Universidade Federal do Rio de Janeiro

Guilherme Vasconcelos da Silva

Grupo Modular Clássico

Rio de Janeiro

2010

Guilherme Vasconcelos da Silva

GRUPO MODULAR CLÁSSICO

1 Volume

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática (Matemática Pura), Instituto de Matemática, Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Ciências (Matemática).

Orientador: Guilherme Augusto de La Rocque Leal

Rio de Janeiro
2010

Agradecimentos

Agradeço a minha maravilhosa noiva. Sem a sua ajuda eu nunca teria conseguido terminar o mestrado, muito menos esta dissertação. Eu te ♡ Patricia!

Agradeço também a minha família, que apesar da distância sempre me apoiou durante estes 2 anos. Sem a ajuda deles também nunca teria conseguido.

Resumo

Neste trabalho fazemos uma introdução ao estudo do Grupo Modular Clássico. No primeiro capítulo definimos formalmente o Grupo Modular Clássico Γ e mostramos que ele é isomorfo ao grupo $PSL(2,\mathbb{Z})$. Como consequência deste isomorfismo deduzimos algumas propriedades de Γ e seus subgrupos. No segundo capítulo apresentamos o modelo de geometria hiperbólica do semi-plano H^2. Definimos uma métrica em H^2 e mostramos algumas propriedades básicas. No terceiro capítulo definimos o conceito de uma região fundamental em H^2 para um dado subgrupo de Γ, e definimos alguns tipos de regiões fundamentais, das quais destacamos os polígonos fundamentais convexos. Terminamos o capítulo obtendo um conjunto de geradores para Γ a partir de um polígono fundamental associado a ele. No apêndice fazemos uma breve menção ao grupo das transformações de Möbius e falamos a respeito de grupos de ação descontinua. Este último é um subgrupo das transformações de Möbius para qual é possível generalizar os resultados do terceiro capítulo.

Palavras-Chave: Grupo Modular Clássico, geometria hiperbólica, regiões fundamentais, transformações de Möbius.

Abstract

In this work we make an introduction to the study of the Classic Modular Group. In chapter one we define formally the Classic Modular Group Γ and show that it is isomorphic to the group $PSL(2,(Z))$. As a consequence of this isomorphism we deduce some properties of Γ and its subgroups. In chapter two we present the semi-plane model of hyperbolic geometry, which we denote by H^2. We define a metric on H^2 and show some of its basic properties. In chapter three we define the concept of a fundamental region in H^2 for a given subgroup of Γ, and define some types of fundamental regions, of which highlight the fundamental convex polygons. We end the chapter by obtaining a set of generators for Γ from a fundamental polygon associated with it. In the appendix we briefly mention the group of Möbius transformations and talk about groups with discontinuous action. The latter is a subgroup of Möbius transformations to which it is possible to generalize the results of the third chapter.

Key-Words: Classic Modular Group, hyperbolic geometry, fundamental regions, Möbius transformations.

Sumário

Introdução

O objetivo deste trabalho é servir como um ponto de partida para o estudo do Grupo Modular Clássico, que denotaremos por Γ. Para atingir este fim, o texto foi escrito assumindo somente uma familiaridade do leitor com operações de matrizes e conceitos básicos da teoria de grupos e análise, e além disto, dividimos o texto em duas partes para que o leitor possa ter uma visão mais geral a respeito das formas que Γ é estudado.

No primeiro capítulo iniciaremos o estudo do Grupo Modular Clássico, começando com uma breve discussão sobre o grupo $SL(2,\mathbb{Z})$. Na seção seguinte, definiremos o Grupo Modular Clássico e mostraremos que ele é isomorfo ao grupo $PSL(2,\mathbb{Z})=\frac{SL(2,\mathbb{Z})}{\{\pm Id\}}$. Em seguida mostraremos alguns resultados sobre a estrutura do Grupo Modular Clássico, entre os quais destacamos o fato do Grupo Modular Clássico ser o produto livre de dois grupos de ordem dois e três. Outros resultados importantes desta seção incluem o fato que, com a exceção de dois, os subgrupos normais do Grupo Modular são livres; a determinação do índice e posto do subgrupo dos comutadores do Grupo Modular e a determinação do posto de todos os subgrupos normais de índice finito do Grupo Modular Clássico.

No capítulo 2 faremos uma breve descrição do modelo do semi-plano complexo H^2 da geometria hiperbólica, definiremos a métrica desse modelo e provaremos que Γ esta contido no seu grupo das isometrias, e definiremos alguns conceitos que serão utilizados no capítulo seguinte.

No capítulo 3 definiremos o conceito de uma região fundamental para um subgrupo G qualquer de Γ, uma região de H^2 que contém exatamente um ponto de cada G-orbita dos elementos de H^2, e também apresentaremos um tipo particular de região fundamental, as regiões fundamentais localmente finitas. Em seguida definiremos os polígonos fundamentais de um grupo G, um tipo particular de região fundamental localmente finita e convexa que possui natureza poligonal, e da qual é possível determinar informações sobre a estrutura do grupo. Para concluir, iremos definir os polígonos de Dirichlet, uma classe de polígonos fundamentais cujo processo de construção será mostrado explicitamente e determinaremos o polígono de Dirichlet de Γ No apêndice faremos uma breve descrição do grupo das transformações de Möbius, e apresentaremos a noção de grupos com ação descontinua, uma classe de subgrupos das transformações de Möbius para qual é possível generalizar os resultados

dos capítulos 2 e 3.

Capítulo 1

O Grupo Modular

1.1 $SL(2,\mathbb{Z})$

Denotamos por $SL(2,\mathbb{Z})$ o grupo multiplicativo das matrizes inversíveis 2x2 com coeficientes inteiros. Este grupo é de importância crucial no estudo do Grupo Modular Clássico.
Nesta seção iremos determinar um conjunto de geradores para $SL(2,\mathbb{Z})$.

Teorema 1.1.1 *Considere as matrizes:*

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

Temos que S e T geram o grupo $SL(2,\mathbb{Z})$.

Demonstração:
1. Vamos mostrar que se A pertence a $SL(2,\mathbb{Z})$ então, $A = CB$, onde B é uma matriz triangular e C pertence ao grupo gerado pelas matrizes $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ e $V = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
De fato, seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, onde $ad - bc = 1$. Temos que, ou $bc \neq 0$ ou $da \neq 0$. Caso $b = 0$ ou $d = 0$ nada temos a fazer pois A já está na forma triangular. Considere então o caso $b \neq 0$, $d \neq 0$.
Agora, suponha sem perda de generalidade que $b \leq d$ (Caso contrario aplique o argumento abaixo a matriz $A' = VA$).
Caso $d = b$, considere a matriz $A_1 = S^{-1}A = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-c & 0 \\ c & d \end{pmatrix}$, multiplicando pela esquerda por S obtemos que $A = SA_1$, de forma que a afirmação é satisfeita.

Caso $b < d$, aplique o algoritmo euclidiano da divisão sobre d e b para obter inteiros r_i,q_i tais que:

$$\begin{aligned} d =& q_o b + r_0 \ , \ |r_0| < |b| \\ b =& q_1 r_0 + r_1 \ , \ |r_1| < |r_0| \\ & \vdots \\ r_{n-2} =& q_n r_{n-1} + r_n, \text{ onde } r_n = 0 \text{ e } r_{n-1} = mdc(d, b). \end{aligned}$$

Podemos utilizar estes inteiros para transformar A numa matriz triangular através dos seguintes produtos de matrizes:

$$VS^{-q_0}VA = \begin{pmatrix} 1 & 0 \\ -q_o & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c - aq_0 & d - q_0 b \end{pmatrix} = \begin{pmatrix} a & b \\ c - aq_0 & r_0 \end{pmatrix}$$

$$V\begin{pmatrix} a & b \\ c - aq_0 & r_0 \end{pmatrix} = \begin{pmatrix} a_1 & r_0 \\ c_1 & b \end{pmatrix}$$

$$VS^{-q_1}V\begin{pmatrix} a_1 & r_0 \\ c_1 & b \end{pmatrix} = \begin{pmatrix} a_1 & r_0 \\ c_1 - a_1 q_1 & b - r_0 q_1 \end{pmatrix} = \begin{pmatrix} a_1 & r_0 \\ c_1 - a_1 q_1 & r_1 \end{pmatrix}$$

$$V\begin{pmatrix} a_1 & r_0 \\ c - aq_1 & r_1 \end{pmatrix} = \begin{pmatrix} a_2 & r_1 \\ c_2 & r_0 \end{pmatrix}$$

$$\vdots$$

$$VS^{-q_n}VA_{n-1} = \begin{pmatrix} 1 & 0 \\ -q_n & 1 \end{pmatrix}\begin{pmatrix} a_n & r_{n-1} \\ c_n & r_{n-2} \end{pmatrix} = \begin{pmatrix} a_{n+1} & r_{n-1} \\ c_{n+1} & 0 \end{pmatrix}.$$

E portanto segue que $A = CA_n = C\begin{pmatrix} a_{n+1} & r_{n-1} \\ c_{n+1} & 0 \end{pmatrix}$, onde C pertence ao grupo gerado por S e V. Segue portanto a afirmação.

2. A matriz A pertence ao grupo gerado pelas matrizes V, S e $E = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

Pelo afirmação anterior temos que $A = CB$ e C pertence ao grupo gerado por S e V. Temos que mostrar agora que B pertence ao grupo gerado por V, S e E. Suponha que B é triangular superior (caso não podemos multiplicar B pela esquerda ou pela direita por V algumas vezes para obter a matriz triangular superior). Temos que $det(A) = det(CB) = 1$, de modo que $det(B) = \pm 1$ e portanto $B = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, onde $a = d = \pm 1$.

Caso $a = d = 1$ temos que $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^b = S^b$. Caso $a = d = -1$, considere a seguinte sequência de produtos de matrizes:

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-b} = \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & b \end{pmatrix}$$
$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & b \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & b \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & b \end{pmatrix} = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}.$$

Portanto neste caso temos que $B = VEVES^{-b}$, de onde segue que B pertence ao grupo gerado por V, E e S.

3. As matrizes $T = VE = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ e S geram $SL(2, \mathbb{Z})$.

Vamos mostrar que combinações das matrizes E, S e V pertencentes a $SL(2, \mathbb{Z})$ podem ser reescritas como combinações das matrizes S e T. Para mostrar isso precisaremos das seguintes igualdades (observe também que $V = V^{-1}$ e $E = E^{-1}$):

$$VE = T \qquad EV = T^{-1}$$
$$ETE = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = T^{-1}$$
$$ES^nE = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = S^{-n}$$

Com essas igualdades, e possível mostrar que $SL(2, \mathbb{Z})$ é gerado por S e T.

Vamos analisar agora o grupo gerado pelas matrizes E,V e S, isto é, o grupo composto de combinações da forma:

$$E^{k_1^E}V^{k_1^V}S^{k_1^S}\ldots E^{k_n^E}V^{k_n^V}S^{k_n^S},$$

onde $k_i^V, k_i^E = 0$ ou 1 e $k_i^S \in \mathbb{Z}$, para $i = 1, \ldots, n$. Observe que nem todas as combinações desta forma pertencem a $SL(2, \mathbb{Z})$, no entanto, todos os elementos de $SL(2, \mathbb{Z})$ têm esta forma.

Para mostrar que podemos rescrever as sequências pertencentes a $SL(2, \mathbb{Z})$ como combinações de T e de S, estudaremos a sequência $E^{k_i^E}V^{k_i^V}S^{k_i^S}$. Vamos analizar as diferentes possibilidades para os valores de k_i^E e k_i^V :

$k_i^E = k_i^V = 0$ ou 1:

$$E^{k_i^E} V^{k_i^V} S^{k_i^S} = T^{k_i^T} S^{k_i^S} \text{ , onde } k_i^T = 1 \text{ ou } 0$$

$k_i^E = 0$, $k_i^V = 1$:

$$E^{k_i^E} V^{k_i^V} S^{k_i^S} = V S^{k_i^S} = VEES^{k_i^S} EE = T^{-1} S^{-k_i^S} E$$

$k_i^E = 1$, $k_i^V = 0$:

$$ES^{k_i^S} = ES^{k_i^S} EE = S^{-k_i^S} E$$

Com isso mostramos que podemos reescrever qualquer sequência da forma $E^{k_i^E} V^{k_i^V} S^{k_i^S}$ como $T^{k_i^T} S^{k_i^S} E^r$, onde $r = 0$ ou 1 e $k_i^T = \pm 1$ ou 0. Note agora que:

$$\begin{aligned} E^{k_i^E} V^{k_i^V} S^{k_i^S} E^{k_{i+1}^E} V^{k_{i+1}^V} S^{k_{i+1}^S} =& T^{k_i^T} S^{k_i^S} E^r E^{k_{i+1}^E} V^{k_{i+1}^V} S^{k_{i+1}^S} \\ =& T^{k_i^T} S^{k_i^S} E^{k'^E_{i+1}} V^{k_{i+1}^V} S^{k_{i+1}^S} \end{aligned}$$

Onde $k'^E_{i+1} = 0$ ou 1. Se tomarmos então uma combinação arbitrária da forma:

$$E^{k_1^E} V^{k_1^V} S^{k_1^S} \dots E^{k_n^E} V^{k_n^V} S^{k_n^S},$$

podemos obter (fazendo o processo de redução acima de 1 até n) uma combinação da forma $T^{k_i^T} S^{k_i^S} \dots T^{k_i^T} S^{k_i^S} E^r$, onde $r = 0$ ou 1. Mostramos com isso que se A pertence ao grupo gerado por E, V e S então ou $A = B$ ou $A = BE$, onde B pertence ao grupo gerado por U e S.

Agora, caso A pertença a $SL(2, \mathbb{Z})$, temos que $det(A) = 1$, de modo que $A = B$. Assim, obtemos que $SL(2, \mathbb{Z})$ é gerado por T e S.

1.2 O Grupo Modular Clássico

Nesta seção definiremos formalmente o Grupo Modular Clássico e mostraremos algumas das propriedades da sua estrutura e de seus subgrupos.

Definição 1.2.1 *O Grupo Modular Clássico, que denotaremos por* Γ*, é o grupo formado pelas transformações:*

$$\begin{aligned} T : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \frac{az+b}{cz+d} \\ ad - bc = 1, \qquad & a, b, c, d \in \mathbb{Z}, \end{aligned}$$

Com sua operação de grupos sendo a composição de funções.

