e* $Y \subset E$ *um subconjunto não vazio. Dizemos que* Y *é* **discreto** *se todo ponto de* Y *é isolado.*

1.3 Teoria Algébrica dos Números

Nesta seção, apresentamos os principais elementos da teoria algébrica dos números. Definimos os principais conceitos e propriedades, além dos principais resultados envolvendo corpos de números, elementos inteiros, traço, norma, discriminante e corpos ciclotômicos, conceitos estes que serão fundamentais para o desenvolvimento de todo o trabalho. Um estudo aprofundado desta teoria pode ser encontrado nas referências [19, 37, 45, 49, 56].

1.3.1 Corpos de Números

Nesta subseção, apresentamos o conceito de corpos de números e algumas propriedades desta importante classe de corpos. Iniciamos com alguns conceitos importantes sobre extensões de corpos.

Definição 1.3.1 *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos. Dizemos que* $\mathbb{K}$ *é uma* **extensão** *de* $\mathbb{L}$ *se* $\mathbb{L} \subseteq \mathbb{K}$ *e denotamos por* $\mathbb{K}/\mathbb{L}$.

Definição 1.3.2 *Sejam* $\mathbb{L} \subseteq \mathbb{K}$ *corpos. O* **grau** *de* $\mathbb{K}$ *sobre* $\mathbb{L}$ *é a dimensão de* $\mathbb{K}$ *como espaço vetorial sobre* $\mathbb{L}$. *Indicaremos o grau de* $\mathbb{K}/\mathbb{L}$ *por* $[\mathbb{K} : \mathbb{L}]$.

Observação 1.3.1 *No caso em que* $[\mathbb{K}:\mathbb{L}]$ *é finito dizemos que* $\mathbb{K}$ *é uma* **extensão finita** *de* $\mathbb{L}$. *Temos também que se* $\mathbb{L}\subseteq\mathbb{K}\subseteq\mathbb{M}$ *então* $[\mathbb{M}:\mathbb{L}]=[\mathbb{M}:\mathbb{K}]\cdot[\mathbb{K}:\mathbb{L}]$ *e que* $[\mathbb{K}:\mathbb{L}]=1$ *se, e somente se,* $\mathbb{K}=\mathbb{L}$.

Definição 1.3.3 *Sejam* $\mathbb{L}\subseteq\mathbb{K}$ *corpos. Um elemento* $\alpha\in\mathbb{K}$ *é chamado* **número algébrico** *sobre* $\mathbb{L}$ *se existe* $f(x)\in\mathbb{L}[x]\backslash\{0\}$ *tal que* $f(\alpha)=0$. *Se* $\alpha\in\mathbb{K}$ *não é algébrico sobre* $\mathbb{L}$ *dizemos que* α *é* **transcendente** *sobre* $\mathbb{L}$.

Observação 1.3.2 *Se* $\alpha\in\mathbb{K}$ *é um número algébrico sobre* $\mathbb{L}$, *então existe um único polinômio mônico* $p(x)$ *de grau mínimo tal que* $p(\alpha)=0$. *Chamamos o polinômio* $p(x)$ *de* **polinômio minimal** *de* α *sobre* $\mathbb{L}$.

Definição 1.3.4 *Um* **corpo de números** $\mathbb{K}$ *é uma extensão finita do corpo* $\mathbb{Q}$ *dos números racionais. Se* $\dim_{\mathbb{Q}}\mathbb{K}=n$, *dizemos que* $\mathbb{K}$ *é um corpo de números de grau* n.

Teorema 1.3.1 *[37] Se* $\mathbb{K}$ *é um corpo de números, então* $\mathbb{K}=\mathbb{Q}(\alpha)$, *para algum número algébrico* α. *Neste caso, se* $p(x)\in\mathbb{Q}[x]$ *é o polinômio minimal de* α *sobre* $\mathbb{Q}$ *de grau* n, *então* $\mathbb{Q}(\alpha)=\{a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1} \ : \ a_i\in\mathbb{Q}, \text{ para todo } i=0,1,\ldots,n-1\}$.

Teorema 1.3.2 *[37] Se* $\mathbb{K}=\mathbb{Q}(\alpha)$ *é um corpo de números de grau* n, *então existem exatamente* n *monomorfismos distintos* $\sigma_i:\mathbb{K}\to\mathbb{C}$ *tal que,* $\sigma_i(\alpha)=\alpha_i$, *para todo* $i=1,\ldots,n$, *onde* $\alpha_1,\ldots,\alpha_n$ *são as raízes do polinômio minimal* $p(x)$ *de* $\alpha\in\mathbb{K}$.

Definição 1.3.5 *Sejam* $\mathbb{K}$ *um corpo de números de grau* n *e* $\sigma_1,\ldots,\sigma_n$ *os* n*-monomorfismos distintos de* $\mathbb{K}$ *em* $\mathbb{C}$.

(i) *Se* $\sigma_i(\mathbb{K})\subseteq\mathbb{R}$, *dizemos que* σ_i *é um* **homomorfismo real**. *Caso contrário, dizemos que* σ_i *é um* **homomorfismo imaginário**.

(ii) *Se* $\sigma_i(\mathbb{K})\subseteq\mathbb{R}$, *para todo* $i=1,\ldots,n$, *dizemos que* $\mathbb{K}$ *é um* **corpo totalmente real**. *Se* $\sigma_i(\mathbb{K})\nsubseteq\mathbb{R}$, *para todo* $i=1,\ldots,n$, *dizemos que* $\mathbb{K}$ *é um* **corpo totalmente imaginário**.

Definição 1.3.6 *Sejam* $\mathbb{L}\subseteq\mathbb{K}$ *uma extensão de corpos e* $f\in\mathbb{L}[x]$. *Dizemos que* $\mathbb{K}$ *é o* **corpo de raízes** *de* f, *e denotamos por* $\mathbb{K}=\mathbb{L}(R_f)$, *se* $\mathbb{K}$ *é o menor corpo contendo* $\mathbb{L}$ *e todas as raízes de* f.

Definição 1.3.7 *Seja* $\mathbb{L}$ *um corpo e* $f(x)\in\mathbb{L}[x]$ *um polinômio não constante. Dizemos que* $f(x)$ *é* **separável** *se todas as raízes de* $f(x)$ *são simples no seu corpo de raízes.*

Definição 1.3.8 *Uma extensão finita* $\mathbb{K}/\mathbb{L}$ *é* **galoisiana** *se* $\mathbb{K}$ *é o corpo de raízes de* $\mathbb{L}$, *para algum* $f(x)\in\mathbb{L}[x]$ *separável.*

Definição 1.3.9 *Sejam* $\mathbb{L}\subseteq\mathbb{K}$ *uma extensão e* $H\subset Aut(\mathbb{K})$, *onde* $Aut(\mathbb{K})$ *é o conjunto dos automorfismos em* $\mathbb{K}$. *O corpo*

$$\mathbb{K}^H=\{\alpha\in\mathbb{K} \ : \ \sigma(\alpha)=\alpha, \text{ para todo } \sigma\in H\},$$

é chamado de **corpo fixo** *pelo conjunto* H.

Definição 1.3.10 *Seja* $\mathbb{L} \subseteq \mathbb{K}$ *uma extensão. O* **grupo de Galois** *de* $\mathbb{K}$ *sobre* $\mathbb{L}$ *é dado por:*

$$Gal(\mathbb{K}/\mathbb{L}) = \{\sigma \in Aut(\mathbb{K}) \ : \ \sigma(\alpha) = \alpha, \ \text{para todo } \alpha \in \mathbb{L}\},$$

onde $Aut(\mathbb{K})$ *é o conjunto dos automorfismos em* $\mathbb{K}$.

Definição 1.3.11 *Uma* **extensão abeliana** *é uma extensão galoisiana na qual o grupo de Galois é abeliano.*

1.3.2 Elementos Inteiros

Nesta seção, definimos os elementos inteiros e o seu anel de inteiros, além de algumas propriedades.

Definição 1.3.12 *Seja* A *um domínio e* $\mathbb{K}$ *o seu corpo de frações. Um elemento* $\alpha \in \mathbb{K}$ *é chamado* **inteiro** *sobre* A *se existe um polinômio mônico* $f(x) \in \mathbb{K}[x]$ *tal que* $f(\alpha) = 0$.

Teorema 1.3.3 *[45] Se* α *é um número complexo que é raiz de um polinômio mônico cujos coeficientes são elementos inteiros, então* α *é um elemento inteiro.*

Definição 1.3.13 *Sejam* A *um domínio e* $\mathbb{K}$ *o seu corpo de frações. O conjunto* $\mathcal{I}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \alpha \text{ é inteiro sobre } A\}$ *é chamado* **anel dos inteiros** *de* A *em* $\mathbb{K}$.

Definição 1.3.14 *Sejam* A *um domínio e* $\mathbb{K}$ *seu corpo de frações. Dizemos que* A *é um* **anel integralmente fechado** *em* $\mathbb{K}$ *se ele contém o anel dos inteiros de* A.

Proposição 1.3.1 *[45] Se* A *é um domínio,* $\mathbb{L}$ *seu corpo de frações,* $\mathbb{K}$ *uma extensão finita de* $\mathbb{L}$ *de grau* n *e* $\mathcal{I}_{\mathbb{K}}$ *o anel de inteiros de* $\mathbb{K}$ *sobre* A*, então* $\mathcal{I}_{\mathbb{K}}$ *é integralmente fechado.*

Definição 1.3.15 *Sejam* $\mathbb{K}$ *um corpo de números de grau* n *e* $\mathcal{I}_{\mathbb{K}}$ *o anel dos inteiros de* $\mathbb{K}$. *Chamamos de* **base integral** *de* $\mathbb{K}$ *ou de* $\mathcal{I}_{\mathbb{K}}$ *uma* $\mathbb{Z}$*-base para o grupo aditivo* $\mathcal{I}_{\mathbb{K}}$.

Observação 1.3.3 *Se* $\{\alpha_1, \ldots, \alpha_n\}$ *é uma base integral* $\mathcal{I}_{\mathbb{K}}$*, então todo elemento* $\alpha \in \mathcal{I}_{\mathbb{K}}$ *pode ser escrito de modo único como* $\alpha = \displaystyle\sum_{i=1}^{n} a_i\alpha_i$*, onde* $a_i \in \mathbb{Z}$ *e para todo* $i = 1, \ldots, n$.

1.3.3 Traço e Norma

Nesta subseção, apresentamos os conceitos de traço e norma para elementos em uma extensão de corpos. Definimos também, o conceito de norma de um ideal do anel dos inteiros de um corpo de números. Além disso, veremos algumas propriedades importantes envolvendo estes conceitos, como uma relação entre as normas de um elemento e de um ideal.

Definição 1.3.16 *Sejam* $\mathbb{K}/\mathbb{L}$ *uma extensão de grau* n *e* $\sigma_1, \ldots, \sigma_n$ *os monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$. *O* **traço** *e a* **norma** *de um elemento* $\alpha \in \mathbb{K}$*, relativamente a extensão* $\mathbb{K}/\mathbb{L}$*, são definidos respectivamente por:*

$$Tr_{\mathbb{K}/\mathbb{L}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad e \quad \mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Observação 1.3.4 *Denotaremos o traço e a norma simplesmente por $Tr(\alpha)$ e $\mathcal{N}(\alpha)$ quando não houver dúvida quanto a extensão que contém o elemento α.*

Proposição 1.3.2 *[45] Sejam $\mathbb{L}$ um corpo de característica zero ou um corpo finito, $\mathbb{K}$ uma extensão de grau n de $\mathbb{L}$ e $\alpha \in \mathbb{K}$. Se $\alpha_1, \ldots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{L}$, então $Tr(\alpha) = \alpha_1 + \alpha_2 + \ldots + \alpha_n$, $\mathcal{N}(\alpha) = \alpha_1\alpha_2 \ldots \alpha_n$ e $p(x) = (x - \alpha_1)\ldots(x - \alpha_n)$, onde $p(x)$ é um polinômio mônico com coeficientes em $\mathbb{K}$ chamado polinômio característico.*

Proposição 1.3.3 *[45] Sejam A um domínio, $\mathbb{L}$ seu corpo de frações (de característica zero) e $\mathbb{K}$ uma extensão finita de $\mathbb{L}$. Se α é um elemento de $\mathbb{K}$ inteiro sobre A, então os coeficientes do polinômio característico $p(x)$ de α relativo a $\mathbb{K}$ e $\mathbb{L}$, em particular, $Tr(\alpha)$ e $\mathcal{N}(\alpha)$, são inteiros sobre A.*

Corolário 1.3.1 *[45] Se A é um anel integralmente fechado, então os coeficientes do polinômio característico de $\alpha \in \mathbb{K}$, em particular, $Tr(\alpha)$ e $\mathcal{N}(\alpha)$ são elementos de A.*

Teorema 1.3.4 *[19] Se A é um anel integralmente fechado, $\mathbb{L}$ seu corpo de frações, $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n e $\mathcal{I}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$, então $\mathcal{I}_{\mathbb{K}}$ é um A-submódulo livre de posto n.*

Definição 1.3.17 *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{I}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{I}$ um ideal não nulo de $\mathcal{I}_{\mathbb{K}}$. A* **norma do ideal** *$\mathfrak{I}$ é definida como sendo a cardinalidade do anel quociente $\mathcal{I}_{\mathbb{K}}/\mathfrak{I}$, isto é,*

$$\mathcal{N}(\mathcal{I}) = \left|\frac{\mathcal{I}_{\mathbb{K}}}{\mathfrak{I}}\right|.$$

Teorema 1.3.5 *[49] Se $\mathfrak{I} = \langle\alpha\rangle$, com $\alpha \neq 0$, é um ideal principal de $\mathcal{I}_{\mathbb{K}}$, então $\mathcal{N}(\mathfrak{I}) = |\mathcal{N}(\alpha)|$.*

Proposição 1.3.4 *[19] Se $\mathfrak{I} \subset \mathcal{I}_{\mathbb{K}}$ é um ideal não nulo, então a norma $\mathcal{N}(\mathfrak{I})$ é finita.*

1.3.4 Discriminantes

Nesta subseção, apresentamos o conceito de discriminante. Este conceito é muito importante na teoria algébrica dos números e é bastante utilizado deste trabalho. Como veremos em algumas situações, através de propriedades envolvendo discriminantes muitos resultados importantes podem ser obtidos.

Definição 1.3.18 *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n, $\mathcal{I}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\{\alpha_1, \ldots, \alpha_n\}$ uma $\mathbb{Z}$-base de $\mathcal{I}_{\mathbb{K}}$. Definimos o* **discriminante** *de $\mathbb{K}$ como sendo um ideal principal de $\mathbb{Z}$ gerado por $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \ldots, \alpha_n)$ e, denotamos por $\mathcal{D}_{\mathbb{K}}$.*

Observação 1.3.5 *Denotaremos o discriminante simplesmente por $\mathcal{D}$ quando não houver dúvida quanto a extensão de corpos utilizada.*

Observação 1.3.6 *Observamos que o ideal da Definição 1.3.18 independe da base escolhida.*

Lema 1.3.1 *[45]***(Lema de Dedekind)** *Sejam G um grupo e $\mathbb{K}$ um corpo. Se $\sigma_1, \ldots, \sigma_n$ são homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$, então $\{\sigma_1, \ldots, \sigma_n\}$ são linearmente independentes sobre $\mathbb{K}$.*

Proposição 1.3.5 *[45] Sejam $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n e $\sigma_1, \ldots, \sigma_n$ os monomorfismos distintos de $\mathbb{K}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{L}$. Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$ então*

$$\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 \neq 0.$$

Demonstração: Por definição, segue que $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \ldots, \alpha_n) = \det(Tr(\alpha_i\alpha_j))$. Como o traço $\alpha_i\alpha_j$ é a soma dos seus conjugados, segue que

$$\begin{aligned} \mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \ldots, \alpha_n) &= \det(Tr(\alpha_i\alpha_j)) = \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) \\ &= \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) = \det(\sigma_k(\alpha_i))\det(\sigma_k(\alpha_j)) \\ &= (\det(\sigma_i(\alpha_j)))^2. \end{aligned}$$

Resta mostrar que $\det(\sigma_i(\alpha_j)) \neq 0$. Suponhamos por absurdo que $\det(\sigma_i(\alpha_j)) = 0$. Assim, as colunas da matriz $(\sigma_k(\alpha_j))_{j,k=1}^{n}$ são linearmente dependentes. Assim, existem $a_1, \ldots, a_n \in \mathbb{K}$, não todos nulos, tal que $\displaystyle\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$ para todo $j = 1, \ldots, n$. Assim, por linearidade concluímos que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$, para todo $\alpha \in \mathbb{K}$, o que contradiz o Lema de Dedekind. Portanto, $\det(\sigma_i(\alpha_j))^2 \neq 0$. ∎

1.3.5 Corpos Ciclotômicos

Como vimos na Definição 1.3.4, um corpo de números é uma extensão finita do corpo $\mathbb{Q}$ dos números racionais. Nesta seção, apresentamos uma classe importante desses corpos, a classe dos corpos ciclotômicos. Esta classe de corpos desempenha um papel muito importante na teoria algébrica dos números uma vez que é possível encontrar o anel dos inteiros algébricos destes corpos e podemos obter uma expressão para calcular o seu discriminante.

Definição 1.3.19 *Seja n um inteiro positivo.*

1. *Dizemos que ζ_n é uma* **raiz n-ésima primitiva da unidade** *se $\zeta_n^n = 1$ e $\zeta_n^m \neq 1$, para todo $1 \leq m \leq n-1$.*

2. *Um* **corpo ciclotômico** *é um corpo da forma $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade.*

3. *O polinômio $\displaystyle\phi_n(x) = \prod_{j=1,\, mdc(j,n)=1}^{n} (x - \zeta_n^j)$ é chamado de $n-$***ésimo polinômio ciclotômico**.

Proposição 1.3.6 *[49] Se n é um inteiro positivo, então $x^n - 1 = \prod_{d|n} \phi_d(x)$.*

Observação 1.3.7 *Como consequência da Proposição 1.3.6, segue que*

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\, d<n} \phi_d(x)}. \tag{1.1}$$

Assim,

1. *Quando $n = p$, onde p é um número primo, segue que*

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1,$$

que é chamado de **p-ésimo polinômio ciclotômico**.

2. *Quando $n = p^r$, onde r é um número inteiro maior que 1 e p é um número primo, segue que*

$$\phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \ldots + x^{p^{r-1}} + 1,$$

que é chamado de **$\mathbf{p^r}$-ésimo polinômio ciclotômico**.

Teorema 1.3.6 *[32] Se n é um inteiro positivo, ζ_n uma raiz n-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ o corpo ciclotômico correspondente, então $[\mathbb{K} : \mathbb{Q}] = \varphi(n)$, onde φ é a função de Euler.*

Teorema 1.3.7 *[56] Se n é um inteiro positivo, ζ_n uma raiz n-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ o corpo ciclotômico correspondente, então*

(i) o anel $\mathcal{I}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\varphi(n)-1}\}$ é uma base integral de $\mathbb{K}$;

(ii) $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo maximal real de $\mathbb{K}$, $\mathcal{I}_{\mathbb{L}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é seu anel dos inteiros e $\{1, \zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-(\frac{\varphi(n)}{2}-1)}\}$ é uma base integral do subcorpo $\mathbb{L}$.

Corolário 1.3.2 *[56] Sejam n um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico, onde ζ_n é uma raiz n-ésima primitiva da unidade. Se $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo maximal real de $\mathbb{K}$, então $[\mathbb{K} : \mathbb{L}] = 2$.*

Proposição 1.3.7 *[56] Os momomorfismos de $\mathbb{K} = \mathbb{Q}(\zeta_n)$ sobre $\mathbb{C}$ são dados por*

$$\{\sigma_i;\ mdc(i,n) = 1 \quad e \quad \sigma_i(\zeta) = \zeta^i,\ onde\ \ i = 1, \ldots, n-1\}.$$

Observação 1.3.8 *Segue, da Proposição 1.3.7, que $\mathbb{K}/\mathbb{Q}$, onde $\mathbb{K} = \mathbb{Q}(\zeta_n)$, é uma extensão de Galois, pois $[\mathbb{K} : \mathbb{Q}] = \varphi(n) = |\mathbb{Z}_n{}^*|$. Além disso, $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_i;\ mdc(i,n) = 1$ e $\sigma_i(\zeta_n) = \zeta_n^i\}$.*

Proposição 1.3.8 *[49] Se $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde ζ_p é uma raiz p-ésima da unidade e p um número primo ímpar, então o discriminante de $\mathbb{K} = \mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ é dado por*

$$\mathcal{D}_{\mathbb{K}} = \mathcal{D}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1,\, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}.$$

Proposição 1.3.9 *[41] Seja $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde ζ_p é uma raiz p-ésima da unidade e p um número primo. Se $\mathbb{L} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ é o subcorpo maximal real de $\mathbb{K}$, então o discriminante de $\mathbb{L}$ sobre $\mathbb{Q}$ é dado por*

$$\mathcal{D}_{\mathbb{L}} = p^{\dfrac{p-3}{2}}.$$

Proposição 1.3.10 *[41] Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde ζ_{p^r} é uma raíz p^r-ésima primitiva da unidade, p um número primo e r um inteiro maior que 1, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$\mathcal{D}_{\mathbb{K}} = \mathcal{D}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{\varphi(p^r)-1}) = \pm p^{p^{r-1}\cdot(r(p-1)-1)}.$$

Teorema 1.3.8 *[56] Sejam n um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. O discriminante do corpo $\mathbb{K} = \mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por*

$$\mathcal{D}_{\mathbb{K}} = (-1)^{\varphi(n)} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}},$$

onde p é um número primo e φ é função de Euler. ■

Para finalizar esta seção, apresentamos a seguir o Teorema de Kronecker-Weber (Teorema 1.3.9), o qual afirma que qualquer extensão abeliana finita dos racionais está contida em um corpo ciclotômico. Esta é a afirmação que irá nos motivar, na Seção 4.2, a relacionar os corpos de números que são vistos na Seção 3.3, com subcorpos maximais reais de corpos ciclotômicos.

Teorema 1.3.9 *[56] Se $\mathbb{K}/\mathbb{Q}$ é uma extensão abeliana finita, então*

$$\mathbb{K} \subseteq \mathbb{Q}(\zeta_n), \tag{1.2}$$

para algum $n \in \mathbb{Z}$ inteiro positivo e ζ_n uma raiz n-ésima primitiva da unidade.

Seja $\mathbb{K}/\mathbb{Q}$ um extensão abeliana finita. Como, pelo Teorema 1.3.9, toda extensão abeliana finita dos racionais está contida num corpo ciclotômico, podemos tomar o menor n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$.

Definição 1.3.20 *O menor $n \in \mathbb{N}$ tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ é denominado* **condutor do corpo** $\mathbb{K}$.

1.4 Geometria Hiperbólica

O objetivo desta seção é apresentar as principais definições e resultados da geometria hiperbólica, de modo a estabelecer condições para que os conceitos de grupo fuchsiano e grupo fuchsiano aritmético possam ser apresentados no Capítulo 2. Para isso, inicialmente apresentamos os modelos da geometria hiperbólica que usaremos no decorrer do trabalho e as tesselações regulares no plano hiperbólico. Os resultados aqui apresentados e um estudo mais aprofundado desta geometria podem ser encontrados nas referências [8, 22, 30, 50, 55].

1.4.1 Modelos Hiperbólicos

Existem muitas maneiras de construirmos a geometria hiperbólica. Estas diferentes construções são chamadas de modelos hiperbólicos. Neste trabalho, discutimos em particular dois modelos euclidianos para a geometria hiperbólica plana que são convenientes para o desenvolvimento da nossa proposta. Estes modelos são chamados de semi-plano superior e disco de Poincaré. Iniciamos definindo e mostrando algumas propriedades do modelo do semi-plano superior.

Definição 1.4.1 *O* **semi-plano superior** *(ou* **plano de Lobachevski***)* $\mathbb{H}^2$ *é o conjunto dos números complexos z com parte imaginária positiva, ou seja,*

$$\mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) > 0\}.$$

O círculo no infinito ou **fronteira de** $\mathbb{H}^2$ *é definido como sendo o conjunto $\partial\mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) = 0\} \cup \{\infty\}$, onde $Im(z)$ denota a parte imaginária de z.*

Observação 1.4.1 *Podemos identificar $\mathbb{C}$ com $\mathbb{R}^2$ notando que o ponto $(x, y) \in \mathbb{R}^2$ pode igualmente ser considerado como o ponto $z = x + yi \in \mathbb{C}$. Assim, podemos definir o semi-plano superior da seguinte forma*

$$\mathbb{H}^2 = \{(x, y) \in \mathbb{R}^2 : y > 0\}.$$

Definição 1.4.2 *Seja $\sigma : [a, b] \to \mathbb{H}^2$ um caminho diferenciável por partes no semi-plano superior $\mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) > 0\}$. O* **comprimento hiperbólico de** σ **em** $\mathbb{H}^2$ *é definido pela integração da função $f(z) = \frac{1}{Im(z)}$ ao longo de σ, isto é,*

$$\| \sigma \|_{\mathbb{H}^2} = \int_\sigma \frac{1}{Im(z)} = \int_a^b \frac{|\sigma'(t)|}{Im(\sigma(t))} dt,$$

onde $|\cdot|$ é o módulo usual de um número complexo e $\sigma'(t)$ é a derivada de $\sigma(t)$.

Iremos agora, definir a distância hiperbólica entre dois pontos de $\mathbb{H}^2$.

Definição 1.4.3 *Sejam $z_1, z_2 \in \mathbb{H}^2$. Definimos a* **distância hiperbólica em** $\mathbb{H}^2$ *entre z_1 e z_2 como*

$$d_{\mathbb{H}^2}(z_1, z_2) = inf\{\| \sigma \|_{\mathbb{H}^2}\},$$

onde $\sigma : [a, b] \to \mathbb{H}^2$ é um caminho diferenciável por partes tal que $\sigma(a) = z_1$ e $\sigma(b) = z_2$, e inf denota o ínfimo do conjunto $\{\| \sigma \|_{\mathbb{H}^2}\}$.

Observamos que o ínfimo é alcançado somente para alguns caminhos e que este caminho é único. Estes caminhos, chamados de geodésicas, são definidos como sendo o caminho de menor comprimento em $\mathbb{H}^2$. Em geral, tem-se a seguinte definição.

Definição 1.4.4 *Uma curva $\sigma : [a, b] \to \mathbb{H}^2$ é chamada* **geodésica** *se para quaisquer $u, v \in [a, b]$ tivermos*

$$d(\sigma(u), \sigma(v)) = inf \left\{ \int_u^v \frac{|\sigma'(t)|}{Im(\sigma(t))} dt \right\},$$

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

Definição 1.4.5 *Sejam $a, b, c, d \in \mathbb{R}$ tal que $ad - bc > 0$. As transformações de $\mathbb{H}^2$ da forma*

$$\gamma(z) = \frac{az+b}{cz+d}, \tag{1.3}$$

onde z é uma variável complexa, são chamadas **transformações de Möbius***.*

As transformações de Möbius podem ser classificadas de acordo com a quantidade de pontos fixos.

Definição 1.4.6 *Seja γ uma transformação de Möbius. Dizemos que:*

(i) γ é **parabólica** *se γ tem somente um ponto fixo em $\partial\mathbb{H}^2$;*

(ii) γ é **elíptica** *se γ tem somente um ponto fixo em $\mathbb{H}^2$;*

(iii) γ é **hiperbólica** *se γ tem dois pontos fixos em $\partial\mathbb{H}^2$.*

Agora, nosso objetivo é apresentar a forma das geodésicas em $\mathbb{H}^2$. Primeiramente, nos resultados a seguir veremos que as transformações de Möbius são isometrias, ou seja, são funções que preservam distâncias em $\mathbb{H}^2$ e que o eixo imaginário é uma geodésica em $\mathbb{H}^2$.

Proposição 1.4.1 *[55] Se γ é uma transformação de Möbius e $z_1, z_2 \in \mathbb{H}^2$, então*

$$d(\gamma(z_1), \gamma(z_2)) = d(z_1, z_2).$$

Demonstração: Se σ é um caminho diferenciável por partes de z_1 para z_2, então $\gamma \circ \sigma$ é um caminho diferenciável por partes de $\gamma(z_1)$ para $\gamma(z_2)$. Assim, precisamos provar que

$$\| \gamma \circ \sigma \| = \| \sigma \|,$$

onde $\| \cdot \|$ denota o comprimento hiperbólico, de acordo com a Definição 1.4.2. Para isso, observamos que para $z = x + yi \in \mathbb{H}^2$ e $\gamma(z) = \frac{az+b}{cz+d}$, tem-se que

$$|\gamma'(z)| = \frac{ad-bc}{|cz+d|^2} \quad \text{e} \quad Im(\gamma(z)) = \frac{ad-bc}{|cz+d|^2} Im(z),$$

onde $|\cdot|$ denota o módulo de um número complexo. Logo,

$$\begin{aligned} \| \gamma \circ \sigma \| &= \int \frac{|(\gamma \circ \sigma)'(t)|}{Im(\gamma \circ \sigma)(t)} dt = \int \frac{|\gamma'(\sigma(t))||\sigma'(t)|}{Im(\gamma \circ \sigma)(t)} dt \\ &= \int \frac{\frac{ad-bc}{|c\sigma(t)+d|^2} |\sigma'(t)|}{\frac{ad-bc}{|c\sigma(t)+d|^2} Im(\sigma(t))} dt = \int \frac{|\sigma'(t)|}{Im(\sigma(t))} dt \\ &= \| \sigma \| . \end{aligned}$$

■

Proposição 1.4.2 *[55] Se $a \leq b$, então a distância hiperbólica entre ia e ib é $\log \frac{b}{a}$, onde ia e ib são números complexos cuja parte real é nula. Mais ainda, a linha vertical unindo ia e ib é o único caminho entre ia e ib com comprimento $\log \frac{b}{a}$, e qualquer outro caminho é estritamente maior que este.*

Demonstração: Seja $\sigma(t) = it$, com $a \leq t \leq b$, um caminho entre ia e ib. Assim, de acordo com a Definição 1.4.2, segue que

$$\| \sigma \| = \int_a^b \frac{|\sigma'(t)|}{Im(\sigma(t))} dt = \int_a^b \frac{1}{t} dt = \log \frac{b}{a}.$$

Agora, seja $\delta(t) = x(t) = iy(t) : [0,1] \to \mathbb{H}^2$ qualquer caminho entre ia e ib. Assim,

$$\begin{aligned} \| \delta \| &= \int_0^1 \frac{\sqrt{x'(t)^2 + y'(t)^2}}{y(t)} dt \\ &\geq \int_0^1 \frac{|y'(t)|}{y(t)} dt \geq \int_0^1 \frac{y'(t)}{y(t)} dt \\ &= \log y(t) \mid_0^1 = \log \frac{b}{a}. \end{aligned}$$

Logo, qualquer caminho unindo ia e ib tem comprimento hiperbólico maior que $\log \frac{b}{a}$, com igualdade quando $x'(t) = 0$, ou seja, quando σ é uma linha vertical unindo ia e ib. ■

Teorema 1.4.1 *[55] As geodésicas em $\mathbb{H}^2$ são semi-círculos ortogonais ao eixo real e retas verticais. Mais ainda, para quaisquer dois pontos z_1 e z_2 em $\mathbb{H}^2$, existe uma única geodésica passando por z_1 e z_2.*

Demonstração: Seja $\mathcal{H}$ o conjunto dos semi-círculos ortogonais ao eixo real e das retas verticais em $\mathbb{H}^2$. Se $z_1, z_2 \in \mathbb{H}^2$, então existe um elemento $H \in \mathcal{H}$ contendo z_1 e z_2. Consideremos γ um transformação de Möbius que $\gamma(z_1)$ e $\gamma(z_2)$ leva z_1 e z_2 no eixo imaginário. É sempre possível obter esta transformação, por exemplo, se H é uma reta vertical com $Re(z) = a$, onde $Re(z)$ é a parte real do número complexo z, então é suficiente tomarmos γ como sendo a translação $z \mapsto z - a$. Assim, pela Proposição 1.4.2, segue que o eixo imaginário é a única geodésica passando por $\gamma(z_1)$ e $\gamma(z_2)$. Aplicando γ^{-1}, segue que H é a única geodésica passando por z_1 e z_2. ■

Exemplo 1.4.1 *Na Figura 1.1 apresentamos algumas geodésicas no semi-plano superior $\mathbb{H}^2$.*

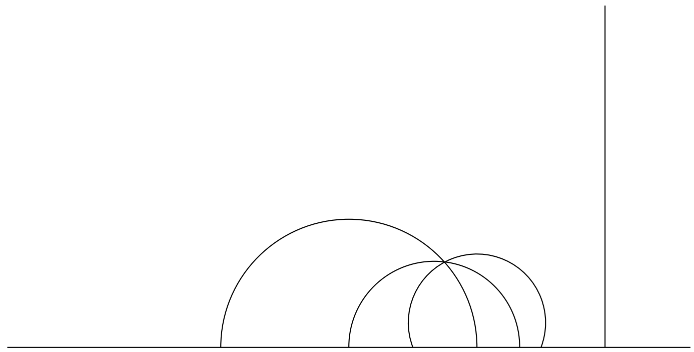

Figura 1.1: *Geodésicas em* $\mathbb{H}^2$

Definição 1.4.7 *Dado um conjunto* $A \subset \mathbb{H}^2$*, a sua* **área hiperbólica***, denotada por* $\mu_{\mathbb{H}^2}(A)$*, é definida como*

$$\mu_{\mathbb{H}^2}(A) = \int_A \frac{1}{(Im(z))^2} dz.$$

A partir de agora iremos considerar um outro modelo para a geometria hiperbólica plana, o disco de Poincaré.

Definição 1.4.8 *O disco* $\mathbb{D}^2 = \{z \in \mathbb{C} : |z| < 1\}$ *é chamado* **disco de Poincaré***. O círculo* $\partial\mathbb{D}^2 = \{z \in \mathbb{C} : |z| = 1\}$ *é chamado círculo no* ∞ *ou* **fronteira de** $\mathbb{D}^2$.

Uma vantagem do disco de Poincaré em relação ao semi-plano superior é que o disco unitário $\mathbb{D}^2$ é um subconjunto limitado do plano euclidiano, facilitando sua visualização. Enquanto que uma vantagem do semi-plano superior em relação ao disco de Poincaré é a facilidade com que as coordenadas cartesianas podem ser utilizadas em cálculos.

Consideremos a função $f : \mathbb{H}^2 \longrightarrow \mathbb{D}^2$ dada por

$$f(z) = \frac{zi + 1}{z + i}. \tag{1.4}$$

Temos que f leva o semi-plano superior $\mathbb{H}^2$ bijetivamente no disco de Poincaré $\mathbb{D}^2$. Além disso, f leva $\partial\mathbb{H}^2$ em $\partial\mathbb{D}^2$ bijetivamente. Esta bijeção nos permite trabalhar com o modelo mais adequado de acordo com a necessidade. Observe que f não é uma transformação de Möbius pois $ad - bc < 0$, onde $a = i$, $b = 1$, $c = 1$ e $d = i$.

Vejamos agora, como são definidos o comprimento e a distância hiperbólica em $\mathbb{D}^2$. Para isso, considere $g(z) = f^{-1}(z)$, com $z \in \mathbb{D}^2$. Logo, g leva $\mathbb{D}^2$ em $\mathbb{H}^2$ e

$$g(z) = \frac{-z + i}{-iz + 1}.$$

Além disso, segue que

$$g'(z) = \frac{-2}{(-iz + 1)^2} \quad \text{e} \quad Im(g(z)) = \frac{1 - |z|^2}{| - iz + 1|^2}.$$

Assim, se σ é um caminho em $\mathbb{D}^2$, então $g \circ \sigma$ é um caminho em $\mathbb{H}^2$. O comprimento de $g \circ \sigma$ é dado por

$$\begin{aligned} \| g \circ \sigma \|_{\mathbb{D}^2} &= \int \frac{|(g \circ \sigma)'(t)|}{Im((g \circ \sigma)(t))} dt = \int \frac{|g'(\sigma(t))||\sigma'(t)|}{Im(g(\sigma(t)))} dt \\ &= \int \frac{2}{1 - |\sigma(t)|^2} |\sigma'(t)| dt. \end{aligned}$$

Portanto, definimos o comprimento e a distância hiperbólica em $\mathbb{D}^2$ da seguinte forma.

Definição 1.4.9 *Seja $\sigma : [a, b] \to \mathbb{D}^2$ um caminho diferenciável por partes no disco de Poincaré $\mathbb{D}^2 = \{z \in \mathbb{C} : |z| < 1\}$. O* **comprimento hiperbólico de σ em $\mathbb{D}^2$** *é obtido pela integração da função $f(z) = \frac{2}{1-|z|^2}$ ao longo de σ, isto é,*

$$\| \sigma \|_{\mathbb{D}^2} = \int_\sigma \frac{2}{1 - |z|^2} = \int_a^b \frac{2}{1 - |\sigma(t)|^2} |\sigma'(t)| dt,$$

onde $|\cdot|$ é o módulo usual de um número complexo.

Definição 1.4.10 *Sejam $z_1, z_2 \in \mathbb{D}^2$. Definimos a* **distância hiperbólica em** $\mathbb{D}^2$, *como*

$$d_{\mathbb{D}^2}(z_1, z_2) = inf\{\| \sigma \|_{\mathbb{D}^2}\},$$

onde $\sigma : [a, b] \to \mathbb{D}^2$ é um caminho diferenciável por partes tal que $\sigma(a) = z_1$ e $\sigma(b) = z_2$, e inf é o ínfimo do conjunto $\{\| \sigma \|_{\mathbb{D}^2}\}$.

Observação 1.4.2 *Se $z_1, z_2 \in \mathbb{H}^2$, então*

$$d_{\mathbb{D}^2}(f(z_1), f(z_2)) = d_{\mathbb{H}^2}(z_1, z_2),$$

onde f é dada na Equação (1.4) e $d_{\mathbb{H}^2}$ como na Definição 1.4.3.

Se γ é uma transformação de Möbius em $\mathbb{H}^2$, então obtemos uma isometria no disco de Poincaré $\mathbb{D}^2$ pela função f que transforma γ em uma transformação de Möbius em $\mathbb{D}^2$, onde f é definida na Equação (1.4). Para isso, consideremos a função $f \circ \gamma \circ f^{-1}$ e sejam $z_1, z_2 \in \mathbb{D}^2$. Utilizando a Observação 1.4.2, segue que

$$\begin{aligned} d_{\mathbb{D}^2}(f \circ \gamma \circ f^{-1}(z_1), f \circ \gamma \circ f^{-1}(z_2)) &= d_{\mathbb{H}^2}(\gamma \circ f^{-1}(z_1), \gamma \circ f^{-1}(z_2)) && (1.5) \\ &= d_{\mathbb{H}^2}(f^{-1}(z_1), f^{-1}(z_2)) = d_{\mathbb{D}^2}(z_1, z_2). && (1.6) \end{aligned}$$

Portanto, $f \circ \gamma \circ f^{-1}$ é uma isometria em $\mathbb{D}^2$.

Definição 1.4.11 *Sejam $a, b \in \mathbb{C}$ tal que $|a|^2 - |b|^2 > 0$. As transformações de $\mathbb{D}^2$ da forma*

$$\gamma(z) = \frac{az + b}{\bar{b}z + \bar{a}},$$

são chamadas **transformação de Möbius em** $\mathbb{D}^2$.

Teorema 1.4.2 *[55] As geodésicas no modelo do disco de Poincaré da geometria hiperbólica são arcos de círculos e diâmetros em $\mathbb{D}^2$ que encontram $\partial\mathbb{D}^2$ ortogonalmente.*

Exemplo 1.4.2 *Na Figura 1.2, apresentamos algumas geodésicas no disco de Poincaré $\mathbb{D}^2$.*

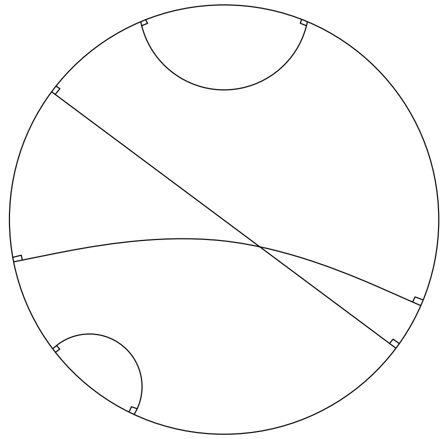

Figura 1.2: *Geodésicas em* $\mathbb{D}^2$

Através da função f dada na Equação (1.4) podemos transferir a Definição 1.4.7 de área hiperbólica de $\mathbb{H}^2$ para $\mathbb{D}^2$, conforme a seguinte definição.

Definição 1.4.12 *Dado um conjunto $A \subset \mathbb{D}^2$, sua* **área hiperbólica**, *denotada por $\mu_{\mathbb{D}^2}(A)$, é definida como*

$$\mu_{\mathbb{D}^2}(A) = \int_A \frac{4}{(1-|z|^2)^2} dz.$$

Observação 1.4.3 *Quando não houver dúvida sobre o modelo hiperbólico utilizado, denotaremos a área hiperbólica de um conjunto A apenas por $\mu(A)$.*

Finalizamos esta subseção resumindo, na Tabela 1.1, os principais resultados vistos para os modelos hiperbólicos do semi-plano superior e do disco de Poincaré.

Modelos Hiperbólicos	**Semi-plano superior** $\mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) > 0\}$	**Disco de Poincaré** $\mathbb{D}^2 = \{z \in \mathbb{C} : \lvert z\rvert < 1\}$
Fronteira	$\partial\mathbb{H}^2 = \mathbb{R} \cup \{\infty\}$	$\partial\mathbb{D}^2 = \{z \in \mathbb{C} : \lvert z\rvert = 1\}$
Comprimento hiperbólico	$\int_a^b \frac{\lvert\sigma'(t)\rvert}{Im(\sigma(t))} dt$	$\int_a^b \frac{2}{1-\lvert\sigma(t)\rvert^2} \lvert\sigma'(t)\rvert dt$
Área hiperbólica	$\mu_{\mathbb{H}^2}(A) = \int_A \frac{1}{(Im(z))^2} dz$	$\mu_{\mathbb{D}^2}(A) = \int_A \frac{4}{(1-\lvert z\rvert^2)^2} dz$
Isometrias	$\gamma(z) = \frac{az+b}{cz+d}$, $a, b, c, d \in \mathbb{R},\ ad - bc > 0$	$\gamma(z) = \frac{az+b}{\bar{b}z+\bar{a}}$, $a, b \in \mathbb{C},\ \lvert a\rvert^2 - \lvert b\rvert^2 > 0$
Geodésicas	semi-retas verticais e semi-círculos ortogonais a $\partial\mathbb{H}^2$	arcos de círculos e diâmetros em $\mathbb{D}^2$ que encontram $\partial\mathbb{D}^2$ ortogonalmente

Tabela 1.1: *Relações entre os modelos hiperbólicos* $\mathbb{H}^2$ *e* $\mathbb{D}^2$

1.4.2 Tesselações Regulares no Plano Hiperbólico

Nesta subseção, apresentamos as tesselações regulares no plano hiperbólico. Veremos que há infinitas tesselações que cobrem o plano hiperbólico utilizando polígonos regulares, enquanto que na geometria euclidiana este número está restrito a 3, a saber: triângulos equiláteros, quadrados e hexágonos regulares. Observamos que o conceito de ângulo em geometria hiperbólica é o mesmo que em geometria euclidiana. Para tais afirmações e para um estudo mais detalhado sugerimos as referências [30, 55].

Quando consideramos a geometria euclidiana, definimos um polígono como sendo um subconjunto do plano euclidiano limitado por semi-retas, que são as geodésicas no plano euclidiano. Um polígono no plano hiperbólico é definido de uma maneira análoga. Vimos no Teorema 1.4.1 que, se $z_1, z_2 \in \mathbb{H}^2 \cup \partial\mathbb{H}^2$, então existe uma única geodésica que passa por z_1 e z_2. Iremos denotar por $[z_1, z_2]$ a parte desta geodésica que conecta z_1 a z_2 e chamamos $[z_1, z_2]$ de **segmento** ou **arco de geodésica** entre z_1 e z_2.

Definição 1.4.13 *Sejam $z_1, z_2, \ldots, z_p \in \mathbb{H}^2 \cup \partial\mathbb{H}^2$. Definimos o* p-**polígono hiperbólico** $\mathcal{P}_p$ *com vértices em $z_1, z_2, \ldots, z_n$ como sendo a região de $\mathbb{H}^2$ limitada pelos segmentos geodésicos*

$$[z_1, z_2], \ldots, [z_{p-1}, z_p], [z_p, z_1].$$

Exemplo 1.4.3 *Como exemplos de polígonos hiperbólicos, na Figura 1.3, apresentamos triângulos hiperbólicos no semi-plano superior e no disco de Poincaré.*

Figura 1.3: *a) Semi-plano superior* *b) Disco de Poincaré*

Definição 1.4.14 *Sejam $z_1, z_2 \in \mathbb{H}^2$ e $[z_1, z_2]$ o seu segmento geodésico. A* **mediatriz** *de $[z_1, z_2]$ é definida como sendo a única geodésica perpendicular a $[z_1, z_2]$ que passa pelo ponto médio de $[z_1, z_2]$.*

Exemplo 1.4.4 *A Figura 1.4 mostra a mediatriz de um segmento geodésico $[z_1, z_2]$, onde $z_1, z_2 \in \mathbb{H}^2$.*

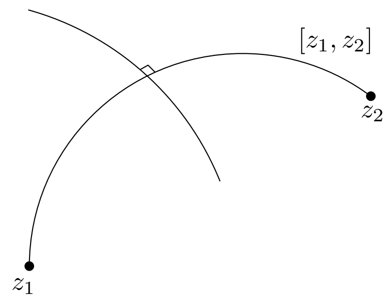

Figura 1.4: *Mediatriz de* $[z_1, z_2]$

A seguir, veremos um resultado, conhecido como Teorema de Gauss-Bonnet para polígonos hiperbólicos que fornece uma expressão para a área de um polígono hiperbólico em termos de seus ângulos. Este teorema é utilizado no estudo de tesselações do plano hiperbólico por polígonos regulares.

Teorema 1.4.3 *[55]* **(Teorema de Gauss-Bonnet para um triângulo hiperbólico)** *Se Δ é um triângulo hiperbólico com ângulos internos α, β e γ, então a área hiperbólica de Δ é dada por*

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

Demonstração: Seja Δ um triângulo hiperbólico com ângulos internos α, β e γ. Inicialmente, vamos supor que Δ tenha pelo menos um de seus vértices na fronteira de $\mathbb{H}^2$. Assim, o ângulo neste vértice é zero. Aplicando uma transformação de Möbius, podemos levar este vértice no infinito sem alterar a área ou os demais ângulos de Δ. Consideremos a transformação de Möbius $z \mapsto z + b$, para um b conveniente e vamos supor que o círculo juntando os outros dois vértices estão centrados na origem de $\mathbb{C}$. Aplicando a transformação de Möbius $z \mapsto kz$, podemos assumir que este círculo tem raio 1. Assim,

$$\mu(\Delta) = \int_\Delta \frac{1}{(Im(z))^2} dz = \int \int_\Delta \frac{1}{y^2} dxdy = \int_a^b dx \int_{\sqrt{-x^2}}^\infty \frac{1}{y^2} dy = \pi - (\alpha + \beta).$$

Agora, vamos supor que Δ não tem vértices em $\partial\mathbb{H}^2$. Sejam A, B e C os vértices de Δ com ângulos internos α, β e γ, respectivamente. Consideremos uma geodésica vertical entre os vértices A e C e, seja δ o ângulo em B entre o lado CB e a geodésica vertical. Dessa forma, podemos construir dois triângulos $AB\infty$ e $CB\infty$, e cada um deles possui um vértice no infinito. Assim, tem-se que

$$\mu(\Delta) = \mu(ABC) = \mu(AB\infty) - \mu(CB\infty).$$

Mas,

$$\mu(AB\infty) = \pi - (\alpha + (\beta + \delta)) \text{ e } \mu(CB\infty) = \pi - ((\pi - \gamma) + \delta).$$

Portanto,

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

■

Observação 1.4.4 *Na geometria euclidiana sabemos que a soma dos ângulos internos de um triângulo é igual a π. Pelo Teorema 1.4.3, segue que na geometria hiperbólica a soma dos ângulos internos de um triângulo hiperbólico é menor que π, atingindo a igualdade apenas quando todos os vértices do triângulo se encontram no infinito.*

Veremos agora o caso geral do Teorema de Gauss-Bonnet.

Teorema 1.4.4 *[55]* **(Teorema de Gauss-Bonnet para um polígono hiperbólico)** *Se $\mathcal{P}_p$ é um polígono hiperbólico de p lados com vértices $v_1, \ldots, v_p$ e ângulos internos $\alpha_1, \ldots, \alpha_p$, então*

$$\mu(\mathcal{P}_p) = (p-2)\pi - (\alpha_1 + \ldots + \alpha_p).$$

Demonstração: Para mostrar o caso geral, basta triangularizar o polígono hiperbólico $\mathcal{P}_p$, aplicar o Teorema 1.4.3 para cada um dos triângulos obtidos na triangularização e somar as áreas. ∎

Analogamente ao caso euclidiano, dizemos que um p-**polígono** é **regular** se todos os seus p lados tem o mesmo comprimento e todos os ângulos internos são iguais. A seguir definimos uma tesselação no plano hiperbólico por polígonos regulares.

Definição 1.4.15 *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**.

Exemplo 1.4.5 *A seguir veremos alguns exemplos de tesselações regulares do plano hiperbólico. Na Figura 1.5, temos a tesselação regular hiperbólica auto-dual $\{8, 8\}$, onde os polígonos desta tesselação tem 8 lados e cada vértice é o encontro de 8 destes polígonos.*

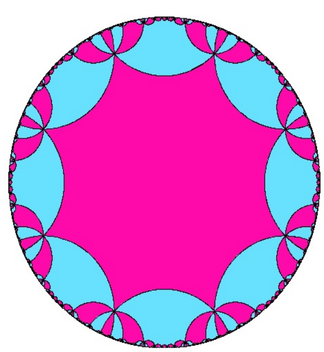

Figura 1.5: *Tesselação hiperbólica $\{8, 8\}$ no disco de Poincaré $\mathbb{D}^2$*

Já na Figura 1.6, temos a tesselação regular hiperbólica $\{10, 5\}$, onde os polígonos desta tesselação tem 10 lados e cada vértice é o encontro de 5 destes polígonos.

