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

Códigos Geométrico e Aritmético de Geodésicas Fechadas

por

Maria Isabelle Silva Borges

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 grau de Mestre em Matemática.

Janeiro/2003

João Pessoa - Pb

Códigos Geométrico e Aritmético de Geodésicas Fechadas

por

Maria Isabelle Silva Borges

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

Área de Concentração: Álgebra

Aprovada por:

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

Prof. Dr. Hélio Pires de Almeida - UFPB

Prof. Dr. Trajano Pires da Nobrega Neto- UNESP

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

Janeiro/**2003**

Agradecimentos

1. A Deus por todo o apoio espiritual e pela forte presença em minha vida.

2. Ao amigo e orientador Prof. Andrade, pela amizade,paciência, dedicação, respeito e acima de tudo pela grande orientação.

3. Ao professor Marivaldo Pereira Matos por todas as contribuições, em especial pelas figuras deste trabalho.

4. Aos professores das disciplinas básicas Fernando Xavier, Nelson Nery e Pedro Venegas que muito contribuiram para a minha formação.

5. Ao professor Hélio Pires de Almeida por toda contribuição e pela ajuda com o estágio docência.

6. Ao professor Trajano Pires da Nobrega Neto por ter participado da banca examinadora e por todas as sugestões.

7. Ao professor Marinaldo Felipe da Silva da Universidade Federal de Rodônia pela ajuda e por todas as sugestões.

8. Ao meu esposo Jader Morais Borges por todo incentivo e principalmente por ter compreendido toda minha ausência durante esses dois anos.

9. Aos meus pais Assis e Guia e Irmãos Maria José, Célia, Josemar, Zeneide, Josivan, Zuleide e Darizy que sempre deram muita força para que eu terminasse meus estudos.

10. Ao meu sogro Antonio Borges Sobrinho e minha sogra Avani Morais Borges, por terem me acolhido em sua casa nestes dois anos.

11. Aos colegas do curso de mestrado, em especial as amigas Anisia Nogueira, Claudilene Gomes da Costa e Solange Delgado.

12. A Sônia, pela competência e gentileza no atendimento aos alunos.

13. Aos Professores do DME - UFCG que contribuiram para minha formação durante toda graduação.

14. A CAPES pelo suporte financeiro para a realização do curso de mestrado.

Dedicatória

Aos meus pais
Assis e Guia , e
ao meu esposo Jader.

Resumo

Geodésicas fechadas associadas a classes de conjugação de matrizes hiperbólicas em $\mathrm{SL}(2,\mathbb{Z})$ podem ser codificadas de duas maneiras diferentes. O código geométrico, com respeito a uma dada região fundamental é obtido por construção universal para grupos Fuchsianos; já o código aritmético, dado por frações contínuas menos, resulta da teoria de redução de Gauss e é específico para o $\mathrm{SL}(2,\mathbb{Z})$. Nesta dissertação apresentamos uma descrição completa das geodésicas fechadas para as quais estes dois códigos coincidam.

Abstract

Closed geodesics associated to conjugacy classes of hyperbolic matrices in $\mathrm{SL}(2,\mathbb{Z})$ can be in two different ways. The geometric code, with respect to a given fundamental region, is obtained by a construction universal for all Fuchsian groups, while the arithmetic code, given by minus continued fractions, comes from the Gauss reduction theory and is specific for $\mathrm{SL}(2,\mathbb{Z})$. In this dissertation we give a complete description of all closed geodesics for which the two codes coincide.

Notação

$\mathbb{Z}_n$ - Anel dos inteiros módulo n

$\theta_{\gamma_1,\gamma_2}$ - Ângulo entre γ_1 e γ_2

$B_r\,(0)$ - Bola aberta centrada em 0 de raio r

$B_r\,[0]$ - Bola fechada centrada em 0 de raio r

aH - Classe lateral à esqueda de H em G

$h(\gamma)$ - Comprimento da curva

$\equiv$ - Congruência

$M_2(\mathbb{R})$ - Conjunto das matrizes 2×2 sobre $\mathbb{R}$

$\mathbb{C}$ - Conjunto dos números complexos

$\mathbb{N}$ - Conjunto dos números naturais

$\mathbb{Z}$ - Conjunto dos números inteiros

$\mathbb{R}$ - Conjunto dos números reais

$\det(A)$ - Determinante de A

DT - Diferencial de T

Δ - Discriminante

$\rho(z,w)$ - Distância hiperbólica entre z e w

$|$ - Divide

$C(T)$ - Eixo da transformação de T

$\widehat{\mathbb{C}}$ - Esfera de Riemann

$T_z\mathcal{H}$ - Espaço tangente

G - Grupo

$\mathrm{Isom}(\mathcal{H})$ - Grupos das isometrias de $\mathcal{H}$

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

$\mathrm{SL}(2,\mathbb{R})$ - Grupo linear especial

$\mathrm{GL}(2,\mathbb{R})$ - Grupo linear geral

$\mathrm{PSL}(2,\mathbb{R})$ - Grupo linear projetivo especial

Γ - Grupo modular

$\frac{G}{H}$ - Grupo quociente de G por H

$\cong$ - Isomorfo

A_n - Matriz do tipo $\begin{pmatrix} n & -1 \\ 1 & 0 \end{pmatrix}$

$\mathrm{mdc}(a, b)$ - Máximo divisor comum de a e b

ds - Métrica hiperbólica

$\lfloor \xi \rfloor$ - Parte inteira do número real ξ

w - Ponto fixo atrator

w_n - Ponto fixo atrator da matriz A_n

u - Ponto fixo repulsor

u_n - Ponto fixo repulsor da matriz A_n

$D_p(\Gamma)$ - Região de Dirichlet para Γ centrada em p

F - Região fundamental

$[z, w]$ - Segmento geodésico que une z a w

$\mathcal{H}$ - Semi plano superior

$\langle g \rangle$ - Subgrupo cíclico de G gerado por g

Sumário

Introdução

As curvas Geodésicas podem ser codificadas por dois tipos de códigos: O código geométrico, com respeito a uma dada região fundamental, é obtido por construção universal para grupos Fuchsianos. O código aritmético, dado por frações contínuas menos, vem da teoria de redução de Gauss e é especifico para $\mathrm{SL}(2,\mathbb{Z})$. O principal objetivo desta dissertação é apresentar condições necessárias e suficientes para que esses dois códigos coincidam.

Antes de apresentarmos o grupo Fuchsiano que trabalharemos durante toda esta dissertação, descreveremos abaixo como ocorre a codificação para um grupo Fuchsiano finitamente gerado qualquer.

Sejam Γ um grupo Fuchsiano finitamente gerado e $\mathcal{D}$ uma região fundamental de Dirichlet para Γ, conforme Figura 1. Temos que tal região tem um número par de lados identificados pelos geradores de Γ que denotamos por $\{\gamma_i\}$. Rotularemos os lados de $\mathcal{D}$ por elementos do conjunto $\{\gamma_i\}$ da seguinte forma: Se um lado s de $\mathcal{D}$ é identificado em $\mathcal{D}$ com o lado $\gamma_j(s)$, rotulamos s por γ_j. Rotulando todas as imagens de s sobre Γ pelo mesmo gerador γ_j, obtemos o rótulo do reticulado inteiro $\mathcal{N}$ da imagem dos lados de $\mathcal{D}$, tal que, cada lado em $\mathcal{N}$ tenha dois rótulos correspondentes às imagens de $\mathcal{D}$ compartilhadas por este lado. Qualquer geodésica orientada em $\mathcal{H}$ pode ser codificada por uma seqüência de geradores de Γ, tal geodésica rotula os lados sucessivos de $\mathcal{N}$ por ela cortados. Para cada corte escolhemos o rótulo correspondente a imagem da geodésica que entra. Esta seqüência descrita é considerada de tal forma que a geodésica não passa através dos vértices de $\mathcal{N}$. Podemos assumir que a geodésica intercepta $\mathcal{D}$ e escolher um ponto inicial sobre o interior de $\mathcal{D}$. Saindo de $\mathcal{D}$, a geodésica entra na imagem vizinha de $\mathcal{D}$ através do lado rotulado, digamos, por γ_1, conforme Figura 1. Portanto, esta imagem é $\gamma_1(\mathcal{D})$, e o primeiro símbolo do código é γ_1. Se ela entra na segunda imagem de $\mathcal{D}$ através

do lado rotulado por γ_2, então a segunda imagem é

$$(\gamma_1\gamma_2\gamma_1^{-1})(\gamma_1(\mathcal{D})) = \gamma_1\gamma_2(\mathcal{D}),$$

e o segundo símbolo é γ_2 e, assim por diante. Consequentemente, obtemos uma seqüência de todas as imagens de $\mathcal{D}$ cruzadas por nossa geodésica na direção de suas orientações:

$$\mathcal{D}, \gamma_1(\mathcal{D}), \gamma_1\gamma_2(\mathcal{D}), \ldots.$$

Se uma geodésica é o eixo de um elemento hiperbólico primitivo $\gamma \in \Gamma$, então

$$\gamma = \gamma_1\gamma_2 \cdots \gamma_n,$$

para algum $n \in \mathbb{N}$. Neste caso, a seqüência é periódica com período mínimo

$$[\gamma_1, \gamma_2, \ldots, \gamma_n].$$

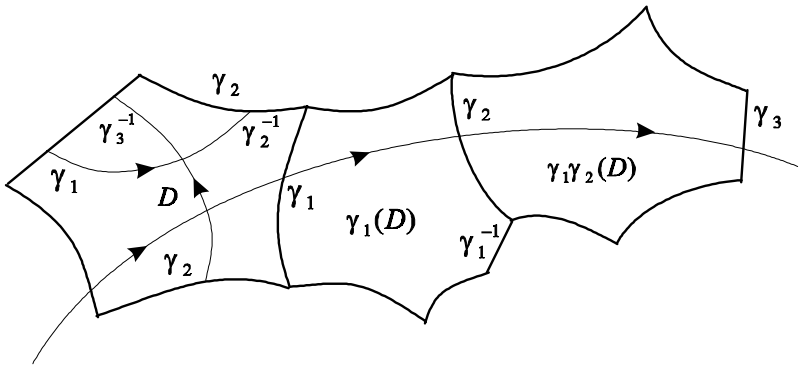

Figura 1. A região de Dirichlet e suas imagens

Mapeando os segmentos da geodésica orientada entre todos os cortes consecutivos do reticulado $\mathcal{N}$, chega-se novamente a $\mathcal{D}$, conforme a Figura 1. Assim, obtemos uma geodésica em $\mathcal{D}$.

A seqüência de codificação descrita acima também pode ser obtida tomando os inversos dos geradores de Γ, isto é,

$$\gamma^{-1} = \gamma_n^{-1} \cdots \gamma_2^{-1}\gamma_1^{-1}.$$

O eixo de um elemento hiperbólico primitivo $C(\gamma)$ torna-se uma geodésica fechada em $\mathcal{D}$. Se a geodésica passa através de um vértice de $\mathcal{D}$, surge ambigüidade em encontrar um código para ela. Neste trabalho nada foi elaborado a este respeito.

Se dois elementos são conjugados em Γ, suas geodésicas fechadas coincidem e, consequentemente, o período de suas seqüências codificada diferem por uma permutação cíclica.

Reciprocamente, se dois elementos hiperbólicos primitivos tem períodos em suas seqüências codificadas que diferem por uma permutação cíclica, então eles são conjugados em Γ, e consequentemente, suas geodésicas fechadas coincidem.

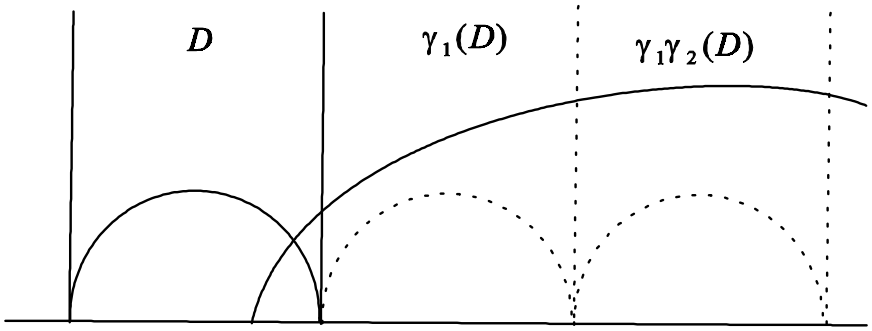

Figura 2. Levantamento da Figura 1. para o plano hiperbólico

Chamaremos o período da seqüência codificada de $C(\gamma)$ com respeito a uma dada região de Dirichlet $\mathcal{D}$, a menos de permutação cíclica, o *código de Morse* de uma geodésica fechada associada a classe de conjugação de γ e denotaremos por

$$[\gamma] = [\gamma_1, \gamma_2, \ldots, \gamma_n] .$$

O eixo da transformação inversa, $C(\gamma^{-1})$, é o mesmo de $C(\gamma)$, mas com direção oposta. Além disso,

$$\left[\gamma^{-1}\right] = \left[\gamma_n^{-1}, \gamma_{n-1}^{-1}, \ldots, \gamma_1\right] .$$

O código de Morse da matriz A, denotado por $[A]$, é o código de Morse da transformação de Möbius correspondente.

Veremos mais tarde que o grupo Fuchsiano considerado nesta dissertação é

$$\Gamma = \mathrm{PSL}(2, \mathbb{Z})$$

e que os geradores são

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

Assim, as geodésicas serão codificadas por uma seqüencia de T's e S's.

Grosseiramente falando, o código geométrico nada mais é do que uma seqüência de números inteiros, onde cada número representa o quantidade de T's entre os S's do código de Morse. Enquanto que o código aritmético é dado pela expansão em frações contínuas do ponto fixo atrator.

Esta dissertação é contituída de quatro capítulos. No capítulo 1 apresentamos um pouco da teoria de frações contínuas, que será utilizada aqui, para representar o código aritmético associado a uma matriz de $\mathrm{SL}(2, \mathbb{Z})$.

Algumas adaptações foram feitas para que essa teoria se encaixasse no nosso problema, ou seja, a expansão em frações contínuas de um número $\xi \in \mathbb{R}$, que seria

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{}{a_{k-1} + \cfrac{1}{a_k}}}}}$$

onde

$$a_0 = \lfloor \xi \rfloor \text{ e } \xi_0 = \frac{1}{\xi - a_0}$$

e indutivamente

$$a_i = \left\lfloor \xi_{i-1} \right\rfloor \text{ e } \xi_i = \frac{1}{\xi_{i-1} - a_i}$$

será considerado aqui como segue

$$\xi = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cfrac{1}{\ddots \cfrac{}{a_{k-1} - \cfrac{1}{a_k}}}}}$$

com

$$a_0 = \lfloor \xi \rfloor + 1 \text{ e } \xi_0 = \frac{1}{a_0 - \xi}$$

e, indutivamente,

$$a_i = \left\lfloor \xi_{i-1} \right\rfloor + 1 \text{ e } \xi_i = \frac{1}{a_i - \xi_{i-1}}.$$

O que chamaremos de fração contínua "menos." Essa modificação foi feita com o único propósito de deixar um elemento α, que tem uma expansão em fração contínua "puramente periódica" no seguinte intervalo

$$\alpha > 1 \text{ e } 0 < \alpha' < 1,$$

onde α' é conjugada a α. Desta forma teremos que uma matriz será "reduzida" se, e somente se, seu ponto fixo atrator tem expansão em fração contínua puramente periódica.

No capítulo 2, falamos um pouco sobre teoria de grupos e além disso, tratamos sobre o grupo modular $\mathrm{PSL}(2, \mathbb{Z})$.

No capítulo 3, estudamos um pouco de geometria hiperbólica, região fundamental.

E por fim, no capítulo 4, tratamos sobre o ponto central da nossa dissertação, que é mostrar as condições necessárias e suficientes para que esses dois códigos coincidam.

Capítulo 1

Frações Contínuas

Neste capítulo apresentaremos uma outra representação de um número real, a qual fornece um visão que não é revelada pela representação decimal. Mais precisamente, a teoria das frações contínuas "menos" está relacionada a teoria da redução de Gauss para formas quadrática inteiras indefinidas de um ponto de vista matricial. Para maiores informações o leitor pode consultar [9].

1.1 Frações contínuas "menos"

Dado qualquer número

$$\xi_0 \in \mathbb{R},$$

definimos

$$a_0 = \lfloor \xi_0 \rfloor + 1 \text{ e } \xi_1 = \frac{1}{a_0 - \xi_0},$$

e o próximo

$$a_1 = \lfloor \xi_1 \rfloor + 1 \text{ e } \xi_2 = \frac{1}{a_1 - \xi_1}$$

e, assim, recursivamente, definimos

$$a_i = \lfloor \xi_i \rfloor + 1 \text{ e } \xi_{i+1} = \frac{1}{a_i - \xi_i}, \tag{1.1}$$

onde

$$\lfloor \xi \rfloor = \max\{n \in \mathbb{Z} : n \leq \xi\}.$$

Como

$$\xi_0 = a_0 - \frac{1}{\xi_1} \text{ e } \xi_1 = a_1 - \frac{1}{\xi_2}$$

temos que

$$\xi_0 = a_0 - \frac{1}{a_1 - \frac{1}{\xi_2}}$$

Assim, repassando $\xi_2, \xi_3, \xi_4, \ldots$, obtemos que

$$\xi_0 = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cfrac{1}{\ddots - \frac{1}{\cdots}}}}.$$

Isto é uma *expansão em fração contínua "menos"* de ξ_0. Note que, $a_i \geq 2$, para todo $i \in \mathbb{N}$, pois se ξ_i é inteiro, então

$$a_i - \xi_i = 1, \forall i \in \mathbb{N} \text{ e } a_i = 2.$$

Se ξ_i não é inteiro, então

$$\begin{aligned} a_{i-1} - 1 &< \xi_{i-1} < a_{i-1} \Rightarrow 0 < a_{i-1} - \xi_{i-1} < 1 \Rightarrow \\ \xi_i &= \frac{1}{a_{i-1} - \xi_{i-1}} > 1, \forall i \in \mathbb{N} \text{ e } a_i = \lfloor \xi_i \rfloor + 1 \geq 2. \end{aligned}$$

Usaremos a notação

$$\xi_0 = (a_0, a_1, \ldots, a_k, \ldots)$$

para designar a fração contínua menos dada por (1.1). Neste caso,

$$(a_0, a_1, \ldots, a_k) = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cfrac{1}{\ddots - \frac{1}{a_k}}}}.$$

Note que,

$$\begin{aligned} (a_0, a_1, \ldots, a_k) &= (a_0, a_1, \ldots, a_{k-2}, a_{k-1} - \frac{1}{a_k}) \\ &= a_0 - \frac{1}{(a_1, a_2, \ldots, a_k)} \\ &= (a_0, (a_1, a_2, \ldots, a_k)). \end{aligned}$$

Mais geralmente,

$$(a_0, a_1, \ldots, a_k) = (a_0, a_1, \ldots a_{i-1}, (a_i, \ldots, a_k)), \text{ para } 1 \leq i < k.$$

Exemplo 1.1 *Expandir em fração contínua menos o número racional*

$$\xi_0 = \frac{3}{17}.$$

Solução. Como

$$\begin{aligned} a_0 &= 1 \text{ e } \xi_1 = \frac{17}{14} \\ a_1 &= 2 \text{ e } \xi_2 = \frac{14}{11} \\ a_2 &= 2 \text{ e } \xi_3 = \frac{11}{8} \\ a_3 &= 2 \text{ e } \xi_4 = \frac{8}{5} \\ a_4 &= 2 \text{ e } \xi_5 = \frac{5}{2} \\ a_5 &= 3 \text{ e } \xi_6 = 2 \\ a_6 &= 3 \text{ e } \xi_7 = 1 \end{aligned}$$

temos que

$$\frac{3}{17} = (1, 2, 2, 2, 2, 3, 3, 2, 2, \ldots).$$

Agora, vamos definir duas seqüências

$$\{\alpha_k\} \text{ e } \{\beta_k\}$$

indutivamente com segue:

$$\begin{aligned} \alpha_{-2} &= 0, \alpha_{-1} = 1 \text{ e } \alpha_i = a_i\alpha_{i-1} - \alpha_{i-2} \text{ para } i \geq 0 \\ \beta_{-2} &= -1, \beta_{-1} = 0 \text{ e } \beta_i = a_i\beta_{i-1} - \beta_{i-2} \text{ para } i \geq 0. \end{aligned} \tag{1.2}$$

Note que, $\beta_0 = 1$, $\beta_1 = a_1\beta_0 \geq \beta_0$, $\beta_2 > \beta_1$, etc., de modo que,

$$1 = \beta_0 \leq \beta_1 < \beta_2 < \beta_3 < \cdots < \beta_k < \cdots$$

e, assim, $\lim_{k\to\infty} \beta_k = \infty$, pois β_k é uma seqüência crescente de inteiros.

