EDIR JUNIOR FERREIRA LEITE

Tópicos de Códigos Geometricamente Uniformes em Espaços Hiperbólicos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2012

EDIR JUNIOR FERREIRA LEITE

Tópicos de Códigos Geometricamente Uniformes em Espaços Hiperbólicos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Diferencial.

Orientador: Prof. Dr. Edson Agustini.

UBERLÂNDIA - MG
2012

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU , MG, Brasil

L533t Leite, Edir Junior Ferreira, 1985-
Tópicos de códigos geometricamente uniformes em espaços hiperbólicos / Edir Junior Ferreira Leite. - 2012.
72 f. : il.

Orientador: Edson Agustini.

Dissertação (mestrado) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Matemática - Teses. 2. Teoria dos reticulados - Teses. 3. Partições (Matemática) - Teses. 4. Grupos fundamentais (Matemática) - Teses. I. Agustini, Edson. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 51

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 158
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Edir Junior Ferreira Leite.

NÚMERO DE MATRÍCULA: 11012MAT007.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Diferencial.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Tópicos de Códigos Geometricamente Uniformes em Espaços Hiperbólicos.

ORIENTADOR: Prof. Dr. Edson Agustini.

A dissertação foi **APROVADA**, em reunião pública, realizada na Sala 1F 119, Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 16 de fevereiro de 2012, às 9:00 horas, com a seguinte Banca Examinadora:

NOME	**ASSINATURA**
Prof. Dr. Henrique Lazari IGCE/UNESP - Universidade Estadual Paulista Campus Rio Claro-SP	
Profª. Drª. Dulce Mary de Almeida FAMAT/UFU - Universidade Federal de Uberlândia	
Prof. Dr. Edson Agustini FAMAT/UFU - Universidade Federal de Uberlândia	EDSON AGUSTINI

Uberlândia, 16 de fevereiro de 2012.

Dedicatória

Dedico esta dissertação aos meus queridos familiares.

Agradecimentos

Agradeço primeiramente a Deus, meu guia, meu caminho e minha salvação.

Agradeço à CAPES pela bolsa que me possibilitou aprender um pouco sobre os segredos da matemática.

Agradeço ao meu orientador, Edson Agustini, pela credibilidade que depositou em mim, pela paciência e principalmente pela sua amizade durante os 3 anos de orientação incluindo o Curso de Especialização em Geometria e o Mestrado.

Agradeço aos meus familiares, pela compreensão, pelo incentivo nos momento difíceis e por sempre me propiciaram um ambiente familiar sadio, dentro dos ensinamentos de Deus.

Agradeço aos amigos que participaram comigo do Programa de Mestrado em Matemática.

Agradeço à Universidade Federal de Uberlândia e à Faculdade de Matemática pelo Programa de Pós-graduação em Matemática.

Agradeço aos professores da Faculdade de Matemática, em especial àqueles com quem cursei alguma disciplina e a professora Dulce Mary de Almeida pelas palavras de incentivo e pela sua amizade desde o Curso de Especialização em Geometria.

LEITE, E. Jr. F. *Tópicos de Códigos Geometricamente Uniformes em Espaços Hiperbólicos.* 2012. 72 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Esta dissertação é um texto detalhado resultante do estudo do artigo [14] de Lazari & Palazzo Jr. (2005), no qual há a generalização dos conceitos de *partições geometricamente uniformes* e *códigos geometricamente uniformes*, amplamente empregados em espaços euclidianos, para espaços hiperbólicos. O principal teorema estudado é uma caracterização de *códigos de classes laterais generalizados* por meio do conceito de *códigos* G*-lineares* (Teorema 4.3). Além do estudo detalhado do artigo, também apresentamos uma pequena contribuição: a demonstração de que o grupo fundamental π_{g} de uma superfície compacta S de gênero $\mathsf{g} \geq 2$, obtida por quociente do plano hiperbólico por π_{g}, é subgrupo normal do grupo gerado pelas reflexões nos lados de um triângulo hiperbólico retângulo que estabelece um ladrilhamento simétrico na região fundamental do π_{g} (Teorema 3.4).

Palavras-chave: Reticulado, Partição, Código, Código G-linear, Grupo Fundamental, Grupo Triângulo.

LEITE, E. Jr. F. *Topics of Geometrically Uniform Codes in Hyberbolic Spaces.* 2012. 72 p. M. Sc. Dissertation, Federal University of Uberlandia, Uberlândia-MG.

Abstract

This dissertation is an extended text resulting from the study of paper [14] by Lazari & Palazzo Jr. (2005), in which there is the generalization of the concepts of *geometrically uniform partitions* and *geometrically uniform codes*, widely used in euclidean spaces, to hyperbolic spaces. The main studied theorem is a characterization of *generalized coset codes* through the concept of G-*linear codes* (Theorem 4.3). Besides the detailed study of the paper, we also establish a small contribution: the proof that the fundamental group π_{g} of a compact surface S of genus $\mathsf{g} \geq 2$, obtained by quocient of a hyperbolic space by π_{g}, is a normal subgroup of the group generated by reflections at the sides of a hyperbolic right triangle that establishes a symmetric tiling in the fundamental region of π_{g} (Theorem 3.4).

Key-words: Lattice, Partition, Code, G-linear Code, Fundamental Group, Triangle Group.

Sumário

Introdução

A teoria dos sistemas de comunicações digitais teve origem a partir do trabalho fundamental [21] de Claude Shannon, do *Bell Laboratories*, publicado em 1948. Neste trabalho foi mostrado que dado um canal de comunicação digital, é possível, com uma codificação adequada, transmitir informações com probabilidade de erro arbitrariamente pequena. O trabalho inicial para a aquisição de bons códigos foi árduo, pois exigia um profundo conhecimento de álgebra abstrata, sendo desenvolvido por um grupo restrito apenas por matemáticos nas décadas de 50 e 60.

Os elementos dos códigos corretores de erros são sequências de símbolos pertencentes a um alfabeto, tomado frequentemente entre os elementos de algum corpo $\mathbb{F}_q$. Mesmo quando os símbolos não têm uma estrutura algébrica natural, um procedimento usual e útil é produzir um rotulamento dos símbolos do alfabeto por elementos de algum grupo, ou seja, definir uma aplicação injetiva do alfabeto no grupo, sujeita a determinadas condições (Seção 3.4).

O conceito de código geometricamente uniforme foi introduzido por David Forney [8] em 1991. Este conceito tem se mostrado muito apropriado no contexto de códigos que podem ser representados como reticulados em espaços euclidianos. Um dos principais objetivos dos códigos geometricamente uniformes está relacionado à construção de partições geometricamente uniformes e em particular na construção de códigos de classes laterais generalizados.

O objetivo deste trabalho é o estudo da extensão do conceito de reticulados e partições geometricamente uniformes no plano hiperbólico conforme estabelecido no artigo [14] de Henrique Lazari e Reginaldo Palazzo Jr., de 2005. Embora os grupos de isometrias hiperbólicos tenham maior complexidade que os grupos de isometrias euclidianos, os procedimentos e os conceitos para partições geometricamente uniformes podem ser considerados os mesmos.

Este trabalho está subdividido do seguinte modo:

O Capítulo 1 descreve e fornece as propriedades básicas das estruturas matemáticas (algébricas e métricas) com maior relevância para a Teoria da Informação e Comunicação.

No Capítulo 2, discorremos sobre alguns tópicos em Geometria Hiperbólica essenciais à nossa dissertação, com o objetivo de tornar acessível a leitura deste trabalho àqueles que, não possuam conhecimentos mais consistentes em tal geometria. Cabendo salientar que, devido ao seu caráter secundário, optamos por uma abordagem "sem muitas demonstrações" dos diversos resultados apontados.

No Capítulo 3 demonstramos que o grupo fundamental π_g de uma superfície compacta S gênero $g \geq 2$, obtida por quociente do plano hiperbólico U por π_g é subgrupo normal do grupo gerado pelas reflexões nos lados de um triângulo hiperbólico retângulo que estabelece um ladrilhamento simétrico na região fundamental do π_g (Teorema 3.4). Este resultado é de vital importância para o estudo de reticulados sobre superfícies compactas os quais, por sua vez, são muito importantes no estudo de códigos corretores de erros, como podemos constatar em [14]. O fato desse resultado ser bastante intuitivo do ponto de vista geométrico faz com que

o mesmo seja amplamente utilizado em textos específicos sobre esse assunto. Entretanto, uma prova desse teorema não é simples e não é apresentada em tais textos. Esta demonstração é a nossa principal contribuição, ressaltando que, também, encontramos uma expressão para os geradores de π_g. Por fim, definimos com detalhes códigos G-lineares e estabelecemos o fato que um reticulado S é $\mathsf{U}(\mathsf{S})$-linear (Teorema 3.7).

O objetivo do Capítulo 4 é estender a teoria das partições geometricamente uniformes ao plano hiperbólico, de modo a permitir que reticulados casados a grupos, como aqueles descritos na Seção 3.4, possam ser decompostos em partições geometricamente uniformes. Mostramos que um código de classes laterais generalizado é $\mathsf{U}(\mathsf{S})$-linear (Teorema 4.3). A extensão da teoria foi feita sob a hipótese geral de que códigos de rótulos são subgrupos normais do grupo de rótulos, concluindo então com o resultado fundamental sobre cadeias de partições geometricamente uniformes hiperbólicas, ou seja, que são cadeias geometricamente uniformes (Teorema 4.4).

Capítulo 1

Grupos e Espaços Métricos

Neste capítulo, apresentamos, de forma sucinta, noções gerais das estruturas matemáticas (algébricas e geométricas) com maior relevância para a Teoria da Informação e Codificação. Para uma abordagem completa, há excelentes livros textos sobre o assunto como, por exemplo: [10], [16], [9], [12], [19] e [20].

1.1 Grupos

Definição 1.1 *Um* ***grupo*** *é um par consistindo de um conjunto não vazio* G *e uma operação binária* $* : G \times G \to G$, *onde denotamos* $*(a, b)$ *por* $a * b$, *satisfazendo as propriedades:*
$G1 : a * (b * c) = (a * b) * c$, $\forall a, b$ *e* $c \in G$. *(Associativa);*
$G2 :$ *Existe* $e \in G$ *tal que* $a * e = e * a = a$, $\forall a \in G$. *(Existência do elemento neutro);*
$G3 :$ *Para cada elemento* $a \in G$, *podemos determinar um elemento* $a^* \in G$ *tal que* $a * a^* = a^* * a = e$. *(Existência do Elemento Inverso).*

Denotamos o grupo por $(G, *)$, ou simplesmente por G, se não houver ambiguidade. No caso de $*$ denotar uma das operações usuais $\cdot$ ou $+$, então denotaremos e por 1 ou 0 e a^* por a^{-1} ou $-a$, respectivamente. Um grupo G é dito **comutativo** ou **abeliano** se estiver satisfeita a condição adicional:
$G4 :$ Para todos a e b em G, $a * b = b * a$. (Propriedade Comutativa).

Exemplo 1.1 *O conjunto* $M - PSK = \left\{ e^{\frac{2k\pi i}{M}} : k = 0, ..., M-1 \right\} \subseteq \mathbb{C}$ *com a operação usual de multiplicação de números complexos é um grupo chamado de* ***grupo cíclico de ordem*** M. *Se denotamos* $\zeta = e^{\frac{2\pi i}{M}}$ *então temos que* $M - PSK = \{\zeta^n : n \in \mathbb{Z}\}$, *(ver Figura 1) e neste caso dizemos que* ζ *é um gerador do* $M - PSK$ *e denotamos também* $M - PSK = \langle \zeta \rangle$.

Definição 1.2 *Seja* G *um grupo. Se* G *possui um número finito de elementos, dizemos que* G *é um* ***grupo finito****. No caso de um grupo* G *ser finito, chamamos de* ***ordem*** *de* G *ao número de elementos do conjunto* G, *denotamos a ordem de* G *por* $|G|$. *Caso contrário, dizemos que* G *é um* ***grupo infinito****.*

Exemplo 1.2 *Seja* X *um conjunto finito com* $n \geq 1$ *elementos, digamos* $X = \{x_1, ..., x_n\}$, *então denotando por* S_X *ou* S_n *o conjunto que consiste de todas as aplicações bijetivas* $\varphi : X \to X$ *munido da operação de composição de funções, resulta que* S_n *é um grupo. Chamamos o grupo* $(S_n, \circ)$ *de* ***grupo simétrico de grau*** n *e os elementos* σ *de* S_n *são também chamados de* ***permutações*** *de* X. *Temos que* $|S_n| = n!$.

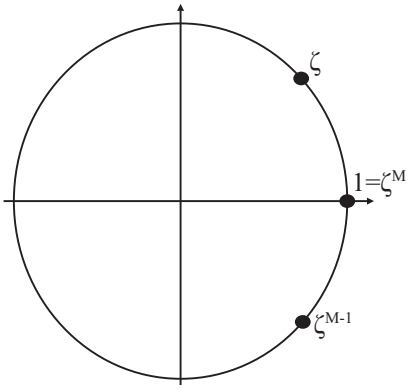


FIGURA 1: *Representação de alguns elementos do grupo* $M - PSK$.

Exemplo 1.3 *Consideremos um polígono regular de* M *lados assentado no circulo*

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}$$

e com um dos vértices no ponto $1 = 1 + 0i$, *vamos denotar por* D_M *o conjunto de todas as simetrias deste polígono, então com a operação de composição de funções,* D_M *é um grupo. Os seus elementos são:*

$$R_k = \begin{bmatrix} \cos\left(\frac{2k\pi}{M}\right) & -\operatorname{sen}\left(\frac{2k\pi}{M}\right) \\ \operatorname{sen}\left(\frac{2k\pi}{M}\right) & \cos\left(\frac{2k\pi}{M}\right) \end{bmatrix},\ k = 0, ..., M-1 \ e$$

$$S \circ R_k \ onde\ S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ isto\ é,\ reflexão\ sobre\ o\ eixo\ real.$$

Notando que $R_k = R^k$ *onde*

$$R = \begin{bmatrix} \cos\left(\frac{2\pi}{M}\right) & -\operatorname{sen}\left(\frac{2\pi}{M}\right) \\ \operatorname{sen}\left(\frac{2\pi}{M}\right) & \cos\left(\frac{2\pi}{M}\right) \end{bmatrix}$$

e que aplicar R^k *nos vértices do polígono equivale a multiplicar estes vértices por* $e^{\frac{2k\pi i}{M}}$, *temos que*

$$D_M = \left\{Id, R, ..., R^{M-1}, S, S \circ R, ..., S \circ R^{M-1}\right\}.$$

Este grupo pode ser também descrito como

$$D_M = \left\langle S, R : R^M = S^2 = Id; R \circ S = S \circ R^{M-1} \right\rangle.$$

Como $R \neq R^{-1} = R^{M-1}$ *se* $M > 2$, *temos que este grupo não é abeliano.* D_M *é chamado de* ***grupo diedral de grau*** M. *A Figura 2 ilustra o caso* $M = 7$.

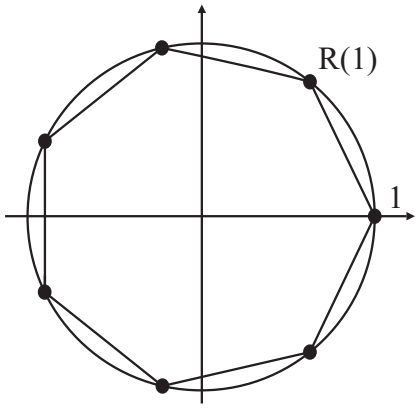


FIGURA 2: *Representação da ação do grupo* D_7 *com elementos em* S^1.

Definição 1.3 *Sejam* G *um grupo e* H *um subconjunto de* G *tal que com a restrição da operação de* G, H *é ele mesmo um grupo, então dizemos que* H *é um* ***subgrupo*** *de* G. *Denotamos o fato de* H *ser um subgrupo de* G *por* $H \leq G$.

Lema 1.1 *Seja* $(G, *)$ *um grupo e* H *um subconjunto não vazio de* G. *Então* $(H, *)$ *é um subgrupo de* G *se, e somente se,* $\begin{cases} (i)\ a * b \in H, \forall a \text{ e } b \in H \\ (ii)\ a^{-1} \in H, \forall a \in H \end{cases}$.

Demonstração:

($\Rightarrow$) Óbvio.
($\Leftarrow$) É claro que vale $a * (b * c) = (a * b) * c$, $\forall a, b$ e $c \in H$. Como a e $a^{-1} \in H$, temos $e = a * a^{-1} \in H$. □

Exemplo 1.4 *Seja* g *um elemento qualquer de um grupo* G, *então o conjunto* $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ *é um subgrupo de* G, *chamado de* ***subgrupo cíclico*** *gerado por* g. *Se* $\langle g \rangle$ *tem ordem finita, então dizemos que* g *tem* ***ordem finita*** *e chamamos de* ***ordem*** *de* g *ao número* $|g| = |\langle g \rangle|$. *Caso contrário, dizemos que* g *tem* ***ordem infinita****.*

Sejam $(G, *)$ um grupo e H um subgrupo de G, então dado $a \in G$ os conjuntos $aH = \{a * b : b \in H\}$ e $Ha = \{b * a : b \in H\}$ são chamados respectivamente de **classe lateral à esquerda módulo** H e **classe lateral à direita módulo** H. Se o número de classes laterais à esquerda ou à direita for finito, então essas quantidades são iguais, e então, este valor comum é chamado de **índice** de H em G e denotado por $[G : H]$. No caso em que valer $aH = Ha$ para todo $a \in G$, dizemos que H é um **subgrupo normal** de G e denotamos $H \lhd G$. Neste caso, o conjunto $G/H = \{aH : a \in G\}$ munido da operação $(aH) * (bH) := (a * b)H$ é um grupo denominado **grupo quociente** de G pelo subgrupo normal H.

Observe que se G é abeliano então todo subgrupo é normal.

Proposição 1.1 *Seja* H *um subgrupo de* $(G, *)$. *São equivalentes:*
(i) $H \lhd G$;
(ii) $aHa^{-1} := \left\{a * h * a^{-1} \in G : h \in H\right\} \subseteq H$, $\forall a \in G$;
(iii) $aHa^{-1} = H$, $\forall a \in G$.

Exemplo 1.5 *Se* $[G : H] = 2$, *então* $H \lhd G$.

Vamos mostrar que $rH = Hr$, $\forall r \in G$. *Se* $r \in H$ *então* $rH = H = Hr$. *Se* $r \notin H$ *temos*

$$\begin{cases} rH \neq H, \\ Hr \neq H. \end{cases}$$

Como $[G : H] = 2$, *existem exatamente duas classes laterais à esquerda, que são* rH *e* H. *Agora, uma relação de equivalência num espaço decompõe o espaço na união disjunta de suas classes de equivalência; assim* $rH = G \backslash H$. *Da mesma forma,* $Hr = G \backslash H$.

Portanto $rH = G \backslash H = Hr$.

Proposição 1.2 *Sejam* $(G, *)$ *um grupo,* H *um subgrupo de* G *e* g *e* $g' \in G$, $g \equiv g'$ *mod* H $\Leftrightarrow (g')^{-1} * g \in H$ *define uma relação de equivalência no conjunto* G.

Demonstração:

(i) $g \equiv g \bmod H$ $\forall g \in G$, pois $g^{-1} * g = e \in H$.

(ii) $g \equiv g' \bmod H \Rightarrow g' \equiv g \bmod H$, pois se $(g')^{-1} * g \in H$ então

$$g^{-1} * g' = \left((g')^{-1} * g\right)^{-1} \in H.$$

(iii) $g \equiv g' \bmod H$ e $g' \equiv z \bmod H \Rightarrow g \equiv z \bmod H$ pois,

$$(g')^{-1} * g \in H \text{ e } z^{-1} * g' \in H \Rightarrow z^{-1} * g = z^{-1} * g' * (g')^{-1} * g \in H.$$

E isto demonstra a proposição. □

Teorema 1.1 ***(Teorema de Lagrange).*** *Sejam* G *um grupo finito e* H *um subgrupo de* G. *Então* $|G| = |H|\,[G : H]$; *em particular, a ordem de* H *e o índice de* H *em* G *dividem a ordem de* G.

Dados os grupos G e H, isto é, $(G, *_1)$ e $(H, *_2)$, dizemos que uma aplicação $f : G \to H$ é um **homomorfismo** quando, para todos g_1 e $g_2 \in G$, $f(g_1 *_1 g_2) = f(g_1) *_2 f(g_2)$. Notemos que a operação no lado esquerdo da igualdade é a operação de G e a operação do lado direito é a de H. Um homomorfismo bijetor é chamado de **isomorfismo**. Quando existir um isomorfismo $f : G \to H$ dizemos que G e H são **isomorfos** e denotamos $G \simeq H$. A relação $\simeq$ é uma relação de equivalência no conjunto de todos os grupos. O fato de dois grupos serem isomorfos significa que eles são indistinguiveis sob o ponto de vista das propriedades dos grupos.

Definição 1.4 *Seja* G *um grupo. Um* ***automorfismo*** *de* G *é um isomorfismo* $f : G \to G$. *O conjunto dos automorfismos de* G *será denotado por* $\mathrm{Aut}(G)$. *É fácil verificar que a composição de dois automorfismos de* G *é um automorfismo de* G *e que* $(\mathrm{Aut}(G), \circ)$ *é um grupo.*

Definição 1.5 *Dado* $f : G \to H$ *um homomorfismo de grupos, a* ***imagem*** *de* f *é o conjunto* $\mathrm{Im}(f) = \{f(g) : g \in G\}$ *e o* ***núcleo*** *de* f *é o conjunto* $\ker(f) = \{g \in G : f(g) = e_H\}$, *sendo* e_H *o elemento neutro de* H.

Proposição 1.3 *Seja* $f : G \to H$ *um homomorfismo de grupos. Então* $\mathrm{Im}(f)$ *é um subgrupo de* H *e* $\ker(f)$ *é um subgrupo normal de* G.

Corolário 1.1 *Sejam* H *e* K *dois subgrupos de* $(G, *)$. *Se* H *ou* K *for normal em* G, *então* $HK = \{h * k : h \in H \text{ e } k \in K\}$ *é um subgrupo de* G.

Proposição 1.4 *Sejam* H, K *dois subgrupos de* G. *Então:*

$$HK \text{ é um subgrupo de } G \Leftrightarrow HK = KH.$$

Proposição 1.5 *Seja* G *um grupo. Sejam* H *e* K *dois subgrupos de* G *tais que* HK *seja um subgrupo. Então,*

$$[HK : K] = [H : H \cap K]$$
$$[HK : H] = [K : H \cap K].$$

Teorema 1.2 ***(Teorema do Homomorfismo).*** *Sejam* G *e* H *grupos. Seja* $f : G \to H$ *um homomorfismo, então*

$$\frac{G}{\ker(f)} \simeq \mathrm{Im}(f).$$

Definição 1.6 *Sejam* K *e* Q *grupos, definimos uma* ***extensão*** *de* K *por* Q *como sendo um grupo* G *tal que:*
(i) K *é um subgrupo normal de* G.
(ii) $\frac{G}{K}$ *é isomorfo a* Q.

Exemplo 1.6 *Seja* n *um inteiro positivo. Sobre* $\mathbb{Z}$*, definimos a relação* $\underset{n}{\equiv}$ *da maneira seguinte: para* a *e* $b \in \mathbb{Z}$*,*

$$a \underset{n}{\equiv} b \Leftrightarrow a - b \text{ é um múltiplo de } n.$$

É imediato verificar que $\underset{n}{\equiv}$ *é uma relação de equivalência, denominada* ***relação de equivalência módulo*** n*. Se* $a \in \mathbb{Z}$*, então,*

$$a + n\mathbb{Z} = \left\{ b \in \mathbb{Z} : b \underset{n}{\equiv} a \right\} = \{a + kn : k \in \mathbb{Z}\}.$$

Denotaremos por $\frac{\mathbb{Z}}{n\mathbb{Z}}$ *o conjunto das classes de equivalência módulo* n*; claramente temos que* $\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$.

Sobre $\frac{\mathbb{Z}}{n\mathbb{Z}}$*, definimos duas operações:*

$$\underset{n}{\oplus}: \begin{array}{ccc} \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} & \longrightarrow & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{x+y} \end{array} \quad e \quad \underset{n}{\odot}: \begin{array}{ccc} \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} & \longrightarrow & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{xy} \end{array}.$$

Logo, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \underset{n}{\oplus}\right)$ *é um grupo finito com* n *elementos.*

Seja $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ *o conjunto dos elementos invertíveis de* $\frac{\mathbb{Z}}{n\mathbb{Z}}$*. Logo,* $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ *é um grupo com a operação* $\underset{n}{\odot}$*, chamado* ***grupo multiplicativo****.*

Se p *é um número primo, então* $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ *é cíclico, isto é,* $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$*, sendo* $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ *um grupo multiplicativo.*

Proposição 1.6 *Sejam* $n \geq 1$ *um inteiro e* $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ *o grupo multiplicativo dos elementos invertíveis de* $\frac{\mathbb{Z}}{n\mathbb{Z}}$*. Então* $\psi : \mathrm{Aut}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \to \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$*, definida por* $\psi(f) = f(\overline{1})$*, é um isomorfismo.*

Conclusão: $\mathrm{Aut}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right) \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$, sendo p um número primo.

Definição 1.7 *Sejam os grupos* $(G_1, *_1)$ *e* $(G_2, *_2)$*. Considere o produto cartesiano* $G_1 \times G_2$ *com a operação*

$$(x_1, x_2) \cdot (y_1, y_2) := (x_1 *_1 y_1, x_2 *_2 y_2).$$

O grupo definido pelo par $(G_1 \times G_2, \cdot)$ *é chamado* ***produto direto*** *de* G_1 *com* G_2*.*

Sejam $(H, \#_1)$ e $(K, \#_2)$ dois grupos quaisquer e suponhamos que podemos definir um homomorfismo:

$$\sigma: \begin{array}{ccc} H & \longrightarrow & \mathrm{Aut}(K) \\ h & \longmapsto & \sigma_h: \begin{array}{ccc} K & \longrightarrow & K \\ k & \longmapsto & \sigma_h(k) \end{array} \end{array}.$$

Nesta situação, dizemos que H **age sobre** K**.** Uma ação **trivial** é aquela em que $\sigma_h = \mathrm{Id}$, para todo $h \in H$, ou seja,

$$\sigma: \begin{array}{ccc} H & \longrightarrow & \mathrm{Aut}(K) \\ h & \longmapsto & \sigma_h: \begin{array}{ccc} K & \longrightarrow & K \\ k & \longmapsto & k \end{array} \end{array}.$$

Considerando uma ação $\sigma : H \to \mathrm{Aut}(K)$ e o conjunto dos pares ordenados:

$$H \times K = \{(h,k) : h \in H \text{ e } k \in K\}.$$

Então $\underset{\sigma}{\cdot}$ denotará a operação definida sobre o conjunto $H \times K$ da seguinte maneira:

$$(h,k) \underset{\sigma}{\cdot} (h',k') := (h\#_1 h', k\#_2 \sigma_h(k')), h \text{ e } h' \in H;\ k \text{ e } k' \in K.$$

Teorema 1.3 *Sejam K e H dois grupos e $\sigma : H \to \mathrm{Aut}(K)$ um homomorfismo. Então, $\left(H \times K, \underset{\sigma}{\cdot}\right)$ é um grupo.*

Definição 1.8 *O grupo $\left(H \times K, \underset{\sigma}{\cdot}\right)$ é chamado de **produto semidireto** de H por K com homomorfismo σ. Ele será denotado por $\left(H \times K, \underset{\sigma}{\cdot}\right)$ ou por $H \underset{\sigma}{\times} K$.*

Exemplo 1.7 *Consideremos $H = \langle a \rangle$ e $K = \langle b \rangle$ dois grupos cíclicos de ordem 2 e 3, respectivamente. Logo, $H \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$ e $K \simeq \frac{\mathbb{Z}}{3\mathbb{Z}}$.*

É fácil ver que $b \longmapsto b^{-1}$ define um automorfismo de K, o que induz a ação de H sobre K:

$$\begin{array}{rccc} \sigma: & H & \longrightarrow & \mathrm{Aut}(K) \\ & a & \longmapsto & \sigma_a : \begin{array}{ccc} K & \longrightarrow & K \\ b & \longmapsto & \varphi_a(b) = b^{-1} \end{array} \end{array}.$$

Portanto, temos definido um produto semidireto

$$H \underset{\sigma}{\times} K = \left\{(1,1),(1,b),(1,b^{-1}),(a,1),(a,b),(a,b^{-1})\right\}.$$

Note que este grupo não é isomorfo a $\frac{\mathbb{Z}}{6\mathbb{Z}}$, pois não e abeliano:

$$(a,1) \underset{\sigma}{\cdot} (a,b^{-1}) = (a \cdot a, 1 \cdot \sigma_a(b^{-1})) = (1,b)$$
$$(a,b^{-1}) \underset{\sigma}{\cdot} (a,1) = (a \cdot a, b^{-1} \cdot \sigma_a(1)) = (1,b^{-1}).$$

Logo, $\frac{\mathbb{Z}}{2\mathbb{Z}} \underset{\sigma}{\times} \frac{\mathbb{Z}}{3\mathbb{Z}} \simeq S_3$.

Em geral, um exemplo de um produto semidireto é o grupo diedral de ordem $2n$.