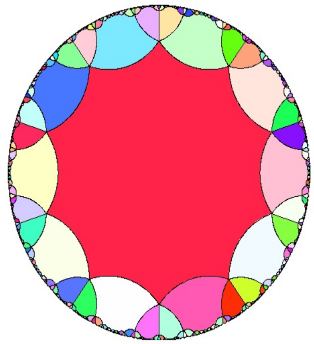

Figura 1.6: *Tesselação hiperbólica* $\{10, 5\}$ *no disco de Poincaré* $\mathbb{D}^2$

Como comentamos no início desta seção, existem infinitas maneiras de tesselar o plano hiperbólico por polígonos regulares e esta é uma vantagem de se trabalhar com a geometria hiperbólica, pois se considerarmos a geometria euclidiana, estas maneiras se restringem a três. Assim, para finalizar esta seção, apresentamos um resultado que garante que existem infinitas maneiras de tesselar o plano hiperbólico por polígonos regulares.

Teorema 1.4.5 *[55] Existe uma tesselação do plano hiperbólico por p-polígonos hiperbólicos regulares, com q desses polígonos se encontrando em cada vértice se, e somente se,*

$$\frac{2\pi}{p} + \frac{2\pi}{q} < \pi. \tag{1.7}$$

Demonstração: Mostraremos apenas que, se existe uma tesselação hiperbólica, então p e q satisfazem a condição (1.7). A implicação contrária necessita de ferramentas que não são apresentadas neste trabalho. Seja α o ângulo interno do polígono regular $\mathcal{P}_p$. Como q destes polígonos se encontram em cada vértice, então $\alpha = \frac{2\pi}{q}$. Assim, pelo Teorema 1.4.4 de Gauss-Bonnet, segue que

$$\mu(\mathcal{P}_p) = (p-2)\pi - p\alpha.$$

Como a área do polígono $\mathcal{P}_p$ deve ser positiva, segue que

$$p\pi - 2\pi - p\frac{2\pi}{q} > 0 \Rightarrow \frac{2\pi}{p} + \frac{2\pi}{q} < \pi.$$

■

Observação 1.4.5 *A inequação apresentada em (1.7) pode ser facilmente utilizada na seguinte forma*

$$(p-2)(q-2) > 4, \tag{1.8}$$

pois as duas inequações são equivalentes, uma vez que,

$$\begin{aligned} \frac{2\pi}{p} + \frac{2\pi}{q} < \pi \quad &\Leftrightarrow \quad \frac{2}{p} + \frac{2}{q} < 1 \\ &\Leftrightarrow \quad 2q + 2p - pq < 0 \\ &\Leftrightarrow \quad 2q + 2p - pq - 4 < -4 \\ &\Leftrightarrow \quad (p-2)(q-2) > 4. \end{aligned}$$

Capítulo 2

Grupos Fuchsianos Aritméticos

Neste capítulo apresentamos o conceito central deste trabalho, os grupos fuchsianos aritméticos. Os grupos fuchsianos aritméticos que consideramos neste trabalho, são aqueles que podem ser identificados com uma álgebra e uma ordem dos quatérnios. Takeuchi em [51], mostrou que existe uma identificação de forma natural entre estes grupos e uma álgebra dos quatérnios. Veremos também neste capítulo, que as ordens dos quatérnios que são apresentadas na Subseção 2.2.2 podem ser definidas como reticulados hiperbólicos devido a sua identificação com os grupos fuchsianos aritméticos. Desta forma, destacamos os resultados necessários, de modo a identificar os grupos fuchsianos aritméticos com os reticulados hiperbólicos.

Iniciamos, na Seção 2.1, apresentando os grupos fuchsianos que podem ser definido de uma forma geral como um subgrupo do grupo formado pelas transformações de Möbius com relação a composição. Como o nosso interesse são os grupos fuchsianos que podem ser associados a uma álgebra e uma ordem dos quatérnios, na Seção 2.2, apresentamos estes conceitos e mostramos os principais resultados. Na Seção 2.3, definimos os grupos fuchsianos aritméticos e apresentamos as condições necessárias e suficientes para mostrar que um grupo fuchsiano é de fato aritmético. Na Seção 2.4, apresentamos os reticulados hiperbólicos que são usados no processo de rotulagem dos sinais de uma constelação de sinais geometricamente uniforme no plano hiperbólico, como proposto em [13]. As propriedades dos reticulados hiperbólicos que destacamos na Seção 2.4, são apresentadas em [11]. Para a elaboração deste capítulo, as referências [11,12,28,30,36,43,51] foram utilizadas.

2.1 Grupos Fuchsianos

O conjunto das transformações de Möbius forma um grupo com relação à composição. Existem muitos subgrupos deste grupo e nesta subseção apresentamos uma classe especial destes subgrupos, chamada grupos fuchsianos, [30]. Na Definição 1.4.5, apresentamos as transformações de Möbius em $\mathbb{H}^2$. Neste contexto, utilizamos um subconjunto particular destas transformações pois é neste subconjunto que definimos os grupos fuchsianos.

Seja $PSL(2,\mathbb{R})$ o conjunto de todas as transformações de Möbius $T_A : \mathbb{H}^2 \longrightarrow \mathbb{H}^2$, definidas por

$$T_A(z) = \frac{az+b}{cz+d}, \tag{2.1}$$

onde $a, b, c, d \in \mathbb{R}$ e $ad - bc = 1$. Cada transformação T_A pode ser representada pela matriz

$$A = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{2.2}$$

onde $A \in SL(2,\mathbb{R})$, sendo $SL(2,\mathbb{R})$ o grupo multiplicativo das matrizes reais A com $\det(A) = 1$, chamado **grupo unimodular**.

Observação 2.1.1 *Seja a seguinte correspondência entre os elementos de $PSL(2,\mathbb{R})$ e $SL(2,\mathbb{R})$:*

$$T_A \in \ PSL(2,\mathbb{R}) \Leftrightarrow A \in \ SL(2,\mathbb{R}).$$

A composta de duas transformações em $PSL(2,\mathbb{R})$ corresponde ao produto de duas matrizes em $SL(2,\mathbb{R})$, e a inversa de $T_A \in PSL(2,\mathbb{R})$ corresponde à inversa de A. Portanto, $PSL(2,\mathbb{R})$ é um grupo com relação à composição. Além disso, a função $\varphi : SL(2,\mathbb{R}) \to PSL(2,\mathbb{R})$, dada por $\varphi(A) = T_A$, é um homeomorfismo sobrejetor cujo núcleo é $\{\pm I_2\}$, onde I_2 é a matriz identidade de ordem 2. Logo, tem-se o seguinte grupo quociente

$$PSL(2,\mathbb{R}) \simeq \frac{SL(2,\mathbb{R})}{\{\pm I_2\}}, \tag{2.3}$$

que é chamado **grupo projetivo linear**.

Teorema 2.1.1 *[30] O grupo $PSL(2,\mathbb{R})$ age sobre $\mathbb{H}^2$ por homeomorfismos.*

Demonstração: Se $T \in PSL(2,\mathbb{R})$ e $w = T(z) = \frac{az+b}{cz+d}$, com $a, b, c, d \in \mathbb{R}$ e $ad - bc = 1$, então

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

de modo que

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

Assim, se $Im(z) > 0$ então $Im(w) > 0$. Logo, mostramos que qualquer transformação dada como na Equação (2.1) leva $\mathbb{H}^2$ nele mesmo. E, como $T(z)$ e sua inversa são contínuas, segue o resultado. ■

As transformações em $PSL(2,\mathbb{R})$ podem ser classificadas de acordo com o valor do módulo do traço de sua matriz associada.

Teorema 2.1.2 *[55] Sejam T_A uma transformação real em $PSL(2,\mathbb{R})$ que não é a identidade e $tr(A)$ o traço da matriz A associada a T_A.*

(i) T_A é parabólica $\Leftrightarrow tr(A)^2 = 4$;

(ii) T_A *é elíptica* $\Leftrightarrow tr(A)^2 < 4$*;*

(iii) T_A *é hiperbólica* $\Leftrightarrow tr(A)^2 > 4$.

Demonstração: De acordo com a Definição 1.4.6, as transformações de Möbius podem ser classificadas dependendo da quantidade de pontos fixos. Assim, se $z_0 \in \mathbb{H}^2 \cup \partial\mathbb{H}^2$ é um ponto fixo de γ, então

$$\gamma(z_0) = \frac{az_0 + b}{cz_0 + d} = z_0 \Leftrightarrow cz_0^2 + (d-a)z_0 - b = 0,$$

que é uma equação quadrática em z_0 com coeficientes reais. Logo,

$$z_0 = \frac{a - d \pm \sqrt{(a-d)^2 + 4bc}}{2c},$$

e, para $c \neq 0$, esta equação possui uma solução real, duas soluções reais ou duas soluções complexas conjugadas, dependendo se o termo dentro da raiz quadrada é positivo, negativo ou nulo. Utilizando as identidades

$$ad - bc = 1 \text{ e } tr(a)^2 = (a+d)^2,$$

segue que

$$(a-d)^2 + 4bc = tr(a)^2 - 4.$$

Analisando as possibilidades para $tr(a)^2$, segue o resultado. Observe que para $c = 0$ devemos ter ∞ e $\frac{b}{d-a}$ como pontos fixos, e se $a = d$ então ∞ será o único ponto fixo. ■

Cada transformação $T \in PSL(2,\mathbb{R})$, como na Equação (2.1), pode ser naturalmente identificada com o elemento $(a,b,c,d) \in \mathbb{R}^4$. Logo, $SL(2,\mathbb{R})$ pode ser identificado com um espaço topológico, identificando seus elementos com o seguinte subconjunto de $\mathbb{R}^4$:

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

e dessa forma, herdando 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, φ com a identidade, forma um grupo cíclico de ordem 2 agindo em E. Assim, definimos uma topologia em $PSL(2,\mathbb{R})$ como o espaço quociente

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

Logo, $PSL(2,\mathbb{R})$ é um grupo topológico com relação a métrica

$$d_{\mathbb{H}^2}(T_1,T_2) = min\{\| (a_1,b_1,c_1,d_1) - (a_2,b_2,c_2,d_2) \|, \| (a_1,b_1,c_1,d_1) - (-a_2,-b_2,-c_2,-d_2) \|\},$$

onde $\| T \| = \sqrt{a^2+b^2+c^2+d^2}$ é a métrica euclidiana induzida de $\mathbb{R}^4$.

Agora, estamos em condições de definir os grupos fuchsianos.

Definição 2.1.1 *Um grupo* Γ *é chamado* **grupo fuchsiano***, se é um subgrupo discreto de* $PSL(2,\mathbb{R})$*.*

Exemplo 2.1.1 *Todo subgrupo finito de $PSL(2,\mathbb{R})$ é um grupo fuchsiano, pois todo subconjunto finito de qualquer espaço métrico é discreto.*

Exemplo 2.1.2 *Sejam $q \in \mathbb{N}$ e*

$$T_\theta(z) = \frac{cos(\frac{\theta}{2})z + sen(\frac{\theta}{2})}{-sen(\frac{\theta}{2}) + cos(\frac{\theta}{2})},$$

a rotação em torno de i, onde i é a unidade imaginária. O subconjunto $\Gamma_{\frac{2\pi}{q}} = \left\{T_{\frac{2\pi j}{q}} : 0 \leq j \leq q-1\right\}$ é um subgrupo finito de $PSL(2,\mathbb{R})$, e portanto, é um grupo fuchsiano.

Exemplo 2.1.3 *O subgrupo das translações inteiras*

$$\Gamma = \{T_n(z) = z + n : n \in \mathbb{Z}\},$$

é um grupo fuchsiano. Já o grupo de todas as translações

$$\gamma = \{T_m(z) = z + m : m \in \mathbb{R}\},$$

não é um grupo fuchsiano, pois não é discreto.

Observação 2.1.2 *Através da função f definida pela Equação (1.4), segue de modo análogo a (1.5), que o grupo discreto Γ_p de isometrias que preservam orientações dadas por $T_p : \mathbb{D}^2 \longrightarrow \mathbb{D}^2$, também é um grupo fuchsiano, dado por transformações da forma*

$$T_p(z) = \frac{az+b}{\bar{b}z+\bar{a}}, \quad a, b \in \mathbb{C}, \quad |a|^2 - |b|^2 = 1, \tag{2.4}$$

onde $T_p \in \Gamma_p < PSL(2,\mathbb{C})$. Além disso, podemos escrever $T_p = f \circ T \circ f^{-1} \in \mathbb{D}^2$, onde $\circ$ é a operação composição e $T \in PSL(2,\mathbb{R})$.

A partir de agora, apresentamos condições para um grupo ser fuchsiano.

Lema 2.1.1 *[30] Se $z \in \mathbb{H}^2$ e $K \subset \mathbb{H}^2$ é compacto, então, o conjunto*

$$H = \{T \in PSL(2,\mathbb{R}) : T(z) \in K\}$$

é compacto.

Lema 2.1.2 *[30] Se $\Gamma \subset PSL(2,\mathbb{R})$ é um grupo com ação propriamente descontínua em $\mathbb{H}^2$, então o conjunto dos pontos fixos por elementos de Γ, ou seja, o conjunto*

$$\{z \in \mathbb{H}^2 : \exists T \in \Gamma, T(z) = z\}$$

é discreto.

Teorema 2.1.3 *[30] $\Gamma \subset PSL(2,\mathbb{R})$ é um grupo fuchsiano se, e somente se, a ação de Γ é propriamente descontínua em $\mathbb{H}^2$.*

Demonstração: Se Γ é um grupo fuchsiano, $z \in \mathbb{H}^2$ e $K \subset \mathbb{H}^2$ um conjunto compacto, então

$$\{T \in \Gamma : T(z) \in K\} = \{T \in PSL(2,\mathbb{R}) : T(z) \in K\} \cap \Gamma.$$

Pelo Lema 2.1.1, segue que o conjunto $\{T \in PSL(2,\mathbb{R}) : T(z) \in K\}$ é compacto. Logo, $\{T \in \Gamma : T(z) \in K\}$ é finito, pois a interseção de um conjunto compacto com um conjunto discreto é compacto. Assim, segue que a ação de Γ é propriamente descontínua em $\mathbb{H}^2$. Agora, suponhamos que Γ age de maneira propriamente descontínua em $\mathbb{H}^2$ mas que Γ não seja discreto em $PSL(2,\mathbb{R})$. Seja z um ponto que não é fixo por qualquer elemento de Γ a não ser a identidade. Podemos garantir a existência deste ponto pelo Lema 2.1.2, já que o conjunto dos pontos fixos por elementos de Γ é discreto. Como Γ não é discreto, segue que existe uma sequência $\{T_n\}$ de elementos distintos de Γ tal que $T_n \to Id$ quando $n \to \infty$. Assim, $T_n(z) \to z$. Mas, como $T_n(z) \neq z$, pois z não é ponto fixo, segue que existe uma sequência de pontos distintos de z convergindo para z, o que contradiz a hipótese de Γ agir de maneira propriamente descontínua em $\mathbb{H}^2$. Portanto, Γ é um grupo fuchsiano. ∎

Definição 2.1.2 *Seja Γ um grupo fuchsiano. Um* **domínio fundamental** *D para Γ é um subconjunto aberto de $\mathbb{H}^2$ tal que*

(i) $\bigcup_{T\in\Gamma}(T(\overline{D})) = \mathbb{H}^2$, onde $\overline{D}$ é o fecho de D e

(ii) Se $T_1, T_2 \in \Gamma$, com $T_1 \neq T_2$, então $T_1(D) \cap T_2(D) = \emptyset$.

Observação 2.1.3 *A Definição 2.1.2, afirma que D é um domínio fundamental se todo ponto de D se encontra no fecho de alguma imagem $T(D)$ e duas imagens distintas não se sobrepõem. Dessa forma, utilizando a Definição 1.4.15, podemos dizer que as imagens de D tesselam $\mathbb{H}^2$.*

Exemplo 2.1.4 *Considere o grupo fuchsiano*

$$\Gamma = \{T_n : T_n(z) = 2^n z,\ n \in \mathbb{Z}\}.$$

Seja

$$D = \{z \in \mathbb{H}^2 : 1 < |z| < 2\}.$$

O conjunto D é um conjunto aberto e

$$1 < |z| < 2 \Rightarrow 2^n < |T_n(z)| < 2^{n+1}.$$

Assim,

$$T_n(D) = \{z \in \mathbb{H}^2 : 2^n < |z| < 2^{n+1}\}$$

e

$$T_n(\overline{D}) = \{z \in \mathbb{H}^2 : 2^n \leq |z| \leq 2^{n+1}\}.$$

Logo, $\mathbb{H}^2 = \bigcup_{n\in\mathbb{Z}}(T_n(\overline{F}))$ e, se $T_n(z)$ e $T_m(z)$ se interceptam, então $n = m$, pela forma como foram construídos os conjuntos. Portanto, D é um domínio fundamental para Γ como mostrado na Figura 2.1.

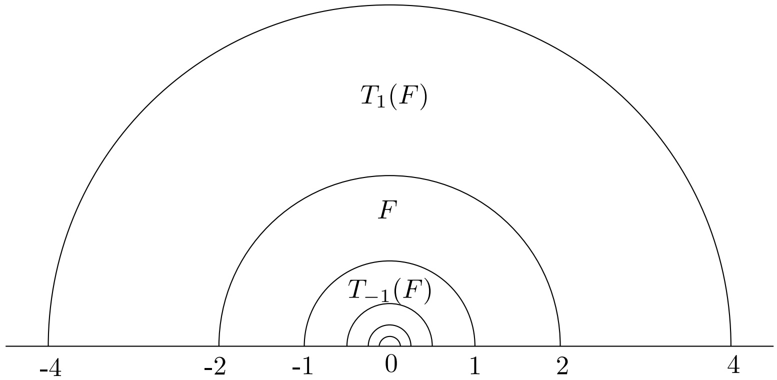

Figura 2.1: *Domínio fundamental e tesselação para* $\Gamma = \{T_n : T_n(z) = 2^n z,\ n \in \mathbb{Z}\}$

Definição 2.1.3 *Sejam* Γ *um grupo fuchsiano e* $z_0 \in \mathbb{H}^2$ *tal que* $T(z_0) \neq z_0$*, para todo* $T \in \Gamma$*. Definimos o* **domínio (região) de Dirichlet** *de* Γ *centrado em* z_0 *como o conjunto*

$$D(z_0) = \{z \in \mathbb{H}^2 : d(z, z_0) \leq d(z, T(z_0)),\ \text{para todo } T \in \Gamma\}.$$

Observação 2.1.4 *Pela Definição 2.1.3, podemos dizer que uma região de Dirichlet é o conjunto de todos os pontos* z *que estão mais próximos de* z_0 *que qualquer outro ponto da órbita* $\Gamma(z_0) = \{T(z_0) : T \in \Gamma\}$ *de* z_0 *sobre* Γ*.*

Para descrever uma região de Dirichlet podemos considerar o seguinte procedimento:

1. Escolha $z_0 \in \mathbb{H}^2$ tal que $T(z_0) \neq z_0$, para todo $T \in \Gamma \backslash \{id\}$;

2. Para todo $T \in \Gamma \backslash \{id\}$ construa o segmento geodésico $[z, T(z)]$;

3. Tome $L_{z_0}(T)$ a mediatriz de $[z_0, T(z_0)]$;

4. Seja $H_{z_0}(T)$ o semi-plano limitado por $L_{z_0}(T)$ que contém z_0 $(H_{z_0}(T))$, consistindo de todos os pontos $z \in \mathbb{H}^2$ que estão mais próximos de z_0 que de $T(z_0)$;

5. Considere
$$D(z_0) = \bigcap_{T \in \Gamma \backslash \{Id\}} H_{z_0}(T).$$

Seja $\mathcal{P}_p$ um polígono hiperbólico de p lados em $\mathbb{D}^2$. Uma **aresta** $u \subset \mathbb{D}^2$ de $\mathcal{P}_p$ é um segmento de $\mathcal{P}_p$ com uma orientação, ou seja, que começa em um vértice de $\mathcal{P}_p$ e termina em outro. Sejam Γ um grupo fuchsiano e $D(p)$ uma região de Dirichlet para Γ_p com um número finito de arestas. Para cada tesselação regular $\{p, q\}$, o polígono $\mathcal{P}_p$ constitui a fronteira do domínio de Dirichlet $D(p)$ de Γ_p. Assim, chamamos também $\mathcal{P}_p$ de **região fundamental** para o grupo Γ_p. Observe que se u é uma aresta de $D(p)$, então $u' = T(u)$ é também uma aresta de $D(p)$, para algum $T \in \Gamma \backslash \{id\}$.

Definição 2.1.4 *Dadas* u *e* u' *duas arestas de* $D(p)$*, dizemos que as arestas* u *e* $u' = T(u)$ *estão emparelhadas e chamamos* T *de* **transformação de emparelhamento**.

Dada uma aresta u de um polígono de Dirichlet $D(p)$, podemos encontrar uma transformação de emparelhamento T associada a u. Para gerar o grupo fuchsiano Γ_p estas transformações devem satisfazer as condições de Poincaré de lados e ângulos mostradas nos próximos resultados. Vejamos inicialmente a definição de ciclo de vértices.

Definição 2.1.5 *Consideremos $v_1, \ldots, v_p$ os p vértices de $\mathcal{P}_p$. Chamamos de* **ciclo de vértices** *a classe de equivalência obtida a partir de cada um dos vértices, ou seja, um ciclo de vértices é um conjunto da forma*

$$\varepsilon_i = \{T(v_i) : v_i \text{ e } T(v_i) \text{ são vértices de } \mathcal{P}_p\}.$$

Definição 2.1.6 *A quantidade de vértices pertencentes a um ciclo de vértices ε_i é chamada de* **comprimento do ciclo** *ε_i.*

Observação 2.1.5 *Para cada dois ciclos de vértices ε_i e ε_j, tem-se que*

(i) $\varepsilon_i \cap \varepsilon_j = \emptyset$ *ou* $\varepsilon_i = \varepsilon_j$;

(ii) $\cup_i \varepsilon_i = \{v_1, \ldots, v_p\}$, *onde* $v_1, \ldots, v_p$ *são os* p *vértices de* $\mathcal{P}_p$.

Se um dos vértices de $\mathcal{P}_p$ é fixo por um elemento elíptico $T \in \Gamma_p$, ou seja, $T(v_i) = v_i$, então todos os vértices do ciclo ε_i são fixos por elementos elípticos de Γ_p e, neste caso, o ciclo de vértices ε_i é chamado **ciclo elíptico**.

Teorema 2.1.4 *[50] Sejam $\mathcal{P}_p$ um domínio de Dirichlet de Γ_p e $v_1, \ldots, v_p$ os p vértices de $\mathcal{P}_p$. Sejam $v_1, \ldots, v_t$, onde $t \leq p$, os vértices de um ciclo e $\delta_1, \ldots, \delta_t$ os ângulos internos nos respectivos vértices. Se m denota a ordem do estabilizador em Γ_p de um dos vértices do ciclo, então*

$$\delta_1 + \ldots + \delta_t = \frac{2\pi}{m}. \tag{2.5}$$

Como consequência do Teorema 2.1.4, segue que se um dos vértices $v_1, \ldots, v_t$, $t \leq p$, de um ciclo de vértices não é ponto fixo, então $m = 1$. Como os grupos fuchsianos Γ_p que iremos considerar não possuem elementos elípticos, então a condição da Equação (2.5) resume-se ao caso $m = 1$, e portanto,

$$\delta_1 + \ldots + \delta_t = 2\pi,$$

onde $t \leq p$. Além disso, dada uma tesselação regular $\{p, q\}$, como cada vértice de $\mathcal{P}_p$ é recoberto por q desses polígonos, segue que os ângulos internos nos respectivos vértices valem $\frac{2\pi}{q}$. Assim, pelo Teorema 2.1.4, segue que cada ciclo deve conter exatamente q vértices e a quantidade de ciclos em uma tesselação $\{p, q\}$ é

$$\frac{p}{q}, \tag{2.6}$$

de modo que q deve dividir p.

Exemplo 2.1.5 *Para uma tesselação regular auto-dual $\{p, p\}$ tem-se apenas 1 ciclo ε de vértices, uma vez que $\frac{p}{p} = 1$.*

Teorema 2.1.5 *[50] Seja $\mathcal{P}_p$ um domínio de Dirichlet de Γ_p. Se $\{T_i : t_i \in \Gamma_p\}$ é o conjunto de elementos de Γ_p que identificam arestas distintas de $\mathcal{P}_p$, então $\{T_i : t_i \in \Gamma_p\}$ forma um conjunto de geradores de Γ_p que satisfazem um conjunto de relações para cada ciclo ε de vértices.*

Através dos Teoremas 2.1.4 e 2.1.5, segue que o grupo fuchsiano Γ_p tem a seguinte representação

$$\Gamma_p = \{T_1, \ldots, T_p \in \mathbb{H}^2 : T_\varepsilon = id\},$$

onde T_ε representa o conjunto de relações entre as transformações que pertencem ao ciclo de vértices ε e id é a função identidade. O conjunto de relações entre as transformações contidas em cada ciclo de vértices ε depende do tipo de emparelhamento utilizado. Obter estas transformações e estudar os diferentes tipos de emparelhamentos é um de nossos objetivos no Capítulo 3.

Agora, iremos considerar os espaços quocientes $\mathbb{H}^2/\Gamma$ e $\mathbb{D}^2/\Gamma_p$ com o intuito de obter uma superfície de Riemann, onde Γ e Γ_p são grupos discretos agindo de maneira propriamente descontínua sobre $\mathbb{H}^2$ ou $\mathbb{D}^2$, respectivamente. O espaço $\mathbb{H}^2/\Gamma$ é construído por meio da seguinte relação de equivalência sobre $\mathbb{H}^2$

$$z_1 \sim z_2 \Leftrightarrow \exists\, T \in \Gamma \text{ tal que } T(z_1) = z_2. \tag{2.7}$$

A classe de equivalência de um elemento $z \in \mathbb{H}^2$, denotada por $[z]$, é dada por $[z] = \Gamma$-órbita de z. Assim, os elementos do espaço $\mathbb{H}^2/\Gamma$ são as Γ-órbitas, isto é,

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

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

Topologicamente, qualquer g-toro $\mathcal{T}_g$ localmente isométrico a $\mathbb{D}^2$ pode ser obtido pelo quociente de $\mathbb{D}^2$ por um grupo fuchsiano Γ_p, isto é, $\mathcal{T}_g = \mathbb{D}^2/\Gamma_p$ (o mesmo para $\mathcal{T}_g = \mathbb{H}^2/\Gamma$). De modo geral, para cada gênero g, a ação do grupo Γ_p em $\mathbb{D}^2$ pode se processar pela identificação das arestas de um polígono regular $\mathcal{P}_p$ de p arestas em $\mathbb{D}^2$ por isometrias que geram Γ_p, as chamadas transformações de emparelhamentos apresentadas na Definição 2.1.4.

A seguir, apresentamos um exemplo de um polígono hiperbólico $\mathcal{P}_p$ de p arestas que poderá ser visto como um domínio de Dirichlet para um dado grupo fuchsiano Γ_p. Através de transformações de emparelhamentos das arestas de $\mathcal{P}_p$ podemos associar este polígono topologicamente a um g-toro.

Exemplo 2.1.6 *Na Figura 2.2, vemos um polígono regular $\mathcal{P}_8$ de 8 arestas em $\mathbb{D}^2$ que pode ser visto como um domínio de Dirichlet para um dado grupo fuchsiano Γ_8. Através das transformações de emparelhamentos das arestas de $\mathcal{P}_8$ podemos topologicamente obter um bi-toro. A construção detalhada destas transformações e do grupo fuchsiano associado serão estudadas no Capítulo 3.*

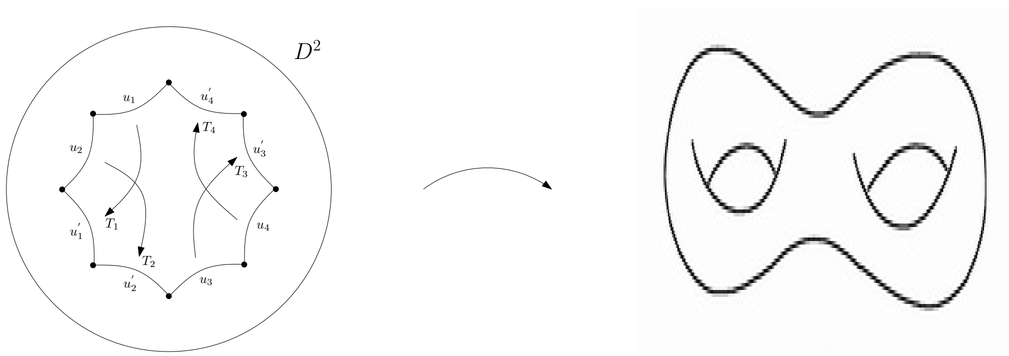

Figura 2.2: *Colagem das arestas de $\mathcal{P}_8$ e obtenção de um toro de gênero 2.*

Definição 2.1.7 *Seja Γ um grupo fuchsiano que possui um polígono de Dirichlet $D(z)$ com um número finito de lados. Se Γ tem todos os vértices em $\mathbb{H}^2$ e nenhum em $\partial\mathbb{H}^2$, dizemos que Γ é um* **grupo fuchsiano co-compacto**.

Dessa forma, nosso interesse será considerar grupos fuchsianos Γ para os quais o espaço quociente $\mathbb{H}^2/\Gamma$ é uma superfície de Riemann compacta. Assim, de acordo com a Definição 2.1.7, o grupo fuchsiano Γ será chamado grupo fuchsiano co-compacto. Os resultados que veremos a seguir caracterizam os grupos fuchsianos co-compactos.

Teorema 2.1.6 *[22] Seja Γ um grupo fuchsiano. Se Γ possui um domínio fundamental convexo não compacto, então $\mathbb{H}^2/\Gamma$ não é compacto.*

Demonstração: Seja D um domínio fundamental convexo e não compacto de Γ. Como D é fechado e não compacto, existe uma sequência ilimitada $\{z_n\}$ de pontos de D. Sem perda de generalidade, vamos assumir que z_n converge para um ponto $p_0 \in \partial\mathbb{H}^2$ quando $n \to \infty$. Dado p um ponto interior de D, a sequência dos segmentos geodésicos ligando p à z_n converge para um raio γ geodésico ligando p à p_0. Mas, como D é convexo e p é ponto interior, segue que γ está contido no interior de D. Logo, se tomarmos uma cobertura de γ que não possua uma cobertura finita por abertos suficientemente pequenos, estes abertos se projetarão homeomorficamente sobre sua imagem e, obteremos que $\mathbb{H}^2/\Gamma$ não é compacto. ■

Corolário 2.1.1 *[22] Um grupo fuchsiano Γ é co-compacto se, e somente se, toda região de Dirichlet for compacta.*

Teorema 2.1.7 *[22] Um grupo fuchsiano Γ é co-compacto se, e somente se, Γ não possui elementos parabólicos e $\mu(\mathbb{H}^2/\Gamma) < \infty$.*

Seja Γ um grupo fuchsiano co-compacto. A assinatura de Γ é um conjunto de dados geométricos os quais são suficientes para reconstruir Γ como um grupo abstrato. A assinatura também nos permite gerar diferentes grupos fuchsianos co-compactos.

Definição 2.1.8 *Se $D(z)$ é um polígono de Dirichlet para um grupo fuchsiano co-compacto Γ, então $D(z)$ tem um número finito de vértices que podem ser vistos como pontos fixos de elementos elípticos de Γ com ordens finitas. Se $m_1, \ldots, m_r$ são as ordens destes elementos elípticos e g é o gênero da superfície compacta e orientável $\mathbb{H}^2/\Gamma$, definimos a* **assinatura** *de Γ como o seguinte conjunto ordenado de inteiros*

$$(g; m_1, \ldots, m_r).$$

Observação 2.1.6 *Se o grupo fuchsiano co-compacto Γ não possuir elementos elípticos, denotamos sua assinatura por $(g; 0, \ldots, 0)$, ou simplesmente por $(g; -)$.*

Teorema 2.1.8 *[30] Se Γ é um grupo fuchsiano co-compacto com assinatura $(g; m_1, \ldots, m_r)$ então*

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

Teorema 2.1.9 *[30] Se $g \geq 0,\ r \geq 0,\ m_k \geq 2\ (1 \leq k \leq r)$ são inteiros 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 $(g; m_1, \ldots, m_r)$.

Corolário 2.1.2 *[22] Toda superfície compacta de gênero $g \geq 2$ pode ser modelada pelo plano hiperbólico, ou seja, cada elemento (transformação) de um grupo fuchsiano que gera uma superfície de Riemann compacta e orientável de gênero $g \geq 2$ consiste somente da identidade e de elementos hiperbólicos.*

Demonstração: Se $g \geq 2$, então $2g - 2 > 0$. Assim, pelo Teorema 2.1.9, segue que existe um grupo fuchsiano co-compacto com assinatura $(g; -)$, ou seja, Γ não possui elementos elípticos. Como Γ é co-compacto, pelo Teorema 2.1.7, segue que Γ também não possui elementos parabólicos. Logo, Γ possui apenas elementos hiperbólicos. Além disso, a ação de Γ em $\mathbb{H}^2$ é livre e a aplicação $\mathbb{H}^2 \to \mathbb{H}^2/\Gamma$ é uma aplicação de recobrimento. Portanto, $\mathbb{H}^2/\Gamma$ é uma superfície compacta de gênero g e $\pi_1(\mathbb{H}^2/\Gamma) = \Gamma$. ∎

Como vamos considerar apenas superfícies $\mathbb{H}^2/\Gamma$ compactas e tendo área finita, os grupos fuchsianos que iremos considerar em nosso trabalho possuem apenas elementos hiperbólicos.

2.2 Álgebra dos Quatérnios

Nesta seção apresentamos resultados básicos sobre álgebra e ordens dos quatérnios. Estes conceitos tem importância fundamental neste trabalho pois os grupos fuchsianos que iremos considerar são os derivados de uma álgebra e de uma ordem dos quatérnios. Veremos também que o interessante será quando pudermos obter uma ordem maximal dos quatérnios, pois desta forma obtemos um rotulamento completo dos pontos da constelação de sinais associada a esta ordem. No Capítulo 4, apresentamos a construção de ordens maximais dos quatérnios para álgebras dos quatérnios que associamos a grupos fuchsianos aritméticos no Capítulo 3.

No decorrer desta seção, consideraremos $\mathbb{K}$ um corpo de característica $\neq 2$ e vamos assumir que todos os anéis são associativos (mas não necessariamente comutativos) com unidade e que o homomorfismo de anéis preserva a unidade. O estudo dos conceitos apresentados nesta seção além de outros resultados sobre álgebra e ordem dos quatérnios podem ser encontrados nas referências [28, 30, 36, 43, 54].

2.2.1 Álgebra dos Quatérnios

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

(i) $a(b + c)ab + ac$;

(ii) $a(\alpha b) = (\alpha a)b = \alpha(ab)$;

(iii) $a(bc) = (ab)c$;

(iv) Existe $1_{\mathcal{A}} \in \mathcal{A}$ tal que $a1_{\mathcal{A}} = 1_{\mathcal{A}}a$.

Definimos ainda o **radical** $\mathcal{I}$ de $\mathcal{A}$ como um ideal de $\mathcal{A}$, $\mathcal{I} \subset \mathcal{A}$, tal que $\mathcal{I}^n = \{0\}$ para algum $n \in \mathbb{N}$. O conjunto

$$\mathcal{Z} = \{x \in \mathcal{A} : xy = yx, \ \forall y \in \mathcal{A}\},$$

é definido como o **centro** de $\mathcal{A}$.

Definição 2.2.1 *Uma álgebra $\mathcal{A}$ é chamada* **simples** *se o radical $\mathcal{I}$ é o trivial, ou seja, $\mathcal{I} = \{0\}$.*

Definição 2.2.2 *Uma $\mathbb{K}$-álgebra $\mathcal{A}$ é chamada* **central** *se o centro $\mathcal{Z} = \mathbb{K}$.*

Definição 2.2.3 *Uma* **álgebra dos quatérnios** *$\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ sobre um corpo de números $\mathbb{K}$ é uma álgebra simples central de dimensão 4 sobre $\mathbb{K}$, com uma base $\{1, i, j, k\}$, satisfazendo a condição de que $i^2 = \alpha$, $j^2 = \beta$, $k = ij = -ji$ e $k^2 = -\alpha\beta$, onde $\alpha, \beta \in \mathbb{K}\backslash\{0\}$.*

Definição 2.2.4 *Seja $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. Se $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{A}$, onde $x_0, x_1, x_2, x_3 \in \mathbb{K}$, então $\overline{x} = x_0 - x_1 i - x_2 j - x_3 k \in \mathcal{A}$ é chamado* **conjugado** *de x.*

Exemplo 2.2.1 *A $\mathbb{R}$-álgebra $\mathcal{H} = (-1, -1)_{\mathbb{R}}$ é o anel dos quatérnios sobre o corpo dos números reais descoberta por Hamilton. Sendo assim, chamamos $\mathcal{H}$ de álgebra dos quatérnios de Hamilton ou Hamiltonianos.*

Exemplo 2.2.2 *O anel $M(2, \mathbb{K})$ das matrizes 2×2 com coeficientes em $\mathbb{K}$ é uma álgebra dos quatérnios sobre $\mathbb{K}$. De fato, tem-se que o isomorfismo $(1, 1)_{\mathbb{K}} \to M(2, \mathbb{K})$ é dado por*

$$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ e } j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Em geral, uma álgebra dos quatérnios $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ sobre um corpo de números $\mathbb{K}$ pode ser vista como uma subálgebra do conjunto das matrizes 2×2, como segue.

Sejam $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ e M_0, M_1, M_2, M_3 matrizes linearmente independentes de $M(2, \mathbb{K}(\sqrt{\alpha}))$, dadas por

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 0 & 1 \\ \beta & 0 \end{pmatrix}, M_3 = \begin{pmatrix} 0 & \sqrt{\alpha} \\ -\beta\sqrt{\alpha} & 0 \end{pmatrix}.$$

Consideremos a aplicação $\varphi : \mathcal{A} \longrightarrow M(2, \mathbb{K}(\sqrt{\alpha}))$, definida por

$$\varphi(x_0 + x_1 i + x_2 j + x_3 k) = x_0 M_0 + x_1 M_1 + x_2 M_2 + x_3 M_3.$$

Das seguintes relações

$$\varphi(i^2) = \alpha I_2,\ \varphi(j^2) = \beta I_2 \text{ e } \varphi(ij) = \varphi(i)\varphi(j) = -\varphi(j)\varphi(i),$$

onde I_2 é a matriz identidade de ordem 2, verifica-se que φ é um isomorfismo de $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ em uma sub-álgebra de $M(2, \mathbb{K}(\sqrt{\alpha}))$. Dessa forma, cada elemento de $\mathcal{A}$ é identificado com

$$x \longmapsto \varphi(x) = \begin{pmatrix} x_0 + x_1\sqrt{\alpha} & x_2 + x_3\sqrt{\alpha} \\ \beta(x_2 - x_3\sqrt{\alpha}) & x_0 - x_1\sqrt{\alpha} \end{pmatrix}. \tag{2.8}$$

Se $\alpha = t^2$, com $t \in \mathbb{K}\backslash\{0\}$, então $\mathcal{A} \simeq M(2, \mathbb{K})$. Neste caso, dizemos que $\mathcal{A}$ é **não ramificada**. Além disso, note que $\mathbb{K}(\sqrt{\alpha}) \simeq \mathbb{K}(\sqrt{\lambda^2\alpha})$, para algum $\lambda \in \mathbb{K}\backslash\{0\}$. Assim, segue o seguinte resultado:

Teorema 2.2.1 *[30] Seja $\mathcal{A}$ uma $\mathbb{K}$-álgebra.*

(i) Se $\alpha \in (\mathbb{K}\backslash\{0\})^2$, então $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}} \simeq M(2, \mathbb{K})$.

(ii) Se $\lambda \in \mathbb{K}\backslash\{0\}$, então $(\alpha, \beta)_{\mathbb{K}} \simeq (\lambda^2\alpha, \beta)_{\mathbb{K}}$.

Definição 2.2.5 *Seja $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. Se cada elemento de $\mathcal{A}$ tem um inverso, então $\mathcal{A}$ é chamada* **álgebra de divisão**.

Agora, queremos caracterizar uma álgebra dos quatérnios de divisão como um anel de divisão não comutativo munido de uma involução padrão. Começamos definindo involuções em $\mathcal{A}$, onde $\mathcal{A}$ é uma $\mathbb{K}$-álgebra.

Definição 2.2.6 *Seja $\mathcal{A}$ uma $\mathbb{K}$-álgebra. Uma* **involução** *$\iota : \mathcal{A} \to \mathcal{A}$ é uma função $\mathbb{K}$-linear que satisfaz*

(i) $\iota(x) = \overline{x}$, para todo $x \in \mathcal{A}$;

(ii) $\iota(1) = 1$;

(iii) $\iota(xy) = \overline{yx}$, para todo $x, y \in \mathcal{A}$.

Definição 2.2.7 *Seja $\mathcal{A}$ uma $\mathbb{K}$-álgebra. Uma involução é chamada* **involução padrão** *se $x\overline{x} \in \mathbb{K}$, para todo $x \in \mathcal{A}$.*

Seja $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. A função

$$x = x_0 + x_1 i + x_2 j + x_3 k \mapsto \overline{x} = 2x_0 - x = x_0 - x_1 i - x_2 j - x_3 k,$$

define uma involução padrão em $\mathcal{A}$, uma vez que

$$x\overline{x} = (x_0 + x_1 i + x_2 j + x_3 k)(x_0 - x_1 i - x_2 j - x_3 k) = x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 \in \mathbb{K}.$$

Definição 2.2.8 *Seja $\mathcal{A}$ uma $\mathbb{K}$-álgebra munido de uma involução padrão em $\mathcal{A}$. Definimos o* **traço reduzido** *e a* **norma reduzida** *de um elemento $x \in \mathcal{A}$ por*

$$Trd(x) = x + \overline{x} \text{ e } Nrd(x) = x\overline{x},$$

respectivamente.

Observação 2.2.1 *[54] Tomando como exemplo a álgebra $M(2, \mathbb{K})$ definida no Exemplo 2.2.2, através de um cálculo direto mostra-se que*

$$Trd(M) = \frac{tr(M)}{2} \text{ e } Nrd(M) = \sqrt{\mathcal{N}(M)},$$

para todo $M \in M(2, \mathbb{K})$ e considerando o isomorfismo definido no Exemplo 2.2.2 calcular $tr(M)$ e $\mathcal{N}(M)$. Essa característica é que caracteriza o nome traço e norma reduzido.

Observação 2.2.2 *[36] Como $x^2 - (x+\overline{x})x + x\overline{x} = 0$, segue que $x \in \mathcal{A}$ é uma raiz do polinômio*

$$p(X) = X^2 - Trd(x)X + Nrd(x) \in \mathbb{K}[X],$$

que chamamos **polinômio característico reduzido** *de x.*

Observação 2.2.3 *[36] A função norma reduzida $Nrd : \mathcal{A} \to \mathbb{K}$ é multiplicativa uma vez que*

$$Nrd(xy) = (xy)\overline{(xy)} = xy\overline{y}\overline{x} = Nrd(x)Nrd(y),$$

para todo $x, y \in \mathcal{A}$. Dessa forma, os elementos invertíveis de $\mathcal{A}$ são precisamente aqueles em que $Nrd(x) \neq 0$, sendo $\frac{\overline{x}}{Nrd(x)}$ o inverso do elemento x. Assim, se $\mathcal{A}^*$ denota o conjunto dos elementos invertíveis de $\mathcal{A}$ e

$$\mathcal{A}^1 = \{x \in \mathcal{A} : Nrd(x) = 1\},$$

então $\mathcal{A}^1 \subset \mathcal{A}^*$.

Exemplo 2.2.3 *Se $\mathcal{H} = (-1, -1)_{\mathbb{R}}$ é a álgebra dos quatérnios de Hamilton então*

$$Trd_{\mathcal{H}}(x) = Trd(x) = x + \overline{x} = 2x_0 \quad \text{e} \quad Nrd_{\mathcal{H}}(x) = Nrd(x) = x\overline{x} = x_0^2 + x_1^2 + x_2^2 + x_3^2,$$

para todo $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{H}$. Considere $\mathcal{H}^1 = \{x \in \mathcal{H} : Nrd_{\mathcal{H}}(x) = 1\}$, o conjunto dos elementos de norma reduzida igual a 1 em $\mathcal{H}$. Assim, se $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{H}^1$, então

$$Nrd_{\mathcal{H}}(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1.$$

Disto, segue que

$$Trd_{\mathcal{H}}(x) = 2x_0 \in [-2, 2], \text{ pois } |x_0| \leq 1.$$

Logo, $Trd_{\mathcal{H}}(\mathcal{H}^1) = [-2, 2]$.

Teorema 2.2.2 *[30] Seja $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. $\mathcal{A}$ é uma álgebra de divisão se, e somente se, $Nrd(x) = 0$ apenas para $x = 0$.*

Demonstração: Se que $\mathcal{A}$ é uma álgebra de divisão e $x \neq 0$, então $x^{-1} \neq 0$. Assim, $Nrd(x)Nrd(x^{-1}) = 1$, e portanto, $Nrd(x) \neq 0$. Reciprocamente, se $x \neq 0$, então $Nrd(x) \neq 0$. Assim, pela Observação 2.2.3, segue que $\frac{\overline{x}}{Nrd(x)}$ é o inverso do elemento x. Logo, $\mathcal{A}$ é uma álgebra de divisão. ∎

Teorema 2.2.3 *[30] Seja $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. Se $\mathcal{A}$ não é isomorfa a $M(2, \mathbb{K})$, então $\mathcal{A}$ é uma álgebra de divisão.*

Demonstração: Observe inicialmente que $\alpha \notin (\mathbb{K}\backslash\{0\})^2$, caso contrário teríamos, pelo Teorema 2.2.1, que $\mathcal{A} \simeq M(2, \mathbb{K})$. Se $\mathbb{F} = \mathbb{K}(i)$ é uma extensão quadrática de $\mathbb{K}$ então $\mathcal{A} = \mathbb{F} + \mathbb{F}j$. Suponhamos que $\mathcal{A}$ não é uma álgebra de divisão. Assim, pelo Teorema 2.2.2, segue que existe $x \in \mathcal{A},\ x \neq 0$, tal que $Nrd(x) = 0$. Se $x = x_0 + x_1 i + x_2 j + x_3 k$, então

$$\begin{array}{rcc} 0 & = & Nrd(x) = x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 \\ & = & (x_0^2 - x_1^2\alpha) - \beta(x_2^2 - x_3^2\alpha) \\ & = & \mathcal{N}(x_0 + ix_1) - \beta\mathcal{N}(x_2 + ix_3), \end{array} \tag{2.9}$$

onde $\mathcal{N}$ é a norma no corpo $\mathbb{F}$ de acordo com a Definição 1.3.16. See $x_2^2 - x_3^2 = 0$, então $\mathcal{N}(x_0 + ix_1) = 0$. E, como não existem divisores de zero em $\mathbb{F}$, segue que $x_0 + ix_1 = 0$. Portanto $x = 0$ o que é uma contradição. Logo, $x_2^2 - x_3^2 \neq 0$. Assim, da Equação (2.9), segue que

$$\beta = \frac{\mathcal{N}(x_0 + ix_1)}{\mathcal{N}(x_2 + ix_3)} = \mathcal{N}(q_0 + iq_1) \Rightarrow \beta = q_0^2 - \alpha q_1^2,$$

onde $q_0, q_1 \in \mathbb{F}$. Agora, vamos construir uma função de $\mathcal{A}$ em $M(2, \mathbb{F})$ que leva os elementos $1, i, j, k$, da base de $\mathcal{A}$, nas seguintes matrizes

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i \mapsto \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}, j \mapsto \begin{pmatrix} q_0 & -q_1 \\ q_1\alpha & -q_0 \end{pmatrix}.$$

Logo,

$$i^2 \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}, j^2 \mapsto \begin{pmatrix} \beta & 0 \\ 0 & 0 \end{pmatrix} \text{ e } ij = -ji,$$

sendo as matrizes acima linearmente independentes. Logo, $\mathcal{A} \simeq M(2, \mathbb{K})$, o que é uma contradição. Portanto, $\mathcal{A}$ é uma álgebra de divisão. ∎

Definição 2.2.9 *Seja $\mathcal{I}_{\mathbb{K}}$ o anel dos inteiros do corpo $\mathbb{K}$ e seja $\mathfrak{p}$ um ideal de $\mathcal{I}_{\mathbb{K}}$. Definimos o* **símbolo de Hilbert** $\left(\frac{a,b}{\mathfrak{p}}\right)$ *pela função $\mathbb{K}\backslash\{0\} \times \mathbb{K}\backslash\{0\} \to \{-1, 1\}$ dada por*

$$\left(\frac{a,b}{\mathfrak{p}}\right) = \begin{cases} 1, & se\ z^2 = ax^2 + by^2 (mod\ \ \mathfrak{p})\ tem\ solução\ não\ trivial\ (x, y, z) \in \mathbb{K}^3; \\ -1, & caso\ contrário. \end{cases}$$

Observação 2.2.4 *Uma álgebra dos quatérnios $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ é dita ramificada no ideal $\mathfrak{p}$ se, e somente se, $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right) = -1$.*

Definição 2.2.10 *Um* **lugar** ν *em um corpo* $\mathbb{K}$ *é uma função* $\nu : \mathbb{K} \to \mathbb{R}\backslash\{0\}$ *tal que, para todo* $x, y \in \mathbb{K}$, *tem-se que*

(i) $\nu(x) \geq 0$, *para todo* $x \in \mathbb{K}$, *e* $\nu(x) = 0$ *se, e somente se,* $x = 0$;

(ii) $\nu(xy) = \nu(x)\nu(y)$;

(iii) $\nu(x + y) = \nu(x) + \nu(y)$.

Definição 2.2.11 *Seja* ν *um lugar em um corpo* $\mathbb{K}$.

(i) Se o lugar ν *satisfaz*

$$\nu(x + y) \leq max\{\nu(x), \nu(y)\}, \tag{2.10}$$

para todo $x, y \in \mathbb{K}$, *dizemos que* ν *é um* **lugar não arquimediano**.

(ii) Se o lugar ν *não é equivalente a nenhum lugar que satisfaz a condição (2.10),* ν *é chamado* **arquimediano**.