Proposição 1.2.1 *Os grupos* Γ *e* $PSL(2, \mathbb{Z}) = \frac{SL(2,\mathbb{Z})}{\pm Id}$ *são isomorfos.*

Demonstração: Considere função φ dado por:

$$\begin{aligned}\varphi : SL(2,\mathbb{Z}) &\longrightarrow \Gamma \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto T(z) = \frac{az+b}{cz+d}.\end{aligned}$$

É de verificação imediata que φ é um homomorfismo de grupos. De fato, dados $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ dois elementos de Γ, temos que:

$$\varphi(A) \circ \varphi(A') = \frac{a\left(\frac{a'z+b'}{c'z+d'}\right)+b}{c\left(\frac{a'z+b'}{c'z+d'}\right)+d} = \frac{(aa'+c'b)z+(bd'+ab')}{(ca'+dc')z+(cb'+dd')} = \varphi(AA').$$

Vamos agora determinar o núcleo de φ. Se $A \in Ker(\varphi)$, temos que $\varphi(A) = \frac{az+b}{cz+d} = z$ $\forall z \in \mathbb{C}$.Vamos tomar alguns valores particulares de z para determinar a, b, c e d:
$z = 0$: Neste caso, temos que $\frac{b}{d} = 0$, e portanto $b = 0$
$z = 1$ e $z = -1$: No primeiro caso temos que $\frac{a}{c+d} = 1$ e no segundo caso temos que $\frac{-a}{-c+d} = 1$. Temos portanto que $c + d = c - d$, de onde concluímos que $d = 0$.
Agora, $A \in SL(2,\mathbb{Z})$, portanto $ad - bc = ad = 1$, portanto $a = d = 1$, de onde concluímos que:

$$ker(\varphi) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}); \frac{az+b}{cz+d} = z \right\} = \{\pm Id\}.$$

Como φ é sobrejetiva, temos pelo teorema de isomorfismos que $\Gamma \cong \frac{SL(2,\mathbb{Z})}{\{\pm Id\}} = PSL(2,\mathbb{Z})$. □

A partir de agora, iremos denotar tanto o grupo das transformações quanto $PSL(2,\mathbb{Z})$ por Γ, sendo que usaremos letras minusculas para representar as transformações e maiúsculas para representar matrizes.

Conforme foi mostrado na seção anterior, o grupo $SL(2,\mathbb{Z})$ têm como um grupo de geradores as matrizes $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ e $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Podemos então considerar como geradores de $SL(2,\mathbb{Z})$ as matrizes T e $U = TS = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Como S e T geram $SL(2,\mathbb{Z})$, é imediato que as matrizes U e T também irão gerar $SL(2,\mathbb{Z})$, pois $S = TU$. Temos também que:

$$T^2 = -Id \text{ e } U^3 = Id.$$

De modo que, se $A \in SL(2,\mathbb{Z})$ temos que:

$$A = (-1)^s U^a T U^{e_1} \dots T U^{e_n} T^b,$$

onde $s = 0$ ou 1, $a = 0, 1$ ou 2, $e_k = 0, 1$ ou 2 $\forall k = 1, \ldots, n$, $b = 0$ ou 1 e $n \in \mathbb{N}$.
Observe que como U e T geram $SL(2, \mathbb{Z})$, temos que $x = \varphi(T)$ e $y = \varphi(U)$ irão gerar Γ (Onde φ é o isomorfismo entre Γ e $PSL(2, \mathbb{Z})$), de modo que se $h \in \Gamma$, então

$$h = y^a x y^{e_1} \ldots x y^{e_n} x^b,$$

onde a, b e n são os mesmo de acima.

Teorema 1.2.1 *Sejam x e y os geradores de Γ descritos acima. Temos que Γ é o produto livre dos grupos $\langle x \rangle$ e $\langle y \rangle$.*

Demonstração: Conforme visto acima, todo elemento de Γ se escreve como uma combinação de x e y, de modo que para mostrar que Γ precisamos somente precisamos mostrar que palavras da forma $y^\alpha x y^{e_1} \ldots x y^{e_n} x^\beta$ não se reduzem a identidade, onde $\alpha = 0, 1$ ou 2, $e_k = 0, 1$ ou 2 $\forall k = 1, \ldots, n$, $\beta = 0$ ou 1 e $n \in \mathbb{N}$.

Observe que isso é equivalente a mostrar que nenhuma palavra da forma $x^b y^{e_1} \ldots x y^{e_n} x^\beta y^{3-\alpha}$ se reduz a identidade, pois $y^\alpha x y^{e_1} \ldots x y^{e_n} x^\beta$ se reduz a identidade se e somente se seu conjugado por y^{2-a} se reduz a identidade. Em vista do isomorfismo entre Γ e $PSL(2, \mathbb{Z})$ podemos mostrar este fato mostrando que nenhum produto da forma $\pm T U^{e_1} \ldots T U^{e_n} T^\beta U^{3-\alpha}$ é igual a $\pm Id$.

Vamos primeiro mostrar que nenhuma palavra da forma $\pm T U^{e_1} \ldots T U^{e_n}$ se reduz a $\pm Id$ caso $n > 0$.
Observe que:

$$TU = -\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ e } TU^2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

de modo que um produto da forma $C = \pm T U^{e_1} \ldots T U^{e_n} = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ têm suas entradas todas com o mesmo sinal, que consideraremos positivo.
considere agora os produtos:

$$CTU = -\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = -\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$
$$CTU^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix},$$

portanto se $C \neq \pm Id$, teremos que $CTU \neq \pm Id$ e $CTU^2 \neq \pm Id$. Assim, como para $n = 1$ vale a afirmação, segue por indução que os produtos da forma $\pm T U^{e_1} \ldots T U^{e_n}$ são diferentes de ± 1.

Resta mostrar que se um produto de matrizes $\pm TU^{e_1} \dots TU^{e_n}$ é diferente de $\pm Id$, então o produto $\pm TU^{e_1} \dots TU^{e_n} T^{\beta} U^{3-\alpha}$ também sera, para todos os valores de α e β. Para mostrar isso vamos considerar o produto para os possíveis valores de α e β:

$$\alpha = 0 \;\; \beta = 1 : \; CT = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = - \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$$

$$\alpha = 2 \;\; \beta = 0 : \; CU = \pm Id \Longleftrightarrow C = U^2, \text{ o que não ocorre.}$$

$$\alpha = 1 \;\; \beta = 0 : \; CU^2 = \pm Id \Longleftrightarrow C = U, \text{ o que não ocorre.}$$

Os casos CTU e CTU^2 já foram discutidos, de modo que $\pm TU^{e_1} \dots TU^{e_n} T^b U^a \neq \pm Id$, de onde concluímos o resultado. □

Teorema 1.2.2 *Seja Γ' o subgrupo dos comutadores de Γ . Temos que $(\Gamma : \Gamma') = 6$, e o grupo Γ/Γ' é cíclico gerado por $\bar{z}$, onde $z = xy$.*

Demonstração:
Γ/Γ' é o grupo gerado por $\bar{x}$ e $\bar{y}$, com as relações $\bar{x}^2 = \bar{1}$, $\bar{y}^3 = \bar{1}$ e $\bar{x}.\bar{y} = \bar{y}.\bar{x}$, de modo que $\Gamma/\Gamma' \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. □

Para os próximos resultados, vamos precisar do teorema de Kurosh de subgrupos de produtos livres, cuja demonstração pode ser encontrada em [4].

Teorema de Kurosh:
Seja $G = \prod^* T_\alpha$ um produto livre e H subgrupo qualquer de G. Temos então que$H = F * \prod^* B_\beta$, onde F é livre ou é $\{1\}$ e cada um dos B_b é conjugado a um subgrupo de algum dos fatores T_α. No caso particular do Grupo Modular o teorema nos diz que, dado H subgrupo de Γ, temos que $H = F * \prod^* B_\beta$, onde cada B_β ou é conjugado de $< x >$ ou conjugado de $< y >$ ou é $\{1\}$.

Teorema 1.2.3 *Seja H subgrupo de Γ, $H \neq \{1\}$. H é livre se, e somente se, H for livre de torção.*

Demonstração: Obviamente se H for livre ele é livre de torção. Reciprocamente, suponha H livre de torção. Pelo teorema de Kurosh, temos que $H = F * \prod^* B_\beta$. Caso algum dos B_β seja não trivial, teríamos elementos de ordem finita em H, absurdo. Assim, $H = F$, como queríamos provar. □

Teorema 1.2.4 *Os únicos elementos de* Γ *de ordem finita são* $1, x, y, y^2$ *e seus conjugados.*

Demonstração:
Seja $u \in \Gamma$ elemento de ordem finita, temos que $\langle u \rangle$ é um grupo cíclico finito e , pelo teorema de Kurosh, $\langle u \rangle = F * \prod^* B_\beta$. Agora, se mais de um dos fatores B_β fosse não trivial, o lado direito da equação não seria finito. Do mesmo modo, caso F seja não trivial, o lado direito também não será finito, portanto $\langle u \rangle$ é conjugado de $\langle x \rangle$ ou de $\langle y \rangle$, de onde temos o resultado. □

Teorema 1.2.5 *Sejam* $u, v \in \Gamma$. *Temos que,* $uv = vu \Leftrightarrow \exists h \in \Gamma$ *tal que* $u = h^{n_1}, v = h^{n_2}$, *onde* $n_1, n_2 \in \mathbb{Z}$

Demonstração: Considere o grupo $\langle u, v \rangle$. Temos que esse é um grupo abeliano, pois u e v comutam. Pelo teorema de Kurosh temos que $\langle u, v \rangle = F * \prod^* B_\beta$. Como ocorreu na demonstração do teorema anterior, temos que se mais de um dos termos for não trivial o lado direito da igualdade será não abeliano, absurdo. Assim, ou $\langle u, v \rangle = F$, ou o subgrupo $\langle u, v \rangle$ será conjugado ao grupo gerado por x ou ao grupo gerado por y.
No primeiro caso temos F livre e abeliano, assim $F = \langle h \rangle$, onde $h \in \Gamma$, assim, temos que $\langle x, y \rangle$ é cíclico, e segue o resultado. □

Definição 1.2.2 *Sejam* $S \subset \Gamma$. *Definimos como fecho normal de* S *o conjunto* $\Delta(S)$ *formado pela interseção de todos os subgrupos normais de* Γ *que contém* S. *No caso particular de* $S = \{x_1, \ldots, x_n\}$ *iremos escrever o fecho normal de* S *como* $\Delta(x_1, \ldots, x_n)$.

Definição 1.2.3 *Denotamos por* Γ^n *o subgrupo gerado pelas n-ésimas potências dos elementos de* Γ.

Observe que Γ^n é totalmente invariante por automorfismos de Γ, isto é, $\sigma(\Gamma^n)$ e em particular é normal em Γ.

Teorema 1.2.6 *Temos que:*

$$\Gamma^2 = \Delta(y) \qquad \Gamma^3 = \Delta(x)$$
$$(\Gamma : \Gamma^2) = 2 \qquad (\Gamma : \Gamma^3) = 3$$
$$\Gamma^2 = \langle y \rangle * \langle xyx \rangle, \quad \Gamma^3 = \langle x \rangle * \left\langle yxy^2 \right\rangle * \left\langle y^2xy \right\rangle.$$

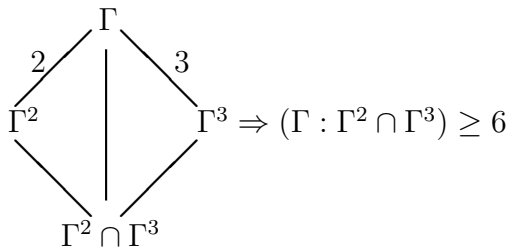
Demonstração:

Observe que $y = (y^2)^{-1} \Rightarrow y \in \Gamma^2$, e temos que Γ^2 é normal em Γ, o que implica que $\Delta(y) \subset \Gamma^2$.

Agora, $\Gamma/\Delta(y)$ é o grupo gerado por $\overline{x}, \overline{y}$ com as relações $\overline{x} \neq \overline{1}, \overline{x}^2 = \overline{1} = \overline{y}$, de modo que que $\Gamma/\Delta(y) \cong \mathbb{Z}_2$ e portanto $(\Gamma : \Delta(y)) = 2$. $\Delta(y) \subset \Gamma^2 \subset \Gamma$, portanto $\Gamma^2 = \Delta(y)$ ou $\Gamma^2 = \Gamma$, no entanto, $x \notin \Gamma^2$, logo $\Gamma^2 = \Delta(y)$.
Repetindo o argumento com x ($x^3 = x \Rightarrow x \in \Gamma^3$), temos que $\Gamma^3 = \Delta(x)$ e $(\Gamma : \Gamma^3) = 3$.
Para mostrarmos que $\Gamma^3 = \langle x \rangle * \langle yxy^2 \rangle * \langle y^2xy \rangle$ e $\Gamma^2 = \langle y \rangle * \langle xyx \rangle$ só precisamos observar o seguinte:
Primeiro os produtos citados acima são de fato livres pois caso contrario existiria uma relação não trivial entre x e y, o que é um absurdo. Agora, $\langle y \rangle * \langle xyx \rangle$ é normal em Γ e contém y, de modo que $\Gamma^2 \subset \langle y \rangle * \langle xyx \rangle$. Agora, $y, xyx \in \Gamma^2$ portanto $\langle y \rangle * \langle xyx \rangle = \Gamma^2$. De forma totalmente análoga obtemos que $\Gamma^3 = \langle x \rangle * \langle yxy^2 \rangle * \langle y^2xy \rangle$. □

Corolário 1.2.1 *Seja Γ' o subgrupo dos comutadores de Γ. Temos que $\Gamma' = \Gamma^2 \cap \Gamma^3$.*

Demonstração: Observe que Γ/Γ^2 e Γ/Γ^3 são grupos abelianos, de modo que Γ^2 e Γ^3 contém Γ', e portanto temos que $\Gamma' \subset \Gamma^2 \cap \Gamma^3$.
Agora, considere o seguinte diagrama:



$\Rightarrow (\Gamma : \Gamma^2 \cap \Gamma^3) \geq 6$

Por outro lado, $(\Gamma : \Gamma') = 6$, assim $(\Gamma : \Gamma^2 \cap \Gamma^3) \leq 6$. Portanto temos que $\Gamma^2 \cap \Gamma^3 = \Gamma'$. □

Teorema 1.2.7 *Com a exceção de Γ, Γ^2 e Γ^3, todo subgrupo normal de Γ livre:*

*Demonstração:*Seja $H \triangleleft \Gamma$ se H é livre de torção,H é livre, então suponha que $\exists g \in H$ tal que $o(g) < \infty$, temos então que g é da forma uxu^{-1}, uyu^{-1} ou uy^2u^{-1} vamos considerar a primeira possibilidade:

Como $H \triangleleft \Gamma$, temos que $x \in H \Rightarrow \Gamma^2 \subset H$. Agora, $(\Gamma : \Gamma^2) = 2 \Rightarrow H = \Gamma$ ou $H = \Gamma^2$.