De fato, tome $H \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$ (cíclico gerado por a) e $K \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$ (cíclico gerado por x), com $n \geq 3$ e considere a ação

$$\begin{array}{rccc} \sigma: & H & \longrightarrow & \mathrm{Aut}(K) \\ & a & \longmapsto & \sigma_a : \begin{array}{ccc} K & \longrightarrow & K \\ x & \longmapsto & x^{-1} \end{array} \end{array}.$$

Portanto, $H \underset{\sigma}{\times} K \simeq D_n$, isto é, $\frac{\mathbb{Z}}{2\mathbb{Z}} \underset{\sigma}{\times} \frac{\mathbb{Z}}{n\mathbb{Z}} \simeq D_n$.

Teorema 1.4 *Sejam G, K e H grupos. Então, existe um homomorfismo $\sigma : K \to \mathrm{Aut}(H)$ tal que G seja isomorfo a $K \underset{\sigma}{\times} H$ se, e somente se, G possui subgrupos $H_1 \simeq H$ e $K_1 \simeq K$ tais que:*
1) $G = K_1H_1 = \{k_1 * h_1 \in G : k_1 \in K_1,\ h_1 \in H_1$ *e* $*$ *é a operação do grupo* $G\}$;
2) $H_1 \lhd G$;
3) $K_1 \cap H_1 = \{e\}$.

Exemplo 1.8 *Seja* G *um grupo de ordem* 15. *Mostremos que* G *é isomorfo a* $\frac{\mathbb{Z}}{15\mathbb{Z}}$.

Seja H, *um subgrupo de ordem* 5 *e seja* K *um subgrupo de ordem* 3, *tais que pelo menos um dos dois é normal a* G. *Então, temos que:*

$$G = KH = \{k * h \in G : k \in K,\ h \in H \text{ e } * \text{ é a operação do grupo } G\}.$$

De fato, pelo Teorema 1.1, KH *pode ter ordem* $1, 3, 5$ *ou* 15.

Os casos 1 *e* 3 *não ocorrem, pois* H *possui ordem* 5 *e* K *ordem* 3. *Agora suponhamos por absurdo que* KH *tenha ordem* 5. *Logo* K *é subgrupo de* H. *Porém pelo mesmo teorema,* K *deve ter ordem* 1 *ou* 5. *Absurdo, pois* K *possui ordem* 3. *Portanto* KH *possui ordem* 15 *e isto prova a igualdade acima e demonstra também que:*

$$K \cap H = \{e\}.$$

Pelo Teorema 1.4, o grupo G *é isomorfo a um produto semidireto de* $\frac{\mathbb{Z}}{5\mathbb{Z}}$ *por* $\frac{\mathbb{Z}}{3\mathbb{Z}}$ *ou a um produto semidireto de* $\frac{\mathbb{Z}}{3\mathbb{Z}}$ *por* $\frac{\mathbb{Z}}{5\mathbb{Z}}$. *Ora, o único homomorfismo de* $\frac{\mathbb{Z}}{3\mathbb{Z}}$ *em* $\mathrm{Aut}\left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right) \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$ *é o homomorfismo trivial, e também o único homomorfismo de* $\frac{\mathbb{Z}}{5\mathbb{Z}}$ *em* $\mathrm{Aut}\left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right) \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$ *é o trivial; logo, a menos de um isomorfismo o produto direto* $\left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right) \simeq \frac{\mathbb{Z}}{15\mathbb{Z}}$ *é o único grupo de ordem* 15. *Portanto o grupo* G *é isomorfo a* $\frac{\mathbb{Z}}{15\mathbb{Z}}$.

1.2 Outras Estruturas Algébricas

Um conjunto não vazio A é dito **anel** se A estiver munido de duas operações binárias denotadas por $+$ e $\cdot$ de modo que $(A, +)$ é um grupo abeliano e também valem as propriedades:
$M1 : a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todos a, b e c em A. (Associativa);
$M2 :$ Existe $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in A$. (Existência do elemento neutro);
$M3 : a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$, para todos a, b e c em A. (Propriedade Distributiva).

Se além destas propriedades, valer:
$M4 :$ Para todos a e b em A, $a \cdot b = b \cdot a$ (Propriedade Comutativa) então dizemos que o anel A é **comutativo**.

Temos que $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \underset{n}{\oplus}, \underset{n}{\odot}\right)$ é um anel, chamado **anel dos inteiros módulo** n.

Um **corpo** é um anel comutativo K tal que dado $a \in K$, se $a \neq 0$, então existe o elemento $a^{-1} \in K$ tal que $a \cdot a^{-1} = 1$.

1.3 Espaços Métricos

Definição 1.9 *Uma* ***topologia*** *no conjunto* X *é uma coleção* Γ *de subconjuntos de* X *que satisfaz:*
(a) $\emptyset, X \in \Gamma$;
(b) *Se* $A_1, ..., A_n \in \Gamma$, *então* $A_1 \cap ... \cap A_n \in \Gamma$;
(c) *Se* $A_i \in \Gamma$ *para todo* $i \in I$, *então* $\underset{i \in I}{\cup} A_i \in \Gamma$.

Os elementos de Γ são chamados de **conjuntos abertos**. O par (X, Γ) é chamado de **espaço topológico**.

Definição 1.10 *Um conjunto* M *é dito* ***espaço métrico*** *quando existe uma função* $d : M \times M \to \mathbb{R}$, *chamada* ***métrica*** *ou* ***distância*** *satisfazendo para todos* x, y *e* $z \in M$:
(i) $d(x, y) \geq 0$ *e* $d(x, y) = 0 \Leftrightarrow x = y$;
(ii) $d(x, y) = d(y, x)$;
(iii) $d(x, z) \leq d(x, y) + d(y, z)$.

Em geral denotamos o espaço métrico por (M, d), ou simplesmente M quando não acarretar ambiguidade.

O par (M, d_{01}) é um espaço métrico, onde M é um conjunto qualquer e $d_{01} : M \times M \to \mathbb{R}$ definida por

$$d_{01}(x, y) = \begin{cases} 1, & \text{se } x \neq y \\ 0, & \text{se } x = y \end{cases}$$

para todos x e $y \in M$ é uma métrica sobre M. Essa métrica é chamada de **métrica zero-um**.

A **distância de Hamming** entre $x = (x_1, ..., x_n)$ e $y = (y_1, ..., y_n) \in M^n$ é definida por

$$d_H(x, y) = \sum_{i=1}^{n} d_{01}(x_i, y_i).$$

Em um espaço métrico (M, d) chamamos um conjunto $A \subseteq M$ de **aberto**, se para todo $x \in A$ existe $\varepsilon > 0$ tal que o conjunto $B(x, \varepsilon) = \{y \in M : d(x, y) < \varepsilon\} \subseteq A$. O conjunto $B(x, \varepsilon)$ é chamado de **bola aberta de centro** x **e raio** ε. Dado $x \in M$ dizemos que x é um ponto **isolado** quando existe $\delta > 0$ tal que $B(x, \delta) = \{x\}$. Um espaço métrico é denominado **discreto** quando todos os seus pontos são isolados. É fácil provar que

$$\Gamma_d = \{A \subseteq M; \forall a \in A, \exists \varepsilon > 0 \text{ tal que } B(a, \varepsilon) \subseteq A\}$$

é uma topologia em M.

Dado um subconjunto A de um espaço métrico M, dizemos que $x \in A$ é um **ponto interior** de A se existe $\varepsilon > 0$ tal que $B(x, \varepsilon) \subseteq A$. O conjunto de todos os pontos interiores de A é demoninado de **interior** de A e denotado por $\overset{\circ}{A}$. O conjunto formado pelos pontos $x \in A$ tais que para todo $\varepsilon > 0$, $B(x, \varepsilon) \cap A \neq \emptyset$ e $B(x, \varepsilon) \cap (M - A) \neq \emptyset$ é chamado de **fronteira** de A e denotado por ∂A.

Definição 1.11 *Uma aplicação* $f : (M, d_1) \to (N, d_2)$ *entre espaços métricos é chamada de* ***contínua*** *se* $f^{-1}(A) \in \Gamma_{d_1}$ *para todo* $A \in \Gamma_{d_2}$.

Teorema 1.5 *Uma aplicação* $f : (M, d_1) \to (N, d_2)$ *entre espaços métricos é contínua se, e somente se, para todo* $a \in M$ *e para todo* $\varepsilon > 0$, *existe* $\delta > 0$ *tal que* $f(B(a, \delta)) \subseteq B(f(a), \varepsilon)$.

Definição 1.12 *Se* M *e* N *são espaços métricos com distâncias* d_M *e* d_N, *respectivamente, então dizemos que uma aplicação* $f : M \to N$ *é uma* ***isometria*** *se* f *é uma bijeção contínua e para todos* x *e* $y \in M$,

$$d_N(f(x), f(y)) = d_M(x, y).$$

Se M é um espaço métrico e $f, g : M \to M$ são isometrias de M, então f^{-1} e $g \circ f$ também são isometrias de M e, portanto, o conjunto $Iso(M)$ de todas as isometrias de M é um grupo com a operação de composição de funções, chamado o **grupo das isometrias** de M.

Definição 1.13 *Seja* $(G, *)$ *um grupo onde está definida uma função* d *que é uma métrica. Dizemos que* d *é compatível com a estrutura de* G *ou é uma* ***métrica de grupo*** *quando para todos* x *e* $y \in G$, $d(x, y) = d(x * y^{-1}, e)$, *ou em notação aditiva* $d(x, y) = d(x - y, 0)$.

Definição 1.14 *Uma* ***figura geométrica*** *é um conjunto finito e limitado de pontos numa região de um espaço métrico* M.

Denotando por I o intervalo fechado unitário $[0,1]$, um **caminho** em um espaço métrico M é uma função contínua $\alpha : I \to M$.

Definição 1.15 *Um espaço* M *é* ***conexo por caminhos*** *se dados dois pontos* x *e* y *quaisquer de* M *existe um caminho* $\alpha : I \to M$ *tal que* $\alpha(0) = x$ *e* $\alpha(1) = y$.

Consideremos pares do tipo (X, x_0), onde $x_0 \in X$ será chamado o **ponto básico** do espaço topológico X.

Dizemos que dois caminhos $\alpha, \beta : I \to M$ com as mesmas extremidades são **homotópicos**, se existe uma função contínua $H : I \times I \to M$ tal que $H(s,0) = \alpha(s)$; $H(s,1) = \beta(s)$; $H(0,t) = \alpha(0) = \beta(0)$; $H(1,t) = \alpha(1) = \beta(1)$ para todos s e $t \in I$. Denotando o fato de α ser homotópico a β por $\alpha \simeq \beta$, temos que a relação $\alpha \simeq \beta$ é uma relação de equivalência na coleção de todos os caminhos em M com as mesmas extremidades. Dado dois caminhos α e β tais que $\alpha(1) = \beta(0)$, definimos

$$\alpha\beta(s) = \begin{cases} \alpha(2s) \text{ se } s \in \left[0, \frac{1}{2}\right] \\ \\ \beta(2s-1) \text{ se } s \in \left[\frac{1}{2}, 1\right] \end{cases}$$

Portanto denotando por $[\alpha]$ a classe de equivalência de α, temos que fica bem definida uma operação no conjunto quociente por $[\alpha][\beta] = [\alpha\beta]$, desde que se considere apenas caminhos fechados em M. Considere agora um ponto $x \in M$ fixado, então um **caminho em** M **com base no ponto** x é um caminho $\alpha : I \to M$ tal que $\alpha(0) = \alpha(1) = x$. O conjunto $\pi_1(M, x)$ constituido pelas classes de homotopia de caminhos fechados em M com base no ponto x constitui um grupo para a operação definida acima. Se M é um espaço conexo por caminhos, então para todos x e $y \in M$, $\pi_1(M, x)$ e $\pi_1(M, y)$ são isomorfos, e neste caso, $\pi_1(M, x)$ é chamado de **grupo fundamental de** M **com base em** x, e denotado por $\pi_1(M)$.

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

Chamamos de **superfície** a um espaço métrico M tal que para todo $x \in M$ existem conjuntos abertos A de M contendo x, B de $\mathbb{R}^2$ e uma bijeção $f : A \to B$ tal que f e f^{-1} são contínuas.

Uma **superfície compacta orientável** de gênero $g \geq 1$ é uma superfície construida do seguinte modo: Considere um polígono regular de $4g$ lados rotulados sequencialmente do seguinte modo:

$$\gamma_1, \varepsilon_1, \gamma_1', \varepsilon_1', ..., \gamma_g, \varepsilon_g, \gamma_g', \varepsilon_g', \tag{1.1}$$

onde em cada 4−upla $\gamma_i, \varepsilon_i, \gamma_i', \varepsilon_i'$ os lados são orientados de acordo com o seguinte esquema:

$$\overset{\gamma_i}{\rightarrow} \quad \overset{\varepsilon_i}{\rightarrow} \quad \overset{\gamma_i'}{\leftarrow} \quad \overset{\varepsilon_i'}{\leftarrow}.$$

Considerando, agora, a relação de equivalencia que identifica os lados $\overset{\gamma_i}{\rightarrow}$ e $\overset{\gamma_i'}{\leftarrow}$; $\overset{\varepsilon_i}{\rightarrow}$ e $\overset{\varepsilon_i'}{\leftarrow}$ coerentemente com as setas e mantem os outros pontos fixos (ou seja, "colamos" os lados de acordo com a orientação), obtemos então a superfície conexa por caminhos, pois um polígono regular é conexo por caminhos. Na Figura 3 ilustramos o caso para $g = 3$:

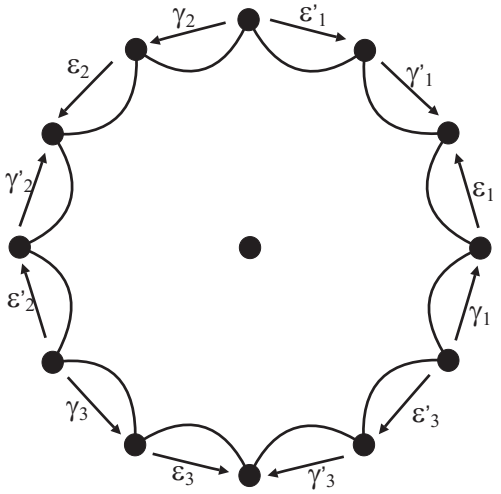


FIGURA 3: *Identificação para* $\mathsf{g} = 3$.

O aspecto da superfície é mostrado na Figura 4.

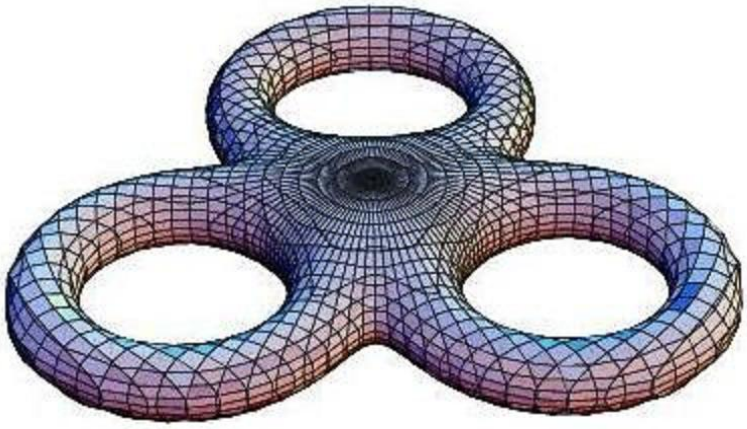


FIGURA 4: *Aspecto da superfície para* $\mathsf{g} = 3$.

Capítulo 2

Tópicos Sobre Geometria Hiperbólica

Este capítulo tem por objetivo a apresentação das principais definições e resultados da Geometria Hiperbólica que estão relacionados aos próximos capítulos. Nossa abordagem não traz demonstrações. Textos de geometria hiperbólica que contém de forma complementar os tópicos aqui apresentados são, por exemplo: [4], [13], [1] e [24].

2.1 Isometrias

Isometrias no Modelo do Semiplano H^2

Seja $\mathbb{C}$ o plano complexo. Usamos as notações usuais para as partes reais e imaginárias de $z = x + iy \in \mathbb{C}$, $\mathrm{Re}(z) = x$ e $\mathrm{Im}(z) = y$. Tomemos a parte superior do plano complexo, $H^2 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Munido da métrica riemanniana

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

também chamada de **métrica hiperbólica do semiplano**. Temos, assim, o modelo do semiplano de Poincaré ou modelo de Lobachewsky para a Geometria Hiperbólica.

Seja $I = [0, 1]$ e $\gamma : I \longrightarrow H^2$ um caminho diferenciável por partes, $\gamma(t) = z(t) = x(t) + iy(t) \in H^2$ com $t \in I$. Então, o comprimento hiperbólico $h(\gamma)$ é dado por

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

A distância hiperbólica $\rho(z, w)$ entre dois pontos z e $w \in H^2$ é definida pela fórmula $\rho(z, w) = \inf\{h(\gamma)\}$, onde o ínfimo é tomado sobre todo γ ligando os pontos z e $w \in H^2$. Logo, para z e $w \in H^2$:

$$d_{H^2}(z, w) = \rho(z, w) = \ln\left(\frac{|z-\overline{w}|+|z-w|}{|z-\overline{w}|-|z-w|}\right).$$

Com esta métrica, o par (H^2, d_{H^2}) constitui um espaço métrico, que é um modelo para o **plano hiperbólico**.

O "bordo" do modelo H^2, que é o conjunto

$$\partial H^2 = \{(x, y) : x \text{ e } y \in \mathbb{R} \text{ e } y = 0\} \cup \{\infty\}$$

é definido como sendo a **fronteira ideal** de H^2. Utilizamos, quando conveniente, a notação

$$\widehat{H^2} = H^2 \cup \partial H^2$$

para denotar a união do modelo e sua fronteira ideal. Um ponto na fronteira ideal de um modelo é dito **ponto ideal**.

Consideremos o grupo linear especial, denotado por $SL(2,\mathbb{R})$, composto pelas matrizes reais $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ com $\det(A) = ad - bc = 1$, no qual a operação considerada é a multiplicação usual de matrizes.

Vamos denotar por M o conjunto de todas as transformação de Möbius, ou seja, transformações fracionais lineares complexas da forma:

$$\begin{array}{rccc} T: & H^2 & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \frac{az+b}{cz+d} \end{array} \text{ tal que } a, b, c \text{ e } d \in \mathbb{R} \text{ e } ad - bc = 1.$$

Notemos que $T(H^2) = H^2$. Nestas condições M é um grupo para a operação de composição de funções de tal modo que a composição de duas transformações corresponde ao produto de duas matrizes de $SL(2,\mathbb{R})$ e a inversa corresponde à matriz inversa.

De fato: se $T_1(z) = \frac{a_1 z+b_1}{c_1 z+d_1}$ e $T_2(z) = \frac{a_2 z+b_2}{c_2 z+d_2}$, então $T_1 \circ T_2(z) = \frac{(a_1a_2+b_1c_2)z+a_1b_2+b_1d_2}{(c_1a_2+d_1c_2)z+c_1b_2+d_1d_2}$, que corresponde ao produto $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} . \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$. Também $T^{-1}(z) = \frac{dz-b}{-cz+a}$, que corresponde à matriz $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}$. Por outro lado, como $T(z) = \frac{(-a)z+(-b)}{(-c)z+(-d)}$ resulta que $-\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ também representa T, e assim, podemos considerar que

$$\begin{array}{rccc} \phi: & SL(2,\mathbb{R}) & \longrightarrow & M \\ & \begin{bmatrix} a & b \\ c & d \end{bmatrix} & \longmapsto & T(z) = \frac{az+b}{cz+d} \end{array}$$

é um homomorfismo sobrejetor de grupos. Além disso, como $Ker(\phi) = \{\pm Id_2\}$, pelo Teorema do Homomorfismo

$$PSL(2,\mathbb{R}) = \frac{SL(2,\mathbb{R})}{\{\pm Id_2\}} \simeq M.$$

que é chamado **grupo topológico especial linear projetivo** das matrizes 2×2 sobre $\mathbb{R}$, isto é,

$$PSL(2,\mathbb{R}) = \left\{ T(z) = \frac{az+b}{cz+d} \in M : \ a, b, c \text{ e } d \in \mathbb{R} \text{ e } ad - bc = 1 \right\}.$$

Podemos ainda estender o domínio de T a $\overline{H^2} = H^2 \cup \mathbb{R} \cup \{\infty\}$. Os pontos de $\mathbb{R} \cup \{\infty\}$ são chamados de pontos ideais de H^2, enquanto que os pontos de H^2 são chamados de pontos ordinários. Para isto definimos:

$T(\infty) = \infty$, no caso $c = 0$;

$T(\infty) = \frac{a}{c}$, no caso $c \neq 0$;

$T\left(-\frac{d}{c}\right) = \infty$, no caso $c \neq 0$;

$T(z) = \frac{az+b}{cz+d}$ nos demais pontos de $\mathbb{R}$.

A importância destas definições encontra-se no fato de que as transformações T são isometrias que preservam orientação e, portanto, pertencem ao $Iso(H^2)$.

Definimos agora o grupo

$$PS^*L(2,\mathbb{R}) = \frac{SL^*(2,\mathbb{R})}{\{\pm Id_2\}},$$

sendo $SL^*(2,\mathbb{R})$ o grupo das matrizes reais 2×2 com determinante ± 1. Com esta definição, $PSL(2,\mathbb{R})$ é subgrupo de índice dois de $PS^*L(2,\mathbb{R})$ e temos o seguinte resultado que estende o fato de $PSL(2,\mathbb{R})$ ser isomorfo ao grupo das transformações de Möbius M.

Proposição 2.1 $\mathrm{Iso}(H^2)$ *é isomorfo ao* $PS^*L(2,\mathbb{R})$.

Como consequência, podemos pensar em $PS^*L(2,\mathbb{R})$ como sendo o grupo composto por transformações de Möbius, ou seja,

$$\mathrm{Iso}(H^2) = \left\langle T(z) = \frac{az+b}{cz+d},\ \varphi(z) = -\overline{z} : z \in H^2;\ a,b,c \text{ e } d \in \mathbb{R} \text{ e } ad-bc=1 \right\rangle, T \in PSL(2,\mathbb{R}).$$

Notemos que φ é uma reflexão pelo eixo imaginário no plano $\mathbb{C}$.

O **grupo ortogonal** denotado por $O(\mathbb{R}^2)$, consiste das matrizes $A \in SL^*(2,\mathbb{R})$ tais que $A \cdot A^t = Id_2$, onde A^t denota a matriz transposta da matriz A, e portanto $\det(A)\cdot\det(A^t) = \det(Id_2) = 1$ e consequentemente $(\det(A)) = \pm 1$, assim $O(\mathbb{R}^2) \leq SL^*(2,\mathbb{R})$. O **grupo ortogonal especial** $SO(\mathbb{R}^2) = \left\{A \in O(\mathbb{R}^2) : \det(A) = 1\right\}$. Os elementos destes grupos são simetrias de qualquer círculo centrado na origem e no mesmo sentido que uma circuferência pode ser considerada um limite de polígonos regulares, os grupos $O(\mathbb{R}^2)$ e $SO(\mathbb{R}^2)$ podem ser considerados como limites de D_M e do $M-PSK$, respectivamente, quando $M \to \infty$.

Classificação de Isometrias em H^2

Há três tipos distintos de isometrias $T(z) = \frac{az+b}{cz+d}$ em $PSL(2,\mathbb{R})$, sendo $ad-bc=1$, diferenciados pelo valor absoluto do traço da matriz associada $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, que chamaremos de traço de T, indicado por $\mathrm{tr}(T) = |a+d|$.
Se $\mathrm{tr}(T) < 2$, T é chamada **isometria elíptica** (ou **rotação hiperbólica**);
Se $\mathrm{tr}(T) = 2$, T é chamada **isometria parabólica**;
Se $\mathrm{tr}(T) > 2$, T é chamada **translação hiperbólica**.

Diremos ainda que duas matrizes $A, B \in SL(2,\mathbb{R})$ são **conjugadas** quando existir $M \in SL(2,\mathbb{R})$ tal que $A = MBM^{-1}$. De modo análogo, duas isometrias $T_A, T_B \in PSL(2,\mathbb{R})$ serão ditas conjugadas quando suas matrizes correspondentes A e B assim o forem. Nesse caso, existe $T_M \in PSL(2,\mathbb{R})$ tal que $T_A = T_M \circ T_B \circ T_M^{-1}$.

Isometrias no Modelo do Disco U

De modo análogo ao do modelo do semiplano, tomemos o disco unitário com centro na origem do plano $\mathbb{C}$, $U = \left\{(x,y) : x \text{ e } y \in \mathbb{R} \text{ e } x^2+y^2 < 1\right\}$. Munido da métrica riemanniana

$$ds = \frac{2\sqrt{dx^2+dy^2}}{1-(x^2+y^2)},$$

também chamada de **métrica hiperbólica do disco unitário**. Temos, assim, o modelo do disco unitário de Poincaré ou modelo de Lobachewsky para a Geometria Hiperbólica.

Seja $I = [0,1]$ e $\gamma : I \longrightarrow U$ um caminho diferenciável por partes, $\gamma(t) = z(t) = x(t) + iy(t) \in U$ com $t \in I$. Então, o comprimento hiperbólico $h(\gamma)$ é dado por

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

A distância hiperbólica $\rho(z,w)$ entre dois pontos z e $w \in U$ é definida pela fórmula $\rho^*(z,w) = \inf\{h(\gamma)\}$, onde o ínfimo é tomado sobre todo γ ligando os pontos z e $w \in U$. Logo, para z e $w \in U$:

$$d_U(z,w) = \rho^*(z,w) = \ln\left(\frac{|1-z\overline{w}|+|z-w|}{|1-z\overline{w}|-|z-w|}\right).$$

Com esta métrica, o par (U, d_U) constitui um espaço métrico, que é um modelo para o **plano hiperbólico**.

Consideremos o grupo linear especial sobre $\mathbb{C}$, denotado por $SL(2,\mathbb{C})$, composto pelas matrizes complexas $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ com $\det(M) = ad - bc = 1$, no qual a operação considerada é a multiplicação usual de matrizes.

O "bordo" do modelo U, que é o conjunto

$$\partial U = \{(x,y) : x \text{ e } y \in \mathbb{R} \text{ e } x^2 + y^2 = 1\}$$

é definido como sendo a **fronteira ideal** de U. Utilizamos, quando conveniente, a notação

$$\widehat{U} = U \cup \partial U$$

para denotar a união do modelo e sua fronteira ideal. Um ponto na fronteira ideal de um modelo é dito **ponto ideal**.

Para que uma transformação de Möbius

$$\begin{array}{rccc} T: & U & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \frac{az+b}{cz+d} \end{array}$$

tenha imagem em U, é necessário que $b = \overline{c}$ e $d = \overline{a}$ e, assim, teremos

$$\begin{array}{rccc} T: & U & \longrightarrow & U \\ & z & \longmapsto & \frac{az+\overline{c}}{cz+\overline{a}} \end{array}$$

com $a\overline{a} - c\overline{c} = 1$.

O conjunto

$$A = \left\{ \begin{bmatrix} a & \overline{c} \\ c & \overline{a} \end{bmatrix} \in SL(2,\mathbb{C}) \right\} \subset SL(2,\mathbb{C})$$

é, na verdade, um subgrupo de $SL(2,\mathbb{C})$ quando consideramos a operação de composição herdada de $SL(2,\mathbb{C})$.

Como no caso do semiplano, o conjunto de transformações de Möbius acima munido da operação de composição usual forma um grupo de tal modo que a composição de duas transformações corresponde ao produto de duas matrizes de A e a inversa corresponde à matriz inversa. Além disso, cada transformação T da forma acima pode ser representada por um par de matrizes $\pm M \in A$. Logo

$$PSL(2,\mathbb{C}) \simeq \frac{A}{\{\pm \mathrm{Id}_2\}}$$

e podemos demonstrar que

$$\mathrm{Iso}(U) = \left\langle T(z) = \frac{az+\overline{c}}{cz+\overline{a}},\ \varphi(z) = -\overline{z} : \ a \text{ e } b \in \mathbb{C} \text{ e } a\overline{a} - c\overline{c} = 1 \right\rangle,\ T \in PSL(2,\mathbb{C}).$$

Como em H^2, notemos que φ é uma reflexão pelo eixo imaginário no plano $\mathbb{C}$.

A classificação de isometrias em $PSL(2,\mathbb{C})$ segue de modo análogo à realizada para $PSL(2,\mathbb{R})$.

2.2 Grupos Fuchsianos

Iniciamos o estudo dos grupos fuchsianos com o conceito de grupo discreto de isometrias. Fizemos o estudo para U; lembrando, entretanto, que tudo que foi feito em U possui análogo em H^2:

Começamos com a estrutura de grupo topológico em $PSL(2,\mathbb{C})$.

Introduzimos uma norma em $PSL(2,\mathbb{C})$ do seguinte modo: seja

$$\begin{array}{rccc} f: & U & \longrightarrow & U \\ & z & \longmapsto & \frac{az+\overline{c}}{cz+\overline{a}} \end{array}$$

isometria em U.

Seja $M = \begin{bmatrix} a & \overline{c} \\ c & \overline{a} \end{bmatrix} \in SL(2,\mathbb{C})$ matriz associada a $f(z) = \frac{az+\overline{c}}{cz+\overline{a}} \in PSL(2,\mathbb{C})$.

Definimos sua norma por

$$\|f\| = \|M\| = \sqrt{|a|^2 + |\overline{c}|^2 + |c|^2 + |\overline{a}|^2} = \sqrt{2|a|^2 + 2|c|^2}.$$

Seja $N \in SL(2,\mathbb{C})$ associada a $g \in PSL(2,\mathbb{C})$. Com a distância induzida $d(f,g) = \|M - N\|$, $PSL(2,\mathbb{C})$ é um **grupo topológico** e a topologia é a induzida pela norma definida acima (é a topologia do $\mathbb{R}^4$).