Seja $\mathbb{K}$ um corpo de números e ν um lugar em $\mathbb{K}$. Um lugar ν em $\mathbb{K}$ define uma métrica em $\mathbb{K}$ tal que $d(x, y) = \nu(x - y)$, para todo $x, y \in \mathbb{K}$, e portanto, define $\mathbb{K}$ como um espaço topológico.

Definição 2.2.12 *Um corpo* $\mathbb{K}$ *é dito* **completo** *em um lugar* ν *se toda sequência de Cauchy em* $\mathbb{K}$ *converge para um elemento de* $\mathbb{K}$.

Teorema 2.2.4 *[36] Sejam* $\mathbb{K}$ *um corpo e* ν *um lugar arquimediano em* $\mathbb{K}$. *Se* $\mathbb{K}$ *é completo então* $\mathbb{K}$ *é isomorfo a* $\mathbb{R}$ *ou a* $\mathbb{C}$, *e o lugar* ν *é equivalente ao valor absoluto usual.*

Para cada lugar ν em um corpo de números $\mathbb{K}$, podemos construir um corpo $\mathbb{K}_\nu$ tal que o lugar ν estende $\mathbb{K}$ para $\mathbb{K}_\nu$ e, $\mathbb{K}_\nu$ é completo com relação a ν. Os elementos de $\mathbb{K}$ são usualmente identificados com suas imagens em $\mathbb{K}_\nu$. Se ν corresponde a um ideal primo $\mathfrak{p}$, lugar não arquimediano, denotamos por $\mathbb{K}_\mathfrak{p}$. Estes corpos, $\mathbb{K}_\nu$ e $\mathbb{K}_\mathfrak{p}$, são chamados **realizações** de $\mathbb{K}$.

Sejam $\mathcal{A}$ uma álgebra dos quatérnios sobre um corpo de números $\mathbb{K}$ e $\mathcal{A}_\nu = \mathcal{A} \otimes_\mathbb{K} \mathbb{K}_\nu$ (respectivamente $\mathcal{A}_\mathfrak{p}$) a álgebra dos quatérnios sobre $\mathbb{K}_\nu$ (respectivamente sobre $\mathbb{K}_\mathfrak{p}$), onde $\otimes$ é o produto tensorial de $\mathbb{K}$-álgebra. Dizemos que $\mathcal{A}$ é ramificada em ν (respectivamente em $\mathfrak{p}$) se $\mathcal{A}_\nu$ (respectivamente $\mathcal{A}_\mathfrak{p}$) é a única álgebra de divisão sobre $\mathbb{K}_\nu$ (respectivamente $\mathbb{K}_\mathfrak{p}$), assumindo que ν não é um monomorfismo complexo.

Teorema 2.2.5 *[36] Seja* $\mathcal{A}$ *uma álgebra dos quatérnios sobre um corpo de números* $\mathbb{K}$. *O número de lugares* ν *em* $\mathbb{K}$ *tal que* $\mathcal{A}$ *é ramificada em* ν *é de cardinalidade par.*

Definição 2.2.13 *Seja* $Ram(\mathcal{A})$ *o conjunto dos ideais primos* $\mathfrak{p}$ *(lugares não Arquimedianos) em que* $\mathcal{A}$ *é ramificada. O* **discriminante reduzido** *de* $\mathcal{A}$ *é o ideal definido por*

$$\mathcal{D}(\mathcal{A}) = \prod_{\mathfrak{p} \in Ram(\mathcal{A})} \mathfrak{p}.$$

Observação 2.2.5 *Note que o anel de matrizes $M(2, \mathbb{K}(\sqrt{\alpha}))$ é a única álgebra dos quatérnios sobre $\mathbb{K}$ que é não ramificada em todos os lugares de $\mathbb{K}$, isto é, é a única álgebra dos quatérnios de discriminante $\mathcal{D}(\mathcal{A}) = \langle 1 \rangle$.*

Exemplo 2.2.4 *Consideremos a álgebra dos quatérnios $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$. O único ideal primo em $\mathcal{A}$ é o ideal principal $\mathfrak{p} = \langle \sqrt{2} \rangle$. De fato, para verificar se $\mathfrak{p} = \langle \sqrt{2} \rangle$ é ramificado em $\mathcal{A}$ precisamos calcular o símbolo de Hilbert $\left(\frac{\sqrt{2},-1}{\sqrt{2}}\right)$. Suponhamos que $\left(\frac{\sqrt{2},-1}{\sqrt{2}}\right) = 1$, ou seja, que existe $(x, y, z) \in \mathbb{Q}(\sqrt{2})^3$ tal que $z^2 = \sqrt{2}x^2 + y^2 (mod \;\; \sqrt{2})$. Assim, $\sqrt{2}$ divide $z^2 - \sqrt{2}x^2 - y^2$. Se $x = x_1 + x_2\sqrt{2}$, $y = y_1 + y_2\sqrt{2}$ e $z = z_1 + z_2\sqrt{2}$, então $\sqrt{2}$ divide*

$$(z_1^2 + 2z_2^2) + 2\sqrt{2}z_1z_2 - \sqrt{2}((x_1^2 + 2x_2^2) + 2\sqrt{2}x_1x_2) + (y_1^2 + 2y_2^2) + 2\sqrt{2}y_1y_2.$$

Como $\sqrt{2}$ é um fator das parcelas $2\sqrt{2}z_1z_2$, $\sqrt{2}((x_1^2 + 2x_2^2) + 2\sqrt{2}x_1x_2)$ e $2\sqrt{2}y_1y_2$, segue que $\sqrt{2}$ divide

$$(z_1^2 + 2z_2^2) + (y_1^2 + 2y_2^2) = (z_1^2 + y_1^2) + 2(z_2^2 + y_2^2)$$

e $\sqrt{2}$ divide $z_1^2 + y_1^2$. Deste modo, obtemos $q_1 + q_2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ tal que $z_1^2 + y_1^2 = 2q_2$ e $q_1 = 0$. Logo, $z_1^2 + y_1^2 \equiv 0 (mod \;\; 2)$. Temos as seguintes possibilidades:

(i) Se $y_1 = 0$ e $z_1 = 2^k$, para algum inteiro k, então

$$(2^k + z_2\sqrt{2})^2 = \sqrt{2}((x_1^2 + 2x_2^2) + 2\sqrt{2}x_1x_2) - 2y_2^2$$

e

$$(2^{2k} + 2.2^k z_2\sqrt{2} + 2z_2^2) = \sqrt{2}(x_1^2 + 2x_2^2 + 2\sqrt{2}x_1x_2) - 2y_2^2.$$

Logo, $\sqrt{2}$ divide x_1^2. Assim, existe $t_1 + t_2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ tal que $x_1^2 = \sqrt{2}(t_1 + t_2\sqrt{2}) = 2t_2 + t_1\sqrt{2}$ e $x_1^4 = 4t_2^2 + 4\sqrt{2}t_1t_2 + 2t_1^2$. E, sendo $t_1 = 0$, segue que $x_1^4 = 4t_2^2 \Rightarrow x_1 = \pm\sqrt{2}\sqrt{t_2} \notin \mathbb{Q}$.

(ii) Se $y_1 = 2^k$ e $z_1 = 0$, para algum inteiro k, então

$$(z_2\sqrt{2})^2 = \sqrt{2}((x_1^2 + 2x_2^2) + 2\sqrt{2}x_1x_2) - (2^k + y_2\sqrt{2})^2$$

e

$$(z_2\sqrt{2})^2 = \sqrt{2}((x_1^2 + 2x_2^2 + 2\sqrt{2}x_1x_2) - (2^{2k} + 2.2^k y_2\sqrt{2} + 2y_2^2).$$

Logo, $\sqrt{2}$ divide x_1^2 e, da mesma forma que no caso (i) obtemos uma contradição.

Assim, concluímos que $\mathfrak{p} = \langle \sqrt{2} \rangle$ é ramificado na álgebra $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})}$. Portanto,

$$\mathcal{D}(\mathcal{A}) = \langle \sqrt{2} \rangle.$$

2.2.2 Ordem dos Quatérnios

Definição 2.2.14 *Sejam $\mathcal{A}$ uma álgebra dos quatérnios sobre um corpo de números $\mathbb{K}$ e R um anel com corpo de frações $\mathbb{K}$. 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 $\mathcal{A} = \mathbb{K}\mathcal{O}$.*

Considerando $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$, com base $\{1, i, j, k\}$, e $\mathcal{I}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$, onde $\alpha, \beta \in \mathcal{I}_{\mathbb{K}}$, segue que

$$\mathcal{O} = \{x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in \mathcal{I}_{\mathbb{K}}\}, \tag{2.11}$$

é uma ordem em $\mathcal{A}$ denotada por $\mathcal{O} = (\alpha, \beta)_{\mathcal{I}_{\mathbb{K}}}$, com a mesma base $\{1, i, j, k\}$ de $\mathcal{A}$. No decorrer deste trabalho, consideramos a ordem $\mathcal{O} = (\alpha, \beta)_{\mathcal{I}_{\mathbb{K}}}$ como a *ordem dos quatérnios usual* para a álgebra dos quatérnios $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$.

Proposição 2.2.1 *[43] Se $\mathcal{A}$ é uma álgebra dos quatérnios e $\mathcal{O} \subseteq \mathcal{A}$ é um subconjunto de $\mathcal{A}$, então $\mathcal{O} \subseteq \mathcal{A}$ é uma R-ordem se, e somente se, todo elemento $x \in \mathcal{O}$ é inteiro sobre R, ou seja, $Trd(x), Nrd(x) \in R$.*

Demostração: Considere $\mathcal{O} = \{x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in R\} \subseteq \mathcal{A}$ e $x \in \mathcal{O}$. Assim, pela Observação 2.2.2, x é raiz do polinômio característico reduzido

$$p(X) = X^2 - Trd(x)X + Nrd(x) \in R[X].$$

Da mesma forma como na Proposição 1.3.3, segue que $Trd(x), Nrd(x) \in R$, e portanto, x é inteiro sobre R. Agora suponhamos que $\mathcal{O} \subseteq \mathcal{A}$ seja um subanel e que todo elemento em $\mathcal{O}$ seja inteiro. Como $\mathcal{A}$ é uma álgebra simples, segue que a forma bilinear $(x, y) \mapsto Trd(xy)$ é não degenerativa. Para mostrar que $\mathcal{O}$ é uma ordem resta mostrar que $\mathcal{O}$ é finitamente gerado. Sejam x_0, x_1, x_2, x_3 uma $\mathbb{K}$-base para $\mathcal{A}$ contida em $\mathcal{O}$. Se $y \in \mathcal{O}$, então $y = \sum_{i=0}^{3} a_i x_i$, $a_i \in \mathbb{K}$. Como $\mathcal{O}$ é um anel, segue que $yx_i \in \mathcal{O}$, e assim,

$$Trd(yx_i) = \sum_j a_j Trd(x_j x_i),$$

com $Trd(x_j x_i) \in R$ pois todo elemento em $\mathcal{O}$ é integral. Como $\mathcal{A}$ é separável, pois é uma álgebra simples, segue que a matriz $(Trd(x_i x_j))_{i,j=0,\dots,3}$ é invertível. Seja $r = det(Trd(x_i x_j))$. Utilizando a regra de Cramer podemos resolver estas equações para a_j e vemos que $a_j \in r^{-1}R$. Logo, $\mathcal{O} \subset r^{-1} \sum_i R x_i$, e portanto, $\mathcal{O}$ é finitamente gerado, ou seja, $\mathcal{O}$ é uma R-ordem em $\mathcal{A}$. ∎

Nosso objetivo agora é definir o discriminante de uma ordem dos quatérnios e mostrar algumas propriedades e resultados importantes sobre este discriminante. Seja $\mathcal{A}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. Para $x_0, x_1, x_2, x_3 \in \mathcal{A}$, definimos

$$\mathcal{D}(x_0, x_1, x_2, x_3) = det(Trd(x_i x_j))_{i,j=0,\dots,3}.$$

Definição 2.2.15 *Seja $\mathcal{O}$ uma R-ordem em uma álgebra dos quatérnios $\mathcal{A}$ sobre $\mathbb{K}$. O* **discriminante reduzido** *de $\mathcal{O}$, $\mathcal{D}(\mathcal{O})$, é o ideal em R gerado pelo conjunto*

$$\{\mathcal{D}(x_0, x_1, x_2, x_3) : x_0, x_1, x_2, x_3 \in \mathcal{O}\}.$$

Observação 2.2.6 *Da mesma forma como vimos na Observação 2.2.1, chamamos o discriminante apresentado na Definição 2.2.15 de reduzido, pois pode-se verificar que é a raiz quadrada do discriminante mostrado na Definição 1.3.18.*

Como $x_i x_j \in \mathcal{O}$, pela Proposição 2.2.1, segue que $Trd(x_i x_j) \in R$, e assim, $\mathcal{D}(\mathcal{O}) \in R$. Sendo x_0, x_1, x_2, x_3 elementos linearmente independentes sobre $\mathbb{K}$, segue que x_0, x_1, x_2, x_3 podem ser tomados como os elementos da base de $\mathcal{O}$, por exemplo. Além disso, como Trd é uma forma bilinear não degenerada em $\mathbb{K}$, segue que $\mathcal{D}(\mathcal{O})$ é um ideal não nulo de R. Disto segue o seguinte resultado:

Teorema 2.2.6 *[43] Se $\mathcal{O}$ tem uma R-base livre x_0, x_1, x_2, x_3, então $\mathcal{D}(\mathcal{O})$ é o ideal principal $det(Trd(x_i x_j))R$.*

Proposição 2.2.2 *[11] Se $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ é uma álgebra dos quatérnios sobre $\mathbb{K}$ e $\mathcal{O} = (\alpha, \beta)_{\mathcal{I}_{\mathbb{K}}}$ a ordem usual em $\mathcal{A}$, onde $\mathcal{I}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$, então o discriminante reduzido de $\mathcal{O}$ é dado por*

$$\mathcal{D}(\mathcal{O}) = \langle 4\alpha\beta \rangle.$$

Demonstração: Seja $\mathcal{O}$ uma ordem dos quatérnios em $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ com uma base x_0, x_1, x_2, x_3 satisfazendo as condições

$$x_0 = 1,\ x_1^2 = \alpha,\ x_2^2 = \beta, x_1 x_2 = \alpha\beta \text{ e } x_1 x_2 = -x_2 x_3,$$

onde $\alpha, \beta \in \mathbb{K}\backslash\{0\}$. Como $Trd(x_i \overline{x_j}) = 0$, para $i \neq j$, segue que a matriz $(Trd(x_i \overline{x_j}))_{i,j=1,\dots,4}$ é dada por

$$(Trd(x_i \overline{x_j})) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2\alpha & 0 & 0 \\ 0 & 0 & 2\beta & 0 \\ 0 & 0 & 0 & 2\alpha\beta \end{pmatrix}.$$

Logo,

$$det(Trd(x_i \overline{x_j})) = 16(\alpha\beta)^2 \Leftrightarrow \sqrt{det(Trd(x_i \overline{x_j}))} = 4\alpha\beta,$$

e portanto,

$$\mathcal{D}(\mathcal{O}) = \langle 4\alpha\beta \rangle.$$

■

Exemplo 2.2.5 *Se $R = \mathbb{Z}[\sqrt{2}]$ o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, então*

$$\mathcal{O} = \{x_0 + x_1 i + x_2 j + x_3 ij \ :\ x_0, x_1, x_2, x_3 \in \mathbb{Z}[\sqrt{2}]\}$$

é uma ordem dos quatérnios em $\mathcal{A}$, denotada por $\mathcal{O} = (\sqrt{2}, -1)_R$, com $\mathbb{Z}$-base $\{1, i, j, ij\}$. Pela Proposição 2.2.2, segue que o discriminante $\mathcal{D}(\mathcal{O})$ de $\mathcal{O} = (\sqrt{2}, -1)_R$, com $\mathbb{Z}$-base $\{1, i, j, ij\}$, é dado por

$$\mathcal{D}(\mathcal{O}) = \langle -4\sqrt{2} \rangle.$$

Proposição 2.2.3 *[54] Se $\mathcal{O} \subseteq \mathcal{O}'$ são R-ordens, então $\mathcal{D}(\mathcal{O}') \mid \mathcal{D}(\mathcal{O})$ com igualdade se, e somente se, $\mathcal{O} = \mathcal{O}'$.*

Observação 2.2.7 *[54] Se $\mathcal{A}$ é uma álgebra dos quatérnios sobre $\mathbb{K}$, pelo Teorema 2.2.6, segue uma caracterização alternativa para o discriminante reduzido de uma R-ordem $\mathcal{O} \subseteq \mathcal{A}$. Para $x_1, x_2, x_3 \in \mathcal{O}$, o discriminante reduzido de $\mathcal{O}$ é um R-submódulo $\mathcal{D}(\mathcal{O})$ de $\mathbb{K}$ gerado por $\{\{x_1, x_2, x_3\} : x_1, x_2, x_3 \in \mathcal{O}\}$, onde*

$$\{x_1, x_2, x_3\} = Trd([x_1, x_2]\overline{x_3}) = (x_1x_2 - x_2x_1)\overline{x_3} - x_3(\overline{x_1x_2} - \overline{x_2x_1}). \tag{2.12}$$

Exemplo 2.2.6 *Sejam $R = \mathbb{Z}[\sqrt{2}]$ o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ e $\mathcal{O} = (\sqrt{2}, -1)_R$ a ordem usual dos quatérnios com $\mathbb{Z}$-base $\{x_0, x_1, x_2, x_3\} = \{1, i, j, ij\}$. Assim, pela Equação (2.12) segue que*

$$\begin{aligned}
(x_1x_2 - x_2x_1)\overline{x_3} - x_3(\overline{x_1x_2} - \overline{x_2x_1}) &= (ij - ji)\overline{k} - k(\overline{ij} - \overline{ji}) \\
&= 2ij\overline{k} - k(2ij) = -4k^2 \\
&= -4\sqrt{2}.
\end{aligned}$$

Logo,

$$\mathcal{D}(\mathcal{O}) = \langle -4\sqrt{2} \rangle,$$

que é o mesmo resultado obtido no Exemplo 2.2.5.

Definição 2.2.16 *Seja R um anel com corpo de frações $\mathbb{K}$. Uma* **ordem maximal** *dos quatérnios $\mathcal{M}$ de uma álgebra dos quatérnios $\mathcal{A}$ é uma R-ordem que não está propriamente contida em nenhuma outra ordem.*

No resultado a seguir veremos que em toda álgebra dos quatérnios existe pelo menos uma ordem maximal.

Proposição 2.2.4 *[43] Toda R-ordem $\mathcal{O}$ em uma álgebra dos quatérnios $\mathcal{A}$ está contida em uma R-ordem maximal $\mathcal{M}$ em $\mathcal{A}$.*

Demonstração: Se $\mathcal{O}$ é uma R-ordem em uma álgebra dos quatérnios $\mathcal{A}$ e C é uma coleção de R-ordens em $\mathcal{A}$ contendo $\mathcal{O}$, então C é não vazio. Seja $\{\mathcal{O}_i\}$ uma cadeia de ordens contendo $\mathcal{O}$ e considere

$$\mathcal{O}' = \sum_i \mathcal{O}_i = \bigcup_i \mathcal{O}_i.$$

Assim, $\mathcal{O}'$ é um subanel de $\mathcal{A}$ contendo R e $\mathbb{K}\mathcal{O}' = \mathcal{A}$. Cada $x \in \mathcal{O}'$ está em $\mathcal{O}_i$ para algum i. Logo, pela Proposição 2.2.1, segue que x é integral sobre R e $\mathcal{O}'$ é uma R-ordem em A. Assim, dada uma cadeia de R-ordens contendo $\mathcal{O}$, tem-se que $\mathcal{O}$ é também uma R-ordem. Pelo Lema de Zorn, segue que existe um elemento maximal neste conjunto, e portanto, C tem um elemento maximal que é uma R-ordem maximal em $\mathcal{A}$. ∎

Para finalizar esta seção, apresentamos condições para que uma ordem dos quatérnios seja maximal. Isto é mostrado através de relações entre os discriminantes da álgebra e das ordens associadas.

Proposição 2.2.5 *[28] Se $\mathcal{M}$ é uma ordem maximal dos quatérnios contendo uma outra ordem dos quatérnios $\mathcal{O}$, ambas sobre uma álgebra dos quatérnios $\mathcal{A}$, então o discriminante reduzido satisfaz a seguinte relação*

$$\mathcal{D}(\mathcal{O}) = \mathcal{D}(\mathcal{M})[\mathcal{M} : \mathcal{O}] \ \text{ e } \ \mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}).$$

Consequentemente, se $\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A})$ então $\mathcal{M}$ é uma ordem maximal dos quatérnios em $\mathcal{A}$.

Exemplo 2.2.7 *Considere a álgebra dos quatérnios $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{K}}$ com a ordem usual associada $\mathcal{O} = (\sqrt{2}, -1)_R$, onde $R = \mathbb{Z}[\sqrt{2}]$ é o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. Através do Exemplo 2.2.5, tem-se que o discriminante de $\mathcal{O}$ é dado por*

$$\mathcal{D}(\mathcal{O}) = -4\sqrt{2}.$$

E, através do Exemplo 2.2.4, tem-se que o discrimante de $\mathcal{A}$ é dado por

$$\mathcal{D}(\mathcal{A}) = \langle \sqrt{2} \rangle.$$

Logo, tem-se que

$$\mathcal{D}(\mathcal{O}) \neq \mathcal{D}(\mathcal{A}),$$

e portanto, pelo Teorema 2.2.5, seque que a ordem usual $\mathcal{O} = (\sqrt{2}, -1)_R$ não é uma ordem maximal dos quatérnios na álgebra $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{K}}$.

Como vimos no Exemplo 2.2.7, a ordem $\mathcal{O}$ apresentada não é maximal. No Capítulo 4, mostramos exemplos de ordens que são maximais.

2.3 Grupos Fuchsianos Aritméticos

De modo geral, dizemos que um subgrupo discreto de $PSL(2, \mathbb{R})$ é um grupo fuchsiano aritmético se este grupo for obtido através de alguma construção aritmética. Os grupos fuchsianos aritméticos que consideramos neste trabalho serão dados no contexto de grupos algébricos lineares. Veremos que estes grupos herdam propriedades de um anel de divisão. Mais precisamente, nosso interesse será quando o grupo fuchsiano for derivado de uma álgebra dos quatérnios sobre um corpo de números totalmente real. Para estes casos, é difícil verificar, exceto para casos triviais, se um grupo fuchsiano é ou não aritmético. Sendo assim, nosso objetivo nesta seção é fornecer condições para que um grupo seja aritmético.

No que segue $\mathbb{K}$ é um corpo de números totalmente real de grau n, ou seja, $\mathbb{K}$ é um corpo de extensão de $\mathbb{Q}$ de grau n tal que todos os n monomorfismos distintos de $\mathbb{K}$ são reais. Os resultados que apresentamos nesta seção e uma estudo mais aprofundado sobre o assunto podem ser encontrados nas referências [22, 28, 30, 51].

Seja $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre um corpo de números totalmente real $\mathbb{K}$, como na Definição 2.2.3. A partir da álgebra $\mathcal{A}$, definimos as seguintes álgebras dos quatérnios

$$\mathcal{A}_\sigma = (\sigma(\alpha), \sigma(\beta))_{\sigma(\mathbb{K})} \text{ e } \mathcal{A}_\sigma \otimes \mathbb{F} = (\sigma(\alpha), \sigma(\beta))_{\mathbb{F}}, \tag{2.13}$$

onde $\sigma : \mathbb{K} \to \mathbb{F}$ é um homomorfismo de $\mathbb{K}$ em outro corpo $\mathbb{F}$ e $\otimes$ é o produto tensorial de $\mathbb{K}$-álgebras . Para o caso em que σ é um monomorfismo de $\mathbb{K}$ em $\mathbb{C}$ segue que

$$\mathcal{A}_\sigma \otimes \mathbb{C} = (\sigma(\alpha), \sigma(\beta))_{\mathbb{C}} \simeq M(2, \mathbb{C}).$$

E, se σ é um monomorfismo de $\mathbb{K}$ em $\mathbb{R}$, então

$$\mathcal{A}_\sigma \otimes \mathbb{R} = (\sigma(\alpha), \sigma(\beta))_{\mathbb{R}} \simeq \mathcal{H} \;\; ou \;\; M(2, \mathbb{R}), \tag{2.14}$$

onde $\mathcal{H}$ é a álgebra dos quatérnios de Hamilton, definida no Exemplo 2.2.1.

Agora, considere $\sigma_1, \ldots, \sigma_n$ os n monomorfismos distintos de $\mathbb{K}$ em $\mathbb{R}$, ou seja, $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, para $i = 1, \ldots, n$, e consideremos σ_1 como sendo a função identidade id. Desta forma, segue por (2.14), que para cada σ_i existe um isomorfismo ρ_i tal que

$$\rho_1 : \mathcal{A}_{\sigma_1} \otimes \mathbb{R} \to M(2, \mathbb{R}) \tag{2.15}$$

e

$$\rho_i : \mathcal{A}_{\sigma_i} \otimes \mathbb{R} \to \mathcal{H}, \text{ com } i = 2, \ldots, n. \tag{2.16}$$

Neste caso, dizemos que $\mathcal{A}$ é não-ramificada no lugar σ_1 e ramificada em todos os outros lugares σ_i, para $i = 2, \ldots, n$.

Se $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$, então pela Definição 2.2.8, segue que

$$Trd(x) = 2x_0 \text{ e } Nrd(x) = x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2,$$

e como $\sigma_1 = id$, segue por (2.14) que $\mathcal{A}_{\sigma_1} \otimes \mathbb{R} = (\sigma_1(\alpha), \sigma_1(\beta))_{\mathbb{R}} = (\alpha, \beta)_{\mathbb{R}}$. Assim, por (2.15), se $x \in \mathcal{A}_{\sigma_1} \otimes \mathbb{R}$, então

$$\rho_1(x) = \varphi(x) = \begin{pmatrix} x_0 + x_1\sqrt{\alpha} & x_2 + x_3\sqrt{\alpha} \\ \beta(x_2 - x_3\sqrt{\alpha}) & x_0 - x_1\sqrt{\alpha} \end{pmatrix},$$

onde φ é o isomorfismo definido em (2.8). Logo,

$$\begin{array}{rcl} det(\rho_1(x)) & = & (x_0 + x_1\sqrt{\alpha})(x_0 - x_1\sqrt{\alpha}) - \beta(x_2 - x_3\sqrt{\alpha})(x_2 + x_3\sqrt{\alpha}) \\ & = & x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 = Nrd(x) \end{array}$$

e

$$tr(\rho_1(x)) = x_0 + x_1\sqrt{\alpha} + x_0 - x_1\sqrt{\alpha} = 2x_0 = Trd(x), \tag{2.17}$$

onde det e tr são o determinante e o traço usual de uma matriz, respectivamente.

Agora, considerando as álgebras $\mathcal{A}_{\sigma_i} \otimes \mathbb{R} = (\sigma_i(\alpha), \sigma_i(\beta))_{\mathbb{R}}$, onde $i = 2, \ldots, n$ e os isomorfismos (2.16), tem-se para $x \in \mathcal{A}_{\sigma_i} \otimes \mathbb{R}$ que

$$Nrd_{\mathcal{H}}(\rho_i(x)) = \sigma_i(Nrd(x)) \text{ e } Trd_{\mathcal{H}}(\rho_i(x)) = \sigma_i(Trd(x)), \tag{2.18}$$

onde $i = 2, \ldots, n$ e, $Trd_{\mathcal{H}}$ e $Nrd_{\mathcal{H}}$ são o traço reduzido e a norma reduzida em $\mathcal{H}$ como no Exemplo 2.2.1.

Teorema 2.3.1 *[30] Seja $\mathcal{A}$ uma álgebra dos quatérnios sobre um corpo de números totalmente real $\mathbb{K}$ satisfazendo (2.15) e (2.16). Se $\mathbb{K} \neq \mathbb{Q}$, então $\mathcal{A}$ é uma álgebra de divisão.*

Demosntração: Se $\mathcal{A}$ não é um álgebra de divisão, então pelo Teorema 2.2.1, segue que

$$\mathcal{A} \simeq M(2, \mathbb{K}) \simeq \mathcal{H}.$$

Como $[\mathbb{K} : \mathbb{Q}] = n \geq 2$ pois $\mathbb{K} \neq \mathbb{Q}$, para qualquer $i > 1$, segue por (2.13) que

$$\mathcal{A}_{\sigma_i} \simeq (1, 1)_{\sigma_i(\mathbb{K})} \simeq M(2, \sigma_i(\mathbb{K})),$$

e portanto,

$$\mathcal{A}_{\sigma_i} \otimes \mathbb{R} \simeq (1, 1)_{\mathbb{R}} \simeq M(2, \mathbb{K}),$$

o que contradiz (2.16) pois $\mathcal{A}_{\sigma_i} \otimes \mathbb{R} \simeq \mathcal{H}$. ■

Seja $\mathcal{O} = (\alpha, \beta)_{\mathcal{I}_{\mathbb{K}}}$ a ordem dos quatérnios usual da álgebra $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ definida em (2.11), onde $\mathcal{I}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$. Considere o grupo dos elementos invertíveis em $\mathcal{O}$ de norma reduzida 1, ou seja,

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

Pela Observação 2.2.3, segue que $\mathcal{O}^1$ é um grupo multiplicativo. Assim, por (2.15), segue que $\rho_1(\mathcal{O}^1)$ é um subgrupo de $SL(2, \mathbb{R})$. Logo, como vimos em (2.3), tem-se que

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

e portanto,

$$\Gamma(\mathcal{A}, \mathcal{O}) = \frac{\rho_1(\mathcal{O}^1)}{\{\pm I_2\}}$$

é um subgrupo de $PSL(2, \mathbb{R})$. Assim, tem-se o seguinte resultado.

Teorema 2.3.2 *[30] $\Gamma(\mathcal{A}, \mathcal{O})$ é um grupo fuchsiano.*

Pela forma como construímos $\Gamma(\mathcal{A}, \mathcal{O})$ vemos que é um grupo fuchsiano obtido de uma forma aritmética. Logo, temos a seguinte definição.

Definição 2.3.1 *Se Γ é um grupo fuchsiano de índice finito de algum $\Gamma(\mathcal{A}, \mathcal{O})$, dizemos que Γ é um grupo fuchsiano derivado de uma álgebra dos quatérnios $\mathcal{A}$, ou ainda, dizemos que Γ é um* **grupo fuchsiano aritmético**.

A partir de agora nosso objetivo é caracterizar os grupos fuchsianos aritméticos através do conjunto dos traços de seus elementos, ou seja, do conjunto

$$\{\pm tr(T) : T \in \Gamma\}. \tag{2.19}$$

Iniciamos com resultados que nos fornecem uma álgebra e uma ordem dos quatérnios para o corpo de números formado pelo conjunto dos traços dado em(2.19).

Teorema 2.3.3 *[30] Sejam Γ um grupo fuchsiano com área hiperbólica $\mu(\mathbb{H}^2/\Gamma) < \infty$ e o conjunto dos traços dado em (2.19). Se $\{\pm tr(T) : T \in \Gamma\} \subset \mathbb{K}_1$, onde $\mathbb{K}_1 = \mathbb{Q}(tr(T) : T \in \Gamma)$ é um corpo de números algébricos com $[\mathbb{K}_1 : \mathbb{Q}] < \infty$, então*

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

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

Corolário 2.3.1 *[30] Sejam Γ um grupo fuchsiano com $\mu(\mathbb{H}^2/\Gamma) < \infty$ e $\mathbb{K}_1 = \mathbb{Q}(tr(T) : T \in \Gamma)$ com $[\mathbb{K}_1 : \mathbb{Q}] < \infty$. Se $\{\pm tr(T) : T \in \Gamma\} \subset \mathcal{I}_{\mathbb{K}_1}$, onde $\mathcal{I}_{\mathbb{K}_1}$ é o anel dos inteiros de $\mathbb{K}_1$, então*

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

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

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

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

Seja $\Gamma \subseteq PSL(2, \mathbb{K})$ um grupo fuchsiano nas condições do Teorema 2.3.3, onde $\mathbb{K} = \mathbb{K}_1(\lambda)$ é uma extensão quadrática de $\mathbb{K}_1$, ou seja, $[\mathbb{K} : \mathbb{K}_1] = 2$. Vamos supor que Γ contém os seguintes elementos

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \text{ e } T_1 = \begin{pmatrix} a_1 & 1 \\ c_1 & d_1 \end{pmatrix}, \text{ com } c_1 \neq 0 \text{ e } \lambda \neq 1.$$

Pode-se verificar que o conjunto

$$\{I_2, T_0, T_1, T_0T_1\},$$

forma uma base para a álgebra $\mathcal{A}[\Gamma]$ sobre $\mathbb{K}_1$. Dessa forma, podemos escrever

$$\mathcal{A}[\Gamma] = \left\{ \begin{pmatrix} a & b \\ \overline{b}c_1 & \overline{a} \end{pmatrix} : a, b \in \mathbb{K},\ c_1 \in \mathbb{K}_1 \right\}, \tag{2.20}$$

onde $\overline{a}$ e $\overline{b}$ são os conjugados de a e b em $\mathbb{K} = \mathbb{K}_1(\lambda)$, respectivamente. Para esta construção segue o seguinte resultado.

Lema 2.3.1 *[30] Se σ é um monomorfimo de $\mathbb{K} = \mathbb{K}_1(\lambda)$ em $\mathbb{C}$ tal que $\sigma|_{\mathbb{K}_1} \neq id$, então para qualquer elemento $T = \begin{pmatrix} a & b \\ \overline{b}c_1 & \overline{a} \end{pmatrix} \in \Gamma$ tem-se que $|\sigma(a)| \leq 1$. Em particular, para $T_1 = \begin{pmatrix} a_1 & 1 \\ c_1 & \overline{a_1} \end{pmatrix} \in \Gamma$, tem-se que $\sigma(c_1) < 0$.*

Munidos da álgebra dos quatérnios $\mathcal{A}[\Gamma]$, da ordem dos quatérnios $\mathcal{O}[\Gamma]$ e dos resultados já apresentados, estamos em condições de provar o resultado mais importante deste capítulo, o qual apresenta uma condição necessária e suficiente para um grupo fuchsiano ser aritmético.

Teorema 2.3.4 *[30] Seja Γ um grupo uchsiano com área hiperbólica $\mu(\mathbb{H}^2/\Gamma) < \infty$. Assim, Γ é derivado de uma álgebra dos quatérnios sobre um corpo de números $\mathbb{K}$ totalmente real se, e somente se, Γ satisfaz as seguintes condições:*

(i) Se $\mathbb{K}_1 = \mathbb{Q}(tr(t) : T \in \Gamma)$, então $[\mathbb{K}_1 : \mathbb{Q}] < \infty$ e $\{\pm tr(T) : T \in \Gamma\} \subset \mathcal{I}_{\mathbb{K}_1}$, onde $\mathcal{I}_{\mathbb{K}_1}$ é o anel dos inteiros algébricos de $\mathbb{K}_1$.

(ii) Se σ é um monomorfismo de $\mathbb{K}_1$ em $\mathbb{C}$ tal que $\sigma \neq id$, então $\sigma(tr(T))$ é limitado em $\mathbb{C}$, para todo $T \in \Gamma$.

Demonstração: Suponhamos inicialmente que Γ é um subgrupo discreto de índice finito em $\Gamma(\mathcal{A}, \mathcal{O})$. Qualquer que seja $T \in \Gamma$ tem-se que $tr(T) \in \mathbb{K}$. Porém, sendo $\mathbb{K}_1 = \mathbb{Q}(tr(T) : T \in \Gamma)$ segue que $\mathbb{K}_1 \subseteq \mathbb{K}$. Logo, $\mathbb{K}_1$ é um corpo de números totalmente real de grau finito. Agora, se $\mathcal{O}$ é uma ordem dos quatérnios, então pela Proposição 2.2.1, segue que $\mathcal{O}$ é inteiro sobre $\mathcal{I}_{\mathbb{K}_1}$. Logo, $Trd(\mathcal{O}) \subset \mathcal{I}_{\mathbb{K}_1}$. Além disso, por (2.17), segue que $tr(T) \in \mathcal{I}_{\mathbb{K}_1}$, para todo $T \in \Gamma$, ou seja, $\{\pm tr(T) : T \in \Gamma\} \subset \mathcal{I}_{\mathbb{K}_1}$. Portanto, a condição (i) está provada.

Agora, suponhamos que $[\mathbb{K}_1 : \mathbb{Q}] = n \geq 2$. Assim, por (2.18), segue que existe $\sigma_i \neq id$, $2 \leq i \leq n$, tal que

$$\sigma_i(tr(T)) \subset Trd_{\mathcal{H}}(\rho_i(\mathcal{O}^1)),$$

para todo $T \in \Gamma$. Por outro lado, dado $x \in \mathcal{O}^1$ tem-se que

$$\sigma_i(Nrd(x)) = Nrd_{\mathcal{H}}(\rho_i(x)).$$

Logo, $\rho_i(\mathcal{O}^1) \subset \mathcal{H}^1 = \{x \in \mathcal{H} : Nrd_{\mathcal{H}}(x) = 1\}$. Mas, pelo Exemplo 2.2.3 segue que $Trd_{\mathcal{H}}(\mathcal{H}^1) = [-2, 2]$ e então,

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

ou seja, $\sigma_i(tr(T)) \in [-2, 2]$, para todo $T \in \Gamma$. Portanto, $\sigma_i(tr(T))$ é limitado em $\mathbb{R}$, para $2 \leq i \leq n$ e para todo $T \in \Gamma$. Resta mostrar que $\mathbb{K}_1 = \mathbb{K}$. Suponhamos que $\mathbb{K}$ seja uma extensão própria de $\mathbb{K}_1$. Assim, para algum $i \in \{2, \ldots, n\}$, tem-se que $\sigma_i \neq id$ e $\sigma_i|_{\mathbb{K}_1} = id$. Pela definição de $\mathbb{K}_1$, segue que $tr(T) = \sigma_i(tr(T))$ está contido no intervalo $[-2, 2]$, para todo $T \in \Gamma$. Logo, pelo Teorema 2.1.2, segue que Γ não possui elementos hiperbólicos, o que contradiz a hipótese de $\mu(\mathbb{H}^2/\Gamma) < \infty$. Portanto, $\mathbb{K}_1 = \mathbb{K}$ e a condição (ii) também é satisfeita.

Reciprocamente, suponhamos agora que as condições (i) e (ii) são satisfeitas. Sejam $\mathbb{K}_1$ um corpo de números de grau n e $\sigma_i : \mathbb{K}_1 \to \mathbb{R}$ os monomorfismos distintos de $\mathbb{K}_1$ em $\mathbb{R}$, com $i = 1, \ldots, n$ e $\sigma_1 = id$. Para cada i vamos estender σ_i para o isomorfismo

$$\psi : \mathbb{K} \to \mathbb{C},$$

onde $\mathbb{K} = \mathbb{K}_1(\lambda)$ e $[\mathbb{K} : \mathbb{K}_1] = 2$. Considerando a álgebra dos quatérnios $\mathcal{A}[\Gamma]$ como em (2.20), tem-se os monomorfismos $\Psi_i : \mathcal{A}[\Gamma] \to M(2, \mathbb{C})$ definidos por

$$\Psi_i(x) = \begin{pmatrix} \psi_i(a) & \psi_i(b) \\ \psi_i(\bar{b}c_1) & \psi_i(\bar{a}) \end{pmatrix},$$

para $i = 1, \ldots, n$, onde $x = \begin{pmatrix} a & b \\ \bar{b}c_1 & \overline{a} \end{pmatrix} \in \mathcal{A}[\Gamma]$. Assim,

$$\mathcal{A}_{\sigma_i} = \mathcal{A}_{\psi_i} = \Psi_i(\mathcal{A}[\Gamma]) = \left\{ \begin{pmatrix} \psi_i(a) & \psi_i(b) \\ \psi_i(\bar{b}c_1) & \psi_i(\overline{a}) \end{pmatrix} : a, b \in \mathbb{K} \right\}$$

é uma álgebra dos quatérnios sobre $\psi_i(\mathbb{K}_1) = \sigma_i(\mathbb{K}_1)$, para $i = 1, \ldots, n$. Para $\sigma_1 = id$ tem-se que

$$\mathcal{A}_{\sigma_1} \otimes \mathbb{R} \simeq M(2, \mathbb{R}).$$

E, como $\psi_i(\overline{a}) = \overline{\psi_i(a)}$, para $i = 2, \ldots, n$, segue que

$$\mathcal{A}_{\sigma_i} = \left\{ \begin{pmatrix} a & b \\ \bar{b}\psi_i(c_1) & \overline{a} \end{pmatrix} : \ a, b \in \psi_i(\mathbb{K}), c_1 \in \mathbb{K}_1 \right\}.$$

Assim, pelo Lema 2.3.1, tem-se que

$$\mathcal{A}_{\sigma_i} \otimes \mathbb{R} \simeq \mathcal{H}, \text{ para } i = 2, \ldots, n.$$

Logo, concluímos que $\mathcal{A}[\Gamma]$ satisfaz as condições (2.15) e (2.16) e então, pelo Teorema 2.3.1, segue que $\mathcal{A}[\Gamma]$ é uma álgebra de divisão sobre $\mathbb{K}_1$. Portanto, Γ é um subgrupo de índice finito em $\Gamma(\mathcal{A}[\Gamma], \mathcal{O}[\Gamma])$, ou seja, Γ é um grupo derivado de uma álgebra dos quatérnios, o que conclui a demonstração. ■

2.4 Reticulados Hiperbólicos

A partir dos conceitos vistos nas Seções 2.2 e 2.3 estamos em condições de apresentar os reticulados hiperbólicos e algumas de suas principais propriedades. Sendo assim, no contexto de teoria de códigos e reticulados, nesta seção, apresentamos a teoria de reticulados hiperbólicos sobre um corpo de números totalmente real. Os resultados e propriedades sobre reticulados hiperbólicos apresentados nesta seção se encontram em [11].

Definição 2.4.1 *Considere $\mathcal{A} = (a, b)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre o corpo de números totalmente real $\mathbb{K}$. Definimos uma R-ordem $\mathcal{O}$ em $\mathcal{A}$ como um* **reticulado hiperbólico** *devido a sua identificação com um grupo fuchsiano aritmético Γ.*

No Capítulo 3, iremos considerar tesselações hiperbólicas $\{p, q\}$ associadas a grupos fuchsianos aritméticos Γ_p identificados em uma ordem dos quatérnios $\mathcal{O}$, ou de acordo com a Definição 2.4.1, com um reticulado hiperbólico. Desse modo, é possível realizar o rotulamento dos sinais de uma constelação de sinais geometricamente uniforme no plano hiperbólico. O rotulamento, apresentado em [42], é obtido pelo quociente de $\mathcal{O}$ por um ideal próprio. E, para que esta rotulagem seja completa, é necessário que as respectivas ordens sejam maximais. Na Seção 4.3, apresentaremos algumas ordens maximais dos quatérnios.

Definição 2.4.2 *Considere $\mathcal{A} = (a, b)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre o corpo de números totalmente real $\mathbb{K}$ e $\mathcal{M} \supseteq \mathcal{O}$ uma R-ordem maximal em $\mathcal{A}$. Definimos $\mathcal{M}$ como um* **reticulado hiperbólico completo** *devido a sua identificação com um grupo fuchsiano aritmético Γ.*

Agora, apresentamos algumas propriedades dos reticulados hiperbólicos como sua matriz geradora, matriz de Gram, volume e discriminante.

Definição 2.4.3 *Seja $\mathcal{O}$ uma ordem dos quatérnios identificada com um grupo fuchsiano Γ e considere a matriz*
$$M = \left(\begin{array}{cc} x_0 + x_1\sqrt{\theta} & r_1(x_2 + x_3\sqrt{\theta}) \\ r_2(x_2 - x_3\sqrt{\theta}) & x_0 - x_1\sqrt{\theta} \end{array} \right),$$
identificada com o elemento $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{O}$. Definimos M como a **matriz geradora** *para o reticulado hiperbólico $\mathcal{O}$.*

Observação 2.4.1 *Observe que o determinante da matriz geradora M, como na Definição 2.4.3, é igual a norma reduzida $Nrd(x)$ do elemento x.*

Definição 2.4.4 *Considere a matriz M nas condições da Definição 2.4.3. A matriz $G = MM^t$ é chamada* **matriz de Gram** *para o reticulado hiperbólico $\mathcal{O}$.*

Definição 2.4.5 *O volume de um reticulado hiperbólico $\mathcal{O}$, denotado por $vol(\mathcal{O})$, é definido pelo volume de uma região fundamental associada ao grupo Γ.*

Um invariante importante associado a um reticulado hiperbólico é seu discriminante que, como veremos a seguir, pode ser definido como o discriminante reduzido de uma ordem dos quatérnios, de acordo com a Definição 2.2.15.

Definição 2.4.6 *O* **discriminante** *$\mathcal{D}(\mathcal{O})$ de $\mathcal{O}$ é definido como a raiz quadrada do $\mathcal{I}_{\mathbb{K}}$-ideal gerado por $det(Trd(x_i\bar{x_j}))_{i,j=1}^4$, onde $\{x_1, x_2, x_3, x_4\}$ é uma $\mathcal{I}_{\mathbb{K}}$-base de $\mathcal{O}$ e $Trd(x_i\bar{x_j})$ é o traço reduzido do elemento $x_i\bar{x_j}$.*

Utilizando estes parâmetros acreditamos ser possível fazer uma classificação dos reticulados hiperbólicos ou então, relacionar tais reticulados com os reticulados euclidianos. Para os reticulados euclidianos já são conhecidas algumas classificações de acordo com a densidade de empacotamento do reticulado, sua diversidade ou distância produto mínima, por exemplo. Como o estudo dos reticulados euclidianos não é o foco para este trabalho, omitimos tais definições, mas sugerimos a referência [16] sobre este assunto.

Uma primeira abordagem sobre esta relação entre reticulados hiperbólicos e reticulados euclidianos será feita na Seção 4.2 onde apresentamos uma associação dos reticulados hiperbólicos que são obtidos neste trabalho com subcorpos maximais reais de corpos ciclotômicos. A motivação para tal associação ocorre do fato de em [4, 7, 29] os autores utilizarem esta classe especial de corpos de números para encontrar bons reticulados de acordo com sua densidade de empacotamento, diversidade e distância produto mínima.

Capítulo 3

Construção de Grupos Fuchsianos Aritméticos

Neste capítulo, nosso objetivo é considerar tesselações hiperbólicas regulares $\{p, q\}$ que geram superfícies de gênero $g \geq 2$, dessa forma tem-se que p e q são funções de g. Além disso, estamos interessados em tesselações $\{p, q\}$ em que é possível obter um grupo fuchsiano aritmético Γ_p asssociado, pois este grupo é a estrutura algébrica de nosso interesse para construir constelações de sinais no plano hiperbólico.

Na Seção 4.3.1, apresentamos uma construção do grupo fuchsiano aritmético Γ_p a partir dos conceitos sobre grupos fuchsianos aritméticos apresentados no Capítulo 2. Na Subseção 3.1.1, apresentamos uma condição necessária para obter grupos fuchsianos aritméticos Γ_p associados a uma tesselação hiperbólica $\{p, q\}$, esta condição é dada através do Teorema 3.1.3, o qual chamamos de condição de Fermat. Mostramos que um grupo fuchsiano aritmético pode ser identificado através da forma de seus geradores, pois assim conseguimos identificar a álgebra e a ordem dos quatérnios associados a este grupo, tornando-o aritmético. A partir destes resultados, na Seção 3.2, apresentamos um algoritmo para obter os geradores de um grupo fuchsiano aritmético.

A tesselação hiperbólica de maior interesse que tratamos neste trabalho é a tesselação auto-dual $\{4g, 4g\}$, com $g \geq 2$, pois para esta tesselação é possível obter grupos fuchsianos aritméticos para diversos valores de g, de acordo com a condição de Fermat. Apesar desta tesselação não ter uma boa densidade de empacotamento, [8], a mesma apresenta uma baixa complexidade computacional devido a sua auto dualidade.

Outras tesselações hiperbólicas que geram superfícies de gênero $g \geq 2$ e que possuem uma melhor densidade de empacotamento, e portanto, reticulados mais densos, também são consideradas neste trabalho. Apresentamos as tesselações $\{4g + 2, 2g + 1\}$ e $\{12g - 6, 3\}$, sendo esta última a tesselação mais densa dentre todas as tesselações hiperbólicas. Porém, o problema que surge em decorrência da mudança da tesselação $\{4g, 4g\}$ para outras tesselações $\{p, q\}$, como as citadas acima, é a dificuldade em determinar valores de p e q em que um grupo fuchsiano aritmético Γ_p pode ser associado, segundo a condição de Fermat.

3.1 Grupo Fuchsiano Aritmético Γ_p

Nosso objetivo, nesta seção, é fornecer condições necessárias para que um grupo fuchsiano aritmético Γ_p possa ser obtido a partir de uma tesselação hiperbólica $\{p, q\}$. Iniciamos fornecendo condições gerais baseadas em resultados conhecidos na literatura, de modo a estabelecer uma conexão entre tesselação hiperbólica e grupos fuchsianos. Esta relação é estabelecida através dos emparelhamentos das arestas do polígono fundamental $\mathcal{P}_p$. Finalizamos, na Subseção 3.1.1, com o resultado mais importante desta seção em que fornecemos uma condição necessária para obter estes grupos, condição esta que chamamos de condição de Fermat, devido a associação deste resultado com os números de Fermat.

Vimos na Subseção 2.1 que uma superfície de Riemann pode ser obtida considerando o espaço quociente $\mathbb{D}^2/\Gamma_p$, onde o grupo Γ_p age de maneira propriamente descontínua sobre $\mathbb{D}^2$ se, e somente se, Γ_p é um grupo fuchsiano, conforme foi visto no Teorema 2.1.3. Com o objetivo de construir constelações de sinais hiperbólicas provenientes de tesselações $\{p, q\}$, a busca dos grupos Γ_p e, portanto, das superfícies $\mathbb{D}^2/\Gamma_p$, é equivalente, por exemplo, à busca dos ideais primos $\mathfrak{p}$, os quais são convenientemente escolhidos no anel dos inteiros $\mathcal{I}_\mathbb{K}$ de um corpo de números $\mathbb{K}$. Neste caso, o objetivo é construir constelações de sinais euclidianas, provenientes dos anéis quocientes $\mathcal{I}_\mathbb{K}/\mathfrak{p}$ que têm estruturas de corpos. Portanto, enquanto que na construção de constelações de sinais no plano euclidiano consideramos quocientes dotados de uma estrutura (que pode ser por exemplo: grupos [18, 44] ou anéis [27, 48]), no plano hiperbólico consideramos superfícies de Riemann.