Proposição 1.1 *Para qualquer* $\theta \in \mathbb{R}_+^*$,

$$(a_0, a_1, \ldots, a_{k-1}, \theta) = \frac{\theta\alpha_{k-1} - \alpha_{k-2}}{\theta\beta_{k-1} - \beta_{k-2}}, \forall k \in \mathbb{Z}_+.$$

Prova. A prova será feita por indução sobre k. Se $k = 0$, o resultado será interpretado como

$$\theta = \frac{\theta\alpha_{-1} - \alpha_{-2}}{\theta\beta_{-1} - \beta_{-2}},$$

o qual é verdadeiro pelas equações (1.2). Se $k = 1$, o resultado é

$$(a_0, \theta) = a_0 - \frac{1}{\theta} = \frac{\theta\alpha_0 - \alpha_{-1}}{\theta\beta_0 - \beta_{-1}}$$

Suponhamos que o resultado seja válido para

$$(a_0, a_1, \ldots, a_{k-1}, \theta).$$

Logo,

$$\begin{aligned}
(a_0, a_1, \ldots, a_k, \theta) &= (a_0, a_1, \ldots, a_{k-1}, a_k - \frac{1}{\theta}) \\
&= \frac{\left(a_k - \frac{1}{\theta}\right)\alpha_{k-1} - \alpha_{k-2}}{\left(a_k - \frac{1}{\theta}\right)\beta_{k-1} - \beta_{k-2}} \\
&= \frac{\theta\left(a_k\alpha_{k-1} - \alpha_{k-2}\right) - \alpha_{k-1}}{\theta\left(a_k\beta_{k-1} - \beta_{k-2}\right) - \beta_{k-1}} \\
&= \frac{\theta\alpha_k - \alpha_{k-1}}{\theta\beta_k - \beta_{k-1}}.
\end{aligned}$$

■

Proposição 1.2 *Seja*

$$x_k = (a_0, a_1, \ldots, a_k), \forall k \in \mathbb{Z}_+.$$

Então

$$x_k = \frac{\alpha_k}{\beta_k}.$$

Prova. Pela Proposição 1.1 e as equações (1.2), obtemos que

$$\begin{aligned}
x_k &= (a_0, a_1, \ldots, a_k) \\
&= \frac{a_k\alpha_{k-1} - \alpha_{k-2}}{a_k\beta_{k-1} - \beta_{k-2}} \\
&= \frac{\alpha_k}{\beta_k}.
\end{aligned}$$

■

Proposição 1.3 *Para todo $i \geq 1$ temos que*

$$\alpha_{i-1}\beta_i - \alpha_i\beta_{i-1} = 1 \;\; e \;\; x_{i-1} - x_i = \frac{1}{\beta_{i-1}\beta_i}.$$

Além disso, a fração $\frac{\alpha_i}{\beta_i}$ é irredutível.

Prova. Pelas equações (1.2), obtemos que

$$\alpha_{-2}\beta_{-1} - \beta_{-2}\alpha_{-1} = 1.$$

Suponhamos que o resultado seja válido para $i-1$, isto é,

$$\alpha_{i-2}\beta_{i-1} - \alpha_{i-1}\beta_{i-2} = 1.$$

Assim, pelas equações (1.2), obtemos que

$$\begin{aligned}
\alpha_{i-1}\beta_i - \alpha_i\beta_{i-1} &= \alpha_{i-1}\left(a_i\beta_{i-1} - \beta_{i-2}\right) - \beta_{i-1}\left(a_i\alpha_{i-1} - \alpha_{i-2}\right) \\
&= \alpha_{i-2}\beta_{i-1} - \alpha_{i-1}\beta_{i-2} \\
&= 1.
\end{aligned}$$

Assim, provamos a primeira parte do teorema. Dividindo por $\beta_{i-1}\beta_i$, obtemos que

$$x_{i-1} - x_i = \frac{1}{\beta_{i-1}\beta_i}.$$

Finalmente, se $d = \text{mdc}(\alpha_i, \beta_i)$, então d divide 1 e, portanto, $d = 1$. Portanto, a fração $\frac{\alpha_i}{\beta_i}$ é irredutível. ■

Observação 1.1 *Note que*

$$\frac{\beta_k}{\beta_{k-1}} = (a_k, a_{k-1}, \ldots, a_2, a_1), \forall k \in \mathbb{N},$$

pois

$$\begin{aligned}
\frac{\beta_1}{\beta_0} &= a_1, \\
\frac{\beta_2}{\beta_1} &= \frac{a_2\beta_1 - \beta_0}{\beta_1} = a_2 - \frac{1}{a_1} \\
&\vdots \\
\frac{\beta_k}{\beta_{k-1}} &= \frac{a_k\beta_{k-1} - \beta_{k-2}}{\beta_{k-1}} = a_k - \frac{1}{\frac{\beta_{k-1}}{\beta_{k-2}}}
\end{aligned}$$

e se $a_0 > 0$, *então*

$$\frac{\alpha_k}{\alpha_{k-1}} = (a_k, a_{k-1}, \ldots, a_1, a_0), \forall k \geq 1,$$

pois

$$\begin{aligned}
\frac{\alpha_1}{\alpha_0} &= a_1 - \frac{1}{a_0}, \\
\frac{\alpha_2}{\alpha_1} &= \frac{a_2\alpha_1 - \alpha_0}{\alpha_1} = a_2 - \frac{1}{\frac{\alpha_1}{\alpha_0}} \\
&\vdots \\
\frac{\alpha_k}{\alpha_{k-1}} &= \frac{a_k\alpha_{k-1} - \alpha_{k-2}}{\alpha_{k-1}} = a_k - \frac{1}{\frac{\alpha_{k-1}}{\alpha_{k-2}}}.
\end{aligned}$$

Proposição 1.4 *Os valores x_k definidos na Proposição* 1.2 *satisfazem*

$$x_j < x_{j-1}.$$

Além disso, $\lim_{k\to\infty} x_k$ *existe e*

$$x_{j+1} < \lim_{k\to\infty} x_k < x_j, \forall j \in \mathbb{Z}_+.$$

Prova. Como

$$x_{i-1} - x_i = \frac{1}{\beta_i \beta_{i-1}} > 0$$

temos que

$$x_j < x_{j-1} \text{ e } x_j > a_0 - 1, \forall j \in \mathbb{Z}_+.$$

Assim, a seqüência x_0, x_1, x_2, ... é decrescente e limitada inferiormente por $a_0 - 1$. Logo, $\lim_{k\to\infty} x_k$ existe. Como

$$\lim_{i\to\infty} (x_{i-1} - x_i) = \lim_{i\to\infty} \frac{1}{\beta_i \beta_{i-1}} = 0,$$

pois $\beta_i < \beta_{i+1}$, temos que

$$x_{j+1} < \lim_{k\to\infty} x_k < x_j, \forall j \in \mathbb{Z}_+.$$

■

Proposição 1.5 *Temos que* $\lim_{k\to\infty} x_k = \xi_0$.

Prova. Pela Proposição 1.1, obtemos que

$$\begin{aligned} \xi_0 &= (a_0, a_1, \ldots, a_{k-1}, \xi_k) \\ &= \frac{\xi_k \alpha_{k-1} - \alpha_{k-2}}{\xi_k \beta_{k-1} - \beta_{k-2}}, \end{aligned} \tag{1.3}$$

com os α_i e β_i dados pelas equações (1.2). Pela Proposição 1.2, obtemos que

$$\begin{aligned} x_{k-1} - \xi_0 &= \frac{\alpha_{k-1}}{\beta_{k-1}} - \xi_0 \\ &= \frac{\alpha_{k-1}}{\beta_{k-1}} - \frac{\xi_k \alpha_{k-1} - \alpha_{k-2}}{\xi_k \beta_{k-1} - \beta_{k-2}} \\ &= \frac{(\alpha_{k-1}\beta_{k-2} + \alpha_{k-2}\beta_{k-1})}{\beta_{k-1}(\xi_k \beta_{k-1} + \beta_{k-2})} \\ &= \frac{1}{\beta_{k-1}(\xi_k \beta_{k-1} + \beta_{k-2})} \\ &\leq \frac{1}{\beta_{k-1}}, \end{aligned}$$

pois $\beta_k < \beta_{k+1}$ e $\xi_k > 0$. Como $\lim_{k\to\infty} \beta_{k-1} = \infty$ temos que

$$\lim_{k\to\infty} (x_{k-1} - \xi_0) = 0.$$

Portanto,

$$\begin{aligned} \xi_0 &= \lim_{k\to\infty} x_k \\ &= \lim_{k\to\infty} (a_0, a_1, \ldots, a_k) \\ &= (a_0, a_1, a_2, \ldots). \end{aligned}$$

■

Uma seqüência infinita de inteiros a_0, a_1, a_2, ... com $a_i \geq 2$, para todo $i \in \mathbb{N}$, determina uma fração contínua menos infinita

$$(a_0, a_1, a_2, \ldots).$$

O valor

$$(a_0, a_1, a_2, \ldots) := \lim_{k\to\infty} (a_0, a_1, a_2, \ldots, a_k).$$

Este limite, sendo o igual $\lim_{k\to\infty} x_k$, existe. Assim, uma outra maneira de escrever este limite é

$$(a_0, a_1, a_2, \ldots) = \lim_{k\to\infty} \frac{\alpha_k}{\beta_k}.$$

O número racional

$$(a_0, a_1, a_2, \ldots, a_k) = \frac{\alpha_k}{\beta_k} = x_k$$

é chamado o *k-ésimo convergente* da fração contínua menos infinita. Neste caso, dizemos que a fração contínua menos infinita *converge* para o valor

$$\lim_{k\to\infty} x_k.$$

Lema 1.1 *Seja*

$$\theta = (a_0, a_1, a_2, \ldots)$$

uma fração contínua menos infinita. Então $a_0 = \lfloor \theta \rfloor + 1$. *Além disso, se*

$$\theta_1 = (a_1, a_2, a_3, \ldots),$$

então

$$\theta = a_0 - \frac{1}{\theta_1}.$$

Assim, indutivamente, obtemos a equação (1.1).

Prova. Pela Proposição 1.4, obtemos que

$$x_1 < \theta < x_0,$$

isto é,

$$a_0 - \frac{1}{a_1} < \theta < a_0.$$

Como $a_1 \geq 2$ temos que

$$a_0 - 1 < \theta < a_0 \Leftrightarrow a_0 < \theta + 1 < a_0 + 1$$

Logo, $a_0 = \lfloor \theta \rfloor + 1$. Finalmente,

$$\begin{aligned} \theta &= \lim_{k\to\infty}(a_0, a_1, a_2, \ldots, a_k) \\ &= \lim_{k\to\infty}\left(a_0 - \frac{1}{(a_1, a_2, \ldots, a_k)}\right) \\ &= a_0 - \frac{1}{\lim_{k\to\infty}(a_1, a_2, \ldots, a_k)} \\ &= a_0 - \frac{1}{\theta_1}. \end{aligned}$$

■

Proposição 1.6 *Duas frações contínuas menos infinitas distintas convergem para valores diferentes.*

Prova. Suponhamos que

$$\theta = (a_0, a_1, a_2, \ldots) = (b_0, b_1, b_2, \ldots).$$

Então, pelo Lema 1.1, $\lfloor \theta \rfloor + 1 = a_0 = b_0$ e

$$a_0 - \frac{1}{(a_1, a_2, \ldots)} = b_0 - \frac{1}{(b_1, b_2, \ldots)}$$

implica que

$$(a_1, a_2, \ldots) = (b_1, b_2, \ldots).$$

Assim, por indução $a_k = b_k$, para todo $k \in \mathbb{Z}_+$. ■

Conclusão 1.1 *Existe uma correspondência biunívoca entre o conjunto dos números reais e o conjunto das seqüências infinitas $a_1, a_2, \ldots a_k, \ldots$, com $a_i \in \mathbb{Z}$ e $a_i \geq 2$, para todo $i \in \mathbb{N}$.*

Exemplo 1.2 *Avaliar a fração contínua menos infinita*

$$(2, 2, 2, \ldots).$$

Solução. Seja

$$\theta = (2, 2, 2, \ldots).$$

Então, pelo Lema 1.1, obtemos que

$$\begin{aligned} \theta &= 2 - \frac{1}{(2, 2, 2, \ldots)} \\ &= 2 - \frac{1}{\theta} \end{aligned}$$

e $\theta^2 - 2\theta + 1 = 0$. Logo,

$$\theta = 1.$$

Proposição 1.7 *Seja $\xi_0 \in \mathbb{R}$ tal que*

$$\xi_0 = (a_0, a_1, a_2, \ldots).$$

Então ξ_0 é um número racional se, e somente se, existir $n \in \mathbb{N}$ tal que $a_k = 2$, para todo $k \geq n$.

Prova. Suponhamos que ξ_0 seja um número racional. Se $\xi_0 = a \in \mathbb{Z}$, então, pela equação (1.1),

$$\xi_0 = (a + 1, 2, 2, \ldots).$$

Se $\xi_0 \in \mathbb{Q}$ e $\xi_0 \notin \mathbb{Z}$, digamos

$$\xi_0 = \frac{c_0}{d_0},$$

com $\text{mdc}(c_0, d_0) = 1$, então, pela equação (1.1),

$$\xi_i = (a_i, a_{i+1}, a_{i+2}, \ldots) = \frac{c_i}{d_i} \in \mathbb{Q},$$

com $\text{mdc}(c_i, d_i) = 1$, para todo $i \geq 1$.

Afirmação. $\xi_n \in \mathbb{Z}$, para algum $n \in \mathbb{N}$.

De fato, suponhamos, por absurdo, que $\xi_n \notin \mathbb{Z}$, para todo $n \in \mathbb{N}$, isto é, $d_n > 1$, para todo $n \in \mathbb{N}$. Além disso,

$$\frac{c_n}{d_n} > 1, \forall n \in \mathbb{N},$$

pois $a_n \geq 2$, para todo $n \in \mathbb{N}$. Como

$$\frac{c_0}{d_0} = a_0 - \frac{1}{\frac{c_1}{d_1}} = a_0 - \frac{d_1}{c_1}$$

temos que

$$\frac{c_0}{d_0} + \frac{d_1}{c_1} = a_0.$$

De modo geral,

$$\frac{c_n}{d_n} + \frac{d_{n+1}}{c_{n+1}} = a_n, \forall n \in \mathbb{N},$$

ou ainda,

$$d_n d_{n+1} + c_n c_{n+1} = a_n c_{n+1} d_n, \forall n \in \mathbb{N}.$$

Desde que c_{n+1} divide $c_n c_{n+1}$ e $a_n c_{n+1} d_n$, para todo $n \in \mathbb{N}$, obtemos que c_{n+1} divide $d_n d_{n+1}$. Como $\text{mdc}(c_{n+1}, d_{n+1}) = 1$ temos que c_{n+1} divide d_n, ou seja, $c_{n+1} < d_n$. Sendo $d_{n+1} < c_{n+1}$, obtemos que

$$d_{n+1} < d_n, \forall n \in \mathbb{N},$$

o que é uma contradição. Reciprocamente, suponhamos que exista $n \in \mathbb{N}$ tal que $a_k = 2$, para todo $k \geq n$. Então

$$\begin{aligned} \xi_0 &= (a_0, a_1, a_2, \ldots a_{n-1}, 2, 2, \ldots) \\ &= (a_0, a_1, a_2, \ldots a_{n-1}, 1) \in \mathbb{Q}. \end{aligned}$$

■

Seja

$$\theta = (a_0, a_1, a_2, \ldots)$$

uma fração contínua menos infinita. Dizemos que ela é *periódica* se existirem k_0 e m tais que

$$a_k = a_{k+m}, \forall k \geq k_0.$$

O menor destes $m's$ é chamado o *período* desta fração. Neste caso, denotaremos esta fração contínua menos infinita por

$$\left(a_0, a_1, \ldots, a_{k_0-1}, \overline{a_{k_0}, a_{k_0+1}, \ldots, a_{k_0+m-1}}\right).$$

Quando $k_0 = 0$, dizemos que ela é *puramente periódica*.

Seja $\theta \in \mathbb{R}$. Dizemos que θ é uma *irracionalidade quadrática* se θ é raiz irracional de um polinômio quadrático com coeficientes em $\mathbb{Z}$.