Definição 2.1 *Um subgrupo* G *de* $PSL(2,\mathbb{C})$ *é* ***discreto*** *quando a topologia induzida de* $PSL(2,\mathbb{C})$ *sobre* G *é discreta.*

Percebemos que um subgrupo discreto de isometrias de U constitui um conjunto discreto de pontos em $\mathbb{R}^4$. Temos a seguinte caracterização dos subgrupos discretos de $PSL(2,\mathbb{C})$.

Proposição 2.2 $G \leq PSL(2,\mathbb{C})$ *é discreto se, e somente se,* $T_n \to Id$, $T_n \in G$ *(convergência na norma definida acima) implica* $\exists n_0 \in \mathbb{N}$ *tal que* $T_n = Id$ *para* $n > n_0$.

Mostremos um exemplo de um grupo não discreto.

Seja s um número irracional. O conjunto $G = \left\{e^{n\pi si} : n \in \mathbb{Z}\right\} \subseteq \mathbb{C}$ com a operação usual de multiplicação de números complexos é um grupo. De fato,

(i) Sejam $e^{n_1\pi si}$, $e^{n_2\pi si}$ e $e^{n_3\pi si}$ em G.

$$\begin{aligned} & e^{n_1\pi si}.(e^{n_2\pi si}.e^{n_3\pi si}) \\ &= (\cos(n_1\pi s) + i\,\mathrm{sen}(n_1\pi s)).((\cos(n_2\pi s) + i\,\mathrm{sen}(n_2\pi s)).(\cos(n_3\pi s) + i\,\mathrm{sen}(n_3\pi s))) \\ &= ((\cos(n_1\pi s) + i\,\mathrm{sen}(n_1\pi s)).(\cos(n_2\pi s) + i\,\mathrm{sen}(n_2\pi s))).(\cos(n_3\pi s) + i\,\mathrm{sen}(n_3\pi s)) \\ &= \left(e^{n_1\pi si}.e^{n_2\pi si}\right).e^{n_3\pi si}. \end{aligned}$$

(ii) Seja $e^{n\pi si} \in G$.

$$e^{n\pi si}.e' = e'.e^{n\pi si} = e^{n\pi si} \Rightarrow e' = 1,$$

que é um elemento de G. Logo existe $e' = 1$ tal que

$$e^{n\pi si}.1 = 1.e^{n\pi si} = e^{n\pi si},\ \forall e^{n\pi si} \in G.$$

(iii) Seja $e^{n\pi si} \in G$.

$$\begin{aligned} e^{n\pi si}.(e^{n\pi si})^* = (e^{n\pi si})^*.e^{n\pi si} = 1 \\ \Rightarrow (e^{n\pi si})^* = e^{-n\pi si}, \end{aligned}$$

que é um elemento de G.

Portanto G é um grupo.

Provemos agora que para todo $n \in \mathbb{Z}$ os pontos $e^{n\pi si}$ são distintos dois a dois, isto é, G é infinito.

Suponhamos, por absurdo, que existe $j \in \mathbb{Z}$ tal que $e^{j\pi si} = e^{(n\pi s+2\pi t)i}$, para algum $n \in \mathbb{Z}$ e $j \in \mathbb{Z} - \{0\}$.

$$js\pi = ns\pi + 2\pi t \Rightarrow j = n + \frac{2t}{s}.$$

Absurdo, pois $j = n + \frac{2t}{s} \notin \mathbb{Z}$.

Logo, G é um grupo infinito contido em S^1 que é compacta. Pelo Teorema de Bolzano-Weierstrass toda sequência limitada em $\mathbb{R}^n$ possui uma subsequência convergente, isto é, G possui um ponto de acumulação.

Portanto G não é discreto.

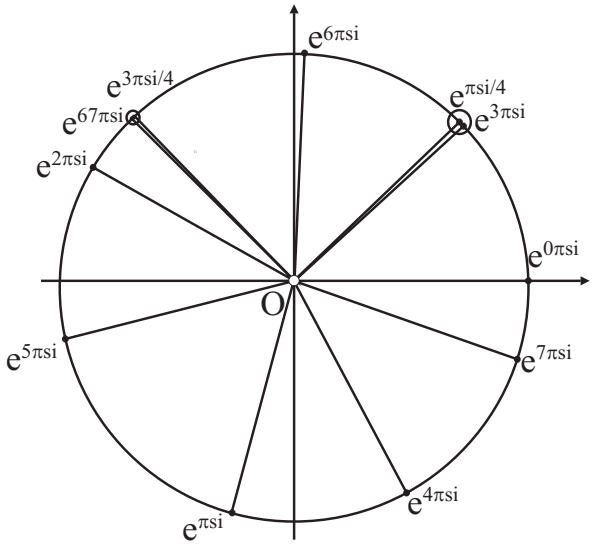


FIGURA 5: *Para* $s = \sqrt{2}$.

Definição 2.2 *Um* ***grupo fuchsiano*** *é um subgrupo discreto de* $PSL(2,\mathbb{C})$ *(ou* $PSL(2,\mathbb{R})$*).*

Proposição 2.3 *Se* $T \in PSL(2,\mathbb{R})$ *(ou* $PSL(2,\mathbb{C})$*) é isometria parabólica ou translação hiperbólica, então* $\langle T \rangle$ *é fuchsiano.*

2.3 Área Hiperbólica e Teorema de Gauss-Bonnet

Nesta seção, abordamos o conceito de área nos modelos de Poincaré e apresentamos um impressionante resultado, provando que a área hiperbólica de um triângulo hiperbólico depende apenas de seus ângulos internos. Este resultado é uma consequência de um famoso teorema chamado Teorema de Gauss-Bonnet que iremos enunciar sem detalhes, pois em nosso trabalho utilizaremos apenas a parte citada acima. Para maiores detalhes consulte [5].

Definição 2.3 *Seja* $A \subset H^2$*. Definimos a área hiperbólica de* A *como sendo*

$$\mu_H(A) = \int_A \frac{1}{y^2} dxdy$$

se a integral estiver bem definida.

Se $A \subset U$*, a definição é análoga:*

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

Observamos que áreas hiperbólicas são invariantes por isometrias de $\mathrm{Iso}(H^2)$ e $\mathrm{Iso}(U)$.

Definimos o **ângulo hiperbólico** entre duas semi-retas hiperbólicas r e s de mesma origem nos modelos de Poincaré como sendo o ângulo (euclidiano) entre suas tangentes (euclidianas) no ponto de intersecção (Figura 6). Assim, a medida de ângulo é feita exatamente como no sentido euclidiano e, portanto, obedece os axiomas relativos a tais medições.

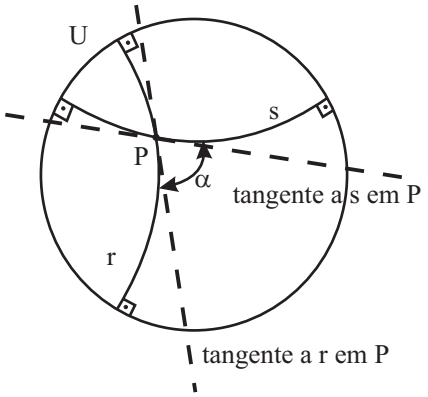


FIGURA 6: *Ângulo hiperbólico no modelo do disco de Poincaré.*

Polígonos em H^2 ou U são definidos como sendo curvas fechadas compostas por um número finito de segmentos geodésicos. No entanto, na geometria hiperbólica, devemos atentar ao fato da possibilidade de existência de vértices na fronteira ideal do modelo (vértices de ângulo zero). Com esta observação, para encontrarmos a área destes polígonos precisamos do seguinte resultado.

Teorema 2.1 ***(Teorema de Gauss-Bonnet - Versão local)*** *Sejam S superfície regular, $R \subset S$ região simples com fronteira α orientada positivamente e parametrizada pelo comprimento de arco em cada arco regular de α. Sejam $\alpha(t_0), ..., \alpha(t_k)$ vértices de α e $\theta_0, ..., \theta_k$ ângulos externos (orientados) de α. Então:*

$$\sum_{i=0}^{k} \int_{t_i}^{t_{i+1}} k_g(t)\,dt + \int_R K(P)\,d\sigma + \sum_{i=0}^{k} \theta_i = 2\pi,$$

sendo k_g curvatura geodésica de cada arco regular e K curvatura gaussiana de S.

A principal consequência deste teorema é a obtenção de áreas em superfícies regulares. Em nosso trabalho, o plano de interesse é o hiperbólico cuja curvatura gaussiana K é igual a -1. Logo temos o reguinte resultado.

Corolário 2.1 *Se Δ é triângulo hiperbólico com ângulos internos α, β, γ, então*

$$\mu_{P_h}(\Delta) = \pi - (\alpha + \beta + \gamma)$$

sendo $P_h = H^2$ ou U.

2.4 Grupos com Ação Propriamente Descontínua

As definições que seguem são válidas para espaços mais gerais que os modelos de Poincaré, por isso serão introduzidas de modo genérico.

Definição 2.4 *Dizemos que uma aplicação contínua $F : M \to M$, sendo M espaço métrico, é um **homeomorfismo** sobre $F(M)$ se F é injetiva e a inversa $F^{-1} : F(M) \to M$ é contínua. Neste caso, M e $F(M)$ são **conjuntos homeomorfos**.*

Uma família $\{A_\alpha : \alpha \in \mathcal{F}\}$ de subconjuntos de um espaço métrico M ($\mathcal{F}$ é um conjunto de índices) é chamada de **localmente finita**, quando, para qualquer conjunto compacto $K \subset M$, temos $A_\alpha \cap K \neq \emptyset$ somente para um número finito de índices $\alpha \in \mathcal{F}$.

Seja M um espaço métrico. Se $x \in M$ e G é grupo de homeomorfismos em M, dizemos que $G_x = \{g(x) : g \in G\}$ é **órbita** de x por G. A **multiplicidade** de um elemento G_x é a ordem do **estabilizador** de x; ou seja, $|E_G(x)|$, sendo $E_G(x) = \{g \in G : g(x) = x\}$ (subgrupo de G que fixa x).

Definição 2.5 *Dizemos que G age de maneira **propriamente descontínua** em M, quando a órbita de qualquer ponto $x \in M$ é localmente finita.*

Um espaço métrico M é **localmente compacto**, quando todo ponto x de M possui uma vizinhança compacta, ou seja, $\exists K_x$ compacto tal que $x \in K_x$.

O resultado abaixo estabelece equivalências importantes envolvendo os conceitos definidos acima.

Proposição 2.4 *Seja G um grupo de homeomorfismos de um espaço métrico M localmente compacto. São equivalentes:*
- A ação de G é propriamente descontínua;
- Para qualquer $x \in M$, existe uma vizinhança aberta V_x de x tal que $g(V_x) \cap V_x \neq \emptyset$ apenas para uma quantidade finita de elementos $g \in G$;
- Para qualquer $x \in M$, $\exists V_x$ aberto contendo x tal que $(g(V_x) \cap V_x \neq \emptyset \Rightarrow g(x) = x, \forall g \in G)$;
- Seja $K \subset M$ compacto. Temos $g(K) \cap K \neq \emptyset$ apenas para um número finito de elementos $g \in G$.

Retornando aos modelos de Poincaré, temos os resultados seguintes.

Proposição 2.5 (i) *Se $x \in H^2$ e $K \subset H^2$ é compacto, então o conjunto*

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

é compacto (topologia de $PSL(2, \mathbb{R})$);
(ii) *Se $G \leq PSL(2, \mathbb{R})$ tem ação propriamente descontínua em H^2, então o conjunto*

$$\left\{x \in H^2 : \exists T \in G \text{ com } T(x) = x\right\}$$

é discreto.

O seguinte resultado é central.

Proposição 2.6 *$G \leq PSL(2, \mathbb{R})$ é fuchsiano se, e somente se, sua ação for propriamente descontínua em H^2.*

Desta proposição e das equivalências acima (Proposição 2.4), resulta que $G \leq PSL(2, \mathbb{R})$ é fuchsiano se, e somente se, a órbita de qualquer ponto de H^2 por G for discreta.

Definição 2.6 *O conjunto de todos os pontos de acumulação das órbitas de pontos $x \in H^2$ por um grupo fuchsiano G é chamado de **conjunto limite** de G e indicado por $\Lambda(G)$.*

Na verdade, $\Lambda(G)$ pode ser obtido apenas pelos pontos de acumulação de uma órbita arbitrária qualquer, pois os pontos de acumulação de qualquer órbita em $\widehat{H^2}$ são os mesmos.

De imediato, temos que se G é fuchsiano, então $\Lambda(G) \subseteq \widehat{H^2}$. Além disso, $\Lambda(G)$ é invariante por elementos de G.

Baseados nestes apontamentos, dizemos que um grupo fuchsiano é de **primeiro tipo** se $\Lambda(G) = \partial H^2$ e de **segundo tipo** caso contrário.

Finalizando, um resultado interessante: $\Lambda(PSL(2, \mathbb{Z})) = \partial H^2$.

2.5 Região Fundamental e Domínio de Dirichlet

Definição 2.7 *Sejam* M *um espaço métrico e* G *um grupo de homeomorfismos agindo de modo propriamente descontínuo em* M*. Dizemos que um subconjunto fechado* $F \subset M$ *é* ***domínio fundamental*** *de* G *se:*
(i) $\bigcup_{g \in G} g(F) = M$;
(ii) $\overset{\circ}{F} \cap g(\overset{\circ}{F}) = \emptyset,\ g \neq Id$;
(iii) $\overset{\circ}{F} \neq \emptyset$.

Em virtude de $\{g(F) : g \in G\}$ formar um ladrilhamento de M, chamamos F, às vezes, de **ladrilho**.

O próximo passo é bastante proveitoso por estabelecer uma relação entre domínios fundamentais de grupos.

Proposição 2.7 *Sejam:*
- M *espaço métrico;*
- G *grupo de isometrias agindo de modo propriamente descontínuo em* M*;*
- F *domínio fundamental de* G*;*
- $K \leq G$ *de índice* $n < \infty$ *e* $g_1, ..., g_n \in G$ *tais que* $G = g_1K \cup ... \cup g_nK$ *seja decomposição de* G *em classes laterais.*

Então $F' = g_1(F) \cup ... \cup g_n(F)$ *é domínio fundamental de* K.

Proposição 2.8 *Dois domínios fundamentais* F_1 *e* F_2 *de um grupo fuchsiano* G *tal que* $\mu_H(F_1) < \infty$ *e* $\mu_H(\partial F_1) = \mu_H(\partial F_2) = 0$ *são tais que* $\mu_H(F_1) = \mu_H(F_2)$.

Como conseqüência dos últimos resultados, temos: se K é um subgrupo de índice $n < \infty$ do grupo fuchsiano G tal que F e F' são domínios fundamentais de G e K respectivamente, $\mu_H(F) < \infty$ e $\mu_H(\partial F) = 0$, então $\mu_H(F') = n\mu_H(F)$.

Como vimos, a órbita de um ponto $p \in H^2$ por um grupo fuchsiano G é discreta. Isto nos remete ao estudo de um tipo especial de conjunto que, a primeira vista, é um candidato natural a domínio fundamental; porém, com propriedades importantes. É o domínio de Dirichlet.

Seja $\mathbb{E}$ um espaço euclidiano ou hiperbólico.

Definição 2.8 *Sejam* G *grupo fuchsiano e* $p \in \mathbb{E}$ *tal que* $T(p) \neq p;\ \forall T \in G$*. O conjunto*

$$D_p(G) = \{x \in \mathbb{E} : d_{\mathbb{E}}(p, x) \leq d_{\mathbb{E}}(T(p), x),\ \forall T \in G\}$$

é chamado de ***domínio de Dirichlet*** *(ou* ***região de Voronoi****) de* G *em* p.

Exemplo 2.1 *A representação no plano* $\mathbb{R}^2$ *dos elementos de um grupo cíclico* $M - PSK$ *com* M *elementos é um conjunto de sinais chamado de* ***Código de Slepian*** *correspondente a um esquema de modulação por fase [22]. As regiões de Voronoi são as regiões internas entre pares de semirretas (mediatrizes dos pontos* ζ^n *e* ζ^{n+1}, $\zeta = e^{\frac{2\pi i}{M}}$*), passando pela origem (Figura 7).*

Proposição 2.9 *Todo domínio de Dirichlet de um grupo fuchsiano em um ponto de* H^2 *é domínio fundamental.*

Como conseqüência deste resultado, todo domínio de Dirichlet é convexo (geodesicamente).

Os próximos resultados mostram como os domínios de Dirichlet podem ser úteis para a compreensão da estrutura de um grupo fuchsiano.

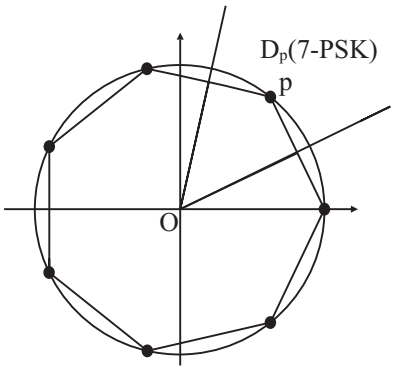


FIGURA 7: *Região de Voronoi do grupo cíclico* $7-\mathsf{PSK}$ *em* $\mathfrak{p}=e^{\frac{2\pi i}{7}}$.

Proposição 2.10 *Sejam* G *grupo fuchsiano e* $\mathfrak{p}\in H^2$ *tal que* $D_\mathfrak{p}(G)$ *é domínio de Dirichlet.*
(i) *O ladrilhamento proveniente de um domínio de Dirichlet de* G *em* $\mathfrak{p}$*;* $\{T(D_\mathfrak{p}(G)) : T\in G\}$*; é localmente finito.*
(ii) *Dado* $x\in \partial D_\mathfrak{p}(G)$*; fronteira de* $D_\mathfrak{p}(G)$*;* $\exists T\in G$*,* $T\neq Id$*, tal que* $T(x)\in \partial D_\mathfrak{p}(G)$.

Estabeleceremos uma distinção entre os vértices da fronteira (composta por geodésicas, raios ou segmentos geodésicos) de um domínio de Dirichlet.

O ponto de encontro de duas arestas distintas de $D_\mathfrak{p}(G)$ é chamado de **vértice ordinário** de $D_\mathfrak{p}(G)$**.** Se G possuir isometrias elípticas de ordem dois, então os pontos fixos destas isometrias estão sobre as arestas da fronteira de $D_\mathfrak{p}(G)$ (e não coincidem com os vértices ordinários). A estes pontos fixos, chamamos de **vértice singulares** de $D_\mathfrak{p}(G)$.

Proposição 2.11 *Sejam* G *grupo fuchsiano,* $\mathfrak{p}\in H^2$ *e* $D_\mathfrak{p}(G)$ *domínio de Dirichlet de* G *em* $\mathfrak{p}$.
(i) *Dada uma aresta* A *de* $D_\mathfrak{p}(G)$*,* $\exists T\in G$*,* $T\neq Id$*; tal que* $A\subset D_\mathfrak{p}(G)\cap T(D_\mathfrak{p}(G))$.
(ii) *Seja* v *vértice de* $D_\mathfrak{p}(G)$*. Temos:*
v *é vértice ordinário de* $D_\mathfrak{p}(G)$ *se, e somente se,* $\exists T$ *e* $T'\in G; T$ *e* $T'\neq Id$ *tais que* $v=D_\mathfrak{p}(G)\cap T(D_\mathfrak{p}(G))\cap T'(D_\mathfrak{p}(G))$**.**

Dizemos que duas arestas A_1 e A_2 de um domínio de Dirichlet $D_\mathfrak{p}(G)$ são equivalentes quando $\exists T\in G$ tal que $T(A_1)=A_2$. É imediato verificar que esta é uma relação de equivalência. Temos o resultado seguinte envolvendo tal relação.

Proposição 2.12 *Cada classe de equivalência de arestas de um domínio de Dirichlet possui dois elementos.*

Por conseguinte, se $D_\mathfrak{p}(G)$ possui uma quantidade finita de arestas, estas necessariamente devem ocorrer em número par. Além disso, dado A_1 aresta de $D_\mathfrak{p}(G)$, $\exists! T\in G$ e $\exists! A_2$ aresta de $D_\mathfrak{p}(G)$ tal que $T(A_1)=A_2$. Por esse motivo, chamamos A_1 e A_2 de **arestas emparelhadas** (ou **identificadas**).

Teorema 2.2 *Seja* Γ *um grupo fuchsiano, então existe uma região fundamental convexa com um número finito de lados se, e somente se,* Γ *é finitamente gerado. Se* F *é um domínio de Dirichlet de* Γ *nestas condições e* $\{T_i\}_{i\in I}$ *é o subconjunto de* Γ *consistindo dos elementos que emparelham os lados de* F*, então:*

$$\Gamma=\left\langle\{T_i\}_{i\in I}\right\rangle.$$

É conveniente também definirmos uma classe de equivalência especial de vértices de um domínio de Dirichlet: os ciclos.

Chamamos de **ciclo** o conjunto

$$C=\{T(x) : x \text{ e } T(x) \text{ são vértices de } D_\mathfrak{p}(G)\}.$$

Teorema 2.3 *Seja* $D_p(G)$ *a região de Dirichlet de* G *em* p. *Sejam* $\theta_1, ..., \theta_t$ *ângulos internos congruentes dos vértices de* $D_p(G)$. *Seja* m *ordem do estabilizador em* G *de um destes vértices. Então* $\theta_1 + ... + \theta_t = \frac{2\pi}{m}$.

2.6 Assinaturas de Grupos Fuchianos

Trabalhamos, neste tópico, com um pouco de espaços quocientes. Particularmente, com $\frac{P_h}{G}$ sendo $P_h = H^2$ ou U e G grupo fuchsiano.

Definição 2.9 *Dizemos que um grupo fuchsiano* G *é* ***co-compacto*** *se* $\frac{P_h}{G}$ *for uma superfície compacta.*

Consideremos G co-compacto e $D_p(G)$ domínio de Dirichlet compacto de G em p. Temos $D_p(G)$ com um número finito de vértices e, portanto, com um número finito de ciclos. Consideremos um eventual ciclo C que possui vértices (ordinários ou singulares) fixados por isometrias elípticas de G. Como os estabilizadores de vértices de um mesmo ciclo são conjugados entre si, estes possuem a mesma ordem nos vértices de um ciclo. Chamemos de m a ordem de um estabilizador de um vértice de C. De modo análogo ao ciclo C, tomemos todos os ciclos de $D_p(G)$ que possuem vértices fixos por isometrias elípticas de G e chamemos de $m_1, ..., m_r$ a ordem de seus estabilizadores de vértices.

Iremos chamar de **assinatura** de G a $(r+1)$−upla $(g, m_1, ..., m_r)$ sendo $m_1, ..., m_r$ obtidos como no parágrafo anterior e g o gênero de $\frac{P_h}{G}$.

Enunciamos abaixo um importante (e impressionante) resultado envolvendo assinaturas.

Teorema 2.4 (i) *Seja* G *grupo fuchsiano co-compacto com assinatura* $(g, m_1, ..., m_r)$. *Temos*

$$\mu_H\left(\frac{P_h}{G}\right) = 2\pi\left(2(g-1) + \sum_{k=1}^{r}\left(1 - \frac{1}{m_k}\right)\right).$$

(ii) *Dados inteiros* g *e* $r \geq 0$, $m_k \geq 2$ *tais que*

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

então existe G, *grupo fuchsiano co-compacto, com assinatura* $(g, m_1, ..., m_r)$.

Como consequência do resultado acima, toda superfície compacta S com gênero $g \geq 2$ pode ser modelada no plano hiperbólico (ou seja, $\exists G$ grupo fuchsiano tal que $S \equiv \frac{P_h}{G}$). Esta consequência pode ser encontrada em [23] e é importantíssima para o desenvolvimento de códigos geometricamente uniformes no plano hiperbólico.

Se G não possui elementos elípticos, então a ação de G em P_h é livre, ou seja, a projeção $p : P_h \to P_h/G$ é uma **aplicação de recobrimento**:

Definição 2.10 *Sejam um plano hiperbólico* P_h *e uma superfície compacta orientável* P_h/G *de gênero* g. *Dizemos que* P_h *é um* ***recobrimento*** *de* P_h/G *se existe uma aplicação* $p : P_h \to P_h/G$, *a saber,* $p(x)$ *é o ponto da região fundamental correspondente ao que* x *ocupa no elemento do ladrilhamento de* P_h *que o contém, e* p *é tal que para cada* $m \in P_h/G$, *existe um conjunto aberto* V *contendo* m, *tal que* $p^{-1}(m) = \cup_\alpha A_\alpha$ *onde os* A_α *são abertos dois a dois disjuntos e para cada* α, $p|_{A_\alpha} : A_\alpha \to V$ *é uma bijeção contínua e com inversa contínua, portanto um homeomorfismo.*

Como mencionado, para que $p : P_h \to P_h/G$ seja uma aplicação de recobrimento, o grupo fuchsiano G associado não pode assumir elementos elípticos. A assinatura de G é dada por $(g, m_1, ..., m_r) = (g, 0, ..., 0)$, que denotaremos por $(g, -)$. Como consequência, o grupo fuchsiano G é formado apenas por elementos hiperbólicos.

2.7 Grupos Triângulos

Seja Δ^*ABC um triângulo de ângulos internos $\widehat{A} = \frac{\pi}{\alpha}, \widehat{B} = \frac{\pi}{\beta}$ e $\widehat{C} = \frac{\pi}{\gamma}$. Sejam a, b e c os lados do triângulo Δ^* opostos aos ângulos $\frac{\pi}{\alpha}, \frac{\pi}{\beta}$ e $\frac{\pi}{\gamma}$ e R_a, R_b e R_c reflexões nas retas que contém os lados a, b e c de Δ^*, respectivamente.

O grupo $\Gamma^*(\alpha, \beta, \gamma) = \langle R_a,\ R_b,\ R_c \rangle$, gerado por R_a, R_b e R_c, é chamado **grupo triângulo**. Quando $\alpha = 2$, denotaremos $\Gamma^*(2, \beta, \gamma)$ simplesmente por $[\beta, \gamma]$.

Chamemos Δ^* de região fundamental do $\Gamma^*(\alpha, \beta, \gamma)$.

2.8 Aplicações Conformes

O significado geométrico da definição abaixo é que ângulos (mas não necessariamente comprimentos) são preservados por aplicações conformes. Para maiores detalhes consulte [5].

Definição 2.11 *Um difeomorfismo $\varphi : S \to \overline{S}$ é chamado uma **aplicação conforme** se para todo $p \in S$ e quaisquer $v_1, v_2 \in T_pS$ temos*

$$\langle d\varphi_p(v_1), d\varphi_p(v_2) \rangle_{\varphi(p)} = \lambda^2(p) \langle v_1, v_2 \rangle_p ,$$

*onde λ^2 é uma função diferenciável em S que nunca se anula; as superfícies S e $\overline{S}$ são então chamadas **conformes**.*

Utilizando a Projeção Estereográfica, observamos que a esfera é localmente conforme a um plano. Porém elas não são isométricas.

Conclusão: Toda isometria é uma aplicação conforme, mas nem toda aplicação conforme é isometria.

2.9 Círculos Isométricos

Seja $T(z) = \frac{az+c}{bz+d} \in PSL(2, \mathbb{R})$, com $b \neq 0$, estendida a $\mathbb{C}$. O círculo

$$I(T) = \{z \in \mathbb{C} : |bz + d| = 1\},$$

que é o lugar geométrico completo de pontos onde a transformação T age como uma isometria euclidiana, é chamado círculo isométrico da transformação T. De forma análoga, quando $T(z) = \frac{az+c}{\overline{c}z+\overline{a}} \in PSL(2, \mathbb{C})$, com $\overline{c} \neq 0$, estendida a $\mathbb{C}$, o círculo isométrico com relação a T é

$$I(T) = \{z \in \mathbb{C} : |\overline{c}z + \overline{a}| = 1\}.$$

Observação: A afirmação de que T da forma $T(z) = \frac{az+c}{bz+d}$ com $ad - bc = 1$ e $|bz + d| = 1$ age como uma isometria euclidiana deve-se ao fato de que, se tomarmos dois pontos z_1 e z_2 em $I(T)$, então

$$\begin{aligned}
|T(z_1) - T(z_2)| &= \left| \frac{az_1 + c}{bz_1 + d} - \frac{az_2 + c}{bz_2 + d} \right| \\
&= \left| \frac{(az_1 + c)(bz_2 + d) - (az_2 + c)(bz_1 + d)}{(bz_1 + d)(bz_2 + d)} \right| \\
&= \frac{|abz_1z_2 + adz_1 + bcz_2 + cd - abz_1z_2 - adz_2 - bcz_1 - cd|}{|bz_1 + d| \,.\, |bz_2 + d|} \\
&= |(ad - bc) z_1 - (ad - bc) z_2| \\
&= |z_1 - z_2| .
\end{aligned}$$

Teorema 2.5 *Seja* $T \in \mathrm{PSL}(2,\mathbb{C})$, *com* $\overline{c} \neq 0$, *estendida a* $\mathbb{C}$. *Os círculos isométricos* $I(T)$ *e* $I\left(T^{-1}\right)$ *tem o mesmo raio, e* $I(T)$ *é levado em* $I\left(T^{-1}\right)$ *pela transformação* T.

