Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Grupos Fuchsianos Identificados em uma Ordem dos Quatérnios

por

Robson Pereira de Sousa

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Março/2009
João Pessoa - PB

Grupos Fuchsianos Identificados em uma Ordem dos Quatérnios

por

Robson Pereira de Sousa

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva - UFPB (Orientador)

Prof. Dr. Orlando Stanley Juriaans - IME-USP

Prof. Dr. Uberlândio Batista Severo - UFPB

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Março/2009

Agradecimentos

- A Deus, por tudo, pois sem Ele nada seria possível.

- Ao Prof. Dr. *Antônio de Andrade e Silva*, pela paciência, incentivo, amizade, compreenção e principalmente por entender o verdadeiro sentido da palavra *orientação*.

- Ao Prof. Dr. *Fernando Antônio Xavier de Sousa*, pela confiança e por me orientar durante o primeiro ano de mestrado.

- Em especial aos meus pais *Nair* e *Laudimiro* e aos meus irmãos *Valdir*, *Vânia*, *Fredson* e *Pericles* que contribuiram decisivamente para minha formação.

- A todos os colegas do curso de mestrado, pelo incentivo e amizade.

- Em especial aos amigos *Roni Guedes*, *Reinilson Silva*, *Jessica Ferreira* e *Jackson Jonas* pela grande amizade.

- A minha noiva *Joelma Martins*, pelo incentivo, carinho, companheirismo e principalmente por ter compreendido toda minha ausência durante esses dois anos.

- Aos professores, Dr.*Aldo Trajano Louredo* e Dr. *Osmundo Alves Maciel* pelo incentivo.

- Aos ex-professores da Pós-Graduação do Departamento de Matemática da UFPB, pelo conhecimento transmitido.

- A CAPES pelo suporte financeiro durante a realização deste trabalho.

Dedicatória

A minha família.
É ela quem faz tudo valer a pena.

Resumo

Katok em [11] e Johansson em [8] propuseram uma maneira aritmética de se obter grupos Fuchsianos, chamados de grupos Fuchsianos aritméticos. Em [9], Johansson mostrou que um grupo Fuchsiano aritmético está associado a uma ordem de uma álgebra dos quaténios $\mathcal{A}$ sobre uma extensão quadrática de $\mathbb{Q}$. Neste trabalho generalizamos este resultado para uma álgebra dos quatérnios sobre K com $[K : \mathbb{Q}] = 2^n$.

Palavras chave: Grupos Fuchsianos, grupos fuchsianos aritméticos, álgebra dos quatérnios, ordem dos quatérnios.

Abstract

Katok in [11] and Johansson in [8] proposed a way to obtain arithmetic Fuchsian groups, called arithmetic Fuchsian groups. In [9], Johansson showed that a arithmetic Fuchsian group is associated to an order of an algebra of the quatenions on a quadratic extension of $\mathbb{Q}$. In this work we generalize this result to an algebra of the quaternions on K with $[K : \mathbb{Q}] = 2^n$.

Key-words: Fuchsian groups, arithmetic fuchsian groups , algebra of the quaternions, order of the quaternions.

Notação

$\mathcal{A}$ - Álgebra dos quatérnios
$\mathbb{I}_K$ - Anel dos inteiros do corpo K
$\mu(A)$ - Área hiperbólica de A
$\arg(a)$ - Argumento de a
$B_r\,(a)$ - Bola aberta centrada em a de raio r
$B_r\,[0]$ - Bola fechada centrada em 0 de raio r
B_ρ - Bola de raio ρ centrado na origem
$\mathcal{Z}(H)$ - Centralizador de H
C_T - Círculo isométrico da transformação T
$M_n(K)$ - Conjunto das matrizes $n \times n$ sobre o corpo K
$M_{m\times n}(K)$ - Conjunto das matrizes $m \times n$ sobre o corpo K
$\mathbb{C}$ - Conjunto dos números complexos
$\mathbb{Z}$ - Conjunto dos números inteiros
$\mathbb{N}$ - Conjunto dos números naturais
$\mathbb{R}$ - Conjunto dos números reais
$\overline{x}$ - Conjugado de x
$\mathcal{U}(R)$ - Conjunto das unidades de R
$\Lambda_z(\Gamma)$ - Conjunto limite de Γ
$||\gamma||$ - Comprimento Hiperbólico da curva γ
$\mathbb{Q}(\sqrt{d})$ - Corpo quadrático
$\det(A)$ - Determinante da matriz A
$\mathbb{B}$ - Disco de Poincaré
$d(p,q)$ - Distância Hiperbólica entre p e q
$d\,(\mathcal{A})$ - Discriminante de $\mathcal{A}$
$\widehat{\mathbb{C}}$ - Esfera de Riemann
$\frac{\mathbb{H}}{\Gamma}$ - Espaço das Órbitas
F/K - Extensão do corpo F sobre o corpo K
g - Gênero
G - Grupo
$\Gamma(\mathcal{A},\mathcal{O})$ - Grupo derivado de uma álgebra dos quatérnios $\mathcal{A}$ cuja ordem é $\mathcal{O}$
Γ - Grupo Fuchsiano
$\mathrm{Isom}(\mathbb{H})$ - Grupos das isometrias de $\mathbb{H}$
$\frac{G}{H}$ - Grupo quociente de G por H
$\mathrm{GL}(n,\mathbb{R})$ - Grupo linear geral
$\mathrm{SL}(2,\mathbb{R})$ - Grupo unimodular
$\mathrm{PSL}(2,\mathbb{R})$ - Grupo linear projetivo especial

$\mathbb{G}$ - Grupo das transformações de Möbius

I - Identidade

$\simeq$ - Isomorfo

$\lim A_n$ - Limite de A_n

ds - Métrica hiperbólica

$||T||$ - Norma da transformação T

$N(x)$ - Norma reduzida de x

$\ker \varphi$ - Núcleo de φ

$\mathcal{O}$ - Ordem dos Quatérnios

$\forall$ - Para todo

$\mathrm{Im}(z)$ - Parte Imaginária do número completo z

$\mathrm{Re}(z)$ - Parte Real do número completo z

$\mathcal{A}^{\varphi} \otimes F$ - Produto tensorial da álgebra $\mathcal{A}^{\varphi}$ com o corpo F

R_0 - Região Fundamental de Ford

$\mathfrak{D}_p(\Gamma)$ - Região de Dirichlet para Γ centrada em p

$\mathcal{F}$ - Região Fundamental

$\mathbb{H}$ - Semi plano superior

$\sum$ - Soma

$\mathrm{Tr}(x)$ - Traço reduzido de x

T_A - Transformação Hiperbólica associada a matriz A

$\mathrm{tr}(A)$ - Traço da matriz A

Sumário

Introdução

Johansson, em [9], mostrou que um grupo Fuchsiano aritmético está associado a uma ordem de uma álgebra dos quatérnios sobre uma extensão quadrática de $\mathbb{Q}$, isto é,

$$[K : \mathbb{Q}] = 2,$$

onde os geradores do grupo fuchsiano são da forma

$$G = \begin{pmatrix} a + b\sqrt{t} & r_1\left(c + d\sqrt{t}\right) \\ r_2\left(c - d\sqrt{t}\right) & a - b\sqrt{t} \end{pmatrix},$$

com a, b, c, $d \in \mathbb{Z}[\theta]$, e $\mathbb{Z}[\theta]$ denota o anel dos inteiros de $\mathbb{Q}(\sqrt{m})$, $m > 0$, $r_1 = -r_2 \in \mathbb{Z}$, $t \in \mathbb{Z}[\theta]$ e $\sqrt{t} \notin \mathbb{Z}[\theta]$.

O principal objetivo deste trabalho é apresentar uma generalização do resultado apresentado por Johansson em [9] para uma álgebra dos quatérnios sobre K, com

$$[K : \mathbb{Q}] = 2^n,$$

ou seja, vamos construir grupos Fuchsianos identificados em uma ordem de uma álgebra dos quatérnios sobre um corpo de números K tal que $[K : \mathbb{Q}] = 2^n$, onde 2^n denota o grau da extensão do corpo dos racionais $\mathbb{Q}$.

Esta dissertação é constituída de quatro capítulos.

No Capítulo 1, apresentamos algumas definições e resultados clássicos sobre geometria hiperbólica, onde definimos os dois modelos para o espaço hiperbólico bidimensional que serão trabalhados ao longo deste texto, a saber, o semiplano superior

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

cuja métrica é obtida a partir do diferencial

$$ds = \frac{|dz|}{\mathrm{Im}(z)} = \frac{\sqrt{dx^2 + dy^2}}{y},$$

e o disco unitário

$$\mathbb{B} := \{z \in \mathbb{C} : |z| < 1\}.$$

cuja métrica é obtida a partir do diferencial

$$ds = \frac{2\,|dz|}{1 - |z|^2}.$$

onde $z = x+yi \in \mathbb{C}$. Apresentamos o grupo linear especial $\mathrm{SL}(2,\mathbb{R})$, o grupo das transformações de Möbius $\mathrm{PSL}(2,\mathbb{R})$ e mostramos que

$$\mathrm{PSL}(2,\mathbb{R}) \simeq \frac{\mathrm{SL}(2,\mathbb{R})}{\{-I, I\}}$$

onde I é a matriz identidade de $\mathrm{SL}(2,\mathbb{R})$. Mais ainda, provamos que os elementos de $PSL(2,\mathbb{R})$ induzem isometrias sobre o semi-plano superior $\mathbb{H}$.

No Capítulo 2, abordamos os conceitos de grupos Fuchsianos (subgrupos discretos de $PSL(2,\mathbb{R})$), aprensentando assim uma série de resultados e definições essenciais para os capítulos subsequentes.

No Capítulo 3, destacamos o conceito de álgebra dos quatérnios e grupos Fuchsianos aritméticos. Consideramos as ordens dos quatérnios $\mathcal{O}$ e caracterizamos os grupos Fuchsianos aritméticos. Mais geralmente, identicamos certos grupos Fuchsianos Γ com uma ordem dos quatérnios $\mathcal{O}$.

Finalmente, no Capítulo 4, apresentamos os principais resultados desta dissertação. Estudamos os grupos Fuchsianos $\Gamma \simeq \Gamma_{4g}$, onde Γ é um subgrupo de $\mathrm{PSL}(2,\mathbb{R})$, no sentido de caracterizá-los quanto a sua aritmeticidade. Primeiro, construimos os grupos Fuchsianos Γ_{4g}. Consideramos o caso $g = 2^n$ e mostramos que esses grupos são derivados de uma álgebra dos quatérnios $\mathcal{A}$ sobre um corpo de números K tal que $[K : \mathbb{Q}] = 2^m$. Nestes casos, identificamos as ordens $\mathcal{O}$ em $\mathcal{A}$ associadas aos grupos Γ_{4g}. Por fim, concluímos esse capítulo, consequentemente esta dissertação, com um exemplo exibindo os geradores de Γ_{4g} para $g = 4$.

Capítulo 1

Geometria Hiperbólica

A geometria hiperbólica constitui o ponto de partida para os capítulos seguintes. Assim, apresentaremos algumas definições e resultados clássicos sobre geometria hiperbólica. Para um tratamento mais completo, recomendamos os livros [5, 11].

1.1 Inversão

Seja $r \in \mathbb{R}$ fixado com $r > 0$. Uma *inversão* de polo O e razão r é a única transformação

$$E : \mathbb{R}^2 - \{(0,0)\} \to \mathbb{R}^2 - \{(0,0)\}$$

tal que $E(P)$ é o único ponto da semirreta OP com $|OP|\,|OE(P)| = r^2$, para todo $P \in \mathbb{R}^2 - \{(0,0)\}$, confira Figura 1.1 com $K = (0,0)$.

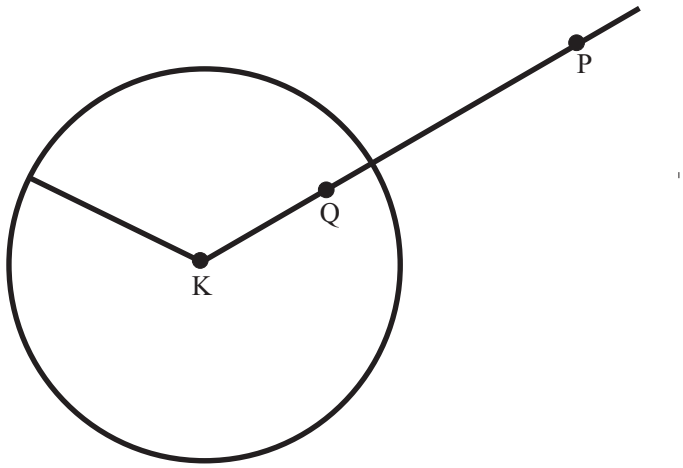

Figura 1.1: Inversão no circulo de centro K.

Sejam $P = (x, y)$ e $Q = E(P) = (u, v)$. Então $Q = (ax, ay)$, onde $a \in \mathbb{R}$ e $a > 0$. Logo, $|OQ| = a\,|OP|$, isto é,

$$u^2 + v^2 = a^2(x^2 + y^2).$$

Como $|OP|\,|OQ| = r^2$ temos que

$$(u^2+v^2)(x^2+y^2) = r^4.$$

Assim, encontrando o valor de a obtemos

$$E(x,y) = \left(\frac{r^2x}{x^2+y^2}, \frac{r^2y}{x^2+y^2}\right) \text{ e } E^{-1} = E.$$

É também sugestivo escrever a inversão de polo O e razão r numa fómula compacta. Para isto, identificando P e $E(P)$ em $\mathbb{R}^2 - \{(0,0)\}$ com z e $z_1 = E(z)$ em $\mathbb{C}^*$, respectivamente, obtemos

$$|zz_1| = r^2 \text{ e } \arg(z_1) = \arg(z).$$

Como $\arg(z) = -\arg(\overline{z})$, as duas equações são satisfeitas, se e somente se,

$$z_1\overline{z} = r^2,$$

pois, $z_1\overline{z} = |z_1|\, e^{i\theta}\, |\overline{z}|\, e^{-i\theta} = |z_1|\,|\overline{z}|$. Assim, temos a seguinte formula para inversão

$$z_1 = \frac{r^2}{\overline{z}}.$$

Observação 1.1 *Se o polo $K \neq P$ e os pontos P, Q e K são identificados com z, z_1 e k em $\mathbb{C} - \{K\}$, obtemos*

$$|(z-k)(z_1-k)| = r^2 \text{ e } \arg(z_1-k) = \arg(z-k).$$

Como $\arg(z-k) = -\arg(\overline{z}-\overline{k})$*, onde $\overline{z}$ e $\overline{k}$ são respectivamente os conjugados de z e k, temos que as duas equações são satisfeitas se, e somente se,*

$$(z_1-k)(\overline{z}-\overline{k}) = r^2.$$

Portanto,

$$z_1 = \frac{k\overline{z} + r^2 - |k|^2}{\overline{z}-\overline{k}}. \tag{1.1}$$

Note que E não está definida em $K = (0,0)$. Assim, para contornarmos este problema vamos escolher um ponto fora de $\mathbb{C}$ e rotular como ∞. Isto nos leva a definir o plano estendido $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, chamado de *esfera de Riemann*. Como

$$\lim_{z\to 0} |z_1| = \lim_{z\to 0} \frac{r^2}{|z|} = \infty,$$

é natural definir $E(0) = \infty$ e $E(\infty) = 0$ e estender E a uma bijeção de $\widehat{\mathbb{C}}$ sobre $\widehat{\mathbb{C}}$. Os pontos de $\mathbb{C} \subset \widehat{\mathbb{C}}$ serão chamados de *pontos finitos*. Diremos que $V \subset \widehat{\mathbb{C}}$ é uma *vizinhança* do ∞, se $\infty \in V$ e existir $r > 0$ tal que

$$\mathbb{C} - B_r[0] \subset V.$$

As regras de cálculo para o ∞ são as seguintes:

$$z + \infty = \infty + z = \infty, \quad z \cdot \infty = \infty \cdot z = \infty,$$

para $z \neq 0$ em $\mathbb{C}$. Convencionaremos escrever

$$\frac{z}{0} = \infty, \quad \frac{z}{\infty} = 0 \text{ se } z \neq 0.$$

1.2 Grupo Linear Geral

Seja $M(2, \mathbb{R})$ o conjunto de todas as 2×2 matrizes sobre $\mathbb{R}$. Então

$$\mathrm{GL}(2, \mathbb{R}) = \{A \in M(2, \mathbb{R}) : \det(A) \neq 0\}$$

com a operação usual de multiplicação de matrizes é um grupo não abeliano, chamado *grupo linear geral*.

Observe que o conjunto

$$\mathrm{SL}(2, \mathbb{R}) = \{A \in GL(2, \mathbb{R}) : \det(A) = 1\}.$$

é um subgrupo de $GL(2, \mathbb{R})$, chamado *grupo linear especial*.

Seja $\mathbb{G}$ o conjunto de todas as transformações $T : \mathbb{C} \to \mathbb{C}$ definidas por

$$T(z) = \frac{az + b}{cz + d},$$

onde $a, b, c, d \in \mathbb{R}$ e $ad - bc = 1$. Então $\mathbb{G}$ com a operação usual de composição de funções é um grupo não abeliano, chamado grupo *das transformações lineares fracionárias* ou grupo *das transformações de Möbius*.

Os grupos $\mathrm{SL}(2, \mathbb{R})$ e $\mathbb{G}$ relacionam-se da seguinte forma: dadas duas transformações $T_A, T_B \in \mathbb{G}$, cujos coeficientes formam, respectivamente, as matrizes $A, B \in \mathrm{SL}(2, \mathbb{R})$, verifica-se facilmente que $T_A \circ T_B = T_{AB}$, ou seja, a composição de transformações em $\mathbb{G}$ corresponde ao produto de matrizes em $\mathrm{SL}(2, \mathbb{R})$. Além disso, claramente a transformação inversa de T_A é $T_{A^{-1}}$. Precisamente, temos o seguinte resultado.

Proposição 1.2 *Se $K = \{-I, I\} \leq \mathrm{SL}(2, \mathbb{R})$, onde I é a matriz identidade. Então*

$$\frac{\mathrm{SL}(2, \mathbb{R})}{K} \simeq \mathbb{G}.$$

Prova. Vamos definir $\varphi : \mathrm{SL}(2, \mathbb{R}) \longrightarrow \mathbb{G}$ por

$$\varphi(A) = \frac{az + b}{cz + d},$$

onde

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R}).$$

É claro que φ está bem definida e é um homomorfismo de grupos sobrejetor. Assim, pelo Teorema de Isomorfismos de Grupos

$$\frac{\mathrm{SL}(2,\mathbb{R})}{\ker\varphi} \simeq \mathbb{G}.$$

Por outro lado, dado $A \in \mathrm{SL}(2,\mathbb{R})$, temos que

$$A \in \ker\varphi \Leftrightarrow \varphi(A) = I.$$

Assim,

$$\frac{az+b}{cz+d} = z \Leftrightarrow cz^2 + (d-a)z - b = 0, \ \forall \ z \in \mathbb{C} \ \text{com} \ z \neq -\frac{d}{c}.$$

Como essa equação tem no máximo duas raízes, temos que $c = b = 0$ e $a = d$. Logo,

$$ad - bc = 1 \Rightarrow a^2 = 1 \Rightarrow a = \pm 1.$$

Portanto,

$$A \in \ker\varphi \Leftrightarrow A = I \ \text{ou} \ A = -I,$$

isto é, $\ker\varphi = K$. ■

Dados $A, B \in \mathrm{SL}(2,\mathbb{R})$, diremos que A *está relacionado com* B, em símbolos $A \sim B$, se e somente se, $B = A$ ou $B = -A$. Portanto,

$$\mathrm{PSL}(2,\mathbb{R}) = \frac{\mathrm{SL}(2,\mathbb{R})}{\{-I, I\}} = \overset{\bullet}{\bigcup} \{A, -A\}, \ \forall \ A \in \mathrm{SL}(2,\mathbb{R}),$$

é chamado o *grupo linear projetivo especial*. Neste caso, não faremos aqui distinção explícita entre o grupo $\mathrm{PSL}(2,\mathbb{R})$ e o grupo das transformações de Möbius $\mathbb{G}$.

Note que, apesar de serem algebricamente iguais, $\mathrm{PSL}(2,\mathbb{R})$ e $\mathbb{G}$ possuem comportamento geométrico diferentes, quando ambos são considerados como transformações de $\mathbb{R}^2$ em $\mathbb{R}^2$ (Identificando $\mathbb{C}$ com $\mathbb{R}^2$ mediante a aplicação natural $x + iy \longmapsto (x, y)$). Por exemplo, a matriz

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

aplicada ao vetor

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

nos dá o vetor

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

enquanto que

$$T(z) = -\frac{1}{z}$$

transforma $z = 1 + i$ no número complexo

$$-\frac{1}{2} + \frac{1}{2}i.$$

Proposição 1.3 *O grupo*

$$\mathrm{PSL}(2,\mathbb{Z}) = \left\{ z \to \frac{az+b}{cz+d} : a,b,c,d \in \mathbb{Z} \ \ e \ \ ad-bc=1 \right\}$$

é gerado pelos elementos

$$S(z) = -\frac{1}{z} \ \ e \ \ T(z) = z+1,$$

o qual é chamado grupo modular.

Prova. De fato, $S(z)$ e $T(z)$ são claramente determinadas pelas matrizes,

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ \text{e} \ C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

respectivamente. Portanto, pela Proposição 1.2, basta provar que $\mathrm{SL}(2,\mathbb{Z})$ é gerado pelas matrizes A e C, onde

$$A^2 = -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Seja

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

Então, usando indução sobre $m(M) = \min\{|a|, |c|\}$ e, se necessário, substituindo M por

$$N = AM = \begin{pmatrix} -c & d \\ a & b \end{pmatrix},$$

podemos supor, sem perda de generalidade, que $|c| \leq |a|$. Assim, há dois casos a serem considerados:

1.º **Caso**. Se $c = 0$, então $\det M = ad = 1$ e $a = d = \pm 1$. Portanto,

$$M = \pm \begin{pmatrix} 1 & \pm b \\ 0 & 1 \end{pmatrix} = \pm C^{\pm b} \in \langle A, C \rangle$$

2.º **Caso**. Seja $0 < |c| \leq |a|$. Então, pelo Algoritmo da Divisão, existem $q, c' \in \mathbb{Z}$ tais que $a = qc + c'$, onde $0 \leq c' < |c|$. Assim,

$$N = C^{-q}M = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-qc & b-qd \\ c & d \end{pmatrix} = \begin{pmatrix} c' & b-qd \\ c & d \end{pmatrix},$$

onde $m(N) = c' < |c|$. Portanto, pela hipótese de indução,

$$M = C^q N \in \langle A, C \rangle,$$

isto é, $\mathrm{SL}(2,\mathbb{Z}) = \langle A, C \rangle$. ■

1.3 Plano Hiperbólico

Apresentaremos dois modelos para o espaço hiperbólico bidimensional: um baseado no semiplano superior

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

e o outro no disco unitário

$$\mathbb{B} := \{z \in \mathbb{C} : |z| < 1\}.$$

Esses dois espaços juntamente com suas respectivas métricas hiperbólicas são designados por *semiplano superior* e *disco de Poincaré*.

No caso do semiplano superior $\mathbb{H}$ a métrica hiperbólica é obtida a partir do diferencial

$$ds = \frac{|dz|}{\mathrm{Im}(z)} = \frac{\sqrt{dx^2 + dy^2}}{y},$$

onde $z = x + yi \in \mathbb{C}$.

Em toda esta dissertação a palavra curva, salvo menção explícita em contrário, significa curva diferenciável por partes. Seja $\gamma : [a, b] \to \mathbb{H}$ uma curva, $\gamma(s) = x(s) + iy(s)$, para todo $s \in [a, b]$, definimos o *comprimento hiperbólico* de γ por:

$$||\gamma|| = \int_a^b \frac{\sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2}}{y(s)} ds.$$

Considerando a função $\varphi : [0, 1] \to [a, b]$ definida por

$$s = \varphi(t) = (1 - t)a + tb, \ \ \forall \ t \in [0, 1]. \tag{1.2}$$

Temos que φ é diferenciável, de modo que a composta

$$\hat{\gamma}(t) = (\gamma \circ \varphi)(t) = \gamma(s)$$

é uma curva diferenciável por partes, onde $\hat{\gamma}(t) = \hat{x}(t) + i\hat{y}(t)$ com $t \in [0, 1]$. Assim,

$$||\hat{\gamma}|| = \int_0^1 \frac{\sqrt{\left(\frac{d\hat{x}}{dt}\right)^2 + \left(\frac{d\hat{y}}{dt}\right)^2}}{\hat{y}(t)} dt \tag{1.3}$$

e

$$\hat{\gamma}(t) = (\gamma \circ \varphi)(t) = \gamma(\varphi(t)) \Rightarrow \hat{x}(t) = x(\varphi(t)) = x(s) \ \text{ e } \ \hat{y}(t) = y(\varphi(t)) = y(s).$$

Pela regra da cadeia

$$\frac{d\hat{x}}{dt} = \frac{dx}{ds}\frac{ds}{dt} = \frac{dx}{ds}(b - a) \ \text{ e } \ \frac{d\hat{y}}{dt} = \frac{dy}{ds}\frac{ds}{dt} = \frac{dy}{ds}(b - a) \tag{1.4}$$

e

$$ds = \frac{ds}{dt}dt = (b - a)dt \tag{1.5}$$

Substituindo os valores das equações (1.4) e (1.5) em (1.3), obtemos

$$\begin{aligned} ||\hat{\gamma}|| &= \int_0^1 \frac{\sqrt{\left(\frac{d\hat{x}}{dt}\right)^2 + \left(\frac{d\hat{y}}{dt}\right)^2}}{\hat{y}(t)} dt = \int_a^b \frac{\sqrt{(b-a)^2\left[\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2\right]}}{y(s)} \frac{ds}{(b-a)} \\ &= \int_a^b \frac{\sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2}}{y(s)} ds = ||\gamma||\,. \end{aligned}$$

Portanto, não há perda de generalidade em considerar as curvas sobre o intervalo $[0,1]$. Assim,

$$||\gamma|| = \int_0^1 \frac{\sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2}}{y(s)} ds.$$

Dados $p, q \in \mathbb{H}$, a *distância hiperbólica* entre p e q, em símbolos $d(p,q)$, é definida por

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

onde o ínfimo é tomado sobre todas as curvas diferenciáveis por partes conectando p e q em $\mathbb{H}$, isto é, todas as curvas diferenciáveis por partes $\gamma : [0,1] \to \mathbb{H}$ com $\gamma(0) = p$ e $\gamma(1) = q$.

Afirmação. d é uma métrica.

De fato, como

$$y > 0 \text{ e } \sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2} \geq 0$$

temos que

$$\frac{\sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2}}{y(s)} \geq 0, \ \ \forall \ s \in [0,1]\,.$$

Portanto,

$$d(p,q) = \inf_\gamma \|\gamma\| = \inf\left(\int_0^1 \frac{\sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2}}{y(s)} ds\right) \geq 0.$$

Por outro lado, para todo $s \in [0,1]$, obtemos

$$\begin{aligned} d(p,q) = \inf_\gamma \|\gamma\| = 0 \Leftrightarrow \|\gamma\| = 0 \Leftrightarrow \frac{\sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2}}{y(s)} = 0 \\ \Leftrightarrow \left(\frac{dx}{ds}^2\right) + \left(\frac{dy}{ds}\right)^2 = 0 \Leftrightarrow \left(\frac{dx}{ds}\right) = \left(\frac{dy}{ds}\right) = 0 \Leftrightarrow p = q. \end{aligned}$$

Agora, seja $\tilde{\gamma} : [0,1] \to \mathbb{H}$ definida por $\tilde{\gamma}(s) = \gamma(1-s)$, para todo $s \in [a,b]$. Então, $\tilde{\gamma}(0) = q$ e $\tilde{\gamma}(1) = p$. Assim, fazendo a substituição $t = 1 - s$, obtemos

$$\begin{aligned} ||\gamma|| &= \int_0^1 \frac{\sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}}{y(t)} dt = -\int_1^0 \frac{\sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2}}{y(1-s)} ds \\ &= \int_0^1 \frac{\sqrt{\left(\frac{dx}{ds}\right)^2 + \left(\frac{dy}{ds}\right)^2}}{y(1-s)} ds = ||\tilde{\gamma}||\,. \end{aligned}$$

Portanto, $\inf ||\gamma|| = \inf ||\tilde{\gamma}||$ e $d(p,q) = d(q,p)$.

Finalmente, dados $p, q, r \in \mathbb{H}$. Sejam

$$\gamma_1 : [0,1] \to \mathbb{H} \text{ e } \gamma_2 : [0,1] \to \mathbb{H}$$

tais que $\gamma_1(0) = p$, $\gamma_1(1) = q$, $\gamma_2(0) = q$ e $\gamma_2(1) = r$. Vamos definir $\gamma : [0,1] \to \mathbb{H}$ por

$$\gamma(t) = \begin{cases} \gamma_1(2t), & \text{se } 0 \leq t \leq \frac{1}{2} \\ \gamma_2(2t-1), & \text{se } \frac{1}{2} \leq t \leq 1 \end{cases}.$$

É claro que γ é uma curva diferenciável por partes com $\gamma(0) = p$, $\gamma(\frac{1}{2}) = q$ e $\gamma(1) = r$. Logo

$$||\gamma|| = ||\gamma_1|| + ||\gamma_2||.$$

Portanto, aplicando o ínfimo na equação anterior, obtemos

$$\inf ||\gamma|| = \inf(||\gamma_1|| + ||\gamma_2||) \leq \inf ||\gamma_1|| + \inf ||\gamma_2||, \text{ ou seja, } d(p,r) \leq d(p,q) + d(q,r).$$

Agora, para definir a métrica hiperbólica no disco de poincaré, vamos considerar a transformação $f : \mathbb{H} \to \mathbb{B}$ definida por

$$f(z) = \frac{z-i}{z+i}.$$

O leitor interessado em mais detalhes sobre essa transformação pode consultar Conway [2]. Assim, a métrica hiperbólica para o disco de Poincaré é dada por

$$d^*(z,w) = d\left(f^{-1}(z), f^{-1}(w)\right), \ \forall \ z, w \in \mathbb{B}.$$

Note que a distância hiperbólica d^* é a mesma que se obtém a partir do diferencial

$$ds = \frac{2\,|dz|}{1-|z|^2}.$$

Existem várias equações equivalentes para obter os valores das distância hiperbólicas entre dois pontos arbitrários dos espaços $(\mathbb{H}, d)$ ou $(\mathbb{B}, d^*)$ (O leitor interessado em mais detalhes pode consultar [5]), por exemplo, para quaisquer p, $q \in \mathbb{H}$,

$$\cosh(p,q) = 1 + \left(\frac{|p-q|^2}{2\,\mathrm{Im}(p)\,\mathrm{Im}(q)}\right). \tag{1.6}$$

Para quaisquer p, $q \in \mathbb{B}$,

$$d(p,q) = \ln\left(\frac{|1-p\overline{q}| + |p-q|}{|1-p\overline{q}| - |p-q|}\right). \tag{1.7}$$

Observe que se $z = 0$, obtemos um caso particular da equação anterior dado por

$$d(0,q) = \ln\left(\frac{1+|q|}{1-|q|}\right) \tag{1.8}$$

Utilizando a equação (1.7) verificaremos que a métrica hiperbólica para o disco $\mathbb{B}$ é invariante pelas transformações lineares fracionárias da forma.

$$T_1(z) = \frac{az+\overline{c}}{cz+\overline{a}}, \;\; |a|^2 - |c|^2 = 1. \tag{1.9}$$

De fato, dados $z, w \in \mathbb{B}$ e uma matriz

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \;\; |a|^2 - |c|^2 = 1.$$

Seja $T_A : \mathbb{C} \to \mathbb{C}$ a transformação induzida pela matriz A. Então

$$\begin{aligned} \left|1 - T_A(z)\overline{T_A(w)}\right| &= \left|1 - \left(\frac{az+\overline{c}}{cz+\overline{a}}\right)\overline{\left(\frac{aw+\overline{c}}{cw+\overline{a}}\right)}\right| \\ &= \left|\frac{(cz+\overline{a})(\overline{cw}+a) - (az+\overline{c})(\overline{aw}+c)}{(cz+\overline{a})(\overline{cw}+a)}\right| \\ &= \frac{|1-z\overline{w}|}{|(cz+\overline{a})(\overline{cw}+a)|} \end{aligned}$$

e

$$\begin{aligned} |T_A(z) - T_A(w)| &= \left|\left(\frac{az+\overline{c}}{cz+\overline{a}}\right) - \left(\frac{aw+\overline{c}}{cw+\overline{a}}\right)\right| \\ &= \frac{|(az+\overline{c})(cw+\overline{a}) - (aw+\overline{c})(cz+\overline{a})|}{|(cz+\overline{a})(cw+\overline{a})|} \\ &= \frac{|z-w|}{\left|(cz+\overline{a})\overline{(cw+\overline{a})}\right|} \\ &= \frac{|z-w|}{|(cz+\overline{a})(\overline{cw}+a)|}, \end{aligned}$$

de modo que

$$\begin{aligned} d(T_A(z), T_A(w)) &= \ln\left(\frac{\left|1 - T_A(z)\overline{T_A(w)}\right| + |T_A(z) - T_A(w)|}{\left|1 - T_A(z)\overline{T_A(w)}\right| - |T_A(z) - T_A(w)|}\right) \\ &= \ln\left(\frac{\frac{|1-z\overline{w}|}{|(cz+\overline{a})(\overline{cw}+a)|} + \frac{|z-w|}{|(cz+\overline{a})(\overline{cw}+a)|}}{\frac{|1-z\overline{w}|}{|(cz+\overline{a})(\overline{cw}+a)|} - \frac{|z-w|}{|(cz+\overline{a})(\overline{cw}+a)|}}\right) \\ &= \ln\left(\frac{|1-z\overline{w}| + |z-w|}{|1-z\overline{w}| - |z-w|}\right) \\ &= d(z,w). \end{aligned}$$

Portanto, a distância é invariante por T_A.