Exemplo 1.3 *Seja $\theta = \sqrt{5} \in \mathbb{R}$. Então θ é uma irracionalidade quadrática, pois θ é raiz irracional de um polinômio quadrático*

$$x^2 - 5 \in \mathbb{Z}[x].$$

Teorema 1.1 *Seja $\xi \in \mathbb{R}$. Então ξ é uma irracionalidade quadrática se, e somente se, sua expansão em fração contínua menos infinita é periódica, exceto o caso em que a parte periódica for 2.*

Prova. Suponhamos que a expansão em fração contínua menos infinita de ξ seja periódica

$$\xi = (b_0, b_1, \ldots, b_k, \overline{a_0, a_1, \ldots, a_{m-1}}) .$$

Seja

$$\begin{aligned} \theta &= (\overline{a_0, a_1, \ldots, a_{m-1}}) \\ &= (a_0, a_1, \ldots, a_{m-1}, \theta) \end{aligned}$$

Então, pela equação (1.3), obtemos que

$$\begin{aligned} \theta &= (a_0, a_1, \ldots, a_{m-1}, \theta) \\ &= \frac{\theta\alpha_{m-1} - \alpha_{m-2}}{\theta\beta_{m-1} - \beta_{m-2}}. \end{aligned}$$

Assim,

$$\beta_{m-1}\theta^2 - (\beta_{m-2} + \alpha_{m-1})\theta + \alpha_{m-2} = 0.$$

Como

$$\beta_{m-1}x^2 - (\beta_{m-2} + \alpha_{m-1})x + \alpha_{m-2} \in \mathbb{Z}[x]$$

temos, pela Proposição 1.3, que θ é uma irracionalidade quadrática. Agora, vamos escrever ξ em termos de θ,

$$\begin{aligned} \xi &= (b_0, b_1, \ldots, b_k, \theta) \\ &= ((b_0, b_1, \ldots b_{i-1}), (b_i, \ldots, b_k), \theta) \\ &= (b_0, b_1, \ldots b_{i-1}) + \frac{1}{(b_i, \ldots, b_k) + \frac{1}{\theta}} \\ &= \frac{(pr + qs)\theta + ps}{qr\theta + qs}, \end{aligned}$$

onde

$$\frac{p}{q} = (b_0, b_1, \ldots, b_{i-1}) \text{ e } \frac{r}{s} = (b_i, b_{i+1}, \ldots, b_k).$$

Sendo ξ da forma

$$\frac{a+\sqrt{b}}{c}, a, b, c \in \mathbb{Z} \text{ com } b > 0 \text{ e } c \neq 0,$$

temos que ξ é semelhante a θ. Portanto, ξ é uma irracionalidade quadrática.

Reciprocamente, suponhamos que ξ seja uma raiz de um polinômio quadrático. Então ξ é da forma

$$\frac{a+\sqrt{b}}{c}, a, b, c \in \mathbb{Z} \text{ com } b > 0 \text{ e } c \neq 0.$$

Note que, b não é um quadrado perfeito, pois θ é irracional. Multiplicando o numerador e o denominador por $|c|$, obtemos que

$$\xi = \frac{ac+\sqrt{bc^2}}{c^2} \text{ ou } \xi = \frac{-ac+\sqrt{bc^2}}{-c^2}.$$

Assim, podemos escrever ξ na forma

$$\xi = \frac{m_0+\sqrt{d}}{q_0},$$

onde

$$q_0 \mid (m_0^2 - d) \text{ e } d, m_0, q_0 \in \mathbb{Z} \text{ com } q_0 \neq 0$$

e d não é um quadrado perfeito. Definimos $\xi_0 = \xi$ e indutivamente

$$a_i = \lfloor \xi_i \rfloor + 1 \text{ e } \xi_{i+1} = \frac{1}{a_i - \xi_i}, i \in \mathbb{Z}_+.$$

Vamos provar que

$$\xi_i = \frac{m_i+\sqrt{d}}{q_i}, m_{i+1} = a_i q_i - m_i \text{ e } q_{i+1} = \frac{m_{i+1}^2 - d}{q_i}. \tag{1.4}$$

Para concluir que a fração contínua menos infinita é periódica, basta encontrar r e s tais que $\xi_r = \xi_s$. Vamos dividir a prova em alguns passos:

1º **Passo**. m_i e q_i são inteiros não nulos.

De fato, se $i = 0$, então m_0 e q_0 são inteiros por construção. Suponhamos que o resultado seja válido para i, isto é, m_i e q_i são inteiros não nulos e

$$q_i \mid (m_i^2 - d).$$

Note que, $m_{i+1} = a_i q_i - m_i$ é um inteiro não nulo. Então a equação

$$\begin{aligned} q_{i+1} &= \frac{m_{i+1}^2 - d}{q_i} \\ &= \frac{(a_i q_i - m_i)^2 - d}{q_i} \\ &= \frac{m_i^2 - d}{q_i} - 2a_i m_i + a_i^2 q_i \end{aligned}$$

prova que q_{i+1} é um inteiro. Além disso, $q_{i+1} \neq 0$, pois se $q_{i+1} = 0$, então $d = a_{i+1}^2$, o que é impossível, visto que d não é um quadrado.

2º **Passo**. $a_i - \xi_i = \frac{1}{\xi_{i+1}}$.

De fato,

$$\begin{aligned} a_i - \xi_i &= a_i - \frac{m_i + \sqrt{d}}{q_i} \\ &= \frac{a_i q_i - m_i - \sqrt{d}}{q_i} \\ &= \frac{m_{i+1} - \sqrt{d}}{q_i} \\ &= \frac{m_{i+1}^2 - d}{q_i(m_{i+1} + \sqrt{d})} \\ &= \frac{q_{i+1}}{m_{i+1} + \sqrt{d}} \\ &= \frac{1}{\xi_{i+1}}. \end{aligned}$$

Assim, pela equação (1.1), obtemos que

$$\xi = \xi_0 = (a_0, a_1, a_2, \ldots).$$

Pela Proposição 1.2, obtemos que

$$\xi_0 = \frac{\xi_k \alpha_{k-1} - \alpha_{k-2}}{\xi_k \beta_{k-1} - \beta_{k-2}}.$$

Se definimos o *conjugado* de $\xi = a + b\sqrt{d}$ como $\xi' = a - b\sqrt{d}$, então

$$\xi_0' = \frac{\xi_k' \alpha_{k-1} - \alpha_{k-2}}{\xi_k' \beta_{k-1} - \beta_{k-2}}.$$

Resolvendo para ξ_k', obtemos

$$\xi_k' = \frac{\beta_{k-2}}{\beta_{k-1}} \left(\frac{\xi_0' - \frac{\alpha_{k-2}}{\beta_{k-2}}}{\xi_0' - \frac{\alpha_{k-1}}{\beta_{k-1}}} \right).$$

Como

$$\lim_{k \to \infty} \frac{\alpha_{k-2}}{\beta_{k-2}} = \lim_{k \to \infty} \frac{\alpha_{k-1}}{\beta_{k-1}} = \xi_0$$

temos que

$$\lim_{k \to \infty} \left(\frac{\xi_0' - \frac{\alpha_{k-2}}{\beta_{k-2}}}{\xi_0' - \frac{\alpha_{k-1}}{\beta_{k-1}}} \right) = 1.$$

Assim, existe $k_0 \in \mathbb{N}$ tal que

$$\left(\frac{\xi_0' - \frac{\alpha_{k-2}}{\beta_{k-2}}}{\xi_0' - \frac{\alpha_{k-1}}{\beta_{k-1}}} \right) > 0 \text{ e } 0 < \xi_k' < 1, \forall k \geq k_0,$$

pois

$$\frac{\beta_{k-2}}{\beta_{k-1}} < 1.$$

Assim, $\xi_k - \xi'_k > 0$, para todo $k \geq k_0$, pois $\xi_k > 1$ para todo $k \geq 1$. Pela equação (1.4), obtemos que

$$\xi_k - \xi'_k = \frac{2\sqrt{d}}{q_k} > 0 \text{ e } q_k > 0, \forall k \geq k_0.$$

Como

$$0 < \frac{m_k - \sqrt{d}}{q_k} < 1 \text{ e } \frac{m_k + \sqrt{d}}{q_k} > 1, \forall k \geq k_0,$$

temos que

$$|m_k - q_k| < \sqrt{d}. \tag{1.5}$$

Como d é um número inteiro positivo fixado temos que a equação (1.5) tem somente um número finito de possíveis valores para $k \geq k_0$. Assim,

$$d - (m_k - q_k)^2 > 0$$

tem somente um número finito de possíveis valores para $k \geq k_0$ e pela equação (1.4)

$$d - (m_k - q_k)^2 = q_k(-q_{k-1} - q_k + 2m_k) \Rightarrow q_k \mid d - (m_k - q_k)^2.$$

Assim, q_k tem somente um número finito de possíveis valores e, assim, m_k. Logo, existem inteiros j e l distintos tais que $m_k = m_j$ e $q_k = q_l$. Portanto, podemos escolher r e s de modo que $r < s$. Pela equação (1.4), obtemos que $\xi_r = \xi_s$ e, portanto,

$$\xi = \xi_0 = (a_0, a_1, a_2, \ldots, a_{r-1}, \overline{a_r, a_{r+1}, a_{r+2}, \ldots, a_{s-1}}),$$

além disso, a parte periódica não pode ser apenas 2, pois ξ é irracional. ■

Corolário 1.1 *Seja $\xi \in \mathbb{R}$ uma irracionalidade quadrática. Se*

$$\xi = (\overline{a_0, a_1, a_2, \ldots, a_{k-1}}), \forall k > 1,$$

então

$$\frac{1}{\xi'} = (\overline{a_{k-1}, a_{k-2}, \ldots, a_1, a_0}).$$

Prova. Como ξ e ξ' são raízes do polinômio

$$f(x) = \beta_{k-1}x^2 - (\beta_{k-2} + \alpha_{k-1})x + \alpha_{k-2} \in \mathbb{Z}[x]$$

temos que

$$\begin{aligned}\xi + \xi' &= \frac{(\beta_{k-2} + \alpha_{k-1})}{\beta_{k-1}} \\ &= \frac{\alpha_{k-1}}{\beta_{k-1}} + \frac{\beta_{k-2}}{\beta_{k-1}}.\end{aligned}$$

Logo,

$$\frac{1}{\xi'} = \lim_{k\to\infty} \frac{\beta_{k-1}}{\beta_{k-2}}.$$

Pela Observação 1.1,

$$\frac{\beta_{k-1}}{\beta_{k-2}} = (a_{k-1}, a_{k-2}, \ldots, a_1, a_0), \forall k > 1.$$

Assim,

$$\frac{1}{\xi'} = (\overline{a_{k-1}, a_{k-2}, \ldots, a_1, a_0}).$$

■

Teorema 1.2 *Seja $\xi \in \mathbb{R}$ uma irracionalidade quadrática. Então ξ tem uma expansão em fração contínua menos puramente periódica se, e somente se, $\xi > 1$ e $0 < \xi' < 1$, onde ξ' denota o conjugado de ξ.*

Prova. Suponhamos que $\xi > 1$ e $0 < \xi' < 1$. Então, fazendo $\xi_0 = \xi$, obtemos, pela equação (1.1), que

$$\frac{1}{\xi'_{i+1}} = a_i - \xi'_i.$$

Como $\xi_0 > 1$ temos que $a_i \geq 2$, para todo $i \in \mathbb{Z}_+$. Segue, indutivamente, que

$$0 < \xi'_i < 1, \forall i \in \mathbb{Z}_+,$$

pois

$$0 < \xi'_0 < 1, a_0 = 2 \Rightarrow a_0 - \xi'_0 > 1 \text{ e } \frac{1}{\xi'_1} > 1.$$

Então

$$0 < a_i - \frac{1}{\xi'_{i+1\,i}} < 1 \text{ e } a_i = \left\lfloor \frac{1}{\xi'_{i+1}} \right\rfloor + 1,$$

pois

$$\xi'_i = a_i - \frac{1}{\xi'_{i+1}}.$$

Por hipótese, existem j e k, com $j < k$, tais que $\xi_j = \xi_k$. Logo, $\xi'_j = \xi'_k$ e

$$a_{j-1} = \left\lfloor \frac{1}{\xi'_j} \right\rfloor + 1 = \left\lfloor \frac{1}{\xi'_k} \right\rfloor + 1 = a_{k-1}$$

e

$$\xi_{j-1} = a_{j-1} - \frac{1}{\xi_j} = a_{k-1} - \frac{1}{\xi_k} = \xi_{k-1}.$$

Assim, $\xi_j = \xi_k$ implica que $\xi_{j-1} = \xi_{k-1}$. Portanto, depois da j-ésima iteração desta implicação, obtemos que

$$\xi_0 = \xi_{k-j} \text{ e } \xi = \xi_0 = (\overline{a_0, a_1, a_2, \ldots, a_{k-j-1}}).$$

Reciprocamente, suponhamos que ξ tenha uma expansão em fração contínua menos puramente periódica, digamos

$$\xi = (\overline{a_0, a_1, a_2, \ldots, a_{k-1}}),$$

onde $a_i \geq 2$, para todo $1 \leq i \leq k-1$. Então $\xi > a_0 \geq 1$ e pela Proposição 1.2, obtemos que

$$\begin{aligned} \xi &= (a_0, a_1, a_2, \ldots, a_{k-1}, \xi) \\ &= \frac{\xi\alpha_{k-1} - \alpha_{k-2}}{\xi\beta_{k-1} - \beta_{k-2}}. \end{aligned}$$

Assim, ξ é raiz do polinômio

$$f(x) = \beta_{k-1}x^2 - (\beta_{k-2} + \alpha_{k-1})x + \alpha_{k-2} \in \mathbb{Z}[x].$$

Como $\xi > 1$ basta provar que f tem uma raiz entre 0 e 1. Note que,

$$f(0) = \alpha_{k-2} > 0,$$

pois $a_i > 1$, para todo $i \in \mathbb{Z}_+$ e

$$\begin{aligned} f(1) &= (\beta_{k-1} - \alpha_{k-1}) - (\beta_{k-2} - \alpha_{k-2}) \\ &= \frac{1}{\beta_{k-1}}(1 - \frac{a_{k-1}}{\beta_{k-1}}) - \beta_{k-1}(\frac{\beta_{k-2}}{\beta_{k-1}} - \frac{\alpha_{k-2}}{\beta_{k-1}}) \\ &\leq -\beta_{k-1}(\frac{\beta_{k-2}}{\beta_{k-1}} - \frac{\alpha_{k-2}}{\beta_{k-1}}) < 0. \end{aligned}$$

Então, pelo Teorema do Valor Intermediário, f contém uma raiz ξ' tal que $0 < \xi' < 1$. ■

1.2 Algoritmo

Nesta seção apresentaremos um algoritmo para determinar a expansão em fração contínua de um número real ξ_0, quando ξ_0 é uma irracionalidade quadrática.

Pela equação (1.4), temos

$$\begin{aligned} q_{i+1} &= \frac{m_{i+1}^2 - d}{q_i} \\ &= \frac{(a_i q_i - m_i)^2 - d}{q_i} \\ &= \frac{m_i^2 - d}{q_i} - 2a_i m_i + a_i^2 q_i \\ &= q_{i-1} - 2a_i m_i + a_i(m_{i+1} + m_i) \\ &= q_{i-1} + a_i(m_{i+1} - m_i). \end{aligned}$$

Iniciando com

$$\xi_0 = \frac{m_0 + \sqrt{d}}{q_0} \text{ e } q_0 \mid (m_0^2 - d),$$

obtemos, para $i \geq 1$, que

$$\begin{aligned} a_0 &= \left\lfloor \frac{m_0 + \sqrt{d}}{q_0} \right\rfloor + 1, \ \ m_1 = a_0 q_0 - m_0, \ \ q_1 = \frac{m_1^2 - d}{q_0} \\ a_1 &= \left\lfloor \frac{m_1 + \sqrt{d}}{q_1} \right\rfloor + 1, \ \ m_2 = a_1 q_1 - m_1, \ \ q_2 = q_0 + a_1(m_2 - m_1) \\ &\vdots \\ a_{i-1} &= \left\lfloor \frac{m_{i-1} + \sqrt{d}}{q_{i-1}} \right\rfloor + 1, \ \ m_i = a_{i-1} q_{i-1} - m_{i-1}, \ \ q_i = q_{i-2} + a_{i-1}(m_i - m_{i-1}). \end{aligned}$$

Exemplo 1.4 *Expandir em fração contínua menos o número irracional*

$$\xi_0 = 4 + \sqrt{12}.$$

Solução. Como

$$\xi_0 = \frac{m_0 + \sqrt{d}}{q_0} \text{ e } q_0 \mid (m_0^2 - d)$$

temos que $m_0 = 4$ e $q_0 = 1$. Logo,

$$\begin{aligned} a_0 &= 8, \ \ m_1 = 4, \ \ q_1 = 4 \\ a_1 &= 2, \ \ m_2 = 4, \ \ q_2 = 1 \\ a_2 &= 8, \ \ m_3 = 4, \ \ q_3 = 4 \\ a_3 &= 2, \ \ m_4 = 4, \ \ q_4 = 1. \end{aligned}$$

Portanto,

$$4 + \sqrt{12} = (\overline{8, 2}).$$

Capítulo 2

Grupos

Neste capítulo apresentaremos alguns resultados clássicos da teoria dos grupos, bem como um pouco da teoria do grupo modular $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$, que "age" no semi-plano superior $\mathcal{H}$ pela transformação de Möbius. Estes resultados serão necessários para a compreensão desta dissertação. O leitor interessado em mais detalhes deve consultar [1, 4, 9, 14].

2.1 Grupos

Um conjunto G equipado com uma operação binária

$$\begin{aligned} * : \ & G \times G \longrightarrow G \\ & (a, b) \longmapsto a * b \end{aligned}$$

é um *grupo* se as seguintes condições são satisfeitas:

1. $a * (b * c) = (a * b) * c$, para todos $a, b, c \in G$.

2. Existe $e \in G$ tal que $e * a = a * e = a$, para todo $a \in G$.

3. Para todo $a \in G$, existe $b \in G$ tal que $a * b = b * a = e$.

O grupo é *abeliano* ou *comutativo* se também vale a condição

4. $a * b = b * a$, para todos $a, b \in G$.

Com o objetivo de simplificar a notação usaremos ab em vez $a * b$. A *ordem* ou *cardinalidade* de um grupo G é o número de elementos de G e denotaremos por $|G|$.

Exemplo 2.1 *Seja $M_2(\mathbb{R})$ o conjunto de todas as 2×2 matrizes sobre $\mathbb{R}$. Então*

$$GL(2,\mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det(A) \neq 0\}$$

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

Solução. Sejam $A, B \in GL(2,\mathbb{R})$. Então, pelo Teorema de Binet,

$$\det(AB) = \det(A)\det(B) \neq 0.$$

Logo, $AB \in GL(2,\mathbb{R})$. Assim, o produto usual de matrizes é uma operação binária em $GL(2,\mathbb{R})$. É claro que esta operação binária é associativa e

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$$

é o elemento identidade de $GL(2,\mathbb{R})$. Finalmente, se

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$$

é tal que $D = \det(A) \neq 0$, então

$$A^{-1} = \frac{1}{D}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

é a inversa de A e

$$\det(A^{-1}) = \frac{1}{\det(A)} \neq 0.$$

Assim,

$$A^{-1} \in GL(2,\mathbb{R}) \text{ e } A^{-1}A = AA^{-1} = I.$$

Exemplo 2.2 *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 $ad - bc \neq 0$. 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.

Sejam G um grupo e H um subconjunto de G. Dizemos que H é um *subgrupo* de G, em símbolos $H \leq G$, se as seguintes condições são satisfeitas:

1. $H \neq \emptyset$;

2. $ab^{-1} \in H$, para todos $a, b \in H$.