O segundo e terceiro caso são equivalentes, pois se $y^2 \in H$, $(y^2)^2 = y \in H$ e nesses caso um argumento análogo mostra que $H = \Gamma^3$ ou $H = \Gamma$ e segue o resultado. □

Corolário 1.2.2 *Γ' é livre de posto 2.*

Demonstração: 'Pelo teorema anterior que Γ' é livre. Vamos mostrar agora que Γ' é gerado por yxy^2x e yxy^2x.
Seja G o subgrupo de Γ gerado por yxy^2x e yxy^2x. Como $yxy^2x, yxy^2x \in \Gamma'$, temos que

$G \subset \Gamma'$. Vamos mostrar agora que G é normal em Γ.
Como Γ é gerado por x e y, para mostrar que G é normal precisamos somente mostrar que $xGx = G$ e yGy^2. Tome $w \in G$, temos que:

$$w = y^{a_1}xy^{3-a_1}xy^{a_2}xy^{3-a_2}x \dots y^{a_n}xy^{3-a_n}x$$

Conjugando w por x obtemos:

$$\begin{aligned} xwx =& x(y^{a_1}xy^{3-a_1}x)(y^{a_2}xy^{3-a_2}x)\dots(y^{a_n}xy^{3-a_n}x)x \\ =& (xy^{a_1}xy^{3-a_1})x(y^{a_2}xy^{3-a_2}x)\dots(y^{a_n}xy^{3-a_n}x)x \\ & \vdots \\ =& (xy^{a_1}xy^{3-a_1})(xy^{a_2}xy^{3-a_2})\dots x(y^{a_n}xy^{3-a_n}x)x \\ =& (xy^{a_1}xy^{3-a_1})(xy^{a_2}xy^{3-a_2})\dots(xy^{a_n}xy^{3-a_n}), \end{aligned}$$

de modo que $xwx \in G$
Conjugando w por y obtemos que:

$$\begin{aligned} ywy^2 =& y(y^{a_1}xy^{3-a_1}x)(y^{a_2}xy^{3-a_2}x)\dots(y^{a_n}xy^{3-a_n}x)y^2 \\ =& (y^{a_1+1}xy^{2-a_1}x)(xyx)(y^{a_2}xy^{3-a_2}x)\dots(y^{a_n}xy^{3-a_n}x)y^2 \\ =& (y^{a_1+1}xy^{2-a_1}x)(xyx)(y^2y)(y^{a_2}xy^{3-a_2}x)\dots(y^{a_n}xy^{3-a_n}x)y^2 \\ =& (y^{a_1+1}xy^{2-a_1}x)(xyxy^2)y(y^{a_2}xy^{3-a_2}x)\dots(y^{a_n}xy^{3-a_n}x)y^2 \\ & \vdots \\ =& (y^{a_1+1}xy^{2-a_1}x)(xyxy^2)(y^{a_2+1}xy^{2-a_2}x)\dots(y)(y^{a_n}xy^{3-a_n}x)(y^2) \\ =& (y^{a_1+1}xy^{2-a_1}x)(xyxy^2)(y^{a_2+1}xy^{2-a_2}x)\dots(y^{a_n+1}xy^{2-a_n}x)(xyxy^2) \end{aligned}$$

e portanto yxy^2 pertence a G, de onde segue que $G \lhd \Gamma$. Observe que temos com isso que G é livre, e possui posto 2.
Agora, vamos mostrar que $\frac{\Gamma}{G}$ é um grupo abeliano. De fato, note que $xyG = xy(y^2xyx)G = yxG$, e portanto como Γ é gerado por x e y, temos que $\frac{\Gamma}{G}$ é um grupo abeliano. Assim, $\Gamma' \subset G$ e segue o resultado.□

O próximo resultado é a respeito do posto de um subgrupo livre de Γ. Para esse resultado vamos precisar do teorema de Schreier sobre postos de subgrupos de grupos livres, cuja demonstração pode ser encontrada em [3] e em [5]:

Teorema (Schreier): Seja G grupo livre de posto r e H subgrupo de G tal que $(G : H) = n$. Temos então que H é livre de posto $1 + n(r - 1)$.

Como consequência do teorema de Schreier temos o seguinte resultado:

Teorema 1.2.8 *Seja H subgrupo normal de Γ, $(\Gamma : H) = \mu < \infty$ e $H \neq \Gamma$, Γ^2 e Γ^3. Então H é livre de posto $r = 1 + \mu/6$.*

Demonstração: Como H é normal e $H \neq \Gamma, \Gamma^2$ e Γ^3, temos que H é livre. Considere agora o subgrupo $\Gamma' \cap H$ de H. Temos que $\Gamma' \cap H$ é um subgrupo livre e normal em Γ, e possui índice finito. Sejam $m = (\Gamma' : \Gamma' \cap H), n = (H : \Gamma' \cap H)$, r o posto de H e R o posto de $\Gamma' \cap H$. Note que o índice de Γ' em Γ é 6 e seu posto é 2. Aplicando o teorema de Schreier em $\Gamma' \cap H \subset \Gamma'$ e $\Gamma' \cap H \subset H$ obtemos que:

$$R = m(2-1) + 1 \text{ e } R = n(r-1) + 1 \Rightarrow m = n(r-1) \Rightarrow r = m/n + 1$$
$$\frac{m}{n} = \frac{(\Gamma' : \Gamma' \cap H)}{(H : \Gamma' \cap H)} = \frac{(\Gamma : \Gamma' \cap H)/(\Gamma : \Gamma')}{(\Gamma : \Gamma' \cap H/(\Gamma : H))} = \frac{\mu}{6} \Rightarrow r = \frac{\mu}{6} + 1.$$

□

1.3 Grupos de congruência

Definição 1.3.1 *Chamamos de grupo principal de congruência de nível n o subgrupo $\Gamma(n)$ de Γ, onde:*

$$\Gamma(n) = \{A \in \Gamma; A = \pm Id \ mod(n)\} = \left\{ A \in \Gamma; A \in \begin{pmatrix} \mathbb{Z}_n + 1 & \mathbb{Z}_n \\ \mathbb{Z}_n & \mathbb{Z}_n + 1 \end{pmatrix} \right\}$$

Uma outra maneira de enxergar $\Gamma(n)$ é como sendo o núcleo do homomorfismo $\theta : \Gamma \longrightarrow PSL(2, \mathbb{Z}_n) = \frac{SL(2,\mathbb{Z}_n)}{\pm Id}$. Como $\Gamma(n)$ é o núcleo de um homomorfismo de Γ, temos que ele é um subgrupo normal de Γ.

Dizemos que um subgrupo G de Γ é um grupo de congruência se $\exists n \in \mathbb{N}$ tal que $\Gamma(n) \subset G$, e dizemos que G tem nível n se n é o menor inteiro tal que isso ocorre.

Para entender melhor a estrutura dos grupos de congruência, vamos estudar o grupo $G(n) = \Gamma/\Gamma(n) \cong PSL(2, \mathbb{Z}_n)$.

Para os próximos resultados estaremos sempre considerando n, m elementos de $\mathbb{N}$, $d = \text{mdc}(n, m)$ e $\delta = \text{mmc}(n, m)$.

Lema 1.3.1 *Seja $A \in \Gamma(d)$. Então existe $X \in \Gamma$ tal que:*

$$(1) \qquad X \equiv Id \ mod(n)$$
$$(2) \qquad X \equiv A \ mod(m).$$

Demonstração:
$A \in \Gamma(d)$. Temos então que $A = Id + dB$, para alguma matriz B com coeficientes inteiros. Tome $X = Id + nY$, $X \equiv Id\ mod(n)$. Temos que:

$$\begin{aligned} X \equiv A\ mod(m) \Leftrightarrow & \\ \Leftrightarrow & Id + nY \equiv Id + dB\ mod(m) \\ \Leftrightarrow & nY \equiv dB\ mod(m) \\ \Leftrightarrow & \frac{n}{d}Y \equiv B\ mod(m/d). \end{aligned}$$

Como $\text{mdc}(\frac{n}{d}, \frac{m}{d}) = 1$ temos que $\frac{n}{dY} \equiv B\ mod(m/d)$ tem solução em $\mathbb{M}_{2x2}(Z)$, assim existe $X \in \mathbb{M}_{2x2}(Z)$ satisfazendo (1) e (2).

Agora, temos como consequência do teorema da forma normal de Smith que existe uma matriz X_0 tal que[1]:

$$X_0 \equiv X\ mod(\delta) \Rightarrow \begin{cases} X_0 \equiv X\ mod(n) \\ X_0 \equiv X\ mod(m) \end{cases}$$

e além disto $\det(X_0) = 1$, de modo que $X_0 \in \Gamma$. Portanto, a matriz X_0 satisfaz as condições do lema, de modo que vale o resultado. □

Lema 1.3.2 *Seja $A \in \Gamma(d)$. Temos então que existem $B \in \Gamma(n)$, $C \in \Gamma(m)$ tais que $A = BC$*

demonstração: Simplesmente tome $B = X$ e $C = X^{-1}A$, onde X é a matriz dada pelo lema anterior. □

Teorema 1.3.1 *Temos que $\Gamma(n), \Gamma(m) \triangleleft \Gamma(d)$ e*

$$\begin{aligned} \Gamma(n)\Gamma(m) &= \Gamma\ mod(d) \\ \Gamma(n) \cap \Gamma(m) &= \Gamma\ mod(\delta) \end{aligned}$$

[1]A forma normal de Smith nos diz que toda matriz pertencente a $\mathbb{M}_{2x2}$ pode ser escrita na forma UAZ, onde A é uma matriz diagonal e U,Z pertencem a $SL(2,\mathbb{Z})$. A demonstração da afirmação será omitida pois não é particularmente interessante, mas ela é feita de forma construtiva, construindo uma matriz $C \in SL(2,\mathbb{Z})$ congruente a $X\ mod(\delta)$ a matriz diagonal que é obtida aplicando a forma normal de smith a X.

Demonstração: Note que tanto $\Gamma(n)$ e $\Gamma(m)$ são subgrupos normais de Γ, de modo que eles são normais em $\Gamma(d)$, de onde concluímos que $\Gamma(n)\Gamma(m) \subset \Gamma(d)$. Como consequência direta do lema 1.3.2 temos a inclusão oposta, de modo que $\Gamma(n)\Gamma(m) = \Gamma(d)$. Para a última afirmação, observe que $\Gamma(\delta) \subset \Gamma(n)$ e $\Gamma(\delta) \subset \Gamma(m)$, de modo que $\Gamma(\delta) \subset \Gamma(n) \cap \Gamma(m)$. Por outro lado, seja $A \in \Gamma(n) \cap \Gamma(m)$. Temos que:

$$\left.\begin{array}{l} A - Id \equiv 0 \ mod(n) \\ A - Id \equiv 0 \ mod(m) \end{array}\right\} \Rightarrow A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \text{onde } m \text{ e } n \text{ dividem } a_{11}-1, a_{22}-1, a_{12} \text{ e } a_{21}$$

De modo que δ divide $a_{11} - 1$, $a_{22} - 1$ a_{12} e a_{21}, e portanto $A \in \Gamma(\delta)$. □

Teorema 1.3.2 *Temos que:*

$$\frac{\Gamma(d)}{\Gamma(n)} \cong \frac{\Gamma(m)}{\Gamma(\delta)}$$

Demonstração: Temos pelo segundo teorema de isomorfismos de grupos que:

$$\frac{\Gamma(n)\Gamma(m)}{\Gamma(n)} \cong \frac{\Gamma(m)}{(\Gamma(n) \cap \Gamma(m))}.$$

Então, pelo teorema anterior, temos que:

$$\Gamma(n)\Gamma(m) = \Gamma(d) \Rightarrow \frac{\Gamma(n)\Gamma(m)}{\Gamma(n)} = \frac{\Gamma(d)}{\Gamma(n)}$$
$$\Gamma(n) \cap \Gamma(m) = \Gamma(\delta) \Rightarrow \frac{\Gamma(m)}{(\Gamma(n) \cap \Gamma(m))} = \frac{\Gamma(m)}{\Gamma(\delta)}.$$

Assim temos o resultado. □

Teorema 1.3.3 *Temos que:*

$$\frac{\Gamma(d)}{\Gamma(\delta)} \cong \frac{\Gamma(d)}{\Gamma(n)} \times \frac{\Gamma(d)}{\Gamma(m)}.$$

Demonstração: Sejam $G = \frac{\Gamma(n)}{\Gamma(\delta)}$ e $H = \frac{\Gamma(m)}{\Gamma(\delta)}$. Pelo teorema anterior, temos que $G \cong \frac{\Gamma(d)}{\Gamma(n)}$ e $H \cong \frac{\Gamma(d)}{\Gamma(m)}$ Agora, sejam $A \in \Gamma(n)$ e $B \in \Gamma(m)$.
$(A - Id) \ \in \mathbb{M}_{2\times 2}(\mathbb{Z}_n)$, $(B - Id) \ \in \mathbb{M}_{2\times 2}(\mathbb{Z}_m)$ de modo que:

$$(A - Id)(B - Id) \in (\mathbb{Z}_{nm}) \text{ e } (B - Id)(A - Id) \in (\mathbb{Z}_{nm}) \Rightarrow$$
$$(A - Id)(B - Id) \equiv 0 \ \ mod(\delta) \text{ e } (B - Id)(A - Id) \equiv 0 \, mod(\delta) \Rightarrow$$
$$AB - A - B + Id \equiv 0 \ \ mod(\delta) \text{ e } BA - B - A + Id \equiv 0 \, mod(\delta) \Rightarrow$$
$$AB \equiv BA \ \ mod(\delta)$$

Assim, se $\bar{A} \in G$ e $\bar{B} \in H$ temos que $\bar{B}\bar{A} = \bar{A}\bar{B}$, e pelo teorema 1.4.1 temos:

$$GH = \frac{\Gamma(n)}{\Gamma(\delta)} \cdot \frac{\Gamma(m)}{\Gamma(\delta)} = \frac{\Gamma(d)}{\Gamma(\delta)},$$

e $G \cap H = \frac{\Gamma(n)}{\Gamma(\delta)} \cap \frac{\Gamma(m)}{\Gamma(\delta)} = \frac{\Gamma(\delta)}{\Gamma(\delta)} = Id$, portanto $GH = G \times H$, de modo que:

$$\frac{\Gamma(d)}{\Gamma(\delta)} = G \times H \cong \frac{\Gamma(d)}{\Gamma(n)} \times \frac{\Gamma(d)}{\Gamma(m)} \ \square$$

Corolário 1.3.1 *Suponha* $mdc(n,m) = 1$. *Temos então que (observando que* $\Gamma(1) = \Gamma$) :

$$G(nm) = \frac{\Gamma}{\Gamma(nm)} \cong \frac{\Gamma}{\Gamma(n)} \times \frac{\Gamma}{\Gamma(m)}$$

Assim o estudo dos grupos $G(n)$, $n \in \mathbb{N}$ se reduz ao estudo dos grupos $G(p^m)$ onde p é primo e $m \in \mathbb{N}$. De fato, se n for um inteiro, cuja decomposição em fatores primos é $n = p_1^{n_1} p_2^{n_2} \dots p_m$, vamos ter que:

$$G(n) = G(p_1^{n_1}) \times G(p_2^{n_2}) \times \ldots \times G(p_m^{n_m}).$$

Vamos agora calcular a ordem de $G(p^n)$, onde p é primo. Para isso, primeiro vamos calcular a ordem de $GL(2, \mathbb{Z}_p)$.