Demonstração:

Seja $T(z) = \frac{az+c}{\overline{c}z+\overline{a}}$ com $a\overline{a} - \overline{c}c = 1$. Daí, $T^{-1}(z) = \frac{-\overline{a}z+c}{\overline{c}z-a}$, $I(T) = \{z \in \mathbb{C} : |\overline{c}z + \overline{a}| = 1\}$ e $I\left(T^{-1}\right) = \{z \in \mathbb{C} : |\overline{c}z - a| = 1\}$. Fazendo $z = x + iy \in I(T)$, então

$$|\overline{c}z + \overline{a}| = 1 \Longrightarrow |\overline{c}(x+iy) + \overline{a}| = 1 \Longrightarrow \left|x + \frac{\overline{a}}{\overline{c}} + iy\right| = \frac{1}{|\overline{c}|} \Longrightarrow \left(x + \frac{\overline{a}}{\overline{c}}\right)^2 + y^2 = \left(\frac{1}{|\overline{c}|}\right)^2,$$

ou seja, $I(T)$ é um círculo euclidiano de centro $-\frac{\overline{a}}{\overline{c}}$ e raio $\dfrac{1}{|\overline{c}|}$. Agora, se $z = x + iy \in I\left(T^{-1}\right)$, então

$$|\overline{c}z - a| = 1 \Longrightarrow \left|x - \frac{a}{\overline{c}} + iy\right| = \frac{1}{|\overline{c}|} \Longrightarrow \left(x - \frac{a}{\overline{c}}\right)^2 + y^2 = \left(\frac{1}{|\overline{c}|}\right)^2,$$

ou seja, $I\left(T^{-1}\right)$ é um círculo euclidiano de centro $\frac{a}{\overline{c}}$ e raio $\frac{1}{|\overline{c}|}$. Portanto, $I(T)$ e $I\left(T^{-1}\right)$ tem o mesmo raio. Suponha agora que $z \in I(T)$, então $z = -\frac{\overline{a}}{\overline{c}} + \frac{1}{|\overline{c}|}e^{i\theta}$, com $\theta \in [0, 2\pi[$, e

$$\begin{aligned}
T(z) &= \frac{a\left(-\frac{\overline{a}}{\overline{c}} + \frac{1}{|\overline{c}|}e^{i\theta}\right) + c}{\overline{c}\left(-\frac{\overline{a}}{\overline{c}} + \frac{1}{|\overline{c}|}e^{i\theta}\right) + \overline{a}} \\
&= \frac{\frac{-a\overline{a}+\overline{c}c}{\overline{c}} + \frac{a}{|\overline{c}|}e^{i\theta}}{-\overline{a} + \frac{\overline{c}}{|\overline{c}|}e^{i\theta} + \overline{a}} \\
&= \frac{-\frac{1}{\overline{c}} + \frac{a}{|\overline{c}|}e^{i\theta}}{\frac{\overline{c}}{|\overline{c}|}e^{i\theta}} \\
&= \left(-\frac{1}{c} + \frac{a}{|\overline{c}|}e^{i\theta}\right)\frac{|\overline{c}|}{\overline{c}e^{i\theta}} \\
&= -\frac{|\overline{c}|}{|c|^2}e^{i(-\theta)} + \frac{a}{\overline{c}} \\
&= -\frac{|\overline{c}|}{|c|^2}(\cos(\theta) - i\,\mathrm{sen}(\theta)) + \frac{a}{\overline{c}}.
\end{aligned}$$

Vejamos que $T(z) \in I\left(T^{-1}\right)$. De fato:

$$|\overline{c}(T(z)) - a|^2 = \left|-\frac{\overline{c}\,|\overline{c}|}{|c|^2}(\cos(\theta) - i\,\mathrm{sen}(\theta)) + a - a\right|^2 = \cos^2(\theta) + \mathrm{sen}^2(\theta) = 1.$$

Logo, $T(I(T)) \subset I\left(T^{-1}\right)$, ou seja, $I(T)$ é levado em $I\left(T^{-1}\right)$ por T. □

Capítulo 3

Códigos e Reticulados

Forney [8] generalizou os códigos de grupos de Slepian permitindo que os elementos do grupo gerador sejam isometrias arbitrárias do espaço euclidiano $\mathbb{R}^n$, ao invés de transformações ortogonais ou translações consideradas de forma separadas. Tais códigos foram denominados códigos geometricamente uniformes.

Estendemos o conceito de reticulados para o plano hiperbólico, marcando assim o uso das tesselações hiperbólicas regulares associadas aos seus correspondentes grupos de simetrias.

Também apresentamos com detalhes o conceito de códigos G-lineares que será utilizado no principal teorema deste trabalho, apresentado no próximo capítulo.

Nas seções deste capítulo utilizamos o modelo do disco unitário U que é equivalente ao semiplano H^2. Para maiores detalhes sobre tais seções indicamos [15], [2], [6], [23], [13], [3], [7], [11] e [25].

3.1 Códigos

Apresentamos nesta seção, resumidamente, conceitos básicos sobre sistemas de comunicações.

Podemos considerar um sistema de comunicações como sendo um conjunto de equipamentos e meios físicos, que tem por objetivo o transporte da informação de uma fonte a um destinatário via um canal de comunicações. De um modo geral, podemos trabalhar com dois tipos de sistemas de comunicações:

(i) **Sistema analógico** onde a informação (ex. voz) é transmitida por meio de sinais elétricos, magnéticos ou eletromagnéticos que variam continuamente em amplitude e/ou freqüência e/ou fase e tempo.

(ii) **Sistema digital** onde a informação é transmitida em uma seqüência de mensagens discretas por meio de sinais elétricos, magnéticos, eletromagnéticos ou luminosos (fibras óticas) que variam em amplitude e/ou fase e/ou freqüência em intervalos fixos de tempo.

Um sistema de comunicações digital pode ser esquematizado basicamente do seguinte modo:

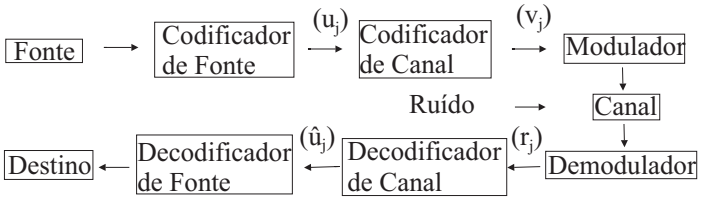


FIGURA 8: *Sistema de Comunicações Digital.*

sendo:

- **Fonte** (de informação): pode ser uma pessoa ou uma máquina que gera uma onda sonora contínua ou uma seqüência de símbolos discretos. Iremos considerar apenas fontes sem memória, ou seja, fontes que emitem mensagens independentes das enviadas anteriormente.

- **Codificador de fonte**: associa as saídas da fonte às seqüências $(u_j) = (u_1, ..., u_k)$ de dígitos (geralmente binários) chamadas de seqüências de informação ou palavras-código fonte. Tendo em vista a eliminação de redundâncias, nesta etapa deve-se utilizar o menor número possível de dígitos por unidade de tempo para representar a saída da fonte. Além disso, a saída da fonte deve ser reconstruída a partir da seqüência de informação associada sem ambiguidades.
- **Codificador de canal**: transforma a palavra-código fonte (u_j) em uma outra seqüência $(v_j) = (v_1, ..., v_n)$ chamada de palavra-código de canal. Este estágio tem por objetivo inserir redundância à seqüência (u_j) com vistas a minimizar a interferência de ruídos no canal.
- **Modulador**: gera formas de ondas que são apropriadas para a transmissão através do canal. O modulador digital transforma símbolos discretos da saída do codificador de canal em um sinal contínuo com duração de T segundos, de tal forma que a amplitude e/ou freqüência e/ou fase seja(m) alterada(s) de acordo com a necessidade.
- **Canal**: é o meio físico por onde a informação é transmitida/armazenada. Alguns exemplos de canais são:
(i) **Canais de transmissão**: linhas telefônicas, meios de propagação de sinais entre antenas de rádio, meios de propagação de sinais entre antenas de microondas, meios de propagação de sinais entre estações terrestres e satélites, fibras óticas, cabos coaxiais, etc.
(ii) **Canais de armazenagem**: fitas cassetes, disquetes de computador, pendrives, CD's, DVD's, memórias de computador, etc.
- **Demodulador**, **decodificador de canal** e **decodificador de fonte**: fazem o inverso do modulador, codificador de canal e codificador de fonte, respectivamente.

Consideremos um espaço métrico (A, d_A) e $I \subseteq \mathbb{Z}$ um subconjunto de índices. Chamamos de **espaço de sequências** A^I sobre o alfabeto A, ao conjunto de todas as sequências $a = (a_i)_{i \in I}$ tal que cada $a_i \in A$. Quando $I = \{i : 1 \leq i \leq n\}$, indicamos A^I por A^n. A **cardinalidade** do alfabeto A, será indicada por $|A|$.

Um **código** C sobre o alfabeto A é qualquer subconjunto não vazio de A^I. Um **código de bloco** C de comprimento n sobre o alfabeto A é qualquer subconjunto não vazio de A^n.

Um código C' obtido de outro código C através de uma permutação de coordenadas, é denominado **equivalente** a C, isto é, códigos equivalentes possuem as mesmas propriedades métricas.

Consideremos o alfabeto A como sendo um grupo finito. Dizemos que o código de bloco C de comprimento n é um **código de grupo** sobre A quando C for um subgrupo de A^n.

3.2 Reticulados Geometricamente Uniformes

Sejam $\mathbb{E}$ espaço de dimensão n com curvatura gaussiana constante, $\mathcal{P} \subset \mathbb{E}$ conjunto finito de pontos e G grupo discreto de isometrias de $\mathbb{E}$. À órbita

$$\mathcal{S} = G_{\mathcal{P}} = \{h(P) : h \in G \text{ e } P \in \mathcal{P}\}$$

de $\mathcal{P}$ por G em $\mathbb{E}$ chamaremos de **reticulado** em $\mathbb{E}$.

Um reticulado $\mathcal{S}$ é dito **geometricamente uniforme** quando o grupo de simetrias $\Gamma(\mathcal{S})$ de $\mathcal{S}$ é transitivo, ou seja, dados dois pontos P e Q de $\mathcal{S}$, existe *uma* simetria $g \in \Gamma(\mathcal{S})$ tal que $g(P) = Q$. Equivalentemente se dado um ponto P em $\mathcal{S}$, existe uma simetria φ em $\Gamma(\mathcal{S})$ tal que $\varphi(P) = Q$, $\forall Q \in \mathcal{S}$, temos que $\mathcal{S}$ é geometricamente uniforme. De fato, sejam Q e Q' em $\mathcal{S}$. Então, existem simetrias φ e σ em $\Gamma(\mathcal{S})$ tais que $\varphi(P) = Q$ e $\sigma(P) = Q'$. Tomemos $\sigma \circ \varphi^{-1}$ em $\Gamma(\mathcal{S})$. Logo,

$$\sigma \circ \varphi^{-1}(Q) = \sigma(P) = Q'.$$

Portanto, $\mathcal{S}$ é um reticulado geometricamente uniforme.

Definição 3.1 *Dado um reticulado S geometricamente uniforme, dizemos que um subgrupo transitivo $U(S)$ de $\Gamma(S)$ é um* ***grupo gerador*** *de S, se $S = \{g(s_0) : g \in U(S)\}$, para s_0 fixo em S, e $U(S)$ é minimal para a geração de S no sentido de que a função $m : U(S) \to S$, $m(g) = g(s_0)$ é uma bijeção.*

Seja $U(\mathcal{S})$ subgrupo de $\Gamma(\mathcal{S})$. Se dados dois pontos P e Q de $\mathcal{S}$, existe *uma única* simetria $g \in U(\mathcal{S})$ tal que $g(P) = Q$, diremos que a ação de $U(\mathcal{S})$ sobre $\mathcal{S}$ é **fortemente transitiva** (nesse caso $|U(\mathcal{S})| = |\mathcal{S}|$).

Exemplo 3.1 *Os reticulados no espaço $\mathbb{R}^n$ obtidos a partir da origem ($\mathcal{P} = \{O\}$) pela ação de um grupo G de translações por n vetores linearmente independentes são os chamados reticulados clássicos do $\mathbb{R}^n$. Tais reticulados são geometricamente uniformes.*

Por outro lado, se $n = 2$, $\mathcal{P} = \{(0,0),(1,0)\} \subset \mathbb{R}^2$ e $G = \left\langle \rho_{\frac{\pi}{8}} \right\rangle$, sendo $\rho_{\frac{\pi}{8}}$ rotação de $\frac{\pi}{8}$ em torno da origem, então o grupo $\Gamma(\mathcal{S})$, sendo $\mathcal{S} = G_{\mathcal{P}}$, de simetrias de $\mathcal{S}$ não é transitivo, portanto, $\mathcal{S}$ não é geometricamente uniforme.

3.3 Reticulados Hiperbólicos

Definição 3.2 *Uma* ***tesselação regular*** *do plano hiperbólico U é uma partição de U por polígonos regulares não sobrepostos todos com o mesmo número de lados sujeitos à restrição de se interceptarem somente em suas arestas ou em vértices, onde se encontram sempre o mesmo número de polígonos. Uma tesselação regular em que q $p-$ágonos regulares se encontram em cada vértice é denotada por $\{p, q\}$.*

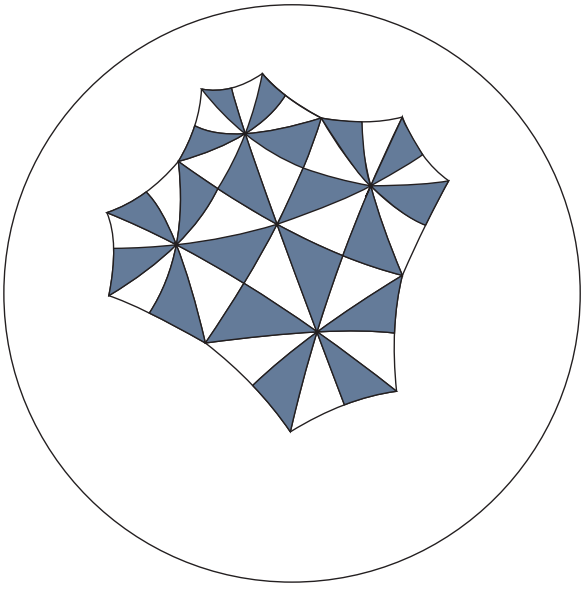


FIGURA 9: *Tesselação* $\{5,4\}$.

Como a soma dos ângulos internos de um triângulo hiperbólico é sempre menor que π temos então que existe uma tesselação $\{p, q\}$ do plano hiperbólico U se, e somente se,

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

Demonstração:

Sejam T um polígono regular com p lados e ângulos internos de medida $\frac{2\pi}{q}$ e S_i a soma dos ângulos internos de T.

Logo,

$$S_i = p\frac{2\pi}{q} \text{ e } S_i < (p-2)\pi.$$

Portanto,

$$(p-2)\pi > S_i = p\frac{2\pi}{q} \Leftrightarrow \pi p - 2\pi > p\frac{2\pi}{q} \Leftrightarrow pq - 2p - 2q > 0$$
$$\Leftrightarrow pq - 2p - 2q + 4 > 4 \Leftrightarrow (p-2)(q-2) > 4.$$

Associado a cada tesselação $\{p, q\}$ existe um grupo que denotaremos $[p, q]$, chamado **o grupo completo de simetrias** de $\{p, q\}$. Este grupo é o grupo de isometrias de U, denominado por $Iso(U)$, gerado pelas reflexões em torno de todas as retas (hiperbólicas) nas quais a tesselação $\{p, q\}$ se reflete nela mesma. O grupo $[p, q]$ é gerado pelas reflexões r_1, r_2 e r_3 nos lados do triângulo hiperbólico com ângulos $\frac{\pi}{2}$, $\frac{\pi}{p}$ e $\frac{\pi}{q}$ como mostrado na Figura 10. Observe que $[p, q]$ é, na verdade, o grupo triângulo $\Gamma^*(2, p, q)$.

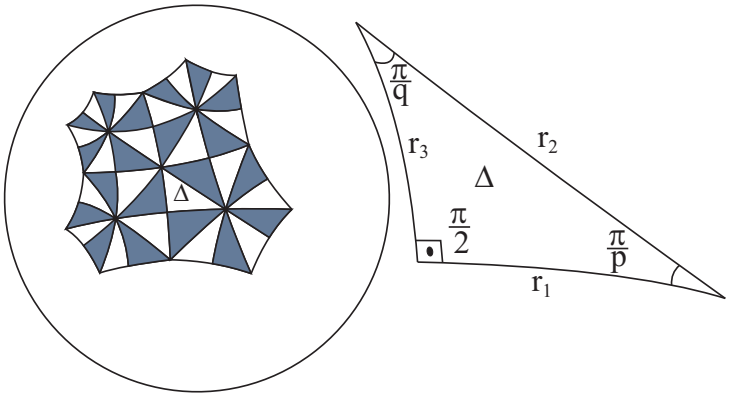


FIGURA 10: *Reflexões Geradoras.*

Consequentemente, a descrição do grupo $[p, q]$ associado com a tesselação $\{p, q\}$ é dado por

$$[p, q] = \left\langle r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_1 \circ r_2)^p = (r_2 \circ r_3)^q = (r_3 \circ r_1)^2 = e \right\rangle.$$

Para verificar esta igualdade, precisamos do seguinte teorema:

Teorema 3.1 *Sejam r_1, r_2 e r_3 reflexões nos lados de um triângulo Δ hiperbólico de ângulos $\frac{\pi}{\alpha}, \frac{\pi}{\beta}$ e $\frac{\pi}{\gamma}$ (α, β e γ, naturais tais que $\frac{\pi}{\alpha} + \frac{\pi}{\beta} + \frac{\pi}{\gamma} < \pi$). Então as imagens F de Δ sob a ação do $\Gamma^*(\alpha, \beta, \gamma)$ formam uma cobertura do plano hiperbólico U sem sobreposição (exceto nos bordos) e*

$$\Gamma^*(\alpha, \beta, \gamma) = \left\langle r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_1 \circ r_2)^\beta = (r_2 \circ r_3)^\gamma = (r_3 \circ r_1)^\alpha = e \right\rangle.$$

Em particular para $\alpha = 2$, temos:

$$[p, q] = \left\langle r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_1 \circ r_2)^p = (r_2 \circ r_3)^q = (r_3 \circ r_1)^2 = e \right\rangle.$$

Demonstração:

Façamos a demonstração em duas partes. A primeira viabiliza a construção do ladrilhamento e a segunda, as composições que representam o elemento neutro e.

(a) Sejam Δ o triângulo hiperbólico ABC com ângulos internos $\widehat{A} = \frac{\pi}{\alpha}, \widehat{C} = \frac{\pi}{\beta}$ e $\widehat{B} = \frac{\pi}{\gamma}$ e lados a, c e b respectivamente opostos aos ângulos $\frac{\pi}{\alpha}$, $\frac{\pi}{\beta}$ e $\frac{\pi}{\gamma}$, sendo r_1 reflexão sobre a reta que contem

o lado de Δ onde estão os ângulos $\frac{\pi}{\alpha}$ e $\frac{\pi}{\beta}$, r_2 reflexão sobre a reta que contem o lado de Δ onde estão os ângulos $\frac{\pi}{\beta}$ e $\frac{\pi}{\gamma}$, r_3 reflexão sobre a reta que contem o lado de Δ onde estão os ângulos $\frac{\pi}{\alpha}$ e $\frac{\pi}{\gamma}$.

Suponhamos, sem perda de generalidade que Δ possui A no centro de U. Então, Δ possui os lados b e c nos "diâmetros" de U.

Tomemos $C_1 = \{T(\Delta) : T \in \langle r_3 \circ r_1, r_1 \rangle\}$ o polígono hiperbólico composto por 2α triângulos isométricos a Δ. Chamemos os triângulos que compõe C_1 de triângulos de ordem um (Figura 11 à esquerda).

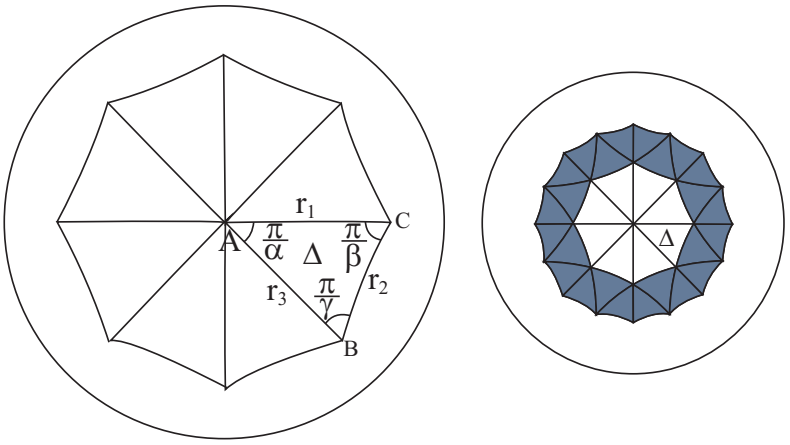


FIGURA 11

Tomando os vértices de C_1 a aplicando um procedimento análogo ao feito com o vértice A de Δ, obtemos um novo polígono hiperbólico que denotamos C_2 e que possui C_1 no seu interior. Os triângulos que compõe C_2 mas não pertencem a C_1 chamaremos de triângulos de ordem dois (Figura 11 à direita).

Mostremos que este procedimento pode ser realizado indefinidamente. Para isto, mostremos que os triângulos de ordem k não se sobrepõem com triângulos de ordens inferiores.

Sabemos que

$$\frac{\pi}{\alpha} + \frac{\pi}{\beta} + \frac{\pi}{\gamma} < \pi.$$

Assim, separamos esta demonstração em três casos:

1º caso: α, β e $\gamma \geq 3$.

Façamos a demonstração por indução: suponhamos que os triângulos de ordem $k-1$ não interceptam (exceto nos bordos) os de ordem inferiores (uma vez que os de ordem 2 não interceptam os de ordem 1).

Os triângulos de ordem $k-1$ formam uma "região anular" $\overline{A}$ em torno do polígono hiperbólico C_{k-2}. Chamemos os triângulos de $\overline{A}$ de $\Delta_1, ..., \Delta_l$. É fácil ver que todo vértice de $\Delta_1, ..., \Delta_l$ que não está em C_{k-2} é comum a dois ou três triângulos de $\overline{A}$ (Figura 12 à esquerda). Juntando esta observação com o fato de α, β e $\gamma \geq 3$, temos que cada ângulo interno de C_{k-1} é $\leq \pi$. Logo, C_{k-1} é convexo.

Tomemos dois lados consecutivos de C_{k-1} com vértices R, S e T e as retas hiperbólicas $MRSM'$ e $N'STN; M, M', N$ e $N' \in \partial U$ que contêm os lados $\overline{RS}$ e $\overline{ST}$ de C_{k-1}. Mais ainda: o interior de C_{k-1} está contido no interior do ângulo hiperbólico $MSNK$. Assim, os triângulos de ordem k em S não possuem interior no ângulo $MSNK$. Como S é arbitrário, temos que os triângulos de ordem k não se sobrepõem com os triângulos de ordem inferior (Figura 12 à direita).

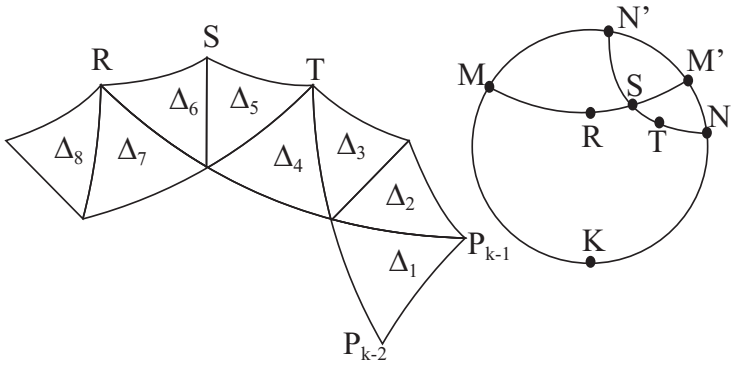


FIGURA 12

Resta mostrar que os triângulos de ordem k não se sobrepõem. Para tanto, dividamos estes triângulos em duas classes:
- Os que possuem dois vértices em comum com C_{k-1}, que chamamos de $Z_1, ..., Z_t$.
- Os que possuem apenas um vértice em comum com C_{k-1}, que chamamos de $E_1, ..., E_u$ (Figura 13 à esquerda).

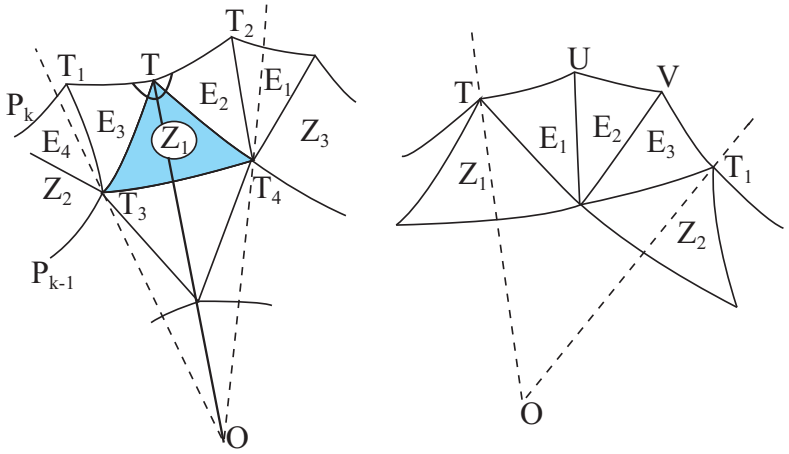


FIGURA 13

Tomemos os segmentos que unem a origem O de U com os vértices de C_k. Sejam R_1, R e R_2 três vértices consecutivos de C_k. Se R é encontro de dois triângulos de ordem k então, $\sphericalangle(\overline{RO}, \overline{RR_1})$ e $\sphericalangle(\overline{RO}, \overline{RR_2}) \leq \frac{2\pi}{3}$.

Se R é encontro de três triângulos de ordem k, o mesmo resultado vale. Demonstraremos por indução.

Como o resultado é verdadeiro para C_2, suponhamos que seja verdadeiro para C_{k-1}. Mostremos que vale para C_k:

Sejam T_1, T e T_2 vértices em C_k, T encontro de três triângulos de ordem k. Tomemos o triângulo $Z_1 = T_3T_4T$ com T_3 e T_4 vértices de C_{k-1} (Figura 13 à esquerda).

De $\sphericalangle(\overline{T_3O}, \overline{T_3T_4})$ e $\sphericalangle(\overline{T_4O}, \overline{T_4T_3}) \leq \frac{2\pi}{3}$ e $\sphericalangle(\overline{T_3T}, \overline{T_3T_4})$ e $\sphericalangle(\overline{T_4T}, \overline{T_4T_3}) \leq \frac{\pi}{3}$ temos que Z_1 está contido no setor de ângulo $\widehat{T_3OT_4}$. Logo, $\sphericalangle(\overline{T_1T}, \overline{TO})$ e $\sphericalangle(\overline{T_2T}, \overline{TO}) \leq \frac{2\pi}{3}$. O que demonstra nossa asserção.

Com isto, chegamos que Z_i, $1 \leq i \leq t$, não se sobrepõem.

Tomemos dois triângulos consecutivos de ordem k do tipo Z_i, digamos Z_1 e Z_2 e todos os triângulos do tipo E_j de ordem k "entre" Z_1 e Z_2 (Figura 13 à direita).

Pelo fato de todos os ângulos dos triângulos que se encontram num ponto serem congruentes, temos, como indicado na Figura 13 à direita, que o polígono $OTUV...T_1$ é convexo, pois todos os seus ângulos internos são $\leq \pi$. Isto mostra que os triângulos do tipo E_i não se sobrepõem. Logo os triângulos de ordem k não se sobrepõem.

Finalmente, mostramos que $\mathcal{F}$ cobre U. Para tanto, tomemos um ponto X pertencente a algum triângulo IJK de $\mathcal{F}$. Tomemos C^* polígono composto pelos triângulos de $\mathcal{F}$ que possuem alguma intersecção com o ΔIJK.

Temos que $d(\partial(\Delta IJK), \partial(C^*)) = d > 0$ (constante). Assim, todo ponto X de $\mathcal{F}$ possui uma vizinhança V_X tal que $B(X, d) \subset V_X$ e V_X pertence a $\mathcal{F}$. Logo, $\bigcup_{X \in \mathcal{F}} V_X = U$.

2^o caso: $\alpha = 2$ e $\beta, \gamma > 4$.

Sem perda de generalidade, tomemos Δ com A na origem do disco unitário U.

Criando os polígonos C_s como anteriormente, temos que C_2 não é convexo pois possui ângulos internos de medida $3\frac{\pi}{2}$(que ocorrem nos vértices dos triângulos do tipo Z_i que não pertencem a C_1, conforme Figura 14).

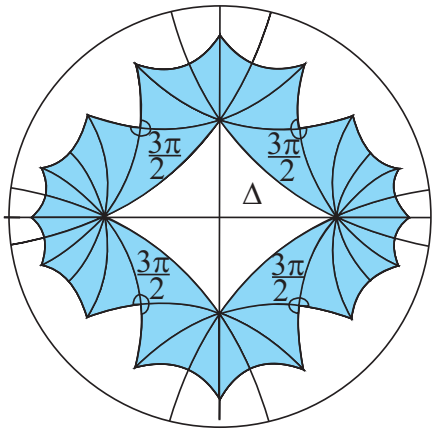


FIGURA 14

Tomemos os triângulos H_i refletidos dos triângulos E_i adjacentes a Z_i em C_2 (Figura 15 à esquerda).