Exemplo 2.3 *Seja*

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

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

Sejam G um grupo e X um subconjunto de G. Seja $\mathcal{F}$ a família de todos os subgrupos de G contendo X, isto é,

$$\mathcal{F} = \{K \leq G : X \subseteq K\}.$$

Como $G \in \mathcal{F}$ temos que $\mathcal{F} \neq \emptyset$. Seja

$$H = \bigcap_{K \in \mathcal{F}} K.$$

É fácil verificar que H é o menor subgrupo de G que contém X, chamado o *subgrupo gerado por* X, e será denotado por $\langle X \rangle$. Se

$$X = \{g_1, \ldots, g_n\},$$

então

$$\langle X \rangle = \langle g_1, \ldots, g_n \rangle.$$

Proposição 2.1 *Sejam* G *um grupo e* X *um subconjunto não vazio de* G*. Então*

$$\langle X \rangle = \{x_1 \cdots x_n : n \in \mathbb{N} \ \ e \ \ x_i \in X \cup X^{-1}\},$$

onde

$$X^{-1} = \{x^{-1} : x \in X\}.$$

■

Seja $g \in G$. Então

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\},$$

chamado de *subgrupo cíclico* de G gerado por g. Um grupo G é chamado *cíclico* se existir $g \in G$ tal que $G = \langle g \rangle$.

Sejam G um grupo e H um subgrupo de G. Dado $a \in G$, o conjunto

$$aH = \{ah : \forall h \in H\}$$

é chamado a *classe lateral à esquerda* de H em G determinada por a. De modo semelhante, podemos definir a classe lateral à direita Ha de H em G. O conjunto de todas as classes laterais à esquerda de H em G formam uma partição de G, que denotamos por $\frac{G}{H}$.

Dados $a, b \in G$, dizemos que a *é congruente a* b *módulo* H se $a^{-1}b \in H$, que denotamos por $a \equiv b \,(\mathrm{mod}\, H)$. É fácil verificar que $\equiv$ é uma relação de equivalência em G e que a classe de equivalência determinada por a é igual a classe lateral à esquerda aH. O elemento a é chamado um *representante* da classe de equivalência. É também fácil verificar que existe uma correspondência biunívoca entre o conjunto das classes laterais à esquerda de H em G e o conjunto das classes laterais à direita de H em G. A cardinalidade do conjunto das classes laterais à esquerda (ou à direita) de H em G é chamado o *índice* de H em G, que denotamos por $(G : H)$.

Sejam G um grupo e H um subgrupo de G. Dizemos que H é um *subgrupo normal* de G, em símbolos $H \trianglelefteq G$, se

$$Ha = aH, \forall a \in G,$$

isto é,

$$aHa^{-1} = H, \forall a \in G.$$

Sejam G um grupo e H um subgrupo de G. Então $\frac{G}{H}$ é um grupo com operação $aHbH = abH$, para todos $a, b \in G$, se, e somente se, H é um subgrupo normal de G. Neste caso, $\frac{G}{H}$ é chamado o *grupo quociente* de G por H.

Sejam G e K dois grupos. Uma aplicação $\sigma : G \longrightarrow K$ é um *homomorfismo de grupos* se

$$\sigma(ab) = \sigma(a)\,\sigma(b), \forall a, b \in G.$$

Um homomorfismo de grupos $\sigma : G \longrightarrow K$ é um *isomorfismo* se σ é bijetora. Quando existir um isomorfismo entre G e K dizemos que G e K são *isomorfos* e denotaremos por $G \simeq K$.

Teorema 2.1 *Seja $\sigma : G \to G'$ um homomorfismo de grupos. Então* $\ker \sigma \trianglelefteq G$ *e*

$$\frac{G}{\ker \sigma} \simeq \operatorname{Im} \sigma \leq G'.$$

■

Sejam G um grupo e X um conjunto não vazio. Uma *ação* de G sobre X é uma função

$$\begin{aligned} * : \quad & G \times X \longrightarrow X \\ & (g, x) \longmapsto g * x \end{aligned}$$

tal que sa seguintes condições são satisfeitas:

1. $e * x = x$, $\forall x \in X$;

2. $(g_1 g_2) * x = g_1 * (g_2 * x)$, $\forall x \in X$ e $\forall g_1,\, g_2 \in G$.

Para cada $g \in G$, a função $\sigma_g : X \longrightarrow X$ definida por $\sigma_g(x) = g * x$, é uma permutação de X, isto é, σ_g é um elemento do grupo simétrico S_X. A função $\varphi : G \to S_X$ definida por $\varphi(g) = \sigma_g$ é um homomorfismo de grupo chamado de uma *representação* de G em S_X. Reciprocamente, qualquer homomorfismo $\phi : G \to S_X$ define uma ação, $gx = \phi(g)(x)$.

Exemplo 2.4 *Sejam $G = (\mathbb{Z}, +)$ e $X = \mathbb{R}$. Então a função $* : G \times X \longrightarrow X$ definida por*

$$*(n, x) = (-1)^n x$$

é uma ação de G em X.

Proposição 2.2 *Sejam $K = \{-I, I\} \leq \mathrm{SL}(2, \mathbb{R})$ e $\mathbb{G}$ o grupo das transformações de Möbius. 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

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

Então é claro que φ está bem definida e é um homomorfismo de grupos sobrejetor. Assim, pelo Teorema 2.1,

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

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

$$\mathrm{PSL}(2,\mathbb{R}) = \frac{\mathrm{SL}(2,\mathbb{R})}{\{-I, I\}} = \dot{\cup}\left\{A, -A\right\}, A \in \mathrm{SL}(2,\mathbb{R}),$$

é chamado o *grupo linear projetivo especial*. Neste caso, não faremos distinção explicita 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 $\mathbb{G}$ têm comportamento geométrico totalmente 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

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

2.2 Grupo modular

Consideremos um elemento $\infty \notin \mathbb{C}$. O conjunto

$$\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$$

será chamado de *esfera de Riemann*. Os pontos de $\mathbb{C} \subset \widehat{\mathbb{C}}$ serão denotados de pontos finitos. Diremos que $V \subset \widehat{\mathbb{C}}$ é uma *vizinhança* do ∞, se $\infty \in V$ e existe $r > 0$ tal que $\mathbb{C} - B_r[0] \subset V$.

O plano complexo $\widehat{\mathbb{C}}$ obtido de $\mathbb{C}$ pela adjunção de ∞ é também chamado plano complexo estendido. As regras de cálculo para o ∞ são as seguintes:

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

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

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

No caso em que a transformação de Möbius T se estende a $\widehat{\mathbb{C}}$, teremos:

$$\begin{array}{c} T\left(-\frac{d}{c}\right) = \infty, \text{ se } c \neq 0 \\ T(\infty) = \frac{a}{c}, \text{ se } c \neq 0 \\ T(\infty) = \infty, \text{ se } c = 0 \end{array} .$$

Teorema 2.2 *Se $T \in \mathrm{PSL}(2, \mathbb{R})$ e $T \neq Id$, então T possui um ou dois pontos fixos.*

Prova. Suponhamos que

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

onde $ad - bc = 1$. Um ponto fixo de T é uma solução da equação

$$T(z) = z.$$

Assim, há dois casos a ser considerado:

1º **Caso**. $c = 0$, neste caso $ad = 1$. Logo,

$$T(z) = a^2 z + ab = a(az+b).$$

Assim, $T(\infty) = \infty$, isto é, T fixa ∞. Os pontos fixos finitos de T são dados pela equação

$$a^2 z + ab = z.$$

Se $a \neq \pm 1$ esta equação possui apenas uma solução

$$z_0 = \frac{ab}{1-a^2}$$

e, neste caso, T possui dois pontos fixos, a saber ∞ e z_0. Por outro lado, se $a = \pm 1$, devemos ter $ab \neq 0$, pois $T \neq Id$. Neste caso, a equação $T(z) = z$ possui uma única solução, a saber $z = \infty$.

2º **Caso**. $c \neq 0$, neste caso,

$$T(\infty) = \frac{a}{c} \neq \infty.$$

Logo, se $T(z) = z$, então z é finito e, além disso,

$$\frac{az+b}{cz+d} = z \Leftrightarrow cz^2 + (d-a)z - b = 0.$$

Esta equação possui uma solução, se

$$D = (a+d)^2 - 4 = 0$$

ou duas soluções, se

$$D = (a+d)^2 - 4 \neq 0.$$

■

Duas matrizes $A, B \in \mathrm{SL}(2,\mathbb{R})$ são chamadas *equivalentes* se elas são conjugadas, isto é, se existir $P \in \mathrm{SL}(2,\mathbb{R})$ tal que $B = PAP^{-1}$. Os autovalores de

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

são as raízes do polinômio não nulo

$$\begin{aligned}\phi_A(x) &= \det(xI - A) \\ &= x^2 - (d+a)x + ad - bc,\end{aligned}$$

o qual depende unicamente da classe de equivalência de A.

Exemplo 2.5 *Sejam*

$$A = \begin{pmatrix} 15 & -8 \\ 2 & -1 \end{pmatrix} \text{ e } B = \begin{pmatrix} 13 & 6 \\ 2 & 1 \end{pmatrix}.$$

Então existe

$$P = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R})$$

tal que

$$B = PAP^{-1}.$$

Neste caso, $\lambda_1 = 7 - 4\sqrt{3}$ *e* $\lambda_2 = 7 + 4\sqrt{3}$*, são os autovalores de* A *e* B*.*

Teorema 2.3 *As classes de equivalência de matrizes de* $\mathrm{SL}(2, \mathbb{R})$ *com autovalores distintos* λ_1 *e* λ_2 *contêm exatamente duas matrizes diagonais, a saber:*

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \text{ e } \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$$

e são caracterizadas pelo par (λ_1, λ_2)*.*

Prova. Suponhamos que

$$\mathbf{v}_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \text{ e } \mathbf{v}_2 = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

são autovetores associados aos autovalores λ_1 e λ_2, respectivamente. É claro que $\mathbf{v}_1$ e $\mathbf{v}_2$ são linearmente independentes e

$$A\mathbf{v}_j = \lambda_j \mathbf{v}_j, j = 1, 2.$$

Assim, a matriz

$$P = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$$

transforma A em

$$PAP^{-1} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

e a caracterização fica clara. ■

Uma *transformação modular* é uma transformação de $\mathrm{PSL}(2,\mathbb{R})$ cujos elementos da matriz associada são inteiros. O conjunto de todas as transformações modulares forma um grupo,

$$\Gamma = \{T_A : A \in \mathrm{SL}(2,\mathbb{Z})\} = \mathrm{PSL}(2,\mathbb{Z}),$$

que chamaremos de *grupo modular*.

Seja

$$\Gamma\prime = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z} \text{ e } ad - bc = 1 \right\}.$$

Pela prova da Proposição 2.2

$$\frac{\Gamma\prime}{\{-I, I\}} \simeq \Gamma.$$

Se

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

então

$$\phi_A(x) = \det \begin{pmatrix} a-x & b \\ c & d-x \end{pmatrix} = x^2 - (a+d)x + 1.$$

Logo, os autovalores são

$$\lambda_{1,2} = \frac{(a+d) \pm \sqrt{(a+d)^2 - 4}}{2}.$$

Claramente $\lambda_1\lambda_2 = 1$. Consequentemente $\lambda_{1,2}$ são inteiros algébricos. Além disso, $\lambda_{1,2}$ são unidades no corpo

$$\mathbb{Q}(\sqrt{(a+d)^2 - 4}).$$

Como $\lambda_1\lambda_2 = 1$ temos que

$$\lambda_1 = \lambda_2 = \begin{cases} 1 & \text{se } a+d=2 \\ -1 & \text{se } a+d=-2 \end{cases}.$$

Assim, $\lambda_{1,2} \notin \mathbb{Q}$ se $|a+d| \neq 2$. Como resultado temos a seguinte classificação:

Uma matriz A em Γ é *parabólica* se

$$|a+d| = 2$$

e, consequentemente, $\lambda_0 = 1$ ou $\lambda_0 = -1$ é o único autovalor de A.

Uma matriz A em Γ é *elíptica* se

$$|a+d| = 0 \text{ ou } |a+d| = 1.$$

e, consequentemente,

$$\lambda_{1,2} = \pm i \in \mathbb{Q}(i) \text{ ou } \lambda_{1,2} = \frac{1 \pm \sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3}).$$

Neste caso o multiplicador

$$\lambda = \frac{\lambda_2}{\lambda_1} = \begin{cases} -1 \text{ se } a+d=0 \\ \frac{-1-\sqrt{-3}}{2} \text{ se } |a+d|=1 \end{cases}$$

Finalmente, o caso que trataremos em nossa dissertação.

Uma matriz A em Γ é *hiperbólica* se

$$|a+d| > 2$$

e, consequentemente,

$$\lambda_{1,2} = \frac{(a+d) \pm \sqrt{(a+d)^2 - 4}}{2}$$

pertencem ao corpo quadrático real

$$\mathbb{Q}(\sqrt{(a+d)^2-4}),$$

pois $(a+d)^2 - 4 > 0$. Neste caso o multiplicador

$$\lambda = \frac{\lambda_2}{\lambda_1} = \lambda_2^2.$$

Teorema 2.4 *O grupo modular Γ é gerado pelos elementos*

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

Prova. Seja

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

Então

$$S \circ g(z) = \frac{-cz-d}{az+b} \text{ e } T^k \circ g(z) = \frac{(a+kc)z+b+kd}{cz+d}, \forall k \in \mathbb{Z}.$$

Mostraremos que g pode ser representada como composição de um número finito de transformações T, T^{-1} e S. Como $ad-bc=1$, os inteiros a e c são relativamente primos ou um deles é igual a 0. Se $a=0$, então $b=-1$ e $c=1$ ou vice-versa. No primeiro caso ficamos com

$$T^{-d}S \circ g = I$$

e, portanto, $g = S \circ T^d$; no segundo caso $g = S \circ T^{-d}$. Analogamente, se

$$c = 0, g(z) = z+b \text{ ou } g(z) = z-b,$$

isto é, $g = T^b$ ou $g = T^{-b}$.

Suponhamos que $a \neq 0$ e $c \neq 0$. O algoritmo de fatoração da matriz correspondente a g é essencialmente o algoritmo Euclidiano para achar o mdc $\{|a|, |c|\}$, que neste caso é igual 1. Podemos assumir que $c > 0$. Se $|a| \geq c$, escreveremos

$$|a| = qc + r, \text{ onde } 0 \leq r < c$$

Se $a > 0$, então aplicamos T^{-q} a g para obtermos

$$T^{-q} \circ g(z) = \frac{rz+b'}{cz+d},$$

e aplicando S, obtemos que

$$S \circ T^{-q} \circ g(z) = \frac{-cz-d}{rz+b'}$$

Se $a < 0$, então aplicando $S \circ T^q$ a g, obtemos que

$$S \circ T^q \circ g(z) = \frac{-cz-d}{rz-b''}.$$

Em ambos os casos, depois do primeiro passo, obtemos

$$\frac{a_1 z+b_1}{c_1 z+d_1} \text{ com } |a_1| \geq |c_1| \text{ e } |a_1| < |a|.$$

Em um número finito de passos, encontraremos

$$\frac{a_n z+b_n}{c_n z+d_n} \text{ com } a_n = \pm 1 \text{ e } c_n = 0$$

que já foi considerado anteriormente. Por fim, se $|a| < |c|$, aplicamos a transformação S e o problema se reduz ao caso já considerado. ■

Exemplo 2.6 *Seja*

$$g(z) = \frac{15z - 8}{2z - 1} \in \mathrm{PSL}(2, \mathbb{Z}).$$

Então

$$g = T^7 \circ S \circ T^{-2} \circ S \circ T^{-1}.$$

Além disso,

$$h(z) = T^{-1} \circ g \circ T(z) = \frac{13z + 6}{2z + 1},$$

ou ainda,

$$h = T^6 \circ S \circ T^{-2} \circ S.$$

Portanto, g e h são conjugadas em $\mathrm{PSL}(2, \mathbb{Z})$.

Capítulo 3

Geometria Hiperbólica

Neste capítulo apresentaremos algumas definições e resultados clássicos sobre geometria hiperbólica. O leitor interessado em mais detalhes pode consultar [14].

3.1 Plano hiperbólico

O *semiplano superior*

$$\mathcal{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\} \subset \mathbb{C}$$

equipado com a métrica

$$ds = \frac{\sqrt{dx^2 + dy^2}}{y} \tag{3.1}$$

é chamado de *plano hiperbólico*. A métrica dada pela Equação (3.1) é chamada *métrica hiperbólica*.

O *espaço tangente* a $\mathcal{H}$ em um ponto z de $\mathcal{H}$ é definido como o espaço de vetores tangentes a z, ou seja,

$$T_z\mathcal{H} = \{\gamma'(0) : \gamma(0) = z\},$$

onde

$$\gamma : [0, 1] \longrightarrow \mathcal{H}$$

é um caminho diferenciavel por partes em $\mathcal{H}$.

A métrica dada pela Equação (3.1) é induzida pelo seguinte produto interno em $T_z\mathcal{H}$: para $\zeta_1 = \xi_1 + i\eta_1$ e $\zeta_2 = \xi_2 + i\eta_2$,

$$\langle \zeta_1, \zeta_2 \rangle = \frac{\xi_1\xi_2 + \eta_1\eta_2}{\operatorname{Im}(z)^2}.$$

Além disso, a norma $\|\cdot\|$ em $T_z\mathcal{H}$ corresponde ao produto interno $\langle\cdot,\cdot\rangle$. O *ângulo* entre ζ_1 e ζ_2 é definido como

$$\cos\theta = \frac{\langle\zeta_1,\zeta_2\rangle}{\|\zeta_1\|\,\|\zeta_2\|}.$$

Seja $\gamma : [0,1] \longrightarrow \mathcal{H}$ um caminho diferenciável por partes,

$$\gamma(t) = \{z(t) = x(t) + iy(t) \in \mathcal{H} : t \in [0,1]\}.$$

O *comprimento da curva* γ é dado por

$$h(\gamma) = \int_0^1 \frac{\sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}}{y(t)} dt. \tag{3.2}$$

Definimos ainda a *distância hiperbólica* entre os pontos z e w de $\mathcal{H}$ como

$$\rho(z,w) = \inf h(\gamma), \tag{3.3}$$

onde o ínfimo é tomado sobre todas as curvas diferenciáveis por partes conectando z e w.

Proposição 3.1 *Toda transformação de Möbius T_A aplica $\mathcal{H}$ em $\mathcal{H}$, onde*

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

Prova. Como

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

temos que

$$\mathrm{Im}\, w = \frac{w-\overline{w}}{2i} = \frac{(ad-bc)(z-\overline{z})}{2i|cz+d|^2} = \frac{\mathrm{Im}\, z}{|cz+d|^2}. \tag{3.4}$$

Portanto, $\mathrm{Im}\, z > 0$ implica que $\mathrm{Im}\, w > 0$. ■

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

$$\rho(\gamma(s),\gamma(t)) = \int_s^t \frac{\sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}}{y(t)} dt, \forall s,t \in [0,1], \tag{3.5}$$

ou seja, se γ minimizar a distância entre os pontos do seu traçado. Além disso, a geodésica é chamada *fechada* se $\gamma(0) = \gamma(1)$.