Teorema 1.3.4 $|GL(2,\mathbb{Z}_p)| = p(p-1)(p^2-1)$.

Demonstração: Seja $A \in \mathbb{M}_{2x2}(\mathbb{Z}_p)$. Temos que $A = (v_1, v_2)$, onde $v_i \in \mathbb{Z}_p^2$. Se A pertence a $GL(2,\mathbb{Z})$ se, e somente se, $det(A) \neq 0$. para que isso ocorra, v_1 e v_2 devem ser l.i. Assim temos $p^2 - 1$ valores possíveis para v_1 (excluímos somente $(0,0)$). Agora, v_2 não pode estar no espaço gerado por v_1, que possui p elementos, de modo que temos $p^2 - p$ valores possíveis para v_2, de onde concluímos que $|GL(2,\mathbb{Z}_p)| = (p^2-p)(p^2-1) = p(p-1)(p^2-1)$. $\square$

Lema 1.3.3 $(GL(2,\mathbb{Z}_p) : SL(2,\mathbb{Z}_p)) = p - 1$.

Demonstração: Seja A matriz pertencente a $GL(2,\mathbb{Z}_p)$, e $det(A) = \epsilon$. Temos que a matriz $A^{-1}\begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix}$ pertence a $SL(2,\mathbb{Z}_p)$, pois $det\left(A^{-1}\begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix}\right) = det\,(A^{-1})\,\epsilon = 1$. Assim, temos que $(A)SL(2,\mathbb{Z}) = \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix} SL(2,\mathbb{Z})$, de modo que o número de classes de equivalência de $\frac{GL(2,\mathbb{Z}_p)}{SL(2,\mathbb{Z}_p)}$ é igual ao número de ϵ pertencentes a $\mathbb{Z}_p$ distintos e diferentes de 0, isto é, $(GL(2,\mathbb{Z}_p) : SL(2,\mathbb{Z}_p)) = p - 1$.
Observe que fazendo algumas ligeiras modificações nesta demonstração obtemos que

$$(GL(2,\mathbb{Z}_p^n) : SL(2,\mathbb{Z}_p^n)) = p^n(1 - \frac{1}{p}),$$

para isso observe que $\epsilon = det(A)$ neste caso é um elemento inversível de $\mathbb{Z}_{p^n}$, de modo que neste caso ϵ possui $p^n(1 - \frac{1}{p})$ valores possíveis distintos. $\square$

Teorema 1.3.5 $|SL(2,\mathbb{Z}_p)| = p(p^2-1)$.

Demonstração: Temos pelo lema anterior que $\left|\frac{GL(2,\mathbb{Z}_p)}{SL(2,\mathbb{Z}_p)}\right| = p-1$, portanto $\frac{|GL(2,\mathbb{Z}_p)|}{p-1} = |SL(2,\mathbb{Z}_p)|$. Agora, $|GL(2,\mathbb{Z}_p)| = p(p-1)(p^2-1)$, de onde concluímos que $|SL(2,\mathbb{Z}_p)| = p(p^2-1)$. □

Vamos agora calcular a ordem de $G(p^n)$. Observe que podemos enxergar $SL(2,\mathbb{Z}_p^n)$ como sendo o conjunto das matrizes A pertencentes a $\mathbb{M}_{2x2}$ cujas entradas tem seus valores no conjunto $0,1,\ldots,p^n-1$ e $mdc(det(A),p^n) = 1$. Podemos então escrever a matriz A como $A_0 + pA_1$, onde as entradas de A_0 tem seus valores no conjunto $0,1,p,\ldots,p-1$, e as entradas de A_1 no conjunto de resíduos modulo P^{n-1} (isto é obtido simplesmente escrevendo as entradas de A na base p, e separando a soma de forma conveniente). Observe que $mdc(det(A),p^n) = 1$, de modo que $mdc(det(A),p) = 1$ e portanto temos que $det(A) \equiv det(A_0)\ mod(p)$. Assim, temos que os A_0 possíveis são os elementos de $SL(2,\mathbb{Z}_p)$, de onde concluímos que o número de matrizes A possíveis é o número de matrizes A_1, que é igual a $p^{4(n-1)}$, vezes o número de matrizes A_0, que é igual a $|GL(2,\mathbb{Z}_p)|$. Temos portanto que $|GL(2,\mathbb{Z}_{p^n})| = p^{4(n-1)}p(p-1)(p^2-1)$, ou equivalentemente:

Teorema 1.3.6 $|GL(2,\mathbb{Z}_{p^n})| = p^{4n}(1-\frac{1}{p})(1-\frac{1}{p^2})$.

Corolário 1.3.2 $|G(P^n)| = p^{3n}(1-\frac{1}{p^2})$

Demonstração: Temos pela observação no final do lema 1.3.3 que $(GL(2,\mathbb{Z}_p^n) : SL(2,\mathbb{Z}_p^n)) = p^{n-1}(p-1)$, e portanto concluímos do teorema 1.3.6 que:

$$|G(P^n)| = \frac{|GL(2,\mathbb{Z}_{p^n})|}{p^n(1-\frac{1}{p})} = p^{3n}(1-\frac{1}{p^2}).$$

□

Teorema 1.3.7 *Seja $n = p_1^{t_1}\ldots p_m^{t_m}$, onde cada p_i é primo. Temos então que:*

$$|G(n)| = n^3 \cdot \prod_{p|n}\left(1-\frac{1}{p^2}\right).$$

Demonstração:

$$G(n) \equiv G(p_1^{t_1}) \times \ldots \times G(p_m^{t_m}) \Rightarrow$$
$$|G(n)| = \prod_{i=1}^{m}\left|G(p_i^{t_i})\right| = \prod_{i=1}^{m} p_i^{3t_i}\left(1-\frac{1}{p_i^2}\right) =$$
$$n^3\prod_{i=1}^{m}\left(1-\frac{1}{p_i^2}\right) = n^3 \cdot \prod_{p|n}\left(1-\frac{1}{p^2}\right). \ \square$$

1.4 Nível de um subgrupo normal

Definição 1.4.1 *Seja $z = xy$(o elemento correspondente a matriz S) e G subgrupo normal de Γ com índice finito μ. Definimos como o nível do subgrupo G o menor inteiro positivo n tal que $z^n \in G$. Este número está bem definido, pois $z^\mu \in G$.*

Observe que a definição de nível anterior coincide com esta. De fato, caso $\Gamma(n)$ seja subgrupo de G, $z^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \Gamma(n) \subset G$, de onde temos que G possui nível n.

Classificação por nível:
É possível classificar os subgrupos de índice finito através de seu nível, por exemplo, os grupos $\Delta(z^n), n \leq 5$ têm índices finitos, e seus índices, denotados por μ são:

n	1	2	3	4	5
μ	1	6	12	24	60

Utilizando o fato que os grupos normais de nível n contém $\Delta(z^n)$ é possível obter uma classificação completa dos subgrupos normais de nível até 5:

Nível	Grupos
1	Γ
2	$\Gamma^2, \Delta(z^2)$
3	$\Gamma^3, \Delta(z^3)$
4	$\Delta(z^4)$
5	$\Delta(z^5)$

Detalhes podem ser encontrados em [7], outros resultados desse tipo pode ser encontrados em [6]

Nível de um subgrupo qualquer:
Seja G um subgrupo qualquer de Γ de índice μ. Temos que se $A \in \Gamma$ então $A^{\mu!} \in G$. De fato, não podem existir mais do que μ potências distintas de A módulo G, logo $\exists n, m \in \mathbb{N}, n < m < 2n$ tais queA^n, A^m pertencem a mesma classe lateral, de modo que $A^{m-n} \in G \Rightarrow A^{\mu!} \in G$.

Agora, seja $C \in \Gamma$, denotamos por $e(C)$ o menor inteiro positivo tal que $\pm C^{-1} S^{e(C)} C \in G$. Definimos como nível do subgrupo G o menor múltiplo comum dos inteiros $e(C)$, onde C percorre Γ, denotamos esse inteiro por n. Observe que $n|\mu!$, pois $e(C)|\mu! \, \forall C \in \Gamma$.

Note que se G têm nível n, então G contém todos os conjugados de S^n(pois $e(C)|n \quad \forall C \in G$), portanto $\Delta(z^n) \subset G$. Reciprocamente, se n é o menor inteiro tal que $\Delta(z^n) \subset G$, o nível de G é n. Assim, no caso de G ser um subgrupo normal, essa definição coincide com a definição 1.4.1.

O resultado a seguir,o teorema de Wohlfahrt nos da um critério para verificar se um dado grupo G é grupo de congruência. Antes de partir para o resultado, vamos precisar do seguinte lema.

Lema 1.4.1 *Seja G subgrupo de Γ tal que:*

$$G \supset \Gamma(mn) \tag{1.1}$$

$$G \supset \Delta(S^n) \tag{1.2}$$

onde n, m são inteiros. Então $G \supset \Gamma(n)$.

Demonstração: Podemos concluir a partir de (1.2) que as matrizes

$$S(nx) = \begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix}, \qquad W(ny) = \begin{pmatrix} 1 & 0 \\ ny & 1 \end{pmatrix} \text{ e}$$

$$V(z) = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -z & 1 \end{pmatrix} = \begin{pmatrix} 1+nz & -n \\ nz^2 & 1-nz \end{pmatrix}$$

pertencem a G, $\forall x, y, z$ naturais. Seja $M \in \Gamma(n)$. Temos que:

$$M = \begin{pmatrix} 1+na_1 & nb_1 \\ nc_1 & 1+nd_1 \end{pmatrix}$$

Vamos construir agora um $x \in \mathbb{Z}$ tal que $\text{mdc}(1 + na + n^2cx, m) = 1$. Primeiro observe que $\text{mdc}(n^2c_1, 1 + na) = 1$, pois $\det(M) = 1$. Agora, sejam, $p_1, p_2, \ldots, p_k$ fatores primos de m. Caso p_1 seja fator de $1 + na$, tome $x_1 = 1$. Caso contrário, tome $x_1 = p_1$. Temos então que p_1 não será um fator de $1 + na_1 + n^2c_1x_1$. Prossiga indutivamente(tomando $x_2 = x_1p_2$ caso p_2 não divida $1 + na_!$ e $x_2 = x_1$ caso, e prossiga desta maneira) e tome $x = x_k$. Temos então que por construção $\text{mdc}(1 + na_1 + n^2c_1x, m) = 1$. Tome agora a matriz M_1 como sendo:

$$M_1 = V(z)M = \begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1+na_1 & nb_1 \\ nc_1 & 1+nd_1 \end{pmatrix} =$$

$$\begin{pmatrix} 1+na_1+n^2c_1x & nb_1+nx(1+nd_1) \\ nc_1 & 1+nd_1 \end{pmatrix} = \begin{pmatrix} 1+na_2 & nb_2 \\ nc_2 & 1+nd_2 \end{pmatrix},$$

onde $a_2 = a_1 + nc_1x, b_2 = b_1 + x(1 + nd_1), c_2 = c_1$ e $d_1 = d_2$.

Considere agora:

$$M_2 = V(z)M_1 = \begin{pmatrix} 1+nz & -n \\ nz^2 & 1-nz \end{pmatrix}\begin{pmatrix} 1+na_2 & nb_2 \\ nc_2 & 1+nd_2 \end{pmatrix} =$$
$$\begin{pmatrix} (1+na_2)(1+nz)-n^2c_2 & (1+nz)nb_2 - n(1+nd_2) \\ nz^2(1+na_2)+nc_2(1-nz) & n^2b_2z^2+(1+nd_2)(1-nz) \end{pmatrix}.$$

Queremos determinar z tal que $(1+na_2)(1+nz)-n^2c_2 \equiv 1 \bmod(nm)$. Isso é equivalente a encontrar z tal que $a_1 - nc + (1+na_1)z \equiv 0 \bmod(m)$ como $\mathrm{mdc}(1+na_1, m) = 1$ essa equação tem solução para z e, para esse valor de z temos que:

$$M_2 \equiv \begin{pmatrix} 1 & (1+nz)nb_2 - n(1+nd_2) \\ nz^2(1+na_2)+nc_2(1-nz) & n^2b_2z^2+(1+nd_2)(1-nz) \end{pmatrix} \bmod(nm) \equiv$$
$$W(nz^2(1+na_2)+nc_2(1-nz))S((1+nz)nb_2 - n(1+nd_2))\bmod(nm) \Rightarrow$$
$$S(-((1+nz)nb_2 - n(1+nd_2)))W(-(nz^2(1+na_2)+nc_2(1-nz)))M_2 \equiv Id \bmod(nm)$$

.