Consideramos emparelhamentos das arestas de polígonos hiperbólicos regulares $\mathcal{P}_p$ com p arestas que estão associados às tesselações hiperbólicas regulares $\{p, q\}$. Seja Γ_p o grupo discreto de isometrias. Através dos Teoremas 2.1.4 e 2.1.5, concluímos que para obter Γ_p a partir de uma tesselação hiperbólica $\{p, q\}$, é necessário considerar um conjunto de emparelhamentos das arestas de $\mathcal{P}_p$, como na Definição 2.1.4, satisfazendo a condição dada na Equação (2.5). Caso esta condição não seja satisfeita não podemos garantir que o grupo Γ_p seja discreto e, para nossa proposta, esta condição deve ser satisfeita, uma vez que desejamos considerar constelações de sinais que são Γ_p-órbita de 0, baricentro de $\mathcal{P}_p$.

Sendo assim, é possível obter o gênero g da superfície compacta resultante $\mathbb{D}^2/\Gamma_p$. O gênero g é obtido através da **característica de Euler**, a qual é definida pela seguinte equação

$$\chi(\mathbb{D}^2/\Gamma_p) = \text{ número de vértices } - \text{ número de arestas } + \text{ número de faces},$$

ou seja,

$$\chi(\mathbb{D}^2/\Gamma_p) = \frac{p}{q} - \frac{p}{2} + 1 = 2 - 2g, \tag{3.1}$$

para superfícies compactas.

Pelo Corolário 2.1.2, segue que toda superfície compacta de gênero $g \geq 2$ pode ser modelada pelo plano hiperbólico. Assim, $\Gamma_p \backslash \{id\}$ possui apenas elementos hiperbólicos. Logo, pela Observação 2.1.6, segue que a assinatura do grupo Γ_p é $(g; -)$, e de acordo com o Teorema 2.1.8, segue que

$$\mu(\mathcal{P}_p) = \mu(\mathbb{D}^2/\Gamma) = 4\pi(g-1).$$

Nesta direção, consideremos uma tesselação hiperbólica $\{p, q\}$, $\mathcal{P}_p$ o polígono fundamental regular de p arestas associado a $\{p, q\}$ e Γ_p o grupo fuchsiano obtido à partir de $\mathcal{P}_p$. Queremos à partir de Γ_p obter uma superfície compacta e orientável $\mathbb{D}^2/\Gamma$ de gênero g. Primeiramente, devemos ter, [8],

$$4g \leq p \leq 12g - 6.$$

Agora, considerando a restrição da relação de equivalência dada em (2.7) sobre o conjunto das arestas de $\mathcal{P}_p$ e pela Definição 2.1.4, verificamos que cada classe de equivalência de arestas, que fazem os emparelhamentos dos lados de um polígono através de uma transformação de emparelhamento, contém exatamente dois elementos. Logo, p deve ser necessariamente um número par.

Seja $\{u_1, \ldots, u_p\}$ o conjunto de arestas de $\mathcal{P}_p$. Assim, para uma aresta $u_i \in \mathcal{P}_p$, segue que existe uma única aresta $u_j \in \mathcal{P}_p$ e uma única transformação de emparelhamento $T \in \Gamma_p$ tal que

$$T(u_i) = u_j \Leftrightarrow T^{-1}(u_j) = u_i,$$

ou seja, a classe de equivalência de u_i é $\{u_i, u_j\}$. Neste caso, dizemos que T relaciona o par $\{u_i, u_j\}$. Observamos ainda que, se T relaciona o par $\{u_i, u_j\}$, então T^{-1} também relaciona. Usamos os símbolos

$$T(u_i) = u_j \Leftrightarrow u_i \to u_j \Leftrightarrow \{u_i, u_j\},$$

para indicar que u_i e u_j pertencem à mesma classe de equivalência.

Por outro lado, como cada vértice de $\mathcal{P}_p$ é recoberto por q desses polígonos, segue pelo Teorema 2.1.4, que cada ciclo de vértices deve conter exatamente q vértices, de modo que q deve dividir p. Estas são as condições que devemos usar para determinar os emparelhamentos das arestas de $\mathcal{P}_p$.

O processo de construção de cada conjunto de emparelhamentos é heurística. Em [40] é feita uma busca exaustiva de 927 tipos de emparelhamentos de arestas de polígonos hiperbólicos regulares que geram superfícies de gênero 3. Nas Seções 3.3, 3.4 e 3.5, apresentamos alguns conjuntos de emparelhamentos de modo a construir grupos fuchsianos para as tesselações específicas $\{4g, 4g\}$, $\{4g + 2, 2g + 1\}$ e $\{12g - 6, 3\}$, respectivamente.

Como um exemplo importante de emparelhamento, citamos o *emparelhamento diametralmente oposto*. Neste tipo de emparelhamento, toda aresta de $\mathcal{P}_p$ é emparelhada com sua aresta diametralmente oposta. Dessa forma, se $\{u_1, \ldots, u_p\}$ é o conjunto de arestas de $\mathcal{P}_p$, então temos a seguinte associação das arestas

$$u_i \to u_{i+\frac{p}{2}}, \text{ para } i = 1, \ldots, \frac{p}{2},$$

ou seja, cada transformação de emparelhamento T_i relaciona o par $\{u_i, u_{i+\frac{p}{2}}\}$, com $i = 1, \ldots, \frac{p}{2}$.

Em codificação quântica topológica, [2], o emparelhamento diametralmente oposto é o mais desejado, pois este é o caminho homologicamente não trivial com a maior distância mínima possível. Como consequência, o código resultante apresenta uma capacidade de correção de erros maior dentre todos os códigos oriundos dos demais emparelhamentos. Observamos que este tipo de emparelhamento não pode ser obtido para uma tesselação $\{p, q\}$ qualquer. Nas tesselações que são consideradas neste trabalho, tem-se que para as tesselações $\{4g, 4g\}$ e $\{4g + 2, 2g + 1\}$

é possível obter um emparelhamento diametralmente oposto das arestas. Já para a tesselação $\{12g-6,3\}$ acreditamos não ser possível obter tal emparelhamento, em razão da busca exaustiva feita em [40] para a tesselação $\{30,3\}$ (proveniente da tesselação $\{12g-6,3\}$, para $g=3$).

Devido a importância deste emparelhamento, durante muitas ocasiões neste trabalho, utilizamos o emparelhamento diametralmente oposto, de modo a exemplificar determinados resultados válidos para emparelhamentos quaisquer.

3.1.1 Geradores do Grupo Γ_p

Relembramos que o objetivo central desta seção, é fornecer uma condição necessária para que possamos encontrar os geradores de um grupo fuchsiano $\Gamma \simeq \Gamma_p$ a partir de uma tesselação $\{p,q\}$, com o intuito de obter a álgebra e a ordem dos quatérnios associadas a este grupo, e portanto, defini-lo como aritmético. Para isso, estabelecemos as condições sobre o polígono $\mathcal{P}_p$ associado a $\{p,q\}$ e sobre a matriz A_1 associada à transformação hiperbólica T_1, pois veremos que a partir da matriz A_1 obtem-se os geradores de Γ.

Seja $\mathcal{P}_p$ o polígono regular com p arestas associada à tesselação $\{p,q\}$. Sem perda de generalidade, podemos supor que $\mathcal{P}_p$ esteja centrado em 0, a origem de $\mathbb{D}^2$. Consideremos

$$u_1, u_2, \ldots, u_p \;\; \text{e} \;\; v_1, v_2, \ldots, v_p, \tag{3.2}$$

as arestas e os vértices de $\mathcal{P}_p$ dispostos em ordem cíclicas no sentido anti-horário, respectivamente. Ligando cada vértice de $\mathcal{P}_p$ ao seu baricentro, obtemos p triângulos hiperbólicos Δ_p. Como $\{p,q\}$ é regular, segue que cada um desses triângulos tem ângulo $\frac{2\pi}{p}$ no vértice que é o baricentro e ângulos $\frac{\pi}{q}$ nos outros dois vértices. Logo, pelo Teorema de Gauss-Bonnet para um triângulo hiperbólico (Teorema 1.4.3), segue que cada triângulo Δ_p tem área igual a

$$\mu(\Delta_p) = \frac{\pi(pq-2q-2p)}{pq}.$$

A Figura 3.1 mostra uma representação do polígono hiperbólico regular $\mathcal{P}_p$ e de um triângulo hiperbólico Δ_p como descritos acima.

Seja $T_1 \in \Gamma_p$ uma isometria que emparelha a aresta u_1 em sua diametralmente oposta, ou seja,

$$T_1(u_1) = u_{\frac{p}{2}+1}.$$

As isometrias que mantém $\mathbb{D}^2$ invariante são as transformações lineares da forma

$$T_1(z) = \frac{az+b}{\bar{b}z+\bar{a}}, \quad \text{onde} \;\; a,b \in \mathbb{C}, \quad |a|^2+|b|^2 = 1.$$

Assim, a matriz associada à transformação T_1 é da forma

$$A_1 = \begin{pmatrix} a & b \\ \bar{b} & \bar{a} \end{pmatrix}, \quad \text{onde} \;\; a,b \in \mathbb{C}, \quad |a|^2+|b|^2 = 1.$$

Através de relações de ângulos e arestas entre uma região fundamental de $\mathcal{P}_p$, cujo baricentro é o ponto 0 de $\mathbb{D}^2$ e do círculo isométrico $I(T_1)$ da isometria T_1, podemos obter os valores $a, b, \bar{a}, \bar{b}$

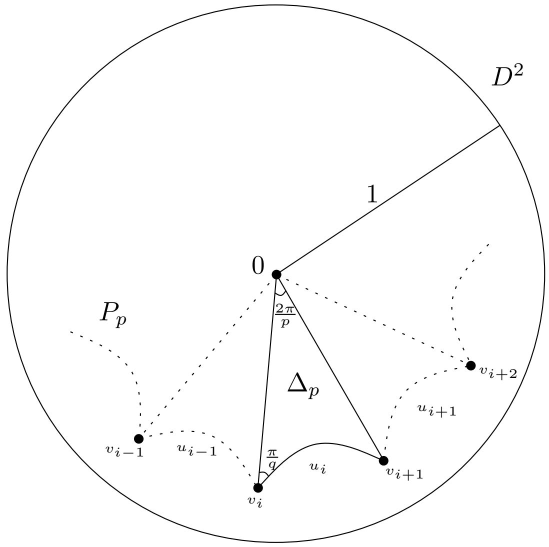

Figura 3.1: *Polígono e triângulo em uma tesselação* $\{p, q\}$ *em* $\mathbb{D}^2$

da matriz A_1, qualquer que seja o emparelhamento utilizado. Se conhecermos a transformação T_1 podemos obter os outros elementos de Γ_p como conjugações elípticas de T_1 por meio de potências de T_C, onde T_C é uma tranformação elíptica de ordem p com matriz associada

$$C = \begin{pmatrix} e^{\frac{i\pi}{p}} & 0 \\ 0 & e^{\frac{-i\pi}{p}} \end{pmatrix}. \tag{3.3}$$

O teorema a seguir fornece a matriz A_1 quando a transformação T_1 emparelha a aresta u_1 com sua diametralmente oposta.

Teorema 3.1.1 *[53] Sejam $\mathcal{P}_p$ o polígono regular de p arestas e Γ_p o grupo fuchsiano, associados à tesselação $\{p, q\}$. Se $T_1 \in \Gamma_p$ é tal que $T_1(u_1) = u_{1+\frac{p}{2}}$, então a matriz A_1 associada à transformação T_1 é dada por*

$$A_1 = \begin{pmatrix} \frac{2\cos\frac{\pi}{q}}{2sen\frac{\pi}{p}} & \frac{\sqrt{2\cos\frac{2\pi}{p}+2\cos\frac{2\pi}{q}}\cdot e^{i\left(\frac{p+1}{p}\right)\pi}}{2sen\frac{\pi}{p}} \\ \frac{\sqrt{2\cos\frac{2\pi}{p}+2\cos\frac{2\pi}{q}}\cdot e^{-i\left(\frac{p+1}{p}\right)\pi}}{2sen\frac{\pi}{p}} & \frac{2\cos\frac{\pi}{q}}{2sen\frac{\pi}{p}} \end{pmatrix}. \tag{3.4}$$

Fazendo uso de um conjunto de emparelhamentos das arestas de $\mathcal{P}_p$, a partir de T_1, determinamos as outras isometrias de emparelhamentos que geram Γ_p, por conjugações da forma $T_i = T_{C^{r_i}} \circ T_1 \circ T_{C^{-r_i}}$, onde r_i é a potência de T_C e sendo T_C a transformação elíptica de ordem p.

Sendo assim, a partir de A_1 e portanto da transformação T_1, tem-se que as matrizes associadas às demais transformações são da forma

$$A_i = C^{r_i} A_1 C^{-r_i}, \text{ onde } i = 2, \ldots, p/2, \tag{3.5}$$

e r_i é a potência de T_C. Por exemplo, em $T_{C^{r_i}}(u_1) = u_i$, r_i representa a quantidade de arestas que u_1 está distante de u_i, com $i = 1, \ldots, p/2$ e considerando a ordem estabelecida em (3.2).

Observação 3.1.1 *O Teorema 3.1.1 é válido para todo tipo de emparelhamento que possui ao menos uma aresta emparelhada com a sua diamentralmente oposta, e as demais matrizes de transformação A_i sempre podem ser obtidas através de relações do tipo visto nas Equações (3.5), onde C^r sempre depende do emparelhamento escolhido.*

Agora, consideremos o grupo $\Gamma = f^{-1} \circ \Gamma_p \circ f \in \mathbb{H}^2$, onde f é como dado em (1.4). Assim, utilizando o isomorfismo definido por f, tem-se que

$$\Gamma \simeq \Gamma_p.$$

Considerando $G_1, \ldots, G_{p/2}$ os geradores do grupo Γ temos, através deste isomorfismo, a seguinte associação entre os geradores de Γ e Γ_p:

$$G_i = f^{-1} A_1 f, \text{ onde } i = 2, \ldots, p/2, \tag{3.6}$$

considerando a multiplicação usual de matrizes. Porém, para o grupo $\Gamma \in \mathbb{H}^2$, tem-se uma representação para os seus geradores que será dada pelo resultado que segue.

Lema 3.1.1 *[53] Se Γ é um grupo fuchsiano aritmético finitamente gerado por $G_1, \ldots, G_l$, então*

$$G_k = \frac{1}{2^s} \begin{pmatrix} x_k + y_k\sqrt{\theta} & z_k + w_k\sqrt{\theta} \\ -z_k + w_k\sqrt{\theta} & x_k - y_k\sqrt{\theta} \end{pmatrix}, \quad \textit{onde} \quad k = 1, \ldots, l, \tag{3.7}$$

$G_k \in M(2, \mathbb{K}(\sqrt{\theta}))$, $s \in \mathbb{N}$, $\theta, x_k, y_k, z_k, w_k \in \mathbb{K}$ e $\mathbb{K}$ um corpo de números totalmente real. Além disso, qualquer elemento $T \in \Gamma$ assume a mesma forma dos geradores de Γ.

Johansson em [28] mostrou que um grupo fuchsiano aritmético está associado a uma ordem $\mathcal{O}$ em uma álgebra dos quatérnios $\mathcal{A}$ sobre uma extensão quadrática $\mathbb{K}$ de $\mathbb{Q}$, onde os geradores de Γ são da forma

$$G_l = \frac{1}{2} \begin{pmatrix} a + b\sqrt{\theta} & r_1(c + d\sqrt{\theta}) \\ -r_2(c - d\sqrt{\theta}) & a - b\sqrt{\theta} \end{pmatrix},$$

onde $\theta, a, b, c, d \in \mathbb{Z}[\theta]$, $r_1 = -r_2 \in \mathbb{Z}$, $\theta \in \mathbb{Z}[\theta]$, $\sqrt{\theta} \notin \mathbb{Z}[\theta]$ e $\mathbb{Z}[\theta]$ é o anel dos inteiros de $\mathbb{K}$. Utilizando o Lema 3.1.1, podemos estender este resultado para extensões de grau maior que 2 e dessa forma, se os geradores do grupo fuchsiano $\Gamma \simeq \Gamma_p$ são da forma dada em (3.7), então, de acordo com o isomorfismo definido em (2.8), mostra-se que o grupo fuchsiano aritmético Γ_p é derivado de uma álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, sobre o corpo de números totalmente real $\mathbb{K} = \mathbb{Q}(\theta)$. Dessa forma, os elementos do grupo fuchsiano aritmético Γ_p podem ser associados com os elementos da ordem dos quatérnios $\mathcal{O} = (\theta, -1)_R$, onde $R = \mathcal{I}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$. Ou ainda, podem ocorrer casos em que a álgebra e a ordem dos quatérnios associadas sejam da forma $\mathcal{A} = (\theta_1, -1)_{\mathbb{K}}$ e $\mathcal{O} = (\theta_1, -1)_R$, com $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta_1 \in \mathbb{K} = \mathbb{Q}(\theta)$ e $R = \mathcal{I}_{\mathbb{K}}$.

Pela Equação (3.6), segue que os geradores G_i's podem ser obtidos a partir das matrizes A_i's, onde $i = 1, \ldots, p/2$. As matrizes A_i's, com $i = 2, \ldots, p/2$, podem ser obtidas a partir da matriz A_1, como vimos em (3.5). Portanto, para obtermos os geradores de Γ_p na forma dada em (3.7), precisamos estabelecer as condições sobre as entradas da matriz A_1, obtida no Teorema 3.1.1.

Note que as operações aplicadas em cada uma das entradas da matriz A_1 mostrada em (3.4) são funções trigonométricas seno e cosseno. Mas, os ângulos da forma $\frac{m\pi}{n}$, com $m, n \in \mathbb{Z}$, para os quais as funções trigonométricas podem ser expressas em termos de radicais finitos de números reais, são limitadas a valores de n que são precisamente aqueles que produzem polígonos construtíveis com régua e compasso.

Construções de polígonos regulares com régua e compasso com $3, 4, 5, 6, 8, 10, 12, 16, 20, 24, 32, 40, 48, 64, \ldots$ lados, datam do período de Euclides. No entanto, Gauss mostrou em 1796, uma condição suficiente para um polígono regular de n lados ser construtível e, a prova desta condição ser necessária é creditada a Wantzel (1836). Com isso, temos o seguinte resultado:

Teorema 3.1.2 *[31](Gauss - Wantzel) Um polígono regular de $n \geq 3$ lados pode ser construído com régua e compasso se, e somente se, n for o produto de uma potência de 2 ou n for o produto de uma potência de 2 com números de Fermat distintos, isto é,*

$$n = 2^k \quad ou \quad n = 2^k p_1 p_2 \ldots p_s,$$

onde k é um inteiro não negativo e os números p_i's são números de Fermat distintos.

Observação 3.1.2 *Um* **número de Fermat** *é um número primo da forma*

$$p_s = 2^{2^s} + 1,$$

onde $s \geq 0$ é um inteiro. Os únicos números de Fermat conhecidos são

$$p_0 = 3; \; p_1 = 5; \; p_2 = 17; \; p_3 = 257; \; p_4 = 65537,$$

e, parece ser improvável que mais serão encontrados, [31].

Dessa forma, como a matriz A_1 dos coeficientes da transformação T_1 é dada por expressões que dependem de seno e cosseno de ângulos da forma $\frac{m\pi}{p}$, $\frac{m\pi}{q}$, com $m \in \mathbb{N}$ e p, q provenientes da tesselação $\{p, q\}$ utilizada, segue que para obtermos entradas em termos de radicais finitos de números reais na matriz A_1, e assim conseguirmos que os geradores G_i's do grupo fuchsiano Γ_p estejam na forma (3.7), devemos estabelecer a condição de que p e q sejam decompostos na forma 2^k ou $2^k p_1 p_2 \ldots p_s$. Com isso, mostramos de forma construtiva o seguinte resultado.

Teorema 3.1.3 (Condição de Fermat) *Se Γ_p é um grupo fuchsiano proveniente de uma tesselação $\{p, q\}$, então é possível encontrar os geradores de $\Gamma \simeq \Gamma_p$ e, portanto, o grupo fuchsiano aritmético, se p e q puderem ser decompostos na forma:*

$$2^k \quad ou \quad 2^k p_1 p_2 \ldots p_s, \tag{3.8}$$

onde k é um inteiro não negativo e os p_i's são números distintos de Fermat.

■

Observação 3.1.3 *Acreditamos que a recíproca deste resultado seja válida para o caso de querermos encontrar grupos fuchsianos aritméticos através de geradores na forma (3.7), com coeficientes num corpo totalmente real. Mas isto não significa que não seja possível encontrar grupos fuchsianos aritméticos para tesselações $\{p, q\}$, onde p e q não são decompostos como em (3.8), através de outros métodos.*

3.2 Algoritmo para a Obtenção de Grupos Fuchsianos Aritméticos

A partir de alguns conceitos em geometria hiperbólica, álgebra dos quatérnios e grupos fuchsianos nosso objetivo é fornecer um algoritmo passa-a-passo para se obter grupos fuchsianos aritméticos a partir de uma tesselação $\{p, q\}$ regular e um emparelhamento fixado. Para que este algoritmo seja eficiente precisamos que algumas condições sejam satisfeitas.

Primeiramente, dados p e q provenientes de uma tesselação regular $\{p, q\}$ precisamos verificar se p e q satisfazem a condição apresentada na inequação (1.8) e a condição de Fermat estabelecida no Teorema 3.1.3.

Além disso, as transformações que fazem o emparelhamento das arestas do polígono hiperbólico regular $\mathcal{P}_p$ associado à tesselação $\{p, q\}$ devem ser hiperbólicas, pois estamos interessados em tesselações que geram superfícies compactas (de Riemann) de gênero $g \geq 2$. Esta condição pode ser garantida através do Teorema 2.1.2 e do Corolário 2.1.2.

Como vimos, a ação do grupo Γ_p em $\mathbb{D}$ pode se processar pela identificação das arestas de um polígono hiperbólico regular $\mathcal{P}_p$ de p arestas em $\mathbb{D}$ por isometrias que geram Γ_p, ou seja, pelas transformações de emparelhamentos que como vimos devem ser hiperbólicas. Além disso, para gerar o grupo fuchsiano Γ_p estas transformações devem satisfazer as condições de Poincaré de lados e ângulos mostradas nos Teoremas 2.1.4 e 2.1.5. Através destes resultados, tem-se que o grupo fuchsiano Γ_p tem a seguinte representação

$$\Gamma_p = \{T_1, \ldots, T_t \in \mathbb{D} : T_\varepsilon = id\}, \tag{3.9}$$

onde T_ε representa o conjunto de relações entre as transformações que pertencem ao ciclo ε e, de acordo com (2.6), a quantidade de ciclos de uma tesselação $\{p, q\}$ é $\frac{p}{q}$. O conjunto de relações entre as transformações contidas em cada ciclo de vértices ε depende do tipo de emparelhamento utilizado, porém, qualquer que seja o tipo de emparelhamento utilizado, estas relações devem satisfazer (3.9) e os ciclos de vértices ε devem satisfazer as condições apresentadas na Observação 2.1.5.

Sabemos que um grupo fuchsiano aritmético $\Gamma[\mathcal{A}, \mathcal{O}]$ é um grupo fuchsiano Γ_p associado a uma álgebra dos quatérnios $\mathcal{A}$ e uma ordem dos quatérnios $\mathcal{O}$, e que nem sempre é possível obter esta associação, ou seja, nem sempre é possível obter um grupo fuchsiano aritmético. Através da condição de Fermat obtemos uma condição necessária. Se os geradores forem apresentados na forma dada em (3.7), dizemos que o grupo fuchsiano $\Gamma \simeq \Gamma_p$ é associado a álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ e ordem dos quatérnios $\mathcal{O} = (\theta, -1)_{I_{\mathbb{K}}}$, onde $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números e $\mathcal{I}_{\mathbb{K}}$ é o seu anel dos inteiros e, portanto, Γ_p é um grupo fuchsiano aritmético.

Para exemplificar o algoritmo, consideramos o emparelhamento diametralmente oposto das arestas do polígono regular hiperbólico $\mathcal{P}_p$, que como vimos, neste tipo de emparelhamento toda aresta de $\mathcal{P}_p$ é emparelhada com a sua diametralmente oposta. Fixando este emparelhamento, em uma tesselação $\{p, q\}$, se tivermos a transformação T_1 que é emparelhada com sua aresta diamentralmente oposta $T_{\frac{p}{2}+1}$, vimos que a sua matriz associada A_1 é dada como em (3.4). Assim, as demais transformações de emparelhamentos serão dadas por

$$A_i = C^{i-1} A_1 C^{-(i-1)},$$

onde $i = 2, \dots, \frac{p}{2}$ e C é a matriz associada à transformação elíptica de ordem p, ou seja,

$$C = \begin{pmatrix} e^{\frac{i\pi}{p}} & 0 \\ 0 & e^{-\frac{i\pi}{p}} \end{pmatrix}.$$

3.2.1 Algoritmo

Agora, munido dos resultados apresentados acima, estamos em condições de estabelecer o algoritmo que éserá estruturado da seguinte forma:

Algoritmo para Obtenção de Grupos Fuchsianos Aritméticos

Sejam $\{p, q\}$ uma tesselação regular e $\mathcal{P}_p$ o polígono regular hiperbólico associado a esta tesselação com um emparelhamento de arestas pré-fixado. Fornecendo como entrada os valores de p e q, este algoritmo fornece como saída uma representação dos geradores G_i's para o grupo fuchsiano aritmético $\Gamma \simeq \Gamma_p$ diretamente ou parcialmente (neste último caso podendo ser facilmente encontrado) na forma dada em (3.7). Podendo assim ser associado a álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ e a ordem dos quatérnios $\mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathbb{K} = \mathbb{Q}(\theta)$ e $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ é o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\theta)$. Ou ainda, podendo ser associado com $\mathcal{A} = (\theta_1, -1)_{\mathbb{K}}$ e $\mathcal{O} = (\theta_1, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathbb{K} = \mathbb{Q}(\theta)$, $\theta_1 \in \mathbb{K}$ e $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$.

- **[Etapa 1 - Entrada]**
  p, q com $(p-2)(q-2) > 4$. Como estamos interessados em tesselações hiperbólicas que geram superfícies de gênero $g \geq 2$ e os valores de p e q são funções de g, segue pelo Teorema 1.4.5 e pela Observação 1.4.5, que p e q devem satisfazer a inequação

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

  e pertencerem a uma tesselação que gera uma superfície de gênero $g \geq 2$.

- **[Etapa 2 - Verificar condição de Fermat]**
  Decompor p e q em fatores primos e verificar se esta decomposição satisfaz a condição de Fermat, estabelecida no Teorema 3.1.3, ou seja, se a decomposição é da forma

  $$p = 2^j p_1 \dots p_r$$

  e

  $$q = 2^k q_1 \dots q_s,$$

  com j, k inteiros não negativos e p_i's e q_i's números distintos de Fermat. Caso contrário, finalizar o algoritmo.

- **[Etapa 3 - Computar matriz A_1]**
  Como pré-fixamos o emparelhamento diametralmente oposto, segue, de acordo com o Teorema 3.1.1, que o cálculo da matriz A_1, neste caso, é dado da seguinte forma:

$$A_1 = \left(\begin{array}{cc} \frac{2\cos\frac{\pi}{q}}{2sen\frac{\pi}{p}} & \frac{\sqrt{2\cos\frac{\pi}{p}+2\cos\frac{\pi}{q}}\cdot e^{i\left(\frac{p+1}{p}\right)\pi}}{2sen\frac{\pi}{p}} \\ \frac{\sqrt{2\cos\frac{\pi}{p}+2\cos\frac{\pi}{q}}\cdot e^{-i\left(\frac{p+1}{p}\right)\pi}}{2sen\frac{\pi}{p}} & \frac{2\cos\frac{\pi}{q}}{2sen\frac{\pi}{p}} \end{array} \right).$$

Observamos que esta matriz pode ser utilizada em qualquer emparelhamento que tenha ao menos uma aresta emparelhada com sua diametralmente oposta. Além disso, qualquer que seja o emparelhamento utilizado, sempre é possível obter a matriz A_1 associada à transformação T_1 através de relações trigonométricas e de congruência entre ângulos e arestas do polígono fundamental $\mathcal{P}_p$.

- **[Etapa 4 - Computar matriz C e sua inversa C^{-1}]**
  Considerando T_C uma transformação elíptica de ordem p, a matriz associada a esta transformação e que queremos computar é dada, como em (3.3), por

$$C = \left(\begin{array}{cc} e^{\frac{i\pi}{p}} & 0 \\ 0 & e^{-\frac{i\pi}{p}} \end{array} \right).$$

  Como $C \in M(2, \mathbb{K})$, segue que C possui inversa C^{-1} que pode ser facilmente calculada.

- **[Etapa 5 - Computar as demais matrizes de transformações A_i's, com $i = 2, \ldots, \frac{p}{2}$]**
  Conhecendo uma transformação que faz o emparelhamento de arestas de $\mathcal{P}_p$, obtida na Etapa 3, as demais transformações podem ser obtidas como conjugações elípticas desta utilizando as matrizes C e C^{-1} obtidas na Etapa 4. Neste caso em que pré-fixamos o emparelhamento diametralmente oposto, estas matrizes são obtidas da seguinte forma: Para $i = 2, \ldots, \frac{p}{2}$ calcular

$$A_i = C^{i-1} A_1 C^{-(i-1)}.$$

- **[Etapa 6 - Computar as inversas, A_i^{-1}'s, das matrizes de transformações A_i's, com $i = 1, \ldots, \frac{p}{2}$]**
  A partir das matrizes de transformações obtidas nas Etapas 3 e 5, calcular as inversas A_i^{-1}'s destas matrizes, com $i = 1, \ldots, \frac{p}{2}$.

- **[Etapa 7 - Verificar condição de hiperbolicidade]**
  Nesta etapa verificamos se todas matrizes de transformações obtidas nas Etapas 3 e 5 são de fato hiperbólicas. Isto é feito através do cálculo do traço destas matrizes da seguinte forma: Para $i = 1, \ldots, \frac{p}{2}$ calcular

$$t_i = tr^2(A_i).$$

  De acordo com o Teorema 2.1.2, para que as transformações associadas a estas matrizes sejam hiperbólicas, devemos ter $t_i > 4$, para todo $i = 1, \ldots, \frac{p}{2}$. Caso $t_i \leq 4$ para algum i, finalizar o algoritmo.

- **[Etapa 8 - Verificar condição de Poincaré]**
  Dado um conjunto de relações em um ciclo de vértices as quais são obtidas de acordo com o emparelhamento utilizado, precisamos verificar se este conjunto de relações, com respeito a operação composição, fornece a função identidade. Para a tesselação $\{p, q\}$, com apenas um ciclo de vértices, como por exemplo, as auto-duais e, fixado o emparelhamento diametralmente oposto, este conjunto de relações é dado da seguinte forma:

$$T_1 \circ T_2^{-1} \circ \ldots \circ T_{\frac{p}{2}-1} \circ T_{\frac{p}{2}}^{-1} \circ T_1^{-1} \circ T_2 \circ \ldots \circ T_{\frac{p}{2}-1}^{-1} \circ T_{\frac{p}{2}},$$

  onde $\circ$ é a operação composição. Assim, considerando as matrizes obtidas nas Etapas 3, 5 e 6, devemos verificar se

$$A_{\frac{p}{2}} A_{\frac{p}{2}-1}^{-1} \ldots A_2 A_1^{-1} A_{\frac{p}{2}}^{-1} A_{\frac{p}{2}-1} \ldots A_2^{-1} A_1 = id,$$

  onde $id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é a matriz identidade de ordem 2 e considerando a multiplicação usual de matrizes.

- **[Etapa 9 - Definir a função f como matriz e computar sua inversa f^{-1} como matriz]**
  A função $f : \mathbb{H}^2 \to \mathbb{D}^2$ dada por

$$f(z) = \frac{zi + 1}{z + i}$$

  nos permite passar as transformações obtidas em $\mathbb{H}^2$ para $\mathbb{D}^2$ e vice-versa. Sendo assim, definimos:

$$F = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}$$

  e calculamos sua inversa F^{-1}, pois $F \in M(2, \mathbb{C})$.

- **[Etapa 10 - Computar matrizes G_i's, com $i = 1, \ldots, \frac{p}{2}$]**
  As matrizes obtidas nas Etapas 3 e 5 associadas às transformações de emparelhamentos T_i's, para $i = 1, \ldots, \frac{p}{2}$, nos fornecem um conjunto de geradores para o grupo fuchsiano Γ_p em $\mathbb{D}^2$, porém os geradores que aparecem na forma (3.7) para um grupo fuchsiano Γ estão em $\mathbb{H}^2$. Utilizando a função f e sua inversa, obtidas na Etapa 9, podemos levar os geradores de Γ_p em $\mathbb{D}^2$ nos geradores de Γ em $\mathbb{H}^2$ tal que $\Gamma_p \simeq \Gamma$. Este isomorfismo é dado da seguinte forma:

$$\phi(T) = f^{-1} \circ T \circ f,$$

  onde $\circ$ é a operação composição e $\phi : \mathbb{D}^2 \to \mathbb{H}^2$. Assim, para $i = 1, \ldots, \frac{p}{2}$ calculamos:

$$G_i = F A_i F^{-1},$$

  com a operação usual de matrizes.

- **[Etapa 11 - Saída]**

Para exemplificar o algoritmo proposto nesta seção, inicialmente apresentamos nas Seções 3.3, 3.4 e 3.5, as construções de tesselações hiperbólicas que satisfazem a condição de gerar superfícies de gênero $g \geq 2$. Assim, em cada uma destas seções exemplos da utilização deste algoritmo para a obtenção dos geradores de grupos fuchsianos aritméticos são apresentados. Além disso, na Subseção 4.3.4, apresentamos um exemplo em que o algoritmo é utilizado passo-a-passo na obtenção dos geradores.

3.3 Grupo Fuchsiano Aritmético $\{4g, 4g\}$

Nesta seção apresentamos construções de grupos fuchsianos aritméticos provenientes da tesselação regular auto-dual $\{4g, 4g\}$, onde $g \geq 2$, no plano hiperbólico. Estas construções buscam generalizar os resultados obtidos em [13] e [53] utilizando o resultado estabelecido no Teorema 3.1.3.

Para estas construções o modelo de espaço hiperbólico a ser usado será o disco de Poincaré, $\mathbb{D}^2$, pelo fato destas tesselações serem apresentadas geometricamente em $\mathbb{D}^2$. Seja $\mathcal{P}_{4g}$ o polígono hiperbólico regular de $4g$ arestas associado a tesselação $\{4g, 4g\}$, onde $g \geq 2$. Sem perda de generalidade, vamos supor que $\mathcal{P}_{4g}$ esteja centrado na origem de $\mathbb{D}^2$. O polígono $\mathcal{P}_{4g}$ tessela o plano hiperbólico $\mathbb{D}^2$, de modo que cada vértice é compartilhado por $4g$ polígonos de mesma forma.

A seguir, veremos duas formas de emparelhamento das arestas para o polígono $\mathcal{P}_{4g}$, as quais denominamos, respectivamente, *emparelhamento normal* e *emparelhamento diametralmente oposto* das arestas de $\mathcal{P}_{4g}$. A partir destes emparelhamentos e, através dos Teoremas 3.3.2 e 3.3.3 , obtemos o grupo fuchsiano aritmético associado. Neste trabalho, Γ_{4g} é usado para indicar o grupo fuchsiano obtido através do emparelhamento normal e Γ_{4g}^* é usado para indicar o grupo fuchsiano obtido através do emparelhamento diametralmente oposto. Estes dois emparelhamentos também serão utilizados na Seção 4.1 para exemplificar que, fixado o gênero g, dois grupos fuchsianos aritméticos provenientes de emparelhamentos diferentes são isomorfos. Escolhemos apresentar estes dois emparelhamentos pelo fato de o primeiro, emparelhamento normal, ser o mais utilizado e ter uma baixa complexidade computacional e, pelo segundo, emparelhamento diametralmente oposto, ser o mais desejado na construção de códigos quânticos topológicos como já citamos no início deste capítulo, o que pode ser visto em [2].

3.3.1 Grupo Fuchsiano Γ_{4g} via Emparelhamento Normal

Para determinar o grupo fuchsiano Γ_{4g} associado a tesselação $\{4g, 4g\}$ onde $g \geq 2$, utilizando o emparelhamento normal das arestas, consideremos as arestas de P_{4g} dispostas na seguinte ordem cíclica fixa no sentido anti-horário

$$u_1, u_2, u_1^{'}, u_2^{'}, \ldots, u_i, u_{i+1}, u_i^{'}, u_{i+1}^{'}, \ldots, u_{2g-1}, u_{2g}, u_{2g-1}^{'}, u_{2g}^{'} \tag{3.10}$$

e as isometrias $T_1, T_2, \ldots, T_{2g}$ tais que

$$T_i(u_i) = u_i^{'}, \quad \text{onde} \quad i = 1, \ldots, 2g. \tag{3.11}$$

Na Figura 3.2, apresentamos um exemplo deste tipo de emparelhamento considerando $g = 2$, ou seja, para a tesselação $\{8, 8\}$.

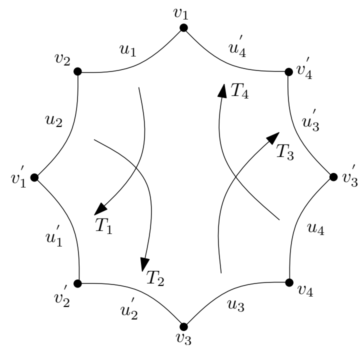

Figura 3.2: $\mathcal{P}_8$-*emparelhamento normal*

Através desses emparelhamentos, obtemos uma superfície compacta e orientável $\mathbb{D}^2/\Gamma_{4g}$ de gênero g. Consideremos agora, T_C como sendo uma transformação elíptica de ordem $4g$ cuja matriz associada é

$$C = \begin{pmatrix} e^{\frac{i\pi}{4g}} & 0 \\ 0 & e^{-\frac{i\pi}{4g}} \end{pmatrix}, \tag{3.12}$$

e tal que

$$T_C(u_1) = u_2 \quad \text{e} \quad T_{C^{r_i}}(u_1) \in \{u_i, u_i', \text{ onde } i = 1, \ldots, 2g\}, \tag{3.13}$$

onde r_i é a potência de T_C.

Sejam A_i as matrizes correspondentes às transformações T_i, com $i = 1, \ldots, 2g$. Assim, segue de (3.11) e (3.13), que

$$\begin{cases} A_i = C^{4j+1} A_1 C^{-(4j+1)}, & i \text{ par e } j = 0, \ldots, g-1; \\ A_i = C^{4k} A_1 C^{-4k}, & i \text{ ímpar e } k = 1, \ldots, g-1. \end{cases}, \quad \text{onde} \quad i = 2, 3, \ldots, 2g \tag{3.14}$$

Logo, uma vez obtido T_1, as outras transformações são obtidos por conjugações elípticas. O teorema abaixo mostra a forma da transformação T_1.

Teorema 3.3.1 *[13] Seja $\mathcal{P}_{4g}$ o polígono hiperbólico regular de $4g$ arestas, cujo grupo fuchsiano associado é Γ_{4g}. Se u_1 é a aresta entre os argumentos $-\frac{\pi}{2}$ e $-\frac{(g-1)\pi}{2g}$ e T_1 a transformação hiperbólica que emparelha as arestas u_1 e u_1' do polígono $\mathcal{P}_{4g}$, então $T_1(z) = \frac{az+b}{\bar{b}z+\bar{a}}$, onde a e b são dados por*

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

e

$$arg(b) = \frac{-(2g+1)\pi}{4g}, \ |b| = \left(\left(tg\frac{(2g-1)\pi}{4g}\right)^2 - 1\right)^{\frac{1}{2}}.$$

As demais transformações hiperbólicas $T_i(u_i) = u_i'$, onde $i = 2, \ldots, 2g$, geradoras do grupo fuchsiano Γ_{4g} e que realizam os outros emparelhamentos de arestas, são obtidas pelas conjugações $T_i = T_{C^{r_i}} \circ T_1 \circ T_{C^{-r_i}}$, onde r_i é a potência de T_C.

Através deste procedimento de determinação dos geradores do grupo fuchsiano Γ_{4g} utilizando o emparelhamento normal, determinamos sua estrutura algébrica através da seguinte representação

$$\Gamma_{4g} = \langle T_1, \ldots, T_{2g} \ : \ T_1 \circ T_2 \circ T_1^{-1} \circ T_2^{-1} \circ \ldots \circ T_i \circ T_{i+1} \circ T_i^{-1} \circ T_{i+1}^{-1} \circ \ldots \circ T_{2g-1} \circ T_{2g} \circ T_{2g-1}^{-1} \circ T_{2g}^{-1} = id \rangle.$$

3.3.2 Grupo Fuchsiano Γ^*_{4g} via Emparelhamento Diametralmente Oposto

Agora, determinamos o grupo fuchsiano, que neste trabalho será denotado por Γ^*_{4g}, associado a tesselação $\{4g, 4g\}$, onde $g \geq 2$, utilizando o emparelhamento diametralmente oposto das arestas. Assim, consideremos

$$u_1, u_2, \ldots, u_{4g-1}, u_{4g}$$

as arestas de $\mathcal{P}_{4g}$ dispostas em ordem cíclica fixa no sentido anti-horário e as isometrias para este emparelhamento $T^*_1, T^*_2, \ldots, T^*_{2g}$ tais que

$$T^*_i(u_i) = u_{i+2g}, \quad \text{onde} \ \ i = 1, \ldots, 2g. \tag{3.15}$$

Na Figura 3.3, apresentamos este tipo de emparelhamento para a tesselação $\{8, 8\}$, ou seja, para a tesselação $\{4g, 4g\}$ e $g = 2$.

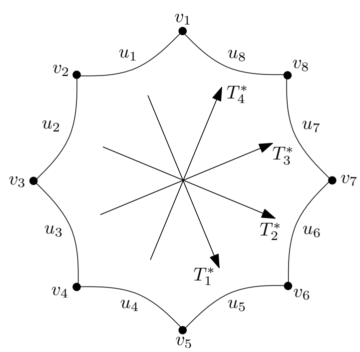

Figura 3.3: $\mathcal{P}_8$-*emparelhamento diametralmente oposto*

Por meio desses emparelhamentos, obtemos uma superfície compacta e orientável $\mathbb{D}^2/\Gamma^*_{4g}$ de gênero g. Da mesma forma como na seção anterior, consideremos T_C uma transformação elíptica de ordem $4g$ com a matriz associada dada em (3.12) tal que

$$T^*_C(u_1) = u_{2g+1} \quad \text{e} \quad T^*_{C^{r_i}}(u_1) \in \{u_i, \ i = 2, \ldots, 4g\}, \tag{3.16}$$

onde r_i é a potência de T^*_C. Assim, conhecendo a transformação T^*_1 podemos escrever as demais transformações como conjugações de T^*_1 por meio de potências de C. Como a transformação T^*_1 emparelha a aresta u_1 com a sua diametralmente oposta u_{2g+1}, segue que a sua matriz associada A^*_1 é dada por (3.4).

Agora, sejam A^*_i as matrizes correspondentes às transformações T^*_i, com $i = 2, \ldots, 2g$. Assim, segue de (3.15) e (3.16), que

$$A^*_i = C^{i-1} A^*_1 C^{-(i-1)}, \quad \text{onde} \ \ i = 2, \ldots, 2g. \tag{3.17}$$

Portanto, por (3.17) e pelo Teorema 3.1.1, obtem-se os geradores do grupo fuchsiano Γ_{4g}^* utilizando o emparelhamento diametralmente oposto das arestas. Assim, podemos determinar a estrutura algébrica deste grupo através da seguinte representação

$$\Gamma_{4g}^* = \langle T_1^*, \ldots, T_{2g}^* \ : \ T_1^* \circ (T_2^*)^{-1} \circ \ldots \circ T_{2g-1}^* \circ (T_{2g}^*)^{-1} \circ (T_1^*)^{-1} \circ T_2^* \circ \ldots \circ (T_{2g-1}^*)^{-1} \circ T_{2g}^* = id \rangle.$$

Através dos resultados que veremos a seguir, identificamos os grupos fuchsianos Γ_{4g} e Γ_{4g}^* com uma ordem e uma álgebra dos quatérnios afim de torná-los grupos fuchsianos aritméticos. Destacamos que estes resultados não levam em consideração o tipo de emparelhamento utilizado para obter o grupo fuchsiano. Sendo assim, nos resultados trataremos apenas de Γ_{4g} que irá simbolizar qualquer grupo fuchsiano proveniente da tesselação regular auto-dual $\{4g, 4g\}$.

Como vimos, uma condição necessária para um grupo fuchsiano ser aritmético é que satisfaça a condição de Fermat, estabelecida no Teorema 3.1.3. Em especial, para a tesselação $\{4g, 4g\}$ podemos estabelecer esta condição para o gênero g da superfície associada e não para $p = q = 4g$, uma vez que $4 = 2^2$. Assim, se g for da forma dada em (3.8), então $4g$ também será.