Uma transformação g de $\mathcal{H}$ sobre $\mathcal{H}$ é chamada uma *isometria* se ela preserva a distância hiperbólica em $\mathcal{H}$, isto é,

$$\rho\left(g(z), g(w)\right) = \rho\left(z, w\right), \forall z, w \in \mathcal{H}.$$

Denotaremos por $\mathrm{Isom}(\mathcal{H})$ o grupo das isometrias de $\mathcal{H}$.

Teorema 3.1 *As transformações de Möbius são isometrias.*

Prova. Seja $T \in \mathrm{PSL}(2, \mathbb{R})$. Então, pela Proposição 3.1, T aplica $\mathcal{H}$ sobre $\mathcal{H}$. Seja $\gamma : I \longrightarrow \mathcal{H}$ uma curva diferenciável por partes dada por

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

Se

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

então

$$w(t) = T(z(t)) = u(t) + iv(t)$$

ao longo da curva γ. Logo,

$$\begin{aligned} \frac{dw}{dz} &= \frac{a(cz + d) - c(az + b)}{(cz + d)^2} \\ &= \frac{1}{(cz + d)^2}. \end{aligned}$$

Pela Equação (3.4), obtemos que

$$v = \frac{y}{|cz + d|^2}.$$

Logo,

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

Assim,

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

Portanto,

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

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

Proposição 3.2 *Seja C um semicírculo ou uma semi-reta ortogonal ao eixo real que toca o eixo real no ponto x_0. Então*

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

aplica C no eixo imaginário positivo, para um valor adequado de w_0. ■

Teorema 3.2 *As geodésicas em $\mathcal{H}$ são semicírculos ou semi-retas ortogonais ao eixo $\mathbb{R}$.*

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

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

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

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

então

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

Assim, este é exatamente o comprimento hiperbólico do segmento do eixo imaginário que une ia e ib, consequentemente, a geodésica que une ia e 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 semi-reta que une z_1 a z_2. Assim, existe, pela Proposição 3.2, 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, pelo Teorema 3.1, concluímos que a geodésica entre z_1 e z_2 é o segmento de L que une z_1 a z_2. ■

Corolário 3.1 *Quaisquer dois pontos $z, w \in \mathcal{H}$ 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 $[z, w]$.* ■

Teorema 3.3 *Toda isometria de $\mathcal{H}$, 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 $\mathcal{H}$ e $\varepsilon \in [z,t]$. Então, pelo Teorema 3.1 e o Corolário 3.1, 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 no Teorema 3.1 que as transformações de $\mathrm{PSL}(2,\mathbb{R})$ são isometrias do plano hiperbólico $\mathcal{H}$.

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 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.

Se

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

for hiperbólica, a transformação T_A terá dois pontos fixos, que são obtidos resolvendo

$$z = \frac{az+b}{cz+d}, \text{ ou seja } cz^2 + (d-a)z - b = 0.$$

Assim, obtemos que

$$w_1 = \frac{(a-d) + \sqrt{(a+d)^2 - 4}}{2c} \text{ ou } w_2 = \frac{(a-d) - \sqrt{(a+d)^2 - 4}}{2c}.$$

O ponto fixo w_i de T pode ser expresso em termos do autovetor

$$\mathbf{v}_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix}$$

associado ao autovalor λ_i, ou seja,

$$w_i = \frac{x_i}{y_i}.$$

Em termos do autovalor λ_i a derivada do ponto fixo w_i pode ser escrita como

$$T'(w_i) = \frac{1}{(cw_i + d)^2} = \frac{1}{\lambda_i^2}.$$

Sejam w e u pontos fixos de uma transformação

$$T : \mathcal{H} \longrightarrow \mathcal{H}.$$

Dizemos que w é *atrator* se

$$T'(w) < 1,$$

e u é *repulsor* se

$$T'(u) > 1.$$

Uma geodésica em $\mathcal{H}$ unindo os dois pontos fixos w e u de uma transformação hiperbólica T é chamada *eixo* de T e será denotada por $C(T)$. Neste caso, $C(T)$ é a semicircunferência de centro

$$(\frac{a-d}{2c}, 0)$$

e raio

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

ou seja,

$$\left| z - \frac{a-d}{2c} \right| = r \Leftrightarrow c(x^2 + y^2) + (d-a)x - b = 0.$$

Seja T uma transformação de Möbius. A *diferencial* de T, denotada por DT, em um ponto z é uma transformação linear que leva o espaço tangente $T_z\mathcal{H}$ sobre $T_{T(z)}\mathcal{H}$ e é por definição a matriz

$$DT = \begin{pmatrix} \frac{\partial u}{\partial x} & \frac{\partial u}{\partial y} \\ \frac{\partial v}{\partial x} & \frac{\partial v}{\partial y} \end{pmatrix}.$$

Teorema 3.4 *Seja $T \in \mathrm{PSL}(2, \mathbb{R})$. Então DT preserva norma em cada ponto no espaço tangente.*

Prova. Para $\zeta \in T_z\mathcal{H}$, temos $DT(\zeta) = T'(z)\zeta$. Como

$$|T'(z)| = \frac{\mathrm{Im}(T(z))}{\mathrm{Im}(z)} = \frac{1}{|cz + d|^2},$$

escrevemos

$$\|DT(\zeta)\| = \frac{|DT(\zeta)|}{\mathrm{Im}(T(z))} = \frac{|T'(z)|\,|\zeta|}{\mathrm{Im}(T(z))} = \frac{|\zeta|}{\mathrm{Im}(z)} = \|\zeta\|\,.$$

■

Corolário 3.2 *Toda transformação em* $\mathrm{PSL}(2,\mathbb{R})$ *preserva ângulo.*

Prova. É fácil verificar que,

$$\langle \zeta_1, \zeta_2 \rangle = \frac{1}{2}(\|\zeta_1\|^2 + \|\zeta_2\|^2 - \|\zeta_1 - \zeta_2\|^2), \forall \zeta_1, \zeta_2 \in T_z\mathcal{H}.$$

Logo,

$$\begin{aligned} \cos\theta &= \frac{\langle \zeta_1, \zeta_2 \rangle}{\|\zeta_1\|\,\|\zeta_2\|} \\ &= \frac{\langle DT(\zeta_1), DT(\zeta_2) \rangle}{\|DT(\zeta_1)\|\,\|DT(\zeta_2)\|}, \forall T \in \mathrm{PSL}(2,\mathbb{R}), \end{aligned}$$

pois T preserva orientação. ■

3.2 Região fundamental

Seja Ω um subgrupo de $\mathrm{Isom}(\mathcal{H})$. Um subconjunto F de $\mathcal{H}$ é uma *região fundamental* para Ω se as seguintes condições são satisfeitas:

1. F é uma região fechada em $\mathcal{H}$ limitada por um número finito de geodésicas;

2. As imagens $T(F)$ cobrem todo o plano hiperbólico $\mathcal{H}$, isto é,

$$\bigcup_{T\in\Omega} T(F) = \mathcal{H};$$

3. Para $T_1 \neq T_2$, as imagens $T_1(F)$ e $T_2(F)$ não têm pontos interiores em comum, isto é,

$$\mathring{F} \cap T(\mathring{F}) = \varnothing, \forall T \in \Omega - \{I\},$$

onde $\mathring{F}$ é o interior da região fundamental F.

A família

$$\{T(F) : T \in \Omega\}$$

é chamada de *tesselação* de $\mathcal{H}$.

Note que, $\mathrm{SL}(2,\mathbb{R})$ pode ser identificado com o seguinte subconjunto de $\mathbb{R}^4$:

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

Assim, a norma em $\mathrm{SL}(2,\mathbb{R})$ é induzida de $\mathbb{R}^4$ do seguinte modo: dado

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

definimos a norma em $\mathrm{SL}(2,\mathbb{R})$ como

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

Além disso, temos a métrica

$$d(A,B) = \|A - B\|.$$

A convergência em $\mathrm{PSL}(2,\mathbb{R})$ pode ser expressada em linguagem de matrizes como segue: se

$$g_n \to g \text{ em } \mathrm{PSL}(2,\mathbb{R}),$$

então existem matrizes A_n e A representando g_n e g, respectivamente, tais que

$$\lim_{n\to\infty} \|A_n - A\| = 0.$$

Um subgrupo Ω de $\mathrm{Isom}(\mathcal{H})$ é chamado *discreto* se

$$T_n \to I,$$

então existe $n_0 \in \mathbb{N}$ tal que

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

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

Exemplo 3.1 *O grupo modular* Γ *é um subgrupo discreto de* $\mathrm{PSL}(2,\mathbb{R})$*, isto é, um grupo Fuchsiano. De fato, seja*

$$A_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \to I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Então

$$a_n \to 1, b_n \to 0, c_n \to 0 \ \ e \ \ d_n \to 1.$$

Como a_n, b_n, c_n e d_n são inteiros temos que existe $n_0 \in \mathbb{N}$ tal que

$$a_n = 1, b_n = 0, c_n = 0 \ \ e \ \ d_n = 1, \forall n \geq n_0.$$

Logo,

$$\begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \forall n \geq n_0.$$

Sejam Ω um grupo Fuchsiano e $p \in \mathcal{H}$ tal que

$$T(p) \neq p, \forall T \in \Omega - \{I\}.$$

Definimos a *região de Dirichlet* para Ω centrada em p como sendo o conjunto

$$D_p(\Omega) = \{z \in \mathcal{H} : \rho(z,p) \leq \rho(z, T(p)), \forall T \in \Omega\}, \tag{3.6}$$

ainda podemos escrever a equação (3.6) como sendo

$$D_p(\Omega) = \{z \in \mathcal{H} : \rho(z,p) \leq \rho(T(z), p), \forall T \in \Omega\},$$

pois a métrica hiperbólica é invariante sob $\mathrm{PSL}(2, \mathbb{R})$.

Para cada $T_1 \in \mathrm{PSL}(2, \mathbb{R})$ fixado,

$$D_p(T_1) = \{z \in \mathcal{H} : \rho(z,p) \leq \rho(z, T_1(p))\}$$

é o conjunto de pontos z que estão mais próximos a p do que de $T_1(p)$.

Teorema 3.5 *A região de Dirichlet $D_p(\Gamma)$, com $p = ki$ e $k > 1$, é o conjunto*

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

Prova. É fácil verificar, conforme Figura 3, que $p = ki$, com $k > 1$, não é fixado por nenhum elemento diferente da identidade de Γ. Além disso, as isometrias

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

estão em Γ e os lados geodésicos de F são bissectores dos segmentos

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

respectivamente. Logo, pelo Teorema 2.4, $D_p(\Gamma) \subseteq F$. Suponhamos, por absurdo, que $D_p(\Gamma) \neq F$. Então existem $z \in \mathring{F}$ e $g \in \Gamma$ tais que $g(z) \in \mathring{F}$. Como

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

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,

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

o que é uma contradição. O mesmo argumento com z e g substituídos por $g(z)$ e g^{-1} nos dá a desigualdade contrária,

$$\mathrm{Im}\, z < \mathrm{Im}\, g(z).$$

Portanto, $D_p(\Gamma) = F$. ■

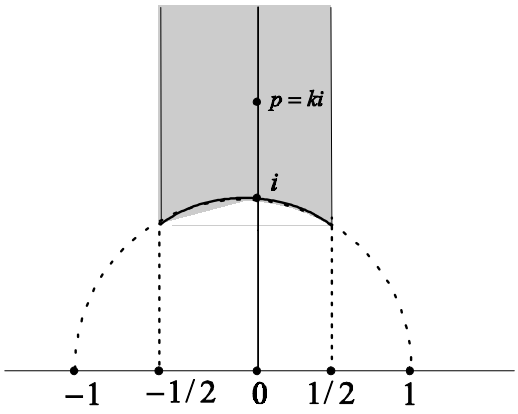

Figura 3. Região fundamental F

Capítulo 4

Códigos Geométrico e Aritmético

Neste capítulo apresentaremos uma construção de códigos geométricos e aritméticos, em especial daremos condições para que estes códigos coincidam. Salvo menção explicita em contrário, T e S representam as transformações

$$z+1 \text{ e } -\frac{1}{z},$$

respectivamente.

4.1 A superfície modular e geodésicas fechadas

Pela Proposição 3.1, a função $* : \Gamma \times \mathcal{H} \longrightarrow \mathcal{H}$ definida por

$$*((T_A, z)) = T_A(z)$$

é uma ação do grupo Γ sobre $\mathcal{H}$. Dados $z, w \in \mathcal{H}$, definimos

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

Então $\sim$ é uma relação de equivalência em $\mathcal{H}$ e

$$\mathcal{H} = \dot{\bigcup_{z \in F}} \mathcal{O}(z),$$

onde

$$\mathcal{O}(z) = \{g(z) : g \in \Gamma\}$$

é a *classe de equivalência* determinada por z ou a *órbita* de z. Para cada $z \in \mathcal{H}$ o conjunto

$$\Gamma_z = \{g \in \Gamma : g(z) = z\}$$

é um subgrupo de Γ chamado o *estabilizador* de z. Além disso, o conjunto quociente ou espaço das órbitas

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

é chamado de *superfície modular*.

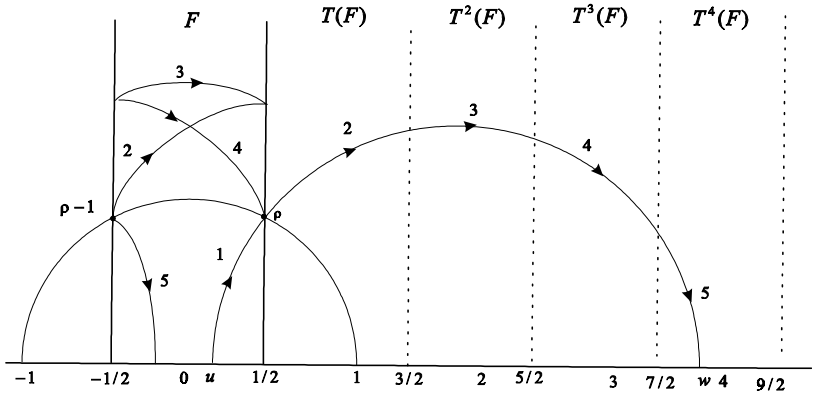

Figura 4. Codificação geométrica

Seja F uma região fundamental para Γ, com o ponto i dividindo dois lados circulares, conforme Figura 5. Sobre a projeção

$$\pi : \mathcal{H} \longrightarrow \frac{\mathcal{H}}{\Gamma}, \pi(z) = \mathcal{O}(z),$$

o lado vertical esquerdo é identificado com o lado vertical direito via a transformação

$$T(z) = z + 1$$

e o lado circular esquerdo é identificado com o lado circular direito pela transformação

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

que fixa i.

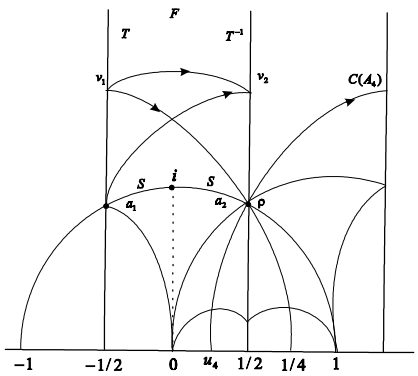

Figura 5. Confinamento da Figura 4. à região F

O *fibrado tangente* a $\mathcal{H}$ é definido por

$$T\mathcal{H} = \{(z, \zeta) : z \in \mathcal{H}, \zeta \in T_z\mathcal{H}\},$$

e o *fibrado tangente unitário* é definido por

$$S\mathcal{H} = \{(z, \zeta) : z \in \mathcal{H}, \zeta \in T_z\mathcal{H}, \|\zeta\| = 1\}.$$

Proposição 4.1 *Geodésicas fechadas sobre a superfície modular* $\frac{\mathcal{H}}{\Gamma}$ *estão em correspondência biunívoca com as classes de conjugação de elementos hiperbólicos em* Γ.

Prova. Sejam $u, w \in \mathbb{R} \cup \{\infty\}$ os pontos fixos repulsor e atrator de uma transformação hiperbólica qualquer $T \in \mathrm{PSL}(2, \mathbb{Z})$. Sejam $z \in C(T)$ e ζ um vetor tangente unitário a $C(T)$ no ponto z. Então $T(z) \in C(T)$. Assim, basta provar que $DT(\zeta)$ é o vetor tangente unitário a $C(T)$ no ponto $T(z)$. De fato, pelo Teorema 3.4,

$$\|DT(\zeta)\| = \|\zeta\| = 1.$$

Portanto, $C(T)$ é uma geodésica fechada em $\frac{\mathcal{H}}{\Gamma}$.

Reciprocamente, suponhamos que C seja uma geodésica fechada sobre $\frac{\mathcal{H}}{\Gamma}$. Vamos levantá-la para $\mathcal{H}$, e assumirmos que ela intercepta a região fundamental F caso contrário, aplicaremos uma transformação de $\mathrm{PSL}(2, \mathbb{Z})$ para movê-la. Seguindo a geodésica em sua direção de u para w ela alcançará um lado de ∂F, aplicamos uma transformação identificando este lado com sua imagem. Consequentemente, obtemos uma geodésica sobre F, que torna-se fechada depois de um número finito de passos. O que significa que existe uma seqüência de geradores de $\mathrm{PSL}(2, \mathbb{Z})$, a saber T, T^{-1} e S, tal que depois de suas aplicações sucessivas retornamos a nossa geodésica original, isto é, para $\gamma_0 \in \mathrm{PSL}(2, \mathbb{Z})$ temos que

$$\gamma_0(C) = C.$$

Segue da classificação dos elementos de $\mathrm{PSL}(2, \mathbb{Z})$ que γ_0 é hiperbólico e C é seu eixo. Se $z \in C$, então

$$\lim_{n\to\infty} \gamma_0^n(z) = u.$$

Consequentemente, se quizermos um elemento hiperbólico cujo eixo é uma geodésica orientada C, devemos tomar $\gamma = \gamma_0^{-1}$. Eixos de transformações conjugadas em $\mathrm{PSL}(2, \mathbb{Z})$ produz a mesma geodésica fechada em $\frac{\mathcal{H}}{\Gamma}$. ■

O período da seqüência de $C(\gamma)$, com respeito a uma dada região de Dirichlet, a menos de permutação cíclica, é chamado o *código de Morse* de uma geodésica fechada associada a classe de conjugação de γ.

O elemento γ, descrito anteriormente, que fixa uma geodésica orientada, é uma "palavra" nos geradores T, T^{-1} e S. Pode-se observar que a seqüência contém pelo menos um S; um S não pode ser seguido por outro S, e um T não pode ser seguido por um T^{-1} e vice-versa. Se escolhemos um ponto inicial na parte circular

$$a_1 \cup a_2$$

da fronteira ∂F, vemos que a seqüência sempre termina por um S. A cada bloco de $T's$ associamos um inteiro positivo igual ao seu comprimento e a cada bloco de $T^{-1\prime}s$ associamos um inteiro negativo cujo valor absoluto é igual ao seu comprimento. Assim, obtemos uma seqüência finita de inteiros

$$[n_1, n_2, \ldots, n_m],$$

definida, a menos de permutações cíclicas, chamada o *código geométrico* da classe de conjugação de γ, que será denotado por $[\gamma]$.