Seja $\gamma : [0,1] \longrightarrow \mathbb{H}$ uma curva. Diremos que γ é uma *geodésica* se

$$d\left(\gamma(s), \gamma(t)\right) = \inf\left(\int_s^t \frac{\sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}}{y(t)} dt\right), \;\; \forall \;\; s,t \in [0,1],$$

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

Proposição 1.4 *O grupo* $\mathrm{PSL}(2,\mathbb{R})$ *age em* $\mathbb{H}$ *por homeomorfismos.*

Prova. Primeiro nos mostraremos que toda transformação de Möbius T_A aplica $\mathbb{H}$ em $\mathbb{H}$, onde

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}).$$

Como

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

e

$$\mathrm{Im}\, u = \frac{u-\overline{u}}{2i}, \ \ \forall \ u \in \mathbb{C},$$

temos que

$$\mathrm{Im}\, w = \frac{w-\overline{w}}{2i} = \frac{(ad-bc)\,(z-\overline{z})}{2i\,|cz+d|^2} = \frac{z-\overline{z}}{2i\,|cz+d|^2} = \frac{\mathrm{Im}\, z}{|cz+d|^2}. \tag{1.10}$$

Portanto, $\mathrm{Im}\, z > 0$ implica que $\mathrm{Im}\, w > 0$. Agora, é claro que $T_A(z)$ e sua inversa são contínuas. ■

Proposição 1.5 *As transformações de Möbius são isometrias, isto é,* $\mathrm{PSL}(2,\mathbb{R})$ *é um subgrupo de* $\mathrm{Isom}(\mathbb{H})$.

Prova. Seja $T \in \mathrm{PSL}(2,\mathbb{R})$. Então, pela Proposição (1.4), $T(\mathbb{H}) = \mathbb{H}$. Seja $\gamma : [0,1] \longrightarrow \mathbb{H}$ uma curva,

$$\gamma(t) = (x(t), y(t)) = x(t) + iy(t) = z(t).$$

Se

$$w = T(z) = \frac{az+b}{cz+d},$$

então

$$w(t) = T(z(t)) = T(x(t)) + iT(y(t)) = u(t) + iv(t)$$

ao longo da curva γ. Logo,

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

Pela equação (1.10), obtemos

$$v = \frac{y}{|cz+d|^2} \Rightarrow \left|\frac{dw}{dz}\right| = \frac{v}{y}.$$

Pela regra da cadeia

$$\frac{dw}{dt} = \frac{dw}{dz}\frac{dz}{dt} \Rightarrow \left|\frac{dw}{dt}\right| = \frac{v}{y}\left|\frac{dz}{dt}\right|.$$

Assim,

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

Portanto,

$$d\left(T(\gamma(s)), T(\gamma(t))\right) = d\left(\gamma(s), \gamma(t)\right),$$

para todo $T \in \mathrm{PSL}(2,\mathbb{R})$. ■

Observação 1.6 *Sejam $z \in \mathbb{H}$ e C um semicírculo ou uma semirreta ortogonal ao eixo real que toca o eixo real no ponto $x_0 \in \mathbb{R}$. Então,*

$$T(z) = -\frac{1}{z - x_0} + w_0 \in \mathrm{PSL}(2,\mathbb{R})$$

aplica C no eixo imaginário positivo, onde w_0 é escolhido adequadamente. De fato, seja $x_1 \in \mathbb{R} \cup \{\infty\}$ outro ponto. Então, $w_0 = 0$ se $x_1 = \infty$ e $w_0 = (x_1 - x_0)^{-1}$ se $x_1 \neq \infty$.

Teorema 1.7 *As geodésicas em $\mathbb{H}$ são semicírculos ou semirretas ortogonais ao eixo $\mathbb{R}$.*

Prova. Sejam $z_1, z_2 \in \mathbb{H}$. Suponhamos que

$$z_1 = ia \text{ e } z_2 = ib \text{ com } b > a.$$

Se $\gamma : I \longrightarrow \mathbb{H}$ é um caminho diferenciável ligando ia a ib, com

$$\gamma(t) = (x(t), y(t)),$$

então

$$\begin{aligned} ||\gamma|| &= \int_0^1 \frac{\sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}}{y(t)}dt \geq \int_0^1 \frac{\left|\frac{dy}{dt}\right|}{y(t)}dt \\ &\geq \int_0^1 \frac{\frac{dy}{dt}}{y(t)}dt = \int_a^b \frac{dy}{y} = \ln\frac{b}{a}. \end{aligned}$$

Assim, este é exatamente o comprimento hiperbólico do segmento do eixo imaginário que une ia a ib, consequentemente, a geodésica que une ia a ib é o segmento do eixo imaginário que os une.

Consideremos agora z_1 e z_2 arbitrários. Seja L o semicírculo Euclidiano único ou semirreta que une z_1 a z_2. Assim, existe, pela Observação 1.6, uma transformação em $\mathrm{PSL}(2,\mathbb{R})$ que mapeia L no eixo imaginário positivo, o que reduz o problema ao caso particular acima. Logo, Pela proposição 1.5, concluímos que a geodésica entre z_1 e z_2 é o segmento de L que une z_1 a z_2. ■

Corolário 1.8 *Quaisquer dois pontos $z, w \in \mathbb{H}$ podem ser unidos por uma única geodésica, e a distância hiperbólica entre z e w é igual ao comprimento hiperbólico do segmento da geodésica que une esses pontos, que denotamos por $[z, w]$.* ■

Proposição 1.9 *Toda isometria de* $\mathbb{H}$*, em particular, toda transformação em* $\mathrm{PSL}(2,\mathbb{R})$*, transforma geodésica em geodésica.*

Prova. Sejam

$$T \in \mathrm{PSL}(2,\mathbb{R}),$$

z, t pontos distintos em $\mathbb{H}$ e $\varepsilon \in [z,t]$. Então, pelo proposição 1.5 e o Corolário 1.8, temos que

$$T(\varepsilon) \in [T(z), T(t)],$$

isto é, T mapeia o segmento $[z,t]$ no segmento $[T(z),T(t)]$ e, portanto, geodésicas em geodésicas. ■

Vimos na Proposição 1.5 que as transformações de $\mathrm{PSL}(2,\mathbb{R})$ são isometrias do plano hiperbólico $\mathbb{H}$. Seja

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}).$$

O sinal do determinante da matriz A, determina a orientação da isometria, ou seja, se

$$ad - bc = 1,$$

então as transformações correspondentes em $\mathrm{PSL}(2,\mathbb{R})$ são isometrias que preservam orientação. Se

$$ad - bc = -1,$$

então, a isometria tem orientação oposta. Assim, as transformações em $\mathrm{PSL}(2,\mathbb{R})$ são isometrias preservando orientação.

Para todo subconjunto $A \subseteq \mathbb{H}$, sua *área hiperbólica* $\mu(A)$, é definida por

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

se essa integral existir. Analogamente, se $A \subset \mathbb{B}$, então

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

Proposição 1.10 *A área hiperbólica é invariante sob todas as transformações em* $\mathrm{PSL}(2,\mathbb{R})$*, isto é, se* $A \subseteq \mathbb{H}$ *e* $\mu(A)$ *existe, então* $\mu(A) = \mu(T(A))$*, para qualquer* $T \in \mathrm{PSL}(2,\mathbb{R})$*.*

Prova. Se $z = x + iy$, então

$$T(z) = \frac{az+b}{cz+d},$$

onde $a,b,c,d \in \mathbb{R}$ e $ad - bc = 1$. Fazendo $w = T(z) = u + iv$ e usando as equações de Cauchy-Riemann, obtemos

$$\frac{\partial(u,v)}{\partial(x,y)} = \frac{\partial u \partial v}{\partial x \partial y} - \frac{\partial u \partial v}{\partial y \partial x} = \left(\frac{\partial u}{\partial x}\right)^2 + \left(\frac{\partial v}{\partial x}\right)^2 = \left|\frac{dT}{dz}\right|^2 = \frac{1}{|cz+d|^4}.$$

Assim, usando (1.10), teremos

$$\mu(T(A)) = \int\limits_{T(A)} \frac{dudv}{v^2} = \int\limits_{A} \frac{1}{\frac{y^2}{|cz+d|^4}} \frac{\partial(u,v)}{\partial(x,y)} dxdy = \int\limits_{A} \frac{|cz+d|^4}{y^2} \frac{1}{|cz+d|^4} dxdy = \mu(A).$$

Portanto, $\mu(A) = \mu(T(A))$, para qualquer $T \in \mathrm{PSL}(2,\mathbb{R})$. ■

Sejam α, β e $\gamma \in \mathbb{H}$. Considerando geodésicas, raios ou segmentos geodésicos conectando estes pontos, obtemos um triângulo geodésico o qual será chamado *triângulo hiperbólico*. O próximo teorema mostra que a área hiperbólica de um triângulo hiperbólico depende apenas de seus ângulos.

Teorema 1.11 (Gauss-Bonnet) *Se Δ é um triângulo hiperbólico com ângulos α, β e δ. Então*

$$\mu(A) = \pi - \alpha - \beta - \delta.$$

Prova. Verifique [5], página 42, Teorema 4.5.

Observe, que se Δ é um triângulo hiperbólico com ângulos α, β e δ. Então, pelo Teorema anterior $\alpha + \beta + \delta < \pi$.

1.4 Grupos Discreto

Seja X um conjunto qualquer, Y um espaço topológico e $f : X \to Y$ uma função. Então é fácil verificar que

$$\tau := \{f^{-1}(A) : A \text{ é um aberto em } Y\}$$

é uma topologia sobre X, chamada de *topologia induzida* por f. Nesta topologia f é contínua.

Exemplo 1.12 *Mostre que $M(2,\mathbb{R})$ é um espaço topológico.*

Prova. É fácil verificar que a função $\varphi : M(2,\mathbb{R}) \to \mathbb{R}^4$ definida por

$$\varphi\left(\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}\right) = (x_1, x_2, x_3, x_4)$$

é bijetora. Logo,

$$\tau := \{\varphi^{-1}(U) : U \text{ é um aberto em } \mathbb{R}^4\}$$

é uma topologia sobre $M(2,\mathbb{R})$. Portanto, $M(2,\mathbb{R})$ é um espaço topológico.

Sejam X, Y espaços topológicos e $f : X \to Y$ uma função. Para $x, y \in X$, definimos

$$x \sim y \Leftrightarrow f(x) = f(y).$$

Então $\sim$ é uma relação de equivalência sobre X e

$$\tau := \{A \subseteq \frac{X}{\sim} : \pi^{-1}(A) \text{ é um aberto em } X\}$$

é uma topologia sobre $\frac{X}{\sim}$, (*chamada de topologia quociente*) coinduzida por

$$\pi : X \to \frac{X}{\sim}.$$

Neste caso, π é contínua e aberta. Note que existe uma única função $\overline{f} : \frac{X}{\sim} \to Y$ tal que $\overline{f} \circ \pi = f$.

Proposição 1.13 *Sejam X, Y espaços topológicos e $f : X \to Y$ uma função sobrejetora e contínua. Então, $\overline{f} : \frac{X}{\sim} \to Y$ é contínua, onde $\overline{f} \circ \pi = f$.*

Prova. Verifique [12], página 66.

Um *grupo topológico* G é um espaço topológico, munido de uma estrutura de grupo tal que as aplicações

$$m : \begin{array}{l} G \times G \to G \\ (x, y) \mapsto x \cdot y \end{array} \quad \text{ou} \quad i : \begin{array}{l} G \to G \\ x \mapsto x^{-1} \end{array},$$

são contínuas.

Sejam G um grupo topológico e H um subgrupo de G. Então H é um subgrupo topológico com a topologia induzida pela inclusão. Em particular, se H é um subgrupo normal de G, então o grupo quociente $\frac{G}{H}$ é um grupo topológico com a topologia coinduzida pela projeção.

Seja G um grupo topológico agindo em um espaço topológico X. Então, esta ação chama-se *contínua* (de classe C^∞) se a aplicação

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \to & gx \end{array}$$

é contínua (é de classe C^∞).

Uma familia $\{A_i\}_{i \in I}$ de subconjuntos de um espaço topológico X chama-se *localmente finita* se cada $x \in X$ possui uma vizinhança que intersecta apenas um número finito de conjuntos A_i ou, equivalentemente, para qualquer subconjunto compacto K em X,

$$A_i \cap K \neq \emptyset$$

apenas para uma quantidade finita de pontos $i \in I$. Diremos que um grupo G age de maneira *propriamente descontínua* sobre X se para cada $x \in X$ a órbita

$$G(x) = \{g(x) : g \in G\} \subseteq X$$

é uma família localmente finita.

Sejam G um grupo topológico e H um subgrupo de G. Diremos que H é um *subgrupo discreto* de G se a topologia induzida sobre H é uma topologia discreta, isto é, se H é um conjunto discreto no espaço topológico G (cada ponto é um conjunto aberto).

Proposição 1.14 *Seja G um grupo topológico e H um subgrupo topológico de G.*

1. *Se H é aberto, então H é também fechado.*

2. *Se H é fechado e o índice $[G : H]$ é finito, então H é aberto.*

3. *H é aberto se, e somente se, o espaço das classes $\frac{G}{H}$ é discreto.*

Prova. Sejam $\{g_i\}_{i\in I}$ um conjunto completo de representates das classes laterais de H em G e $i_0 \in I$ o índice com $g_{i_0} \in H$. Então o complementar de H em G é

$$G - H = \bigcup_{i\neq i_0} g_i H.$$

(1) Se H é aberto, então os g_iH também o são. Portanto, se H é aberto, $G - H$ é também aberto, pois é uma união arbitrária de conjuntos abertos e desta forma H é fechado.

(2) Se H é fechado, então os g_iH também o são. Como I é finito temos que $G-H$ é fechado, pois $G - H$ é uma união finita de conjuntos fechados. Portanto, H é aberto.

(3) Observe que $\frac{G}{H}$ é discreto se, e somente se, todos os conjuntos unitários $\{gH\}_{g\in H}$ são abertos em $\frac{G}{H}$; pela homogeneidade do espaço das classes $\frac{G}{H}$, temos que esse caso ocorre se, e somente se, $\{H\} = \pi(H)$ é um subconjunto discreto de $\frac{G}{H}$. Agora, se H é aberto, então $\pi(H)$ também o é, pois π é uma aplicação aberta. Por outro lado, se $\pi(H)$ é aberto, então $H = \pi^{-1}(\pi(H))$ também o é, pois π é contínua. ■

Já vimos, no Exemplo 1.12, que $M(2,\mathbb{R})$ é um espaço topológico com a topologia induzida por $\mathbb{R}^4$. Assim, $\mathrm{GL}(2,\mathbb{R})$ e $\mathrm{SL}(2,\mathbb{R})$ também o são. Portanto, o grupo $\mathrm{PSL}(2,\mathbb{R})$ é um espaço topológico no qual uma transformação $T \in \mathrm{PSL}(2,\mathbb{R})$,

$$T(z) = \frac{az+b}{cz+d},$$

pode ser identificada com o ponto $(a, b, c, d) \in \mathbb{R}^4$. Mais precisamente, como um espaço topológico, $\mathrm{SL}(2,\mathbb{R})$ pode ser identificado com o subconjunto

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

de $\mathbb{R}^4$. Se definirmos $-\varphi : E \to E$ por $-\varphi(a, b, c, d) = (-a, -b, -c - d)$, então $-\varphi$ é um homeomorfismo. Além disso, $G = \{\varphi, -\varphi\}$, onde φ é a função identidade sobre E é um grupo cíclico de ordem 2 agindo sobre E. Portanto, $\mathrm{PSL}(2,\mathbb{R})$ é um grupo topológico com a topologia quociente

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

A *norma* em $\mathrm{PSL}(2,\mathbb{R})$ é induzida de $\mathbb{R}^4$ da seguinte forma: para cada $T \in \mathrm{PSL}(2,\mathbb{R})$,

$$T(z) = \frac{az+b}{cz+d},\ \ ad - bc = 1,$$

definimos

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

Neste caso, $\mathrm{PSL}(2,\mathbb{R})$ é um espaço métrico com a métrica $d(T,S) = ||T - S||$.

Sejam

$$A_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}), \ \forall \ n \in \mathbb{N}.$$

Diremos que $A_n \to A$ se $a_n \to a$, $b_n \to b$, $c_n \to c$ e $d_n \to d$. Se $A, B, A_n, B_n \in \mathrm{SL}(2,\mathbb{R})$ são tais que, $A_n \to A$ e $B_n \to B$, então é fácil verificar que $A_nB_n \to AB$.

Lema 1.15 *Seja H um subgrupo de $\mathrm{SL}(2,\mathbb{R})$. Então H é discreto se, e somente se, não existe uma sequência $A_n \in H$, $n \in \mathbb{N}$, de elementos distintos, tais que $A_n \to I$.*

Prova. Suponhamos, por absurdo, que H não seja discreto. Então, dado $A \in \mathrm{SL}(2,\mathbb{R})$, existe uma sequência $\{A_n\}_{n\in\mathbb{N}}$ em H de elementos distintos tal que $A_n \to A$. Logo,

$$A_{n+1}A_n^{-1} \to AA^{-1} = I.$$

Afirmação. $S = \{A_{n+1}A_n\}_{n\in\mathbb{N}}$ é um conjunto infinito.
De fato, se S é um conjunto finito, então existe um n_0 tal que $A_{n+1}A_n = I$, para todo $n > n_0$, o que é impossível, pois $\{A_n\}_{n\in\mathbb{N}}$ é uma sequência de elementos distintos em H. Assim, S é infinito. Portanto, existe uma subsequência de S que converge para I, o que é uma contradição. ■

Observação 1.16 *Seja H um subgrupo de $\mathrm{SL}(2,\mathbb{R})$. Então H é discreto se, e somente se, para qualquer sequência $\{A_n\}_{n\in\mathbb{N}}$ em H com $A_n \to I$, existe $n_0 \in \mathbb{N}$ tal que*

$$A_n = I, \ \forall \ n \geq n_0.$$

Capítulo 2

Região Fundamental e a Região de Dirichlet

Neste capítulo, vamos destacar os conceitos de grupos Fuchsiano e de região fundamental de um grupo Fuchsiano. Para um tratamento mais completo, recomendamos os livros [5, 11].

2.1 Grupos Fuchsiano

Vamos iniciar esta seção classificando os elementos do grupo

$$\mathrm{PSL}(2,\mathbb{R}) = \frac{\mathrm{SL}(2,\mathbb{R})}{\{-I, I\}}.$$

Seja $\mathrm{tr} : M(2,\mathbb{R}) \to \mathbb{R}$ a função traço. Então tr é uma transformação linear tal que $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ e

$$\mathrm{tr}(A) = \mathrm{tr}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + d.$$

Diremos que $A \in \mathrm{SL}(2,\mathbb{R})$ e a transformação $T_A \in \mathrm{PSL}(2,\mathbb{R})$ é:

1. Elíptica se $\mathrm{tr}(A) < 2$.
2. Parabólica se $\mathrm{tr}(A) = 2$.
3. Hiperbólica se $\mathrm{tr}(A) > 2$.

O traço de uma matriz é invariante por conjugação, isto é, $\mathrm{tr}(BAB^{-1}) = \mathrm{tr}(A)$, para todas $A \in M(2,\mathbb{R})$ e $B \in \mathrm{GL}(2,\mathbb{R})$. Logo a classificação acima é invariante por conjugação.

Observação 2.1 *O número* 2 *da definição depende exclusivamente do número de autovalores reais da matriz A. De fato, o polinômio característico de* $A \in \mathrm{SL}(2,\mathbb{R})$ *é*

$$\begin{aligned} p_A(x) &= x^2 - (a+d)x + ad - bc \\ &= x^2 - \mathrm{tr}(A)x + \det(A) \\ &= x^2 - \mathrm{tr}(A)x + 1, \end{aligned}$$

onde $\Delta = \mathrm{tr}(A)^2 - 4$. *Assim, há três casos a serem considerados*:

1.º ***Caso***. *Se* $\Delta > 0$, *então* A *possui dois autovalores reais distintos* λ_1 *e* λ_2. *Portanto, a menos de conjugação,* A *pode ser escrita na forma*

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Como $\det(A) = 1$ *temos que* $\lambda_2 = \frac{1}{\lambda_1}$. *Neste caso,*

$$\mathrm{tr}(A) = \lambda_1 + \frac{1}{\lambda_1} > 2.$$

2.º ***Caso***. *Se* $\Delta = 0$, *então* A *possui um único autovalore real. Logo,* $p_A(x) = (x - \lambda)^2$. *Portanto, a menos de conjugação,* A *pode ser escrita na forma*

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix},$$

onde

$$\lambda = \frac{1}{2}\,\mathrm{tr}(A) = \frac{1}{2}(a + d) = 1.$$

Neste caso, $\mathrm{tr}(A) = 2$.

3.º ***Caso***. *Se* $\Delta < 0$, *então* A *possui dois autovalores complexos conjugados* λ *e* $\overline{\lambda}$. *Como* $|\lambda|^2 = \det(A) = 1$ *temos que* $\lambda = e^{i\theta}$, *para todo* $\theta \in [0, 2\pi]$. *Portanto, a menos de conjugação,* A *pode ser escrita sob a forma*

$$\begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix}.$$

Neste caso, $\mathrm{tr}(A) < 2$.

Assim, temos o seguinte resultado:

Teorema 2.2 *Seja* $T_A \in \mathrm{PSL}(2, \mathbb{R})$ *com* $T_A \neq I$, *então existe uma matriz* $B \in \mathrm{SL}(2, \mathbb{R})$ *tal que* $T_B \circ T_A \circ T_{B^{-1}}$ *é uma das seguintes matrizes*

$$\begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix}, \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix},$$

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

Portanto, a menos de conjugação, podemos supor que a matriz A seja uma das matrizes do Teorema 2.2, conforme A seja elíptica, parabólica ou hiperbólica, respectivamente.

Lema 2.3 *Seja* $\mathbb{H}$ *o plano hiperbólico. Se* $w \in \mathbb{H}$ *e* K *é um subconjunto compacto de* $\mathbb{H}$, *então o conjunto*

$$E = \{T \in \mathrm{PSL}(2, \mathbb{R}) : T(w) \in K\}$$

é compacto.

Prova. Seja

$$F = \{A \in \mathrm{SL}(2,\mathbb{R}) : T_A(w) \in K\}.$$

Então, $F \subset \mathrm{SL}(2,\mathbb{R})$, $\pi : \mathrm{SL}(2,\mathbb{R}) \to \mathrm{PSL}(2,\mathbb{R})$ definida por $\pi(A) = T_A$ é contínua e $\pi(F) = E$. Assim, basta provar que F é compacto.

Sejam $A_0 \in \mathrm{SL}(2,\mathbb{R})$ e $A_n \in F$ uma sequência tal que $A_n \to A_0$. Então,

$$T_{A_n}(w) \in K \text{ ou } T_{A_n}(w) \to T_{A_0}(w),$$

Logo, $A_0 \in F$, pois K é compacto. Portanto F é fechado.

Como K é limitado temos que existem constantes $M_1 > 0$ e $M_2 > 0$ tais que $|z| < M_1$ e $\mathrm{Im}(z) \geq M_2$, para todo $z \in K$. Em particular, para todo

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in F,$$

obtemos

$$\left|\frac{aw+b}{cw+d}\right| < M_1 \text{ e } \mathrm{Im}\left(\frac{aw+b}{cw+d}\right) \geq M_2.$$

Assim,

$$z = \frac{aw+b}{cw+d} = \frac{(aw+b)\overline{(cw+d)}}{|cw+d|^2} = \frac{ac\,|w|^2 + adw + bc\overline{w} + bd}{|cw+d|^2}$$

implica que

$$\mathrm{Im}(\frac{aw+b}{cw+d}) = \mathrm{Im}(z) = \frac{z-\overline{z}}{2i} = \frac{w-\overline{w}}{2i\,|cw+d|^2} = \frac{\mathrm{Im}(w)}{|cw+d|^2} \geq M_2.$$

Logo,

$$|cw+d|^2 \leq \frac{\mathrm{Im}\, w}{M_2}$$

Portanto,

$$|aw+b| < M_1\,|cw+d| \leq M_1 \left(\frac{\mathrm{Im}\, w}{M_2}\right)^{\frac{1}{2}}.$$

Consequentemente a, b, c e d, são limitados, ou seja, F é limitado. ■

Lema 2.4 *Sejam $\mathbb{H}$ o plano hiperbólico e H um subgrupo de $\mathrm{PSL}(2,\mathbb{R})$ agindo de maneira propriamente descontínua sobre $\mathbb{H}$. Então o conjunto*

$$F_H = \{z \in \mathbb{H} : T(z) = z,\ \forall\ T \in H\}$$

é discreto.

Prova. Primeiro observe que se H age de maneira propriamente descontínua sobre $\mathbb{H}$, então, para um $z \in \mathbb{H}$, o conjunto

$$\{T \in H : T(B_\varepsilon(z)) \cap B_\varepsilon(z)\} \neq \emptyset$$

é finito, onde $B_\varepsilon(z)$ é uma bola hiperbólica. Em particular, o conjunto

$$F = \{T \in H : d(z, T(z)) < \varepsilon\}$$

é finito. Portanto, existe $n_0 \in \mathbb{N}$ tal que $d(z, T_n(z)) > \varepsilon$, para todo $n > n_0$.

Suponhamos, por absurdo, que o conjunto F_H não seja discreto. Então existem sequências $\{z_n\}_{n\in\mathbb{N}}$ em $\mathbb{H}$ e $\{T_n\}_{n\in\mathbb{N}}$ em H tais que $z_n \to z$ e $T_n(z_n) = z_n$. Logo,

$$\begin{aligned} d\left(T_n(z), z\right) &\leq d\left(T_n(z), T_n(z_n)\right) + d(T_n(z_n), z) = d(z, z_n) + d(z_n, z) = 2d(z_n, z) \\ &\Rightarrow d\left(T_n(z), z\right) \to 0, \end{aligned}$$

o que é uma contradição, pois F é finito. ■

Definição 2.5 *Um* grupo Fuchsiano Γ *é um subgrupo discreto de* $\mathrm{PSL}(2, \mathbb{R})$.

Exemplo 2.6 *O subgrupo discreto* $\mathrm{PSL}(2, \mathbb{Z})$ *de* $\mathrm{PSL}(2, \mathbb{R})$ *é um grupo Fuchsiano.*

Teorema 2.7 *Seja* Γ *um subgrupo de* $\mathrm{PSL}(2, \mathbb{R})$. *Então* Γ *é um grupo Fuchsiano se, e somente se, a ação de* Γ *sobre* $\mathbb{H}$ *é propriamente descontínua.*

Prova. Suponhamos que Γ seja discreto. Então para todo $z \in \mathbb{H}$ e todo subconjunto compacto K em $\mathbb{H}$,

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

Assim, pelo Lema 2.3, o conjunto

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

é compacto. Logo,

$$\{T \in \Gamma : T(z) \in K\}$$

é finito. Portanto, a ação de Γ sobre $\mathbb{H}$ é propriamente descontínua.

Reciprocamente, suponhamos que Γ não seja discreto em $\mathrm{PSL}(2, \mathbb{R})$. Então, pelo Lema 2.4, existe $z \in \mathbb{H}$ tal que $T(z) \neq z$, para todo $T \in \Gamma - \{I\}$. Assim, existe uma sequência $\{T_n\}_{n\in\mathbb{N}}$ de elementos distintos de Γ tal que $T_n \to I$. Portanto, $T_n(z) \to z$, o que é uma contradição.

■

Considere a ação

$$\begin{aligned} : \quad \Gamma \times X &\longrightarrow X \\ (T, x) &\longmapsto T(x) \end{aligned}$$

de um grupo Γ como homeomorfismos de um espaço topológico X, ou seja, para todo $T \in \Gamma$, a tranformação $x \to T(x)$ é um homeomorfismo de X, $I(x) = x$ e $S(T(x)) = ST(x)$. Diremos que a ação de Γ é:

1. *efetiva* se $T(x) = x$ para todo $x \in X$ se e somente se $T = I$.

2. *livre* se $T(x) = x$ para algum $x \in X$ se e somente se $T = I$.

Sejam X um espaço métrico e Γ um grupo de homeomorfismos agindo sobre X de maneira propriamente descontínua. Um subconjunto fechado $\mathcal{F} \subset X$, com $\mathring{\mathcal{F}} \neq \emptyset$ ou $int(\mathcal{F}) \neq \emptyset$, chama-se uma *região fundamental* de Γ se as seguintes condições são satisfeitas:

1. $\bigcup_{T \in \Gamma} T(\mathcal{F}) = X$.
2. $\mathring{\mathcal{F}} \cap T(\mathring{\mathcal{F}}) = \emptyset$, para todo $T \in \Gamma - \{I\}$.

A familia

$$\{T(\mathcal{F}) : T \in \Gamma\}$$

chama-se *tesselação* ou *ladrilhamento* de X. Observamos que se $\mathcal{F}$ é uma região fundamental de Γ, então $T(\mathcal{F})$ também o é, para todo $T \in \Gamma$. Para cada grupo Fuchsiano Γ, está associada uma região fundamental $\mathcal{F}$, resultado da ação de Γ sobre $\mathbb{H}$.

Exemplo 2.8 *Seja* $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ *o grupo cíclico gerado por* $T_1(z) = z + 1$. *Então,*

$$\mathcal{F}_k(\Gamma) = \{z \in \mathbb{H} : k \leq \mathrm{Re}(z) \leq k + 1\},$$

para cada k*, é região fundamental resultado da ação de* Γ *sobre* $\mathbb{H}$.

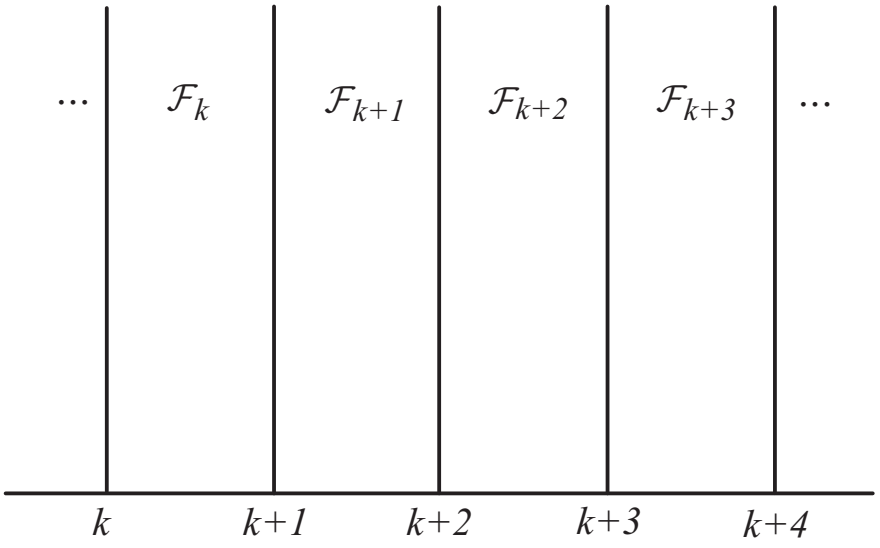

Figura 2.1: Região fundamental do grupo cíclico $\Gamma = \langle z + 1 \rangle$.