De onde segue por (1.2) que $S(-((1+nz)nb_2 - n(1+nd_2)))W(-(nz^2(1+na_2)+nc_2(1-nz)))M_2 \in G$, de onde concluímos que $M \in G$. □

Teorema 1.4.1 (Wohlfahrt)*Seja G subgrupo de Γ de nível n. Então G é um grupo de congruência se, e somente se, $G \supset \Gamma(n)$.*

Demonstração: A volta é automática da definição de grupo de congruência. Suponha então que G seja um grupo de congruência. Então existe m inteiro positivo tal que $\Gamma(m) \subset G$ e portanto $\Gamma(nm) \subset G$. Agora, G tem nível n, logo $\Delta(S^n) \subset G$, e pelo lema anterior temos o resultado. □

Capítulo 2

Geometria hiperbólica

Neste capítulo iremos apresentar o modelo do semi-plano complexo superior que utilizaremos no estudo de Γ. Começaremos definindo o conjunto e a métrica que será utilizada e mostraremos que as transformações de Γ pertencem ao grupo de isometrias do plano hiperbólico, e definiremos a noção de geodésicas, além de mostrar algumas outras propriedades sobre o plano hiperbólico.

2.1 O plano hiperbólico

Vamos começar fazendo uma descrição do modelo de geometria hiperbólica que será utilizado neste trabalho.
Considere o semi-plano superior do plano complexo:

$$H^2 = \{x + iy; y > 0\}$$

Usaremos esse conjunto, dotado da métrica que iremos definir a seguir como o nosso modelo de geometria hiperbólica.

Primeiro vamos definir o conceito do comprimento de uma curva diferenciável em H^2. Seja $\gamma : [a, b] \to H^2$ uma curva diferenciável em H^2. Definimos o comprimento de γ, denotado por $\|\gamma\|$, como sendo:

$$\|\gamma\| = \int_a^b \frac{\left|\gamma'(t)\right|}{\operatorname{Im}\left[\gamma(t)\right]} dt.$$

Como métrica tomamos então a função ρ dada por:

$$\begin{aligned} \rho : H^2 \times H^2 &\to \mathbb{R}_+^* \\ (z, w) &\mapsto \inf \|\gamma\|, \end{aligned}$$

onde o ínfimo e tomado entre todas as curvas γ que ligam z e w.

Teorema 2.1.1 *Temos que*

$$\rho : H^2 \times H^2 \to \mathbb{R}_+^*$$
$$(z, w) \mapsto inf\|\gamma\|,$$

é uma métrica para H^2.

Demonstração: Temos diretamente da definição que ρ é uma função não negativa, pois $0 \leq \|\gamma\|$ para toda curva γ ligando z a w.
Temos também que $\rho(z, w) = 0 \Leftrightarrow z = w$. De fato, se $z = w$ temos que $\rho(z, w) = 0$, pois a curva $\gamma(t) = z$ e tal que $\|\gamma\| = 0$, de modo que $\inf\|\gamma\| \leq 0$. Agora, suponha $z \neq w$. Temos, se $\gamma(t) = x(t) + iy(t)$ é uma curva ligando z a w, temos que $\|\gamma\| = \int_a^b \frac{|\gamma'(t)|}{\mathrm{Im}[\gamma(t)]} dt \geq \int_a^b \frac{|y'(t)|}{y(t)} dt = \log(|z/w|) > 0$, pois $z \neq w$. Assim, temos que se $z \neq w$, $\rho(z, w) = \inf\|\gamma\| > 0$. Temos portanto que $\rho(z, w) = 0 \Leftrightarrow z = w$.
Obviamente temos que $\rho(z, w) = \rho(z, w)$, pois o comprimento das curvas que ligam z a w não depende da sua orientação.
Para mostrar a desigualdade triangular, considere z, w, h elementos quaisquer de H^2. se α_1 é uma curva que liga z a h e α_2 é uma curva que liga h a w, temos que a curva

$$\alpha = \begin{cases} \alpha_1(2t), \text{ se } 0 \leq t \leq 1/2 \\ \alpha_2(2t - 1/2), \text{ se } 1/2 \leq t \leq 1 \end{cases},$$

é uma curva que liga z a w, e temos também que $\|\alpha\| = \|\alpha_1\| + \|\alpha_2\|$. Temos que $\rho(z, w) \leq \|\alpha\| = \|\alpha_1\| + \|\alpha_2\|$, portanto tomando o ínfimo para α_1 e α_2 obtemos que $\rho(z, w) \leq \rho(z, h) + \rho(h, w)$
Assim, concluímos que ρ é uma métrica para H^2. □

Vamos agora dar uma forma explícita para calcular a distância entre dois pontos. Para isso vamos antes mostrar 2 lemas.

Lema 2.1.1 *Seja* $g : H^2 \to H^2$ *transformação da forma* $g(z) = \frac{az+b}{cz+d}$, *onde* a, b, c *e* d *são números reais tais que* $ad - bc \neq 0$. *Temos que,* $\forall z, w \in H^2$, $\rho(z, w) = \rho(g(z), g(w))$

Demonstração: Seja $g(z) = \frac{az+b}{cz+d}$ uma função de H^2 em H^2 como descrita acima.
Considere $z = x + iy \in H^2$. Temos que:

$$|g'(z)| = \left|\frac{a(cz + d) - c(az + b)}{(cz + d)^2}\right| = \left|\frac{ad - bc}{(cz + d)^2}\right| = \frac{ad - bc}{|cz + d|^2}$$

e

$$\mathrm{Im}\,[g(z)] = \mathrm{Im}\left[\frac{a(x + iy) + b}{c(x + iy) + d}\right] = \mathrm{Im}\left[\frac{(a(x + iy) + b)(c(x - iy) + d)}{(c(x + iy) + d)(c(x - iy) + d)}\right]$$
$$= \frac{y(ad - bc)}{|cz + d|^2} = \frac{y(ad - bc)}{|cz + d|^2}.$$

Tomando o quociente obtemos que:

$$\frac{|g'(z)|}{\operatorname{Im}[g(z)]} = \frac{|cz+d|^2}{y(ad-bc)}\frac{(ad-bc)}{|cz+d|^2} = \frac{1}{y} = \frac{1}{\operatorname{Im}[z]}.$$

De onde obtemos que:

$$\|g(\gamma)\| = \int_a^b \frac{|g'(\gamma(t))| \cdot |\gamma'(t)|}{\operatorname{Im}[g(\gamma(t))]}dt = \int_a^b \frac{|\gamma'(t)|}{\operatorname{Im}[\gamma(t)]}dt = \|\gamma\|.$$

□

Observe que com este lema temos que as transformações de Γ são isometrias de H^2.

Lema 2.1.2 *Sejam $z, w \in H^2$. Temos que existe uma transformação $g(z) = \frac{az+b}{cz+d}$, onde $a, b, c, d \in \mathbb{R}$ tal que $g(w) = iw'$ e $g(z) = iz'$, onde $w', z' \in \mathbb{R}$.*

Demonstração: Tome z e w pontos quaisquer de H^2 e seja L o círculo ou reta contendo w e z perpendicular ao eixo real. Seja α um ponto de encontro de L com o eixo real. Considere a transformação $h_1(t) = t - \alpha$. Temos que $L_1 = h_1(L)$ é um círculo ou reta que passa pelo ponto 0+i0, de modo que seus pontos satisfazem uma equação da forma $Az\bar{z} + Bz + C\bar{z} = 0$. Agora, aplicando a transformação $h_2(t) = -1/t$ em L_1 obtemos o conjunto L_2, cujos pontos satisfazem a equação da reta $Cz + B\bar{z} + A = 0$ perpendicular ao eixo real. Assim, temos que a transformação $g(t) = \frac{1}{-(t-\alpha)} + \beta$, onde β é um dos pontos de encontro do eixo real com L_2, leva L no eixo imaginário. □

Teorema 2.1.2 *Sejam $w, z \in H^2$. Temos que:*

$$(1)\rho(z,w) = log\left(\frac{|z-\bar{w}| + |z-w|}{|z-\bar{w}| - |z-w|}\right)$$
$$(2)cosh(\rho(z,w)) = 1 + \frac{|z-w|^2}{2Im[z]\,Im[w]}$$
$$(3)senh(\frac{1}{2}\rho(z,w)) = \frac{|z-w|}{2(Im[z]\,Im[w])^{1/2}}$$
$$(4)cosh(\frac{1}{2}\rho(z,w)) = \frac{|z-\bar{w}|}{2(Im[z]\,Im[w])^{1/2}}$$
$$(5)tanh(\frac{1}{2}\rho(z,w)) = \left|\frac{z-w}{z-\bar{w}}\right|$$

Demonstração: Vamos mostrar que estas equações são equivalentes.
Primeiro observe que a função $\cosh(x)=\frac{e^x+e^{-x}}{2}$ é uma bijeção para valores reais positivos de x, de modo que (tomando $z = x_1 + iy_1$ e $w = x_2 + iy_2$):

$$\rho(z,w) = \log\left(\frac{|z-\bar{w}| + |z-w|}{|z-\bar{w}| - |z-w|}\right) \Leftrightarrow \cosh(\rho(z,w)) = \frac{e^{\log\left(\frac{|z-\bar{w}|+|z-w|}{|z-\bar{w}|-|z-w|}\right)} + e^{-\log\left(\frac{|z-\bar{w}|+|z-w|}{|z-\bar{w}|-|z-w|}\right)}}{2}$$

$$\begin{aligned}
\frac{e^{\log\left(\frac{|z-\bar{w}|+|z-w|}{|z-\bar{w}|-|z-w|}\right)}+e^{-\log\left(\frac{|z-\bar{w}|+|z-w|}{|z-\bar{w}|-|z-w|}\right)}}{2} &= \frac{1}{2}\left(\frac{|z-\bar{w}|+|z-w|}{|z-\bar{w}|-|z-w|}-\frac{|z-\bar{w}|-|z-w|}{|z-\bar{w}|+|z-w|}\right)\\
&= \frac{1}{2}\left(\frac{(|z-\bar{w}|+|z-w|)^2+(|z-\bar{w}|-|z-w|)^2}{|z-\bar{w}|^2-|z-w|^2}\right)\\
&= \frac{|z-\bar{w}|^2+|z-w|^2}{|z-\bar{w}|^2-|z-w|^2}\\
&= \frac{2x_1^2+2x_2^2+2y_1^2+2y_2^2-4x_1x_2}{4y_1y_2}\\
&= \frac{2x_1^2+2x_2^2+2y_1^2+2y_2^2-4x_1x_2\pm 4y_1y_2}{4y_1y_2}\\
&= \frac{2|z-w|^2+4y_1y_2}{4y_1y_2}=1+\frac{|z-w|^2}{2\mathrm{Im}\,[z]\,\mathrm{Im}\,[w]}
\end{aligned}$$

Assim, (1) $\Leftrightarrow$ (2). As demais equivalências são obtidas de forma análoga.
Agora, observe que ambos os lados da equação (2) são invariantes pelas transformações g descritas no lema 2.1.1. A invariância do lado esquerdo segue diretamente do lema e a invariância do lado direito é obtida através de uma conta direta.

Temos também pelo lema 2.1.2 que para todo $z, w \in H^2$ que existem uma aplicação g tal que $g(z) = iz'$ e $g(w) = iw'$, onde $z', w' \in \mathbb{R}$. De modo que precisamos mostrar que vale (2) para pontos da forma ip e iq, onde $p, q \in \mathbb{R}$.

Considere agora a curva

$$\gamma(t) = x(t) + iy(t) \qquad 0 \leq t \leq 1,$$

tal que $\gamma(0) = ip$ e $\gamma(1) = iq$. Temos que:

$$\|\gamma\| = \int_0^1 \frac{|x'(t)+iy'(t)|}{y(t)}dt \geq \int_0^1 \frac{y'(t)}{y(t)}dt = \log(q/p).$$

Agora, tomando $\gamma(t) = i(p+t(q-p))$ temos que $\|\gamma\| = \log(q/p)$, de modo que $\rho(ip, iq) = \log(q/p)$. Substituindo essa igualdade em (2) obtemos no lado esquerdo que:

$$\cosh(\rho(ip, iq)) = \frac{e^{\log(q/p)}+e^{-\log(q/p)}}{2} = \frac{p^2+q^2}{2pq}$$

E no lado direito que:

$$1+\frac{|i(p-q)|^2}{2pq} = 1+\frac{(p-q)^2}{2pq} = 1+\frac{p^2-2pq+q^2}{2pq} = 1-1+\frac{p^2+q^2}{2pq} = \frac{p^2+q^2}{2pq}.$$

Assim, temos que vale (2), portanto segue o resultado. □

Terminamos esta seção fazendo uma breve menção da topologia e medida que utilizaremos para H^2.

Um subconjunto A de H^2 é dito aberto se, $\forall x \in A$ temos que existe $r > 0$ tal que $B(x, r) = \{z \in H^2; \rho(z, x) < r\} \subset A$. Nesta topologia, um conjunto K é compacto se e somente se toda sequencia de Cauchy contida em K converge para um ponto em K e K e totalmente limitado. Denotaremos o fecho de um conjunto A nesta topologia por $\widetilde{A}$.

A medida que consideraremos é a medida de Borel obtida pela topologia descrita acima. Vale observar que conjuntos em H^2 que têm medida de lebesgue nula também possuem medida de Borel nula nesta topologia.

2.2 Geodésicas

Nesta seção descreveremos as geodésicas do plano hiperbólico, isso é, as curvas com o menor comprimento que ligam 2 pontos quaisquer de H^2.

Definição 2.2.1 *Chamamos de geodésicas as curvas de H^2 obtidas pela interseção de uma reta ou círculo perpendicular ao eixo real com o semi-plano superior H^2.*

A partir dessa definição podemos concluir algumas propriedades sobre as geodésicas:

Proposição 2.2.1

(1) Sejam z e w pontos de H^2. Então existe uma única geodésica contendo z e w.
(2) Duas geodésicas distintas de H^2 se encontram no máximo em um único ponto.
(3) Dadas 2 geodésicas L_1 e L_2 de H^2 temos que existe uma isometria $g \in PSL(2, \mathbb{R})$ tal que $g(L_1) = L_2$
Demonstração: (1) e (2) seguem diretamente da definição de geodésicas.