Além disso, temos que

$$\gamma = T^{n_1} S T^{n_2} S \cdots T^{n_m} S.$$

Uma outra maneira de se obter o código geométrico de uma geodésica fechada C é contar o número de vezes que C toca o lado vertical da fronteira de F, um inteiro positivo é associado ao número de toques que a geodésica dá sobre o lado vertical direito, e um inteiro negativo para cada bloco de toques dado no lado vertical esquerdo. Na Figura 6, temos a geodésica fechada em F correspondendo a classe de conjugação da matriz

$$A = \begin{pmatrix} 15 & -8 \\ 2 & -1 \end{pmatrix}$$

e o seu código geométrico é

$$[A] = [6, -2].$$

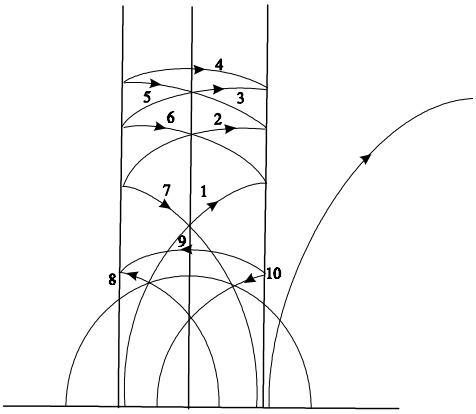

Figura 6. Segmentos geodésicos

Exemplo 4.1 *O eixo de*

$$A_4 = \begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix},$$

passando pelo vértice ρ, correspondendo à geodésica fechada

$$C(A_4) = x^2 + y^2 - 4x + 1 = 0$$

em F, são mostrados na Figura 5. *O seu código de Morse é dado por*

$$[T, T, T, T, S]$$

e o seu código geométrico é dado por

$$[4]\,.$$

A idéia de frações contínuas menos que estudamos no Capítulo 1, será utilizada agora para determinar outro código classificando geodésicas fechadas a partir de superfície modular, que resulta da teoria de redução de Gauss. Este código é uma seqüência finita de inteiros

$$(n_1, \ldots, n_m)\,, \ \text{com} \ n_i \geq 2,$$

definidos a menos de permutação cíclica, que é a expansão em frações contínuas menos do ponto fixo atrator w associado a uma transformação de $PSL(2, \mathbb{Z})$. Esse código será chamado *código aritmético* da classe de conjugação de A e será denotado por

$$(A)\,.$$

Proposição 4.2 *Duas irracionalidades quadráticas são obtidas uma da outra por aplicação de uma transformação de* $\mathrm{PSL}(2, \mathbb{Z})$ *se, e somente se, os seus períodos nas expansões em frações contínuas menos são permutações cíclicas uma da outra.*

Prova. Suponhamos que duas irracionalidades quadráticas tenham seus períodos na expansão em frações contínuas menos que sejam permutações cíclicas um do outro. Então um pode ser obtido do outro por aplicações sucessivas das transformações

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

Portanto, elas são obtidas uma da outra por aplicação de uma transformação de $\mathrm{PSL}(2, \mathbb{Z})$, pois T e S geram $\mathrm{PSL}(2, \mathbb{Z})$.

Reciprocamente, suponhamos que duas irracionalidades quadráticas sejam obtidas uma da outra por aplicação de uma transformação de $\mathrm{PSL}(2, \mathbb{Z})$. Como T e S geram $\mathrm{PSL}(2, \mathbb{Z})$, provaremos a afirmação usando apenas essas duas transformações.

Seja w uma irracionalidade quadrática, digamos

$$w = (a_0, a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m}}) .$$

Então

$$T^{\pm 1}(w) = (a_0 \pm 1, a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m}}) .$$

No caso de S, primeiro observamos que se $a_0 \geq 2$, então

$$S(w) = (0, a_0, a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m}})$$

que é uma legítima expansão em frações contínua menos. É fácil verificar que

$$S^2 = I \text{ e } (ST)^3 = I$$

ou, equivalentemente,

$$S^2 = I \text{ e } STSTST = I \tag{4.1}$$

Note que,

$$STSTST = I \Rightarrow STS = T^{-1}ST^{-1} \text{ e } ST^{-1}S = TST$$

e para $n \geq 2$

$$ST^{-n}S = TS\underbrace{T^2S \cdots T^2S}_{(n-1)-\text{vezes}}T.$$

Se $a_0 \leq -1$, então

$$S(w) = (1, \underbrace{2, \ldots, 2}_{(-a_0-1)-\text{vezes}}, a_1 + 1, a_2, \ldots, a_k, \overline{a_{k+1}, ..., a_{k+m}}).$$

Se $a_0 = 0$, então

$$S(w) = (a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m}}) .$$

Finalmente, se $a_0 = 1$ e $a_1 \geq 3$, então

$$S(w) = (-1, a_1 - 1, a_2, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m}}) .$$

Como w é irracional temos, pela Proposição 1.7, que existe pelo menos um a_i no período que é maior do que ou igual a 2. Assim, suponhamos que

$$a_s \geq 3 \text{ e } a_i = 2, 1 \leq i \leq s-1.$$

Então $S(w) = (-s, a_s - 1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m}})$. ■

Exemplo 4.2 *Sejam*

$$w_1 = 3 + \sqrt{7} \text{ e } w_2 = \frac{3 + \sqrt{7}}{2}$$

duas irracionalidades quadráticas. Então existe $g \in \mathrm{SL}(2, \mathbb{R})$ *tal que*

$$g(w_1) = w_2.$$

De fato, é fácil verificar que expansão em frações contínuas menos de w_1 *e* w_2 *são*:

$$w_1 = (\overline{6, 2}) \text{ e } w_2 = (\overline{2, 6}),$$

respectivamente. Logo,

$$S(w_1) = (0, 6, 2, 6, 2, \ldots) \Rightarrow T^2 S(w_1) = (2, 6, 2, 6, \ldots),$$

isto é, existe $g = T^2 S \in \mathrm{SL}(2, \mathbb{R})$ *tal que*

$$g(w_1) = w_2.$$

4.2 Teoria da redução para $\mathrm{SL}(2, \mathbb{Z})$

Considere um conjunto de elementos com uma relação de equivalência. De maneira geral, a teoria da redução é um algoritmo que tem por objetivo encontrar representantes canônicos em cada classe de equivalência. Tais representantes são chamados elementos "reduzidos". Cada classe de equivalência contém um conjunto canônico de elementos

reduzidos que formam um ciclo de modo natural, e seguindo o algoritmo da redução pode-se passar de um dado elemento dentro de sua classe de equivalência para um elemento reduzido por um número finito de passos. Aplicando o mesmo algoritmo para um elemento reduzido, obtemos todos os elementos reduzidos em seu ciclo.

No algoritmo da redução para grupos Fuchsianos, todos elementos que interceptam os eixos de uma dada região fundamental F são chamados *reduzidos*. O ciclo Γ-conjugado de elementos reduzidos consiste de todos elementos reduzidos com o mesmo código Morse, e a interseção de seus eixos com F cerca a geodésica fechada associada a esta classe de conjugação particular.

Proposição 4.3 *Cada matriz hiperbólica*

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

corresponde a uma forma quadrática binária inteira indefinida

$$Q_A(x, y) = cx^2 + (d - a)xy - by^2$$

e vice-versa. ■

Duas formas quadráticas binárias inteiras

$$Q_1(x, y) = A_1x^2 + B_1xy + C_1y^2 \text{ e } Q_2(x, y) = A_2x^2 + B_2xy + C_2y^2$$

são ditas *equivalentes no sentido estrito* se existir

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

tal que

$$Q_2(ax + by, cx + dy) = Q_1(x, y)$$

Exemplo 4.3 *As formas quadráticas*

$$Q_1(x, y) = 2x^2 - 12xy - 6y^2 \text{ e } Q_2(x, y) = 2x^2 - 16xy + 8y^2$$

são equivalentes no sentido estrito, pois existe

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$$

tal que

$$\begin{aligned} Q_2(x+y,y) &= 2(x+y)^2 - 16(x+y)y + 8y^2 \\ &= 2x^2 + 4xy + 2y^2 - 16xy - 16y^2 + 8y^2 \\ &= 2x^2 - 12xy - 6y^2 \\ &= Q_1(x,y). \end{aligned}$$

Proposição 4.4 *Duas matrizes hiperbólicas com o mesmo traço são conjugadas em* $\mathrm{SL}(2,\mathbb{Z})$ *se, e somente se, as formas quadráticas correspondentes* (*com o mesmo discriminante*) *são equivalentes no sentido estrito.* ■

Uma matriz hiperbólica em $\mathrm{SL}(2,\mathbb{Z})$ é chamada *reduzida* se seus pontos fixos atrator e repulsor w e u satisfazem

$$w > 1 \text{ e } 0 < u < 1. \tag{4.2}$$

Exemplo 4.4 *A matriz*

$$A = \begin{pmatrix} 15 & -8 \\ 2 & -1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

é reduzida, pois

$$w = 4 + 2\sqrt{3} \ \ e \ \ u = 4 - 2\sqrt{3}$$

satisfazem a equação (4.2).

O conjunto de matrizes reduzidas conjugadas a uma dada matriz A é chamado de $A-$*ciclo*.

Seja F uma região fundamental para $\mathrm{SL}(2,\mathbb{Z})$. Uma matriz hiperbólica $A \in \mathrm{SL}(2,\mathbb{Z})$ é chamada $F-$*reduzida* se ela é reduzida e seu eixo intercepta F. Além disso, ela é dita *totalmente* $F-$*reduzida* se todas as matrizes do A-ciclo são $F-$reduzidas.

Observação 4.1 *Sejam*

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

e

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

com $|a+d|>2$, $c\neq 0$ *e reduzida. Então* A *é* $F-$*reduzida se*

$$y(\frac{1}{2}) \geq \frac{\sqrt{3}}{2},$$

onde

$$y = y(x) = \sqrt{\frac{b+(a-d)x-cx^2}{c}}.$$

conforme figura 7.

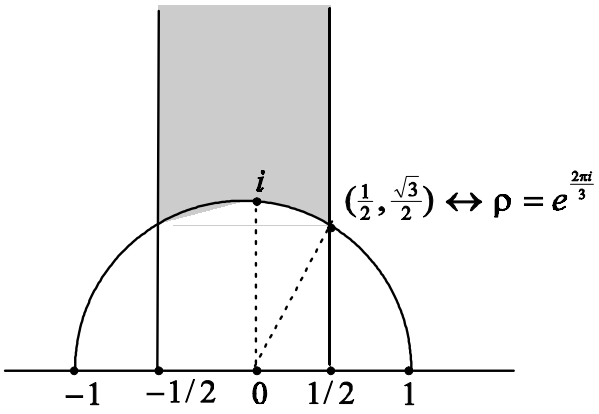

Figura 7.

Uma matriz hiperbólica $A \in \Gamma$ é chamada *primitiva* se ela não pode ser escrita como potência de uma outra matriz hiperbólica.

Exemplo 4.5 *A matriz hiperbólica*

$$A = T^4S = \begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix} \in \Gamma$$

é primitiva.

Lema 4.1 *Se* $\gamma_1, \gamma_2 \in \Gamma$ *são elementos hiperbólicos que possuem um ponto fixo em comum. Então o outro ponto fixo também coincide. Consequentemente, eles têm os mesmos eixos e ambos são potência de uma matriz primitiva com o mesmo eixo.*

Prova. Por uma conjugação canônica podemos assumir que γ_1 e γ_2 fixam ∞. Suponhamos, por absurdo, que

$$\gamma_1(z) = \lambda z \ \ (\lambda > 1) \ \text{ e } \ \gamma_2(z) = \mu z + k \ \ (\mu \neq 1, k \neq 0).$$

Assim,

$$\gamma_1^{-n}\gamma_2\gamma_1^n(z) = \mu z + \lambda^{-n}k.$$

Logo, a matriz que representa $\mu z + \lambda^{-n} k$ é

$$\begin{pmatrix} \mu & \lambda^{-n} k \\ 0 & 1 \end{pmatrix}$$

e

$$\left\| \gamma_1^{-n} \gamma_2 \gamma_1^n \right\| = \sqrt{\mu^2 + \lambda^{-2n} k^2 + 1}$$

é limitado com $n \to \infty$, consequentemente, a seqüência

$$\left\{ \gamma_1^{-n} \gamma_2 \gamma_1^n \right\}_{n \in \mathbb{N}}$$

contém uma subseqüência convergente de termos distintos, o que é uma contradição, pois Γ é discreto. Assim, $k = 0$ e, portanto, γ_1 e γ_2 fixam o zero. ■

Proposição 4.5 *Duas matrizes hiperbólicas A e B em $\mathrm{SL}(2, \mathbb{Z})$ com o mesmo traço, são conjugadas em $\mathrm{SL}(2, \mathbb{Z})$ se, e somente se, seus pontos fixos atratores (repulsores) têm períodos nas suas expansões em frações contínuas menos que são permutações cíclicas um do outro.*

Prova. Sejam w_A e w_B os pontos fixos atratores de A e B, respectivamente, tais que seus períodos nas suas expansões em frações contínuas menos diferem por uma permutação cíclica. Então, pela Proposição 4.2, existe $C \in \mathrm{SL}(2, \mathbb{Z})$ tal que

$$w_A = C w_B.$$

Então as matrizes CBC^{-1} e A têm o mesmo ponto fixo atrator w_A. Assim, pelo Lema 4.1,

$$CBC^{-1} = A \text{ ou } CBC^{-1} = A^{-1},$$

pois elas têm o mesmo traço. Como w_A é um ponto atrator para CBC^{-1} e A temos que $CBC^{-1} = A$.

Reciprocamente, suponhamos que duas matrizes em $\mathrm{SL}(2, \mathbb{Z})$ são conjugadas. Então seus pontos fixos atratores w_A e w_B são obtidos um do outro por aplicação de uma matriz $C \in \mathrm{SL}(2, \mathbb{Z})$. Assim, pela Proposição 4.2, o período nas suas expansões em frações contínuas menos de w_A e w_B diferem por uma permutação cíclica. ■

Exemplo 4.6 *As matrizes*

$$A = \begin{pmatrix} 15 & -8 \\ 2 & -1 \end{pmatrix}, B = \begin{pmatrix} 13 & 6 \\ 2 & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$$

são conjugadas, pois os pontos fixos atratores

$$w_A = 4 + 2\sqrt{3} \ \ e \ \ w_B = 3 + 2\sqrt{3}$$

têm expansão em frações contínuas menos

$$w_A = (\overline{8, 2}) \ \ e \ \ w_B = (7, \overline{2, 8}).$$

O lema seguinte nos dá uma descrição de matrizes reduzidas em termos de suas entradas.

Lema 4.2 *Seja*

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

com $a + d > 2$. Então A é reduzida se, e somente se,

$$c > 0, \ \ a + b - c - d > 0 \ \ e \ \ b < 0.$$

Além disso, se A é reduzida, então

1. $a > 0$, $c + d > 0$ *e* $d \leq 0$;
2. $\frac{a+b}{c+d} < w < \frac{a}{c}$.

Prova. Suponhamos que A seja reduzida, ou seja,

$$w > 1 \ \text{ e } \ 0 < u < 1.$$

Como $a + d > 2$ temos que os pontos fixos atrator e repulsor w e u são dados por

$$w = \frac{(a - d) + \sqrt{D}}{2c} \ \text{ e } \ u = \frac{(a - d) - \sqrt{D}}{2c},$$

onde $D = (a + d)^2 - 4$. Assim,

$$\frac{a - d + \sqrt{D}}{2c} > 1 \Rightarrow \frac{a - d - 2c + \sqrt{D}}{2c} > 0.$$

Logo,

$$a - d - 2c + \sqrt{D} > 0 \ \text{ e } \ c > 0$$

ou

$$a - d - 2c + \sqrt{D} < 0 \ \text{ e } \ c < 0.$$

Por outro lado,

$$\frac{a-d-\sqrt{D}}{2c} < 1 \Rightarrow \frac{a-d-2c-\sqrt{D}}{2c} < 0.$$

Logo,

$$a-d-2c-\sqrt{D} > 0 \text{ e } c < 0$$

ou

$$a-d-2c-\sqrt{D} < 0 \text{ e } c > 0.$$

Portanto, analizando estas inequações, obtemos que

$$c > 0 \text{ e } |a-d-2c| < \sqrt{D}$$

Além disso,

$$|a-d-2c| < \sqrt{D} \Leftrightarrow (a-d-2c)^2 < (a+d)^2 - 4$$

e, depois de alguns cálculos e usando $ad-bc=1$, chegamos a

$$a+b-c-d > 0.$$

Finalmente, como

$$\frac{a-d-\sqrt{D}}{2c} > 0$$

temos que $bc < 0$. Logo, $b < 0$, pois $c > 0$.