Nestas condições, tem-se os seguintes resultados:

Teorema 3.3.2 *Se g é como em* (3.8), *onde $g \geq 2$ é o gênero da superfície associada à tesselação $\{4g, 4g\}$, então os elementos do grupo fuchsiano $\Gamma \simeq \Gamma_{4g}$ são identificados, via isomorfismo, com os elementos do grupo dos invertíveis $\mathcal{O}^1$ da ordem $\mathcal{O} = (\theta, -1)_R$ ou $\mathcal{O} = (\theta_1, -1)_R$, onde $R = \mathcal{I}_{\mathbb{K}}$ é o anel dos inteiros do corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$, $\theta_1 \in \mathbb{K}$ e θ ou θ_1 dependendo do gênero g. Consequentemente, $\{1, \sqrt{\theta}, Im, \sqrt{\theta}Im\}$ é uma R-base para o reticulado $\mathcal{O}$, sendo Im a unidade imaginária.*

Demonstração: Faremos a demostração considerando o caso da ordem dos quatérnios obtida ser $\mathcal{O} = (\theta, -1)_R$, pois como $\theta_1 \in \mathbb{K} = \mathbb{Q}(\theta)$ segue que $\theta_1 = a + b\theta$, onde $a, b \in \mathbb{Q}$, e a demostração seguiria de modo análogo. Assim, fixado um gênero g e o elemento θ correspondente, podemos obter a seguinte ordem dos quatérnios

$$\mathcal{O} = (\theta, -1)_R = \{x = x_0 + x_1 i + x_2 j + x_3 k; x_0, x_1, x_2, x_3 \in R\},$$

onde $R = \mathcal{I}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\theta)$. Tem-se que $\mathcal{O}$ é uma ordem na álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, tal que

$$i^2 = \theta, \quad j^2 = -1 \ \text{ e } \ k = ij = -ji.$$

Seja $\mathcal{O}^1 = \{x \in \mathcal{O} : Nrd(x) = 1\}$, o conjunto dos elementos invertíveis de $\mathcal{O}$. Consideremos as seguintes matrizes M_0, M_1, M_2 e M_3 em $M(2, \mathbb{Q}(\sqrt{\theta}))$, dadas por

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix}, M_2 = \begin{pmatrix} 0 & 1 \\ \beta & 0 \end{pmatrix}, M_3 = \begin{pmatrix} 0 & \sqrt{\alpha} \\ -\beta\sqrt{\alpha} & 0 \end{pmatrix}.$$

De modo análogo à construção do isomorfismo dado em (2.8), consideremos φ uma aplicação da álgebra $\mathcal{A} = (\theta, -1)_{\mathbb{Q}(\theta)}$ em $M(2, \mathbb{Q}(\sqrt{\theta}))$, definida por

$$\varphi(x_0 + x_1 i + x_2 j + x_3 k) = x_0 M_0 + x_1 M_1 + x_2 M_2 + x_3 M_3. \tag{3.18}$$

Dessa forma, cada elemento de $\mathcal{A} = (\theta, -1)_{\mathbb{Q}(\theta)}$ é identificado com

$$x \longmapsto \varphi(x) = \begin{pmatrix} x_0 + x_1\sqrt{\theta} & x_2 + x_3\sqrt{\theta} \\ -x_2 + x_3\sqrt{\theta} & x_0 - x_1\sqrt{\theta} \end{pmatrix}.$$

Para $\Gamma \simeq \Gamma_{4g}$, segue que seus geradores são como em (3.7). Assim, considerando as operações da ordem $\mathcal{O}$ no anel R, se $T \in \Gamma_{4g}$, então pelo Lema 3.1.1, segue que

$$T = \frac{1}{2^s}\begin{pmatrix} x_k + y_k\sqrt{\theta} & z_k + w_k\sqrt{\theta} \\ -z_k + w_k\sqrt{\theta} & x_k - y_k\sqrt{\theta} \end{pmatrix},$$

onde $s \in \mathbb{N}$ e $x_k, y_k, z_k, w_k \in \mathbb{Z}[\theta]$. Logo, T é identificado com o elemento

$$x = \frac{x_k}{2^s} + \frac{y_k}{2^s}i + \frac{z_k}{2^s}j + \frac{w_k}{2^s}k,$$

onde $x \in \mathcal{O}^1 \subset \mathcal{O} = (\theta, -1)_R$, através do isomorfismo $\varphi : \mathcal{A} \to \varphi(\mathcal{A})$, definido em (3.18), ou seja, $\varphi(x) = T$, com $i^2 = \theta,\ j^2 = -1,\ k = ij$ e $x_k, y_k, z_k, w_k \in \mathbb{Z}[\theta]$. Portanto, cada elemento do grupo fuchsiano $\Gamma \simeq \Gamma_{4g}$ é identificado, via o isomorfismo φ, com um elemento $x \in \mathcal{O}^1 \subset \mathcal{O} = (\theta, -1)_R$ e $\{1, i, j, k\} = \{1, \sqrt{\theta}, Im, \sqrt{\theta}Im\}$ é uma R-base de $\mathcal{O}$. ∎

Teorema 3.3.3 *Se g é como em (3.8), onde $g \geq 2$ é o gênero da superfície associada à tesselação $\{4g, 4g\}$, então o grupo fuchsiano $\Gamma \simeq \Gamma_{4g}$, associado ao polígono hiperbólico regular $\mathcal{P}_{4g}$, é derivado de uma álgebra de divisão dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ ou $\mathcal{A} = (\theta_1, -1)_{\mathbb{K}}$ sobre o corpo de números totalmente real $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta_1 \in \mathbb{K}$ e θ ou θ_1 depende do gênero g.*

Demonstração: Da mesma forma como no Teorema 3.3.2, faremos a demonstração considerando a álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$. Assim, fixado um gênero g e o elemento θ correspondente, consideremos $T \in \Gamma \simeq \Gamma_{4g}$. Pelo Lema 3.1.1, segue que podemos escrever T da seguinte forma:

$$T = \frac{1}{2^s}\begin{pmatrix} x_k + y_k\sqrt{\theta} & z_k + w_k\sqrt{\theta} \\ -z_k + w_k\sqrt{\theta} & x_k - y_k\sqrt{\theta} \end{pmatrix},$$

onde $s \in \mathbb{N}$ e $x_k, y_k, z_k, w_k \in \mathbb{Z}[\theta]$. Logo, vimos no Teorema 3.3.2 que existe $x \in \mathcal{O}^1 \subset \mathcal{O} = (\theta, -1)_R$, da forma

$$x = \frac{x_k}{2^s} + \frac{y_k}{2^s}i + \frac{z_k}{2^s}j + \frac{w_k}{2^s}k,$$

tal que $\varphi(x) = T$, onde φ é como definida como no Teorema 3.3.2. Assim,

$$tr(T) = tr(\varphi(x)) = Trd(x) = \frac{2x_k}{2^s} \in R,$$

sendo $R = \mathcal{I}_{\mathbb{K}}$. Como $T \in \Gamma$, segue que $tr(T) \in \mathcal{I}_{\mathbb{K}}$, para todo $T \in \Gamma$, ou seja, $\{tr(T) : T \in \Gamma\} \subset \mathcal{I}_{\mathbb{K}}$. Por outro lado, tem-se que

$$\mathbb{K} = \mathbb{Q}(tr(T) : T \in \Gamma) = \mathbb{Q}(\theta).$$

Disto segue a primeira condição do Teorema 2.3.4. Agora, se $\phi : \mathbb{K} \to \mathbb{R}$ é dada por $\phi(\theta) = -\theta$, então ϕ é um homomorfismo e podemos estendê-lo ao isomorfismo $\psi : \mathbb{L} \to \psi(\mathbb{L})$, com $\psi(\mathbb{L}) \subset \mathbb{C}$, definido por

$$\psi(x + y\sqrt{\theta}) = \phi(x) = \phi(y)i\sqrt{\theta},\ x, y \in \mathbb{K},\ \mathbb{L} = \mathbb{K}(\sqrt{\theta}) \text{ e } [\mathbb{L} : \mathbb{K}] = 2.$$

De acordo com o Teorema 2.3.3, consideremos a álgebra dos quatérnios $\mathcal{A}[\Gamma]$ sobre $\mathbb{K}(\theta)$

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

Usando as expressões dos geradores como em (3.7), segue que

$$\mathcal{A}[\Gamma] = \left\{ \begin{pmatrix} a_1 & b_1 \\ -\bar{b_1} & \bar{a_1} \end{pmatrix} : a_1, b_1 \in \mathbb{L} \right\},$$

onde $\bar{a_1}$ e $\bar{b_1}$ são os conjugados de a_1 e b_1 em $\mathbb{L}$, respectivamente. Seja $\Psi : \mathcal{A}[\Gamma] \to M(2, \mathbb{C})$ o mergulho definido por

$$\Psi(\alpha) = \begin{pmatrix} \Psi(a_1) & \Psi(b_1) \\ \Psi(\bar{b_1}) & \Psi(\bar{a_1}) \end{pmatrix}.$$

Assim, $\mathcal{A}^{\psi} = \Psi(\mathcal{A}[\Gamma]) = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \psi(\mathbb{L}) \right\}$ e então $\mathcal{A}^{\psi} \otimes \mathbb{R} \simeq \mathbb{H}$, [30]. Por outro lado, se T é um elemento de Γ e $tr(T) = a + \bar{a}$, então usando o mesmo raciocínio do Exemplo 2.2.1, segue que

$$\phi(a) + \phi(\bar{a}) = \phi(a + \bar{a}) \in [-2, 2].$$

Logo, $\phi(tr(\Gamma))$ é limitado em $\mathbb{R}$. Mas como $a + \bar{a} \in \mathbb{K} = \mathbb{Q}(\theta)$, segue que $\phi(a + \bar{a}) = \psi(a + \bar{a})$, ou seja,

$$\psi(a + \bar{a}) \in [-2, 2].$$

Portanto, $\psi(tr(\Gamma))$ é limitado em $\mathbb{C}$, satisfazendo a segunda condição do Teorema 2.3.4. Concluímos então que $\Gamma \simeq \Gamma_{4g}$ é derivado de uma álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ sobre o corpo de números totalmente real $\mathbb{K} = \mathbb{Q}(tr(T) : T \in \Gamma) = \mathbb{Q}(\theta)$, onde θ depende do gênero g da superfície associada. ∎

Vimos que os geradores G_l de $\Gamma \simeq \Gamma_{4g}$, com $l = 1, \ldots, 2g$, podem ser escritos da seguinte forma

$$G_l = \frac{1}{2^s} \begin{pmatrix} x_k + y_k\sqrt{\theta} & z_k + w_k\sqrt{\theta} \\ -z_k + w_k\sqrt{\theta} & x_k - y_k\sqrt{\theta} \end{pmatrix}, \quad \text{onde} \quad k = 1, \ldots, l,$$

onde $G_l \in M(2, \mathbb{K}(\sqrt{\theta}))$, $s \in \mathbb{N}$, $\theta, x_k, y_k, z_k, w_k \in \mathbb{Z}[\theta] \subseteq \mathcal{I}_{\mathbb{K}}$, $\mathbb{K} = \mathbb{Q}(\theta)$ e θ dependendo do gênero g da superfície. Pelos Teoremas 3.3.2 e 3.3.3, este elemento θ será o mesmo proveniente da álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ e da ordem dos quatérnios $\mathcal{O} = (\theta, -1)_R$ associada.

Para sabermos o grau $[\mathbb{K} : \mathbb{Q}]$ da extensão $\mathbb{K}|\mathbb{Q}$, devemos conhecer o valor de θ, que como vimos, depende do gênero g da superfície.

Utilizando o algoritmo proposto na Seção 3.2 obtemos diversos valores de θ para os quais são possíveis obter os grupos fuchsianos aritméticos provenientes da tesselação $\{4g, 4g\}$. Abaixo, discriminamos os valores de θ obtidos e mais adiante explicitaremos alguns deles através de exemplos.

$$\theta = \begin{cases} \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}} & \text{, contendo } n \text{ radicais, para } g = 2^n; \\ \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}} & \text{, contendo } n+1 \text{ radicais, para } g = 3\cdot 2^n,\ n \geq 1; \\ \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}} & \text{, contendo } n+2 \text{ radicais, para } g = 5\cdot 2^n; \\ \sqrt{2+\sqrt{2+\ldots+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}} & \text{, contendo } n+3 \text{ radicais, para } g = 3\cdot 5\cdot 2^n. \end{cases} \tag{3.19}$$

Dessa forma, para estes valores de θ, temos os seguintes diagramas para determinar o grau das extensões correspondentes:

$$2^n \left[\begin{array}{l} \mathbb{Q}(\theta) \\ \vdots n-2 \\ \mathbb{Q}(\sqrt{2+\sqrt{2}}) \\ |2 \\ \mathbb{Q}(\sqrt{2}) \\ |2 \\ \mathbb{Q} \end{array} \right. \quad 2^{n+1} \left[\begin{array}{l} \mathbb{Q}(\theta) \\ \vdots n-1 \\ \mathbb{Q}(\sqrt{2+\sqrt{3}}) \\ |2 \\ \mathbb{Q}(\sqrt{3}) \\ |2 \\ \mathbb{Q} \end{array} \right. \quad 2^{n+2} \left[\begin{array}{l} \mathbb{Q}(\theta) \\ \vdots n-1 \\ \mathbb{Q}\left(\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}\right) \\ |2 \\ \mathbb{Q}\left(\sqrt{10+2\sqrt{5}}\right) \\ |2 \\ \mathbb{Q}(\sqrt{5}) \\ |2 \\ \mathbb{Q} \end{array} \right. \quad 2^{n+3} \left[\begin{array}{l} \mathbb{Q}(\theta) \\ \vdots n-1 \\ \mathbb{Q}\left(\sqrt{2+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}\right) \\ |2 \\ \mathbb{Q}\left(\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}\right) \\ |2 \\ \mathbb{Q}\left(\sqrt{30+6\sqrt{5}}\right) \\ |2 \\ \mathbb{Q}(\sqrt{5}) \\ |2 \\ \mathbb{Q} \end{array} \right.$$

Logo,

$$[\mathbb{K}:\mathbb{Q}] = \begin{cases} 2^n & , \quad \text{se } g = 2^n \\ 2^{n+1} & , \quad \text{se } g = 3\cdot 2^n,\ n \geq 1 \\ 2^{n+2} & , \quad \text{se } g = 5\cdot 2^n \\ 2^{n+3} & , \quad \text{se } g = 3\cdot 5\cdot 2^n. \end{cases}$$

A seguir, apresentamos um exemplo dos resultados apresentados nos Teoremas 3.3.2 e 3.3.3, para o caso $g = 5$, ou seja, para a tesselação $\{20, 20\}$.

Exemplo 3.3.1 *Seja $\mathcal{P}_{20}$ o polígono hiperbólico regular associado à tesselação $\{20, 20\}$. Vamos considerar o emparelhamento diametralmente oposto das arestas de $\mathcal{P}_{20}$. Utilizando o algoritmo proposto na Seção 3.2, obtemos os seguintes geradores para o grupo fuchsiano aritmético Γ_{20}^*:*

$$G_1^* = \frac{1}{8}\begin{pmatrix} x_1 + 4\sqrt[4]{10+2\sqrt{5}} & -w_1\sqrt[4]{10+2\sqrt{5}} \\ -w_1\sqrt[4]{10+2\sqrt{5}} & x_1 - 4\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + 4i - w_1k)\ ,$$

$$G_2^* = \frac{1}{8}\begin{pmatrix} x_1 + y_1\sqrt[4]{10+2\sqrt{5}} & -w_2\sqrt[4]{10+2\sqrt{5}} \\ -w_2\sqrt[4]{10+2\sqrt{5}} & x_1 - y_1\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + y_1 i - w_2k)\ ,$$

$$G_3^* = \frac{1}{8}\begin{pmatrix} x_1 + y_2\sqrt[4]{10+2\sqrt{5}} & -y_2\sqrt[4]{10+2\sqrt{5}} \\ -y_2\sqrt[4]{10+2\sqrt{5}} & x_1 - y_2\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + y_2 i - y_2 k) \ ,$$

$$G_4^* = \frac{1}{8}\begin{pmatrix} x_1 + w_2\sqrt[4]{10+2\sqrt{5}} & -y_1\sqrt[4]{10+2\sqrt{5}} \\ -y_1\sqrt[4]{10+2\sqrt{5}} & x_1 - w_2\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + w_2 i - y_1 k) \ ,$$

$$G_5^* = \frac{1}{8}\begin{pmatrix} x_1 + w_1\sqrt[4]{10+2\sqrt{5}} & -4\sqrt[4]{10+2\sqrt{5}} \\ -4\sqrt[4]{10+2\sqrt{5}} & x_1 - w_1\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + w_1 i - 4k) \ ,$$

$$G_6^* = \frac{1}{8}\begin{pmatrix} x_1 + w_1\sqrt[4]{10+2\sqrt{5}} & 4\sqrt[4]{10+2\sqrt{5}} \\ 4\sqrt[4]{10+2\sqrt{5}} & x_1 - w_1\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + w_1 i + 4k) \ ,$$

$$G_7^* = \frac{1}{8}\begin{pmatrix} x_1 + w_2\sqrt[4]{10+2\sqrt{5}} & y_1\sqrt[4]{10+2\sqrt{5}} \\ y_1\sqrt[4]{10+2\sqrt{5}} & x_1 - w_2\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + w_2 i + y_1 k) \ ,$$

$$G_8^* = \frac{1}{8}\begin{pmatrix} x_1 + y_2\sqrt[4]{10+2\sqrt{5}} & y_2\sqrt[4]{10+2\sqrt{5}} \\ y_2\sqrt[4]{10+2\sqrt{5}} & x_1 - y_2\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + y_2 i + y_2 k) \ ,$$

$$G_9^* = \frac{1}{8}\begin{pmatrix} x_1 + y_1\sqrt[4]{10+2\sqrt{5}} & w_2\sqrt[4]{10+2\sqrt{5}} \\ w_2\sqrt[4]{10+2\sqrt{5}} & x_1 - y_1\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + y_1 i + w_2 k) \ ,$$

$$G_{10}^* = \frac{1}{8}\begin{pmatrix} x_1 + 4\sqrt[4]{10+2\sqrt{5}} & w_1\sqrt[4]{10+2\sqrt{5}} \\ w_1\sqrt[4]{10+2\sqrt{5}} & x_1 - 4\sqrt[4]{10+2\sqrt{5}} \end{pmatrix} = \frac{1}{8}\varphi(x_1 + 4i + w_1 k) \ ,$$

onde

$$\begin{aligned}
x_1 &= 8 + 8\sqrt{5} + 2(1+\sqrt{5})\sqrt{10+2\sqrt{5}},\\
y_1 &= 4 + 2\sqrt{10+2\sqrt{5}},\\
w_1 &= 4 + 4\sqrt{5} + (1+\sqrt{5})\sqrt{10+2\sqrt{5}},\\
y_2 &= 6 + 2\sqrt{5} + 2(1+\sqrt{5})\sqrt{10+2\sqrt{5}} \quad e\\
w_2 &= 6 + 2\sqrt{5} + (1+\sqrt{5})\sqrt{10+2\sqrt{5}}.
\end{aligned}$$

Assim, de acordo com os Teoremas 3.3.2 e 3.3.3, segue que a ordem dos quatérnios associada com o grupo fuchsiano Γ_{20}^* derivado da álgebra dos quatérnios $\mathcal{A} = (\sqrt{10+2\sqrt{5}}, -1)_{\mathbb{K}}$, é $\mathcal{O} = (\sqrt{10+2\sqrt{5}}, -1)_R$, onde $R = \mathbb{Z}[\sqrt{10+2\sqrt{5}}]$, $\mathbb{K} = \mathbb{Q}(\sqrt{10+2\sqrt{5}})$ e $[\mathbb{K} : \mathbb{Q}] = 4$.

Observe que para o caso da expansão $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2+\sqrt{3}}}}$, em (3.19), consideramos $n \geq 1$. Para o caso de $n = 0$, ou seja, $g = 3$ e a tesselação $\{12, 12\}$, segue do Exemplo 3.3.2 abaixo, que a ordem dos quatérnios associada ao grupo fuchsiano aritmético Γ_{12} é do tipo $\mathcal{O} = (\theta_1, -1)_R$, e este grupo é derivado de uma álgebra dos quatérnios do tipo $\mathcal{A} = (\theta_1, -1)_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\theta)$, $R = \mathbb{Z}[\theta]$ e $\theta_1 \in \mathbb{K} = \mathbb{Q}(\theta)$.

Exemplo 3.3.2 *Seja $\mathcal{P}_{12}$ o polígono hiperbólico regular associado à tesselação $\{12, 12\}$. Consideremos agora o emparelhamento normal das arestas de $\mathcal{P}_{12}$. Utilizando o algoritmo proposto na Seção 3.2, obtemos os seguintes geradores para o grupo fuchsiano aritmético Γ_{12}:*

$$G_1 = \frac{1}{2}\begin{pmatrix} -x_1 + y_1\sqrt[4]{3+2\sqrt{3}} & z_1 + w_1\sqrt[4]{3+2\sqrt{3}} \\ -z_1 + w_1\sqrt[4]{3+2\sqrt{3}} & -x_1 - y_1\sqrt[4]{3+2\sqrt{3}} \end{pmatrix} = \frac{1}{2}\varphi(-x_1 + y_1 i + z_1 j + w_1 k)\ ,$$

$$G_2 = \frac{1}{2}\begin{pmatrix} x_1 - w_1\sqrt[4]{3+2\sqrt{3}} & z_1 + y_1\sqrt[4]{3+2\sqrt{3}} \\ -z_1 + y_1\sqrt[4]{3+2\sqrt{3}} & x_1 + w_1\sqrt[4]{3+2\sqrt{3}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - w_1 i + z_1 j + y_1 k)\ ,$$

$$G_3 = \frac{1}{2}\begin{pmatrix} x_1 + w_1\sqrt[4]{3+2\sqrt{3}} & z_1 - w_1\sqrt[4]{3+2\sqrt{3}} \\ -z_1 - w_1\sqrt[4]{3+2\sqrt{3}} & x_1 - w_1\sqrt[4]{3+2\sqrt{3}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + w_1 i + z_1 j - w_1 k)\ ,$$

$$G_4 = \frac{1}{2}\begin{pmatrix} x_1 + y_1\sqrt[4]{3+2\sqrt{3}} & z_1 + w_1\sqrt[4]{3+2\sqrt{3}} \\ -z_1 + w_1\sqrt[4]{3+2\sqrt{3}} & x_1 - y_1\sqrt[4]{3+2\sqrt{3}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + y_1 i + z_1 j + w_1 k)\ ,$$

$$G_5 = \frac{1}{2}\begin{pmatrix} x_1 + y_1\sqrt[4]{3+2\sqrt{3}} & z_1 - y_1\sqrt[4]{3+2\sqrt{3}} \\ -z_1 - y_1\sqrt[4]{3+2\sqrt{3}} & x_1 - y_1\sqrt[4]{3+2\sqrt{3}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + y_1 i + z_1 j - y_1 k)\ ,$$

$$G_6 = \frac{1}{2}\begin{pmatrix} x_1 - y_1\sqrt[4]{3+2\sqrt{3}} & z_1 - w_1\sqrt[4]{3+2\sqrt{3}} \\ -z_1 - w_1\sqrt[4]{3+2\sqrt{3}} & x_1 + y_1\sqrt[4]{3+2\sqrt{3}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - y_1 i + z_1 j - w_1 k)\ ,$$

onde $x_1 = -2-\sqrt{3}$, $y_1 = 1+\sqrt{3}$, $z_1 = 3+2\sqrt{3}$ *e* $w_1 = -1+\sqrt{3}$. *Como* $x_1, y_1, z_1, w_1 \in \mathbb{Z}[\sqrt{3}]$, *de acordo com os Teoremas 3.3.2 e 3.3.3, segue que a ordem dos quatérnios associada com o grupo fuchsiano* Γ_{12} *derivado da álgebra dos quatérnios* $\mathcal{A} = (\sqrt{3+2\sqrt{3}}, -1)_{\mathbb{K}}$, *é* $\mathcal{O} = (\sqrt{3+2\sqrt{3}}, -1)_R$, *onde* $R = \mathbb{Z}[\sqrt{3}]$, $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, $\sqrt{3+2\sqrt{3}} \in \mathbb{Q}(\sqrt{3})$ *e* $[\mathbb{K} : \mathbb{Q}] = 2$.

3.4 Grupo Fuchsiano Aritmético $\{4g+2, 2g+1\}$

Consideremos agora a tesselação regular $\{4g+2, 2g+1\}$, ou seja, os polígonos desta tesselação contêm $4g+2$ lados e cada vértice é o encontro de $2g+1$ desses polígonos. Esta tesselação gera superfícies de gênero g e para cada g, podemos obter o grupo fuchsiano Γ_{4g+2} associado através da identificação das arestas de um polígono regular $\mathcal{P}_{4g+2}$, de $4g+2$ arestas em $\mathbb{D}^2$.

Por outro lado, o grupo fuchsiano aritmético nem sempre pode ser obtido para qualquer gênero g desta tesselação, pois não temos muitos valores de g tais que $p = 4g+2$ e $q = 2g+1$ satisfaçam a condição de Fermat (Teorema 3.1.3). Os casos $g = 2$, tesselação $\{10, 5\}$, e $g = 7$, tesselação $\{30, 15\}$, serão os casos tratados neste trabalho para exemplificar tais tesselações. Observamos que para $2 < g < 7$ não temos nenhum valor de g que satisfaça a condição de Fermat. De fato, para estes valores temos as seguintes tesselações: $\{14, 7\}$, $\{18, 9\}$, $\{22, 11\}$ e $\{26, 13\}$, para $g = 3, 4, 5$ e 6, respectivamente, cujos valores de p e q de cada uma destas tesselações não podem ser decompostos como potências de 2 ou potências de 2 e números distintos de Fermat.

Construimos dois grupos fuchsianos obtidos através de dois emparelhamentos diferentes, sendo que um deles é o emparelhamento diametralmente oposto que como vimos é o caminho homologicamente não trivial com a maior distância mínima possível. Neste trabalho, Γ^*_{4g+2} é usado para indicar o grupo fuchsiano obtido através do emparelhamento diametralmente oposto e $\Gamma^{\bullet}_{4g+2}$ é usado para indicar o grupo fuchsiano obtido através de um emparelhamento diferente que será apresentado na Seção 3.4.2.

3.4.1 Grupo Fuchsiano Γ^*_{4g+2} via Emparelhamento Diametralmente Oposto

Seja $\mathcal{P}_{4g+2}$ o polígono hiperbólico regular de $4g+2$ arestas associado a tesselação $\{4g+2, 2g+1\}$, onde $g \geq 2$ é o gênero da superfície associada. Consideremos

$$u_1, u_2, \ldots, u_{4g+2} \;\; \text{e} \;\; v_1, v_2, \ldots, v_{4g+2}$$

como as arestas e os vértices de $\mathcal{P}_{4g+2}$, respectivamente, dispostos em ordem cíclica fixa no sentido anti-horário. Utilizando o emparelhamento diametralmente oposto, as isometrias $T^*_1, T^*_2, \ldots, T^*_{2g+1}$ para este emparelhamento são tais que

$$T^*_i(u_i) = u_{i+2g+1}, \;\; \text{onde} \;\; i = 1, \ldots, 2g+1. \tag{3.20}$$

Por meio destes emparelhamentos, obtemos uma superfície compacta e orientável $\mathbb{D}^2/\Gamma^*_{4g+2}$ de gênero g. Se conhecermos a transformação T^*_1 podemos escrever os outros elementos de Γ_{4g+2} como conjugações de T^*_1 por meio de potências de T^*_C, onde T^*_C é uma tranformação elíptica de ordem $4g+2$ com matriz associada

$$C = \begin{pmatrix} e^{\frac{i\pi}{4g+2}} & 0 \\ 0 & e^{-\frac{i\pi}{4g+2}} \end{pmatrix}, \tag{3.21}$$

tal que

$$T^*_C(u_1) = u_{2g+2} \quad \text{e} \quad T^*_{C^{r_i}}(u_1) \in \{u_i, \;\; \text{onde} \;\; i = 2, \ldots, 4g+2\}, \tag{3.22}$$

onde r_i é a potência de T^*_C. Como a transformação T^*_1 emparelha a aresta u_1 com a sua diametralmente oposta u_{2g+2}, segue que a sua matriz associada A^*_1 é dada por (3.4).

Agora, sejam A^*_i as matrizes correspondentes às transformações T^*_i, com $i = 2, \ldots, 2g+1$. Assim, segue de (3.20) e (3.22) que

$$A^*_i = C^{i-1} A^*_1 C^{-(i-1)}, \;\; \text{onde} \;\; i = 2, \ldots, 2g+1. \tag{3.23}$$

Portanto, por (3.17) e pelo Teorema 3.1.1, obtemos os geradores do grupo fuchsiano Γ^*_{4g+2} utilizando o emparelhamento diametralmente oposto das arestas. Para esta tesselação, por (2.6), devemos ter

$$\frac{p}{q} = \frac{4g+2}{2g+1} = 2$$

ciclos de vértices de comprimento $q = 2g+1$. Estes ciclos de vértices são dados por

$$\varepsilon_1 = \{v_1, v_3, \ldots, v_{4g+1}\} = \{v_{2i+1} | i = 0, \ldots, 2g\} \;\; \text{(vértices ímpares)}$$

e

$$\varepsilon_2 = \{v_2, v_4, \ldots, v_{4g+2}\} = \{v_{2i} | i = 1, \ldots, 2g+1\} \;\; \text{(vértices pares)}.$$

Assim, por meio do processo de construção dos ciclos ε_1 e ε_2, podemos determinar a estrutura algébrica deste grupo através da seguinte representação

$$\Gamma^*_{4g+2} = \langle T^*_1, \ldots, T^*_{2g+1} \; : \; T^*_1 \circ (T^*_2)^{-1} \circ T^*_3 \circ \ldots \circ T^*_{2g-1} \circ (T^*_{2g})^{-1} \circ (T^*_{2g+1})^{-1} = id$$

$$\text{e} \quad (T_1^*)^{-1} \circ T_2^* \circ (T_3^*)^{-1} \circ \ldots \circ (T_{2g-1}^*)^{-1} \circ T_{2g}^* \circ (T_{2g+1}^*)^{-1} = id\rangle.$$

Com o intuito de exemplificar este processo e obter além do grupo fuchsiano, também o grupo fuchsiano aritmético, vamos considerar $g = 2$, ou seja, a tesselação $\{10, 5\}$. Para o emparelhamento diametralmente oposto temos a seguinte associação das arestas:

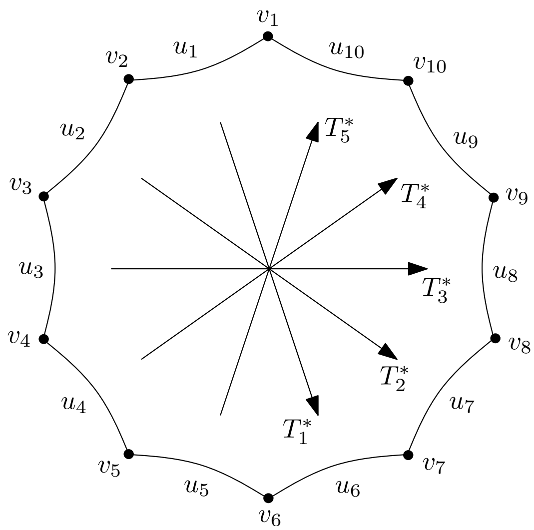

Figura 3.4: P_{10}-*emparelhamento diametralmente oposto*

Dessa forma, as isometrias para este emparelhamento são dadas por

$$T_i^*(u_i) = u_{i+5}, \quad \text{onde} \;\; i = 1, \ldots, 5. \tag{3.24}$$

Como a transformação T_1^* emparelha a aresta u_1 com sua diametralmente oposta, pelo Teorema 3.1.1, segue que

$$A_1^* = \begin{pmatrix} \frac{2\cos\frac{\pi}{5}}{2sen\frac{\pi}{10}} & \frac{\sqrt{2\cos\frac{\pi}{5}+2\cos\frac{2\pi}{5}}\cdot e^{i\frac{11\pi}{10}}}{2sen\frac{\pi}{10}} \\ \frac{\sqrt{2\cos\frac{\pi}{5}+2\cos\frac{2\pi}{5}}\cdot e^{-i\frac{11\pi}{10}}}{2sen\frac{\pi}{10}} & \frac{2\cos\frac{\pi}{5}}{2sen\frac{\pi}{10}} \end{pmatrix}, \tag{3.25}$$

e as demais matrizes correspondentes às transformações T_i^*, $i = 2, \ldots, 5$, obtidas através de conjugações da matriz A_1^*, são dadas por

$$A_i^* = C^{i-1} A_1^* C^{-(i-1)}, \quad \text{onde} \;\; i = 2, \ldots, 5. \tag{3.26}$$

Por meio desses emparelhamentos, obtemos uma superfície compacta e orientável $\mathbb{D}^2/\Gamma_{10}^*$ de gênero 2. Assim, a estrutura algébrica deste grupo fuchsiano tem a seguinte representação

$$\Gamma_{10}^* = \langle T_1^*, \ldots, T_5^* \;:\; T_1^* \circ (T_2^*)^{-1} \circ T_3^* \circ (T_4^*)^{-1} \circ T_5^* = Id \text{ e } (T_1^*)^{-1} \circ T_2^* \circ (T_3^*)^{-1} \circ T_4^* \circ (T_5^*)^{-1} = id\rangle.$$

Consideremos agora $g = 7$, ou seja, a tesselação $\{10, 5\}$, porém ainda considerando o emparelhamento diametralmente oposto das arestas, como apresentado na Figura 3.4 para a tesselação $\{10, 5\}$. As isometrias associadas ao polígono regular hiperbólico $\mathcal{P}_{30}$ são dadas por:

$$T_i^*(u_i) = u_{i+15}, \quad \text{onde} \;\; i = 1, \ldots, 15. \tag{3.27}$$

Como a transformação T_1^* emparelha a aresta u_1 com sua diametralmente oposta, pelo Teorema 3.1.1, segue que

$$A_1^* = \begin{pmatrix} \frac{\frac{2sen\frac{\pi}{15}}{2\sin\frac{\pi}{30}}}{} & \frac{\sqrt{2\cos\frac{\pi}{15}+2\cos\frac{2\pi}{15}}\cdot e^{i\frac{31\pi}{30}}}{2sen\frac{\pi}{30}} \\ \frac{\sqrt{2\cos\frac{\pi}{15}+2\cos\frac{2\pi}{15}}\cdot e^{-i\frac{31\pi}{30}}}{2sen\frac{\pi}{30}} & \frac{2\cos\frac{\pi}{15}}{2sen\frac{\pi}{30}} \end{pmatrix}, \tag{3.28}$$

e as demais matrizes correspondentes as transformações T_i^*, onde $i = 2, \ldots, 15$, obtidas através de conjugações da matriz A_1^*, são dadas por

$$A_i^* = C^{i-1} A_1^* C^{-(i-1)}, \quad \text{onde} \quad i = 2, \ldots, 15. \tag{3.29}$$

Por meio desses emparelhamentos, obtemos uma superfície compacta e orientável $\mathbb{D}^2/\Gamma_{30}^*$ de gênero 2. Assim, a estrutura algébrica deste grupo fuchsiano tem a seguinte representação

$$\Gamma_{30}^* = \langle T_1^*, \ldots, T_{15}^* \ : \ T_1^* \circ (T_2^*)^{-1} \circ \ldots \circ (T_{14}^*)^{-1} \circ T_{15}^* = Id \text{ e } (T_1^*)^{-1} \circ T_2^* \circ \ldots \circ T_{14}^* \circ (T_{15}^*)^{-1} = id \rangle.$$

3.4.2 Grupo Fuchsiano $\Gamma_{10}^\bullet$ via um Emparelhamento Diferente

Com o intuito de mostrar um isomorfismo entre dois grupos fuchsianos aritméticos provenientes de emparelhamentos diferentes, que será visto na Seção 4.1, veremos agora a contrução do grupo fuchsiano $\Gamma_{10}^\bullet$ proveniente da tesselação $\{4g+2, 2g+1\}$, para $g = 2$, utilizando um outro tipo de emparelhamento sem ser o emparelhamento normal e o diametralmente oposto. Para isso, consideremos as arestas $u_1, u_2, \ldots, u_{10}$ do polígono fundamental $\mathcal{P}_{10}$ associadas da forma como na Figura 3.5.

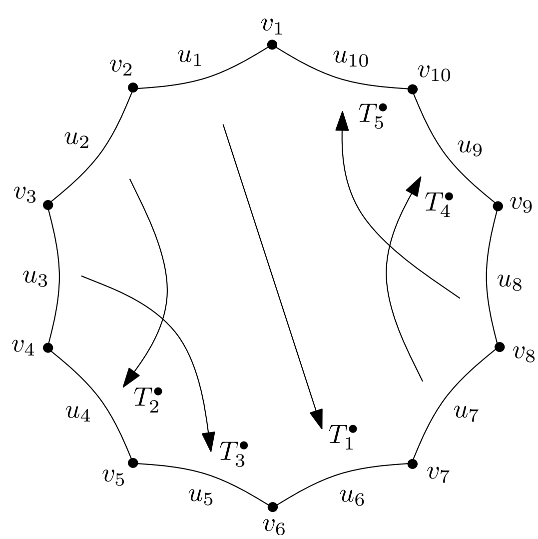

Figura 3.5: *Outro emparelhamento das arestas de* $\mathcal{P}_{10}$

As isometrias para este emparelhamento são

$$T_1^\bullet(u_1) = u_6, \ T_2^\bullet(u_2) = u_4, \ T_3^\bullet(u_3) = u_5, \ T_4^\bullet(u_7) = u_9 \text{ e } T_5^\bullet(u_8) = u_{10}. \tag{3.30}$$

Como a transformação $T_1^\bullet$ emparelha a aresta u_1 com sua diametralmente oposta, segue que $A_1^\bullet = A_1^*$, obtida em (3.25). E, as demais matrizes $A_i^\bullet$'s correspondentes às transformações $T_i^\bullet$'s, com $i = 2, \ldots, 5$, obtidas através de conjugações da matriz $A_1^\bullet$, são dadas por

$$A_2^\bullet = C^{-2}A_1^\bullet C^{-1},\ A_3^\bullet = C^{-1}A_1^\bullet C^{-2},\ A_4^\bullet = C^3A_1^\bullet C^4 \text{ e } A_5^\bullet = C^4A_1^\bullet C^3. \tag{3.31}$$

Por meio desses emparelhamentos, obtemos novamente uma superfície compacta e orientável $\mathbb{D}^2/\Gamma_{10}^\bullet$ de gênero 2. Dessa forma, a estrutura algébrica deste grupo fuchsiano tem a seguinte representação

$$\Gamma_{10}^\bullet = \langle T_1^\bullet, \ldots, T_5^\bullet \ :\ T_1^\bullet \circ T_4^\bullet \circ (T_5^\bullet)^{-1} \circ (T_4^\bullet)^{-1} \circ T_5^\bullet = Id \text{ e } (T_1^\bullet)^{-1} \circ T_2^\bullet \circ (T_3^\bullet)^{-1} \circ (T_2^\bullet)^{-1} \circ T_3^\bullet = id\rangle.$$

Os próximos resultados mostram o processo de identificação dos grupos fuchsianos aritméticos derivados de uma álgebra dos quatérnios sobre um corpo de números totalmente real. As demostrações seguem de modo análogo à dos Teoremas 3.3.2 e 3.3.3.

Teorema 3.4.1 *Os elementos dos grupos fuchsianos Γ_{10}^*, e $\Gamma_{10}^\bullet$ são identificados, via isomorfismo, com os elementos da ordem dos quatérnios $\mathcal{O} = (\sqrt{5}, -1)_R$, onde $R = \mathbb{Z}\left[\frac{\sqrt{10+2\sqrt{5}}}{2}\right]$.*

Teorema 3.4.2 *O grupo fuchsiano Γ_{10}^* e $\Gamma_{10}^\bullet$, associados com o polígono hiperbólico regular $\mathcal{P}_{10}$, são derivados da álgebra dos quatérnios $\mathcal{A} = (\sqrt{5}, -1)_{\mathbb{K}}$, sobre o corpo de números totalmente real $\mathbb{K} = \mathbb{Q}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)$, onde $[\mathbb{K} : \mathbb{Q}] = 4$.*

Na Seção 4.1.1, apresentamos exemplos da forma dos geradores que caracterizam os grupos fuchsianos aritméticos Γ_{10}^* e $\Gamma_{10}^\bullet$ provenientes da tesselação $\{4g + 2, 2g + 1\}$, para $g = 2$, de acordo com os Teoremas 3.4.1 e 3.4.2.

3.5 Grupo Fuchsiano Aritmético $\{12g - 6, 3\}$, para $g = 3$

Nesta seção consideramos a tesselação $\{12g-6, 3\}$, com $g \geq 2$. Os polígonos desta tesselação contêm $12g - 6$ lados e cada vértice é o encontro de 3 desses polígonos. Esta tesselação gera superfícies de gênero g e para cada g, podemos obter o grupo fuchsiano Γ_{12g-6} associado através da identificação das arestas de um polígono regular $\mathcal{P}_{12g-6}$, de $12g-6$ arestas em $\mathbb{D}^2$. Da mesma forma, como vimos para a tesselação $\{4g+2, 2g+1\}$ na Seção 3.4, o grupo fuchsiano aritmético nem sempre pode ser obtido para qualquer gênero g da tesselação $\{12g - 6, 3\}$, pois não temos muitos valores de g tais que $p = 12g - 6$ satisfaz a condição de Fermat (Teorema 3.1.3). De modo a exemplificar a construção destes grupos para esta tesselação, consideramos a tesselação $\{30, 3\}$, ou seja, o grupo fuchsiano aritmético Γ_{30}. Observamos que para $g = 2$ não é possível obter o grupo fuchsiano aritmético associado através da construção proposta neste trabalho, pois $p = 18$ não pode ser decomposto como potências de 2 ou potências de 2 e números distintos de Fermat.

Seja $\mathcal{P}_{30}$ o polígono hiperbólico regular de 30 arestas associado a tesselação $\{30, 3\}$, ou seja, associado a tesselação $\{12g - 6, 3\}$ para $g = 3$. Consideremos

$$u_1, u_2, \ldots, u_{30} \ \text{ e } \ v_1, v_2, \ldots, v_{30}$$

como as arestas e os vértices de $\mathcal{P}_{30}$, respectivamente, dispostos em ordem cíclica fixa no sentido anti-horário.

Para esta tesselação acreditamos não ser possível obter o emparelhamento diametralmente oposto, pois em [40] foi feita uma busca exaustiva de 927 tipos de emparelhamentos de arestas de polígonos hiperbólicos regulares que geram superfícies de gênero 3, e para a tesselação $\{30,3\}$, não foi encontrado um emparelhamento em que todas as arestas são identificadas com a sua diametralmente oposta. Dessa forma, utilizando um dos emparelhamentos apresentado em [40] o qual foi descrito detalhadamente em [20], construímos este grupo através da seguinte associação das arestas:

$$\{u_1,u_{16}\},\{u_2,u_{17}\},\{u_3,u_{30}\},\{u_4,u_7\},\{u_5,u_{20}\},\{u_6,u_{21}\},\{u_8,u_{29}\},\{u_9,u_{12}\},$$

$$\{u_{10},u_{25}\},\{u_{11},u_{26}\},\{u_{13},u_{28}\},\{u_{14},u_{23}\},\{u_{15},u_{18}\},\{u_{19},u_{22}\},\{u_{24},u_{27}\}.$$

Através da Figura 3.6, vemos como este emparelhamento é obtido no polígono regular hiperbólico $\mathcal{P}_{30}$.

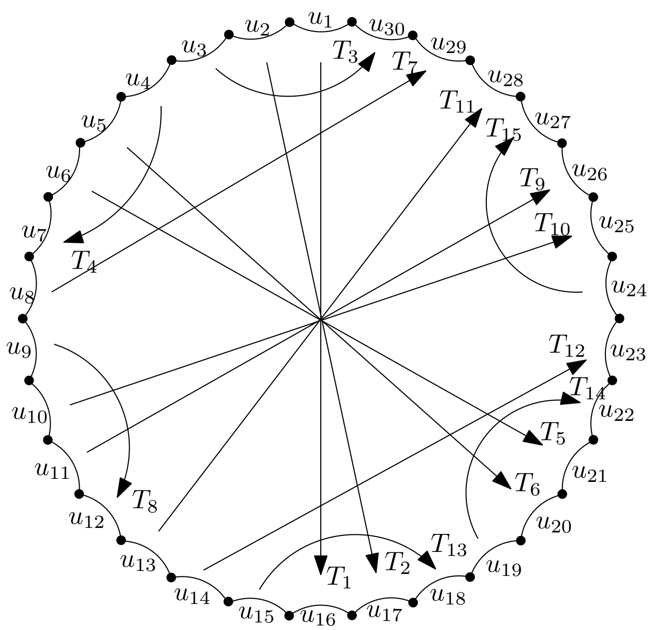

Figura 3.6: *Emparelhamento das arestas de* $\mathcal{P}_{30}$

Assim, as isometrias $T_1,T_2,\ldots,T_{15}$ para este emparelhamento são tais que

$$\begin{array}{c} T_i(u_i)=u_{i+6g-3} \;\text{ e }\; T_i(u_{i+1})=u_{i+6g-2}, \quad \text{onde } \; i=1,2; \\ T_i(u_{3+5i})=u_{12g-6-i} \;\text{ e }\; T_i(u_{4+5i})=u_{7+5i}, \quad \text{onde } \; i=0,1; \\ T_i(u_{6g+5i})=u_{6g-3-i} \;\text{ e }\; T_i(u_{6g+1+5i})=u_{6g+4+5i}, \quad \text{onde } \; i=0,1; \\ T_i(u_{5g-2})=u_{11g-5}, \end{array} \tag{3.32}$$

onde $g=3$.

Por meio destes emparelhamentos, obtemos uma superfície compacta e orientável $\mathbb{D}^2/\Gamma_{30}$ de gênero $g=3$. Se conhecermos a transformação T_1 podemos escrever os outros elementos de Γ_{30}

como conjugações de T_1 por meio de potências de T_C, onde T_C é uma tranformação elíptica de ordem 30 com matriz associada

$$C = \begin{pmatrix} e^{\frac{i\pi}{30}} & 0 \\ 0 & e^{-\frac{i\pi}{30}} \end{pmatrix}, \tag{3.33}$$

e tal que

$$T_C(u_1) = u_{16} \quad \text{e} \quad T_{C^{r_i}}(u_1) \in \{u_i, \text{ onde } \ i = 2, \ldots, 30\}, \tag{3.34}$$

onde r_i é a potência de T_C. Como a transformação T_1 emparelha a aresta u_1 com sua diametralmente oposta u_{16}, pelo Teorema 3.1.1, segue que

$$A_1 = \begin{pmatrix} \frac{2\cos\frac{\pi}{3}}{2sen\frac{\pi}{30}} & \frac{\sqrt{2\cos\frac{\pi}{15}+2\cos\frac{2\pi}{3}}\cdot e^{i\frac{31\pi}{30}}}{2sen\frac{\pi}{30}} \\ \frac{\sqrt{2\cos\frac{\pi}{15}+2\cos\frac{2\pi}{3}}\cdot e^{-i\frac{31\pi}{30}}}{2sen\frac{\pi}{30}} & \frac{2\cos\frac{\pi}{3}}{2sen\frac{\pi}{30}} \end{pmatrix}. \tag{3.35}$$

Para esta tesselação, por (2.6), tem-se

$$\frac{p}{q} = \frac{12g-6}{3} = \frac{30}{3} = 10$$

ciclos de vértices de comprimento $q = 3$. Estes ciclos de vértices serão dados por

$$\begin{array}{rcr} \varepsilon_1 = \{v_1, v_{17}, v_3\} & , & \varepsilon_2 = \{v_2, v_{18}, v_{16}\} \\ \varepsilon_3 = \{v_4, v_8, v_{30}\} & , & \varepsilon_4 = \{v_5, v_{21}, v_7\} \\ \varepsilon_5 = \{v_6, v_{22}, v_{20}\} & , & \varepsilon_6 = \{v_9, v_{13}, v_{29}\} \\ \varepsilon_7 = \{v_{10}, v_{26}, v_{12}\} & , & \varepsilon_8 = \{v_{11}, v_{27}, v_{25}\} \\ \varepsilon_9 = \{v_{13}, v_{29}, v_9\} & , & \varepsilon_{10} = \{v_{14}, v_{24}, v_{28}\}. \end{array}$$

Assim, por meio do processo de construção dos ciclos $\varepsilon_1, \ldots, \varepsilon_{10}$, podemos determinar a estrutura algébrica deste grupo através da seguinte representação

$$\begin{aligned} \Gamma_{30} \;=\; & \langle T_1, \ldots, T_{15} \;:\; T_1 \circ (T_2)^{-1} \circ T_3 = id; \;\; T_2 \circ (T_{13})^{-1} \circ (T_1)^{-1} = id; \\ & T_4 \circ T_7 \circ (T_3)^{-1} = id; \;\; T_5 \circ (T_6)^{-1} \circ (T_4)^{-1} = id; \;\; T_6 \circ (T_{14})^{-1} \circ (T_5)^{-1} = id; \\ & T_8 \circ T_{11} \circ (T_7)^{-1} = id; \;\; T_9 \circ (T_{10})^{-1} \circ (T_8)^{-1} = id; \;\; T_{10} \circ (T_{15})^{-1} \circ (T_9)^{-1} = id; \\ & T_{11} \circ (T_7)^{-1} \circ T_8 = id; \;\; T_{12} \circ T_{15} \circ (T_{11})^{-1} = id \rangle. \end{aligned}$$

Os próximos resultados mostram o processo de identificação dos grupos fuchsianos aritméticos derivados de uma álgebra dos quatérnios sobre um corpo de números totalmente real. As demostrações seguem de modo análogo à dos Teoremas 3.3.2 e 3.3.3, de acordo com a forma de seus geradores.

Teorema 3.5.1 *[53] Os elementos do grupo fuchsiano Γ_{30} são identificados, via isomorfismo, com os elementos da ordem dos quatérnios $\mathcal{O} = (-4+2\theta, -1)_R$, onde $R = \mathbb{Z}[\theta_1]$ e*

$$\theta = \sqrt{9 + \sqrt{5} + \sqrt{30 - 6\sqrt{5}}} \quad e \quad \theta_1 = \sqrt{3} + \theta. \tag{3.36}$$

Teorema 3.5.2 *[53] O grupo fuchsiano Γ_{30}, associado com o polígono hiperbólico regular $\mathcal{P}_{30}$, é derivado da álgebra dos quatérnios $\mathcal{A}=(-4+2\theta,-1)_{\mathbb{K}}$, sobre o corpo de números totalmente real $\mathbb{K}=\mathbb{Q}(\theta_1)$, onde $[\mathbb{K}:\mathbb{Q}]=8$ e, θ e θ_1 são dados como em (3.36).*

Para finalizar, apresentamos um exemplo, construído em [53], que mostra a forma dos geradores do grupo fuchsiano aritmético Γ_{30} de acordo com os Teoremas 3.5.1 e 3.5.2. Segue através dos geradores e dos Teoremas 3.5.1 e 3.5.2, que o grupo fuchsiano aritmético Γ_{30} é um exemplo de grupo fuchsiano aritmético derivado de uma álgebra dos quatérnios do tipo $\mathcal{A}=(\theta_1,-1)_{\mathbb{K}}$, onde $\theta_1\in\mathbb{K}=\mathbb{Q}(\theta)$.

Exemplo 3.5.1 *[53] Seja $\mathcal{P}_{30}$ o polígono hiperbólico regular associado à tesselação $\{30,3\}$. Consideremos o emparelhamento das arestas de $\mathcal{P}_{30}$ como apresentado na Figura 3.6. Os geradores para o grupo fuchsiano aritmético Γ_{30} obtidos através deste emparelhamento são:*

$$
\begin{aligned}
G_1 &= \begin{pmatrix} \frac{x_1+2\sqrt{-4+2\theta}}{8} & \frac{-w_1\sqrt{-4+2\theta}}{8} \\ \frac{-w_1\sqrt{-4+2\theta}}{8} & \frac{x_1-2\sqrt{-4+2\theta}}{8} \end{pmatrix} &= \varphi(\tfrac{x_1}{8}+\tfrac{1}{4}i-\tfrac{w_1}{8}k)\ , \\
G_2 &= \begin{pmatrix} \frac{2x_1-y_2\sqrt{-4+2\theta}}{16} & \frac{-w_2\sqrt{-4+2\theta}}{16} \\ \frac{-w_2\sqrt{-4+2\theta}}{16} & \frac{2x_1+y_2\sqrt{-4+2\theta}}{16} \end{pmatrix} &= \varphi(\tfrac{x_1}{8}-\tfrac{y_2}{16}i-\tfrac{w_2}{16}k)\ , \\
G_3 &= \begin{pmatrix} \frac{4x_1-y_3\sqrt{-4+2\theta}}{32} & \frac{w_3\sqrt{-4+2\theta}}{96} \\ \frac{w_3\sqrt{-4+2\theta}}{96} & \frac{4x_1+y_3\sqrt{-4+2\theta}}{32} \end{pmatrix} &= \varphi(\tfrac{x_1}{8}-\tfrac{y_3}{32}i+\tfrac{w_3}{96}k)\ , \\
G_4 &= \begin{pmatrix} \frac{4x_1-y_4\sqrt{-4+2\theta}}{32} & \frac{-w_4\sqrt{-4+2\theta}}{32} \\ \frac{-w_4\sqrt{-4+2\theta}}{32} & \frac{4x_1+y_4\sqrt{-4+2\theta}}{32} \end{pmatrix} &= \varphi(\tfrac{x_1}{8}-\tfrac{y_4}{32}i-\tfrac{w_4}{32}k)\ , \\
G_5 &= \begin{pmatrix} \frac{2x_1-y_5\sqrt{-4+2\theta}}{16} & \frac{-w_5\sqrt{-4+2\theta}}{16} \\ \frac{-w_5\sqrt{-4+2\theta}}{16} & \frac{2x_1+y_5\sqrt{-4+2\theta}}{16} \end{pmatrix} &= \varphi(\tfrac{x_1}{8}-\tfrac{y_5}{16}i-\tfrac{w_5}{16}k)\ , \\
G_6 &= \begin{pmatrix} \frac{2x_1-y_6\sqrt{-4+2\theta}}{16} & \frac{w_6\sqrt{-4+2\theta}}{16} \\ \frac{w_6\sqrt{-4+2\theta}}{16} & \frac{2x_1+y_6\sqrt{-4+2\theta}}{16} \end{pmatrix} &= \varphi(\tfrac{x_1}{8}-\tfrac{y_6}{16}i+\tfrac{w_6}{16}k)\ ,
\end{aligned}
$$

onde

$$
\begin{aligned}
&x_1 = 8+4\sqrt{5}+(3+\sqrt{5})\sqrt{30-6\sqrt{5}}, \quad w_1 = 3\sqrt{3}+\sqrt{15}+(2+\sqrt{5})\sqrt{10-2\sqrt{5}} \\
&y_2 = 9+5\sqrt{5}+(2+\sqrt{5})\sqrt{30-6\sqrt{5}}, \quad w_2 = \sqrt{3}+\sqrt{15}+\sqrt{10-2\sqrt{5}} \\
&y_3 = 12+8\sqrt{5}+(3+\sqrt{5})\sqrt{30-6\sqrt{5}}, \quad w_3 = 24\sqrt{3}+12\sqrt{15}+(5\sqrt{3}+3\sqrt{15})\sqrt{30-6\sqrt{5}} \\
&y_4 = 6+2\sqrt{5}+(1+\sqrt{5})\sqrt{30-6\sqrt{5}}, \quad w_4 = 10\sqrt{3}+6\sqrt{15}+(7+3\sqrt{5})\sqrt{10-2\sqrt{5}} \\
&y_5 = 11+3\sqrt{5}+(2+\sqrt{5})\sqrt{30-6\sqrt{5}}, \quad w_5 = \sqrt{3}+\sqrt{15}+(2+\sqrt{5})\sqrt{10-2\sqrt{5}} \\
&y_6 = 7+3\sqrt{5}+(2+\sqrt{5})\sqrt{30-6\sqrt{5}}, \quad w_6 = 5\sqrt{3}+\sqrt{15}+(2+\sqrt{5})\sqrt{10-2\sqrt{5}}
\end{aligned}
$$

e

$$\theta = \sqrt{9+\sqrt{5}+\sqrt{30-6\sqrt{5}}}.$$

Como $x_1,w_1,y_2,w_2,y_3,w_3,y_4,w_4,y_5,w_5,y_6,w_6\in\mathbb{Z}[\theta_1]$, onde $\theta_1=\sqrt{3}+\theta$, segue através dos Teoremas 3.5.1 e 3.5.2, que a ordem dos quatérnios associada com o grupo fuchsiano Γ_{30} derivado da álgebra dos quatérnios $\mathcal{A}=(-4+2\theta,-1)_{\mathbb{K}}$, é $\mathcal{O}=(-4+2\theta,-1)_R$, onde $R=\mathbb{Z}[\theta_1]$, $\mathbb{K}=\mathbb{Q}(\theta_1)$ e $[\mathbb{K}:\mathbb{Q}]=8$.