Agora, sejam L_1 e L_2 geodésicas de H^2. Temos pelo lema 2.1.2 que existem transformações g_1 e g_2 que levam L_1 e L_2 no eixo imaginário.Temos então que $g_2^{-1}(g_1(L_1)) = L_2$. □

Para os próximos resultados vamos precisar de mais algumas definições:

Definição 2.2.2 *Sejam $z, w \in H^2$. Chamamos o segmento aberto de uma geodésica o conjunto, que denotaremos por (z, w), definido da seguinte maneira:*

Tome L a única geodésica passando por z e w e considere agora a aplicação $\gamma : [0, 1] \to L$ parametrização tal que $\gamma(0) = z$, $\gamma(1) = w$. Tomamos o conjunto (z, w) como sendo o conjunto $\gamma((0, 1))$. Definimos de maneira análoga o segmento fechado $[z, w]$ e os segmentos $(z, w]$ e $[z, w)$

Na demonstração do teorema 2.1.2 mostramos que, dados dois pontos ip e iq, $p, q \in \mathbb{R}$ e α uma curva ligando os dois pontos temos que $\rho(ip, iq) = \|\alpha\|$ se é somente se α esta contida

no eixo imaginário. Em outras palavras, $\|\gamma\| = \rho(iq, ip)$ se somente se $\gamma : [0,1] \to H^2$ é uma parametrização do segmento de geodésica $[iq, ip]$.

Agora, dados dois pontos quaisquer z e w de H^2, considerando a transformação dada pelo lema 2.1.2 obtemos o seguinte resultado:

Teorema 2.2.1 *Sejam $z, w \in H^2$. Temos que uma curva γ ligando z a w satisfaz:*

$$\|\gamma\| = \rho(z, w)$$

se, e somente se, $\gamma : [0,1] \to H^2$ é uma curva que liga z a w $[z, w]$.

Utilizando um raciocínio análogo a esse (considerar o problema somente no eixo imaginário e depois utilizar das isometrias) obtemos também que:

Teorema 2.2.2 *Sejam $z \neq w$ pontos de H^2. temos que:*

$$\rho(z, w) = \rho(z, \zeta) + \rho(\zeta, w)$$

se, e somente se, $\zeta \in [z, w]$.

2.3 Conjuntos convexos

Dizemos que um subconjunto C de H^2 é convexo se e somente se, dados z e w elementos arbitrários de C, o segmento de geodésica $[z, w]$ está contido em C . Podemos concluir diretamente da definição algumas propriedades sobre conjuntos convexos:

Proposição 2.3.1 *Seja $g \in \Gamma$:*
(1) Se C for um conjunto convexo, então $g(C)$ também sera, para toda isometria g do plano hiperbólico.
(2) Se C for um conjunto convexo, então também serão convexos os conjuntos C^0 e $\widetilde{C}$.(O interior e o fecho hiperbólicos do conjunto C respectivamente)
(3) Se $C_1, C_2, \ldots$ forem conjuntos convexos tais que $C_1 \subset C_2 \subset \ldots$, então $\bigcup_{n\in\mathbb{N}} C_n$ é um conjunto convexo.
(4) Se $C_{\alpha\lambda\in\Lambda}$ for uma família qualquer de conjuntos convexos. Temos que, $\bigcap_{\lambda\in\Lambda} E_\lambda$ é um conjunto convexo.

Capítulo 3

Regiões fundamentais

3.1 Domínios fundamentais

Definição 3.1.1 *Seja G um subgrupo de Γ. Dizemos que um conjunto $F \subset H^2$ é um conjunto fundamental para G em H^2 se F contém exatamente um ponto de cada G-órbita dos elementos de H^2, isto é:*

$$|F \cap O_G(z)| = 1 \ , \forall z \in H^2,$$

onde $O_G(z) = \{g(z); g \in G\}$.
Temos diretamente da definição que:

$$\bigcup_{g \in G} g(F) = H^2.$$

Definição 3.1.2 *Seja G um subgrupo de Γ. Um conjunto $D \subset H^2$ é dito um domínio fundamental para G se e somente se D satisfaz as seguintes propriedades:*

(1) *D é um domínio, isto é, D é um aberto conexo.*

(2) *$\exists F$ conjunto fundamental para G tal que $D \subset F \subset \widetilde{D}$*

(3) *∂D é um conjunto de medida nula.*

Temos então que, se D é um domínio fundamental para G então:

$$D \cap g(D) = \emptyset$$
$$\bigcup_{g \in G} g(\widetilde{D}) = H^2$$

3.2 Domínios fundamentais localmente finitos

Nessa seção iremos estudar um tipo particular de domínio fundamental, sobre o qual podemos obter algumas propriedades interessantes sobre a estrutura dos subgrupos de Γ.

Definição 3.2.1 *Seja G subgrupo de Γ. Um domínio fundamental D para G é dito localmente finito se e so se $\forall K \subset H^2$ compacto tivermos que K intercepta somente um número finito de G-imagens de $\widetilde{D}$, isto é,*

$$\left|\left\{g \in G; g(\widetilde{D}) \cap K \neq \emptyset\right\}\right| < \infty.$$

Temos diretamente da definição o seguinte lema:

Lema 3.2.1 *Seja D é um domínio fundamental para um grupo G. D é localmente finito se e somente se para todo ponto z pertencente a H^2 existe uma vizinhança V compacta de z e $\{g_1, g_2, \ldots, g_n\} \subset G$ tais que:*

$$z \in g_1(\widetilde{D}) \cap \ldots \cap g_n(\widetilde{D})$$
$$V \subset g_1(\widetilde{D}) \cup \ldots \cup g_n(\widetilde{D})$$
$$h(D) \cap V = \emptyset \text{ se, e somente se, } h \neq g_i,\ i = 1, \ldots, n.$$

Demonstração: Suponha D dominio fundamental localmente finito. Seja V_0 uma vizinhança compacta de um ponto z pertencente a H^2. Por hipótese temos que V_0 só intercepta um número finito de G-imagens de $\widetilde{D}$, digamos $g_1(\widetilde{D}), \ldots, g_t(\widetilde{D})$.
Para cada i temos que, ou $z \notin g_i(\widetilde{D})$ ou $z \in g_i(\widetilde{D})$. Caso $z \notin g_i(\widetilde{D})$ tome V_i tal que $V_i \subset V_{i-1} \cap (g_i(\widetilde{D}))^c$. Caso $z \in g_i(\widetilde{D})$ tome $V_i = V_{i-1}$. Repetindo esse processo indutivamente de $i = 1$ ate $i = t$ obtemos a vizinhança V desejada, e tomaremos como $\{g_1, g_2, \ldots, g_n\}$ os g_i tais que $z \in g_i(\widetilde{D})$.

Para mostrar a recíproca, simplesmente observamos que se K é um compacto de H^2, a família de vizinhanças que existem pela afirmação do lema forma uma cobertura para K, tendo portanto uma subcobertura finita e um número finito de elementos de G cuja interseção com K é não vazia. □

Terminamos esta seção dando um teorema que nos mostra uma importante propriedade dos domínios fundamentais localmente finitos.

Teorema 3.2.1 *Seja D domínio fundamental localmente finito para um grupo G. Então o conjunto $G_0 = \left\{g \in G : g(\widetilde{D}) \cap \widetilde{D} \neq \emptyset\right\}$ gera G.*

Demonstração: Sejam G^* o grupo gerado por G_0 e $z \in H^2$. Temos que existe $g \in G$ tal que $g(z) \in \widetilde{D}$. Seja $h \neq g$ tal que $h(z) \in \widetilde{D}$, temos que $h(z) \in h(h^{-1}(\widetilde{D}) \cap g^{-1}(\widetilde{D})) = \widetilde{D} \cap g^{-1}(\widetilde{D})$,

de modo que $hg^{-1} \in G_0 \Rightarrow G^*hg^{-1} = G^* \Rightarrow G^*h = G^*g$.
Temos portanto que a aplicação

$$\theta : H^2 \to G/G^*$$
$$z \mapsto G^*g$$

está bem definida. Através do estudo dessa aplicação obteremos o resultado.
Seja $z \in H^2$. Como D é um domínio localmente finito, temos pelo lema 3.2.1 que existem $\{g_1, g_2, \ldots, g_n\} \subset G$ tal que $z \in g_1(\widetilde{D}) \cap \ldots \cap g_n(\widetilde{D})$ e V vizinhança de z tal que $V \subset g_1(\widetilde{D}) \cup \ldots \cup g_n(\widetilde{D})$. Se $w \in V$, $\exists\, j \in \{1, \ldots, n\}$ tal que $w \in g_j(\widetilde{D})$ e portanto $\theta(w) = G^*(g_j)^{-1} = \theta(z)$, de modo que para todo $z \in H^2$, existe uma vizinhança V de z tal que $\theta_{|V}$ é constante, e portanto usando um simples argumento de conexidade temos que θ é constante em H^2. Assim, $\theta(z) = \theta(w)$ para todo $z, w \in H^2$. Em particular, tomando $z \in D$ e $w \in g^{-1}(D)$, onde g é um elemento de G qualquer, temos que:

$$G^* = \theta(z) = \theta(w) = G^*g \Rightarrow g \in G^* \Rightarrow G \subset G^* \Rightarrow G = G^*.$$

De onde segue o resultado. □

3.3 Polígonos fundamentais convexos

Nesta seção iremos estudar um tipo especial de domínio fundamental, os que possuem natureza poligonal.
Vamos começar com algumas definições:

Definição 3.3.1 *Seja G subgrupo de Γ. Dizemos que um conjunto $P \subset H^2$ é um polígono fundamental convexo para G se P é um domínio fundamental convexo localmente finito para G.*

Definição 3.3.2 *Sejam G subgrupo de Γ e P um polígono fundamental para G. Seja $g \in G$. dizemos que o conjunto $\widetilde{P} \cap g(\widetilde{P})$ é um lado de P se $\widetilde{P} \cap g(\widetilde{P}) \neq \emptyset$. Se $g, h \in G$ são transformações tais que $\widetilde{P} \cap g(\widetilde{P}) \cap h(\widetilde{P}) \neq \emptyset$ dizemos que $\widetilde{P} \cap g(\widetilde{P}) \cap h(\widetilde{P})$ é um vértice de P.*

Proposição 3.3.1 *Seja P polígono fundamental para $G \subset \Gamma$. Temos que se $\widetilde{P} \cap g(\widetilde{P})$ é um lado de P, então $\widetilde{P} \cap g(\widetilde{P})$ é um segmento de geodésica.*

Demonstração: Como $\widetilde{P}$ é um conjunto convexo, temos que $g(\widetilde{P})$ é convexo e portanto $\widetilde{P} \cap g(\widetilde{P})$ é subconjunto convexo. Agora, suponha por absurdo que existam z_1, z_2 e z_3 pontos que não pertençam a mesma geodésica. Como $\widetilde{P} \cap g(\widetilde{P})$ é convexo, temos que os segmentos

$[z_1, z_2]$, $[z_1, z_3]$ e $[z_2, z_3]$ estão contidos em $\widetilde{P} \cap g(\widetilde{P})$, de modo que conjunto T limitado por estas geodésicas esta contido em $\widetilde{P} \cap g(\widetilde{P})$ (Pela convexidade de $\widetilde{P} \cap g(\widetilde{P})$). Agora, T não possui medida nula, mas ∂P é um conjunto de medida nula e $T \subset \widetilde{P} \cap g(\widetilde{P}) \subset \partial P$, absurdo. Logo $\widetilde{P} \cap g(\widetilde{P})$ é um segmento de geodésica.
□

Observe que temos desta proposição que um vértice é um ponto, pois é a interseção de duas geodésicas.
Vamos agora dar algumas propriedades dos polígonos fundamentais:

Teorema 3.3.1 *Seja P um polígono fundamental convexo para um subgrupo G de Γ. Temos que:*
(1) $\forall z \in \partial P$, $\exists g \in G$, $g \neq Id$ tal que $g(z) \in \partial P$.
(2) P têm um número enumerável de lados e vértices.
(3) Dado um conjunto compacto K contido em H^2 qualquer, temos que somente um número finito de lados e vértices de P intercepta K.
(4) ∂P é a união dos lados de P
(5) Os vértices de P estão contidos em exatamente 2 lados de P e são os pontos finais desses lados.

Demonstração:
1. Observe que P é localmente finito, de modo que para todo z pertencente a H^2 existem $g_1, g_2, \ldots, g_t \in G$ e uma vizinhança V de z tais que

$$z \in g_1(\widetilde{P}) \cap \ldots \cap g_t(\widetilde{P})$$
$$V \subset g_1(\widetilde{P}) \cup \ldots \cup g_t(\widetilde{P})$$

e $V \cap g(\widetilde{P}) \neq \emptyset$ somente se $g = g_j$ para algum $j = 1, \ldots t$. $z \in \partial P$, assim podemos tomar $g_1 = Id$. Agora, caso t=1, teríamos que $V \subset \widetilde{P}$, o que é um absurdo pois $z \in \partial P$. Assim, $t \geq 2$ e temos que vale (1).

2. Temos que (2) segue diretamente do fato de G ser enumerável.

3. Agora, (3) segue diretamente do fato de P ser localmente finito.

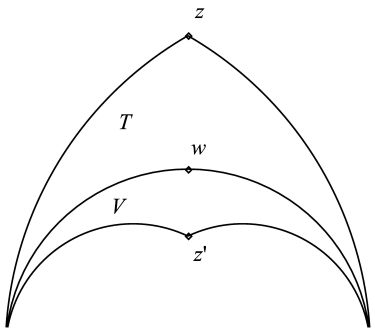
4. Vamos agora mostrar (4). Primeiro observe que $\widetilde{P} \cap g(\widetilde{P}) \subset \partial P$ para todo $g \in G$. Agora, seja w ponto de ∂P. Temos que toda vizinhança de w contem pontos de P, e pontos fora de P distintos de w. Assim, é possível encontrar uma sequência de pontos w_n contida

em ∂P tal que w_n converge para w. Temos que toda vizinhança compacta de w encontra somente um número finito de G-imagens de $\widetilde{P}$, de modo que $\exists g \in G$ e uma subsequencia $\{w_{n_k}\}_{k\in\mathbb{N}}$ de w_n tal que $w_{n_k} \subset \widetilde{P} \cap g(\widetilde{P})$, e assim temos que $w \in \widetilde{P} \cap g(\widetilde{P})$. Temos portanto que:

$$\partial P \subset \bigcup_{g\in G} \widetilde{P} \cap g(\widetilde{P}),$$

de onde temos o resultado.