Reciprocamente, as duas primeiras condições implicam que

$$|a-d-2c| < \sqrt{D}$$

e, portanto, $w > 1$ e $u < 1$. A primeira e a terceira condição implicam que

$$|a-d| < \sqrt{D}.$$

Logo, $u > 0$, pois

$$a-d > c-b > 0.$$

Portanto, A é reduzida. Agora vamos provar a segunda parte do lema, como

$$a-d > \sqrt{D} \text{ e } \frac{a}{c} > w > 1$$

temos que $a > 0$. Assim,

$$\begin{aligned} Q_A\left(\frac{a+b}{c+d}, 1\right) &= c\left(\frac{a+b}{c+d}\right)^2 + (d-a)\left(\frac{a+b}{c+d}\right)^2 - b \\ &= \frac{-a-b+c+d}{(c+d)^2} < 0 \end{aligned}$$

e, pela equação (4.2),

$$\frac{a+b}{c+d} < w.$$

Além disso,

$$\frac{1}{c+d} = \frac{a}{c} - \frac{a+b}{c+d} > 0 \Rightarrow c+d > 0.$$

Finalmente,

$$bc \leq -1 \text{ e } ad = 1 + bc \leq 0 \Rightarrow d \leq 0.$$

■

Corolário 4.1 *Seja A uma matriz reduzida. Então $A(x)$ é uma função crescente sobre $\mathbb{R} \cup \{\infty\}$, para $x > 1$. Para qualquer número $x > 1$ a seqüência $\{A^n(x)\}$ (convergindo para w) é decrescente se $x > w$ e é crescente se $1 < x < w$.*

Prova. Seja

$$\begin{aligned} A(x) &= \frac{ax+b}{cx+d} \\ &= \frac{a}{c} - \frac{\frac{1}{c^2}}{x + \frac{d}{c}}. \end{aligned}$$

Se

$$x > -\frac{d}{c} \geq 0,$$

então $A(x)$ é uma função crescente com concavidade voltada para baixo e tem uma assíntota horizontal

$$y = \frac{a}{c}.$$

Pelo item 1. do Lema 4.2, obtemos que

$$-\frac{d}{c} < 1.$$

Note que,

$$x > w \Leftrightarrow -\frac{cx^2 + (d-a)x - b}{cx+d} < 0 \Leftrightarrow A(x) < x$$

e

$$1 < x < w \Leftrightarrow -\frac{cx^2 + (d-a)x - b}{cx+d} > 0 \Leftrightarrow A(x) > x.$$

Portanto, a seqüência $\{A^n(x)\}$ é decrescente se $x > w$ e é crescente se $1 < x < w$. ■

Proposição 4.6 (Algoritmo da redução) *Existe um número finito de matrizes reduzidas em* $\mathrm{SL}(2,\mathbb{Z})$ *com um dado traço* t *e* $|t|>2$. *Toda matriz hiperbólica com traço* t *pode ser reduzida por um número finito de conjugações padrão. Aplicada a uma matriz reduzida esta conjugação dá uma outra matriz reduzida. Toda matriz reduzida conjugada a* A *é obtida de* A *por um número finito de conjugações padrão. Deste modo, o conjunto de matrizes reduzidas é decomposto em ciclos disjuntos de matrizes conjugadas.*

Prova. Suponhamos que

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

seja reduzida. Seja $k=a-d-2c$. Então, pelo Lema 4.2, temos que

$$|k|<\sqrt{D}$$

e, conseqüentemente, k pode assumir apenas um número finito de valores para um dado

$$D=t^2-4.$$

Assim,

$$D-k^2=4c(a+b-c-d)>0.$$

Logo,

$$c \mid \left(\frac{D-k^2}{4}\right)$$

e, também, pode assumir apenas um número finito de valores. Agora, vamos escrever a, b e d em termos de c e k do seguinte modo:

$$\begin{aligned} a &= \frac{t+k+2c}{2} \\ b &= \frac{D-k^2}{4c}-(k+c) \\ d &= \frac{t-k-2c}{2} \end{aligned}$$

e, portanto, obtemos um número finito de matrizes reduzidas com um dado traço t.

Seja A uma matriz hiperbólica em $\mathrm{SL}(2,\mathbb{Z})$ tal que seu ponto fixo atrator tenha expansão em frações contínuas menos

$$\left(a_0,a_1,\ldots,a_k,\overline{a_{k+1},\ldots,a_{k+m}}\right).$$

Conjugando A por $S^{-1}T^{-a_0}$, obtemos uma matriz

$$A_0 = S^{-1}T^{-a_0}AT^{a_0}S,$$

e, indutivamente,

$$A_i = S^{-1}T^{-a_i}A_{i-1}T^{a_i}S, i = 1, 2, \ldots$$

O ponto atrator w da matriz

$$A_k = (S^{-1}T^{-a_k}S^{-1}\cdots T^{a_1}S^{-1}T^{-a_0})A(S^{-1}T^{-a_k}S^{-1}\cdots T^{a_1}S^{-1}T^{-a_0})^{-1}$$

tem uma expansão em frações contínuas menos puramente periódica

$$w = (\overline{a_{k+1}, \ldots, a_{k+m}})$$

Logo, pelo Teorema 1.2,

$$w > 1 \text{ e } 0 < u < 1,$$

isto é, A_k é reduzida. Aplicando o mesmo procedimento a A_k, obtemos m matrizes reduzidas em uma seqüência correspondente ao período de w.

Finalmente, se duas matrizes reduzidas são conjugadas, então seus pontos fixos atratores têm seus períodos nas suas expansões em frações contínuas menos que diferem por uma permutação cíclica. Portanto, elas pertencem ao mesmo ciclo e são obtidas uma da outra por um número finito de conjugações padrão. ■

Lema 4.3 *Sejam $n \geq 2$ um inteiro,*

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

e w um número real satisfazendo as seguintes condições:

1. $c > 0$ *e* $c + d > 0$;
2. $n - 1 < w < n$;
3. $\frac{a+b}{c+d} < w < \frac{a}{c}$.

Então

$$n - 1 < \frac{a}{c} \leq n.$$

Prova. Pelos itens 2. e 3., obtemos que

$$n - 1 < w < \frac{a}{c}.$$

Logo,

$$n - 1 < \frac{a}{c}.$$

Agora, vamos provar que

$$\frac{a}{c} \leq n.$$

Suponhamos, por absurdo, que

$$n < \frac{a}{c}.$$

Então, pelos itens 2. e 3., obtemos que

$$\frac{a+b}{c+d} < n < \frac{a}{c},$$

ou seja,

$$ac + bc < nc(c+d) < ac + ad.$$

Como

$$ad - bc = 1$$

temos que

$$0 < nc(c+d) - (ac+bc) < 1,$$

o que é uma contradição, pois

$$nc(c+d) - (ac+bc) \in \mathbb{Z}.$$

Portanto,

$$\frac{a}{c} \leq n.$$

■

Lema 4.4 *Sejam*

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

uma matriz hiperbólica com $c > 0$ *e*

$$A^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}, \forall n \in \mathbb{Z}.$$

Então

$$c_n > c \ \ ou \ \ c_n < 0, \forall n \in \mathbb{Z}^*.$$

Prova. Como todas as transformações em

$$\{A^n : n \in \mathbb{Z}\},$$

exceto a identidade, têm os mesmos eixos, temos que o polinômio quadrático correspondente Q_{A^n} deve ser múltiplo de Q_A. Logo,

$$c_n = c\lambda_n,\ b_n = b\lambda_n \text{ e } a_n - d_n = (a-d)\lambda_n,$$

para algum λ_n. Sejam $t = \operatorname{tr} A$ e $t_n = \operatorname{tr} A_n$. Então comparando o discriminante de Q_{A^n} e Q_A, obtemos que

$$\lambda_n^2 = \frac{t_n^2 - 4}{t^2 - 4}.$$

Sejam

$$\mu > 1 \text{ e } \frac{1}{\mu} < 1$$

os autovalores de A. Então

$$t = \mu + \frac{1}{\mu} \text{ e } t_n = \mu^n + \frac{1}{\mu^n}.$$

Como

$$\begin{aligned} t_n - t &= \mu^n + \frac{1}{\mu^n} - \mu - \frac{1}{\mu} \\ &= \mu^n + \mu^{-n} - \mu - \mu^{-1} \\ &= \mu^{-n}(\mu^{n-1} - 1)(\mu^{n+1} - 1) > 0 \end{aligned}$$

temos que $|\lambda_n| > 1$. Portanto,

$$c_n > c \text{ ou } c_n < 0, \forall n \in \mathbb{Z}^*.$$

■

Proposição 4.7 *Sejam $n_i \geq 2$, $i = 1, \ldots, m$, inteiros,*

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

uma matriz hiperbólica primitiva com traço positivo e ponto fixo atrator

$$w = (\overline{n_1, \ldots, n_m}).$$

Então ela pode ser representada na forma

$$A = T^{n_1} S T^{n_2} S \cdots T^{n_m} S,$$

onde

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \ e \ S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Prova. Sejam

$$A_0 = A, w_0 = w, A_s = S^{-1}T^{-n_s} \cdots S^{-1}T^{-n_1} A = \begin{pmatrix} a_s & b_s \\ c_s & d_s \end{pmatrix}$$

e

$$w_s = S^{-1}T^{-n_s} \cdots S^{-1}T^{-n_1} w_0 = (\overline{n_{s+1}, \ldots, n_m, n_1, \ldots, n_s}). \tag{4.3}$$

Como

$$\begin{aligned} A_s A A_s^{-1} &= \left(S^{-1}T^{-n_s} \cdots S^{-1}T^{-n_1} A\right) A \left(S^{-1}T^{-n_s} \cdots S^{-1}T^{-n_1} A\right)^{-1} \\ &= \left(S^{-1}T^{-n_s} \cdots S^{-1}T^{-n_1} A\right) A (T^{n_1} S \cdots T^{n_s} S) \end{aligned}$$

temos que w_s é o ponto fixo atrator de $A_s A A_s^{-1}$, após alguns cálculos chegamos que

$$A_s A A_s^{-1}(w_s) = w_s.$$

Além disso, w_s tem uma expansão em frações contínuas menos puramente periódica. Desde que m é o menor período de w_0 temos que

$$w_s \neq w_0,$$

para todo s, $s < m$. Assim, $A_s \neq I$, para todo s, $s < m$. Portanto,

$$c_s \neq 0, 0 \leq s < m,$$

pois se $c_s = 0$, então $a_s d_s = 1$. Logo,

$$A_s(z) = z + b_s.$$

Assim, o segundo ponto fixo de A_s é

$$w_s' = w_0' + b.$$

Por hipótese,

$$0 < w'_s < 1$$

implica que $b = 0$, o que é impossível.

Agora vamos usar indução sobre s para provar que A_s, w_s e n_{s+1} satisfazem as condições 1., 2. e 3. do Lema 4.3, para $0 \leq s < m$ e $A_m = I$. Se $s = 0$, então

$$n_1 - 1 < w_0 < n_1.$$

Logo, temos a condição 2. e pelo Lema 4.2 as condições 1. e 3. Suponhamos que o resultado seja válido para

$$0 < s - 1 < m,$$

isto é,

$$c_{s-1} > 0, c_{s-1} + d_{s-1} > 0, n_s - 1 < w_{s-1} < n_s \text{ ou } \frac{a_{s-1} + b_{s-1}}{c_{s-1} + d_{s-1}} < w_{s-1} < \frac{a_{s-1}}{c_{s-1}}.$$

Então, pelo Lema 4.3, obtemos que

$$n_s - 1 < \frac{a_{s-1}}{c_{s-1}} \leq n_s$$

e, portanto,

$$c_s = n_s c_{s-1} - a_{s-1} > 0 \text{ ou } c_s < c_{s-1}. \tag{4.4}$$

Além disso,

$$c_s + d_s = n_s(c_{s-1} - d_{s-1}) - (a_{s-1} + b_{s-1}) > 0.$$

Logo, A_s satisfaz a condição 1. Pela equação (4.3), A_s satisfaz a condição 2.

$$n_{s+1} - 1 < w_s < n_{s+1}$$

e

$$\frac{a_s}{c_s} = S^{-1}T^{-n_s}\left(\frac{a_{s-1}}{c_{s-1}}\right) \text{ ou } \frac{a_s + b_s}{c_s + d_s} = S^{-1}T^{-n_s}\left(\frac{a_{s-1} + b_{s-1}}{c_{s-1} + d_{s-1}}\right).$$

Assim, pelo Corolário 4.1 para $S^{-1}T^{-n_s}$, obtemos que

$$\frac{a_s + b_s}{c_s + d_s} < w_s < \frac{a_s}{c_s},$$

ou seja, A_s satisfaz a condição 3..

Pela equação (4.4) os c_s decresce com s até zero. Finalmente, vamos provar que $c_m = 0$. Suponhamos, por absurdo, que $c_m > 0$. Então, pela equação (4.4), obtemos que

$$c_m < c_{m-1} < c.$$

Por outro lado, como

$$A_m(w_0) = w_0$$

temos, pelo Lema 4.1, que

$$A_m = A^n,$$

para algum $n \in \mathbb{Z}$. Assim, pelo Lema 4.4, obtemos

$$c_m > c \text{ ou } c_m < 0,$$

o que é uma contradição. Portanto, $A_m = I$. ■

Corolário 4.2 *Sejam $n_i \geq 2$, $i = 1, \ldots, m$, inteiros e*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Então a matriz

$$A = A_{n_1} \cdots A_{n_m}, \text{ onde } A_{n_i} = T^{n_i} S$$

é hiperbólica com traço positivo, reduzida e

$$(A) = (n_1, \ldots, n_m).$$

Prova. Se $m = 1$, então

$$T^{n_1} S = \begin{pmatrix} n_1 & -1 \\ 1 & 0 \end{pmatrix}$$

e $\operatorname{tr} T^{n_1} S = n_1$. Se $m = 2$, então

$$T^{n_1} S T^{n_2} S = \begin{pmatrix} n_1 n_2 - 1 & -n_1 \\ n_2 & -1 \end{pmatrix}$$

e $\operatorname{tr} T^{n_1} S T^{n_2} S = n_1 n_2 - 2$. Assim, indutivamente, obtemos que $\operatorname{tr} A > 2$ e pelo Lema 4.2 A é reduzida. Seja

$$w = (\overline{n_1, \ldots, n_m}).$$

Então é fácil verificar que

$$A(w) = w.$$

Afirmação. $w > 1$.

De fato, suponhamos, por absurdo, que $w < 1$. Então é fácil verificar que A^{-1} é hiperbólica com traço positivo e que w é ponto fixo atrator de A^{-1}. Assim, pela Proposição 4.7, obtemos que

$$A = A^{-1},$$

o que é uma contradição. ■

Passaremos agora para o teorema principal de nossa dissertação, que dá condições necessária e suficiente para que os códigos geometrico e aritmético coincidam.

Teorema 4.1 *Sejam*

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

e

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

com $|a + d| > 2$, $c \neq 0$ *e reduzida. Então as seguintes condições são equivalentes*:

1. *A matriz A é totalmente F−reduzida*;
2. *Os códigos aritméticos e geométricos de A coincidem*;
3. *Todos os segmentos geodésicos(componentes da geodésica) em F correspondentes a classe de conjugação de A são orientados no sentido horário.*

Prova. (1. $\Longrightarrow$ 2.) Suponhamos que A seja totalmente $F-$reduzida. Então os eixos de todas as matrizes do $A-$ciclo entram em F através do lado a_2 e saem de F através do lado v_2(ver Figura 8), pois elas são orientadas no sentido horário. Seja

$$w = (\overline{n_1, \ldots, n_m})$$

a expansão em frações contínuas menos do ponto fixo atrator w de A. Então o eixo de $T^{-1}AT$ entra em F através de v_1 e sai através de v_2. Suponhamos que os eixos de

$$T^{-i}AT^i, 1 \leq i < k,$$

tenham a mesma propriedade e o eixo de $T^{-k}AT^k$ entra em F através de v_1 e sai através de a_1 ou a_2.

Afirmação. $k = n_1$.

De fato, suponhamos, por absurdo, que $k < n_1$. Então o eixo de

$$T^{-n_1}AT^{n_1}$$

não intercepta F, o que é uma contradição, pois

$$S^{-1}T^{-n_1}AT^{n_1}S$$

é F-reduzida. Por outro lado, como o eixo de

$$T^{-n_1+1}AT^{n_1+1}$$

não intercepta F temos que $k = n_1$. Assim, o eixo de

$$T^{-n_1}AT^{n_1}$$

sairá de F através de a_1 e o primeiro número do código geométrico $[A]$ é n_1. Note que, o eixo da matriz reduzida

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

não pode passar através do ponto i, pois fazendo $z = i$ na equação

$$c\,|z|^2 + (d-a)x - b = 0$$

obtemos que $c = b$, o que é uma contradição, pois $c > 0$ e $b < 0$. O mesmo argumento vale se o eixo de A passa através do vértice ρ de F. Neste caso, o eixo de

$$T^{-n_1}AT^{n_1}$$

passa através do vértice $\rho - 1$. Continuando este procedimento e contando os números de $T's$ entre os $S's$, obtemos que o código geométrico de A é da forma

$$[n_1, \ldots, n_m]\,,$$

isto é, ele é igual ao seu código aritmético.

(2. $\Longrightarrow$ 1.) Suponhamos, por absurdo, que A não seja totalmente F-reduzida. Então existe alguma matriz no $A-$ciclo que não é $F-$reduzida. Vamos assumir que A seja

reduzida mas não $F-$reduzida. Então A é F_1-reduzida, onde $F_1 = TS(F)$ e seu eixo entrar em F_1 através do lado $TS(v_2)$, conforme Figura 8. Portanto, o eixo de sua conjugada

$$T^{-1}S^{-1}T^{-1}ATST$$

intercepta F no sentido anti-horário e sai do lado v_1 de F. Isto significa que, na decomposição de A existe pelo menos um T^{-1}, em outras palavras, o código geométrico de A contém pelo menos um número negativo, o que é uma contradição.

(1. $\Longrightarrow$ 3.) Note que a interseção dos eixos das matrizes do A-ciclo com F constitui somente uma parte da geodésica fechada em F representando a classe de conjugação de A, isto é, sua parte reduzida. As partes restantes representam o deslocamento do eixo das geodésicas reduzidas. Vimos que todos segmentos geodésicos obtidos no processo venha ser no sentido horário.

(3. $\Longrightarrow$ 1.) Suponhamos, por absurdo, que A não seja totalmente F-reduzida. Então, de modo análogo, pelo menos um dos segmentos contidos na geodésica fechada associada à classe de conjugação de A é orientado no sentido anti-horário, o que é uma contradição.

■

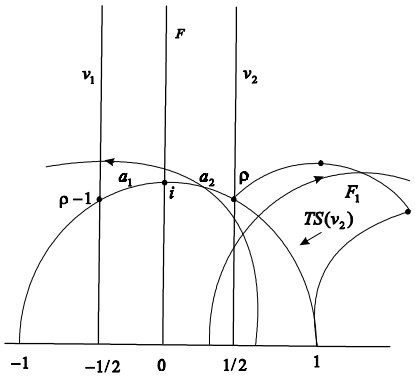

Figura 8. Ilustração do Teorema 4.1

Lema 4.5 *Se*

$$A = A_{n_1} \cdots A_{n_i} \cdots A_{n_m}$$

é totalmente $F-$reduzida e $n > n_i$, então

$$A(n) = A = A_{n_1} \cdots A_n \cdots A_{n_m}$$

é totalmente $F-$reduzida.