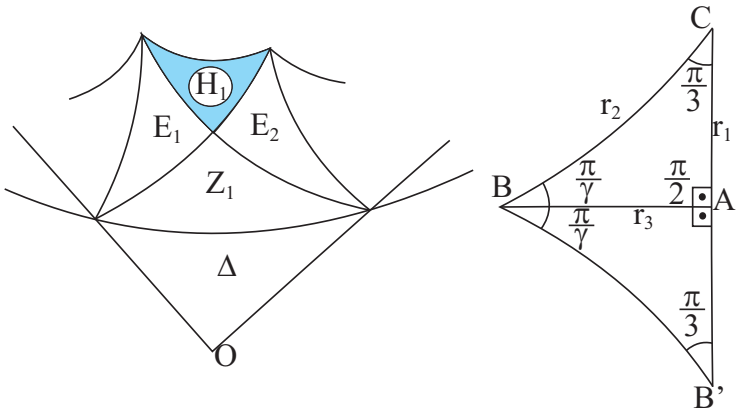


FIGURA 15

Temos, assim, que $C_2 \cup_i H_i = C_2'$ é um polígono convexo e podemos utilizar raciocínio análogo ao do 1^o caso para este caso.

3^o caso: $\alpha = 2$, $\beta = 3$ e $\gamma > 6$.

Tomemos Δ e aplicamos a reflexão r_3 de modo a obter um novo triângulo Δ' de ângulos $\frac{\pi}{3}, \frac{\pi}{3}$ e $2\frac{\pi}{\gamma} < \frac{\pi}{3}$ (Figura 15 à direita). Temos que Δ' está de acordo com as hipóteses do 1^o caso.

(b) É fácil ver que $r_1^2 = r_2^2 = r_3^2 = Id$.

Sabemos que $r_1 \circ r_2 = \rho_{C, 2\frac{\pi}{\beta}}$: rotação de centro C e giro $2\frac{\pi}{\beta}$. Logo, $(r_1 \circ r_2)^\beta = \left(\rho_{C, 2\frac{\pi}{\beta}}\right)^\beta = Id$. Analogamente, $(r_2 \circ r_3)^\gamma = (r_3 \circ r_1)^\alpha = Id$.

Portanto,

$$r_1^2 = r_2^2 = r_3^2 = (r_1 \circ r_2)^\beta = (r_2 \circ r_3)^\gamma = (r_3 \circ r_1)^\alpha = \mathrm{Id}.$$

Logo,

$$\Gamma^*(\alpha, \beta, \gamma) = \left\langle r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_1 \circ r_2)^\beta = (r_2 \circ r_3)^\gamma = (r_3 \circ r_1)^\alpha = e \right\rangle.$$

Em particular para $\alpha = 2$, temos:

$$[p, q] = \left\langle r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_1 \circ r_2)^p = (r_2 \circ r_3)^q = (r_3 \circ r_1)^2 = e \right\rangle.$$

□

Se $\alpha = \beta = \gamma = \infty$, teremos uma tesselação $\{\infty, \infty, \infty\}$ com grupo $\Gamma^*(\infty, \infty, \infty)$. Logo o grupo fuchsiano $\Gamma^*(\infty, \infty, \infty)$ não é co-compacto, pois $\frac{U}{\Gamma^*(\infty,\infty,\infty)}$ não é uma superfície compacta (Figura 16).

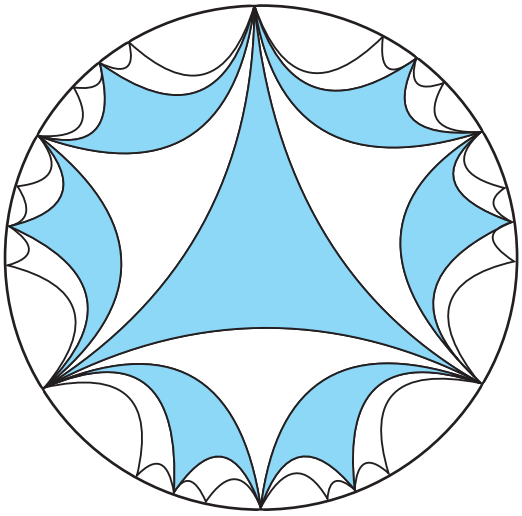


FIGURA 16: *Tesselação* $\{\infty, \infty, \infty\}$.

Dada uma tesselação $\{p, q\}$ com grupo $[p, q]$ então a sua tesselação dual é $\{q, p\}$ com grupo $[q, p]$. É imediato que $[p, q]$ e $[q, p]$ são isomorfos, mas as tesselações $\{p, q\}$ e $\{q, p\}$ diferem a menos de uma translação e coincidem se, e somente se, $p = q$. O caso $p = q$ é chamado de **autodual** e se $p = q = 4g$, para algum inteiro $g \geq 2$, então a tesselação $\{4g, 4g\}$ é tal que a identificação dos lados dos polígonos torna U um recobrimento de uma superfície compacta orientável M de gênero g.

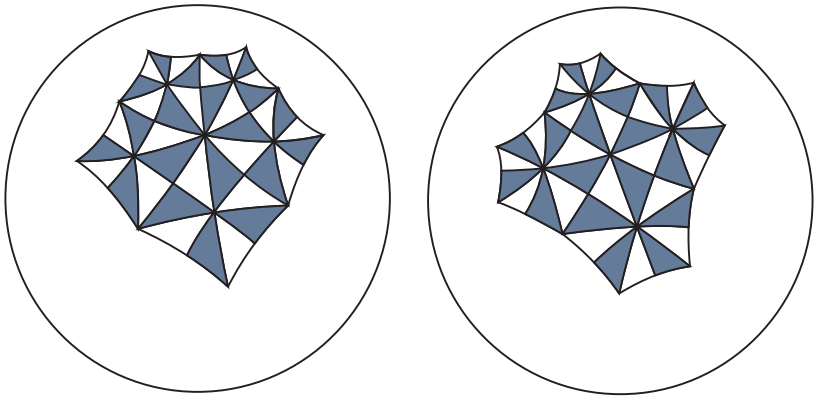


FIGURA 17: *Tesselações* $\{4, 5\}$ *e* $\{5, 4\}$.

A teoria das superfícies de Riemann nos fornece as seguintes informações: todas as superfícies de Riemann fechadas de gênero $g \geq 2$ podem ser mapeadas por um polígono não euclidiano hiperbólico T_{4g} com $4g$ lados e vértices, onde os lados são identificados em pares. Uma vez que T_{4g} pode ser considerado no Modelo do Disco de Poincaré $U \subset \mathbb{C}$ para a Geometria Hiperbólica, existe uma métrica natural, a métrica hiperbólica, em T_{4g} que nos permite trabalhar com um mapeamento conforme. O polígono T_{4g} será então uma região canônica fundamental para o grupo fundamental desta superfície, dado por

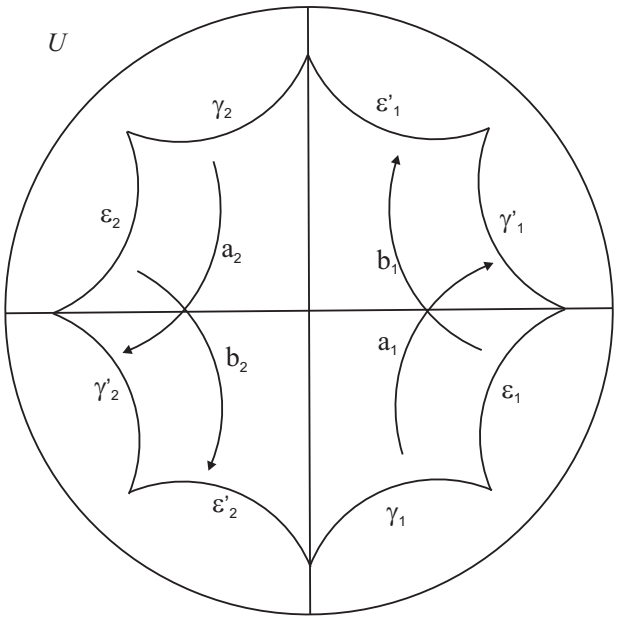
$$\pi_g = \left\langle a_1, ..., a_g, b_1, ..., b_g : \prod_{i=1}^{g} [a_i, b_i] = e \right\rangle,$$

sendo $\prod_{i=1}^{g} [a_i, b_i] = a_1 b_1 a_1^{-1} b_1^{-1} ... a_g b_g a_g^{-1} b_g^{-1}$ [17].

As isometrias a_i e b_i $(i = 1, ..., g)$ produzem uma tesselação autodual $\{4g, 4g\}$ com réplicas congruentes do T_{4g} de tal forma que em cada vértice, $4g$ destas réplicas se encontram.

Percorrendo a fronteira do polígono T_{4g} no sentido horário, a disposição das setas nos dá uma "palavra" $w = a_1 b_1 a_1^{-1} b_1^{-1} ... a_g b_g a_g^{-1} b_g^{-1}$, a qual representa um caminho fechado na superfície.

Se $\varphi : T_{4g} \to S$ é a aplicação quociente (que identifica os lados do polígono T_{4g} para formar a superfície compacta S) do T_{4g} sobre S, então cada duas arestas de T_{4g} é transformada em uma curva fechada. A reunião das $2g$ curvas fechadas assim obtidas terão um ponto x_0 em comum [17]. As Figuras 18 e 19 ilustram a ação de φ para $g = 2$.



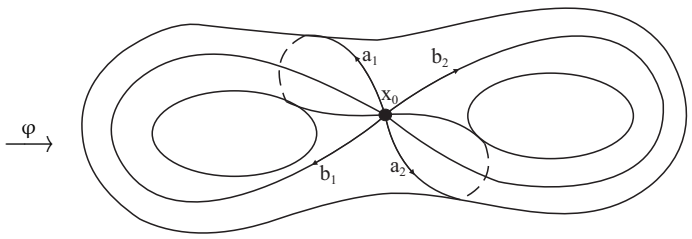


FIGURA 19

FIGURA 18

Sem perda de generalidade, vamos supor que T_{4g} esteja centrado na origem de U. Considerando também as arestas do T_{4g} dispostas em ordem cíclica no sentido antihorário:

$$\gamma_1, \varepsilon_1, \gamma_1', \varepsilon_1', ..., \gamma_g, \varepsilon_g, \gamma_g', \varepsilon_g',$$

e as isometrias hiperbólicas $a_1, ..., a_g, b_1, ..., b_g$ (os geradores do grupo fuchsiano π_g) temos:

$$a_k(\gamma_k) = \gamma_k' \text{ e } b_j(\varepsilon_j) = \varepsilon_j', \text{ sendo } k, j = 1, ..., g. \tag{3.1}$$

Por meio desses emparelhamentos, obtemos uma superfície compacta e orientável $\frac{U}{\pi_g}$ de gênero g. Portanto, definido por uma tesselação autodual $\{4g, 4g\}$, temos um polígono hiperbólico regular T_{4g} de $4g$ arestas, que por sua vez está associado a um grupo fuchsiano π_g com assinatura $(g, -)$.

Pelo Teorema 2.4 que é uma consequência do Teorema de Gauss-Bonnet, temos o seguinte lema, que será útil na demonstração do Teorema 3.3.

Lema 3.1 *A área da região fundamental do* π_g *é* $4\pi(g-1)$.

Observamos que a inexistência do somatório $\sum_{k=1}^{r}\left(1-\frac{1}{m_k}\right)$ na medida da área hiperbólica de $\frac{U}{\pi_g}$ no Lema 3.1, é equivalente a inexistência de elementos elípticos no grupo π_g. Isto é suficiente para que tenhamos o quociente $\frac{U}{\pi_g}$ localmente isométrico a U.

Consideremos agora T_C como sendo uma transformação elíptica de ordem $4g$ com matriz associada

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

de modo que $T_C(\gamma_1)=\varepsilon_1$, isto é:

$$\begin{aligned} T_C(\gamma_1) &= \frac{\left(\cos\left(\frac{\pi}{4g}\right)+i\,\mathrm{sen}\left(\frac{\pi}{4g}\right)\right)\gamma_1+0}{0\gamma_1+\left(\cos\left(\frac{\pi}{4g}\right)-i\,\mathrm{sen}\left(\frac{\pi}{4g}\right)\right)} \\ &= \frac{\left(\cos\left(\frac{\pi}{4g}\right)+i\,\mathrm{sen}\left(\frac{\pi}{4g}\right)\right)\gamma_1}{\cos\left(\frac{\pi}{4g}\right)-i\,\mathrm{sen}\left(\frac{\pi}{4g}\right)}\cdot\frac{\cos\left(\frac{\pi}{4g}\right)+i\,\mathrm{sen}\left(\frac{\pi}{4g}\right)}{\cos\left(\frac{\pi}{4g}\right)+i\,\mathrm{sen}\left(\frac{\pi}{4g}\right)} \\ &= \frac{\left(\cos^2\left(\frac{\pi}{4g}\right)+i\left(2\cos\left(\frac{\pi}{4g}\right)\mathrm{sen}\left(\frac{\pi}{4g}\right)\right)-\mathrm{sen}^2\left(\frac{\pi}{4g}\right)\right)\gamma_1}{\cos^2\left(\frac{\pi}{4g}\right)+\mathrm{sen}^2\left(\frac{\pi}{4g}\right)} \\ &= \left(\cos\left(\frac{\pi}{2g}\right)+i\,\mathrm{sen}\left(\frac{\pi}{2g}\right)\right)\gamma_1 \\ &= e^{i\frac{\pi}{2g}}\gamma_1=\varepsilon_1 \end{aligned}$$

e r_k é a potência de T_C tal que

$$(T_C)^{r_k}(\gamma_1)=T_{C^{r_k}}(\gamma_1)\in\{\gamma_k,\varepsilon_k,\gamma_k',\varepsilon_k'\},\ k=1,...,g. \tag{3.2}$$

Isto permite escrever os geradores do π_g como conjugações de a_1 por meio de potências de T_C. Por exemplo, queremos uma transformação a_2 de modo que $a_2(\gamma_2)=\gamma_2'$. Mas, $a_1(\gamma_1)=\gamma_1'$ e $T_{C^4}(\gamma_1)=\gamma_2$. Disso segue que $T_{C^{-4}}(\gamma_2)=\gamma_1$. Logo,

$$a_1\left(T_{C^{-4}}(\gamma_2)\right)=\gamma_1'\Leftrightarrow T_{C^4}\left(a_1\left(T_{C^{-4}}(\gamma_2)\right)\right)=T_{C^4}(\gamma_1')=\gamma_2',$$

ou seja,

$$T_{C^4}\circ\ a_1\circ\ T_{C^{-4}}(\gamma_2)=\gamma_2'.$$

Dessa forma, basta considerarmos $a_2=T_{C^4}\circ\ a_1\circ\ T_{C^{-4}}$. Para os demais casos, usando 3.1 e 3.2 obtemos,

$$A_k=C^{4(k-1)}A_1C^{-4(k-1)}\text{ e }B_j=C^{4j-3}A_1C^{-4j+3},$$

onde A_k e B_j sâo as matrizes correspondentes às transformações a_k e b_j, respectivamente, com $k,\ j=1,...,g$.

Portanto, de posse do gerador a_1 estamos, conseqüentemente, determinando os demais geradores. O próximo teorema nos mostra a forma do gerador a_1.

Teorema 3.2 *Seja* T_{4g} *o polígono hiperbólico regular de* $4g$ *arestas, cujo grupo fuchsiano associado é* π_g *com assinatura* $(g,-)$. *Consideremos* γ_1 *como sendo a aresta entre os argumentos* $-\frac{\pi}{2}$ *e* $-\frac{(g-1)\pi}{2g}$ *e* a_1 *a transformação hiperbólica que emparelha as arestas* γ_1 *e* γ_1' *do polígono* T_{4g}. *Então*

$$a_1(z) = \frac{az+c}{\overline{c}z+\overline{a}}$$

onde a *e* c *são dados por*

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

$$|c| = \left(\left(\operatorname{tg}\left(\frac{(2g-1)\pi}{4g}\right)\right)^2 - 1\right)^{\frac{1}{2}} \ \ e \ \ \arg(c) = -\frac{(2g+1)\pi}{4g}.$$

Demonstração:

Ligando por geodésicas o baricentro do polígono T_{4g} com seus vértices, obtemos $4g$ triângulos hiperbólicos em T_{4g} cada um com área $\frac{\pi(g-1)}{g}$ e com ângulo $\frac{\pi}{2g}$ para o vértice que é o baricentro do T_{4g}.

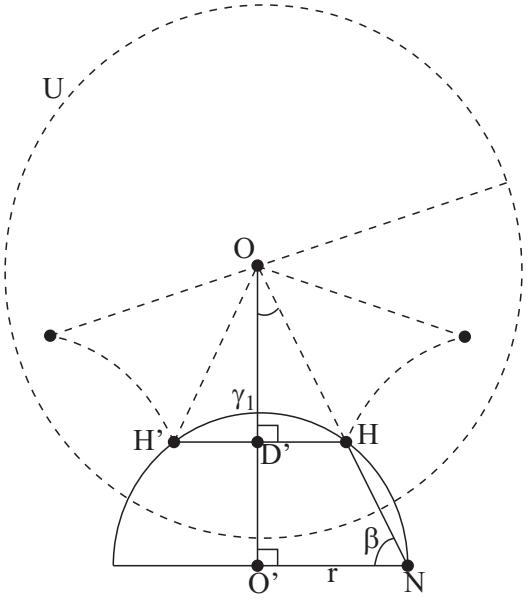


FIGURA 20: *Encontrando geradores do grupo fundamental* π_g.

A Figura 20 mostra parte da região fundamental T_{4g}, um polígono regular de $4g$ lados de uma tesselação $\{4g,4g\}$ com o baricentro determinado pelo ponto $O = 0$, centro do disco de Poincaré. Consideremos o círculo isométrico de centro no ponto O' e raio r contendo γ_1 dada pelo arco $H'H$, $D' = OO' \cap H'H$ e o ponto N pertecente a este círculo tal que $\widehat{OO'N} = \frac{\pi}{2}$. Logo os triângulos euclidianos $OO'N$ e $OD'H$ são semelhantes e daí os pontos O, H e N são colineares. Como $OO'N$ é um triângulo retângulo temos que

$$\frac{\overline{OO'}}{r} = \operatorname{tg}\left(\frac{(2g-1)\pi}{4g}\right).$$

Seja

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

a matriz associada à transformação hiperbólica $a_1(z) = \frac{az+c}{\bar{c}z+\bar{a}}$. Seja $a_1^{-1}(z)$ a transformação inversa de $a_1(z)$. Então, $a_1^{-1}(z) = \frac{-\bar{a}z+c}{\bar{c}z-a}$. A matriz associada a $a_1^{-1}(z)$ é dada por

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

Da demonstração do Teorema 2.5, os centros isométricos de $I(a_1)$ e $I(a_1^{-1})$ são $\frac{-\bar{a}}{\bar{c}}$ e $\frac{a}{\bar{c}}$, respectivamente.

Como $a_1(\gamma_1) = \gamma_1'$, a transformação $T_{C^{-2}}$ leva o círculo isométrico $I(a_1^{-1})$ em $I(a_1)$. Vamos usar o fato de $T_{C^{-2}}\left(\frac{a}{\bar{c}}\right) = \frac{-\bar{a}}{\bar{c}}$ para determinar os elementos da matriz A_1. Como,

$$T_{C^{-2}}\left(\frac{a}{\bar{c}}\right) = e^{-\frac{i\pi}{g}}\frac{a}{\bar{c}},$$

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

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

$$-\cos\left(\frac{\pi}{g}\right) = -\cos\left(2\pi - \frac{\pi}{g}\right) = -\cos\left(\frac{(2g-1)\pi}{g}\right),$$

e

$$-\mathrm{sen}\left(\frac{\pi}{g}\right) = \mathrm{sen}\left(2\pi - \frac{\pi}{g}\right) = \mathrm{sen}\left(\frac{(2g-1)\pi}{g}\right).$$

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

Novamente da demonstração do Teorema 2.5, temos $|\bar{c}| = \frac{1}{r}$, sendo r o raio do círculo que contém γ_1 e $\overline{OO'} = \frac{|-\bar{a}|}{|\bar{c}|} = \frac{|\bar{a}|}{|\bar{c}|}$, uma vez que o centro de $I(a_1)$ é $\frac{-\bar{a}}{\bar{c}}$, implicando $|a| = |\bar{a}| = \frac{\overline{OO'}}{r} = \tan\left(\frac{(2g-1)\pi}{4g}\right)$. Logo,

$$a = |a|\,e^{i\arg(a)} = \mathrm{tg}\left(\frac{(2g-1)\pi}{4g}\right)\left(\cos\left(\frac{(2g-1)\pi}{2g}\right) + i\,\mathrm{sen}\left(\frac{(2g-1)\pi}{2g}\right)\right).$$

Como $a\bar{a} - \bar{c}c = 1$, temos $|a|^2 - |c|^2 = 1$, logo $|c| = \left(\left(\mathrm{tg}\left(\frac{(2g-1)\pi}{4g}\right)\right)^2 - 1\right)^{\frac{1}{2}}$. Como γ_1 é uma aresta entre os argumentos $-\frac{\pi}{2}$ e $-\frac{(g-1)\pi}{2g}$, temos que $\arg\left(-\frac{\bar{a}}{\bar{c}}\right) = -\frac{(2g-1)\pi}{4g}$. Com isso, temos:

$$-\frac{\bar{a}}{\bar{c}} = \left|\frac{\bar{a}}{\bar{c}}\right| e^{i\arg\left(-\frac{\bar{a}}{\bar{c}}\right)} \Rightarrow \bar{c} = -|\bar{a}|\,e^{-i\frac{(2g-1)\pi}{2g}}\frac{|\bar{c}|}{|\bar{a}|}e^{i\frac{(2g-1)\pi}{4g}} \Rightarrow$$
$$\bar{c} = -|\bar{c}|\,e^{-i\frac{(2g-1)\pi}{4g}},$$

resultando na seguinte relação,

$$\begin{aligned}\bar{c} &= -|\bar{c}|\left(\cos\left(\frac{(2g-1)\pi}{4g}\right) - i\,\mathrm{sen}\left(\frac{(2g-1)\pi}{4g}\right)\right) \\ &= |\bar{c}|\left(-\cos\left(\frac{(2g-1)\pi}{4g}\right) + i\,\mathrm{sen}\left(\frac{(2g-1)\pi}{4g}\right)\right).\end{aligned}$$

Mas, $2g-1 \leq 2g$ implicando que $0 \leq \frac{\pi(2g-1)}{4g} \leq \frac{\pi}{2}$. Com isso,

$$-\cos\left(\frac{(2g-1)\pi}{4g}\right) = \cos\left(\pi - \frac{(2g-1)\pi}{4g}\right) = \cos\left(\frac{(2g+1)\pi}{4g}\right),$$
$$\operatorname{sen}\left(\frac{(2g-1)\pi}{4g}\right) = \operatorname{sen}\left(\pi - \frac{(2g-1)\pi}{4g}\right) = \operatorname{sen}\left(\frac{(2g+1)\pi}{4g}\right),$$
$$\overline{c} = |\overline{c}|\left(\cos\left(\frac{(2g+1)\pi}{4g}\right) + i\operatorname{sen}\left(\frac{(2g+1)\pi}{4g}\right)\right).$$

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

$$c = \left(\left(\operatorname{tg}\left(\frac{(2g-1)\pi}{4g}\right)\right)^2 - 1\right)^{\frac{1}{2}} e^{-i\frac{(2g+1)\pi}{4g}}.$$

□

As demais transformações hiperbólicas $a_k(\gamma_k) = \gamma_k'$ e $b_j(\varepsilon_j) = \varepsilon_j'$ geradores do grupo fuchsiano π_g que realizam os outros emparelhamentos de arestas são obtidas pelas conjugações

$$a_k = T_{C^{4(k-1)}} \circ a_1 \circ T_{C^{-4(k-1)}},\ b_j = T_{C^{4j-3}} \circ a_1 \circ T_{C^{-4j+3}}.$$

Por meio do processo de construção do grupo π_g, podemos determinar sua estrutura algébrica através de sua apresentação que é dada por,

$$\left\langle a_1, ..., a_g, b_1, ..., b_g : \prod_{i=1}^{g} [a_i, b_i] = e \right\rangle.$$

De fato, por construção, podemos verificar que existe um vértice $w \in T_{4g}$ tal que

$$a_1 b_1 a_1^{-1} b_1^{-1} ... a_g b_g a_g^{-1} b_g^{-1}(w) = w.$$

Mas, o estabilizador de w,

$$\{d \in \pi_g : d(w) = w\},$$

é constituído apenas da identidade [13].

Exemplo 3.2 *Tesselação* $\{8,8\}$ *no plano hiperbólico* U.

Consideremos T_C *como sendo uma transformação elíptica de ordem* 8 *com matriz associada*

$$C = \begin{pmatrix} e^{\frac{i\pi}{8}} & 0 \\ 0 & e^{\frac{-i\pi}{8}} \end{pmatrix},$$

de modo que $T_C(\gamma_1) = e^{\frac{i\pi}{4}}\gamma_1 = \varepsilon_1$ *e* r_k *é a potência de* T_C *tal que*

$$(T_C)^{r_k}(\gamma_1) = T_{C^{r_k}}(\gamma_1) \in \{\gamma_k, \varepsilon_k, \gamma_k', \varepsilon_k'\},\ k = 1, 2.$$

Pelo processo anterior, temos:

$$A_1 = A_1,\ B_1 = CA_1C^{-1}$$
$$A_2 = C^4A_1C^{-4} \text{ e } B_2 = C^5A_1C^{-5},$$

onde A_1, B_1, A_2 *e* B_2 *são as matrizes correspondentes às transformações* a_1, b_1, a_2 *e* b_2, *respectivamente.*

Seja T_8 *o polígono hiperbólico regular de* 8 *arestas, cujo grupo fuchsiano associado é* π_8 *com assinatura* $(2,-)$. *Temos que a aresta* γ_1 *entre os argumentos* $-\frac{\pi}{2}$ *e* $-\frac{\pi}{4}$ *está contida na circunferência de centro* $\left(\frac{\sqrt{3+2\sqrt{2}}}{\sqrt{2+2\sqrt{2}}}\left(\sqrt{2-\sqrt{2}} - i\sqrt{2+\sqrt{2}}\right)\right)$ *e raio* $\frac{1}{\sqrt{2+2\sqrt{2}}}$. *De fato, aplicando a rotação de centro* O *e ângulo* $\frac{3\pi}{8}$ *na curva* γ_1, *obtemos:*

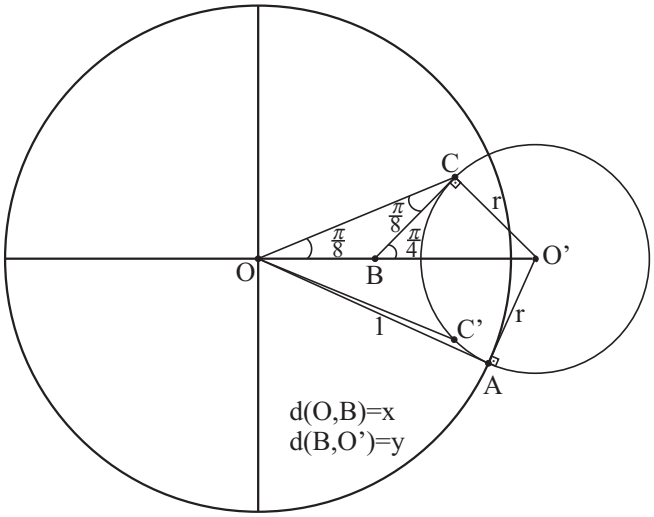


FIGURA 21: *Encontrando expressões para isometrias.*

Observemos que $\mathsf{OAO'}$ *é reto em* A *e* $\mathsf{BCO'}$ *é reto em* C. *Além disso,* $\widehat{\mathsf{B}} = \frac{\pi}{8} + \frac{\pi}{8} = \frac{\pi}{4}$. *No triângulo* $\mathsf{BCO'}$ *temos*

$$\operatorname{sen}\left(\frac{\pi}{4}\right) = \frac{r}{y} \Longrightarrow y = \frac{2r}{\sqrt{2}} = r\sqrt{2}$$

e

$$\cos\left(\frac{\pi}{4}\right) = \frac{x}{y} \Longrightarrow x = \frac{\sqrt{2}}{2} r\sqrt{2} = r.$$

No triângulo $\mathsf{OO'A}$ *temos*

$$\begin{aligned}
(x+y)^2 = r^2 + 1 &\Longrightarrow \\
\left(r + r\sqrt{2}\right)^2 = r^2 + 1 &\Longrightarrow \\
r^2\left(1+\sqrt{2}\right)^2 = r^2 + 1 &\Longrightarrow \\
r^2\left(\left(1+\sqrt{2}\right)^2 - 1\right) = 1 &\Longrightarrow \\
r^2 = \frac{1}{2+2\sqrt{2}} &\Longrightarrow \\
r = \frac{1}{\sqrt{2+2\sqrt{2}}}.&
\end{aligned}$$

Além disso,

$$\begin{aligned}
|x+y| &= \sqrt{r^2\left(1+\sqrt{2}\right)^2} \\
&= \sqrt{\frac{1}{2+2\sqrt{2}}\left(1+2\sqrt{2}+2\right)} \\
&= \sqrt{1 + \frac{1}{2+2\sqrt{2}}} \\
&= \frac{\sqrt{3+2\sqrt{2}}}{\sqrt{2+2\sqrt{2}}}.
\end{aligned}$$