2.2 Grupos Fuchsianos Co-compactos

Seja Γ um grupo Fuchsiano de $\mathrm{PSL}(2, \mathbb{R})$ agindo de maneira propriamente descontínua sobre $\mathbb{H}$. Dados $z, w \in \mathbb{H}$, definimos

$$z \sim w \Leftrightarrow \text{ existe } T \in \Gamma \text{ tal que } w = T(z).$$

Então $\sim$ é uma relação de equivalência sobre $\mathbb{H}$.

A classe de equivalência

$$[z] = \{w \in \mathbb{H} : w \sim z\} = \{T(z) : T \in \Gamma\}$$

é chamada de *órbita* de z e será denotada por $\Gamma(z)$. Assim, obtemos a partição de $\mathbb{H}$:

$$\mathbb{H} = \overset{\bullet}{\bigcup_{z \in \mathbb{H}}} \Gamma(z).$$

Neste caso, o espaço das órbitas

$$\frac{\mathbb{H}}{\Gamma} = \frac{\mathbb{H}}{\sim} = \{\Gamma(z) : z \in \mathbb{H}\}$$

é um espaço topológico com a topologia coinduzida pela projeção

$$\pi : \mathbb{H} \to \frac{\mathbb{H}}{\Gamma}.$$

Como a área sobre o quociente $\frac{\mathbb{H}}{\Gamma}$ é induzida pela área hiperbólica sobre $\mathbb{H}$, então $\mu\left(\frac{\mathbb{H}}{\Gamma}\right)$ está bem definida e

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) = \mu(\mathcal{F}),$$

onde $\mathcal{F}$ a região fundamental obtida através da ação de Γ sobre $\mathbb{H}$.

Se

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) < \infty$$

e $\mathcal{F}$ é uma região fundamental para essa ação. Então, a restrição de π a $\mathcal{F}$ identifica os pontos congruentes (eles estão na mesma órbita) de $\mathcal{F}$, os quais estão necessariamente em sua fronteira $\partial\mathcal{F}$. O espaço

$$\frac{\mathbb{B}}{\Gamma}$$

é construindo analogamente.

Um grupo Fuchsiano Γ chama-se *co-compacto* se o espaço quociente

$$\frac{\mathbb{H}}{\Gamma}$$

for compacto. Obviamente, se Γ possuir região fundamental compacta $\mathcal{F}$, então Γ é compacto, pois a restrição de π a $\mathcal{F}$ é sobrejetora.

Seja X um espaço topológico. Diremos que X é um *espaço de Hausdorff* se para quaisquer $x, y \in X$, com $x \neq y$, existem abertos A e B em X tais que

$$x \in A, \;\; y \in B \;\text{ e }\; A \cap B = \emptyset.$$

Proposição 2.9 *Seja X uma variedade Hausdorff e Γ um grupo agindo em X como homeomorfismos. O espaço quociente*

$$\frac{X}{\Gamma}$$

é uma variedade Hausdorff e a projeção $\pi : X \to \frac{X}{\Gamma}$ é uma aplicação de recobrimento se e somente se a ação de Γ em X for livre e propriamente descontínua.

Prova. Verifique [5], página 102, Teorema 6.25.

Teorema 2.10 *Um grupo Fuchsiano* Γ *é co-compacto se, e somente se,* Γ *não possui elementos parabólicos e*

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) < \infty.$$

Prova. Verifique [5], página 128, Corolário 7.32.

Como vamos considerar apenas superfícies $\frac{\mathbb{H}}{\Gamma}$ compactas e tendo área finita, os grupos Fuchsianos considerados em nosso trabalho não possuem elementos parabólicos.

2.3 Região de Dirichlet

Seja Γ um grupo Fuchsiano de $\mathrm{PSL}(2,\mathbb{R})$. Então, pelo Lema 2.4, existe $p \in \mathbb{H}$ tal que $T(p) \neq p$, para todo $T \in \Gamma - \{I\}$. Chama-se *região de Dirichelet* centrado em p ao conjunto

$$\mathfrak{D}_p(\Gamma) = \{z \in \mathbb{H} : d(z,p) \leq d(z,T(p)),\ \forall\ T \in \Gamma\}. \tag{2.1}$$

Como T é uma isometria temos que

$$d(z,T(p)) = d(T^{-1}(z),p).$$

Assim, para determinar $\mathfrak{D}_p(\Gamma)$ podemos considerar em cada órbita $\Gamma(w)$ os pontos mais próximos de p, ou seja,

$$\mathfrak{D}_p(\Gamma) = \{z \in \mathbb{H} : d(z,p) \leq d(T(z),p),\ \forall\ T \in \Gamma\}. \tag{2.2}$$

Além disso, para cada $T \in \mathrm{PSL}(2,\mathbb{R})$ fixado,

$$\{z \in \mathbb{H} : d(z,p) \leq d(z,T(p)\}$$

é o conjunto dos pontos z que estão mais próximos na métrica hiperbólica a p do que a $T(p)$. Como $p \in \mathfrak{D}_p(\Gamma)$, temos que $\mathfrak{D}_p(\Gamma)$ contém uma vizinhança de p, pois a órbita $\Gamma(p)$ é úm conjunto discreto. Portanto, $\mathring{\mathfrak{D}}_p(\Gamma) \neq \emptyset$.

Sejam $p, q \in \mathbb{H}$ pontos distintos. Chama-se de *bissetor perpendicular* do segmento geodésico $[p,q]$ a única geodésica passando por w e ortogonal a $\overline{pq}$, onde w é o ponto médio de $[p,q]$. Para cada $T \in \mathrm{PSL}(2,\mathbb{R})$ fixado, denotaremos o bissetor perpendicular do segmento geodésico $[p,T(p)]$ por

$$L_p(T) = \{z \in \mathbb{H} : d(z,p) = d(z,T(p))\},$$

o qual é a fronteira topológica de

$$H_p(T) = \{z \in \mathbb{H} : d(z,p) \leq d(z,T(p))\}.$$

Note que

$$\mathfrak{D}_p(\Gamma) = \bigcap_{T \in \Gamma} H_p(T),$$

onde $T \neq I$.

Lema 2.11 *A geodésica dada pela equação*

$$L_p = \{z \in \mathbb{H} : d(z,p) = d(z,q)\}$$

é o bissetor perpendicular do segmento geodésico $[p,q]$.

Prova. Pela Observação 1.6, podemos supor que $p = i$, $q = r^2 i$, com $r > 0$. Então $w = ri$ e o bissetor perpendicular é dado pela equação $|z| = r$. Por outro lado, considerando a equação 1.6, obtemos

$$d(z,p) = d(z,q) \Leftrightarrow \frac{|z-p|^2}{\mathrm{Im}(z)} = \frac{|z-q|^2}{r^2\,\mathrm{Im}(z)} \Leftrightarrow r^2\,|z-p|^2 = |z-q|^2$$

se, e somente se, $|z| = r$. ■

Proposição 2.12 *Sejam* Γ *é um grupo Fuchsiano e* $p \in \mathbb{H}$ *tal que* $T(p) \neq p$, *para todo* $T \in \Gamma - \{I\}$. *Então,* $\mathfrak{D}_p(\Gamma)$ *é uma região fundamental para* Γ.

Prova. Sejam $z \in \mathbb{H}$ e $\Gamma(z)$ a órbita de z. Como $\Gamma(z)$ é um conjunto discreto temos que existe $z_0 \in \Gamma(z)$ tal que à distância $d(z_0,p)$ seja a menor possível. Assim,

$$d(z_0,p) \leq d(T(z_0),p), \ \ \forall\ T \in \Gamma.$$

Logo, pela equação 2.2, $z_0 \in \mathfrak{D}_p(\Gamma)$. Portanto, $\mathfrak{D}_p(\Gamma)$ contém pelo menos um representante de cada órbita.

Agora, dados p e q no interior de $\mathfrak{D}_p(\Gamma)$, vamos provar que eles não podem pertencer à mesma órbita. Se

$$d(z,p) = d(T(z),p),$$

para algum $T \in \Gamma - \{I\}$, então

$$d(z,p) = d(z,T^{-1}(p)),$$

de modo que $z \in L_p(T^{-1})$. Então $z \notin \mathfrak{D}_p(\Gamma)$ ou $z \in \partial(\mathfrak{D}_p(\Gamma))$. Assim, se z pertence ao interior de $\mathfrak{D}_p(\Gamma)$, então

$$d(z,p) < d(T(z),p), \ \ \forall\ T \in \Gamma - \{I\}\,.$$

Portanto, se p e q estão em uma mesma órbita $\Gamma(z)$, então

$$d(z,p) < d(z,q) \ \text{ e } \ d(z,q) < d(z,p),$$

o que é uma contradição. Logo, o interior de $\mathfrak{D}_p(\Gamma)$ contém no máximo um representante de cada órbita. ■

Exemplo 2.13 *Seja* $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$. *Então*

$$\mathcal{F} = \left\{ z \in \mathcal{H} : |z| \geq 1 \ \ e \ \ |\mathrm{Re}(z)| \leq \frac{1}{2} \right\}$$

é uma região de Dirichlet $D_p(\Gamma)$, *com* $p = ki$, $k > 1$.

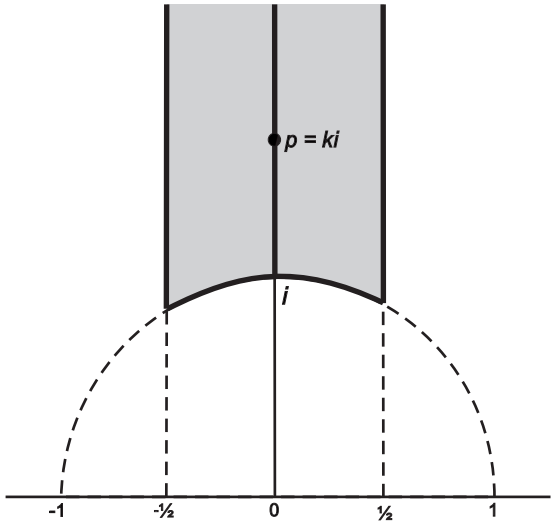

Figura 2.2: Região de Dirichlet para Γ centrada em $p = ki$.

Prova. É fácil verificar, que $T(p) \neq p$ para todo $T \in \Gamma - \{I\}$. Além disso, os lados geodésicos de $\mathcal{F}$ são bissetores dos segmentos

$$[p, T(p)]\,, \left[p, T^{-1}(p)\right] \text{ e } [p, S(p)]\,,$$

respectivamente. Logo, pelo Teorema 2.21, $\mathfrak{D}_p(\Gamma) \subseteq \mathcal{F}$. Suponhamos, por absurdo, que $\mathfrak{D}_p(\Gamma) \neq \mathcal{F}$, isto é, $\mathfrak{D}_p(\Gamma) \subset \mathcal{F}$. Então existem $z \in \mathring{\mathcal{F}}$ e $T \in \Gamma$ tais que $T(z) \in \mathring{\mathcal{F}}$. Como

$$T(z) = \frac{az + b}{cz + d}$$

temos que

$$\begin{aligned} |cz + d|^2 &= c^2 |z|^2 + 2\,\mathrm{Re}(z)cd + d^2 \\ &> c^2 + d^2 - |cd| \\ &= (|c| - |d|)^2 + |cd| > 0, \end{aligned}$$

pois $|z| > 1$, $\mathrm{Re}(z) > -\frac{1}{2}$ e $ad - bc = 1$. Logo,

$$|cz + d| > 1$$

e, consequentemente,

$$\mathrm{Im}\, T(z) = \frac{\mathrm{Im}(z)}{|cz + d|^2} < \mathrm{Im}(z).$$

O mesmo argumento substituindo z e T por $T(z)$ e T^{-1} nos dá a desigualdade contrária,

$$\mathrm{Im}\, z < \mathrm{Im}\, T(z),$$

o que é uma contradição. Portanto, $D_p(\Gamma) = \mathcal{F}$.

2.4 Círculos Isométricos e a Região Fundamental de Ford

Dada a isometria hiperbólica

$$T(z) = \frac{az+b}{cz+d} \in \mathrm{PSL}(2,\mathbb{R})$$

temos que sua derivada complexa é dada por

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

Assim, se tivermos uma curva diferenciável por partes $z = z(t)$ tal que $|cz(t)+d| \equiv 1$, então a integral de linha

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

isto é, o comprimento Euclidiano das curvas $z(t)$ e $(T \circ z)(t)$ coincidem. Disso decorre que a distância hiperbólica ao longo da curva e a distância euclidiana ao longo da mesma são preservadas. Logo, a restrição de T a esta curva é uma isometria Euclidiana.

Se $c \neq 0$, então

$$|cz+d| = 1 \Leftrightarrow \left|z + \frac{d}{c}\right| = \frac{1}{|c|},$$

isto é, o conjunto de pontos nos quais T age como isometrias tanto no sentido hiperbólico quanto no sentido Euclidiano é um semi-círculo Euclidiano de centro $-\frac{d}{c}$ e raio $r = \frac{1}{|c|}$.

Seja

$$T(z) = \frac{az+b}{cz+d} \in \mathrm{PSL}(2,\mathbb{R})$$

uma isometria de $\mathbb{H}$ com $c \neq 0$. Chamamos *círculo isométrico* de T ao conjunto

$$C_T = \{z \in \mathbb{H} : |cz+d| = 1\}.$$

Logo, se

$$T(z) = \frac{az+\overline{b}}{bz+\overline{a}} \in \mathbb{B}, \;\; b \neq 0,$$

então

$$C_T = \{z \in \mathbb{B} : \left|\overline{b}z + \overline{a}\right| = 1\}.$$

Se Γ é um grupo Fuchsiano cujos elementos são isometrias que preservam orientação no disco unitário $\mathbb{B}$, então por 1.9

$$T(z) = \frac{az+\overline{c}}{cz+\overline{a}}, \;\; |a|^2 - |c|^2 = 1, \;\; T \in \Gamma.$$

Logo, considerando

$$\check{C}_T = \{z \in \mathbb{C} : \left|\overline{b}z + \overline{a}\right| > 1\}.$$

Definimos

$$R_0 = \overline{\bigcap_{T \in \Gamma} \check{C}_T \cap \mathbb{B}}$$

Como sendo o fecho do conjunto de pontos em $\mathbb{B}$ que são exteriores aos circulos isométricos de todas as transformações do grupo Γ. R_0 estabelece uma região fundamental para Γ $[11, p.61]$, chamada *região fundamental de Ford*.

Proposição 2.14 *Os círculos isométricos C_T e $C_{T^{-1}}$ possuem o mesmo raio e C_T é levado em $C_{T^{-1}}$ pela transformação T.*

Prova. Verifique [11], página 58, Teorema 3.3.4.

Proposição 2.15 *Círculos isométricos são geodésicas em $\mathbb{H}$.*

Prova. Seja $T = \frac{az+b}{cz+d} \in \mathrm{PSL}(2,\mathbb{R})$. Então o centro de C_T é $\frac{-d}{c} \in \mathbb{R}$. Portanto, C_T é ortogonal ao o eixo real. ■

Um subgrupo $\Gamma \in \mathrm{PSL}(2,\mathbb{R})$ é chamado *elementar* se existir $z \in \overline{\mathbb{H}} = \mathbb{H} \cup \partial(\mathbb{H})$ tal que a órbita $\Gamma(z)$ é finita.

Teorema 2.16 *Seja Γ um grupo Fuchsiano não-elementar. Então, Γ possui elementos hiperbólicos.*

Prova. Verifique [5], página 69, Teorema 5.29.

Definição 2.17 *Sejam Γ um grupo Fuchsiano e $z \in \mathbb{H}$.*

1. *Chamamos de conjunto limite de Γ determinado por z ao conjunto*

$$\Lambda_z(\Gamma) = \{\xi \in \mathbb{H} : \xi \text{ é ponto de acumulação de } \Gamma(z)\}.$$

2. *Chamamos de conjunto limite de Γ ao conjunto*

$$\Lambda(\Gamma) = \bigcup_{z \in \mathbb{H}} \Lambda_z(\Gamma).$$

Exemplo 2.18 *Seja Γ o grupo gerado por $T(z) = 2z$. Então*

$$\lim_{n\to\infty} |T^n(z)| = \lim_{n\to\infty} 2^n |z| = \infty \text{ e } \lim_{n\to\infty} \left|T^{-n}(z)\right| = \lim_{n\to\infty} 2^{-n} |z| = 0$$

de modo que

$$\Lambda(\Gamma) = \Lambda_z(\Gamma) = \{0, \infty\}.$$

De modo genérico o conjunto limite satisfaz a seguinte propriedade essencial.

Teorema 2.19 *$\Lambda(\Gamma)$ é $\Gamma-$invariante, ou seja, dado $\xi \in \Lambda(\Gamma)$ e $T \in \Gamma$, $T(\xi) \in \Lambda(\Gamma)$.*

Prova. Considere $\xi \in \Lambda(\Gamma)$ e $T \in \Gamma$. Como $\xi \in \Lambda(\Gamma)$, existe uma sequência $(T_n)_{n=1}^{\infty}$ de elementos distintos de Γ tal que $T_n(z) \to \xi$. Como $TT_nT^{-1} \in \Gamma$ e

$$\left(TT_nT^{-1}\right)(T(z)) = T\left(T_n(z)\right) \to T(\xi)$$

concluimos que $T(\xi) \in \Lambda(\Gamma)$. ■

Teorema 2.20 *Seja Γ um grupo Fuchsiano e suponha que $\Lambda(\Gamma)$ possua mais do que dois pontos. Então uma das duas possibilidades ocorre.*

1. $\Lambda(\Gamma) = \partial_\infty \mathbb{H}$, *onde* $\partial_\infty \mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) = 0\} \cup \infty$.
2. $\Lambda(\Gamma)$ *é perfeito e magro (ou seja, todo ponto de* $\Lambda(\Gamma)$ *é ponto de acumulação de* $\Lambda(\Gamma)$*, e o complemtar de* $\Lambda(\Gamma)$ *é denso).*

Prova. Verifique [5], página 113, Teorema 7.15.

Diremos que um grupo Fuchsiano é de primeiro tipo se $\Lambda(\Gamma) = \partial_\infty \mathbb{H}$. O grupo Γ será dito de segundo tipo se $\Lambda(\Gamma) \neq \partial_\infty \mathbb{H}$.

2.5 Assinatura de um Grupo Fuchsiano

Sejam Γ um grupo Fuchsiano co-compacto e $\mathfrak{D}_{z_0}(\Gamma)$ uma região de Dirichlet de Γ. Existem em $\mathfrak{D}_{z_0}(\Gamma)$ um número finito de vértices, digamos r, que são pontos fixos de elementos elípticos de Γ (confira [5] seção 7.4 página 128). Se $m_1, \ldots, m_r$ são as ordens desses elementos elípticos e g o gênero da superfície compacta e orientável $\frac{\mathbb{H}}{\Gamma}$, então o conjunto ordenado de inteiros

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

é chamada a *assinatura* de Γ.

Caso o grupo Fuchsiano Γ não possua elementos elípticos, sua assinatura é

$$(g; 0, \ldots, 0)$$

ou, simplismente, $(g; -)$. O teorema que segue relaciona a área de $\frac{\mathbb{H}}{\Gamma}$ com a assinatura de Γ.

Teorema 2.21 *Seja Γ um grupo Fuchsiano co-compacto com assinatura $(g; m_1, \ldots, m_r)$. Então*

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

Prova. Verifique [11], página 91, Teorema 4.3.1.

Observe no Teorema anterior que se o grupo Γ não possuir elementos elípticos, então

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) = 2\pi\left[(2g-2)\right] = 4\pi(g-1).$$

O próximo Teorema afirma que se $\mathbb{X}$ é uma superfície compacta com gênero $g \geq 2$ então existe um grupo Fuchsiano Γ tal que $\mathbb{X} \equiv \frac{\mathbb{H}}{\Gamma}$.

Corolário 2.22 *Toda superfície compacta com gênero $g \geq 2$ pode ser modelada no plano hiperbólico.*

Prova. Verifique [5], página 113, Corolário 7.13.

No Capítulo 4 vamos considerar tesselações hiperbólicas. A partir dessas tesselações, iremos modelar no plano hiperbólico superfícies compactas orientáveis, de modo a obter os geradores dos grupos fuchsianos associados a reticulados hiperbólicos.

Definição 2.23 *Uma* tesselação regular *no plano hiperbólico é uma partição deste plano por polígonos regulares não sobrepostos, todos congruentes, sujeitos à restrião de somente se interceptarem em suas arestas ou vértices e de modo a termos o mesmo número de polígonos partilhando um mesmo vértice independente do vértice.*

Uma tesselação regular constituída de polígonos de p lados, onde cada vértice e recoberto por q polígonos será denotada por $\{p, q\}$. No caso em que $p = q$, a tesselação hiperbólica $\{p, q\}$ é chamada *auto-dual*.

Observação 2.24 *Como a soma dos ângulos internos de um triângulo hiperbólico é menor que* π, $\{p, q\}$ *é uma tesselação hiperbólica se, e somente se*

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

ou seja, se, e somente se

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

Por outro lado, como a soma dos ângulos internos de um triângulo euclidiano é igual a π, $\{p, q\}$ *é uma tesselação no plano Euclidiano, se, e somente se*

$$\frac{2\pi}{p} + \frac{2\pi}{q} = \pi$$

ou seja, se, e somente se

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

Capítulo 3

Álgebra dos Quatérnios e Grupos Fuchsianos Aritméticos

Neste capítulo, vamos considerar o conceito de álgebra dos quatérnios $\mathcal{A}$, bem como sua relação com grupos Fuchsianos aritméticos Γ. Para um tratamento mais completo, recomendamos os livros [4, 14, 19, 23].

3.1 Álgebras

O estudo de álgebras preocupa-se com objetos possuindo duas operações binárias e uma composição externa relacionadas pelas leis distributivas. O principal objetivo desta seção é apresentar os conceitos de álgebras, subálgebras, homomofismos de álgebras, dentre outros que serão necessários para as seções subseqüentes. Em toda esta seção, a palavra anel, salvo menção explícita em contrário, significa anel comutativo com identidade.

Definição 3.1 *Seja A um anel. Uma* álgebra H *sobre A ou uma A-*álgebra *é um anel H tal que $(H,+)$ é um A-módulo livre F e o seguinte axioma é satisfeito*

$$a(\alpha\beta) = (a\alpha)\beta = \alpha(a\beta), \ \ \forall \ a \in A \ \ e \ \ \alpha, \beta \in H.$$

Além disso, a álgebra H é comutativa se esta é comutativa sob sua estrutura de anel.O *posto* e uma *base* de uma A-álgebra H significa o posto e uma base, respectivamente, do A-módulo livre $(H,+) = F$.

Diremos que uma *álgebra H* é uma *A-álgebra com divisão* se todo elemento não nulo α em H tem um inverso em H, isto é,

$$\mathcal{U}(H) = H - \{0\}.$$

Sejam H uma A-álgebra e L um subconjunto não vazio de H. Diremos que L é uma *subálgebra* de H se L com as propriedades herdadas de H é uma A-álgebra ou, equivalentemente,

1. Se $\alpha, \beta \in L$, então $\alpha + \beta \in L$.

2. Se $a \in A$ e $\alpha \in L$, então $a\alpha \in L$.

3. Se $\alpha, \beta \in L$, então $\alpha\beta \in L$.

Proposição 3.2 (Álgebras com unidade) *Seja H um anel com identidade qualquer. Então H é uma K-álgebra com identidade e se, e somente se, existir um homomorfismo de anéis $f : A \to H$ tal que $f(A) \subseteq \mathcal{Z}(H)$ e $f(1) = e$. Em particular, $H = \mathbb{C}$ é uma $\mathbb{R}$-álgebra com unidade e $\mathbb{C} = f(A) = \mathcal{Z}(H)$.*

Prova. Suponhamos que H seja uma A-álgebra com identidade e. Então a função $f : A \to H$ definida por $f(a) = ae$ é um monomorfismo de anéis. De fato,

$$f(a+b) = (a+b)e = ae + be = f(a) + f(b)$$

e

$$f(ab) = (ab)e = a(be^2) = a(be)e) = (ae)(be) = f(a)f(b),$$

para todos $a, b \in A$.

Finalmente, dados $a, b \in A$,

$$\begin{aligned} f(a) &= f(b) \Rightarrow a\alpha = a(e\alpha) = (ae)\alpha = (be)\alpha = b(e\alpha) = b\alpha \\ &\Rightarrow (a-b)\alpha = 0, \ \forall \ \alpha \in H, \end{aligned}$$

isto é, $a = b$. Portanto,

$$A \simeq f(A) = \{ae : a \in A\}$$

é um subanel de H. Assim, $f(1) = 1e = e$ e $f(A) \subseteq \mathcal{Z}(H)$, pois

$$f(a)\alpha = (ae)\alpha = a(e\alpha) = a(\alpha e) = \alpha(ae) = \alpha f(a), \ \forall \ \alpha \in H.$$

Reciprocamente, vamos definir a composição externa de A sobre H por

$$a\alpha = f(a)\alpha, \ \forall \ a \in A \text{ e } \alpha \in H.$$

Agora, é fácil verificar os axiomas de A-módulo. ■

Exemplo 3.3 *Seja H uma A-álgebra. É fácil verificar que $\mathcal{Z}(H)$ é uma sub-álgebra comutativa de H. Se H é uma A-álgebra com unidade tal que $A = \mathcal{Z}(H)$, diremos que H é uma* A-álgebra central. *Em particular, se $\alpha \in \mathcal{U}(H)$ e $\alpha \in \mathcal{Z}(H)$, então $\alpha^{-1} \in \mathcal{Z}(H)$.*

Teorema 3.4 (Álgebras das Matrizes) *Sejam A um anel com unidade e $M_n(A)$ o conjunto de todas as matrizes $n \times n$ com entradas em A. Então, $M_n(A)$ é uma A-álgebra com unidade central e de dimensão n^2.*

Prova. É fácil verificar que o conjunto $M_{mn}(A)$ de todas as matrizes $m \times n$ com entradas em A munido com as operações de adição $\mathbf{A} + \mathbf{B}$ definida por

$$\mathbf{A} + \mathbf{B} = [a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$$

e composição externa $a\mathbf{A}$ definida por

$$a\mathbf{A} = a[a_{ij}] = [aa_{ij}]$$

é um A-módulo livre com base ordenada lexicograficamente

$$S = \{\mathbf{E}_{ij} : i, j = 1, \ldots, n\},$$

isto é,

$$\mathbf{E}_{11}, \ldots, \mathbf{E}_{1n}, \mathbf{E}_{21}, \ldots, \mathbf{E}_{2n}, \ldots, \mathbf{E}_{n1}, \ldots, \mathbf{E}_{nn}.$$

O produto dos elementos básicos em $M_n(A)$ é dado por

$$\mathbf{E}_{ij}\mathbf{E}_{kl} = \delta_{jk}\mathbf{E}_{il} = \begin{cases} \mathbf{E}_{il}, & \text{se } j = k \\ \mathbf{O}, & \text{se } j \neq k. \end{cases}$$

Assim, cada $\mathbf{A} \in M_n(A)$ pode ser escrito de modo único sob a forma

$$\mathbf{A} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\mathbf{E}_{ij}.$$

Observe que a função $f : A \to M_n(A)$ definida por $f(a) = a\mathbf{I}$ é um monomorfismo de anéis. Logo, $A \subseteq \mathcal{Z}(M_n(A))$. Por outro lado, dado $\mathbf{A} \in \mathcal{Z}(M_n(A))$, temos que

$$\mathbf{AB} = \mathbf{BA}, \ \forall \ \mathbf{B} \in M_n(A).$$

Em particular,

$$\mathbf{A}\mathbf{E}_{ij} = \mathbf{E}_{ij}\mathbf{A}, \ \ i, j = 1, \ldots, n.$$

Como

$$\begin{aligned} \mathbf{E}_{ij}\mathbf{A} &= \mathbf{E}_{ij}\left(\sum_{k=1}^{n}\sum_{l=1}^{n} a_{kl}\mathbf{E}_{kl}\right) = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{kl}\mathbf{E}_{ij}\mathbf{E}_{kl} \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n} a_{kl}\delta_{jk}\mathbf{E}_{il} = \sum_{l=1}^{n} a_{jl}\mathbf{E}_{il} = [b_{rs}], \end{aligned}$$

onde $b_{rs} = a_{jl}\delta_{ri}\delta_{sl}$, é a j-ésima linha de $\mathbf{A}$ e

$$\begin{aligned} \mathbf{A}\mathbf{E}_{ij} &= \left(\sum_{k=1}^{n}\sum_{l=1}^{n} a_{kl}\mathbf{E}_{kl}\right)\mathbf{E}_{ij} = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{kl}\mathbf{E}_{kl}\mathbf{E}_{ij} \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n} a_{kl}\delta_{li}\mathbf{E}_{kj} = \sum_{k=1}^{n} a_{ki}\mathbf{E}_{kj} = [c_{pq}], \end{aligned}$$

onde $c_{pq} = a_{ki}\delta_{pk}\delta_{qj}$, é a i-ésima coluna de $\mathbf{A}$, temos que

$$b_{rs} = c_{pq} \Rightarrow r = p = i = k, \ \ s = q = j = l \Rightarrow a_{jj} = a_{ii} \text{ e } a_{ij} = 0, \text{ se } i \neq j$$

Portanto, $\mathbf{A} = a\mathbf{I}$, para algum $a = a_{11} \in A$, isto é, $A = \mathcal{Z}(M_n(A))$. ■

Sejam H e L duas A-álgebras. Uma função $f : H \longrightarrow L$ é um *homomorfismo de A-álgebras* se as seguintes condições são satisfeitas:

1. $f(\alpha+\beta)=f(\alpha)+f(\beta)$, para todos $\alpha,\beta\in H$.

2. $f(a\alpha)=af(\alpha)$, para todo $\alpha\in H$ e $a\in A$.

3. $f(\alpha\beta)=f(\alpha)f(\beta)$, para todos $\alpha,\beta\in H$.

Diremos que H e L são *equivalentes* se existir um isomorfismo (*homomorfismo bijetivo de A-álgebras*) de álgebras de H sobre L. Se $\mathfrak{a}$ é um subconjunto não vazio de H, diremos que $\mathfrak{a}$ é um *ideal* de H se as seguintes condições são satisfeitas:

1. Se $\alpha,\beta\in\mathfrak{a}$, então $\alpha+\beta\in\mathfrak{a}$.

2. Se $a\in A$ e $\alpha\in\mathfrak{a}$, então $a\alpha\in\mathfrak{a}$ e $\alpha a\in\mathfrak{a}$.

3. Se $\lambda\in H$ e $\alpha\in\mathfrak{a}$, então $\lambda\alpha\in\mathfrak{a}$ e $\alpha\lambda\in\mathfrak{a}$.

Seja H uma A-álgebra. Diremos que H é uma *A-álgebra simples* se $H^2\neq\{0\}$ e os únicos ideais de H são $\{0\}$ e H. Note que, se H é uma A-álgebra com identidade, então $H^2\neq\{0\}$ é sempre verdadeiro.

Exemplo 3.5 *Toda A-álgebra com divisão é uma A-álgebra simples.*

Prova. Sejam H uma A-álgebra com divisão e $\mathfrak{a}$ um ideal de H. Suponhamos que $\mathfrak{a}\neq\{0\}$. Então $\mathfrak{a}$ contém um elemento não nulo $a\in H$. Logo, dado $\beta\in H$, obtemos

$$\beta=\beta e=(\beta\alpha^{-1})\alpha\in\mathfrak{a}.$$

Portanto, $\mathfrak{a}=H$.

3.2 Álgebra dos Quatérnios

Os grupos Fuchsianos que vamos considerar, são os grupos Fuchsianos derivados de uma álgebra $\mathcal{A}$. Para isto, veremos o conceito de álgebra dos quaternios e algumas de suas propriedades.