Prova. Vamos escrever $A(n)$ na forma

$$\begin{aligned} A(n) &= \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} n & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1a_2n + b_1a_2 - a_1c_2 & a_1b_2n + b_1b_2 - a_1d_2 \\ c_1a_2n + d_1a_2 - c_1c_2 & c_1b_2n + d_1b_2 - c_1d_2 \end{pmatrix}, \end{aligned}$$

onde

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \text{ ou } \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

pode ser igual a matriz I. Seja

$$\begin{aligned} f(n) &= \frac{a_1a_2n + b_1a_2 - a_1c_2 - c_1b_2n - d_1b_2 + c_1d_2}{c_1a_2n + d_1a_2 - c_1c_2 - a_1b_2n - b_1b_2 + a_1d_2} - 2 \\ &= \frac{(a_1a_2 - c_1b_2)n + (b_1a_2 - a_1c_2 - d_1b_2 + c_1d_2)}{(c_1a_2 - a_1b_2)n + (d_1a_2 - c_1c_2 - b_1b_2 + a_1d_2)} - 2. \end{aligned}$$

Então $f(n_i) \geq 0$, pois $A = A(n_i)$ é totalmente $F-$reduzida. Como $f(n)$ é uma transformação de Möbius, a menos de uma constante, temos que $f'(n) > 0$ se, e somente se, o determinante da matriz correspondente é positivo. Sendo o determinante da matriz associada a $f(n)$ igual a

$$D = a_1^2 - c_1^2 + a_2^2 - b_2^2$$

temos que $D > 0$, pois se

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \neq I$$

é reduzida, então pelo Lema 4.3

$$\frac{a_1}{c_1} > n_1 - 1 \geq 3 - 1 = 2.$$

Logo,

$$a_1^2 > 4c_1^2 > c_1^2 \Rightarrow a_1^2 - c_1^2 > 0.$$

Se

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = I,$$

então

$$a_1^2 - c_1^2 = 1 > 0.$$

Finalmente, pelo Lema 4.2, obtemos que

$$a_1^2 - c_1^2 + a_2^2 - b_2^2 > a_2^2 - b_2^2 = (a_2 - b_2)(a_2 + b_2) > 0.$$

Assim, se

$$\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

é reduzida, então

$$a_2 + b_2 > c_2 + d_2 > 0$$

e é trivial se

$$\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = I.$$

Portanto, $f(n) > f(n_i) \geq 0$. ■

Lema 4.6 *Sejam $m, n \in \mathbb{N}$ e*

$$A_m = T^m S = \begin{pmatrix} m & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

1. *Se $x > 1$ e $m \geq 3$, então $A_m(x) > 1$.*

2. *Se $x > 1$, então*

$$A_6 A_6(x) > A_6 A_3 A_6(x).$$

3. *Se $x > 1$, então*

$$A_4^n(x) > A_3(x).$$

4. *Se $x > 1$, então*

$$(A_6 A_3)^n(x) > A_4(x).$$

Prova. 1. Note que

$$\begin{aligned} A_m(x) - 1 &= \frac{mx - 1}{x} - 1 \\ &= \frac{(m-1)x - 1}{x} > 0, \forall x > 1, \end{aligned}$$

pois

$$m \geq 3 \Rightarrow m - 1 \geq 2 \Rightarrow (m-1)x \geq 2x > 2 \Rightarrow (m-1)x - 1 > 0.$$

2. Note que

$$\begin{aligned} A_6A_6(x) - A_6A_3A_6(x) &= \frac{35x-6}{6x-1} - \frac{96x-17}{17x-3} \\ &= \frac{19x^2-9x+1}{102x^2-35x+3} > 0, \end{aligned}$$

pois

$$19x^2 - 9x + 1 = 19x(x-1) + 10x + 1 > 0, \forall x > 1,$$

e

$$102x^2 - 35x + 3 = 102x(x-1) + 67x + 1 > 0, \forall x > 1.$$

Portanto,

$$A_6A_6(x) > A_6A_3A_6(x), \forall x > 1$$

3. Note que

$$A_4(x) > A_3(x)$$

pois

$$A_4(x) - A_3(x) = \frac{4x-1}{x} - \frac{3x-1}{x} = 1.$$

Pelo Corolário 4.1, obtemos que

$$A_4^n(x) \to w_4 = 2 + \sqrt{3}.$$

Como

$$w_4 > A_3(x)$$

temos que

$$A_4^n(x) > A_3(x).$$

4. Segue de maneira análoga a 3. ■

Lema 4.7 *O conjunto solução de*

$$\frac{1}{x} + \frac{1}{y} \geq \frac{1}{2} \ \textit{com} \ x, y \in \mathbb{N},$$

é

$$\mathcal{S} = \{\{p,2\},\{2,q\},\{3,3\},\{3,4\},\{4,3\},\{3,5\},\{5,3\}\},$$

onde $p, q \in \mathbb{N}$.

Prova. Note que

$$\frac{1}{x}+\frac{1}{y}>\frac{1}{2} \Leftrightarrow xy-2x-2y<0.$$

Assim,

$$xy-2x-2y<0 \Leftrightarrow xy-2x-2y+4<4 \Leftrightarrow (x-2)(y-2)<4.$$

Logo,

$$\begin{aligned} x &= 2 \text{ e } y=q \\ y &= 2 \text{ e } x=p \\ x-2 &= 1 \text{ e } 0<y-2<4 \\ y-2 &= 1 \text{ e } 0<x-2<4. \end{aligned}$$

Portanto, o conjunto solução da equação

$$\frac{1}{x}+\frac{1}{y}>\frac{1}{2}$$

é

$$\mathcal{S}=\{\{p,2\},\{2,q\},\{3,3\},\{3,4\},\{4,3\},\{3,5\},\{5,3\}\}.$$

De modo inteiramente análogo, prova-se que as únicas soluções da equação

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{2}$$

são os pares

$$\{3,6\},\{6,3\} \text{ e } \{4,4\}.$$

■

Teorema 4.2 *Seja A uma matriz hiperbólica tal que*

$$(A)=(n_1,\ldots,n_m).$$

Então A é totalmente $F-$reduzida se, e somente se,

$$\frac{1}{n_i}+\frac{1}{n_{i+1}}\leq\frac{1}{2},\forall i \pmod m,$$

isto é,

$$\{n_i,n_{i+1}\}\notin\mathcal{S},\forall i \pmod m.$$

Prova. Suponhamos que (A) contenha um par $\{k, n\}$ tal que $\{k, n\} \in \mathcal{S}$. Então passando, se necessário, a uma matriz no A-ciclo, podemos assumir que

$$n_1 = n \text{ e } n_m = k.$$

Se

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

então o seu eixo tem equação

$$c\,|z|^2 + (d-a)x - b = 0,$$

onde $z = x + iy$. Vamos assumir que A é reduzida, pois os códigos são invariantes por conjugação. Assim, o seu eixo intercepta o círculo

$$|z| = 1.$$

Além disso, ele intercepta F se $x \leq \frac{1}{2}$ e não intercepta F se $x > \frac{1}{2}$. Pelo Corolário 4.2, obtemos que

$$A = A_n A_{n_2} \cdots A_k,$$

onde

$$A_{n_i} = T^{n_i} S = \begin{pmatrix} n_i & -1 \\ 1 & 0 \end{pmatrix}.$$

Fazendo

$$B = A_{n_2} \cdots A_{n_{m-1}} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

obtemos, pelo Corolário 4.2, que B é reduzida ou $B = I$. Logo,

$$\begin{aligned} A &= \begin{pmatrix} n & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} k & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} a'nk - c'k + b'n - d & -a'n + c' \\ a'k + b' & -a' \end{pmatrix}. \end{aligned}$$

Assim,

$$\begin{aligned} \frac{a-d}{c-b} - 2 &= \frac{a'nk - c'k + b'n - d + a'}{a'k + b' + a'n - c'} - 2 \\ &= \frac{(nk - 2(n+k) + 1)a' - (k-3)c' + (n-2)b' - (d' + c')}{a'k + b' + a'n - c'}. \end{aligned} \tag{4.5}$$

Pelo Corolário 4.2 $a+d>2$ e pelo Lema 4.2 $c-b>0$, isto é, o denominador de (4.5) é positivo. Agora, se B é reduzida, então pelo Corolário 4.2 $a^{'}+d^{'}>2$. Assim, pelo Lema 4.2

$$c^{'}>0,\ \ c^{'}+d^{'}>0 \text{ e } b^{'}<0.$$

se $B=I$, então

$$c^{'}=b^{'}=0 \text{ e } d^{'}=a^{'}=1.$$

Como $\{k,n\}\in\mathcal{S}$. temos que

$$nk-2(n+k)+1\leq 0. \tag{4.6}$$

Assim, em qualquer caso, o numerador de equação (4.5) é negativo. Portanto, pela prova do Lema 4.5, A não é F-reduzida.

Reciprocamente, consideremos as seguintes matrizes

$$A_4=\begin{pmatrix}4 & -1\\ 1 & 0\end{pmatrix}, A_3A_6=\begin{pmatrix}17 & -3\\ 6 & -1\end{pmatrix} \text{ e } A_6A_3=\begin{pmatrix}17 & -6\\ 3 & -1\end{pmatrix}.$$

Seus pontos fixos atratores e repulsores são

$$w_4=2+\sqrt{3}, w_{36}=\frac{3+\sqrt{7}}{2} \text{ e } w_{63}=3+\sqrt{7},$$

e

$$u_4=2-\sqrt{3}, u_{36}=\frac{3-\sqrt{7}}{2} \text{ e } u_{63}=3-\sqrt{7},$$

respectivamente. Assim, essas matrizes são reduzidas com códigos aritméticos

$$(4), (3,6) \text{ e } (6,3).$$

Seus eixos passam através do vértice

$$\rho=\frac{1}{2}+\frac{\sqrt{3}}{2}i$$

de F, conforme Figura 9. Portanto, as três matrizes são totalmente F-reduzidas.

Sejam $\mathcal{A}$ o conjunto de todos os códigos aritméticos

$$(n_1,\ldots,n_m)$$

tais que

$$\{n_i,n_{i+1}\}\notin\mathcal{S},\forall i \mod(m),$$

isto é,

$$\mathcal{A} = \{(n_1, \ldots, n_m) : \{n_i, n_{i+1}\} \notin \mathcal{S}, \forall i \mod(m)\}$$

e

$$(n_1, \ldots, n_m) \in \mathcal{A}.$$

Se $n_i > 6$ é adjacente a 3, então podemos decrescê-lo em uma unidade e, ainda, obtemos um código em $\mathcal{A}$. Analogamente, decrescendo um $n_i \geq 5$ não adjacente a 3, em uma unidade, também, obtemos um código em $\mathcal{A}$. Claramente, partindo de um código particular, podemos aplicar este procedimento um número finito de vezes até que se chegue a um código que não possamos mais decrescer, caso contrário, chegariamos a um código com um par em $\mathcal{S}$. Este código será chamado de *código mínimo* de $\mathcal{A}$. Reciprocamente, cada código de $\mathcal{A}$ pode ser obtido de um código mínimo por um número finito de procedimentos contrários. Por exemplo, todo código em $\mathcal{A}$ não contendo um 3 pode ser obtido do código (4). Assim, pelo Lema 4.5, basta provar que todos os códigos mínimos em $\mathcal{A}$ são totalmente $F-$reduzidos.

Seja (A) um código mínimo diferente de

$$(4)\,, (3,6) \text{ e } (6,3)\,.$$

Então (A) contém pelo menos um 3 e, a menos de permutação cíclica, pode ser representado como uma série de blocos da forma

$$\{6, 3, 6, \ldots, 3, 6, 4, \ldots, 4\}\,.$$

Note que, alguns dos blocos podem não conter 4 de modo algum, mas ele ainda começa e termina com 6 e, se eles estão próximo a cada outro, teremos o par

$$\{6, 6\}$$

no código. Para provar que A é totalmente $F-$reduzida, há seis casos a ser considerado:
1º **Caso**. Se

$$A = A_6 A_3 A_6 \cdots A_4^{n_1} \cdots A_4^{n_2} \cdots A_6 A_3 A_6 A_4^{n_m},$$

onde $n_i \geq 0$ e $n_m > 0$, então

$$w_A > w_{63} \text{ e } u_A < u_{63}.$$

De fato, pelo Corolário 4.1 a transformação de Möbius correspondente a qualquer matriz reduzida representa uma função crescente para o valor real $x > 1$. Além disso, pelo Lema

4.6 podemos substituir A_3 por $A_4^{n_i}$ com $n_i > 0$ e inserir uma A_3 entre quaisquer dois vizinhos dos A_6's, para obtermos

$$w_A = A_6A_3A_6\cdots A_4^{n_1}\cdots A_4^{n_2}\cdots A_6A_3A_6A_4^{n_m}w_A > (A_6A_3)^N w_A,$$

para algum $N > 0$. Se $w_A \leq w_{63}$, então, pelo Corolário 4.1,

$$(A_6A_3)^N w_A \geq w_A,$$

o que é uma contradição. Portanto, $w_A > w_{63}$. Pelo Corolário 1.1

$$\frac{1}{u_A}$$

tem o período contrário ao de w_A. Logo,

$$\frac{1}{u_A} = A_4^{n_m}A_6A_3A_6\cdots A_4^{n_1}\cdots A_6A_3A_6\frac{1}{u_A} > (A_3A_6)^N\frac{1}{u_A},$$

e, assim,

$$\frac{1}{u_A} > w_{36} = \frac{1}{u_{63}}.$$

Portanto, $u_A < u_{63}$. Logo, o eixo de A cerca o eixo de A_6A_3 e A intercepta F propriamente.

2º **Caso**. Se

$$A = A_6A_3A_6\cdots A_4^{n_1}\cdots A_6A_3,$$

então, de modo análogo ao 1º **Caso**,

$$w_A > w_{63} \text{ e } u_A < u_{63}.$$

Logo, o eixo de A cerca o eixo de A_6A_3 e A intercepta F propriamente.

3º **Caso**. Se

$$A = A_6A_3A_6\cdots A_4^{n_1}\cdots A_4^{n_2}\cdots A_6A_3A_6,$$

então

$$w_A > w_{63} \text{ e } u_A < u_{63}.$$

De fato, de modo análogo ao 1º **Caso**, obtemos $M > 0$ tal que

$$w_A = A_6A_3A_6\cdots A_4^{n_1}\cdots A_4^{n_2}\cdots A_6A_3A_6w_A \geq (A_6A_3)^M A_6w_A.$$

Pelo Lema 4.6, temos que

$$w_A > A_4A_6w_A > A_3A_6w_A.$$

Portanto, $w_A > w_{36}$. Assim,

$$A_6 w_A = 6 - \frac{1}{w_A} > 6 - \frac{1}{w_{36}} = w_{63}$$

e, portanto, $w_A > w_{63}$. Desde que

$$\frac{1}{u_A} > w_{36}$$

temos que $u_A < u_{63}$. Logo, o eixo de A cerca o eixo de A_6A_3 e A intercepta F propriamente.

4º **Caso**. Se

$$A = A_6A_3A_6 \cdots A_4^{n_1} \cdots A_6A_3A_6,$$

então, de modo análogo ao 1º **Caso**,

$$w_A > w_{63} \text{ e } u_A < u_{63}.$$

Logo, eixo de A cerca o eixo de A_3A_6 e A intercepta F propriamente.

5º **Caso**. Se

$$A = A_4^{n_1} A_6A_3A_6A_3 \cdots A_6A_3A_6A_4^{n_m},$$

onde $n_i > 0$ e $n_m > 0$, então

$$w_A > w_4 \text{ e } u_A < u_4.$$

De fato, pelo Lema 4.6, obtemos que

$$\begin{aligned} w_A &= A_4^{n_1} A_6A_3A_6A_3 \cdots A_6A_3A_6A_4^{n_m}(w_A) \\ &> A_4^{n_1} (A_6A_3)^k w_A \\ &> A_4^{n_1+1} w_A. \end{aligned}$$

Portanto, $w_A > w_4$. Desde que

$$\frac{1}{u_A} > w_4$$

temos que

$$u_A < \frac{1}{w_4} = u_4.$$

Logo, eixo de A cerca o eixo de A_4 e A intercepta F propriamente.

6º **Caso**. Se

$$A = A_4^{n_1} A_6A_3A_6A_3 \cdots A_6A_3A_6,$$

onde $n_1 > 0$, então pelo item 3. do Lema 4.6 e de modo análogo ao 4º **Caso**,

$$w_A > w_4 \text{ e } u_A < u_4.$$

Logo, eixo de A cerca o eixo de A_3A_6 e A intercepta F propriamente. ■

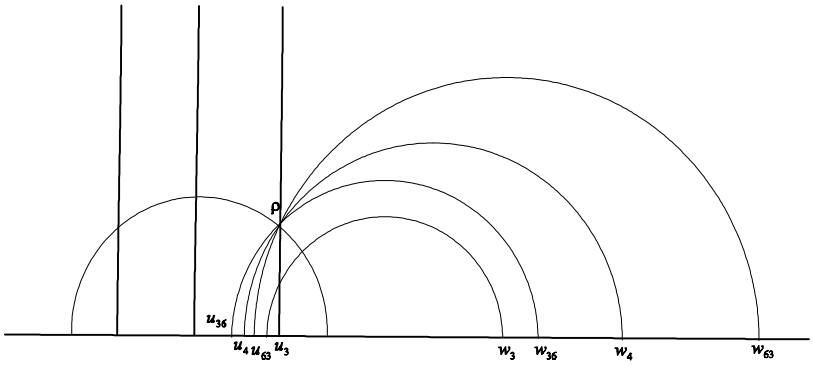

Figura 9. Eixos das matrizes A_3, A_4, A_3A_6 e A_6A_3

Corolário 4.3 *As únicas matrizes primitivas totalmente F-reduzidas cujos eixos passam pelo vértice ρ de F são*:

$$A_4, A_3A_6 \ \textit{e}\ A_6A_3.$$

Prova. Vimos na prova do Teorema 4.2, que o eixo de qualquer matriz totalmente F-reduzida com um código mínimo diferente de uma potência de

$$A_4, A_3A_6 \ \text{ou}\ A_6A_3.$$

contém o eixo de alguma das três transformações A_4, A_3A_6, A_6A_3 e, portanto, intercepta F propriamente e não passa através de ρ. Pelo Lema 4.5 o mesmo é verdade para alguma matriz totalmente F-reduzida que não tem um código mínimo. ■

Referências Bibliográficas

[1] Bhattacharya, P. B.; Jain, S. K. and Nagpaul, S. R., *Basic Abstract Algebra*. Cambridge, New York, 1995.

[2] Churchill, R. V., *Variáveis Complexas e suas Aplicações*, McGRAW-HILL. 1975.

[3] Conway, J. B., *Functions of Complex Variable*, Springer-Verlag. 1975.

[4] Garcia, A. L. e Lequain, Y., *Álgebra: Um Curso de Introdução*. IMPA, Rio de Janeiro, 1988.

[5] Gouvêa, F. Q., *Formas Modulares.* IMPA, 1990.

[6] Hardy, G. H. and Wright, E. M., *An Introduction to the Theory of Numbers.* Oxford Science Publications, 1979.

[7] Katok, S., *Fuchsian Groups*, The University of Chicago Press, Chicago and London, 1992.

[8] Katok, S., "Coding of closed geodesic after Gauss and Morse," Published in *Geometriae Dedicata*, 63: 123-145, 1996.

[9] Katok, S., *Continued fractions, Hyperbolic Geometry and Quadratic Forms*, Course Notes for Math. 497 Reu Program, 2001.

[10] Lemos, M., *17º Colóquio Brasileiro de Matemática.* IMPA, 1989.

[11] Lins Neto, A., *Funções de uma variável complexa,* Projeto Euclides, 1996.

[12] Niven, I.; Zuckerman, H. S. and Hugh, L. M., *An introduction to the theory of numbers,* Fifth Edition, 1991.

[13] Rédei, L., *Algebra.* U. K.: Pergamon, London, 1967.

[14] Schoeneberg, B., *Elliptic Modular Functions.* Springer-Verlag, 1974.

[15] Silva, M. F. da, *Codificação de Geodésicas Fechadas Simples em Superfícies Hiperbólicas.*UNICAMP, FEEC, Tese de Doutorado, março 2002.

[16] Spindler, K., *Abstract Algebra with Applications*, Vol 1. Dekker, 1994.