Tomemos a_1 *a transformação hiperbólica que emparelha as arestas* γ_1 *e* γ_1' *do polígono* T_8*, definida por* $a_1(z) = \frac{az+c}{\bar{c}z+\bar{a}}$*. Então pelo Teorema 3.2, temos:*

$$\arg(a) = \frac{3\pi}{4}, \ \ |a| = \operatorname{tg}\left(\frac{3\pi}{8}\right) \Rightarrow |a| = \sqrt{\frac{1-\cos\left(\frac{3\pi}{4}\right)}{\cos\left(\frac{3\pi}{4}\right)+1}} \Rightarrow |a| = \sqrt{\frac{2+\sqrt{2}}{2-\sqrt{2}}},$$

$$|c| = \left(\left(\operatorname{tg}\left(\frac{3\pi}{8}\right)\right)^2 - 1\right)^{\frac{1}{2}} \Rightarrow |c| = \sqrt{2+2\sqrt{2}} \ e \ \arg(c) = -\frac{5\pi}{8}.$$

Logo,

$$a = |a|\, e^{i\arg(a)} = \sqrt{\frac{2+\sqrt{2}}{2-\sqrt{2}}}\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \frac{\sqrt{2}}{2}\left(-\sqrt{3+2\sqrt{2}} + i\sqrt{3+2\sqrt{2}}\right)$$

$$e\ c = |c|\, e^{i\arg(c)} = \sqrt{2+2\sqrt{2}}\left(-\sqrt{\frac{1+\cos\left(-\frac{5\pi}{4}\right)}{2}} - i\sqrt{\frac{1-\cos\left(-\frac{5\pi}{4}\right)}{2}}\right)$$

$$= \frac{\sqrt{2+2\sqrt{2}}}{2}\left(-\sqrt{2-\sqrt{2}} - i\sqrt{2+\sqrt{2}}\right) = -\frac{\sqrt[4]{2}}{2}\left(\sqrt{2} + i\left(2+\sqrt{2}\right)\right).$$

Sejam $c_1 = \frac{\sqrt{2}}{2}$ *e* $c_2 = \frac{\sqrt[4]{2}}{2}$*. Portanto,*

$$a_1(z) = \frac{\left(-c_1\sqrt{3+2\sqrt{2}} + ic_1\sqrt{3+2\sqrt{2}}\right)z - c_2\left(\sqrt{2} + i\left(2+\sqrt{2}\right)\right)}{-c_2\left(\sqrt{2} - i\left(2+\sqrt{2}\right)\right)z + \left(-c_1\sqrt{3+2\sqrt{2}} - ic_1\sqrt{3+2\sqrt{2}}\right)},$$

$$a_2(z) = e^{i\pi}\left(a_1\left(e^{-i\pi}(z)\right)\right)$$

$$= \frac{\left(c_1\sqrt{3+2\sqrt{2}} - ic_1\sqrt{3+2\sqrt{2}}\right)z - c_2\left(\sqrt{2} + i\left(2+\sqrt{2}\right)\right)}{-c_2\left(\sqrt{2} - i\left(2+\sqrt{2}\right)\right)z + \left(c_1\sqrt{3+2\sqrt{2}} + ic_1\sqrt{3+2\sqrt{2}}\right)},$$

$$b_1(z) = e^{\frac{i\pi}{4}}\left(a_1\left(e^{-i\frac{\pi}{4}}(z)\right)\right)$$

$$= (c_1 + ic_1)\frac{\left(-c_1\sqrt{3+2\sqrt{2}} + ic_1\sqrt{3+2\sqrt{2}}\right)(c_1z(1-i)) - c_2\left(\sqrt{2} + i\left(2+\sqrt{2}\right)\right)}{-c_2\left(\sqrt{2} - i\left(2+\sqrt{2}\right)\right)(c_1z(1-i)) + \left(-c_1\sqrt{3+2\sqrt{2}} - ic_1\sqrt{3+2\sqrt{2}}\right)} \ e$$

$$b_2(z) = e^{i\frac{5\pi}{4}}\left(a_1\left(e^{-i\frac{5\pi}{4}}(z)\right)\right)$$

$$= (-c_1 - ic_1)\frac{\left(-c_1\sqrt{3+2\sqrt{2}} + ic_1\sqrt{3+2\sqrt{2}}\right)(c_1z(-1+i)) - c_2\left(\sqrt{2} + i\left(2+\sqrt{2}\right)\right)}{-c_2\left(\sqrt{2} - i\left(2+\sqrt{2}\right)\right)(c_1z(-1+i)) + \left(-c_1\sqrt{3+2\sqrt{2}} - ic_1\sqrt{3+2\sqrt{2}}\right)}.$$

A Figura 18 foi construida no programa Maple 12*. Para isto utilizamos a aresta* γ_1 *entre os argumentos* $-\frac{\pi}{2}$ *e* $-\frac{\pi}{4}$*,* T_C *e as isometrias* a_1, b_1, a_2 *e* b_2*.*

Teorema 3.3 *O grupo fundamental* π_g *é um subgrupo de índice* $8g$ *do grupo triângulo* $[4g, 4g]$*.*

Demonstração:

Verificar que $\pi_g \leq [4g, 4g]$ tem índice $8g$ é equivalente a verificar que o triângulo hiperbólico Δ^* de ângulos internos $\frac{\pi}{2}, \frac{\pi}{4g}$ e $\frac{\pi}{4g}$ ladrilha (por reflexões) T_{4g}, a região fundamental do π_g, com $8g$ ladrilhos. Seja O o centro da região poligonal T_{4g}. Para tanto, consideremos os pontos médios

$m_1, ..., m_{4g}$ dos lados de T_{4g} e os segmentos geodésicos que ligam o centro a estes pontos médios. Chamemos os vértices de T_{4g} de $\nu_1, ..., \nu_{4g}$ tal que m_j está entre ν_j e ν_{j+1}, para $j = 1, ..., 4g$, sendo $\nu_{4g+1} = \nu_1$ (Figura 22 à esquerda).

Os pontos O, m_j, ν_{j+1} e m_{j+1} formam um losango hiperbólico L de ângulos internos $\frac{\pi}{2g}, \frac{\pi}{2}, \frac{\pi}{2g}$ e $\frac{\pi}{2}$ respectivamente.

Afirmamos que o segmento geodésico $O\nu_{j+1}$ divide L em dois triângulos hiperbólicos congruentes.

Para verificarmos esta asserção, observamos do fato de T_{4g} ser um polígono regular com centro O e:

$$\overline{m_j\nu_{j+1}} \equiv \overline{\nu_{j+1}m_{j+1}},\ \widehat{Om_j}\nu_{j+1} \equiv \nu_{j+1}\widehat{m_{j+1}O} \text{ com medida } \frac{\pi}{2} \text{ e } \overline{Om_j} \equiv \overline{Om_{j+1}}.$$

Logo pelo caso LAL de congruência temos que os triângulos são congruentes.

Seja Δ^* o triângulo hiperbólico de vértices O, ν_1 e m_1.

Definamos:

(i) r_1 como sendo a reflexão com eixo geodésico contendo Om_1 (base de Δ^*).

(ii) r_2 e r_3 como sendo as reflexões com eixos geodésicos contendo $O\nu_1$ e $\nu_1 m_1$ respectivamente (lados de Δ^*).

(iii) $[4g, 4g] = \langle r_1, r_2, r_3 \rangle$.

Assim, Δ^* é a região fundamental de $[4g, 4g]$ e a órbita de Δ^* por $[4g, 4g]$, $[4g, 4g]\,\Delta^*$, é um ladrilhamento de T_{4g}, ou seja, $[4g, 4g]\,\Delta^*$ é um ladrilhamento em U e $\frac{[4g,4g]\Delta^*}{\pi_g}$ é um ladrilhamento no g-toro $\frac{U}{\pi_g}$.

Quanto à cardinalidade, pelo Lema 3.1 a área da região fundamental do π_g é $4\pi(g-1)$ e, pelo Corolário 2.1, temos que a área da região fundamental de $[4g, 4g]$ é:

$$\pi - \left(\frac{\pi}{2} + \frac{\pi}{4g} + \frac{\pi}{4g}\right) = \frac{\pi(g-1)}{2g}.$$

Seja I o índice $[[4g, 4g] : \pi_g]$. Logo,

$$4\pi(g-1) = I\frac{\pi(g-1)}{2g}, \text{ o que equivale a } I = 8g.$$

□

Sejam $\Pi \subset U$ a região fundamental de um grupo de isometrias Γ e Γ' um subgrupo de índice finito de Γ. Consideremos o ladrilhamento de $\frac{U}{\Gamma'}$ por cópias de $h\Pi$ para algum $h \in \Gamma$. Este ladrilhamento em $\frac{U}{\Gamma'}$ será dito **simétrico** quando a órbita $\Gamma'\Pi$ puder ser mapeada, por algum $r \in \Gamma$, em qualquer outra órbita da forma $\Gamma'\overline{h}\Pi$ com $\overline{h} \in \Gamma$ arbitrário.

Abaixo segue o teorema que é nossa principal contribuição neste trabalho.

Teorema 3.4 *Sejam* $[4g, 4g]$ *grupo triângulo e* π_g *o grupo fundamental da superfície compacta* S *de gênero* $g \geq 2$, *obtida pelo quociente de* U *por* π_g. *Então* π_g *é um subgrupo normal do* $[4g, 4g]$ *e* $[4g, 4g] = D_{4g} \underset{\sigma}{\times} \pi_g$, *sendo* $D_{4g} = \langle s, r : r^{4g} = s^2 = Id;\ r \circ s = s \circ r^{4g-1} \rangle$ *o grupo diedral de grau* $4g$.

Demonstração:

Temos $\pi_g \leq [4g, 4g]$ de índice $8g$ (Teorema 3.3) e

$$T_{4g} = h_1\Delta^* \cup h_2\Delta^* \cup ... \cup h_{8g}\Delta^*$$

é tal que $h_1 = r_2$, $h_2 = r_1$, $h_{2n-1} = r_2h_{2n-2}$, $h_{2n} = r_1h_{2n-3}$, $h_{8g-1} = r_2h_{8g-2}$ e $h_{8g} = Id$, $\forall n = 2, ..., 4g-1$.

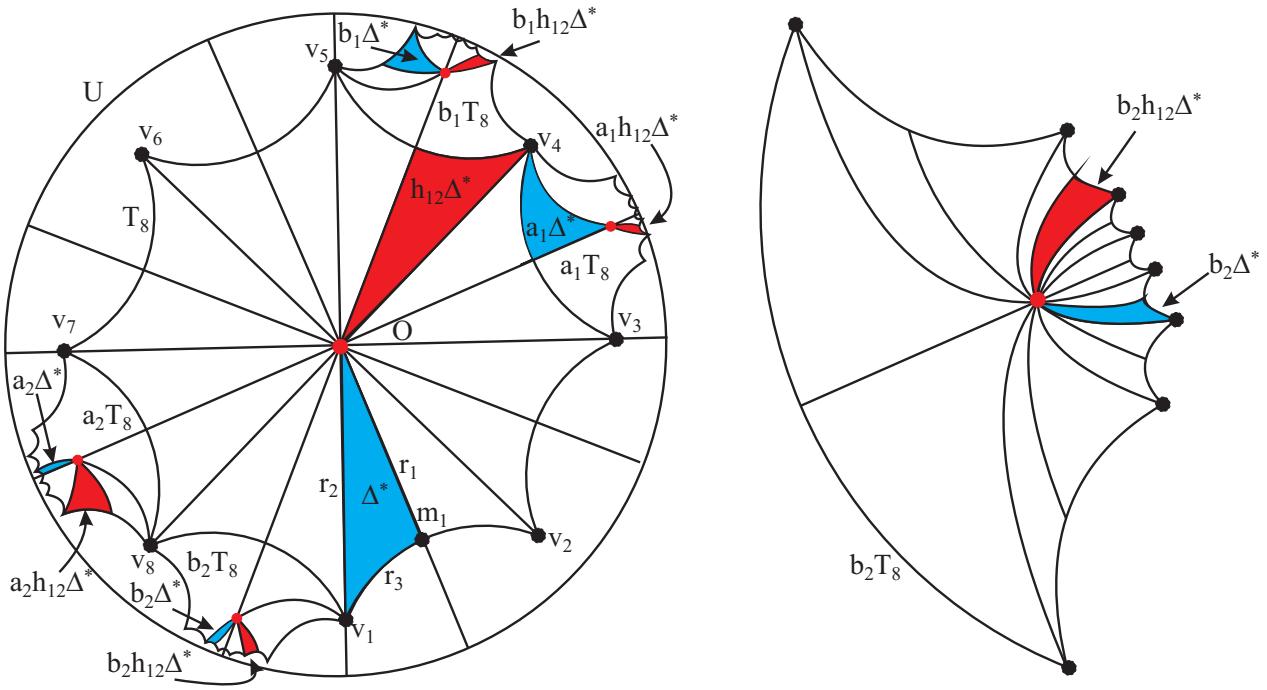


FIGURA 22

Logo,

$$[4g, 4g] = \pi_g h_1 \cup \pi_g h_2 \cup ... \cup \pi_g h_{8g}$$

é a decomposição de $[4g, 4g]$ em classes laterais à direita da forma $\pi_g h_i$, $i = 1, ..., 8g$. Essa decomposição é justificada pelo fato dos geradores r_1, r_2 e r_3 de $[4g, 4g]$ estarem em classes laterais da forma $\pi_g h_i$.

Sejam $\pi_g\Delta^*$ e $\pi_g\overline{h}\Delta^*$ com $\overline{h} \in [4g, 4g]$, órbitas em U. Logo, existem dois triângulos Δ_1^* e Δ_2^* nessas órbitas em T_{4g}. Logo, existe $f = h_i$ para algum i tal que $f(\Delta_1^*) = \Delta_2^*$, fazendo com que $f\pi_g\Delta^* = \pi_g\overline{h}\Delta^*$, ou seja, o ladrilhamento de $\frac{U}{\pi_g}$ por cópias da órbita $\pi_g\Delta^*$ é simétrico.

Um ladrilho em $\frac{U}{\pi_g}$ é a órbita $\pi_g h_i\Delta^* = \{h' h_i\Delta^* : h' \in \pi_g\}$ de um ladrilho $h_i\Delta^*$ do T_{4g}.

Parte das órbitas $\pi_2\Delta^*$ e $\pi_2 h_{12}\Delta^*$, para o caso $g = 2$, são apresentadas esquematicamente na Figura 22 à esquerda, nas cores azul e vermelha, respectivamente. A Figura 22 à direita é uma ampliação da região b_2T_8, sendo b_2 uma das isometrias que geram π_2.

Assim, a simetria do ladrilhamento de $\frac{U}{\pi_g}$ significa que a órbita $\pi_g\Delta^*$ pode ser mapeada, por algum $f \in [4g, 4g]$, em qualquer outra órbita da forma $\pi_g\overline{h}\Delta^*$ com $\overline{h} \in [4g, 4g]$ arbitrário. Mas se $f\pi_g\Delta^* = \pi_g\overline{h}\Delta^*$, então $fh' = h''\overline{h}$, com $h', h'' \in \pi_g$. Segue que $h'\pi_g = (h'')^{-1}\pi_g = \pi_g$ e, portanto,

$$\overline{h}\pi_g = (h'')^{-1} fh'\pi_g = (h'')^{-1} f\pi_g = (h'')^{-1}\pi_g\overline{h} = \pi_g\overline{h},$$

ou seja, π_g é um subgrupo normal do $[4g, 4g]$.

Mostremos agora que $[4g, 4g] = D_{4g} \underset{\sigma}{\times} \pi_g$.

Temos que D_{4g} é um subgrupo de ordem $8g$. Então, temos pelo Corolário 1.1 que:

$$[4g, 4g] = D_{4g}\pi_g = \{k \circ r \in [4g, 4g] : k \in D_{4g} \text{ e } r \in \pi_g\},$$

pois a ordem do $[4g, 4g]$ é igual a ordem do $D_{4g}\pi_g$. Logo da Proposição 1.5 temos:

$$8g = [D_{4g}\pi_g : \pi_g] = [D_{4g} : D_{4g} \cap \pi_g].$$

Como D_{4g} é um subgrupo de ordem $8g$, temos:

$$D_{4g} \cap \pi_g = \{e\}.$$

Portanto pelo Teorema 1.4, existe um homomorfismo $\sigma : D_{4g} \to Aut(\pi_g)$ tal que $[4g,4g]$ seja isomorfo a $D_{4g} \underset{\sigma}{\times} \pi_g$. □

Observemos a normalidade do π_g em $[4g,4g]$ implica na simetria do ladrilhamento de $\frac{U}{\pi_g}$ por cópias de $h\Delta^*$, com $h \in [4g,4g]$. De fato, se $\overline{h}\pi_g = \pi_g\overline{h}$ para todo $\overline{h} \in [4g,4g]$, então $\overline{h}$ mapeia a órbita $\pi_g\Delta^*$ numa órbita arbitrária $\pi_g\overline{h}\Delta^*$; fazendo com que o ladrilhamento de $\frac{U}{\pi_g}$ por cópias de $h\Delta^*$ seja simétrico.

O Teorema 3.4, cuja prova não é simples, é de vital importância para o estudo de reticulados sobre superfícies compactas os quais, por sua vez, são muito importantes no estudo de códigos corretores de erros, como podemos constatar em [14].

Seja $\Gamma^*(2,p,q)$ um grupo triângulo, tendo como região fundamental um triângulo Δ^*ABC cujos ângulos internos são $\widehat{A} = \frac{\pi}{2}, \widehat{B} = \frac{\pi}{q}$ e $\widehat{C} = \frac{\pi}{p}$, sendo r_1 reflexão sobre a reta que contem o lado de Δ^* onde estão os ângulos $\frac{\pi}{2}$ e $\frac{\pi}{p}$, r_2 reflexão sobre a reta que contem o lado de Δ^* onde estão os ângulos $\frac{\pi}{p}$ e $\frac{\pi}{q}$ e r_3 reflexão sobre a reta que contem o lado de Δ^* onde estão os ângulos $\frac{\pi}{2}$ e $\frac{\pi}{q}$. Associado com o grupo triângulo temos o grupo Fuchsiano,

$$\Gamma(2,p,q) = \Gamma^*(2,p,q) \cap PSL(2,\mathbb{C}),$$

com assinatura $(0;\ 2,\ p,\ q)$ e região fundamental $\Delta^* \cup r_1(\Delta^*)$.

De fato, como r_1, r_2 e $r_3 \notin PSL(2,\mathbb{C})$, temos que $\Gamma^*(2,p,q)$ não é um grupo Fuchsiano. Entretanto, tomemos $\Gamma(2,p,q) = \Gamma^*(2,p,q) \cap PSL(2,\mathbb{C})$. Temos $\Gamma^*(2,p,q) = \Gamma(2,p,q) \cup \Gamma(2,p,q)r_1$, pois se $S \in \Gamma^*(2,p,q) - \Gamma(2,p,q)$, então Sr_1 é a composição de duas isometrias com orientação inversa, então Sr_1 preserva orientação e assim $Sr_1 \in PSL(2,\mathbb{C})$. Também, $Sr_1 \in \Gamma^*(2,p,q)$, então $Sr_1 \in \Gamma(2,p,q)$ e $S = (Sr_1)r_1 \in \Gamma(2,p,q)r_1$. Segue que $\{T(\Delta^*) : T \in \Gamma^*(2,p,q)\}$ forma uma tesselação de U. Logo Δ^* é a região fundamental do $\Gamma^*(2,p,q)$. Agora seja k um ponto de Δ^*. As imagens do $\Gamma^*(2,p,q)$ do ponto k são pontos correspondentes de outros triângulos da tesselação, assim eles formam um conjunto discreto. Assim a orbita do $\Gamma(2,p,q)$ de cada ponto de U é um conjunto discreto. Portanto $\Gamma(2,p,q)$ é um grupo fuchsiano e $\Delta^* \cup r_1(\Delta^*)$ é a região fundamental do $\Gamma(2,p,q)$. Pelo Teorema 2.3 temos que $\{B, B' = r_1(B)\}$ é um ciclo elíptico e ambos os vértices são estabilizados por um grupo cíclico de ordem $m_1 = q$, $\{C\}$ é um ciclo elíptico, C é estabilizado por um grupo cíclico de ordem $m_2 = p$ e $\{A\}$ é um ciclo elíptico, A é estabilizado por um grupo cíclico de ordem $m_3 = 2$, pois

$$\frac{\pi}{q} + \frac{\pi}{q} = \frac{2\pi}{m_1} \Rightarrow m_1 = q,$$
$$\frac{\pi}{p} + \frac{\pi}{p} = \frac{2\pi}{m_2} \Rightarrow m_2 = p \text{ e}$$
$$\frac{\pi}{2} + \frac{\pi}{2} = \frac{2\pi}{m_3} \Rightarrow m_3 = 2.$$

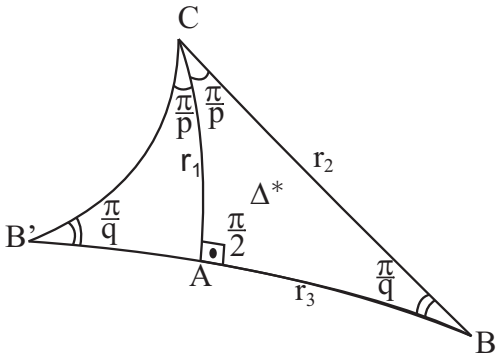


FIGURA 23

Logo, $\frac{U}{\Gamma(2,p,q)}$ decompõe em 3 vértices, 2 bordos (temos 2 pares de lados na região fundamental), e 1 face simplesmente conexa. Pela Fórmula de Euler, temos

$$2 - 2g = 3 - 2 + 1 = 2 \Rightarrow g = 0.$$

"Identificando" os lados AB com AB' e CB com CB' obtemos uma superfície homeomorfa com a esfera. Assim a assinatura do $\Gamma(2, p, q)$ é $(0; 2, p, q)$.

Deste modo, o grupo $\Gamma(2, p, q)$ é um subgrupo de índice 2 do grupo triângulo $\Gamma^*(2, p, q)$. Logo $\Gamma(2, p, q) \lhd \Gamma^*(2, p, q)$, pelo Exemplo 1.5.

Portanto π_g é um subgrupo normal de índice $4g$ do grupo Fuchsiano $\Gamma(2, 4g, 4g)$. De fato, temos $\pi_g \lhd [4g, 4g]$ e $\Gamma(2, 4g, 4g) \lhd [4g, 4g]$. Logo $r\pi_g = \pi_g r$, $\forall r \in [4g, 4g]$. Mas $\Gamma(2, 4g, 4g) \leq [4g, 4g]$. Disto segue que $r\pi_g = \pi_g r$, $\forall r \in \Gamma(2, 4g, 4g)$ e dai concluimos que $\pi_g \lhd \Gamma(2, 4g, 4g)$. Quanto ao índice, pelo Lema 3.1 a área da região fundamental do π_g é $4\pi(g-1)$ e pelo Corolário 2.1, temos que a área da região fundamental do $\Gamma(2, 4g, 4g)$ é:

$$\pi - \left(\frac{2\pi}{4g} + \frac{\pi}{4g} + \frac{\pi}{4g}\right) = \frac{\pi(g-1)}{g}.$$

Seja I o índice $[\Gamma(2, 4g, 4g) : \pi_g]$. Logo,

$$4\pi(g-1) = I\frac{\pi(g-1)}{g} \Rightarrow I = 4g.$$

Tesselações regulares da forma $\{4g, 4g\}$ podem ser encontradas como subtesselações da tesselação associada a um grupo triângulo Γ^*, ou à sua parte fuchsiana Γ com região fundamental Δ^*, ou $\Delta = \Delta^* \cup r_1(\Delta^*)$, a partir da determinação de $4g$−ágonos, formados por reuniões de cópias de Δ ou Δ^*, com as respectivas identificações de seus lados de forma a gerar uma superfície orientável de gênero g. Esse procedimento é equivalente a determinar um subgrupo do Γ isomorfo a π_g, o grupo fundamental da superfície compacta orientável de gênero g. Assim, os grupos triângulo se tornam o ambiente adequado para busca de tesselações relevantes para o propósito de projetar reticulados.

3.4 Reticulados Casados a Grupos

Definição 3.3 *Um reticulado S em um espaço métrico (M, d) é **casado** a um grupo $(G, *)$ se existir uma aplicação sobrejetiva $m : G \to S$, tal que para todo g e $g' \in G$,*

$$d(m(g), m(g')) = d(m(g * (g')^{-1}), m(e)).$$

Chamamos m de **aplicação casada**, e se m é injetiva dizemos que m^{-1} é um **rotulamento casado**.

Proposição 3.1 *Se $m : G \to S$ é uma aplicação casada então $H = m^{-1}(m(e))$ $= \{g \in G : m(g) = m(e)\}$ é um subgrupo de G e $g \equiv g'$ mod H se, e somente se, $m(g) = m(g')$.*

Demonstração:

Sejam g e $g' \in H$, isto é, $m(g) = m(e) = m(g')$. Como m é uma aplicação casada, temos:

$$d(m(g^{-1}), m(e)) = d(m(\left(g^{-1}\right)^{-1} * e), m(e)) = d(m(g), m(e)) = 0.$$

Como d é uma métrica em M, temos $m(g^{-1}) = m(e)$. Logo $g^{-1} \in H$.

Temos agora:

$$d(m(g * g'), m(e)) = d(m(\left(g^{-1}\right)^{-1} * g'), m(e)) = d(m(g^{-1}), m(g')) = 0.$$

Novamente como d é uma métrica em M, temos $m(g * g') = m(e)$. Logo $g * g' \in H$. Portanto, $H \leq G$.

Pela Proposição 1.2, temos:

$$\begin{aligned} g \equiv g' \bmod H &\Leftrightarrow (g')^{-1} * g \in H \Leftrightarrow m((g')^{-1} * g) = m(e) \\ &\Leftrightarrow d(m(g'), m(g)) = d(m((g')^{-1} * g), m(e)) = 0 \Leftrightarrow m(g) = m(g'). \end{aligned}$$

□

Assim, qualquer aplicação casada m corresponde a uma bijeção $gH \longmapsto m(g)$ das classes laterais à esquerda de H em G nos elementos de S. É imediato que se $H \lhd G$, então a aplicação quociente $\overline{m} : \frac{G}{H} \to S$ é um rotulamento casado. Dizemos que um rotulamento $m : G \to S$ é um **rotulamento efetivo** se H não contem um subgrupo normal de G não trivial (ou seja $\neq \{e\}$). Neste caso, dizemos que S é **efetivamente casado** a G. Esta é a situação geral porque se S não é efetivamente casado a G, então tomando $H' \neq H$ como o maior subgrupo normal de G contido em H, resulta que a função $\widetilde{m} : \frac{G}{H'} \to S$ fica bem definida, equivalentemente,

$$\widetilde{m}(g) = \widetilde{m}(g') \Leftrightarrow gH' = g'H' \text{ e } (g')^{-1} * g \in H' \subseteq H.$$

Exemplo 3.3 *Sejam A um espaço métrico com métrica d_A e G um grupo que possui uma métrica d_G tal que existe uma função $m : G \to A$ que é uma isometria. Então temos para quaisquer g e $h \in G$ que*

$$d_A(m(g), m(h)) = d_G(g, h) = d_G(g * h^{-1}, e) = d_A(m(g * h^{-1}), m(e)),$$

logo por definição m é um rotulamento casado.

Teorema 3.5 *Existe um rotulamento casado entre um reticulado S e um grupo $(G, *)$ se, e somente se, G é isomorfo a um subgrupo transitivo de $\Gamma(S)$, o grupo das simetrias de S.*

Demonstração:

Seja Θ um subgrupo transitivo de $\Gamma(S)$ com $\Theta \simeq G$, digamos $S = \{\theta(s) : \theta \in \Theta\}$ para um $s \in S$ fixo. Definimos, então, $m : \Theta \to S$ por $m(\sigma) = \sigma(s)$. Logo m é bijetiva. Com isso temos para σ e $\tau \in \Theta$ que

$$\begin{aligned} d_S(\sigma(s), \tau(s)) &= d_S(\sigma^{-1}\sigma(s), \sigma^{-1}\tau(s)) \\ &= d_S(s, \sigma^{-1}\tau(s)) = d_S(m(e), m(\sigma^{-1}\tau)) \end{aligned}$$

o que mostra que m é um rotulamento casado.

Reciprocamente, se $m : G \to S$ é um rotulamento casado (ou seja, podemos escrever $S = \{m(g) : g \in G\}$), vamos definir para cada $h \in G$, $f_h : S \to S$, $f_h(m(g)) = m(h * g)$ para cada $m(g) \in S$, então temos que

$$\begin{aligned} d_S(f_h(m(g_1), f_h(m(g_2))) &= d_S(m(h * g_1), m(h * g_2)) \\ &= d_S(m(g_1^{-1} * h^{-1} * h * g_2), m(e)) = d_S(m(g_1^{-1} * g_2), m(e)) \\ &= d_S(m(g_1), m(g_2)) \end{aligned}$$

e portanto, f_h é uma isometria de S para cada h. Com isto, fica definida uma função $f : G \to \Gamma(S)$. Se h_1 e $h_2 \in G$, temos que para todo $s = m(g) \in S$,

$$\begin{aligned} f_{h_1 * h_2}(m(g)) &= m((h_1 * h_2) * g) = m(h_1 * (h_2 * g)) \\ &= f_{h_1}(m(h_2 * g)) = f_{h_1}\left(f_{h_2}(m(g))\right) = \left(f_{h_1} \circ f_{h_2}\right)(m(g)). \end{aligned}$$

Logo, f é um homomorfismo. Além disso, se $f_h(m(g)) = m(g)$ para todo $m(g) \in S$, então $m(h * g) = m(g)$, $\forall g \in G$ e como m é um rotulamento casado, resulta que $h * g = g$, $\forall g \in G \Rightarrow h = e$.