Teorema 3.6 *Seja K um corpo de característica $\neq 2$. Se $\mathcal{A}$ é uma álgebra com divisão não comutativa de dimensão 4 sobre K, então podemos escolher uma base 1, i, j e k para $\mathcal{A}$ satisfazendo*

$$i^2=a,\ \ j^2=b\ \ e\ \ k=ij=-ji,$$

onde $a,b\in K-\{0\}$. Neste caso, é usual dar-se a operação de multiplicação da álgebra $\mathcal{A}$ por meio de uma tábua de multiplicação

$\bullet$	1	i	j	k
1	1	i	j	k
i	i	a	k	aj
j	j	$-k$	b	$-bi$
k	k	$-aj$	bi	$-ab$

e estender isto por linearidade para uma multiplicação sobre $\mathcal{A}$.

Prova. Claramente todo elemento de $\mathcal{A}$ satisfaz um polinômio de grau menor do que ou igual a 4 com coeficientes em K. Se para algum $\alpha \in \mathcal{A}$ o polinômio minimal de α é de grau 4, então 1, α, α^2 e α^3 são linearmente independentes sobre K e, portanto, formam uma base de $\mathcal{A}$ sobre K. Como as potências de α comutam entre si teríamos que $\mathcal{A}$ é comutativo, o que é impossível. Logo, todo elemento em $\mathcal{A}$ satisfaz um polinômio de grau menor do que ou igual a 3 com coeficientes em K. Suponhamos agora que para algum $a \in \mathcal{A}$ o polinômio minimal é de grau 3. Então 1, α e α^2 são linearmente independetes sobre K e, além disso, existe $\beta \in \mathcal{A}$ tal que $\beta \notin K(\alpha)$. Assim, 1, α, α^2 e β formam uma base de $\mathcal{A}$ sobre K. Em particular, podemos escrever

$$\alpha\beta = c_0 + c_1\alpha + c_2\alpha^2 + c_3\beta$$

com $c_i \in K$, $i = 0, 1, 2, 3$, ou, equivalentemente

$$(\alpha - c_3)\,\beta = c_0 + c_1\alpha + c_2\alpha^2.$$

Como $\alpha \notin K$ temos que $\alpha - c_3 \neq 0$ e, portanto,

$$\beta = (\alpha - c_3)^{-1}\left(c_0 + c_1\alpha + c_2\alpha^2\right) \in K(\alpha),$$

o que é uma contradição. Logo, se $\alpha \in \mathcal{A}$ e $\alpha \notin K$, o polinômio minimal de α sobre K é quadrático.

Seja $\alpha \in \mathcal{A}$, $\alpha \notin K$. Então, 1 e α formam uma base de $K(\alpha)$ sobre K. Seja $\beta \in \mathcal{A}$ tal que $\beta \notin K(\alpha)$.

Afirmação. 1, α, β e $\alpha\beta$ são linearmente independentes sobre K.
De fato, suponhamos que

$$c_0 + c_1\alpha + c_2\beta + c_3\alpha\beta = 0$$

com $c_i \in K$, $i = 0, 1, 2, 3$. Então

$$(c_2 + c_3\alpha)\,\beta = -c_0 - c_1\alpha.$$

Se $c_2 + c_3\alpha = 0$, então $c_2 = c_3 = 0$, pois 1 e α são linearmente independentes, e consequentemente, $c_0 = c_1 = 0$. Se $c_2 + c_3\alpha \neq 0$, então

$$\beta = (c_2 + c_3\alpha)^{-1}(-c_0 - c_1\alpha) \in K(\alpha)$$

o que contradiz a escolha de β. Portanto, 1, α, β e $\alpha\beta$ formam uma base de $\mathcal{A}$ sobre K.

Agora, construiremos a partir desta base a base desejada. Já vimos que o polinômio de β sobre K é quadrático e a característica de K é $\neq 2$, então podemos escrever este polinômio sob a forma

$$x^2 + 2cx + d, \;\; c, d \in K.$$

Seja $j = \beta + c$. Então $j \notin K(\alpha)$, pois $\beta \notin K(\alpha)$. Assim, 1, α, j e αj formam uma base de $\mathcal{A}$ sobre K. Além disso,

$$j^2 = (\beta + c)^2 = \beta^2 + 2c\beta + c^2 = b,$$

onde $b = -d + c^2 \in K$. Seja $j_0 = \alpha^{-1} j \alpha$. Então $j_0 \neq j$, pois $\mathcal{A}$ é não comutativo, e

$$j_0^2 = \alpha^{-1} j^2 \alpha = \alpha^{-1} b \alpha = j^2.$$

Logo, para $x = j - j_0$, temos que

$$x \neq 0 \text{ e } xj + j_0 x = 0.$$

Portanto,

$$-j = x^{-1} j_0 x = (\alpha x^{-1}) j (\alpha x).$$

Seja $i = \alpha x$. Se $i \in K$ ou j é um polinômio em i, então j comuta com i e, consequentemente, $-j = j$, o que é impossível, pois a característica de K é $\neq 2$. Assim, $i \notin K$, $j \notin K(i)$ e 1, i, j e k formam uma base de $\mathcal{A}$ sobre K.

Agora, como $-j = i^{-1} j i$ temos que $-i = jij^{-1}$. Portanto, i e i^{-1} possuem o mesmo polinômio minimal. Como a característica de K é $\neq 2$ e o polinômio minimal de i é quadrático concluímos que $i^2 = a \in K$. ■

Observação 3.7 *Não é para toda escolha de a e b em K que o Teorema* 3.6 *determina uma álgebra com divisão $\mathcal{A}$ sobre K, com uma base $\{1, i, j, k\}$ de $\mathcal{A}$ satisfazendo*

$$i^2 = a, \ \ j^2 = b \ \text{ e } \ k = ij = -ji,$$

onde $a, b \in K - \{0\}$. Por exemplo, se a ou b for um quadrado em K uma tal álgebra não existe.

Proposição 3.8 *Seja $\mathcal{A}$ uma álgebra com divisão não comutativa de dimensão* 4 *sobre K. Então existe uma base* 1, *i, j e k para $\mathcal{A}$ satisfazendo*

$$i^2 = a, \ \ j^2 = b \ \text{ e } \ k = ij = -ji,$$

onde $a, b \in K - \{0\}$. Se $b \neq n(\alpha) = x_0^2 - a x_1^2$, para todo $\alpha = x_0 + x_1 i \in K(i)$, então, uma tal álgebra sempre existe.

Prova. Se $x \in \mathcal{A}^*$, então

$$x = x_0 + x_1 i + x_2 j + x_3 k = x_0 + x_1 i + (x_3 + x_4 i) j, \ \ x_0, x_1, x_2, x_3 \in K.$$

Assim, devemos provar que x é invertível. Se $x_3 + x_4 i = 0$, então $x = x_0 + x_1 i \neq 0$ é invertível em $K(i)$. Portanto, em $\mathcal{A}$. Se $x_3 + x_4 i \neq 0$, então $x_3 + x_4 i$ é invertível em $K(i)$ e

$$(x_3 + x_4 i)^{-1} x = (x_3 + x_4 i)^{-1} (x_0 + x_1 i) + j.$$

Logo, para provar que x é invertível basta mostrar que todo elemento da forma

$$y + zi + j$$

é invertível. Note que

$$(y + zi + j)(y - zi - j) = y^2 - az^2 - b \in K^*,$$

pois

$$y^2 - az^2 - b = 0 \Rightarrow b = y^2 - az^2,$$

o que é impossível. Portanto,

$$(y + zi + j)^{-1} = \frac{y - zi - j}{y^2 - az^2 - b}.$$

■

A álgebra $\mathcal{A}$ será denotada por

$$\mathcal{A} = \left(\frac{a, b}{K}\right) \text{ ou } \mathcal{A} = (a, b)_K.$$

A álgebra $\mathcal{A} = (a, b)_K$ obtida pela construção acima é chamada de *álgebra dos quatérnios* sobre K e a base $\{1, i, j, k\}$ é chamada de *base de definição* da álgebra. Os elementos de uma álgebra dos quatérnios são chamados de *quatérnios*, os elementos de K são chamados *quatérnios escalares* ou simplesmente *escalares* e os elementos de $[i, j, k]$ são chamados *quatérnios puros* ou simplesmente *puros*, o conjunto dos quatérnios puros será denotado por

$$\mathcal{A}_0 = \left(\frac{a, b}{K}\right)^0 = \{x_1 i + x_2 j + x_3 k : x_1, x_2, x_3 \in K\}.$$

Em particular, se $K = \mathbb{R}$ e $a = b = -1$, então a álgebra $\mathcal{A}$ é chamada a álgebra dos quaternios de Hamilton e denotada por $\mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$.

Sejam $\mathcal{A} = (a, b)_K$ uma álgebra sobre K e $x \in \mathcal{A}$, digamos

$$x = x_0 + x_1 i + x_2 j + x_3 k, \;\; x_0, x_1, x_2, x_3 \in K.$$

Então

$$\overline{x} = x_0 - x_1 i - x_2 j - x_3 k$$

chama-se o *conjugado* de x. Além disso, para quaisquer $x, y \in \mathcal{A}$ e $a \in K$, valem as seguintes propriedades:

$$\overline{ax} = a\overline{x}, \;\; \overline{x + y} = \overline{x} + \overline{y}, \;\; \overline{xy} = \bar{x}\bar{y} \text{ e } \overline{\overline{x}} = x.$$

A *norma reduzida* de x e o *traço reduzido* de x, denotados, respectivamente, por $N(x)$ e $\mathrm{Tr}(x)$, são definidos como

$$N(x) = x\overline{x} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \text{ e } \mathrm{Tr}(x) = x + \overline{x} = 2x_0 \tag{3.1}$$

Em particular, $N(x)$ e $\mathrm{Tr}(x)$ são escalares tais que

$$N(x) = N(\overline{x}) \text{ e } \mathrm{Tr}(x) = \mathrm{Tr}(\overline{x})$$

Observe que para quaisquer x e $y \in \mathcal{A}$ a função norma satisfaz

$$N(xy) = (xy)(\overline{xy}) = (xy)(\bar{x}\bar{y}) = (x\overline{x})(\overline{y}y) = N(x) \cdot N(y) \text{ e } N(1) = 1. \tag{3.2}$$

Finalmente, x é *puro* se, e somente se, $\overline{x} = -x$ e x é *escalar* se, e somente se, $\overline{x} = x$. Portanto,

$$x^2 = \begin{cases} -N(x) & \text{se } x \text{ é puro} \\ N(x) & \text{se } x \text{ é escalar} \end{cases}$$

ou seja, $x^2 \in K$ se, e somente se, x é puro ou é escalar.

Lema 3.9 *Seja $\mathcal{A} = (a,b)_K$ uma álgebra dos quatérnios. Então, $x \in \mathcal{A}$ é invertível se, e somente se, $N(x) \neq 0$. Neste caso,*

$$x^{-1} = \frac{1}{N(x)}\overline{x}.$$

Prova. Suponhamos que x^{-1} exista. Então

$$x^{-1}N(x) = x^{-1}(x\overline{x}) = \overline{x}.$$

Logo, $N(x) \neq 0$. Portanto, $\mathcal{A}$ é uma álgebra com divisão.

Reciprocamente, suponhamos que $N(x) \neq 0$. Então

$$[N(x)^{-1}\overline{x}]x = N(x)^{-1}\overline{x}x = N(x)^{-1}N(x) = 1,$$

e analogamente, $x[N(x)^{-1}\overline{x}] = 1$. Portanto, x é invertível. ■

Proposição 3.10 *A álgebra dos quatérnios $\mathcal{A} = (a,b)_K$ é uma álgebra central simples.*

Prova. Seja

$$x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{Z}(\mathcal{A}),\ \ x_0, x_1, x_2, x_3 \in K,$$

Então,

$$0 = xk - kx = 2(x_1 i + x_2 j)k \Rightarrow x_1 = x_2 = 0.$$

De modo análogo, prova-se que $x_3 = 0$. Portanto, $\mathcal{Z}(\mathcal{A}) = K$. Finalmente, sejam $\mathfrak{a}$ um ideal de $\mathcal{A}$ e

$$x = x_0 + x_1 i + x_2 j + x_3 k \in \mathfrak{a} - \{0\},\ \ x_0, x_1, x_2, x_3 \in K.$$

Se $x_1 = x_2 = x_3 = 0$, então $x = x_0 \in K^*$ e $1 = xx^{-1} = x^{-1}x \in \mathfrak{a}$, ou seja, $\mathfrak{a} = \mathcal{A}$. Se $x_l \neq 0$, para algum $l = 1, 2, 3$, então

$$xk - kx = 2(x_1 i + x_2 j)k \in \mathfrak{a}.$$

Logo

$$y = x_1 i + x_2 j \in \mathfrak{a}.$$

Assim,

$$yj + jy = 2x_2 b \in \mathfrak{a}.$$

Como $2x_2 b \in K$ temos que $\mathfrak{a} = \mathcal{A}$. Portanto, $\mathcal{A} = (a,b)_K$ é uma álgebra central simples. ■

Proposição 3.11 *Seja H uma álgebra qualquer sobre K. Sejam $u, v \in H$ tais que*

$$u^2 = a, \;\; v^2 = b \;\; e \;\; uv = -vu,$$

onde $a, b \in K - \{0\}$. Então, o subespaço gerado por 1, u, v e uv é uma sub-álgebra de H isomorfa a $(a, b)_K$, isto é,

$$[1, u, v, uv] = \{x_0 + x_1u + x_2v + x_3uv : x_0, x_1, x_2, x_3 \in K\} \simeq \mathcal{A} = \left(\frac{a, b}{K}\right).$$

Prova. Seja $D = [1, u, v, uv]$. Então é fácil verificar, usando a tábua de multiplicação, que D é um anel e, portanto, uma álgebra sobre K. Seja

$$\varphi : \mathcal{A} \to D$$

definida por

$$\varphi(1) = 1, \;\; \varphi(i) = u, \;\; \varphi(j) = v \;\; \text{e} \;\; \varphi(k) = uv.$$

Então φ é um homomorfismo de álgebra sobrejetor e

$$\ker \varphi = \{x \in \mathcal{A} : \varphi(x) = 0\}$$

é um ideal de $\mathcal{A}$. Portanto, $\ker \varphi = \{0\}$ e φ é injetora, pois $\varphi \neq 0$. ■

Exemplo 3.12 *A álgebra*

$$\left(\frac{1, -1}{K}\right) \simeq M_2(K).$$

Neste caso, $(1, -1)_K$ não é uma álgebra com divisão.

Solução. Seja $\mathbf{E}_{11}, \mathbf{E}_{12}, \mathbf{E}_{21}$ e $\mathbf{E}_{22}$ a base definindo $M_2(K)$. Consideremos as matrizes

$$\mathbf{I} = \mathbf{E}_{11} + \mathbf{E}_{22}, \;\; \mathbf{M} = \mathbf{E}_{21} + \mathbf{E}_{12} \;\; \text{e} \;\; \mathbf{N} = \mathbf{E}_{21} - \mathbf{E}_{12}.$$

Então

$$\mathbf{M}^2 = \mathbf{I}, \;\; \mathbf{N}^2 = -\mathbf{I} \;\; \text{e} \;\; \mathbf{MN} = -\mathbf{NM}.$$

Portanto, pela Proposição 3.11,

$$M_2(K) = \{x_0\mathbf{I} + x_1\mathbf{M} + x_2\mathbf{N} + x_3\mathbf{MN} : x_0, x_1, x_2, x_3 \in K\} \simeq \left(\frac{1, -1}{K}\right).$$

Lema 3.13 *Seja $\mathcal{A} = (a, b)_K$ uma álgebra dos quatérnios. Então, $x \in \mathcal{A}^*$ é puro se, e somente se, $x^2 \in \mathcal{Z}(\mathcal{A})$, mas $x \notin \mathcal{Z}(\mathcal{A})$.* ■

Proposição 3.14 *Sejam $\mathcal{A}_1$, $\mathcal{A}_2$ duas álgebras de quatérnios e $\varphi : \mathcal{A}_1 \to \mathcal{A}_2$ um isomorfismo de álgebras.*

1. *Se $x \in \mathcal{A}_1$ é puro, então $\varphi(x) \in \mathcal{A}_2$ é puro.*

2. Para cada $x \in \mathcal{A}_1$,

$$\overline{\varphi(x)} = \varphi(\overline{x}), \;\; N(\varphi(x)) = \varphi(N(x)) \;\; e \;\; \mathrm{Tr}(\varphi(x)) = \varphi(\mathrm{Tr}(x)).$$

Prova. Vamos provar apenas o item (2). Dado $x \in \mathcal{A}_1$ com $x = x_0 + y$, onde $y \in \mathcal{A}^*$ é puro. Logo, pelo item (1), $\varphi(y)$ é puro. Assim,

$$\overline{\varphi(x)} = \overline{\varphi(x_0) + \varphi(y)} = \overline{\varphi(x_0)} + \overline{\varphi(y)} = \varphi(x_0) - \varphi(y) = \varphi(x_0 - y) = \varphi(\overline{x}).$$

De modo análogo, prova-se que $\mathrm{Tr}(\varphi(x)) = \varphi(\mathrm{Tr}(x))$. ■

Proposição 3.15 *Sejam $a, b, s, t \in K^*$. Então*:

1.
$$\left(\frac{1, a}{K}\right) \simeq \left(\frac{1, -1}{K}\right) \simeq \left(\frac{a, -a}{K}\right) \simeq \left(\frac{a, 1-a}{K}\right).$$

2.
$$\left(\frac{b, a}{K}\right) \simeq \left(\frac{a, b}{K}\right) \simeq \left(\frac{as^2, bt^2}{K}\right).$$

3.
$$\left(\frac{a, ab}{K}\right) \simeq \left(\frac{a, -b}{K}\right).$$

Prova. Vamos provar apenas o item (2). Seja $\{1, i, j, k\}$ a base definindo $(a, b)_K$. Consideremos $u = si$ e $v = tj$. Então

$$u^2 = as^2, \;\; v^2 = bt^2 \;\text{ e }\; uv = -vu.$$

Portanto, pela Proposição 3.11,

$$\left(\frac{as^2, bt^2}{K}\right) = \{x_0 + x_1 u + x_2 v + x_3 uv : x_0, x_1, x_2, x_3 \in K\} \simeq \left(\frac{a, b}{K}\right).$$

■

Seja $\mathcal{A} = (a, b)_K$ uma álgebra dos quatérnios. Então

$$\frac{1}{2}[N(x+y) - N(x) - N(y)] = \frac{1}{2}(x\overline{y} + y\overline{x}) = \frac{1}{2}\,\mathrm{Tr}(x\overline{y}) \in K, \;\; \forall \;\; x, y \in \mathcal{A}.$$

Assim, a função $B : \mathcal{A} \times \mathcal{A} \to K$ definida por

$$B(x, y) = \frac{1}{2}\,\mathrm{Tr}(x\overline{y})$$

é claramente uma forma bilinear simétrica sobre $\mathcal{A}$ não degenerada e a forma quadrática associada $q : \mathcal{A} \to K$ é dada por

$$q(x) = B(x, x) = N(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2, \;\; \forall \;\; x \in \mathcal{A}.$$

Note que se x é escalar e y é puro, então $x\overline{y}$ é puro, pois $x\overline{y} = \overline{xy} = -xy$. Logo,

$$B(x, y) = \frac{1}{2}\,\mathrm{Tr}(x\overline{y}) = 0.$$

Se x e y são puros, então

$$B(x,y) = \frac{1}{2}(x\overline{y} + y\overline{x}) = -\frac{1}{2}(xy + yx).$$

Assim,

$$B(x,y) = 0 \Leftrightarrow xy = -yx.$$

Finalmente, $q(x) = x^2$ se x é escalar e $q(x) = -x^2$ se x é puro. Portanto, o discriminante de $\mathcal{A}$ é igual a

$$d(\mathcal{A}) = \Delta(1,i,j,k) = \det\left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & -b & 0 \\ 0 & 0 & 0 & ab \end{bmatrix}\right)(K^*)^2 = (ab)^2(K^*)^2 = 1,$$

pois pela Proposição A.5 $d(\mathcal{A}) = \det(M)(K^*)^2$ (onde M é a matriz simétrica associada a B) é um elemento do grupo quociente

$$\frac{K^*}{(K^*)^2}.$$

Além disso, notamos que $\{1,i,j,k\}$ é uma base ortogonal de $\mathcal{A}$ com relação a B.

3.3 Ordens

Em toda esta seção, salvo menção explícita em contrário, K é um corpo de números algébricos totalmente real e $\mathbb{I}_K$ é o anel dos inteiros de K.

Sejam

$$\mathcal{A} = \left(\frac{a,b}{K}\right)$$

um álgebra dos quatérnios e $\mathbf{E}_{11}, \mathbf{E}_{12}, \mathbf{E}_{21}$ e $\mathbf{E}_{22}$ a base definindo $M_2\left(K(\sqrt{a})\right)$. Considere as matrizes

$$\mathbf{I} = \mathbf{E}_{11} + \mathbf{E}_{22},\ \ \mathbf{M} = \sqrt{a}(\mathbf{E}_{11} - \mathbf{E}_{22})\ \text{ e }\ \mathbf{N} = b\mathbf{E}_{12} + \mathbf{E}_{21}.$$

Então

$$\mathbf{M}^2 = a\mathbf{I},\ \ \mathbf{N}^2 = b\mathbf{I}\ \text{ e }\ \mathbf{MN} = -\mathbf{NM}.$$

Portanto, pela Proposição 3.11, existe uma sub-álgebra $[\mathbf{I},\mathbf{M},\mathbf{N},\mathbf{MN}]$ de $M_2\left(K(\sqrt{a})\right)$ tal que

$$[\mathbf{I},\mathbf{M},\mathbf{N},\mathbf{MN}] = \{x_0\mathbf{I} + x_1\mathbf{M} + x_2\mathbf{N} + x_3\mathbf{MN} : x_0,x_1,x_2,x_3 \in K\} \simeq \left(\frac{a,b}{K(\sqrt{a})}\right).$$

A imersão

$$\varphi : \left(\frac{a,b}{K}\right) \to M_2\left(K(\sqrt{a})\right)$$

definida por

$$\varphi(1) = \mathbf{I},\ \ \varphi(i) = \mathbf{M},\ \ \varphi(j) = \mathbf{N}\ \text{ e }\ \varphi(k) = \mathbf{MN}$$

é chamada de *imersão de Cayley*. Portanto, cada elemento

$$x \in \left(\frac{a,b}{K}\right)$$

pode ser identificado com

$$x \leftrightarrow \varphi(x) = g_x = \begin{pmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{pmatrix}.$$

Observe que $N(x) = \det(g_x)$ e $\mathrm{Tr}(x) = \mathrm{Tr}(g_x)$.

Observação 3.16 *Se a é um quadrado, isto é, $a = t^2$, para algum $t \in K - \{0\}$, então $\mathcal{A} \simeq M_2(K)$. Caso contrário, $\mathcal{A} \simeq [\mathbf{I}, \mathbf{M}, \mathbf{N}, \mathbf{MN}]$ é uma sub-álgebra com divisão de $M_2(K(\sqrt{a}))$.*

Lema 3.17 *Sejam $b = p$ um número primo e a qualquer resíduo não quadrático módulo p. Então*

$$\mathcal{A} = \left(\frac{a,b}{\mathbb{Q}}\right)$$

é uma álgebra com divisão.

Prova. Suponhamos, por absurdo, que $\mathcal{A}$ não seja uma álgebra com divisão. Então, pelo Lema 3.9, existe $x \in \mathcal{A}$, $x \neq 0$ tal que

$$x_0^2 - x_1^2 a - x_2^2 p + x_3^2 ap = 0 \tag{3.3}$$

e podemos supor, sem perda de generalidade, que

$$x_0, x_1, x_2 \text{ e } x_3$$

sejam relativamente primos. Então

$$x_0^2 \equiv a x_1^2 \,(\mathrm{mod}\, p)\,. \tag{3.4}$$

Se $p \nmid x_1$, então x_1^2 é um resíduo quadrático módulo p, o que é impossível, pois ax_1^2 não é um resíduo quadrático módulo p. Logo, $p \mid x_1$ e$p \mid x_0$. Assim,

$$x_2^2 \equiv a x_3^2 \,(\mathrm{mod}\, p)\,.$$

De modo análogo, $p \mid x_2$ e $p \mid x_3$, o que é uma contradição. ■

Sejam

$$\mathcal{A} = \left(\frac{a,b}{K}\right)$$

uma álgebra dos quatérnios sobre K e $\varphi : K \to F$ uma imersão de corpos. Definimos

$$\mathcal{A}^\varphi = \left(\frac{\varphi(a), \varphi(b)}{\varphi(K)}\right) \text{ e } \mathcal{A}^\varphi \otimes F = \left(\frac{\varphi(a), \varphi(b)}{F}\right),$$

onde $\mathcal{A}^{\varphi} \otimes F$ denota o produto tensorial da álgebra $\mathcal{A}^{\varphi}$ com F. Assim, definindo

$$\psi : \mathcal{A} \otimes_{\varphi} F \to \mathcal{A}^{\varphi} \otimes F$$

por

$$\psi((x_0 + x_1 i + x_2 j + x_3 k) \otimes \alpha) = \alpha(\varphi(x_0) + \varphi(x_1)u + \varphi(x_2)v + \varphi(x_3)uv)$$

onde $\{1, i, j, k\}$ e $\{1, u, v, uv\}$ são bases definindo $\mathcal{A}$ e $\mathcal{A}^{\varphi} \otimes F$, respectivamente. Então ψ é um isomorfismo de álgebras, de modo que

$$\mathcal{A} \otimes_{\varphi} F \simeq \mathcal{A}^{\varphi} \otimes_{\varphi} F.$$

Portanto, o produto tensorial $\mathcal{A}^{\varphi} \otimes_{\varphi} F$ continua sendo uma álgebra central simples. Para cada imersão de corpos $\varphi : K \to F$ chamamos

$$\mathcal{A}^{\varphi} = \left(\frac{\varphi(a), \varphi(b)}{\varphi(K)}\right)$$

de *lugar da álgebra dos quatérnios* $\mathcal{A}$.

Como K é um corpo de números algébricos totalmente real temos que $[K, \mathbb{Q}] = n$ e as n imersões distintas $\varphi_i : K \to \mathbb{C}$ são tais que $\varphi_i(K) \subset \mathbb{R}$, ou seja, são imersões de K em $\mathbb{R}$. Portanto, os n lugares distintos são definidos pelos $\mathbb{R}$-isomorfismos

$$\rho_1 : \mathcal{A}^{\varphi_1} \otimes \mathbb{R} \to M(2, \mathbb{R}) \text{ e } \rho_i : \mathcal{A}^{\varphi_i} \otimes \mathbb{R} \to \mathcal{H} \tag{3.5}$$

onde φ_i é uma imersão de K em $\mathbb{R}$, $i = 2, ..., n$ e $\varphi_1 = I$ é a identidade. Diremos que $\mathcal{A}$ é *não ramificada* ou *fatorável* no lugar φ_1 e *ramificada* nos lugares infinitos φ_i, $2 \leq i \leq n$, isto é,

$$\left(\frac{a, b}{K}\right) \otimes \mathbb{R} \simeq \left(\frac{\varphi_1(a), \varphi_1(b)}{\mathbb{R}}\right) \simeq M_2(\mathbb{R}) \text{ e } \left(\frac{a, b}{K}\right) \otimes \mathbb{R} \simeq \left(\frac{\varphi_i(a), \varphi_i(b)}{\mathbb{R}}\right) \simeq \mathcal{H}.$$

Dado $x \in \mathcal{A}$, verificamos através cálculos simples que

$$N(x) = \det(\rho_1(x)) \text{ e } \operatorname{Tr}(x) = \operatorname{tr}(\rho_1(x)). \tag{3.6}$$

Neste caso, identificando

$$x_j \leftrightarrow \rho_i(x_j),$$

com $j = 0, 1, 2, 3$ e $2 \leq i \leq n$, obtemos

$$\varphi_i(N(x)) = N_{\mathcal{H}}(\rho_i(x)) \text{ e } \varphi_i(\operatorname{Tr}(x)) = \operatorname{Tr}_{\mathcal{H}}(\rho_i(x)). \tag{3.7}$$

Exemplo 3.18 *Sejam*

$$\mathcal{H} = \left(\frac{-1, -1}{\mathbb{R}}\right) \text{ e } \mathcal{H}^1 = \{x \in \mathcal{H} : N(x) = 1\}.$$

Então

$$\operatorname{Tr}_{\mathcal{H}}(\mathcal{H}^1) = \{\operatorname{Tr}_{\mathcal{H}}(x) : x \in \mathcal{H}^1\} = [-2, 2].$$

De fato, dado

$$x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{H}^1,$$

obtemos

$$N(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1.$$

Logo,

$$\text{Tr }_{\mathcal{H}}(x) = 2x_0 \in [-2, 2]\,,$$

pois $|x_0| \leq 1$. *A recíproca é clara. Portanto,* $\text{Tr }_{\mathcal{H}}(\mathcal{H}^1) = [-2, 2]$.

Teorema 3.19 *Seja* $\mathcal{A}$ *uma álgebra dos quaténios sobre* K *satisfazendo* (3.5). *Se* $K \neq \mathbb{Q}$, *então* $\mathcal{A}$ *é uma álgebra com divisão.*

Prova. Suponhamos, por absurdo, que $\mathcal{A}$ não seja uma álgebra com divisão. Então pelo Exemplo 3.12

$$\mathcal{A} \simeq \left(\frac{1,1}{K}\right) \simeq M_2(K).$$

Como $[K, \mathbb{Q}] = n > 1$ temos que

$$\mathcal{A}^{\varphi_i} \simeq \left(\frac{1,1}{\varphi_i(K)}\right) \simeq M_2(\varphi_i(K)),\ \ \forall\ i > 1.$$

Portanto,

$$\mathcal{A}^{\varphi_i} \otimes \mathbb{R} \simeq M_2(\mathbb{R}) \not\simeq \mathcal{H},$$

o que é uma contradição. ■

Sejam V um espaço vetorial qualquer sobre K de dimensão finita e M um subconjunto de V que é um $\mathbb{I}_K$-módulo com as operações induzidas de V. Definimos

$$KM = \{\alpha x : \alpha \in K,\ \ x \in M\}\,.$$

Como M é um $\mathbb{I}_K$-módulo e K é o corpo quociente de $\mathbb{I}_K$ (ver [3]) temos que

$$KM = \left\{a^{-1}x : a \in \mathbb{I}_K,\ \ a \neq 0,\ \ x \in M\right\}.$$

Portanto, KM é um subespaço de V, ou seja,

$$KM = [M] = \left\{\sum_{i=1}^{m} a_i x_i : m \in \mathbb{N},\ \ a_i \in K \text{ e } x_i \in M\right\}.$$

Um $\mathbb{I}_K$-módulo M chama-se um *reticulado* em V se existir uma base

$$\beta = \{x_1, \ldots, x_n\}$$

de V tal que

$$M \subseteq \mathbb{I}_K x_1 + \cdots + \mathbb{I}_K x_n = \{a_1 x_1 + \cdots + a_n x_n : a_i \in \mathbb{I}_K\}.$$

Diremos que M é um *reticulado completo* em V se, além disso,

$$KM = V.$$

Em particular,

$$\mathbb{I}_K x_1 + \cdots + \mathbb{I}_K x_n = \{a_1 x_1 + \cdots + a_n x_n : a_i \in \mathbb{I}_K\}$$

é um reticulado completo em V.

Como K é um espaço vetorial sobre K temos que K é um $\mathbb{I}_K$-módulo com as operações induzidas. Seja $\mathfrak{a}$ um subconjunto de K com $\mathfrak{a} \neq \{0\}$. Diremos que $\mathfrak{a}$ é um *ideal fracionário* de K se as seguintes condições são satisfeitas:

1. $\mathfrak{a}$ é $\mathbb{I}_K$-módulo.

2. Existe $b \in \mathbb{I}_K^*$ tal que $b\mathfrak{a} \subseteq \mathbb{I}_K$.

Note que isto é equivalente a: $\mathfrak{a}$ é um reticulado completo em K tal que $K\mathfrak{a} = K$. Portanto, qualquer ideal de $\mathbb{I}_K$ é necessariamente um ideal fracionário de K, pois é possível provar que $\mathbb{I}_K$ é um anel Noetheriano.