5. Seja w ponto pertencente ao segmento de geodésica $\widetilde{P} \cap g(\widetilde{P})$ tal que w não seja um ponto final de $\widetilde{P} \cap g(\widetilde{P})$. Tome z ponto de P e construa um triângulo hiperbólico T que tenha como vértices z e os pontos finais do segmento $\widetilde{P} \cap g(\widetilde{P})$. Temos que $\widetilde{P} \cap g(\widetilde{P})$ será o lado oposto ao vértice z, e além disto temos que o interior de T esta contido em P. Tome agora um ponto $z' \in g(P)$ e construa um triangulo V com z' como um dos vértices e os pontos finais do segmento $\widetilde{P} \cap g(\widetilde{P})$ como os outros dois. De modo análogo a T temos que o lado oposto ao vértice z será $\widetilde{P} \cap g(\widetilde{P})$ e o interior desse triangulo por sua vez está contido em $g(P)$. Temos então a situação mostrada na figura a seguir, de onde concluímos w pertence a $\widetilde{P} \cap h(\widetilde{P})$ se, e somente se $h = g$.



□

Teorema 3.3.2 *Seja G subgrupo de Γ, e P um polígono fundamental convexo para G. Temos que o conjunto $G^* = \{g \in G;\ \widetilde{P} \cap g(\widetilde{P})$ é um lado de $P\}$ é um conjunto de geradores para G.*

Demonstração: Esse resultado e obtido como consequência do teorema 3.2.1 , precisamos mostrar somente que se $h \in G$ tal que $\widetilde{P} \cap h(\widetilde{P}) \neq \emptyset$, então h vai estar no grupo gerado por G^*.

Seja $w \in \widetilde{P} \cap h(\widetilde{P})$, onde h é elemento de G tal que $\widetilde{P} \cap h(\widetilde{P}) \neq \emptyset$. Como P é localmente finito, existem $r > 0$ tal que $B = z \in H^2; \rho(z, w) < r$ e $h_0, h_1, \ldots, h_n$ elementos de G (onde $h_0 = id$ e $h_j = h$ para algum $j \neq 0$) tais que:

$$w \in h_0(\widetilde{P}) \cap \ldots \cap h_n(\widetilde{P})$$
$$B \subset h_0(\widetilde{P}) \cup \ldots \cup h_n(\widetilde{P})$$

Diminuindo r se necessário, podemos assumir (como consequência direta de (3) do teorema 3.3.1) que os únicos lados que cruzam B são os que contêm w (no caso, os lados definidos pelos $h_i \in G^*$) e que, ou B não contém vértices, ou o único vértice de B é w.
Caso w não seja um vértice de P, temos, usando um argumento semelhante à demonstração do item (5) do teorema 3.3.1, que w está contido em somente um lado $\widetilde{P} \cap h_1(\widetilde{P})$, e temos o caso 1 mostrado pela Figura 3.1 .
Caso w seja um vértice de P, podemos reordenar os h_i obter o caso 2 mostrado pela Figura 3.2 . (tome os h_i de forma que $h_i(\widetilde{P}) \cap h_i - 1(\widetilde{P}) \neq \emptyset$) Em ambos os casos, temos que

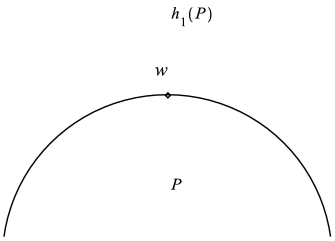


Figura 3.1:

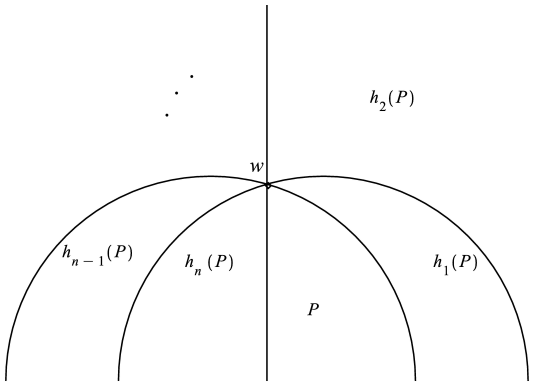


Figura 3.2:

cada polígono $h_i(P)(i \neq 0)$ tem um lado comum com o seu antecessor, isto é, temos que $h_{i-1}(\widetilde{P}) \cap h_i(\widetilde{P}) \neq \emptyset$, portanto $h_{i-1}^{-1}(h_{i-1}\widetilde{P} \cap h_i(\widetilde{P})) = \widetilde{P} \cap h_{i-1}^{-1}h_i(\widetilde{P}) \neq \emptyset$, sendo portanto um lado de P. Assim, temos que $\exists g_s \in G^*$ tal que:

$$g_s = h_{i-1}^{-1}h_i \Rightarrow h_{i-1}g_s = h_i$$

Como $h_0 = Id$, prosseguindo indutivamente concluímos que todos os h_i estão no grupo gerado por G^*, em particular $h \in G^*$, e segue o resultado.
□

Vamos concluir esta seção com a seguinte definição:

Definição 3.3.3 *Chamamos um conjunto $C = O_g(z) \cap \widetilde{P}$ de ciclo de $\widetilde{P}$. Esses conjuntos são finitos da forma $\{z_1, z_2, \ldots, z_n\}$, e dizemos que n é o comprimento de C.*

3.4 Polígonos de Dirichlet

Nesta seção iremos descrever a construção de um tipo particular de polígono fundamental, os polígonos de Dirichlet. Antes vamos precisar de algumas definições:

Definição 3.4.1 *Sejam G subgrupo de Γ e w um elemento de H^2 que não é fixo por nenhum elemento de G. Seja agora $g \in G$, $g \neq Id$. Definimos os conjuntos:*

$$\begin{aligned} L_g(w) &= \left\{z \in H^2; \rho(z,w) = \rho(z,g(w))\right\} \\ H_g(w) &= \left\{z \in H^2; \rho(z,w) < \rho(z,g(w))\right\} \\ &= \left\{z \in H^2; \rho(z,w) < \rho(g^{-1}(z),w)\right\}. \end{aligned}$$

Observe que $L_g(w)$ é lugar geométrico dos pontos que distam de w o mesmo que de $g(w)$ e $w \neq g(w)$, de modo que $L_g(w)$ é uma geodésica [1] e $H_g(w)$ é o semi-plano limitado por $L_g(w)$ que contém w.

Definição 3.4.2 *Definimos como o polígono de Dirichlet de centro w para o grupo G o conjunto:*

$$D_G(w) = \bigcap_{g \in G,\, g \neq Id} H_g(w)$$

Vamos agora dar algumas propriedades de simetria dos polígonos de Dirichlet.

Proposição 3.4.1 *Seja G subgrupo de Γ e z elemento de H^2 tal que z não é fixo por nenhum elemento de G e h elemento qualquer de Γ. Temos que:*

$$\begin{aligned} &z \in D_G(w) \Leftrightarrow w \in D_G(z) \\ &z \in H_g(w) \Leftrightarrow w \in H_g(z) \\ &h(D_G(w)) = D_{hGh^{-1}}(h(w)) \end{aligned}$$

Demonstração: Observe que $z \in H_g(w) \Leftrightarrow w \in H_{g^{-1}}(z)$ pois $z \in H_g(w) \Leftrightarrow \rho(z,w) < \rho(z,g(w)) \Leftrightarrow \rho(z,w) < \rho(g^{-1}(z),w) \Leftrightarrow w \in H_{g^{-1}}(z)$, de onde concluímos que $z \in D_G(w) \Leftrightarrow w \in D_G(z)$.

[1] A demonstração deste fato é identica a mostrar no plano euclidiano que a reta é o lugar geométrico que equidista de 2 pontos.

Temos que $h(z) \in H_{hgh^{-1}}(h(w)) \Leftrightarrow \rho(h(z), h(w)) < \rho(h(z), h(g(w))) \Leftrightarrow \rho(z, w) < \rho(z, g(w)) \Leftrightarrow z \in H_g(w) \Leftrightarrow w \in H_g(z)$.

Assim, temos que $h(D_G(w)) = D_{hGh^{-1}}(h(w))$. Em particular, se $h \in G$, temos que $h(D_G(w)) = D_G(h(w))$.

□

Teorema 3.4.1 *O polígono de Dirichlet $D_G(w)$ é um polígono fundamental convexo para G.*

Demonstração: Temos que para todo g pertencente a G o conjunto $H_g(w)$ é um convexo, pois é um semi-plano limitado pela geodésica $L_g(w)$. Temos portanto que o conjunto

$$D_G(w) = \bigcap_{g \in G,\, g \neq Id} H_g(w)$$

é um conjunto convexo. Temos ainda que $D_G(w)$ é não vazio, pois $w \in H_G(w)$.

Agora, considere K subconjunto compacto qualquer de H^2. Vamos mostrar que $K \cap L_g(w) \neq \emptyset$ somente para um número finito de $g \in G$, para isso considere $\{g_0, g_1, \ldots\}$ uma enumeração de G. Observe que $\rho(w, L_{g_n}(w)) = \frac{1}{2}\rho(w, g_n(w))$. Temos também que $\lim_{n\to\infty} \rho(w, g_n(w)) = \infty$, pois caso contrário, a sequência $g_n(w)$ estaria contida em um disco compacto centrado em w, de modo que possuiria um ponto de acumulação, absurdo, pois G possui uma ação descontínua em H^2. Assim $\lim_{n\to\infty} \rho(w, g_n(w)) = \infty$, e portanto, $\rho(w, K) < \infty$, de modo que:

$$\rho(L_{g_n}(w), K) + \rho(K, w) \geq \rho(L_{g_n}(w), w) \Rightarrow \rho(L_{g_n}(w), K) > \rho(L_{g_n}(w), w) - \rho(K, w) \to \infty$$

Então, para n grande o suficiente temos que $\rho(L_{g_n}(w), K) > 0$ e portanto $K \cap L_g(w) \neq \emptyset$, exceto para um número finito de n. Temos portanto que $D_G(w)$ é localmente finito.

Seja $z \in \widetilde{D}_G(w)$. Temos então que existe um disco fechado K com centro z tal que $\forall g \in G$, ou $K \subset H_g(w)$ ou $z \in L_g(w)$. Agora, caso $z \in D_G(w)$ a segunda possibilidade não pode ocorrer, assim concluímos que $K \subset D_G(w)$, então tomando um disco aberto menor contido em K concluímos que $D_G(w)$ é aberto.

Com isso concluímos também que, se z e um elemento de $\partial D_G(w)$, então z pertence a $L_g(w)$ para algum $g \in G$. Como a medida de $L_g(w)$ é nula para todo g e G conjunto enumerável, temos que $\partial D_G(w)$ é um conjunto de medida nula.

Vamos mostrar agora que existe F conjunto fundamental para G tal que:

$$D_G(w) \subset F \subset \widetilde{D}_G(w).$$

Seja $z \in H^2$ ponto qualquer de H^2 e considere $O_G(z)$. temos que existe um ponto $z^* \in O_G(z)$ tal que:

$$\rho(w, z^*) \leq \rho(w, g(w)),\ \forall g \in G.$$

Tal z^* existe, pois como mostramos anteriormente anteriormente, dado $K > 0$, existe somente um número finito de $g \in G$ tais que $g(z) < K$, podendo escolher z^* como sendo o $g(z)$ tal que $\rho(g(z), w)$ é mínimo.

Agora, observe que se $z \in D_G(w)$,

$$\rho(z,w) < \rho(z, g(w))\, \forall g \neq Id \Rightarrow \rho(z,w) < \rho(g^{-1}(z), w)\, \forall g \neq Id,$$

de modo que podemos escolher $z^* \in O_G(z)$ como sendo o próprio ponto z de H^2, portanto podemos construir um conjunto F formado pelos z^* de tal modo que $D_G(w) \subset F$

Vamos mostrar agora que $F \subset \widetilde{D}_G(w)$. Tome $z \in F$, e considere o segmento de geodésica $[w, z)$. Temos que $w \in D_G(w) \Rightarrow w \notin L_g(w)\, \forall g \in G$. Suponha por absurdo que algum segmento $L_g(w)$ intercepte (w, z). Temos que:

$$\rho(z,w) > \rho(z, g(w)) = \rho(g^{-1}(z), w),$$

pois $z \notin L_g(w) \cap H_g(w)$. Mas isso é absurdo, pois $z \in F$. Assim $L_g(w) \cap (w, z) = \emptyset$ $\forall g \neq Id \Rightarrow (w, z) \subset D_G(w) \Rightarrow z \in \widetilde{D}_G(w) \Rightarrow F \subset \widetilde{D}_G(w)$. Assim $D_G(w)$ é um domínio fundamental convexo de G. Resta mostrar que $D_G(w)$ é localmente finito.

Observe que se $K \subset H^2$ for um conjunto compacto, dado qualquer z ponto de H^2, temos que existe um disco fechado centrado em z que contém K, de modo que para mostrar que $D_G(w)$ é localmente finito podemos considerar somente dos discos centrados em w.