Portanto, $Ker(f) = \{e\}$ e f é injetiva. Assim, $G \simeq Im(f) = \Theta \leq \Gamma(S)$. Finalmente, dado $s = m(e)$, se $h \in G$ é tal que $m(h) = s' \in S$, então $f_h(s) = f_h(m(e)) = m(h * e) = m(h) = s'$ e desse modo Θ é um subgrupo transitivo. □

3.5 G-linearidade

Um **mapeamento** é uma função $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ definida por

$$\phi(c) = (\beta(c), \gamma(c)) = (\beta(c_1), ..., \beta(c_n), \gamma(c_1), ..., \gamma(c_n)),\ \forall c = (c_1, ..., c_n) \in \mathbb{Z}_4^n;$$

onde as funções $\beta : \mathbb{Z}_4 \to \mathbb{Z}_2$ e $\gamma : \mathbb{Z}_4 \to \mathbb{Z}_2$ são especificadas na tabela abaixo:

c	0	1	2	3
$\beta(c)$	0	0	1	1
$\gamma(c)$	0	1	1	0

.

Um código binário C de comprimento $2n$ $\left(C \subseteq \mathbb{Z}_2^{2n}\right)$ é chamado $\mathbb{Z}_4$**-linear** se a menos de uma permutação de coordenadas, $C = \phi(H)$ para algum subgrupo H de $\mathbb{Z}_4^n$.

Abaixo generalizamos o conceito de $\mathbb{Z}_4$-linearidade para um grupo G qualquer.

Sejam G um grupo, d uma métrica de grupo em G e C um código de comprimento n sobre o alfabeto A e cuja métrica é d'. Diremos que C é G**-linear** se C, ou um código equivalente C', for imagem de um código de grupo H sobre o grupo G, isto é, $C = \phi(H)$, onde $\phi : G^n \to A^n$ é uma isometria entre os espaços métricos G^n e A^n.

Observação: Pelo Exemplo 3.3, $\phi : H \to C$ é um rotulamento casado e pelo Teorema 3.5 H é isomorfo a um grupo transitivo de simetrias de C.

Teorema 3.6 *O grupo de simetrias* $\Gamma(\mathbb{Z}_2^n)$ *do espaço* n*-dimensional* $(\mathbb{Z}_2^n, d_H)$ *é dado por* $\Gamma(\mathbb{Z}_2^n) \simeq \mathbb{Z}_2^n \underset{\varphi}{\times} S_n$, *sendo que o símbolo* $\underset{\varphi}{\times}$ *representa produto semidireto e* S_n *grupo simétrico de grau* n.

Exemplo 3.4 *Considere o grupo de simetrias de* $\mathbb{Z}_2^k$, *isto é,* $\Gamma(\mathbb{Z}_2^k) \simeq \mathbb{Z}_2^k \underset{\varphi}{\times} S_k$.
1) Quando $k = 2$, *temos que* $\Gamma(\mathbb{Z}_2^2) \simeq \mathbb{Z}_2^2 \underset{\varphi}{\times} S_2 \simeq D_4$. *De fato, consideremos o homomorfismo* $\varphi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_2^2)$ *definido por* $\varphi(0) = Id_{\mathbb{Z}_2^2} \in Aut(\mathbb{Z}_2^2)$ *e* $\varphi(1) \in Aut(\mathbb{Z}_2^2)$ *dado por*

$$\varphi(1)(00) = 00,\ \varphi(1)(01) = 10,\ \varphi(1)(10) = 01 \text{ e } \varphi(1)(11) = 11.$$

Note que $a = (1, 10)$ *e* $b = (1, 00)$ *satisfaz* $a^4 = b^2 = (0, 00)$ *e* $ba = a^3b = (0, 01)$. *Assim, identificando* r *com* a *e* s *com* b, *temos que* $\mathbb{Z}_2^2 \underset{\varphi}{\times} S_2 \simeq D_4 = \left\langle s, r : r^4 = s^2 = Id;\ r \circ s = s \circ r^3 \right\rangle$.

Como $U(\mathbb{Z}_2^2) = \mathbb{Z}_4$ *é um subgrupo de* D_4 *cuja ação é fortemente transitiva sobre* $\mathbb{Z}_2^2$*, obtemos que os códigos*

$$C_1 = \mathbb{Z}_2^2 = \{(0,0),(0,1),(1,0),(1,1)\},\ C_2 = \{(0,0),(1,1)\}\ \textit{e}\ C_3 = \{(0,0)\}$$

são $\mathbb{Z}_4$*-lineares.*
2) Quando $k = 3$*, temos que* $\Gamma(\mathbb{Z}_2^3) \simeq \mathbb{Z}_2^3 \underset{\varphi}{\times} S_3$*. Considere o subgrupo de* $\Gamma(\mathbb{Z}_2^3)$ *gerado pelas simetrias obtidas por uma rotação* r *de* $\frac{\pi}{2}$ *em torno do eixo paralelo ao eixo* Oz *e passando pelo centro de gravidade do cubo e por uma reflexão* s *em relação ao plano* xOy *passando pelo centro de gravidade do cubo (conforme Figura 24). Estas duas simetrias geram o subgrupo* D_4 *isomorfo a* $U(\mathbb{Z}_2^3) = \mathbb{Z}_4 \times \mathbb{Z}_2$*. Como* $U(\mathbb{Z}_2^3) = \mathbb{Z}_4 \times \mathbb{Z}_2$ *é um subgrupo de* $\Gamma(\mathbb{Z}_2^3)$ *cuja ação é fortemente transitiva sobre* $\mathbb{Z}_2^3$*, obtemos os códigos* $\mathbb{Z}_4 \times \mathbb{Z}_2$*-lineares. Por exemplo, tomemos*

$$\mathbb{Z}_2^3 = \{(0,0,0),(0,0,1),(0,1,0),(1,0,0),(0,1,1),(1,0,1),(1,1,0),(1,1,1)\}$$

e o mapeamento $\phi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_2^3$ *definido por*

$$\phi(c) = (\gamma(c_1), \beta(c_1), \gamma(c_2)), \forall c = (c_1, c_2) \in \mathbb{Z}_4 \times \mathbb{Z}_2,$$

isto é:

$$\phi(0,0) = (0,0,0);\ \phi(0,1) = (0,0,1);\ \phi(2,1) = (1,1,1);\ \phi(2,0) = (1,1,0);$$
$$\phi(3,0) = (0,1,0);\ \phi(1,0) = (1,0,0);\ \phi(1,1) = (1,0,1)\ e\ \phi(3,1) = (0,1,1).$$

Logo, $\phi(\mathbb{Z}_4 \times \mathbb{Z}_2) = \mathbb{Z}_2^3$*. Portanto* $\mathbb{Z}_2^3$ *é* $\mathbb{Z}_4 \times \mathbb{Z}_2$*-linear.*

Exemplo 3.5 *Seja*

$$C = \{(0,0,0,0),(1,0,0,0),(0,0,1,0),(1,0,1,0),(1,1,0,0),(0,1,0,0),(1,1,1,0),(0,1,1,0)\} \subset \mathbb{Z}_2^4$$

um código binário de comprimento 4*. Temos que* C *é um subgrupo de* $\mathbb{Z}_2^4$*. Tomemos o mapeamento* $\phi : \mathbb{Z}_4^2 \to \mathbb{Z}_2^4$ *definido acima. Logo*

$$\phi^{-1}(C) = \left\{(a,b) \in \mathbb{Z}_4^2 : \phi(a,b) \in C\right\} = \{(0,0),(3,0),(1,0),(2,0),(2,3),(1,3),(0,3),(3,3)\},$$

pois

$$\phi(0,0) = (0,0,0,0);\ \phi(3,0) = (1,0,0,0);\ \phi(1,0) = (0,0,1,0);\ \phi(2,0) = (1,0,1,0);$$
$$\phi(2,3) = (1,1,1,0);\ \phi(1,3) = (0,1,1,0);\ \phi(0,3) = (0,1,0,0)\ e\ \phi(3,3) = (1,1,0,0).$$

Mais ainda $\phi^{-1}(C)$ *é um subgrupo de* $\mathbb{Z}_4^2$ *e* $\phi(\phi^{-1}(C)) = C$*. Portanto pela definição de* $\mathbb{Z}_4$*-linearidade,* C *é um código* $\mathbb{Z}_4$*-linear.*

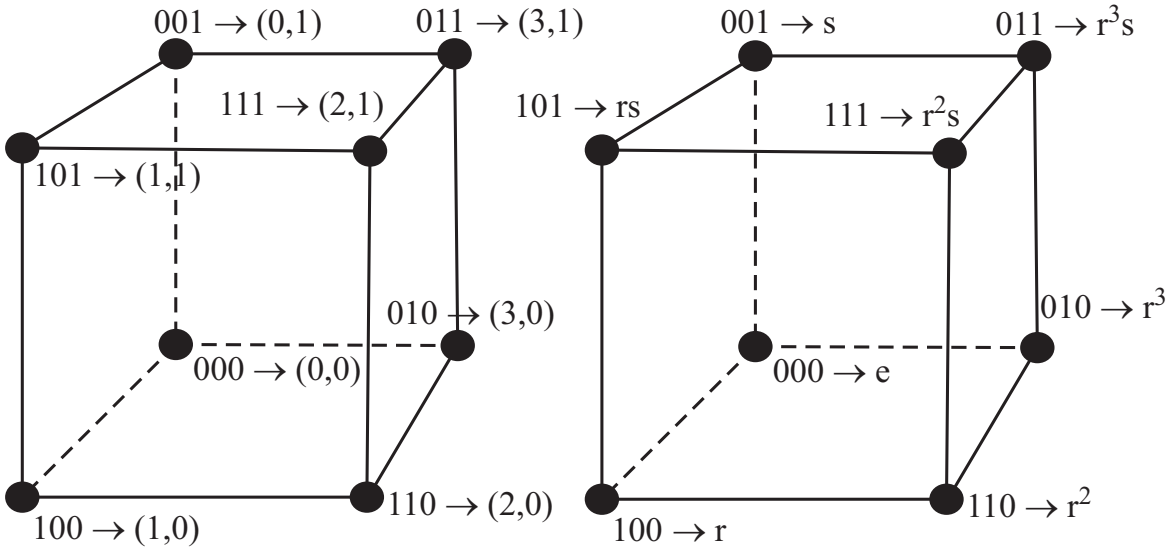


FIGURA 24

Encontrar o mapeamento $\phi : G \to A$ é, em princípio, um problema difícil. Todavia, como o alfabeto A está casado ao grupo G e ϕ é uma bijeção, a procura por este mapeamento é equivalente a determinar um subgrupo transitivo isomorfo ao grupo de simetrias de A conforme Teorema 3.5.

Uma das principais utilidades do conceito de G-linearidade é a obtenção de códigos binários a partir de códigos lineares sobre o grupo G, conforme [11].

Tendo em vista os resultados acima, concluimos que o principal objetivo buscado na G-linearidade é uma certa uniformidade geométrica do seu alfabeto, ou seja, determinar um subgrupo $U(A^n)$ do grupo de simetrias $\Gamma(A^n)$ que seja isomorfo ao grupo abstrato G e sua ação sobre A^n seja fortemente transitiva. Portanto, códigos G-lineares em A^n correspondem a subgrupo de G^n mapeados pelo rotulamento casado ϕ, estendido componente a componente.

3.6 Resultados Envolvendo Reticulados Geometricamente Uniformes

Exemplo 3.6 *Consideremos a tesselação* $\{8,8\}$, *no plano disco unitário* U. *Então o conjunto* S *constituido pelos centros dos octógonos da tesselação (ou equivalentemente dos vértices dos octógonos da tesselação dual) é geometricamente uniforme, já que para cada* $x \in S$ *fixo, temos que*

$$S = \left\{ g(x) : g \in [8,8] = \left\langle r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_1 \circ r_2)^8 = (r_2 \circ r_3)^8 = (r_3 \circ r_1)^2 = e \right\rangle \right\},$$

logo, dados D *e* E, *que são centros dos octógonos, sempre haverá uma composição* r *de reflexões nos lados do triângulo hiperbólico* Δ^* *com ângulos* $\frac{\pi}{2}, \frac{\pi}{8}$ *e* $\frac{\pi}{8}$ *de* A, B *e* C *e lados* a, b *e* c *respectivamente, sendo* r_1 *reflexão sobre a reta que contem o lado de* Δ^* *onde estão os ângulos* $\frac{\pi}{2}$ *e* $\frac{\pi}{8}, r_2$ *reflexão sobre a reta que contem o lado de* Δ^* *onde estão os ângulos* $\frac{\pi}{8}$ *e* $\frac{\pi}{8}$ *e* r_3 *reflexão sobre a reta que contem o lado de* Δ^* *onde estão os ângulos* $\frac{\pi}{2}$ *e* $\frac{\pi}{8}$, *(Figura 25) tal que* $r(D) = E$.

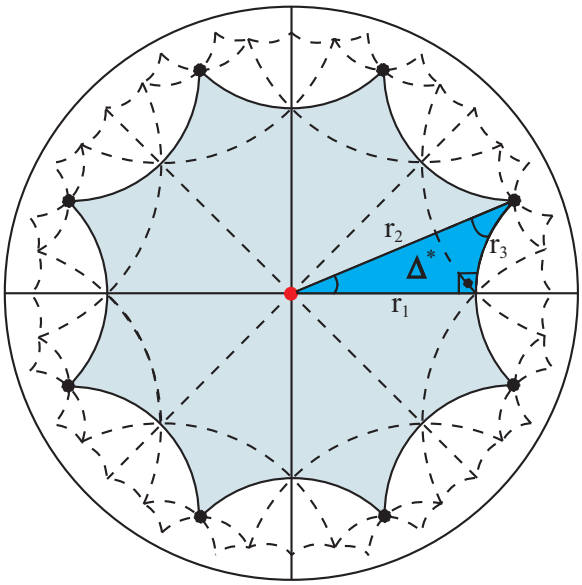


FIGURA 25

Como $[8,8] = D_8 \underset{\sigma}{\times} \pi_2$, *onde* $D_8 = \mathbb{Z}_8 \underset{\varphi}{\times} \mathbb{Z}_2$, *então* $D_8(x) = \{g(x) : x \in S \text{ fixo};\ g \in D_8\} = P$ *é um conjunto de vértices de um octógono e* P *é ele mesmo geometricamente uniforme com* $\Gamma(P) = D_8$. *Todavia,* $|P| = 8$ *e* $|D_8| = 16$. *Assim,* $\Gamma(P)$ *tem mais elementos que o necessário*

para gerar P. *Contudo, tomando os subgrupos* $G_1 = \mathbb{Z}_8$ *e* $G_2 = \mathbb{Z}_4 \times_{\varphi} \mathbb{Z}_2$ *contidos em* D_8 *então, temos, que* $P = G_1(x) = G_2(x)$. *Como* G_1 *e* G_2 *não são isomorfos, pois* $\mathbb{Z}_4 \times_{\varphi} \mathbb{Z}_2$ *não é abeliano, e* G_1 *e* G_2 *são subgrupos próprios de* D_8, *concluimos que um reticulado pode ter um grupo de simetrias com mais elementos que o próprio conjunto, como pode ter grupos de simetrias com o mesmo número de elementos, grupos estes não isomorfos.*

O teorema abaixo estabelece a importância dos códigos G-lineares, enquanto códigos geometricamente uniformes.

Teorema 3.7 *Seja* S *um reticulado, então são equivalentes as seguintes afirmações:*
(i) S *é geometricamente uniforme;*
(ii) *Existe um rotulamento casado entre* S *e o grupo* $U(S)$;
(iii) S *é* $U(S)$*-linear com* $m : U(S) \to S$.

Demonstração:

(i) $\Leftrightarrow$ (ii) segue do Teorema 3.5, e (i) $\Leftrightarrow$ (iii) segue imediatamente do Exemplo 3.3. □

Este resultado mostra que a existência da G-linearidade, sob o ponto de vista da construção de códigos geometricamente uniformes, está vinculada à determinação do grupo de simetrias do reticulado associado, isto é, todo reticulado S é $U(S)$-linear. Este resultado é de vital importância para o estudo de reticulados sobre superfícies compactas quocientes obtidas dos planos euclidiano e hiperbólico por um grupo de isometrias, os quais, por sua vez, são muito importantes no estudo de códigos corretores de erros, como podemos constatar em [14].

Lema 3.2 *Seja* S *um reticulado geometricamente uniforme e* P *e* $Q \in S$ *quaisquer. Então existe uma isometria* $g \in \Gamma(S)$ *tal que* $g(P) = Q$ *e* $g(D_P(S)) = D_Q(S)$. *Em outras palavras, as regiões de Voronoi são todas congruentes.*

Demonstração:

Temos que $R \in D_P(S)$ se, e somente se, $d(P,R) \leq d(g(P),R)$ mas

$$\begin{aligned} d(g(R),Q) &= d(g(R),g(P)) = d(R,P) \\ &\leq d(R,g(P)) = d(g(R),g(g(P))) = d(g(R),g(Q)). \end{aligned}$$

Logo $g(R) \in D_Q(S)$ e $g(D_P(S)) \subseteq D_Q(S)$. Tomemos g^{-1} e seja $A \in D_Q(S)$.
Sabemos que $A \in D_Q(S)$ se, e somente se, $d(Q,A) \leq d(g^{-1}(Q),A)$ mas

$$\begin{aligned} d(g^{-1}(A),P) &= d(g^{-1}(A),g^{-1}(Q)) = d(A,Q) \\ &\leq d(A,g^{-1}(Q)) = d(g^{-1}(A),g^{-1}(g^{-1}(Q))) = d(g^{-1}(A),g^{-1}(P)). \end{aligned}$$

Logo $g^{-1}(A) \in D_P(S) \Rightarrow A \in g(D_P(S))$ e daí $D_Q(S)) \subseteq g(D_P(S))$.
Portanto $g(D_P(S)) = D_Q(S)$. □

O fato de toda região de Voronoi de um reticulado S geometricamente uniforme ter a mesma forma é uma propriedade simétrica muito importante porque a forma da região de Voronoi determina quase todas as propriedades de S que são importantes no estabelecimento de comunicação digital. A recíproca deste lema não é verdadeira.

Capítulo 4

Partições Geometricamente Uniformes Hiperbólicas

O conceito de partição geometricamente uniforme foi proposto por Forney, [8], no contexto de reticulados euclidianos.

Neste capítulo generalizamos o conceito de partições geometricamente uniformes em espaços Hiperbólicos. Também mostramos uma caracterização de códigos de classes laterais generalizados através do conceito de códigos G-lineares, conforme estabelecido em [15].

Um dos principais objetivos de códigos geometricamente uniformes é a construção de partições geometricamente uniformes e em particular códigos de classes laterais generalizados.

Embora os grupos de isometrias hiperbólicos tenham maior complexidade que os grupos de isometrias euclidianos os procedimentos e os conceitos para partições geometricamente uniformes podem ser considerados os mesmos.

O objetivo deste capítulo é estender a teoria de modo a permitir que reticulados casados a grupos, possam ser decompostos em partições geometricamente uniformes.

4.1 Partições Geometricamente Uniformes Hiperbólicas

Definição 4.1 *Seja* S *um reticulado geometricamente uniforme, digamos* $S = \{u(s_0) : u \in U(S)\}$ *para algum* s_0 *fixo em* S. *Seja* U' *um subgrupo normal de* $U(S)$, *grupo gerador do reticulado* S. *A órbita de* s_0 *por* U' *será denotada por* S', *onde* $S' = \{u(s_0) : u \in U'\}$, *segue que se*

$$U(S) = U' \cup U'a \cup U'b \cup ...$$

é a decomposição de $U(S)$ *em classes de* U', *então a partição de* S *é dada por*

$$S = U's_0 \cup U'as_0 \cup U'bs_0 \cup ...,$$

denotada por S/S', *e é chamada uma* ***partição geometricamente uniforme***. *Denotamos* $U(S')$ *por* U'.

Teorema 4.1 ***(Teorema de Forney).*** *Se* S/S' *é uma partição geometricamente uniforme, então os elementos de* S/S' *são geometricamente uniformes, mutuamente congruentes e tem* U' *como grupo gerador comum.*

Demonstração:

Seja A denotado por $A = U(S)/U'$. Se $a \in A$; $a = U'u_a = u_aU'$ para algum $u_a \in U(S)$. Denotando por $S'(a)$ o elemento correspondente da partição S/S' temos que:

$$S'(a) = u_aU'(s_0) = \bigcup_{u \in U'} u_a\,[u(s_0)] = u_a \left[\bigcup_{u \in U'} u(s_0) \right] = u_a(S').$$

Portanto, $S'(a) \simeq S'$ e para cada $a \in A$, os $S'(a)$ são todos congruentes. Por outro lado,

$$S'(a) = U'u_a(s_0) = \bigcup_{u \in U'} u\,[u_a(s_0)]$$

é a órbita de $u_a(s_0)$ por U'. Logo, todos os $S'(a)$ são geometricamente uniformes com grupo gerador comum U'. □

A partir deste Teorema faz sentido utilizar a notação $U(S')$ para U'.

Exemplo 4.1 *No espaço euclidiano $\mathbb{R}^n$, se Λ é um reticulado geometricamente uniforme e Λ' é um subreticulado de Λ de índice finito, então qualquer reticulado $S = \Lambda + a$, $a \in \mathbb{R}^n$ é particionado em $|\Lambda/\Lambda'|$ subreticulados de reticulados geometricamente uniformes $\Lambda' + a + v$ com $v \in [\Lambda/\Lambda']$ para algum conjunto completo de representantes $[\Lambda/\Lambda']$ de Λ módulo Λ'. Por exemplo:*

Sejam o reticulado $\Lambda = \mathbb{Z}^2$, o subreticulado $\Lambda' = 2\mathbb{Z}^2$ e a partição $\Lambda/\Lambda' = \mathbb{Z}^2/2\mathbb{Z}^2$ (Figura 26). Observe que $|\Lambda/\Lambda'| = 4$, podendo ser representados por: $2\mathbb{Z}^2 = 2\mathbb{Z}^2 + (0,0)$; $2\mathbb{Z}^2 + (1,0)$; $2\mathbb{Z}^2 + (0,1)$ e $2\mathbb{Z}^2 + (1,1)$.

Note que neste caso $U(\mathbb{Z}^2) = \langle e_1, e_2\rangle$, $U(2\mathbb{Z}^2) = \langle 2e_1, 2e_2\rangle$, $U(2\mathbb{Z}^2 + (1,0)) = \langle 2e_1, 2e_2\rangle + e_1$, $U(2\mathbb{Z}^2 + (0,1)) = \langle 2e_1, 2e_2\rangle + e_2$ e $U(2\mathbb{Z}^2 + (1,1)) = \langle 2e_1, 2e_2\rangle + e_1 + e_2$. Logo $\mathbb{Z}^2 = \{u(0,0) : u \in \langle e_1, e_2\rangle\}$.

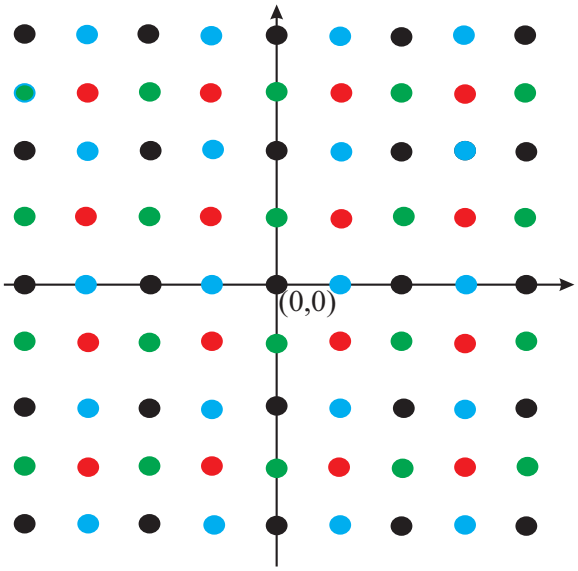


FIGURA 26

No caso hiperbólico, temos alguns pontos a considerar: Como a tesselação dual é gerada pelas translações, então a condição equivalente a $T(\Lambda) = \Lambda$, onde T denota translação, é exatamente o fato de a tesselação ser autodual. Isto é equivalente a ser do tipo $\{p, p\}$. No caso autodual, como o grupo π_g tem uma única relação $\left(\prod_{i=1}^{g} [a_i, b_i] = e\right)$, segue que π_g só tem o elemento neutro de ordem finita. Quando isto ocorre dizemos que o mesmo é um **grupo livre de torção**.

4.2 Rotulamentos Isométricos

Definição 4.2 *Seja S/S' uma partição geometricamente uniforme. Dizemos que um grupo A é um **grupo de rótulos** para S/S' se existe um isomorfismo*

$$m : A \to \frac{U(S)}{U(S')},$$

m *é chamado de* ***isomorfismo de rotulamento.*** *A aplicação bijetiva*

$$\overline{m} : A \to \frac{S}{S'},$$

definida pela composição do isomorfismo de rotulamento com a bijeção

$$\frac{U(S)}{U(S')} \to \frac{S}{S'}$$

é chamado de ***rotulamento isométrico*** *dos subconjuntos de* S *pertencentes à partição* S/S'**.**

Podemos visualizar esta definição pelo diagrama:

$$\begin{array}{ccccc} A & \to & \frac{U(S)}{U(S')} & \to & \frac{S}{S'} \\ a & \mapsto & u_a U' & \mapsto & \overline{m}(a) = u_a(S') = \{u_a u(s_0) : u \in U'\} \end{array} .$$

O fato de $\overline{m}$ ser uma função bem definida é consequência de que se $u_a U' = v U'$, então $v^{-1}u_a \in U' = U(S')$. Logo, $v^{-1}u_a(S') = S'$. Portanto, $u_a(S') = v(S')$.

As seguintes propriedades são imediatas:

(i) $\overline{m}(e_A) = S'$, onde e_A denota o elemento neutro de A;
(ii) $\left|\frac{S}{S'}\right| = \left|\frac{U(S)}{U(S')}\right| = |A|$.

Uma partição S/S' admite rotulamento isométrico por um grupo A se:

(a) S é geometricamente uniforme;
(b) Os subconjuntos da partição geometricamente uniformes são mutuamente congruentes;
(c) Existem grupos de isometrias $U(S)$ e $U(S')$ tais que $U(S)$ gera S, $U(S')$ gera S', $U(S') \lhd U(S)$ e $A \simeq \frac{U(S)}{U(S')}$.

Definição 4.3 *A aplicação bijetiva* $\overline{m} : A \to S/S'$ *que leva um rótulo* $a \in A$ *no subconjunto* $\overline{m}(a) \subseteq S$ *induzida pela partição* S/S' *é denominada* ***aplicação de rotulamento****.*

O teorema a seguir mostra uma condição necessária e suficiente para se obter um rotulamento isométrico.

Teorema 4.2 *Uma aplicação de rotulamento* $\overline{m} : A \to S/S'$ *é um rotulamento isométrico se, e somente se, para todo* $a \in A$ *existe uma isometria* $u_a : S/S' \to S/S'$ *tal que para todo* $b \in A$, $\overline{m}(ab) = u_a(\overline{m}(b))$.

Demonstração:

Se $\overline{m} : A \to S/S'$ é um rotulamento isométrico, do isomorfismo $A \simeq \frac{U(S)}{U(S')}$ temos que $ab \mapsto u_{ab}U'$ e $ab \mapsto u_a U' u_b U' = u_a u_b U'$ e da bijeção $\frac{U(S)}{U(S')} \to \frac{S}{S'}$ temos que $u_{ab}U' \mapsto u_{ab}S'$ e $u_a u_b U' \mapsto u_a u_b S'$. Logo $u_{ab}S' = u_a u_b S'$.

Portanto,

$$\overline{m}(ab) = u_{ab}S' = u_a u_b S' = u_a[\overline{m}(b)]$$

Reciprocamente, se vale $\overline{m}(ab) = u_a(\overline{m}(b))$, para todos $a, b \in A$, então $u_{ab}S' = u_a u_b S'$. Logo $u_{ab}U' = u_a u_b U' = u_a U' u_b U'$, isto é, $A \simeq \frac{U(S)}{U(S')}$.

Portanto $\overline{m}$ é um rotulamento isométrico. □

Exemplo 4.2 *Sejam o reticulado* $S = \mathbb{Z}^2$*, o subreticulado* $S' = 2\mathbb{Z}^2$*, o centro* O *do quadrado* $\overline{0123}$*, o grupo de rótulos* $A = \mathbb{Z}_4$ *para a partição* $S/S' = \mathbb{Z}^2/2\mathbb{Z}^2$ *e a região fundamental* R *do quociente* S/S' *(Figura 27).*

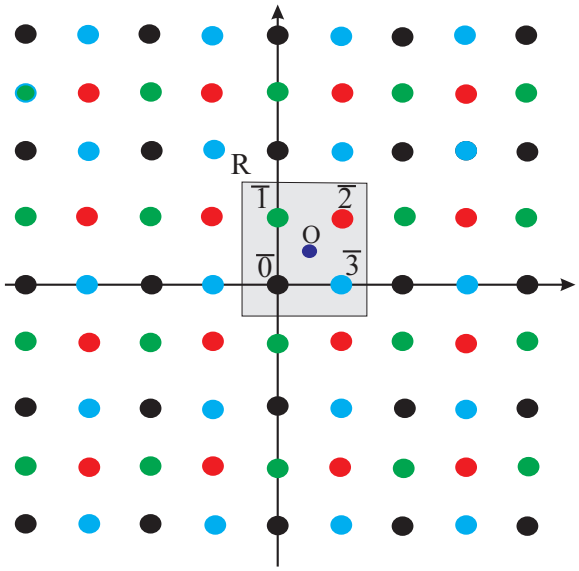


FIGURA 27

Para $a = \overline{0}$ uma isometria u_a é a identidade.
Para $a = \overline{1}$ uma isometria u_a é a rotação de centro O e ângulo $\frac{\pi}{2}$ no sentido horário.
Para $a = \overline{2}$ uma isometria u_a é a rotação de centro O e ângulo π.
Para $a = \overline{3}$ uma isometria u_a é a rotação de centro O e ângulo $\frac{\pi}{2}$ no sentido antihorário.