Observação 3.20 *Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais fracionários de K, então*

$$\mathfrak{a} + \mathfrak{b}, \ \ \mathfrak{ab}, \ \ \mathfrak{a} \cap \mathfrak{b} \ \ e \ \ \mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathbb{I}_K\}$$

são ideais fracionários de K. Portanto, o conjunto de todos os ideais fracionários de K forma um grupo com a operação binária $\mathfrak{ab}$, elemento identidade $\mathbb{I}_K$ e elemento inverso $\mathfrak{a}^{-1}$.

Lema 3.21 *Sejam V um espaço vetorial qualquer sobre K de dimensão finita e L um reticulado completo em V. Então um $\mathbb{I}_K$-módulo M em V é um reticulado em V se, e somente se, existe $b \in \mathbb{I}_K^*$ tal que $bM \subseteq L$.*

Prova. Suponhamos que M seja um $\mathbb{I}_K$-reticulado em V. Então existe uma base

$$\beta = \{x_1, \ldots, x_n\}$$

de V tal que

$$M \subseteq \mathbb{I}_K x_1 + \cdots + \mathbb{I}_K x_n.$$

Como L um reticulado completo em V temos que L contém uma base

$$\gamma = \{y_1, \ldots, y_n\}$$

de V. Logo, existem únicos $r_{ij} \in K$ tais que

$$x_j = \sum_{i=1}^{n} r_{ij} y_i, \ \ j = 1, \ldots, n.$$

Fazendo

$$r_{ij} = \frac{a_{ij}}{b_{ij}} \text{ e } b_j = b_{1j}b_{2j}\cdots b_{nj} \in \mathbb{I}_K^*,$$

obtemos $b_j r_{ij} \in \mathbb{I}_K$, para todos i e j. (Neste caso, o conjunto gerado pelos r_{ii} é um ideal fracionário de K). Assim, existe $b = b_1 b_2 \cdots b_n \in \mathbb{I}_K^*$ tal que

$$bx_j \subseteq \mathbb{I}_K y_1 + \cdots + \mathbb{I}_K y_n \subseteq L.$$

Portanto, existe $b \in \mathbb{I}_K^*$ tal que $bM \subseteq L$.

Reciprocamente, suponhamos que existe $b \in \mathbb{I}_K^*$ tal que $bM \subseteq L$. Como L um reticulado completo em V temos que L contém uma base

$$\gamma = \{z_1, \ldots, z_n\}$$

de V tal que

$$L \subseteq \mathbb{I}_K z_1 + \cdots + \mathbb{I}_K z_n.$$

Então

$$M \subseteq b^{-1}L \subseteq \mathbb{I}_K(b^{-1}z_1) + \cdots + \mathbb{I}_K(b^{-1}z_n).$$

Portanto, M é um reticulado em V. ■

Corolário 3.22 *Sejam V um espaço vetorial qualquer sobre K de dimensão finita e U um subespaço de V com $M \subseteq U \subseteq V$. Então M é um reticulado em V se, e somente se, M é um reticulado em U.*

Prova. Como U é um subespaço de V temos que U contém uma base

$$\alpha = \{x_1, \ldots, x_k\}$$

que é parte de uma base

$$\beta = \{x_1, \ldots x_k, x_{k+1}, \ldots, x_n\}$$

de V Fazendo

$$L_1 = \mathbb{I}_K x_1 + \cdots + \mathbb{I}_K x_k \text{ e } L = \mathbb{I}_K x_1 + \cdots + \mathbb{I}_K x_n.$$

Assim, se M é um reticulado em U, então existe $b \in \mathbb{I}_K^*$ tal que $bM \subseteq L_1 \subseteq L$. Portanto, M é um reticulado em V.

Reciprocamente, suponhamos que M seja um reticulado em V. Então existe $b \in \mathbb{I}_K^*$ tal que $bM \subseteq L$. Logo,

$$bM \subseteq L \cap U = L_1,$$

pois $M \subseteq U$. Portanto, M é um reticulado em U. ■

Observação 3.23 *Sejam V um espaço vetorial qualquer sobre K de dimensão finita.*

1. *Qualquer $\mathbb{I}_K$-submódulo de um reticulado M em V é um reticulado.*

2. *Se M e L são reticulados em V, então $M \cap L$ é um reticulado em V. Além disso, aM, $\mathfrak{a}M$ e $M + L$ são reticulados, para todo $a \in K$ e ideal fracionário $\mathfrak{a}$ de K, onde*

$$\mathfrak{a}M = \left\{ \sum_{i=1}^{m} a_i x_i : m \in \mathbb{N},\ a_i \in \mathfrak{a} \ \text{ e } \ x_i \in M \right\}.$$

3. *É claro que $\mathbb{I}_K x$ e $x\mathbb{I}_K$ são reticulados em V, para todo $x \in K$. Portanto,*

$$\mathfrak{a}_1 z_1 + \cdots + \mathfrak{a}_k z_k$$

é um reticulado em V, para todo ideal fracionário $\mathfrak{a}_i$ de K e $z_i \in K$. Em particular, qualquer $\mathbb{I}_K$-módulo finitamente gerado em V é um reticulado em V.

Seja $\mathcal{O}$ um subanel de $\mathcal{A}$ com a mesma unidade de $\mathcal{A}$. Diremos que $\mathcal{O}$ é uma $\mathbb{I}_K$-*ordem* em $\mathcal{A}$ se $\mathcal{O}$ é um $\mathbb{I}_K$-módulo finitamente gerado e

$$\mathcal{A} = K\mathcal{O}$$

ou, equivalentemente, $\mathcal{O}$ é um reticulado completo em $\mathcal{A}$. Às vezes, chamamos uma $\mathbb{I}_K$-ordem $\mathcal{O}$ em $\mathcal{A}$ de *reticulado hiperbólico*. Note que $xy \in \mathcal{O}$, para todos $x, y \in \mathcal{O}$, e qualquer elemento $x \in \mathcal{O}$ é inteiro sobre $\mathbb{I}_K$, pois $\mathbb{I}_K[x] \subseteq \mathcal{O}$ é um $\mathbb{I}_K$-módulo finitamente gerado. Portanto,

$$N(x), \mathrm{Tr}(x) \in \mathbb{I}_K, \ \ \forall \ x \in \mathcal{O}.$$

Observação 3.24 *Seja*

$$M = \mathbb{I}_K x_0 + \mathbb{I}_K x_1 + \mathbb{I}_K x_2 + \mathbb{I}_K x_3.$$

Então M é um reticulado em $\mathcal{A}$. Assim, os conjuntos

$$\mathcal{O}_E(M) = \{x \in \mathcal{A} : xM \subset M\} \ \text{ e } \ \mathcal{O}_D(M) = \{x \in \mathcal{A} : Mx \subset M\}$$

são ordens em $\mathcal{A}$, pois são subanéis de $\mathcal{A}$ e $\mathbb{I}_K$-submódulos de M.

Exemplo 3.25 *Seja $\mathcal{A} = (a, b)_K$ uma álgebra dos quatérnios.*

1. *Se $a = b = -1$ e $K = \mathbb{Z}$, então $\mathcal{O} = (-1, -1)_{\mathbb{Z}}$ é uma $\mathbb{Z}$-ordem em $\mathcal{A}$. Além disso, $\mathcal{O}_0 = \mathcal{O} + \alpha\mathbb{Z} = [1, i, j, \alpha]$, onde*

$$\alpha = \frac{1 + i + j + ij}{2}$$

é uma $\mathbb{Z}$-ordem em $\mathcal{A}$ tal que $\mathcal{O} \subset \mathcal{O}_0$.

2. *Se $\mathcal{A} = M_2(K)$, então $\mathcal{O} = M_2(\mathbb{I}_K)$ é uma $\mathbb{I}_K$-ordem em $\mathcal{A}$.*

Seja $\mathcal{O}$ uma $\mathbb{I}_K$-ordem em $\mathcal{A}$. O *discriminante* de $\mathcal{O}$, denotado por $d(\mathcal{O})$, é igual a raiz quadrada do ideal em $\mathbb{I}_K$ gerado pelo conjunto

$$\left\{ \det(\mathrm{Tr}(x_i \cdot \overline{x_j})) : 0 \leq i, j \leq 3 \right\}. \tag{3.8}$$

onde $x_i \in \mathcal{O}$. Note que $d(\mathcal{O}) \neq \{0\}$, pois a forma bilinear associada a Tr é não degenerada.

Proposição 3.26 *Seja $\mathcal{O}$ uma $\mathbb{I}_K$-ordem em $\mathcal{A}$. Se $\mathcal{O}$ possui uma base $\{u_1, u_2, u_3, u_4\}$, então*

$$d(\mathcal{O}) = [\det(\mathrm{Tr}(u_i u_j))]^{\frac{1}{2}} = [\det(\mathrm{Tr}(u_i u_j))a : \exists \ \ a \in \mathbb{I}_K]^{\frac{1}{2}}$$

Prova. Claramente

$$[\det(\mathrm{Tr}(u_i u_j))]^{\frac{1}{2}} \subseteq d(\mathcal{O}).$$

Por outro lado, sejam $x_1, x_2, x_3, x_4 \in \mathcal{O}$, de modo que

$$x_i = \sum_{k=1}^{4} a_{ik} u_k,$$

onde $a_{ik} \in \mathbb{I}_K$. Então

$$\det(\mathrm{Tr}(x_i x_j) = \det(\mathbf{A}) \det(\mathrm{Tr}(u_i u_k) \det(\mathbf{A}^t) \in [\det(\mathrm{Tr}(u_i u_j))] \Rightarrow d(\mathcal{O}) \subseteq [\det(\mathrm{Tr}(u_i u_j))]^{\frac{1}{2}},$$

onde $\mathbf{A} = (a_{ik})$ e $\det(\mathbf{A}) \in \mathbb{I}_K$. Portanto, $d(\mathcal{O}) = [\det(\mathrm{Tr}(u_i u_j))]^{\frac{1}{2}}$. ■

Corolário 3.27 *Sejam $\mathcal{O}$ e $\mathcal{O}_0$ duas $\mathbb{I}_K$-ordem em $\mathcal{A}$. Se $\mathcal{O} \subseteq \mathcal{O}_0$, então $d(\mathcal{O}) \subseteq d(\mathcal{O}_0)$ e $d(\mathcal{O}) = d(\mathcal{O}_0)$ implica que $\mathcal{O} = \mathcal{O}_0$.* ■

Exemplo 3.28 *Sejam $\mathcal{A} = (a, b)_K$, onde $a, b \in \mathbb{I}_K^*$. Então*

$$\mathcal{O} = (a, b)_{\mathbb{I}_K} = \{x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in \mathbb{I}_K\}$$

é uma ordem em $\mathcal{A}$. Como $\{u_1, u_2, u_3, u_4\} = \{1, i, j, k\}$ é a base definindo $\mathcal{O}$ temos que $(\mathrm{Tr}(u_i u_j))$ é a seguinte matriz diagonal:

$$(\mathrm{Tr}(u_i u_j)) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2a & 0 & 0 \\ 0 & 0 & -2b & 0 \\ 0 & 0 & 0 & 2ab \end{pmatrix}.$$

Portanto,

$$d(\mathcal{O}) = 4ab = 4\mathbb{I}_K. \tag{3.9}$$

Em particular, se $K = \mathbb{Q}$, $a = b = -1$ e

$$\{u_1, u_2, u_3, u_4\} = \left\{1, i, j, \frac{1 + i + j + k}{2}\right\},$$

então $d(\mathcal{O}) = 2\mathbb{Z}$.

Observação 3.29 *Sejam*

$$\mathcal{A} = \left(\frac{\sqrt{2}, -1}{K}\right)$$

uma álgebra dos quaténios sobre $K = \mathbb{Q}(\sqrt{2})$ e $\mathbb{I}_K = \mathbb{Z}[\sqrt{2}]$. Então

$$\mathcal{A} = \left(\frac{\sqrt{2}, -1}{K}\right) \simeq \left(\frac{-\sqrt{2}, -1}{K}\right) = \mathcal{A}_1 \ \ e \ \ d(\mathcal{A}) = d(\mathcal{A}_1) = \left[\sqrt{2}\right].$$

Teorema 3.30 *Seja $\mathcal{C}$ um subanel de $\mathcal{A}$ contendo $\mathbb{I}_K$ tal que $K\mathcal{C} = \mathcal{A}$. Se cada $a \in \mathcal{C}$ é inteiro sobre $\mathbb{I}_K$, então $\mathcal{C}$ é uma $\mathbb{I}_K$-ordem em $\mathcal{A}$. Reciprocamente, qualquer $\mathbb{I}_K$-ordem em $\mathcal{A}$ possui estas propriedades.*

Prova. Suponhamos que $\mathcal{C}$ seja um subanel de $\mathcal{A}$ contendo $\mathbb{I}_K$ tal que $K\mathcal{C} = \mathcal{A}$. Então

$$\mathcal{A} = \sum_{i=1}^{4} Ku_i,$$

onde $u_i \in \mathcal{C}$. Temos que

$$a = \det\left(\operatorname{tr}(u_i u_j)\right) \in \mathbb{I}_K^*,$$

pois os u_i são inteiros sobre $\mathbb{I}_K$.

Afirmação.

$$\mathcal{C} \subseteq a^{-1} \sum_{i=1}^{4} \mathbb{I}_K u_i.$$

De fato, seja $x \in \mathcal{C}$, de modo que

$$x = \sum_{i=1}^{4} r_i u_i \in K.$$

Então

$$\operatorname{tr}(xu_j) = \sum_{i=1}^{4} r_i \operatorname{tr}(u_i u_j), \;\; 1 \leq j \leq 4.$$

Como $xu_j \in \mathcal{C}$ temos que $\operatorname{tr}(xu_j) \in \mathbb{I}_K$. Pela Regra de Cramer

$$r_i = \frac{b_i}{a}, \;\; 1 \leq i \leq 4,$$

onde $b_i \in \mathbb{I}_K$. Assim,

$$\mathcal{C} \subseteq a^{-1} \sum_{i=1}^{4} \mathbb{I}_K u_i.$$

Portanto, $\mathcal{C}$ é um reticulado em $\mathcal{A}$. ■

Sejam $\mathcal{A}$ uma álgebra e $\mathcal{M}$ uma $\mathbb{I}_K$-ordem em $\mathcal{A}$. Diremos que $\mathcal{M}$ é uma $\mathbb{I}_K$-*ordem maximal* em $\mathcal{A}$ se $\mathcal{M} \neq \mathcal{A}$ e se $\mathcal{O}$ é uma $\mathbb{I}_K$-ordem em $\mathcal{A}$ tal que $\mathcal{M} \subseteq \mathcal{O} \subseteq \mathcal{A}$, então $\mathcal{M} = \mathcal{O}$ ou $\mathcal{O} = \mathcal{A}$.

Exemplo 3.31 *$\mathcal{M} = M_2(\mathbb{I}_K)$ é uma $\mathbb{I}_K$-ordem maximal em $\mathcal{A} = M_2(K)$. Mais geralmente, se R é um domínio integralmente fechado, então $\mathcal{M} = M_2(R)$ é uma R-ordem maximal em $\mathcal{A} = M_2(K)$, onde K é o corpo quociente de R.*

Prova. Sejam $\mathcal{O}$ uma $\mathbb{I}_K$-ordem em $\mathcal{A}$ tal que $\mathcal{M} \subseteq \mathcal{O} \subseteq \mathcal{A}$ e consideremos o conjunto

$$\mathfrak{a} = \{a \in K : a \text{ é uma entrada de alguma matriz de } \mathcal{O}\}.$$

Então é fácil verificar que $\mathfrak{a}$ é um subanel de K contendo $\mathbb{I}_K$ tal que $K\mathfrak{a} = K$. Assim, $\mathfrak{a}$ é uma $\mathbb{I}_K$-ordem em K. Portanto, $\mathbb{I}_K = \mathfrak{a}$ ou $\mathfrak{a} = K$, pois $\mathbb{I}_K$ é uma $\mathbb{I}_K$-ordem maximal em K. Logo, $\mathcal{M} = \mathcal{O}$ ou $\mathcal{O} = \mathcal{A}$.

Teorema 3.32 *Qualquer álgebra $\mathcal{A}$ contém pelo menos uma $\mathbb{I}_K$-ordem maximal em $\mathcal{A}$.*

Prova. Já vimos que uma álgebra $\mathcal{A}$ contém uma $\mathbb{I}_K$-ordem $\mathcal{O}$. Seja $\mathcal{F}$ a família de todos as $\mathbb{I}_K$-ordem $\mathcal{L}$ em $\mathcal{A}$ com $\mathcal{O} \subseteq \mathcal{L}$ e $\mathcal{L} \neq \mathcal{A}$. Então $\mathcal{F} \neq \emptyset$, pois $\mathcal{O} \in \mathcal{F}$. Dados $\mathcal{L}, \mathcal{K} \in \mathcal{F}$, definimos

$$\mathcal{L} \leq \mathcal{K} \Leftrightarrow \mathcal{L} \subseteq \mathcal{K}.$$

Então $\preceq$ é uma relação de ordem parcial sobre $\mathcal{F}$. Seja $\mathcal{C} = \{\mathcal{L}_i : i \in I\}$ uma cadeia qualquer de $\mathcal{F}$. Então

$$\mathcal{M} = \bigcup_{i \in I} \mathcal{L}_i$$

é um subanel de $\mathcal{A}$ contendo $\mathbb{I}_K$ tal que $K\mathcal{M} = \mathcal{A}$. De fato, é claro que $\mathcal{M} \neq \emptyset$, pois $0 \in \mathcal{L}_i$, para todo $i \in I$. Dados $x, y \in \mathcal{M}$, existem $i, j \in I$ tais que $x \in \mathcal{L}_i$ e $y \in \mathcal{L}_j$. Como $\mathcal{C}$ é uma cadeia temos que $\mathcal{L}_i \subseteq \mathcal{L}_j$ ou $\mathcal{L}_j \subseteq \mathcal{L}_i$, digamos $\mathcal{L}_i \subseteq \mathcal{L}_j$. Logo, $x, y \in \mathcal{L}_j$ e $x - y, xy \in \mathcal{L}_j$, pois $\mathcal{L}_i$ é uma $\mathbb{I}_K$-ordem em $\mathcal{A}$. Portanto, $x - y, xy \in \mathcal{M}$ e $\mathcal{M}$ é um subanel de $\mathcal{A}$. Como qualquer elemento de $\mathcal{M}$ é inteiro sobre $\mathbb{I}_K$ temos, pelo Teorema 3.30, que $\mathcal{M}$ é uma $\mathbb{I}_K$-ordem em $\mathcal{A}$. É claro que $\mathcal{M}$ é uma cota superior de $\mathcal{C}$.

Finalmente, pelo Lema de Zorn, $\mathcal{M}$ é um elemento maximal de $\mathcal{F}$. Portanto, $\mathcal{M}$ é uma $\mathbb{I}_K$-ordem maximal em $\mathcal{A}$ contendo $\mathcal{O}$. ■

Teorema 3.33 *Seja $\mathcal{O}$ uma $\mathbb{I}_K$-ordem em $\mathcal{A}$. Então existe uma base $\{e_1, e_2, e_3, e_4\}$ de $\mathcal{A}$ e um ideal fracionário $\mathfrak{a}$ de K tal que*

$$\mathcal{O} = \{a_1e_1 + x_2e_2 + x_3e_3 + x_4x_4 : a_1 \in \mathfrak{a},\ \ x_i \in \mathbb{I}_K\}.$$

Prova. Verifique [15], página 212.

Exemplo 3.34

$$\mathcal{A} = \left(\sqrt{2}, -1\right)_{\mathbb{Q}(\sqrt{2})}$$

$\{1, i, j, k\}$ *uma base de $\mathcal{A}$ satisfazendo*

$$i = \sqrt[4]{2},\ \ j = \mathrm{Im}$$

e $\mathcal{O} = \left(\sqrt{2}, -1\right)_R$, onde

$$R = \left\{\frac{x}{2^n} : x \in \mathbb{Z}[\sqrt{2}]\ \ e\ \ n \in \mathbb{N}\right\}.$$

Então $d(\mathcal{O}) = \left[\sqrt{2}\right]$. Além disso, como observado em 3.29,

$$\mathcal{A} \simeq \mathcal{A}_1 = \left(-1, -\sqrt{2}\right)_{\mathbb{Q}(\sqrt{2})}\ \ e\ \ d(\mathcal{A}) = \left[\sqrt{2}\right].$$

Desta forma, $\mathcal{O}$ é uma R-ordem maximal em $\mathcal{A}$.

Para cada $\mathbb{I}_K$-ordem $\mathcal{O}$ em $\mathcal{A}$, consideremos o conjunto $\mathcal{O}^1$ definido por

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

É claro que $\mathcal{O}^1$ é um grupo multiplicativo. Já vimos que

$$N(x) = \det(\rho_1(x)).$$

(ρ_1 dado em 3.5) Assim, $\rho_1(\mathcal{O}^1)$ é um subgrupo de $\mathrm{SL}(2,\mathbb{R})$. Portanto, o grupo derivado de uma álgebra dos quatérnios $\mathcal{A} = (a,b)_K$, cuja $\mathbb{I}_K$-ordem é $\mathcal{O}$ e denotado por $\Gamma(\mathcal{A},\mathcal{O})$, é definido por

$$\Gamma(\mathcal{A},\mathcal{O}) = \frac{\rho_1(\mathcal{O}^1)}{\{\pm I\}} \leq \frac{\mathrm{SL}(2,\mathbb{R})}{\{\pm I\}} \simeq \mathrm{PSL}(2,\mathbb{R}).$$

Teorema 3.35 *Seja $\mathcal{A} = (a,b)_K$ uma álgebra dos quatérnios e $\mathcal{O}$ uma $\mathbb{I}_K$-ordem em $\mathcal{A}$. Então $\Gamma(\mathcal{A},\mathcal{O})$ é um grupo Fuchsiano.*

Prova. Vamos provar para o caso em que a álgebra com divisão é

$$\mathcal{A} = (a,b)_{\mathbb{Q}}, \quad a > 0$$

e

$$\mathcal{O} = \{x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in \mathbb{Z}\}.$$

Para o caso de um corpo de números $\mathbb{Q}(\theta)$ a prova é análogo com algumas adaptações. Consideremos uma vizinhança de I em $\mathrm{SL}(2,\mathbb{R})$, digamos

$$V_I = \left\{(g_{ij}) \in \mathrm{SL}(2,\mathbb{R}) : |g_{11} - 1| < \frac{1}{2},\ |g_{12}| < \frac{1}{2},\ |g_{21}| < \frac{1}{2} \text{ e } |g_{22} - 1| < \frac{1}{2}\right\}.$$

Seja

$$g_x \in \rho_1(\mathcal{O}^1) \cap V_I.$$

Então

$$g_x = \begin{pmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{pmatrix}, \text{ com } x_0, x_1, x_2, x_3 \in \mathbb{Z}.$$

onde $g_{11} = x_0 + x_1\sqrt{a}$, $g_{22} = x_0 - x_1\sqrt{a}, g_{12} = x_2 + x_3\sqrt{a}$ e $g_{21} = b(x_2 - x_3\sqrt{a})$. Assim,

$$|g_{11} + g_{22} - 2| = |(g_{11} - 1) + (g_{22} - 1)| < 1 \Rightarrow 2\,|x_0 - 1| < 1$$

Logo, $x_0 = 1$. Como $b > 1$ temos que

$$\left|x_2 - x_3\sqrt{a}\right| = \frac{1}{b}\,|g_{21}| < \frac{1}{2b} < \frac{1}{2}.$$

Portanto,

$$|2x_2| = \left|(x_2 + x_3\sqrt{a}) + (x_2 - x_3\sqrt{a})\right| < 1 \Rightarrow x_2 = 0.$$

Por outro lado, como

$$\left|x_1\sqrt{a}\right| < \frac{1}{2} \text{ e } \left|x_3\sqrt{a}\right| < \frac{1}{2}$$

temos que

$$x_1 = x_3 = 0$$

Portanto, $g_x = I$ e

$$\Gamma(\mathcal{A}, \mathcal{O})$$

é um subgrupo discreto de $\mathrm{PSL}(2, \mathbb{R})$, ou seja, é um grupo Fuchsiano. ■

3.4 Grupos Fuchsianos Aritméticos

Em toda esta seção, salvo menção explícita em contrário, K é um corpo de números algébricos totalmente real e $\mathbb{I}_K$ é o anel dos inteiros de K.

Sejam $\mathcal{A} = (a, b)_K$ uma álgebra dos quatérnios, $\mathcal{O}$ uma $\mathbb{I}_K$-ordem em $\mathcal{A}$ e Γ um grupo Fuchsiano de $\Gamma(\mathcal{A}, \mathcal{O})$. Diremos que Γ é um *grupo Fuchsiano derivado da álgebra dos quatérnios* $\mathcal{A}$ se o índice de Γ em $\Gamma(\mathcal{A}, \mathcal{O})$ for finito.

Dois grupos Γ_1 e Γ_2 são chamados *comensuráveis* se a interseção $\Gamma_1 \cap \Gamma_2$ tem índice finito em Γ_1 e Γ_2. Diremos que um grupo Γ é um *grupo Fuchsiano aritmético* se Γ é comensurável com algum $\Gamma(\mathcal{A}, \mathcal{O})$. Observe, por definição, que um grupo Fuchsiano derivado de uma álgebra dos quatérnios $\mathcal{A}$ é aritmético.

Mostraremos agora que podemos caracterizar os grupos fuchsianos aritméticos através do conjunto dos traços dos seus elementos

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

que é o principal objetivo desta seção. Antes, vamos apresentar um serié de resultados que nos conduzirá ao nosso objetivo.

Lema 3.36 *Sejam Γ um grupo Fuchsiano de $\mathrm{PSL}(2, K)$ tal que área hiperbólica*

$$\mu(\frac{\mathbb{H}}{\Gamma}) < \infty$$

e $\mathrm{tr}(\Gamma) \subset K$. Então existem um corpo de números algébricos F e $h \in \mathrm{SL}(2, \mathbb{R}))$ tais que $h^{-1}\Gamma h \subseteq \mathrm{PSL}(2, F)$.

Prova. Verifique [11], página 120, Lema 5.3.1.

Teorema 3.37 *Suponhamos válidas as hipóteses do Lema* 3.36 *e considere*

$$K_0 := \mathbb{Q}(\,\mathrm{tr}(T) : T \in \Gamma).$$

Então

$$\mathcal{A}\,[\Gamma] = K_0\,[\Gamma] = \left\{ \sum_{i=1}^{d} a_i T_i : a_i \in K_1,\ \ T_i \in \Gamma \right\}$$

é uma álgebra dos quatérnios sobre K_0.

Prova. Como Γ é um grupo Fuchsiano não elementar temos, pelo Lema 3.36, que Γ contém os elementos

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \ (\lambda \neq 1) \text{ e } T_1 = \begin{pmatrix} a_1 & 1 \\ c_1 & d_1 \end{pmatrix} \ (c_1 \neq 0) \tag{3.10}$$

e que $\Gamma \subseteq \mathrm{PSL}(2, F)$, onde $F = K_0(\lambda)$ é K_0 ou uma extensão quadrática de K_0, ou seja, $[F : K_0] = 2$. Para simplificar a notação, vamos indicar a álgebra $\mathcal{A}[\Gamma]$ por $\mathcal{A}$. De modo que $\mathcal{A} \subseteq M(2, F)$ e $1 < \dim_{K_0}(\mathcal{A}) \leq 8$. Sejam $\mathfrak{a}$ um ideal de $\mathcal{A}$ e

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{a}.$$

Então $T^n = 0$, para algum $n \in \mathbb{N}$. Logo, $\det(T) = 0$. Como $ad = bc$ temos que $\mathrm{tr}(T^n) = \mathrm{tr}(T)^n$, ou seja,

$$(a + d)^n = 0 \Leftrightarrow \mathrm{tr}(T) = a + d = 0. \tag{3.11}$$

Logo,

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda^{-1} c & \lambda^{-1} d \end{pmatrix} \in \mathfrak{a} \Leftrightarrow \lambda a + \lambda^{-1} d = 0. \tag{3.12}$$

Portanto, $a = d = 0$. Analogamente,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ c_1 & d_1 \end{pmatrix} \in \mathfrak{a}.$$

Assim, $bc_1 + c = 0$ e $bc(c_1 - a_1 d_1) = 0$. Portanto,

$$bc = 0 \Rightarrow b = c = 0.$$

Consequentemente $\mathfrak{a} = \{0\}$.

Finalmente, seja

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{Z}(\mathcal{A}).$$

Então

$$TT_0 = T_0 T \Rightarrow c(\lambda^2 - 1) = 0 \text{ e } b(\lambda^2 - 1) = 0.$$

Assim, $b = c = 0$. Mas, T também comuta com T_1. Logo, $a = d$. Assim, $T = aI$, Por outro lado, $\mathrm{tr}(T') \in K_0$, para todo $T' \in \mathcal{A}$. Portanto,

$$\mathrm{tr}(T) = a + d = 2a \Rightarrow a \in K_0,$$

ou seja,

$$\mathcal{Z}(\mathcal{A}) = \{aI : a \in K_0\} \simeq K_0.$$

Finalmente, a dimensão de $\mathcal{A}$ sobre K é um quadrado de um inteiro. Portanto, $\dim_{K_1}(\mathcal{A}) = 4$. ■

Lema 3.38 *Seja* Γ *um grupo Fuchsiano com*

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) < \infty, \;\; K_0 = \mathbb{Q}(\mathrm{tr}(T) : T \in \Gamma), \;\; [K_0 : \mathbb{Q}] < \infty \;\; e \;\; \mathrm{tr}(\Gamma) \subset \mathbb{I}_{K_0}.$$

Então

$$\mathcal{O} = \mathcal{O}[\Gamma] = \mathbb{I}_{K_0}[\Gamma] = \left\{ \sum_{i=1}^{d} a_i T_i : a_i \in \mathbb{I}_{K_0}, \;\; T_i \in \Gamma \right\}$$

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

Prova. É claro que $\mathcal{O}$ é um subanel de $\mathcal{A}$ que gera $\mathcal{A}$ sobre K_0. Assim, resta provar que $\mathcal{O}$ é finitamente gerada como $\mathbb{I}_{K_0}$-módulo. Pelo Lema 3.36, podemos supor que Γ contém os elementos

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \;\; (\lambda \neq 1) \;\; \mathrm{e} \;\; T_1 = \begin{pmatrix} a_1 & 1 \\ c_1 & d_1 \end{pmatrix} \;\; (c_1 \neq 0).$$

e que $\Gamma \subseteq \mathrm{PSL}(2, K)$, onde $F = K_0(\lambda)$. Dado

$$T = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{O} \Rightarrow \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda^{-1} c & \lambda^{-1} d \end{pmatrix} \in \mathcal{O}.$$

Logo,

$$\lambda a + \lambda^{-1} d, a + d \in \mathbb{I}_{K_0}.$$

Note que λ e λ^{-1} são unidades em F e $\mathbb{I}_{K_0}$ é um subanel de $\mathbb{I}_F$. Assim, a e d pertencem a um ideal fracionário

$$\frac{1}{\lambda^2 - 1}\mathbb{I}_{K_0}$$

de F. Logo,

$$aa_1 + bc_1, c + dd_1 \in \frac{1}{\lambda^2 - 1}\mathbb{I}_{K_0}.$$

Portanto, $\mathcal{O}$ é um $\mathbb{I}_{K_0}$-submódulo de um $\mathbb{I}_{K_0}$-módulo livre de posto 4, ou seja, $\mathcal{O}$ é finitamente gerado como $\mathbb{I}_{K_0}$-módulo. ■

Note que o conjunto

$$\{I, T_0, T_1, T_0 T_1\}$$

é uma base de definição $\mathcal{A}[\Gamma]$ sobre K_0. Consequentemente,

$$\mathcal{A}[\Gamma] = \left\{ \begin{pmatrix} a & b \\ b' c_1 & a' \end{pmatrix} : a, b \in F, \;\; c_1 \in K_0 \right\},$$

onde a' e b' são os conjugados de a e b em $F = K_0(\lambda)$, respectivamente.