Seja K um disco compacto com centro w e raio r. Seja $g \in G$ tal que $g(\widetilde{D}_G(w)) \cap K \neq \emptyset$. Temos então que $\exists z \in \widetilde{D}_G(w)$ tal que $\rho(g(z), w) \leq r$. Agora, $z \in \widetilde{D}_G(w)$, de modo que:

$$\begin{aligned}
\rho(w, g(w)) \leq & \rho(w, g(z)) + \rho(g(z), g(w)) \\
\leq & r + \rho(z, w) \\
\leq & r + \rho(w, g(z)) \\
\leq & 2r.
\end{aligned}$$

Mas agora, como foi argumentado anteriormente, se pegarmos uma enumeração qualquer de G, digamos $\{g_0, g_1, \ldots\}$, temos que $\lim_{n\to\infty} \rho(w, g_n(w)) = \infty$. Como r está fixado, temos então que somente um número finito de $g \in G$ tais que $g(\widetilde{D}_G(w)) \cap K \neq \emptyset$, de modo que $D_G(w)$ é localmente finito. □

Teorema 3.4.2 *Seja $\{z_1, \ldots, z_n\}$ um ciclo na fronteira de um polígono de Dirichlet $D_G(z)$. Então:*

$$\rho(z_1, w) = \rho(z_2, w) = \ldots = \rho(z_n, w)$$

Demonstração: Seja $z_1, z_2 \in \partial D_G(w)$ tais que $\exists h \in G$ tal que $h(z_1) = z_2$. Considere o segmento de geodésica $[w, z_1)$ temos que:

$$[w, z_1) \subset D_G(w) \Rightarrow h([w, z_1)) \subset h(D_G(w))$$

Agora, $h([w, z_1)) = [h(w), z_2) \subset h(D_G(w)) = D_G(h(w))$, de modo que $z_2 \in \partial D_G(w) \cap \partial D_G(w)$, de modo que:

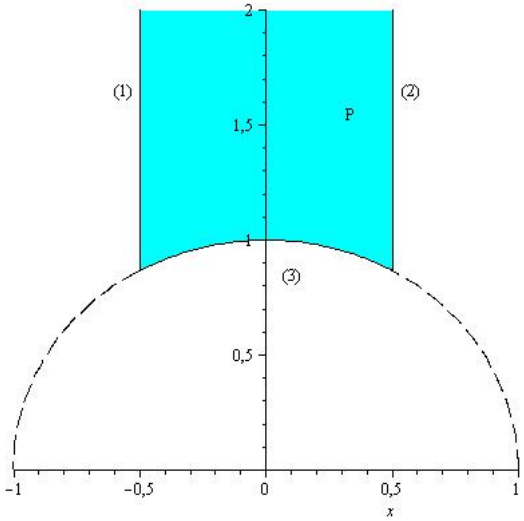
$$\rho(z_2, w) \leq \rho(z_2, g_1(w)) \ \forall g_1 \in G$$
$$\rho(z_2, h(w)) \leq \rho(z_2, g_2(h(w))) \ \forall g_2 \in G$$

Tomando então $g_1 = h$ e $g_2 = h^{-1}$ temos que:

$$\left.\begin{array}{ll} \rho(z_2, w) & \leq \rho(z_2, h(w)) \\ \rho(z_2, h(w)) & \leq \rho(z_2, w) \end{array}\right\} \Rightarrow \rho(z_2, w) = \rho(z_2, h(w))$$
$$\rho(z_2, w) = \rho(z_2, h(w)) = \rho(h^{-1}(z_2), h^{-1}(h(w))) = \rho(z_1, w).$$

Temos portanto o resultado. □

Vamos agora ver um exemplo concreto de polígono de Dirichlet, o polígono $D_\Gamma(w)$, onde $w = iv$ e v é um real positivo qualquer. Para simplificar a notação, iremos denotar $D_\Gamma(w)$ por D e $L_g(w)$, $H_g(w)$ por L_g e H_g respectivamente. Mostraremos que o polígono P a seguir é D.



Vamos mostrar que os lados de P, (1)=$\{z = -1/2 + iy \in H^2; y \in \mathbb{R}\}$, (2)=$\{z = 1/2 + iy \in H^2; y \in \mathbb{R}\}$ e (3)=$\{z = 1/2 + iy \in H^2; x, y \in \mathbb{R} \text{ e } x^2 + y^2 = 1\}$ estão contidos em L_s,$L_{s^{-1}}$ e L_u respectivamente, onde $s(z)= z + 1$, $u(z)= \frac{-1}{z}$. Para isso, observe que $\tanh(\frac{1}{2}\rho(z, w)) = \left|\frac{z - w}{z - \bar{w}}\right|$. De modo que, dado $g \in \Gamma$ temos que $\rho(z, w) = \rho(z, g(w)) \Leftrightarrow \left|\frac{z - w}{z - \bar{w}}\right| = \left|\frac{z - g(w)}{z - \bar{g(w)}}\right|$

Vamos mostrar que $(1) \subset L_s$.Temos que se z está em (1), $z = it - 1/2$, para algum $t > 0$.

Temos que:

$$\begin{aligned} z \in L_s \Leftrightarrow & \left|\frac{z-w}{z-\bar{w}}\right| = \left|\frac{z-s(w)}{z-s(\bar{w})}\right| \\ \Leftrightarrow & \left|\frac{i(t-v)-1/2}{i(t+v)-1/2}\right| = \left|\frac{i(t-v)-1/2+1}{i(t+v)-1/2+1}\right| = \left|\frac{i(t-v)+1/2}{i(t+v)+1/2}\right| \\ \Leftrightarrow & \frac{\sqrt{1/4+(v-t)^2}}{\sqrt{1/4+(v+t)^2}} = \frac{\sqrt{1/4+(v-t)^2}}{\sqrt{1/4+(v+t)^2}} \end{aligned}$$

De onde concluímos que $(1) \subset L_s$
A demonstração de $(2) \subset L_{s^{-1}}$ é totalmente análoga à de $(1) \subset L_s$.

Temos que se $z \in (3)$, então $|z| = 1$ ou de modo equivalente, $z = \cos t + i \sin t$, assim:

$$\begin{aligned} |z-w| &= |\cos t + i(\sin t - v)| \\ |z-\bar{w}| &= |\cos t + i(\sin t + v)|, \end{aligned}$$

de modo que:

$$\begin{aligned} |z+iv|^2 &= \cos^2(t) + \sin^2(t) + 2iv\sin(t) + v^2 \\ &= 1 + 2iv\sin(t) + v^2 \\ |z-iv|^2 &= \cos^2(t) + \sin^2(t) - 2iv\sin(t) + v^2 \\ &= 1 - 2iv\sin(t) + v^2 \end{aligned}$$

Agora, temos que $z \in L_u \Leftrightarrow \left|\frac{z-w}{z-\bar{w}}\right| = \left|\frac{z-u(w)}{z-\bar{u}(w)}\right|$:

$$\begin{aligned} \frac{|z-iv|^2}{|z+iv|^2} = \frac{1-2iv\sin(t)+v^2}{1+2iv\sin(t)+v^2} = \\ \frac{1/v^2+1-2i\sin(t)/v}{1/v^2+1+2i\sin(t)/v} = \frac{|z-u(iv)|^2}{|z+u(iv)|^2} \end{aligned}$$

De onde concluímos que $z \in L_u \Rightarrow (3) \subset L_u$

Assim, concluímos que os lados de P são segmentos de $L_{s^{-1}}$, L_s e L_u, portanto temos que $D \subset P$. Suponha agora por absurdo que $D \neq P$.

Tome $w \in P - \widetilde{D}$. D é um polígono fundamental para Γ, de modo que existem $h \in \Gamma$ e $z \in \widetilde{D}$ tais que $h(z) = w$, onde $h(z) = \frac{az+b}{cz+d}$, onde a, b, c e d pertencem a $\mathbb{Z}$ e $ad - bc = 1$.
Temos que:

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

Como $(|c| - |d|)^2 + |cd|$ é um inteiro, temos que $(|c| - |d|)^2 + |cd| \geq 1$ de onde concluímos que $|cz + d| > 1$.
Então:

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

Podemos usar esse mesmo argumento trocando z e h por $h(z)$ e h^{-1}, de modo que Im[$h(z)$]>Im[z]>Im[$h($ absurdo. Então, concluímos que $D = P$.

Observe que isto nos dá uma demonstração geométrica de quem são os geradores de Γ através do Teorema 3.3.2. Temos que os lados de P são L_u, L_s e $L_{s^{-1}}$, de modo que o conjunto G^* associado a P é o conjunto $\{u, s, s^{-1}\}$. Como G^* gera Γ, temos então que Γ é gerado por u e s.

Apêndice A

Transformações de Möbius

A.1 O Grupo das transformações de Möbius

O objeto de estudo deste trabalho, o Grupo Modular Clássico, é parte de um grupo muito maior, o grupo das Transformações de Möbius, que denotaremos por $\mathcal{M}$. Nesta seção iremos falar um pouco a respeito deste grupo.

Definição A.1.1 *O grupo das transformações de Möbius $\mathcal{M}$ é o grupo formado pelas aplicações da forma:*

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

Onde $ad - bc \neq 0$ e $a, b, c, d \in \mathbb{C}$.

De forma análoga ao que ocorre com Γ, é possível fazer uma identificação entre $\mathcal{M}$ e $\frac{GL(2,\mathbb{C})}{\{\pm Id\}}$. Essa identificação é obtida exatamente com a mesma aplicação mostrada no Capítulo 1.

Podemos dar a $\mathcal{M}$ a estrutura de um grupo topológico usando a métrica que iremos definir da seguinte maneira:

Sejam $A, B \in \mathcal{M}$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Defina a função:

$$\begin{aligned} [,] : \mathcal{M} \times \mathcal{M} &\to \mathbb{C} \\ [A, B] &= tr(AB^*) = a\bar{a'} + b\bar{b'} + c\bar{c'} + d\bar{d'} \end{aligned}$$

Temos que esta aplicação satisfaz:

$$(1)\, [A, A] \geq 0, \text{ valendo a igualdade se e somente se } A = 0$$

$$(2)\, [\lambda A_1 + \beta A_2, B] = \lambda\, [A_1, B] + \beta\, [A_2, B]$$

$$(3)\, [A, B] = \overline{[B, A]}$$

De modo que $[A, B]$ é um produto escalar, assim temos que a aplicação $\|A\| = [A, A]^{1/2} = \left(|a|^{1/2} + |b|^{1/2} + |c|^{1/2} + |d|^{1/2}\right)$ é uma norma para $\mathcal{M}$, de modo que $\|A - B\|$ é uma métrica para $\mathcal{M}$.

Terminamos essa seção definindo uma classe de subgrupos de $\mathcal{M}$, os grupos discretos:

Definição A.1.2 *Dizemos que um subgrupo G de $\mathcal{M}$ é discreto se, e somente se, o conjunto $\{A \in G; \|A\| < K\}$ for finito para todo $K > 0$.*

Entre os subgrupos discretos de $\mathcal{M}$ temos o grupo modular clássico Γ, que devido ao fato das suas entradas serem inteiros, satisfaz a definição para ser um grupo discreto.

A.2 Subgrupos descontínuos

Nesta seção iremos mostrar alguns resultados sobre uma classe de subgrupos de $\mathcal{M}$, da qual Γ faz parte, os grupos que possuem ação descontínua em H^2. Vamos começar definindo o conceito de ação descontínua em um contexto mais geral:

Definição A.2.1 *Seja X um espaço topológico e G um grupo de homeomorfismos de X em X. Dizemos que G age de forma descontínua em X se, e somente se, para todo conjunto compacto K de X tivermos:*

$$g(K) \cap K = \emptyset$$

exceto por um número finito de $g \in G$.

Podemos concluir diretamente da definição algumas propriedades sobre grupos com ação descontínua:

Teorema A.2.1 *Seja G grupo que age de forma descontínua em X. Então:*
(1) Todo subgrupo de G age de forma descontínua em X.
(2) Se θ é um homeomorfismo de X em X, temos que $\theta G \theta^{-1}$ age de forma descontínua em X.
(3) Se Y é um subconjunto de X tal que $g(Y) \subset Y$ para todo $g \in G$, temos que G age de forma descontínua em Y.
(4) Sejam $x \in X$ e $g_1, g_2, \ldots$ elementos distintos de G. Temos então que a sequencia $\{g_n(x)\}_{n\in\mathbb{N}}$ não converge.

Demonstração: Sejam H subgrupo de G e K subconjunto compacto de X. Temos que $g(K) \cap K = \emptyset$ para quase todo g em G, de modo que, como $H \subset G$, $h(K) \cap K = \emptyset$ para quase todo $h \in H$, logo vale (1).

Agora seja θ homeomorfismo de X em X, K conjunto compacto de X. Temos que $\theta^{-1}(K)$ é um conjunto compacto de X, de forma que $g(\theta^{-1}(K)) \cap \theta^{-1}(K) = \emptyset$ para quase todo g

pertencente a G, de onde concluímos que $\theta(g(\theta^{-1}(K)) \cap \theta^{-1}(K)) = \theta g(\theta^{-1}(K)) \cap (K) = \emptyset$, assim concluímos (2).

A demonstração de (3) é imediata, simplesmente observe que se K é um subconjunto compacto de Y, K é um subconjunto compacto de X.

Vamos provar (4) por contradição. Suponha por absurdo que exista $y \in X$ tal que $g_n(x) \to y$. Considere o conjunto:

$$K = \{y, x, g_1(x), g_2(x), \ldots\}$$

Temos que K é compacto, no entanto $g_n(x) \in g_n(K) \cap K \; \forall n \in \mathbb{N}$, absurdo. Assim, vale (4). □

Em relação ao grupo das transformações de Möbius, temos que os subgrupos discretos de $\mathcal{M}$ possuem ação descontínua em H^2[1]. Temos como consequência deste fato que Γ e seus subgrupos possuem ação descontínua em H^2, de modo que o teorema acima é valido tomando $X = H^2$ e $G = \Gamma$.

Finalizamos com a observação que toda teoria do Capítulo 3 pode ser generalizada para grupos com ação descontínua em H^2 sem nenhuma alteração, pois a única propriedade utilizada de Γ é justamente a propriedade de Γ ter uma ação descontínua em H^2.

[1] A demonstração deste fato foge do escopo deste trabalho.

Referências Bibliográficas

[1] BEARDON, A. F. *The geometry of discrete groups*. New York: Springer-Verlag, 1983.

[2] NEWMAN, M. *Intregal matrices*. New York: Academic Press, 1972.

[3] SCHENKMAN, E. *Group theory*. New York: Van Nostrand Reinhold, 1965.

[4] KUROSH, A. G. *The theory of groups*. Volume I,II. New York: Chelsea Publishing Company, 1955.

[5] WILHELM, M.; KARRASS, A.; SOLITAR, D. *Combinatorial group theory*. presentation of groups in terms of generators and relations. New York: John Wiley & Sons, Inc, 1966.

[6] MCQUILIAN, D. L. *Classification of normal congruence subgroups of the modular group* American Journal of Mathematics. Washington, Vol.87 No. 2 p.285-296, 1965.

[7] NEWMAN, M. *Classification of normal subgroups of the modular group*. Transactions of the American Mathematical Society. Washington, Vol. 126, No. 2, p. 267-277, 1967.