Capítulo 4

Isomorfismo entre Grupos Fuchsianos Aritméticos, Descrição de Corpos de Números Totalmente Reais como Subcorpos de Corpos Ciclotômicos e Ordens Maximais dos Quatérnios

Como mencionado no Capítulo 2 nosso interesse é obter grupos fuchsianos que podem ser associados a uma álgebra e uma ordem dos quatérnios, os quais chamamos de grupos fuchsianos aritméticos, com o intuito de obter constelações de sinais no plano hiperbólico. No Capítulo 3, construímos de fato estes grupos considerando tesselações hiperbólicas regulares $\{p, q\}$ que geram superfícies de gênero $g \geq 2$. Neste sentido, nosso objetivo neste capítulo é apresentar algumas aplicações decorrentes da construção destes grupos, principalmente na área da teoria de códigos e reticulados.

Iniciamos, na Seção 4.1, apresentando um isomorfismo entre grupos fuchsianos aritméticos provenientes de emparelhamentos diferentes. Uma motivação para a construção deste isomorfismo segue pelo fato de que em codificação quântica topológica o emparelhamento diametralmente oposto é o mais desejado, pois este é o caminho homologicamente não trivial com a maior distância mínima possível, [2]. Como consequência, o código resultante apresenta uma capacidade de correção de erros maior dentre todos os códigos oriundos dos demais emparelhamentos. Porém, até então, os grupos fuchsianos obtidos na literatura apresentavam em sua construção o emparelhamento normal devido a sua baixa complexidade computacional. Sendo assim, utilizando o referido isomorfismo, fixado o gênero g da superfície pode-se utilizar o grupo fuchsiano aritmético proveniente de qualquer tipo de emparelhamento, pois são dois a dois isomorfos.

Além disso, na Seção 4.2, descrevemos alguns dos corpos de números que utilizamos para construir grupos fuchsianos aritméticos no Capítulo 3, como subcorpos maximais reais de corpos ciclotômicos pelo fato destes sucorpos serem totalmente reais. Mais precisamente, os corpos utilizados são os corpos da forma $\mathbb{K} = \mathbb{Q}(\theta)$, onde θ é dado em (3.19). Utilizando radicais e trigonometria, nos resultados que veremos na Seção 4.2, estabelecemos relações entre subcorpos maximais reais de corpos ciclotômicos e extensões de corpos envolvendo radicais finitos.

Uma primeira abordagem neste aspecto foi feita em [21] utilizando o corpo de números totalmente real $\mathbb{Q}(\theta)$, onde $\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}$, tendo como objetivo obter a estrutura dos subcorpos do corpo ciclotômico $\mathbb{Q}(\zeta_{2^r})$. Nossa motivação neste e nos demais casos que são tratados neste trabalho está em caracterizar os corpos de números totalmente reais obtidos a partir destas relações, além de seu anel dos inteiros, com o intuito de obter ordens maximais dos quatérnios para álgebras dos quatérnios em que temos interesse em construir grupos fuchsianos aritméticos.

Além desta primeira motivação, Giraud et al., em [25], conjecturam que o homomorfismo canônico do anel de inteiros de $\mathbb{Q}(\theta)$, onde $\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}$, pode ser utilizado para construir um reticulado $\mathbb{Z}^n$-rotacionado. Posteriormente em [4] e [7], de modo independente, os autores apresentam uma construção de reticulados $\mathbb{Z}^n$-rotacionados utilizando o subcorpo maximal real do 2^r-ésimo corpo ciclotômico $\mathbb{Q}(\zeta_{2^r})$, que são bons para o canal com desvanecimento do tipo Rayleigh. Já em [29], também utilizando subcorpos maximais reais de corpos ciclotômicos, foram obtidas versões rotacionadas do reticulado D_n para $n = 2^{r-2}$, para $r \geq 5$, sendo estes simultaneamente eficientes para ambos os canais, gaussiano e do tipo Rayleigh. Sendo assim, acreditamos que com a associação de grupos fuchsianos aritméticos com subcorpos maximais reais de corpos ciclotômicos, será possível mostrar relações entre os reticulados hiperbólicos, caracterizados por ordens dos quatérnios maximais, com versões rotacionadas do reticulado $\mathbb{Z}^n$ ou do reticulado D_n.

Para finalizar, na Seção 4.3, apresentamos as ordens maximais dos quatérnios, ou equivalentemente os reticulados hiperbólicos completos, associados a grupos fuchsianos aritméticos obtidos no Capítulo 3. Os grupos obtidos no Capítulo 3 foram construídos utilizando a ordem usual dos quatérnios $\mathcal{O} = (\theta, -1)_R$, que é caracterizada pelo anel dos inteiros $R = \mathcal{I}_{\mathbb{K}}$ e com a mesma base $\{1, i, j, k\}$ da álgebra $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ associada. Esta ordem usual não é maximal para os casos tratados neste trabalho (ver caso particular no Exemplo 2.2.7). Porém, quando uma ordem maximal dos quatérnios é identificada com os elementos de um grupo fuchsiano via isomorfismo, tornando-o aritmético, temos um rotulamento completo dos pontos da constelação de sinal associada. Neste sentido, nosso objetivo, na Seção 4.3, é obter ordens maximais dos quatérnios $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_R$, identificadas através de uma base, para algumas álgebras dos quatérnios as quais possibilitaram a construção de grupos fuchsianos aritméticos descritos no Capítulo 3. Como veremos, estas ordens maximais não são imediatas para os corpos de números tratados neste trabalho e quanto mais aumentamos o grau das extensões destes corpos sobre os racionais, maior a complexidade para obter uma base que caracteriza estas ordens maximais. Para obter tais bases o uso do *software Magma* foi indispensável.

Neste capítulo são apresentados também, na Subseção 4.3.4, dois exemplos utilizando os conceitos e resultados vistos durante todo este trabalho com o intuito de dar mais clareza aos resultados apresentados.

4.1 Isomorfismo entre Grupos Fuchsianos Aritméticos

O objetivo desta seção é mostrar que existe um isomorfismo entre dois grupos fuchsianos aritméticos derivados de uma mesma tesselação $\{p, q\}$, porém que foram obtidos utilizando emparelhamentos diferentes. Para exemplificar tais resultados iremos provar este isomorfimo para a tesselação $\{4g, 4g\}$ utilizando os grupos Γ_{4g} e Γ^*_{4g}, e para a tesselação $\{4g+2, 2g+1\}$ para o gênero fixado $g = 2$, ou seja, para a tesselação $\{10, 5\}$ utilizando os grupos Γ^*_{10} e $\Gamma^\bullet_{10}$. Lembramos que os grupos Γ_{4g}, Γ^*_{4g}, Γ^*_{10} e $\Gamma^\bullet_{10}$ foram construídos nas Seções 3.3 e 3.4.

Na Seção 3.3 apresentamos os grupos fuchsianos Γ_{4g} e Γ^*_{4g} da tesselação $\{4g, 4g\}$ obtidos através do emparelhamento normal e do emparelhamento diametralmente oposto das arestas. O resultado a seguir mostra que existe um isomorfismo entre estes dois grupos.

Teorema 4.1.1 *Se $\Gamma_{4g}, \Gamma^*_{4g} \subset PSL(2, \mathbb{C})$ são grupos fuchsianos associados à tesselação $\{4g, 4g\}$ provenientes dos emparelhamentos normal e diametralmente oposto, respectivamente, então $\Gamma_{4g} \simeq \Gamma^*_{4g}$.*

Demonstração: Dado um gênero g, consideremos Γ_1 e Γ_2 grupos fuchsianos em $\mathbb{H}^2$, ou seja, subgrupos de $PSL(2, \mathbb{R})$. Assim,

$$\Gamma_1 = f^{-1} \circ \Gamma_{4g} \circ f \quad \text{e} \quad \Gamma_2 = f^{-1} \circ \Gamma^*_{4g} \circ f,$$

onde f é como em (1.4). A existência destes grupos é garantida pela Observação 2.1.2. Além disso, se considerarmos os isomorfismos de grupos $\phi_1 : \Gamma_1 \longrightarrow \Gamma_{4g}$ e $\phi_2 : \Gamma_2 \longrightarrow \Gamma^*_{4g}$ dados por

$$\phi_1(T) = \phi_2(T) = f^{-1} \circ T \circ f,$$

segue que

$$\Gamma_1 \simeq \Gamma_{4g} \quad \text{e} \quad \Gamma_2 \simeq \Gamma^*_{4g}.$$

Para $i = 1, \ldots, 2g$, sejam A_i e A^*_i as matrizes correspondentes às transformações T_i e T^*_i, respectivamente. Assim,

$$G_i = f^{-1} A_i f \quad \text{e} \quad G^*_i = f^{-1} A^*_i f,$$

são os geradores dos grupos Γ_1 e Γ_2, respectivamente, onde $i = 1, \ldots, 2g$ e considerando a multiplicação usual de matrizes. Como $\Gamma_1, \Gamma_2 \subset PSL(2, \mathbb{R})$, segue pelo Lema 3.1.1, que os correspondentes geradores G_i e G^*_i são da forma dada em (3.7). E, pela forma como foram construídos os grupos Γ_1 e Γ_2, definidos a partir de Γ_{4g} e Γ^*_{4g}, segue que $G_i, G^*_i \subset M(2, \mathbb{Q}(\sqrt{\theta}))$, ambos para o mesmo valor de θ, onde θ depende do gênero g e é como em (3.19). Logo, existe um isomorfismo $\psi : \Gamma_1 \longrightarrow \Gamma_2$ em que

$$\psi(G_i) = G^*_i.$$

Portanto, pela cadeia de isomorfismos

$$\Gamma_{4g} \simeq \Gamma_1 \simeq \Gamma_2 \simeq \Gamma^*_{4g},$$

segue que $\Gamma_{4g} \simeq \Gamma^*_{4g}$. ■

O resultado a seguir estabelece o isomorfismo entre os grupos fuchsianos aritméticos Γ^*_{10} e $\Gamma^\bullet_{10}$ construídos na Seção 3.4, onde a prova segue de forma análoga ao do Teorema 4.1.1, através da forma dos geradores destes grupos.

Teorema 4.1.2 *Se $\Gamma^*_{10}, \Gamma^\bullet_{10} \subset PSL(2, \mathbb{C})$ são grupos fuchsianos associados a tesselação $\{4g + 2, 2g + 1\}$ provenientes dos emparelhamentos apresentados na Seção 3.4, então $\Gamma^*_{10} \simeq \Gamma^\star_{10}$.*

Demostração: Segue de forma análoga ao Teorema 4.1.1, porém considerando a forma dos geradores de Γ^*_{10} e $\Gamma^\bullet_{10}$, e o valor de $\theta = \sqrt{5}$ fixo. ■

4.1.1 Exemplos

Como uma aplicação do Teorema 4.1.1, apresentamos a seguir dois exemplos onde obtemos os geradores dos grupos fuchsianos aritméticos Γ_{4g} e Γ_{4g}^*, para $g = 4$, utilizando o algoritmo proposto na Seção 3.2 e mostrando que estes grupos são isomorfos, através do Teorema 4.1.1.

Exemplo 4.1.1 *Seja $\mathcal{P}_{16}$ o polígono hiperbólico regular associado à tesselação $\{16, 16\}$. Consideremos o emparelhamento normal das arestas de $\mathcal{P}_{16}$. Utilizando o algoritmo proposto na Seção 3.2, obtemos os seguintes geradores para o grupo fuchsiano aritmético Γ_{16} :*

$$G_1 = \frac{1}{2}\begin{pmatrix} x_1 - y_1\sqrt[4]{2+\sqrt{2}} & z_1 - w_1\sqrt[4]{2+\sqrt{2}} \\ -z_1 - w_1\sqrt[4]{2+\sqrt{2}} & x_1 + y_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - y_1 i + z_1 j - w_1 k) \ ,$$

$$G_2 = \frac{1}{2}\begin{pmatrix} x_1 - w_1\sqrt[4]{2+\sqrt{2}} & z_1 + y_1\sqrt[4]{2+\sqrt{2}} \\ -z_1 + y_1\sqrt[4]{2+\sqrt{2}} & x_1 + w_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - w_1 i + z_1 j + y_1 k) \ ,$$

$$G_3 = \frac{1}{2}\begin{pmatrix} x_1 + y_1\sqrt[4]{2+\sqrt{2}} & z_1 + w_1\sqrt[4]{2+\sqrt{2}} \\ -z_1 + w_1\sqrt[4]{2+\sqrt{2}} & x_1 - y_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + y_1 i + z_1 j + w_1 k) \ ,$$

$$G_4 = \frac{1}{2}\begin{pmatrix} x_1 + w_1\sqrt[4]{2+\sqrt{2}} & z_1 - y_1\sqrt[4]{2+\sqrt{2}} \\ -z_1 - y_1\sqrt[4]{2+\sqrt{2}} & x_1 - w_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + w_1 i + z_1 j - y_1 k) \ ,$$

$$G_5 = \frac{1}{2}\begin{pmatrix} x_1 - y_1\sqrt[4]{2+\sqrt{2}} & z_1 + w_1\sqrt[4]{2+\sqrt{2}} \\ -z_1 + w_1\sqrt[4]{2+\sqrt{2}} & x_1 + y_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - y_1 i + z_1 j + w_1 k) \ ,$$

$$G_6 = \frac{1}{2}\begin{pmatrix} x_1 + w_1\sqrt[4]{2+\sqrt{2}} & z_1 + y_1\sqrt[4]{2+\sqrt{2}} \\ -z_1 + y_1\sqrt[4]{2+\sqrt{2}} & x_1 - w_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + w_1 i + z_1 j + y_1 k) \ ,$$

$$G_7 = \frac{1}{2}\begin{pmatrix} x_1 + y_1\sqrt[4]{2+\sqrt{2}} & z_1 - w_1\sqrt[4]{2+\sqrt{2}} \\ -z_1 - w_1\sqrt[4]{2+\sqrt{2}} & x_1 - y_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + y_1 i + z_1 j - w_1 k) \ ,$$

$$G_8 = \frac{1}{2}\begin{pmatrix} x_1 - w_1\sqrt[4]{2+\sqrt{2}} & z_1 - y_1\sqrt[4]{2+\sqrt{2}} \\ -z_1 - y_1\sqrt[4]{2+\sqrt{2}} & x_1 + w_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - w_1 i + \tfrac{z_1}{2} j - \tfrac{y_1}{2} k) \ ,$$

onde $x_1 = 2 + \sqrt{2+\sqrt{2}}$, $y_1 = 2 + \sqrt{2} + 2\sqrt{2+\sqrt{2}}$, $z_1 = (1+\sqrt{2})(2 + \sqrt{2+\sqrt{2}})$ e $w_1 = \sqrt{2}$. Assim, de acordo com o Teorema 3.3.2, segue que a ordem dos quatérnios associada com Γ_{16} é $\mathcal{O} = (\sqrt{2+\sqrt{2}}, -1)_R$, onde $R = \mathbb{Z}[\sqrt{2+\sqrt{2}}]$ e, de acordo com o Teorema 3.3.3, segue que Γ_{16} é derivado da álgebra dos quatérnios $\mathcal{A} = (\sqrt{2+\sqrt{2}}, -1)_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ e $[\mathbb{K} : \mathbb{Q}] = 4$.

Exemplo 4.1.2 *Seja $\mathcal{P}_{16}$ o polígono hiperbólico regular associado à tesselação $\{16, 16\}$. Vamos considerar agora o emparelhamento diametralmente oposto das arestas de $\mathcal{P}_{16}$. Utilizando o algoritmo proposto na Seção 3.2, obtemos os seguintes geradores para o grupo fuchsiano aritmético Γ_{16}^*:*

$$G_1^* = \frac{1}{2}\begin{pmatrix} x_1 + y_1\sqrt[4]{2+\sqrt{2}} & -w_1\sqrt[4]{2+\sqrt{2}} \\ -w_1\sqrt[4]{2+\sqrt{2}} & x_1 - y_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + y_1 i - w_1 k) ,$$

$$G_2^* = \frac{1}{2}\begin{pmatrix} x_1 + y_2\sqrt[4]{2+\sqrt{2}} & -w_2\sqrt[4]{2+\sqrt{2}} \\ -w_2\sqrt[4]{2+\sqrt{2}} & x_1 - y_2\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + y_2 i - w_2 k) ,$$

$$G_3^* = \frac{1}{2}\begin{pmatrix} x_1 + w_2\sqrt[4]{2+\sqrt{2}} & -y_2\sqrt[4]{2+\sqrt{2}} \\ -y_2\sqrt[4]{2+\sqrt{2}} & x_1 - w_2\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + w_2 i - y_2 k) ,$$

$$G_4^* = \frac{1}{2}\begin{pmatrix} x_1 + w_1\sqrt[4]{2+\sqrt{2}} & -y_1\sqrt[4]{2+\sqrt{2}} \\ -y_1\sqrt[4]{2+\sqrt{2}} & x_1 - w_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + w_1 i - y_1 k) ,$$

$$G_5^* = \frac{1}{2}\begin{pmatrix} x_1 + w_1\sqrt[4]{2+\sqrt{2}} & y_1\sqrt[4]{2+\sqrt{2}} \\ y_1\sqrt[4]{2+\sqrt{2}} & x_1 - w_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + w_1 i + y_1 k) ,$$

$$G_6^* = \frac{1}{2}\begin{pmatrix} x_1 + w_2\sqrt[4]{2+\sqrt{2}} & y_2\sqrt[4]{2+\sqrt{2}} \\ y_2\sqrt[4]{2+\sqrt{2}} & x_1 - w_2\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + w_2 i + y_2 k) ,$$

$$G_7^* = \frac{1}{2}\begin{pmatrix} x_1 + y_2\sqrt[4]{2+\sqrt{2}} & w_2\sqrt[4]{2+\sqrt{2}} \\ w_2\sqrt[4]{2+\sqrt{2}} & x_1 - y_2\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + y_2 i + w_2 k) ,$$

$$G_8^* = \frac{1}{2}\begin{pmatrix} x_1 + y_1\sqrt[4]{2+\sqrt{2}} & w_1\sqrt[4]{2+\sqrt{2}} \\ w_1\sqrt[4]{2+\sqrt{2}} & x_1 - y_1\sqrt[4]{2+\sqrt{2}} \end{pmatrix} = \frac{1}{2}\varphi(x_1 + y_1 i + w_1 k) ,$$

onde $x_1 = 2+2\sqrt{2}(1+\sqrt{2+\sqrt{2}})$, $y_1 = \sqrt{2}$, $w_1 = 2+\sqrt{2}+2\sqrt{2+\sqrt{2}}$, $y_2 = \sqrt{2}(1+\sqrt{2+\sqrt{2}})$ *e* $w_2 = 2+\sqrt{2}+\sqrt{2}\sqrt{2+\sqrt{2}}$*. Assim, de acordo com os Teoremas 3.3.2 e 3.3.3, segue que a ordem dos quatérnios associada com o grupo fuchsiano* Γ_{16}^* *derivado da álgebra dos quatérnios* $\mathcal{A} = (\sqrt{2+\sqrt{2}}, -1)_{\mathbb{K}}$*, é* $\mathcal{O} = (\sqrt{2+\sqrt{2}}, -1)_R$*, onde* $R = \mathbb{Z}[\sqrt{2+\sqrt{2}}]$, $\mathbb{K} = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ *e* $[\mathbb{K} : \mathbb{Q}] = 4$*.*

Os exemplos a seguir mostram o isomorfismo estabelecido no Teorema 4.1.2 entre os grupos Γ_{10}^* e $\Gamma_{10}^\bullet$ provenientes da tesselação $\{10, 5\}$, onde os geradores dos grupos Γ_{10}^* e$\Gamma_{10}^\bullet$ foram obtidos utilizando o algoritmo apresentado na Seção 3.2.

Exemplo 4.1.3 *Seja a tesselação* $\{10, 5\}$ *e considere o emparelhamento diametralmente oposto das arestas, sobre as arestas do polígono* $\mathcal{P}_{10}$*. Utilizando o algoritmo proposto na Seção 3.2 obtemos os seguintes geradores para o grupo fuchsiano aritmético* Γ_{10}^* *:*

$$G_1^* = \frac{1}{2}\begin{pmatrix} x_1 - \sqrt[4]{5} & -w_1\sqrt[4]{5} \\ -w_1\sqrt[4]{5} & x_1 + \sqrt[4]{5} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - i - w_1 k),$$

$$G_2^* = \frac{1}{2^2}\begin{pmatrix} t_1 - x_1\sqrt[4]{5} & -l_1\sqrt[4]{5} \\ -l_1\sqrt[4]{5} & t_1 + x_1\sqrt[4]{5} \end{pmatrix} = \frac{1}{2^2}\varphi(t_1 - x_1 i - l_1 k),$$

$$G_3^* = \frac{1}{2^2}\begin{pmatrix} t_1 - y_1\sqrt[4]{5} & 0 \\ 0 & t_1 + y_1\sqrt[4]{5} \end{pmatrix} = \frac{1}{2^2}\varphi(t_1 - y_1 i),$$

$$G_4^* = \frac{1}{2^2}\begin{pmatrix} t_1 - x_1\sqrt[4]{5} & l_1\sqrt[4]{5} \\ l_1\sqrt[4]{5} & t_1 + x_1\sqrt[4]{5} \end{pmatrix} = \frac{1}{2^2}\varphi(t_1 - x_1 i + l_1 k),$$

$$G_5^* = \frac{1}{2}\begin{pmatrix} x_1 - \sqrt[4]{5} & w_1\sqrt[4]{5} \\ w_1\sqrt[4]{5} & x_1 + \sqrt[4]{5} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - i + w_1 k),$$

onde $x_1 = 3+\sqrt{5}, w_1 = \sqrt{5+2\sqrt{5}}$, $t_1 = 6+2\sqrt{5}$, $l_1 = \sqrt{10+2\sqrt{5}}$ *e* $y_1 = 2+2\sqrt{5}$. *Assim, de acordo com os Teoremas 3.4.1 e 3.4.2, segue que a ordem dos quatérnios associada ao grupo* Γ_{10}^**, derivado da álgebra dos quatérnios* $\mathcal{A} = (\sqrt{5}, -1)_{\mathbb{K}}$*, é* $\mathcal{O} = (\sqrt{5}, -1)_R$*, onde* $R = \mathbb{Z}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)$, $\mathbb{K} = \mathbb{Q}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)$ *e* $[\mathbb{K}:\mathbb{Q}] = 4$.

Exemplo 4.1.4 *Considere novamente a tesselação* $\{10, 5\}$ *mas agora com o emparelhamento das arestas de* $\mathcal{P}_{10}$ *como apresentado na Figura 3.5 e através das isometrias (3.30). Utilizando o algoritmo apresentado na Seção 3.2, obtemos os seguintes geradores para o grupo* $\Gamma_{10}^\bullet$*:*

$$G_1^\bullet = \frac{1}{2}\begin{pmatrix} x_1 - \sqrt[4]{5} & -w_1\sqrt[4]{5} \\ -w_1\sqrt[4]{5} & x_1 + \sqrt[4]{5} \end{pmatrix} = \frac{1}{2}\varphi(x_1 - i - w_1 k),$$

$$G_2^\bullet = \frac{1}{2}\begin{pmatrix} w_1 & -z_1 - l_1\sqrt[4]{5} \\ z_1 - l_1\sqrt[4]{5} & w_1 \end{pmatrix} = \frac{1}{2}\varphi(w_1 - z_1 j - l_1 k),$$

$$G_3^\bullet = \frac{1}{2^2}\begin{pmatrix} 2w_1 - y_1\sqrt[4]{5} & -2z_1 - l_1\sqrt[4]{5} \\ 2z_1 - l_1\sqrt[4]{5} & 2w_1 + y_1\sqrt[4]{5} \end{pmatrix} = \frac{1}{2^2}\varphi(2w_1 - y_1 i - 2z_1 j - l_1 k),$$

$$G_4^\bullet = \frac{1}{2}\begin{pmatrix} w_1 & -z_1 + l_1\sqrt[4]{5} \\ z_1 + l_1\sqrt[4]{5} & w_1 \end{pmatrix} = \frac{1}{2}\varphi(w_1 - z_1 j + l_1 k),$$

$$G_5^\bullet = \frac{1}{2^2}\begin{pmatrix} 2w_1 + y_1\sqrt[4]{5} & -2z_1 + l_1\sqrt[4]{5} \\ 2z_1 + l_1\sqrt[4]{5} & 2w_1 - y_1\sqrt[4]{5} \end{pmatrix} = \frac{1}{2^2}\varphi(2w_1 + y_1 i - 2z_1 j + l_1 k),$$

onde $x_1 = 3+\sqrt{5}, w_1 = \sqrt{5+2\sqrt{5}}$, $z_1 = 2+\sqrt{5}$, $l_1 = 1+\sqrt{5}$ *e* $y_1 = \sqrt{10+2\sqrt{5}}$. *Assim, de acordo com o Teorema 3.4.1, segue que a ordem dos quatérnios associada com* $\Gamma_{10}^\bullet$ *é* $\mathcal{O} = (\sqrt{5}, -1)_R$*, onde* $R = \mathbb{Z}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)$ *e, de acordo com o Teorema 3.4.2, segue que* $\Gamma_{10}^\bullet$ *é derivado da álgebra dos quatérnios* $\mathcal{A} = (\sqrt{5}, -1)_{\mathbb{K}}$*, onde* $\mathbb{K} = \mathbb{Q}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)$ *and* $[\mathbb{K}:\mathbb{Q}] = 4$.

Observação 4.1.1 *Embora os geradores vistos nos exemplos anteriores terem a mesma forma, como em* (3.7)*, tem-se que são distintos em cada uma das tesselações e para g fixado. Disto segue que estes geradores geram grupos fuchsianos aritméticos diferentes, entretando, pelo Teorema 4.1.1, segue que os grupos apresentados nos Exemplos 4.1.1 e 4.1.2 são isomorfos. O mesmo ocorre com os grupos obtidos nos Exemplos 4.1.3 e 4.1.4, segundo o Teorema 4.1.2. Além disso, ambos os grupos fuchsianos aritméticos são derivados da mesma álgebra dos quatérnios. No caso da tesselação* $\{16, 16\}$*, os grupos* Γ_{16} *e* Γ_{16}^* *são derivados da álgebra dos quatérnios* $\mathcal{A} = (\sqrt{2+\sqrt{2}}, -1)_{\mathbb{K}}$*, onde* $\mathbb{K} = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ *e para a tesselação* $\{10, 5\}$*, os grupos* Γ_{10}^* *e* $\Gamma_{10}^\bullet$ *são derivados da álgebra dos quatérnios* $\mathcal{A} = (\sqrt{5}, -1)_{\mathbb{K}}$*, onde* $\mathbb{K} = \mathbb{Q}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)$.

4.2 Descrição de Corpos de Números Totalmente Reais como Subcorpos de Corpos Ciclotômicos

Nosso objetivo nesta seção é associar corpos de números totalmente reais, caracterizados por expansões finitas de radicais, com subcorpos de corpos ciclotômicos. É de grande interesse trabalhar com corpos ciclotômicos pois esta classe de corpos desempenha um papel muito importante na teoria algébrica dos números uma vez que são conhecidos os anéis dos inteiros algébricos destes corpos e pode-se obter uma expressão para calcular o seu discriminante. Esta associação em que estamos interessados se dá pelo Teorema de Kronecker-Weber (Teorema 1.3.9), que diz que toda extensão abeliana finita dos racionais está contida em um corpo ciclotômico, e o menor $n \in \mathbb{N}$ tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ é chamado condutor do corpo $\mathbb{K}$ (Definição 1.3.20).

Se $\theta \in \mathbb{R}$ então pela fórmula do arco metade para cossenos da trigonometria, segue que

$$\cos\theta = \pm\sqrt{\frac{1+\cos 2\theta}{2}}. \tag{4.1}$$

Considerando $\theta = \frac{\pi}{n}$, onde $n \in \mathbb{N}$, tem-se que

$$\cos\left(\frac{\pi}{n}\right) = \sqrt{\frac{1+\cos\left(\frac{2\pi}{n}\right)}{2}} = \frac{1}{2}\sqrt{2+2\cos\left(\frac{2\pi}{n}\right)},$$

e então

$$2\cos\left(\frac{\pi}{n}\right) = \sqrt{2+2\cos\left(\frac{2\pi}{n}\right)}. \tag{4.2}$$

Agora, seja

$$\zeta_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$$

a raiz n-ésima da unidade. Assim, a raiz n-ésima da unidade real será dada por

$$\begin{array}{rcl} \zeta_n + \zeta_n^{-1} & = & e^{\frac{2\pi i}{n}} + e^{-\frac{2\pi i}{n}} \\ & = & \cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right) + \cos\left(-\frac{2\pi}{n}\right) + isen\left(-\frac{2\pi}{n}\right) \\ & = & \cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right) + \cos\left(\frac{2\pi}{n}\right) - isen\left(\frac{2\pi}{n}\right) \\ & = & 2\cos\left(\frac{2\pi}{n}\right). \end{array} \tag{4.3}$$

Assim, sejam $\mathbb{L} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ o subcorpo maximal real de $\mathbb{L}$. A partir dos conceitos trigonométricos e dos resultados sobre corpos ciclotômicos apresentados na Subseção 1.3.5, nos resultados a seguir apresentamos associações de corpos de números totalmente reais caracterizados por expansões finitas de radicais com os subcorpos $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, para valores específicos de n.

Iniciamos com o caso em que $n = 2^r$ apresentado em [21].

Proposição 4.2.1 *[21] Se $\zeta_{2^r} = e^{\frac{2\pi i}{2^r}}$ é uma raiz 2^r-ésima primitiva da unidade, com $r > 2$, então $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1}) = \mathbb{Q}(\theta)$, onde*

$$\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}},$$

contendo $r-2$ radicais.

Demonstração: Inicialmente observemos que pela Equação (4.3), segue que

$$\zeta_{2^r} + \zeta_{2^r}^{-1} = 2\cos\left(\frac{\pi}{2^{r-1}}\right). \tag{4.4}$$

Faremos a demonstração por indução sobre $r > 2$. Se $r = 3$, então pela Equação (4.4) segue que

$$\zeta_8 + \zeta_8^{-1} = 2\cos\left(\frac{\pi}{4}\right) = 2\frac{\sqrt{2}}{2} = \sqrt{2},$$

contendo 1 radical. Da mesma forma, se $r = 4$, então pela Equação (4.4) segue que

$$\zeta_{16} + \zeta_{16}^{-1} = 2\cos\left(\frac{\pi}{8}\right) = \sqrt{2 + 2\cos\frac{\pi}{8}} = \sqrt{2+\sqrt{2}},$$

contendo 2 radicais. Suponha por indução que o resultado seja válido para r, ou seja,

$$\zeta_{2^r} + \zeta_{2^r}^{-1} = 2\cos\left(\frac{\pi}{2^{r-1}}\right) = \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}, \tag{4.5}$$

contendo $r-2$ radicais. Agora, demonstraremos que o resultado é válido para $r+1$. De fato, como pela Equação (4.4),

$$\zeta_{2^{r+1}} + \zeta_{2^{r+1}}^{-1} = 2\cos\left(\frac{\pi}{2^r}\right),$$

segue pela Equação (4.2) que

$$\zeta_{2^{r+1}} + \zeta_{2^{r+1}}^{-1} = \sqrt{2 + 2\cos\left(\frac{\pi}{2^{r-1}}\right)}.$$

Logo, pela hipótese de indução, dada na Equação (4.5), segue que o resultado é válido para $r+1$, ou seja,

$$\zeta_{2^{r+1}} + \zeta_{2^{r+1}}^{-1} = \sqrt{2+\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}},$$

contendo $r+1$ radicais. Portanto, $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1}) = \mathbb{Q}(\theta)$, onde $\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}$, contendo $r-2$ radicais. ■

Agora, veremos alguns outros casos de nosso interesse, em que obtivemos relações entre subcorpos maximais reais de corpos ciclotômicos e corpos de números totalmente reais dados através de expansões finitas de radicais.

Proposição 4.2.2 *Se* $\zeta_{3.2^r} = e^{\frac{2\pi i}{3.2^r}}$ *é uma raiz* 3.2^r*-ésima primitiva da unidade, com* $r > 1$*, então* $\mathbb{K} = \mathbb{Q}(\zeta_{3.2^r} + \zeta_{3.2^r}^{-1}) = \mathbb{Q}(\theta)$*, onde*

$$\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}},$$

contendo $r-1$ *radicais.*

Demonstração: A demostração será por indução sobre $r > 1$. Observe, inicialmente, que pela Equação (4.3) segue que

$$\zeta_{3.2^r} + \zeta_{3.2^r}^{-1} = 2\cos\left(\frac{\pi}{3.2^{r-1}}\right). \tag{4.6}$$

Se $r = 2$, então pela Equação (4.6) segue que

$$\zeta_{12} + \zeta_{12}^{-1} = 2\cos\left(\frac{\pi}{6}\right) = 2\frac{\sqrt{3}}{2} = \sqrt{3},$$

contendo 1 radical. Da mesma forma, se $r = 3$, então pela Equação (4.6) segue que

$$\zeta_{24} + \zeta_{24}^{-1} = 2\cos\left(\frac{\pi}{12}\right) = \sqrt{2 + 2\cos\frac{\pi}{6}} = \sqrt{2+\sqrt{3}},$$

contendo 2 radicais. Suponhamos agora, que o resultado seja válido para r, ou seja,

$$\zeta_{3.2^r} + \zeta_{3.2^r}^{-1} = 2\cos\left(\frac{\pi}{3.2^{r-1}}\right) = \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}}, \tag{4.7}$$

contendo $r-1$ radicais. Agora, demonstraremos que o resultado é válido para $r+1$. De fato, como pela Equação (4.6),

$$\zeta_{3.2^{r+1}} + \zeta_{3.2^{r+1}}^{-1} = 2\cos\left(\frac{\pi}{3.2^r}\right),$$

segue pela Equação (4.2) que

$$\zeta_{3.2^{r+1}} + \zeta_{3.2^{r+1}}^{-1} = \sqrt{2 + 2\cos\left(\frac{\pi}{3.2^{r-1}}\right)}.$$

Logo, pela Equação (4.7), segue que o resultado é válido para $r+1$, ou seja,

$$\zeta_{3.2^{r+1}} + \zeta_{3.2^{r+1}}^{-1} = \sqrt{2+\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}}},$$

contendo r radicais. Portanto, $\mathbb{K} = \mathbb{Q}(\zeta_{3.2^r}+\zeta_{3.2^r}^{-1}) = \mathbb{Q}(\theta)$, onde $\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}}$, contendo $r-1$ radicais. ■

Proposição 4.2.3 *Se $\zeta_{5.2^r} = e^{\frac{2\pi i}{5.2^r}}$ é uma raiz 5.2^r-ésima primitiva da unidade, com $r > 1$, então $\mathbb{K} = \mathbb{Q}(\zeta_{5.2^r} + \zeta_{5.2^r}^{-1}) = \mathbb{Q}(\theta)$, onde*

$$\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}},$$

contendo r radicais.

Demonstração: A demonstração será por indução sobre $r > 1$. Observe, inicialmente, que pela Equação (4.3) segue que

$$\zeta_{5.2^r} + \zeta_{5.2^r}^{-1} = 2\cos\left(\frac{\pi}{5.2^{r-1}}\right). \tag{4.8}$$

Se $r = 2$, então pela Equação (4.8) segue que

$$\zeta_{20} + \zeta_{20}^{-1} = 2\cos\left(\frac{\pi}{10}\right) = \frac{\sqrt{10+2\sqrt{5}}}{2},$$

contendo 2 radicais, pois pela Equação (4.1), segue que

$$\cos\left(\frac{\pi}{10}\right) = \sqrt{\frac{1+\cos\left(\frac{\pi}{5}\right)}{2}} = \sqrt{\frac{1+\frac{1}{4}(1+\sqrt{5})}{2}} = \frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Da mesma forma, se $r = 3$, então pela Equação (4.8) segue que

$$\zeta_{40} + \zeta_{40}^{-1} = 2\cos\left(\frac{\pi}{20}\right) = \sqrt{2+2\cos\frac{\pi}{10}} = \sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}},$$

contendo 3 radicais. Suponhamos agora, que o resultado seja válido para r, ou seja,

$$\zeta_{5.2^r} + \zeta_{5.2^r}^{-1} = 2\cos\left(\frac{\pi}{5.2^{r-1}}\right) = \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}}, \tag{4.9}$$

contendo r radicais. Agora, demonstraremos que o resultado é válido para $r+1$. De fato, como pela Equação (4.8),

$$\zeta_{5.2^{r+1}} + \zeta_{5.2^{r+1}}^{-1} = 2\cos\left(\frac{\pi}{5.2^{r}}\right),$$

segue pela Equação (4.2) que

$$\zeta_{5.2^{r+1}} + \zeta_{5.2^{r+1}}^{-1} = \sqrt{2+2\cos\left(\frac{\pi}{5.2^{r-1}}\right)}.$$

Logo, pela Equação (4.9), segue que o resultado é válido para $r+1$, ou seja,

$$\zeta_{5.2^{r+1}} + \zeta_{5.2^{r+1}}^{-1} = \sqrt{2+\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}}},$$

contendo $r+1$ radicais. Portanto, $\mathbb{K} = \mathbb{Q}(\zeta_{5.2^r} + \zeta_{5.2^r}^{-1}) = \mathbb{Q}(\theta)$, onde

$$\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}},$$

contendo r radicais. ■

Proposição 4.2.4 *Se* $\zeta_{3.5.2^r} = e^{\frac{2\pi i}{3.5.2^r}}$ *é uma raiz* $3.5.2^r$*-ésima primitiva da unidade, com* $r > 1$*, então* $\mathbb{K} = \mathbb{Q}(\zeta_{3.5.2^r} + \zeta_{3.5.2^r}^{-1}) = \mathbb{Q}(\theta)$*, onde*

$$\theta = \sqrt{2 + \sqrt{2 + \ldots + \frac{\sqrt{7 + \sqrt{5} + \sqrt{30 + 6\sqrt{5}}}}{2}}},$$

contendo $r + 2$ *radicais.*

Demonstração: A demonstração será por indução sobre $r > 1$. Observe, inicialmente, que pela Equação (4.3), segue que

$$\zeta_{3.5.2^r} + \zeta_{3.5.2^r}^{-1} = 2\cos\left(\frac{\pi}{3.5.2^{r-1}}\right). \tag{4.10}$$

Se $r = 2$, então pela Equação (4.10) segue que

$$\zeta_{60} + \zeta_{60}^{-1} = 2\cos\left(\frac{\pi}{30}\right) = \frac{\sqrt{7 + \sqrt{5} + \sqrt{30 + 6\sqrt{5}}}}{2},$$

contendo 4 radicais, onde a última igualdade foi obtida utilizando o *software Mathematica*. Da mesma forma, se $r = 3$, então pela Equação (4.10) segue que

$$\zeta_{120} + \zeta_{120}^{-1} = 2\cos\left(\frac{\pi}{60}\right) = \sqrt{2 + 2\cos\frac{\pi}{30}} = \sqrt{2 + \frac{\sqrt{7 + \sqrt{5} + \sqrt{30 + 6\sqrt{5}}}}{2}},$$

contendo 5 radicais. Suponhamos agora, que o resultado seja válido para r, ou seja,

$$\zeta_{3.5.2^r} + \zeta_{3.5.2^r}^{-1} = 2\cos\left(\frac{\pi}{3.5.2^{r-1}}\right) = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \frac{\sqrt{7 + \sqrt{5} + \sqrt{30 + 6\sqrt{5}}}}{2}}}}, \tag{4.11}$$

contendo $r + 2$ radicais. Agora, demonstraremos que o resultado é válido para $r + 1$. De fato, como pela Equação (4.10),

$$\zeta_{3.5.2^{r+1}} + \zeta_{3.5.2^{r+1}}^{-1} = 2\cos\left(\frac{\pi}{3.5.2^r}\right),$$

segue pela Equação (4.2) que

$$\zeta_{3.5.2^{r+1}} + \zeta_{3.5.2^{r+1}}^{-1} = \sqrt{2 + 2\cos\left(\frac{\pi}{3.5.2^{r-1}}\right)}.$$

Logo, pela Equação (4.11), segue que o resultado é válido para $r + 1$, ou seja,

$$\zeta_{3.5.2^{r+1}} + \zeta_{3.5.2^{r+1}}^{-1} = \sqrt{2 + \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \frac{\sqrt{7 + \sqrt{5} + \sqrt{30 + 6\sqrt{5}}}}{2}}}}},$$

contendo $r+3$ radicais. Portanto, $\mathbb{K} = \mathbb{Q}(\zeta_{3.5.2^r} + \zeta_{3.5.2^r}^{-1}) = \mathbb{Q}(\theta)$, onde

$$\theta = \sqrt{2 + \sqrt{2 + \ldots + \frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}},$$

contendo $r+2$ radicais. ■

Através dos resultados apresentados nas Proposições 4.2.1, 4.2.2, 4.2.3 e 4.2.4, segue as seguintes relações entre subcorpos maximais reais de corpos ciclotômicos e corpos de números totalmente reais obtidos através de expansões finitas de radicais.

$$\mathbb{K} = \begin{cases} \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}\right) & \text{, com } r > 2; \\ \mathbb{Q}(\zeta_{3.2^r} + \zeta_{3.2^r}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}}\right) & \text{, com } r > 1; \\ \mathbb{Q}(\zeta_{5.2^r} + \zeta_{5.2^r}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}}\right) & \text{, com } r > 1; \\ \mathbb{Q}(\zeta_{3.5.2^r} + \zeta_{3.5.2^r}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\ldots+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}}\right) & \text{, com } r > 1. \end{cases} \tag{4.12}$$

4.3 Ordens Maximais dos Quatérnios

No decorrer desta seção consideramos álgebras dos quatérnios do tipo $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ ou do tipo $\mathcal{A} = (\theta_1, -1)_{\mathbb{K}}$, onde $\theta_1 \in \mathbb{K}$ e $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números totalmente real. Nosso objetivo é, para cada álgebra $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, obter uma ordem maximal dos quatérnios $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ é o anel dos inteiros de $\mathbb{K}$ (ou $\mathcal{M} \supseteq \mathcal{O} = (\theta_1, -1)_{\mathcal{I}_{\mathbb{K}}}$ quando $\mathcal{A} = (\theta_1, -1)_{\mathbb{K}}$).

Estas ordens maximais dos quatérnios são caracterizadas através de uma base $B = \{x_0, x_1, x_2, x_3\}$, com $x_0, x_1, x_2, x_3 \in \mathcal{I}_{\mathbb{K}}$ e as formas para estas bases B foram obtidas com o auxílio do *software Magma*. Mais precisamente, com o auxílio do *software Magma*, obtivemos a forma para base B em casos particulares e a partir de então obtemos as generalizações.

Em todos os casos que serão vistos, para comprovar que uma ordem $\mathcal{M}$ caracterizada pela base B é de fato uma ordem maximal dos quatérnios utilizamos as Proposições 2.2.1 e 2.2.5. Ou seja, para mostrar que $\mathcal{M}$ é uma ordem dos quatérnios precisamos verificar que

$$Trd(x_i), Nrd(x_i) \in \mathcal{I}_{\mathbb{K}}, \text{ para todo } x_i \in B, \text{ onde } i = 0, \ldots, 3. \tag{4.13}$$

Para mostrar que $\mathcal{M}$ é maximal, mostramos que

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}), \tag{4.14}$$

onde $\mathcal{D}(\mathcal{M})$ é o discriminante da ordem $\mathcal{M}$ e $\mathcal{D}(\mathcal{A})$ é o discriminante da álgebra $\mathcal{A}$.

Na Subseção 4.3.1, apresentamos as ordens dos quatérnios maximais para as álgebras

$$\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})} \qquad \text{e} \qquad \mathcal{A} = \left(\frac{\sqrt{10+2\sqrt{5}}}{2}, -1\right)_{\mathbb{Q}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)},$$

cujas bases associadas não apresentam a mesma forma obtida nas generalizações das álgebras dos quatérnios do tipo $\mathcal{A} = (\theta, -1)_{\mathbb{Q}(\theta)}$, generalizações estas que são apresentadas na Subseção 4.3.2. Para finalizar, na Subseção 4.3.3, apresentamos as ordens maximais dos quatérnios para as álgebras

$$\mathcal{A} = (3 + 2\sqrt{3}, -1)_{\mathbb{Q}(\sqrt{3})} \qquad \text{e} \qquad \mathcal{A} = (\sqrt{5}, -1)_{\mathbb{Q}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)},$$

que são exemplos de álgebras dos quatérnios do tipo $\mathcal{A} = (\theta_1, -1)_{\mathbb{Q}(\theta)}$, onde $\theta_1 \in \mathbb{Q}(\theta)$.

Como em todos os casos que são apresentados nas subseções subsequentes nosso objetivo é provar as condições (4.13) e (4.14), repetições de expressões se fazem necessárias a fim de tornar o processo o mais claro possível.

4.3.1 Ordens Maximais dos Quatérnios para $\mathcal{A} = (\theta, -1)_{\mathbb{K}=\mathbb{Q}(\theta)}$, onde $\theta = \sqrt{2}$ ou $\theta = \frac{\sqrt{10+2\sqrt{5}}}{2}$

Nesta subseção, apresentamos os primeiros resultados que obtivemos sobre ordens maximais dos quatérnios para as álgebras dos quatérnios

$$\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{Q}(\sqrt{2})} \qquad \text{e} \qquad \mathcal{A} = \left(\frac{\sqrt{10+2\sqrt{5}}}{2}, -1\right)_{\mathbb{Q}\left(\frac{\sqrt{10+2\sqrt{5}}}{2}\right)}.$$

Estas álgebras são casos particulares de álgebras dos quatérnios do tipo $\mathcal{A} = (\theta, -1)_{\mathbb{K}=\mathbb{Q}(\theta)}$, as quais gereralizamos suas ordens maximais dos quatérnios na Seção 4.3.2. Estes casos são mostrados separadamente, pois para $\theta = \sqrt{2}$ e $\theta = \frac{\sqrt{10+2\sqrt{5}}}{2}$, as bases associadas não apresentam a mesma forma obtida nas generalizações.

Para demonstrar os resultados a seguir mostramos que as bases obtidas para estas ordens satisfazem as condições (4.13) e (4.14).

Teorema 4.3.1 *Se $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ é uma álgebra dos quatérnios, onde $\theta = \sqrt{2}$, $\mathbb{K} = \mathbb{Q}(\theta)$ e $m = [\mathbb{K} : \mathbb{Q}] = 2$, então $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ caracterizada pela base*

$$B = \left\{1, i, \frac{1}{2}((\theta+1) + \theta i + j), \frac{1}{2}((\theta+1)i + k)\right\}$$

é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$.

Demonstração: Inicialmente mostraremos que $\mathcal{M}$ é caracterizada através da base B é de fato uma ordem. Pela Proposição 2.2.1, segue que $\mathcal{M}$ é uma ordem se, e somente se, todo elemento em $\mathcal{M}$ é inteiro, ou seja,

$$x \in \mathcal{M} \Leftrightarrow Trd(x), Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}].$$

Mostraremos este fato para os elementos de B, pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. De fato, tem-se que

$$
\begin{array}{ccc}
Trd(1) = 2 & , & Nrd(1) = 1 \\
Trd(i) = 0 & , & Nrd(i) = -\sqrt{2} \\
Trd(\frac{1}{2}((\sqrt{2}+1)+\sqrt{2}i+j)) = \sqrt{2}+1 & , & Nrd(\frac{1}{2}((\sqrt{2}+1)+\sqrt{2}i+j)) = 1 \\
Trd(\frac{1}{2}((\sqrt{2}+1)i+ij)) = 0 & , & Nrd(\frac{1}{2}((\sqrt{2}+1)i+ij)) = -\sqrt{2}-1.
\end{array}
$$

Logo, $Trd(x), Nrd(x) \in \mathbb{Z}[\sqrt{2}]$, para todo $x \in B$ e assim, $\mathcal{M}$ é uma ordem. Falta mostrar que é maximal. Para isso, pela Proposição 2.2.5, segue que precisamos verificar que

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}).$$

No Exemplo 2.2.4, vimos que o único ideal primo que se ramifica em $\mathcal{A}$ é o ideal $\mathfrak{p} = \sqrt{2}$, ou seja,

$$\mathcal{D}(\mathcal{A}) = \langle\sqrt{2}\rangle.$$

De acordo com a Proposição 2.2.6 e por (2.12), segue que o discriminante de $\mathcal{M}$ é dado por

$$
\begin{aligned}
\mathcal{D}(\mathcal{M}) &= (x_1x_2 - x_2x_1)\bar{x_3} - x_3(\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1}) \\
&= (i.\tfrac{1}{2}((\theta+1)+\theta i+j) - \tfrac{1}{2}((\theta+1)+\theta i+j).i)\tfrac{1}{2}((-\theta+1)i-k) - \\
&\quad \tfrac{1}{2}((\theta+1)i+k)(-i.\tfrac{1}{2}((\theta+1)-\theta i-j) - \tfrac{1}{2}((\theta+1)+\theta i+j).-i) \\
&= (\tfrac{1}{2}ij - \tfrac{1}{2}ji)(-\tfrac{1}{2}((\theta+1)i+k) - \tfrac{1}{2}((\theta+1)i+k)(\tfrac{1}{2}ij - \tfrac{1}{2}ji) \\
&= -\tfrac{1}{2}(\theta+1)ki - \tfrac{1}{2}k^2 - \tfrac{1}{2}(\theta+1)ik - \tfrac{1}{2}k^2 \\
&= -k^2 \ = \ -\theta \ = \ -\sqrt{2}.
\end{aligned}
$$

Logo,

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}) = \langle\sqrt{2}\rangle.$$

Portanto, $\mathcal{M}$ é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$ caracterizada pela base B. ■

A ordem maximal dos quatérnios $\mathcal{M} \supseteq \mathcal{O} = (\sqrt{2}, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$ caracterizada pela base

$$B = \left\{1, i, \frac{1}{2}((\sqrt{2}+1)+\sqrt{2}i+j), \frac{1}{2}((\sqrt{2}+1)i+k)\right\},$$

obtida no Teorema 4.3.1, produz um reticulado hiperbólico completo quando é associada ao grupo fuchsiano aritmético Γ_8, proveniente da tesselação $\{8, 8\}$, independente do emparelhamento utilizado.