Lema 3.39 *Seja* Γ *um grupo Fuchsiano de* $\mathrm{PSL}(2, K)$ *tal que área hiperbólica*

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) < \infty.$$

Suponhamos que Γ *satisfaça as seguintes condições*:

1. *Seja* $K_0 = \mathbb{Q}(\mathrm{tr}(T) : T \in \Gamma)$. *Então* K_0 *é um corpo de números algébricos sobre* $\mathbb{Q}$ *com* $[K_0 : \mathbb{Q}] < \infty$ *e* $\mathrm{tr}(\Gamma) \subset \mathbb{I}_{K_0}$.

2. *Seja* φ *qualquer imersão de* K_0 *em* $\mathbb{C}$ *tal que* $\varphi \neq I$. *Então* K_0 *é totalmente real. Além disso,* $\varphi(\mathrm{tr}(\Gamma)) \subseteq [-2, 2]$.

Prova. Dado $T \in \Gamma$. Sejam

$$a \text{ e } \frac{1}{a}$$

os autovalores de uma matriz associada à transformação T e φ qualquer imersão de K_0 em $\mathbb{C}$ tal que $\varphi \neq I$. Então Estendemos φ a um isomorfismo ψ de $K_0(a)$ em $\mathbb{C}$.

Afirmação. $|\psi(a)| = 1$.

De fato, suponhamos, por absurdo, que $|\psi(a)| \neq 1$. Então, pela desigualdade

$$|\varphi(\mathrm{tr}(T^m))| = \left|(\psi(a))^m + \frac{1}{(\psi(a))^m}\right| \geq \left||\psi(a)|^m - \frac{1}{|\psi(a)|^m}\right|,$$

o conjunto

$$\{\varphi(\mathrm{tr}(T^m)) : m \in \mathbb{Z}\}$$

é não limitado, o que contradiz a condição (2). Portanto,

$$\varphi(\mathrm{tr}(T)) = \psi(a) + \frac{1}{\psi(a)} = \psi(a) + \overline{\psi(a)} = 2\,\mathrm{Re}(\psi(a)) \text{ e } |\varphi(\mathrm{tr}(T))| \leq 2\,|\psi(a)| = 2,$$

ou seja, $\varphi(\mathrm{tr}(T))$ é um número real contido no intervalo $[-2, 2]$. ■

Proposição 3.40 *Seja* φ *qualquer imersão de* $K = K_0(\lambda)$ (K_0 *dado no Lema anterior*) *em* $\mathbb{C}$ *tal que* $\varphi|_{K_0} \neq I$. *Então*

$$|\varphi(a)| \leq 1, \ \forall \ T = \begin{pmatrix} a & b \\ b'c_1 & a' \end{pmatrix} \in \Gamma,$$

Em particular, para

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

obtemos $\varphi(c_1) < 0$.

Prova. Seja

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \in \Gamma.$$

Então, pelo Lema 3.39,

$$TT_0^n \in \Gamma \text{ e } |\varphi(\mathrm{tr}(TT_0^n))| \leq 2. \tag{3.13}$$

Novamente, pelo Lema 3.39, obtemos

$$|\varphi(\lambda)| = 1 \text{ e } \frac{1}{\lambda} = \lambda'.$$

Assim,

$$\varphi(a') = \overline{\varphi(a)} \ \forall \ a = \alpha_0\lambda + \alpha_1\lambda' \in K. \tag{3.14}$$

Portanto, K é um corpo de números totalmente real. Por outro lado, sendo

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

obtemos

$$\varphi(\mathrm{tr}(TT_0^n)) = \varphi(a\lambda^n) + \varphi(a'(\lambda')^n) = \varphi(a\lambda^n) + \overline{\varphi(a\lambda^n)} = 2\,\mathrm{Re}(\varphi(a)\varphi(\lambda^n)).$$

Logo,

$$|\mathrm{Re}(\varphi(a)\varphi(\lambda^n))| \leq 1. \tag{3.15}$$

Como $\varphi(\lambda)^n \neq 1$, para todo $n \in \mathbb{Z}$, temos que o conjunto

$$\{\varphi(\lambda)^m : m \in \mathbb{Z}\}$$

é um subgrupo denso de

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}.$$

Portanto,

$$|\mathrm{Re}(\varphi(a) \cdot z)| \leq 1, \ \forall \ z \in S^1.$$

Assim, $|\varphi(a)| \leq 1$.

Finalmente, aplicando o mesmo raciocínio ao elemento T_1, obtemos $|\varphi(a_1)| \leq 1$. Por outro lado,

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

Portanto, $\varphi(c_1) < 0$, pois $c_1 \neq 0$. ■

Proposição 3.41 *Seja* Γ *um grupo Fuchsiano de* $\mathrm{PSL}(2, K)$ *tal que área hiperbólica*

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) < \infty.$$

Se Γ *satisfaz as condições* (1) *e* (2) *do Lema* 3.39*, então* $\mathcal{A}[\Gamma]$ *satisfaz* (3.5).

Prova. Já vimos que Γ contém

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

Provaremos que $K = K_0(\lambda)$ é uma extensão própria de K_0. Se K é uma extensão própria de $\mathbb{Q}$, então existe uma imersão $\chi : K \to \mathbb{C}$ tal que $\chi(K_0) \neq I$. Por outro lado, $\chi(\lambda)$ e $\frac{1}{\chi(\lambda)}$ são raízes da equação $x^2 - \chi(t_0)x + 1 = 0$, onde $t_0 = \mathrm{tr}(T_0)$. Pelo Lema 3.39, temos que $|\chi(t_0)| < 2$. Portanto, $\chi(K) = \chi(K_0(\lambda)) \subseteq \mathbb{C} - \mathbb{R}$. Como K_0 é totalmente real temos que $\chi(K_0)$ real e

$K_0 \subset K$. Se $K_0 = \mathbb{Q}$, então t_0 é um inteiro racional tal que $|t_0| > 2$. Portanto, $x^2 - t_0 x + 1$ é irredutível sobre $\mathbb{Q}$. Fazendo $\lambda' = \frac{1}{\lambda}$. Já vimos que

$$\operatorname{tr}(T_1) = a_1 + d_1 \in K_0 \text{ e } \operatorname{tr}(T_0 T_1) = a_1\lambda + d_1\lambda' \in K_0. \tag{3.16}$$

Como λ e λ' são linearmente independentes sobre K_0 temos que existem únicos $\alpha_0, \alpha_1, \delta_0, \delta_1 \in K_0$ tais que

$$a_1 = \alpha_0\lambda + \alpha_1\lambda' \text{ e } d_1 = \delta_0\lambda + \delta_1\lambda'.$$

Logo,

$$(\alpha_0\lambda + \alpha_1\lambda')\,\lambda + (\delta_0\lambda + \delta_1\lambda')\,\lambda' = (\alpha_0\lambda' + \alpha_1\lambda)\,\lambda' + (\delta_0\lambda' + \delta_1\lambda)\,\lambda.$$

Assim,

$$(\alpha_0 - \delta_1)\,\lambda^2 + (\delta_1 - \alpha_0)\,(\lambda')^2 = 0 \Rightarrow \alpha_0 = \delta_1.$$

De 3.16, temos que

$$\alpha_0\lambda + \alpha_1\lambda' + \delta_0\lambda + \delta_1\lambda' = \alpha_0\lambda' + \alpha_1\lambda + \delta_0\lambda' + \delta_1\lambda.$$

Logo,

$$\alpha_0 + \delta_0 - \alpha_1 - \delta_1 = 0 \Rightarrow \alpha_1 = \delta_0.$$

De modo que $d_1 = a_1'$. Como $\det(T_1) = 1$ temos que $c_1 \in K_0$. Consequentemente,

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda' \end{pmatrix} \ (\lambda \neq 1) \text{ e } T_1 = \begin{pmatrix} a_1 & 1 \\ c_1 & a_1' \end{pmatrix} \ (c_1 \neq 0).$$

Seja $\{\varphi_i\}$, $1 \leq i \leq n$, as n imersões distintas de K_0 em $\mathbb{R}$ com $\varphi_1 = I$. Então

$$\psi_i : K \to \psi_i(K),$$

é um isomorfismo com $K = K_0(\lambda)$ e $[K : K_0] = 2$. Logo,

$$\chi_i : \mathcal{A}[\Gamma] \to M_2(\mathbb{R}),$$

definido por

$$\chi_i(T) = \begin{pmatrix} \psi_i(a) & \psi_i(b) \\ \psi_i(b'c) & \psi_i(a') \end{pmatrix}, \text{ onde } T = \begin{pmatrix} a & b \\ b'c & a' \end{pmatrix},$$

é uma imersão. Portanto,

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

é uma álgebra dos quatérnios sobre $\chi_i(K_0) = \varphi_i(K_0)$. Assim,

$$\mathcal{A}^{\varphi_1} \simeq M_2(\mathbb{R}).$$

Pela prova da Proposição 3.40 com $\psi_i(a') = \overline{\psi_i(a)}$, para $2 \leq i \leq n$, concluímos que

$$\mathcal{A}^{\varphi_i} = \left\{ \begin{pmatrix} a & b \\ \overline{b}\psi_i(c_1) & \overline{a} \end{pmatrix} : a, b \in \psi_i(K), \ c_1 \in K_0 \right\},$$

ou seja, $\mathcal{A}^{\varphi_1} \otimes \mathbb{R} \simeq \mathcal{H}$. ■

Teorema 3.42 *Seja* Γ *um grupo Fuchsiano de* $\mathrm{PSL}(2,K)$ *tal que área hiperbólica*

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) < \infty.$$

Então Γ *é derivado de uma álgebra dos quatérnios* $\mathcal{A}$ *sobre um corpo de números* K *totalmente real se, e somente se,* Γ *satisfaz as seguintes condições*:

1. *Se* $K_0 = \mathbb{Q}(\mathrm{tr}(T) : T \in \Gamma)$, *então* K_0 *é um corpo de números algebrícos sobre* $\mathbb{Q}$ *com* $[K_0 : \mathbb{Q}] < \infty$ *e* $\mathrm{tr}(\Gamma) \subset \mathbb{I}_{K_0}$.

2. *Seja* φ *qualquer imersão de* K_0 *em* $\mathbb{C}$ *tal que* $\varphi \neq I$. *Então* $\varphi(\mathrm{tr}(\Gamma))$ *é limitado em* $\mathbb{C}$.

Prova. Suponhamos que Γ seja um subgrupo de índice finito em $\Gamma(\mathcal{A}, \mathcal{O})$. Então $\mathrm{tr}(T) \in K$, para todo $T \in \Gamma$. Portanto, K_0 é totalmente real, pois $K_0 \subseteq K$. Como $\mathrm{Tr}(\mathcal{O}) \subset \mathbb{I}_{K_0}$ temos que $\mathrm{tr}(\Gamma) \subset \mathbb{I}_{K_0}$. Seja φ qualquer imersão de K_0 em $\mathbb{C}$ tal que $\varphi \neq I$. Por 3.7,

$$\varphi_i(\mathrm{tr}(\Gamma)) \subset \mathrm{Tr}(\rho_i(\mathcal{O}^1)),$$

para $2 \leq i \leq n$ e $[K_0 : \mathbb{Q}] = n$. Por outro lado,

$$\varphi_i(N(x)) = N(\rho_i(x)), \ \forall \ x \in \mathcal{O}^1.$$

Assim,

$$\rho_i(\mathcal{O}^1) \subset \mathcal{H}^1 = \{x \in \mathcal{H} : N(x) = 1\}.$$

Já vimos, pelo Exemplo 3.18, que $\mathrm{Tr}(H^1) = [-2, 2]$. Portanto,

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

ou seja, $\varphi_i(\mathrm{tr}(\Gamma))$ é limitado em $\mathbb{R}$. Vamos mostrar que $K = K_0$. Suponhamos que K seja uma extensão própria de K_0. Então existe uma imersão $\varphi : K \to \mathbb{R}$ com $\varphi \neq I$ tal que $\varphi|_{K_0} = I$. Portanto, pela definição de K_0, obtemos

$$\varphi(\mathrm{tr}(\Gamma)) = \mathrm{tr}(\Gamma) \subset [-2, 2].$$

Isso significa que Γ não contém elementos hiperbólicos, o que contradiz o fato de

$$\mu\left(\frac{\mathbb{H}}{\Gamma}\right) < \infty.$$

Reciprocamente, note que pelos Lemas 3.36, 3.39 e pela Proposição 3.41, $\mathcal{A}[\Gamma]$ e $\mathcal{O}[\Gamma]$ satisfazem as condições de uma álgebra de quatérnios. Por outro lado, claramente Γ é um subgrupo de $\Gamma(\mathcal{A}[\Gamma], \mathcal{O}[\Gamma])$. Como

$$\mu\left(\frac{\Gamma(\mathcal{A}[\Gamma], \mathcal{O}[\Gamma])}{\mathbb{H}}\right) < \infty$$

temos que Γ é um subgrupo de índice finito em $\Gamma(\mathcal{A}[\Gamma], \mathcal{O}[\Gamma])$. Portanto, Γ é um grupo Fuchsiano derivado de uma álgebra dos quatérnios. ■

Observação 3.43 *Na condição* (1) *do Teorema* 3.42, *o anel* $\mathbb{I}_{K_0}$, *pode ser substituido por um anel* R *tal que* $\mathbb{I}_{K_0} \subseteq R \subseteq K_0$, *desde que* $\mathcal{O} = (a, b)_R$ *e* $\mathcal{A} = (a, b)_{K_0}$.

Capítulo 4

Aplicações

Neste capítulo, estudaremos os grupos Fuchsianos $\Gamma \simeq \Gamma_{4g}$, onde Γ é um subgrupo de $\mathrm{PSL}(2,\mathbb{R})$, no sentido de caracterizá-los quanto a sua aritmeticidade. Estudaremos, também, detalhadamente os grupos Γ_{4g}, para o caso $g = 2^m$, e mostraremos que esses grupos são derivados de uma álgebra dos quatérnios $\mathcal{A}$ sobre um corpo de números K tal que $[K:\mathbb{Q}] = 2^m$. Nestes casos, identificaremos as ordens $\mathcal{O}$ em $\mathcal{A}$ associadas aos grupos Γ_{4g}.

4.1 Determinação do Grupo Fuchsiano Γ_{4g}

Nesta seção introduzimos o grupo Fuchsiano Γ_{4g}. Em toda este capítulo, salvo menção explícita em contrário, o modelo de espaço hiperbólico é o disco de Poincaré $\mathbb{B}$.

O grupo Γ_{4g} é construído como segue: Considerando uma tesselação auto-dual

$$\{4g, 4g\}, g \geq 2,$$

temos que

$$(4g-2)(4g-2) = 4(2g-1)(2g-1) > 4,$$

logo, por 2.24 existe uma tesselação hiperbólica $\{4g, 4g\}, g \geq 2$. Seja P_{4g} o polígono hiperbólico regular de $4g$ arestas associado a essa tesselação (confira figura 4.1). O polígono P_{4g} tessela o plano hiperbólico $\mathbb{B}$, de modo que cada vértice é compartilhando por $4g$ polígonos de mesma forma. Logo, para cada g, Γ_{4g} é um grupo que tem P_{4g} como domínio fundamental. Podemos supor, sem perda de generalidade, que P_{4g} esteja centrado na origem de $\mathbb{B}$. Consideremos, também, as arestas de P_{4g} dispostas na seguinte ordem cíclica fixa no sentido antihorário:

$$\tau_1, \varepsilon_1, \tau_1', \varepsilon_1', \ldots, \tau_g, \varepsilon_g, \tau_g', \tau_g', \varepsilon_g'.$$

A partir do poligono P_{4g} apresentaremos um procedimento aritmético (Teorema 4.2) com o objetivo de determinar as transformações de Möbius que realizam os emparelhamentos das correspondentes arestas. Os emparelhamentos são realizados por isometrias hiperbólicas

$$T_1, S_1, \ldots, T_{2g}, S_{2g}$$

(os geradores do grupo Fuchsiano Γ_{4g}) tais que

$$T_k(\tau_k) = \tau_k' \text{ e } S_j(\varepsilon_j) = \varepsilon_j', \ \ k, j = 1, \ldots, g. \tag{4.1}$$

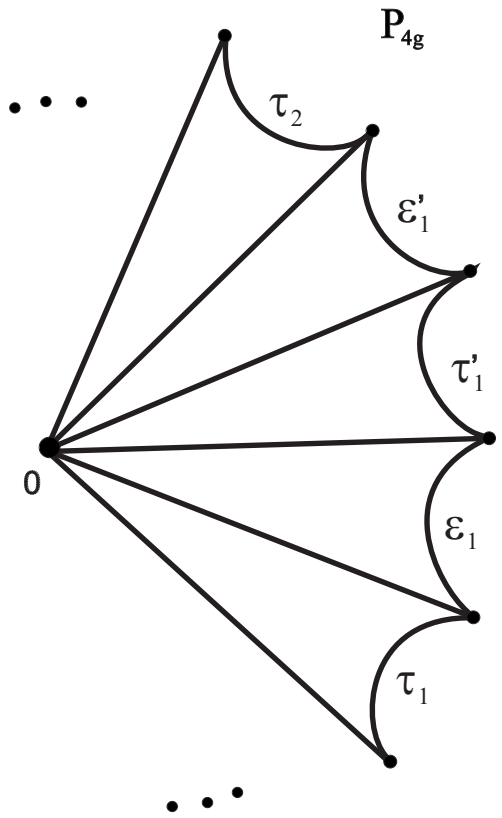

Figura 4.1: Polígono hiperbólico regular de $4g$ arestas.

Para explicitarmos tal tesselação basta determinar a transformação T_1 associada ao emparelhamento da aresta τ_1 com a aresta τ_1', isto é, $T_1(\tau_1) = \tau_1'$. As demais transformações são obtidas através de conjugações

$$T_i = T_{C^{r_i}} T_1 T_{C^{-r_i}} \text{ e } S_i = T_{C^{p_i}} T_1 T_{C^{-p_i}},$$

onde

$$T_C(z) = e^{\frac{i\pi}{2g}} z$$

é uma transformação elíptica de ordem $4g$ que leva a aresta τ_1 na aresta adjacente do polígono P_{4g}, no sentido antihorário; o indíce r_i é a potência da transformação elíptica que leva a aresta τ_1 em cada uma das arestas $\tau_i, \tau_i', \varepsilon_i, \varepsilon_i'$ para $i = 1, \ldots, g$ e $p_i = r_i - 1$. Uma outra forma de explicitarmos tal tesselação é considerando a tranformação elíptica T_C de ordem $4g$ com matriz associada

$$C = \begin{pmatrix} e^{\frac{i\pi}{4g}} & 0 \\ 0 & e^{\frac{-i\pi}{4g}} \end{pmatrix}, \tag{4.2}$$

de modo que $T_C(\tau_1) = \varepsilon_1$ e r_k é a potência de C tal que

$$T_C^{r_k}(\tau_1) = T_{C^{r_k}}(\tau_1) \in \{\tau_k, \varepsilon_k, \tau_k', \varepsilon_k'\}, \;\; k = 1, \ldots, g. \tag{4.3}$$

Isto permite escrever os geradores de Γ_{4g} como conjugações de T_1 por meio de potências de T_C. Por exemplo, queremos uma transformação T_2, de modo que $T_2(\tau_2) = \tau_2'$. Mas,

$$T_1(\tau_1) = \tau_1' \;\text{ e }\; T_{C^4}(\tau_1) = \tau_2,$$

onde T_{C^4} é a tranformação elíptica de ordem $4g$ com matriz associada C^4. Assim, $T_{C^{-4}}(\tau_2) = \tau_1$. Logo,

$$T_1\left(T_{C^{-4}}(\tau_2)\right) = \tau_1' \Leftrightarrow T_{C^4}\left(T_1\left(T_{C^{-4}}(\tau_2)\right)\right) = T_{C^4}(\tau_1') = \tau_2',$$

ou seja,

$$T_{C^4} \circ T_1 \circ T_{C^{-4}}(\tau_2) = \tau_2'.$$

Dessa forma, basta considerarmos

$$T_2 = T_{C^4} \circ T_1 \circ T_{C^{-4}}.$$

Para os demais casos, usando 4.1 e 4.3 obtemos,

$$A_k = C^{4(k-1)} A_1 C^{-4(k-1)} \;\text{ e }\; B_j = C^{4j-3} A_1 C^{-4j+3}, \tag{4.4}$$

onde A_k e B_j são matrizes correspondentes às transformações T_k e S_j, respectivamente com $k, j = 1, \ldots, g$. Com algumas manipulações algébricas, podemos expressar os geradores do grupo Γ_{4g} em 4.4 sob a forma:

$$A_l = \begin{cases} C^{2(l-1)} A_1 C^{-2(l-1)} & \text{para } l \text{ ímpar} \\ C^{(2l-3)} A_1 C^{-(2l-3)} & \text{para } l \text{ par} \end{cases} \tag{4.5}$$

Definindo uma tesselação auto-dual $\{4g, 4g\}$, temos um polígono hiperbólico regular P_{4g}, de $4g$ arestas, que por sua vez está associado a um grupo Fuchsiano Γ_{4g}, cuja assinatura é $(g, -)$. Portanto, a área hiperbólica de P_{4g} é dada por

$$\mu(P_{4g}) = \mu\left(\frac{\mathbb{B}}{\Gamma_{4g}}\right) = 4\pi(g-1). \tag{4.6}$$

Note que a inexistência do somatório

$$\sum_{k=1}^{r}\left(1 - \frac{1}{m_k}\right)$$

na medida da área hiperbólica de $\frac{\mathbb{B}}{\Gamma_{4g}}$ em 4.6 fornecida pela Teorema 2.21, é equivalente a inexistência de elementos elípticos no grupo Γ_{4g}. Isto é suficiente para que tenhamos o quociente $\frac{\mathbb{B}}{\Gamma_{4g}}$ localmente isométrico a $\mathbb{B}$.

Observe pela Figura 4.2, que se considerarmos o baricentro do poligono P_{4g} e ligá-lo aos seus vértices por segmentos de retas, obteremos $4g$ triângulos hiperbólicos em P_{4g} cada um com área

$$\frac{4\pi(g-1)}{4g} = \frac{\pi(g-1)}{g}$$

e com ângulo $\frac{\pi}{2g}$ para o vértice que é o baricentro de P_{4g}. Por definição de tesselação regular $\{4g, 4g\}$, decorre que cada vértice em P_{4g} tem que ser recoberto por $4g$ polígonos regulares do tipo P_{4g}, ou seja, cada vértice deve possuir ângulo

$$\frac{\pi}{2g}.$$

Desse modo os triângulos hiperbólicos obtidos são isósceles com ângulos

$$\frac{\pi}{2g}$$

para o vértice no baricentro de P_{4g} e com ângulos

$$\frac{\pi}{4g}$$

nos outros dois vértices de P_{4g}. A Figura 4.2, exibe uma região fundamental P_{4g}, ou seja, um polígono regular de $4g$ lados de uma tesselação regular

$$\{4g, 4g\}$$

com baricentro determinado pelo centro $O = (0, 0)$ no disco de Poincaré, com as arestas $\varepsilon'_g, \tau_1, \varepsilon_1$ dadas, respectivamente, pelos arcos EH', $H'H$ e HF. Tomaremos o ponto D como o centro do círculo isométrico C_{T_1} da transformação T_1, o ponto N em C_{T_1}, G como o ponto médio do arco Euclidiano $H'H$, R como o raio de C_{T_1}, r como a reta tangente ao círculo isométrico C_{T_1} no ponto H,

$$\gamma, \alpha, \beta, d, e, k$$

como os ângulos determinados pelas relações trigonométricas dos triângulos Euclidianos $\widehat{OD'H}$ e $\widehat{ODN}$, e $\hat{t}$ como o ângulo determinado pela interseção da reta r e o segmento $\overline{ON}$, hipotenusa do triângulo $\widehat{ODN}$.

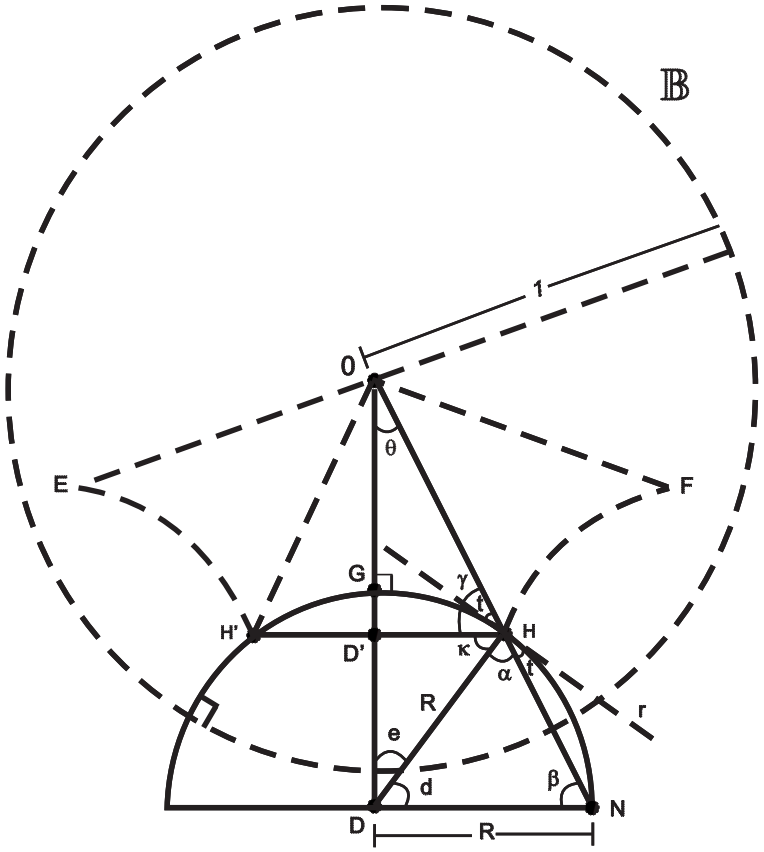

Figura 4.2: Triângulo $\{4g, 4g\}$.

Com o objetivo de determinar uma das transformações do grupo Fuchsiano Γ_{4g}, desenvolveremos a seguir, uma sequência de cálculos culminando na Proposição 4.1 e no Teorema 4.2. Para isto, consideremos C como sendo a matriz de rotação associada ao elemento elíptico T_C, de ordem $4g$, isto é,

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

Sejam

$$A_1 = \begin{pmatrix} a & c \\ \overline{c} & \overline{a} \end{pmatrix},$$

a matriz associada à transformação hiperbólica

$$T_1(z) = \frac{az + c}{\overline{c}z + \overline{a}}.$$

e $T_1^{-1}(z)$ a transformação inversa de $T_1(z)$. Então

$$T_1^{-1}(z) = \frac{-\overline{a}z + c}{\overline{c}z - a}$$

e a matriz associada a $T_1^{-1}(z)$ é dada por

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

Os centros isométricos de T_1 e T_1^{-1} são

$$C_{T_1} = -\frac{\overline{a}}{\overline{c}} \text{ e } C_{T_1^{-1}} = \frac{a}{\overline{c}},$$

respectivamente. Como $T_1(\tau_1) = \tau_1'$ temos que a transformação $T_{C^{-2}}$ leva o círculo isométrico C_{T_1} em $C_{T_1^{-1}}$. Note que os elementos da matriz A_1 são determinados por

$$T_{C^{-2}}\left(-\frac{\overline{a}}{\overline{c}}\right) = \frac{a}{\overline{c}},$$

pois

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

Logo,

$$a = \pm\,|a|\,\sqrt{-e^{-\frac{i\pi}{g}}}.$$

Se

$$x = \ln\sqrt{-e^{-\frac{i\pi}{g}}},$$

então

$$e^{2x} = -e^{-\frac{i\pi}{g}} = -\cos\left(\frac{\pi}{g}\right) + i\,\mathrm{sen}\left(\frac{\pi}{g}\right).$$

Como $g \geq 2$ temos que

$$0 \leq \frac{\pi}{g} \leq \frac{\pi}{2}.$$

Consequentemente,

$$-\cos\left(\frac{\pi}{g}\right) = -\cos\left(\pi - \frac{\pi}{g}\right) = \cos\left(\frac{(g-1)\pi}{g}\right) \text{ e } \mathrm{sen}\left(\frac{\pi}{g}\right) = \mathrm{sen}\left(\pi - \frac{\pi}{g}\right) = \mathrm{sen}\left(\frac{(g-1)\pi}{g}\right).$$

Sendo

$$e^{2x} = e^{i\frac{(g-1)\pi}{g}},$$

obtemos

$$x = i\frac{(g-1)\pi}{2g} \text{ e } \arg(a) = \frac{(g-1)\pi}{2g}.$$

Podemos supor, sem perda de generalidade, que τ_1 seja a aresta entre

$$\arg(-\frac{\pi}{2}) \text{ e } \arg\left(\frac{(g-1)\pi}{2g}\right),$$

proveniente do círculo isométrico C_{T_1}. Este círculo é obtido da transformação hiperbólica

$$T_1(z) = \frac{az + c}{\overline{c}z + \overline{a}}$$

pela equação

$$|\overline{c}z + \overline{a}| \equiv 1 \Leftrightarrow \left| z - \left(-\frac{\overline{a}}{\overline{c}} \right) \right| \equiv \frac{1}{|\overline{c}|} = R$$

satisfeita precisamente nos pontos em que $T_1(z)$ é simultaneamente uma isometria hiperbólica e Euclidiana. A Figura 4.2, mostra a relação que podemos obter com os triângulos Euclidianos mencionados. Por semelhança de triângulos, obtemos

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

Como já vimos o ângulo

$$\hat{t} = \frac{\pi}{4g},$$

logo, observando a Figura 4.2 temos que

$$\alpha + \frac{\pi}{4g} = \frac{\pi}{2},\ \text{ ou seja, }\ \alpha = \frac{\pi}{2} - \frac{\pi}{4g} = \frac{(2g-1)\,\pi}{4g}.$$

Por outro lado, sendo $\widehat{ODN}$ um triângulo retângulo Euclidiano, no ponto D, obtemos

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

ou seja $\alpha = \beta$. Assim, concluímos que o triângulo $\widehat{DHN}$ é isósceles com $\overline{DH} = \overline{DN}$. Consequentemente, $\overline{DN} = R$, onde R é o raio do círculo isométrico C_{T_1}. Portanto, concluímos que

$$\tan\left(\frac{(2g-1)\,\pi}{4g}\right) = \frac{\overline{OD}}{R},\ \text{ ou seja, }\ \overline{OD} = R\tan\left(\frac{(2g-1)\,\pi}{4g}\right).$$

Com esta consideração vamos apresentar a Proposição 4.1, a qual nos fornecerá as coordenadas polares dos vértices do polígono P_{4g}.

Proposição 4.1 *Seja P_{4g} o polígono regular de $4g$ lados, cujo grupo Fuchsiano associado é Γ_{4g} com assinatura $(g,-)$. Os vértices do polígono P_{4g}, em coordenadas polares, são da forma*

$$w_k = \rho \cdot e^{i\frac{2\pi\cdot k}{4g}},\ \ k = 0, \ldots, 4g-1,$$

onde $\rho = \overline{OH}$ (confira Figura 4.2).