4.3 Propriedades Elementares dos Rotulamentos Isométricos

Dado um rotulamento isométrico $\overline{m} : A \to S/S'$ existem várias transformações de rotulamentos simples que resultam em rotulamentos isométricos. A seguir apresentaremos alguns resultados elementares dos rotulamentos isométricos.

Proposição 4.1 *Se* $\overline{m} : A \to S/S'$ *é um rotulamento isométrico e* $T : A \to A$ *é um automorfismo, então o rotulamento* $\overline{m} \circ T : A \to S/S'$ *definido por* $a \mapsto \overline{m}[T(a)]$ *é também um rotulamento isométrico.*

Demonstração:

Como T é um automorfismo de A temos que T leva todos elementos de A em elementos de A, logo como $\overline{m}$ é um rotulamento isométrico temos que $\overline{m} \circ T$ também é um rotulamento isométrico. □

Proposição 4.2 *Se* $\overline{m} : A \to S/S'$ *é um rotulamento isométrico então o rotulamento* $\overline{m}t_b : A \to S/S'$ *definido por* $a \mapsto \overline{m}(ab)$ *para qualquer* $b \in A$ *é também um rotulamento isométrico.*

Demonstração:

Como $\overline{m}$ é um rotulamento isométrico temos pelo Teorema 4.2 que para todo $a \in A$ existe uma isometria $u_a : S/S' \to S/S'$ tal que $\overline{m}(ab) = u_a(\overline{m}(b))$, $\forall b \in A$. Logo temos que $\overline{m}t_b$ é um rotulamento isométrico. □

As duas proposições acima implicam que se a partição S/S' admite um rotulamento isométrico com grupo de rótulos A, então alguma transformação afim definida por $a \mapsto T(a) + b$ onde a e $b \in A$, também produz um rotulamento isométrico. É interessante notar que em um espaço métrico onde a métrica natural é a métrica de Hamming uma transformação afim é uma isometria.

Proposição 4.3 *Se $\overline{m} : A \to S/S'$ é um rotulamento isométrico, e u é uma simetria em $U(S)$, então o rotulamento $\overline{m}_u : A \to S/u(S')$ definido por $a \mapsto u[\overline{m}(a)]$ é um rotulamento isométrico.*

Demonstração:

A demonstração desta proposição decorre diretamente do Teorema 4.2. □

4.4 Códigos Geometricamente Uniformes em Espaços de Sinais

A próxima definição estabelece o que se entende por um reticulado geometricamente uniforme no espaço.

Sejam $(A, *)$ um grupo e $I \subseteq \mathbb{Z}$ um conjunto (eventualmente finito). Considere o espaço de sequências $A^I = \{(a_k)_{k\in I} : a_k \in A,\ \forall k \in I\}$, onde A denota o alfabeto e I um conjunto de índices. Considere a estrutura natural de grupo em A^I. Para todos a e $b \in A^I$, $a * b = (a_k * b_k)_{k\in I}$. Dados um reticulado S, uma partição geometricamente uniforme S/S' e um conjunto de rótulos A, extendemos de maneira natural a aplicação de rotulamento isométrico para

$$\underline{m} : A^I \to (S/S')^I.$$

Desta forma, chamamos de **código de rótulos** a qualquer subconjunto $D \subseteq A^I$. Logo, $\underline{m}(c) = (\overline{m}(c_k))_{k\in I}$, $c \in D$, é a sequência de subconjuntos de S selecionados pela sequência de rótulos $c \in D$ pela aplicação de rotulamento $\overline{m}$. Com estas notações, um **código de espaço de sinais** é estabelecido como

$$C(S/S', D) = \bigcup_{c\in D} \underline{m}(c).$$

Como

$$C(S/S', D) = \bigcup_{c\in D} \underline{m}(c) = \bigcup_{c\in D} (\overline{m}(c_k))_{k\in I}, \text{ sendo } c = (c_k)_{k\in I},$$

temos que $C(S/S', D) \subseteq S^I$.

Definição 4.4 *Uma sequência de sinais $s \in S^I$, $s = (s_k)_{k\in I}$, é uma **sequência código** ou, equivalentemente, um elemento de $C(S/S', D)$ se existe algum $c \in D$ tal que $s_k \in \overline{m}(c_k)$, para todo $k \in I$.*

Se $S \subseteq \mathbb{R}^n$, então $C(S/S', D) \subseteq (\mathbb{R}^n)^I$. Devemos notar que como o plano hiperbólico P_h não é um espaço vetorial normado compatível com a métrica hiperbólica, não há uma forma padrão para produtos análogos ao produto cartesiano.

Um codificador para o código de rótulos D gera uma sequência codificada de rótulos $c = (c_k)_{k\in I}$ pertencentes a D. A sequência individual c é determinada por uma sequência adequada de dados na entrada do codificador. Agora, a aplicação de rotulamento $\overline{m}$ é usada para determinar a sequência de subconjuntos $\underline{m}(c) = (\overline{m}(c_k))_{k\in I}$. Outros dados de entrada são usados então para determinar um elemento (sequência) específico de $\underline{m}(c)$ para que possa ser transmitido através do canal. Esta última operação é de natureza secundária, as propriedades

de um código gerado por um codificador deste tipo dependem fundamentalmente das propriedades do código de espaço de sinais $C(S/S', D)$ que são determinados pela entrada a ser codificada por D.

Os resultados seguintes descrevem como um codificador deve ser projetado nos códigos de espaços de sinais hiperbólicos.

Seja S/S' uma partição geometricamente uniforme gerada por uma partição cujos grupos geradores são $U(S)$ e $U(S')$, e $A \simeq \frac{U(S)}{U(S')}$ é o grupo de rótulo.

Definição 4.5 *Sejam S/S' uma partição geometricamente uniforme com grupo de rótulos A e $D \subseteq A^I$ um subgrupo normal $\left(D \lhd A^I\right)$, então um* ***código de classes laterais generalizado*** *é o subconjunto*

$$C(S/S', D) = \{s \in \underline{m}(c) : c \in D\} \subseteq S^I.$$

O teorema a seguir fornece uma conexão entre a G-linearidade e os códigos de classes laterais generalizados.

Teorema 4.3 *Nas hipóteses da Definição 4.5, um código de classes laterais generalizado é um código $U(S)$-linear.*

Demonstração:

Como S é geometricamente uniforme seja o rotulamento dado por:

$$\begin{array}{rccc} \mu: & G = U(S)^I & \to & S^I \\ & u & \mapsto & u(s_0) \end{array}$$

para algum s_0 fixo em S^I. Denotando $A^I = \frac{U(S)^I}{U(S')^I} = \left\{uU(S')^I : u \in U(S)^I\right\}$ e o rotulamento isométrico estendido bem definido

$$\begin{array}{rccc} \underline{m}: & A^I & \to & (S/S')^I \\ & uU(S')^I & \mapsto & u(S')^I \end{array} .$$

De fato, se $uU(S')^I = vU(S')^I$, então $u^{-1}v \in U(S')^I$. Logo $u^{-1}v(S')^I = (S')^I$. Portanto, $u(S')^I = v(S')^I$. Seja, agora, $H = \left\{u \in G : uU(S')^I \in D\right\}$, então se u e $v \in H$, temos que $u(U')^I$ e $v(U')^I \in D$ e como $D \leq A^I$, temos que $uv^{-1}(U')^I \in D$ e $uv^{-1} \in H$. Como $e \in H$, temos que $H \leq G$. Por outro lado, como

$$\mu(H) = \{u(s_0) : u \in H\} = \bigcup_{u(U')^I \in D} u(S')^I = \bigcup_{c \in D} \underline{m}(c) = C(S/S', D),$$

isto mostra que $C(S/S', D)$ é $U(S)$-linear. □

A definição proposta originalmente por Forney, [8], impõe a condição de que o grupo de rótulos A seja abeliano. Em nossa proposta mais geral temos que impor somente a condição de que o código D seja um subgrupo normal do grupo A^I.

Definição 4.6 *As classes laterais de D podem ser escritas como Da, onde $a \in A^I$. Para cada classe lateral o rotulamento $\underline{m} : A^I \to (S/S')^I$ define subconjuntos de S^I chamados de* ***rótulos transladados*** *de $C(S/S', D)$ dados por*

$$C(S/S', Da) = \bigcup_{c \in D} \underline{m}(ca).$$

Lema 4.1 *Se* $C(S/S', D)$ *é um código de classes laterais generalizado, então*

$$\left(\frac{S^I}{S'^I}\right) \simeq \left(\frac{S}{S'}\right)^I$$

é uma partição geometricamente uniforme e $\underline{m} : A^I \to (S/S')^I$ *é um rotulamento isométrico para esta partição.*

Demonstração:

(a) $U(S^I) = U(S)^I$. De fato, se $\underline{s_0} = (s_{0,k})_{k\in I}$ onde $s_{0,k} = s_0$ para todo $k \in I$, então dado $s = (s_k)_{k\in I} \in S^I$ existe um $u_k \in U(S)$ tal que $u_k(s_0) = s_k$ para todo $k \in I$. Assim, tomando $u = (u_k)_{k\in I}$ temos que $u \in U(S)^I$ e $u(\underline{s_0}) = (u_k(s_0))_{k\in I} = s$. Por outro lado, se $H \leq U(S)^I$, então $H = \prod_{k\in I} H_k$ onde $H_k \leq U(S)$ para todo $k \in I$, e se $U(S^I) = H \nleqq U(S)^I$ temos $H_k \nleqq U(S)$ para todo $k \in I$, mas neste caso teremos $S^I = H\underline{s_0} = \left(\prod_{k\in I} H_k\right)(\underline{s_0}) = \prod_{k\in I}(H_k s_0)$, isto é, $S = H_k s_0$, $\forall k \in I$, contrariando a minimalidade de $U(S)$. Portanto $U(S^I) = U(S)^I$;
(b) $\frac{U(S)^I}{U(S')^I} = \left(\frac{U(S)}{U(S')}\right)^I$. De fato, dados $u = (u_k)_{k\in I}$ e $v = (v_k)_{k\in I} \in U(S)^I$, temos $uv = (u_k v_k)_{k\in I}$. Logo,

$$\begin{aligned}(u_k)_{k\in I}U(S')^I &= \left\{(u_k)_{k\in I}(w_k)_{k\in I} : (w_k)_{k\in I} \in U(S')^I\right\}\\ &= \left\{(u_k w_k)_{k\in I} : (w_k)_{k\in I} \in U(S')^I\right\} = (u_k U(S'))_{k\in I}.\end{aligned}$$

Portanto $\frac{U(S)^I}{U(S')^I} = \left(\frac{U(S)}{U(S')}\right)^I$;
(c) $U(S')^I \lhd U(S)^I$ segue da definição de normalidade e do fato de que $U(S') \lhd U(S)$ por hipótese;
(d) $\underline{m} : A^I \to (S/S')^I$ é uma isometria onde $\frac{U(S)^I}{U(S')^I}$ induz uma partição geometricamente uniforme $\frac{S^I}{S'^I}$ com espaço de rótulos $A^I \simeq \frac{U(S)^I}{U(S')^I}$. □

Lema 4.2 *Com as notações anteriores, se* $D \lhd A^I$, *então com as estruturas induzidas,* $(S')^I \leq C(S/S', D) \leq S^I$. *Com isso temos os isomorfismos:*

$$\frac{S^I}{C(S/S', D)} \simeq \frac{A^I}{D};\ \frac{C(S/S', D)}{(S')^I} \simeq D \ \ e \ \ \frac{S^I}{(S')^I} \simeq \frac{A^I}{e_{A^I}} \simeq A^I,$$

ou seja, as cadeias de partições de grupos $S^I/C(S/S', D)/(S')^I$ *e* $A^I/D/e_{A^I}$ *são isomorfas.*

Demonstração:

A demonstração será feita para o caso $|I| = 1$. Para o caso geral, segue através da consideração de coordenadas.

$$\begin{array}{ccccc} A & \to & \frac{U(S)}{U(S')} & \to & \frac{S}{S'} \\ a & \mapsto & u_a U' & \mapsto & \overline{m}(a) = u_a(S') \end{array}$$

$$\begin{array}{ccc} U(S) & \xrightarrow{f} & S \\ | & & | \\ V & \to & C(S/S', D) \\ | & & | \\ U(S') & \to & S' \end{array}$$

(a) $C(S/S', D) \leq S$. Se ϕ e $\psi \in C(S/S', D)$, então existem c_1 e $c_2 \in D$ tais que $\phi \in \overline{m}(c_1) = u_{c_1}S'$ e $\psi \in \overline{m}(c_2) = u_{c_2}S'$. Se $f : U(S) \to S$ é a bijeção que induz a estrutura de grupo em S, então existem v e $w \in U(S)$ tais que $f(v) = \phi$ e $f(w) = \psi$. Com isso,

$$vU' = u_{c_1}U'$$
$$wU' = u_{c_2}U',$$

onde $vw \in u_{c_1}U'u_{c_2}U' = u_{c_1}u_{c_2}U' = u_{c_1c_2}U'$ e $f(vw) = \phi\psi \in \overline{m}(c_1c_2) = u_{c_1c_2}S'$. Portanto, $\phi\psi \in C(S/S', D)$.

Além disso, como $vU' = u_{c_1}U'$, resulta que $(vU')^{-1} = (u_{c_1}U')^{-1}$ ou $v^{-1}U' = u_{c_1}^{-1}U' = u_{c_1^{-1}}U'$. Portanto, $\phi^{-1} \in \overline{m}(c_1^{-1}) \in C(S/S', D)$ e $C(S/S', D) \leq S$;
(b) $S' \leq C(S/S', D)$. Como $C(S/S', D) = \underset{c\in D}{\cup} \overline{m}(c)$, definimos $V := f^{-1}(C(S/S', D))$. Assim, $V \leq U(S)$ e

$$V = f^{-1}(C(S/S', D)) = f^{-1}\left(\underset{c\in D}{\cup} \overline{m}(c)\right) = \underset{c\in D}{\cup} f^{-1}(\overline{m}(c)) = \underset{c\in D}{\cup} u_cU'.$$

Em particular, $m(1) = U' \subseteq V$, e segue que

$$S' = f(U') \subseteq f(V) = C(S/S', D) \text{ e } S' \leq C(S/S', D);$$

(c) $\frac{A}{D} \simeq \frac{S}{C(S/S',D)}$. Como $V = f^{-1}(C(S/S', D))$, temos tomando quocientes em f que

$$\frac{U(S)}{V} \simeq \frac{S}{C(S/S', D)}.$$

Considerando

$$\Phi : A \to U(S),\ a \longmapsto u_aV.$$

Temos que Φ está bem definida porque $u_1U' = u_2U'$ implica $u_2^{-1}u_1 \in U' \subseteq V$. Portanto, $u_1V = u_2V$. Temos também que $\ker \Phi = D$.

De fato, provar que $\ker \Phi = D$ e equivalente a provar que $u_a \in V$ se, e somente se, $a \in D$. ($\Rightarrow$) Seja $u_a \in V$. Logo,

$$u_aU' \subseteq V \Rightarrow u_aS' = \overline{m}(a) \subseteq C(S/S', D) \Rightarrow a \in D.$$

($\Leftarrow$) Seja $a \in D$. Logo,

$$u_aS' \subseteq C(S/S', D) \Rightarrow u_aU' \subseteq V \Rightarrow u_a \in V$$

Portanto,

$$\frac{A}{D} \simeq \frac{U(S)}{V} \simeq \frac{S}{C(S/S', D)};$$

$$\begin{array}{ccccc} & & U(S) & \xrightarrow{f} & S \\ & & | & & | \\ A & \xrightarrow{m} & \frac{U(S)}{U(S')} & \xrightarrow{\bar{f}} & \frac{S}{S'} \end{array}$$

(d) $D \simeq \frac{D}{\{e\}} \simeq \frac{C(S/S',D)}{S'}$. Considerando, agora,

$$m : A \to \frac{U(S)}{U(S')}$$

o isomorfismo de rotulamento dado por $m(c) = u_c U'$, temos que

$$m(D) = \frac{V}{U(S')}.$$

De fato, como $a \in D \Leftrightarrow u_a \in V$, temos:

$$m(D) = \bigcup_{a \in D} u_a U' = \bigcup_{u_a \in V} u_a U' = \frac{V}{U(S')},$$

isto é,

$$D \simeq \frac{V}{U(S')}. \tag{4.1}$$

Fazendo agora $f \mid V$ e tomando quocientes, temos

$$\frac{V}{U(S')} \simeq \frac{C(S/S', D)}{S'}, \tag{4.2}$$

de 4.1 e 4.2 temos então que:

$$D \simeq \frac{C(S/S', D)}{S'};$$

Por fim, $\frac{S}{S'} \simeq A$ segue diretamente do rotulamento isométrico $\overline{m}$. □

Lema 4.3 *Os rótulos transladados de* $C(S/S', D)$ *são as classes à direita de* $C(S/S', D)$ *em* S^I *sob a estrutura de grupo induzida pela* $f : U(S)^I \to S^I$, *definida por* $f(u) = u(\underline{s_0})$.

Demonstração:

Sejam $f : U(S)^I \to S^I$ a bijeção que induz a estrutura de grupo em S^I, $a \in A^I$ e $C(S/S', Da)$ um rótulo transladado de $C(S/S', D)$.

$$\begin{aligned} f^{-1}(C(S/S', Da)) &= f^{-1}\left(\bigcup_{c \in D} \underline{m}(ca)\right) = \bigcup_{c \in D} f^{-1}(\underline{m}(ca)) = \bigcup_{c \in D} u_{ca}(U')^I \\ &= \bigcup_{c \in D} u_c u_a (U')^I = \left[\bigcup_{c \in D} u_c (U')^I\right] u_a = \left[\bigcup_{c \in D} f^{-1}(\underline{m}(c))\right] f^{-1}(f(u_a)) \\ &= \left[f^{-1}\left(\bigcup_{c \in D} \underline{m}(c)\right)\right] f^{-1}(f(u_a)) = f^{-1}\left[\left(\bigcup_{c \in D} \underline{m}(c)\right) f(u_a)\right] \\ &= f^{-1}\left[(C(S/S', D))\, f(u_a)\right]. \end{aligned}$$

Então segue que

$$C(S/S', Da) = C(S/S', D) f(u_a).$$

□

Os três lemas anteriores asseguram a validade da extensão do Teorema de Forney para códigos de classes laterais generalizados sendo propostos.

Teorema 4.4 *Se* $C(S/S', D)$ *é um código de classes laterais generalizado, então*

$$S^I / C(S/S', D) / (S')^I$$

é uma cadeia de partições geometricamente uniformes e os rótulos transladados $C(S/S', Da)$ *de* $C(S/S', D)$ *são geometricamente uniformes, mutuamente congruentes e tem grupo de simetrias comum* $U(C(S/S', D)) = V$.

Corolário 4.1 *Se* $C(S/S', D)$ *é um (transladado de* $\mathfrak{a}$*) código de classes laterais generalizado, então:*
$(\mathfrak{a})$ *As regiões de Voronoi associadas com duas sequências código* s *e* $s' \in C(S/S', D)$ *são congruentes;*
(b) *O perfil de distância* $DF(s) = \{\|s - s'\| : s' \in C(S/S', D)\}$ *de um dado ponto de sinal fixo* $s \in C(S/S', D)$ *a todos os pontos* $s' \in C(S/S', D)$ *independe de* s.

Exemplo 4.3 *Com a notação introduzida no Teorema 4.3, definimos, por um* s_0 *arbitrário em* U, *o reticulado* $S = [4,5](s_0)$ *e o subconjunto* $S' = P(s_0)$, *sendo* $[4,5]$ *o grupo completo de simetrias da tesselação* $\{4,5\}$ *e* $P = [4,5] \cap PSL(2,\mathbb{C})$, *ou seja,* P *é a parte fuchsiana de* $[4,5]$ *(Figura 28). Temos que* P *é um subgrupo normal de índice* 2 *do grupo* $[4,5]$. *Como uma consequência, temos* $U(S) = [4,5]$ *e* $U(S') = P$. *Pelo Teorema 4.3, o grupo de rótulos*

$$A = \frac{U(S)}{U(S')} = \{P; r_1 P\} \simeq \mathbb{Z}_2,$$

onde denotamos $\mathbb{Z}_2 = \{1, r_1\}$.

Com a notação introduzida nas Definições 4.2 e 4.5, o rotulamento

$$\overline{m} : A \to \frac{S}{S'}$$

tem a forma $\overline{m}(1) = s_0$ *módulo* P *e* $\overline{m}(r_1) = r_1(s_0)$ *módulo* P, *ou seja,* $\overline{m}(P) = S'$ *e* $\overline{m}(r_1 P) = r_1 S'$. *Agora, tomando* $I = \{1,2\}$, *temos a extensão natural para o rotulamento*

$$\underline{m} : A^2 \to \left(\frac{S}{S'}\right)^2.$$

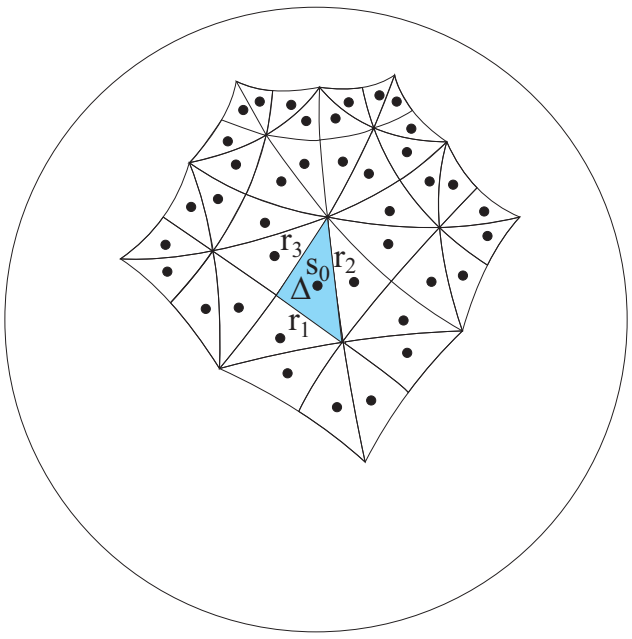


FIGURA 28: *Tesselação* $\{4,5\}$.

Denotando $A^2 = \{(1,1); (1,r_1); (r_1,1); (r_1,r_1)\}$ *e considerando o código de rótulos* $D_1 = \{(1,1); (1,r_1)\}$, *temos o código do espaço de sinal:*

$$C(S/S', D_1) = \bigcup_{c \in D} \{\underline{m}(c)\},$$

onde $s = (s_1, s_2) \in C(S/S', D_1)$ *se, e somente se, existe* $(c_1, c_2) \in D_1$ *tal que* $s_i \in \overline{m}(c_i)$ *para* $i = 1,2$. *Para o caso em consideração,* $c_1 = 1$, *segue que* $s \in S' \times S'$ *ou* $s \in S' \times r_1(S')$. *Portanto,*

$C(S/S', D_1) = (S' \times S') \cup (S' \times r_1(S'))$. *Da mesma maneira, definimos* $D_2 = \{(1,1);(r_1,1)\}$ *e* $D_3 = \{(1,1);(r_1,r_1)\}$, *obtemos o código do espaço de sinal* $C(S/S', D_2) = (S' \times S') \cup (r_1(S') \times S')$ *e* $C(S/S', D_3) = (S' \times S') \cup (r_1(S') \times r_1(S'))$, *respectivamente.*

Exemplo 4.4 *Considerando o grupo*

$$A^3 = \{(1,1,1);(1,1,r_1);(1,r_1,1);(1,r_1,r_1);(r_1,1,1);(r_1,1,r_1);(r_1,r_1,1);(r_1,r_1,r_1)\}$$

e o grupo de rótulos

$$D_1 = \{(1,1,1);(1,1,r_1);(1,r_1,1);(1,r_1,r_1)\},$$

similarmente ao processo anterior, seguindo o código do espaço de sinal obtemos

$$C(S/S', D_1) = (S' \times S' \times S') \cup (S' \times S' \times r_1(S')) \cup (S' \times r_1(S') \times S') \cup (S' \times r_1(S') \times r_1(S')).$$

Capítulo 5

Conclusões e Perspectivas Futuras

O presente trabalho teve como finalidade estender ao plano hiperbólico os conceitos de códigos geometricamente uniformes, partições geometricamente uniformes e códigos de classes laterais generalizados. Além de estabelecer uma relação entre os códigos e o conceito de G-linearidade.

Como na Teoria da Informação e Codificação existem canais de comunicação sem memória que podem ser modelados por meio de superfícies compactas com gêneros $\mathsf{g} \geq 1$ ([18]), e, como tais superfícies são naturalmente obtidas como quocientes entre o plano hiperbólico e grupos fuchsianos, o estudo desenvolvido neste trabalho tem destacada importância teórica.

Além disso, uma extensão natural dos estudos desenvolvidos neste trabalho pode ser conduzida em espaços hiperbólicos de dimensões maiores do que 2, utilizando, por exemplo, grupos kleinianos em espaços hiperbólicos tridimensionais. Outra perspectiva de futuros estudos pode ser voltada para aplicações práticas dos códigos geometricamente uniformes em espaços hiperbólicos. Neste caso, mergulhos isométricos de espaços hiperbólicos em espaços euclidianos podem ser bastante úteis, uma vez que, na atualidade, a grande parte dos códigos corretores de erros de bloco podem ser representados como reticulados em algum espaço euclidiano.

Referências Bibliográficas

[1] Anderson, J. *Hyperbolic Geometry*. New York: Springer-Verlag. 1999.

[2] Agustini, E. *Constelações de Sinais em Espaços Hiperbólicos.* Tese de Doutorado, IMECC-UNICAMP, Brasil, 2002.

[3] Araujo, M. C. *Caracterizações Algébrica e Geométrica dos Códigos Propelineares*, Tese de Doutorado, DT-FEEC-UNICAMP, Maio 2000.

[4] Beardon, A. *The Geometry of Discrete Groups.* New York: Springer-Verlag. 1983.

[5] Carmo, M. P. *Geometria Diferencial de Curvas e Superfícies.* Rio de Janeiro: Sociedade Brasileira de Matemática. (Coleção Textos Universitários). 2005.

[6] Carvalho, E. D. *Construção e Rotulamento de Constelações de Sinais Geometricamente Uniformes em Espaços Euclidianos e Hiperbólicos.* Tese de Doutorado, FEEC-UNICAMP, Brasil, 2001.

[7] Coxeter, H. M. S. & Moser W. O. J. *Generators And Relations For Discrete Groups.* Berlin, Springer, 1965.

[8] Forney, Jr. G. D. *Geometrically Uniform Codes.* IEEE Trans. Inf. Theory, v. 37 no. 5, p. 1241-1260, Sep. 1991.

[9] Fraleigh, J. B. *A Firt Course In Abstract Algebra,* Reading, Addison-Wesley, 1989.

[10] Garcia, A. & Lequain Y. *Elementos de Álgebra.* Rio de Janeiro: IMPA,2008.

[11] Geronimo, J. R. *Extensão da $\mathbb{Z}_4$-linearidade via Grupo de Simetrias*, Tese de Doutorado, DT-FEEC-UNICAMP, Fev. 1997.

[12] Herstein, I. N. *Topics in Algebra, 2nd. Edition.* New York, Wiley, 1975.

[13] Katok, S. *Fuchsian Groups.* Chicago: The University of Chicago Press. 1992.

[14] Lazari, H. & Palazzo Jr. R. "Geometrically Uniform Hyperbolic Codes". In: *Computational and Applied Mathematics.* v. 24, n. 2, 2005, p. 173-192.

[15] Lazari, H. *Uma Contribuição à Teoria dos Códigos Geometricamente Uniformes Hiperbólicos*, Tese de Doutorado, FEEC-UNICAMP, Brasil, 2000.

[16] Lima, E. L. *Espaços Métricos.* Rio de Janeiro: IMPA. 1977.

[17] Lima, E. L. *Grupo Fundamental e Espaços de Recobrimento.* Rio de Janeiro: IMPA. 1993.

[18] Lima, J. D. & Palazzo Jr. R. *Embedding discrete memoryless channels on compact and minimal surfaces.* IEEE Information Theory Workshop, India. 2002.

[19] Magnus, W. , Karras A. & Solitar D. *Combinatorial Group Theory.* New York, Interscience, 1966.

[20] Rotman, J. J. *The Theory of Groups, An Introduction.* Boston, Allyn and Bacon, 1973.

[21] Shannom, C. E. *A Mathematical Theory of Communication.* Bell Syst. Tech. J., vol. 27, pp. 379-423 e 623-656, julho/outubro, 1948.

[22] Slepian, D. *Group Codes for the Gaissian Channel.* Bell Sys. Tech. Journal, vol. 37, 1968, p. 575-602.

[23] Stillwell, J. *Geometry of Surfaces.* New York: Springer-Verlag. 1992.

[24] Stillwell, J. *Sources of Hyperbolic Geometry* (History of Mathematics v. 10). American Mathematical Society, 1996.

[25] Vieira, V. L. *Grupos Fuchsianos Aritméticos Identificados em Ordens dos Quatérnios para Construção de Constelações de Sinais,* Tese de Doutorado, FEEC-UNICAMP, Brasil, 2007.