Teorema 4.3.2 *Se $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ é uma álgebra dos quatérnios, onde $\theta = \frac{\sqrt{10+2\sqrt{5}}}{2}$, $\mathbb{K} = \mathbb{Q}(\theta)$ e $m = [\mathbb{K} : \mathbb{Q}] = 4$, então $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, caracterizada pela base*

$$B = \left\{1, i, \frac{1}{2}(\theta^3 + j), -\frac{1}{2\theta}((\theta^3 - 2)i + k)\right\}$$

é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$.

Demonstração: Inicialmente mostraremos que $\mathcal{M}$ caracterizada através da base B é de fato uma ordem. Pela Proposição 2.2.1, segue que $\mathcal{M}$ é uma ordem se, e somente se, todo elemento em $\mathcal{M}$ é inteiro, ou seja,

$$x \in \mathcal{M} \Leftrightarrow Trd(x), Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}\left[\frac{\sqrt{10+2\sqrt{5}}}{2}\right].$$

Mostraremos este fato para os elementos de B, pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. De fato, tem-se que

$$\begin{array}{ccc}
Trd(1) = 2 & , & Nrd(1) = 1 \\
Trd(i) = 0 & , & Nrd(i) = -\theta \\
Trd(\frac{1}{2}(\theta^3 + j)) = \theta^3 & , & Nrd(\frac{1}{2}(\theta^3 + j)) = 5\theta^2 - 6 \\
Trd(-\frac{1}{2\theta}((\theta^3 - 2)i + k)) = 0 & , & Nrd(-\frac{1}{2\theta}((\theta^3 - 2)i + k)) = -\theta^3 + \theta^2.
\end{array}$$

Logo, $Trd(x), Nrd(x) \in \mathbb{Z}\left[\frac{\sqrt{10+2\sqrt{5}}}{2}\right]$, para todo $x \in B$ e assim, $\mathcal{M}$ é uma ordem. Falta mostrar que é maximal. Para isso, pela Proposição 2.2.5, segue que precisamos verificar que

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}).$$

Como a álgebra $\mathcal{A}$ é não ramificada, segue que $\mathcal{D}(\mathcal{A}) = \langle 1 \rangle$. De acordo com a Proposição 2.2.6 e por (2.12), segue que o discriminante de $\mathcal{M}$ é dado por

$$\begin{aligned}
\mathcal{D}(\mathcal{M}) &= (x_1x_2 - x_2x_1)\bar{x_3} - x_3(\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1}) \\
&= (i.\tfrac{1}{2}(\theta^3 + j) - \tfrac{1}{2}(\theta^3 + j).i)\tfrac{1}{2\theta}((\theta^3 - 2)i + k) - \\
&\quad + \tfrac{1}{2\theta}((\theta^3 - 2)i + k)(-i.\tfrac{1}{2}(\theta^3 - j) - \tfrac{1}{2}(\theta^3 - j).(-i)) \\
&= (\tfrac{1}{2}ij - \tfrac{1}{2}ji)(-\tfrac{1}{2\theta}((\theta^3 - 2)i + k)) + \tfrac{1}{2\theta}((\theta^3 - 2)i + k)(\tfrac{1}{2}ij - \tfrac{1}{2}ji) \\
&= \tfrac{1}{2\theta}(\theta^3 - 2)ki - \tfrac{1}{2\theta}k^2 + \tfrac{1}{2\theta}(\theta^3 - 2)ik + \tfrac{1}{2\theta}k^2 \\
&= -\tfrac{k^2}{\theta} = 1.
\end{aligned}$$

Logo,

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}) = \langle 1 \rangle.$$

Portanto, $\mathcal{M}$ é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$ caracterizada pela base B. ■

A ordem maximal dos quatérnios $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ e $\theta = \frac{\sqrt{10+2\sqrt{5}}}{2}$, caracterizada pela base

$$B = \left\{1, i, \frac{1}{2}(\theta^3 + j), -\frac{1}{2\theta}((\theta^3 - 2)i + k)\right\},$$

obtida no Teorema 4.3.2, produz um reticulado hiperbólico completo quando é associada ao grupo fuchsiano aritmético Γ_{20}, proveniente da tesselação $\{20, 20\}$, independente do emparelhamento utilizado.

4.3.2 Generalizações das Ordens Maximais dos Quatérnios para $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$

Sejam $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ uma álgebra dos quatérnios, onde $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números álgebricos totalmente real e $m = [\mathbb{K} : \mathbb{Q}]$ pode ser dado através do grau do polinômio minimal $p(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$, com $a_i \in \mathbb{Z}$, associado a θ. Nosso objetivo, nesta seção, é obter uma ordem maximal dos quatérnios $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ para a álgebra $\mathcal{A}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ é o anel dos inteiros de $\mathbb{K}$.

Estamos interessados em obter ordens maximais dos quatérnios para as álgebras dos quatérnios via os grupos fuchsianos aritméticos obtidos no Capítulo 3. Alguns valores de θ que foram utilizados para obter estes grupos na Seção 3.3, associados à tesselação auto-dual $\{4g, 4g\}$ e utilizando álgebras dos quatérnios do tipo $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, são dados abaixo:

$$\theta = \begin{cases} \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}} & \text{, contendo } n \text{ radicais e } m = 2^n; \\ \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}} & \text{, contendo } n+1 \text{ radicais e } m = 2^{n+1},\ n \geq 1; \\ \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}} & \text{, contendo } n+2 \text{ radicais e } m = 2^{n+2}; \\ \sqrt{2+\sqrt{2+\ldots+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}} & \text{, contendo } n+3 \text{ radicais e } m = 2^{n+3}. \end{cases} \tag{4.15}$$

Os corpos de números $\mathbb{K} = \mathbb{Q}(\theta)$, para os valores de θ dados acima também podem ser escritos como subcorpos maximais reais de corpos ciclotômicos, como apresentado na Seção 4.2 em (4.12).

De agora em diante, mostraremos resultados que fornecem as ordens maximais dos quatérnios para álgebras dos quatérnios do tipo $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ e para os valores de θ dados em (4.15). Na Seção 4.3.1, vimos os casos particulares quando $\theta = \sqrt{2}$ e $\theta = \frac{\sqrt{10+2\sqrt{5}}}{2}$. A seguir, apresentamos as generalizações das ordens maximais dos quatérnios através da generalização da base B destas ordens.

Como já mencionamos para mostrar que $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ é uma ordem dos quatérnios caracterizada por uma base B, pela Proposição 2.2.1, tem-se que verificar se todo elemento de

$\mathcal{M}$ é inteiro em $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$. Precisamos mostrar este fato para os elementos da base B, pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. No caso do traço dos elementos da base podemos mostrar de uma forma geral que $Trd(x) \in \mathcal{I}_{\mathbb{K}}$, para todo $x \in B$, qualquer que seja o valor de $m = [\mathbb{K} : \mathbb{Q}]$. Porém, para o caso da norma dos elementos da base não podemos afirmar que este fato é valido para qualquer valor de m. Assim, para o caso da norma devemos mostrar que $Nrd(x) \in \mathcal{I}_{\mathbb{K}}$, para todo $x \in B$, para cada valor de m e θ, pré-fixados.

Além disso, da mesma forma como procedemos para os casos particulares, para mostrar que $\mathcal{M}$ é maximal, precisamos verificar se o discriminante de $\mathcal{M}$ satisfaz a condição (4.14), ou seja, que $\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A})$. Pela Definição 2.2.13, segue que o discriminante reduzido de $\mathcal{A}$ é o ideal gerado pelo produto dos primos que se ramificam em $\mathcal{A}$. Assim, uma maneira de calcular o discriminante de uma álgebra dos quatérnios $\mathcal{A}$, é utilizar o símbolo de Hilbert $\left(\frac{a,b}{\mathcal{P}}\right)$, visto na Definição 2.2.9, já que uma álgebra dos quatérnios $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$ é ramificada no ideal $\mathcal{P}$ se, e somente se, $\left(\frac{\alpha,\beta}{\mathcal{P}}\right) = -1$. Devido a complexidade algébrica envolvida para mostrar este fato para valores de $m \neq 2$, utilizamos o *software Magma* para fornecer o valor do discriminante $\mathcal{D}(\mathcal{A})$, ou seja, para mostrar que $\mathcal{A}$ é não ramifcada. Sendo assim, utilizando o *software Magma*, obtivemos que para as álgebras que são apresentadas nos resultados que seguem, $\mathcal{D}(\mathcal{A}) = \langle 1 \rangle$, ou seja, $\mathcal{A}$ é não ramificada.

Agora, estamos em condições de apresentar os resultados que fornecem as generalizações das ordens maximais dos quatérnios para os valores de θ mostrados em (4.15).

Teorema 4.3.3 *Seja $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ uma álgebra dos quatérnios, onde*

$$\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2}}}$$

contendo n radicais, $n > 1$, $\mathbb{K} = \mathbb{Q}(\theta)$ e $m = [\mathbb{K} : \mathbb{Q}] = 2^n$. Considere a base dada por

$$B = \left\{1, i, \frac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) + \theta^{m-1} i + j),\right.$$

$$\left. -\frac{1}{2\theta}(2 + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3})i + k)\right\}.$$

Se $Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$, então $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$ caracterizada pela base B.

Demonstração: Inicialmente, mostraremos que $\mathcal{M}$ caracterizada através da base B é de fato uma ordem. Pela Proposição 2.2.1, segue que $\mathcal{M}$ é uma ordem se, e somente se, todo elemento em $\mathcal{M}$ é inteiro. Mostraremos este fato para os elementos de B pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. Para a norma, segue por hipótese que

$$Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta], \text{ para todo } x \in B.$$

Resta mostrar que $Trd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$.

- Para $x_0 = 1 \in B$, tem-se que

$$Trd(x_0) = 1 + 1 = 2 \in \mathcal{I}_{\mathbb{K}}.$$

- Para $x_1 = i \in B$, tem-se que

$$Trd(x_1) = i + (-i) = 0 \in \mathcal{I}_{\mathbb{K}}.$$

- Para $x_2 = \frac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) + \theta^{m-1}i + j) \in B$, tem-se que

$$\begin{aligned} Trd(x_2) &= \tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) + \theta^{m-1}i + j) \\ &\quad + \tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) - \theta^{m-1}i - j) \\ &= \theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3} \in \mathcal{I}_{\mathbb{K}}. \end{aligned}$$

- Para $x_3 = -\frac{1}{2\theta}(2 + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3})i + k) \in B$, inicialmente consideremos o polinômio minimal associado a $\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2}}}$ dado por

$$p(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + 2, \text{ onde } a_i \in \mathbb{Z}.$$

Assim, tem-se que

$$\theta^m + a_{m-1}\theta^{m-1} + \ldots + a_1\theta + 2 = 0,$$

e portanto,

$$\theta(\theta^{m-1} + a_{m-1}\theta^{m-2} + \ldots + a_1) = -2,$$

e assim,

$$\theta^{m-1} + a_{m-1}\theta^{m-2} + \ldots + a_1 = -\frac{2}{\theta}.$$

Deste modo,

$$\begin{aligned} Trd(x_3) &= -\tfrac{1}{2\theta}(2 + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3})i + k) \\ &\quad - \tfrac{1}{2\theta}(2 - (\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3})i - k) \\ &= -\tfrac{1}{\theta} - \tfrac{1}{\theta} = -\tfrac{2}{\theta} = \theta^{m-1} + a_{m-1}\theta^{m-2} + \ldots + a_1 \in \mathcal{I}_{\mathbb{K}}. \end{aligned}$$

Logo, $\mathcal{M}$ caracterizada pela base B é uma ordem. Falta mostrar que é maximal. Para isso, de acordo com a Proposição 2.2.5, segue que precisamos verificar que

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Tem-se que:

$$\begin{aligned} x_1x_2 - x_2x_1 &= i.\tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) + \theta^{m-1}i + j) \\ &\quad - \tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) + \theta^{m-1}i + j).i \\ &= \tfrac{1}{2}ij - \tfrac{1}{2}ji = ij = k, \end{aligned}$$

e

$$\begin{aligned}\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1} &= -i.\tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) - \theta^{m-1}i - j)\\ &\quad -\tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) - \theta^{m-1}i - j).i\\ &= \tfrac{1}{2}ij - \tfrac{1}{2}ji = ij = k.\end{aligned}$$

Assim, de acordo com a Proposição 2.2.6 e por (2.12), segue que o discriminante de $\mathcal{M}$ é dado por

$$\begin{aligned}\mathcal{D}(\mathcal{M}) &= (x_1x_2 - x_2x_1)\bar{x_3} - x_3(\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1})\\ &= k.\tfrac{1}{2\theta}(2 + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3})i + k)\\ &\quad +\tfrac{1}{2\theta}(2 + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3})i + k).k\\ &= \tfrac{1}{2\theta}k^2 + \tfrac{1}{2\theta}k^2 = \tfrac{k^2}{\theta} = 1.\end{aligned}$$

Logo,

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Portanto, $\mathcal{M}$ caracterizada pela base B é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$. ■

As ordens maximais dos quatérnios descritas através do Teorema 4.3.3 quando associadas, via isomorfismo, com os elementos do grupo fuchsiano aritmético Γ_{4g} proveniente da tesselação $\{4g, 4g\}$, para $g = 2^n$ com $n > 1$, podem ser definidas como um reticulado hiperbólico completo, pois produzem um rotulamento completo dos pontos da constelação de sinais associada, onde o grupo fuchsiano aritmético Γ_{4g} foi obtido na Seção 3.3 e não depende do tipo de emparelhamento utilizado.

Exemplo 4.3.1 *Consideremos a álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ e a ordem dos quatérnios $\mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, ambas com a base usual*

$$\{1, i, j, k\}, \text{ com } i^2 = \theta, \ j^2 = -1 \text{ e } k = ij = -ji,$$

onde $\theta = \sqrt{2 + \sqrt{2}}$, $\mathbb{K} = \mathbb{Q}(\theta)$, $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ e $[\mathbb{K} : \mathbb{Q}] = 4$. Agora, consideremos outra base dada por

$$B = \left\{1, i, \frac{1}{2}((\theta^3 + \theta^2 + 1) + \theta^3 i + j), -\frac{1}{2\theta}(2 + (\theta^3 + \theta^2 - 1)i + k)\right\}.$$

Vamos calcular a norma reduzida dos elementos de B. Tem-se que

$$Nrd(1) = 1$$

$$Nrd(i) = -\theta$$

$$Nrd(\tfrac{1}{2}((\theta^3 + \theta^2 + 1) + \theta^3 i + j)) = -\theta^3 + 5\theta^2 + \theta - 2$$

$$Nrd(-\tfrac{1}{2\theta}(2 + (\theta^3 + \theta^2 - 1)i + k)) = -\theta^3 - 2\theta^2 + 3.$$

Logo, $Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$. Portanto, pelo Teorema 4.3.3, segue que $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ caracterizada pela base B é uma ordem maximal dos quatérnios para a álgebra

$\mathcal{A}$. Esta ordem maximal dos quatérnios é um reticulado hiperbólico completo quando associado ao grupo fuchsiano aritmético Γ_{16}, proveniente da tesselação $\{16, 16\}$.

Teorema 4.3.4 *Seja $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ uma álgebra dos quatérnios, onde*

$$\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \sqrt{3}}}}$$

contendo $n+1$ radicais, $n > 0$, $\mathbb{K} = \mathbb{Q}(\theta)$ e $m = [\mathbb{K} : \mathbb{Q}] = 2^{n+1}$. Considere a base dada por

$$B = \left\{1, -\frac{1}{\theta}i, \frac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}}) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1)i + j),\right.$$

$$\left.\frac{1}{2}(\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}})i + k)\right\}.$$

Se $Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$, então $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$ caracterizada pela base B.

Demonstração: Inicialmente mostraremos que $\mathcal{M}$ caracterizada através da base B é de fato uma ordem. Pela Proposição 2.2.1, segue que $\mathcal{M}$ é uma ordem se, e somente se, todo elemento em $\mathcal{M}$ é inteiro. Mostraremos este fato para os elementos de B, pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. Para a norma, tem-se por hipótese que

$$Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta], \text{ para todo } x \in B.$$

Resta mostrar que $Trd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$.

- Para $x_0 = 1 \in B$, tem-se que

$$Trd(x_0) = 1 + 1 = 2 \in \mathcal{I}_{\mathbb{K}}.$$

- Para $x_1 = -\frac{1}{\theta}i \in B$, tem-se que

$$Trd(x_1) = -\frac{1}{\theta}i + \frac{1}{\theta}i = 0 \in \mathcal{I}_{\mathbb{K}}.$$

- Para $x_2 = \frac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}}) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1)i + j) \in B$, tem-se que

$$\begin{aligned} Trd(x_2) &= \tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}}) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1)i + j) \\ &\quad + \tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}}) - (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1)i - j) \\ &= \theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}} \in \mathcal{I}_{\mathbb{K}}. \end{aligned}$$

- Para $x_3 = \frac{1}{2}(\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}})i + k) \in B$, tem-se que

$$\begin{aligned} Trd(x_3) &= \tfrac{1}{2}(\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}})i + k) \\ &\quad + \tfrac{1}{2}(\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1) - (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}})i - k) \\ &= \theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 \in \mathcal{I}_{\mathbb{K}}. \end{aligned}$$

Logo, $\mathcal{M}$ caracterizada pela base B é uma ordem. Falta mostrar que é maximal. Para isso, de acordo com a Proposição 2.2.5, segue que precisamos verificar que

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Tem-se que

$$\begin{aligned} x_1x_2 - x_2x_1 &= -\tfrac{1}{\theta}i.\tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}}) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1)i + j) \\ &\quad -\tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}}) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1)i + j).(-\tfrac{1}{\theta}i) \\ &= -\tfrac{1}{2\theta}ij + \tfrac{1}{2\theta}ji = -\tfrac{k}{\theta}, \end{aligned}$$

e

$$\begin{aligned} \bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1} &= \tfrac{1}{\theta}i.\tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}}) - (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1)i - j) \\ &\quad -\tfrac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}}) - (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1)i - j).\tfrac{1}{\theta}i \\ &= -\tfrac{1}{2\theta}ij + \tfrac{1}{2\theta}ji = -\tfrac{k}{\theta}. \end{aligned}$$

Assim, de acordo com a Proposição 2.2.6 e por (2.12), segue que o discriminante de $\mathcal{M}$ é dado por

$$\begin{aligned} \mathcal{D}(\mathcal{M}) &= (x_1x_2 - x_2x_1)\bar{x_3} - x_3(\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1}) \\ &= -\tfrac{k}{\theta}.\tfrac{1}{2}(\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1) + (\theta^{m-1} - \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}})i - k) \\ &\quad -\tfrac{1}{2}(\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1) + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta + 1 - \theta^{m-\frac{m}{2}})i + k).(-\tfrac{k}{\theta}) \\ &= \tfrac{1}{2\theta}k^2 + \tfrac{1}{2\theta}k^2 = \tfrac{k^2}{\theta} = 1. \end{aligned}$$

Logo,

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Portanto, $\mathcal{M}$ caracterizada pela base B é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$. ■

As ordens maximais dos quatérnios descritas através do Teorema 4.3.4 quando associadas, via isomorfismo, com os elementos do grupo fuchsiano aritmético Γ_{4g} proveniente da tesselação $\{4g, 4g\}$, para $g = 3.2^n$ com $n > 0$, podem ser definidas como um reticulado hiperbólico completo, pois produzem um rotulamento completo dos pontos da constelação de sinais associada, onde o grupo uchsiano aritmético Γ_{4g} foi obtido na Seção 3.3 e não depende do tipo de emparelhamento utilizado.

Exemplo 4.3.2 *Consideremos a álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ e a ordem dos quatérnios $\mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, ambas com a base usual*

$$\{1, i, j, k\}, \ \text{com } i^2 = \theta, \ j^2 = -1 \text{ e } k = ij = -ji,$$

onde $\theta = \sqrt{2 + \sqrt{2 + \sqrt{3}}}$, $\mathbb{K} = \mathbb{Q}(\theta)$, $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ e $[\mathbb{K} : \mathbb{Q}] = 8$. Agora, consideremos outra base dada por

$$B = \left\{1, -\frac{1}{\theta}i, \frac{1}{2}((\theta^7 + \theta^6 + \theta^5 + \theta^3 + \theta^2 + \theta + 1) + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1)i + j),\right.$$
$$\left.\frac{1}{2}((\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1) + (\theta^7 + \theta^6 + \theta^5 + \theta^3 + \theta^2 + \theta + 1)i + k)\right\}.$$

Vamos calcular a norma reduzida dos elementos de B. Tomando

$x_0 = 1$;
$x_1 = -\frac{1}{\theta}i$;

$x_2 = \frac{1}{2}((\theta^7 + \theta^6 + \theta^5 + \theta^3 + \theta^2 + \theta + 1) + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1)i + j)$;

$x_3 = \frac{1}{2}((\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1) + (\theta^7 + \theta^6 + \theta^5 + \theta^3 + \theta^2 + \theta + 1)i + k)$,

segue que

$$Nrd(x_0) = 1 \ ; \ Nrd(x_1) = \theta^7 - 8\theta^5 + 20\theta^3 - 16\theta$$

$$Nrd(x_2) = -319\theta^7 - 317\theta^6 + 1172\theta^4 - 1102\theta^3 - 1098\theta^2 + 70\theta + 70;$$

$$Nrd(x_3) = -268\theta^7 - 162\theta^6 + 1019\theta^5 + 637\theta^4 - 963\theta^3 - 611\theta^2 + 61\theta + 39.$$

Logo, $Nrd(x_i) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x_i \in B$, onde $i = 0, \ldots, 3$. Portanto, pelo Teorema 4.3.4, segue que $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ caracterizada pela base B é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$. Esta ordem maximal dos quatérnios é um reticulado hiperbólico completo quando associado ao grupo fuchsiano aritmético Γ_{48}, proveniente da tesselação $\{48, 48\}$.

Teorema 4.3.5 *Seja $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ uma álgebra dos quatérnios, onde*

$$\theta = \sqrt{2 + \sqrt{2 + \ldots + \sqrt{2 + \frac{\sqrt{10 + 2\sqrt{5}}}{2}}}}$$

contendo $n + 2$ radicais, $n > 0$, $\mathbb{K} = \mathbb{Q}(\theta)$ e $m = [\mathbb{K} : \mathbb{Q}] = 2^{n+2}$. Considere a base dada por

$$B = \left\{1, -\frac{1}{\theta}i, \frac{1}{2}(\theta^{m-2^n} + j), \frac{1}{2}(\theta^{m-2^n}i + k)\right\}.$$

Se $Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$, então $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$ caracterizada pela base B.

Demonstração: Inicialmente, mostraremos que $\mathcal{M}$ caracterizada através da base B é de fato uma ordem. Pela Proposição 2.2.1, segue que $\mathcal{M}$ é uma ordem se, e somente se, todo elemento em $\mathcal{M}$ é inteiro. Mostraremos este fato para os elementos de B, pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. Para a norma, segue por hipótese que

$$Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta], \text{ para todo } x \in B.$$

Resta mostrar que $Trd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$.

- Para $x_0 = 1 \in B$, tem-se que
$$Trd(x_0) = 1 + 1 = 2 \in \mathcal{I}_{\mathbb{K}}.$$
- Para $x_1 = -\frac{1}{\theta}i \in B$, tem-se que
$$Trd(x_1) = -\frac{1}{\theta}i + \frac{1}{\theta}i = 0 \in \mathcal{I}_{\mathbb{K}}.$$
- Para $x_2 = \frac{1}{2}(\theta^{m-2^n} + j) \in B$, tem-se que
$$Trd(x_2) = \frac{1}{2}(\theta^{m-2^n} + j) + \frac{1}{2}(\theta^{m-2^n} - j) = \theta^{m-2^n} \in \mathcal{I}_{\mathbb{K}}.$$
- Para $x_3 = \frac{1}{2}(\theta^{m-2^n}i + k) \in B$, tem-se que
$$Trd(x_3) = \frac{1}{2}(\theta^{m-2^n}i + k) - \frac{1}{2}(\theta^{m-2^n}i + k) = 0 \in \mathcal{I}_{\mathbb{K}}.$$

Logo, $\mathcal{M}$ caracterizada pela base B é uma ordem. Falta mostrar que é maximal. Para isso, de acordo com a Proposição 2.2.5, segue que precisamos verificar que

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Assim, de acordo com a Proposição 2.2.6 e por (2.12), segue que o discriminante de $\mathcal{M}$ é dado por

$$\begin{aligned}
\mathcal{D}(\mathcal{M}) &= (x_1x_2 - x_2x_1)\bar{x_3} - x_3(\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1}) \\
&= (-\tfrac{1}{\theta}i \cdot \tfrac{1}{2}(\theta^{m-2^n} + j) - \tfrac{1}{2}(\theta^{m-2^n} + j)(-\tfrac{1}{\theta}i))(-\tfrac{1}{2}(\theta^{m-2^n}i + k)) \\
&\quad -\tfrac{1}{2}(\theta^{m-2^n}i + k)(\tfrac{1}{\theta}i \cdot \tfrac{1}{2}(\theta^{m-2^n} - j) - \tfrac{1}{2}(\theta^{m-2^n} - j) \cdot \tfrac{1}{\theta}i) \\
&= -\tfrac{k}{\theta}(-\tfrac{1}{2}(\theta^{m-2^n}i + k)) - \tfrac{1}{2}(\theta^{m-2^n}i + k)(-\tfrac{k}{\theta}) \\
&= \tfrac{1}{2\theta}k^2 + \tfrac{1}{2\theta}k^2 = \tfrac{k^2}{\theta} = 1.
\end{aligned}$$

Logo,

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Portanto, $\mathcal{M}$ caracterizada pela base B é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$. ∎

As ordens maximais dos quatérnios descritas através do Teorema 4.3.5 quando associadas, via isomorfismo, com os elementos do grupo fuchsiano aritmético Γ_{4g} proveniente da tesselação $\{4g, 4g\}$, para $g = 5.2^n$ com $n > 0$, podem ser definidas como um reticulado hiperbólico completo pois produzem um rotulamento completo dos pontos da constelação de sinais associada, onde o grupo fuchsiano aritmético Γ_{4g} foi obtido na Seção 3.3 e não depende do tipo de emparelhamento utilizado.

Exemplo 4.3.3 *Consideremos a álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ e a ordem dos quatérnios $\mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, ambas com a base usual*

$$\{1, i, j, k\}, \text{ com } i^2 = \theta,\ j^2 = -1 \text{ e } k = ij = -ji,$$

onde $\theta = \sqrt{2 + \frac{\sqrt{10+2\sqrt{5}}}{2}}$, $\mathbb{K} = \mathbb{Q}(\theta)$, $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ e $[\mathbb{K} : \mathbb{Q}] = 8$. Agora, consideremos outra base dada por

$$B = \left\{1, -\frac{1}{\theta}i, \frac{1}{2}((\theta^6 + j), \frac{1}{2}(\theta^6 i + k)\right\}.$$

Vamos calcular a norma reduzida dos elementos de B. Assim,

$$Nrd(1) = 1$$

$$Nrd(-\tfrac{1}{\theta}i) = \theta^7 - 8\theta^5 + 19\theta^3 - 12\theta$$

$$Nrd(\tfrac{1}{2}((\theta^6 + j)) = 55\theta^6 - 190\theta^4 + 133\theta^2 - 11$$

$$Nrd(\tfrac{1}{2}(\theta^6 i + k)) = -55\theta^7 + 190\theta^5 - 133\theta^3 + 11\theta.$$

Logo, $Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$. Portanto, pelo Teorema 4.3.5, $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ caracterizada pela base B é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$. Esta ordem maximal dos quatérnios é um reticulado hiperbólico completo quando associado ao grupo fuchsiano aritmético Γ_{40}, proveniente da tesselação $\{40, 40\}$.

Teorema 4.3.6 *Sejm $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ uma álgebra dos quatérnios, onde*

$$\theta = \sqrt{2 + \sqrt{2 + \ldots + \frac{\sqrt{7 + \sqrt{5} + \sqrt{30 + 6\sqrt{5}}}}{2}}}$$

contendo $n + 3$ radicais, $\mathbb{K} = \mathbb{Q}(\theta)$ e $m = [\mathbb{K} : \mathbb{Q}] = 2^{n+3}$. Considere a base dada por

$$B = \left\{1, -\frac{1}{\theta}i, \frac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n}) + j), \frac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n})i + k)\right\}.$$

Se $Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$, então $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$ caracterizada pela base B.

Demonstração: Inicialmente, mostraremos que $\mathcal{M}$ caracterizada através da base B é de fato uma ordem. Pela Proposição 2.2.1, segue que $\mathcal{M}$ é uma ordem se, e somente se, todo elemento em $\mathcal{M}$ é inteiro. Mostraremos este fato para os elementos de B, pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. Para a norma, segue por hipótese que

$$Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta], \text{ para todo } x \in B.$$

Resta mostrar que $Trd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x \in B$.

- Para $x_0 = 1 \in B$, tem-se que

$$Trd(x_0) = 1 + 1 = 2 \in \mathcal{I}_{\mathbb{K}}.$$

- Para $x_1 = -\frac{1}{\theta}i \in B$, tem-se que

$$Trd(x_1) = -\frac{1}{\theta}i + \frac{1}{\theta}i = 0 \in \mathcal{I}_{\mathbb{K}}.$$

- Para $x_2 = \frac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n}) + j) \in B$, tem-se que

$$\begin{aligned} Trd(x_2) &= \tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n}) + j) + \tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n}) - j) \\ &= \theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n} \in \mathcal{I}_{\mathbb{K}}. \end{aligned}$$

- Para $x_3 = \frac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n})i + k) \in B$, tem-se que

$$Trd(x_3) = \frac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n})i + k) - \frac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n})i + k) = 0 \in \mathcal{I}_{\mathbb{K}}.$$

Logo, $\mathcal{M}$ caracterizada pela base B é uma ordem. Falta mostrar que é maximal. Para isso, de acordo com a Proposição 2.2.5, precisamos verificar que

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Tem-se que

$$\begin{aligned} x_1x_2 - x_2x_1 &= -\tfrac{1}{\theta}i \cdot \tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n}) + j) - \tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n}) + j)(-\tfrac{1}{\theta}i) \\ &= -\tfrac{1}{2\theta}ij + \tfrac{1}{2\theta}ji = -\tfrac{k}{\theta} \end{aligned}$$

e

$$\begin{aligned} \bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1} &= \tfrac{1}{\theta}i \cdot \tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n}) - j) - \tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n}) - j) \cdot \tfrac{1}{\theta}i \\ &= -\tfrac{1}{2\theta}ij + \tfrac{1}{2\theta}ji = -\tfrac{k}{\theta}. \end{aligned}$$

Assim, de acordo com a Proposição 2.2.6 e por (2.12), segue que o discriminante de $\mathcal{M}$ é dado por

$$\begin{aligned}
\mathcal{D}(\mathcal{M}) &= (x_1x_2 - x_2x_1)\bar{x_3} - x_3(\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1}) \\
&= -\tfrac{k}{\theta}(-\tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n})i + k)) - \tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n})i + k)(-\tfrac{k}{\theta}) \\
&= \tfrac{k}{\theta}(-\tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n})i + k)) - \tfrac{1}{2}((\theta^{5\cdot 2^n} + \theta^{3\cdot 2^n} + \theta^{2^n})i + k)(-\tfrac{k}{\theta}) \\
&= \tfrac{1}{2\theta}k^2 + \tfrac{1}{2\theta}k^2 = \tfrac{k^2}{\theta} = 1.
\end{aligned}$$

Logo,

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Portanto, $\mathcal{M}$ caracterizada pela base B é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$. ■

As ordens maximais dos quatérnios descritas através do Teorema 4.3.6 quando associadas, via isomorfismo, com os elementos do grupo fuchsiano aritmético Γ_{4g} proveniente da tesselação $\{4g, 4g\}$, para $g = 3.5.2^n$, podem ser definidas como um reticulado hiperbólico completo pois produzem um rotulamento completo dos pontos da constelação de sinais associada, onde o grupo fuchsiano aritmético Γ_{4g} foi obtido na Seção 3.3 e não depende do tipo de emparelhamento utilizado.

Exemplo 4.3.4 *Consideremos a álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$ e a ordem dos quatérnios $\mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, ambas com a base usual*

$$\{1, i, j, k\}, \text{ com } i^2 = \theta,\ j^2 = -1 \text{ e } k = ij = -ji,$$

onde $\theta = \sqrt{2 + \frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}$, $\mathbb{K} = \mathbb{Q}(\theta)$, $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ e $[\mathbb{K} : \mathbb{Q}] = 16$. Agora, consideremos outra base dada por

$$B = \left\{1, -\frac{1}{\theta}i, \frac{1}{2}((\theta^{10} + \theta^6 + \theta^2) + j), \frac{1}{2}((\theta^{10} + \theta^6 + \theta^2)i + k)\right\}.$$

Vamos calcular a norma reduzida dos elementos de B. Tomando

$$x_0 = 1\ ;\ x_1 = -\tfrac{1}{\theta}i;$$

$$x_2 = \tfrac{1}{2}((\theta^{10} + \theta^6 + \theta^2) + j);$$

$$x_3 = \tfrac{1}{2}((\theta^{10} + \theta^6 + \theta^2)i + k),$$

segue que

$$Nrd(x_0) = 1\ ;\ Nrd(x_1) = \theta^{15} - 16\theta^{13} + 105\theta^{11} - 364\theta^9 + 714\theta^7 - 784\theta^5 + 440\theta^3 - 96\theta$$

$$Nrd(x_2) = -283\theta^{14} - 2738\theta^{12} + 11263\theta^{10} - 24284\theta^8 + 28252\theta^6 - 16446\theta^4 + 3668\theta^2 - 38$$

$$Nrd(x_3) = 283\theta^{15} + 2738\theta^{13} - 11263\theta^{11} + 24284\theta^9 - 28252\theta^7 + 16446\theta^5 - 3668\theta^3 + 38\theta.$$

Logo, $Nrd(x_i) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, para todo $x_i \in B$, onde $i = 0, \ldots, 3$. Portanto, pelo Teorema 4.3.6, segue que $\mathcal{M} \supseteq \mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$ caracterizada pela base B é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$. Esta ordem maximal dos quatérnios é um reticulado hiperbólico completo quando associado ao grupo fuchsiano aritmético Γ_{120}, proveniente da tesselação $\{120, 120\}$.

4.3.3 Ordens Maximais dos Quatérnios para $\mathcal{A} = (\theta_1, -1)_{\mathbb{K}=\mathbb{Q}(\theta)}$

As ordens maximais dos quatérnios vistas até agora foram obtidas para álgebras dos quatérnios do tipo $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\theta)$. Entretanto, vimos que em alguns tipos de situações em que desejamos construir grupos fuchsianos aritméticos, um outro tipo de álgebra dos quatérnios se faz necessária. Como por exemplo, quando obtivemos o grupo fuchsiano aritmético Γ_{12} no Exemplo 3.3.2, e os grupos fuchsianos aritméticos Γ_{10}^{*} e $\Gamma_{10}^{\bullet}$ através dos Exemplos 4.1.3 e 4.1.4, respectivamente. Dessa forma, a seguir veremos algumas ordens maximais dos quatérnios para álgebras dos quatérnios do tipo $\mathcal{A} = (\theta_1, -1)_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\theta)$ e $\theta_1 \in \mathbb{Q}(\theta)$.

Seguindo a mesma direção dos resultados vistos nas seções anteriores, para mostrar que as ordens que apresentamos a seguir são de fato maximais, mostraremos que estas ordens satisfazem as condições (4.13) e (4.14).

Teorema 4.3.7 *Se $\mathcal{A} = (3 + 2\theta, -1)_{\mathbb{K}}$ é uma álgebra dos quatérnios, onde $\theta = \sqrt{3}$, $\mathbb{K} = \mathbb{Q}(\theta)$, $\theta_1 = 3 + 2\theta \in \mathbb{Q}(\theta)$ e $m = [\mathbb{K} : \mathbb{Q}] = 2$, então $\mathcal{M} \supseteq \mathcal{O} = (3 + 2\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, caracterizada pela base*

$$B = \left\{1, \frac{1}{2}((-\theta + 1) + (-\theta + 1)i), \frac{1}{2}((-\theta + 1) + (-\theta + 1)j), \frac{1}{2}(1 + i + j + k)\right\}$$

é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$.

Demonstração: Inicialmente, mostraremos que $\mathcal{M}$ caracterizada através da base B é de fato uma ordem. Pela Proposição 2.2.1, segue que $\mathcal{M}$ é uma ordem se, e somente se, todo elemento em $\mathcal{M}$ é inteiro, ou seja,

$$x \in \mathcal{M} \Leftrightarrow Trd(x), Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{3}].$$

Mostraremos este fato para os elementos de B, pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. De fato, tem-se que

$$\begin{array}{ccc} Trd(1) = 2 & , & Nrd(1) = 1 \\ Trd(\frac{1}{2}((-\theta + 1) + (-\theta + 1)i)) = 1 - \theta & , & Nrd(\frac{1}{2}((-\theta + 1) + (-\theta + 1)i)) = 1 - \theta \\ Trd(\frac{1}{2}((-\theta + 1) + (-\theta + 1)j)) = 1 - \theta & , & Nrd(\frac{1}{2}((-\theta + 1) + (-\theta + 1)j)) = 2 - \theta \\ Trd(\frac{1}{2}(1 + i + j + k)) = 1 & , & Nrd(\frac{1}{2}(1 + i + j + k)) = -1 - \theta. \end{array}$$

Logo, $Trd(x), Nrd(x) \in \mathbb{Z}[\sqrt{3}]$, para todo $x \in B$ e assim $\mathcal{M}$ é uma ordem. Falta mostrar que é maximal. Para isso, pela Proposição 2.2.5, segue que precisamos verificar que

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}).$$

Procedendo de modo análogo ao Exemplo 2.2.4, mostramos que o único ideal primo que se ramifica em $\mathcal{A}$ é o ideal $\mathfrak{p} = \sqrt{3}$. Logo $\mathcal{D}(\mathcal{A}) = \langle\sqrt{3}\rangle$. Pela Proposição 2.2.6 e por (2.12), segue que o discriminante de $\mathcal{M}$ é dado por

$$\begin{aligned}\mathcal{D}(\mathcal{M}) &= (x_1x_2 - x_2x_1)\bar{x_3} - x_3(\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1}) \\ &= (-\theta+2)k\tfrac{1}{2}(1-i-j-k) - \tfrac{1}{2}(1+i+j+k)(-\theta+2)k \\ &= -(-\theta+2)k^2 = -(-\theta+2)(3+2\theta) = -\theta = -\sqrt{3}.\end{aligned}$$

Logo,

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}) = \langle\sqrt{3}\rangle.$$

Portanto, $\mathcal{M}$ é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$ caracterizada pela base B. ■

A ordem maximal dos quatérnios $\mathcal{M} \supseteq \mathcal{O} = (3+2\sqrt{3}, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{3}]$ caracterizada pela base

$$B = \left\{1, \frac{1}{2}((-\sqrt{3}+1) + (-\sqrt{3}+1)i), \frac{1}{2}((-\sqrt{3}+1) + (-\sqrt{3}+1)j), \frac{1}{2}(1+i+j+k)\right\},$$

obtida no Teorema 4.3.7, produz um reticulado hiperbólico completo quando é associada ao grupo fuchsiano aritmético Γ_{12}, proveniente da tesselação $\{4g, 4g\}$, para $g = 3$, ou seja, para a tesselação $\{12, 12\}$, independente do emparelhamento utilizado.

Teorema 4.3.8 *Se $\mathcal{A} = (\sqrt{5}, -1)_{\mathbb{K}}$ é uma álgebra dos quatérnios, onde $\mathbb{K} = \mathbb{Q}(\theta)$, $\theta_1 = \sqrt{5} \in \mathbb{Q}(\theta)$, $\theta = \frac{\sqrt{10+2\sqrt{5}}}{2}$ e $m = [\mathbb{K} : \mathbb{Q}] = 4$, então $\mathcal{M} \supseteq \mathcal{O} = (\sqrt{5}, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$, caracterizada pela base*

$$B = \left\{1, \left(-\frac{1}{2} + \theta - \frac{3}{10}\theta^3\right)(5+i), \left(2 + \frac{3}{2}\theta - \frac{1}{2}\theta^2 - \frac{1}{2}\theta^3\right)(1+j), \left(\frac{1}{2}\theta - \frac{1}{5}\theta^3\right)(5+i+5j+k)\right\}$$

é uma ordem maximal dos quatérnios para a álgebra $\mathcal{A}$.

Demonstração: Inicialmente, mostraremos que $\mathcal{M}$ caracterizada através da base B é de fato uma ordem. Pela Proposição 2.2.1, segue que $\mathcal{M}$ é uma ordem se, e somente se, todo elemento em $\mathcal{M}$ é inteiro, ou seja,

$$x \in \mathcal{M} \Leftrightarrow Trd(x), Nrd(x) \in \mathcal{I}_{\mathbb{K}} = \mathbb{Z}\left[\frac{\sqrt{10+2\sqrt{5}}}{2}\right].$$

Mostraremos este fato para os elementos de B, pois os demais elementos de $\mathcal{M}$ são obtidos por combinações lineares dos elementos de B. De fato, tem-se que

$$Trd(1) = 2;$$

$$Trd((-\tfrac{1}{2} + \theta - \tfrac{3}{10}\theta^3)(5+i)) = -5 + 10\theta - 3\theta^2;$$

$$Trd((2 + \tfrac{3}{2}\theta - \tfrac{1}{2}\theta^2 - \tfrac{1}{2}\theta^3)(1+j)) = 4 + 3\theta - \theta^2 - \theta^3;$$

$$Trd((\tfrac{1}{2}\theta - \tfrac{1}{5}\theta^3(5+i+5j+k)) = 5\theta - 2\theta^3,$$

e

$$Nrd(1) = 1;$$

$$Nrd((-\tfrac{1}{2} + \theta - \tfrac{3}{10}\theta^3)(5+i)) = 28 - 27\theta - 6\theta^2 + 8\theta^3;$$

$$Nrd((2 + \tfrac{3}{2}\theta - \tfrac{1}{2}\theta^2 - \tfrac{1}{2}\theta^3)(1+j)) = 8 + 7\theta - 2\theta^2 - 2\theta^3;$$

$$Nrd((\tfrac{1}{2}\theta - \tfrac{1}{5}\theta^3(5+i+5j+k)) = -1 + 2\theta^2.$$

Logo, $Trd(x), Nrd(x) \in \mathbb{Z}\left[\frac{\sqrt{10+2\sqrt{5}}}{2}\right]$, para todo $x \in B$ e assim, $\mathcal{M}$ é uma ordem. Falta mostrar que é maximal. Para isso, pela Proposição 2.2.5, segue que precisamos verificar que

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}).$$

Assim,

$$\begin{aligned} x_1x_2 - x_2x_1 &= ((-\tfrac{1}{2} + \theta - \tfrac{3}{10}\theta^3)(5+i)(2 + \tfrac{3}{2}\theta - \tfrac{1}{2}\theta^2 - \tfrac{1}{2}\theta^3)(1+j) \\ &\quad -(2 + \tfrac{3}{2}\theta - \tfrac{1}{2}\theta^2 - \tfrac{1}{2}\theta^3)(1+j)(-\tfrac{1}{2} + \theta - \tfrac{3}{10}\theta^3)(5+i)) \\ &= \tfrac{1}{5}(5\theta - \theta^3)k, \end{aligned}$$

e

$$\begin{aligned} \bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1} &= ((-\tfrac{1}{2} + \theta - \tfrac{3}{10}\theta^3)(5-i)(2 + \tfrac{3}{2}\theta - \tfrac{1}{2}\theta^2 - \tfrac{1}{2}\theta^3)(1-j) \\ &\quad -(2 + \tfrac{3}{2}\theta - \tfrac{1}{2}\theta^2 - \tfrac{1}{2}\theta^3)(1-j)(-\tfrac{1}{2} + \theta - \tfrac{3}{10}\theta^3)(5-i)) \\ &= \tfrac{1}{5}(5\theta - \theta^3)k. \end{aligned}$$

Pela Proposição 2.2.6 e por (2.12) , segue que o discriminante de $\mathcal{M}$ é dado por

$$\begin{aligned} \mathcal{D}(\mathcal{M}) &= (x_1x_2 - x_2x_1)\bar{x_3} - x_3(\bar{x_1}\bar{x_2} - \bar{x_2}\bar{x_1}) \\ &= \tfrac{1}{5}(5\theta - \theta^3)k(\tfrac{1}{2}\theta - \tfrac{1}{5}\theta^3(5-i-5j-k) - \tfrac{1}{5}(5\theta - \theta^3)k(\tfrac{1}{2}\theta - \tfrac{1}{5}\theta^3(5+i+5j+k) \\ &= \tfrac{1}{2}(1 + (5-2\theta^2)i - j + (5-2\theta^2)k) + \tfrac{1}{2}(1 - (5-2\theta^2)i + j - (5-2\theta^2)k) \ - \sqrt{3} \\ &= 1. \end{aligned}$$

Logo,

$$\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A}) = \langle 1 \rangle.$$

Portanto, $\mathcal{M}$ é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$ caracterizada pela base B. ■

A ordem maximal dos quatérnios $\mathcal{M} \supseteq \mathcal{O} = (\sqrt{5}, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\theta]$ e $\theta = \frac{\sqrt{10+2\sqrt{5}}}{2}$, caracterizada pela base

$$B = \left\{1, \left(-\frac{1}{2} + \theta - \frac{3}{10}\theta^3\right)(5+i), \left(2 + \frac{3}{2}\theta - \frac{1}{2}\theta^2 - \frac{1}{2}\theta^3\right)(1+j), \left(\frac{1}{2}\theta - \frac{1}{5}\theta^3\right)(5+i+5j+k)\right\},$$

obtida no Teorema 4.3.8, produz um reticulado hiperbólico completo quando é associada ao grupo fuchsiano aritmético Γ_{10}, proveniente da tesselação $\{4g+2, 2g+1\}$ para $g = 2$, ou seja, para a tesselação $\{10, 5\}$, independente do emparelhamento utilizado.

Para finalizar esta seção, exemplificamos os resultados vistos sobre ordens maximais dos quatérnios através da Tabela 4.1, onde apresentamos ordens maximais dos quatérnios para diferentes valores de θ.

θ	$\mathbb{Z}[\theta]$-base B de $\mathcal{M}$
$\sqrt{2}$	$\{1, i, \frac{1}{2}((\theta+1)+\theta i+j), \frac{1}{2}((\theta+1)i+k)\}$
$\sqrt{3}$ e $\theta_1 = 3+2\sqrt{3}$	$\{1, i, \frac{1}{2}(1+(1+\theta)i+j), \frac{1}{2}((1+\theta)+i+k)\}$
$\sqrt{2+\sqrt{2}}$	$\{1, i, \frac{1}{2}((\theta^3+\theta^2+1)+\theta^3 i+j), -\frac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)\}$
$\frac{\sqrt{10+2\sqrt{5}}}{2}$ e $\theta_1 = \sqrt{5}$	$\{1, (-\frac{1}{2}+\theta-\frac{3}{10}\theta^3)(5+i), (2+\frac{3}{2}\theta-\frac{1}{2}\theta^2-\frac{1}{2}\theta^3)(1+j), (\frac{1}{2}\theta-\frac{1}{5}\theta^3(5+i+5j+k)\}$
$\frac{\sqrt{10+2\sqrt{5}}}{2}$	$\{1, i, \frac{1}{2}(\theta^3+j), (-\frac{1}{2}\theta+\frac{1}{10}\theta^3)((\theta^3-2)i+k)\}$
$\sqrt{2+\sqrt{3}}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}((\theta^3+\theta+1)+(\theta^3+\theta^2+\theta+1)i+j), \frac{1}{2}((\theta^3+\theta^2+\theta+1)+(\theta^3+\theta+1)i+k)\}$
$\sqrt{2+\sqrt{2+\sqrt{2}}}$	$\{1, i, \frac{1}{2}((\theta^7+\theta^6+\theta^4+1)+\theta^7 i+j), -\frac{1}{2\theta}(2+(\theta^7+\theta^6+\theta^4-1)i+k)\}$
$\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}(\theta^6+j), \frac{1}{2}(\theta^6 i+k)\}$
$\sqrt{2+\sqrt{2+\sqrt{3}}}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}((\theta^7+\theta^6+\theta^5+\theta^3+\theta^2+\theta+1)+(\theta^7+\theta^6+\theta^5+\theta^4+\theta^3+\theta^2+\theta+1)i+j),$ $\frac{1}{2}((\theta^7+\theta^6+\theta^5+\theta^4+\theta^3+\theta^2+\theta+1)+(\theta^7+\theta^6+\theta^5+\theta^3+\theta^2+\theta+1)i+k)\}$
$\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}(\theta^5+\theta^3+\theta+j), \frac{1}{2}((\theta^5+\theta^3+\theta)i+k)\}$
$\sqrt{2+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}(\theta^{12}+j), \frac{1}{2}(\theta^{12}i+k)\}$
$\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{3}}}}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}((\theta^{15}+\theta^{14}+\ldots+\theta^9+\theta^7+\theta^6+\ldots+\theta+1)+(\theta^{15}+\theta^{14}+\ldots+\theta+1)i+j),$ $\frac{1}{2}((\theta^{15}+\theta^{14}+\ldots+\theta+1)+(\theta^{15}+\theta^{14}+\ldots+\theta^9+\theta^7+\theta^6+\ldots+\theta+1)i+k)\}$
$\sqrt{2+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}(\theta^{10}+\theta^6+\theta^2+j), \frac{1}{2}((\theta^{10}+\theta^6+\theta^2)i+k)\}$
$\sqrt{2+\sqrt{2+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}(\theta^{24}+j), \frac{1}{2}(\theta^{24}i+k)\}$
$\sqrt{2+\sqrt{2+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}}$	$\{1, -\frac{1}{\theta}i, \frac{1}{2}(\theta^{20}+\theta^{12}+\theta^4+j), \frac{1}{2}((\theta^{20}+\theta^{12}+\theta^4)i+k)\}$

Tabela 4.1: *Bases que caracterizam as ordens maximais dos quatérnios para diferentes valores de* θ

4.3.4 Exemplos

Para finalizar, apresentamos dois exemplos de forma completa onde explicitamos os resultados obtidos durante todo o trabalho. Acreditamos que através destes exemplos o leitor terá uma melhor compreensão do trabalho que foi desenvolvido e também irá conseguir conectar os conceitos e resultados apresentados nestes trabalho. Escolhemos para estes exemplos, a construção dos grupos Γ_8^* e Γ_{16}^*.