Prova. Note, pela Figura 4.2, que o lado $\overline{D'H}$ é paralelo a $\overline{DN}$ o que implíca $\gamma \equiv \beta$. Logo, $k = \gamma - \beta$. Por outro lado,

$$\cos(k) = \frac{\overline{DN}}{R},\ \text{ ou seja, }\ \overline{DN} = R \cdot \cos(k).$$

Observando o triângulo $\widehat{ODN}$, obtemos

$$\cos(\beta) = \frac{\overline{D'H}}{\overline{OH}},\ \text{ ou seja, }\ \overline{OH} = \frac{\overline{D'H}}{\cos(\beta)}.$$

■

Teorema 4.2 *Seja P_{4g} o polígono hiperbólico regular de $4g$ arestas, cujo grupo Fuchsiano associadao é Γ_{4g} com assinatura $(g,-)$. Consideremos u_1 como sendo a aresta entre os argumentos*

$$-\frac{\pi}{2} \;\; e \;\; -\frac{(g-1)\pi}{2g}$$

e T_1 a transformação hiperbólica que emparelha as arestas u_1 e u_1' do poligono P_{4g}. Então

$$T_1(z) = \frac{az+c}{\overline{c}z+\overline{a}},$$

onde a e b são dados por

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

e

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

As demais transformações hiperbólicas $T_k(\tau_k) = \tau_k'$ e $S_j(\varepsilon_j) = \varepsilon_j'$ geradoras do grupo Fuchsiano Γ_{4g} que realizam os emparelhamentos são obtidas pelas conjugações

$$T_k = T_{C^{r_k}} T_1 T_{C^{-r_k}} \;\; e \;\; S_j = T_{C^{p_i}} T_1 T_{C^{-p_i}}.$$

Prova. Já vimos que

$$|c| = \frac{1}{R} \text{ e } \overline{OD} = \frac{|a|}{|c|} = R\,|a|\,,$$

pois $\overline{OD}$ é a distância da origem O ao centro do círculo isométrico $D = -\frac{\overline{a}}{\overline{c}}$. Assim,

$$\overline{OD} = R\tan\left(\frac{(2g-1)\,\pi}{4g}\right) \Rightarrow |a| = \tan\left[\frac{(2g-1)\,\pi}{4g}\right].$$

Logo,

$$a = |a|\,e^{i\arg(a)} = \tan\left[\frac{(2g-1)\pi}{4g}\right]\left(\cos\frac{(g-1)\pi}{2g} + i\,\mathrm{sen}\,\frac{(g-1)\pi}{2g}\right).$$

Como

$$|a|^2 - |c|^2 = 1$$

temos que

$$\begin{aligned} |c|^2 &= |a|^2 - 1 = \left(\tan\left[\frac{(2g-1)\pi}{4g}\right]\right)^2 - 1 \text{ ou} \\ |c| &= \left(\left(\tan\left[\frac{(2g-1)\pi}{4g}\right]\right)^2 - 1\right)^{\frac{1}{2}}. \end{aligned}$$

Observando o triângulo Euclidiano $\widehat{ODN}$, obtemos

$$\arg\left(-\frac{a}{c}\right) = \frac{\pi}{4g}.$$

Logo,

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

Portanto,

$$\overline{c} = -\,|\overline{c}|\left(\cos\frac{(2g-1)\,\pi}{4g} - i\,\mathrm{sen}\,\frac{(2g-1)\pi}{4g}\right) = |\overline{c}|\left(-\cos\frac{(2g-1)\,\pi}{4g} + i\,\mathrm{sen}\,\frac{(2g-1)\pi}{4g}\right).$$

Por outro lado, como $1 \leq 2g-1$ temos que

$$0 \leq \frac{\pi(2g-1)}{g} \leq \frac{\pi}{2}.$$

Assim,

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

e

$$\mathrm{sen}\left(\frac{(2g-1)\pi}{4g}\right) = \mathrm{sen}\left(\pi - \frac{(2g-1)\pi}{4g}\right) = \mathrm{sen}\left(\frac{(2g+1)\pi}{4g}\right).$$

Logo,

$$\overline{c} = |\overline{c}|\left(\cos\left(\frac{(2g+1)\,\pi}{4g}\right) + i\,\mathrm{sen}\left(\frac{(2g+1)\pi}{4g}\right)\right) = |\overline{c}|\,e^{\frac{(2g+1)\pi}{4g}}.$$

Portanto,

$$\arg(c) = -\left(\frac{2g+1}{4g}\right)\pi$$

e

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

Note, pelo triângulo Euclidiano $\widehat{ODN}$, que

$$|a| = \tan\beta.$$

Consequentemente, $|c|$ pode ser determinado indiretamente. Assim,

$$\arg(a) = e = \frac{(g-1)\pi}{2g},\ \ |a| = \tan\beta,\ \ |c| = \left([\tan\beta]^2 - 1\right)^{\frac{1}{2}}\ \text{ e }\ \arg(c) = -\gamma,$$

o que é suficiente para obtermos os elementos

$$a, \overline{a}, c, \overline{c} \in \mathbb{C}$$

da transformação hiperbólica T_1. ■

4.2 O caso $g = 2^n$

Nesta seção consideramos os grupos Fuchsianos Γ_{4g} com $g = 2^n$. Nosso objetivo principal é provar que Γ_{4g} é derivado de uma álgebra dos quatérnios $\mathcal{A}$ sobre um corpo de números K, $[K : \mathbb{Q}] = 2^n$, onde 2^n é o gênero da superfície

$$\frac{\mathbb{B}}{\Gamma_{4g}},$$

bem como determinar a ordem dos quatérnios $\mathcal{O}$ em $\mathcal{A}$ associada ao grupo Γ_{4g}. Com isso, generalizamos o processo de identificação dos grupos Fuchsianos Γ_{4g} em ordens dos quatérnios.

Proposição 4.3 *Se $g = 2^n$ com $n > 0$, então*

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

onde

$$\theta = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2 + \sqrt{2}}}}$$

possui n radicais.

Prova. Como $g = 2^n$, temos que

$$2 \tan \frac{(2g-1)\pi}{4g} \cos \frac{(g-1)\pi}{2g} = 2 + 2 \cos \frac{\pi}{2^{n+1}}.$$

Por outro lado, para qualquer $x \in \mathbb{R}$,

$$2 \cos x = \sqrt{2 + 2 \cos 2x}.$$

Assim, para $n \in \mathbb{N}$ vale a igualdade

$$2 \cos \frac{\pi}{2^{n+1}} = \sqrt{2 + 2 \cos \frac{\pi}{2^n}}. \tag{4.7}$$

Para $n = 1$, isto é, para $g = 2$,

$$2 + 2 \cos \frac{\pi}{4} = 2 + \sqrt{2}.$$

Suponhamos, como hipótese de indução, que o resultado seja válido para n, ou seja,

$$2 + 2 \cos \frac{\pi}{2^{n+1}} = 2 + \theta,$$

onde θ possui n radicais. Assim, pela equação 4.7, obtemos

$$2 \cos \frac{\pi}{2^{n+2}} = \sqrt{2 + 2 \cos \frac{\pi}{2^{n+1}}} = \sqrt{2 + \theta}$$

possuindo $n + 1$ radicais. ■

Observe que $\cos\frac{\pi}{g}$ e $\operatorname{sen}\frac{\pi}{g}$ bem como $\cos\frac{k\pi}{g}$ e $\operatorname{sen}\frac{k\pi}{g}$, para todo $k \in \mathbb{Z}$, $g = 2^n$, podem ser calculados a partir da igualdade 4.7. De modo que, para qualquer $r \in \mathbb{Z}$, $r \neq \pm 1$, a matriz C^r pode ser escrita sob a forma

$$C^r = \begin{pmatrix} x & 0 \\ 0 & \overline{x} \end{pmatrix},$$

onde $x = a + bi$, $a, b \in \mathbb{Q}(\theta)$, e

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

Consideremos a isometria $f : \mathbb{H} \to \mathbb{B}$ definida por

$$f(z) = \frac{zi+1}{z+i},$$

temos que

$$\Gamma = f^{-1}\Gamma_{4g} f$$

é um subgrupo de $\mathrm{PSL}(2,\mathbb{R})$. Além disso, a aplicação $\xi : \Gamma \to \Gamma_{4g}$ definida por

$$\xi(T) = f^{-1} T f$$

é claramente um isomorfismo de grupos. Assim, $\Gamma \simeq \Gamma_{4g}$. Sejam $G_l = f^{-1}A_1 f$ os geradores de Γ, para $l = 1, \ldots, 2^{n+1}$. Usando as Proposição 4.3, as equações (4.5) e o Teorema 4.2, temos que os geradores G_l são dados por

$$G_l = \frac{1}{2}\begin{pmatrix} x_l + y_l\sqrt{\theta} & z_l + w_l\sqrt{\theta} \\ -z_l + w_l\sqrt{\theta} & x_l - y_l\sqrt{\theta} \end{pmatrix}, \ l = 1, \ldots, 2^{n+1}, \tag{4.8}$$

onde $x_l, y_l, z_l, w_l \in \mathbb{Z}[\theta]$ e θ é dado pela Proposição 4.3.

Com o objetivo de provar que, para cada $g = 2^n$, o grupo Γ_{4g} é derivado de uma álgebra dos quatérnios $\mathcal{A}$ sobre um corpo K, $[K : \mathbb{Q}] = 2^n$, consideremos o anel dos inteiros de $K = \mathbb{Q}(\theta)$.

Proposição 4.4 *Sejam $K = \mathbb{Q}(\theta)$ e θ dado na Proposição* 4.3. *Então o anel de inteiros de K é*

$$\mathbb{I}_K = \mathbb{Z}[\theta].$$

Prova. Como θ é um inteiro algébrico, claramente $\mathbb{Z}[\theta] \subset \mathbb{I}_K$. Para mostrar a outra inclusão seja G um subgrupo aditivo de $\mathbb{I}_K$ de posto 2^n com uma $\mathbb{Z}$-base

$$\left\{1, \theta, \ldots, \theta^{2n-1}\right\}.$$

Os 2^n monomorfismos $\varphi_i : K \to \mathbb{R}$ são dados por

$$\varphi_i(\theta) = \sqrt{2 \pm \sqrt{2 \pm \cdots \pm \sqrt{2 \pm \sqrt{2}}}},$$

pois os elementos $\varphi_i(\theta)$ são raízes do polinômio minimal de θ sobre $\mathbb{Q}$,

$$f_\theta(x) = x^{2^n} + a_{2^n-2}x^{2^n-2} + a_{2^n-4}x^{2^n-4} + \cdots + a_2x^2 + 2 \in \mathbb{Z}[x],$$

cujos coeficientes, exceto o lider, são pares. Assim, o discriminante

$$\Delta\left[1,\theta,\ldots,\theta^{2n-1}\right]=2^k,\ \text{ para algum }\ k\in\mathbb{N}.$$

Logo, pelo Teorema A.12 com $p=2$, concluímos que não existe nenhum inteiro algébrico da forma

$$\frac{1}{2}(\lambda_1+\lambda_2\theta+\cdots+\lambda_{2^n}\theta^{2^n-1}),$$

onde $0\leq\lambda_i\leq 1$, $i=1,\ldots,2^n$, caso contrário, existiriam $\lambda_i,\lambda_j\in\{0,1\}$ tais que

$$\frac{\lambda_i^{2^n}\pm 2\lambda_j^{2^n}}{4}\in\mathbb{Z}-\{0\},$$

o que é impossível. Portanto, $G=\mathbb{I}_K$, ou seja, $\mathbb{I}_K=\mathbb{Z}[\theta]$. ■

Proposição 4.5 *Seja Γ um grupo Fuchsiano artitmético finitamente gerado por $G_1,\ldots,G_l$, com*

$$G_k=\begin{pmatrix} x_k+y_k\sqrt{\theta} & z_k+w_k\sqrt{\theta}\\ -z_k+w_k\sqrt{\theta} & x_k-y_k\sqrt{\theta}\end{pmatrix},\ \ k=1,\ldots,l,$$

onde $G_k\in M(2,K\left(\sqrt{\theta}\right))$ e $\theta,x_k,y_k,z_k,w_k\in K$, sendo K um corpo. Então qualquer elemento $T\in\Gamma$ é escrito da mesma forma dos geradores de Γ.

Prova. Sejam G_1 e G_2 dois geradores de Γ, digamos

$$G_1=\begin{pmatrix} x_1+y_1\sqrt{\theta} & z_1+w_1\sqrt{\theta}\\ -z_1+w_1\sqrt{\theta} & x_1-y_1\sqrt{\theta}\end{pmatrix}\ \text{ e }\ G_2=\begin{pmatrix} x_2+y_2\sqrt{\theta} & z_2+w_2\sqrt{\theta}\\ -z_2+w_2\sqrt{\theta} & x_2-y_2\sqrt{\theta}\end{pmatrix}.$$

Se

$$G_1\cdot G_2=\begin{pmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix},$$

então

$$\begin{aligned}
a_{11} &= x_1x_2-z_1z_2+(y_1y_2+w_1w_2)\theta+(x_1y_2+x_2y_1+z_1w_2-z_2w_1)\sqrt{\theta},\\
a_{22} &= x_1x_2-z_1z_2+(y_1y_2+w_1w_2)\theta-(x_1y_2+x_2y_1+z_1w_2-z_2w_1)\sqrt{\theta},\\
a_{21} &= -z_1x_2-x_1z_2-(y_1w_2+w_1y_2)\theta+(-z_1y_2+x_2w_1+x_1w_2+y_1z_2)\sqrt{\theta},\\
a_{12} &= z_1x_2+x_1z_2+(y_1w_2+w_1y_2)\theta+(-z_1y_2+x_2w_1+x_1w_2+y_1z_2)\sqrt{\theta}.
\end{aligned}$$

■

Proposição 4.6 *Sejam a álgebra $\mathcal{A}=(a,b)_K$ com uma K-base $\{1,i,j,k\}$, $r\in\mathbb{N}-\{0\}$ fixado e o conjunto*

$$R=\left\{\frac{\alpha}{r^m}:\alpha\in\mathbb{I}_K\ \ e\ \ m\in\mathbb{N}\right\},$$

onde $\mathbb{I}_K$ é o anel de inteiros do corpo K. Então

$$\mathcal{O}=(a,b)_R=\{x=x_0+x_1i+x_2j+x_3k:x_0,x_1,x_2,x_3\in R\}$$

é uma ordem em $\mathcal{A}$.

Prova. É claro que R é um subanel de K contendo $\mathbb{I}_K$ e que $\mathcal{O}$ é um R-módulo. Por outro lado, se $\beta \in K$, então existe $c \in \mathbb{Z} - \{0\}$ tal que $c\beta \in \mathbb{I}_K$. Assim, para qualquer $x_l \in K$, existem $c_l \in \mathbb{Z} - \{0\}$ tais que $c_l x_l = \alpha_l \in \mathbb{I}_K$, $l = 0, 1, 2, 3$. Logo, dado

$$x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{A},$$

existe $\gamma \in K$ tal que $x = \gamma x'$, com $x' \in \mathcal{O}$, ou seja, $\mathcal{A} = K\mathcal{O}$. Portanto, $\mathcal{O}$ é uma ordem em $\mathcal{A}$. ■

Teorema 4.7 *Para cada $g = 2^n$ com $n > 0$, os elementos do grupo Fuchsiano $\Gamma \simeq \Gamma_{4g}$ são identificados, via isomorfismo (digamos φ, é tal que Γ é um subgrupo de $\Gamma(\mathcal{A}, \mathcal{O})$, onde $\mathcal{O} \subset \mathcal{A}$) com elementos do grupo dos invertíveis $\mathcal{O}^1$ da ordem*

$$\mathcal{O} = \left(\frac{\theta, -1}{R}\right),$$

onde

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

e θ é dado na Proposição 4.3. *Consequentemente,*

$$\left\{1, \sqrt{\theta}, \mathrm{Im}, \sqrt{\theta}\,\mathrm{Im}\right\}$$

é uma R-base para o reticulado $\mathcal{O}$, onde Im *é a unidade imaginária.*

Prova. Como os elementos do grupo Fuchsiano $\Gamma \simeq \Gamma_{4g}$ são identificados, via isomorfismo, digamos φ tal que

$$\Gamma_{4g} \simeq \Gamma \leq \Gamma(\mathcal{A}, \mathcal{O}) = \frac{\varphi(\mathcal{O}^1)}{\{\pm I_2\}},$$

onde $\mathcal{O} \subset \mathcal{A}$. Consideremos as matrizes $M_0, M_1, M_2, M_3 \in M\left(2, \mathbb{Q}\sqrt{\theta}\right)$ definidas por

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

Se $T \in \Gamma$, então, pela Proposição 4.5 e a definição dos geradores G_l, obtemos

$$T = \frac{1}{2^s} \begin{pmatrix} x_l + y_l\sqrt{\theta} & z_l + w_l\sqrt{\theta} \\ -z_l + w_l\sqrt{\theta} & x_l - y_l\sqrt{\theta} \end{pmatrix},$$

onde $s \in \mathbb{N}$ e $x_l, y_l, z_l, w_l \in \mathbb{Z}[\theta]$. Portanto, T é identificado com o elemento

$$x = \frac{x_l}{2^s} + \frac{y_l}{2^s} i + \frac{z_l}{2^s} j + \frac{w_l}{2^s} k \in \mathcal{O}^1 \subset \mathcal{O} = \left(\frac{\theta, -1}{R}\right),$$

através do isomorfismo $\varphi : A \to \varphi(\mathcal{A})$. Neste caso,

$$\varphi(A) \subset M_2(K, \sqrt{\theta})$$

com $\mathcal{A} = \left(\frac{\theta,-1}{K}\right)$ e $K = \mathbb{Q}(\theta)$.

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

ou seja,

$$\varphi(x) = T, \;\; i^2 = \theta, \;\; j^2 = -1, \;\; k = ij \;\text{ e }\; x_l, y_l, z_l, w_l \in \mathbb{Z}\left[\theta\right].$$

Portanto, cada elemento do grupo Fuchsiano $\Gamma \simeq \Gamma_{4g}$ é identificado, via o isomorfismo φ, com um elemento $x \in \mathcal{O}^1$ e

$$\left\{1, \sqrt{\theta}, \mathrm{Im}, \sqrt{\theta}\,\mathrm{Im}\right\}$$

é uma R-base de $\mathcal{O}$. ■

Teorema 4.8 *Para cada $g = 2^n$ com $n > 0$, o grupo Fuchsiano $\Gamma \simeq \Gamma_{4g}$, associado ao polígono hiperbólico regular P_{4g}, é derivado de uma álgebra de divisão dos quatérnios*

$$\mathcal{A} = \left(\frac{\theta,-1}{K}\right)$$

sobre o corpo de números $K = \mathbb{Q}(\theta)$, $[K : \mathbb{Q}] = 2^n$ e θ é dado na Proposição (4.3).

Prova. Pela Proposição 4.5, qualquer elemento $T \in \Gamma$ pode ser escrito sob a forma

$$T = \frac{1}{2^s}\begin{pmatrix} x_l + y_l\sqrt{\theta} & z_l + w_l\sqrt{\theta} \\ -z_l + w_l\sqrt{\theta} & x_l - y_l\sqrt{\theta} \end{pmatrix},$$

onde $s \in \mathbb{N}$ e $x_l, y_l, z_l, w_l \in \mathbb{Z}\left[\theta\right]$. Portanto, pelo Teorema 4.7, existe

$$x = \frac{x_l}{2^s} + \frac{y_l}{2^s} i + \frac{z_l}{2^s} j + \frac{w_l}{2^s} k \in \mathcal{O}^1$$

tal que

$$\varphi(x) = T.$$

Logo,

$$\mathrm{tr}(T) = \mathrm{tr}(\varphi(x)) = \mathrm{Tr}(x) = \frac{2x_l}{2^s} \in R.$$

Portanto, $\mathrm{tr}(\Gamma) \subset R$. Por outro lado, para o caso $g = 2^n$, obtemos

$$K = \mathbb{Q}(\mathrm{tr}(T) : T \in \Gamma) = \mathbb{Q}(\theta)$$

Essa igualdade pode ser verificada usando o fato de

$$\mathrm{tr}(T) \in \mathbb{Q}(\,\mathrm{tr}(T_1)), \;\; \forall \;\, T \in \Gamma \;\text{ e }\; \mathrm{tr}(T_1) = 2 + \theta.$$

Assim, a primeira condição do Teorema 3.42 é satisfeita.

Agora, seja $\varphi_2 : K \to \mathbb{R}$ um homomorfismo dado por $\varphi_2(\theta) = -\theta$, o qual estendemos ao isomofismo

$$\psi_2 : L \to \psi_2(L),$$

definido por

$$\psi_2(x+y\sqrt{\theta}) = \varphi_2(x) + \varphi_2(y)i\sqrt{\theta},\ ,\ \ \forall\ x,y \in K,$$

onde $L = K(\sqrt{\theta})$, $[L:K] = 2$. Consideremos agora a álgebra dos quatérnios $\mathcal{A}[\Gamma]$ sobre $K = \mathbb{Q}(\theta)$, confira Teorema 3.37,

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

Usando as definições dos geradores de Γ, obtemos

$$\mathcal{A}[\Gamma] = \left\{ \begin{pmatrix} a_1 & b_1 \\ -b_1' & a_1' \end{pmatrix} : a_1, b_1 \in L \right\},$$

onde a_1' e b_1' são os conjugados de a_1 e b_1 em L, respectivamente. Observe que L é uma extensão de K tal que $[L:K] = 2$, pois $x^2 - \theta$ é o polinômio minimal de $\sqrt{\theta}$. Seja

$$\Psi : \mathcal{A}[\Gamma] \to M(2,\mathbb{C})$$

a imersão definida por

$$\Psi(\alpha) = \begin{pmatrix} \psi_2(a_1) & \psi_2(b_1) \\ -\psi_2(b_1') & \psi_2(a_1') \end{pmatrix}.$$

Então

$$\mathcal{A}^{\psi_2} = \Psi(\mathcal{A}[\Gamma]) = \left\{ \begin{pmatrix} a & b \\ \overline{b} & \overline{a} \end{pmatrix} : a, b \in \psi_2(L) \right\}.$$

Pela Proposição 3.41, temos que

$$\mathcal{A}^{\varphi_2} \otimes \mathbb{R} \simeq H.$$

Por outro lado, se T é um elemento qualquer de Γ e

$$\mathrm{tr}(T) = a + a'$$

, então, pelo o Exemplo 3.18, obtemos

$$\psi_2(a) + \psi_2(a') \in [-2,2].$$

Como $a + a' \in K = \mathbb{Q}(\theta)$ temos

$$\psi_2(a) + \psi_2(a') = \psi_2(a+a') = \varphi_2(a+a'),$$

ou seja,

$$\varphi_2(a+a') \in [-2,2].$$

Portanto, $\varphi_2(\mathrm{tr}(\Gamma))$ é limitado em $\mathbb{C}$. Logo, a segunda condição do Teorema 3.42 é satisfeita. Portanto, Γ é derivado de uma álgebra dos quatérnios $\mathcal{A}$. ■

Pelo Teorema 4.8 temos que o espaço das órbitas

$$\frac{\mathbb{H}}{\Gamma}$$

é compacto (veja [11], página 76). Mas por construção, os emparelhamentos das arestas de P_{4g} são realizadas, de modo que a superfície

$$\frac{\mathbb{H}}{\Gamma}$$

seja compacta e orietável. Portanto, para os grupos $\Gamma \simeq \Gamma_{4g}$, $g = 2^n$, $n \in \mathbb{N}$ qualquer, vale a reciproca do seguinte resultado:

Teorema 4.9 *Seja Γ um grupo Fuchsiano derivado de uma álgebra de divisão dos quatérnios. Então o espaço quociente $\frac{\mathbb{H}}{\Gamma}$ é compacto.*

Prova. Verifique [11], página129, Teorema 5.4.1.

Para finalizarmos este Capítulo apresentaremos, como um exemplo, os geradores do grupo Fuchsiano Γ_{4g} para $g = 4$.

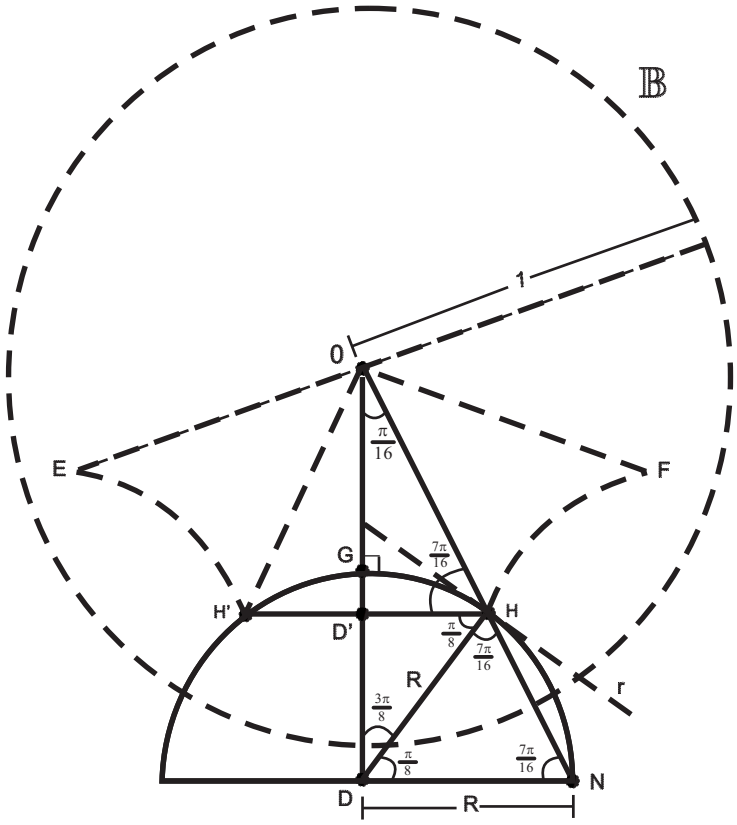

Figura 4.3: Triângulo $\{16, 16\}$.

Seja

$$C = \begin{pmatrix} e^{\frac{i\pi}{16}} & 0 \\ 0 & e^{\frac{-i\pi}{16}} \end{pmatrix}$$

a matriz de rotação que leva uma aresta em outra aresta adjacente no sentido antihorário em P_{16}. Pelo teorema 4.2, temos que T_1 é definida por

$$A_1 = \begin{pmatrix} a & b \\ \overline{b} & \overline{a} \end{pmatrix},$$

com

$$\arg(a) = \frac{3\pi}{8}, |a| = \tan\frac{7\pi}{16}, |b| = \left(\left(\tan\frac{7\pi}{16}\right)^2 - 1\right)^{\frac{1}{2}} \text{ e } \arg(b) = -\frac{9\pi}{16}.$$

Logo,

$$a = |a|\, e^{i\arg(a)} = \tan\frac{7\pi}{16}\left(\cos\frac{3\pi}{8} + i\,\mathrm{sen}\,\frac{3\pi}{8}\right)$$

e

$$b = |b|\, e^{i\arg(b)} = \left(\left(\tan\frac{7\pi}{16}\right)^2 - 1\right)^{\frac{1}{2}} e^{-\frac{9\pi}{16}i}.$$

Assim,

$$A_1 = \begin{pmatrix} \frac{x_1\left(1+i\left(1+\sqrt{2}\right)\right)}{2} & \frac{-\left(\sqrt{2}+iy_1\right)\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-(2-iy_1)\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1\left(1-i\left(1+\sqrt{2}\right)\right)}{2} \end{pmatrix}.$$

é a matriz associada a transformação T_1 que realiza o emparelhamento da aresta τ_1 com τ_1' em P_{16}, onde

$$x_1 = 2 + \sqrt{2+\sqrt{2}} \text{ e } y_1 = 2 + \sqrt{2} + 2\sqrt{2+\sqrt{2}}.$$

Observe, que

$$C = \begin{pmatrix} x + yi & 0 \\ 0 & x - yi \end{pmatrix}$$

onde

$$2x = \sqrt{2+\sqrt{2+\sqrt{2}}} \text{ e } 2y = \sqrt{2-\sqrt{2+\sqrt{2}}}.$$

Portanto, usando as igualdades 4.5 e o fato de

$$G_l = f^{-1}A_l f, l = 1, \ldots, 8,$$

obtemos os seguintes geradores do grupo Fuchsiano aritmético $\Gamma \simeq \Gamma_{16}$:

$$G_1 = \begin{pmatrix} \frac{x_1-y_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{z_1-w_1\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-z_1-w_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1+y_1\sqrt[4]{2+\sqrt{2}}}{2} \end{pmatrix} = \varphi(\frac{x_1}{2} - \frac{y_1}{2}i + \frac{z_1}{2}j - \frac{w_1}{2}k),$$

$$G_2 = \begin{pmatrix} \frac{x_1-w_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{z_1+y_1\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-z_1+y_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1+w_1\sqrt[4]{2+\sqrt{2}}}{2} \end{pmatrix} = \varphi(\frac{x_1}{2} - \frac{w_1}{2}i + \frac{z_1}{2}j + \frac{y_1}{2}k),$$

$$G_3 = \begin{pmatrix} \frac{x_1+y_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{z_1+w_1\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-z_1+w_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1-y_1\sqrt[4]{2+\sqrt{2}}}{2} \end{pmatrix} = \varphi(\frac{x_1}{2} + \frac{y_1}{2}i + \frac{z_1}{2}j + \frac{w_1}{2}k),$$

$$G_4 = \begin{pmatrix} \frac{x_1+w_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{z_1-y_1\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-z_1-y_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1-w_1\sqrt[4]{2+\sqrt{2}}}{2} \end{pmatrix} = \varphi(\frac{x_1}{2} + \frac{w_1}{2}i + \frac{z_1}{2}j - \frac{y_1}{2}k),$$

$$G_5 = \begin{pmatrix} \frac{x_1 - y_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{z_1 + w_1\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-z_1 + w_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1 + y_1\sqrt[4]{2+\sqrt{2}}}{2} \end{pmatrix} = \varphi(\frac{x_1}{2} - \frac{y_1}{2}i + \frac{z_1}{2}j - \frac{w_1}{2}k),$$

$$G_6 = \begin{pmatrix} \frac{x_1 + w_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{z_1 + y_1\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-z_1 + y_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1 - w_1\sqrt[4]{2+\sqrt{2}}}{2} \end{pmatrix} = \varphi(\frac{x_1}{2} + \frac{w_1}{2}i + \frac{z_1}{2}j + \frac{y_1}{2}k),$$

$$G_7 = \begin{pmatrix} \frac{x_1 + y_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{z_1 - w_1\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-z_1 - w_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1 - y_1\sqrt[4]{2+\sqrt{2}}}{2} \end{pmatrix} = \varphi(\frac{x_1}{2} + \frac{y_1}{2}i + \frac{z_1}{2}j - \frac{w_1}{2}k),$$

$$G_8 = \begin{pmatrix} \frac{x_1 - w_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{z_1 - y_1\sqrt[4]{2+\sqrt{2}}}{2} \\ \frac{-z_1 - y_1\sqrt[4]{2+\sqrt{2}}}{2} & \frac{x_1 + w_1\sqrt[4]{2+\sqrt{2}}}{2} \end{pmatrix} = \varphi(\frac{x_1}{2} - \frac{w_1}{2}i + \frac{z_1}{2}j - \frac{y_1}{2}k),$$

onde

$$z_1 = (1+2)\left(2 + \sqrt{2+\sqrt{2}}\right) \text{ e } w_1 = \sqrt{2}.$$

Assim, pelo Teorema 4.7 temos que a ordem associada ao grupo Fuchsiano

$$\Gamma \simeq \Gamma_{16}$$

é

$$\mathcal{O} = \left(\frac{\sqrt{2+\sqrt{2}}, -1}{R}\right),$$

onde

$$R = \left\{\frac{\alpha}{2^m} : \alpha \in \mathbb{Z}[\theta] \text{ e } m \in \mathbb{N}\right\}, \theta = \sqrt{2+\sqrt{2}}$$

e

$$\left\{1, \sqrt[4]{2+\sqrt{2}}, \mathrm{Im}, \sqrt[4]{2+\sqrt{2}}\,\mathrm{Im}\right\}$$

é uma R-base de $\mathcal{O}$.

Para $\{16, 16\}$, temos um polígono hiperbólico regular P_{16}, de 16 arestas, que por sua vez está associado ao grupo Fuchsiano Γ_{16}.

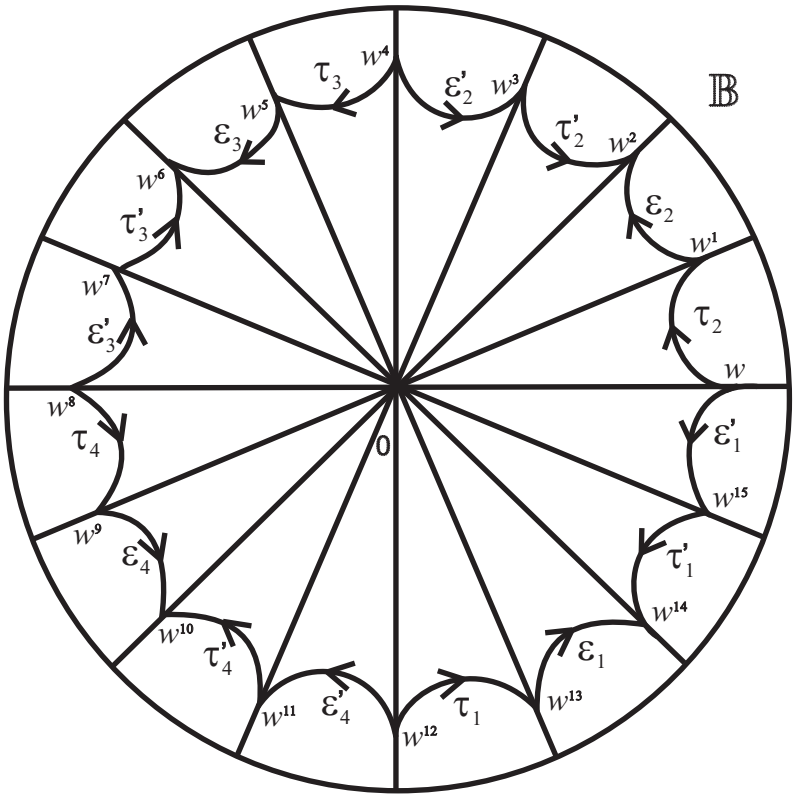

Figura 4.4: Tesselação $\{16, 16\}$ no plano Hiperbólico.

Apêndice A

Resultados Básicos

Neste apêndice, apresentaremos alguns resultados que serão necessários para o entendimento do exposto nos capítulos anteriores. O leitor interessado em mais detalhes pode consultar [3, 13, 18, 20].

A.1 Módulos

Nesta seção apresentaremos alguns resultados clássicos da teoria de módulos que serão necessários para a compreensão desta dissertação. Em toda esta seção a palavra anel significa, salvo menção explícita em contrário, anel comutativo com unidade.

Seja R um anel. Um *R-módulo* V é um grupo comutativo aditivo equipado com uma aplicação $R \times V \to V$,

$$R \times V \longrightarrow V, (r, \mathbf{v}) \longmapsto r\mathbf{v},$$

satisfazendo as seguintes propriedades:

1. $r(s\mathbf{v}) = (rs)\mathbf{v}$, para quaisquer $r, s \in R$ e $\mathbf{v} \in V$.
2. $(r + s)\mathbf{v} = r\mathbf{v} + s\mathbf{v}$, para quaisquer $r, s \in R$ e $\mathbf{v} \in V$.
3. $r(\mathbf{u} + \mathbf{v}) = r\mathbf{u} + r\mathbf{v}$, para qualquer $r \in R$ e $\mathbf{u}, \mathbf{v} \in V$.
4. $1\mathbf{v} = \mathbf{v}$, para todo $\mathbf{v} \in V$.

Note que, se R é um corpo, então um R-módulo é um espaço vetorial sobre R.

Um subconjunto não-vazio W de um R-módulo V é um *R-submódulo* de V se as seguintes condições são satisfeitas:

1. Para quaisquer $\mathbf{w}_1, \mathbf{w}_2 \in W$, têm-se $\mathbf{w}_1 - \mathbf{w}_2 \in W$.
2. Para quaisquer $r \in R$ e $\mathbf{w} \in W$, têm-se $r\mathbf{w} \in W$.

Sejam V um R-módulo e W um R-submódulo de V sobre R. Se $\mathbf{v}$ é um elemento arbitrário de V, escrevemos $[\mathbf{v}] = \mathbf{v} + W$ para representar o conjunto de todas as somas $\mathbf{v} + \mathbf{w}$, com $\mathbf{w} \in W$, isto é,

$$[\mathbf{v}] = \{\mathbf{v} + \mathbf{w} : \mathbf{w} \in W\}.$$

Estes conjuntos são chamados *classes laterais* de W em V. Estas classes particionam V em subconjuntos mutuamente disjuntos de mesma cardinalidade.

No teorema seguinte, utilizaremos as classes laterais de um R-submódulo W e de um R-módulo V, para definir um novo R-módulo, chamado *módulo quociente de V por W*, que será denotado por

$$\frac{V}{W}.$$

Teorema A.1 *Sejam V um R-módulo e W um R-submódulo de V. Então as classes laterais de W em V formam um R-módulo com as seguintes operações de adição e multiplicação por escalar*:

1. $[\mathbf{v}_1] + [\mathbf{v}_2] = [\mathbf{v}_1 + \mathbf{v}_2]$, *para quaisquer* $\mathbf{v}_1, \mathbf{v}_2 \in V$.
2. $r[\mathbf{v}] = [r\mathbf{v}]$, *para qualquer* $r \in R$ *e* $\mathbf{v} \in V$. ■

Sejam X um subconjunto de um R-módulo V e

$$\mathcal{F} = \{W : W \text{ é submódulo de } V \text{ e } X \subset W\}.$$

Então

$$\langle X \rangle = \bigcap_{W \in R} W$$

é o menor R-submódulo de V contendo X e será chamado de *R-submódulo gerado por X*. É claro que

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} r_i \mathbf{x}_i : n \in N, \ \mathbf{x}_i \in X \text{ e } r_i \in R \right\}.$$

Se $X = \{\mathbf{v}\}$, isto é, X consiste de um único elemento, então,

$$\langle \mathbf{v} \rangle = \{r\mathbf{v} : r \in R\} = Rv$$

e $\langle \mathbf{v} \rangle$ será chamado de *R-submódulo cíclico gerado por* $\mathbf{v}$.

Quando existir um subconjunto finito $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ de um R-módulo V tal que $V = \langle X \rangle$, dizemos que V é um *R-módulo finitamente gerado* e, neste caso,

$$V = \langle X \rangle = R\mathbf{x}_1 + \cdots + R\mathbf{x}_n.$$

Sejam U e V dois R-módulos. Uma função $T : U \to V$ é um *R-homomorfismo* se as seguintes condições são satisfeitas:

1. $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$, para todo $\mathbf{u}, \mathbf{v} \in U$.

2. $T(r\mathbf{u}) = rT(\mathbf{u})$, para todo $\mathbf{u} \in U$ e $r \in R$.

Um R-homomorfismo $T : U \longrightarrow V$ é um *R-isomorfismo* se T for bijetora. Denotaremos por

$$\mathrm{Hom}_R(U, V) = \{T : U \longrightarrow V : T \text{ é um } R\text{-homomorfismo}\}.$$

Em particular, quando $U = V$ temos que $\mathrm{Hom}_R(V, V) = \mathrm{End}_R(V)$.

Teorema A.2 (Propriedade Universal da Projeção) *Sejam V, W R-módulos e U um R-submódulo de V. Então para cada R-homomorfismo $T : V \to W$ com $U \subseteq \ker T$ existe um único R-homomorfismo $T_1 : \frac{V}{U} \to W$ tal que $T_1 \circ p = T$, e $p : V \to \frac{V}{U}$, onde p é um homomorfismo canônico $v \mapsto [v]$.* ■

Sejam V um R-módulo e X qualquer subconjunto não-vazio de V. Dizemos que V é um *R-módulo livre* sobre X se para cada elemento $v \in V$ existirem únicos elementos

$$x_1, x_2, \ldots, x_n \in X \text{ e } r_1, r_2, \ldots, r_n \in R$$

tais que

$$\mathbf{v} = r_1x_1 + r_2x_2 + \cdots + r_nx_n.$$

Dizemos que X é uma *R-base*.

Teorema A.3 *Sejam V, W R-módulos e $p : V \to W$ um R-homomorfismo sobrejetor. Então para cada R-homomorfismo $T : U \to W$ com U um R-módulo livre existe um único R-homomorfismo $S : U \to V$ tal que $T = p \circ S$.*

Prova. Como $U = R^{(X)}$ para algum conjunto não-vazio X de U e p é sobrejetor temos que para cada $x \in X$ existe algum $\mathbf{w}_x \in V$ tal que $p(\mathbf{w}_x) = T(e_x)$. Sendo $U = R^{(X)}$ um R-módulo livre temos que existe um único R-homomorfismo $S : U \to V$ tal que $S(e_x) = w_x$. Portanto,

$$(p \circ S)(e_x) = p(S(e_x)) = p(w_x) = T(e_x),$$

Concluímos daí que, $T = p \circ S$. ■

Teorema A.4 *Sejam R um domínio principal e V um R-módulo livre de posto n, onde o posto é visto como a cardinalidade da base do R-módulo. Então todo R-submódulo W de V é livre com posto $m \leq n$.* ■

Vamos denotar o conjunto de todas as transformações R-bilineares de $U \times V$ em W por

$$\mathcal{L}^2(U, V; W).$$

Sejam V um F-espaço vetorial e $\mathbf{v}_1, \ldots, \mathbf{v}_n$ vetores de V. Então $[B(\mathbf{v}_i, \mathbf{v}_j)]$ é uma matriz $n \times n$ sobre F. O *discriminante* de $\mathbf{v}_1, \ldots, \mathbf{v}_n$ com relação a B é definido por

$$\det([B(\mathbf{v}_i, \mathbf{v}_j)])$$

e será denotado por

$$\Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n).$$

Proposição A.5 *Sejam V um F-espaço vetorial e $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma F-base qualquer para V. Sejam $\mathbf{w}_1, \ldots, \mathbf{w}_n$ vetores quaisquer de V. Se*

$$\mathbf{w}_i = \sum_{j=1}^{n} a_{ij}\mathbf{v}_j, i = 1, \ldots, n,$$

com $a_{ij} \in F$, então

$$\Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = (\det \mathbf{A})^2 \Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n),$$

onde $\mathbf{A} = [a_{ij}]$.

Prova. Seja

$$\mathbf{w}_k = \sum_{l=1}^{n} a_{kl}\mathbf{v}_l, k = 1, \ldots, n.$$

Então é fácil verificar que

$$B(\mathbf{w}_i, \mathbf{w}_k) = \sum_{l=1}^{n} \left(\sum_{j=1}^{n} a_{ij} B(\mathbf{v}_j, \mathbf{v}_l) \right) a_{kl}.$$

Portanto,

$$[B(\mathbf{w}_i, \mathbf{w}_k)] = \mathbf{A}[B(\mathbf{v}_j, \mathbf{v}_l)]\mathbf{A}^t \text{ e } \Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = (\det \mathbf{A})^2 \Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n).$$

■

Corolário A.6 *Sejam V um F-espaço vetorial e $\mathbf{w}_1, \ldots, \mathbf{w}_n$ vetores quaisquer de V. Se $\mathbf{w}_1, \ldots, \mathbf{w}_n$ são linearmente dependentes, então*

$$\Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = 0.$$

■

A.2 Extensões de Corpos

Sejam K e F dois corpos. Dizemos que F é uma *extensão* de K se $K \subseteq F$ e será denotada por $K \subseteq F$ ou F/K.

Sejam F uma extensão de K e $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$. Então

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

denotará o menor subcorpo de F contendo $\alpha_1, \alpha_2, \ldots, \alpha_n$ e K. Uma extensão F de K é chamada *finitamente gerada sobre* K se existir $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ tais que

$$F = K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Se existir $\alpha \in F$ tal que $F = K(\alpha)$, dizemos que F é uma *extensão simples* de K e α é chamado um *elemento primitivo* de F sobre K.

Sejam F uma extensão de K e α um elemento de F. Dizemos que α é *algébrico* sobre K se existirem $a_0, a_1, \ldots, a_n \in K$, com $a_n \neq 0$, tais que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

isto é, existe um polinômio não-nulo $f \in K[x]$ tal que $f(\alpha) = 0$. Caso contrário, α é *transcendente* sobre K. Note que todo $\alpha \in K$ é algébrico sobre K, pois α é raiz do polinômio $p = x - \alpha \in K[x]$. Se todo elemento de uma extensão $K \subseteq F$ for algébrico sobre K, dizemos que F é uma *extensão algébrica*.

Proposição A.7 *Sejam F uma extensão de K e α um elemento de F. Então a função $\phi : K[x] \to F$ definida por $\phi(f) = f(\alpha)$ é um homomorfismo de anéis tal que*:

1. $\operatorname{Im}\phi = K[\alpha]$ *e* $K \subseteq K[\alpha] \subseteq F$.
2. α *é transcendente sobre K se, e somente se,* $\ker\phi = \{0\}$.
3. α *é algébrico sobre K se, e somente se,* $\ker\phi \neq \{0\}$.
4. $\frac{K[x]}{\ker\phi} \simeq K[\alpha]$. ■

Sejam F uma extensão de K e $\alpha \in F$ algébrico sobre K. Como

$$\frac{K[x]}{\langle p\rangle} \simeq K[\alpha] \subset F.$$

Segue-se que $\frac{K[x]}{\langle p\rangle}$ é um domínio. Logo, $\langle p\rangle$ é um ideal primo primo. Sendo $K[x]$ um domínio de fatoração, isto implica que $\langle p\rangle$ é um ideal maximal. Portanto, p é irredutível, e denotamos $p = \operatorname{irr}(\alpha, K)$. Assim, $K[\alpha]$ é um corpo e $K[\alpha] = K(\alpha)$.

Seja $K \subseteq F$ uma extensão. Então F com as operações de adição

$$\begin{array}{rccc} + : & F \times F & \to & F \\ & (a,b) & \mapsto & a+b \end{array}$$

e multiplicação por escalar

$$\begin{array}{rccc} \cdot : & K \times F & \to & F \\ & (\lambda, a) & \mapsto & \lambda a \end{array},$$

é um K-espaço vetorial. O *grau* de uma extensão $K \subseteq F$, denotado por $[F : K]$, é a dimensão de F visto como K-espaço vetorial. A extensão será chamada *finita* se $[F : K] = n < \infty$. Caso contrário, a extensão será chamada *infinita*.

Teorema A.8 *Sejam F uma extensão de K e α um elemento de F. Então α é algébrico sobre K se, e somente se, $K(\alpha)$ é uma extensão finita de K. Neste caso, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base para $K(\alpha)$ e $[K(\alpha) : K] = n$.* ■

Proposição A.9 *Sejam $K \subseteq F \subseteq E$ corpos tais que $[E : F]$ e $[F : K]$ sejam finitos. Então $[E : K]$ é finito e*

$$[E : K] = [E : F]\,[F : K]$$

■

Sejam K um corpo e $f \in K[x]$. Um *corpo de decomposição* de f sobre K é uma extensão de F sobre K tal que

1. f se fatora em F;
2. F é minimal com respeito à condição 1., isto é, se f se fatora em Z com $K \subseteq Z \subseteq F$, então $Z = F$.

Teorema A.10 *Seja K um corpo. Então qualquer $f \in K[x]$ possui um corpo de decomposição.*

■

Seja K um corpo. Dizemos que K é *algebricamente fechado* se qualquer polinômio não constante sobre K pode ser decomposto em fatores lineares sobre K. Um *fecho algébrico* de K é uma extensão algébrica F de K tal que as seguintes condições são satisfeitas:

1. F é algebricamente fechado.
2. F é minimal com respeito à condição 1., isto é, se Z é um corpo algebricamente fechado tal que $K \subseteq Z \subseteq F$, então $Z = F$.

Vamos denotar o fecho algébrico de K por $\overline{K}$. Neste caso, $\overline{K}$ é uma extensão algébrica de K.

Seja $K \subseteq F$ uma extensão. Dizemos que F é *normal* se F é um corpo de decomposição de alguma família $\mathcal{F} \subseteq K[x]$ de polinômios sobre K.

Proposição A.11 *Sejam $F = K[\alpha]$ com α algébrico, $p = \mathrm{irr}(\alpha, K) \in K[x]$ e N uma extensão normal de K contendo α. Se $\beta \in N$, então as seguintes condições são equivalentes*:

1. *$\beta \in N$ é uma raiz de p.*
2. *$p = \mathrm{irr}(\alpha, K) = \mathrm{irr}(\beta, K)$.*
3. *Existe um único K-isomorfismo $\sigma : K(\alpha) \to K(\beta)$, com $\sigma(\alpha) = \beta$.*
4. *Existe um K-automorfismo $\varphi : N \to N$, com $\varphi(\alpha) = \beta$.* ■

Se pelo menos uma (e portanto todas) das quatro condições da Proposição A.11 for satisfeita, dizemos que β é um *conjugado de α sobre K*. Conseqüentemente, o número de K-imersões de $K(\alpha)$ em N é menor ou igual ao número de raízes de p, isto é,

$$\mathrm{Hom}_K(F, N) \leq \partial(p) = [K[\alpha] : K].$$

Sejam $p \in K[x]$ um polinômio irredutível sobre K e L um corpo de decomposição para p. Dizemos que p é *separável* sobre K se todas as raízes de p em L são simples ou, equivalentemente,

$$\mathrm{mdc}(p, p') = 1.$$

Seja $f \in K[x]$ um polinômio qualquer. Dizemos que f é *separável* sobre K se cada um de seus fatores irredutíveis é separável sobre K.

Sejam F/K uma extensão e $\alpha \in F$. Dizemos que α é *separável* sobre K se α é algébrico sobre K e $\mathrm{irr}(\alpha, K)$ é separável sobre K. Dizemos que F/K é uma *extensão separável* se cada elemento de F for separável sobre K.

Teorema A.12 *Seja $\mathbb{I}_K$ o anel dos inteiros do corpo K e G um subgrupo aditivo de $\mathbb{I}_K$ de posto igual a $[K : \mathbb{Q}]$, com uma $\mathbb{Z}-$base $\{\alpha_1, \alpha_2, ..., \alpha_n\}$. Se $G \neq \mathbb{I}_K$ então, existe um inteiro álgebrico da forma*

$$\frac{1}{p}(\lambda_1\alpha_1 + ... + \lambda_n\alpha_n)$$

onde $0 \leq \lambda_i \leq p-1$, $\lambda_i \in \mathbb{Z}$, $i = 1, ..., n$, e p é um primo tal que p^2 divide $\Delta_G = \Delta(\alpha_1, \alpha_2, ..., \alpha_n)$.

A.3 Traços e Normas

Nesta seção, todas as extensões de K, salvo menção explícita em contrário, são separáveis.

Sejam F uma extensão finita de K com $[F : K] = n$ e $\alpha \in F$. Então a função $\phi_\alpha : F \to F$ definida por $\phi_\alpha(\beta) = \alpha\beta$ é claramente uma transformação K-linear sobre F. Logo, a função $\varphi : F \to \mathrm{End}_K F = \mathrm{Hom}_K(F, F)$ definida por $\varphi(\alpha) = \phi_\alpha$ é um homomorfismo de anéis injetor. Portanto, podemos identificar F com um subcorpo do anel $\mathrm{End}_K F$. Se

$$\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$$

é uma K-base para F e

$$\phi_\alpha(\alpha_j) = \sum_{i=1}^{n} a_{ij}\alpha_i, j = 1, \ldots, n,$$

então

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A})$$

é o *polinômio característico* de α sobre K, onde $\mathbf{A} = [a_{ij}]$ é a matriz $n \times n$ da transformação linear ϕ_α em relação à K-base $\mathcal{B}$.

Seja $\mathbf{A}$ a matriz da transformação linear ϕ_α em relação à alguma K-base. O *traço* e a *norma* de α são definidos por

$$\mathrm{tr}(\alpha) = \mathrm{tr}(\mathbf{A}) \text{ e } N(\alpha) = \det(\mathbf{A}).$$

Proposição A.13 *Seja F uma extensão de K com $[F : K] = n$.*

1. $\mathrm{tr}(a\alpha + b\beta) = a\,\mathrm{tr}(\alpha) + b\,\mathrm{tr}(\beta)$, *para todo $a, b \in K$ e $\alpha, \beta \in F$.*

2. $\mathrm{tr}(a) = na$, *para todo* $a \in K$.

3. $N(\alpha\beta) = N(\alpha)N(\beta)$, *para todo* $\alpha, \beta \in F$.

4. $N(a) = a^n$, *para todo* $a \in K$. ■

Suponhamos que

$$f_\alpha(x) = (x - \alpha_0) \cdots (x - \alpha_{n-1})$$

em $\overline{K}$. Então

$$\mathrm{tr}(\alpha) = \sum_{j=0}^{n-1} \alpha_j \text{ e } N(\alpha) = \prod_{j=0}^{n-1} \alpha_j.$$

De fato, se

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A}) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

então

$$a_{n-1} = -\mathrm{tr}(\mathbf{A}) \text{ e } a_0 = (-1)^n \det(\mathbf{A}).$$

Por outro lado, é fácil verificar que

$$\sum_{j=0}^{n-1} \alpha_j = -a_{n-1} \text{ e } \prod_{j=0}^{n-1} \alpha_j = (-1)^n a_0.$$

Portanto, $\mathrm{tr}(\alpha) \in K$ e $N(\alpha) \in K$.

Corolário A.14 *Seja* F *uma extensão de* K *com* $[F : K] = n$. *Se* $\sigma_i : F \longrightarrow \overline{K}$, $i = 1, \ldots, n$, *são as* K*-imersões deF em* $\overline{K}$, *então para todo* $\alpha \in F$ *temos que*

$$\mathrm{tr}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \text{ e } N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Além disso,

$$\mathrm{tr}(g(\alpha)) = \sum_{i=1}^{n} g(\alpha_i) \text{ e } N(g(\alpha)) = \prod_{i=1}^{n} g(\alpha_i),$$

para todo $\alpha \in F$ *e* $g \in K[x]$, *onde* $\alpha_i = \sigma_i(\alpha)$, $i = 1, \ldots, n$. ■

A função $B : F \times F \to K$ definida por $B(\alpha, \beta) = \mathrm{tr}(\alpha\beta)$ é claramente uma forma K-bilinear simétrica. Logo, por definição, o discriminante de uma K-base

$$\mathcal{B} = \{1, \theta, \ldots, \theta^{n-1}\}$$

para F é

$$\Delta(\mathcal{B}) = \det(\mathrm{tr}(\theta^{i+j})).$$

Se $\mathcal{B}' = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ é uma outra base de F tal que

$$\alpha_i = \sum_{j=0}^{n-1} a_{ij}\theta^j,$$

onde $\mathbf{B} = [a_{ij}]$ é a matriz mudança de base, então pela Proposição A.5 temos que

$$\Delta(\mathcal{B}') = (\det \mathbf{B})^2 \Delta(\mathcal{B}).$$

Proposição A.15 *Seja F uma extensão de K com $[F:K]=n$.*

1. *Se $\sigma_i : F \longrightarrow \overline{K}$, $i=1,\ldots,n$, são as K-imersões de F, onde F é algebricamente fechado, então*

$$\Delta(\mathcal{B}) = (\det(\sigma_i(\alpha_j)))^2$$

onde

$$\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$$

é uma K-base para F.

2. *Se $F = K(\alpha)$ e $p = \mathrm{irr}(\alpha, K) \in K[x]$, então*

$$\Delta(\mathcal{B}') = (-1)^{\frac{n(n-1)}{2}} N(p'(\alpha)) = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\sigma_j(\alpha) - \sigma_i(\alpha))^2,$$

onde

$$\mathcal{B}' = \{1, \alpha, \ldots, \alpha^{n-1}\}$$

é uma K-base para F.

Prova. Vamos provar apenas o item (1). Sejam

$$\mathbf{A} = [a_{ij}] \text{ e } \mathbf{A}^t = [b_{ij}]$$

onde $a_{ij} = \sigma_i(\alpha_j)$ e $b_{ij} = a_{ji}$. Então

$$\mathbf{A}^t\mathbf{A} = [c_{ij}],$$

onde

$$c_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj} = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \mathrm{tr}(\alpha_i\alpha_j).$$

Logo,

$$\Delta(\mathcal{B}') = \det(\mathrm{tr}(\alpha_i\alpha_j)) = \det(\mathbf{A}^t\mathbf{A}) = (\det(\mathbf{A}))^2.$$

■

Teorema A.16 *Seja F uma extensão finita de K. Então as seguintes condições são equivalentes*:

1. $\mathrm{tr} : F \to K$ *é sobrejetora.*
2. *Existe $\alpha \in F^*$ tal que $\mathrm{tr}(\alpha) \neq 0$.*
3. *A forma bilinear $B : F \times F \to K$ definida por $B((\alpha,\beta)) = \mathrm{tr}(\alpha\beta)$ é não-degenerada.*

Prova. É claro que (2. $\Rightarrow$ 1.). Para provar que (1. $\Rightarrow$ 2.), suponhamos que exista $\alpha \in F$ com $\mathrm{tr}(\alpha) = b \neq 0$. Logo,

$$\mathrm{tr}(cb^{-1}\alpha) = cb^{-1}\,\mathrm{tr}(\alpha) = cb^{-1}b = c, \forall c \in K.$$

Portanto, tr é sobrejetora.

(1. $\Rightarrow$ 3.) Suponhamos que tr seja sobrejetora. Então existe $\alpha \in F^*$ tal que $\mathrm{tr}(\alpha) \neq 0$. Dado $\beta \in F^*$, existe $\alpha\beta^{-1} \in F$ tal que

$$B(\alpha\beta^{-1}, \beta) = \mathrm{tr}(\alpha\beta^{-1}\beta) = \mathrm{tr}(\alpha) \neq 0.$$

Portanto, B é não degenerada.

(3. $\Rightarrow$ 1.) Segue da definição. ■

A.4 Inteiros Algébricos

Sejam $R \subseteq S$ uma extensão de anéis e α um elemento de S. Dizemos que α é um *inteiro algébrico* sobre R se existir $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

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

Se todo elemento de uma extensão $R \subseteq S$ for inteiro, dizemos que S é uma *extensão inteira* de R.

Teorema A.17 *Sejam $R \subseteq S$ uma extensão de anéis e α um elemento de S. Então as seguintes condições são equivalentes*:

1. *α é um inteiro sobre R;*
2. *$R[\alpha]$ é um R-módulo finitamente gerado;*
3. *Existe um anel Z com $R[\alpha] \subseteq Z \subseteq S$ tal que Z é um R-módulo finitamente gerado;*
4. *Existe um $R[\alpha]$-módulo V, o qual é um R-módulo finitamente gerado e cujo*

$$\mathrm{Ann}_{R[\alpha]}(V) = \{0\}.$$

■

Seja $R \subseteq S$ uma extensão de anéis. O *fecho inteiro* de R em S é definido como

$$R_S = \{\alpha \in S : \alpha \text{ é inteiro sobre } R\}.$$

Dizemos que R é *integralmente fechado* em S se $R_S = R$.

Teorema A.18 *Sejam $R \subseteq S \subseteq T$ extensões de anéis.*

1. *Se S é um R-módulo finitamente gerado, então S é uma extensão inteira de R.*

2. *Se $\alpha_1, \ldots, \alpha_n \in S$ são inteiros sobre R, então $R[\alpha_1, \ldots, \alpha_n]$ é um R-módulo finitamente gerado.*

3. *R_S é um anel com $R \subseteq R_S \subseteq S$.*

4. *Se $S = R_T$, então S é integralmente fechado em T.* ■

Proposição A.19 *Sejam R um dominio, K seu corpo quociente com $R_K = R$, F uma extensão finita de K e $S = R_F$.*

1. *Se $\alpha \in S$, então $\sigma_i(\alpha)$ são inteiros sobre R, onde $\sigma_i : F \longrightarrow \overline{K}$, $i = 1, \ldots, n$, são as K-imersões de F em $\overline{K}$.*

2. *Se $\alpha \in S$, então $\mathrm{tr}(\alpha), N(\alpha) \in R$.*

3. *$\alpha \in U(S)$ se, somente se, $N(\alpha) \in U(R)$.*

4. *Se $\alpha \in R$ é tal que $N(\alpha)$ é irredutível em R, então α é irredutível em S.*

5. *Qualquer elemento de F pode ser escrito na forma $\frac{c}{a}$, onde $c \in S$ e $a \in R$. Em particular, F é o corpo quociente de S, ou seja, $F = R^{-1}S$.*

Prova. 1. Seja $\alpha \in S$. Então existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

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

Logo

$$0 = \sigma_i(0) = \sigma_i\left(\sum_{i=0}^{n} a_i\alpha^i\right) = \sum_{i=0}^{n} a_i\sigma_i(\alpha^i).$$

Portanto, $\sigma_i(\alpha)$ inteiro sobre R.

2. É claro que o $\mathrm{tr}(\alpha) \in K$ e $N(\alpha) \in K$. Por outro lado, como $\sigma_i(\alpha)$ são inteiros sobre R temos, pelo Corolário A.14, que $\mathrm{tr}(\alpha)$ e $N(\alpha)$ são inteiros sobre R. Logo, $\mathrm{tr}(\alpha), N(\alpha) \in R_K = R$.

3. Suponhamos que $\alpha \in U(S)$. Então existe $\beta \in S$ tal que $\alpha\beta = 1$. Logo,

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Portanto, $N(\alpha) \in U(R)$. Reciprocamente, se $N(\alpha) \in U(R)$, então existe $a \in R$ tal que $aN(\alpha) = 1$. Logo,

$$1 = aN(\alpha) = a\prod_{j=1}^{n}\sigma_j(\alpha).$$

Como $\sigma_j = id$, para algum $j = 1, \ldots, n$, temos que $\alpha \in U(S)$, onde

$$\alpha^{-1} = (a\prod_{i=1, i\neq j}^{n}\sigma_i(\alpha)).$$

4. Segue da definição de elemento irredutível e do item 3.

5. Dado $\alpha \in F$. Como α é algébrico sobre K temos que existem $r_0, r_1, \ldots, r_{n-1} \in K$ tais que

$$r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Fazendo

$$r_i = \frac{a_i}{b_i} \text{ e } \beta = b_0 b_1 \cdots b_{n-1} \in R,$$

obtemos

$$c_0 + c_1(\alpha\beta) + \cdots + c_{n-1}(\alpha\beta)^{n-1} + (\alpha\beta)^n = 0.$$

Assim, $\beta\alpha \in S = R_F$. Portanto, existe $c \in S$ tal que $\alpha = \frac{c}{\beta}$. ■

Referências Bibliográficas

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

[2] Conway, J. B., *Functions of one Complex Variable*. Springer-Verlag, 2nd. ed., 1973.

[3] Endler, O. *Teoria dos Números Algébricos*. IMPA, Rio de Janeiro, 1985.

[4] Felzenszwalb, B. *Álgebras de Dimensão Finita*. IMPA, Rio de Janeiro, 1979.

[5] Firer, M. *Grupos fuchsianos*. Notas de Aula, IMECC-UNICAMP, 2001.

[6] Garcia, A. L. e Lequain, Y., *Álgebra*: *Um Curso de Introdução*. IMPA, Rio de Janeiro, 1988.

[7] Gonçalves, A. *Introdução à Álgebra*. IMPA, Rio de Janeiro, 1979.

[8] Johansson, S. *On Fundamental Domains of Arithmetic Fuchsian Groups*. www.math.chalmers.se/~sj/forskning.html.

[9] Johansson, S. *Genera of Arithmetic Fuchsian Groups*. www.math.chalmers.se/~sj/forskning.html.

[10] Johansson, S. *A Description of Quaternion Algebra*. www.math.chalmers.se/~sj/forskning.html.

[11] Katok, S. *Fuchsian Groups*. The University of Chicago Press, 1992.

[12] Lima, E. L., *Elementos de Topologia Geral*, LTC, 2.ª ed., 1976.

[13] MacLane, S. and Birkhoff, G. *Algebra*. Macmillan Company, 1968.

[14] Maclachlan, C. e Reider, A. W. *The Arithmetic of Hyperbolic 3-Manifolds*. Spring-Verlag, Berlim-Heidelberg-New York, 2003.

[15] O'Meara, O. T. *Introduction to Quadratic Forms*. Spring-Verlag, Berlim-Heidelberg-New York, 1973.

[16] Reiner, I. *Maximal Orders*. Academic Press, London, 1975.

[17] Ribenboin, P. *Algebraic Numbers*. New York, Wiley-Interscience, 1972.

[18] Samuel, P., *Algebraic Theory of Numbers.* Hermann, Paris 1970.

[19] Silva, A. A., *Notas de Aulas*, Depto de Matemática, UFPB - Campus I.

[20] Stewart, I.N. e Tall, D.O. *Algebraic Number Theory*. Chapman and Hall, 1996.

[21] Vieira, V. L. *Grupos Fuchsianos Aritméticos Identificados em Ordens dos Quatérnios para Construção de Constelações de Sinais*. Tese de Doutorado, FEEC-UNICAMP, 2007.

[22] Vieira, V. L. e Júnios, R. P. *"Grupos Fuchsianos Identificados em uma Ordem dos Quatérnios sobre uma Extensão dos Racionais de grau* 2^n*"*, XXII Simpósio Brasileiro de Telecomunicações. Campinas, São Paulo 2005.

[23] Vignéras, M. F. *Aritmétique des Algébres de Quaternions*. Spring-Verlag, Berlim-Heidelberg-New York, 1980.

[24] Weiss, E., *Algebraic Number Theory*, Dover, 1998.