1. Construção do Grupo Fuchsiano Aritmético Γ_8^* Proveniente da Tesselação $\{8,8\}$ via Ordens Maximais dos Quatérnios

Neste exemplo, determinamos o grupo fuchsiano aritmético Γ_8^* proveniente da tesselação $\{4g, 4g\} = \{8, 8\}$ com $g = 2$, utilizando o emparelhamento diametralmente oposto das arestas do polígono fundamental $\mathcal{P}_8$ de 8 lados, de acordo com a Figura 4.1.

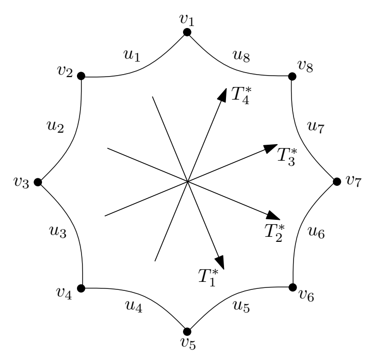

Figura 4.1: $\mathcal{P}_8$-*emparelhamento diametralmente oposto*

Consideremos $u_1, \ldots, u_8$ as arestas do polígono $\mathcal{P}_8$ dispostas em ordem cíclica no sentido anti-horário. As isometrias para este emparelhamento são T_1, T_2, T_3, T_4 tais que

$$T_i(u_i) = u_{i+4}, \quad \text{onde} \quad i = 1, \ldots, 4.$$

Por meio destes emparelhamentos, obtemos uma superfície compacta e orientável $\mathbb{D}^2/\Gamma_8^*$ de gênero 2.

A estrutura algébrica deste grupo tem a seguinte representação:

$$\Gamma_8^* = \langle T_1, T_2, T_3, T_4 : T_1 \circ T_2^{-1} \circ T_3 \circ T_4^{-1} \circ T_1^{-1} \circ T_2 \circ T_3^{-1} \circ T_4 = id \rangle. \tag{4.16}$$

Agora, aplicando passo a passo o algoritmo apresentado na Seção 3.2, encontraremos os geradores do grupo fuchsiano aritmético.

- **[Etapa 1 - Entrada]**
  Como $p = q = 8$, segue que $(p-2)(q-2) = (8-2)(8-2) = 36 > 4$.

- **[Etapa 2 - Verificar condição de Fermat]**
  Como $p = q = 8 = 2^3$, segue que p e q satisfazem a condição de Fermat, estabelecida no Teorema 3.1.3.

- **[Etapa 3 - Computar matriz A_1]**
Para o emparelhamento diametralmente oposto, de acordo com o Teorema 3.1.1, a matriz A_1 é dada por:

$$A_1 = \begin{pmatrix} \frac{2\cos\frac{\pi}{8}}{2sen\frac{\pi}{8}} & \frac{\sqrt{4\cos\frac{\pi}{4}}\cdot e^{i\frac{9\pi}{8}}}{2sen\frac{\pi}{8}} \\ \frac{\sqrt{4\cos\frac{\pi}{4}}\cdot e^{-i\frac{9\pi}{8}}}{2sen\frac{\pi}{8}} & \frac{2\cos\frac{\pi}{8}}{2sen\frac{\pi}{8}} \end{pmatrix} = \begin{pmatrix} \sqrt{3+2\sqrt{2}} & -\frac{\sqrt{3+2\sqrt{2}}+i}{2^{1/4}} \\ -\frac{\sqrt{3+2\sqrt{2}}-i}{2^{1/4}} & \sqrt{3+2\sqrt{2}} \end{pmatrix}.$$

- **[Etapa 4 - Computar matriz C e sua inversa C^{-1}]**
A matriz associada à transformação elíptica é dada por

$$C = \begin{pmatrix} e^{\frac{i\pi}{8}} & 0 \\ 0 & e^{-\frac{i\pi}{8}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(\sqrt{2+\sqrt{2}}+i\sqrt{2-\sqrt{2}}) & 0 \\ 0 & \frac{1}{2}(\sqrt{2+\sqrt{2}}-i\sqrt{2-\sqrt{2}}) \end{pmatrix},$$

e a sua inversa é dada por

$$C^{-1} = \begin{pmatrix} \frac{1}{2}(\sqrt{2+\sqrt{2}}-i\sqrt{2-\sqrt{2}}) & 0 \\ 0 & \frac{1}{2}(\sqrt{2+\sqrt{2}}+i\sqrt{2-\sqrt{2}}) \end{pmatrix}.$$

- **[Etapa 5 - Computar as demais matrizes de transformações A_i's, com $i = 2, 3, 4$]**
Para o emparelhamento diametralmente oposto, estas matrizes são obtidas da seguinte forma:

$$A_i = C^{i-1}A_1C^{-(i-1)},$$

para $i = 2, 3, 4$. Assim, tem-se que

$$A_2 = CA_1C^{-1} = \begin{pmatrix} \sqrt{3+2\sqrt{2}} & -\frac{(1+i)(\sqrt{3+2\sqrt{2}}+i)}{2^{3/4}} \\ \frac{(1+i)(\sqrt{3+2\sqrt{2}}+i)}{2^{3/4}} & \sqrt{3+2\sqrt{2}} \end{pmatrix},$$

$$A_3 = C^2A_1C^{-2} = \begin{pmatrix} \sqrt{3+2\sqrt{2}} & \frac{1-i\sqrt{3+2\sqrt{2}}}{2^{1/4}} \\ \frac{1+i\sqrt{3+2\sqrt{2}}}{2^{1/4}} & \sqrt{3+2\sqrt{2}} \end{pmatrix},$$

$$A_4 = C^3A_1C^{-3} = \begin{pmatrix} \sqrt{3+2\sqrt{2}} & \frac{(1+i)+(1-i)\sqrt{3+2\sqrt{2}}}{2^{3/4}} \\ \frac{(1+i)(\sqrt{3+2\sqrt{2}}-i)}{2^{3/4}} & \sqrt{3+2\sqrt{2}} \end{pmatrix}.$$

- **[Etapa 6 - Computar as inversas, A_i^{-1}'s, das matrizes de transformações A_i's, com $i = 1, 2, 3, 4$]**
Para as matrizes de transformações A_i's, com $i = 1, 2, 3, 4$, obtidas nas Etapas 3 e 5, tem-se que

$$A_1^{-1} = \begin{pmatrix} \sqrt{3+2\sqrt{2}} & \frac{\sqrt{3+2\sqrt{2}}+i}{2^{1/4}} \\ \frac{\sqrt{3+2\sqrt{2}}-i}{2^{1/4}} & \sqrt{3+2\sqrt{2}} \end{pmatrix},$$

$$A_2^{-1} = \begin{pmatrix} \sqrt{3+2\sqrt{2}} & \frac{(1+i)(\sqrt{3+2\sqrt{2}}+i)}{2^{3/4}} \\ \frac{(1-i)(\sqrt{3+2\sqrt{2}}-i)}{2^{3/4}} & \sqrt{3+2\sqrt{2}} \end{pmatrix},$$

$$A_3^{-1} = \begin{pmatrix} \sqrt{3+2\sqrt{2}} & -\frac{1-i\sqrt{3+2\sqrt{2}}}{2^{1/4}} \\ -\frac{1+i\sqrt{3+2\sqrt{2}}}{2^{1/4}} & \sqrt{3+2\sqrt{2}} \end{pmatrix},$$

$$A_4^{-1} = \begin{pmatrix} \sqrt{3+2\sqrt{2}} & -\frac{(1-i)(\sqrt{3+2\sqrt{2}}+i)}{2^{3/4}} \\ -\frac{(1+i)(\sqrt{3+2\sqrt{2}}-i)}{2^{3/4}} & \sqrt{3+2\sqrt{2}} \end{pmatrix}.$$

- **[Etapa 7 - Verificar condição de hiperbolicidade]**
  Considerando as matrizes A_i's, com $i = 1, 2, 3, 4$, obtidas nas Etapas 3 e 5, tem-se que

  $$t_i = tr^2(A_i) = \left(2\sqrt{3+2\sqrt{2}}\right)^2 = 4(3+2\sqrt{2}) = 12 + 8\sqrt{2} > 4,$$

  onde $i = 1, 2, 3, 4$. Logo, $t_i > 4$ para todo $i = 1, 2, 3, 4$, e portanto, todas as transformações associadas a estas matrizes são hiperbólicas.

- **[Etapa 8 - Verificar condição de Poincaré]**
  De acordo com a representação do grupo fuchsiano Γ_8^* dada em (4.16), precisamos verificar que

  $$T_1 \circ T_2^{-1} \circ T_3 \circ T_4^{-1} \circ T_1^{-1} \circ T_2 \circ T_3^{-1} \circ T_4 = id.$$

  De fato, considerando as matrizes associadas a estas tranformações, que foram obtidas nas Etapas 3,5 e 6 tem-se que

  $$A_4 A_3^{-1} A_2 A_1^{-1} A_4^{-1} A_3 A_2^{-1} A_1 = I_2,$$

  onde $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é a matriz identidade de ordem 2 e considerando a multiplicação usual de matrizes.

- **[Etapa 9 - Definir função f como matriz e computar sua inversa f^{-1} como matriz]**
  Considerando que a função $f : \mathbb{H}^2 \to \mathbb{D}^2$ é dada por

  $$f(z) = \frac{zi+1}{z+i},$$

  tem-se que

  $$F = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \text{ e } F^{-1} = \begin{pmatrix} -\frac{i}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{i}{2} \end{pmatrix}$$

- **[Etapa 10 - Computar matrizes G_i's, com $i = 1, 2, 3, 4$]**
  Utilizando as matrizes de transformações obtidas nas Etapas 3 e 5, e as matrizes associadas a função f e f^{-1}, obtidas na Etapa 9, os geradores são dados por:

  $$G_i = F A_i F^{-1},$$

  onde $i = 1, 2, 3, 4$ e considerando a operação usual de matrizes. Assim, tem-se que

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

$$G_2 = \begin{pmatrix} \frac{2+2\sqrt{2}}{2} + \frac{(2+\sqrt{2})\sqrt[4]{2}}{2} & -\frac{\sqrt{2}\sqrt[4]{2}}{2} \\ -\frac{\sqrt{2}\sqrt[4]{2}}{2} & \frac{2+2\sqrt{2}}{2} - \frac{(2+\sqrt{2})\sqrt[4]{2}}{2} \end{pmatrix}, \tag{4.17}$$

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

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

- **[Etapa 11 - Saída]**

Munidos dos geradores, veremos agora como associar o grupo fuchsiano Γ_8^* com a álgebra dos quatérnios $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, e a uma ordem maximal dos quatérnios $\mathcal{M}$ desta álgebra sobre o anel $R = \mathbb{Z}[\sqrt{2}]$, podendo assim ser definida como um reticulado hiperbólico completo. Isto será feito através da identificação dos elementos da ordem $\mathcal{M}$ com os geradores G_1, G_2, G_3, G_4 como mostrados em (4.17).

Seja $x = x_0 + x_1 i + x_2 j + x_3 ij \in \mathcal{A}$, com $i^2 = \sqrt{2},\ j^2 = -1,\ ij = -ji$ e $x_0, x_1, x_2, x_3 \in \mathbb{Q}(\sqrt{2})$. Sejam M_0, M_1, M_2, M_3 matrizes linearmente independentes de $M(2, \mathbb{K}(\sqrt{\sqrt{2}}))$, dadas por

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} \sqrt{\sqrt{2}} & 0 \\ 0 & -\sqrt{\sqrt{2}} \end{pmatrix}, M_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, M_3 = \begin{pmatrix} 0 & \sqrt{\sqrt{2}} \\ \sqrt{\sqrt{2}} & 0 \end{pmatrix}.$$

Consideremos a aplicação $\varphi : \mathcal{A} \longrightarrow M(2, \mathbb{K}(\sqrt{\sqrt{2}}))$, definida por

$$\varphi(x_0 + x_1 i + x_2 j + x_3 k) = x_0 M_0 + x_1 M_1 + x_2 M_2 + x_3 M_3.$$

Como $\varphi(i^2) = \sqrt{2} I_2,\ \varphi(j^2) = -I_2$ e $\varphi(ij) = \varphi(i)\varphi(j) = -\varphi(j)\varphi(i)$, onde $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, verifica-se que φ é um isomorfismo de $\mathcal{A}$ em uma sub-álgebra de $M(2, \mathbb{K}(\sqrt{\sqrt{2}}))$. Dessa forma, cada elemento de $\mathcal{A}$ é identificado com

$$x \longmapsto \varphi(x) = \begin{pmatrix} x_0 + x_1\sqrt{\sqrt{2}} & x_2 + x_3\sqrt{\sqrt{2}} \\ -(x_2 - x_3\sqrt{\sqrt{2}}) & x_0 - x_1\sqrt{\sqrt{2}} \end{pmatrix}. \tag{4.18}$$

Através de (4.18), vemos que os geradores obtidos em (4.17) são identificados, via o isomorfismo φ, com os seguintes elementos de $\mathcal{A}$:

$$g_1 = \frac{2+2\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i - \frac{2+\sqrt{2}}{2} ij,$$

$$g_2 = \frac{2+2\sqrt{2}}{2} + \frac{2+\sqrt{2}}{2} i - \frac{\sqrt{2}}{2} ij, \tag{4.19}$$

$$g_3 = \frac{2+2\sqrt{2}}{2} + \frac{2+\sqrt{2}}{2}i + \frac{\sqrt{2}}{2}ij,$$
$$g_4 = \frac{2+2\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i + \frac{2+\sqrt{2}}{2}ij.$$

Agora, apresentamos uma ordem maximal de $\mathcal{A}$ e associamos seus elementos com os geradores obtidos em (4.19) e, portanto em (4.17). Como visto, estamos considerando a álgebra dos quatérnios $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ e $i^2 = \sqrt{2}$, $j^2 = -1$, $ij = -ji$, com base $\{1, i, j, ij\}$.

Definimos o discriminante reduzido da álgebra dos quatérnios $\mathcal{A}$, $\mathcal{D}(\mathcal{A})$, na Definição 2.2.13, como o produto dos ideais primos que se ramificam em $\mathcal{A}$. Pelo Exemplo 2.2.4, segue que o único ideal primo que se ramifica em $\mathcal{A}$ é o ideal principal $\mathfrak{a} = \langle 0, 1\rangle \subset \mathbb{Z}[\sqrt{2}]$, ou seja,

$$\mathcal{D}(\mathcal{A}) = \langle\sqrt{2}\rangle.$$

Se $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$ é o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, então

$$\mathcal{O} = \{y_0 + y_1 i + y_2 j + y_3 ij \ : \ y_0, y_1, y_2, y_3 \in \mathbb{Z}[\sqrt{2}]\}$$

é uma ordem dos quatérnios em $\mathcal{A}$ denotada por $\mathcal{O} = (\sqrt{2}, -1)_{\mathcal{I}_{\mathbb{K}}}$ com $\mathbb{Z}$-base $\{1, i, j, ij\}$. O discriminante $\mathcal{D}(\mathcal{O})$ de $\mathcal{O}$, de acordo com o Exemplo 2.2.6, é dado por

$$\mathcal{D}(\mathcal{O}) = \sqrt{32} = 4\sqrt{2}.$$

Pelo Exemplo 2.2.7, vimos que esta ordem não é maximal.

Através do Teorema 4.3.1, mostramos que existe uma ordem $\mathcal{M} \supset \mathcal{O} = (\sqrt{2}, -1)_{\mathcal{I}_{\mathbb{K}}}$ com a seguinte base

$$B = \left\{1, i, \frac{1}{2}((\sqrt{2}+1) + \sqrt{2}i + j), \frac{1}{2}((\sqrt{2}+1)i + ij)\right\},$$

tal que $\mathcal{M}$ é uma ordem maximal dos quatérnios da álgebra dos quatérnios $\mathcal{A}$.

Agora, falta associar os elementos da ordem $\mathcal{M}$ aos elementos do grupo fuchsiano Γ_8^*, e para isso precisamos mostrar que $g_1, g_2, g_3, g_4 \in \mathcal{M}$, onde g_1, g_2, g_3, g_4 são como em (4.19). Para isso, é suficiente mostrar que g_1, g_2, g_3, g_4 podem ser escritos como combinação linear dos elementos de B.

- Para g_1, tomando $a_1 = 1+\sqrt{2}$, $b_1 = 2+2\sqrt{2}$, $c_1 = 0$, $d_1 = -2-\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, tem-se que

$$\begin{aligned} & a_1 \cdot 1 + b_1 \cdot i + c_1 \cdot \tfrac{1}{2}((\sqrt{2}+1) + \sqrt{2}i + j) + d_1 \cdot \tfrac{1}{2}((\sqrt{2}+1)i + ij) \\ = \quad & 1 + \sqrt{2} + (2+2\sqrt{2})i + 0 + (-2-\sqrt{2})(\tfrac{1}{2}((\sqrt{2}+1)i + ij)) \\ = \quad & 1 + \sqrt{2} + \tfrac{\sqrt{2}}{2} - \tfrac{2+\sqrt{2}}{2}ij = g_1. \end{aligned}$$

- Para g_2, tomando $a_2 = 1+\sqrt{2}$, $b_2 = 2+2\sqrt{2}$, $c_2 = 0$, $d_2 = -\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, tem-se que

$$\begin{aligned} & a_2 \cdot 1 + b_2 \cdot i + c_2 \cdot \tfrac{1}{2}((\sqrt{2}+1) + \sqrt{2}i + j) + d_2 \cdot \tfrac{1}{2}((\sqrt{2}+1)i + ij) \\ = \quad & 1 + \sqrt{2} + (2+\sqrt{2})i + 0 - \sqrt{2}(\tfrac{1}{2}((\sqrt{2}+1)i + ij)) \\ = \quad & 1 + \sqrt{2} + \tfrac{2+\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}ij = g_2. \end{aligned}$$

- Para g_3, tomando $a_3 = 1+\sqrt{2},\ b_3 = 0,\ c_3 = 0,\ d_3 = \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, tem-se que

$$\begin{array}{rc} & a_3 \cdot 1 + b_3 \cdot i + c_3 \cdot \frac{1}{2}((\sqrt{2}+1)+\sqrt{2}i+j) + d_3 \cdot \frac{1}{2}((\sqrt{2}+1)i+ij) \\ = & 1+\sqrt{2}+0+0+\sqrt{2}(\frac{1}{2}((\sqrt{2}+1)i+ij)) \\ = & 1+\sqrt{2}+\frac{2+\sqrt{2}}{2}+\frac{\sqrt{2}}{2}ij = g_3. \end{array}$$

- Para g_4, tomando $a_4 = 1+\sqrt{2},\ b_4 = -2-\sqrt{2},\ c_4 = 0,\ d_4 = 2+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, tem-se que

$$\begin{array}{rc} & a_4 \cdot 1 + b_4 \cdot i + c_4 \cdot \frac{1}{2}((\sqrt{2}+1)+\sqrt{2}i+j) + d_4 \cdot \frac{1}{2}((\sqrt{2}+1)i+ij) \\ = & 1+\sqrt{2}-(2+\sqrt{2})i+0+(2+\sqrt{2})(\frac{1}{2}((\sqrt{2}+1)i+ij)) \\ = & 1+\sqrt{2}+\frac{\sqrt{2}}{2}+\frac{2+\sqrt{2}}{2}ij = g_4. \end{array}$$

Logo, $g_1, g_2, g_3, g_4 \in \mathcal{M}$, ou seja, os elementos da ordem $\mathcal{M}$ podem ser associados, via isomorfismo, com os elementos do grupo fuchsiano Γ_8^*. Portanto, Γ_8^* é um grupo fuchsiano aritmético derivado da álgebra dos quatérnios $\mathcal{A} = (\sqrt{2}, -1)_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, cujos elementos são associados, via isomorfismo, com os elementos da ordem dos quatérnios maximal $\mathcal{M} \supset \mathcal{O} = (\sqrt{2}, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$.

2. Construção do Grupo Fuchsiano Aritmético Γ_{16}^* Proveniente da Tesselação $\{16, 16\}$ via Ordens Maximais dos Quatérnios

Consideremos, agora, a álgebra dos quatérnios $\mathcal{A} = (\theta, -1)_{\mathbb{K}}$, onde $\theta = \sqrt{2+\sqrt{2}}$ e $\mathbb{K} = \mathbb{Q}(\theta)$. Sendo $\mathcal{O} = (\theta, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2+\sqrt{2}}]$, a ordem usual dos quatérnios associada a $\mathcal{A}$, consideremos $\mathcal{M} \supseteq \mathcal{O}$ a sua ordem maximal dos quatérnios associada. Através do Teorema 4.3.3 e do Exemplo 4.3.1, segue que a base B que caracteriza esta ordem maximal $\mathcal{M}$ é dada por:

$$B = \left\{1, i, \frac{1}{2}(\theta^3+\theta^2+1), -\frac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)\right\}.$$

Agora, vamos mostrar que os geradores do grupo fuchsiano aritmético Γ_{16}^* podem ser associados aos elementos da ordem maximal dos quatérnios $\mathcal{M}$, podendo assim definir esta ordem maximal dos quatérnios como um reticulado hiperbólico completo.

Utilizando o emparelhamento diamentralmente oposto, no Exemplo 4.1.2 apresentamos a forma dos geradores do grupos fuchsiano aritmético Γ_{16}^*, obtidos através do algoritmo apresentado na Seção 3.2. Da mesma forma como na construção do grupo Γ_8^* visto anteriormente, através do isomorfismo definido em (4.18), segue que os geradores obtidos no Exemplo 4.1.2 , são identificados via o isomorfismo φ, com os seguintes elementos de $\mathcal{A}$:

$$g_1 = -1-2\theta+\theta^2+\theta^3+\frac{\theta^2-2}{2}i-\frac{2\theta+\theta^2}{2}k,$$

$$g_2 = -1-2\theta+\theta^2+\theta^3+\frac{-2-2\theta+\theta^2+\theta^3}{2}i+\frac{2\theta-\theta^2-\theta^3}{2}k,$$

$$g_3 = -1 - 2\theta + \theta^2 + \theta^3 + \frac{-2\theta + \theta^2 + \theta^3}{2} i - \frac{-2 - 2\theta + \theta^2 + \theta^3}{2} k,$$

$$g_4 = -1 - 2\theta + \theta^2 + \theta^3 + \frac{2\theta + \theta^2}{2} i - \frac{-2 + \theta^2}{2} k, \tag{4.20}$$

$$g_5 = -1 - 2\theta + \theta^2 + \theta^3 + \frac{2\theta + \theta^2}{2} i + \frac{-2 + \theta^2}{2} k,$$

$$g_6 = -1 - 2\theta + \theta^2 + \theta^3 + \frac{-2\theta + \theta^2 + \theta^3}{2} i + \frac{-2 - 2\theta + \theta^2 + \theta^3}{2} k,$$

$$g_7 = -1 - 2\theta + \theta^2 + \theta^3 + \frac{-2 - 2\theta + \theta^2 + \theta^3}{2} i - \frac{2\theta - \theta^2 - \theta^3}{2} k,$$

$$g_8 = -1 - 2\theta + \theta^2 + \theta^3 + \frac{\theta^2 - 2}{2} i + \frac{2\theta + \theta^2}{2} k,$$

onde $\theta = \sqrt{2 + \sqrt{2}}$. Agora, falta associar os elementos da ordem $\mathcal{M}$ aos elementos do grupo fuchsiano Γ_{16}^*, e para isso precisamos mostrar que $g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8 \in \mathcal{M}$, onde $g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8$ são como em (4.20). Para isso, é suficiente mostrar que $g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8$ podem ser escritos como combinação linear dos elementos de B.

- Para g_1, tomando $a_1 = -1-2\theta^2+\theta^3,\ b_1 = -4-2\theta+6\theta^2+3\theta^3,\ c_1 = 0,\ d_1 = 2\theta^2+\theta^3 \in \mathbb{Z}[\theta]$, tem-se que

$$\begin{aligned} & a_1 \cdot 1 + b_1 \cdot i + c_1 \cdot \tfrac{1}{2}(\theta^3 + \theta^2 + 1) + d_1 \cdot (-\tfrac{1}{2\theta}(2 + (\theta^3 + \theta^2 - 1)i + k)) \\ = \ & -1 - 2\theta^2 + \theta^3 + (-4 - 2\theta + 6\theta^2 + 3\theta^3)i + 0 + (2\theta^2 + \theta^3)(-\tfrac{1}{2\theta}(2 + (\theta^3 + \theta^2 - 1)i + k)) \\ = \ & -1 - 2\theta + \theta^2 + \theta^3 + \tfrac{\theta^2 - 2}{2} i - \tfrac{2\theta + \theta^2}{2} k = g_1. \end{aligned}$$

- Para g_2, tomando $a_2 = -1 - 4\theta + 2\theta^2 + 2\theta^3,\ b_2 = -4 - 2\theta + 5\theta^2 + 3\theta^3,\ c_2 = 0,\ d_2 = -2 + 2\theta^2 + \theta^3 \in \mathbb{Z}[\theta]$, tem-se que

$$\begin{aligned} & a_2 \cdot 1 + b_2 \cdot i + c_2 \cdot \tfrac{1}{2}(\theta^3 + \theta^2 + 1) + d_2 \cdot (-\tfrac{1}{2\theta}(2 + (\theta^3 + \theta^2 - 1)i + k)) \\ = \ & -1 - 4\theta + 2\theta^2 + 2\theta^3 + (-4 - 2\theta + 5\theta^2 + 3\theta^3)i + (-2 + 2\theta^2 + \theta^3)(-\tfrac{1}{2\theta}(2 + (\theta^3 + \theta^2 - 1)i + k)) \\ = \ & -1 - 2\theta + \theta^2 + \theta^3 + \tfrac{-2-2\theta+\theta^2+\theta^3}{2} i + \tfrac{2\theta - \theta^2 - \theta^3}{2} k = g_2. \end{aligned}$$

- Para g_3, tomando $a_3 = -3 - 4\theta + 2\theta^2 + 2\theta^3,\ b_3 = -2 - 2\theta + 4\theta^2 + 2\theta^3,\ c_3 = 0,\ d_3 = -2 - 2\theta + \theta^2 + \theta^3 \in \mathbb{Z}[\theta]$, tem-se que

$$\begin{aligned} & a_3 \cdot 1 + b_3 \cdot i + c_3 \cdot \tfrac{1}{2}(\theta^3 + \theta^2 + 1) + d_3 \cdot (-\tfrac{1}{2\theta}(2 + (\theta^3 + \theta^2 - 1)i + k)) \\ = \ & -3 - 4\theta + 2\theta^2 + 2\theta^3 + (-2 - 2\theta + 4\theta^2 + 2\theta^3)i + (-2 - 2\theta + \theta^2 + \theta^3)(-\tfrac{1}{2\theta}(2 + (\theta^3 + \theta^2 - 1)i + k \\ = \ & -1 - 2\theta + \theta^2 + \theta^3 + \tfrac{-2\theta+\theta^2+\theta^3}{2} i - \tfrac{-2-2\theta+\theta^2+\theta^3}{2} k = g_3. \end{aligned}$$

- Para g_4, tomando $a_4 = -3-2\theta+2\theta^2+\theta^3,\ b_4 = \theta^2+\theta^3,\ c_4 = 0,\ d_4 = -2\theta+\theta^3 \in \mathbb{Z}[\theta]$, tem-se que

$$\begin{aligned} & a_4\cdot 1 + b_4\cdot i + c_4\cdot \tfrac{1}{2}(\theta^3+\theta^2+1) + d_4\cdot(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& -3-2\theta+2\theta^2+\theta^3+(\theta^2+\theta^3)i+0+(-2\theta+\theta^3)(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& -1-2\theta+\theta^2+\theta^3+\tfrac{2\theta+\theta^2}{2}i-\tfrac{-2+\theta^2}{2}k = g_4. \end{aligned}$$

- Para g_5, tomando $a_5 = 1-2\theta+\theta^3,\ b_5 = 2\theta-\theta^3,\ c_5 = 0,\ d_5 = 2\theta-\theta^3 \in \mathbb{Z}[\theta]$, tem-se que

$$\begin{aligned} & a_5\cdot 1 + b_5\cdot i + c_5\cdot \tfrac{1}{2}(\theta^3+\theta^2+1) + d_5\cdot(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& 1-2\theta+\theta^3+(2\theta-\theta^3)i+0+(2\theta-\theta^3)(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& -1-2\theta+\theta^2+\theta^3+\tfrac{2\theta+\theta^2}{2}i+\tfrac{-2+\theta^2}{2}k = g_5. \end{aligned}$$

- Para g_6, tomando $a_6 = 1,\ b_6 = 2-3\theta^2-\theta^3,\ c_6 = 0,\ d_6 = 2+2\theta-\theta^3 \in \mathbb{Z}[\theta]$, tem-se que

$$\begin{aligned} & a_6\cdot 1 + b_6\cdot i + c_6\cdot \tfrac{1}{2}(\theta^3+\theta^2+1) + d_6\cdot(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& 1+(2-3\theta^2-\theta^3)i+0+(2+2\theta-\theta^3)(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& -1-2\theta+\theta^2+\theta^3+\tfrac{-2\theta+\theta^2+\theta^3}{2}i+\tfrac{-2-2\theta+\theta^2+\theta^3}{2}k = g_6. \end{aligned}$$

- Para g_7, tomando $a_7 = -1,\ b_7 = 2-4\theta^2-2\theta^3,\ c_7 = 0,\ d_7 = 2-2\theta^2-\theta^3 \in \mathbb{Z}[\theta]$, tem-se que

$$\begin{aligned} & a_7\cdot 1 + b_7\cdot i + c_7\cdot \tfrac{1}{2}(\theta^3+\theta^2+1) + d_7\cdot(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& -1+(2-4\theta^2-2\theta^3)i+0+(2-2\theta^2-\theta^3)(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& -1-2\theta+\theta^2+\theta^3+\tfrac{-2-2\theta+\theta^2+\theta^3}{2}i-\tfrac{2\theta-\theta^2-\theta^3}{2}k = g_7. \end{aligned}$$

- Para g_8, tomando $a_8 = -1-4\theta+\theta^3,\ b_8 = 2+2\theta-5\theta^2-3\theta^3,\ c_8 = 0,\ d_8 = -2\theta^2-\theta^3 \in \mathbb{Z}[\theta]$, tem-se que

$$\begin{aligned} & a_8\cdot 1 + b_8\cdot i + c_8\cdot \tfrac{1}{2}(\theta^3+\theta^2+1) + d_8\cdot(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& -1-4\theta+\theta^3+(2+2\theta-5\theta^2-3\theta^3)i+0+(-2\theta^2-\theta^3)(-\tfrac{1}{2\theta}(2+(\theta^3+\theta^2-1)i+k)) \\ = \;& g_8 = -1-2\theta+\theta^2+\theta^3+\tfrac{\theta^2-2}{2}i+\tfrac{2\theta+\theta^2}{2}k = g_8, \end{aligned}$$

onde $\theta = \sqrt{2+\sqrt{2}}$. Logo, $g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8 \in \mathcal{M}$, ou seja, os elementos da ordem $\mathcal{M}$ podem ser associados, via isomorfismo, com os elementos do grupo fuchsiano Γ_{16}^*. Portanto, Γ_{16}^* é um grupo fuchsiano aritmético derivado da álgebra dos quatérnios $\mathcal{A} = (\sqrt{2+\sqrt{2}}, -1)_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{2+\sqrt{2}})$, cujos elementos são associados, via isomorfismo, com os elementos da ordem dos quatérnios maximal $\mathcal{M} \supset \mathcal{O} = (\sqrt{2+\sqrt{2}}, -1)_{\mathcal{I}_{\mathbb{K}}}$, onde $\mathcal{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2+\sqrt{2}}]$.

Capítulo 5

Conclusões e Perspectivas

Um dos principais objetivos quando se propõe novos sistemas de comunicações é que estes sistemas apresentem ganhos de codificação e menor complexidade quando comparados com os sistemas já conhecidos. Foi visto que na busca por constelações de sinais com melhor desempenho, constelações associadas à superfícies com gênero $g \geq 2$ tem sido estudadas. Além disso, no espaço hiperbólico existem infinitas possibilidades de se obter reticulados regulares associados à tesselações hiperbólicas. Ganhos de codificação podem ser obtidos quando se utiliza constelações de sinais hiperbólicos quando comparados com as constelalações de sinais no espaço euclidiano, [10].

Nesta temática vimos que muitos trabalhos têm sido realizados com o objetivo de obter constelações de sinais e códigos geometricamente uniformes no espaço hiperbólico, [1,10,13,33,42,53]. Porém, sentimos a necessidade de fornecer um ferramental mais algébrico para que tais códigos e reticulados possam ser construídos. Como vimos, os grupos fuchsianos aritméticos formam uma estrutura algébrica a partir da qual a construção de constelações de sinais pode ser realizada. Dessa forma, o objetivo central deste trabalho foi fornecer condições para que possamos de fato construir esta estrutura algébrica, os grupos fuchsianos aritméticos. Acreditamos que esta dificuldade encontrada anteriormente para obter estes grupos possa ser fortemente diminuída com os resultados apresentados neste trabalho, a saber, a condição de Fermat, Teorema 3.1.3, e o algoritmo proposto na Seção 3.2, o qual implementamos utilizando o *software Maple*.

Apesar de não ser a tesselação mais densa, a tesselação $\{4g, 4g\}$ é a tesselação mais utilizada nos trabalhos sobre esta temática, devido a sua autodualidade e sua baixa complexidade computacional. Sendo assim, neste trabalho procuramos apresentar esta tesselação de forma detalhada como visto na Seção 3.3 e também durante todo o trabalho para exemplificar os demais resultados. Construímos os grupos fuchsianos provenientes da tesselação $\{4g, 4g\}$ utilizando o emparelhamento normal, como em [13], e também considerando o emparelhamento diametralmente oposto, sendo que este último não havia sido tratado nos trabalhos citados. Outras tesselações também foram consideradas tais como a tesselação $\{4g+2, 2g+1\}$ na Seção 3.4, que como vimos pode ser obtida utilizando o emparelhamento diametralmente oposto, e também apresentamos um outro tipo de emparelhamento para esta tesselação, diferente dos emparelhamentos usual e diametralmente oposto, e a tesselação $\{12g-6, 3\}$ na Seção 3.5, que é a tesselação mais densa dentre todas as tesselações hiperbólicas.

A partir dos emparelhamentos apresentados nas Seções 3.3 e 3.4, na Seção 4.1 foi apresentado um isomorfismo entre grupos fuchsianos aritméticos para a tesselação $\{4g, 4g\}$ utilizando os grupos Γ_{4g} e Γ_{4g}^{*}, e para a tesselação $\{4g+2, 2g+1\}$ para o gênero fixado $g = 2$, ou seja, para a tesselação $\{10, 5\}$ utilizando os grupos Γ_{10}^{*} e $\Gamma_{10}^{\bullet}$.

Na Seção 4.2, descrevemos alguns dos corpos de números que utilizamos para construir grupos fuchsianos aritméticos no Capítulo 3, como subcorpos maximais reais de corpos ciclotômicos, tendo como objetivo relacionar estes reticulados hiperbólicos (ordens dos quatérnios) com reticulados euclidianos em trabalhos futuros. Uma associação entre reticulados hiperbólicos e reticulados euclidianos foi apresentada em [3], onde os autores utilizam uma ordem maximal de uma álgebra dos quatérnios, sobre um corpo de números totalmente complexo, para encontrar uma versão do reticulado E_8. Sendo assim, acreditamos que utilizando técnicas semelhantes às apresentadas em [3], podemos associar reticulados euclidianos com os reticulados hiperbólicos apresentados neste trabalho.

Através dos resultados apresentados nas Proposições 4.2.1, 4.2.2,4.2.3 e 4.2.4, obtivemos as seguintes relações entre subcorpos maximais reais de corpos ciclotômicos e corpos de números totalmente reais obtidos através de expansões finitas de radicais.

$$\mathbb{K} = \begin{cases} \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1}) = \mathbb{Q}(\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}) & \text{, com } r > 2; \\ \mathbb{Q}(\zeta_{3.2^r} + \zeta_{3.2^r}^{-1}) = \mathbb{Q}(\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}}) & \text{, com } r > 1; \\ \mathbb{Q}(\zeta_{5.2^r} + \zeta_{5.2^r}^{-1}) = \mathbb{Q}(\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}}) & \text{, com } r > 1; \\ \mathbb{Q}(\zeta_{3.5.2^r} + \zeta_{3.5.2^r}^{-1}) = \mathbb{Q}(\sqrt{2+\sqrt{2+\ldots+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}}) & \text{, com } r > 1. \end{cases}$$

Finalizamos o trabalho, apresentando ordens maximais dos quatérnios para algumas álgebras dos quatérnios que foram associadas a grupos fuchsianos aritméticos no Capítulo 3. Estas ordens maximais dos quatérnios, quando associadas à grupos fuchsianos aritméticos produzem um rotulamento completo dos pontos da constelação de sinais associada. Tais ordens foram caracterizadas através de uma base B, e para obter tal base e também mostrar que caracterizam de fato uma ordem maximal dos quatérnios o uso do *software Magma* foi indispensável. Na Tabela 4.1, apresentamos a forma das bases das ordens maximais dos quatérnios obtidas neste trabalho. Na Subseção 4.3.4, apresentamos exemplos que conectam os conceitos e resultados apresentados neste trabalho.

Observamos que a implementação do algoritmo proposto na Seção 3.2 foi obtida durante o período de 6 meses do doutorado sanduíche em que estive na San Diego State University sob a supervisão do Prof. Dr. J. Carmelo Interlando. Ainda, no mesmo período, foram obtidas as ordens maximais dos quatérnios apresentadas na Seção 4.3, em parceria com a Profa. Dra. Cátia Regina de Oliveira Quilles Queiroz da Universidade Federal de Alfenas (co-orientadora), durante seu pós doutorado na mesma instituição, e ambas sob supervisão do Prof. Dr. J. Carmelo Interlando.

Perspectivas

A seguir, apresentamos de maneira sucinta alguns tópicos que podem ser objetos de estudos para trabalhos futuros, a partir dos resultados apresentados neste trabalho.

- Construção de grupos fuchsianos aritméticos para outras tesselações hiperbólicas regulares, como por exemplo as tesselações do tipo $\{8g-4,4\}$ as quais foram utilizadas em [15] na construção de codificação de geodésicas.

- Obtenção de ordens maximais dos quatérnios para grupos fuchsianos aritméticos associados a outras tesselações a diferentes da $\{4g,4g\}$ e $\{4g+2,2g+1\}$, como por exemplo para as tesselações $\{12g-6,3\}$ e $\{8g-4,4\}$.

- Utilizar as tesselações apresentadas neste trabalho para estabelecer conexões entre espaços euclidianos e espaços hiperbólicos através da teoria de Teichm$\ddot{u}$ller.

- Associação de reticulados hiperbólicos com reticulados euclidianos da seguinte forma: obtenção de versões rotacionadas de reticulados conhecidos utilizando ordens maximais dos quatérnios e propondo uma classificação dos reticulados hiperbólicos como é feito para reticulados euclidianos, como por exemplo, em relação a densidade de centro ou diversidade.

- A partir dos grupos fuchsianos obtidos neste trabalho, obter um particionamento de conjuntos no espaço hiperbólico, como proposto para o caso euclidiano em [52].

Publicações

Os seguintes trabalhos decorrentes dos resultados apresentados nesta tese de doutorado foram apresentados e/ou publicados:

- C. W. O. Benedito, C. R. O. Q. Queiroz, J. Carmelo Interlando, R. Palazzo Jr. *Hyperbolic lattices obtained from arithmetic fuchsian groups via hyperbolic tesselations* In: 2013 North American School of Information Theory, IEEE Information Theory Society, Purdue University, West Lafayette, Indiana, USA, 2013.

- C.R.O.Q. Queiroz, C. W. O. Benedito, J. Carmelo Interlando, R. Palazzo Jr. *Maximal Quaternion Orders derived from* $\{4g,4g\}$ *tessellations* In: 2013 North American School of Information Theory, IEEE Information Theory Society, Purdue University, West Lafayette, Indiana, USA, 2013.

- C. W. O. Benedito, R. Palazzo Jr. *An isomorphism between two arithmetic fuchsian groups using different edge-pairings* In: Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory, 2012, Pomorie. Algebraic and Combinatorial Coding Theory Proceedings. Printed in Bulgaria: Bulgarian Academy of Sciences, 2012. p.335 - 340

- C. W. O. Benedito, R. Palazzo Jr. *A necessary condition for obtaining arithetic fuchsian groups derived from quaternion orders* In: XXII Brazilian Algebra Meeting, 2012, Salvador. Program and abstracts of the XXII Brazilian Algebra Meeting. Salvador: UFBA, 2012. p.71

- C. W. O. Benedito, R. Palazzo Jr. *Isomorfismos entre Grupos fuchsianos Aritméticos Provenientes da Tesselação* $\{4g, 4g\}$ *via Emparelhamentos* In: XXXIV Congresso Nacional de Matemática Aplicada e Computacional, 2012, Águas de Lindóia. Anais do CNMAC. , 2012. v.4. p.159 - 165

Submissões

- C. W. O. Benedito, R. Palazzo Jr, J. Carmelo Interlando. *An algorithm to construct arithmetic fuchsian groups derived from quaternion algebras and the corresponding hyperbolic lattices* (Submetido)

- C. R. O. Q. Queiroz, C. W. O. Benedito, J. Carmelo Interlando, R. Palazzo Jr. *Hyperbolic Lattices with Complete Labeling Derived from* $\{4g, 4g\}$ *Tessellations* In: 4th International Castle Meeting on Coding Theory and Applications (Aceito)

Bibliografia

[1] E. Agustini. Constelações de sinais em espaços hiperbólicos. Tese de Doutorado, IMECC-UNICAMP, 2002.

[2] C. D. Albuquerque, R. Palazzo Jr., and E.B. Silva. Topological quantum codes on compact surfaces with genus $g \geq 2$. *J Math Phys*, 50(2):023513–023513–20, 2009.

[3] C. Alves and J.-C. Belfiore. Lattices from maximal orders into quaternion algebras. *Journal of Pure and Applied Algebra*, Available online 29 April 2014.

[4] A. A. Andrade, C. Alves, and T. B. Carlos. Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$. *International Journal of Applied Mathematics*, 19:321–331, 2006.

[5] A. A. Andrade, A.J. Ferrari, C.W.O. Benedito, and S.I.R. Costa. Constructions of algebraic lattices. *Computational and Applied Mathematics*, 29(3):493–505, 2010.

[6] C. Bavard. Disques extrémaux et surfaces modulaires. *Annales de la Faculté des Sciences de Toulouse*, V(2):191–202, 1996.

[7] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo. New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the rayleigh fading channel. *IEEE Trans. Inform. Theory*, 50(4):702–714, 2004.

[8] A. Beardon. *Geometry of discret groups*. Springer-Verlag, New York, 1983.

[9] J. Boutros, E. Viterbo, C. Ratello, and J.-C. Belfiore. Good lattice constellations for both rayleigh fading and gaussian channels. *IEEE Trans. Inform. Theory*, 42(2):502–517, 1996.

[10] E. Brandani. Constelações de sinais e análise de desempenho no plano hiperbólico. Tese de Doutorado, FEEC-UNICAMP, 2000.

[11] E. D. Carvalho and A. A. Andrade. Hyperbolic lattices: a new propose for coding theory. *International Journal of Applied Mathematics*, 24(1):65–72, 2011.

[12] E. D. Carvalho, A. A. Andrade, and R. Jr. Palazzo. Quaternion oders over quadratic integer rings from arithmetic fuchsian groups. *International Journal of Applied Mathematics*, 25(3):393–404, 2012.

[13] E.D. Carvalho. Construção e rotulamento de constelações de sinais geometricamente uniformes em espaços euclidianos e hiperbólicos. Tese de Doutorado, FEEC-UNICAMP, fevereiro 2001.

[14] R. G. Cavalcante, H. Lazari, J. D. Lima, and R. Jr. Palazzo. A new approach to the design of digital communication systems. *Editors - AMS - DIMACS*, 68:145–177, 2005.

[15] D. P. B. Chaves. Sistemas dinâmicos de eventos discretos com aplicação ao fluxo geodésico em superfícies hiperbólicas. Tese de Doutorado, FEEC-UNICAMP, 2011.

[16] J.H. Conway and N.J.A. Sloane. *Sphere packing, lattices and groups.* Springer-Verlag, New York, 1999.

[17] S.I.R. Costa, Augustini E. Muniz, M., and R. Jr. Palazzo. Graphs, tessellations, and perfect codes on flat tori. *IEEE Trans. Inform. Theory*, 50(10):2363–2377, 2004.

[18] X.D. Dong and C.B. Soh. Group of algebraic integer used for coding qam signal. *IEEE Trans. Inform. Theory*, 44(5):1848–1860, 1998.

[19] O. Endler. *Teoria dos números algébricos.* Projeto Euclides, Impa, Rio de Janeiro, 1986.

[20] M. Faria. Coordenadas fricke e empacotamento hiperbólico de discos. Tese de Doutorado, IMECC-UNICAMP, 2005.

[21] E.R. Fávaro. Corpos de condutor potência de primo, anéis de inteiros, reticulados e mínimo euclidiano. Tese de Doutorado, IBILCE-Unesp, 2012.

[22] M. Firer. *Grupos fuchsianos.* Notas de Aula, IMECC-UNICAMP, 2001.

[23] G.D. Forney. Geometrically uniform codes. *IEEE Trans. Inform. Theory*, IT 37:1241–1260, 1991.

[24] A. Garcia and Y. Lequain. *Elementos de álgebra.* Projeto Euclides, IMPA, Rio de Janeiro, 2003.

[25] X. Giraud, E. Boutilon, and J. C. Belfiore. Algebraic tools to build modulation schemes for fading channels. *IEEE Trans. Inform. Theory*, 43(3):938–952, 1997.

[26] A. Gonçalves. *Introdução à álgebra.* Projeto Euclides, IMPA, Rio de Janeiro, 1999.

[27] K. Huber. Codes over gaussian integers. *IEEE Trans. Inform. Theory*, 40(1):207–216, 1994.

[28] S. Johansson. On fundamental domains of arithmetic fuchsian groups. *Math. Comp.*, 229:339–349, 2000.

[29] G. C. Jorge. Reticulados q-ários e algébricos. Tese de Doutorado, IMECC-UNICAMP, 2012.

[30] S. Katok. *Fuchsian groups.* The University of Chicago Presse, Chicago, 1992.

[31] M. Krížek, F. Luca, and L. Somer. *17 Lectures on Fermat numbers: From number theory to geometry*. Springer-Verlag, New York, 2001.

[32] S. Lang. *Álgebra*. Addison-Wesleyl, New York, 1972.

[33] H. Lazari. Uma contribuçião à teoria de códigos geometricamente uniformes hiperbólicos. Tese de Doutorado, FEEC-UNICAMP, 2000.

[34] E.L. Lima. *Elementos de topologia geral*. Livros Técnicos e Científicos, IMPA, Rio de Janeiro, 1976.

[35] E.L. Lima. *Espaços métricos*. Projeto Euclides, IMPA, Rio de Janeiro, 2009.

[36] C. Maclachlan and A.W. Reid. *The arithmetic of hyperbolic 3-manifolds*. Springer-Verlag, New York, 2003.

[37] D.A. Marcus. *Number fields*. Springer-Verlag, New York, 1977.

[38] F. C. P. Milies. *Álgebra moderna*. Atual Editora, São Paulo, 1972.

[39] J.R. Munkres. *Topology: a first course*. Prentice-Hall, Inc., 1975.

[40] G. Nakamura. Generic fundamental polygons for surfaces of genus three. *Kodai Math. J.*, 27:88–104, 2004.

[41] F. Oggier. Algebraic methods for channel coding. Ph.D. thesis, École Polytechnique Fédeérale de Lausanne, 2005.

[42] C.R.O.Q. Queiroz. Códigos geometricamente uniformes derivados de grafos sobre anéis quocientes de inteiros e de ordens dos quatérnios. Tese de Doutorado, FEEC-UNICAMP, 2011.

[43] I. Reiner. *Maximal orders*. Clarendon Press, Oxford, 2003.

[44] J. Rifà. Groups of complex integers used as qam signals. *IEEE Trans. Inform. Theory*, 41(5):1512–1516, 1995.

[45] P. Samuel. *Algebraic theory of numbers*. Hermann, Paris, 1970.

[46] C.E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27:379–423, 623–656, 1948.

[47] D. Slepian. Group codes for the gaussian channel. *Bell Syst. Tech. J.*, 47:575–602, 1968.

[48] E. Spiegel. Codes over $\mathbb{Z}_m$. *Inform and Control*, (35):48–51, 1977.

[49] I.N. Stewart. *Algebraic number theory*. Chapman and Hall, London, 1987.

[50] J. Stillwell. *Geometry of surfaces*. Springer-Verlag, New York, 2000.

[51] K. Takeuchi. A characterization of arithmetic fuchsian groups. *J. Math. Soc. Japan*, 27(4):600–612, 1975.

[52] G. Ungerboeck. Channel coding with multilevel/phase signals. *IEEE Trans. Inform. Theory*, 28(1):55–67, 1982.

[53] V.L. Vieira. Grupos fuchsianos artiméticos identificados em ordens dos quatérnios para construção de constelações de sinais. Tese de Doutorado, FEEC-UNICAMP, 2007.

[54] J. Voight. *The arithmetic of quaternion algebras*. book in preparation.

[55] C. Walkden. *Hyperbolic geometry*. MATH30141/60771, Manchester University.

[56] L. Washington. *Introduction to cyclotomic fields*. Springer-Verlag, New York, 1982.

Índice Remissivo